Logius
DigiD
High Level Design

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR	WIJZIGINGEN
PI3-S4	13-08-2020	10.2e	Alle wijzigingen geaccepteerd en document historie geschoond van voorgaande PI regels
PI1-S3	08-02-2021	10.2 e	Wijzigingen geaccepteerd, namen bijgewerkt, SEC classificatie bijgewerkt, copyright bijgewerkt.

REVIEW EN GOEDKEURING

BEDRIJF	NAAM	DATUM	PARAAF
Capgemini	10.2e		
Capgemini	10.2e		
Capgemini	10.2e		
Logius	10.2e	26-02-2019	
Logius	10.2e	26-02-2019	
Logius	10.2e	26-02-2019	

DISTRIBUTIE

BEDRIJF	NAAM	VERSIE-NUMMER	MEDIA	ACTIE
Logius	Logius ART A&M	laatste	Sharepoint	
Capgemini	DigiD teams	laatste	Sharepoint	

OPSLAG

LOCATIE	TOEGANG	ADMINISTRATEUR
Sharepoint 90-External - 40 - Architectuur DigiD 5	Logius	
Sharepoint 02-Services-01-01-02-Architecture	Capgemini	

Inhoudsopgave

1 Inleiding

1.1 Doel van dit Document

Dit document beschrijft de high level infrastructuur architectuur van de DigiD voorziening op een conceptueel en logisch niveau. Het omvat de requirements en de uitgangspunten voor het infrastructuur ontwerp.

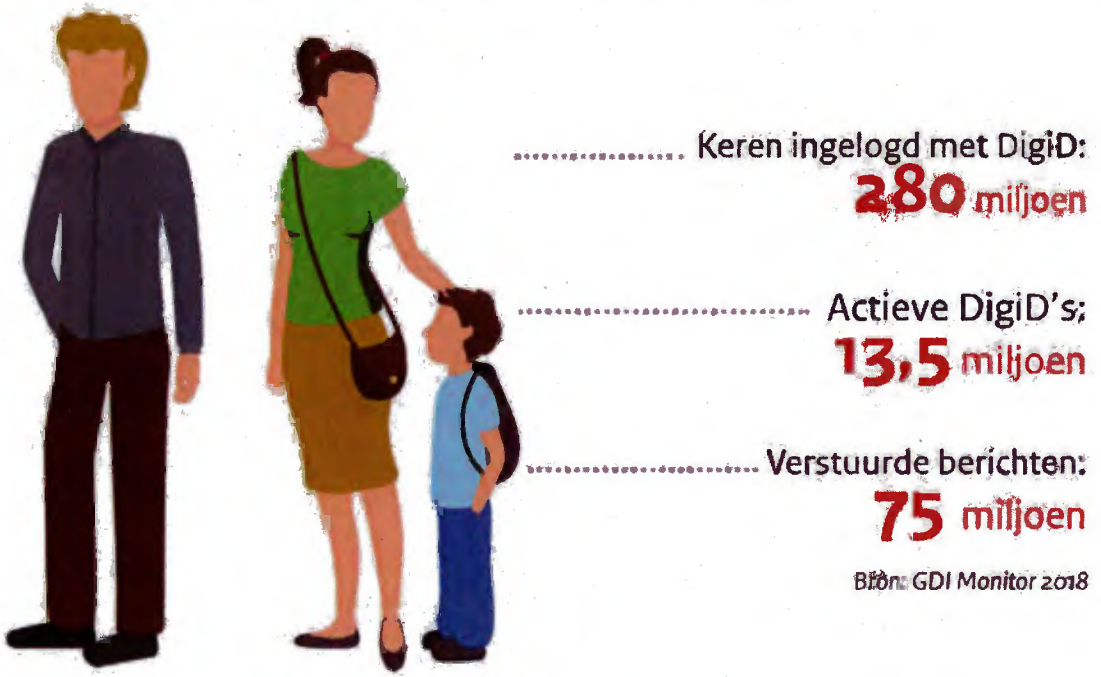
1.2 Doelgroep

Dit document is bedoeld voor Architecten en Applicatie beheerders van alle betrokken partijen. Het is een leidraad voor de systeem- en applicatiearchitecten van Capgemini en Logius.

2 Scope Beheer en Onderhoud

2.1 DigiD

DigiD is een centrale authenticatiedienst voor e-processen van Nederlandse overheidsorganisaties. Eind 2018 telt DigiD meer dan 600 afnemers (gemeenten, provincies, belastingdienst, UWV, IBG etc.) en ongeveer 13.500.000 Burgers die via de voornoemde afnemers zich bij DigiD authenticeren.



Bovenstaande figuur komt uit het rapport "NL DIGIbeter - Agenda Digitale Overheid"

Dit rapport beschrijft ook dat de strategie voor de komende jaren is,

- om de groep rechthebbenden op DigiD te verbreden en
- ervoor te zorgen dat meer mensen DigiD op het betrouwbaarheidsniveau 'substantieel' gaan gebruiken.
- Ook wordt DigiD op betrouwbaarheidsniveau 'hoog' aangeboden.
- Daarnaast wordt gewerkt aan het toelaten van een of meer private eID middelen en
- wordt het mogelijk dat ook eID middelen uit andere EU lidstaten in Nederland gebruikt kunnen worden. Dit betekent dat er dan naast DigiD ook alternatieve inlogmiddelen zijn.

DigiD 5 is de huidige versie van DigiD. Sinds versie 5 is DigiD in beheer bij Capgemini en is deze voorziening gehost op het EASI Platform in de ODC's AM2 en AM3.

2.2 Historie

Vanaf 1 oktober 2016 is Capgemini verantwoordelijk voor het applicatiebeheer en doorontwikkeling van de DigiD applicatie. In de huidige situatie is hosting en infrastructuurbeheer bij het Overheidsdatacenter (ODC) ondergebracht, dit is het EASI platform dat door Logius Managed Services wordt afgenomen van Equinix.

Capgemini is verantwoordelijk voor beheer en onderhoud en stuurt operationeel 10.1c 10.1c aan.

Doelstellingen bij de aanbesteding aan Capgemini was onder meer om een splitsing tussen het beheer van de Applicatie en het beheer van de infrastructuur te realiseren; dit door middel van het migreren van de DigiD-applicatie naar de generieke Infrastructuur van Logius, het EASI-platform.

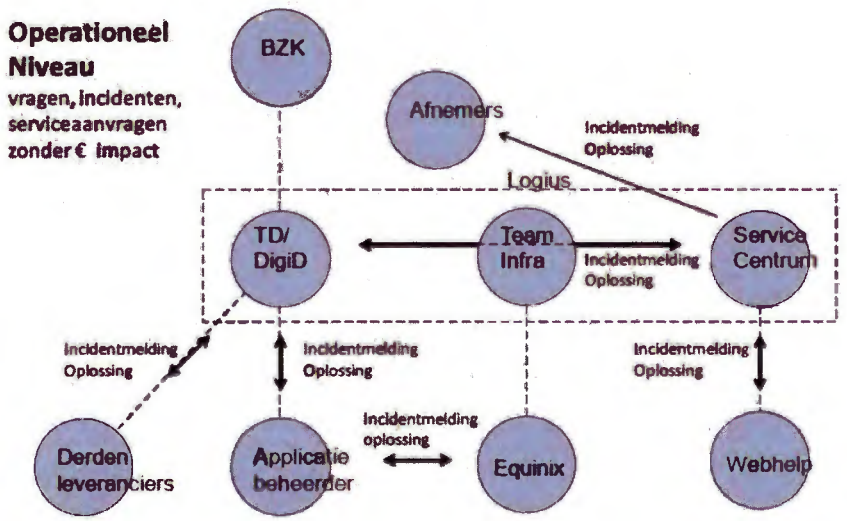
2.3 Beheer en onderhoud

Capgemini heeft de volgende twee taken:

- applicatiebeheer en doorontwikkeling(onderhoud, testen, release management);
- service Integrator (aansturing operationeel beheer).

Cruciaal bij de uitvoering van applicatiebeheer en doorontwikkeling van DigiD is het blijvend voldoen aan de voor DigiD geldende normenkaders. Hiervoor bestaat niet alleen vanuit Logius, maar tevens vanuit de politiek en samenleving veel aandacht.

2.4 Partijen



Figuur 1 Betrokken Partijen

De volgende partijen (opdrachtgever, regievoering, afnemers en leveranciers) zijn te onderscheiden:

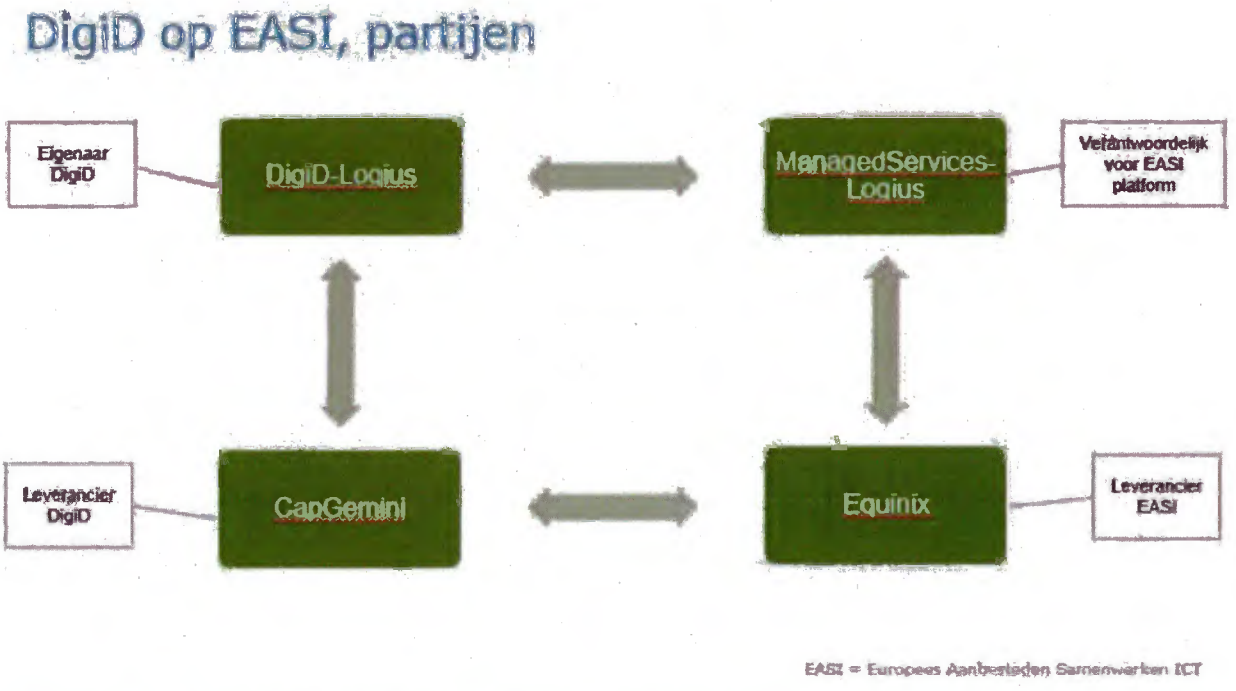
- BZK: beleidsopdrachtgever;
- Afnemers: Belastingdienst, UWV, VNG (gemeenten), SVB, Zorgverzekeraars, etc.;
- Logius: regievoering[1], functioneel beheer en service desk (2e lijns);

[1] Regievoering omvat: visieontwikkeling, architectuur, service- en productmanagement, contract en demand management, informatiebeveiliging, normkaders, auditing, planning doorontwikkeling, tactisch ketenbeheer, etc.

- Logius TD: eindverantwoordelijk en aanspreekpunt voor de klant, ketenregisseur, operationele aansturing van de Service Integrator;
- Logius I&S: verantwoordelijk voor infrastructuur en servicecentrum van alle Logius voorzieningen.
- Capgemini, applicatiebeheer dienstverlener: onderhoud[2], testen, release management en Service Integrator (aansturing operationeel beheer); 10.1c
10.1c
- Equinix: technisch beheer 10.1c en onderhoud van de infrastructuur;
- SSC-ICT Haaglanden: technisch beheer en onderhoud van de Kantoor Automatisering (relevant voor het beheer van de applicatie);
- Derden leveranciers, 10.1c
10.1c

2.4.1 Logius

DigiD wordt voor de overheid beheerd door 'Logius', dit is de dienst digitale overheid. Logius is onderdeel van het ministerie van Binnenlandse Zaken. Zie voor meer informatie https://www.logius.nl/over-logius/.



Logius is hierbij de eigenaar van de voorziening DigiD, maar is ook verantwoordelijk voor het EASI Platform. Intern Logius zijn dit twee geschieden afdelingen. Capgemini is de leverancier van de voorziening DigiD. Equinix is de leverancier van het EASI Platform.

Tussen Capgemini en Equinix 10.1c

[2]Onderhoud omvat:
- preventief onderhoud: het voorkomen van fouten;
- correctief onderhoud: bugfixing;
- adaptief onderhoud: functionele en technische verbeteringen (=doorontwikkeling);
- perfectief onderhoud: verbetering van de dienstverlening.

2.4.2 Equinix

Leverancier van het EASI platform 10.1c

2.4.3 Capgemini

Capgemini is als Service Integrator primair verantwoordelijk voor de operationele aansturing van andere externe dienstverleners met betrekking tot de Voorziening DigiD, met andere woorden, het initiatief om afspraken met de andere betrokken leveranciers te maken en te bewaken, teneinde de gehele keten van dienstverleners rond de Voorziening DigiD, in operationele zin goed te laten functioneren, berust bij Capgemini. Daarnaast is Capgemini ook de Applicatie Beheerder van de applicaties van de voorziening.

3 Ontwerp input

Deze paragraaf beschrijft de input van ontwerp; de business requirements aan de applicatie, en uitgangspunten en aannames.

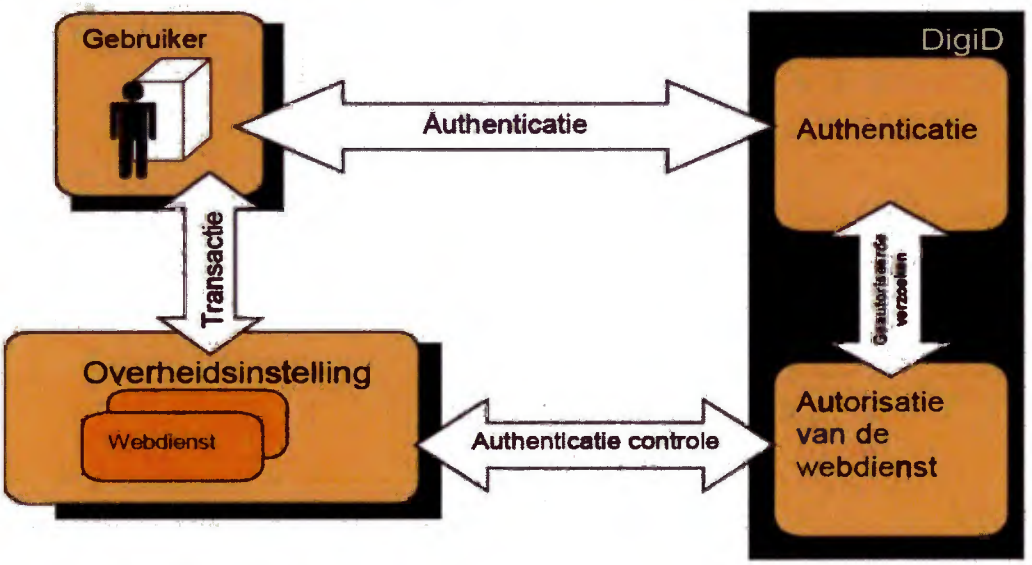
3.1 Applicatie beschrijving

DigiD staat voor Digitale Identiteit. Het biedt een centrale authenticatie (SSO) voor toegang tot Internet websites van onder andere Overheid en Zorg.

De dienst is gebaseerd op SAML (Security Assertion Markup Language). Bij SAML zijn er 3 rollen:

- de gebruiker,
- de Identity provider (IDP) en
- de service provider (SP).

Als een gebruiker wil inloggen bij een service provider (bijvoorbeeld Belastingdienst, waterschap, zorginstelling) dan routeert die partij zijn authenticatie verzoek naar de Identity provider, die na succesvolle authenticatie een SAML token aan de Internet sessie van de gebruiker toevoegt. Dit token dient als tijdelijke sleutel tot diensten bij de service provider.



Figuur 2 Positionering DigiD

3.2 Functional Requirements

Aan de applicatie worden een aantal business requirements gesteld, deze staan beschreven in de Use Case beschrijvingen die worden beheerd door Logius.

3.2.1 Actoren

De volgende tabel geeft een overzicht van Actoren waarvoor de Use Cases zijn opgesteld.

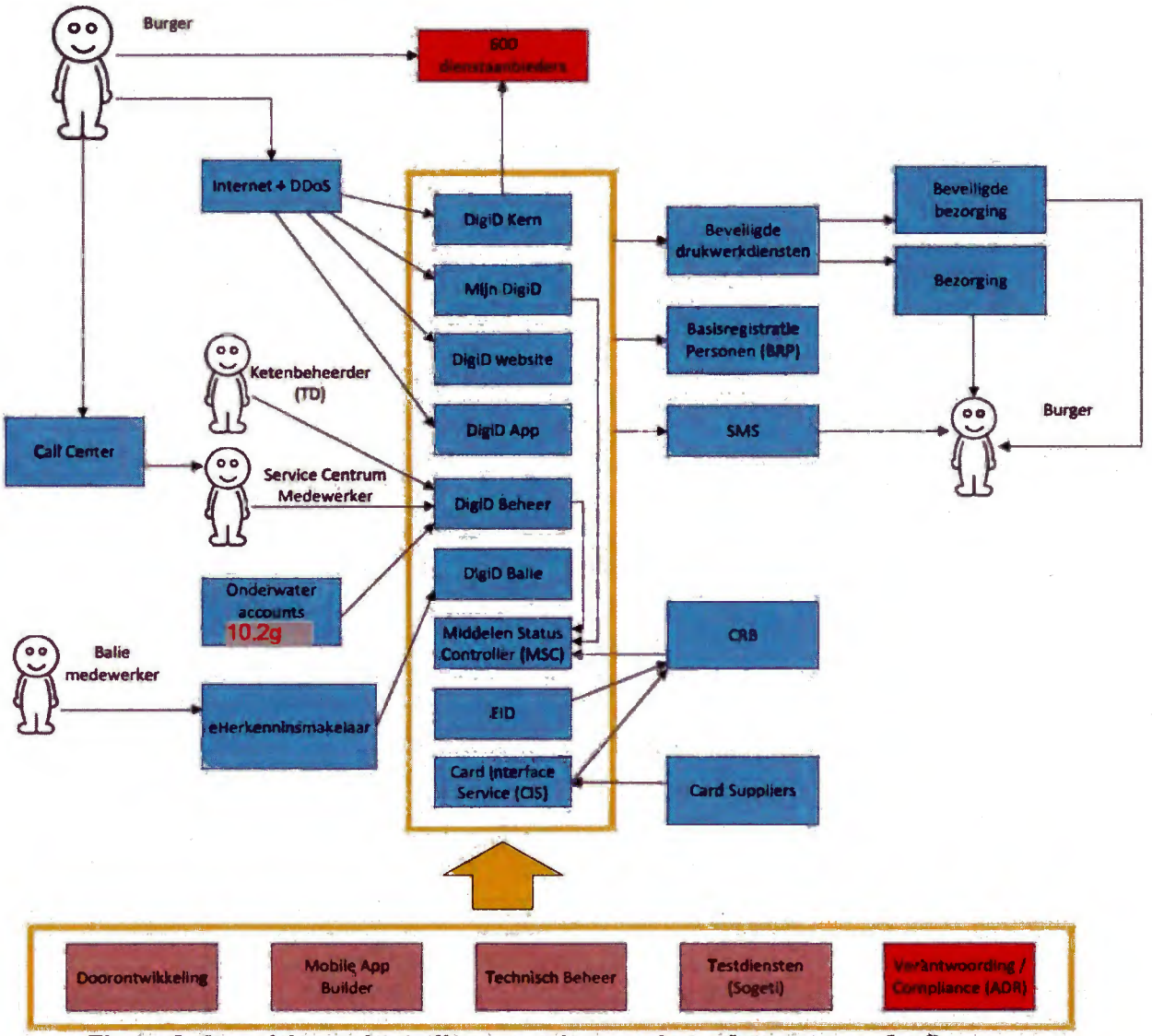
Personen	

Eindgebruiker	Een eindgebruiker is een burger, die via Internet met een browser gebruik maakt van de DigiD Applicatie of middels een mobiel apparaat gebruik maakt van de DigiD App.
Beheerder	Een beheerder is een werknemer van de Service Organisatie (SO) van Logius, of een leverancier van SO, die operationeel en technisch beheer uitvoert rond DigiD. Een voorbeeld van een beheerder is een medewerker van Servicebeheer die webdiensten aansluit, een medewerker van de Servicedesk die een probleem met een DigiD Account onderzoekt. Er bestaat ook een speciale klasse beheerders, de superbeheerder, die bevoegdheden aan beheerders mag toekennen.
Baliemedewerkers	Baliemedewerkers maken gebruik van eHerkenning voor authenticatie en autorisatie van de DigiD Balie applicatie. De autorisatie en authenticatie is voorwaardelijk voor de toegang tot de baliefunctie.
Niet-personen	
Tijd (chronos)	Chronos is een actor die na verloop van tijd bepaalde handelingen verricht met het systeem. Chronos wordt gebruikt om interacties van het systeem met eindgebruikers te specificeren, die automatisch, na een bepaald tijdsverloop, door het systeem zelf worden gestart.
Webdienst	Een webdienst is een verzameling van (één of meerdere) webpagina's van een dienstverlener (ook wel afnemer genoemd). De webpagina's maken gebruik van DigiD voor de authenticatie van eindgebruikers. In bepaalde uitzonderlijke gevallen kunnen eindgebruikers via een webdienst (10.2g [redacted]) een DigiD Account aanvragen.

Tabel 1: Actoren Use Cases

De **eindgebruiker** moet in staat zijn een Account aan te vragen, Activeren en vervolgens in staat zijn DigiD te gebruiken als authenticatie middel bij een **webdienst**. Daarnaast moet hij in staat zijn, zijn gegevens te beheren.

3.2.1.1 Leveranciers, afnemers en gebruikers



Figuur 3: Overzicht van koppelingen met leveranciers, afnemers en gebruikers

Bovenstaande afbeelding geeft een overzicht van de koppelingen met Leveranciers, afnemers en gebruikers. De actoren en applicaties zijn hierin weergegeven.

3.3 Non Functional Requirements

Voor het ontwerp worden een aantal 'non functional requirements' (kwaliteitseisen) gehanteerd:

- PAP eisen
- Dienstverlening eisen
- IB eisen
- Uitrol eisen

- Migratie eisen

3.3.1 Product Acceptatie eisen

De niet-functionele eisen zijn opgenomen in de Product Acceptance Plan (PAP) van DigiD.

De volgende eisen uit de PAP zijn van invloed geweest op de infrastructuur architectuur:

#	Category	Criterium
ACC2.1.1	Beveiliging	Normenkaders
ACC2.1.2	Beveiliging	Lekken van informatie
ACC2.2.1	Beveiliging	Aanvallen
ACC2.2.2	Beveiliging	Accountability
ACC2.2.3	Beveiliging	Zwakheden
ACC2.3.1	Beveiliging	Persoonsgegevens
ACC2.4.1	Beveiliging	PKI Overheid
ACC2.5.1	Beveiliging	DNSSEC
ACC2.5.2	Beveiliging	Cookies
ACC2.5.4	Beveiliging	Ingetrokken certificaten
ACC4.1.1	Connectiviteit	IPv4 en IPv6
ACC4.1.3	Connectiviteit	Productie omgevingen
ACC5.1.1	Continuiteit	Backup- en restorefaciliteiten
ACC5.2.2	Continuiteit	Degradatiemogelijkheden
ACC5.2.4	Continuiteit	Redundantie
ACC6.1.1	Controleerbaarheid	Leveranciers rapportages
ACC7.1.1	Flexibiliteit	Lineair schaalbaar
ACC10.2.1	Herbruikbaarheid	Account beheer
ACC11.1.1	Infrastructuur	Loadbalancing
ACC11.1.2	Infrastructuur	Gemeenschappelijk dienstenplatform
ACC11.1.3	Infrastructuur	Acceptatie omgevingen - ACC1
ACC11.1.4	Infrastructuur	Acceptatie omgevingen - ACC2, ACC3 en ACC4
ACC11.1.5	Infrastructuur	Ketentest omgevingen
ACC14.2.10	Performance	RDA aanvragen
ACC15.1.1	Standaarden	Pas toe of leg uit
ACC16.1.3	Testbaarheid	Performance test
ACC26.18	Documentatie	Architectuur documentatie

3.3.2 Dienstverlening eisen

De dienstverlening staat beschreven in het Service Niveau Overeenkomst (SNO) en in het Dossier Afspraken en Procedures (DAP).

- SNO – Het wat – "SNO ICT DigiD-X"
- DAP – Het hoe - "Dossier Afspraken en Procedures DigiD"

De SNO afspraken van DigiD met afnemers is opgenomen in het document:

- Klant SNO – "Serviceniveauovereenkomst voor klanten DigiD"

Verder zijn er SNO afspraken gemaakt door Logius met RvIG (BRP) en RDW (CRB).

Deze eisen hebben invloed gehad op het ontwerp van de infrastructuur. Onder andere

- Goud vanwege hoge beschikbaarheidseis (zie DAP)
- Restoretijden hebben mede bepaald hoe we de backup hebben ingericht (online, onsite, offsite)
- Redundantie vanwege hoge beschikbaarheid

3.3.3 Informatiebeveiligingseisen

Informatiebeveiligingseisen zijn te vinden in het DigiD informatiebeveiligingsplan plus bijlagen.

- Informatiebeveiligingsplan DigiD
- Informatiebeveiligingsbeleid DigiD
- Confrontatiematrix DigiD

Tevens dient er ook rekening gehouden te worden met een aantal normen en kaders:

- BIR - Baseline Informatiebeveiliging Rijksdienst (BIR:2012, stand oktober 2016)
- BIR – Operationele handreiking Informatiebeveiliging (bron)
- DigiD ICT beveiligingsassessments
- Logius Normenkader (in casu het Studierapport Normen voor beheersing uitbestede ICT-beheerprocessen, het NOREA rapport)
- NCSC - Nationaal Cyber Security Centrum (Versie 2, 31-08-2015)
- VIR – Voorschrift Informatiebeveiliging Rijksdienst-Bijzondere informatie (VIR 2009/01/01)

De volgende BIR eisen zijn van invloed geweest op de infrastructuur architectuur:

BIR Eis	Omschrijving
A.10.1.2	Wijzigingsbeheer
A.10.4.1	Maatregelen tegen virussen
A.10.5.1	Reservekopieën maken (backups)
A.10.6.2	Beveiliging van netwerkdiensten
A.10.10.1	Aanmaken auditlogbestanden
A.10.10.2	Controle van systeemgebruik
A.10.10.3	Bescherming van informatie in logbestanden
A.10.10.4	Logbestanden van administrators en operators
A.10.10.5	Registratie van storingen
A.11.2.2	Beheer van speciale bevoegdheden
A.11.2.3	Beheer van gebruikerswachtwoorden
A.11.4.3	Identificatie van netwerkapparatuur
A.11.4.5	Scheiding van netwerken
A.11.5.1	Beveiligde inlogprocedures

A.11.5.4	Gebruik van systeemhulpmiddelen
A.11.5.5	Time-out van sessies
A.12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen
A.12.3.2	Sleutelbeheer
A.12.4.3	Toegangsbeheer voor broncode van programmatuur
A.15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen

3.3.4 Uitrol eisen

De volgende uitrol eisen zijn van toepassing:

- Voor het uitrollen van de OTAP omgevingen geldt dat er met O begonnen wordt en dat P de laatste omgeving is.
- Daarbij zijn de omgevingen A2 en PP2 gereserveerd voor spoed patches.
- Twee weken voor uitrol op productie wordt uitgerold op de PP1 voor afnemer acceptatie testen
- De A3 en A4 omgeving zijn bedoeld voor het testen van geplande functionele wijzigingen.
- De A3 wordt gebruikt voor security en pentesten
- De A5 is voor ketentesten (o.a. voor DigiD Hoog)
- De A6 is voor projecten, zoals 10.1c
- De A1 omgeving is productie-like qua capaciteit, configuratie en beschikbaarheid en is daarmee geschikt voor performance testen.

3.4 Overige uitgangspunten

In dit HLD wordt uitgegaan van de volgende uitgangspunten:

S1 : *Applicatie management*
Capgemini is verantwoordelijk voor applicatie beheer en operationeel beheer.

S2 : *Housing en Hosting*
10.1c

S3 : *Connectiviteit*
Connectiviteit is verantwoordelijkheid van 10.1c in combinatie met overheidsnetwerken

S4 : *Licenties*
Licenties voor gebruikte producten zijn eigendom van Logius. Het betreft hier alleen licenties voor Open Source producten.

S5 : *Versleuteling intern verkeer*
10.2g

S6 : *VPC*
De dienst VPC wordt gebruikt voor Omgeving scheiding en voor het centraal plaatsen van functies met een zelfde doel voor meerdere omgevingen of voorzieningen. Nieuwe te ontwikkelen diensten geschikt voor Logiusbrede inzet worden in een zelfstandige VPC geplaatst.

4 Ontwerp

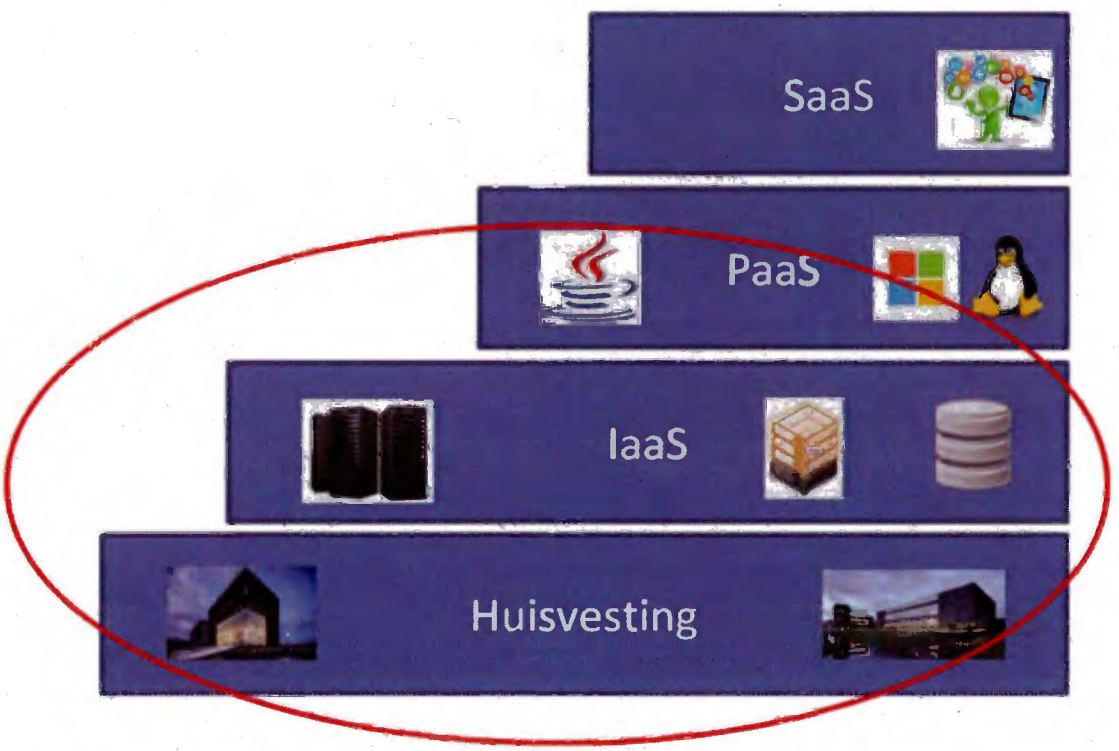
Dit hoofdstuk beschrijft het infrastructuur ontwerp van de voorziening DigiD 5 op een hoog abstractie niveau.

4.1 EASI platform

Zoals al in hoofdstuk 2 is aangegeven wordt in de infrastructuur gebruik gemaakt van de producten en diensten van het Managed Services platform (EASI).

Hiermee wordt de volgende PAP eis afgedekt.

ACC11.1.2	Infrastructuur	Gemeenschappelijk dienstenplatform	DigiD is zoveel mogelijk opgebouwd door middel van generieke diensten zoals aangeboden binnen de EASI/managed services product dienstencatalogus (PDC).



De diensten van dit platform bevinden zich, zoals aangegeven in het rode gebied in de bovenstaande figuur, op het gebied van:

- Huisvesting
- Infrastructure As A Service
- Platform As A Service

Huisvesting houdt o.a. in de datacenter zelf (locatie), kasten en bijhorende zaken zoals stroom,koeling etc.

Bij Infrastructure As A Service moet men denken aan virtuele machines, netwerk, firewalls etc.

Bij Platform As A Service gaat het o.a. om het aanbieden van het besturingssysteem (OS).

Software As A Service wordt niet geleverd binnen het EASI Platform.

4.1.1 Platform producten en diensten

Hieronder vallen de volgende zaken die DigiD afneemt van het Platform:

Service	Part	Beschrijving
Mail	Centrale Toegangslaag	Mailserver PDC Image: Mail relay domein beschermd, Mail relay
Firewall (Reverse Proxy)	Centrale Toegangslaag	Firewall (Reverse Proxy)
Forward Proxy	Centrale Toegangslaag	Forward Proxy
DDOS Wasstraat	Centrale Toegangslaag	DDOS Wasstraat
DigiNetwerk	Centrale Toegangslaag	DigiNetwerk (GemNet) toegang en IP reeks
Image	Machine	Images kunnen gebaseerd worden op een beperkte set geharde OS images ("Golden Images") die vanuit Managed Services beschikbaar worden gesteld, of door eigen Images ("Custom Image"). *NB: De dienst Image is onderdeel van de dienst Machine, maar kan niet apart worden besteld.*
Internet	Centrale Toegangslaag	Internet toegang en IP reeks
SIEM IDS/IPS	Securitylogging en –monitoring centraal	SIEM IDS/IPS
NTP	Centrale Voorzieningen	NTP
DNS	Centrale Voorzieningen	DNS
Backup/Restore	Centrale Voorzieningen	Backup/Restore
Authenticatie (LDAP)	Centrale Voorzieningen	Authenticatie (LDAP)
VPC	VPC's	Elke omgeving is een VPC (zie ook VPC's). Daarnaast zijn er twee Beheer VPC's een VPC met ondersteunende servers voor test en omtwikkling en een aparte VPC voor Logging Monitoring en Backup functionaliteit.
Appliance		Kast met stroom tbv de loadbalancers
Schijf	Onderdeel van Machine of los	Bij virtuele machines is dit vanuit de hypervisor op Storage Area Network (SAN) geïmplementeerd maar kan ook beschikken over Network Attacted Storage (NAS-opslag). NAS wordt over het algemeen gekozen als het opslagmedium gedeeld moet worden door meerdere Machines Kan als NAS aan meerdere machines gekoppeld worden

		Zie PDC voor verschillende prestatievormen (IOPS, latency)
Machine		Combinatie van Server, Schijf en Image
Hardware Geschelden Encryptie		Dienst om cryptografische bewerkingen te laten plaatsvinden op separate en fysiek beveiligde hardware (HSM's)

10.1c

4.1.2 Loadbalancer Appliance (special)

DigiD maakt gebruik van 10.1c loadbalancers. Deze was, ten tijde van de migratie, niet leverbaar als product binnen het EASI platform.

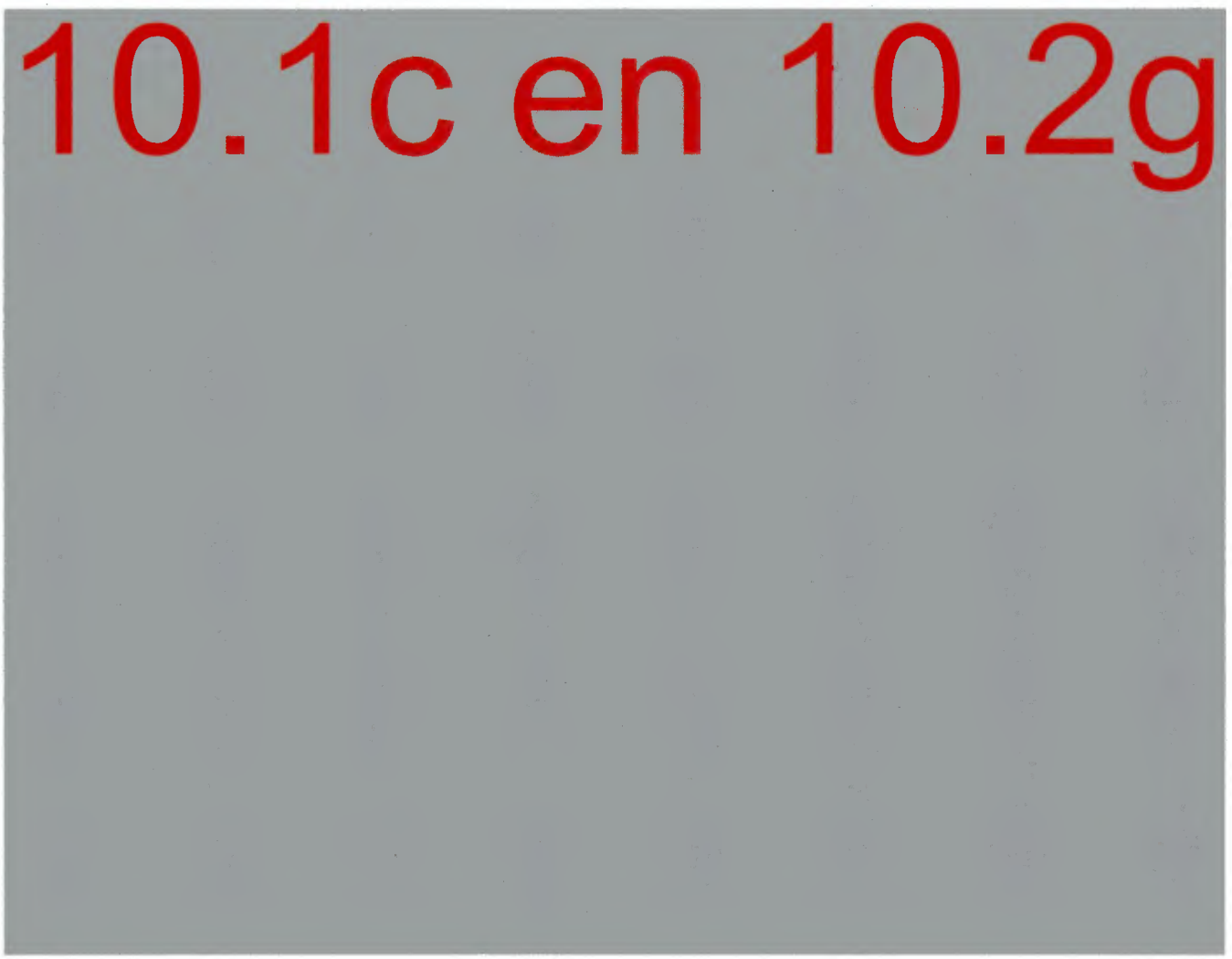
Om deze fysieke apparaten toch beschikbaar te maken binnen de virtuele omgevingen, is deze middels de dienst Appliance toegankelijk gemaakt.

10.1c en 10.2g

10.1c en 10.2g

4.2 Platform en Voorziening

Het EASI platform is een virtueel platform. De hosting is fysiek. Het volgende figuur uit de PDC geeft de samenhang hiervan weer.


10.1c en 10.2g

De belangrijkste onderdelen van de plaat worden in de volgende paragrafen beschreven. In het kort bevat het EASI platform:

- Een centrale toegangslaag welke toegang geeft tot DigiNetwerk en Internet.
- Een DDOS wasstraat dat voor DigiD apart te configureren is.
- Een externe firewall met o.a. IDS (Intrusion Detection System).
- De Beheer-VPC welke voor de applicatiebeheerder/leverancier de toegang biedt om de infrastructuur van de voorziening (DigiD) te beheren.
- De Applicatie-VPC's waarmee de verschillende omgevingen van de voorziening zijn opgezet. Dit is inclusief firewalls en netwerk gebaseerd op een 3-Tier model.
- 10.1c en 10.2g
- De centrale voorzieningen waarin producten staan die de voorziening afneemt van het platform. Zoals bijvoorbeeld NTP (Network Time Protocol), SIEM (Security Information and Event Management) en 2-factor authenticatie voor technische beheerders.

Het blok Infrastructuurbeheerdomein geeft componenten weer die binnen scope van de platform leverancier vallen.

Met name de gemaakte keuzes en het ontwerp van de Beheer-VPC en de Applicatie-VPC's zijn onderwerp van de documentatie van DigiD. Voor de overige zaken wordt verwezen naar de Platform documentatie.

4.2.1 Virtual Private Cloud (VPC)

Op EASI platform worden meerdere voorzieningen gehost. Denk aan voorzieningen als MijnOverheid en DigiD Machtigen.

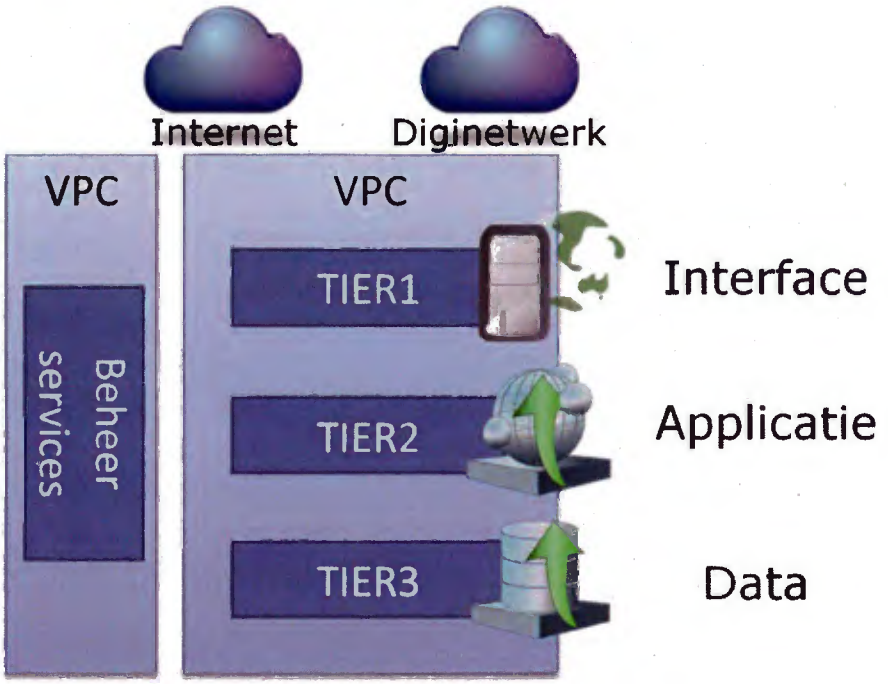
Per voorziening zijn meerdere omgevingen mogelijk. Deze worden van het platform afgenomen als de dienst VPC. Elke omgeving, OTAP, van DigiD is dus een VPC binnen het platform.

Bij DigiD is daarnaast gekozen om servers met een gezamenlijk doel voor meerdere omgevingen in een aparte VPC te plaatsen 10.2g

Een VPC is een afgeschermde virtuele omgeving. Hiermee wordt de afscheiding van productie omgevingen gewaarborgd, zoals beschreven in de volgende PAP eisen:

ACC11.1.3	Infrastructuur	Acceptatie omgevingen - A1
ACC11.1.4	Infrastructuur	Acceptatie omgevingen - A2, A3 en A4
ACC11.1.5	Infrastructuur	Ketentest omgevingen

VPC



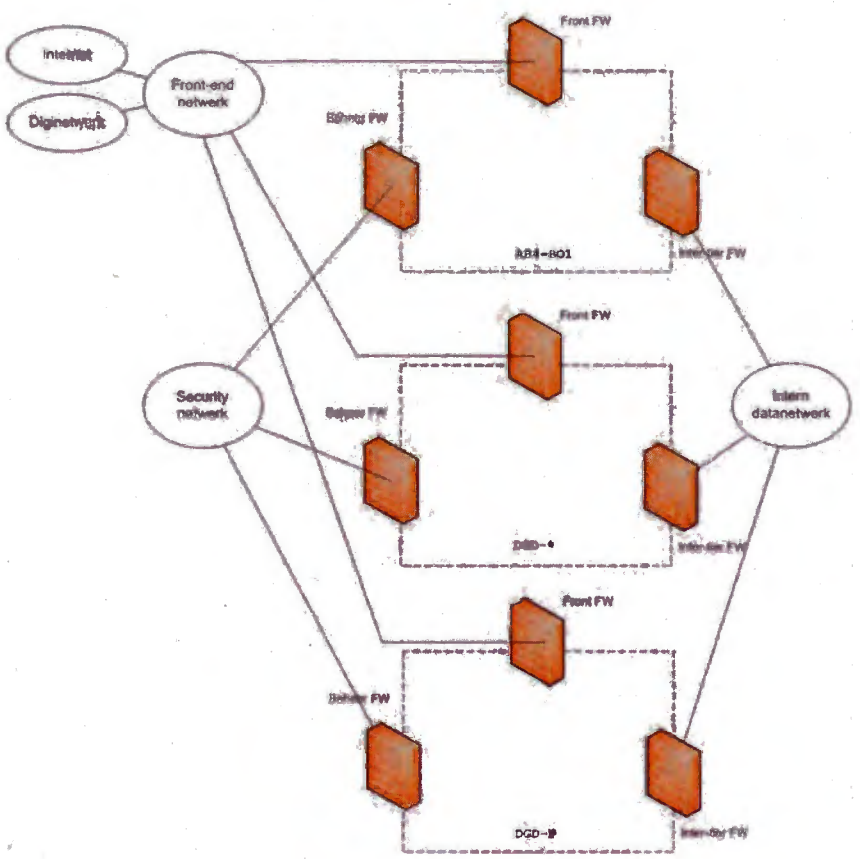
Een VPC bestaat uit drie gescheiden netwerk zones (Tiers) waarvoor dmv firewalls de verkeersstroom toegang wordt geregeld. De Firewalls zijn onderdeel van het VPC product en zijn dus in beheer bij de platform leverancier (Equinix). De beheerder van de omgeving bepaalt welke servers in de Tiers worden opgesteld en beheert deze via een apart Netwerk vanuit de Beheer Services. De VPC wordt verder beschreven in het PDC. Het beheerverkeer en het productieverkeer is hiermee dus gescheiden.

4.2.1.1 Zonering

Behalve een scheiding tussen productie en beheer onderkennen we echter meer netwerk zones. In de PDC Managed Services staat beschreven hoe de verschillende zones zijn ingericht.

We onderkennen de volgende netwerken:

- Front-End Netwerk
- Interne Datanetwerk (productie verkeer)
- Security Netwerk (beheer verkeer)
- Storage Netwerk



VPC Overzicht

Bovenstaande figuur geeft weer hoe productie- en beheer verkeer volledig gescheiden zijn geïmplementeerd. Het laat de samenhang tussen de verschillende VPC's zien en de EASI-netwerken die zorg dragen voor het datatransport tussen VPC's of VPC's en Internet/Diginetwerk.

Het storage netwerk is hier niet weergegeven, omdat dit netwerk alleen toegang geeft tot de dienst NAS Schijf.
10.2g
10.2g
Welke richtlijnen er zijn voor het toestaan van verkeersstromen door de FW's en hoe hiermee de tierscheiding binnen een VPC wordt bewaakt, staat beschreven in het document 10.2g

Geldende BIR eis

A.11.4.5	Scheiding van netwerken

4.3 Datacenters

Het EASI Platform wordt aangeboden op verschillende Overheid Data Centers (ODC). Daarnaast kunnen op een ODC diensten worden aangeboden die niet onder het EASI platform vallen.

10.2g en 10.1c

4.4 Overzicht omgevingen voorziening DigiD

10.2g en 10.1c

Voor de voorziening DigiD onderkennen we dus verschillende omgevingen. De volgende tabel geeft de omgevingen weer en of ze over twee locaties beschikbaar zijn (redundantie).

Omgeving	Beschrijving	Redundant
	Beheer VPC Capgemini	Ja
	Beheer VPC 10.1c	Ja
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
O1	Ontwikkel omgeving	Nee
T1, T2	Systeemtest 1 en 2	Nee
A1	Acceptatie 1	Ja
A2 t/m A6	Acceptatie 2 t/m 6	Nee
PP1	Pre Productie 1	Ja
PP2	Pre Productie 2	Ja
P	Productie	Ja

In de volgende paragrafen worden de DigiD VPC's nader toegelicht. 10.2g [redacted]

4.4.1 OTAP Omgevingen

De OTAP omgevingen zijn de O1, T1..2, A1..6, PP1, PP2 en P. Hierbij onderkennen we de volgende verschillen en overeenkomsten.

- De productie omgevingen zijn de enige omgevingen, waarvan de applicaties publiek beschikbaar zijn.
- PreProd1 en PreProd2 zijn functioneel identiek aan de Productie omgeving, ten behoeve van testen van Dienstaanbieders en leverancier.
- Acceptatie 1 is fysiek en functioneel identiek aan de productieomgeving, o.a. bedoeld voor representatieve load en performance testen;
- Acceptatie 2, 3, 4, 5 en 6 zijn omgevingen die functioneel identiek zijn aan de productieomgeving, maar niet redundant over de twee datacenters heen.
- Ontwikkel en test omgevingen zijn beschikbaar voor het doorontwikkel team van Capgemini. Zij zijn verantwoordelijk voor bouw en onderhoud van de DigiD 5 functionaliteit en het systeemtesten daarvan, voordat dit overgedragen wordt aan Logius voor functionele testen. De test en ontwikkelomgevingen zijn alleen beschikbaar voor Capgemini.
- De omgevingen hebben gecontroleerd toegang tot het Internet. Dit wordt geregeld door Firewall rules en reverse proxies.

4.4.2 Beheer VPC ab4-bo1

De Beheer VPC Capgemini is bedoeld voor beheertaken die verwacht worden van de leverancier. Hieronder valt o.a.

- Installatie van nieuwe componenten
- Doorvoeren configuratie aanpassingen
- Deployment van applicatie releases

Het gaat hier dus om beheertaken die onder de verantwoordelijkheid vallen van de leverancier. De Beheer VPC is specifiek van een bepaalde leverancier en bij een transitie zal een andere leverancier een andere beheer VPC toegewezen krijgen.

10.2g

In deze omgeving vinden we een EASI opstapserver (OS) van het platform om de toegang af te schermen en DigiD Beheerservers (BS) die de leverancier de tools biedt om haar beheertaken uit te voeren.

Vulnerability Scanning (VS) tools zijn door de leverancier ook vanuit deze VPC bereikbaar.

4.4.3 Beheer VPC ab4-bo2

Deze speciale (onderaannemer) Beheer VPC is opgezet om 10.1c afgeschermde toegang te geven t.b.v. van monitoring en beheer van, uitsluitend, de DigiD loadbalancers

Vanuit deze omgeving is alleen beperkte beheer toegang mogelijk tot de fysieke loadbalancer appliances in de dgd-a1 en de dgd-p VPC.

10.1c én 10.2g

Hiermee wordt het monitoring van de loadbalancers, 10.1c en 10.2g mogelijk gemaakt binnen de kaders van het EASI platform.

Omdat deze Beheer VPC op enkele punten aangepast is t.a.v. van de standaard in het EASI platform, heeft Logius goedkeuring gegeven voor de afwijkingen:

- Geen LDAP koppeling 10.1c en 10.2g
- Externe verkeersstromen naar Tier2

De afscherming 10.1c en 10.2g in een aparte VPC (VLAN), de beperkingen op de verkeerstromen en logging naar de Logserver van de voorziening zijn hiervoor als risico mitigerende maatregelen goedgekeurd.

Ontwerpbeslissing: 10.1c en 10.2g

4.4.4 Ondersteuning 10.1c en 10.2g

10.1c en 10.2g

4.4.5 Logging, Monitoring en Backup 10.1c en 10.2g

10.1c en 10.2g

Ontwerpbeslissing: 10.1c en 10.2g

Ontwerpbeslissing: 10.1c en 10.2g

Ontwerpbeslissing: 10.1c en 10.2g

4.4.6 Externe services

DigiD is afhankelijk van de volgende externe services.

Service	Toelichting
Domain Name Server	DNS wordt als dienst afgenomen van het Algemene Zaken. In de DNS staan de domeinnaam registraties van het DigiD domein
Drukwerkdiensten	10.1c is de leverancier van drukwerkdiensten. 10.1c
Basis Registratie Personen	Koppeling met de "Gemeentelijke Basis Administratie" via het GBA-V koppelvlak ten behoeve van adressering van brieven en verifieren NIK/Paspoort.
SMS	10.1c is de leverancier van SMS diensten.

eHerkenning	De baliemedewerkers worden geauthentiseerd en geautoriseerd voor de Balie applicatie middels eHerkenning. 10.1c
PKI Overheid	Certificaten zijn nodig voor de authenticatie van de verschillende services (bijvoorbeeld GBA-V services) en voor encryptie middels SSL voor communicatie met derde partijen. Deze certificaten worden besteld bij Logius. Logius is ook de leverancier van het PKI Overheid stelsel.
CRB	Centraal Rijbewijzen- en Bromfietscertificatenregister bij RDW, nodig om gegevens van een burger op te zoeken om een rijbewijs mee uit te kunnen lezen door de RDA

4.4.7 Scheiding OTA en P omgevingen

Naast de omgevingscheiding die geborgd wordt vanuit de VPC onderkennen we een afscheiding van productionele omgevingen. Namelijk de Productie (PreProd en Productie) zone en de OTA (Ontwikkel, Test, Acceptatie) zone. De scheiding in twee zones is gemaakt om zeker te zijn dat dataverkeer in één van de OTA omgevingen nooit een verstoring kan veroorzaken in het productie verkeer. De meest belangrijkste reden is om Load performance testen in de OTA omgeving mogelijk te maken, zonder dat dit het productieverkeer verstoort, maar ook vanuit het kader van IB maatregelen is deze scheiding aangebracht.

Kanttekening: Echter doordat het niet vastligt hoe servers verdeeld worden over de hypervisors blijkt deze scheiding in de praktijk geen garantie te zijn dat OTA testen geen invloed hebben op de P performance. De juiste maatregelen hiervoor zijn nog onderwerp van discussie

Met de dienst Cluster kan wel worden aangegeven dat een groep servers niet tegelijk op dezelfde hypervisor mogen draaien. Deze optie dient te worden ingezet bij clusters en multiserver configuraties, zoals Container en Applicatie Servers.

De volgende apparatuur is geïmplementeerd voor iedere zone:

- Firewall's & IDS Modules 10.1c),
- Switches 10.1c),
- Load balancers 10.1c)

De volgende componenten worden gedeeld tussen de zones:

- SMTP servers (10.1c),
  De SMTP servers hebben een relatieve lage load. Er wordt ook geen extra load verwacht bij een Load performancetest,
- DNS servers (dienst afgenomen van Algemene Zaken),
  De DNS functionaliteit kan niet gescheiden worden, aangezien alle omgevingen gebruik maken van de digid.nl DNS-zone..
- Centrale voorzieningen van het platform: LDAP, Radius, NTP en het SAN
  Deze diensten worden door het platform met hoge beschikbaarheid geleverd.
- Hypervisors
  Het ligt niet vast hoe de servers verdeeld zijn over de hypervisors, dit wordt door het platform zelf bepaald, maar het virtuele platform is een gezamenlijke component.
- SAN
  Hoewel de dienst Schijf per server te bestellen is, wordt de daadwerkelijke storage verdeeld uit een gezamenlijk SAN per datacenter.
- DigiNetwerk connectie(10.1c)
  De DigiNetwerk connectie biedt verbinding naar de GBA-V, naar CRB voor DigiD Hoog en Substantieel en ontsluit de CMS, Balie en Beheer applicatie voor de specifieke doelgroepen. Deze wordt niet

gebruikt in alle omgevingen. In diverse OTA omgevingen wordt gebruik gemaakt van Stubs gedurende testen. Ondanks dat elke omgeving zijn eigen Internet facing firewalls heeft, zijn ze gekoppeld aan dezelfde Diginetwerk routers

- Internet(10.1c)
  Ondanks dat elke omgeving zijn eigen Internet facing firewalls heeft, zijn ze gekoppeld aan dezelfde Internet routers.
- Logging Monitoring en Backup
  10.2g
- Ondersteuning
  10.2g
- Beheer toegang
  De Beheer omgeving wordt gebruikt voor toegang tot de omgevingen door geautoriseerde Capgemini beheerders/ontwikkelaars. Er is wel een scheiding gemaakt in OTA en P toegang voor het Doorontwikkelingteam en Beheerteam door de inzet van verschillende beheer- en toegangsrechten,
  10.2g
- 10.1c
  10.1c Dit is de eerste toegang tot alle omgevingen die
  10.1c en onderdeel van de Beheertoegang
- Dienst Hardware Gescheiden Encryptie
  Deze centrale voorziening levert wel een fysieke HSM per omgeving (of locatie van een redundante omgeving). Echter deze zijn geplaatst in 1 gezamenlijke VPC met een interface in twee gezamelijke private VLAN's. 10.2g

4.5 Server en Disk Sizing

De virtuele server selectie, en bijhorende schijven, voor de DigiD 5 omgeving is gebaseerd op de volgende criteria:

- Selectie servers uit de Product en diensten catalogus (PDC) vanuit het EASI Managed Services platform.
- Server gegevens aangeleverd vanuit het Consortium waarop DigiD 4 in productie was voorafgaand aan de migratie van het Consortium naar Capgemini.
- Informatie vanuit de architectuur documenten behorende bij de DigiD 4 systeemomgeving
- Als gevolg van de schaalbaarheid van de DigiD applicatie is de applicatie geschaald over meerdere applicatieservers. Dit heeft voordelen zoals mogelijke performance uitbreiding, redundante uitvoering en risico verlaging bij uitval van één server.
- Het aantal servers is gevalideerd gedurende performance load testen van de oplossing, met als resultaat het aantal servers zoals beschreven in de architectuur documentatie.

4.5.1 Plaatsing servers

De initiële omvang van DigiD 5 was gebaseerd op een theoretisch model, dat gevalideerd is gedurende load testen tijdens het migratie traject. Gebaseerd op de uitkomst van deze load testen en informatie vanuit de DigiD 4 applicatie is het aantal servers vastgesteld voor DigiD 5 op het EASI Managed Services platform.

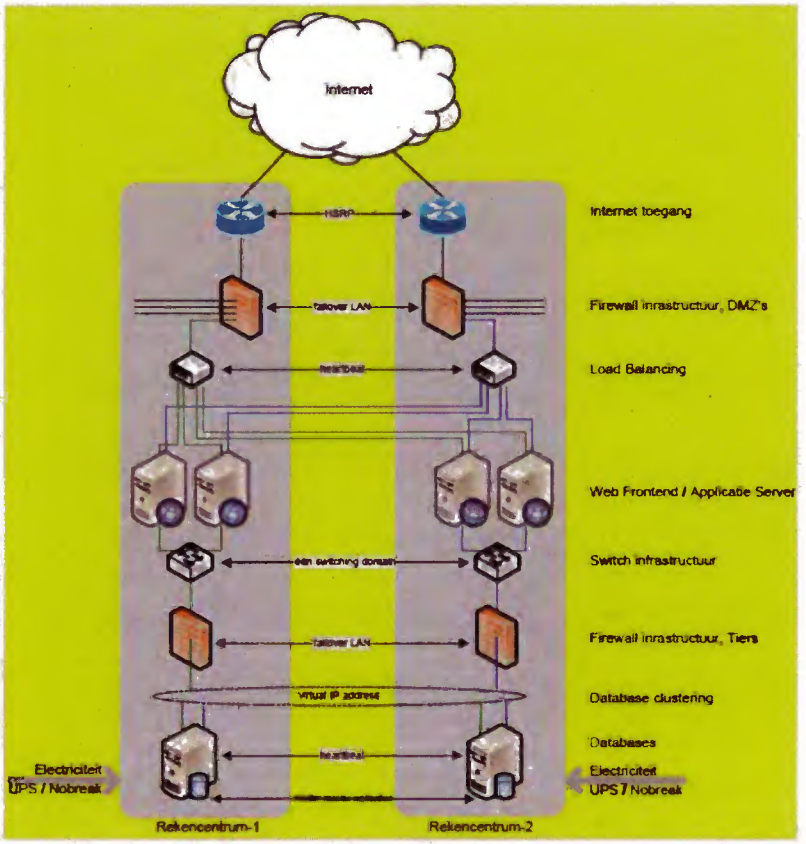
- De omvang van de OTAP omgevingen is gebaseerd op het minimaal aantal servers wat nodig is om DigiD te laten functioneren:
  - één databaseserver
  - één Applicatieserver
- Voor de productie en A1 omgeving zijn deze opgeschaald naar het volume wat nodig is om de performance eisen te halen
- De productie en A1 omgevingen moeten fysiek gelijk zijn.
- In verband met beschikbaarheidseisen moeten de Productie Preprod1, PreProd2 en Acceptatie1 redundant zijn over de twee datacenters.
- Voor additionele functionaliteit zijn de volgende servers/diensten toegevoegd:
  - De SMTP dienst 10.1c
  - DNS dienst afgenomen van Algemene Zaken
  - Servers in de ontwikkel- en test omgevingen ten behoeve van doorontwikkeling en systeemtesten
  - 10.2g
  - Servers in de Beheer omgeving incl. IPSec koppelingen ten behoeve van beheerwerkzaamheden vanuit Capgemini 10.1c

Gegeven het beperkte gebruik met betrekking tot DigiD Balie zijn er geen extra aparte servers nodig gebleken voor deze functionaliteit. Hierdoor is deze module geïmplementeerd op alle Applicatie servers ipv separaat.

4.6 Redundantie

De voor DigiD 5 benodigde infrastructuur is geconfigureerd en geplaatst over twee data centers heen. Dit om DigiD zoveel mogelijk te beschermen tegen uitval van een component, zelfs op data center niveau. De basis van deze oplossing zit in de connectie tussen de twee data centers, wat het mogelijk maakt om de omgeving als één omgeving te zien. Deze connectie is een onderdeel van het EASI Managed Services Platform waarbij stretched VLAN's geïmplementeerd zijn. Additioneel is redundantie gerealiseerd op verschillende lagen in de infrastructuur, zoals uit onderstaande figuur blijkt.

In deze figuur is de architectuur van de Productie en Acceptatie 1 weergegeven als voorbeeld. Dezelfde principes zijn ook geldig voor de overige omgevingen, behalve voor de A2, A3, A4, A5 en A6, aangezien deze zich uitsluitend op één data center bevinden.



De volgende redundantie opties zijn geïmplementeerd:

- Producten en Diensten afgenomen van het EASI Managed Services platform:
  - Identieke data centers, geografisch verspreid, om te beschermen tegen uitval van het volledige data center.
  - Dubbele power supply op beide data centers, publieke energie aansluiting incl. lokale generator (ISO50001 gecertificeerd)
  - Dubbele Internet connectie. Connectie in elk van de twee datacenters met seamless failover
  - Dubbele DigiNetwerk connectie. Connectie in elk van de twee datacenters met seamless failover
  - Dubbele connectiviteit tussen beide data centers om te voorkomen dat de datacenters in een "split-brain" modus komen
  - De netwerk componenten (Firewall, Loadbalancers, routers) zijn met minimaal een component vertegenwoordigd in elk data center. De loadbalancers beschikken over een heartbeat om tijdig een failover in gang te kunnen brengen.
  - Elk data center heeft twee netwerk switches zodat uitval van een single switch niet leidt tit een verminderde capaciteit, aangezien alle servers aangesloten zijn op beide switches in een redundantie setup
  - De inhoud van de 10.1c databases zijn gerepliceerd over de twee database servers per omgeving (waar van toepassing), dit geldt voor alle database servers.
  - Er zijn meerdere Applicatieservers, die de load over kunnen nemen als één Applicatieserver uitvalt.

In het geval van een failover van één van de componenten kan er enig data of sessie verlies zijn. De volgende tabel laat de schade zien in het geval van uitval van één van de redundante componenten. De uitval betreft alleen de gebruikers die ten tijde van de uitval gebruik maken van het betreffende component.

Component	Schade
Internet connectie	Gebruikers ondervinden een tijdelijke onderbreking. In sommige gevallen kan een sessie verloren zijn. De gebruiker dient dan opnieuw aan te loggen.
Firewall	Alle open netwerk sessies zijn verloren. Gebruikers moeten waarschijnlijk een refresh van de sessie of de laatst actie opnieuw uitvoeren
Load Balancer	Alle open netwerk sessies zijn verloren. Gebruikers moeten waarschijnlijk een refresh van de sessie of de laatst actie opnieuw uitvoeren
Applicatie server	De actieve applicatie sessie is verloren. De gebruiker moet het process herstarten. Data is niet lokaal opgeslagen op de Applicatie server, zodat een andere Applicatie-server het volgende verzoek kan behandelen.
Network Switch	De complete infrastructuur in een datacenter is niet beschikbaar. Het andere data center is beschikbaar voor alle verzoeken, maar met een verminderde overall performance. Gebruikers moeten wellicht hun sessie refreshen of herstarten of anders het gehele proces herstarten.
Database	Het failover mechanisme zal automatisch de tweede database server binnen 1 minuut selecteren. Gebruikers ondervinden een korte onderbreking. Gebruikers moeten wellicht hun sessie refreshen of herstarten of anders het gehele proces herstarten. De tussen twee databases gerepliceerde data kan verloren zijn (maximaal 15 minuten).
Andere combinaties	De uitval heeft betrekking op alle hierboven beschreven effecten voor de betreffende gebruikers.

Alle hierboven weergegeven mogelijkheden zijn in lijn met de Service Level Agreement, waarin staat dat er een dataloss mag zijn van 15 minuten in het geval van een failover. Overal waar een sessieverlies vermeld staat, kan dit een tijdelijke onbeschikbaarheid van de dienst betekenen gedurende enkele seconden gedurende de failover, Gedurende deze onbeschikbaarheid is het niet mogelijk om het proces te herstarten of een refresh van de web pagina uit te voeren.

4.7 DigID Applicaties

De DigiD 5 applicatie bestaat uit drie verschillende web applicaties.

Applicatie	Beschrijving
DigiD Burger Applicatie	Bevat authenticatie en account raadplegen / activering en beheer functionaliteit ("Mijn DigiD")
DigiD Beheer Applicatie	De beheer applicatie wordt door Logius functioneel Ketenbeheer gebruikt voor het beheer van de DigiD 5 applicatie.

DigiD Balie Applicatie	Deze applicatie is speciaal voor DigiD in het buitenland en biedt functionaliteit voor de 'Baliemedewerker' om de DigiD aanvragen zonder brieven te verwerken..

De reden voor deze scheiding ligt in de beveiliginggrenzen voor deze functies. De authenticatie component moet beschikbaar zijn via het Internet, terwijl de beheer interface alleen beschikbaar mag zijn vanuit het Logius beheer netwerk via DigiNetwerk. De Balie component moet beschikbaar zijn vanuit de ambassades en consulaten en bepaalde gemeenten. Deze scheiding is geconfigureerd in de firewall en vereist afgescheiden web applicaties op verschillende externe IP-adressen.

Additionele Web Applicaties zijn beschikbaar voor testen van verschillende omgevingen. De volgende tabel toont deze applicaties en hun beschikbaarheid.

Applicatie	Omschrijving
App Stub	Met deze stub wordt de werking van een App op een specifiek apparaat gesimuleerd. De in te scannen QR code van de DigiD website kan naar het browser scherm van de stub gesleept worden om het scannen te simuleren.
CRB Stub	Ten behoeve van DigiD 5.3 is een koppelvlak met CRB (RDW) gerealiseerd. Met de CRB stub kunnen de relevante rijbewijs gegevens worden opgehaald om een aangeboden document te kunnen valideren tijdens de verhoging naar niveau substantieel.
GBA Stub	Een stub is in alle omgevingen, behalve de productieomgeving, beschikbaar, om de GBA-V server van de Nederlandse overheid te simuleren. Deze stub wordt gebruikt in (load) test scenario's waar een connectie met de echte GBA-V service niet toegestaan is. De Stub is tevens een onderdeel van de preproductie omgevingen. Deze Stub wordt daar gebruikt omdat deze omgeving veel meer accounts moet bevatten dan de echte GBA-V test omgevingen. Deze accounts worden gebruikt door alle "Afnemers" wanneer ze hun applicaties testen tegen de DigD preproductie omgevingen. De GBA Stub is niet bereikbaar van buiten het systeem. De GBA Stub is alleen intern bereikbaar vanuit de DigiD Burger en Beheer applicaties.
SMS Stub	Toont verstuurde SMSjes in een browser scherm
SAML Tools	Biedt met een webinterface, ondersteuning voor validatie van berichten en inlogtesten voor het SAML koppelvlak
CGI Tools	Biedt met een webinterface, ondersteuning voor inlogtesten voor het CGI koppelvlak
Config Applicatie	De Config applicatie is beschikbaar in de Ontwikkel, Test1, Test2, A2, A3, A4, A5 en A6 omgevingen voor het faciliteren van de testen. Deze applicatie biedt toegang tot de applicatie configuratie, wat nodig is voor het testen van bepaalde scenario's. Tevens biedt het toegang naar een pagina met activatie codes die nodig zijn, omdat deze omgevingen geen activatie brieven sturen met deze codes.

De tabel hieronder geeft een overzicht van alle web applicaties die beschikbaar zijn per omgeving

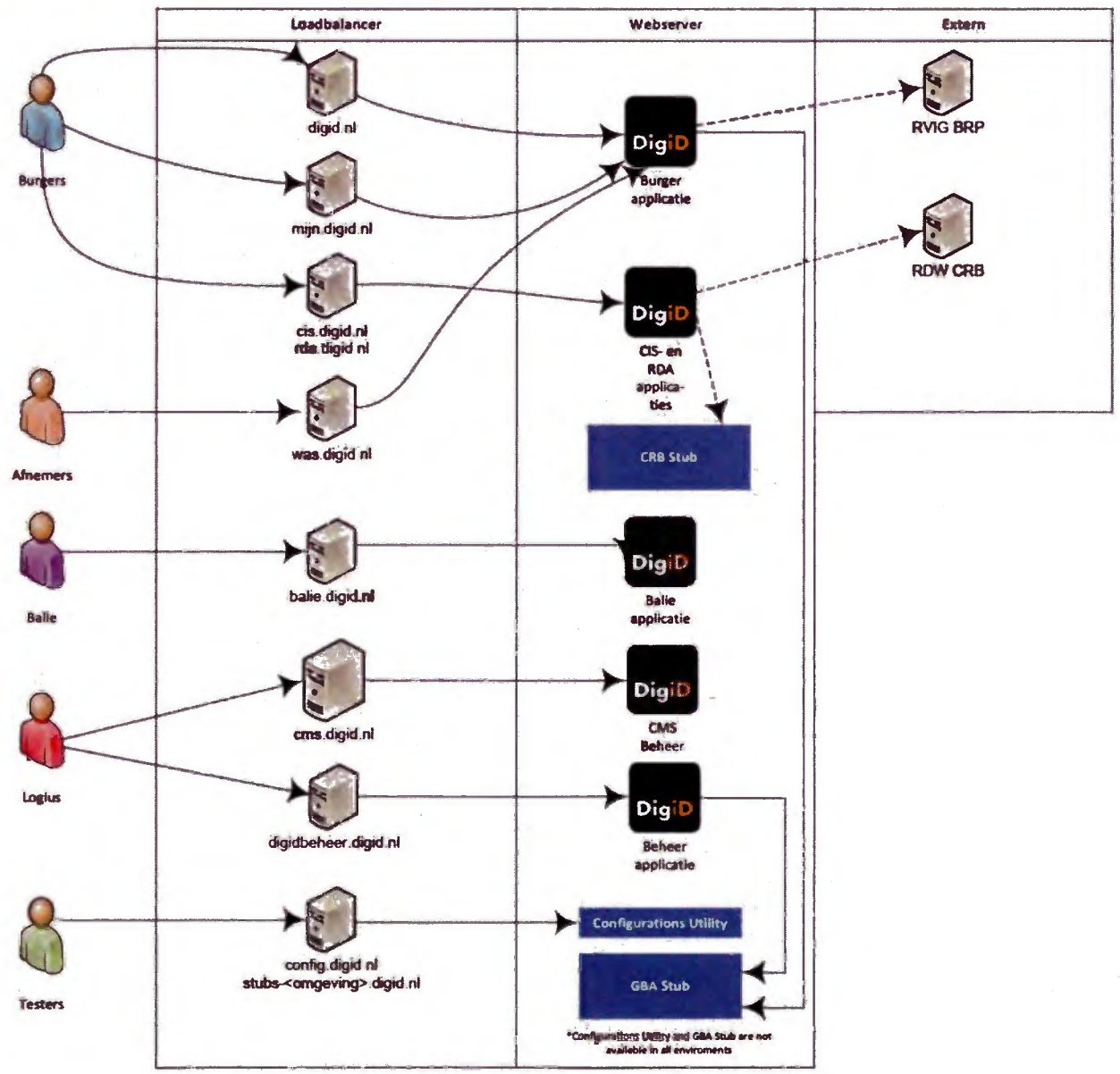
Applicatie	O	T1	T2	A1	A2	A3	A4	A5	A6	PP1	PP2	Productie
DigiD Burger	√	√	√	√	√	√	√	√	√	√	√	√
DigiD Beheer	√	√	√	√	√	√	√	√	√	√	√	√
DigiD Balie	√	√	√	√	√	√	√	√	√	√	√	√
MSC	√	√	√	√	√	√	√	√	√	√	√	√
App Stub	√	√	√	√	-	√	√	√	√	-	-	-
CRB Stub	√	√	√	√	-	√	√	√	√	-	-	-
GBA Stub	√	√	√	√	√			√	√	√	√	-

SMS Stub	√	√	√	√	-	√	√	√	√	-	-	-
SAML Tools	√	√	√	-	-	-	-	-	-	-	-	-
CGI Tools	√	√	√	√	-	√	√	√	√	-	-	-
Config	√	√	√	√	√	√	√	√	√	-	-	-

De GBAStub applicatie is niet op alle omgevingen waar deze beschikbaar is gekoppeld. Afhankelijk van het type test wat gewenst is, kan deze in de configuratie gekoppeld worden.

4.7.1 URL's

De applicaties zijn bereikbaar middels meerdere URL's. Dit is afhankelijk van de functionaliteit. De volgende figuur toont een schematisch overzicht, gevolgd door een meer gedetailleerde uitleg van de verschillende URL's en een overzicht van de URL's per omgeving.



4.7.1.1 Toepassing URL's

URL	Omschrijving
https://digid.nl	Deze URL wordt gebruikt door de Nederlandse burgers wanneer ze gebruik willen maken van de Authenticatie functie. Deze URL wordt voor meerdere functies gebruikt: Authenticatie – Authenticatie tegen DigiD, /aanvragen – Aanvragen van een nieuw DigiD account, /activeer_digid – Activeren van een nieuw DigiD account, /herstel_account – Herstellen van een DigiD account waarvan het wachtwoord niet meer bekend is bij de betreffende burger Als een gebruiker middels http toegang zoekt naar deze URL, wordt hij gestuurd naar de https:// digid.nl website, inclusief het originele zoek pad. Als een gebruiker middels het HTTPS protocol toegang zoekt naar deze URL, wordt hij gestuurd naar de root van de https://digid.nl website.
https://mijn.digid.nl	Deze URL wordt door de Nederlandse burgers gebruikt voor hun eigen account beheer. Een gebruiker kan middels zijn account inloggen en zijn Account historie bekijken, settings wijzigen etc, De Nederlands burger kan zowel een web browser als de DigiD-APP gebruiken.
https://was.digid.nl	Deze URL wordt gebruikt door overheidsinstanties (Afnemers). Deze URL is geconfigureerd in de diverse systemen van deze organisaties. Om tegemoet te komen aan de eis W29 ("...De inspanning voor de Afnemers dient zo veel mogelijk te worden beperkt."), mag deze URL in principe niet gewijzigd worden.
https://digidbeheer.digid.nl	Deze URL wordt gebruikt voor toegang tot de applicatie beheer interface.
https://balie.digid.nl	Deze URL toont de Balie applicatie en wordt gebruikt door medewerkers van ambassades, gemeenten en consulaten om burgers van een DigiD account te voorzien via de "Buitenland" procedure. Medewerkers van de ambassade zijn geautoriseerd voor gebruik van de Balie module via een redirect naar eHerkenning. De "Burger" applicatie (digid.nl) wordt gebruikt voor het burgers proces in deze procedure.
https://msc.digid.nl	Deze URL wordt door het RDW gebruikt om de Middelen Status Controler aan te roepen
https://config-<env>.digid.nl	Deze URL biedt toegang tot test tools en applicatie configuratie settings. Niet aanwezig op productie.
https://stubs-<env>.digid.nl	Deze URL biedt toegang tot test tools en webinterfaces van stubs. Niet aanwezig op productie.

De hierboven weergegeven lijst is van toepassing op de productieomgeving. De andere omgevingen (Acceptatie1-6, preproductie1-2) hebben een vergelijkbare benaming, inclusief de omgeving naam , bijvoorbeeld voor A1 (Acceptatie1):

- https://a1.digid.nl/
- https://mijn.a1.digid.nl/

- https://was-a1.digid.nl/
- https://digidbeheer-a1.digid.nl/
- https://balie-a1.digid.nl/
- https://config-a1.digid.nl/
- https://stubs-a1.digid.nl/
- https://msc-a1.digid.nl/

De URL's voor de beheer interface zijn alleen beschikbaar via het Logius beheer network en zijn daarom niet in de public DNS Servers opgenomen.

10.2g

4.7.2 Cliënt certificaten check

Sommige interfaces/koppelvlakken gebruiken cliënt certificaten voor het authenticeren van de connecterende partij. Dit is in de loadbalancer geconfigureerd. Voor de "was" URL vraagt de loadbalancer altijd om een cliënt certificaat. Als een "afnemer" toegang zoekt naar een URL wat een certificaat vereist, wordt de validiteit van dat certificaat op basis van de volgende criteria gecontroleerd:

- Is het certificaat ondertekend door een geautoriseerde CSP,
- Valt de huidige datum binnen de validiteitdatum van het certificaat?
- Is het certificaat niet ingetrokken door de CSP (CRL check).

Bij de basiscontrole worden, alle PKI Overheid certificaten geaccepteerd. Aangezien de meeste afnemers alleen hun eigen certificaten aanbieden en niet de gehele keten tot aan de root, is een complete lijst van valide CSP's, inclusief alle intermediaire en verstrekkende CA's, om tegen te controleren, beschikbaar in de infrastructuur. Deze lijst wordt bijgehouden middels service vragen vanuit Logius.

Los van de basis certificaatcontroles, controleert de DigiD infrastructuur alle aangeleverde cliënt certificaten tegen een white list. Dit om te voorkomen dat iedereen met een valide PKI-Overheid certificaat toegang krijgt tot de DigiD afnemer interface. De whitelist is per omgeving en interface ingesteld.

In het geval dat de infrastructuur toegang gebaseerd op certificaat controles toestaat, wordt de certificaat (SHA1) fingerprint toegevoegd in een HTTP header, wat verstuurd wordt naar de applicatie voor verdere verwerking.

De whitelist wordt automatisch onderhouden door de applicatie.

De volgende tabel toont de lijst van URL's per interface waarvoor cliënt certificaat authenticatie vereist is.

Interface	URL
WSDL authenticatie	/was/services/WSDigiDSectorAuthenticatiePortType
WSDL administratie	/services/SectoradministratiePort /services/SectoradministratiePort.xsd /svb/aanvragen/nieuw
SAML	/saml/idp/resolve_artifact

Backlog

In dit hoofdstuk staat benoemd wat er nog verwerkt moet worden in het DLD.

#	Toelichting	Locatie	Planning

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

NL QEMS
Logius / DigiD

Opvolging bevindingen security tests

Referentie	*r5.0 migratie - opvolging bevindingen security tests*
Versie	*<0 x>*
Versie datum	*15 juni 2021*
Auteur	*<auteur>*


SEC2
Customer Confidential
Access individually, on a need-to-know basis, and with clear association to customer engagement

DOCUMENTHISTORIE

VERSIE	DATUM	AUTEUR	WIJZIGINGEN
0.1	3-10-2016	10.2.e	
0.2	5-10-2016	10.2.e	Bijgewerkt met A1 en PP2

REVIEW EN GOEDKEURING

BEDRIJF	NAAM	DATUM	PARAAF

DISTRIBUTIE

BEDRIJF	NAAM	VERSIE-NUMMER	MEDIA	ACTIE

OPSLAG

LOCATIE	TOEGANG	ADMINISTRATEUR
Teamforge		

Inhoudsopgave

1 Inleiding

1.1 Algemeen

In dit document staan de bevindingen en de door Capgemini uitgevoerde / uit te voeren acties vermeld vanuit de door Sogeti uitgevoerde security testen op de volgende door Capgemini beheerde DigiD omgevingen:

- Acceptatie 1
- Acceptatie 2
- Acceptatie 3
- Acceptatie 4
- PreProd 1
- PreProd 2
- Productie

1.2 Beschikbare testrapportage

- DigiD Migratie – A2, A3, A4, PP1 Kenmerk: 42100181 Datum 22-9-2016 Status Definitief Versie 1.0
- DigiD Migratie Productie Kenmerk 42100989 Datum 22-09-2016 Status
- 201609 - Initiële Rapportage DigiD migratie PP2 v1.0
- Rapportage DigD Migratie – ACC1

2 Acceptatie 1

2.1 Bevindingen

Op de ACC1 omgeving zijn de volgende ongewenste verkeersstromen geconstateerd:

Er is verkeer mogelijk naar de volgende IP adressen op de volgende poorten vanaf diverse servers.

2.2 Acties Capgemini

Capgemini heeft de hierboven vermelde verkeerstromen toegevoegd in het Detail Level Design plan, zodat werkelijkheid overeenstemt met de documentatie.

3 Acceptatie 2

3.1 Bevindingen

Op de ACC2 omgeving zijn de volgende ongewenste verkeersstromen geconstateerd:

Er is verkeer mogelijk naar de volgende IP adressen op de volgende poorten vanaf dgd-A4-as1.

IP	Poort
10.2.g	

Allereerst de constatering da 10.2.g geen server is in de Acceptatie 2 omgeving, maar onderdeel is van de Acceptatie 4 omgeving. Aannäme is dat hier 10.2.g hoort te staan.

3.2 Acties Capgemini

Capgemini heeft de hierboven vermelde verkeerstromen toegevoegd in het Detail Level Design plan, zodat werkelijkheid overeenstemt met de documentatie.

4 Acceptatie 3

4.1 Bevindingen

Op de ACC3 omgeving zijn de volgende ongewenste verkeersstromen geconstateerd:

Er is verkeer mogelijk naar de volgende IP adressen op de volgende poorten 10.2.g.

IP adres	Poort
10.2.g	

4.2 Acties Capgemini

Capgemini heeft de hierboven vermelde verkeerstromen toegevoegd in het Detail Level Design plan, zodat werkelijkheid overeenstemt met de documentatie.

5 Acceptatie 4

5.1 Bevindingen

Op de ACC4 omgeving zijn de volgende ongewenste verkeersstromen geconstateerd:

Er is verkeer mogelijk naar de volgende IP adressen op de volgende poorten 10.2.g

IP adres	Poort
10.2.g	

5.2 Acties Capgemini

Capgemini heeft de hierboven vermelde verkeerstromen toegevoegd in het Detail Level Design plan, zodat werkelijkheid overeenstemt met de documentatie.

6 PreProductie 1

6.1 Bevinding verkeerstroom 443 en advies

Op de Preprod1 omgeving waren de volgende verkeerstromen mogelijk van buitenaf:

Vanaf IP adres	Naar IP adres	Hostname	Naar VPC	Protocol	Poort	Service
10.2.g	144.43.243.180	balie-preprod1.digid.nl	dgd-pp1	TCP	443	ssl/http
10.2.g	144.43.243.176	preprod1.digid.nl	dgd-pp1	TCP	443	ssl/http

De balie koppeling gaat via DigiNetwerk lopen. Hiervoor loopt de wijziging.

De tweede koppeling is noodzakelijk voor de aansluiting van de afnemers. Dit is beschreven in het Detail Design Plan.

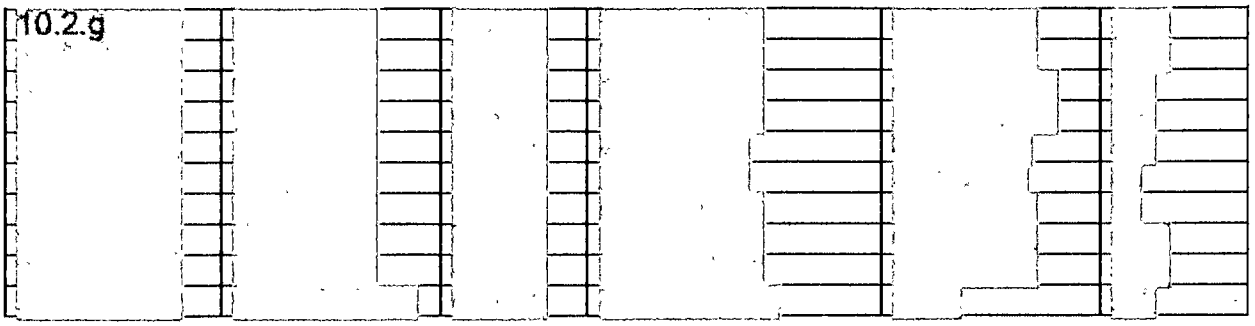
6.2 Bevindingen overige verkeerstromen

Er is verkeer mogelijk naar de volgende IP adressen op de volgende poorten 10.2.g .

Allereerst de constatering dat 10.2.g geen server is in de PreProd1 omgeving, maar onderdeel is van de Acceptatie 4 omgeving. Aanname is dat hier 10.2.g hoort te staan.

Tevens was er verkeer mogelijk van:

Van IP	Van Hostname	Van VPC	Naar IP	Naar Hostname	Poort
10.2.g					



6.3 Acties Verkeerstromen Capgemini

Capgemini heeft de hierboven overige vermelde verkeerstromen toegevoegd in het Detail Level Design plan, zodat werkelijkheid overeenstemt met de documentatie.

7 PreProductie 2

7.1 Bevindingen en acties Capgemini

Kwetsbaarheid	Actie
Verouderde 10.2g software	10.2g
Er is een verouderde versie 10.2g 10.2g op diverse hosts	10.2g Als beheermaatregel wordt de afgestemde Patchprocedure gehanteerd.
De 10.2g server-status pagina is beschikbaar op diverse hosts	10.2g Mag alleen toegankelijk zijn voor Localhost. 10.2g

8 Productie

8.1 Bevindingen en acties Capgemini

Indien gearceerd zijn dit nog openstaande acties

Kwetsbaarheid	Actie
Verouderde 10.2g software	10.2g Als beheermaatregel wordt de afgestemde Patchprocedure gehanteerd.
Er is een verouderde versie 10.2g 10.2g gedetecteerd op diverse hosts	10.2g Als beheermaatregel wordt de afgestemde Patchprocedure gehanteerd.
Op diverse hosts 10.2g 10.2g een standaardpagina beschikbaar.	Deze zijn verwijderd en worden middels aangepast deployscript ook niet meer gedeployed vanuit nieuwe releases.
De 10.2g server-status pagina is beschikbaar op diverse hosts	10.2g Mag alleen toegankelijk zijn voor Localhost 10.2g
De host stuurt bij het redirecten van de gebruiker geen HSTS-header mee. In andere gevallen (op andere hosts) wordt er wel een HSTS-header meegestuurd. Bovendien wordt er redirect naar een site met het HTTP-protocol in plaats van HTTPS.	10.2g
Er is een host gevonden op 10.2.g op het netwerk met een open poor 10.2g Het betreft waarschijnlijk een webserver. Deze webserver is bereikbaar vanaf alle applicatieservers 10.2.g	Dit is in onderzoek bij Capgemini.
Op de Productie omgeving zijn de volgende ongewenste verkeersstromen geconstateerd: 10.2g	10.2g Staat beschreven in DLD 10.2g Staat beschreven in DLD 10.2g Tekstfout in securitytestrapport 10.2g Staat beschreven in DLD

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport

Securitytest DigiD 5.1

Kenmerk: 2016110301

Datum	7-12-2016
Status	Definitief
Versie	1.1

Na oplevering eindrapport is deze rubricering beëindigd.

Rubricering	derubricering
Vaststeller	10.2e
Functie	10.2e

Colofon

Kenmerk	2016110301
Versienummer	1.1
Contactpersoon	10.2.e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
23-11-2016	0.1	Sogeti	Initiële versie
01-12-2016	1.0	Sogeti	Gereviewde versie
07-12-2016	1.1	Sogeti	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2.e	Opdrachtgever	10.2e	Logius
10.2.e	10.2e	10.2e	Logius
10.2.e	10.2e	10.2e	Sogeti
10.2.e	10.2e	10.2e	Sogeti
10.2.e	10.2e	10.2e	Logius
10.2.e	10.2e	10.2e	Logius
10.2.e	10.2e	10.2e	Logius

Inhoud

Managementsamenvatting

Inleiding

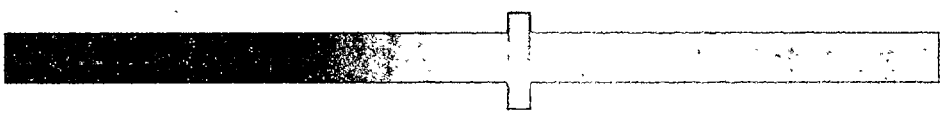
Logius heeft Sogeti gevraagd een securitytest uit te voeren op de acceptatieomgeving van DigiD 5.1. Het onderzoek is gestart op 15 november 2016 en is uitgevoerd onder supervisie van 10.2.e .

De aanleiding tot deze securitytest betreft de release van DigiD versie 5.1. Het doel is inzicht te krijgen in het beveiligingsniveau van DigiD en de risico's die Logius loopt indien Release 5.1 in de productieomgeving wordt geïnstalleerd. Daarnaast is het doel het beveiligingsniveau te handhaven of te verbeteren nadat er wijzigingen in de applicatie zijn aangebracht, en detectie of eerder geconstateerde risico's zijn weggenomen en er geen nieuwe risico's zijn geïntroduceerd als gevolg van deze wijzigingen. Tevens ligt de focus op een aantal specifieke changes in de beheermodule welk gerelateerd zijn aan de beveiliging, en tevens een hertest van een eerdere bevinding.

Dit rapport bevat de resultaten van de test.

Conclusies en aanbevelingen

Het beveiligingsniveau van de DigiD-omgeving wordt op basis van het uitgevoerde onderzoek ingeschat op:



Onvoldoende Voldoende

Positieve punten:

- De CSRF bevinding van de voorgaande rapportage is opgelost in de huidige release.

Punten ter verbetering:

- De implementatie van de anti-CSRF maatregelen behoeft fine-tuning om deze waterdicht te maken.

- Er zijn twee bevindingen gedaan op het cryptografisch vlak. Deze cryptografische configuratie behoeft meer aandacht om bij te blijven bij de huidige technische standaarden.

Aanvullingen Logius

Logius heeft kennisgenomen van de resultaten van de Securitytest R5.1 en heeft de gerapporteerde bevindingen beoordeeld op impact. Een aantal bevindingen was al bekend vanuit eerder uitgevoerde securitytesten. Toen en ook deze keer zijn deze bevindingen geaccepteerd als known error. Een aantal andere bevindingen zijn nieuw. Vastgesteld is dat deze bevindingen niet het gevolg zijn van de aanpassingen in het kader van R5.1. De risico's van deze bevindingen zijn beoordeeld als laag. Dit security testrapport zal deel uitmaken van het Vrijgaveadvies dat aan de stuurgroep DigiD zal worden gegeven om DigiD R5.1 op het productieplatform van DigiD te installeren. Opvolging van de openstaande bevindingen vindt plaats vanuit het reguliere beheerproces.

1 Inleiding

1.1 Opdrachtformulering

Deze securitytest richt zich op de acceptatieomgeving van DigiD 5.1. Het onderzoek bestaat uit een greybox securitytest op de applicatie en de bijbehorende infrastructuur.

Zie PvA Securitytest DigiD 5.1 v1.0 hoofdstuk 2, 'Opdrachtformulering'.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd.

1.3 Scope

Onderwerp	URL	IP-adres
Mijn DigiD	https://mijn.a3.digid.nl	144.43.243.145
Aanvragen	https://a3.digid.nl/aanvragen	144.43.243.144
Activeren	https://a3.digid.nl/activeer_digid	144.43.243.144
Herstellen	https://a3.digid.nl/herstellen	144.43.243.144
Koppelvlakken	https://was-a3.digid.nl	144.43.243.146
Beheermodule	https://digidbeheer-a3.digid.nl	144.43.243.148

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Info	Totaal
Logica	0	0	0	0	0	0	0
Authenticatie	0	0	0	0	0	0	0
Sessiemanagement	0	0	0	0	0	0	0
Toegang	0	0	0	0	0	0	0
Invoerafhandeling	0	0	2	0	0	0	2
Omgeving	0	0	0	0	0	0	0
Servers	0	0	1	3	0	0	4
Totaal	**0**	**0**	**3**	**3**	**0**	**0**	**6**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

De bevindingen hebben betrekking op twee beleidsdomeinen uit de NCSC-richtlijnen.

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	Geen opmerkingen
Toelichting	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	Geen opmerkingen
Toelichting	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	Geen opmerkingen
Toelichting	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	Bevindingen #3 en #6 hebben hier betrekking op.
Toelichting	

[1] Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

B.05	Contractmanagement
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	Geen opmerkingen
Toelichting	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	Geen opmerkingen
Toelichting	

Uitvoeringsdomein

U/TV.01	Toegangsvoorzieningsmiddelen
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	Bevindingen #1, #2 en #5 hebben hier betrekking op
Toelichting	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	

Oordeel	Geen opmerkingen
Toelichting	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	Geen opmerkingen
Toelichting	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot het geen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	Geen opmerkingen
Toelichting	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.02	**Beschikbaarheid van netwerken**
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	Geen opmerkingen

Toelichting	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) bevelligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	Geen opmerkingen
Toelichting	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	Geen opmerkingen
Toelichting	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	Geen opmerkingen
Toelichting	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	Geen opmerkingen
Toelichting	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	Geen opmerkingen
Toelichting	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	Geen opmerkingen

Toelichting	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	Geen opmerkingen
Toelichting	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	Geen opmerkingen
Toelichting	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	Geen opmerkingen
Toelichting	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	Geen opmerkingen
Toelichting	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	Bevinding #4 heeft hier betrekking op.
Toelichting	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	Geen opmerkingen
Toelichting	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	Geen opmerkingen
Toelichting	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen bevindingen gedaan in deze categorie.

3.2 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen bevindingen gedaan in deze categorie.

3.3 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen bevindingen gedaan in deze categorie.

3.4 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen bevindingen gedaan in deze categorie.

3.5 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beinvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

Kwetsbaarheid: Cross Site Request Forgery				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
1	-	**Middel**	Laag.	Middel.

Er zijn vier Cross-Site Request Forgeries (CSRF) gevonden behorende bij twee verschillende acties:

- Acceptatie van een vier ogen review: https://digidbeheer-a3.digid.nl/four_eyes_review/<review_id>/accept
- Afwijzing van een vier ogen review: https://digidbeheer-a3.digid.nl/four_eyes_review/<review_id>/withdraw
- Beëindig een gebruikerssessie: https://digidbeheer-a3.digid.nl/destroy_session
- Start een gebruikerssessie: https://digidbeheer-a3.digid.nl/sign_in

De eerste twee CSRF's zijn middels een GET-methode aanroepbaar. Deze CSRF's kunnen er voor zorgen dat een aanvaller een ingelogde gebruiker via bijvoorbeeld phishing kan verleiden tot een onbewuste handeling op de site van DigiD.

De laatste twee CSRF's zorgen ervoor dat zolang een kwaadaardige website open staat, de gebruiker constant wordt uitgelogd, waardoor er in feite een denial-of-service plaatsvindt voor de gebruiker in kwestie.

Kwetsbaarheid: Cross Site Request Forgery replay attack				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
2	-	**Middel**	Laag.	Middel.

Tijdens de test is gebleken dat het mogelijk is om gedurende een actieve sessie een anti-CSRF token te hergebruiken. Het is aan te raden om een CSRF token eenmalig te accepteren en de geldigheid hiervan daarna te laten vervallen. Wanneer de sessie wordt beëindigd en opnieuw wordt ingelogd is het niet meer mogelijk om het anti-CSRF token te hergebruiken.

3.6 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen bevindingen gedaan in deze categorie.

3.7 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze servers kunnen meer informatie of diensten bevatten dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

Kwetsbaarheid: SSL/TLS – SWEET32 attack				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
3	-	**Laag**	Laag.	Laag.

Een analyse van de geaccepteerde SSL ciphers op port 443 van de DigID beheer server toont dat gebruik wordt gemaakt van zwakkere SSL ciphers. Deze zijn vatbaar voor de SWEET32 aanval.

```
nmap –p 443 –script ssl-enum-ciphers digidbeheer-a3.digid.nl
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-18 14:55 CET
Nmap scan report for digidbeheer-a3.digid.nl (144.43.243.148)
Host is up (0.035s latency).
Other addresses for digidbeheer-a3.digid.nl (not scanned): 2a04:9a00:1010:1300::b
PORT    STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength:
```

Kwetsbaarheid: Verouderde software				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
4	-	**Middel**	Laag.	Middel.

De 10.2g en 10.1d server op mijn.a3.digid.nl en a3.digid.nl heeft het versienummer 10.2g en 10.1d Deze versie 10.2g en 10.1d is verouderd 10.2g en 10.1d en kent enkele bekende kwetsbaarheden. De aanbeveling is om de software 10.2g en 10.1d te upgraden.

Kwetsbaarheid: HSTS header ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
5	-	**Laag**	Laag.	Laag.

De server van digidbeheer-a3.digid.nl maakt geen gebruik van de HSTS header, die verbinding via een versleutelde verbinding afdwingt. Aanbeveling is om de header *"Strict-Transport-Security: max-age=60000; includeSubDomains"* mee te sturen.

Kwetsbaarheid: SAML signing met zwak versleutelingsalgoritme				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact in geval van misbruik**
6	-	**Laag**	Laag.	Laag.

DigiD authenticatie maakt gebruik van SAML. Deze SAML berichten worden gesigneerd door de server. Deze signering gebeurd met RSA-SHA1, welke als onveilig wordt beschouwd. Aan te bevelen is minimaal RSA-SHA256 te gebruiken om de SAML berichten te signeren.

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-around' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport

DigiD R5.2

Kenmerk: 201622

Datum	24-01-2017
Status	Definitief
Versie	1.0

Rubricering derubricering

derubricering

Colofon

Kenmerk	201622
Versienummer	1.0
Contactpersoon	10.2.e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
20-01-2017	0.1	Sogeti Nederland B.V.	Initiële versie
24-01-2017	0.2	Sogeti Nederland B.V.	Interne review
24-01-2017	0.3	Sogeti Nederland B.V.	Commentaar verwerkt
24-01-2017	0.4	Sogeti Nederland B.V.	Interne review
25-01-2017	1.0	Sogeti Nederland B.V.	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
			Logius
10.2.e	10.2e	10.2e	Logius
10.2.e	10.2e	10.2e	Sogeti
10.2.e	10.2e	10.2e	Sogeti
10.2.e	10.2e	10.2e	Sogeti

Inhoud

derubricering

Managementsamenvatting

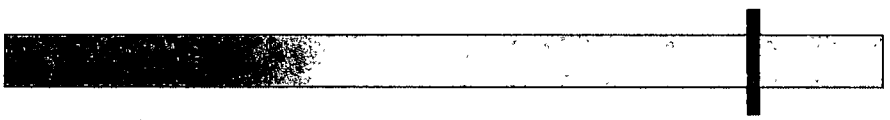
Inleiding

Logius heeft Sogeti gevraagd een securitytest uit te voeren op de acceptatieomgeving van DigiD. Het onderzoek is gestart op 16 januari 2017 en is uitgevoerd door 102.e [redacted].

Conclusies en aanbevelingen

Samenvattend resultaat n.a.v. de scope van de securitytest.

- De applicatie telt voor het complexe landschap weinig bevindingen. Er zijn geen bevindingen gedaan met hoge of kritieke risicoclassificatie;
- Op het koppelvlak tussen de app en de back-endsystemen zijn geen bevindingen gedaan. Door toetsing van de techniek is gebleken dat zowel de implementatie, e.g. certificate pinning, als de gebruikte cryptografische methode voldoen aan de gestelde normen.



Onvoldoende Voldoende

Punten ter verbetering.

- Het is mogelijk om meerdere malen tegelijkertijd te zijn ingelogd in DigiD. Aanvullend mist de logging informatie die dit inzichtelijk maakt. De applicatie biedt daarbij de mogelijkheid om de logging uit het zicht van de gebruiker te krijgen. Een aanvaller kan deze mogelijkheden gebruiken om een gebruikerssessie over te nemen en zijn sporen te verbergen.

  Zorg ervoor dat naast de correcte implementatie van sessiebeheer ook de logging verrijkt wordt met informatie waarmee de burger zelf inzicht in mogelijk misbruik kan krijgen.

- De applicatie bevat bij de installatie meegekomen directories en informatieve foutmeldingen. Een aanvaller kan deze gegevens gebruiken om inzicht te krijgen in de gebruikte componenten en technologieën.

  Activeer en bied alleen functionaliteit en informatie aan die functioneel nodig is voor de werking van het systeem. Werk daarbij het installatie- en patch proces bij zodat alleen de benodigde functionaliteit blijft bestaan op de server.

Aanvullingen Logius

Logius heeft kennisgenomen van de resultaten van de Securitytest R5.2 en deze besproken met Sogeti. De gerapporteerde bevindingen zijn beoordeeld op impact. Vastgesteld is dat de bevindingen geen gevolg zijn van de aanpassingen die zijn uitgevoerd als onderdeel van R5.2. Opvolging en verdere analyse van bevindingen en aanbevelingen vindt plaats vanuit het reguliere beheerproces. Het Security Testrapport en de ingeschatte impact van de bevindingen zal onderdeel uitmaken van het advies dat aan de stuurgroep DigiD zal worden gegeven ten aanzien van de vrijgave van DigiD R5.2.

1 Inleiding

1.1 Opdrachtformulering

De aanleiding tot deze securitytest betreft release 5.2 van DigiD. Het informatiebeveiligingsbeleid van Logius schrijft voor dat de producten van Logius periodiek worden getest op zwakheden door middel van een zogenaamde securitytest (ook wel penetratietest of pentest genoemd).

Het doel is inzicht te krijgen in het beveiligingsniveau van DigiD en de risico's die Logius loopt indien Release 5.2 in de productieomgeving wordt geïnstalleerd.

Daarnaast is het doel het beveiligingsniveau te handhaven of te verbeteren nadat er wijzigingen in de applicatie zijn aangebracht, en detectie of eerder geconstateerde risico's zijn weggenomen en er geen nieuwe risico's zijn geïntroduceerd als gevolg van deze wijzigingen.

Tevens is gevraagd om extra focus te leggen op de aanpassingen die als onderdeel van Release 5.2 zijn doorgevoerd en die gerelateerd zijn aan beveiliging. Dit betreft in het bijzonder de implementatie van een opgesteld cryptografisch ontwerp in het kader van de DigiD app en een uitbreiding van het in DigiD geimplementeerde 'vier ogen principe'.

Ook is het verzoek een hertest uit te voeren van een eerdere bevinding gerelateerd aan de koppeling van de gebruikerssessie en het gebruikte IP adres.

De nadruk van de testen ligt op de technische beveiligingsrisico's. In overleg met Logius zal er, waar nodig, naar de business risico's gekeken worden.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd, welke aanvullend beschreven is in het bijbehorende Plan van Aanpak.

1.3 Scope van de werkzaamheden

'De securitytest richt zich op de gehele DigiD applicatie, doch zal zoals besproken specifieke focus leggen op aanpassingen die als onderdeel van Release 5.2 zijn doorgevoerd en die gerelateerd zijn aan beveiliging.

1.3.1 Het betreft de volgende changes in DigiD mobiel:

ID	Userstory
52.1.1.MD	Overzicht activeren DigiD app in Mijn DigiD
52.1.2.MD	Genereren QR-code
52.1.3.MD	Uitwisselen app gegevens
52.1.4.MD	Koppelcode
52.1.5.MD	Challenge-response & symmetrische sleutel
52.1.6.MD	Pincode
52.1.7.MD	Afronden activering

52.1.8.Au	Authenticeren met de DigiD app – Invullen gebruikersnaam en genereren sessie_ID
52.1.9.Au	Authenticeren met de Digid app en QR-code scan
52.1.10.Be	Switch

Voor het testen van DigiD mobiel wordt de app aan de testers van Sogeti verstrekt. Hier wordt ook naar de datastromen tussen de app en DigiD Kern gekeken, waaronder MitM mogelijkheden. Binnen deze app is met name de cryptografische implementatie van belang. Hiervoor is de werking in de vorm van een beschreven document gedeeld.

De encryptie heeft invloed op de volgende drie cases:
- Enrollment
- Authenticatie (Web to App)
- Authenticatie (Mobile Web to App)

1.3.2 Het betreft de volgende changes in Vier Ogen principe:

ID	Userstory
52.2.1.Be	Aanpassing S022 Wijzig webdienst
52.2.2.Be	Concurrency bij wijzigen
52.2.3.Be	Nieuw detailscherm S102 Accorderen wijziging webdienst
52.2.4.Be	Aanpassing S023 Nieuwe webdienst
52.2.5.Be	Afhankelijkheden Beheeraccounts en Rollen
52.2.6.Be	Afhankelijkheden Webdiensten

Hiernaast zal een algehele security test worden uitgevoerd ter detectie van eventuele regressie dan wel ongeautoriseerde of onbedoelde changes.

De securitytest richt zich op de volgende systemen in de *A3* omgeving:

Onderwerp	URL	IP-adres
Mijn DigiD	https://mijn.a3.digid.nl	144.43.243.145
Aanvragen	https://a3.digid.nl/aanvragen	144.43.243.144
Activeren	https://a3.digid.nl/activeer_digid	144.43.243.144
Herstellen	https://a3.digid.nl/herstellen	144.43.243.144
Koppelvlakken	https://was-a3.digid.nl	144.43.243.146
Beheermodule	https://digidbeheer-a3.digid.nl	145.21.253.97

Aanvullend is het verzoek gedaan om de volgende testgevallen expliciet te benoemen:
- Controle op http
- Controle op foutafhandeling
- Controle op de koppeling IP adres en sessie.

1.4 Buiten scope van de securitytest

In het kader van deze opdracht worden door de auditor de volgende werkzaamheden niet uitgevoerd.
- Alle websites en referenties die niet op het onderliggende systeem aanwezig zijn.
- De organisatie, fysieke ruimten en documentatie.
- DOS aanvallen of andere performance gerelateerde testen vallen buiten de scope, wel dient er naar beschikbaarheid gekeken te worden.

- Het aanbrengen van veranderingen aan systemen, het verwijderen of aanpassen van gegevens of het veroorzaken van andere verstoringen.
- De mobile app wordt zelf, buiten de hierboven genoemde aspecten, niet meegenomen in deze security test. Deze worden in de reguliere NCSC test meegenomen.

1.5 Manier van testen

De securitytest zal bestaan uit een (non-intrusive) vulnerability assessment met een diepgang greybox.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Logica						
Authenticatie						
Sessiemanagement			2			2
Toegang						
Invoerafhandeling			1	1		2
Omgeving						
Servers			3	2		5
Totaal			**6**	**3**		**9**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Kleur	Uitleg	Aantal
[redacted]	Niet getest, buiten scope.	17
	De norm wordt nageleefd.	22
	De norm wordt gedeeltelijk nageleefd.	5
[redacted]	Er wordt afgeweken van de norm.	0

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	[redacted]
Toelichting Processen worden niet getest tijdens een penetratietest.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	[redacted]
Toelichting Processen worden niet getest tijdens een penetratietest	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende)	

[1] Zie. https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

maatregelen.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Toelichting Certificaat is authenticatie, m.a.w. iedereen die gebruik maakt van de computer met het geïnstalleerde certificaat kan hiermee inloggen/de applicatie bereiken.	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Toelichting	

De invoer wordt voor bepaalde velden aan de client-side gecontroleerd en geeft een onverwachte fout bij het verwerken aan de server-side.	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Toelichting Default content en niet correct afgehandelde foutmeldingen geven informatie over het systeem.	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Toelichting Het is door de gekozen oplossing technisch gezien niet mogelijk om uit te loggen.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Toelichting Default content en niet correct afgehandelde foutmeldingen tonen informatie over het systeem.	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	

Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.02	**Beschikbaarheid van netwerken**
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	[redacted]
Toelichting DDoS en andere performancetesten vallen buiten de scope van de penetratietest.	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	

Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Toelichting Logius voert periodiek security tests uit waar vulnerability-assessments een onderdeel van zijn.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Toelichting Logius voert periodiek pentratietesten uit waar vulnerability-assessments een onderdeel van zijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.06	**Logging**

Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Toelichting Onvolledige logging, acties worden niet getoond, en geen identificerende kenmerken voor sessies (i.v.m. meerdere sessies die actief kunnen zijn).	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Toelichting Processen worden niet getest tijdens een penetratietest.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

De client betreft hier zowel de app als de webbrowser.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Een overzicht van deze bevindingen.

Gelijktijdige sessies				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
1		**Midden**	Midden	Hoog

Betreffende hosts

https://mijn.a3.digid.nl

Omschrijving

Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging

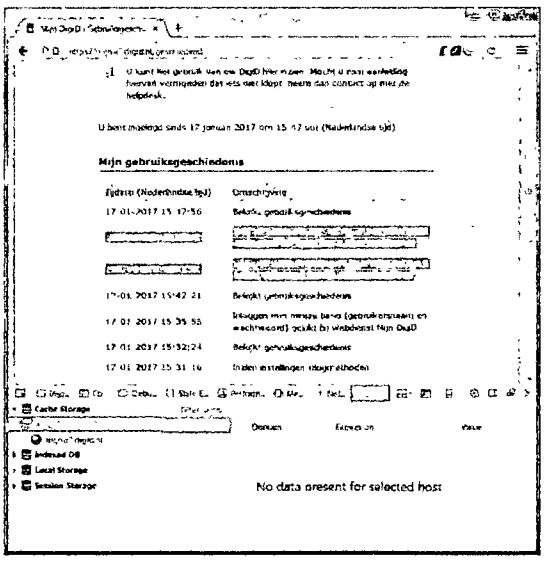
Een gebruikers-ID is gebonden aan één persoon. Meer dan één gelijktijdige sessie voor deze persoon betekent of dat andere sessies niet goed worden afgesloten of vergeten of dat een kwaadwillende de sessie beheert.

Aanbeveling

Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Op deze manier kan de gebruiker nooit worden uitgesloten door een vergeten sessie of een kwaadwillende. Als een kwaadwillende bijvoorbeeld een sessie start, kan de gebruiker dit als een waarschuwing zien dat er iets met zijn account is. Daarnaast kan een gebruiker dan inloggen om zo de sessie van de kwaadwillende af te sluiten.

Details

Het is mogelijk om op de mijn.a3.digid.nl omgeving meerdere actieve sessies per DigiD account te hebben. Dit houdt in dat er op meerdere apparaten wordt ingelogd met één DigiD account. Op dit moment toont de gebruikersgeschiedenis hiervan alleen twee inlogacties die binnen twee minuten van elkaar plaatsvinden, zoals in dit volgende screenshot:



Het was daarna mogelijk om op beide systemen acties uit te voeren op de mijnDigiD omgeving.

Sessies zijn niet aan een IP gebonden				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
2		**Opgelost**	Laag	Hoog

Betreffende hosts

https://mijn.a3.digid.nl

Opgelost

De DigiD applicatie heeft de mogelijkheid om ip-adressen te koppelen aan een gebruikerssessie. Voor de geteste A3 omgeving stond deze parameter op een incorrecte waarde. Tijdens de testperiode is deze aangepast en is de bevinding na hertest niet meer aangetroffen.

Omschrijving

De applicatiesessie is niet gekoppeld aan een IP-adres. Hierdoor is het mogelijk om een actieve sessie over te nemen op een ander IP-adres dan het IP-adres waar de sessie is geïnitieerd.

Bedreiging

Actieve sessie die worden gecompromitteerd kunnen worden gebruikt vanaf andere locaties / IP-adressen.

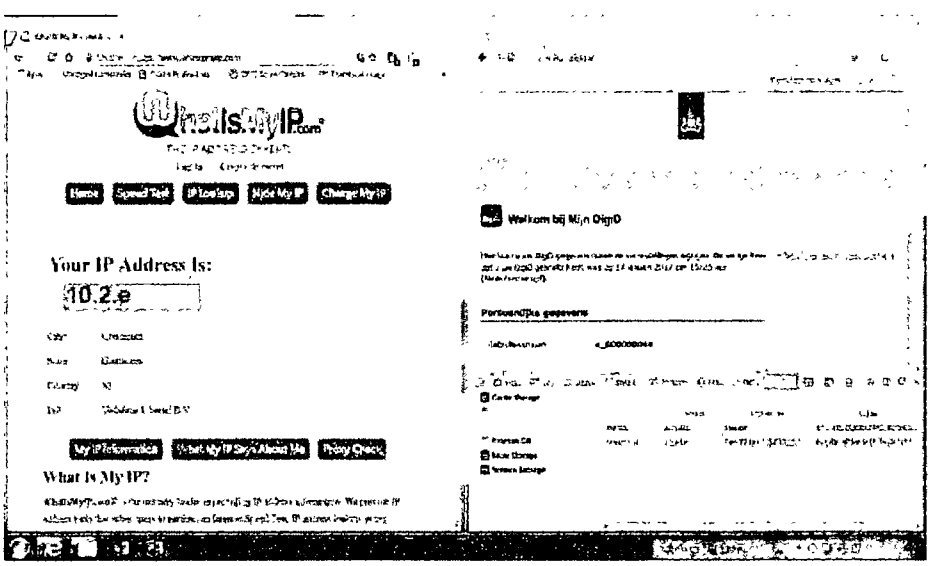
Aanbeveling

Bij het initiëren van de sessie moet deze aan een IP-adres worden gekoppeld. Daarna moet er bij elke actie worden gecontroleerd of de sessie vanaf het initiële IP-adres wordt gebruikt. Zo niet moet de sessie vernietigd worden.

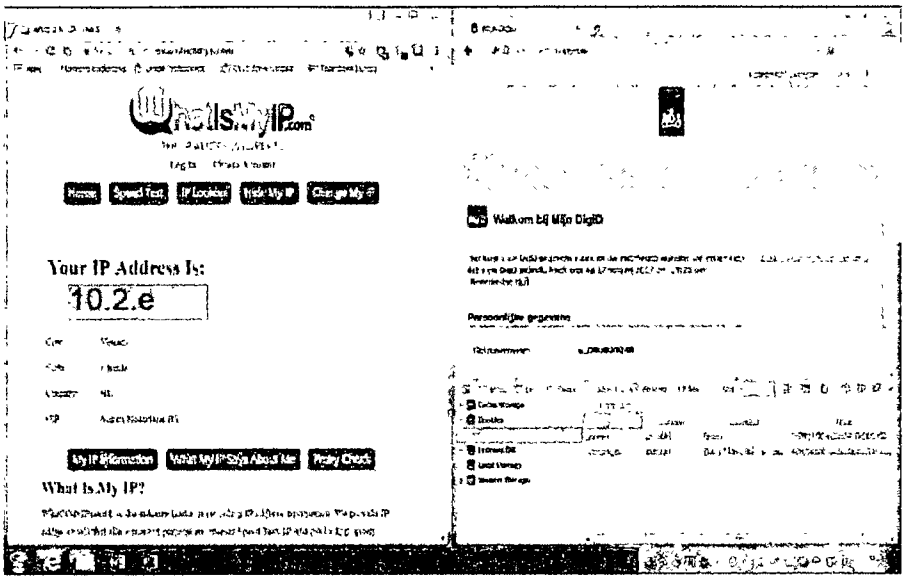
Details

In de mijnDigid omgeving vindt geen controle plaats of een sessie wordt gebruikt van een vast IP-adres.

In het volgende voorbeeld is te zien dat 1 sessie te gebruiken is op verschillende IP adressen. In eerste instantie werkt de actieve sessie (40e30ece.....) op IP adres 10.2.e :



Daarna wordt er van netwerk gewisseld 10.2.e) en worden de schermen ververst:



Het blijft mogelijk om binnen de actieve sessie pagina's aan te roepen. Het is aanbevolen om een sessie te koppelen aan een IP adres om te voorkomen dat actieve sessies gekaapt kunnen worden en op een ander IP adres kunnen worden misbruikt.

Geen mogelijkheid tot uitloggen				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
3		**Midden**	Midden	Midden

Betreffende hosts

https://digidbeheer-a3.digid.nl

Omschrijving

De applicatie bevat geen mogelijkheid om de gebruiker uit te loggen.

Bedreiging

Doordat de beheerder niet kan uitloggen heeft de beheerder geen mogelijkheid om de sessie af te breken. Hierdoor blijven sessies onnodig lang geldig. Een aanvaller heeft daardoor langer de mogelijkheid om de sessie over te nemen en een eventuele overname van de sessie kan langer misbruikt worden.

Aanbeveling

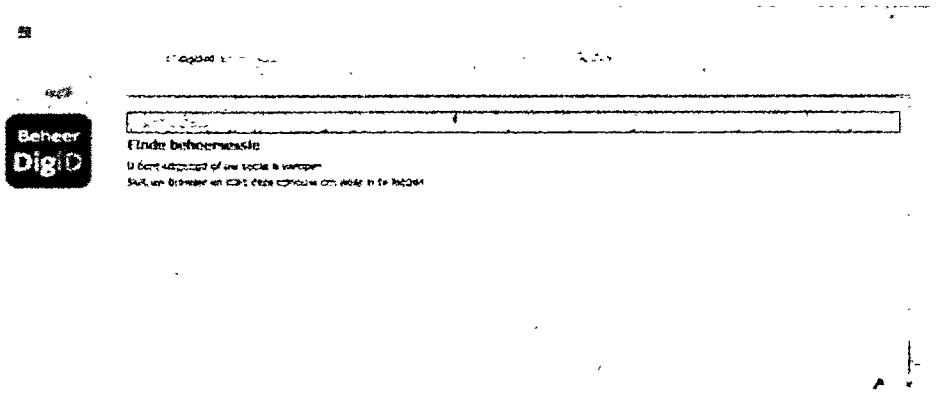
Regel de mogelijkheid in waarmee een gebruiker uit kan loggen. Door het uitloggen dient de sessie volledig afgebroken te worden.

Details

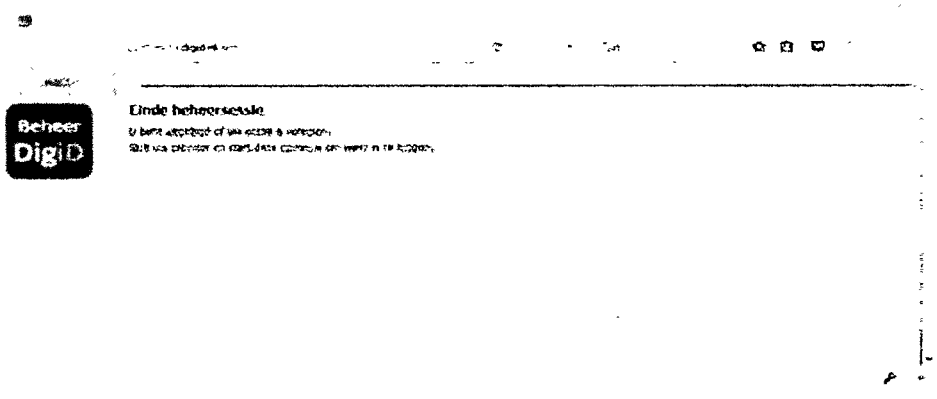
De beheerder kan inloggen op de digidbeheeromgeving met behulp van de client-side certificaten die zijn geleverd. Het scherm dat getoond wordt van de applicatie bevat ook de functie voor uitloggen, echter, deze lijkt niet correct te werken.

Wanneer de beheerder hierop klikt, wordt een 'destroy_session' call gedaan naar de server. Deze stuurt daarop een bericht terug met de

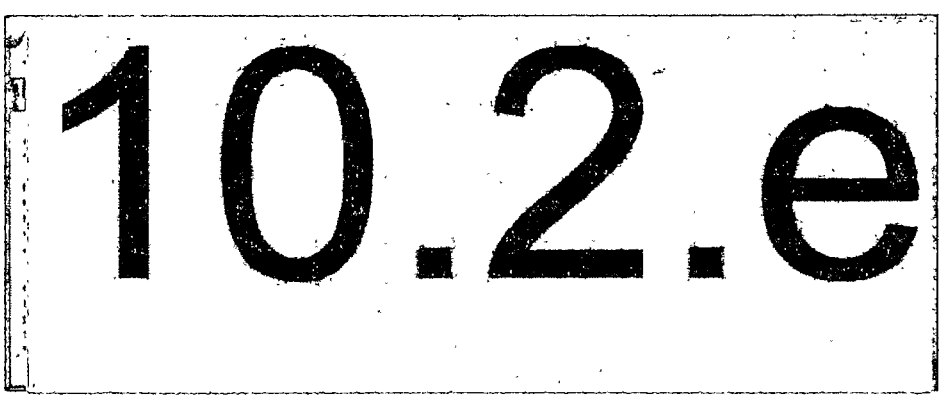
melding dat de browser opnieuw gestart moet worden zodat de gebruiker opnieuw kan inloggen. Echter, wanneer de browser gewoon open wordt gelaten, en de hoofdpagina van de omgeving (digidbeheer-a3.digid.nl) herladen wordt, blijkt de beheerder alsnog, dan wel opnieuw, ingelogd te zijn.



Wanneer de hoofdpagina opnieuw wordt opgevraagd verschijnt een afwijkende melding:



Bij het voor een tweede keer aanspreken van de hoofdpagina, verschijnt deze met de inhoud. Hij reageert daarbij alsof de beheerder gewoon ingelogd is:



De browser detecteert dat het om een verlopen sessie gaat en geeft een redirect op om weer uit te loggen. Deze is echter af te vangen door de

javascript die de redirect triggert uit te zetten. Hierdoor is het mogelijk gebruik te blijven maken van de beheerapplicatie.

Er wordt een nieuw sessie id aangeleverd vanuit de server. Het veranderen van dit sessie id naar de oorspronkelijke sessie id heeft geen effect. Het nieuwe sessie id blijft door de server in gebruik en de gebruiker is opnieuw, niet nog steeds, ingelogd. Dit lijkt een direct resultaat van het feit dat het certificaat als authenticatiemiddel wordt gebruikt.

Het is aan te raden de authenticatie voor de applicatie en de toegang tot de dienst los te koppelen. Zorg ervoor dat het certificaat alleen toegang verleent tot de dienst, en plaats een additioneel authenticatiemiddel tussen de gebruiker en de functionaliteit en inhoud van de applicatie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken door een matrix op te bouwen van de autorisaties en vervolgens horizontaal (andere rollen) en verticaal (andere gegevens) deze rechten proberen te escaleren.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

Onvoldoende invoervalidatie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
4		**Midden**	Laag	Hoog

Betreffende hosts

https://mijn.a3.digid.nl

Omschrijving

De invoer wordt door de server onvoldoende gevalideerd.

Bedreiging

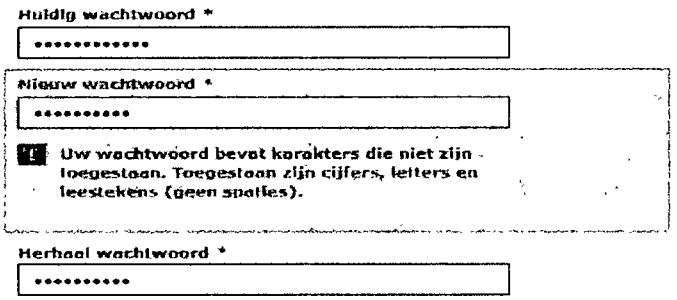
De gebruiker kan in principe alle communicatie van de client naar de server beïnvloeden. Dit betekent dat hij onverwachte, ongeldige of kwaadwillende invoer kan versturen en dat hij in de client ingebouwde controlemechanismen kan omzeilen. Als de server aanneemt dat de client alleen geldige en juiste invoer verstuurt kan een aanvaller wellicht data achterhalen of aanpassen of de werking van de applicatie beïnvloeden door de invoer te manipuleren.

Aanbeveling

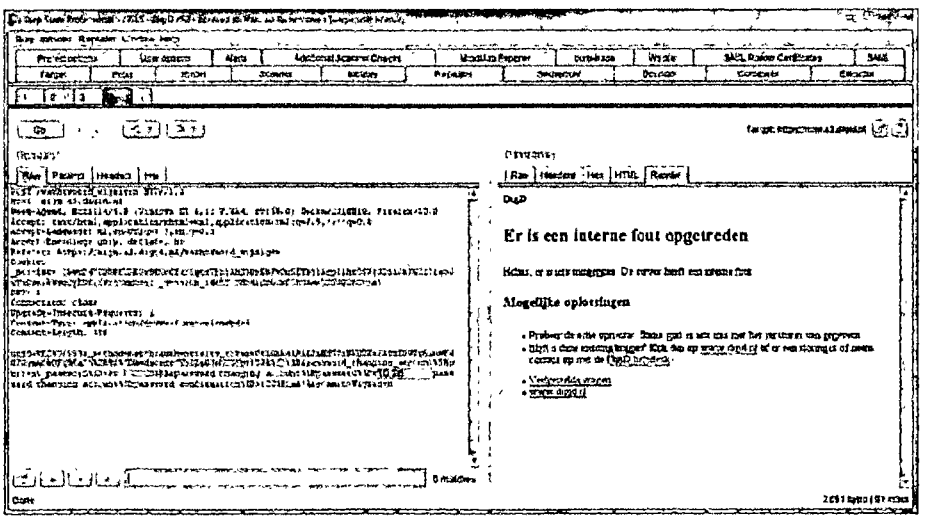
Zorg ervoor dat alle invoer door de server wordt gecontroleerd en gevalideerd voordat deze wordt verwerkt, opgeslagen of getoond.

Details

Bij het wijzigen van een wachtwoord moet het nieuwe wachtwoord aan diverse condities voldoen. Eén ervan is dat er alleen cijfers, letters en leestekens mogen worden gebruikt. In onderstaande voorbeeld wordt een diakritisch teken (å) meegenomen in het wachtwoord: 10.2g. Wanneer dit via de front-end verloopt, komt er een nette melding dat er ongeldige tekens worden gebruikt, zoals hieronder te zien.



Echter, wanneer het wachtwoord direct aan de back-end wordt geleverd (het request wordt afgevangen en in-transit aangepast) wordt er een melding getoond die afwijkt van de functionele melding. Dit lijkt op een niet afgehandelde foutsituatie:



Zorg ervoor dat de data die door de gebruiker wordt gestuurd ook op de server gevalideerd wordt op juiste tekens zodat een aanvaller het verkeer niet kan misbruiken om dit soort fouten te genereren of data dan wel code op de server te zetten die eventueel misbruikt kan worden.

Manipulatie zichtbaarheid loggegevens				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
5		**Laag**	Midden	Laag

Betreffende hosts

https://mijn.a3.digid.nl

Omschrijving

Een applicatie implementeert logging van verzoeken en transacties voor het uitvoeren van audits op het systeem. Mochten er toekomstige vragen ontstaan over (de juistheid van) bepaalde verwerkingen in het systeem kan een audit log onderdeel zijn van de bewijsvoering en/of assurance.

Bedreiging

Als een gebruiker van het systeem invloed kan uitoefenen op de inhoud van de gelogde entries of deze log functie (tijdelijk) kan uitschakelen verlaagt dit de auditeerbaarheid van het systeem.

Aanbeveling

Ontwerp de logpaden binnen de applicatie. Bepaal hierin welke gegevens worden gelogd en op welke punten in het proces dit plaats vindt. Houdt hierbij rekening met de gevoeligheid van de inhoud van de logging. Implementeer tevens een aparte logserver waar de notities voor het audit log naar worden gestuurd. Dit aparte component dient er zorg voor te dragen dat audit log entries niet kunnen worden gemuteerd of verwijderd buiten de reguliere processen hiervoor om.

Details

Wanneer een burger is ingelogd op de Digid omgeving, kan men de gebruikersgeschiedenis van het account bekijken. Deze worden opgedeeld in pagina's, met elk x acties. Ongeacht de hoeveelheid pagina's die werkelijk bestaan – content bevatten met gebruikersacties die worden weergegeven – is het mogelijk om elk willekeurig nummer in te vullen, zoals;

```
https://mijn.a3.digid.nl/geschiedenis?page=35900341
```

Dit toont het gebruikersgeschiedenisscherm waarin geen acties te zien zijn. Het aantal acties dat deze account heeft uitgevoerd zijn niet voldoende om deze pagina te vullen, en ziet er als volgt uit;

Gebruiksgeschiedenis

U kunt het gebruik van uw DigiD hier inzien. Mocht u een aanduiding hiervan vermoeden dat iets niet klopt, neem dan contact op met de helpdesk.

U bent ingelogd sinds 16 januari 2017 om 11:13 uur (Nederlandse tijd)

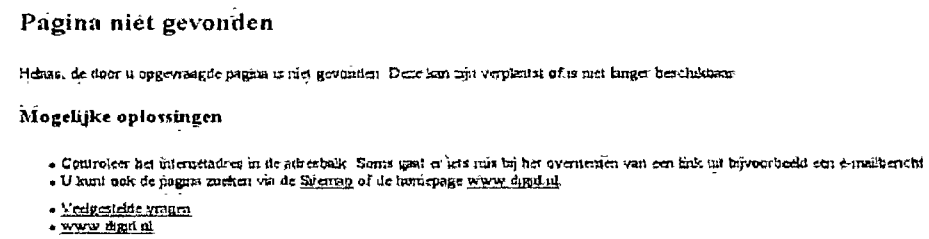
Mijn gebruiksgeschiedenis

Tijdstip (Nederlandse tijd) Omschrijving
Vorige | 1 | | 3364 | Volgende
Meer Mijn gegevens

Dit is te herhalen tot en met pagina 10000000. Wanneer er echter een pagina hoger dan 100000 wordt opgevraagd, verschijnt er een foutmelding.

https://mijn.a3.digid.nl/geschiedenis?page=10000001

Dit leidt tot;



Pagina niet gevonden

Helaas, de door u opgevraagde pagina is niet gevonden. Deze kan zijn verplaatst of is niet langer beschikbaar.

Mogelijke oplossingen

- Controleer het internetadres in de adresbalk. Soms gaat er iets mis bij het overnemen van een link uit bijvoorbeeld een e-mailbericht
- U kunt ook de pagina zoeken via de Sitemap of de homepage www.digid.nl.
- Veelgestelde vragen
- www.digid.nl

De hoeveelheid pagina's die een burger maximaal kan bekijken zouden niet beperkt moeten zijn, tenzij de burger op een andere manier (sms/email/app) notities kan ontvangen over acties. Bestaat dit tweede kanaal niet **en** is de hoeveelheid pagina's handmatig beperkt, dan bestaat de kans dat een aanvaller zijn gedane acties buiten de voor de gebruiker zichtbare gebruikersgeschiedenis kan schuiven.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Zo kan de manier van authenticatie en autorisatie per omgeving verschillen, maar wel gebruik maken van dezelfde bronnen. Ook kunnen afhankelijkheden zijn tussen verspreide bronnen. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

Default content				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
6		**Laag**	Midden	Laag

Betreffende hosts

https://a3.digid.nl
https://mijn.a3.digid.nl

Omschrijving

De software wordt meegeleverd met voorbeeldcontent of -functionaliteit, zoals een management console met standaard gebruikersnaam en wachtwoord dan wel een 'lorem ipsum' tekst.

Bedreiging

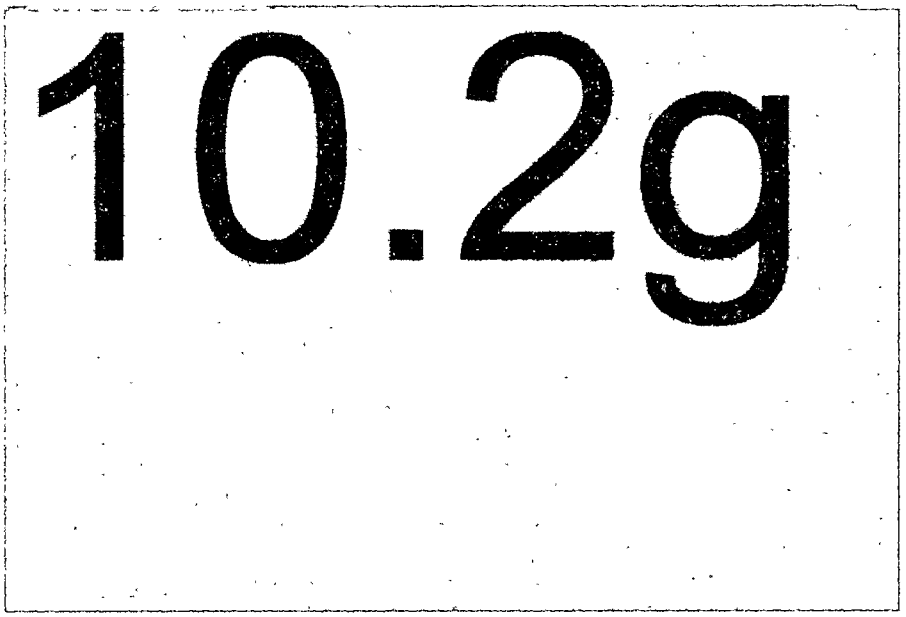
De informatie in de default content kan gebruikt worden om de software te identificeren of standaard zwakheden uit te buiten. Bij een standaard gebruikersnaam en wachtwoord combinatie is het voor een aanvaller vrij eenvoudig om in te loggen en instellingen te wijzigen.

Aanbeveling

Zet niet gebruikte standaardmogelijkheden uit, verwijder de standaardteksten en pas standaardwachtwoorden altijd aan.

Details

De webserver bevat nog onderdelen die bij een installatie standaard worden geïnstalleerd. Deze zijn in dit geval niet opgeruimd en geven de aanvaller daarmee inzicht in de gebruikte componenten.
Het bezoeken van de URLs 10.2g dat nog niet alle default content is verwijderd. Zie het volgende screenshot:



Zorg ervoor dat deze standaardinstallatieonderdelen verwijderd worden, en werk de installatieprocedure bij zodat dit bij de installatie gelijk wordt afgevangen.

Information disclosure – Versieinformatie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
7		Midden	Hoog	Laag

Betreffende hosts

https://a3.digid.nl

Omschrijving

Systemen geven vaak zelf onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een default instelling van de software.

Bedreiging

Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling

Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versieinformatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details

Het is op dit moment mogelijk de software en versie van de server te achterhalen. Bij het doen van een ongeldig verzoek naar de server toont deze de software en de versie bij de foutafhandeling. Dit gebeurt bij het gebruiken van een methode die niet ondersteund wordt;

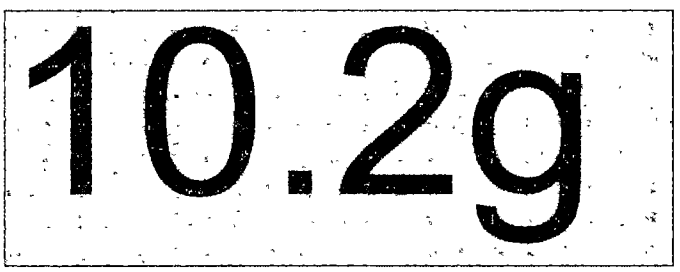
Request

```
TRACE /assets/favicon.ico HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101
Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Cookie:
_persist=!Pvo8TqF0kwwca50Or90XoCZarSqtsbJ3R8xZ+u1blWIYsOpH1Orru3AB7mS
RQtNbTkk/sctOb7ewSop4Dwk/pnwCduPkFvJBT/Idgvo=;
_session_id=9d83c95e90594ee8cfd29363230becef
Connection: close
```

Maar ook bij het aanroepen van een niet geldige URL, zoals;

```
https://mijn.a3.digid.nl/aanvragen%-1
```

De server toont daarop de volgende melding:



Pas de foutafhandeling op de server aan zodat er geen informatie over de achterliggende architectuur wordt gestuurd.

Onvolledige logging – geen uitlogacties in gebruikergeschiedenis				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
8		**Midden**	Midden	Midden

Betreffende hosts

https://mijn.a3.digid.nl

https://a3.digid.nl

Omschrijving

Een log wordt gebruikt om alle gebeurtenissen van een bepaald proces of systeem bij te houden, ook wel logging genoemd. Het kan voorkomen dat logging minder informatie weergeeft dan noodzakelijk is voor het correct interpreteren van de informatie in het systeem.

Bedreiging

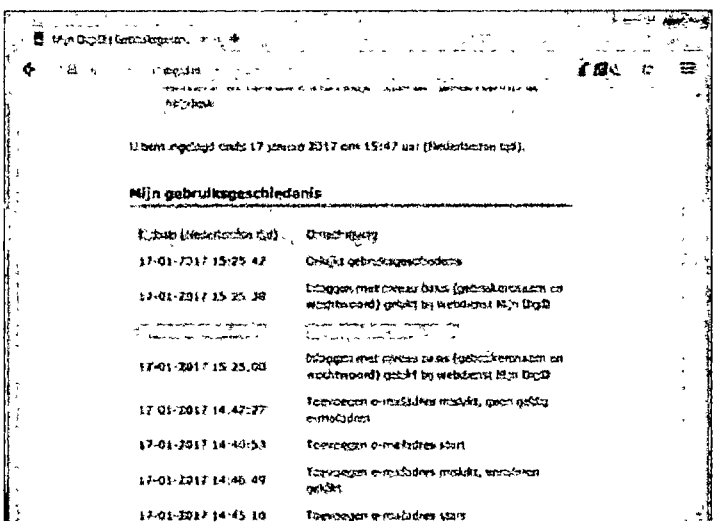
Door gebrekkige logging kunnen mogelijke technische problemen en aanvallen onopgemerkt blijven. Tevens kunnen gebeurtenissen niet meer worden achterhaald en herleid in geval van misbruik.

Aanbeveling

Registreer alle gebeurtenissen op elke server en elk proces. Controleer deze logs periodiek om technische problemen en/of aanvallen te kunnen detecteren en in de toekomst te kunnen mitigeren.

Details

Het is aanbevolen om de uitlogacties, die vanuit de gebruiker worden geïnitieerd, ook vast te leggen in de gebruikersgeschiedenis. Dit zal een gebruiker beter inzicht geven in het gebruik van het account en het daarbij mogelijk maken om security incidenten sneller waar te nemen. Op dit moment worden alleen de verlopen sessies getoond in de gebruikersgeschiedenis:



Onvolledige logging - geen identificerende kenmerken van sessie of apparaat waarmee is ingelogd in gebruikersgeschiedenis				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
9		**Midden**	Midden	Midden

Betreffende hosts

https://mijn.a3.digid.nl

https://a3.digid.nl

Omschrijving

Een log wordt gebruikt om alle gebeurtenissen van een bepaald proces of systeem bij te houden, ook wel logging genoemd. Het kan voorkomen dat

logging minder informatie weergeeft dan noodzakelijk is voor het correct interpreteren van de informatie in het systeem.

Bedreiging

Door gebrekkige logging kunnen mogelijke technische problemen en aanvallen onopgemerkt blijven. Tevens kunnen gebeurtenissen niet meer worden achterhaald en herleid in geval van misbruik.

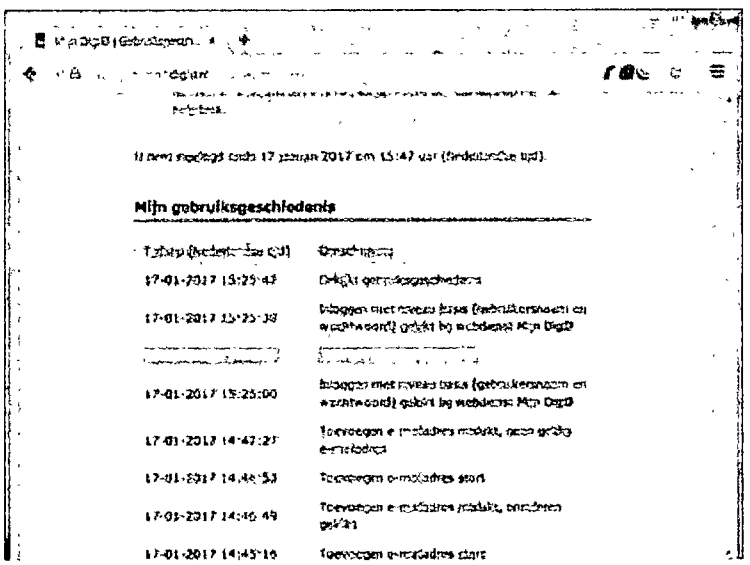
Aanbeveling

Registreer alle gebeurtenissen op elke server en elk proces. Controleer deze logs periodiek om technische problemen en/of aanvallen te kunnen detecteren en in de toekomst te kunnen mitigeren.

Details

De logging toont op dit moment geen identificerende kenmerken voor de sessie of het apparaat waarmee de gebruiker is ingelogd. Daar het mogelijk is om met meerdere apparaten tegelijkertijd in te loggen met hetzelfde DigiD – wat leidt tot twee sessies voor één Digid (zie bevinding 1: gelijktijdige sessies) – is het aan te raden deze als dusdanig te kenmerken. Dit zal een gebruiker beter inzicht geven in het gebruik van het account en het daarbij mogelijk maken om security incidenten sneller waar te nemen.

Zoals hieronder te zien is dat op dit moment nog niet het geval;



4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport

DigiD R5.3 en Substantieel

Kenmerk: 2017/14

Datum	5-7-2017
Status	Definitief
Versie	1.0

Rubricering derubricering

Colofon

Kenmerk	2017/14
Versienummer	1.0
Contactpersoon	10.2.e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
13-06-2017	0.1	Sogeti Nederland B.V.	Initiële versie
13-06-2017	0.2	Sogeti Nederland B.V.	Interne review
27-06-2017	0.9	Sogeti Nederland B.V.	Resultaten hertest verwerkt
5-7-2017	1.0	Sogeti Nederland B.V.	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2.e	10.2.e		
10.2.e	10.2.e	10.2.e	Logius
10.2.e	10.2.e	10.2.e	Logius
10.2.e	10.2.e	10.2.e	Logius
10.2.e	10.2.e	10.2.e	Logius
10.2.e	10.2.e	10.2.e	Sogeti
10.2.e	10.2.e	10.2.e	Sogeti
10.2.e	10.2.e	10.2.e	Sogeti
10.2.e		10.2.e	Capgemini

Inhoud

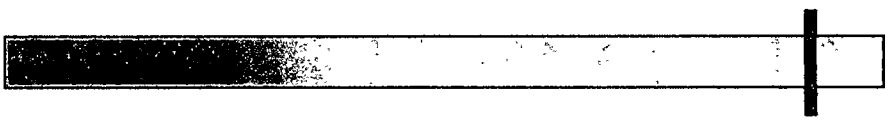
Managementsamenvatting

Inleiding

Logius heeft Sogeti gevraagd een securitytest uit te voeren op de acceptatieomgeving van DigiD. Het onderzoek is uitgevoerd op 11 mei 2017 en van 6 juni 2017 tot en met 12 juni 2017 en is uitgevoerd door 102.e. Tevens is er een hertest op een aantal gedane bevindingen uitgevoerd op 20 juni 2017.

Conclusies en aanbevelingen

- De applicatie telt voor het complexe landschap weinig bevindingen. Er zijn geen bevindingen gedaan met hoge of kritieke risicoclassificatie;
- Tijdens de hertest op 20-06-2017 is een aanzienlijk deel van de bevindingen opgelost. Deze zijn in de rapportage gemarkeerd als opgelost.



Onvoldoende Voldoende

Punten ter verbetering.

- Het is mogelijk om meerdere malen tegelijkertijd te zijn ingelogd in DigiD. Er geldt wel een restrictie op IP-adres. Een aanvaller zou echter veel moeite moeten doen om een sessie over te nemen en deze te misbruiken.

  Zorg voor een correcte implementatie van sessiemanagement. Zorg daarnaast voor logging waarbij gebruikers zelf inzicht kunnen krijgen in mogelijk misbruik.

- De logica in de applicatie is te gebruiken zodat er een grote hoeveelheid e-mails wordt gestuurd naar een gebruiker als er herhaaldelijk e-mail adres wordt toegevoegd aan een gebruiker en daarna weer wordt verwijderd.

  Controleer of deze functionaliteit naar behoren werkt of aangepast dient te worden.

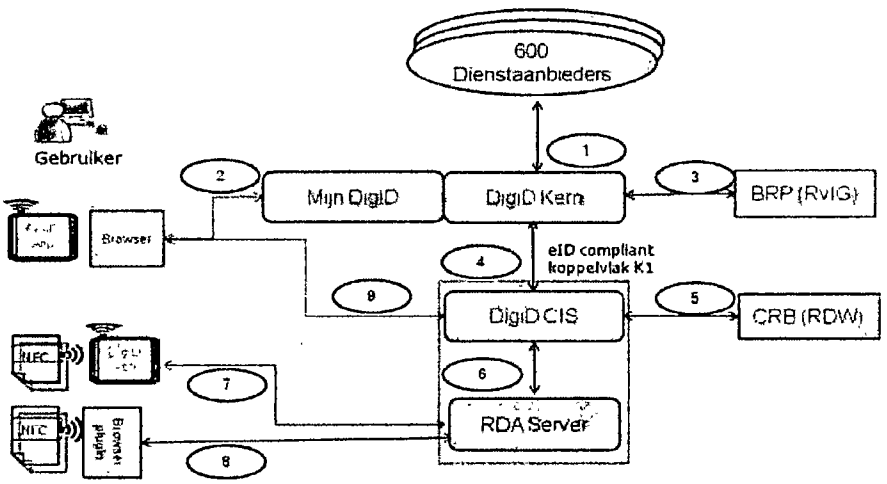
Aanvullingen Logius

Reactie van Logius.

1 Inleiding

1.1 Opdrachtformulering

De aanleiding tot deze securitytest betreft de realisatie en beoogde implementatie van het betrouwbaarheidsniveau Substantieel. Daartoe heeft Logius aanpassingen doorgevoerd aan DigiD als onderdeel van Release 5.3, is een RDA-server aan DigiD toegevoegd, is de DigiD app gewijzigd, is een nieuwe koppeling naar RDW gerealiseerd en is de koppeling met de BRP aangepast.



Het doel is om inzicht te krijgen in het beveiligingsniveau van DigiD en de risico's die Logius loopt indien de aanpassingen in uitbreidingen ten gevolge van DigiD Substantieel in de productieomgeving worden geïnstalleerd.

Daarnaast is het doel het beveiligingsniveau te handhaven of te verbeteren nadat er wijzigingen in de applicatie zijn aangebracht, en detectie of eerder geconstateerde risico's zijn weggenomen en er geen nieuwe risico's zijn geïntroduceerd als gevolg van deze wijzigingen.

Het gaat om het vaststellen van de beveiliging van geheel DigiD; er zal extra aandacht worden geschonken aan de wijzigingen en uitbreidingen als gevolg van de implementatie van DigiD Substantieel.

Ook is het verzoek een hertest uit te voeren van een eerdere bevinding gerelateerd aan de koppeling van de gebruikerssessie en het gebruikte IP adres.

De nadruk van de testen ligt op de technische beveiligingsrisico's. In overleg met Logius zal er, waar nodig, naar de business risico's gekeken worden.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd, zoals beschreven in het bijbehorende Plan van Aanpak.

1.3 Scope van de werkzaamheden

De Scope is *de gehele* DigiD applicatie, inclusief het koppelvlak met de app, met *extra aandacht voor* de aanpassingen die als onderdeel van R5.3 aan DigiD zijn uitgevoerd en de uitbreidingen van DigiD die in het kader van DigiD Substantieel zijn uitgevoerd. Dit zijn:

- DigiD kern is uitgebreid
- BRP connect is uitgebreid
- CIS is uitgebreid
- CRB is nieuw
- RDA server is nieuw
- De connectie App->RDA is nieuw

De wijzigingen in usecases hebben onderstaande productrisico's tot gevolg en krijgen extra aandacht tijdens de test:

Productrisico's met betrekking tot DigiD kern/CIS/RDA/admin/balie/reporting	
Er is sprake van informatie leakage o.a. b j QR-code, meldingen, foutmeldingen waardoor er meer informatie wordt vrijgegeven dan nodig. Deze informatie kan misbruikt worden door kwaadwillenden.	5.3
Bij het gebru k van de SMS-code is er een kans dat de code wordt onderschept waardoor daar misbru k van gemaakt kan worden	5.3
De testfunctionaliteit is in productie te activeren	5.3
Productrisico's met betrekking tot de app	
In SDK zitten onveilige onderdelen waardoor de verbinding tussen app en RDA onveilig is	Subs
Er wordt gebruik gemaakt van onveilige protocollen waardoor misbru k gemaakt kan worden van de applicaties	5 3 / Subs
Er is sprake van informatie leakage o.a. b j meldingen en foutmeldingen waardoor er meer informatie wordt vr jgegeven dan nodig. Deze informatie kan misbru kt worden door kwaadwillenden.	Subs
Productrisico's met betrekking tot de keten	
Bij het gebru k van de CRB koppeling lekken van gegevens (zoals BSN en rijbewijsnummer) waarmee misbruik gepleegd kan worden.	5 3
Productrisico's met betrekking tot overig beheer (Capgemini)	
Het bl jkt mogelijk om ongeautoriseerd toegang te krijgen tot het id.ie [redacted] waardoor niveau Substantieel onvoldoende betrouwbaar is (hangt aan CR005)	Subs
Logging RDA blijkt niet te werken waardoor er geen analyse van misbruik kan plaatsvinden.	5.3
De logging van de RDA server is toegankelijk voor onbevoegden zodat logging ongeautoriseerd gewijzigd kan worden of ingezien kan worden	Subs
De RDA is toegankelijk voor onbevoegden zodat er veilgiheidsrisico's ontstaan.	Subs
Firewall instellingen blijken onjuist waardoor er veiligheidsrisico's bestaan.	5.3 / Subs
Productrisico's specifiek met betrekking tot de beveiliging	
Software bl jkt onvoldoende beveiligd tegen inbraak waardoor kwaadwillenden ongeautoriseerde toegang hebben met het systeem DigiD	5.3 / Subs
Productrisico's met betrekking tot de PAP	
De opgeleverde producten (software e.d.) voldoen niet aan de PAP eisen	5.3 / Subs

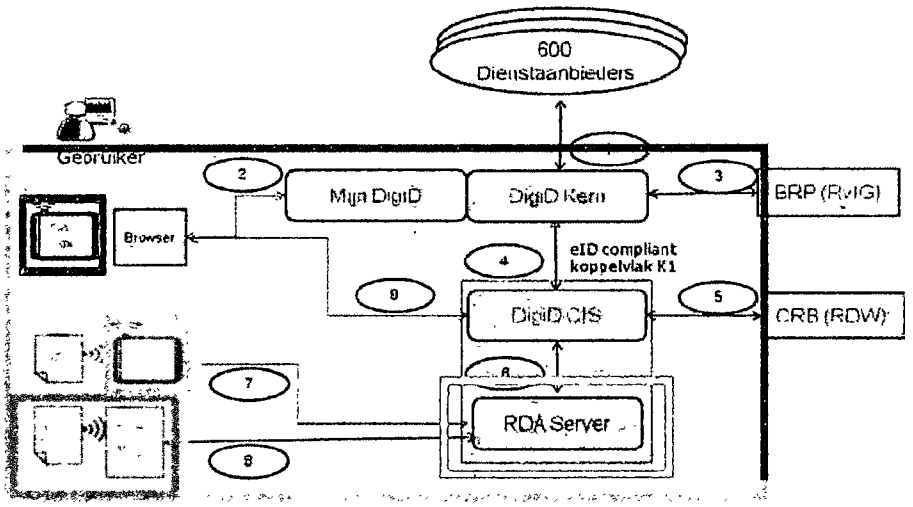
Hiernaast is een algehele securitytest uitgevoerd ter detectie van eventuele regressie dan wel ongeautoriseerde of onbedoelde changes.

Aanvullend is het verzoek gedaan om de volgende testgevallen expliciet te benoemen:

- Controle op gebruik HTTPS;
- Controle op foutafhandeling;
- Controle op de koppeling IP-adres en sessie.

De scope wordt grafisch weergegeven in onderstaande afbeelding door de rode omlijning. Het blauwe kader valt buiten scope. Dit onderdeel, de browser plug-in, wordt nog niet in gebruik genomen. *Het koppelvlak tussen de toekomstige browser plug-in en de RDA server is wel gecontroleerd.*

Binnen het groene kader zijn alle koppelingen met de RDA-server, en alle risico's die samenhangen daarmee en bijvoorbeeld met het oneigenlijk toegang krijgen tot de RDA-server of vanuit daar tot de VPC's op het platform wel onderzocht. De applicatie zelf is buiten scope. Het oranje kader omlijnt de app. Ook deze valt buiten scope. Het koppelvlak naar DigiD kern, DigiD CIS en de RDA server wordt wel meegenomen.



De securitytest richtte zich op de volgende systemen in de *A3* omgeving[1]:

Onderwerp	URL	IP-adres
Mijn DigiD	https://mijn.a3.digid.nl	144.43.243.145
Aanvragen	https://a3.digid.nl/aanvragen	144.43.243.144
Activeren	https://a3.digid.nl/activeer_digid	144.43.243.144
Herstellen	https://a3.digid.nl/herstellen	144.43.243.144
Koppelvlakken	https://was-a3.digid.nl	144.43.243.146
Beheermodule	https://digidbeheer-a3.digid.nl	144.43.243.148
Balie	https://balie-a3.digid.nl	144.43.243.147
DigiD CIS	https://cis-a3.digid.nl	144.43.243.150

[1] In het overleg over de 10.2g upgrade is aan de orde gekomen dat de A3 en A4 omgevingen niet geheel representatief voor Productie zijn. Dit kan mogelijk de testresultaten beïnvloeden.

RDA	https://rda-a3.digid.nl	144.43.243.152

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

De resultaten van de hertest zijn meegenomen; opgeloste bevindingen zijn opgenomen in de kolom *opgelost*.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Opgelost	Totaal
Client-side controls				2			2
Logica							
Authenticatie						2	2
Sessiemanagement			1			1	2
Functie specifieke invoer							
Toegang							
Invoerafhandeling				1			1
Omgeving							
Servers			2	2	1	6	11
Totaal			3	5	1	9	18

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[2], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Kleur	Uitleg	Aantal
	Niet getest, buiten scope.	17
	Er wordt niet afgeweken van de norm.	21
	De norm wordt gedeeltelijk nageleefd.	5
	Er wordt afgeweken van de norm.	0

Beleidsdomein

B.01	Informatiebeveiligingsbeleid
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	

[2] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de	

vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Toelichting: Er bestaat een kans dat, door het gebruik van zwakkere block ciphers in de versleutelde communicatie, verkeer tijdens transport kan worden afgeluisterd.	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Toelichting: Default content en niet correct afgehandelde foutmeldingen geven informatie over het systeem.	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Toelichting: Het is mogelijk voor een gebruiker om via hetzelfde IP adres meerdere sessies open te hebben.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	

derubricering

Toelichting: Default content toont informatie over het systeem.	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.02	**Beschikbaarheid van netwerken**
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Toelichting: DDoS en andere performancetesten vallen buiten de scope van de penetratietest.	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	

Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Toelichting: Logius voert periodiek security tests uit waar vulnerability-assessments een onderdeel van zijn.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Toelichting: Logius voert periodiek security tests uit waar vulnerability-assessments een onderdeel van zijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	

Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Toelichting: Geen identificerende kenmerken voor sessies (i.v.m. meerdere sessies die actief kunnen zijn).	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

Secure-flag ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
1		Laag	Laag	Laag

Betreffende hosts
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de *Secure*-flag mee te geven in de *Set-cookie*-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding, kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruik maakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker naar een HTTP-pagina binnen het domein van de applicatie te lokken. Tenzij er gebruik gemaakt wordt van de *HTTP Strict Transport Security*-header zal de browser de cookies dan naar deze (niet-bestaande) pagina versturen waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van de cookie naar de gebruiker moet Secure op de volgende manier aan de Set-Cookie-header worden toegevoegd:
Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; ***Secure***
Voor meer informatie over de Secure-flag en hoe deze te implementeren zie: https://www.owasp.org/index.php/SecureFlag

Let wel: Als de cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan de cookie op dat moment nog onderschept worden.

Details
De host: cis-a3.digid.nl stuurt de volgende twee cookies zonder secure flag:

```
_digid_cis_session
persist_cis
```

HTTP Response:

```
HTTP/1.1 200 OK
Date: Tue, 06 Jun 2017 10:02 12 GMT
X-Request-Id: 7e9125e6-52e0-4fb5-9a53-b1026846b06b
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-Runtime: 0.006606
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _digid_cis_session=8e5456f9aa7649671e0f76d15131e707;
path=/; expires=Tue, 06 Jun 2017 10:17:12 -0000; HttpOnly
Status: 200 OK
Content-Length: 2
Connection: close
Content-Type: text/plain; charset=utf-8
Set-Cookie:
persist_cis=!hEWlPQwdnHZGWZV8aojjirYC1E4er4DlbOE2mm9Gwv7i6nrVYh8ZwFix7
cHJ7b3BFeUVAbFo3jVjZwHNBKMwrgNAxqmzQtdN6vBnL/U=; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

ok
```

De host rda-a3.digid.nl stuurt de volgende cookie zonder secure flag:

```
JSESSIONID
```

HTTP Response:

```
HTTP/1.1 403 Forbidden
Set-Cookie: JSESSIONID=D35AFC867998BCB5C276CA45A3810C46; Path=/;
HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 114
Date: Wed, 07 Jun 2017 11:03:57 GMT
Connection: close
Set-Cookie:
_persist='bymZFjXtaJKprDT+5aqg61TJU5Hb5XaeQ60fq9dIABHTcvIZuhkzI9MZIiaP
0nTfKIU2xC0QcP7tWm2QIGo987zHivFvNpL6Y2so1q0=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest 20-6-2017
Deze kwetsbaarheid was niet verholpen op het moment van de hertest.

HTTP Request:

```
GET /host-manaager/ HTTP/1.1

Host: rda-a3.digid.nl

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Language: nl,en-US;q=0.7,en;q=0.3

Connection: close

Upgrade-Insecure-Requests: 1
```

HTTP Response:

```
HTTP/1.1 404 Not Found

Set-Cookie: JSESSIONID=28485FCEF1B3CD163558DAE303063E1; Path=/;
HttpOnly

Content-Type: text/html;charset=ISO-8859-1

Content-Length: 114

Date: Tue, 20 Jun 2017 05:54:09 GMT

Connection: close

Set-Cookie:
_persist=!y2pL9VDjpfabbR7+5aqg61TJU5Hb5aTlOeQLU0pBnVq5XIs8yINDqps3mgkk
YfXVVEgLKuEv1fGoqzr2tlAdluJHDiUbpPyomb3zNq0=;domain=.digid.nl;
HttpOnly;secure; path=/

X-FRAME-OPTIONS: SAMEORIGIN

Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

HttpOnly-flag ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
2		Laag	Laag	Laag

Betreffende hosts
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de *HttpOnly*-flag mee te geven in de *Set-Cookie*-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog gebruiken bij HTTP-verzoeken. De cookies kunnen dan niet gelezen of aangepast worden door client-side code zoals JavaScript en Flash.

Bedreiging
Als een aanvaller code kan uitvoeren in de browser van de gebruiker (bijvoorbeeld middels Cross-Site Scripting) heeft hij bij het ontbreken van de HttpOnly-flag ook toegang tot de cookies. Hij kan deze dan uitlezen en manipuleren, waardoor het in sommige gevallen mogelijk is om de sessie-id te stelen en de sessie van de gebruiker over te nemen.

Aanbeveling
Bij het versturen van de cookie naar de gebruiker moet HttpOnly op de volgende manier aan de Set-Cookie-header worden toegevoegd:
Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; ***HttpOnly***
Voor meer informatie over HttpOnly-cookies en hoe deze te implementeren zie: https://www.owasp.org/index.php/HttpOnly

Details

De host cis-a3.digid.nl stuurt de volgende cookie zonder HTTP only flag:

```
persist_cis
```

HTTP Response:

```
HTTP/1.1 200 OK
Date: Tue, 06 Jun 2017 10:02:12 GMT
X-Request-Id: 7e9125e6-52e0-4fb5-9a53-b1026846b06b
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-Runtime: 0.006606
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _digid_cis_session=8e5456f9aa7649671e0f76d15131e707;
path=/; expires=Tue, 06 Jun 2017 10:17:12 -0000; HttpOnly
Status: 200 OK
Content-Length: 2
Connection: close
Content-Type: text/plain; charset=utf-8
Set-Cookie:
persist_cis=!hEWlPQwdnHZGWZV8aojjirYC1E4er4DlbOE2mm9Gwv7i6nrVYh8ZwFix7
cHJ7b3BFeUVAbFo3jVjZwHNBKMwrgNAxqmzQtdN6vBnL/U=; path=/;
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

ok
```

Hertest 20-6-2017

Deze kwetsbaarheid was niet verholpen op het moment van de hertest voor host cis-a3.digid.nl. Voor host rda-a3.digid.nl is de kwetsbaarheid verholpen.

De host rda-a3.digid.nl stuurt de volgende cookie zonder HttpOnly flag:

```
JSESSIONID
```

HTTP Response:

```
HTTP/1.1 403 Forbidden
Set-Cookie: JSESSIONID=D35AFC867998BCB5C276CA45A3810C46; Path=/;
HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 114
Date: Wed, 07 Jun 2017 11:03:57 GMT
Connection: close
Set-Cookie:
_persist='bymZFjXtaJKprDT+5aqg6lTJU5Hb5XaeQ60fq9dIABHTcvIZuhkzI9MZIiaP
0nTfKIU2xC0QcP7tWm2QIGo987zHivFvNpL6Y2solq0=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet-doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Een overzicht van deze bevindingen.

Information disclosure				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
3		Opgelost	Zeer laag	Zeer laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Het systeem geeft informatie vrij over de (interne) werking/logica van het systeem zelf, de onderliggende infrastructuur, privacy gevoelige data of gerelateerd aan toegangsmanagement.

Bedreiging

De informatie kan een aanvaller inzicht verlenen welke als een springplank kan dienen voor aanvallen op het systeem: gelekte sessietokens kunnen het toegangsbeheer ondermijnen, versieinformatie ontsluit het patchlevel, stacktraces geven inzicht in interne logica en gebruikte technologie, open directories over het onderliggende besturingsysteem, hostnames en IP-adressen geven inzicht in de netwerkimplementatie, etc.

Aanbeveling

Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie, en zorg dat foutmeldingen aan eindgebruikers zonder systeeminformatie getoond worden.

Details

10.2g

Een aanvaller kan deze informatie gebruiken als springplank voor misbruik van het systeem..

Hernoem het authenticatie realm zodat hier geen technologie-informatie uit te herleiden is.

HTTP request:

```
GET 10.2g HTTP/1.1
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie:
_persist=!mOg0sJk4PDBM7/7+5aqg61TJU5Hb5VKr9H+jy9CVIQfiqEgyk/7LT8vcS1Oh
hfdvgBt2JLQVFlpS3zmB6V4JdWPb1mrXrC3Bh1P9m94=;
JSESSIONID=D3CFA044ABE02B3F6A1CBDDDC83BA1C5
Connection: close
```

HTTP response:

```
HTTP/1.1 401 Unauthorized
Cache-Control: private
Expires: Thu, 01 Jan 1970 01:00:00 CET
10.2g
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2044
Date: Thu, 11 May 2017 10:39:29 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest 20-6-2017
De kwetsbaarheid was verholpen op het moment van de hertest.

Authenticatie door middel van Basic Authentication				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
4		Opgelost	Zeer laag	Zeer laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Onveilige verzending van credentials zoals gebruikersnaam en wachtwoord.

Bedreiging

Er zijn talloze manieren om authenticatie te implementeren in een applicatie. In dit geval wordt gebruikgemaakt van Basic Authentication. Dit komt erop neer dat de combinatie van gebruikersnaam en wachtwoord met base64 wordt geëncodeerd. Bij elk verzoek dat naar de server gestuurd wordt, wordt de geëncodeerde string meegestuurd. Dit is een van de minst veilige methoden van verzending, omdat base64-encodering eenvouding terug te draaien is en dus geen bescherming biedt.

Aanbeveling

Verstuur bij voorkeur alleen een op tijd gebaseerde afgeleide van de inloggegevens mee. Meestal is een afgeleide al voldoende om als authenticatiefactor te dienen. Als het technisch noodzakelijk is de credentials onversleuteld naar de server te sturen, zorg er dan voor dat de applicatie *stateful* is en dit maar maximaal 1x per sessie gebeurt.

derubricering

Details

Deze bevinding is tijdens de hertest opgelost

De 10.2g pagina maakt gebruik van Basic Authentication. Vervang het authenticatiemechanisme voor een veiligere variant.

HTTP request:

```
GET 10.2g HTTP/1.1
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie:
_persist=!mOg0sJk4PDBM7/7+5aqg61TJU5Hb5VKr9H+jy9CVIQfiqEgyk/7LT8vcS1Oh
hfdvgBr2JLQVFlpS3zmB6V4JdWPb1mrXrC3Bh1P9m94=;
JSESSIONID=D3CFA044ABE02B3F6A1CBDDDC83BA1C5
Connection: close
```

HTTP response:

```
HTTP/1.1 401 Unauthorized
Cache-Control: private
Expires: Thu, 01 Jan 1970 01:00:00 CET
10.2g
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2044
Date: Thu, 11 May 2017 10:39:29 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest 20-6-2017
Deze kwetsbaarheid is tijdens de hertest verholpen en geverifieerd.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de inloggegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client meestuurt naar de server. Hiermee wordt de actie geautoriseerd.

Een overzicht van deze bevindingen.

Sessies zijn niet aan een IP gebonden				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
5		Opgelost	Laag	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
De applicatiesessie is niet gekoppeld aan een IP-adres. Hierdoor is het mogelijk om een actieve sessie over te nemen op een ander IP-adres dan het IP-adres waar de sessie is geïnitieerd.

Bedreiging

Actieve sessie die worden gecompromitteerd kunnen worden gebruikt vanaf andere locaties / IP-adressen.

Aanbeveling

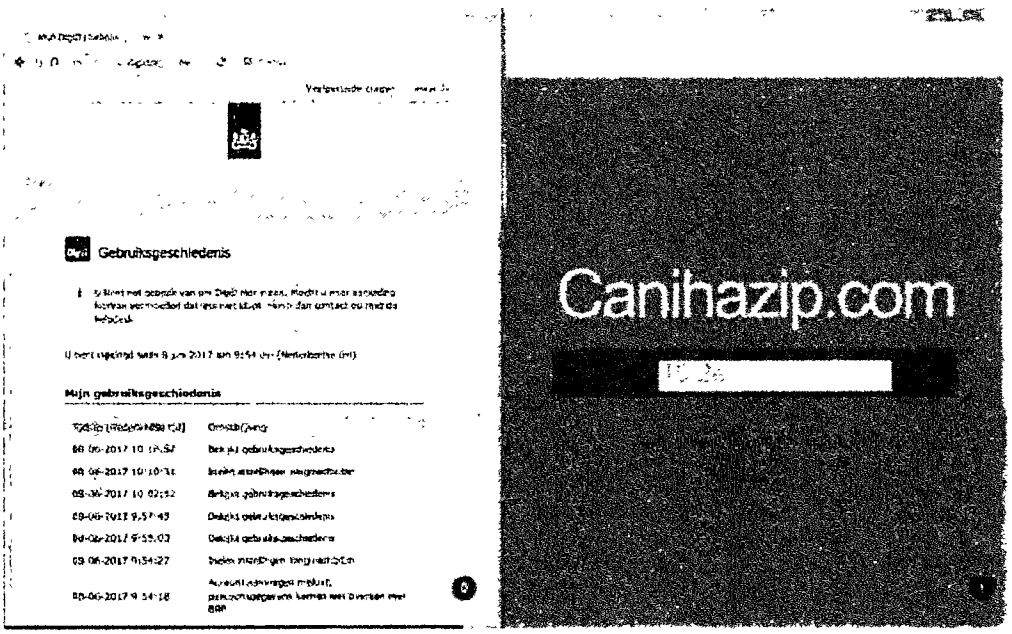
Bij het initiëren van de sessie moet deze aan een IP-adres worden gekoppeld. Daarna moet er bij elke actie worden gecontroleerd of de sessie vanaf het initiële IP-adres wordt gebruikt. Zo niet moet de sessie vernietigd worden.

Details

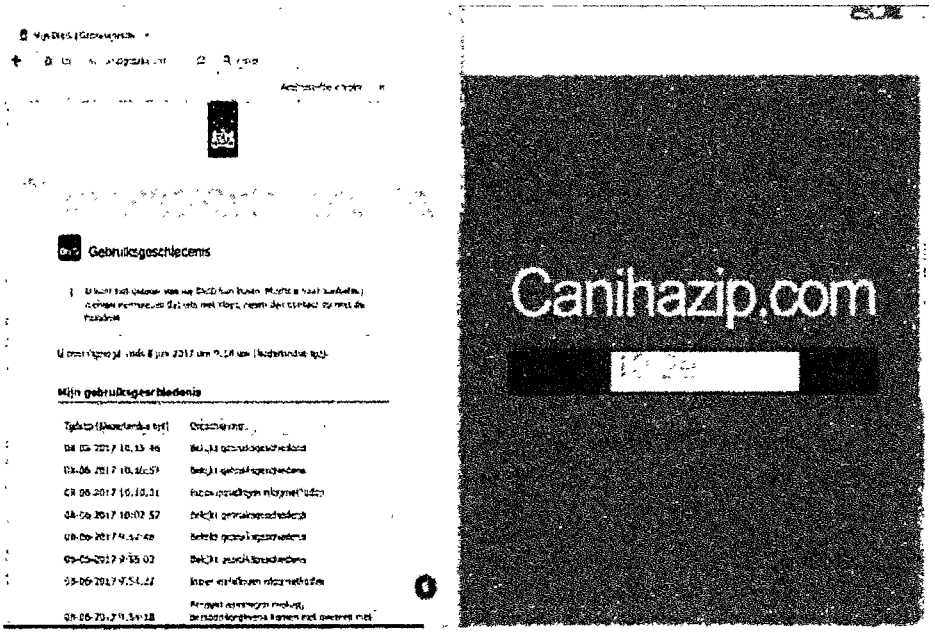
Deze bevinding is tijdens de test opgelost

In de mijnDigiD-omgeving vindt geen controle plaats of een sessie wordt gebruikt vanuit een vast IP-adres.

In het volgende voorbeeld is te zien dat 1 sessie te gebruiken is op verschillende IP-adressen. In eerste instantie werkt de actieve sessie op IP-adres 10.2e :



Daarna wordt er van netwerk gewisseld 10.2e en worden de schermen ververst:



Het blijft mogelijk om binnen de actieve sessie pagina's aan te roepen.

Hertest 20-6-2017
Deze kwetsbaarheid is het security assessment verholpen en geverifieerd.

Gelijktijdige sessies				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
6		Midden	Laag	Hoog

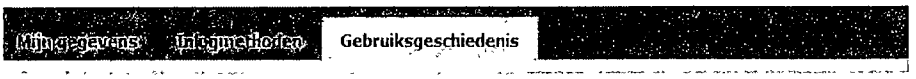
Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging
Wanneer er meerdere gelijktijdige sessies voor dezelfde gebruiker kunnen bestaan betekent dit dat oude sessies niet automatisch worden afgesloten. Dit geeft een aanvaller de mogelijkheid om oude sessies te misbruiken, ook als de gebruiker al een nieuwe sessie heeft opgestart.

Aanbeveling
Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Op deze manier kan de gebruiker nooit worden uitgesloten door een vergeten sessie of een kwaadwillende. Als een kwaadwillende bijvoorbeeld een sessie start, kan de gebruiker dit als een waarschuwing zien dat er iets met zijn account is. Daarnaast kan een gebruiker dan inloggen om zo de sessie van de kwaadwillende af te sluiten.

Details
Het is mogelijk om op de Mijn DigiD-omgeving meerdere actieve sessies per DigiD-account te hebben. Dit houdt in dat er op meerdere apparaten wordt ingelogd met één DigiD-account. De gebruikersgeschiedenis toont de inlogacties:



DigiD

Gebruiksgeschiedenis

U kunt het gebruik van uw DigiD hier inzien. Mocht u naar aanleiding hiervan vermoeden dat iets niet klopt, neem dan contact op met de helpdesk.

U bent ingelogd sinds 12 juni 2017 om 12:11 uur (Nederlandse tijd).

Mijn gebruiksgeschiedenis

Tijdstip (Nederlandse tijd)	Omschrijving
12-06-2017 12:12:07	Bekijkt gebruiksgeschiedenis
12-06-2017 12:12:05	Inzien instellingen inlogmethoden
12-06-2017 12:11:59	Bekijkt gebruiksgeschiedenis
12-06-2017 12.11.57	Inzien instellingen inlogmethoden
12-06-2017 12.11:53	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD
12-06-2017 12:11:49	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD
12-06-2017 10:58:41	Controle e-mail is verzonden
12-06-2017 10:58:07	Sessie verlopen (Mijn DigiD)

Het is ook mogelijk om met beide sessies acties uit te voeren op de Mijn DigiD-omgeving.

Ook met verschillende browsers is het mogelijk om meerdere actieve sessies te hebben.

Hertest 20-6-2017
Deze kwetsbaarheid was geen onderdeel van de hertest.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan bepaalde eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruikmaakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of de verwerking en uitvoer kan worden beïnvloed door het invoeren van niet-verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

Cross-Site Request Forgery				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
18		Laag	Laag	Laag

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Bij het verwerken van ingevulde formulieren zou gecontroleerd moeten worden of het verzoek van de eigen site afkomstig is.

Bedreiging

Wanneer bij het verwerken van ingevulde formulieren niet wordt gecontroleerd of het verzoek van de eigen site afkomstig is, is het mogelijk om POST acties vanaf een andere site uit te voeren. Indien er gebruik gemaakt wordt van authenticatie, dan wordt deze actie uitgevoerd in dezelfde browser als waarin een gebruiker op de legitieme website is ingelogd.

Aanbeveling

CSRF kan voorkomen worden door het gebruik van een niet te voorspellen token in een formulier of URL van elke HTTP request. Zo'n token moet op zijn minst uniek zijn per verzoek.

Details

Om de authenticiteit van gebruikersacties te waarborgen, maakt DigiD gebruikt van zogenoemde CSRF-tokens. Deze token zorgen ervoor dat acties alleen uitgevoerd kunnen worden als een bepaalde waarde wordt meegestuurd met deze acties. Deze waarde wordt voordat de actie kan worden uitgevoerd met de eindgebruiker gedeeld. Aangezien deze waarde alleen binnen de sessie van de gebruiker bekend is, kan een aanvaller geen verzoeken namens andere gebruikers doen.

Voor CSRF-token zijn over het algemeen twee soorten implementaties: session-based en request-based. Bij request-based wordt per verwachte actie één token gebruikt. En bij session-based wordt één en dezelfde token gebruikt gedurende de hele sessie en is geldig voor alle acties binnen die sessie.

Binnen DigiD wordt voor iedere actie een CSRF-token gegenereerd. Dit duidt op een request-based implementatie. Echter zit er geen relatie tussen de specifieke actie waarvoor deze token gegenereerd is. Dit betekend dat iedere CSRF-token dat binnen de sessie bekend is voor bij iedere actie kan worden gebruikt.

De acties die daadwerkelijk iets aanpassen aan het profiel van de gebruiker, vereisen naast de token ook een wachtwoord, waardoor de kans op misbruik aanzienlijk laag is. Maar aangezien er blijkbaar effort in CSRF-tokens is gestoken om deze per actie te genereren lijkt het erop dat deze werking niet overeenkomt met de beoogde doel van deze beveiliging.

Hertest 20-6-2017
Deze kwetsbaarheid was geen onderdeel van de hertest.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

Information disclosure				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
7		Opgelost	Zeer laag	Zeer laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Het systeem geeft informatie vrij over de (interne) werking/logica van het systeem zelf, de onderliggende infrastructuur, privacygevoelige data of gerelateerd aan toegangsmanagement.

Bedreiging

De informatie kan een aanvaller inzicht verlenen welke als een springplank kan dienen voor aanvallen op het systeem: gelekte sessietokens kunnen het toegangsbeheer ondermijnen, versleinformatie ontsluit het patchlevel, stacktraces geven inzicht in interne logica en gebruikte technologie, open directories over het onderliggende besturingsysteem, hostnames en IP-adressen geven inzicht in de netwerkimplementatie, etc.

Aanbeveling

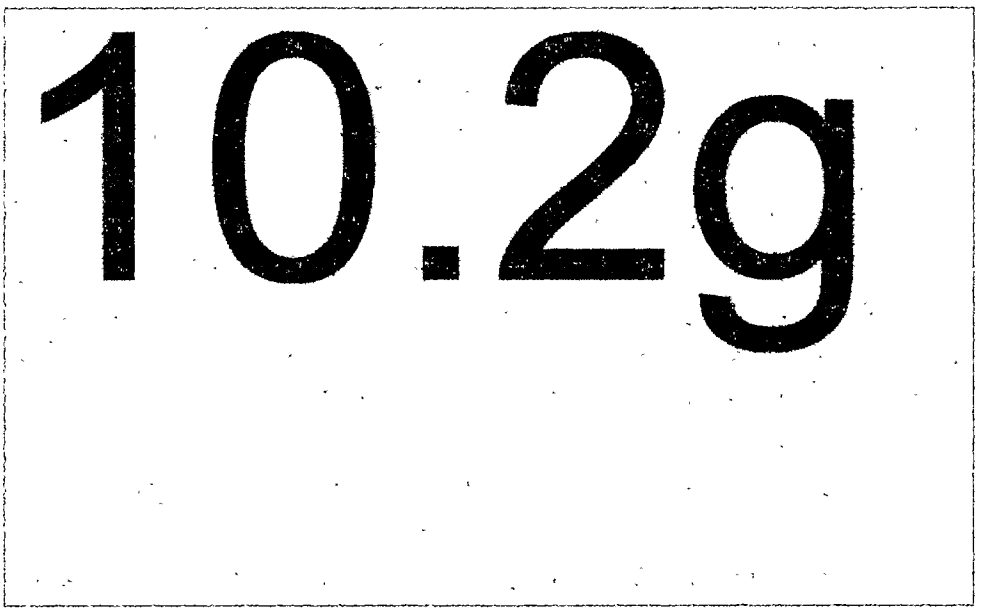
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie, en zorg dat foutmeldingen aan eindgebruikers zonder systeeminformatie getoond worden.

Details

Deze bevinding is tijdens de hertest opgelost

Wanneer met */host-manager/html* met foutieve credentials bezocht wordt geeft deze het gebruik 10.2g vrij middels een foutmelding.

Een aanvaller kan deze informatie gebruiken als springplank voor misbruik van het systeem..
Configureer de webserver om alleen gebruiksvriendelijke foutmeldingen weer te geven waaruit geen (technische) informatie af te leiden is over de gebruikte technologie.



HTTP request:

```
GET 10.2g
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie:
_persist=!mOg0sJk4PDBM7/7+5aqg6lTJU5Hb5VKr9H+jy9CVIQfiqEgyk/7LT8vcS1Oh
hfdvgBr2JLQVFlpS3zmB6V4JdWPblmrXrC3Bh1P9m94=;
JSESSIONID=D3CFA044ABE02B3F6A1CBDDDC83BA1C5
Connection: close
Authorization: Basic cm9vdDpyb290
```

HTTP response:

```
HTTP/1.1 401 Unauthorized
Cache-Control: private
Expires: Thu, 01 Jan 1970 01:00:00 CET
10.2g
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 2044
Date: Thu, 11 May 2017 10:39:39 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains


10.2g
```

10.2g

Hertest 20-6-2017
Deze kwetsbaarheid is tijdens de hertest verholpen en geverifieerd.

Information disclosure				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
8		Zeer laag	Zeer laag	Zeer laag

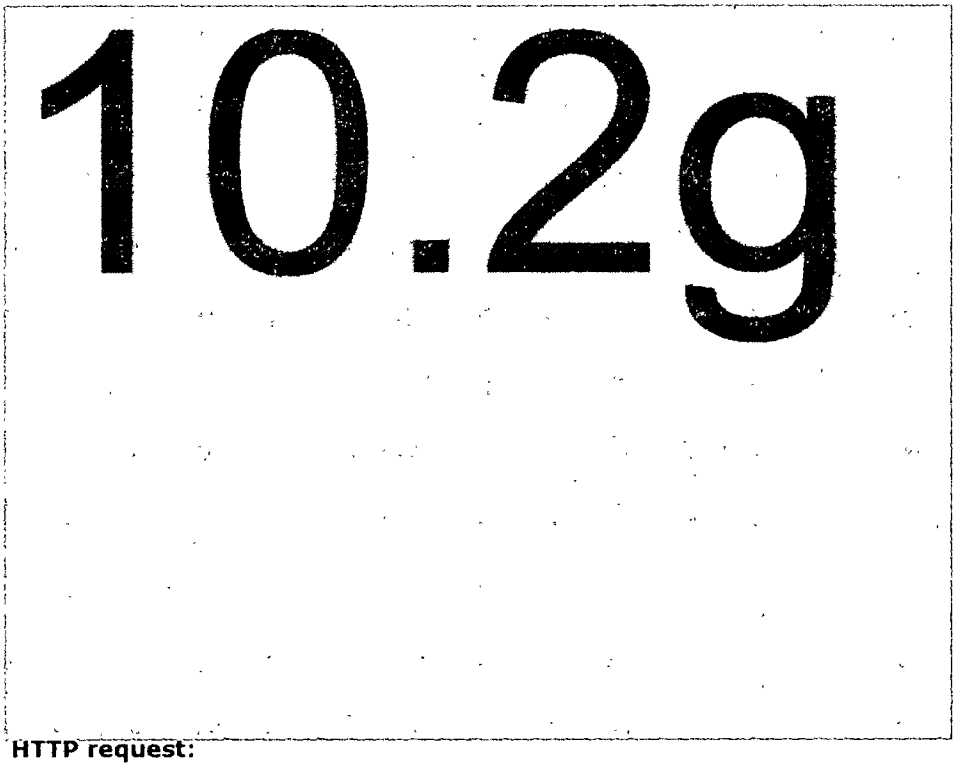
Betreffende hosts
rda-a3.digid.nl

Omschrijving
Het systeem geeft informatie vrij over de (interne) werking/logica van het systeem zelf, de onderliggende infrastructuur, privacy gevoelige data of gerelateerd aan toegangsmanagement.

Bedreiging
De informatie kan een aanvaller inzicht verlenen welke als een springplank kan dienen voor aanvallen op het systeem: gelekte sessietokens kunnen het toegangsbeheer ondermijnen, versieinformatie ontsluit het patchlevel, stacktraces geven inzicht in interne logica en gebruikte technologie, open directories over het onderliggende besturingsysteem, hostnames en IP-adressen geven inzicht in de netwerkimplementatie, etc.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie, en zorg dat foutmeldingen aan eindgebruikers zonder systeeminformatie getoond worden.

Details
Bij het bezoeken van */idp* wordt het gebruik van de 10.2g
10.2g software vrijgegeven via een standaardpagina.
Een aanvaller kan deze informatie gebruiken als springplank voor misbruik van het systeem.
Ontsluit geen toegang tot deze webpagina. Wanneer deze ontsluiting operationeel nodig is, ontsluit deze dan alleen voor een beperkt aantal IP adressen zoals bijvoorbeeld alleen intern gebruik.



HTTP request:

```
GET /idp/ HTTP/1.1
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie:
_persist=!mOg0sJk4PDBM7/7+5aqg6lTJU5Hb5VKr9H+jy9CVIQfiqEgyk/7LT8vcS1Oh
hfdvgBr2JLQVF1pS3zmB6V4JdWPb1mrXrC3Bh1P9m94=;
JSESSIONID=D3CFA044ABE02B3F6A1CBDDDC83BA1C5
Connection: close
```

HTTP response:

```
HTTP/1.1 200 OK
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Content-Length: 1225
Date: Thu, 11 May 2017 11:06:47 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

10.2g
```

Hertest 20-6-2017
Deze kwetsbaarheid was niet verholpen op het moment van de hertest.

Verouderde software				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
9		Laag	Laag	Laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Er wordt verouderde software gebruikt waarin bekende kwetsbaarheden aanwezig zijn. Ontwikkelaars brengen patches en nieuwe versies uit om nieuwe functionaliteit en features toe te voegen aan hun software, maar ook om gevonden beveiligingsproblemen op te lossen.

Bedreiging

Het systeem in kwestie maakt gebruik van verouderde software dan wel verouderde versies van software, waarvan bekend is dat deze zwakheden bevatten. Voor veel verouderde systemen zijn kant-en-klare modules beschikbaar die deze zwakheden misbruiken. Aanvallers kunnen deze modules gebruiken om systemen aan te vallen.

Aanbeveling

Update de software zodat er gebruik wordt gemaakt van de meest recente en stabiele versie van de software en implementeer een patchmanagementproces. Een alternatief hier is dat de firewall wordt ingesteld om pogingen tot uitbuiting van de kwetsbaarheden te detecteren en te mitigeren. Dit laatste is alleen aan te raden als een tijdelijke oplossing tot het systeem is bijgewerkt.

Details

10.2g

Het is niet duidelijk of de kwetsbaarheid ook daadwerkelijk uit te nutten is, aangezien er geen verdere toegang tot deze software is.
Update naar de laatste versie 10.2g waarin deze library geupdate is naar een niet kwetsbare versie.

HTTP request:

```
GET 10.2g
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://rda-a3.digid.nl/idp/static/
Cookie:
_persist=!mOg0sJk4PDBM7/7+5aqg61TJU5Hb5VKr9H+jy9CVIQfiqEgyk/7LT8vcS1Oh
hfdvgBr2JLQVF1pS3zmB6V4JdWPb1mrXrC3Bh1P9m94=;
JSESSIONID=D3CFA044ABE02B3F6A1CBDDDC83BA1C5
Connection: close
```

HTTP response:

```
HTTP/1.1 200 OK
Last-Modified: Wed, 29 Jun 2016 09:32:08 GMT
Content-Type: application/javascript
Content-Length: 145855
Date: Thu, 11 May 2017 11:13:56 GMT
```

```
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Vary: Accept-Encoding
```

10.2g

Hertest 20-6-2017
Deze kwetsbaarheid was niet verholpen op het moment van de hertest.

Denial-of-Service – SMS data				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
10		Opgelost	Midden	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Het systeem is zo te manipuleren dat de server een grote hoeveelheid SMS-data naar een gebruiker stuurt.

Bedreiging
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mobiele apparaat niet meer kan gebruiken.

Aanbeveling
Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een verzoek naar SMS herstel is gegaan in een vooraf bepaalde periode.

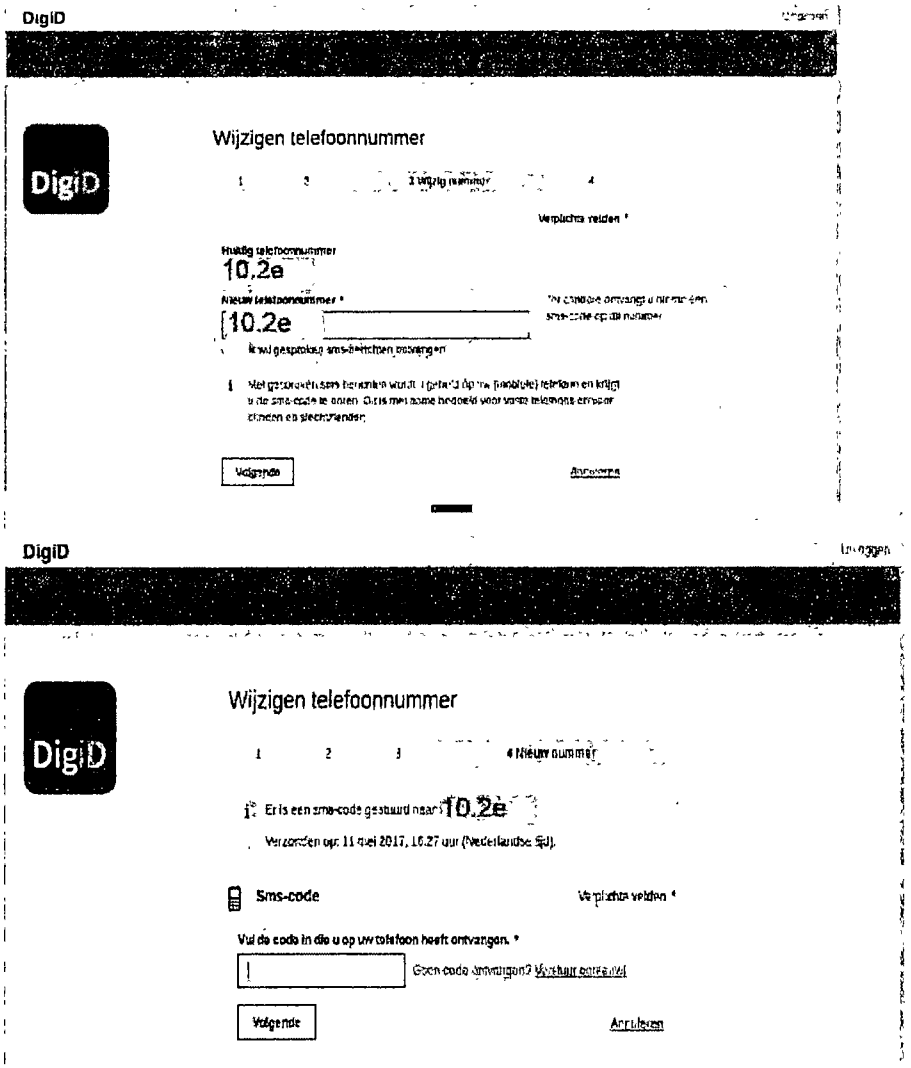
Details

Deze bevinding is tijdens de test opgelost

Druk op Telefoonnummer wijzigen

Telefoonnummer 10.2e i › Telefoonnummer wijzigen

Kies *ik kan een sms ontvangen op mijn oude telefoonnummer.*
Vul gegevens in (dus wachtwoord en code die je krijgt via sms).
Vervolgens vul je bij nieuw telefoonnummer het gewenste nummer in en drukt op volgende.



Echter kunnen de volgende requests als een macro worden aangeroepen om dit proces te blijven herhalen:

Request

```
GET /telefoonnummer/wijzigen HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://a3.digid.nl/sms_controleren
Cookie:
_persist=!wUhXk4rWZGOSOnf+5aqg6lTJU5Hb5YdrlXXzRg65KBKSBJKgOPbqqk2OsvVQ
3lBWFTgvrToCL/Vm3oANMhHlWyCARhFTEo3MYYJQ5SA=;
_session_id=45311a7dc4e68532ff29adf288a228ff
Connection: close
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 11 May 2017 13:39:15 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
```

```
X-Request-Id: 920c7a16-8a6f-4cbb-a250-f5be50f2407f
X-Runtime: 0.039418
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Request 2

```
POST /telefoonnummer HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/telefoonnummer/wijzigen
Cookie:
_persist='wUhXk4rWZGOSOnf+5aqg6lTJU5Hb5YdrlXXzRg65KBKSBJKgOPbqqk2OsvVQ
3lBWFTgvrToCL/Vm3oANMhHlWyCARhFTEo3MYYJQ5SA=;
_session_id=45311a7dc4e68532ff29adf288a228ff
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 233

utf8=%E2%9C%93&_method=patch&authenticity_token=euti9duuMIclsET2t%2FDh
Jt6%2Bg4CR%2FIb%2FVTCas5P6dP0MMd1518vmkHYfhF9C9q9QMOmBdr2%2FlpEBEKJkd0
0qUw%3D%3D&account%5Bmobiel_nummer%5D[redacted]
[redacted]=0&commit=Volgende
```

Response 2

```
HTTP/1.1 302 Found
Date: Thu, 11 May 2017 13:39:25 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 39692f29-577e-40c1-99d5-46427455ccb8
X-Runtime: 0.032175
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Location: https://a3.digid.nl/sms_versturen
Status: 302 Found
Content-Type: text/html; charset=utf-8
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 99

<html><body>You are being <a
href="https://a3.digid.nl/sms_versturen">redirected</a>.</body></html>
```

Request 3

```
GET /sms_versturen HTTP/1.1
Host: a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/telefoonnummer/wijzigen
Cookie:
_persist='wUhXk4rWZGOSOnf+5aqg6lTJU5Hb5YdrlXXzRg65KBKSBJKgOPbqqk2OsvVQ
3lBWFTgvrToCL/Vm3oANMhHlWyCARhFTEo3MYYJQ5SA=;
_session_id=45311a7dc4e68532ff29adf288a228ff
Connection: close
```

Response 3

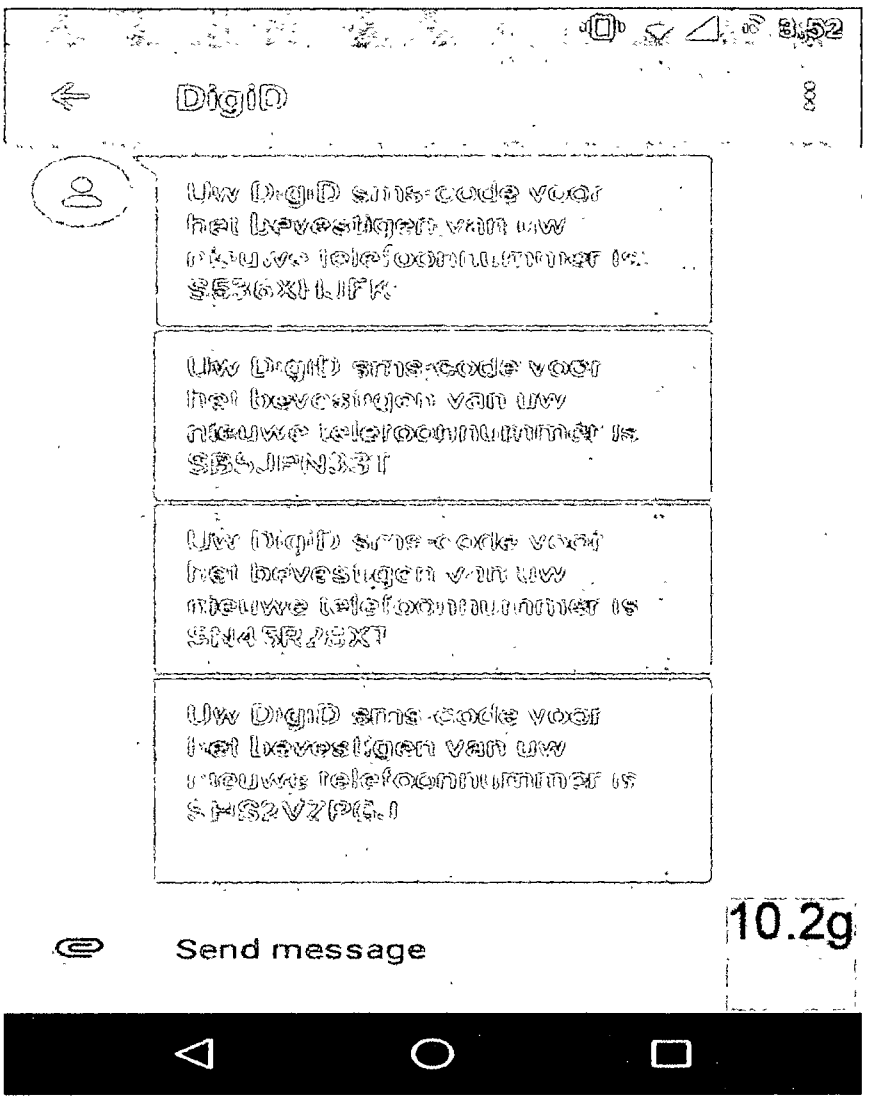
```
HTTP/1.1 302 Found
Date: Thu, 11 May 2017 13:39:25 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection. 1; mode=block
X-Request-Id: fa93a800-c78f-42f1-9fd7-f3f8dfc42ecb
X-Runtime: 0.052959
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00 00:00 GMT
Location  https://a3.digid.nl/sms_controleren
Status: 302 Found
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html><body>You are being <a
href="https://a3.digid.nl/sms_controleren">redirected</a>.</body></htm
l>
```

Request 4

```
GET /telefoonnummer/wijzigen HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://a3.digid.nl/sms_controleren
Cookie:
_persist='wUhXk4rWZGOSOnf+5aqg6lTJU5Hb5YdrlXXzRg65KBKSBJKgOPbqqk2OsvVQ
3lBWFTgvrToCL/Vm3oANMhHlWyCARhFTEo3MYYJQ5SA=;
_session_id=45311a7dc4e68532ff29adf288a228ff
Connection: close
```

Response 4

```
HTTP/1.1 200 OK
Date: Thu, 11 May 2017 13:39:29 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1, mode=block
X-Request-Id: b05c26e6-f48b-4d67-adf5-71628b0fc35d
X-Runtime  0.031332
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type. text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```



Hertest 20-6-2017
Deze bevinding is tijdens het security assessment opgelost en geverifieerd.

HTTP TRACE-methode toegestaan				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
11		Opgelost	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl
a3.digid.nl
was-a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
digidbeheer-a3.digid.nl

Omschrijving

Op de server wordt naast de GET- en POST-methode ook de TRACE HTTP-methode ondersteund. Middels HTTP TRACE kan een kopie worden gevraagd van de door de gebruiker gestuurde aanvraag.

Bedreiging

Het cookie kan tegen XSS aanvallen beschermd worden door de *HttpOnly* flag te gebruiken. Deze bescherming kan omzeild worden door gebruik te maken van een TRACE aanvraag. In het antwoord worden onder andere ook alle cookiegegevens meegestuurd.

Aanbeveling

Zorg ervoor dat alleen GET- en POST-methodes ondersteund worden.
Voor meer informatie zie: https://www.owasp.org/index.php/Cross_Site_Tracing

Details

Het is mogelijk om een TRACE request te sturen naar de genoemde hosts. Daardoor wordt de aanvraag van de gebruiker gereflecteerd in de response van de server. Hier kunnen ook scripts worden uitgevoerd. Een voorbeeld:

Voorbeeldrequest:

```
TRACE / HTTP/1.1
Host: a3.digid.nl
Cookie: <script>alert(1)</script>
Connection: close
```

Voorbeeldresponse:

```
HTTP/1.1 200 OK
Date: Tue, 06 Jun 2017 12:51:07 GMT
Content-Type: message/http
Connection: close
Set-Cookie:
_persist=!t6Z2FPQzJ0Lsn5P+5aqg6lTJU5Hb5cUqH8zj52PF2szvudCxmql9rOPbyZKW
RJE0n73CGMLMD6PHVLrfFhvTwFkfDxVFQwlrVxiQQ2Q=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 136
```

10.2g

Hertest 20-6-2017

Deze kwetsbaarheid was verholpen op het moment van de hertest.

Weak Block cipher – 64 bit TLS Sweet32				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
12		Midden	Laag	Midden

Betreffende hosts

mijn.a3.digid.nl
a3.digid.nl
was-a3.digid.nl
balie-a3.digid.nl
cls-a3.digid.nl
rda-a3.digid.nl

Omschrijving

De TLS server maakt gebruik van algoritmes die intern 64-bit block ciphers gebruiken.

Bedreiging

64-bit block ciphers zijn kwetsbaar voor een zogenaamde birthday attack, waarbij de kans dat twee willekeurig gegenereerde waarden overeenkomen hoger dan 50% is. Dit wordt vervolgens gebruikt om een zogenaamde collision te forceren, waarmee achterhaald kan worden wat de originele waarde was van een versleuteld stukje data. Gegeven genoeg data (de ontdekkers hadden 785GB aan HTTPS verkeer nodig) is het mogelijk om met een man-in-the-middle attack de waarde van bijvoorbeeld een versleutelde cookie te achterhalen.

Aanbeveling

Schakel de kwetsbare block ciphers uit binnen TLS. Indien dit niet mogelijk is, zorg er dan voor dat geheime waarden (zoals een sessie token) met een hoge frequentie veranderen. Dit verzekert dat eventueel (gedeeltelijk) achterhaalde waarden niet meer valide zijn, en daarmee geen waarde meer hebben voor aanvallers.

Details

De server ondersteunt cipher suites die gebruik maken van 64-bit block ciphers:

```
443/tcp open  https   syn-ack ttl 64
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
```

derubricering

```
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
```

Schakel ondersteuning voor deze cipher suites uit.

Hertest 20-6-2017
Deze kwetsbaarheid was geen onderdeel van de hertest.

Default content				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
13		Opgelost	Laag	Laag

Betreffende hosts

mijn.a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
digidbeheer-a3.digid.nl

Omschrijving

De software wordt meegeleverd met voorbeeldcontent of -functionaliteit, zoals een managementconsole met standaardgebruikersnaam en -wachtwoord dan wel een 'lorem ipsum' tekst.

Bedreiging

De informatie in de default content kan gebruikt worden om de software te identificeren of standaardzwakheden uit te buiten. Bij het gebruik van een standaardgebruikersnaam en -wachtwoord is het voor een aanvaller vrij eenvoudig om in te loggen en instellingen te wijzigen.

Aanbeveling

Zet niet-gebruikte standaardmogelijkheden uit, verwijder de standaardteksten en pas standaardwachtwoorden altijd aan.

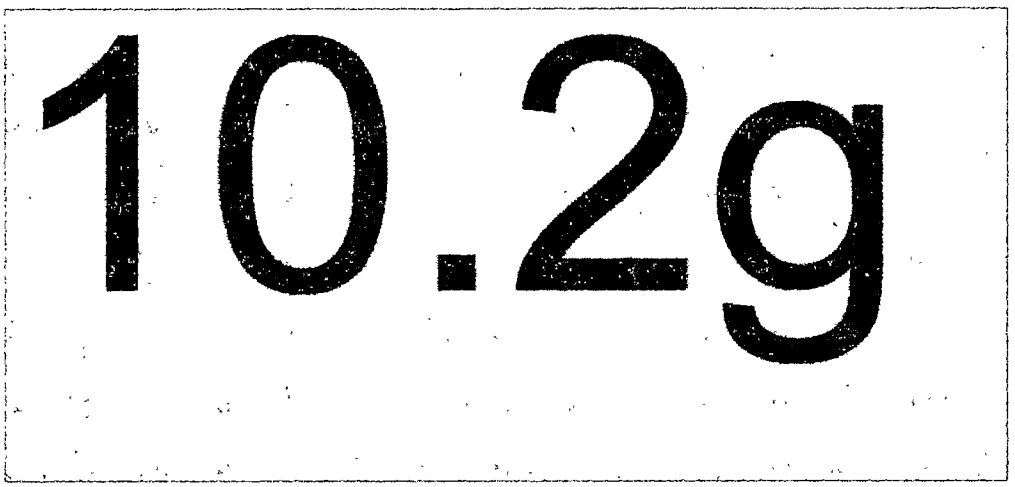
Details

Deze bevinding is tijdens de hertest opgelost

Er kan een 10.2g worden gevonden op een standaard 10.2g Dit geeft inzicht in de gebruikte software.

mijn.a3.digid.nl 10.2g
balie-a3.digid.nl 10.2g
digidbeheer-a3.
cis-a3.digid.nl 10.2g

derubricering



Hertest 20-6-2017
Deze kwetsbaarheid is tijdens de hertest verholpen en geverifieerd.

Default admin pagina locatie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
14		Opgelost	Laag	Midden

Betreffende hosts
rda-a3.digid.nl

Omschrijving
Geïnstalleerde software dan wel geïmplementeerde hardware maakt vaak gebruik van standaardlocaties en -poorten voor administratieve toegang.

Bedreiging
Deze standaardlocaties zijn bekend en zijn voor een aanvaller gemakkelijk te achterhalen. Bij bekende kwetsbaarheden zijn deze locaties dan ook makkelijk te bereiken en uit te buiten.

Aanbeveling
In eerste instantie is het van belang dat men zich bewust is van het feit dat standaardlocaties gebruikt worden. Afhankelijk van de kwetsbaarheden en de mate waarin de dienst als bedrijfskritisch wordt beschouwd, kan er gekeken worden naar mogelijkheden om de inlogpagina's en ports te verplaatsen dan wel te wijzigen, te verbergen of de gebruikerstoegang te whitelisten op basis van IP of SSL/TLS-verbinding. Er zijn hier meerdere opties aanwezig, waarbij de keuze altijd afhangt van de omstandigheden.

Details

Deze bevinding is tijdens de hertest opgelost

10.2g is beschikbaar op de standaardlocatie, daarom kan deze eenvoudig gevonden worden.

10.2g

Hertest 20-6-2017
Deze kwetsbaarheid is tijdens de hertest verholpen en geverifieerd.

Vreemde HTTP-methodes toegestaan				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
15		Laag	Laag	Laag

Betreffende hosts
rda-a3.digid.nl

Omschrijving
Op de server worden naast GET, HEAD en POST ook andere methodes toegestaan.

Bedreiging
Deze methodes kunnen op de server voor ongewilde resultaten en responses zorgen.

Aanbeveling
Sta alleen de door de applicatie gebruikte HTTP-methodes toe op basis van whitelisting.

Details
Naast de GET, HEAD en POST zijn er ook andere methodes beschikbaar om uit te voeren, deze kunnen worden misbruikt door de gebruiker.

HTTP Request

```
OPTIONS / HTTP/1.1
Host: rda-a3.digid.nl
Connection: close
```

HTTP Response

```
HTTP/1.1 200 OK
Allow: GET, HEAD, POST, PUT, DELETE, OPTIONS
Content-Length: 0
Date: Wed, 07 Jun 2017 12:58:04 GMT
Connection: close
Set-Cookie:
_persist=!p/AXNxmNPy39hcD+5aqg6lTJU5Hb5ZkfMPk+Pc/Pw7Fuav+TqDth7AO681L3
17AfRYdEEb98aLnyWDy2/v0j/PedTr8Za9nkenVLNFY=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest 20-6-2017
Deze kwetsbaarheid was niet verholpen op het moment van de hertest.

Information disclosure – Versieinformatie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
16		Opgelost	Laag	Laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Systemen geven vaak zelf onbedoeld aan welke versie van de software geïnstalleerd is. Dit is meestal een standaardinstelling van de software.

Bedreiging

Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in de specifieke softwareversie.

Aanbeveling

Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen versieinformatie van systemen en software in cookies of HTTP-headers mee. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details

Deze bevinding is tijdens de hertest opgelost

10.2g

Request:

```
NOMETHOD /idp/ HTTP/1.1
Host: rda-a3.digid.nl
Cookie: o05vaga08r
Connection: close
```

Response:

```
HTTP/1.1 501 Not Implemented
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 1130
Date: Wed, 07 Jun 2017 11:07:35 GMT
Connection: close
Set-Cookie:
_persist=!rzRjobRipuhGr0b+5aqg61TJU5Hb5d0ZmzRhpPb4ULnFJYcMTR4zNbR2qn2b
PmG7gdhyCSsmqIXyfmboaf17OAAGLVIXR/iF0+UUoyc=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

10.2g

10.2g

Hertest 20-6-2017
Deze kwetsbaarheid is tijdens de hertest verholpen en geverifieerd.

Denial of Service – E-mail versturen				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
17		Midden	Laag	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Het systeem is zo te manipuleren dat de server een grote hoeveelheid e-mails naar een gebruiker stuurt.

Bedreiging
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling
Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een e-mail is gestuurd naar de gebruiker

Details
Het is mogelijk om via de DigiD applicatie een continue stroom (gesproken) emails te versturen naar een willekeurig emailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.

DigiD heeft de mogelijkheid om de een email adres te koppelen aan het account van de gebruiker waarmee een gemakkelijke herstelfunctionaliteit wordt toegevoegd. Hier heeft mijn DigiD de optie telefoonnummer toevoegen/wijzigen.

Wachtwoordherstel

Wachtwoord herstellen met uw e-mailadres
Niet actief

Wilt u eenvoudig een nieuw wachtwoord kunnen instellen als u deze niet meer weet? Vraag de extra controle via sms aan en geef uw e-mailadres op via e-mailadres toevoegen.

Als er naar 'e-mail adres' toevoegen wordt genavigeerd verschijnt onderstaande vraag om een email op te geven.

Wanneer er een emailadres wordt opgegeven en op de volgende knop drukt wordt onderstaande request verzonden:

Request:

```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
```

derubricering

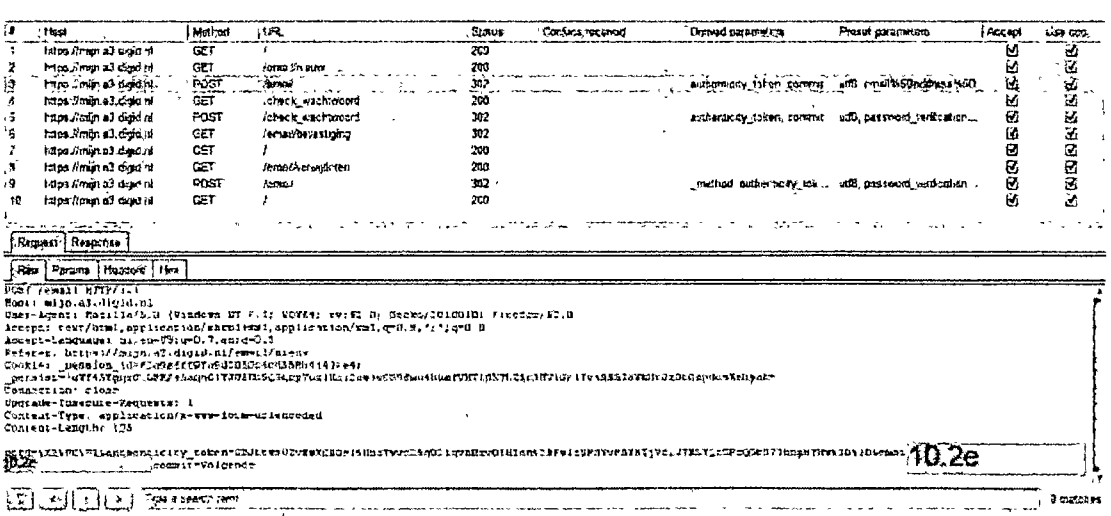
```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0)
Gecko/20100101 Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Referer: https://mijn.a3.digid.nl/email/nieuw
Cookie: _session_id=62a9e6ff9fa9d2050c4cd358b4144ee4;
_persist=!gWf45Egqx0bLPR/+5aqg61TJU5Hb5Q5gcpYuz1Ho12uw+wCG96mu4huafVHT
10X7LZ3r3HViGr1IviS5SIaW kNrJz8t0zpdosXebyak=
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 195
utf8=%E2%9C%93&authenticity_token=6DJEtwsUZvMwXCBOe19HnzTyvc25qD2lgvh8
zvOIH3dn%2BFw3zUR8YvP5WM
TjVf1V7MSYQzCRzQGk8Y3hnpbYNw%3D%3D&email%5Baddress%5D=10.2e
&commit=V olgende
```

De reponse zorgt er voor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatie code naar het email adres. Deze code moet binnen een bepaalde periode wordt opgegeven anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wilt versturen verschijnt de melding dat er al een code onderweg en na meer dan 10 minuten een nieuwe code kan worden aangevraagd. "Er is nog een e-mail onderweg naar u. Vanaf 13:41 uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen." Echter is het mogelijk om het nog-niet geactiveerde e-mailadres te verwijderen van het account.

Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg is dat de gebruiker bovenstaande actie nog een keer kan uit voor het zelfde of andere e-mailadressen.

Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.



Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:

noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:57	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:57	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:57	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:57	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:57	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:56	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			
noreply@a3.digid.nl	Uw DigiD e-mailadres is gewijzigd	do 11-5-2017 13:56	11 KB
Geachte heer/mevrouw, Het aan uw DigiD gekoppelde e-mailadres is zojuist gewijzigd. Bij een wijziging van het e-mailadres stuurt DigiD automatisc			

Er bestaat het gevaar dat als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail, de mail wordt aangemerkt als spam of phising. Bij voldoende aanmeldingen hiervan kan de gebruikte mailserver op de zwarte lijst komen te staan van een organisatie als Spamhaus, waardoor er geen mails meer worden geaccepteerd.

Hertest 20-6-2017

Deze kwetsbaarheid was niet verholpen op het moment van de hertest.

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work around' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport

DigiD release 5.4

Kenmerk: 201724

Datum	22-08-2017
Status	Definitief
Versie	1.0

Rubricering derubricering

Colofon

Kenmerk	2017/24
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
18-08-2017	0.1	Sogeti Nederland B.V.	Initiële versie
18-08-2017	0.2	Sogeti Nederland B.V.	Interne review
22-08-2017	1.0	Sogeti Nederland B.V.	Feedback verwerkt, Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

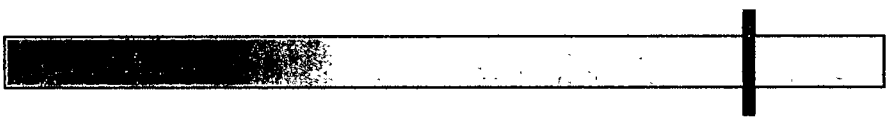
Managementsamenvatting

Inleiding

Logius heeft Sogeti gevraagd een securitytest uit te voeren op de acceptatieomgeving van DigiD. Het onderzoek is uitgevoerd van 14 augustus 2017 tot en met 17 augustus 2017 [redacted]

Conclusies en aanbevelingen

- Er zijn tijdens de test geen bevindingen gedaan met een hoge of zeer hoge risicoclassificatie.
- Logius heeft gevraagd om een aantal openstaande bevindingen uit release 5.3 opnieuw te testen. Deze bevindingen zijn allen gemarkeerd als opgelost.



Onvoldoende Voldoende

Punten ter verbetering.

- De logica in de applicatie is te misbruiken zodat er een grote hoeveelheid e-mails wordt gestuurd naar een gebruiker als er herhaaldelijk e-mail adres wordt toegevoegd aan een gebruiker en daarna weer wordt verwijderd.

  Controleer of deze functionaliteit naar behoren werkt of aangepast dient te worden.

- Een gebruiker kan zijn account blijven gebruiken als deze wordt opgeschort als de gebruiker op dat moment is ingelogd. Als een aanvaller is ingelogd en zijn sessie actief houdt kan hij acties blijven uitvoeren.

  Controleer of deze functionaliteit naar behoren werkt of aangepast dient te worden.

Aanvullingen Logius

Reactie van Logius.

1 Inleiding

1.1 Opdrachtformulering

De aanleiding tot deze securitytest betreft de nieuwe 5.4 release van DigiD. Het gaat om het vaststellen van de het beveiligingsniveau van DigiD; er zal extra aandacht worden geschonken aan de risico's die de wijzigingen en uitbreidingen als gevolg van de implementatie van DigiD Release 5.4 met zich meebrengen.

Daarnaast is het doel het beveiligingsniveau te handhaven of te verbeteren nadat er wijzigingen in de applicatie zijn aangebracht, en detectie of eerder geconstateerde risico's zijn weggenomen en er geen nieuwe risico's zijn geïntroduceerd als gevolg van deze wijzigingen.

De nadruk van de testen ligt op de technische beveiligingsrisico's. Tijdens het overleg met Logius over de rapportage zal er ook naar de business risico's gekeken worden die de bevindingen met zich meebrengen.

De opdracht is geheel conform het Security Testplan uitgevoerd.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd, zoals beschreven in het bijbehorende Plan van Aanpak.

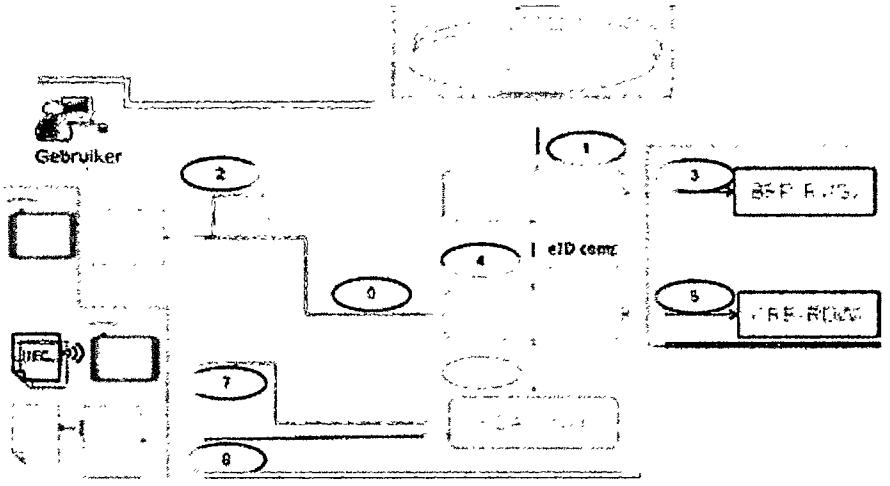
1.3 Scope

De scope van deze security test is de DigiD applicatie, gezien vanaf een extern oogpunt, met extra aandacht voor de risico's als gevolg van aanpassingen die als onderdeel van R5.4 aan DigiD zijn uitgevoerd.

In scope:

- Alle services zoals ontsloten naar eindgebruikers.
- Het verkeer tussen de mobiele applicatie en de backend.
- Het verkeer tussen de browser plugin en de backend.

Onderstaande schematische weergave geeft een visuele representatie van deze scope:



Op basis van de PRA (Product Risico Analyse, zie *'PRA DigiD R5.4 spreadsheet versie 0.3A.xls'*) zijn binnen de aanpassingen een vijftal aandachtsgebieden geïdentificeerd in deze release met mogelijke security impact. Deze risico's hebben extra aandacht gekregen tijdens de test:

7.1. *DigiD Substantieel / 54.1 01.Au en 54.1.04 Au , Webdienst vereist substantieel - schermen en controles*
Risico dat de functie misbruikt wordt op security-gebied: het gaat er om dat de autorisatiecode in het SAML-bericht niet gemanipuleerd kan worden
13.1 *DigiD Substantieel / 54.1.03.Ov Sms proces specifiek zijn*
Geen specifiek risico, wel expliciet aandacht geven
29.3 *IB wachtwoordreset wijzigen wachtwoord / 54 3.01. Het Wachtwoordherstel & wijzigen email en/of telefoonnummer*
Geen specifiek risico, wel expliciet aandacht geven

Hiernaast is een algehele security test uitgevoerd ter detectie van eventuele regressie dan wel ongeautoriseerde of onbedoelde changes. Speciale aandacht geniet de upgrade van het Ruby programmeer-framework.

Logius heeft aangegeven dat de uiteindelijk gerealiseerde scope van R5.4 afwijkt van de scope die is gehanteerd in de product risico analyse en in het opstellen van het Plan van Aanpak van de securitytest van R5.4.
De mogelijkheid om de DigID app te activeren, *zonder* dat vereist is om al te beschikken over een account op Midden niveau met SMS, maakt geen onderdeel uit van R5.4 (wel van de volgende release). Een op deze wijze geactiveerde app is een randvoorwaarde om het proces van wachtwoordherstel via de app in te gaan. Omdat deze functionaliteit geen onderdeel (meer) uitmaakt van de scope van R5.4 zijn de volgende in het Plan van Aanpak benoemde product risico's niet getest in deze securitytest:

25.5 *DigiD app als zelfstandig middel / 54.5.01 MD en 54.5.03.MD , Wachtwoord opnieuw instellen via DigiD app - controles en schermen*
Geen specifiek risico, wel expliciet aandacht geven
41.5 *DigiD app als zelfstandig middel / 54.5.09.MD Wachtwoord opnieuw instellen via DigiD app afhankelijk van uitgifteproces DigiD app*
Geen specifiek risico, wel expliciet aandacht geven

De securitytest heeft zich specifiek gericht op de volgende systemen in de *A3* omgeving:

Onderwerp	URL	IP-adres
Mijn DigID	https://mijn.a3.digid.nl	144.43.243.145
Aanvragen	https://a3.digid.nl/aanvragen	144.43.243.144
Activeren	https://a3.digid.nl/activeer_digid	144.43.243.144
Herstellen	https://a3.digid.nl/herstellen	144.43.243.144
Koppelvlakken	https://was-a3.digid.nl	144.43.243.146
Beheermodule	https://digidbeheer-a3.digid.nl	144.43.243.148
Balie	https://balie-a3.digid.nl	144.43.243.147
DigiD CIS	https://cis-a3.digid.nl	144.43.243.150
RDA	https://rda-a3.digid.nl	144.43.243.152
DigID App	https://a3.digid.nl/apps	144.43.243.144

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 4.1 voor een toelichting op de risicoclassificatie.

Risico Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Opgelost	Totaal
Client-Side Controls					2		2
Logica							
Authenticatie							
Sessiemanagement			2				2
Toegang							
Invoerafhandeling							
Omgeving							
Servers			2			1	3
Totaal			**4**		**2**	**1**	**7**

Tijdens de test op DigiD 5.3 zijn een aantal bevindingen gedaan die bij de test op 5.4 specifiek opnieuw zijn getest. Deze bevindingen zijn:

Mantis ID	Omschrijving	Opgelost
450948	[IB] Pentest R5.3 #1 Secure Flag ontbreekt	Ja
450949	[IB] Pentest R5.3 #2 HttpOnly-flag ontbreekt	Ja
450955	[IB] Pentest R5.3 #9 Verouderde software	Ja
450958	[IB] Pentest R5.3 #15 Vreemde HTTP-methodes toegestaan	Ja

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Kleur	Uitleg	Aantal
	Niet getest, buiten scope.	24
	Er wordt niet afgeweken van de norm.	16
	De norm wordt gedeeltelijk nageleefd.	3
	Er wordt afgeweken van de norm.	0

Beleidsdomein

B.01	Informatiebeveiligingsbeleid
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	

derubricering

U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Toelichting: Er bestaat een kans dat, door het gebruik van zwakkere block ciphers in de versleutelde communicatie, verkeer tijdens transport kan worden afgeluisterd.	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Toelichting: Het is mogelijk voor een gebruiker om via hetzelfde IP adres meerdere sessies open te hebben.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: De architectuur van DigiD wordt niet getest tijdens een penetratietest	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	

Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	
Toelichting: Tijdens een externe pentest kan niet worden gecontroleerd of processen en bestanden geïsoleerd zijn.	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Toelichting: Tijdens een externe pentest kan niet worden gecontroleerd platform-netwerkkoppeling goed is ingeregeld.	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting: Tijdens een externe pentest kan niet worden gecontroleerd of de interne hardening goed is ingeregeld.	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting: Tijdens een externe pentest kan niet worden gecontroleerd of de interne communicatie betrouwbaar is.	
U/NW.02	**Beschikbaarheid van netwerken**
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Toelichting:	

Tijdens een externe pentest kan niet worden gecontroleerd of de zonering betrouwbaar is.	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Toelichting: DDoS en andere performancetesten vallen buiten de scope van de penetratietest.	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Toelichting: Interne toegang is buiten scope voor deze penetratietest	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Toelichting: Er is geen bewijs of aanwijzing gevonden dat van de norm wordt afgeweken.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	

Toelichting: Logius voert periodiek security tests uit waar vulnerability-assessments een onderdeel van zijn.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Toelichting: Logius voert periodiek security tests uit waar vulnerability-assessments een onderdeel van zijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Toelichting: Geen identificerende kenmerken voor sessies (i.v.m. meerdere sessies die actief kunnen zijn).	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Toelichting: Processen worden niet getest tijdens een penetratietest.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

Secure-flag ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
1		Zeer Laag	Laag	Zeer Laag

Betreffende hosts
balie-a3.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de "Secure"-flag mee te geven in de 'Set-cookie'-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruik maakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker naar een HTTP-pagina binnen het domein van de applicatie te lokken. Tenzij er gebruik gemaakt wordt van de 'HTTP Strict Transport Security'-header zal de browser de cookies dan naar deze (niet-bestaande) pagina versturen waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van de cookie naar de gebruiker moet Secure op de volgende manier aan de Set-Cookie-header worden toegevoegd:
'Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; "Secure"'"

Voor meer informatie over de Secure-flag en hoe deze te implementeren zie: https://www.owasp.org/index.php/SecureFlag
Let wel: Als de cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan de cookie op dat moment nog onderschept worden.

Details
De host: balie-a3.digid.nl heeft de volgende cookie zonder secure vlag:

```
_digid_balie_session
```

Request:

```
GET / HTTP/1.1
Host: balie-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://balie-a3.digid.nl/saml/sp/logout
Cookie: _session_id=5f3b1d861dd9d3637bba744eabcab307;
_persist=!BqSJTElPtuY0I4/+5aqg6lTJU5Hb5UWVpy3/UocNrFjeV+P4PcRPyxH4LEOe
S+HVv1Y0bXbELCnt1qE0eKxM+QzWPWgQm9R4vu7u8b4=;
persist_cis=!t9BuYLOe7suKRQ18aojjirYC1E4er65r08mogQl8xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDEiSy2x+03/+o=;
_digid_balie_session=2c748e0bfda4a4b46c5cfd74c2b53cf8
Connection: close
Upgrade-Insecure-Requests: 1
```

Response Headers:

```
HTTP/1.1 302 Found
Date: Mon, 14 Aug 2017 11:09:27 GMT
Cache-Control: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 38f5cf8b-e322-4524-b293-480fb78ad2ae
X-Runtime: 0.007100
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Set-Cookie: _digid_balie_session=2c748e0bfda4a4b46c5cfd74c2b53cf8;
path=/; expires=Mon, 14 Aug 2017 11:24:27 -0000; HttpOnly
Location: https://balie-a3.digid.nl/front_desk_relations/new
Status: 302 Found
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Content-Security-Policy (CSP) header ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
2		Zeer Laag	Zeer Laag	Laag

Betreffende hosts
mijn.a3.digid.nl
a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving

Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP header niet is geimplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en 'inline-scripts' niet worden uitgevoerd:
Content-Security-Policy: default-src self

Details
De server stuurt de CSP header niet mee. Hierdoor wordt niet optimaal gebruik gemaakt van beschermende maatregelen in de browser.
Het is aanbevolen om de server zo te configureren dat deze header wel wordt meegestuurd.
Voorbeeld Request:

```
GET / HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Connection: close
Upgrade-Insecure-Requests: 1
```

Response header:

```
HTTP/1.1 200 OK
Date: Tue, 15 Aug 2017 07:04:08 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: eb8e85ae-965a-46b8-bbc9-5fb070d911bb
X-Runtime: 0.112121
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Een overzicht van deze bevindingen.

Gelijktijdige sessies				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
3		Midden	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging

Wanneer er meerdere gelijktijdige sessies voor dezelfde gebruiker kunnen bestaan betekent dit dat oude sessies niet automatisch worden afgesloten. Dit geeft een aanvaller de mogelijkheid om oude sessies te misbruiken, ook als de gebruiker al een nieuwe sessie heeft opgestart.

Aanbeveling

Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Dit verkleint de kans dat een aanvaller een oude sessie van een gebruiker misbruikt. Daarnaast wordt een gebruiker automatisch gewaarschuwd als een aanvaller een sessie namens hem start. Bij vermoedens van misbruik kan een gebruiker een eventuele oude sessie sluiten door nogmaals in te loggen.

Details

Het is mogelijk om op de Mijn DigiD-omgeving meerdere actieve sessies per DigiD account te hebben. Dit houdt in dat er op meerdere apparaten wordt ingelogd met één DigiD account. De gebruikersgeschiedenis toont de inlogacties:

Gebruiksgeschiedenis

U kunt het gebruik van uw DigiD hier inzien. Mocht u naar aanleiding hiervan vermoeden dat iets niet klopt, neem dan contact op met de helpdesk.

U bent ingelogd sinds 15 augustus 2017 om 13:21 uur (Nederlandse tijd).

Mijn gebruiksgeschiedenis

Tijdstip (Nederlandse tijd)	Omschrijving
15-08-2017 13:21:58	Bekijkt gebruiksgeschiedenis
15-08-2017 13:21:49	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD
15-08-2017 13:21:45	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD

Naar Mijn gegevens

Het is ook mogelijk om met beide sessies acties uit te voeren op de Mijn DigiD-omgeving. Ga na of het nodig is voor een gebruiker om twee gelijktijdige sessies toe te staan.

Onjuist afbreken van sessie na opschorten account				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
4		Midden	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

In sommige gevallen kan bepaalde functionaliteit waarvoor authenticatie nodig is nog steeds worden gebruikt nadat de sessie afgebroken zou moeten zijn.

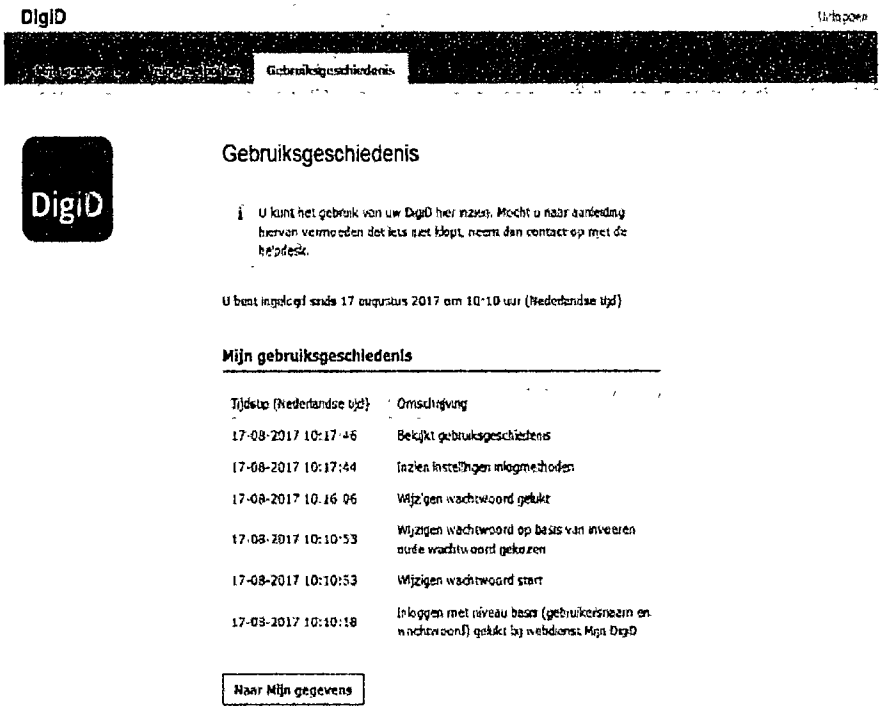
Bedreiging

Door het onjuist afbreken van een sessie kan een aanvaller nog gebruikmaken van functionaliteit die in de sessie verkregen is, ondanks dat de sessie niet meer geldig zou moeten zijn.

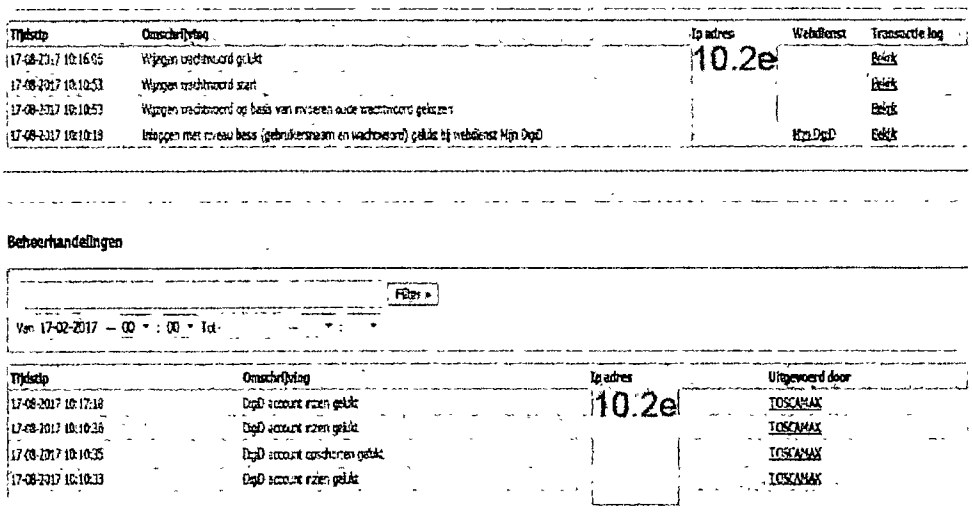
Aanbeveling

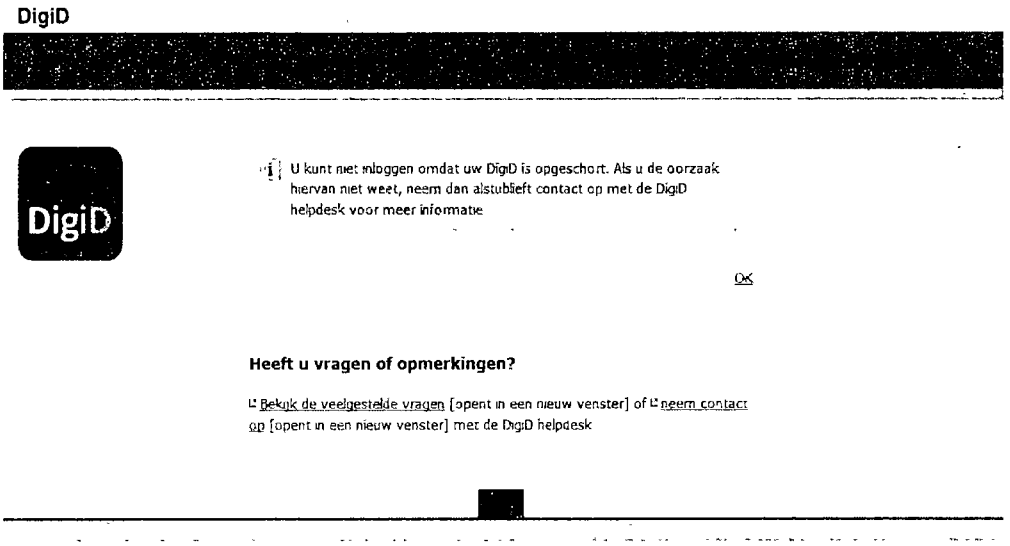
Zorg ervoor dat geen functionaliteit beschikbaar blijft na het afbreken van een sessie.

Details
Een gebruiker kan, mits hij is ingelogd, acties blijven uitvoeren als in de tussentijd zijn of haar account is opgeschort. Het lijkt erop alsof sessies niet server-side beëindigd worden als een account wordt opgeschort in het admingedeelte. Hieronder is te zien dat een gebruiker zijn wachtwoord om 10:16 heeft gewijzigd:



Tussen het inloggen en het starten van de actie is zijn account opgeschort:





3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen bevindingen gedaan in deze onderzoekscategorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

Weak Block cipher – 64 bit TLS Sweet32				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
5		Midden	Laag	Midden

Betreffende hosts

balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving

De TLS server maakt gebruik van algoritmes die intern 64-bit block ciphers gebruiken.

Bedreiging

64-bit block ciphers zijn kwetsbaar voor een zogenaamde birthday attack, waarbij de kans dat twee willekeurig gegenereerde waarden overeenkomen hoger dan 50% is. Dit wordt vervolgens gebruikt om een zogenaamde collision te forceren, waarmee achterhaald kan worden wat de originele waarde was van een versleuteld stukje data. Gegeven genoeg data (de ontdekkers hadden 785GB aan HTTPS verkeer nodig) is het mogelijk om met een man-in-the-middle attack de waarde van bijvoorbeeld een versleutelde cookie te achterhalen.

Aanbeveling

Schakel de kwetsbare block ciphers uit binnen TLS.

Indien dit niet mogelijk is, zorg er dan voor dat geheime waarden (zoals een sessie token) met een hoge frequentie veranderen. Dit verzekert dat eventueel (gedeeltelijke) achterhaalde waarden niet meer valide zijn, en daarmee geen waarde meer hebben voor aanvallers.

Details

De server ondersteunt cipher suites die gebruik maken van 64-bit block ciphers:

```
List of 64-bit block cipher suites supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    TLSv1
      ECDHE-RSA-DES-CBC3-SHA          Kx=ECDH         Au=RSA
Enc=3DES-CBC(168)          Mac=SHA1
      DES-CBC3-SHA                    Kx=RSA          Au=RSA
Enc=3DES-CBC(168)          Mac=SHA1
```

```
The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Schakel ondersteuning voor deze cipher suites uit.

Information disclosure – Dienstinformatie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
6		Opgelost	Laag	Laag

Betreffende hosts

rda-a3.digid.nl

Omschrijving

Bij het installeren van diensten op de server wordt er vaak een standaardpagina gegenereerd waarmee de beheerder kan verifiëren of het onderdeel correct geïnstalleerd is en op dit moment actief is.

Bedreiging

Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in een specifieke software- of hardwareversie.

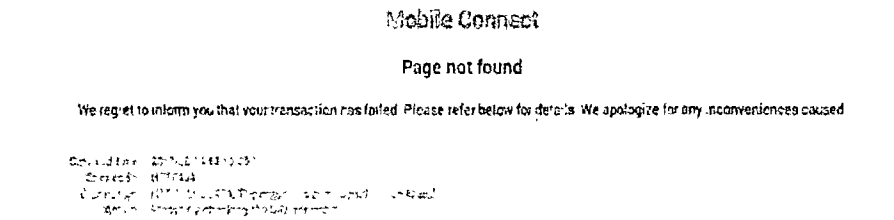
Aanbeveling

Stel in dat deze pagina alleen beschikbaar voor de beheerder van het systeem, door bijvoorbeeld gebruik te maken van whitelisting. Een andere optie is om deze pagina te verwijderen dan wel aan te passen naar een standaardmelding.

Details

Deze bevinding is tijdens de test gemarkeerd als opgelost

Door een pagina die niet bestaat achter https://rda-a3.digid.nl/idp/ te plaatsen wordt er een standaard not found pagina getoond. Hierbij kan worden achterhaald dat er gebruik wordt gemaakt van de mobileconnect service.



Denial of Service – Email versturen				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
7		Midden	Laag	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het systeem is zo te manipuleren dat de server een grote hoeveelheid emails naar een gebruiker stuurt.

Bedreiging

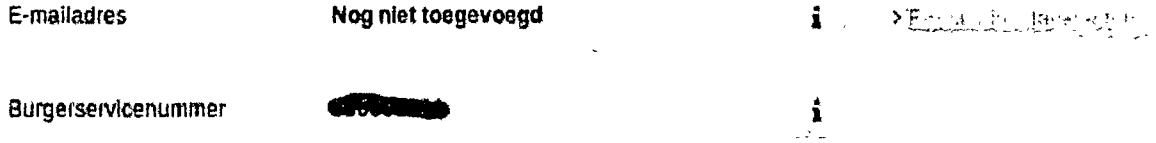
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling

Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een email is gestuurd naar de gebruiker.

Details

Het is mogelijk om via de DigiD applicatie een continue stroom emails te versturen naar een willekeurig e-mailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.



Wanneer er een e-mailadres wordt opgegeven en op de volgende knop wordt knop wordt gedrukt wordt onderstaande request verzonden:

```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
```

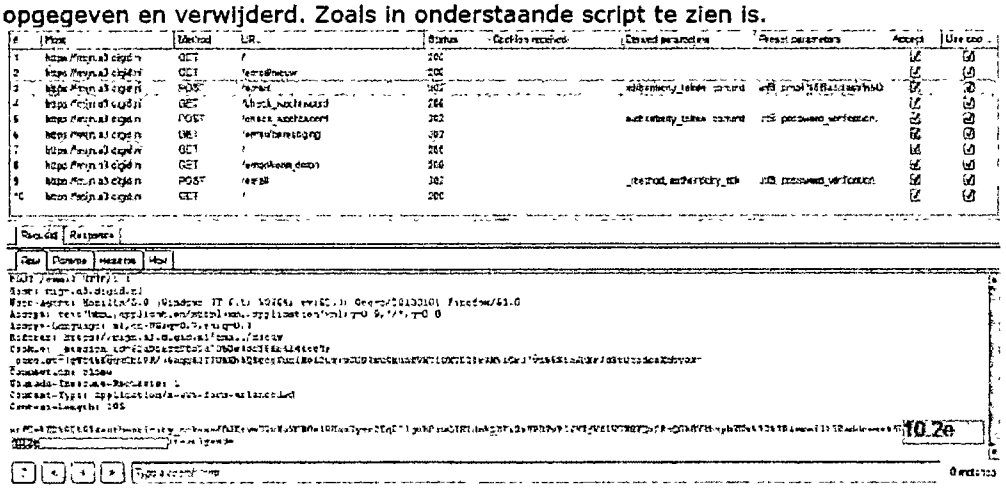
```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/email/nieuw
Content-Type: application/x-www-form-urlencoded
Content-Length: 201
Cookie: _session_id=b112cca5cd799b8a426083f6076822e8;
_persist=!OWAYhwuOz3MxOfj+5aqg6lTJU5Hb5ZGZXgyuOQ3RaXAbsSqHBitJ4v310JX0
zjzc1nixxqmpazpl55wKVrve0WRNs7ehRX0JfdWstO4=;
persist_cis=!t9BuYLOe7suKRQ18aojjirYC1E4er65r08mogQ18xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDEiSy2x+03/+o=
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=GvI8j37pHUO9s%2BaufoIjm4Zjef%2Bn4blo
f6bsbV%2BVjwKwuVM7X7RcGZ8dWvSkb8BTsUIHqNpuLc5%2BM1ACFIReSg%3D%3D&email
%5Baddress%5D=10.2e&commit=Volgende
```

De reponse zorgt er voor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

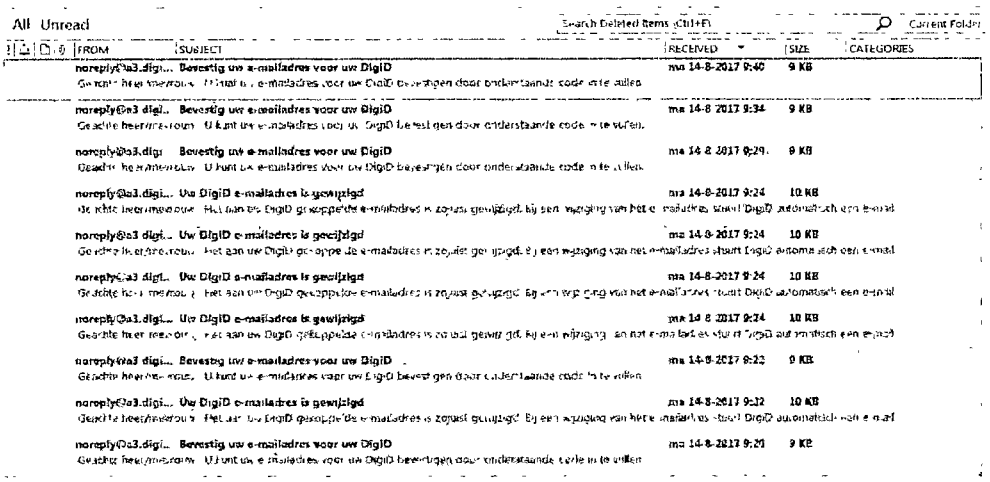
Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatie code naar het email adres. Deze code moet binnen een bepaalde periode wordt opgegeven anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wilt versturen verschijnt de melding dat er al een code onderweg en na meer dan 10 minuten een nieuwe code kan worden aangevraagd. "Er is nog een e-mail onderweg naar u. Vanaf 13:41 uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen." Echter is het mogelijk om het nog-niet geactiveerde e-mailadres te verwijderen van het account.

Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg is dat de gebruiker bovenstaande actie nog een keer kan uit voor het zelfde of andere e-mailadressen.

Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.



Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:



Er bestaat het gevaar dat als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail, de mail wordt aangemerkt als spam of phising.

4 Bijlagen

4.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-around' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rapport securitytest

DigiD release 5.5

Kenmerk:

Datum	28 november 2017
Status	Concept
Versie	1.0

Na *<einddatum/gebeurtenis>* is deze rubricering beëindigd.
Rubricering derubricering
Vaststeller
Functie

Colofon

Kenmerk	201728
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
23-11-2017	0.1	Sogeti	Initiële versie
28-11-2017	1.0	Sogeti	Definitieve versie

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

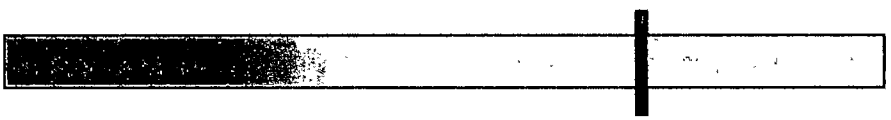
Managementsamenvatting

Inleiding

Het informatiebeveiligingsbeleid van Logius schrijft voor dat de producten van Logius periodiek worden getest op zwakheden door middel van een zogenaamde securitytest (ook wel penetratietest of pentest genoemd). De aanleiding tot deze securitytest was de aanstaande release 5.5 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het bevelligingsniveau van de release voldoende is, maar dat er desondanks ruimte is voor verbetering. Er zijn geen bevindingen gedaan met een risiconiveau hoger dan Midden. Tijdens de test zijn er geen negatieve bevindingen gedaan met betrekking tot de *certificate pinning* in de productieversies van de mobiele app voor DigiD.



Onvoldoende Voldoende

Punten ter verbetering:

- De gebruiker kan meerdere keren tegelijk ingelogd zijn. Dit verhoogt de kans dat één van zijn sessies misbruikt wordt door een aanvaller; bevinding 8.
  Aanbeveling: Zorg dat de gebruiker maar één sessie kan hebben.
- De instellingen van de beveiligde verbinding tussen de gebruiker en de server kunnen verbeterd worden; bevinding 5.
  Aanbeveling: Verander de instellingen.

Conclusie hertest:

- Het is nog steeds mogelijk om als gebruiker meerdere actieve sessies te hebben; bevinding 8.
  Aanbeveling: Breek bestaande sessies automatisch af zodra er een nieuwe gestart wordt.
- Het is nog steeds mogelijk om het systeem herhaaldelijk e-mail te laten versturen naar een e-mailadres naar keuze; bevinding 10.
  Aanbeveling: Zorg dat het aantal verstuurde e-mails beperkt wordt.
- Er zijn 3 bevindingen uit de vorige securitytest opgelost; bevindingen 6, 9 en 11.

Aanvullingen Logius

Reactie van Logius.

[Om de conclusies en integriteit van de opsteller/opdrachtnemer te respecteren (ook i.v.m. mogelijke audits), kan Logius hier een aanvullende reactie plaatsen ten aanzien van de geconstateerde zaken. De opdrachtnemer kan niet altijd de gehele context zien, waarbinnen deze opdracht is uitgevoerd.

1 Inleiding

1.1 Opdrachtformulering

De opdracht is grotendeels conform het Security Testplan uitgevoerd.

De scope van deze securitytest was de gehele DigiD-applicatie, waarbij de nadruk lag op de wijzigingen en uitbreidingen die in release 5.5 worden doorgevoerd. Hierbij moet opgemerkt worden dat een aanzienlijk deel van de wijzigingen kleine inhoudelijke aanpassingen betreft. Deze wijzigingen worden voldoende getest tijdens de functionele test van release 5.5[1] en behoeven dus geen extra aandacht tijdens de securitytest. Daarnaast is een belangrijk deel van de uitbreidingen ter voorbereiding van de toevoeging van DigiD Hoog in een toekomstige release. Deze toevoegingen worden in release 5.5 nog niet in productie genomen en waren nog niet functioneel. Derhalve kon de beveiliging van deze toevoegingen in deze securitytest nog niet onderzocht worden.

Tijdens het testtraject van de vorige release van DigiD is gebleken dat er naast de externe tests ook de wens is om interne tests uit te laten voeren op de DigiD-omgeving. De externe tests zijn de gebruikelijke securitytest op de DigiD-applicatie vanuit het oogpunt van de gebruiker of aanvaller van buitenaf. De interne tests moeten zich richten op de DigiD-infrastructuur en -omgeving vanuit het oogpunt van een gebruiker of aanvaller die al toegang heeft tot één of meerdere lagen van de interne omgeving. Op deze manier kan onder andere onderzocht worden welke risico's er bestaan wanneer een aanvaller erin slaagt de buitenste laag van beschermingsmechanismen, zoals de centrale firewall van Equinix, te doorbreken[2].

Tijdens deze securitytest zou een eerste interne test gedaan worden om te onderzoeken welke bedreiging er bestaat wanneer een aanvaller erin slaagt het buitenste beschermingsmechanisme van de omgeving – de centrale firewall van [redacted] – te doorbreken of omzeilen. In de voorbereiding is er uiteindelijk voor gekozen om pas bij de volgende release van DigiD te beginnen met de interne tests[3].

Zie 'PVA securitytest – DigiD 5.5 v1.0.docx', hoofdstuk 2, 'Opdrachtformulering'.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd.

De securitytest heeft bestaan uit een vulnerability assessment met een diepgang greybox (deels whitebox en deels blackbox) en betreft een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A3-omgeving.

---

[1] *Zie ook het Master TestPlan voor release 5.5*

[2] *Bij een defense-in-depth-strategie worden er meerdere lagen van beveiligingsmechanismen toegepast om een systeem te beschermen, zodat er ook bij het wegvallen van één van de lagen bescherming overblijft. In het geval van DigiD wordt onder andere gebruikgemaakt van verschillende firewalls, gescheiden subnets voor onderdelen van de omgeving, en beveiligingen op applicatieniveau*

[3] *Zie e-mail van 3 november 2017*

De aandachtsgebieden met betrekking tot DigiD Hoog en de statuscontroler waren buiten scope voor deze securitytest omdat ze in release 5.5 nog niet functioneel zijn en de beveiliging ervan derhalve niet getest kon worden. Tijdens de securitytest is ook gelet worden op eventuele regressie dan wel ongeautoriseerde of onbedoelde veranderingen.

Tijdens eerdere tests op DigiD is een aantal bevindingen gedaan dat bij de test op release 5.5 specifiek opnieuw moest worden getest. Logius heeft de lijst van deze bevindingen niet voor aanvang van de test opgeleverd. Gedurende het attack window heeft Sogeti het rapport over de vorige securitytest ontvangen zodat de bevindingen uit dat rapport opnieuw getest konden worden. Deze bevindingen worden besproken in hoofdstuk 4. De mantis-nummers voor de betreffende bevindingen ontbreken nog omdat die niet in het oude rapport voorkomen (deze worden altijd pas na oplevering van het rapport door Logius aangemaakt).

Daarnaast heeft Logius een lijst opgesteld van bevindingen uit eerdere tests die om businessredenen (nog) niet opgelost kunnen worden. Deze bevindingen worden gezien als geaccepteerde risico's. Tijdens de securitytest moest gecontroleerd worden of deze bevindingen nog steeds aanwezig waren. De resultaten van deze controle zouden in een apart hoofdstuk van het securitytestrapport opgenomen worden. Logius heeft de lijst niet voor het opstellen van het rapport opgeleverd, waardoor het mogelijk is dat deze bevindingen nu als 'normale' bevinding in het rapport opgenomen zijn. Het aparte hoofdstuk ontbreekt vanzelfsprekend.

Op verzoek van Logius is ook gecontroleerd of de productieversies van de mobiele apps voor DigiD correct gebruikmaken van *Certificate pinning*.

Zie 'PVA securitytest – DigiD 5.5 v1.0.docx', hoofdstuk 4, 'Aanpak' en hoofdstuk 7, 'Aanpak securityassessment'.

2 Resultaten

2.1 Cumulatief overzicht

Een totaaloverzicht van het aantal geconstateerde bevindingen.
Zie paragraaf 5.1 voor een toelichting op de risicoclassificatie. In de tabel hieronder geven aantallen tussen haakjes bevindingen aan die tijdens het hertest-onderdeel van deze test opgelost gebleken zijn.

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
NCSC-richtlijnen						
Client-side controls				1	1 (1)	2
Logica						
Authenticatie			1		2	3
Sessiemanagement			(1)			
Toegang						
Invoerafhandeling						
Omgeving						
Servers			1 (1)	1	1	3
Totaal			**2**	**2**	**4**	**8**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[4], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	

[4] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

Buiten scope voor deze test.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope voor deze test.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.01	**Operationeel beleid voor webapplicaties**
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Buiten scope voor deze test.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Buiten scope voor deze test.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Geen bevindingen.	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Bevindingen 1, 7 en 10	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Bevindingen 5 en 11	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Bevinding 2	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit	

en vertrouwelijkheid garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Bevindingen 8 en 3	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Buiten scope voor deze test.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Geen bevindingen.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Geen bevindingen.	
U/PW.04	**Isolatie van processen/bestanden**
Beperk de impact bij misbruik van processen.	
Oordeel	
Geen bevindingen.	
U/PW.05	**Toegang tot beheermechanismen**
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Buiten scope voor deze test.	
U/PW.06	**Platform-netwerkkoppeling**
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Buiten scope voor deze test.	
U/PW.07	**Hardening van platformen**
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Bevinding 4	
U/PW.08	**Platform- en webserverarchitectuur**
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/NW.01	**Operationeel beleid voor netwerken**
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting	
U/NW.02	**Beschikbaarheid van netwerken**
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	

Oordeel	
Buiten scope voor deze test.	
U/NW.03	**Netwerkzonering**
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Buiten scope voor deze test.	
U/NW.04	**Protectie- en detectiefunctie**
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Buiten scope voor deze test.	
U/NW.05	**Beheer- en productieomgeving**
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Buiten scope voor deze test.	
U/NW.06	**Hardening van netwerken**
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Bevinding 4	
U/NW.07	**Netwerktoegang tot webapplicatie**
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	
Geen bevindingen.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Buiten scope voor deze test.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Buiten scope voor deze test.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Buiten scope voor deze test.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Buiten scope voor deze test.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	

Oordeel	
Deze test is onderdeel van het voldoen aan deze richtlijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Buiten scope voor deze test.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingselsen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Buiten scope voor deze test.	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Buiten scope voor deze test.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Buiten scope voor deze test.	
C.09	**Patchmanagement**
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Buiten scope voor deze test.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope voor deze test.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Geen bevindingen.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

Content-Security-Policy header implementatiefout				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
1	Nnb	Laag	Zeer laag	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven. De policy welke door de server verstuurd wordt is niet correct/veilig.

Bedreiging
Wanneer de CSP header niet correct is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwen code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP policy zo strak mogelijk, waarbij onveilig gedrag niet toegelaten wordt. Bouw vanuit hier de policy uit met alleen die functionaliteit welke nodig is. Gebruik hierbij voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Details
De server gebruikt niet de meest veilige opties voor de Conten Security Policy-header.

```
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
```

Er worden potentieel onveilige inline-elementen en het gebruik van de *eval*-functie toegestaan.

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Een overzicht van deze bevindingen.

Directe gebruikersnaam enumeratie				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
2	Nnb	Zeer laag	Zeer laag	Laag

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het systeem geeft informatie over het bestaan van gebruikersnamen.

Bedreiging

Kennis over bestaande gebruikersnamen geeft een aanvaller mogelijkheden voor verdere aanvallen. Het systeem kan aangevallen worden door bijvoorbeeld een bruteforce aanval uit te voeren op de gebruikersnamen. De gebruiker kan aangevallen worden door een denial-of-service aanval middels account blokkades, of social engineering wanneer email addressen achterhaald kunnen worden.

Aanbeveling

Het systeem maar dient generieke meldingen te tonen die geen informatie geeft over het bestaan van gebruikersnamen. Bijvoorbeeld voor een wachtwoord vergeten functionaliteit: "Indien het account bestaat, zijn de instructies voor het wijzigen van het wachtwoord verzonden".

Details
De Mijn DigiD-omgeving biedt in het scherm gebruiksgeschiedenis aan de eindgebruiker de mogelijkheid om in te zien welke acties zijn uitgevoerd op de omgeving. Wanneer het account voor de eerste keer wordt geactiveerd, dan wordt de gebruikersnaam getoond in de geschiedenis:

```
<tr class='table-row'>
<td class='table-cell--history-date'>20-11-2017 11:39:06</td>
<td class='table-cell'>Activeren gelukt (u_000000036, basis)</td>
</tr>
```

In het geval dat een sessie wordt overgenomen, dan kan de aanvaller via de geschiedenis de gebruikersnaam achterhalen. Dit is een zeer laag risico, maar voor *defence in depth* is het aanbevolen om geen gebruikersnamen te tonen binnen de omgeving.

Wachtwoordsterkte onvoldoende				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
3	Nnb	Zeer laag	Zeer laag	Laag

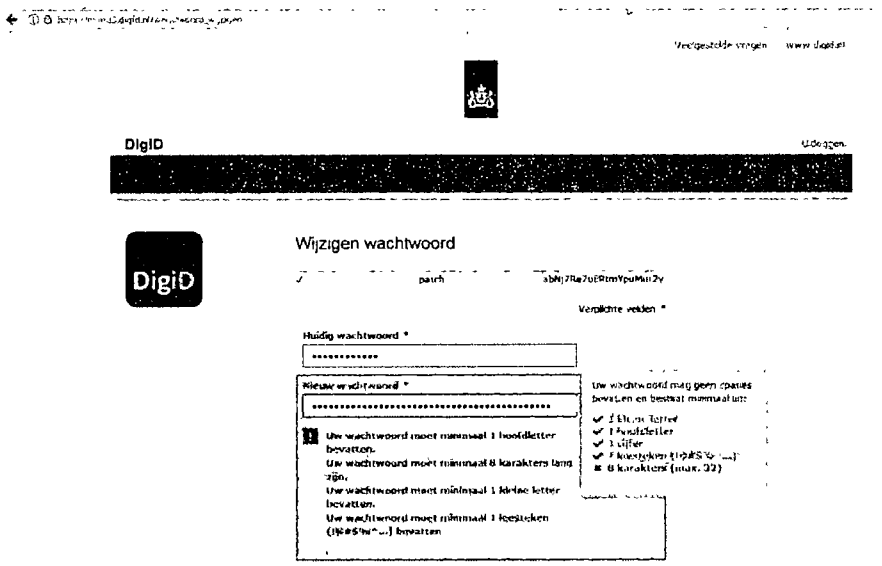
Betreffende hosts
mijn.a3.digid.nl

Omschrijving
De eisen die door de applicatie aan het wachtwoord van de gebruiker gesteld worden zijn niet veilig genoeg.

Bedreiging
Zwakke wachtwoorden zouden door middel van een bruteforce attack kunnen worden 'gekraakt'.

Aanbeveling
Door eisen te stellen aan de kwaliteit van wachtwoorden, wordt de kans kleiner dat ze kunnen worden 'gekraakt'. Het wachtwoord van een applicatie zou voldoende sterk moet zijn om een bruteforce attack te weerstaan. De bepalende factor hierin is de lengte en niet de gebruikte tekenset. Indien relatief korte wachtwoorden een vereiste of toegestaan zijn, dan zouden deze bijvoorbeeld ten minste moeten bestaan uit een combinatie van een kleine letter, een hoofdletter, een cijfer en/of een leesteken om de gebruikte tekenset zo groot mogelijk te maken.

Details
De minimumlengte van een wachtwoord is 8 tekens en het is aanbevolen om de minimumeis op te hogen naar 12 tekens. Daarnaast is het niet aanbevolen om een maximum aan de wachtwoordlengte te stellen, want dat beperkt de gebruiker in het kiezen van een lange *pass phrase*.



3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet

verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Er zijn geen bevindingen in deze categorie.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

Open poorten				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
4		Zeer laag	Zeer laag	Zeer laag

Betreffende hosts

mijn.a3.digid.nl
a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving

Tijdens het onderzoek is er gekeken welke netwerkpoorten er op de systemen geopend zijn en welke services er (waarschijnlijk) op die poorten luisteren.

Bedreiging

Een open poort is zeker niet altijd een bedreiging; het is immers noodzakelijk om poorten open te zetten als systemen met elkaar moeten communiceren. Als er echter poorten onbedoeld of onnodig openstaan heeft een aanvaller meer mogelijkheden om een systeem aan te vallen.

Aanbeveling

Controleer de lijst met gevonden open poorten om te zien of er poorten open staan die gesloten kunnen worden.

Details

Op de servers staat naast poort 443 ook poort 80 open. Het is aanbevolen om enkel poort 443 open te zetten, want de dienst moet enkel via HTTPS worden aangeboden. Daarnaast tonen zoekmachines vaak standaard de HTTPS-pagina. Voor een publieke dienst als DigiD is het echter

noodzakelijk om voor een zo groot mogelijke groep burgers toegankelijk te zijn. Die eis, in combinatie met het minimale risico van de bevinding, verantwoordt de keuze om poort 80 open te houden om gebruikers automatisch door te kunnen sturen naar poort 443.

BEAST (Browser Exploit Against SSL/TLS)				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
5	Nnb	Laag	Zeer laag	Midden

Betreffende hosts

was-a3.digid.nl
digibeheer-a3.digid.nl
mijn.a3.digid.nl

Omschrijving

De SSL/TLS implementatie op de server maakt het mogelijk om een voorspelbare ciphertext te genereren uit plaintext.

Bedreiging

In cryptografie is Cipher Block Chaining (CBC) een veelgebruikte methode om de voorspelbaarheid van encrypted data te verminderen. Het doel is om te voorkomen dat dezelfde data (plaintext) tot dezelfde encrypted data (ciphertext) leidt gedurende het encryptieproces. Hiervoor wordt een zogenaamde initialization vector (IV) gebruikt, die uniek is voor elk bericht in elke sessie. CBC encrypt ieder blok data en gebruikt deze data ook als input voor de encryptie van het volgende blok data: het "chainen". Dit doel wordt ondermijnd door oudere implementaties van SSL/TLS, waardoor in sommige situaties de IV voorspelbaar is, dus ook de ciphertext. Dit op zijn beurt kan gebruikt worden om (delen van) de plaintext data terug te berekenen vanuit de encrypted data.

Aanbeveling

Upgrade naar TLSv1.2. Een andere, niet aan te raden, oplossing is het gebruiken van encryptie zonder CBC.

Details

De verbinding tussen de server en de gebruiker is mogelijk kwetsbaar voor BEAST omdat er CBC-ciphers ondersteund worden:

```
Negotiated cipher suite: ECDHE-RSA-AES256-
SHA|TLSv1|Kx=ECDH|Au=RSA|Enc=AES-CBC(256)|Mac=SHA1
```

4 Hertest

In dit hoofdstuk worden bevindingen uit een test op een eerdere release van DigID opnieuw behandeld.

Hertest: Secure-flag ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
6	Nb	Zeer laag	Laag	Zeer laag

Betreffende hosts
balie-a3.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de "Secure"-flag mee te geven in de 'Set-cookie'-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruik maakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker naar een HTTP-pagina binnen het domein van de applicatie te lokken. Tenzij er gebruik gemaakt wordt van de 'HTTP Strict Transport Security'-header zal de browser de cookies dan naar deze (niet-bestaande) pagina versturen waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van de cookie naar de gebruiker moet Secure op de volgende manier aan de Set-Cookie-header worden toegevoegd:
Set-Cookie: [NAAM]=[WAARDE]; path=[PAD]; **Secure**

Voor meer informatie over de Secure-flag en hoe deze te implementeren zie: https://www.owasp.org/index.php/SecureFlag
Let wel: Als de cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan de cookie op dat moment nog onderschept worden.

Details
Bevindingen hertest release 5.5:
De bevinding is opgelost; de server stelt de cookie nu in mét de Secure-flag:

Response headers:

```
HTTP/1.1 200 OK
Date: Mon, 20 Nov 2017 08:41:00 GMT
Cache-Control: max-age=0, private, must-revalidate
X-XSS-Protection: 1; mode=block
X-Request-Id: 54c4c326-a4ff-4d41-a875-a81c7b196ac0
X-Frame-Options: SAMEORIGIN
X-Runtime: 0.050550
```

```
X-Content-Type-Options: nosniff
Set-Cookie:
_digid_balie_session=ae1fbe6f8bfe8a58841e4abeb71755a0;Secure; path=/;
expires=Mon, 20 Nov 2017 08:56:00 -0000; HttpOnly
ETag: W/"2df788c8fbec05a02799e589dc65eb58"
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Originele bevinding:
De host balie-a3.digid.nl heeft de volgende cookie zonder secure vlag:
_digid_balie_session

Request:

```
GET / HTTP/1.1
Host: balie-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language. en-US,en;q=0.5
Referer: https://balie-a3.digid.nl/saml/sp/logout
Cookie: _session_id=5f3b1d861dd9d3637bba744eabcab307;
_persist='BqSJTElPtuY0I4/+5aqg6lTJU5Hb5UWVpy3/UocNrFjeV+P4PcRPyxH4LEOe
S+HVv1Y0bXbELCnt1qE0eKxM+QzWPWgQm9R4vu7u8b4=;
persist_cis=!t9BuYLOe7suKRQ18aojjirYC1E4er65r08mogQl8xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDE1Sy2x+03/+o=;
_digid_balie_session=2c748e0bfda4a4b46c5cfd74c2b53cf8
Connection: close
Upgrade-Insecure-Requests: 1
```

Response Headers:

```
HTTP/1.1 302 Found
Date: Mon, 14 Aug 2017 11:09·27 GMT
Cache-Control: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 38f5cf8b-e322-4524-b293-480fb78ad2ae
X-Runtime: 0.007100
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Set-Cookie: _digid_balie_session=2c748e0bfda4a4b46c5cfd74c2b53cf8;
path=/; expires=Mon, 14 Aug 2017 11:24:27 -0000; HttpOnly
Location: https://balie-a3.digid.nl/front desk relations/new
Status: 302 Found Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest: Content-Security-Policy (CSP) header ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
7	Nb	Zeer laag	Zeer laag	Laag

Betreffende hosts
a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
digidbeheer-a3.digid.nl
rda-a3.digid.nl
was-a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en 'inline-scripts' niet worden uitgevoerd:
Content-Security-Policy: default-src self

Details
Bevindingen hertest release 5.5:
De servers maken nog steeds geen gebruik van de Content Security Policy-header.

Originele bevinding:
De server stuurt de CSP header niet mee. Hierdoor wordt niet optimaal gebruik gemaakt van beschermende maatregelen in de browser.
Het is aanbevolen om de server zo te configureren dat deze header wel wordt meegestuurd.
Voorbeeldrequest:

```
GET / HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en,q=0.3
Connection: close
Upgrade-Insecure-Requests. 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Tue, 15 Aug 2017 07:04:08 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: eb8e85ae-965a-46b8-bbc9-5fb070d911bb
X-Runtime: 0.112121
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00.00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
```

```
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Hertest: Gelijktijdige sessies				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
8	Nb	Midden	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging

Wanneer er meerdere gelijktijdige sessies voor dezelfde gebruiker kunnen bestaan betekent dit dat oude sessies niet automatisch worden afgesloten. Dit geeft een aanvaller de mogelijkheid om oude sessies te misbruiken, ook als de gebruiker al een nieuwe sessie heeft opgestart.

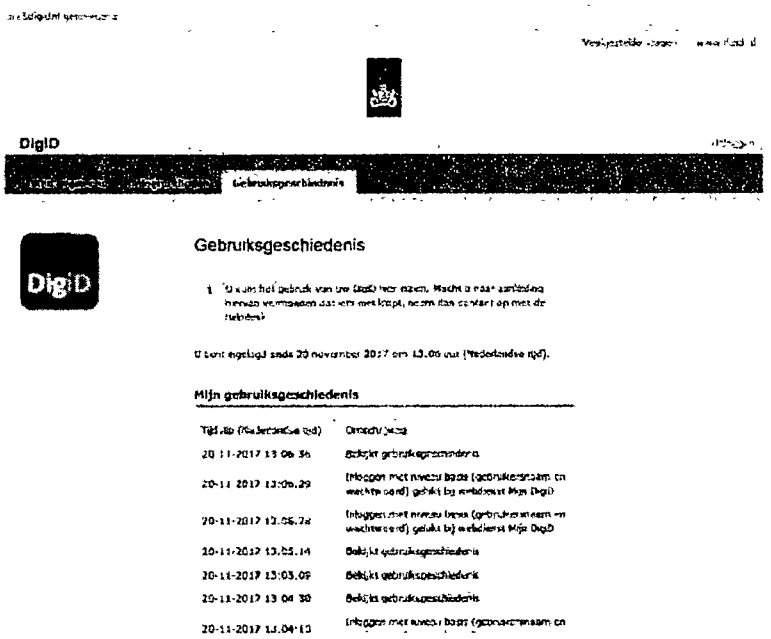
Aanbeveling

Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Dit verkleint de kans dat een aanvaller een oude sessie van een gebruiker misbruikt. Daarnaast wordt een gebruiker automatisch gewaarschuwd als een aanvaller een sessie namens hem start. Bij vermoedens van misbruik kan een gebruiker een eventuele oude sessie sluiten door nogmaals in te loggen.

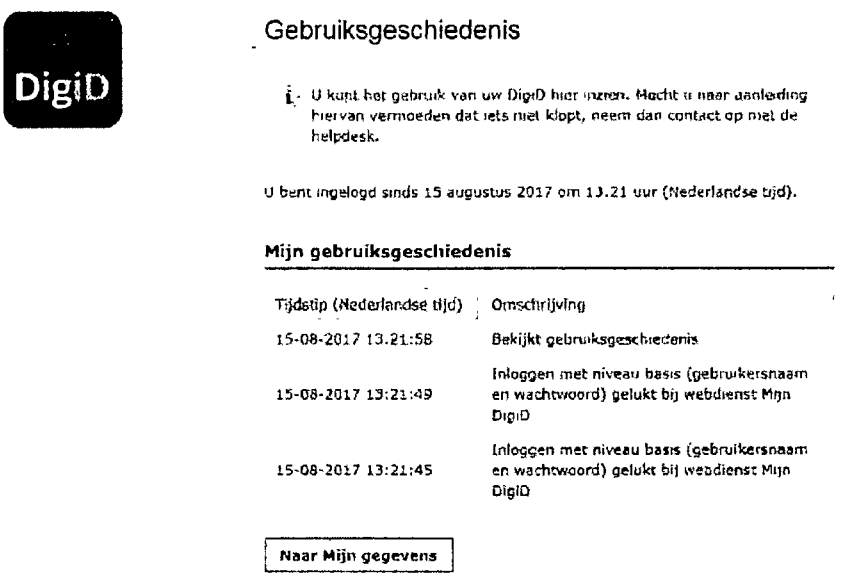
Details

Bevindingen hertest release 5.5:

Het is nog steeds mogelijk om tegelijkertijd meerdere actieve sessies per account te hebben. In het volgende screenshot is te zien dat er kort na elkaar is ingelogd.



Originele bevinding:
Het is mogelijk om op de Mijn DigiD-omgeving meerdere actieve sessies per DigiD account te hebben. Dit houdt in dat er op meerdere apparaten wordt ingelogd met één DigiD account. De gebruikersgeschiedenis toont de inlogacties:



Het is ook mogelijk om met beide sessies acties uit te voeren op de Mijn DigiD-omgeving. Ga na of het nodig is voor een gebruiker om twee gelijktijdige sessies toe te staan.

Hertest: Onjuist afbreken van sessie na opschorten account				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
9	Nb	Midden	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

In sommige gevallen kan bepaalde functionaliteit waarvoor authenticatie nodig is nog steeds worden gebruikt nadat de sessie afgebroken zou moeten zijn.

Bedreiging

Door het onjuist afbreken van een sessie kan een aanvaller nog gebruikmaken van functionaliteit die in de sessie verkregen is, ondanks dat de sessie niet meer geldig zou moeten zijn.

Aanbeveling

Zorg ervoor dat geen functionaliteit beschikbaar blijft na het afbreken van een sessie.

Details

Bevindingen hertest release 5.5:

Deze bevinding is gedaan in het onderzoek van release 5.4 en in het huidige onderzoek gehertest. In de huidige test zijn de volgende stappen doorgelopen

1. Op Mijn DigiD is ingelogd met een gebruiker
2. Gebruiker gaat naar wachtwoord wijzigen
3. Op https://digidbeheer-a3.digid.nl/ wordt het account opgeschort, terwijl de gebruiker nog een actieve sessie heeft
4. De gebruiker krijgt de volgende melding als hij zijn wachtwoord probeert te wijzigen:

Request:

```
POST /wachtwoord_wijzigen HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:57.0)
Gecko/20100101 Firefox/57.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://mijn.a3.digid.nl/wachtwoord_wijzigen
Content-Type: application/x-www-form-urlencoded
Content-Length: 340
Cookie: _session_id=b919cdbcf7f6de9c1da274c298d1dc42;
_persist='O+/gZwDjikvEzPMZzh+/BjbEK230waIwhXHxBqf9Ql8E6eVkZh+Brwm7Mmuu
FCJ0n2VXtfKo8SWZFu/G4MzyT3mll0WSwpFQbaGt3N0=
Connection: close
Upgrade-Insecure-Requests: 1
utf8=%E2%9C%93&_method=patch&authenticity_token=ApTjMswc3C33FWd2V0feMQ
wryggFqJ2DuQliOFlhYR%2FkBTrwNYrplDrLLMJYtefoPls6wlFvDwUJPRCHZk9jBg%3D%
3D&password_changing_account%5Bcurrent_password%5D=Pw_000000036&passwo
rd_changing_account%5Bpassword%5D=Pw_000000036n&password_changing_acco
unt%5Bpassword_confirmation
```

Response:

```
HTTP/1.1 200 OK
Date: Wed, 22 Nov 2017 12:05:33 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 50ddda9e-a458-4c3c-8bb7-aef02124541c
```

```
X-Runtime: 0.015902
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=f26c0d71c17795b054dc323976cce6dc;Secure;
domain=.digid.nl; path=/; HttpOnly
Status: 200 OK
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Connection: close
Set-Cookie:
_persist=!W11CwhMYKvK0IRoZzh+/BjbEK230wWeTwrRZ5FYZ8KXiRi/qRNeBBJTiBpvO
Uh0301QUQvza01XP5WB4vu0b1s11KBgeFpcCTZAXgso=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 3271
<!DOCTYPE html>
[.. knip ..]
<div class="block-with-icon--information"><p>U kunt niet inloggen
omdat uw DigiD is opgeschort. Als u de oorzaak hiervan niet weet, neem
dan alstublieft contact op met de DigiD helpdesk voor meer
informatie.</p></div>
<div class="actions"><a class="actions__left--link"
href="https://a3.digid.nl/">OK</a>
</div>
[.. knip ..]
```

Hieruit kan geconcludeerd worden dat het niet meer mogelijk is om acties uit te voeren met een opgeschort account.

Hertest: Denial-of-Service – Email versturen				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
10	Nb	Midden	Laag	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het systeem is zo te manipuleren dat de server een grote hoeveelheid emails naar een gebruiker stuurt.

Bedreiging

Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling

Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een email is gestuurd naar de gebruiker.

Details

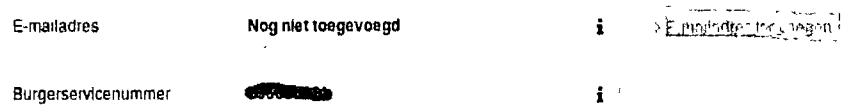
Bevindingen hertest release 5.5:

Het is nog steeds mogelijk om via de onderstaande methode een grote hoeveelheid e-mail naar een willekeurig e-mailadres te sturen:

Datum: Vandaag

noreply@a3.digid.nl	Bevestig uw e-mailadres ...	wo 22-11-2017 13:18	10 kB
noreply@a3.digid.nl	Bevestig uw e-mailadres ...	wo 22-11-2017 13:12	10 kB
noreply@a3.digid.nl	Bevestig uw e-mailadres ...	wo 22-11-2017 13:08	10 kB
noreply@a3.digid.nl	Uw DigiD e-mailadres is g...	wo 22-11-2017 13:07	11 kB
noreply@a3.digid.nl	Bevestig uw e-mailadres ...	wo 22-11-2017 13:07	10 kB
noreply@a3.digid.nl	Bevestig uw e-mailadres ...	wo 22-11-2017 13:07	10 kB
noreply@a3.digid.nl	Uw DigiD e-mailadres is g...	wo 22-11-2017 13:05	11 kB
noreply@a3.digid.nl	Uw DigiD e-mailadres is g...	wo 22-11-2017 13:02	11 kB
noreply@a3.digid.nl	Uw DigiD e-mailadres is g...	wo 22-11-2017 13:01	11 kB
noreply@a3.digid.nl	Uw DigiD e-mailadres is g...	wo 22-11-2017 13:00	11 kB

Originele bevinding:
Het is mogelijk om via de DigiD applicatie een continue stroom emails te versturen naar een willekeurig e-mailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.



Wanneer er een e-mailadres wordt opgegeven en op de volgende knop wordt knop wordt gedrukt wordt onderstaande request verzonden:

```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/email/nieuw
Content-Type: application/x-www-form-urlencoded
Content-Length: 201
Cookie: _session_id=b112cca5cd799b8a426083f6076822e8;
_persist='OWAYhwuOz3MxOfj+5aqg61TJU5Hb5ZGZXgyuOQ3RaXAbsSqHB1tJ4v3l0JX0
zjzclnixxqmpazpl55wKVrve0WRNs7ehRX0JfdWstO4=;
persist_cis=!t9BuYLOe7suKRQ18aojjirYC1E4er65r08mogQ18xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDE1Sy2x+03/+o=
Connection: close
Upgrade-Insecure-Requests: 1
utf8=%E2%9C%93&authenticity_token=GvI8j37pHUO9s%2BaufoIjm4Zjef%2Bn4blo
f6bsbV%2BVjwKwuVM7X7RcGZ8dWvSkb8BTsUIHqNpuLc5%2BM1ACFIReSg%3D%3D&email
%5Baddress%5D=[redacted]%40sogeti.com&commit=Volgende
```

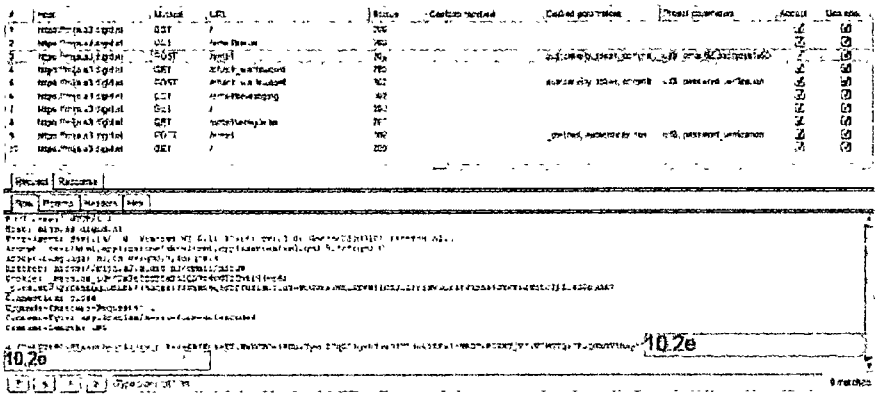
De reponse zorgt ervoor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatie code naar het email adres. Deze code moet binnen een bepaalde periode wordt opgegeven anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wilt versturen verschijnt de melding dat er al een code onderweg en na meer dan 10 minuten een nieuwe code kan worden aangevraagd. "Er is nog een e-mail onderweg naar u. Vanaf 13:41 uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen."
Echter is het mogelijk om het nog-niet geactiveerde e-mailadres te verwijderen van het account.

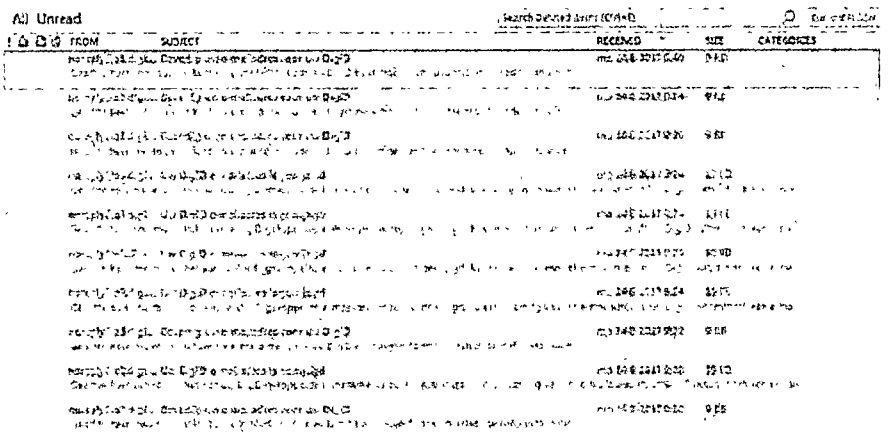
Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg

Is dat de gebruiker bovenstaande actie nog een keer kan uit voor hetzelfde of andere e-mailadressen.

Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.



Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:



Er bestaat het gevaar dat als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail, de mail wordt aangemerkt als spam of phising.

Hertest: Weak Block cipher – 64 bit TLS Sweet32				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
11	Nb	Midden	Laag	Midden

Betreffende hosts

balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving

De TLS-server maakt gebruik van algoritmes die intern 64-bit block ciphers gebruiken.

Bedreiging

64-bit block ciphers zijn kwetsbaar voor een zogenaamde birthday attack, waarbij de kans dat twee willekeurig gegenereerde waarden overeenkomen hoger dan 50% is. Dit wordt vervolgens gebruikt om een zogenaamde collision te forceren, waarmee achterhaald kan worden wat de originele waarde was van een versleuteld stukje data. Gegeven genoeg data (de ontdekkers hadden 785GB aan HTTPS-verkeer nodig) is het mogelijk om met een man-in-the-middle attack de waarde van bijvoorbeeld een versleutelde cookie te achterhalen.

Aanbeveling

Schakel de kwetsbare block ciphers uit binnen TLS.

Indien dit niet mogelijk is, zorg er dan voor dat geheime waarden (zoals een sessie token) met een hoge frequentie veranderen. Dit verzekert dat eventueel (gedeeltelijke) achterhaalde waarden niet meer valide zijn, en daarmee geen waarde meer hebben voor aanvallers.

Details

Bevindingen hertest release 5.5:

De bevinding is opgelost; de zwakke ciphers worden niet meer ondersteund.

Originele bevinding:

De server ondersteunt cipher suites die gebruik maken van 64-bit block ciphers:

```
List of 64-bit block cipher suites supported by the remote server :
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)
    TLSv1
          ECDHE-RSA-DES-CBC3-SHA Kx=ECDH Au=RSA Enc=3DES-CBC(168)
Mac=SHA1
          DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1
The fields above are :
  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Schakel ondersteuning voor deze cipher suites uit.

5 Bijlagen

5.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-arround' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdsrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

5.2 Aanpak

Tijdens de test wordt een groot aantal controles uitgevoerd. Hierbij wordt onder andere gebruikgemaakt van een checklist op basis van de *Web Application Hacker's Handbook* met de volgende onderdelen:

Logic	Client-side checks	Hidden fields
		Cookies - HTTP / Secure flag etc.
		Local privacy vulnerabilities
		Autocomplete forms
		Preset parameters
		ASP.net ViewState
		Field length limit
		Javascript Validation
		ClickJacking
		Disabled elements
		Java applets
		ActiveX
		Shockwave Flash
		Executables
	Logic Errors	Multistage
		Incomplete input
		Transaction logic
Authentication	Direct attacks	Password quality rules
		Username enumeration
		Password guessing

	Speciale functies	Account recovery
		Remember me functions
		Impersonation / Account hijacking
	Managing credentials	Username uniqueness
		Credential predictability
		Unsafe transmission
		Unsafe distribution
	Logic Errors	Autentication errors
		Fail-open conditions
		Multistage
Session management	Generation	Token logic/meaning
		Token predictability
	Handling	Insecure transmission of tokens
		Token disclosure in logs
		Mapping of tokens to sessions
		Concurrent sessions
		Session termination
		Fixation
		CSRF
		Caching
		Persistent cookies
		Fixed session ID
		Cookie Scope
Access	Segregation	Different accounts
		Insecure access control method
		Horizontal Privilige escalation
		Vertical Privilige escalation
	Controle	Anonymous
Input handling	Fuzzing	SQL injection
		Reflected XSS
		Stored XSS
		OS Command injection
		Path traversal
		Script Injection
		File upload fields
		File Inclusion
	Functie specifiek	SMTP injection
		Code flaws
		DOM-based attacks
		Frame injection
		HTTP Header Injection
		Arbitrary Redirection
		SOAP injection

		LDAP injection
		XPATH injection
Environment	Interfaces	Segregation in shared infrastructures
		Segregation between ASP-hosted apps
Server	Implementation	Default credentials
		Default content
		HTTP method
		Proxy
		Virtual hosting
	Software	Native software flaws
		Known vulnerabilities
	Configuration	Known bugs
		Services
		Disclosure
		OS
		Ports
		TLS encryption
		SSL Certificate
		TLS Implementation
		TLS version

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport

DigiD release 5.6

Kenmerk: 42103996 (Logius) 201801 (Sogeti)

Datum	6 februari 2018
Status	Definitief
Versie	1.1

Na oplossing van alle bevindingen in dit rapport is deze rubricering beëindigd.

Rubricering	derubricering
Vaststeller	10.2e
Functie	10.2e

Colofon

Kenmerk	42103996 (Logius) 201801 (Sogeti)
Versienummer	1.1
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
18-01-2018	0.1	Sogeti	Initiële versie
18-01-2018	0.2	Sogeti	Interne review
23-01-2018	0.3	Sogeti	Definitief concept
23-01-2018	0.4	Sogeti	Opmerkingen 10.2e
26-01-2018	0.9	Sogeti	Verwerken feedback Logius
05-02-2018	1.0	Sogeti	Definitieve versie
06-02-2018	1.1	Sogeti	Verduidelijking Managementsamenvatting

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

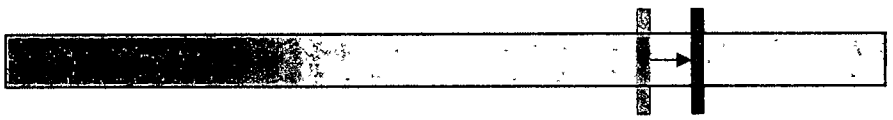
Managementsamenvatting

Inleiding

Het informatiebeveiligingsbeleid van Logius schrijft voor dat de producten van Logius periodiek worden getest op zwakheden door middel van een zogenaamde securitytest (ook wel penetratietest of pentest genoemd). De aanleiding tot deze securitytest was de aanstaande release 5.6 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.6, zoals getest op de A3-omgeving, voldoende is, maar dat er desondanks ruimte is voor verbetering. Er zijn in tegenstelling tot de vorige test geen bevindingen gedaan met een risiconiveau hoger dan Laag. Daarom is de algemene beoordeling van het beveiligingsniveau positief bijgesteld.



Onvoldoende Voldoende

Punten ter verbetering (nieuwe bevindingen):

- De sessiecookies van de gebruikers voldoen niet aan de PAP-eisen; bevinding 1.
  Aanbeveling: Pas de instelling van de cookies aan.
- Door een afbeelding toe te voegen aan een pagina kan een beheerder mogelijk verzoeken doen namens andere gebruikers; bevindingen 2 en 5.
  Aanbeveling: Controleer of de optie van het toevoegen van afbeeldingen noodzakelijk is. Controleer de locatie van afbeeldingen strenger.
- De instellingen van de beveiligde verbinding tussen de gebruiker en de server kunnen marginaal verbeterd worden; bevinding 3.
  Aanbeveling: Verander de instellingen.

Conclusie terugkerende bevindingen:

- De mogelijkheden om de integriteit van de pagina's te beschermen met instructies voor de browser worden niet of niet optimaal benut; bevindingen 4 en 5.
  Aanbeveling: Pas de instellingen op de server aan zodat de mogelijkheden wel benut worden.
- De servers hebben open poorten die niet direct door de applicatie gebruikt worden; bevinding 6.
  Aanbeveling: Onderzoek of de poorten nog nodig zijn of accepteer het minimale risico.

Aanvullingen Logius

Logius heeft kennisgenomen van de resultaten van de Securitytest R5.6 en deze besproken met Sogeti. De gerapporteerde bevindingen zijn beoordeeld op impact. Vastgesteld is dat de bevindingen geen gevolg zijn van de aanpassingen die zijn uitgevoerd als onderdeel van R5.6. Opvolging en verdere analyse van bevindingen en aanbevelingen vindt plaats vanuit het reguliere beheerproces. Het Security Testrapport en de ingeschatte impact van de bevindingen zal onderdeel uitmaken van het advies dat aan de stuurgroep DigiD zal worden gegeven ten aanzien van de vrijgave van DigiD R5.6.

1 Inleiding

1.1 Opdrachtformulering

De scope van deze securitytest was de gehele DigiD-applicatie, waarbij de nadruk lag op de gehele applicatie en aandacht werd gegeven aan de risico's door de wijzigingen en/of uitbreidingen die in release 5.6 worden doorgevoerd. Hierbij moet opgemerkt worden dat een aanzienlijk deel van de wijzigingen kleine inhoudelijke aanpassingen betreft.

Daarnaast is een belangrijk deel van de uitbreidingen ter voorbereiding van de toevoeging van DigiD Hoog in een toekomstige release. Deze toevoegingen worden in release 5.6 nog niet in productie genomen en zijn nog niet technisch geïmplementeerd. Derhalve kon de beveiliging van deze toevoegingen in deze securitytest nog niet onderzocht worden. Wel werd onderzocht of de ongebruikte onderdelen misbruikt konden worden. Tijdens het testtraject van de vorige releases van DigiD is gebleken dat er naast de externe tests ook de wens is om interne tests uit te laten voeren op de DigiD-omgeving. Echter verviel de interne test tijdens deze securitytest door het ontbreken van de later genoemde functionaliteiten.

Zie 'PVA securitytest – DigiD 5.6 v1.0.pdf', hoofdstuk 2, 'Opdrachtformulering'.

1.2 Aanpak

De testaanpak is geheel conform het Security Testplan uitgevoerd.

De securitytest heeft bestaan uit een vulnerability assessment met een diepgang greybox (hierbij krijgen de testers beschikking over documentatie en gebruikersrechten op het systeem, zodat het systeem met enige diepgang kan worden onderzocht) en betreft een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A3-omgeving.

De aandachtsgebieden met betrekking tot DigiD Hoog en de statuscontroler waren buiten scope voor deze securitytest omdat ze in release 5.6 nog niet functioneel zijn en de beveiliging ervan derhalve niet getest kon worden. Tijdens de securitytest is ook gelet worden op eventuele regressie dan wel ongeautoriseerde of onbedoelde veranderingen.

Sommige bevindingen uit de voorgaande test zijn nog niet opgelost. Deze terugkerende bevindingen worden besproken in hoofdstuk 4. Daarnaast heeft Logius een lijst opgesteld van bevindingen uit eerdere tests die om businessredenen (nog) niet opgelost zijn. Deze bevindingen worden gezien als geaccepteerde risico's. Tijdens de securitytest moest gecontroleerd worden of deze bevindingen nog steeds aanwezig waren. De resultaten van deze controle zijn in een apart hoofdstuk van het securitytestrapport (hoofdstuk 5) opgenomen.

Zie 'PVA securitytest – DigiD 5.6 v1.0.pdf', hoofdstuk 4, 'Aanpak' en bijlage 5.1, 'Aanpak securitytest'.

2 Resultaten

2.1 Cumulatief overzicht

Hieronder staat een totaaloverzicht van de bevindingen in dit rapport. Zie paragraaf 7.1 voor een toelichting op de risicoclassificatie.

In Tabel 1 zijn zowel nieuwe bevindingen (zie hoofdstuk 3) opgenomen als terugkerende bevindingen die nog niet opgelost zijn (zie hoofdstuk 4). NB de bevindingen uit eerdere tests die door Logius als geaccepteerde risico's zijn aangemerkt worden in Tabel 2 vermeld.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Tabel 1: Nieuwe en terugkerende bevindingen

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Client-side controls				1 | 1	1	3
Logica						
Authenticatie						
Sessiemanagement						
Toegang						
Invoerafhandeling				1		1
Omgeving						
Servers					1 | 1	2
Totaal				**3**	**3**	**6**

In Tabel 2 worden de door Logius geaccepteerde risico's weergegeven. Deze bevindingen worden in hoofdstuk 5 besproken.

Tabel 2: Geaccepteerde risico's

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Totaal
Client-side controls						
Logica						
Authenticatie						
Sessiemanagement			1			1
Toegang						
Invoerafhandeling			1			1
Omgeving						
Servers				1		1
Totaal			**2**	**1**		**3**

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Buiten scope voor deze test.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope voor deze test.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.01	**Operationeel beleid voor webapplicaties**

[1] Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Buiten scope voor deze test.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Buiten scope voor deze test.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Geen bevindingen.	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Bevindingen 2, 4 en 5	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Bevinding 3	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Geen bevindingen.	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Geen bevindingen.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Buiten scope voor deze test.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Geen bevindingen.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Geen bevindingen.	

U/PW.04	Isolatie van processen/bestanden
Beperk de impact bij misbruik van processen.	
Oordeel	
Geen bevindingen.	
U/PW.05	Toegang tot beheermechanismen
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Buiten scope voor deze test.	
U/PW.06	Platform-netwerkkoppeling
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Buiten scope voor deze test.	
U/PW.07	Hardening van platformen
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Bevindingen 1 en 6	
U/PW.08	Platform- en webserverarchitectuur
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/NW.01	Operationeel beleid voor netwerken
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting	
U/NW.02	Beschikbaarheid van netwerken
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Buiten scope voor deze test.	
U/NW.03	Netwerkzonering
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Buiten scope voor deze test.	
U/NW.04	Protectie- en detectiefunctie
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Buiten scope voor deze test.	
U/NW.05	Beheer- en productieomgeving
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Buiten scope voor deze test.	
U/NW.06	Hardening van netwerken
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Bevinding 6	
U/NW.07	Netwerktoegang tot webapplicatie
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	

Geen bevindingen.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Buiten scope voor deze test.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Buiten scope voor deze test.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Buiten scope voor deze test.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Buiten scope voor deze test.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Deze test is onderdeel van het voldoen aan deze richtlijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Buiten scope voor deze test.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Buiten scope voor deze test.	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Buiten scope voor deze test.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Buiten scope voor deze test.	
C.09	**Patchmanagement**

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Buiten scope voor deze test.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope voor deze test.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Geen bevindingen.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

Cookie-domein te breed				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
1	Nnb	Laag	Zeer Laag	Laag

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Een cookie wordt standaard gebonden aan het (sub)domein dat de cookie heeft aangemaakt. Via de *Domain* parameter van de *Set-Cookie* header kan de cookie echter ook voor een specifiek domein en al zijn subdomeinen beschikbaar gemaakt worden. Een applicatie kan alleen cookies aanmaken voor zijn eigen domein en bovenliggende domeinen, met uitzondering van top-level domeinen zoals .com of .nl.

Bedreiging
Wanneer een cookie wordt ingesteld met de *Domain* parameter (bijvoorbeeld: `Domain=.example.com`) stuurt de browser de cookie ook naar alle pagina's die onder subdomeinen van dat domein vallen (bijvoorbeeld: www.example.com en shop.example.com). Hierdoor kan het voorkomen dat de cookie van een applicatie ook verstuurd wordt naar andere applicaties die onder hetzelfde hoofddomein vallen. Dit zou de werking van die applicaties kunnen verstoren. Daarnaast zou het kunnen leiden tot het uitlekken van de cookie als de andere applicaties of hun infrastructuur kwetsbaarheden bevatten.

Aanbeveling
Bij het aanmaken van belangrijke cookies moeten de *Domain* en *Path* parameters altijd zo specifiek mogelijk ingesteld worden. Hierdoor wordt de kans dat de cookie buiten de applicatie terechtkomt tot een minimum beperkt. In sommige gevallen kan dit betekenen dat de *Domain* parameter beter weggelaten kan worden. Bijvoorbeeld: de sessiecookie

voor https://shops.example.com/flowers zou als volgt aangemaakt kunnen worden: *Set-Cookie: session=[SESSION_TOKEN]; Path=/flowers/; Secure; HttpOnly*. Merk hierbij op dat de *Domain* parameter bewust is weggelaten om ervoor de zorgen dat de browser de cookie alleen naar pagina's binnen het domein shops.example.com verstuurt en niet naar pagina's binnen subdomeinen van dat domein. Zie voor meer informatie RFC6265 (http://tools.ietf.org/html/rfc6265), met name secties 5.2.3 en 5.3.6.

Details
Wanneer een gebruiker inlogt stelt de server een sessiecookie in voor het domein *.digid.nl*. Hierdoor zal de browser van de gebruiker de cookie meesturen met verzoeken naar *alle* subdomeinen van digid.nl. De PAP-eisen[2] van Logius stellen dat cookies subdomein-specifiek ingesteld moeten worden. ACC2.5.2: "Cookies zijn secure en httponly en **subdomein specifiek**."

Request:

```
POST /inloggen HTTP/1.1
Host: a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://a3.digid.nl/inloggen
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 311

utf8=%E2%9C%93&authenticity_token=PYMaBrreJlLPEeUnHr9F7kZGP4mh8hNZdevi
4c7UPvUZKKcLUCUsC8CslVkczvfIPqvpx2xY%2B6wRavrAhsMTlw%3D%3D&authenticat
ion%5Btype_account%5D=basis&authentication%5Bdigid_username%5D=u_XXX&a
uthentication%5Bwachtwoord%5D=Pw_XXX&authentication%5Bremember_login%5
D=0&commit=Inloggen
```

Response headers:

```
HTTP/1.1 302 Found
Date: Thu, 18 Jan 2018 09:51:07 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 944d8ee7-73a8-44b7-8c92-3a10efc01a02
X-Runtime: 0.149709
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=d1b343c0c1e8c4ce8919a1f1f5624cc0;Secure;
domain=.digid.nl; path=/; HttpOnly
Location: https://a3.digid.nl/saml/idp/redirect_with_artifact
Status: 302 Found
Content-Type: text/html; charset=utf-8
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
Content-Length: 117
```

[2] *Zie 'Logius-DGD-PAP-v2.3.xlsx'*

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

Onvoldoende invoervalidatie Daring Fireball markup				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
2	Nnb	Laag	Zeer Laag	Laag

Betreffende hosts

.digidbeheer-a3.digid.nl

Omschrijving

De website maakt gebruik van Daring Fireball markup. Hierbij worden de speciale combinaties van deze markup door de server onvoldoende gevalideerd.

Bedreiging

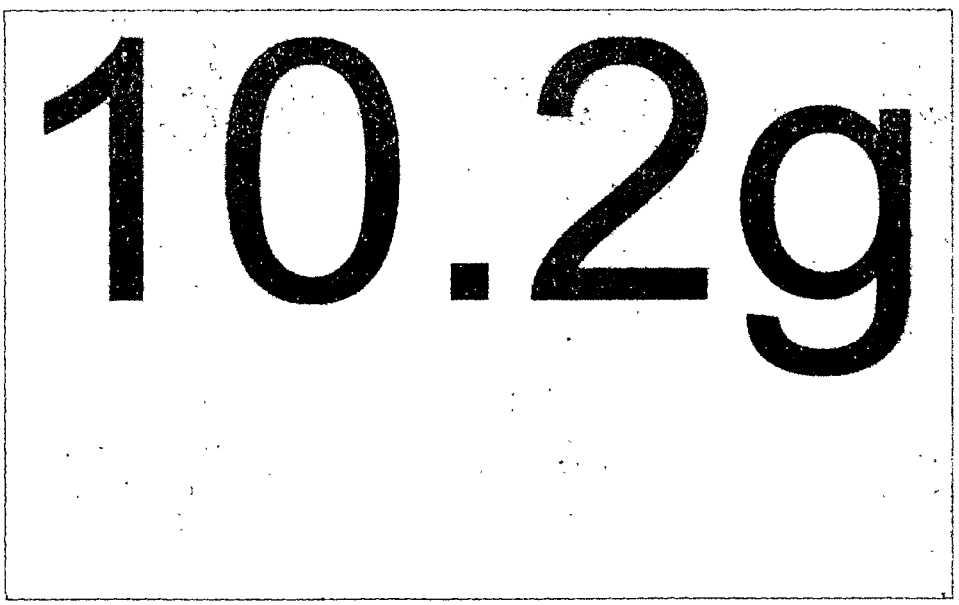
Het is mogelijk om via deze opmaaktaal een afbeelding toe te voegen aan een pagina. Dit kan ook een afbeelding zijn op een ander domein dat *.digid.nl. Ook kan er een URL gebruikt worden die helemaal geen afbeelding is. Wanneer een gebruiker de pagina vervolgens bezoekt wordt deze URL door de browser aangeroepen. Dit kan bijvoorbeeld gebruikt worden om een CSRF-kwetsbaarheid op een andere website te misbruiken.

Aanbeveling

Zorg ervoor dat alle invoer door de server wordt gecontroleerd en gevalideerd voordat deze wordt verwerkt, opgeslagen of getoond. Controleer of het nodig is dat er afbeeldingen kunnen worden ingeladen van andere domeinen dan het DigID-domein.

Details

In het beheerportaal is het mogelijk om berichten te schrijven en te bewerken:



In het voorbeeld hierboven is te zien dat er een afbeelding wordt toegevoegd met als URL 10.2g Zodra een

gebruiker het bericht bezoekt stuurt de browser een verzoek naar die URL om de afbeelding te kunnen tonen. Hieronder is te zien dat de machine met IP-adres [redacted] een verzoek binnenkrijgt op poort [redacted]:

```
root@kali:/# nc -nlvp [redacted]
listening on [any] [redacted] ...
connect to [redacted] from (UNKNOWN) [redacted]
GET / HTTP/1.1
Host: 10.234.171.16:1234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
```

Het is belangrijk om op te merken dat het momenteel alleen binnen het beheerportaal mogelijk is om op deze manier verzoeken naar andere domeinen te doen; binnen dit portaal wordt de CSP-header[3] niet gebruikt waardoor het mogelijk is afbeeldingen van andere domeinen in te laden. In de DigiD-applicatie voor burgers wordt de CSP-header wel gebruikt, waardoor moderne browsers het inladen van afbeeldingen van andere domeinen zullen tegenhouden.
Een 'afbeelding' die een verzoek uitvoert *binnen* het DigiD-domein zal ook werken binnen de DigiD-applicatie voor burgers; Hierdoor kan een beheerder eventueel verzoeken binnen DigiD uitvoeren namens burgers.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

SSL/TLS downgrade				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
3	Nnb	Zeer laag	Zeer laag	Zeer laag

Betreffende hosts

a3.digid.nl
mijn.a3.digid.nl
was-a3.digid.nl
digidbeheer.a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving

[3] *Content Security Policy, zie ook https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP en bevindingen 4 en 5 in dit rapport.*

De applicatie maakt gebruik van een SSL/TLS tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.

openssl s_client -connect host:443 -state -fallback_scsv -tls1_1

Bedreiging

Als een aanvaller kan optreden als 'man in the middle' kan een aanvaller de handshake veranderen. Als op deze wijze een SSL/TLS tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling

Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 12). Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details

De server maakt geen gebruik van TLS Fallback SCSV.

```
root@kali:~/# sslscan 144.43.243.145
Version: 1.11.10-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Testing SSL server 144.43.243.145 on port 443 using SNI name
144.43.243.145

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
```

4 Terugkerende bevindingen

In dit hoofdstuk worden bevindingen uit een test op een eerdere release van DigiD opnieuw behandeld. Bevindingen in dit hoofdstuk zijn reeds bekend bij Logius, maar (nog) niet als geaccepteerd risico aangemerkt of opgelost.

Content-Security-Policy header implementatiefout				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
4	Nb	Laag	Zeer laag	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaadt die niet als vertrouwd is aangegeven. De policy welke door de server verstuurd wordt is niet correct/veilig.

Bedreiging
Wanneer de CSP header niet correct is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwen code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP policy zo strak mogelijk, waarbij onveilig gedrag niet toegelaten wordt. Bouw vanuit hier de policy uit met alleen die functionaliteit welke nodig is. Gebruik hierbij voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Details
Bevindingen release 5.6:
De server gebruikt nog steeds niet de meest veilige opties voor de Content Security Policy-header.

Originele bevinding:
De server gebruikt niet de meest veilige opties voor de Content Security Policy-header.

Request:

```
GET / HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
```

```
Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _session_id=fae19c44d5192bf0f3551e27546522b9;
_persist='U7EvyshiVdfK8cUZzh+/BjbEK230wQjbW4A+14jHDGj9P5rosiyHT0PHj4JT
pBVVs1HcsQ6Re26hZga5BNoPUv4dDnh9Cwj1yOdDhW0=
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Mon, 15 Jan 2018 09:53:57 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 246a28eb-08b4-4513-860e-89bccb5e16dc
X-Runtime: 0.060513
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Er worden potentieel onveilige inline-elementen en het gebruik van de *eval*-functie toegestaan.

Content-Security-Policy (CSP) header ontbreekt				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
5	Nb	Zeer laag	Zeer laag	Laag

Betreffende hosts
balie-a3.digid.nl
cis-a3.digid.nl
digidbeheer-a3.digid.nl
rda-a3.digid.nl
was-a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
Een voorbeeld waarbij geen externe scripts worden geladen en 'inline-scripts' niet worden uitgevoerd:
Content-Security-Policy: default-src self

Details
Bevindingen release 5.6:
Een deel van de servers maakt nog steeds geen gebruik van de Content Security Policy-header.

Originele bevinding:
De server stuurt de CSP header niet mee. Hierdoor wordt niet optimaal gebruik gemaakt van beschermende maatregelen in de browser. Het is aanbevolen om de server zo te configureren dat deze header wel wordt meegestuurd.
Voorbeeldrequest:

```
GET / HTTP/1.1
Host: was-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _session_id=---verwijderd---; _persist=---verwijderd---;
persist_cis=---verwijderd---
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 404 Not Found
Date: Wed, 17 Jan 2018 10.06:03 GMT
X-Request-Id: 06c9be68-a52f-41ce-baf6-e71f5140eb53
X-Runtime: 0.002673
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
Set-Cookie: _persist=---verwijderd---;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Open poorten				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
6	Nb	Zeer laag	Zeer laag	Zeer laag

Betreffende hosts
mijn.a3.digid.nl
a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl

balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl

Omschrijving
Tijdens het onderzoek is er gekeken welke netwerkpoorten er op de systemen geopend zijn en welke services er (waarschijnlijk) op die poorten luisteren.

Bedreiging
Een open poort is zeker niet altijd een bedreiging; het is immers noodzakelijk om poorten open te zetten als systemen met elkaar moeten communiceren. Als er echter poorten onbedoeld of onnodig openstaan heeft een aanvaller meer mogelijkheden om een systeem of haar gebruikers aan te vallen.

Aanbeveling
Controleer de lijst met gevonden open poorten om te zien of er poorten open staan die gesloten kunnen worden.

Details
Bevindingen release 5.6:
Poort 80 staat nog steeds open.

Originele bevinding:
Voor de domeinnaam digi.nl staat naast poort 443 ook poort 80 open. Het is aanbevolen om enkel poort 443 open te zetten, want de dienst moet enkel via HTTPS worden aangeboden. Daarnaast tonen zoekmachines vaak standaard de HTTPS-pagina. Ook kan er gebruikgemaakt worden van HSTS-preloading[4]. Voor een publieke dienst als DigiD is het echter noodzakelijk om voor een zo groot mogelijke groep burgers toegankelijk te zijn. Die eis, in combinatie met het minimale risico van de bevinding, verantwoordt de keuze om poort 80 open te houden om gebruikers automatisch door te kunnen sturen naar poort 443. Bij een volgende test kan deze bevinding eventueel op de lijst met geaccepteerde risico's geplaatst worden.

[4] *https://hstspreload.org/*

5 Geaccepteerde risico's

Logius heeft een aantal bevindingen uit eerdere tests aangemerkt als geaccepteerde risico's. Die bevindingen worden in dit hoofdstuk besproken.

Gelijktijdige sessies				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
7	Nb	Midden	Midden	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging

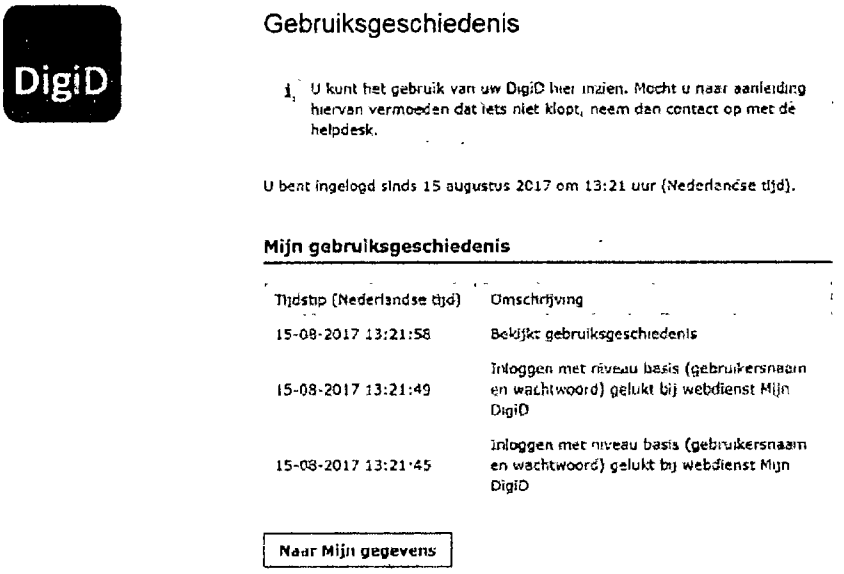
Wanneer er meerdere gelijktijdige sessies voor dezelfde gebruiker kunnen bestaan betekent dit dat oude sessies niet automatisch worden afgesloten. Dit geeft een aanvaller de mogelijkheid om oude sessies te misbruiken, ook als de gebruiker al een nieuwe sessie heeft opgestart.

Aanbeveling

Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Dit verkleint de kans dat een aanvaller een oude sessie van een gebruiker misbruikt. Daarnaast wordt een gebruiker automatisch gewaarschuwd als een aanvaller een sessie namens hem start. Bij vermoedens van misbruik kan een gebruiker een eventuele oude sessie sluiten door nogmaals in te loggen.

Details

Het is mogelijk om op de Mijn DigiD-omgeving meerdere actieve sessies per DigiD-account te hebben. Dit houdt in dat er op meerdere apparaten wordt ingelogd met één DigiD account. De gebruikersgeschiedenis toont de inlogacties:



DigiD

Gebruiksgeschiedenis

U kunt het gebruik van uw DigiD hier inzien. Mocht u naar aanleiding hiervan vermoeden dat iets niet klopt, neem dan contact op met de helpdesk.

U bent ingelogd sinds 15 augustus 2017 om 13:21 uur (Nederlandse tijd).

Mijn gebruiksgeschiedenis

Tijdstip (Nederlandse tijd)	Omschrijving
15-08-2017 13:21:58	Bekijkt gebruiksgeschiedenis
15-08-2017 13:21:49	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD
15-08-2017 13:21:45	Inloggen met niveau basis (gebruikersnaam en wachtwoord) gelukt bij webdienst Mijn DigiD

Naar Mijn gegevens

Het is ook mogelijk om met beide sessies acties uit te voeren op de Mijn DigiD-omgeving. Ga na of het nodig is voor een gebruiker om twee gelijktijdige sessies toe te staan.

Denial-of-Service – Email versturen				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
8	Nb	Midden	Laag	Midden

Betreffende hosts

mijn.a3.digid.nl

Omschrijving

Het systeem is zo te manipuleren dat de server een grote hoeveelheid emails naar een gebruiker stuurt.

Bedreiging

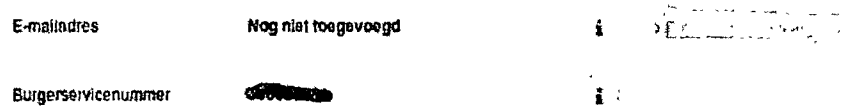
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling

Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een email is gestuurd naar de gebruiker.

Details

Het is mogelijk om via de DigiD applicatie een continue stroom emails te versturen naar een willekeurig e-mailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.



E-mailadres Nog niet toegevoegd

Burgerservicenummer [redacted]

Wanneer er een e-mailadres wordt opgegeven en op de volgende knop wordt knop wordt gedrukt wordt onderstaande request verzonden:

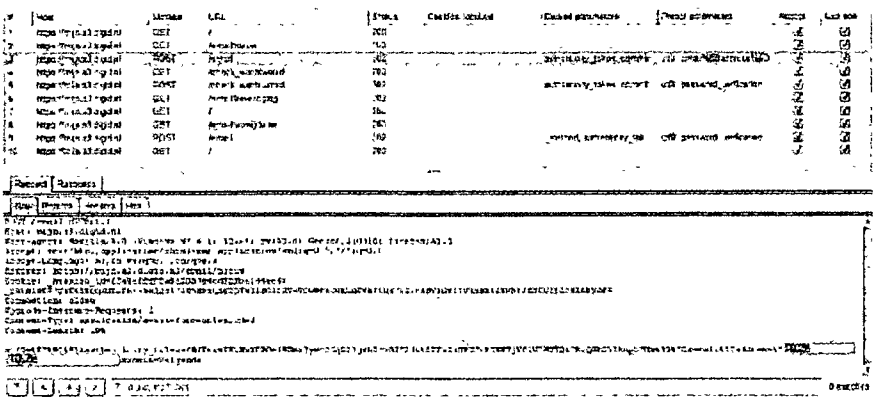
```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/email/nieuw
Content-Type: application/x-www-form-urlencoded
Content-Length: 201
Cookie: _session_id=b112cca5cd799b8a426083f6076822e8;
_persist=!OWAYhwuOz3MxOfj+5aqg61TJU5Hb5ZGZXgyuOQ3RaXAbsSqHBitJ4v310JX0
zjzc1nixxqmpazpl55wKVrve0WRNs7ehRX0JfdWstO4=;
persist_cis=!t9BuYLOe7suKRQ18aojjirYC1E4er65r08mogQl8xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDEiSy2x+03/+o=
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=GvI8j37pHUO9s%2BaufoIjm4Zjef%2Bn4blo
f6bsbV%2BVjwKwuVM7X7RcGZ8dWvSkb8BTsUIHqNpuLc5%2BM1ACFIReSg%3D%3D&email
%5Baddress%5D=[redacted]40sogeti.com&commit=Volgende
```

De reponse zorgt ervoor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

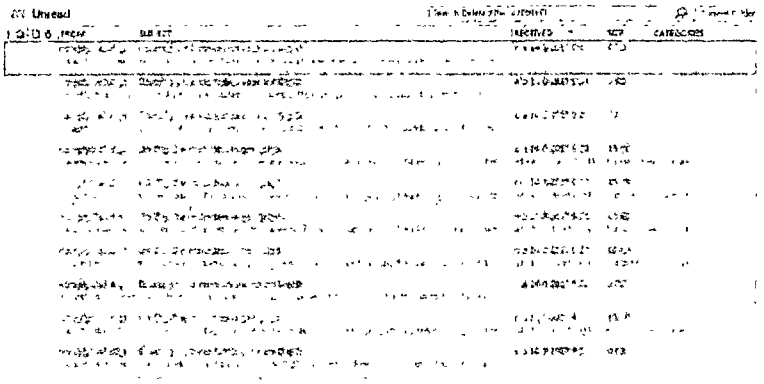
Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatie code naar het email adres. Deze code moet binnen een bepaalde periode wordt opgegeven anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wilt versturen verschijnt de melding dat er al een code onderweg en na meer dan 10 minuten een nieuwe code kan worden aangevraagd. "Er is nog een e-mail onderweg naar u. Vanaf 13:41 uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen." Echter is het mogelijk om het nog-niet geactiveerde e-mailadres te verwijderen van het account.

Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg is dat de gebruiker bovenstaande actie nog een keer kan uit voor hetzelfde of andere e-mailadressen.

Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.



Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:



Er bestaat het gevaar dat als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail, de mail wordt aangemerkt als spam of phising.

BEAST (Browser Exploit Against SSL/TLS)				
ID	**Mantis nr. Clientele nr.**	**Risico op misbruik**	**Kans op misbruik**	**Impact op misbruik**
9	Nb	Laag	Zeer laag	Midden

Betreffende hosts

was-a3.digid.nl
digibeheer-a3.digid.nl
mijn.a3.digid.nl

Omschrijving

De SSL/TLS implementatie op de server maakt het mogelijk om een voorspelbare ciphertext te genereren uit plaintext.

Bedreiging

In cryptografie is Cipher Block Chaining (CBC) een veelgebruikte methode om de voorspelbaarheid van encrypted data te verminderen. Het doel is om te voorkomen dat dezelfde data (plaintext) tot dezelfde encrypted data (ciphertext) leidt gedurende het encryptieproces. Hiervoor wordt een zogenaamde initialization vector (IV) gebruikt, die uniek is voor elk bericht in elke sessie. CBC encrypt ieder blok data en gebruikt deze data ook als input voor de encryptie van het volgende blok data: het "chainen". Dit doel wordt ondermijnd door oudere implementaties van SSL/TLS, waardoor in sommige situaties de IV voorspelbaar is, dus ook de ciphertext. Dit op zijn beurt kan gebruikt worden om (delen van) de plaintext data terug te berekenen vanuit de encrypted data.

Aanbeveling

Upgrade naar TLSv1.2. Een andere, niet aan te raden, oplossing is het gebruiken van encryptie zonder CBC.

Details

De verbinding tussen de server en de gebruiker is mogelijk kwetsbaar voor BEAST omdat er CBC-ciphers ondersteund worden:

```
Negotiated cipher suite: ECDHE-RSA-AES256-
SHA|TLSv1|Kx=ECDH|Au=RSA|Enc=AES-CBC(256)|Mac=SHA1
```

6 PAP-eisen

Hieronder wordt van de relevante eisen uit het document Logius-DGD-PAP-v2.3.xlsx aangegeven of de omgeving eraan voldoet of niet, voor zover dat op basis van de test te zeggen is.

#	Categorie	Criterium	Omschrijving
ACC2.1.2	Beveiliging	Lekken van informatie	DigiD mag geen (persoons)gegevens of informatie prijsgeven anders dan de eigen gegevens of informatie die nodig zijn voor de werking van het systeem en waar de gebruiker expliciet voor geautoriseerd is. Wanneer het niet tegen gehouden kan worden zal dit gelimiteerd moeten zijn en geaccepteerd worden door Logius. Daarnaast zal de reactie die het systeem geeft nooit meer informatie tonen dan de burger al weet. Dit betreft bijvoorbeeld informatie over het wel of niet voorkomen van informatie in de applicatie, informatie over de werking van het systeem, informatie over versienummeringen en gegevens over een andere persoon.
Geen bevindingen			
ACC2.2.3	Beveiliging	Zwakheden	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)
Geen bevindingen			
ACC2.3.1	Beveiliging	Persoonsgegevens	De privacy gevoelige (tot natuurlijke personen herleidbare) gegevens moeten versleuteld worden Dit geldt voor: 1) Data in transport: zodra de gegevens de systeemgrenzen het fysieke afgeschermde DigiD ruimte in het datacentrum verlaat/overschrijden. 2) Data at rest: De disk volumes waarop persoonsgegevens opgeslagen worden zijn versleuteld en de swap partities ook. Persoonsgegevens worden alleen verwerkt of opgeslagen op basis van als hiervoor een duidelijk, voorafgaand bepaald en uitdrukkelijk omschreven vastgesteld doel. Doel, streefwaarde en toleranties Als privacy gevoelige gegevens
Bevinding: 3			
ACC2.5.1	Beveiliging	DNSSEC	De records van het DigiD domein zijn ondertekend en voldoen aan de DNSSEC standaard.
Geen bevindingen			

ACC2.5.2	Beveiliging	Cookies	Cookies zijn veilig, betekenisloos, uniek en tijdelijk
Bevinding: 1			
ACC2.5.4	Beveiliging	Ingetrokken certificaten	DigiD controleert certificaten van anderen op geldigheid, herleidbaarheid tot de vigerende root (huidig: 'Staat der Nederlanden Root CA G2)' en of het certificaat niet ingetrokken is
Geen bevindingen			
ACC4.1.1	Connectiviteit	IPv4 en IPv6	DigiD is bereikbaar en bruikbaar via zowel het internet protocol versie vier (IPv4) als het internet protocol versie zes (IPv6).
Buiten scope			
ACC5.2.1	Continuïteit	Controle berichten	Het verzenden van berichten aan DigiD die niet voldoen aan de specificaties, leidt tot een foutmelding richting de verzender van het bericht. Het systeem zal verder geen hinder ondervinden van deze berichten die niet aan de specificaties voldoen. Tevens moet er een signalering naar de beheerder gaan (dit is een vorm van beveiligingsincident) en moeten er operationele procedures zijn ingericht om contact op te nemen met ketenpartners om oorzaak op te sporen. Het is onderdeel van de systeemtest van de leverancier om bewust foutieve berichten naar een koppelvlak te sturen en de juiste afhandeling te controleren.
Geen bevindingen			
ACC5.2.2	Continuïteit	Degradatiemogelijkheden	Bij verstoring van de dienstverlening over een enkel koppelvlak is de dienstverlening van de rest van het systeem gewaarborgd. Voorbeeld 1: Bij het uitvallen van de verbindingen met de GBA-V, blijft het mogelijk om te authenticeren via DigiD. Voorbeeld 2: Als de koppeling met de SMS gateway uitvalt, of het om een andere reden niet mogelijk is om sms'jes te versturen, dient aanvragen/activeren/authenticatie op basis van alleen naam/wachtwoord te blijven functioneren.
Buiten scope			
ACC2.2.3	Beveiliging	Zwakheden	DigiD bevat geen veelvoorkomende zwakheden zoals benoemd door OWASP in de category Vulnerability. (https://www.owasp.org/index.php/Category:Vulnerability)
Geen bevindingen			

7 Bijlagen

7.1 Risicoclassificatie

Risico	Toelichting risicoclassificatie
Zeer hoog	In productie zou dit beoordeeld worden als een calamiteit. De bevinding is een 'showstopper'. Hierbij kan worden gedacht aan situaties dat er geen gebruik van kan worden gemaakt, of situaties die een onaanvaardbaar beveiligingsrisico inhouden. Er is geen 'work-around' voorhanden.
Hoog	In productie: een prio 1 incident. Het productieproces wordt ernstig benadeeld. Alternatieven zijn kostbaar, zeer tijdrovend of op korte termijn niet voorhanden.
Midden	In productie: een prio 2 incident. Een alternatief is voorhanden. De bevinding is te verwachten tijdens een testperiode maar de bevinding zou niet voor mogen komen in productie.
Laag	In productie: een prio 3 incident. Een vervelende, irritante situatie voor het productieproces maar er valt mee te leven.
Zeer laag	In productie zou dit niet als incident worden gekenmerkt. Verfraaiing, verduidelijkingen en verbeteringen die geen wezenlijke verandering van de voorziening inhouden.

7.1 Aanpak

Tijdens de test wordt een groot aantal controles uitgevoerd. Hierbij wordt onder andere gebruikgemaakt van een checklist op basis van de *Web Application Hacker's Handbook* met de volgende onderdelen:

Logic	Client-side checks	Hidden fields
		Cookies - HTTP / Secure flag etc.
		Local privacy vulnerabilities
		Autocomplete forms
		Preset parameters
		ASP.net ViewState
		Field length limit
		Javascript Validation
		ClickJacking
		Disabled elements
		Java applets
		ActiveX
		Shockwave Flash
		Executables
	Logic Errors	Multistage
		Incomplete input
		Transaction logic
Authentication	Direct attacks	Password quality rules
		Username enumeration
		Password guessing

	Speciale functies	Account recovery
		Remember me functions
		Impersonation / Account hijacking
	Managing credentials	Username uniqueness
		Credential predictability
		Unsafe transmission
		Unsafe distribution
	Logic Errors	Autentication errors
		Fail-open conditions
		Multistage
Session management	Generation	Token logic/meaning
		Token predictability
	Handling	Insecure transmission of tokens
		Token disclosure in logs
		Mapping of tokens to sessions
		Concurrent sessions
		Session termination
		Fixation
		CSRF
		Caching
		Persistent cookies
		Fixed session ID
		Cookie Scope
Access	Segregation	Different accounts
		Insecure access control method
		Horizontal Privilige escalation
		Vertical Privilige escalation
	Controle	Anonymous
Input handling	Fuzzing	SQL injection
		Reflected XSS
		Stored XSS
		OS Command injection
		Path traversal
		Script Injection
		File upload fields
		File Inclusion
	Functie specifiek	SMTP injection
		Code flaws
		DOM-based attacks
		Frame injection
		HTTP Header Injection
		Arbitrary Redirection
		SOAP injection

		LDAP injection
		XPATH injection
Environment	Interfaces	Segregation in shared infrastructures
		Segregation between ASP-hosted apps
Server	Implementation	Default credentials
		Default content
		HTTP method
		Proxy
		Virtual hosting
	Software	Native software flaws
		Known vulnerabilities
	Configuration	Known bugs
		Services
		Disclosure
		OS
		Ports
		TLS encryption
		SSL Certificate
		TLS Implementation
		TLS version

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Security Testrapport
DigiD release 5.7

Kenmerk: 500905

Datum	07-05-2018
Status	Definitief
Versie	1.0

Na oplossen bevindingen is deze rubricering beëindigd.

Rubricering	derubricering
Vaststeller	10.2e
Functie	Vertegenwoordiger opdrachtgever

Colofon

Kenmerk	**500905**
Versienummer	1.0
Contactpersoon	10.2e
Organisatie	Logius Postbus 96810 2509 JE Den Haag servicecentrum@logius.nl

Documentbeheer

Datum	Versie	Auteur	Opmerkingen
23-04-2018	0.1	Sogeti	Initiële versie
23-04-2018	0.2	Sogeti	Interne review
24-04-2018	0.3	Sogeti	Reviewcommentaar Logius verwerkt
01-05-2018	0.4	Sogeti	Reviewcommentaar Logius verwerkt, aanvulling Logius toegevoegd aan rapportage
07-05-2018	1.0	Sogeti	Reviewcommentaar Logius verwerkt, aanvulling Logius toegevoegd aan rapportage

Verzendlijst

Naam	Rol	Functie	Bedrijf
10.2e			

Inhoud

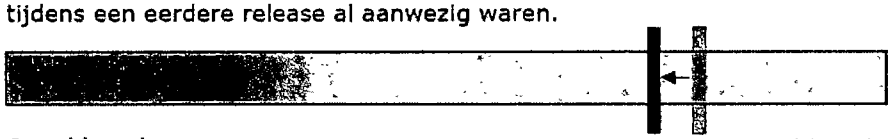
Managementsamenvatting

Inleiding

Het informatiebeveiligingsbeleid van Logius schrijft voor dat de producten van Logius periodiek worden getest op zwakheden door middel van een zogenaamde securitytest (ook wel penetratietest of pentest genoemd). De aanleiding tot deze securitytest was de aanstaande release 5.7 van DigiD. De test was bedoeld om het beveiligingsniveau van deze release van DigiD vast te stellen.

Conclusies en aanbevelingen

Op basis van de test kan gesteld worden dat het beveiligingsniveau van de DigiD-applicatie, in versie R5.7, zoals getest op de A3-omgeving voldoende is. Ondanks dat een aantal bevindingen die op de nieuwe eID-server zijn geïntroduceerd nog tijdens de testperiode zijn opgelost, heeft een aantal nieuwe bevindingen op de reeds bestaande servers het beveiligingsniveau negatief beïnvloed. Deze nieuwe bevindingen zijn door Sogeti niet direct te koppelen aan veranderingen die er tijdens release 5.7 zijn gedaan op de servers en de kans bestaat ook dat deze bevindingen tijdens een eerdere release al aanwezig waren.



Onvoldoende Voldoende

Punten ter verbetering (nieuwe bevindingen):

- Een aantal headers die de gebruiker beschermen tijdens het gebruiken van de applicatie worden door de server niet standaard meegestuurd. Bevinding 5.7.3 (laag), Bevinding 5.7.4 (laag).
  Aanbeveling: Stuur deze headers mee vanuit de server om de gebruiker beter te beschermen tijdens het gebruik van de applicatie.
- De mogelijkheid bestaat dat een aanvaller bepaalde waardes in meegestuurde headers kan veranderen, zodat er cookies voor het verkeerde domein worden aangeleverd door de server. Bevinding 5.7.6 (laag).
  Aanbeveling: Zorg ervoor dat de invoer van een gebruiker nooit zonder controle gereflecteerd wordt als de server de invoer terugstuurt.

Punten ter verbetering (terugkerende bevindingen):

- Het oplossen van drie eerder gedane bevindingen maakte geen onderdeel uit van de scope van R5.7. Deze drie bevindingen zijn op verzoek van Logius specifiek opnieuw getest, en derhalve als terugkerend gerapporteerd.

Algemene opmerkingen:

- Tijdens de test zijn in totaal 20 bevindingen gedaan. Daarvan waren er 9 nieuw, 3 terugkerend en 8 eerder geaccepteerd door Logius. Van de 9 nieuwe bevindingen zijn er tijdens de testperiode

6 direct opgelost. Een van deze opgeloste bevindingen betrof een hoog risico.

Aanvullingen Logius

Logius heeft kennisgenomen van de resultaten van de Securitytest R5.7. De gerapporteerde bevindingen zijn beoordeeld op impact. Ten aanzien van 6 bevindingen is tijdens de testperiode een oplossing doorgevoerd. Van de openstaande nieuwe bevindingen (5.7.3, 5.7.4, 5.7.6) is vastgesteld dat doorvoeren van een oplossing niet blokkerend is voor verdere uitrol van R5.7. Opvolging en verdere analyse van deze bevindingen en aanbevelingen vindt plaats vanuit het reguliere beheerproces. Het Security Testrapport en de ingeschatte impact van de bevindingen zal onderdeel uitmaken van het advies dat aan de stuurgroep DigiD zal worden gegeven ten aanzien van de vrijgave van DigiD R5.7.

Sogeti heeft ook op eerdere releases een securitytest uitgevoerd en bevindingen gedaan. Reactie van Logius ten aanzien van nog openstaande bevindingen uit deze voorgaande rapportages:

Release en volgnr.	Bevinding	Risico inschatting	Status Logius	Oplossen?
5.3.17	Denial of Service – Email versturen	Midden	Staat gepland om opgelost te worden in R5.8	Gepland voor R5.8.
5.4.2	Content-Security-Policy (CSP) header ontbreekt	Laag	Beleid omtrent CSP en de wijze van toepassen dient nog vastgesteld te worden.	Nog te bepalen.
5.4.3	Gelijktijdige sessies	Midden	Is op dit moment gewenste functionaliteit. DigiD architect geeft aan dat dienstaanbieders (waaronder MijnDigiD) eigenlijk toestaan dat er meerdere gelijktijdige sessies aanwezig zijn. DigiD kern kan niet de (lokale) sessie beëindigen. Hij gaat nog na hoe banken hier mee omgaan. Mogelijk aanpassen in een volgende release.	Impact nog onvoldoende bekend.
5.5.1	Content-Security-Policy header implementatiefout	Zeer Laag	Beleid omtrent CSP en de wijze van toepassen dient nog vastgesteld te worden.	Gepland voor R5.8.
5.5.3	Wachtwoordsterkte onvoldoende	Zeer Laag	In de context van DigiD-gebruik is het ophogen van een minimumaantal karakters voor een wachtwoord van 8 naar	Nee.

			12 karakters niet wenselijk. Naar het nu bestaande maximum van 32 karakters wordt nog een keer gekeken.	
5.5.4	Open poorten	Zeer Laag	In de context van DigiD is het dichtzetten van poort 80 op dit moment geen optie. Voor de domeinnaam digid.nl staat naast poort 443 ook poort 80 open. Voor een publieke dienst als DigiD is het noodzakelijk om voor een zo groot mogelijke groep burgers toegankelijk te zijn. Om die reden is het een "by design" keuze om poort 80 (http) open te houden, om gebruikers automatisch door te kunnen sturen naar poort 443 (https). Wanneer de loadbalancer in tier 1 van de betreffende omgeving een http request ontvangt, wordt dit automatisch redirected naar https, dit voorkomt dat een burger een "page not found" krijgt wanneer hij DigiD via http benadert.	Nee.
5.5.5	BEAST (Browser Exploit Against SSL/TLS)	Laag	Deze Cipher Block Chaining (CBC) suites worden ondersteund door DigiD. Die kunnen op dit moment nog niet uitgezet worden omdat daarmee (te) veel burgers uitgesloten worden. Het is een browser attack en in moderne browsers zit daarvoor een beveiligingsmechanisme ingebouwd.	Voorlopig niet, tenzij de betreffende ciphers als onbetrouwbaar worden geclassificeerd.

5.6.1	Cookie-domein te breed	Laag	De beveiligingsspecialist geeft aan dat de cookie-policy nog besproken wordt. Oplossing heeft veel impact op het huidige design. Oplossen is pas zinvol als er een beslissing is genomen over de cookie-policy.	Impact nog onvoldoende bekend.
5.6.2	Onvoldoende invoervalidatie Daring Fireball markup	Laag	Dit risico beperkt zich tot de beheermodule en de beheerdersrollen. Mogelijk oplossen in een volgende release.	Ja, nog niet ingepland.
5.6.3	SSL/TLS downgrade	Zeer Laag	De aard van deze bevinding en de mogelijkheid van misbruik is nog niet geheel duidelijk en zal nog nader onderzocht worden.	Impact nog onvoldoende bekend.
5.6.8	Directe gebruikersnaam enumeratie	Zeer Laag	Indien een aanvaller een sessie kan overnemen of toegang zou krijgen tot de loggegevens dan kan deze meer zien dan alleen de gebruikersnaam. Ook zaken als BSN en telefoon nummer (06) zijn dan zichtbaar. Dit is inherent aan de zaken die we loggen.	Nee.

1 Inleiding

1.1 Opdrachtformulering

In het kader van DigiD R5.7 worden verschillende securitytesten uitgevoerd. Een Attack&Penetration test wordt uitgevoerd op de aangepaste en ontwikkelde apps en er wordt een securitytest uitgevoerd vanuit intern aanvalsperspectief. Sogeti is gevraagd een securitytest uit te voeren vanuit extern aanvalsperspectief.

De scope van deze securitytest was de gehele DigiD-applicatie, waarbij de nadruk ligt op de risico's door de wijzigingen en/of uitbreidingen die in release 5.7 worden doorgevoerd. Een belangrijk deel van de uitbreidingen zijn wijzigingen buiten DigiD Kern voor de toevoeging van DigiD Hoog. Deze toevoegingen zorgen ervoor dat deze release groter en complexer is dan de voorgaande releases.

1.2 Aanpak

De securitytest bestond uit een vulnerability assessment met een diepgang greybox (hierbij krijgen de testers beschikking over documentatie en gebruikersrechten op het systeem, zodat het systeem met enige diepgang kan worden onderzocht) en betreft een externe test vanuit het oogpunt van een aanvaller vanaf het internet. Deze test is uitgevoerd vanuit het Sogeti kantoor in Amersfoort. De test is uitgevoerd in de A3-omgeving.

2 Resultaten

2.1 Cumulatief overzicht

Hieronder staat een totaaloverzicht van de bevindingen in dit rapport. Zie paragraaf 6.1 voor een toelichting op de risicoclassificatie.

In Tabel 1 zijn zowel nieuwe bevindingen opgenomen als terugkerende bevindingen die nog niet opgelost zijn.

Legenda:
Nieuwe bevindingen worden als volgt weergegeven: 1
Terugkerende bevindingen worden als volgt weergegeven: 1

Tabel 1: Nieuwe en terugkerende bevindingen

Risico / Onderzoekscategorie	Zeer hoog	Hoog	Midden	Laag	Zeer laag	Opgelost	Totaal
Client-side controls				2 0	1	2	5
Logica							
Authenticatie							
Sessiemanagement							
Toegang							
Invoerafhandeling				1		1	2
Omgeving							
Servers			0 1		0 1	3	5
Totaal			**1**	**3**	**2**	**6**	**12**

De geaccepteerde risico's van Logius zijn de volgende bevindingen.

- Content-Security-Policy header implementatiefout
- Gelijktijdige sessies
- BEAST (Browser Exploit Against SSL/TLS)
- Cookie-domein te breed
- Directe gebruikersnaam enumeratie
- Wachtwoordsterkte onvoldoende
- Open poorten
- Onvoldoende invoervalidatie Daring Fireball markup

Deze bevindingen worden opgesomd in hoofdstuk 4.

2.2 NCSC-richtlijnen

De basis voor dit testonderdeel zijn de ICT-beveiligingsrichtlijnen voor webapplicaties, versie 2015[1], uitgegeven door het Nationaal Cyber Security Centrum (NCSC).

Beleidsdomein

B.01	**Informatiebeveiligingsbeleid**
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.02	**Toegangsvoorzieningsbeleid**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Buiten scope voor deze test.	
B.03	**Risicomanagement**
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.	
Oordeel	
Buiten scope voor deze test.	
B.04	**Cryptografiebeleid**
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (dataclassificatie B.01/03).	
Oordeel	
Buiten scope voor deze test.	
B.05	**Contractmanagement**
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.	
Oordeel	
Buiten scope voor deze test.	
B.06	**ICT-landschap**
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.	
Oordeel	
Buiten scope voor deze test.	

Uitvoeringsdomein

U/TV.01	**Toegangsvoorzieningsmiddelen**
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.01	**Operationeel beleid voor webapplicaties**

[1] *Zie: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html*

derubricering

De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.	
Oordeel	
Buiten scope voor deze test.	
U/WA.02	**Webapplicatiebeheer**
Effectief en veilig realiseren van de dienstverlening.	
Oordeel	
Buiten scope voor deze test.	
U/WA.03	**Webapplicatie-invoer**
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.	
Oordeel	
Bevinding 5.7.6, 5.7.12	
U/WA.04	**Webapplicatie-uitvoer**
Voorkom manipulatie van het systeem van andere gebruikers.	
Oordeel	
Bevindingen 5.7.3, 5.7.4 en 5.7.5	
U/WA.05	**Betrouwbaarheid van gegevens**
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.	
Oordeel	
Bevinding 5.7.11	
U/WA.06	**Webapplicatie-informatie**
Beperk het (onnodig) vrijgeven van informatie tot een minimum.	
Oordeel	
Geen bevindingen.	
U/WA.07	**Webapplicatie-integratie**
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.	
Oordeel	
Geen bevindingen.	
U/WA.08	**Webapplicatiesessie**
Voorkomen dat derden de controle over een sessie kunnen krijgen.	
Oordeel	
Geen bevindingen.	
U/WA.09	**Webapplicatiearchitectuur**
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/PW.01	**Operationeel beleid voor platformen en webservers**
Betrouwbare ondersteuning van de programmatuur die op het platform draait.	
Oordeel	
Buiten scope voor deze test.	
U/PW.02	**Webprotocollen**
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.	
Oordeel	
Geen bevindingen.	
U/PW.03	**Webserver**
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.	
Oordeel	
Geen bevindingen.	

U/PW.04	Isolatie van processen/bestanden
Beperk de impact bij misbruik van processen.	
Oordeel	
Geen bevindingen.	
U/PW.05	Toegang tot beheermechanismen
Voorkomen van misbruik van beheervoorzieningen.	
Oordeel	
Buiten scope voor deze test.	
U/PW.06	Platform-netwerkkoppeling
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.	
Oordeel	
Buiten scope voor deze test.	
U/PW.07	Hardening van platformen
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Geen bevindingen.	
U/PW.08	Platform- en webserverarchitectuur
Een platform bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Geen bevindingen.	
U/NW.01	Operationeel beleid voor netwerken
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.	
Oordeel	
Toelichting	
U/NW.02	Beschikbaarheid van netwerken
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.	
Oordeel	
Buiten scope voor deze test.	
U/NW.03	Netwerkzonering
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.	
Oordeel	
Buiten scope voor deze test.	
U/NW.04	Protectie- en detectiefunctie
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.	
Oordeel	
Buiten scope voor deze test.	
U/NW.05	Beheer- en productieomgeving
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.	
Oordeel	
Buiten scope voor deze test.	
U/NW.06	Hardening van netwerken
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.	
Oordeel	
Geen bevindingen.	
U/NW.07	Netwerktoegang tot webapplicatie
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.	
Oordeel	

Geen bevindingen.	
U/NW.08	**Netwerkarchitectuur**
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.	
Oordeel	
Buiten scope voor deze test.	

Beheersingsdomein

C.01	**Servicemanagementbeleid**
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.	
Oordeel	
Buiten scope voor deze test.	
C.02	**Compliancemanagement**
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.	
Oordeel	
Buiten scope voor deze test.	
C.03	**Vulnerability-assessments**
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de webapplicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.	
Oordeel	
Buiten scope voor deze test.	
C.04	**Penetratietestproces**
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).	
Oordeel	
Deze test is onderdeel van het voldoen aan deze richtlijn.	
C.05	**Technische controlefunctie**
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.	
Oordeel	
Buiten scope voor deze test.	
C.06	**Logging**
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.	
Oordeel	
Buiten scope voor deze test.	
C.07	**Monitoring**
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.	
Oordeel	
Buiten scope voor deze test.	
C.08	**Wijzigingenbeheer**
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	
Oordeel	
Buiten scope voor deze test.	
C.09	**Patchmanagement**

derubricering

Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.	
Oordeel	
Buiten scope voor deze test.	
C.10	**Beschikbaarheidbeheer**
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.	
Oordeel	
Buiten scope voor deze test.	
C.11	**Configuratiebeheer**
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.	
Oordeel	
Geen bevindingen.	

3 Bevindingen met aanbevelingen

In de volgende paragrafen volgt per onderzoekscategorie een gedetailleerde beschrijving van de geconstateerde bevindingen met aanbevelingen.

3.1 Client-side Controls

Vaak worden maatregelen op de client gebruikt om eisen aan de data die naar de server verstuurd worden te controleren. Het gebruik van deze maatregelen biedt echter geen garanties; de client is immers volledig in het beheer van de eindgebruiker. Daarom moeten alle eisen die aan de data gesteld worden op de server gecontroleerd worden. In dit onderzoeksgebied is onderzocht of alle invoer die de server ontvangt wordt gecontroleerd alvorens deze verwerkt wordt.

Een overzicht van deze bevindingen.

3.1.1 Secure-flag ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.1	nnb	Zeer Laag (Opgelost)	Zeer Laag	Laag

Host
eid-a3.digid.nl

Omschrijving
De server stuurt cookies naar de gebruiker zonder de "Secure"-flag mee te geven in de 'Set-cookie'-header. Wanneer de flag gebruikt wordt zullen browsers die dat ondersteunen de cookies alleen nog naar de server terugsturen wanneer er gebruikgemaakt wordt van een beveiligde HTTPS-verbinding.

Bedreiging
Wanneer cookies verstuurd worden via een onbeveiligde HTTP-verbinding kan een aanvaller met toegang tot het netwerkverkeer de cookies onderscheppen. Zo kan hij wellicht gevoelige informatie inzien of de sessie van de gebruiker overnemen zonder dat hij hier een gebruikersnaam of wachtwoord voor nodig heeft. Ook als de applicatie nergens gebruik maakt van onbeveiligde verbindingen kan een aanvaller proberen de gebruiker naar een HTTP-pagina binnen het domein van de applicatie te lokken. Tenzij er gebruik gemaakt wordt van de 'HTTP Strict Transport Security'-header zal de browser de cookies dan naar deze (niet-bestaande) pagina versturen waardoor de aanvaller ze kan onderscheppen.

Aanbeveling
Bij het versturen van de cookie naar de gebruiker moet Secure op de volgende manier aan de Set-Cookie-header worden toegevoegd:
'Set-Cookie: [COOKIENAAM]=[COOKIEWAARDE]; path=[COOKIEPAD]; "Secure"'''

Voor meer informatie over de Secure-flag en hoe deze te implementeren zie: https://www.owasp.org/index.php/SecureFlag
Let wel: Als de cookie in eerste instantie naar de gebruiker gestuurd wordt over een onbeveiligde verbinding kan de cookie op dat moment nog onderschept worden.

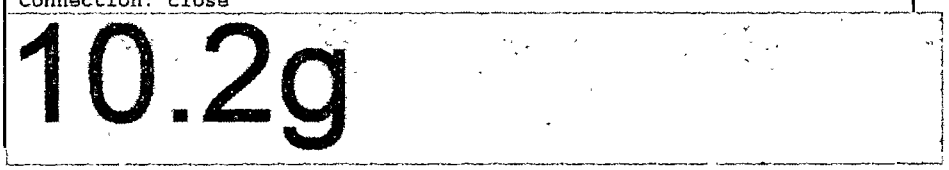
Details
De cookie JSESSIONID wordt gezet zonder Secure flag.

Request:

```
GET / HTTP/1.1
Host: eid-a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 403
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Set-Cookie: JSESSIONID=9C343140DF477382D49F19B066C830AB; Path=/;
HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Language: nl
Content-Length: 299
Date: Mon, 16 Apr 2018 08:56:13 GMT
Connection: close
```



Update hertest:
De cookie JSESSIONID wordt niet meer gebruikt op de eID-server en ook niet meer gezet. De bevinding is hierbij dan ook gemarkeerd als opgelost.

3.1.2 HTTP Strict Transport Security (HSTS) header ontbreekt

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.2	Nnb	Zeer Laag (Opgelost)	Zeer Laag	Laag

Betreffende hosts
eid-a3.digid.nl

Omschrijving
HTTP Strict Transport Security (HSTS) is een beveiligingsuitbreiding in moderne browsers, speciaal ontwikkeld om het downgraden van HTTPS naar HTTP te voorkomen. De server initieert dit door een extra header toe

te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt hij het gebruik van HTTPS af. Dit houdt in dat hij niet langer HTTP-verzoeken toestaat naar het betreffende domein.

Bedreiging
Wanneer de HSTS header niet is geïmplementeerd kan een aanvaller in een Man-in-the-Middle situatie een HTTPS-verzoek downgraden naar HTTP. Hierdoor worden gegevens onversleuteld verstuurd waardoor ze voor iedereen met toegang tot het verkeer leesbaar zijn.

Aanbeveling
Implementeer HSTS door de volgende response header toe te voegen:
Strict-Transport-Security: max-age=31536000
De beperking kan ook automatisch voor alle subdomeinen opgelegd worden:
Strict-Transport-Security: max-age=31536000; includeSubDomains
Meer informatie over de HSTS header vind u hier:
https://www.owasp.org/index.php/HTTP_Strict_Transport_Security

Details
Er wordt gebruik gemaakt van HTTPS maar de server stuurt geen HSTS header mee.

Request:

```
GET / HTTP/1.1
Host: eid-a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

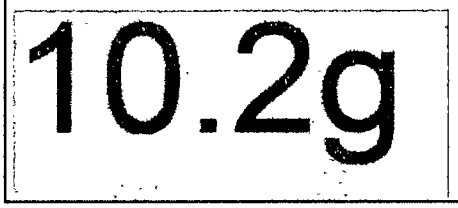
Response:

```
HTTP/1.1 403
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Set-Cookie: JSESSIONID=9C343140DF477382D49F19B066C830AB; Path=/;
HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Language: nl
Content-Length: 299
Date: Mon, 16 Apr 2018 08:56:13 GMT
[redacted]
```

Update hertest:
De HSTS header wordt nu wel meegestuurd in server responses.

```
HTTP/1.1 403
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
```

```
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Type: text/html
Content-Language: nl
Date: Fri, 20 Apr 2018 08:16:54 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```



3.1.3 *Anti-Cross-Site-Scripting-header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.3	Nnb	Laag	Zeer Laag	Midden

Betreffende hosts
rda-a3.digid.nl

Omschrijving
Een aantal browsers, waaronder Chrome, Safari en Internet Explorer 8 en hoger bieden standaard bescherming tegen bepaalde Cross-Site-Scripting-aanvallen. Deze bescherming kan ook afgedwongen worden door een speciale header aan de server responses toe te voegen. De server stuurt deze header nu niet mee.

Bedreiging
Gebruikers kunnen de bescherming handmatig uitschakelen, waardoor het voor aanvallers makkelijker wordt om een cross-site-scripting-aanval uit te voeren.

Aanbeveling
Stuur de speciale anti-Cross-Site-Scripting-header mee om de browser te instrueren de bescherming in te schakelen:
'X-XSS-Protection: 1'
De header kan ook worden uitgebreid om de browser te instrueren verdachte pagina's helemaal niet weer te geven door middel van de volgende toevoeging:
X-XSS-Protection: 1; mode=block
Bij het gebruik van deze uitgebreide header, wordt een lege pagina getoond met enkel een # en een waarschuwing aan de gebruiker.
Voor meer informatie, zie:
https://blogs.msdn.microsoft.com/ieinternals/2011/01/31/controlling-the-xss-filter/

Details
Het volgende voorbeeld is voor rda-a3.digid.nl.
In de header van het request mist de anti-cross-site-scripting header.

Request:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
```

```
(Test:map_codes)
Host: rda-a3.digid.nl
Connection: Keep-Alive
```

Response:

```
HTTP/1.1 200 OK
accept-ranges: bytes
etag: W/"13-1488876285000"
last-modified: Tue, 07 Mar 2017 08:44:45 GMT
content-type: text/html
content-length: 13
date: Mon, 16 Apr 2018 08:40:26 GMT
connection: keep-alive
set-cookie:
_persist=!sNOCHb7Y6TquaLAZzh+/BjbEK230wcbUC/gp5C3MFy5gPeSnumWS8+BZyJHU
VsOKr7ru4WV68AawKgfl8x6eo4RNWl9vaOkbN1JrgKs=;domain=.digid.nl;
HttpOnly;secure; path=/
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000 ; includeSubDomains
```

3.1.4 *X-Content-Type-Options header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.4	Nnb	Laag	Laag	Laag

Betreffende hosts
was-a3.digid.nl
rda-a3.digid.nl

Omschrijving
De anti-MIME-sniffing header X-Content-Type-opties is niet ingesteld op nosniff.

Bedreiging
Door het ontbreken van deze header wordt in oudere versies van Internet Explorer en Chrome MIME-sniffing toegepast op de response-body. Dit kan de response-body in een ander formaat weergeven dan het opgegeven content-type. Huidige (sinds begin 2014) versies van Firefox maken altijd gebruik van het opgegeven content-type (als er een is ingesteld).

Aanbeveling
Zorg ervoor dat de webserver de Content-Type header goed meestuurt, en dat de header X-Content-Type-Options is ingesteld op nosniff voor alle webpagina's.

Details
Het volgende voorbeeld is voor rda-a3.digid.nl.
In de header van het response mist de X-Content-Type-Options header.

Request:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
(Test:map_codes)
Host: rda-a3.digid.nl
Connection: Keep-Alive
```

Response:

```
HTTP/1.1 200 OK
accept-ranges: bytes
etag: W/"13-1488876285000"
last-modified: Tue, 07 Mar 2017 08:44:45 GMT
content-type: text/html
content-length: 13
date: Mon, 16 Apr 2018 08:40:26 GMT
connection: keep-alive
set-cookie:
_persist=!sNOCHb7Y6TquaLAZzh+/BjbEK230wcbUC/gp5C3MFySgPeSnumWS8+BZyJHU
VsOKr7ru4WV68AawKgfl8x6eo4RNWl9vaOkbN1JrgKs=;domain=.digid.nl;
HttpOnly;secure; path=/
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000 ; includeSubDomains
```

3.1.5 *Content-Security-Policy (CSP) header ontbreekt*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.5	Nnb	Zeer laag	Zeer laag	Laag

Hosts
balie-a3.digid.nl
was-a3.digid.nl
cls-a3.digid.nl
rda-a3.digid.nl
digidbeheer-a3.digid.nl
eid-a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven.

Bedreiging
Wanneer de CSP header niet is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwde code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP-header door de volgende header toe te voegen aan een server response:
Content-Security-Policy: "policy"
Vul hierbij de policy in met voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Een voorbeeld waarbij geen externe scripts worden geladen en 'inline-scripts' niet worden uitgevoerd:
Content-Security-Policy: default-src self

Details
De server stuurt de CSP header niet mee. Hierdoor wordt niet optimaal gebruik gemaakt van beschermende maatregelen in de browser. Het is aanbevolen om de server zo te configureren dat deze header wel wordt meegestuurd.

Voorbeeld request was-a3.digid.nl

```
GET / HTTP/1.1
Host: was-a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: _session_id=4e4cbd796dc2f346895c1f6e0aa57030;
_persist='cvLEZXG5eTUhROMZzh+/BjbEK230wVSu9PH7x2uMH/0CHZ1/aJJ1A1ZcfbnF
gz6SJdgo3oNqfVfJHGjzoBkqqsAXg+weHHhzgPHG89Y=
Connection: close
Upgrade-Insecure-Requests: 1
```

Voorbeeld response

```
HTTP/1.1 404 Not Found
Date: Tue, 17 Apr 2018 07:20:34 GMT
X-Request-Id: 9951914a-8782-4a60-add2-c9dcc9faef80
X-Runtime: 0.001974
Content-Length: 3061
Status: 404 Not Found
Connection: close
Content-Type: text/html; charset=UTF-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

3.2 Logica

Applicaties verwerken gegevens. Om te zien of daarbij bepaalde aannames zijn gedaan of niet doordachte keuzes zijn gemaakt, zijn de volgende datastromen onderzocht:

- Van server naar client;
- binnen de client; en
- van de client terug naar de server.

Er zijn geen nieuwe bevindingen in deze categorie.

3.3 Authenticatie

Webapplicaties bevatten vaak een authenticatiemechanisme om toegang tot bepaalde onderdelen van de applicatie te beperken. In dit onderdeel wordt onderzocht of de authenticatie omzeild kan worden, of dat er informatie gelekt wordt waardoor het makkelijker wordt gemaakt om het authenticatiemechanisme aan te vallen.

Er zijn geen nieuwe bevindingen in deze categorie.

3.4 Sessiemanagement

Om bij te houden of een gebruiker is aangemeld in een applicatie worden niet iedere keer de login gegevens over de lijn gestuurd. Normaliter

genereert de applicatie een token of ticket die de client mee stuurt naar de server. Hiermee wordt de actie geautoriseerd.

Er zijn geen nieuwe bevindingen in deze categorie.

3.5 Toegang

Om toegang te krijgen tot bepaalde functionaliteit zal aan een eisen voldaan moeten worden. Tijdens de test is gekeken in hoeverre hiervan wordt afgeweken.

Er zijn geen nieuwe bevindingen in deze categorie.

3.6 Functie specifieke invoer

Naast directe kwetsbaarheden in de invoerafhandeling, zijn er ook kwetsbaarheden die zich alleen voordoen bij het gebruik van specifieke functies. Hierbij moet bijvoorbeeld gedacht worden aan functies die communiceren met een database, functies die XML verwerken of functies waarmee software wordt aangeroepen. Een aanval die gebruik maakt van zo'n kwetsbaarheid raakt meestal ook andere applicaties of systemen. Tijdens de test is onderzocht of het manipuleren van de invoer kan leiden tot bijvoorbeeld SQL-injectie, het injecteren van XML-entities of buffer overflows.

Er zijn geen nieuwe bevindingen in deze categorie.

3.7 Invoerafhandeling

Een applicatie doet zijn verwerking en genereert uitvoer aan de hand van de invoer van de gebruiker of andere systemen. Hier wordt getest of deze verwerking en/uitvoer kan worden beïnvloed door het invoeren van niet verwachte gegevens. Hiervoor bepalen we binnen de scope van de applicatie alle mogelijke invoerplaatsen.

Een overzicht van deze bevindingen.

3.7.1 Reflectie in header

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.6	Nnb	Laag	Laag	Laag

Betreffende hosts
a3.digid.nl
mijn.a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl
eid-a3.digid.nl

Omschrijving
Gegevens die door de server worden gestuurd naar de gebruiker bevatten veelal instructies voor browsers in de vorm van headers, naast natuurlijk de uiteindelijke content van de pagina. Meestal kunnen de meegestuurde headers niet worden beïnvloed of aangepast door de gebruiker. In dit geval is dit wel mogelijk.

Bedreiging
Door het wijzigen van bepaalde invoer die naar de server wordt gestuurd, kan een aanvaller bijvoorbeeld de inhoud van een teruggestuurde header controleren. De invoer wordt direct gereflecteerd naar de gebruiker in de uitvoer.

Aanbeveling
Filter alle mogelijke invoer van de gebruiker en zorg dat er geen headerwaardes direct gewijzigd kunnen worden door invoer in een web request te veranderen.

Details
De waarde van de cookie _persist in headers van de a3.digid.nl site is te beinvloeden door in de request de Host header aan te passen.

Normaal request:

```
GET / HTTP/1.1
Host: a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Mon, 16 Apr 2018 09:11:29 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: f7fa273d-748d-479f-a679-a6481e9299d5
X-Runtime: 0.012203
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy  default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=06cf0231d38abbb56731d026048c6d26;Secure;
domain=.digid.nl; path=/; HttpOnly
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie:
_persist='VZdlboA/GhKJMQgZzh+/BjbEK230wdtLFySe+x11KmhX57PGKM+0OJhflo/9
Salw8Zwe2POpUce00FcpW3g2VmqzbxrTLdYRYad+6AQ=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

Als de host in de request wordt aangepast:

```
GET / HTTP/1.1
Host: sogeti.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response headers:

```
HTTP/1.1 200 OK
Date: Mon, 16 Apr 2018 13:30:41 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: bbf751db-1f77-4d9e-9463-2757bfa2ceab
X-Runtime: 0.012570
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=97a0609b02517cf93d904402fad94072;Secure;
domain=.digid.nl; path=/; HttpOnly
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Set-Cookie:
_persist=!MJk6VzFsep7OU0IZzh+/BjbEK230wf7dK/lvJah5dDUXBQOBmLFWko64E8w2
gNXwN6/tKNFxmUmxBRq+pajUtPyEP38OM9VA6+VFBj0=;domain=.sogeti.com;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

De cookie is nu geldig voor het domein sogeti.com. Het invoeren van bepaalde andere tekens zorgt voor een 400 Bad Request. Er kan niet uit de header regel worden gebroken, dus het toevoegen van extra headers is niet mogelijk.

Request met toevoegen Secure;

```
GET / HTTP/1.1
Host: sogeti.com, Secure
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 400 Bad Request
Date: Mon, 16 Apr 2018 13:33:01 GMT
Content-Length: 347
Connection: close
Content-Type: text/html; charset=iso-8859-1
Set-Cookie:
_persist='owTWJRTRdNaNxD8Zzh+/BjbEK230wQ8LSDdog2c4dSmM9w/U3OtANpRe+9p8
cqDO9j4XQU/YZTuU1DuNe8VFSmcgrSQPLF+1C0cJqBk=;domain=.sogeti.com;
Secure; HttpOnly;secure, path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not
understand.<br />
</p>
<p>Additionally, a 400 Bad Request
error was encountered while trying to use an ErrorDocument to handle
the request.</p>
</body></html>
```

3.7.2 *Stored Cross-Site Scripting*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.7	Nnb	Hoog (Opgelost)	Hoog	Hoog

Betreffende hosts
digidbeheer-a3.digid.nl
config-a3.digid.nl

Omschrijving
Het is mogelijk om waarden aan de server aan te leveren die opgeslagen worden op een bepaalde website. Deze waarden zal de server aan de gebruiker tonen, dan wel uitvoeren in de context van de webpagina wanneer deze bezocht wordt.

Bedreiging
Als in plaats van geaccepteerde waarden HTML code of JavaScript ingevoerd wordt, zal dit worden uitgevoerd wanneer de betreffende pagina geladen wordt. Een gevolg hiervan is dat een kwaadwillende o.a. de cookiegegevens van alle bezoekers kan verzamelen.

Aanbeveling
Zorg er voor dat de input van de parameters wordt gevalideerd op het verwachte type, zoals tekst en datum, of specifieker zoals een postcode en telefoonnummer. Dit is niet de volledige oplossing, maar is een mitigerende maatregel die ook andere problemen kan verhelpen.
Voor een volledige oplossing, op basis van de context waar de data terecht komt (CSS, HTMLEntity, JavaScript en URL), zou encoding moeten worden toegepast bij de uitvoer naar de client. De gebruikte encoding zou op basis van whitelisting (ook wel positive security model) moeten werken. Dit wil zeggen dat alle karakters omgezet moeten worden behalve een specifieke lijst van karakters welke geen schade kunnen toebrengen.
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

Details
Het is mogelijk om code toe te voegen aan de gebruikersnaam bij het aanmaken van een nieuw DigiD-account. Het punt waar de code wordt ingevoerd (de gebruikersomgeving – nieuwe gebruiker aanmaken (DigiD aanvragen)) is anders dan het punt waar de code wordt uitgevoerd (DigiD beheeromgeving/config-omgeving).

De code wordt in eerste instantie alleen uitgevoerd indien het account wordt bekeken waaraan de code in de gebruikersnaam is toegevoegd. Vervolgens wordt de code uitgevoerd voor iedereen die de beheerpagina bezoekt omdat het account aan de recent bekeken pagina's is toegevoegd.

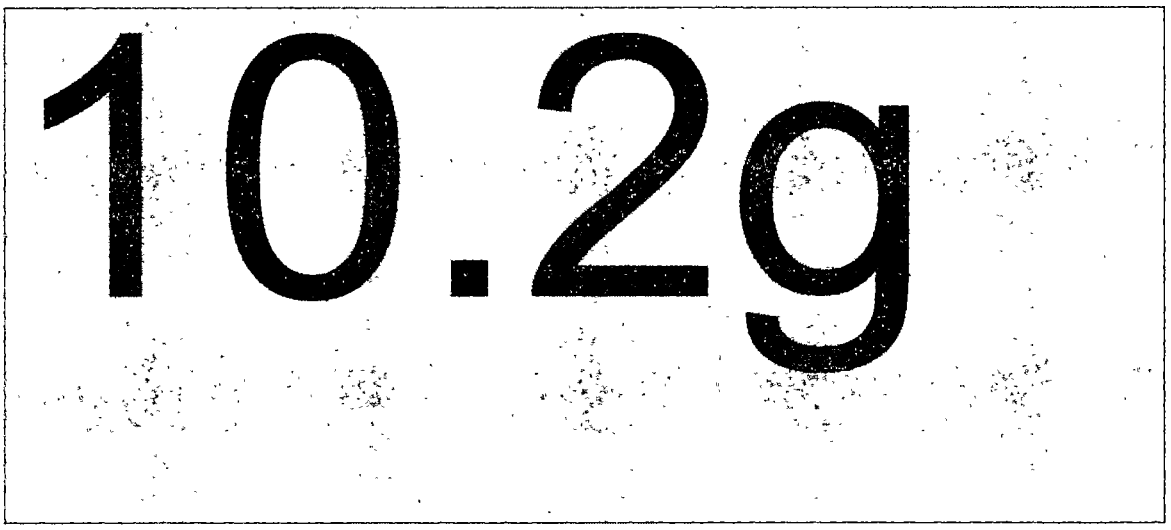
Op de config-omgeving wordt de code uitgevoerd op het moment dat op de gebruikersnaam wordt geklikt om de gebruikersnaam te kopiëren.
Via onderstaande request wordt een gebruiker aangemaakt met code in zijn gebruikersnaam.

Als voorbeeld wordt deze gebruikersnaam gebruikt:
kiAa<script>alert(1)</script>

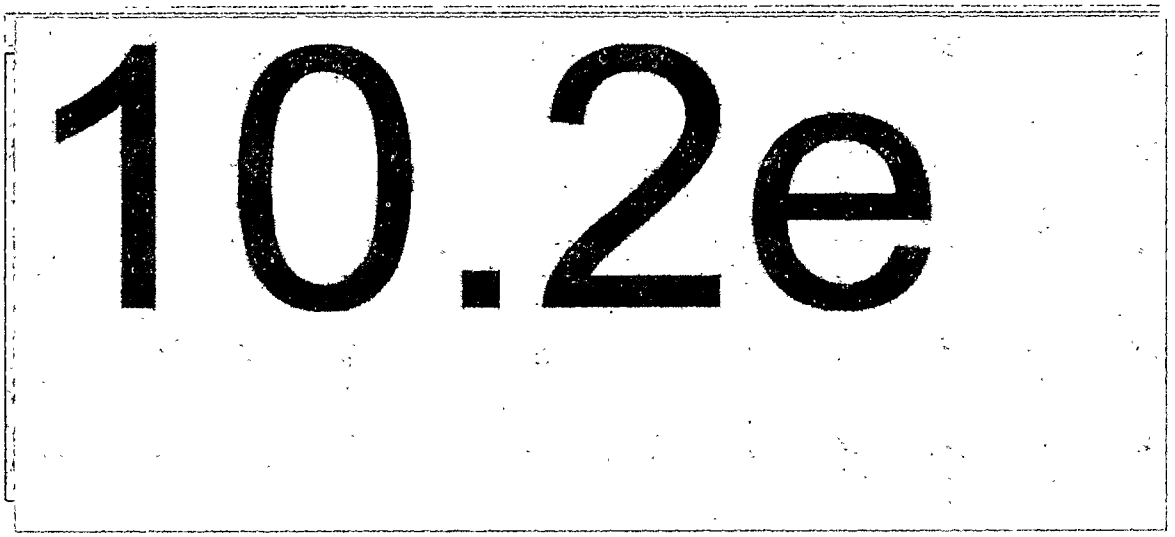
Request:

```
POST /nieuw_digid HTTP/1.1
Host: a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding. gzip, deflate
Referer: https://a3.digid.nl/nieuw_digid
Content-Type: application/x-www-form-urlencoded
Content-Length: 491
Cookie: _session_id=8de56f92aa47b430fe6b67fb95358cf1;
_persist='xALrmwHQFydXJmsZzh+/BjbEK230wUTvr7wlb8WHuGljKdtqOXYwXIBsgIHk
Vtalub/V+ZyeuYA54DFQSrA3jmWtMpeJFQc6nkReXmA=
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&_method=put&authenticity_token=tmjFrSE%2B%2F2Z%2BtivW6U
F52k9HXTegmrw7X70HiceULdgqixlCSGQ0y4f7B4iNrApdpIZCIvuMAajNf66aofjv4g%3
D%3D&account%5Bgebruikersnaam%5D=kiAa%3Cscript%3Ealert%281%29%3C%2Fscr
ipt%3E&account%5Bpassword%5D=Wachtw00rd%26&account%5Bpassword_confirma
tion%5D=Wachtw00rd%26&account%5Bsms_tools_attributes%5D%5B0%5D%5Bphone
_number%5D=0611111111&account%5Bsms_tools_attributes%5D%5B0%5D%5Bgespr
oken_sms%5D=0&account%5Bemail_attributes%5D%5Badres%5D=&commit=Volgend
e
```

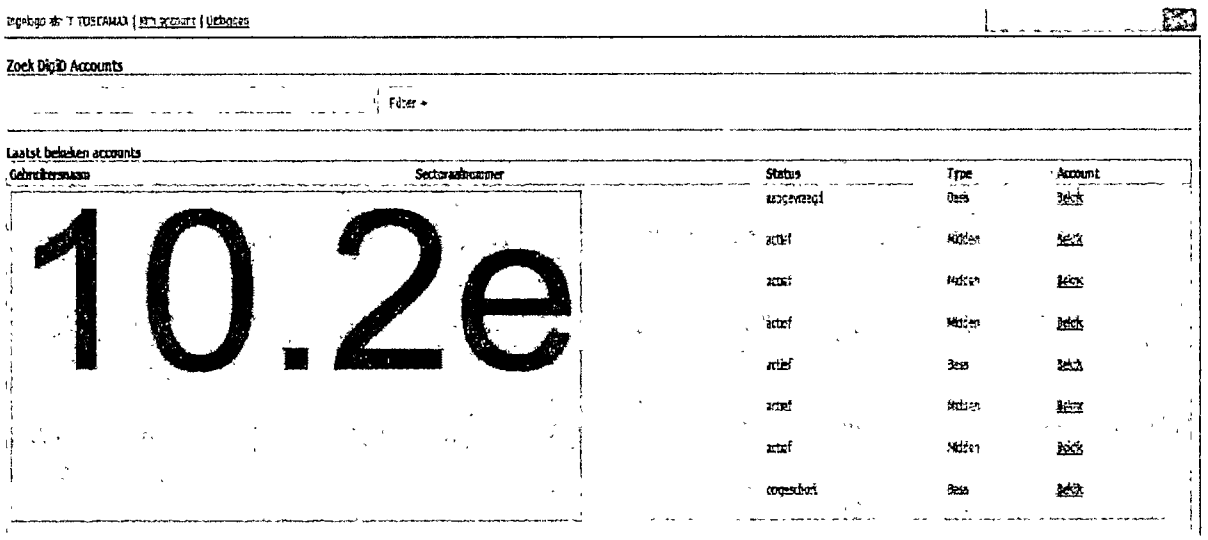
Vervolgens wordt deze code uitgevoerd op de beheermodule en de config-omgeving:



derubricering



Update hertest:
De output wordt inmiddels ge-escaped op de beheeromgeving:



De bevinding is nog wel aanwezig op de config-omgeving, aangezien die niet in productie draait is het directe risico gemitigeerd. Wel wordt aanbevolen om op alle mogelijke plekken de uitvoer te encoderen, ook om in de toekomst problemen te voorkomen.

3.8 Omgeving

De security van een systeem kan sterk afhankelijk zijn van de omgeving waarin het is aangesloten. Hier wordt getest op mogelijkheden om beveiliging van systemen te omzeilen via de omgeving.

Er zijn geen nieuwe bevindingen in deze categorie.

3.9 Servers

Applicaties zijn afhankelijk van de infrastructuur waar zij op draaien. Deze kan meer bieden dan de applicatie nodig heeft of niet up-to-date zijn.

Een overzicht van deze bevindingen.

3.9.1 *Information disclosure – Serverinformatie*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.8	Nnb	Zeer Laag (Opgelost)	Laag	Zeer Laag

Betreffende hosts
eid-a3.digid.nl

Omschrijving
Systemen geven vaak zelf onbedoeld informatie over de software die op het systeem is geïnstalleerd. Dit is waarschijnlijk een default instelling van de software.

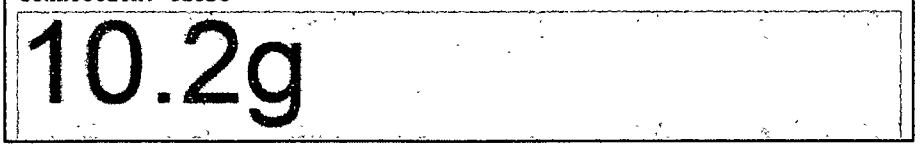
Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om te zoeken naar reeds bekende zwakheden in een specifiek softwarepakket.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Stuur geen informatie over systemen en software in cookies of HTTP headers mee. Zorg dat foutmeldingen zonder specifieke systeeminformatie getoond worden.

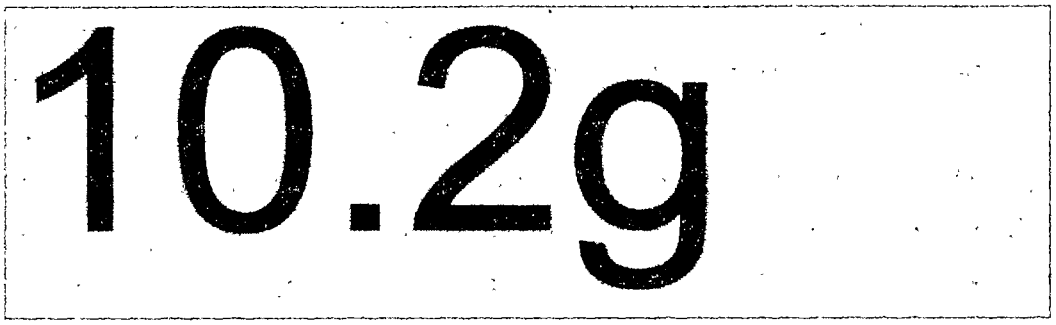
Details
De standaard foutmelding van pagina's op eid-a3.digid.nl is een foutmelding van het Spring Java framework. Het gebruik van dit framework is dan ook indirect af te leiden uit deze foutmelding.

Voorbeeld response:

```
HTTP/1.1 403
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Set-Cookie: JSESSIONID=9C343140DF477382D49F19B066C830AB; Path=/;
HttpOnly
Content-Type: text/html;charset=ISO-8859-1
Content-Language: nl
Content-Length: 299
Date: Mon, 16 Apr 2018 08:56:13 GMT
Connection: close
```

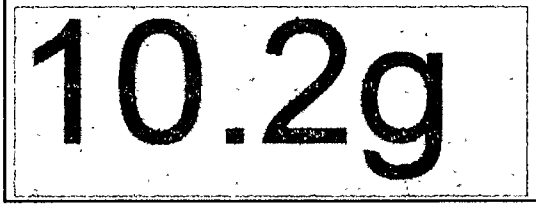


Resultaat:



Update hertest:
De server toont nu een foutmelding die niet te herleiden is naar de gebruikte serversoftware.

```
HTTP/1.1 403
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Type: text/html
Content-Language: nl
Date: Fri, 20 Apr 2018 08:16:54 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```



3.9.2 *Vreemde HTTP methods toegestaan*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.9	Nnb	Laag (Opgelost)	Laag	Laag

Betreffende hosts
eid-a3.digid.nl

Omschrijving
Op de server worden naast GET, HEAD en POST ook andere methodes toegestaan.

Bedreiging
Deze methodes kunnen op de server voor ongewilde resultaten en responses zorgen.

Aanbeveling
Sta alleen de door de applicatie gebruikte HTTP-methodes toe op basis van whitelisting.

Details
De volgende HTTP methodes zijn toegestaan: GET, HEAD, POST, PUT, DELETE, OPTIONS en TRACE (zie hieronder). De HTTP TRACE request returned de OPTIONS in een 405 not implemented error:

Request:

```
TRACE / HTTP/1.1
Host: eid-a3.digid.nl
Connection: Keep-Alive
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None)
(Test:httpoptions: OPTIONS /)
```

Response:

```
HTTP/1.1 405
Allow: HEAD, DELETE, POST, GET, OPTIONS, PUT
Content-Length: 0
Date: Mon, 16 Apr 2018 12:30:22 GMT
Connection: close
```

Update hertest:
De bevinding is opgelost. De server reageert alleen nog op GET, POST en HEAD requests.

3.9.3 *Information disclosure – Stack trace*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.10	Nnb	Laag (Opgelost)	Laag	Laag

Betreffende hosts
eid-a3.digid.nl

Omschrijving
Het systeem geeft informatie weg over de programmastructuur en de functies en libraries die worden gebruikt. Dit gebeurt in de vorm van een 'stack trace' in een foutmelding.

Bedreiging
Deze informatie kan door een aanvaller worden gebruikt om meer te leren over de werking van het programma voor het vinden van een kwetsbaarheid, of om te zoeken naar reeds bekende zwakheden in gebruikte libraries.

Aanbeveling
Stuur alleen informatie naar de client die noodzakelijk is voor de werking van de applicatie. Zorg dat foutmeldingen zonder systeeminformatie getoond worden.

Details
De server toont een stack trace bij bepaalde antwoorden (in dit geval een 500 Internal Server Error). Een voorbeeld:

Request:

```
GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
Host: eid-a3.digid.nl
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept: application/json
Accept-Language: en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 500
Content-Type: application/json;charset=UTF-8
Date: Mon, 16 Apr 2018 15:03:53 GMT
Connection: close
```

Update hertest:
De server toont nu geen stack traces meer:

```
HTTP/1.1 500
Content-Type: application/json;charset=UTF-8
Date: Fri, 20 Apr 2018 09:04:14 GMT
Connection: close
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

{"status":500,"timestamp":1524215054884}
```

3.9.4 SSL/TLS downgrade

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.11	Nnb	Zeer laag	Zeer laag	Zeer laag

Betreffende hosts
mijn.a3.digid.nl
was-a3.digid.nl
digidbeheer-a3.digid.nl
balie-a3.digid.nl
cis-a3.digid.nl
rda-a3.digid.nl
a3.digid.nl
eid-a3.digid.nl

Omschrijving
De applicatie maakt gebruik van een SSL/TLS tunnel, bijvoorbeeld door de toepassing van het HTTPS protocol. De client en server stemmen het gebruik hiervan met elkaar af middels een handshake aan het begin van de communicatie.

Bedreiging
Als een aanvaller kan optreden als 'man in the middle' kan deze de handshake veranderen. Als op deze wijze een SSL/TLS tunnel kan worden omzeild of een lagere versie wordt gebruikt dan gewenst is er sprake van een zogenaamde "downgrade". Voor de gebruiker blijft de verbinding over een minder veilig kanaal lopen. Hierdoor kan een aanvaller eventueel gecommuniceerde informatie inzien en veranderen. De aanvaller

onderhoudt de SSL/TLS verbinding met de applicatie als dit vereist wordt door de applicatie.

Aanbeveling
Zorg ervoor dat alle referenties die binnen de eigen invloedssfeer vallen gebruik maken van de juiste referenties (altijd naar HTTPS). Pas daarnaast ook HTTP Strict Transport Security (HSTS) toe wat voor sommige browsers het gebruik van HTTPS afdwingt. Let er wel op dat HSTS een compenserende maatregel is, sommige browser ondersteunen geen HSTS (bijvoorbeeld Internet Explorer pas vanaf versie 12). Daarnaast zorgt het gebruik van TLS Fallback SCSV dat altijd de sterkste ciphersuites worden gebruikt.

Details
Voorbeeld voor was-a3.digid.nl:

```
root@kali:~# sslscan was-a3.digid.nl
Version: 1.11.11-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 144.43.243.146

Testing SSL server was-a3.digid.nl on port 443 using SNI name was-
a3.digid.nl

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV
```

3.9.5 *Denial of Service – Email versturen*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.7.12	Nnb	Midden	Laag	Midden

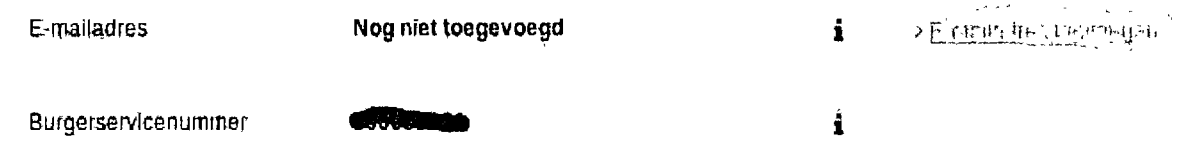
Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Het systeem is zo te manipuleren dat de server een grote hoeveelheid emails naar een gebruiker stuurt.

Bedreiging
Hierdoor kan een applicatie deels, of volledig onbeschikbaar worden voor gebruikers. Ook kan het ervoor zorgen dat de gebruiker zijn mail niet meer kan gebruiken.

Aanbeveling
Zorg ervoor dat er aan de serverkant wordt gecontroleerd of er al een email is gestuurd naar de gebruiker.

Details
Het is mogelijk om via de DigiD applicatie een continue stroom emails te versturen naar een willekeurig e-mailadres. Voorwaarde hiervoor is wel dat de aanvaller een geldig DigiD account heeft bemachtigd.



Wanneer er een e-mailadres wordt opgegeven en op de volgende knop wordt knop wordt gedrukt wordt onderstaande request verzonden:

```
POST /email HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://mijn.a3.digid.nl/email/nieuw
Content-Type: application/x-www-form-urlencoded
Content-Length: 201
Cookie: _session_id=b112cca5cd799b8a426083f6076822e8;
_persist='OWAYhwuOz3MxOfj+5aqg6lTJU5Hb5ZGZXgyuOQ3RaXAbsSqHBitJ4v3l0JX0
zjzclnixxqmpazpl55wKVrve0WRNs7ehRX0JfdWstO4=,
persist_cis='t9BuYLOe7suKRQl8aojjirYC1E4er65r08mogQl8xvudLAPKe2Ruw7YxL
H43h653IDPtbLKTNKzJRN84yOdOCUdWFKDEiSy2x+03/+o=
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=GvI8j37pHUO9s%2BaufoIjm4Zjef%2Bn4blo
f6bsbV%2BVjwKwuVM7X7RcGZ8dWvSkb8BTsUIHqNpuLc5%2BMlACFIReSg%3D%3D&email
%5Baddress%5D=[redacted]&commit=Volgende
```

De reponse zorgt ervoor dat een scherm wordt getoond met daarop het verzoek om een wachtwoord op te geven.

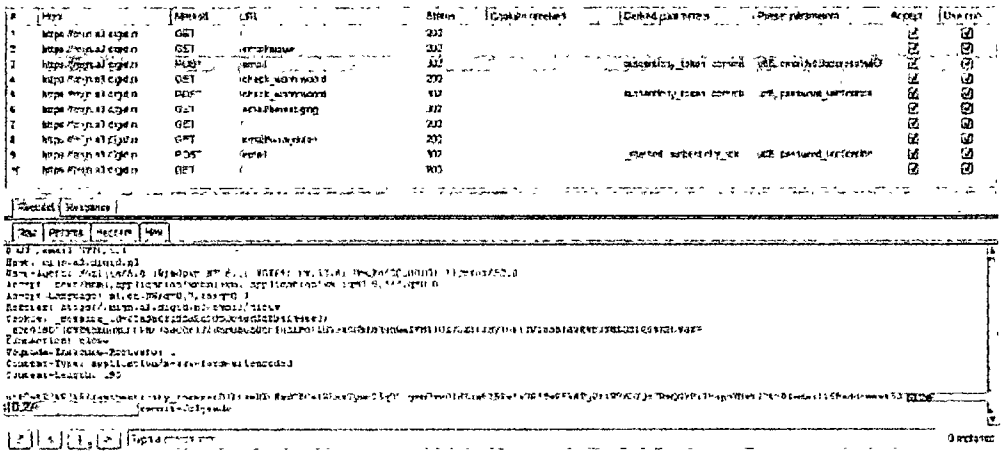
Nadat een correct wachtwoord is verzonden zal DigiD een email sturen met een verificatie code naar het email adres. Deze code moet binnen een bepaalde periode wordt opgegeven anders vervalt deze. Wanneer de eindgebruiker de code nog een keer wilt versturen verschijnt de melding dat er al een code onderweg en na meer dan 5 minuten een nieuwe code kan worden aangevraagd.

"Er is nog een e-mail onderweg naar u. Vanaf xx:xx uur (Nederlandse tijd) kunt u uw e-mailadres weer wijzigen."

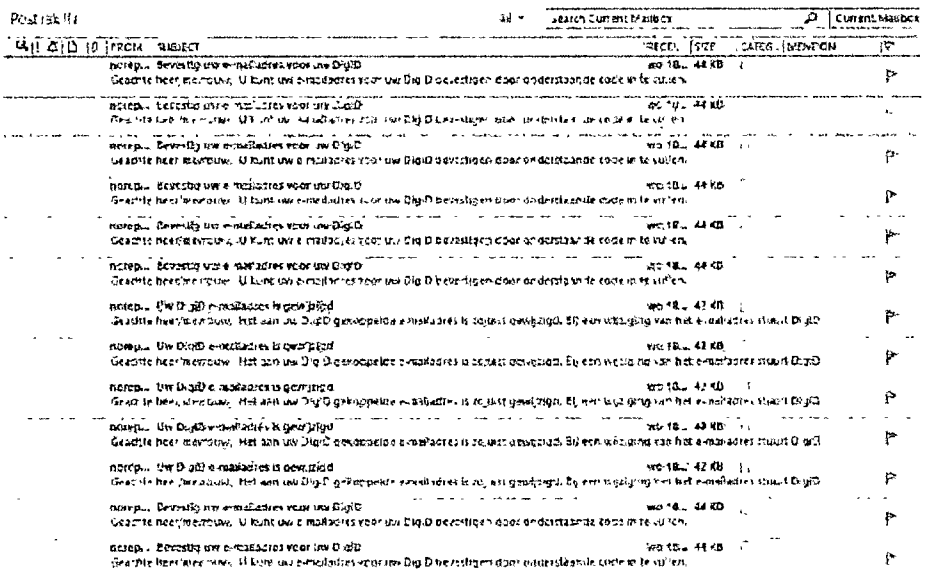
Echter is het mogelijk om het nog-niet geactiveerde e-mailadres te verwijderen van het account.

Na het opgeven van het correcte wachtwoord zijn alle meldingen van een gekoppeld maar nog niet geactiveerd e-mailadres verdwenen. Het gevolg is dat de gebruiker bovenstaande actie nog een keer kan uit voor hetzelfde of andere e-mailadressen.
Deze actie is te automatiseren, waarna er continue een e-mail wordt opgegeven en verwijderd. Zoals in onderstaande script te zien is.

derubricering



Deze e-mails worden ook daadwerkelijk verzonden, zoals in onderstaand voorbeeld is te zien:



Er bestaat het gevaar dat als de mail naar veel verschillende personen wordt verstuurd, en deze verwachten geen mail. De mail wordt aangemerkt als spam of phishing. waarmee het verzendadres op een spamblacklist kan komen te staan en mailservers die daar gebruik van maken meer mails accepteren van dit adres.

derubricering

4 Geaccepteerde risico's

Hieronder volgt een lijst van bevindingen uit eerdere tests die om businessredenen (nog) niet opgelost kunnen worden. Deze bevindingen zijn nog niet opgelost en worden gezien als geaccepteerde risico's. De resultaten zijn dus reeds bekend.

4.1.1 BEAST (Browser Exploit Against SSL/TLS)

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.1	Nnb	Laag	Zeer Laag	Midden

Betreffende hosts
a3.digid.nl
balie-a3.digid.nl
cls-a3.digid.nl
digidbeheer-a3.digid.nl
eid-a3.digid.nl
mijn.a3.digid.nl
was-a3.digid.nl
rda-a3.digid.nl

Omschrijving
De SSL/TLS implementatie op de server maakt het mogelijk om een voorspelbare ciphertext te genereren uit plaintext.

Bedreiging
In cryptografie is Cipher Block Chaining (CBC) een veelgebruikte methode om de voorspelbaarheid van encrypted data te verminderen. Het doel is om te voorkomen dat dezelfde data (plaintext) tot dezelfde encrypted data (ciphertext) leidt gedurende het encryptieproces. Hiervoor wordt een zogenaamde initialization vector (IV) gebruikt, die uniek is voor elk bericht in elke sessie. CBC encrypt ieder blok data en gebruikt deze data ook als input voor de encryptie van het volgende blok data: het "chainen". Dit doel wordt ondermijnd door oudere implementaties van SSL/TLS, waardoor in sommige situaties de IV voorspelbaar is, dus ook de ciphertext. Dit op zijn beurt kan gebruikt worden om (delen van) de plaintext data terug te berekenen vanuit de encrypted data.

Aanbeveling
Upgrade naar TLSv1.2. Een andere, niet aan te raden, oplossing is het gebruiken van encryptie zonder CBC.

Details
De verbinding tussen de server en de gebruiker is mogelijk kwetsbaar voor BEAST omdat er CBC-ciphers ondersteund worden, in combinatie met TLS 1.0. Een voorbeeld:

```
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
```

4.1.2 *Gelijktijdige sessies*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.2	Nnb	Midden	Midden	Midden

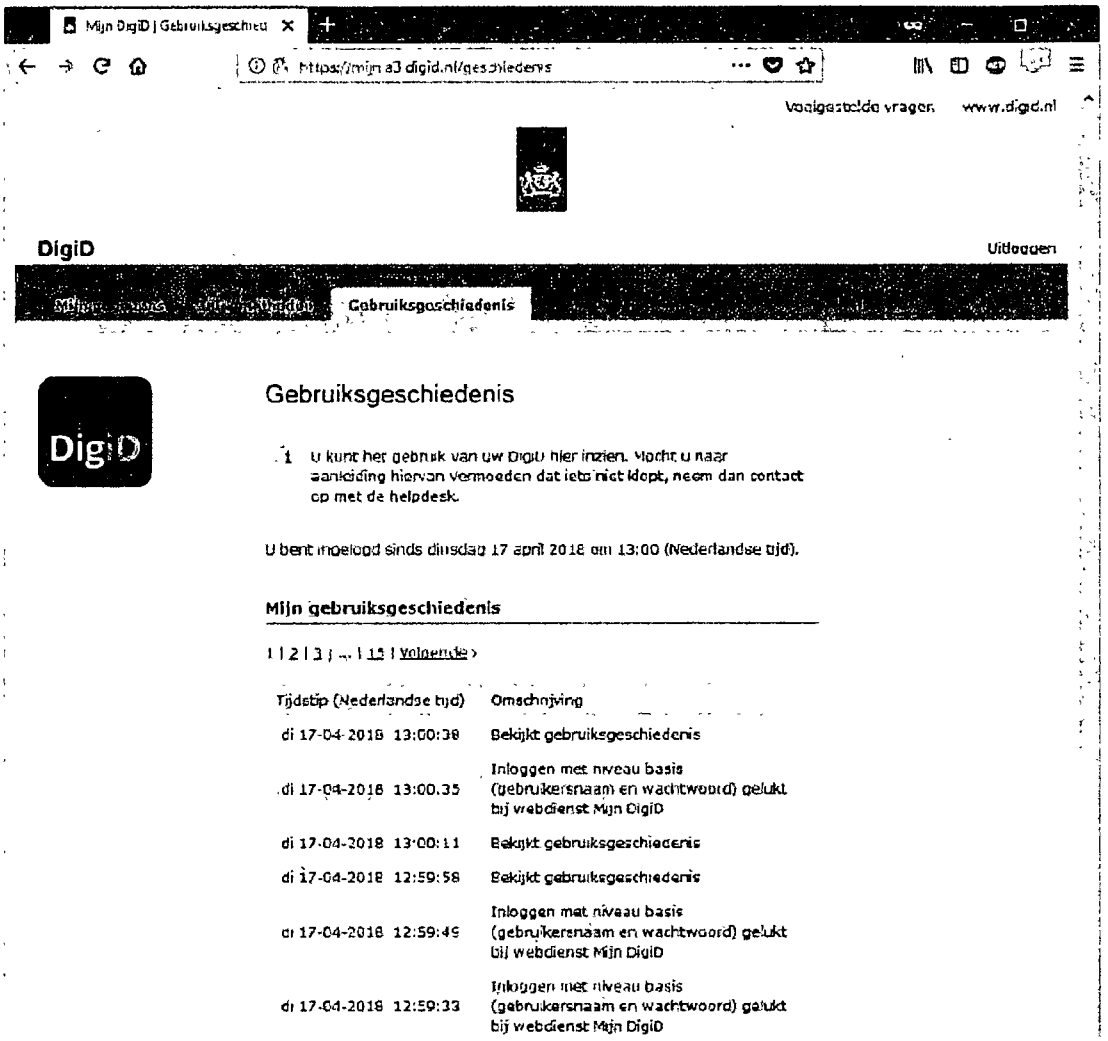
Betreffende hosts
mijn.a3.digid.nl
a3.digid.nl

Omschrijving
Het is mogelijk voor een gebruiker om meerdere sessies gelijktijdig open te hebben.

Bedreiging
Wanneer er meerdere gelijktijdige sessies voor dezelfde gebruiker kunnen bestaan betekent dit dat oude sessies niet automatisch worden afgesloten. Dit geeft een aanvaller de mogelijkheid om oude sessies te misbruiken, ook als de gebruiker al een nieuwe sessie heeft opgestart.

Aanbeveling
Als een gebruiker die al een sessie open heeft staan een nieuwe sessie opent, dient de oude sessie afgesloten te worden. Dit verkleint de kans dat een aanvaller een oude sessie van een gebruiker misbruikt. Daarnaast wordt een gebruiker automatisch gewaarschuwd als een aanvaller een sessie namens hem start. Bij vermoedens van misbruik kan een gebruiker een eventuele oude sessie sluiten door nogmaals in te loggen.

Details
Het is ook mogelijk om met beide sessies acties uit te voeren op de Mijn DigiD-omgeving. Ga na of het nodig is voor een gebruiker om twee gelijktijdige sessies toe te staan.



4.1.3 *Content-Security-Policy header implementatiefout*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.3	Nnb	Laag	Zeer Laag	Midden

Betreffende hosts
mijn.a3.digid.nl

Omschrijving
Content Security Policy (CSP) is een beveiligingsuitbreiding in moderne browsers speciaal ontwikkeld om te voorkomen dat content vanaf een onvertrouwde bron ingeladen/uitgevoerd wordt. De server initieert dit door een extra header toe te voegen aan de responses die hij verstuurt. Wanneer een browser die deze functionaliteit ondersteunt eenmaal deze header heeft ontvangen dwingt deze het meegegeven beleid af. Dit houdt in dat hij niet langer content inlaad die niet als vertrouwd is aangegeven. De policy welke door de server verstuurd wordt is niet correct/veilig.

Bedreiging
Wanneer de CSP header niet correct is geïmplementeerd kan een aanvaller content inladen vanaf een onvertrouwde bron. Hierdoor kan bijvoorbeeld onvertrouwen code (XSS) uitgevoerd worden, of ongewilde content getoond worden alsof deze op de aangevallen pagina staat.

Aanbeveling
Implementeer de CSP policy zo strak mogelijk, waarbij onveilig gedrag niet toegelaten wordt. Bouw vanuit hier de policy uit met alleen die functionaliteit welke nodig is. Gebruik hierbij voor de website toepasselijke "directives", zoals gedocumenteerd op bijvoorbeeld https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives

Details

Request

```
GET / HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://mijn.a3.digid.nl/email/verwijderen
Cookie: _session_id=dcf620f340761d4bb8f2630bb470f8a4;
_persist=!7bsMXMGK5aQZ6moZzh+/BjbEK230wXpWLGR1T0tl0c/TdJzLRuj5KaIQkiE/
iacJtJbGm/k94HZHV+nHzMTVB/tiCeIUzaoWIVdWwfw=
Connection: close
Upgrade-Insecure-Requests: 1


*Response*

bc.. HTTP/1.1 200 OK
Date: Tue, 17 Apr 2018 09:05:20 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 961fe3bd-2875-4122-b4c3-b3bd7b176c87
X-Runtime: 0.094422
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data:;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Status: 200 OK
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
```

4.1.4 *Cookie-domein te breed*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.4	Nnb	Laag	Zeer Laag	Laag

Betreffende hosts
a3.digid.nl
mijn-a3.digid.nl
was-a3.digid.nl

digidbeheer-a3.digid.nl
cis-a3.digid.nl
eid-a3.digid.nl
rda-a3.digid.n

Omschrijving
Een cookie wordt standaard gebonden aan het (sub)domein dat de cookie heeft aangemaakt. Via de "Domain" parameter van de 'Set-Cookie' header kan de cookie echter ook voor een specifiek domein en al zijn subdomeinen beschikbaar gemaakt worden. Een applicatie kan alleen cookies aanmaken voor zijn eigen domein en bovenliggende domeinen, met uitzondering van top-level domeinen zoals .com of .nl.

Bedreiging
Wanneer een cookie wordt ingesteld met de "Domain" parameter (bijvoorbeeld: Domain=.example.com) stuurt de browser de cookie ook naar alle pagina's die onder subdomeinen van dat domein vallen (bijvoorbeeld: www.example.com en shop.example.com). Hierdoor kan het voorkomen dat de cookie van een applicatie ook verstuurd wordt naar andere applicaties die onder hetzelfde hoofddomein vallen. Dit zou de werking van die applicaties kunnen verstoren. Daarnaast zou het kunnen leiden tot het uitlekken van de cookie als de andere applicaties of hun infrastructuur kwetsbaarheden bevatten.

Aanbeveling
Bij het aanmaken van belangrijke cookies moeten de "Domain" en "Path" parameters altijd zo specifiek mogelijk ingesteld worden. Hierdoor wordt de kans dat de cookie buiten de applicatie terechtkomt tot een minimum beperkt. In sommige gevallen kan dit betekenen dat de "Domain" parameter beter weggelaten kan worden. Bijvoorbeeld: de sessiecookie voor https://shops.example.com/flowers zou als volgt aangemaakt kunnen worden: 'Set-Cookie: session=[SESSION_TOKEN]; Path=/flowers/; Secure; HttpOnly. Merk hierbij op dat de 'Domain" parameter bewust is weggelaten om ervoor de zorgen dat de browser de cookie alleen naar pagina's binnen het domein shops.example.com verstuurt en niet naar pagina's binnen subdomeinen van dat domein. Zie voor meer informatie RFC6265 (http://tools.ietf.org/html/rfc6265), met name secties 5.2.3 en 5.3.6.

Details
Wanneer een gebruiker inlogt stelt de server een sessiecookie in voor het domein .digid.nl. Hierdoor zal de browser van de gebruiker de cookie meesturen met verzoeken naar alle subdomeinen van digid.nl. De PAP-eisen van Logius stellen dat cookies subdomein-specifiek ingesteld moeten worden. ACC2.5.2: "Cookies zijn secure en httponly en subdomein specifiek."

Request cis-a3.digid.nl

```
GET / HTTP/1.1
Host: cis-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 19 Apr 2018 09:30:17 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 02a5c1cb-e435-4792-8973-918bcee98519
X-Runtime: 0.004799
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie:
_digid_cis_session=545b99a8a3159fad149475ae8b136208;Secure; path=/;
expires=Thu, 19 Apr 2018 09:45:17 -0000; HttpOnly
Status: 200 OK
Content-Length: 2
Connection: close
Content-Type: text/plain; charset=utf-8
Set-Cookie:
persist_cis='eXILb6t2P9Zdo0oFDcfBngrAvVDj7TBXkX4lrG3oxHVoSPcd+EvQbt/tR
+8eIJWt6+IVW9icbSQNHc3Omt31OMdfPBDFFwze07WyMxQ=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

ok
```

Request mijn.a3.digid.nl

```
GET / HTTP/1.1
Host: mijn.a3.digid.nl
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: nl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: _session_id=77f921f566f1358ccbb7a6b5be7ed653;
_persist='Tn247dxnf0C+RosZzh+/BjbEK230wd2jwCesJrJFihASef69Jgx2EwxIq7Ee
wPqwa07g6AGtwXsV8zwOCX7kI8Kl6V5aC4fwaIDpuOI=
Connection: close
Upgrade-Insecure-Requests  1
```

Response:

```
HTTP/1.1 302 Found
Date: Tue, 17 Apr 2018 08:56:04 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-XSS-Protection: 1; mode=block
X-Request-Id: 8af904c1-85e7-4191-aeb5-d0f7fa85176c
X-Runtime: 0.016703
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; img-src 'self' data ;
script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self'
'unsafe-inline'
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Set-Cookie: _session_id=090b9c4b9e62545731385a30e452a52b;Secure;
domain=.digid.nl; path=/; HttpOnly
Location:  ****SNIP*****
```

Request rda-a3.digid.nl

```
GET / HTTP/1.1
Host: rda-a3.digid.nl
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
ETag: W/"13-1488876285000"
Last-Modified: Tue, 07 Mar 2017 08:44:45 GMT
Content-Type: text/html
Content-Length: 13
Date: Thu, 19 Apr 2018 12:06:32 GMT
Connection: close
Set-Cookie:
_persist=!2w5RctvWRVH6h0sZzh+/BjbEK230wfgaMttx7RNjjpnoeQdp2Mpfk1xRY+Bg
DfTQag49aI1zvKu/m7aJg243bUdTXYhfj30Oijb3HWg=;domain=.digid.nl;
HttpOnly;secure; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

<html></html>
```

4.1.5 *Wachtwoordsterkte onvoldoende*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.5	Nnb	Zeer laag	Zeer laag	Zeer laag

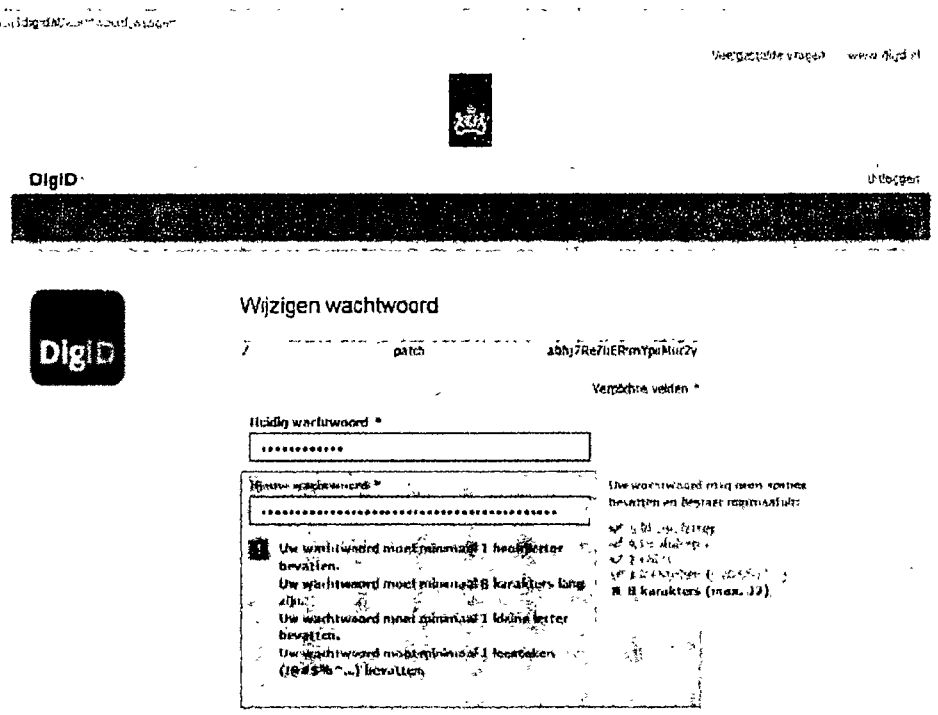
Betreffende host
a3.digid.nl
mijn.a3.digid.nl

Omschrijving
De eisen die door de applicatie aan het wachtwoord van de gebruiker gesteld worden zijn niet veilig genoeg.

Bedreiging
Zwakke wachtwoorden zouden door middel van een bruteforce attack kunnen worden 'gekraakt'.

Aanbeveling
Door eisen te stellen aan de kwaliteit van wachtwoorden, wordt de kans kleiner dat ze kunnen worden 'gekraakt'. Het wachtwoord van een applicatie zou voldoende sterk moet zijn om een bruteforce attack te weerstaan. De bepalende factor hierin is de lengte en niet de gebruikte tekenset. Indien relatief korte wachtwoorden een vereiste of toegestaan zijn, dan zouden deze bijvoorbeeld ten minste moeten bestaan uit een combinatie van een kleine letter, een hoofdletter, een cijfer en/of een leesteken om de gebruikte tekenset zo groot mogelijk te maken.

Details
De minimumlengte van een wachtwoord is 8 tekens en het is aanbevolen om de minimumeis op te hogen naar 12 tekens. Daarnaast is niet aanbevolen om een maximum aan de wachtwoordlengte te stellen, want dat ontneemt de gebruiker om gebruik te maken van pass phrases.



4.1.6 *Onvoldoende invoervalidatie Daring Fireball markup*

ID	Mantis nr. Clientele nr.	Risico op misbruik	Kans op misbruik	Impact op misbruik
5.6.7	Nnb	Laag	Zeer Laag	Laag

Betreffende hosts

digidbeheer-a3.digid.nl

Omschrijving

De website maakt gebruik van Daring Fireball markup. Hierbij worden de speciale combinaties van deze markup door de server onvoldoende gevalideerd.

Bedreiging

Het is mogelijk om via deze opmaaktaal een afbeelding toe te voegen aan een pagina. Dit kan ook een afbeelding zijn op een ander domein dat *.digid.nl. Ook kan er een URL gebruikt worden die helemaal geen afbeelding is. Wanneer een gebruiker de pagina vervolgens bezoekt wordt deze URL door de browser aangeroepen. Dit kan bijvoorbeeld gebruikt worden om een CSRF-kwetsbaarheid op een andere website te misbruiken.

Aanbeveling

Zorg ervoor dat alle invoer door de server wordt gecontroleerd en gevalideerd voordat deze wordt verwerkt, opgeslagen of getoond. Controleer of het nodig is dat er afbeeldingen kunnen worden ingeladen van andere domeinen dan het DigiD-domein.

Details