Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Raad van State
Afdeling IT-beheer
t.a.v. [redacted]
Postbus 20019
2500 EA Den Haag

10,2.e

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag

Inlichtingen
[redacted]
T 06 [redacted]
[redacted]@minfin.nl

10,2,e

Ons kenmerk
ADR/2015/1105

Uw brief (kenmerk)
-

Bijlage
1

Datum 30 juli 2015
Betreft Hertoets norm B5-3 betreffende de DigiD ICT-beveiligingsassessment Raad van State over het jaar 2014

Geachte [redacted]

10,2,e

Hierbij doen wij u de resultaten van de hertoets toekomen ter zake van de eerder uitgevoerde DigiD ICT-beveiligingsassessment over het jaar 2014 op de DigiD-aansluiting – nr. 642024 - 'Digitaal Loket' van de Raad van State naar de stand per 29 april 2015.

Het onderzoek heeft plaatsgevonden zoals met u op 15 juli 2015 mondeling is overeengekomen. Wij hebben ons ter zake gericht op het vaststellen van het daadwerkelijk bestaan van de door de Raad van State geïmplementeerde technische beveiligingsmaatregelen in de ICT-voorziening 'Digitaal Loket', teneinde te voldoen aan de gestelde eis van norm B5-3 uit de DigiD ICT-beveiligingsrichtlijn van Logius.

Wij willen u en uw collega's danken voor het vertrouwen in ons en voor de prettige samenwerking gedurende het onderzoek.

De rapportage dient u zo spoedig mogelijk aan Logius te sturen.

Met vriendelijke groet,

[redacted]

10,2,e

Auditdienst Rijk
Directeur ADR

Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Raad van State
Afdeling IT-beheer
t.a.v. [redacted] 10,2,e
Postbus 20019
2500 EA Den Haag

Auditdienst Rijk
Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Inlichtingen
[redacted]
T 070-[redacted] 10,2,e
[redacted]@minfin.nl

Ons kenmerk
ADR/2015/1105

Uw brief (kenmerk)
-

Bijlagen
Geen

Datum: 29 juli 2015
Betreft: Hertoets van norm B5-3 ter zake van de eerder uitgevoerde DigiD ICT-beveiligingsassessment over het jaar 2014, naar de stand per 29 april 2015, over de aansluiting van het 'Digitaal Loket' van de Raad van State.

Met het assurancerapport met kenmerk ADR-2015-690, d.d. 29 april 2015, is invulling gegeven aan het uitvoeren van een onderzoek naar het voldoen aan het normenkader zoals beschreven in de 'Norm ICT-beveiligingsassessments DigiD' van Logius. De daarin gestelde normen die een oordeel "voldoet niet" bevatten zijn voor Logius aanleiding geweest om van de aansluitende organisaties een hertoets van de betreffende normen te verlangen. In voornoemd assurancerapport gold dat voor de norm B5-3.
Logius heeft in haar brief (met kenmerk Logius/2015/U004088) van 11 juni 2015 aan de Raad van State verzocht maatregelen te treffen teneinde uiterlijk op 11 oktober 2015 aan deze gestelde norm uit de DigiD ICT-beveiligingsrichtlijn te voldoen.

De Raad van State heeft (na de uitkomsten van de ICT-beveiligingsassessment over het jaar 2014) intern een verbeterplan opgesteld, hetwelk in de maanden mei en juni 2015 heeft geresulteerd tot het implementeren van de benodigde technische beveiligingsmaatregelen in het 'Digitaal Loket'.
Op verzoek van de Raad van State is in de week van maandag 13 juli 2015 door de Auditdienst Rijk een hertoets uitgevoerd op voornoemde norm die onderdeel uitmaakt van de DigiD ICT-beveiligingsrichtlijn. Hieronder is de uitkomst van deze werkzaamheden voor norm B5-3 nader beschreven en voorzien van een oordeel.

Maatregel nummer:	Omschrijving
B5-3	Sla gevoelige gegevens versleuteld of gehashed op.

Opzet en bestaan	
Korte omschrijving van uitgevoerde werkzaamheden:	*Tijdens de DigiD ICT-beveiligingsassessment over het jaar 2014, naar de stand per 29 april 2015, is vastgesteld dat HTML- en PDF-A bestanden ten behoeve van het 'Digitaal Loket' op één van de 'Digitaal Loket' servers in de DMZ-omgeving worden bewaard.* [redacted] *) is afkomstig vanuit het bedrijfsproces van de Raad van State (eis van onweerlegbaarheid). Deze vastleggingen vormen voor de Raad Van State een mogelijk bewijs omtrent het 'onweerlegbare gebruik' van het 'Digitaal Loket' door de rechtzoekende op basis waarvan de ontvankelijkheid van de rechtzoekende in voorkomende gevallen door de Raad kan worden beoordeeld.* Ondervraging en observatie: interviews en waarneming ter plaatse met de verantwoordelijke functionarissen en beheerders. Schriftelijke documentatie: beoordeling van de doorgevoerde- en goedgekeurde Request for Change (kenmerk W01068 d.d. 18 mei 2015) met betrekking tot het [redacted] opslaan van BSN-nummers in de samengestelde bestandsnamen van de gegeneerde HTML- en PDF-A bestanden op de 'Digitaal Loket' –server in de DMZ-omgeving. Op de onderhavige server is door waarneming ter plaatse door ons op 15 juli 2015 vastgesteld dat per 17 juni 2015 hashing van BSN-nummers van de gegenereerde bestandsnamen, overeenkomstig het gestelde van norm B5-3, plaatsvindt.
Oordeel:	**Voldoet**

10,1,b + 10,2,g

10,1,b + 10,2,g

Bronnen (namen van documenten, bestanden, screen prints, enz.)
1a. Change (RfC) kenmerk W01068 Digitaal Loket, d.d. 18 mei 2015
1b. Diverse emailberichten inzake oplossingsrichtingen versus eisen business
1c. Printscreen 'Digitaal Loket' server per 17 juni 2015 met hashing van HTML- en PDF-A bestanden
1d. Printscreen source code aanpassing (gedeeltelijk) [redacted]

Ons kenmerk
ADR/2015/1105

10,1,b + 10,2,g

In deze gerichte follow-up audit is het bestaan van norm B5-3, naar de stand per 15 juli 2015, voldoende bevonden.

In de DigiD ICT-beveiligingsassessment over het jaar 2015 zullen de opzet en het bestaan voor deze norm worden geëvalueerd.

Datum:	29 juli 2015
Naam:	[redacted]
Organisatie:	Auditdienst Rijk – Ministerie van Financiën
Handtekening:	[redacted]

10,2,e

10,2,e