Ministerie van Economische Zaken

Taskforce eHerkenning

eOvB

Prinses Beatrixlaan 2
2595 AL Den Haag
www.rijksoverheid.nl/ez

**Contactpersoon**

*Prowductowner Identificatie en autheticatie*

# memo

Calamiteitenoefening eHerkenning

**Datum**
14 januari 2019

**Kopie aan**
nvt

**Bijlagen**
2

## Evaluatie e-Herkenning ketenoefening TenderNed en eCert

Aanleiding voor de oefening is de Wet digitale overheid (Wet do), die het gebruik van erkende inlogmiddelen zoals eHerkenning verplicht stelt. Het gebruik van andere (eigen) middelen is dan niet meer toegestaan. Dit betekent dat RVO applicaties als TenderNed en eCert deze middelen die als fallback beschikbaar zijn niet meer mag gebruiken. Hierdoor ontstaat een exclusieve afhankelijkheid van eHerkenning voor de dienstverlening door deze applicaties. Doel van de oefening is om in kaart te brengen wat de gevolgen zijn van uitval van (een van de partijen) binnen eHerkenning.

## Dienstverlening van TenderNed en eCert

Bedrijven kunnen alleen via *TenderNed* inschrijven op nationale en Europese aanbestedingen. Het gaat jaarlijks om in totaal ruim 73 miljard euro, waarbij meer dan 70.000 leveranciers betrokken zijn. Het betreft jaarlijks ongeveer 10.000 aanbestedingen, die op meerdere dagen per week vaste momenten sluiten (kluissluitingen) .  Als bedrijven niet voor sluiting hebben kunnen inschrijven door een storing kan dit tot grote schadeclaims leiden.

Voor het exporteren van dierlijke producten, levensmiddelen, planten en groenten is een exportcertificaat nodig van de *eCert*, onderdeel van de NVWA. Een dergelijk certificaat is voor een exporteur cruciaal, aangezien een product anders niet in het desbetreffende land mag worden ingevoerd. De te exporteren goederen vertegenwoordigen vaak grote waarde.
Ongeveer 5.000 bedrijven maken regelmatig van eCert gebruik.

## Opzet van de oefening



De oefening richtte zicht op de verdeling van taken, bevoegdheden en verantwoordelijkheden bij een storing binnen eHerkenning.

Belangrijke vragen daarbij zijn:

- Wie informeert wie?
- Wie neemt eigenaarschap van de storing?
- Hoe houden de partijen elkaar op de hoogte van de voortgang?
- Welke gevolgen heeft het voor de eindgebruiker?
- Welke maatregelen kan je nog treffen na invoering van de Wet Digitale Overheid (WDO)?

Initieel zouden alle partijen betrokken worden: crisisstaf RVO en Crisisstaf EZ, IB-coördinatoren TenderNed, RVO.nl en DICTU, Directeur RVO, directeur Nationale Programma's en DG-ETM/MC. Gedurende de voorbereiding bleek het niet te lukken om alle partijen te betrekken in de oefening, daarmee kwam in de oefening meer de nadruk te liggen op het operationeel-tactisch niveau.

Uiteindelijke deelnemers waren:

- Coördinator calamiteiten/procesbewaker TenderNed
- Manager PIANOo
- Chief Product Owner TenderNed
- Informatiebeveiliging
- Communicatieadviseur PIANOo-TenderNed
- DICTU Servicemanager TenderNed
- DICTU Servicemanager DICTU TVS
- Manager eOvB
- Directie Klant, Advies en Informatie
- Product owner eOvB
- Functioneel beheerder eOvB
- Functioneel beheerder e-Certis NVWA
- Vertegenwoordiger Digidentity (middelenleverancier en eHerkenningsmakelaar)

De nadruk tijdens de oefening lag niet op het oplossen van de storing, maar op de communicatie, informatiedeling en het storingsproces. Daarbij hebben de deelnemers ook gebruik gemaakt van een app.
Bij de oefening zijn de betrokken partijen (vertegenwoordigers van TenderNed; RVO eOvB; DICTU TVS en; NvWA) vanaf hun werkplek geïnformeerd over een storing die eindgebruikers ervaarden bij het gebruik maken van e-Herkenning als inlogmiddel voor onder andere TenderNed en e-certNL. Via de verschillende partijen moesten de deelnemers uitzoeken waar het probleem zat en bij wie ze welke acties konden neer leggen. Enkele schakels binnen de keten werden gesimuleerd via een responscel (o.a. de servicedesken, media, eindgebruikers, e-herkenningsmakelaars en middelenleveraniers) door vertegenwoordigers van TenderNed, DICTU, eOvB en Digidentity.

De oefening duurde twee uur. Enkele eindgebruikers klagen bij de servicedesk van TenderNed en NVWA over problemen met het bereiken van de dienst. Ogenschijnlijk lijkt het probleem bij TenderNed en de NvWA te zitten. Gedurende het eerste uur blijkt dat het probleem bij eHerkenning zit. In het tweede uur blijkt dat er een storing bij een middelenleverancier de oorzaak is. De RVO-onderdelen worden geconfronteerd met druk vanuit eindgebruikers, bestuurders en politiek.

**Bevindingen**

- Er is een mis-match in de keten tussen de escalatietijd die TenderNed hanteert (bijgevoegd) en de SLA die geldt tussen de eindgebruiker (ondernemer) en de middelenleverancier (storingstijd van 4 uur). Daarnaast gaat deze tijd pas lopen vanaf het moment dat het probleem wordt gesignaleerd bij de middelenleverancier. Eén kluissluiting kan al een enorm probleem zijn voor TenderNed.

- In de toekomst gaat het aantal gebruikers omhoog, de ‘achterdeuren’ worden medio 2019 dichtgezet en daarmee groeit de wens om een hogere snelheid te ontwikkelen van escalaties en interventies.

- Er is binnen RVO te weinig zicht op de status van de dienstverlening door eHerkenning. Het is voor RVO-onderdelen van belang om eerder dan eindgebruiker te weten dat er een storing is. In de oefening speelde de crisis alleen bij RVO.nl, maar een dergelijke storing heeft impact op alle eHerkenning partijen/gebruikers, bij elk onderdeel van de overheid.

## Oplossingsrichtingen

- Een optie is ondernemers te adviseren meerdere inlogmiddelen aan te schaffen. Dat advies is ook al uitgedragen, maar krijgt in de praktijk weinig tot geen opvolging.

- Een “versnelde overstap procedure” (naar een andere middelenleverancier). De NVWA geeft aan dat zij denken “in minuten”, ook een spoedprocedure duurt minimaal een uur en dat is ook al te lang. .

- Er is behoefte aan het melden van een storing bij (een van de partijen binnen) eHerkenning. Dit bijvoorbeeld door een RFC in te dienen. Dit scheelt waarschijnlijk veel meldingen en is ook dienstverlening voor eindgebruikers.

- Monitoring, escalatie en oplossingen (bij keten brede storingen) als verantwoordelijkheid beleggen bij één “toezichthouder” of “eigenaar”. Er is centrale coördinatie nodig vanwege het vroegtijdig kunnen oppikken van early-warning-signals om daarmee schade te beperken.

- Eindconclusie is dat zowel bij de NVWA en TenderNed er behoefte blijft aan een achterdeur, omdat op teveel plekken het nog mis kan gaan en er geen (volledige) redundantie is.

Afsprakenstelsel Eletronische Toegangsdiensten/service level (https://afsprakenstelsel.etoegang.nl.)

*Classificatie van incidenten*

*Incident*

Een gebeurtenis die niet tot de standaardoperatie van een elektronische toegangsdienst behoort en die mogelijk impact c.q. risico oplevert ten aanzien van de kwaliteit, beschikbaarheid, integriteit en/of vertrouwelijkheid van (informatie binnen) het afsprakenstelsel. Incidenten kunnen bijvoorbeeld gaan om

- Verstoringen: dit zijn gebeurtenissen die er toe leiden dat (onderdelen van) de dienstverlening van eHerkenning/Idensys beperkt of niet beschikbaar zijn;
- Informatiebeveiligingsincidenten: waaronder verlies van USB stick, laptop, losse harde schijf en ook signaleringen van hackpogingen, pogingen tot binnendringen in het systeem of malware;
- Fraude of vermoeden van fraude door bijvoorbeeld een medewerker of hacker.

*Calamiteit*

Een incident waarvoor aan één van de volgende voorwaarden is voldaan:

- Verwachte verstoringsduur overstijgt de afgesproken Responsetijden binnen het Beschikbaarheidsvenster;
- Betrokkenheid van tenminste twee deelnemers;
- Directe en ernstige hinder;
- Impact op vertrouwelijkheid en integriteit;
- Meldplichtig datalek als bedoeld in de Meldplicht datalekken.

*Crisis*

Een incident waarvoor aan één van de volgende voorwaarden is voldaan:

- De calamiteit heeft een grote impact op de uitstraling/imago van eHerkenning/Idensys en het

vertrouwen van bedrijven en overheidsdienstverleners in het stelsel;
- De verwachte verstoring i.e. onbeschikbaarheid van het stelsel duur langer dan 48 uur;
- Bij de calamiteit spelen politieke beslissingen/implicaties;
- De calamiteit betreft een fundamentele juridische of technische kwetsbaarheid (dus betrekking hebbend op opzet of structuur van Elektronische Toegangsdiensten).

*Responsetijden*

Voor de verschillende activiteiten van de Deelnemers, Beheerorganisatie en BSNk kunnen andere responsetijden gelden.

| | |
|---|---|
| Voor Ondersteuning: | Ontvangstbevestiging binnen 4 werkuren<br>Oplossing/antwoord binnen 5 werkdagen |
| Afhandeling van incidenten: | Oplossing binnen 4 uur |

*Melden van incidenten*

Elke deelnemer moet incidenten direct na ontdekking melden bij (de incident manager van) de beheerorganisatie.