



Samenwerkingsprotocol Logius – Agentschap Telecom

Partijen:

Agentschap Telecom, vertegenwoordigd door de Directeur - Hoofdinspecteur mr. drs. P.A. Spijkerman, verder te noemen: AT.

en

De Minister van Binnenlandse Zaken en Koninkrijksrelaties, vertegenwoordigd door de directeur Logius, de heer dr. ir. R. Papenhuijzen, verder te noemen: Logius.

Achtergrond:

- Bij elektronisch (berichten)verkeer kan gebruik gemaakt worden van certificaten die kunnen worden gebruikt bij het bezoeken van beveiligde websites, het controleren van elektronische ondertekening van berichten of documenten of het bekijken van versleutelde informatie en zorgen voor een veilige uitwisseling van informatie;
- Een vanuit de Nederlandse overheid geïnitieerd en afgegeven certificaat is PKIoverheid (Staat der Nederlanden Root CA);
- PKIoverheid certificaten ondersteunen de functies authenticatie (controleren van identiteit), elektronische handtekeningen en versleuteling van informatie;
- PKIoverheid gekwalificeerde certificaten worden aangeboden door gekwalificeerde verleners van vertrouwensdiensten;
- Bij het toezicht op de naleving van voorschriften en vereisten voor de uitgifte van deze gekwalificeerde PKIoverheid certificaten zijn AT en Logius in verschillende rollen betrokken;
- AT is belast met het wettelijk toezicht op in Nederland gevestigde verleners van vertrouwensdiensten (hierna: TSP's) en de registratie van in Nederland gevestigde verleners van vertrouwensdiensten die (gekwalificeerde) certificaten aan het publiek aanbieden;
- Logius is belast met het ondersteunen van de elektronische dienstverlening aan burgers en bedrijven door de noodzakelijke infrastructurele basisvoorzieningen van PKIoverheid te beheren en verder te ontwikkelen en er op toe te zien dat de TSP's voldoen aan het Programma van Eisen (PvE) waarin de normen van het PKIoverheid afsprakenstelsel staan opgenomen waar een toetredende TSP aan moet voldoen;
- Ten behoeve van het toezicht op de regelnaleving door de TSP's, is een goede samenwerking vereist tussen AT en Logius;
- Logius een gelijksoortig samenwerkingsprotocol heeft afgesloten met de Autoriteit Consument en Markt (ACM) en dit nieuwe samenwerkingsprotocol het bestaande samenwerkingsprotocol zal vervangen als AT de toezichthoudende rol van ACM heeft overgenomen;
- Per 1 juli 2016 is de Autoriteit Consument en Markt (ACM) aangewezen als tijdelijk toezichthouder¹. In de periode tussen 1 juli 2016 en de inwerkingtreding van de Uitvoeringswet EU-verordening elektronische identiteiten en vertrouwensdiensten² worden ingevolge werkafspraken tussen ACM en AT, meldingen (namens ACM) bij AT in ontvangst genomen;

¹ Artikel 2 lid 1 van het Besluit van de Minister van Economische Zaken tot tijdelijke aanwijzing van een toezichthoudend orgaan, 29 juni 2016, NR WJZ / 16094083.

² Het bij koninklijke boodschap van 17 februari 2016 ingediende voorstel van wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) (Stb. 2017, nr. 13).



- Op het moment dat de Uitvoeringswet EU-verordening elektronische identiteiten en vertrouwensdiensten in werking is getreden is de Minister van Economische Zaken, uitgevoerd door AT de toezichthouder;
- Dit protocol regelt de samenwerking tussen AT en Logius.

Kernbegrippen:

· Public Key Infrastructure (PKI):

Een stelsel van afspraken, technologieën en partijen dat ten doel heeft om betrouwbare versleuteling van elektronisch gegevensverkeer mogelijk te maken door de relatie te waarborgen tussen een publieke sleutel en de identiteit van diens eigenaar.

Een publieke sleutel of public key is een voor iedereen toegankelijke code met behulp waarvan gegevens versleuteld respectievelijk ontcijferd kunnen worden. Deze gegevens kunnen alleen ontcijferd worden c.q. versleuteld zijn met de corresponderende geheime sleutel, die alleen de eigenaar van het sleutelpaar kent.

· PKIoverheid:

Een Public Key Infrastructure die de Rijksoverheid heeft ingericht en onderhoudt.

PKIoverheid heeft primair de verlening van certificaatsdiensten aan overheidsorganisaties ten doel, maar ook private partijen kunnen PKIoverheid certificaten gebruiken.

Het PKIoverheid stelsel kent vooralsnog certificaten die kunnen worden gebruikt bij:

- Het zetten van een elektronische handtekening gebaseerd op een gekwalificeerd certificaat;
- Het authenticeren en versleutelen van websites;
- Het op afstand authenticeren van personen of services;
- Het versleutelen van berichten.

· Policy Authority:

De Policy Authority (PA) van de PKI voor de overheid (PA PKIoverheid) ondersteunt de Minister van Binnenlandse Zaken en Koninkrijksrelaties bij het beheer over de PKI voor de overheid. Een van de taken van de PA PKIoverheid is om te controleren dat de eisen van PKIoverheid worden nageleefd door de toetredende TSP's en het controleren van de werkzaamheden van TSP's die onder de root van de PKI voor de overheid certificaten uitgeven. Logius is de PA PKIoverheid.

· Gekwalificeerde certificaten:

Een digitaal certificaat dat voldoet aan de vereisten die bij en krachtens de eIDAS verordening³ en de Telecommunicatiewet, zoals gewijzigd in de Uitvoeringswet EU-verordening elektronische identiteiten en vertrouwensdiensten, worden gesteld. Dit zijn eisen aan het certificaat zelf en eisen aan de wijze van uitgifte.

· TSP of verlener van vertrouwensdiensten:

Een natuurlijke persoon of rechtspersoon die een of meer gekwalificeerde of niet-gekwalificeerde vertrouwensdiensten verleent. In de eIDAS verordening, de Telecommunicatiewet en afgeleide regelgeving wordt deze aangeduid als verlener van vertrouwensdiensten (Trust Service Provider of TSP).

In het kader van PKIoverheid kan de TSP diensten verlenen in verband met de beveiliging van websites, authenticatie op afstand, elektronische handtekeningen en de versleuteling van elektronische berichten.

³ Verordening (EU) Nr. 910/2014 Europees Parlement en de Raad, 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.



· Calamiteit:

Een gebeurtenis die de bedrijfsvoering zodanig in gevaar kan brengen dat daardoor de continuïteit van één of meerdere vertrouwensdiensten in gevaar komt.

· Incident:

Een gebeurtenis die geen onderdeel uitmaakt van de standaardwerking van een vertrouwensdienst en die een onderbreking van, of een reductie in, de kwaliteit van die vertrouwensdienst veroorzaakt of kan veroorzaken.

· Security Breach:

Een inbreuk op de veiligheid en/of integriteit van een informatiesysteem, die een aanzienlijk effect op één of meer vertrouwensdiensten heeft.

Inleiding:

- Verleners van vertrouwensdiensten (TSP's) die gekwalificeerde certificaten aanbieden moeten voldoen aan eIDAS verordening en de relevante bepalingen in de Telecommunicatiewet, ter uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten⁴ (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten).
- TSP's die zijn toegetreden tot PKIoverheid, zijn verplicht aan de vereisten uit het Programma van Eisen van de PA PKIoverheid te voldoen. Op grond van dit Programma controleert Logius als PA PKIoverheid de naleving van deze vereisten door de TSP's.
- Artikel 21 lid 1 e-IDAS verordening stelt voor het aanbieden van gekwalificeerde vertrouwensdiensten dat indien verleners van vertrouwensdiensten die niet over de status gekwalificeerd beschikken de intentie hebben gekwalificeerde vertrouwensdiensten te gaan leveren, zij bij het toezichthoudend orgaan een kennisgeving van hun voornemen in moeten dienen. Artikel 2.5b lid 1 en 2 van de Telecommunicatiewet stelt dat een mededeling van een verlener van vertrouwensdiensten aan de Minister van Economische zaken waaruit het voornemen tot het verlenen van gekwalificeerde vertrouwensdiensten blijkt, wordt aangemerkt als een aanvraag tot toekenning van de status gekwalificeerd aan die verlener en de door hem in die mededeling aangeduide vertrouwensdiensten. AT als onderdeel van het Ministerie van Economische Zaken neemt een aanvraag niet in behandeling, indien de aanvrager buiten Nederland gevestigd is.
- AT houdt toezicht op in Nederland gevestigde verleners van vertrouwensdiensten.
- Voor controle op naleving van de gestelde eisen door de toegetreden TSP's tot PKIoverheid wordt door AT en Logius onder andere gebruik gemaakt van de jaarlijkse surveillance of controle audits van TSP's door geaccrediteerde conformiteitbeoordelingsinstanties, informatie die Logius als PA PKIoverheid opvraagt bij de toegetreden TSP's en informatie die wordt verzameld tijdens controle op locatie.
- Samenloop van bevoegdheden/verantwoordelijkheden tussen Logius en AT doet zich voor bij het toezicht op TSP's die vertrouwensdiensten aanbieden en toegetreden zijn tot PKIoverheid.

⁴ Het bij koninklijke boodschap van 17 februari 2016 ingediende voorstel van wet tot wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten (uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten) (Stb. 2017, nr. 13).



Samenwerkingsprotocol

Artikel 1 Samenwerking en het aanleveren van informatie

1. Logius en AT staan elkaar op verzoek of, voor zover nodig ambtshalve, met raad en daad bij. Zij overleggen met elkaar over de uitleg van wettelijke begrippen.
2. Logius en AT informeren elkaar over en weer tijdig over een incident en/of een calamiteit en/of een security breach en reageren zo spoedig mogelijk op een verzoek tot bijstand.
3. Logius en AT verstrekken schriftelijk dan wel mondeling elkaar de benodigde informatie in het belang van een te verrichten onderzoek, voor zover de bedrijfsvertrouwelijkheid van informatie daarbij niet geschaad wordt en binnen het kader van de uitvoering van de aan de partijen toegewezen taken en (wettelijke) bevoegdheden en verplichtingen.
4. In het geval zowel Logius als AT voornemens zijn op te treden tegen een TSP in het kader van PKIoverheid, wordt dit optreden onderling afgestemd voor zover dit binnen het kader van de uitvoering van de aan de partijen toegewezen taken en (wettelijke) bevoegdheden en verplichtingen mogelijk is.
5. Logius en AT treden in het kader van hun respectievelijk controlerende en toezichthoudende rol op de TSP's voorafgaand aan beslissingen, resultaten of overige mededelingen waar nodig in overleg en overigens informeren zij elkaar.

Artikel 2 Overleg

1. Logius en AT wijzen beide een contactpersoon aan die primair optreedt als aanspreekpunt voor de uitvoering van dit protocol.
2. Ieder kwartaal, of zoveel vaker als nodig is, vindt overleg plaats tussen - in ieder geval - de contactpersonen van Logius en AT over lopende zaken.
3. De directeur van Logius en de verantwoordelijk manager binnen AT bespreken in elk geval jaarlijks de stand van zaken betreffende de uitvoering van dit protocol en de samenwerking tussen Logius en AT.

Artikel 3 Publiciteit

1. Logius en AT publiceren dit protocol op hun websites.
2. Logius en AT informeren elkaar en stemmen voor zover nodig onderling af over de publicatie van beslissingen, resultaten of overige mededelingen die betrekking hebben op TSPs in het kader van PKIoverheid voor zover dit binnen het kader van de uitvoering van de aan de partijen toegewezen taken en (wettelijke) bevoegdheden en verplichtingen mogelijk is.

Artikel 4 Aanpassingen en wijzigingen

1. Logius en AT kunnen in onderling overleg op grond van bijzondere omstandigheden besluiten om af te wijken van de afspraken in dit protocol.
2. Dit protocol kan in onderling overleg tussentijds worden aangepast of aangevuld en zal in overeenstemming worden gebracht met eventuele wetwijzigingen.

Artikel 5 Inwerkingtreding, evaluatie en werkingsduur

1. Dit samenwerkingsprotocol heeft een werkingsduur van één jaar en treedt in werking met ingang van de dag dat AT de toezichthoudende rol van ACM heeft overgenomen wat plaatsvindt op het moment dat de Uitvoeringswet EU-verordening elektronische identiteiten en vertrouwensdiensten in werking treedt.
2. Evaluatie van het protocol vindt plaats in het overleg, genoemd in artikel 2, derde lid, van dit protocol.



3. Als dit protocol niet schriftelijk en tenminste zes maanden voor de vervaldatum wordt opgezegd door één der partijen, wordt het geacht te zijn verlengd met één jaar onder dezelfde voorwaarden.

Ondertekening

Aldus overeengekomen in tweevoud

Datum: 25-4-2017
Logius,

Dr. ir. R. Papenhuijzen
Directeur

Datum: 20 maart 2017
Agentschap Telecom,

mr. drs. P.A. Spijkerman
Directeur-Hoofdinspecteur

Relevante regelgeving

- eIDAS verordening (Verordening (EU) Nr. 910/2014 Europees Parlement en de Raad, 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG);
- Besluit vertrouwensdiensten;
- Relevante bepalingen in de Telecommunicatiewet in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten;
- Regeling vertrouwensdiensten;
- Besluit aanwijzing toezichthouders Telecommunicatiewet;
- Instellingsbesluit baten-lastendienst Logius 2010.