Change 425 definitief (SPOED)

Changemanagement Programma van Eisen PKIoverheid

Feb 20, 2020

<table>
<tr><td>Oorspronkelijke datum indiening</td><td>20 Jan 2020</td></tr>
<tr><td>Extern opgelegd</td><td>Ja</td></tr>
<tr><td>Indiener</td><td>Mozilla</td></tr>
<tr><td>Auteur voorstel</td><td>Jochem van den Berge</td></tr>
<tr><td>Spoed</td><td>Ja</td></tr>
<tr><td>Toepassing</td><td>
<table>
<tr><td>PvE Deel 1: Introductie</td><td></td><td>PvE deel 3d: Autonome Apparaten</td><td>√</td></tr>
<tr><td>PvE deel 2 Algemene eisen aan TSP's</td><td></td><td>PvE deel 3e: Server</td><td>√</td></tr>
<tr><td>PvE Deel 3: Basiseisen</td><td></td><td>PvE deel 3f: Extended Validation</td><td>√</td></tr>
<tr><td>PvE Deel 3: Aanvullende Eisen</td><td></td><td>PvE deel 3g: Private Services</td><td>√</td></tr>
<tr><td>PvE deel 3a: Organisatie Persoon</td><td>√</td><td>PvE deel 3h: Private Server</td><td>√</td></tr>
<tr><td>PvE deel 3b: Organisatie Services</td><td>√</td><td>PvE deel 3i: Private Personen</td><td>√</td></tr>
<tr><td>PvE deel 3c: Burger</td><td>√</td><td>PvE deel 4: Begrippenlijst</td><td></td></tr>
</table>
</td></tr>
<tr><td>Bestaande eis (zo ja, welke)</td><td>4.9.1-pkio52</td></tr>
<tr><td>Omschrijving verzoek</td><td>In Mozilla Policy 2.7 worden er nieuwe eisen c.q. verduidelijkingen gesteld aan de manier wanneer certificaten dienen te worden ingetrokken. Deze eisen komen momenteel niet tot uiting in het PvE PKIoverheid</td></tr>
<tr><td>Tekstvoorstel</td><td>Eis 4.9.1-pkio52 wordt alleen aangepast qua scope, deze is voortaan alleen maar van toepassing op delen 3g, 3h en 3i (Private)

Er komen twee nieuwe eisen, 4.9.1-pkio187en 4.9.1-pkio188.

eis 4.9.1-pkio187, van toepassing op delen 3a t/m 3d:
Certificaten zullen worden ingetrokken wanneer:
• de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleent met terugwerkende kracht ook geen toestemming;
• de TSP beschikt over voldoende bewijs dat de privésleutel van de abonnee (die behoort bij het corresponderende certificaat) is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel, SSCD, SUD of QSCD, gestolen of vermoedelijk gestolen sleutel, SSCD, SUD of QSCD of vernietigde sleutel, SSCD, SUD of QSCD indien van toepassing;</td></tr>
</table>

- een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft afgesloten;
- de TSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service);
- de TSP bepaald dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft gesloten;
- de TSP bepaald dat informatie in het certificaat niet juist of misleidend is;
- de TSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP;
- De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen).
- Indien er sprake is van 1 van de gebeurtenissen zoals beschreven in hoofdstuk 6.2 van de Mozilla Root Store Policy

eis 4.9.1-pkio188, van toepassing op delen 3e en 3f:

Certificaten zullen worden ingetrokken wanneer:

- de abonnee aangeeft dat het oorspronkelijke verzoek voor een certificaat niet was toegestaan en de abonnee verleent met terugwerkende kracht ook geen toestemming;
- de TSP beschikt over voldoende bewijs dat de privésleutel van de abonnee (die behoort bij het corresponderende certificaat) is aangetast of er is het vermoeden van compromittatie, of er is sprake van inherente beveiligingszwakheid, of dat het certificaat op een andere wijze is misbruikt. Een sleutel wordt als aangetast beschouwd in geval van ongeautoriseerde toegang of vermoede ongeautoriseerde toegang tot de private sleutel, verloren of vermoedelijk verloren private sleutel, SSCD, SUD of QSCD, gestolen of vermoedelijk gestolen sleutel, SSCD, SUD of QSCD of vernietigde sleutel, SSCD, SUD of QSCD indien van toepassing;
- een abonnee niet aan zijn verplichtingen voldoet zoals verwoord in deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft afgesloten;
- de TSP op de hoogte wordt gesteld of anderszins zich bewust wordt van een wezenlijke verandering in de informatie, die in het certificaat staat. Voorbeeld daarvan is: verandering van de naam van de certificaathouder (service);
- de TSP bepaald dat het certificaat niet is uitgegeven in overeenstemming met deze CP of het bijbehorende CPS van de TSP of de overeenkomst die de TSP met de abonnee heeft gesloten;
- de TSP bepaald dat informatie in het certificaat niet juist of misleidend is;

	• de TSP haar werkzaamheden staakt en de CRL en OCSP dienstverlening niet wordt overgenomen door een andere TSP; • De PA van PKIoverheid vaststelt dat de technische inhoud van het certificaat een onverantwoord risico met zich meebrengt voor abonnees, vertrouwende partijen en derden (b.v. browserpartijen). • Indien er sprake is van 1 van de gebeurtenissen zoals beschreven in hoofdstuk 6.1 van de Mozilla Root Store Policy. Hierbij dient de TSP zich te houden aan de termijnen voor intrekking zoals gesteld in hoofdstuk 6.1 van voorgaand document.
Impactanalyse	voor TLS/SSL zou dit weinig verschil moeten maken ten opzichte van huidige verplichtingen (daar dit voortkomt uit de al van kracht zijnde Baseline Requirements). Voor S/MIME is er sprake van een verzwaring (qua redenen voor intrekking) maar is er meer speelruimte daar Mozilla (en de PA) bewust geen termijnen specificeren op welke termijn certificaten moeten worden ingetrokken.
Argumentatie	Zie omschrijving.
Uitspraak Wijzigingenoverleg	SPOED
Uitspraak Stelseloverleg	SPOED
Uiterlijke datum effectuering wijziging	17 Feb 2020