Domeinen Organisatie (G2), Organisatie Persoon (G3)

Versie: 1.4
Datum: 01 November 2016
PvE 3a: 4.3

Inhoudsopgave

1 INTRODUCTIE OP CERTIFICATE POLICY 7

1.1 Achtergrond 7

1.2 Verwijzingen naar de CPS 7

1.3

1 Introductie op Certificate Policy

1.1 Achtergrond

1.5 CPS-beheer

x

t

3 Identificatie en Authentificatie

3.1 Naamgeving

3.1.1-1 Soorten naamformaten

t

3.1.3-1 Pseudoniemen

3.1.4 Geschillen

3.2 Initiële identiteitsvalidatie

3.2.2.1 verificatie Organisatie

t t

3.2.2.2 authenticatie Organisatorische eenheid

t t

3.2.3.1 Authenticatie van persoonlijke identiteit

3.2.5.1 Autorisatie van de certificaathouder

x

x

x

x

t

3.2.5.2 Verantwoordelijkheid Abonnee

3.3 Identificatie en Authenticatie bij vernieuwing van een Certificaat

3.3.1 Aanvraag tot vernieuwing

3.3.1.1 Hergebruik sleutels bij vernieuwing certificaat

3.3.1.2 Controle bij aanvraag vernieuwing certificaat

3.3.2 Hergebruik sleutels na intrekking certificaat

t

4.9.3.2 Beschikbaarheid intrekking management service

4.9.3.3 Vastlegging reden van intrekking

4.9.3.4 Certificaat status informatie

4.9.3.5 Beschikbaarheid intrekking management service

4.9.3.6 Geldigheid CRL

4.9.3.6 Issuing subordinatie CA

x

5.1.8 Externe backup

x

x

5.2 Procedurele Beveiliging

5.2.1 Risico analyse

5.2.2 audit externe organisaties

5.2.4.1 Vertrouwelidaarvoor

t

5.2.4.2 Aantal personen vereist per operationele handeling

t

t

x
x
x
x
x
x

x

x

x

t

x
x
x
x
x
x
x

5.5.2 Bewaarperiode voor het archief

5.5.3 Bescherming van het archief

5.5.4 Back-up procedures m.b.t. het archief

5.5.5 Eisen voor de time-stamping van gegevens

t

5.7 Aantasting en Continuïteit

s]• Z (š v ^]• •š Œ Z }À ŒÇ WŒ}PŒ uu _U À •šP o P]v Z š Yµ}

5.7.4.1 Continuïteit van de bedrijfsvoering na calamiteit

t

6 Technische beveiligingsmaatregelen

6.1 Generatie en installatie van het sleutelpaar

6.1.1 Sleutelpaar generatie

6.1.1.1 Genereren van sleutelparen voor de CSP sub CA

6.1.1.2 Genereren van sleutelparen van de certificaathouders

6.1.1.3 Algoritme van sleutelparen van de certificaathouders

6.1.2 Overdracht van private sleutel en SSCD aan certificaathouder

6.2 Private sleutel bescherming

6.2.1 Standaarden en controles van de cryptografische module (HSM)

6.2.2

6.2.9 Methoden voor deactivatie van de private sleutel

6.2.10 Methode voor de vernietiging van de private sleutel

6.2.11 Œ Ç ‰ š } P Œ ( ] • Z o • •] ( ] š] À v u } µ o v ^ ^ [•

6.2.111 Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen

6.2.112 Alternatieve eisen voor veilige middelen

t

x
x

6.3.2 Gebruiksduur van sleutels en eindgebruikercertificaten

6.4 Activeringsgegevens

6.4.1.1 Genereren en installeren van activeringsgegevens

6.4.1.2 Deblokkering van activeringsgegevens

6.5 Computerbeveiliging

6.5.1 Technische maatregelen inzake computerbeveiliging

x
x
x

x

x
x

t

6.7.1.2 Intern testen Netwerk beveiliging

6.7.1.3 Extern testen Netwerk beveiliging

t

7 Certificaatprofiel

7.1.1 Certificaatprofiel t Authenticiteitcertificaten

PKI Overheid User Authentication–QVO User Auth EKUs				

t

7.1.2 Certificaatprofiel t Handtekeningcertificaten

PKI Overheid User Authentication-QVO User QualSign				
/••µ Œ{ }µvšŒÇE u				
/••µ Œ{KŒP v]• š]}vE				
/••µ Œ{KŒP v]ì š]}vh				
/••µ Œ{ }uu}vE u				

t

8 Conformiteitbeoordeling

8.1 Certificatie en registratie bij OPTA

8.2 De verhouding van de auditor met de beoordeelde entiteit

8.3 Scope van de audit

x
x
x
x
x
x

8.4 Acties ondernomen vanwege deficiëntie

t

9 Algemene en juridische bepalingen

9.1 Tarieven

9.1.1

x

t

x

9.6.3 Aansprakelijkheid Vertrouwende Partijen

x

x

x

t

x

x

x

x

x

t

9.11 individuele kennisgeving en communicatie met betrokken partijen

o š Œ } v] • Z ‰ } • š U Œ] À v µ • ‰ } • š U (Æ v Á ‰ P] v [• Ì µ o o v • Z] l Œ

9.12 Wijziging

9.12.1 Wijzigingsprocedure

x
x

9.12.2 Notificatie van wijzigingen

t

Bijlage A t Definities en Afkortingen Tm 0 g 0 G [( )] TJ ET Q q 0.000008871 0 595

t