

Vr Gr 5.1.2e

-----Oorspronkelijk bericht-----

Van: 5.1.2e <5.1.2e@webweaving.org>

Verzonden: woensdag 2 september 2020 20:36

Aan: 5.1.2e <5.1.2e@dictu.nl>; 5.1.2e <5.1.2e@egeniq.com>; 5.1.2e <5.1.2e@dictu.nl>

Onderwerp: Varianten / HSM opties

Wat hebben we nog als vrijheden ?

Allereerst - heel zwaar inzetten voor coronamelder-api.nl op geen recoke voor einde jaar of 1-november - en vol in de aanval op KPN haar haastige willen 'ruimen'.

Dan het sig-cert.

Denk dat de vraag belangrijk wordt of we:

- a heel zeker weten dat we de bestaande priv-keys niet kunnen importeren ?

want als dat kan - dan versimpeld het probleem voorlopig een tot het verbieden van revoke door Logius.

Maar we verbeteren het beveiligingsniveau niet. Key was er buiten dus "window dressing".

Ook geen stap richting de toekomstige manier van werken en processen.

Dan de praktische opties:

- 1 Ceremonies pauzeren totdat de KPN aan het werk gaat.
- 2 Alleen testen met new-new en huidige ceremonies gewoon doorzetten.
bewust gekozen om 2 dingen te splitsen. HSM integratie en migreren naar nieuwe Root los van elkaar

En voorlopig het oud-oud op disk blijven gebruiken.

en tzt de oud-nieuw apart testen en doorlopen (maar nu al wel CSRs maken)/

=> dit is wat jij bedoelt 5.1.2e? Ik snap niet wat jij bedoelt *

- 3 op HSMs een tweede, self-signed, cert creëren - _of_ huidige CSR (ook) tekenen met eigen key in de HSM.

Deze pubkey -ook- inbouwen in de app. Te veel improvisatie en te complex tijdens de overgangs periode mag G3 en die specifieke pubkey en EV.

Dan overstappen - en als EV laat is - tussen stap via die self signed pubkey.

En daar aircover voor krijgen bij Logius & duidelijk als stap naar EV.

- 4 Iets doen met een commerciële CA
- 5 Iets doen via de NL private tree voor m2m.

maar dan moet je wel erg veel uitleggen qua CAB forum beloftes.

Zijn er nog meer plekken waar we ruimte hebben ?

5.1.2e

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.

De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.

The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.