To: 5.1.2e)[5.1.2e @dictu.nl]
From: 5.1.2e)
Sent: Thur 9/3/2020 8:44:48 AM
Subject: RE: Besluit in TOP overleg ?
Received: Thur 9/3/2020 8:44:48 AM

Dank. Ik acht Logius wel haalbaar

Van: 5.1.2e) < 5.1.2e @dictu.nl>
Verzonden: donderdag 3 september 2020 10:35
Aan: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: FW: Besluit in TOP overleg ?

Hallo 5.1.2e

Zie beneden; op verzoek van 5.1.2e doorgestuurd.

Vr Gr 5.1.2e

Van: 5.1.2e)
Verzonden: donderdag 3 september 2020 09:00
Aan: 5.1.2e < 5.1.2e >; 5.1.2e < 5.1.2e @egeniq.com>; 5.1.2e)
< 5.1.2e @dictu.nl>; 5.1.2e) < 5.1.2e @dictu.nl>; me@ 5.1.2e 5.1.2e)
< 5.1.2e @dictu.nl>
CC: 5.1.2e < 5.1.2e @icloud.com>; 5.1.2e < 5.1.2e >
Onderwerp: Besluit in TOP overleg ?

Hallo allen

Als we even de feiten zoals ze nu zijn op een rijtje zetten staan we hier.
We staan nu hier:

1. Snelste nieuw levering nieuw certificaat uit oude PKI-O Tree door KPN **11-9-2020**
2. TST-HSM integratie testen dan niet eerder dan 14-9-2020
3. ACC-HSM + 1 week (want ceremonie en key naar apple / google , doorlooptijd etc)
4. PRD-HSM + 1 week
5. Dus per 28-9-2020 begin van vervanging certificaten van oude tree/root naar nieuwe tree/root

➔ doorlooptijd weken

6. Per 30-9-2020 vervallen de certificaten uit de oude PKI-O Tree.

Ook DICTU is door QuoVadis op die manier de wacht aangezegd; wij moeten dit serieus nemen.
Een poging bij Logius te vragen of we langer door mogen met certificaten uit de oude PKI-O Tree is onzeker in de uitkomst.

Deze planning kan dus niet.

In simpele woorden de opties:

1. Volgorde wijzigen.

Traject van migreren naar certificaten uit de nieuwe Root eerst doen; HSM integratie later.
nadeel: Draaien op lager beveiligingsniveau (niveau van nu)
voordeel: Voorkom dat de CoronaMelder uit de lucht gaat omdat we niet tijdig overgegaan zijn naar de nieuwe PKI-O Tree.

2. HSM integratie anders doen.

Lager beveiligingsniveau kiezen en proberen sleutels te importeren.
Nadeel: window dressing en nog steeds het zwaard van Damocles rond de overgang naar de nieuwe PKI-O Tree en ook lager beveiligingsniveau en moet ook nog uitgezocht worden.

3. Logius overtijgen en zorgen dat de datum 30-9 van tafel gaat en dan dus gewoon volgens plan door.

Voordeel: plan gewoon doorvoeren.
Nadeel: onzeker of ze dit doen, Logius en KPN

Duidelijk ?

Ik denk optie 3 als het kan, anders helaas 1
In 2 zie ik niet veel

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 erbuiten dus "window dressing".
Ook geen stap richting de toekomstige manier van werken en processen.

Dan de praktische opties:

1 Ceremonies pauseren 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 creeren - _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