To: (10)(2e))[(10)(2e) @minvws.nl]; (10)(2e) [(10)(2e) @minbzk.nl]
From: (10)(2e)
Sent: Wed 9/2/2020 3:33:29 PM
Subject: Fwd: Verzoek om Dispensatie G3 certificaat tot 1 November ten behoeve van de CoronaMelder
Received: Wed 9/2/2020 3:33:42 PM

FYI. Wel even lezen!
(10)(2e)
+316 (10)(2e)

Begin forwarded message:

From: (10)(2e) <(10)(2e)>
Subject: Re: Verzoek om Dispensatie G3 certificaat tot 1 November ten behoeve van de CoronaMelder
Date: 2 September 2020 at 17:14:49 CEST
To: PKIoverheid <(10)(2e) @logius.nl>
Cc: "(10)(2e) " <(10)(2e) @logius.nl>, "(10)(2e) (10)(2e)) - Logius" <(10)(2e) @logius.nl>, "(10)(2e) " <(10)(2e) @logius.nl>, "(10)(2e))" <(10)(2e) @dictu.nl>, (10)(2e) <(10)(2e) @dictu.nl>, (10)(2e) <(10)(2e) @icloud.com>

(10)(2e)
Ter terugkoppeling & als vraag:

1) contact met juiste afdeling KPN is gelegd.

Men zegt uiterst resource constraint te zijn - maar hoopt eind volgende week in staat te zijn het CSR te kunnen signen.

Als dat gehaald wordt, is er net genoeg tijd voor migratie van de burger hun applicaties via de google/apple appstores voor 1 November. Want anders zal er een week(je) bij moeten.

Mocht de 1 November deadline erg belangrijk zijn voor de PKIOverheid - dan is het misschien goed dat KPN dit ook weet.

Want men leek dit als een vrij arbitraire datum te zien.

2) De KPN is zeer voortvarend haar klanten pro-actief aan het voorzien van nieuwe EV certificaten `out of the blue'. Daarvoor natuurlijk hulde.

Maar met de mededeling dat corresponderende G3 versie 4 weken na dagtekening actief wordt in getrokken.

Is dit in uw opdracht ? En zo ja - dan vrees ik dat we ook hiervoor dispensatie voor zullen moeten aanvragen; want dat is (ver) voor 1 November.

En met de vertraging bij KPN is dat al krap.

Want wij zullen minimaal 6 weken parallel moeten runnen om de upgrades in het veld toe te staan via de normale appstore routes.

Bedankt voor all hulp vandaag en met vriendelijke groet,

(10)(2e)

On 31 Aug 2020, at 14:23, (10)(2e) < (10)(2e) > wrote:

Dank voor dit bericht.
Onze TSP is KPN B.V. - de certificaten zijn geissued (en zouden dus genieuwd moeten worden) door

Issuer: C=NL, O=KPN B.V./organizationIdentifier=NTRNL-27124701, CN=KPN BV PKIoverheid Organisatie Server CA - G3

Wij zullen uw suggestie van M2M voor de toekomst meenemen; want in aanzet was ons opgelegd om te voldoen/te functioneren in het CAB Forum geleide stelsel.

De gesprekken om hier meer ruimte te krijgen zullen de nodige tijd in beslag nemen - want hier moet de EU en Google/Apple ook hun medewerking aan verleden/aanpassingen maken..

Ik denk wel dat we nu veel meer kans maken - nu we een goed voorbeeld hebben (want het is nu niet niet meer het wat theoretische verhaal van destijds - er is een voorbeeld).

Met vriendelijke groet,

(10)(2e)

On 31 Aug 2020, at 14:16, (10)(2e) < (10)(2e) @logius.nl > wrote:

Geachte heer (10)(2e), beste (10)(2e),

Hierbij verleent de Policy Authority (PA) PKIoverheid dispensatie aan het programma Digitale Ondersteuning Bestrijding COVID-19 met de mobiele app "CoronaMelder" om een aantal PKIoverheid G3 server certificaten voor de API, de distributie en de CDN in test/acceptatie en productie, te mogen laten tekenen; en deze tot 1 december 2020 te mogen gebruiken.

Om deze dispensatie goed te kunnen verwerken is het voor ons wel van belang dat u doorgeeft wie uw TSP is zodat wij dit ook met de betreffende partij kunnen afstemmen.

Daar de certificaten die onder de publieke root (voorheen G3, nu EV) vallen onderhevig zijn aan vaak veranderende eisen in het web ecosysteem raadt de PA voor machine-to-machine verkeer certificaten uit de PKIoverheid private root aan. Deze certificaten vallen buiten het beleid van de browserpartijen en zijn daarom de betere keuze voor vitale (besloten) systemen.

Ik ga er vanuit u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,

(10)(2e)
(10)(2e)
.....
Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Wilhelmina van Pruisenweg 52 | 2595 AN | Den Haag
Postbus 96810 | 2509 JE | Den Haag
.....

T 06 – (10)(2e)
.....
Dienst digitale overheid
.....

-----Oorspronkelijk bericht-----
Van: (10)(2e) < (10)(2e) >
Verzonden: maandag 31 augustus 2020 13:17
Aan: (10)(2e) < (10)(2e) @logius.nl>
CC: PKIoverheid < (10)(2e) @logius.nl>; (10)(2e)) - Logius
< (10)(2e) @logius.nl>; (10)(2e)
< (10)(2e) @logius.nl>; (10)(2e)) < (10)(2e) @dictu.nl>
Onderwerp: Re: Verzoek om Dispensatie G3 certificaat tot 1 November ten behoeve van de CoronaMelder

(10)(2e) ,

Bedankt voor de enorme snelheid op vrijdag (en we konden later op die vrijdag dankzij dit de juiste key-ceremnies voor de HSM's doorlopen).

Wat is de volgende stap voor het aanbieden van de CSR ter tekening (met name of dit bij onze bestaande KPN provider kan - of naar een andere partij moet) ?

Want KPN geeft aan dat dit 'niet conform de afspraken met Logius' is.

Met vriendelijke groet,

(10)(2e)

On 28 Aug 2020, at 15:21, (10)(2e)
< (10)(2e) @logius.nl> wrote:

Beste (10)(2e) ,

Omwille van duidelijkheid en snelheid met betrekking tot dit issue
deel ik alvast per mail ons voornemen De gevraagde dispensatie te verlenen.
Wij zullen dit nog bevestigen op de geëigende wijze.

Op de gestelde adviesvraag komen we ook zo snel als mogelijk terug.

Met vriendelijke groet,

(10)(2e)
(10)(2e) Logius
06 (10)(2e)

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e)
< (10)(2e) < (10)(2e) @webweaving.org>>

Datum: vrijdag 28 aug. 2020 3:09 PM
Aan: (10)(2e)
<(10)(2e)@logius.nl<(10)(2e)@logius.nl>>
Kopie: (10)(2e)
<(10)(2e)@minbzk.nl<(10)(2e)@minbzk.nl>>,
(10)(2e)
<(10)(2e)@minvws.nl<(10)(2e)@minvws.nl>>
Onderwerp: Verzoek om Dispensatie G3 certificaat tot 1 November ten behoeve van de CoronaMelder

Beste (10)(2e),

De mobiele coronamelder applicatie maakt gebruikt van een aantal certificaten onder het G3 Stamcertificaat; en bevat een 'hardcoded' beveiliging die hierop expliciet controleert (z.g. pinning; een pin op G3).

Op dit moment zijn er ruim een miljoen van deze applicaties gedistribueerd in de eerste GGD regio's; en wordt de finale HSM infrastructuur op dit moment gereed gemaakt voor productie voor de rest van het land volende week.

Om de transitie weg van G3 te faciliteren wordt er nu een versie uitgerold naar alle burgers die ook de EV stam accepteert. Echter - het zal minimaal 6 weken duren (en waarschijnlijk langer) totdat het leeuwendeel van de burgers deze versie heeft.

Dus hierbij verzoekt het programma Digitale Ondersteuning Bestrijding COVID-19 met de mobiele app "CoronaMelder" om dispensatie om, tot 1 November 2020, een aantal certificaten voor de API, de distributie en de CDN in test/acceptatie en productie, te mogen laten tekenen; en deze tot 1 November te mogen gebruiken (in parallel met de nieuwere certificaten onder EV).

Doel van deze dispensatie is de ruim 1 Miljoen gebruikers te behouden; alsmede het opgebouwde vertrouwen in de samenleving.

Tevens vragen wij uw advies over de te volgen procedure - met name bij welke RA dient dit Certificate Signing Request ingediend te worden (de huidige certificaten zijn van KPN, de infrastructuur wordt door het CIBG bij KPN beheerd) voor een G3 handtekening.

Met vriendelijke groet,

(10)(2e) / 071 (10)(2e)

CC: (10)(2e), (10)(2e), (10)(2e), (10)(2e), (10)(2e)

damage of any kind resulting from the risks inherent in the electronic transmission of messages.