To: 5.1.2e [5.1.2e]; 5.1.2e)[5.1.2e @minvws.nl]
Cc: 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e
Sent: Mon 2/8/2021 7:35:02 PM
Subject: RE: Toepassing Coronavirus
Received: Mon 2/8/2021 7:35:28 PM

Hi,

Dit gaat over het inzetten van je mobiele telefoon voor authenticatie. Voor ons kan dat interessant zijn voor het verbinden van je testresultaat aan de juiste persoon. We zijn al aan het kijken naar het gebruik van de SIM card in de telefoon maar dat is technisch lastig. Zoals ik de mail hieronder begrijp gebruikt hij ipv de simkaart een pki smart card. Vind ik interessant, maar voor het testbewijs denk ik niet heel praktisch. Je zou elke Nederlander dan zo'n pki smart card moeten sturen.

Maar kan wel heel interessant zijn voor andere toepassingen. Bijv inloggen van zorg medewerkers bij applicatie mbv je telefoon en zo'n kaart.

Misschien interessant een keer een vrijblijvende demo te vragen. Ik zou het wel even willen zien.

Met vriendelijke groet,
5.1.2e
On 7 Feb 2021, 14:23 +0100, 5.1.2e) <5.1.2e @minvws.nl>, wrote:

> Ter info. Wat zal ik terug schrijven?
>
> Overigens is de app terug brengen tot een authenticatie app wel een beperkte blik
>
> Groet!
>
> 5.1.2e
>
> Verzonden met BlackBerry Work
> (www.blackberry.com)
>
> Van: 5.1.2e <5.1.2e 5.1.2e >
> Datum: zondag 07 feb. 2021 2:14 PM
> Aan: 5.1.2e) <5.1.2e @minvws.nl<5.1.2e @minvws.nl>>
> Onderwerp: FW: Toepassing Coronavirus
>
> Dag 5.1.2e
>
> Als VWS toch overweegt om een eigen (Idemix) authenticatie APP te laten ontwikkelen is een nieuwe cryptografische techniek die ik recent heb ontwikkeld mogelijk interessant.
> Deze cryptografische techniek vertrekt juist van de beperkingen in de reguliere crypto hardware (SE/TEE) van mobiele apparaten en beoogt op basis daarvan een mobiele authenticatie APP te maken op betrouwbaarheidsniveau eIDAS Hoog.
> De moeilijkheid daarbij is de kennisfactor (de 'PIN') omdat daar onvoldoende support voor is in de reguliere crypto hardware.
> De kunst is daarbij om echt 'sole control' te krijgen zoals een PKI smart card en ik denk dat ik daar in geslaagd ben.
> De techniek kan worden gebruikt in een federatie zoals de DigiD APP maar ook rechtstreeks zoals de IRMA APP, daarmee is het ook een basis voor de 'online identiteit'.
> Lokale versleuteling van attributen is triviaal als de APP sterk kan authenticeren: je vraagt daarmee gewoon de benodigde sleutels op.

Dat ik verwacht dat hiermee eIDAS Hoog gehaald kan worden concludeer ik uit het feit dat de bottleneck daarvoor kennelijk niet in de reguliere crypto hardware van mobiele apparaten zit.
Er zijn namelijk al twee middelen genotificeerd op eIDAS Hoog die ook gebruik maken van de reguliere crypto hardware (ITSME, Digidenity), zij het dat dit proprietary oplossingen zijn; mijn methode zal open zijn.

NB Meer dan 90% van alle mobiele apparaten bezit de reguliere crypto hardware (SE/TEE) zodat een authenticatie APP op betrouwbaarheidsniveau Substantieel of Hoog hier m.i. verplicht gebruik van zou moeten maken vanuit het 'stand der techniek' principe. Zoals ik onder aangeef kan IRMA dit nu niet. Mijn opmerkingen hierover naar het IRMA team 5.1.2e worden simpel afgedaan met dat 5.1.2e Tjsa.

5.1.2e

Met vriendelijke groet, Kind regards

5.1.2e
T: 5.1.2e
5.1.2e 5.1.2e

** If you receive this e-mail in error then I kindly request you to inform me immediately and to delete the e-mail. **

From: 5.1.2e < 5.1.2e
Sent: Friday, 5 February 2021 14:01
To: 5.1.2 5.1.2e >
Cc: 5.1.2e)' < 5.1.2e @minvws.nl>; 5.1.2 5.1.2e >;
5.1.2e 5.1.2e 5.1.2e 5.1.2e >; 5.1.2e
< 5.1.2e @logius.nl>
Subject: RE: Toepassing Coronavirus

Dag 5.1.2e

Wij hebben hier al een tijdje terug over gesproken zie ik nu.
Daar heb ik toen nog even over nagedacht en een cryptografische schets gemaakt.

Belangrijke security/privacy eisen zijn:

* Vaccinatie APP moet niet te clonen zijn. Hier ga je denk ik al een uitdaging krijgen bij Idemix. Omdat Idemix een geraffineerd protocol is, passen de private signeer sleutels niet in de reguliere crypto hardware (SE/TEE) van mobiele apparaten; software sleutels zijn eenvoudig te kopiëren. De SE van Apple ondersteunt alleen ECDSA. De TEE van Android (eigenlijk de hardware backed keystore) kent wel RSA maar niet die variant wordt verlangt door Idemix die ook echt anders werkt.
* Vaccinatie APP moet beschermen tegen dwang. Er moeten voorkomen dat zo maar iedere partij aan burgers kan gaan vragen te bewijzen of ze gevaccineerd zijn. Alleen toegelaten partijen moeten dat kunnen.

De Irma APP heeft overigens vergelijkbare zorgpunten.
Het tweede zorgpunt heeft elke decentrale authenticatie oplossing; federatieve authenticatie heeft dus ook privacy voordelen! Je kunt gewoon niet aanloggen met DigiD bij bol.com.
Dit is ook de reden dat de (decentrale) 5.1.2e eID kaart dezelfde toegangsbeveiliging bevat (Terminal Authentication) als EU paspoorten voor de vingerafdrukken.
Is ook de reden dat die eID kaart zo weinig populair is bij dienstverleners.

5.1.2e

Met vriendelijke groet, Kind regards

5.1.2e

5.1.2e

** If you receive this e-mail in error then I kindly request you to inform me immediately and to delete the e-mail. **

From: 5.1.2e < 5.1.2e @logius.nl< 5.1.2e @logius.nl>>
Sent: Friday, 5 February 2021 11:13
To: 5.1.2 5.1.2e < 5.1.2e @webweaving.org>>
Cc: 5.1.2e) < 5.1.2e @minvws.nl< 5.1.2e @minvws.nl>>; 5.1.2e
< 5.1.2e < 5.1.2e @mobach.nl>>; 5.1.2e
< 5.1.2e < 5.1.2e @dewinter.com>>; 5.1.2e
< 5.1.2e < 5.1.2e @cmptr.nl>>
Subject: Toepassing Coronavirus

Beste 5.1.2e

Naar aanleiding van de eerdere mail m.b.t. de ondersteuningsvraag i.r.t. Utimaco firmware ontwikkeling ten behoeve van de registratie van Coranavirus testresultaten is door de Logius directie gevraagd om jullie hierbij te helpen en mee te denken waar mogelijk.

Naast het delen van de ervaring die wij hebben op dat gebied zou ik graag de aandacht willen vragen voor de mogelijkheden die reeds worden geboden op basis van polymorfe pseudoniemen. Dit systeem is volledig operationeel, flexibel en op functioneel en beveiligingsgebied grondig getest.

Om de mogelijkheden scherper te krijgen heb ik contact gezocht met onze cryptografisch architect, 5.1.2e
Het systeem op basis van polymorfe pseudoniemen ondersteunt authenticatie op niveau hoog, iets wat zeker wenselijk zal zijn voor jullie toepassing. Het zou hiermee mogelijk moeten zijn om op relatief korte termijn een vaccinatieregister/testregister op te kunnen zetten.

Mocht je meer willen weten over deze mogelijkheden dan organiseer ik graag een kennissessie.

Uiteraard ondersteunen we ook graag bij de ingeslagen richting.

Met vriendelijke groet,

5.1.2e