Stichting Privacy By Design
privacybydesign.foundation
Nijmegen, 24 mei 2018

Opmerking vooraf: deze reactie zal door de stichting Privacy by Design op haar eigen website gepubliceerd worden. De stichting heeft geen bezwaar tegen openbaarmaking op internetconsultatie.nl.

LS,

Bij deze wil ik graag gebruik maken van de mogelijkheid om te reageren op het *Controleprotocol eID 2018*, zoals op 3 mei 2018 door het ministerie BZK gepubliceerd is op de website internetconsultatie.nl. Ik reageer als voorzitter van de stichting Privacy by Design. Deze stichting werkt aan attribuut-gebaseerde authenticatie en digitale ondertekening, via het (open source) identiteitsplatform IRMA, met een gelijknamige app. Deze werkzaamheden kleuren de inhoud van de onderstaande opmerkingen.

Het Controleprotocol eID wordt voorgesteld als Nederlandse leidraad voor de beoordeling of een authenticatiemiddel voldoet aan de Europese eIDAS-uitvoeringsverordening 1502[1]. Die verordening beschrijft criteria voor betrouwbaarheidsniveaus laag, substantieel en hoog. Het is het leidende onderliggende document. Het Controleprotocol eID geeft een heel eigen interpretatie aan die verordening 1502. Ik kom daar op het eind op terug.

De stichting maakt fundamenteel bezwaar tegen het feit dat het Controleprotocol eID — zonder basis in de eIDAS-uitvoeringsverordening 1502 — een traditionele centralistische ICT-architectuur dwingend voorschrijft waardoor innovatie gehinderd wordt — en daarmee nieuwe gebruiksmogelijkheden en nieuwe vormen van privacybescherming uitgesloten worden. Het Controleprotocol eID lijkt zich te beperken tot de werk/denk-wijze van traditionele, op standaard chipkaart en paspoort gebaseerde technologie van 10 à 15 jaar geleden; daarmee wordt geen (of veel te weinig) ruimte gelaten voor nieuwere goedkopere technologieën, met name voor inmiddels gangbare technologieën die gebaseerd zijn op apps op smart

[1] Zie https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002.

phones. Dit is pijnlijk in het licht van voortgaande ontwikkelingen waarbij chipkaarten steeds minder gebruikelijk worden (en door velen zelfs als achterhaalde technologie beschouwd worden).

Hieronder zullen deze bezwaren nader uitgewerkt worden. Daarbij zal soms vermeld worden hoe de IRMA app functioneert, enerzijds om aan te tonen dat er daadwerkelijk alternatieven zijn voor de dwingend voorgeschreven architectuur, en anderzijds om te laten zien hoe een alternatief er uit zou kunnen zien.

1. Het Controleprotocol eID gaat bij de beschrijving van het beoogde authenticatiemiddel uit van een eenheid van drager en inhoud (attributen van de gebruiker). Die inhoud wordt bij registratie van de gebruiker (en uitgifte van het middel) eenmalig bepaald en vastgelegd in het middel. Allerlei bepalingen gaan uit van deze eenheid van middel en inhoud, bijv. over:

   - schorsing, herroeping, en re-activering van het middel;
   - verlenging en vervanging van het middel;
   - geldigheid van het middel.

   Impliciet wordt er van uitgegaan dat de drager en de inhoud daarvan onlosmakelijk verbonden zijn[2].

   Deze eenheid van drager en inhoud is gebruikelijk bij traditionele chipkaarten, maar is verre van noodzakelijk. Sterker nog, alternatieve authenticatiemiddelen, met name die gebaseerd zijn op apps, kennen deze koppeling niet.

   Bij registratie van de gebruiker in de IRMA app wordt een persoonlijke cryptografische sleutel eenmalig gegenereerd, en verdeeld over de app en een server die belast is met herstel/anti-misbruik functionaliteit[3]. Toegang tot die sleutel wordt afgeschermd via een PIN, gekozen door de gebruiker zelf. Het gebruik van alle attributen in de app kan gestopt (geschorst) worden door het centrale deel van de cryptografische sleutel onbruikbaar te maken.

[2]Het beeld van drager en inhoud is expliciet terug te vinden in de voorgenomen definitiebepalingen die als bijlage toegevoegd zijn aan het Controleprotocol eID. Daarin wordt een definitie gegeven van 'identificatiemiddel', namelijk als: "elektronisch middel dat persoonsidentificatiegegevens bevat en ...". (Om onduidelijke redenen wordt in het Controleprotocol eID de term 'authenticatiemiddel' gebruikt terwijl in de bijlage 'identificatiemiddel' gedefinieerd wordt.)

[3]In de huidige fase draait deze server onder verantwoordelijkheid van de stichting Privacy by Design.

Gedurende de gehele life cycle van de IRMA app kan de gebruiker zelf attributen toevoegen en verwijderen. De inhoud (de attributen) staat daarmee volkomen los van de drager. Geldigheid en geldigheidsduur is bijvoorbeeld gekoppeld aan attributen, en niet aan de drager. Het moge duidelijk zijn dat dit veel grotere flexibiliteit en toepassingsmogelijkheden geeft, bijvoorbeeld door attributen toe te laten die een kortere geldigheidsduur hebben dan de drager (zoals huisadressen of toegangskaarten voor een evenement).

2. Het Controleprotocol eID schrijft voor dat bij registratie van de gebruiker ook identificatie van die gebruiker plaatsvindt — met een bepaald betrouwbaarheidsniveau. Ook dit is op geen enkele manier noodzakelijk.

   Bij registratie van een nieuwe IRMA gebruiker vindt geen enkele identificatie plaats. De gebruiker krijgt enkel een willekeurige gebruikersnaam (een pseudoniem) toegekend en kan zelf kiezen of een (eigen) email adres aan dit pseudoniem gekoppeld wordt. Identificatie van de gebruiker is pas noodzakelijk wanneer de IRMA app van inhoud (attributen) voorzien wordt.

   Terzijde: afgedwongen identificatie van deelnemers bij registratie schrikt nieuwe gebruikers in de praktijk af en hindert daardoor de adoptie van een nieuwe authenticatiemiddel.

3. Het Controleprotocol eID gaat er van uit dat de aanbieder van het middel de enige partij is die inhoud (attributen) eenmalig op/in het authenticatiemiddel kan zetten. Bovendien worden voor alle gebruikers in principe dezelfde (typen van) attributen toegevoegd.

   Dit is een ernstige beperking van de gebruiksmogelijkheden. Attributen kunnen immers uit veel verschillende bronnen komen (overheid, banken, telecoms, verzekeraars, (web)winkeliers, zorgaanbieders, etc. etc.). De aanbieder van het middel heeft typisch geen toegang tot al die bronnen. Bovendien zijn niet alle deze attributen op iedereen van toepassing: attributen over professionals in de gezondheidszorg (zoals in het BIG register) zijn bijvoorbeeld alleen van toepassing op zulke zorgprofessionals. Bij een authenticatiemiddel dat breed gebruik beoogt is het dus essentieel dat differentiatie van attributen mogelijk is.

   Inderdaad, in de IRMA app kunnen gebruikers zelf een persoonlijk "paspoort" samenstellen van attributen die op hen van toepassing zijn. De attributen kunnen uit velerlei bronnen afkomstig zijn[4]. Bovendien kunnen

[4]Voor een indruk, zie de uitgifte pagina privacybydesign.foundation/uitgifte van de stichting.

deze attributen niet slechts eenmalig, maar voortdurend toegevoegd (en ook verwijderd) worden.

4. Het betrouwbaarheidsniveau wordt in het Controleprotocol eID gekoppeld aan het authenticatiemiddel.

   Dit is een onnatuurlijke beperking. Het betrouwbaarheidsniveau moet gekoppeld zijn aan de bron van de attributen, niet (enkel) aan het middel. In een IRMA app kan bijvoorbeeld het 'naam' attribuut meerdere keren voorkomen, uit verschillende bronnen. Een naam kan bijvoorbeeld afkomstig zijn van het Facebook account van de gebruiker, of van de bank van de gebruiker. De dienstaanbieder (*relying party*) kan van ieder attribuut (cryptografisch) vaststellen wat de bron is — via een digitale handtekening die de bron op attributen plaatst — en daarmee zelf bepalen of deze bron voldoende betrouwbaar is. De dienstaanbieder bepaalt voor iedere toepassing dus zelf welke attributen uit welke bron geaccepteerd worden voor authenticatie. Ook hier draagt loskoppeling van de drager bij aan de gebruiksmogelijkheden.

   Hogere betrouwbaarheidsniveaus zijn ook in deze opzet mogelijk. Bepaalde attributen kunnen bijvoorbeeld alleen na *face-to-face* authenticatie aan een gebruiker uitgegeven worden. Op die manier kan *de facto* een betrouwbaarheidsniveau 'substantieel' of 'hoog' gerealiseerd worden, ook al lijkt dit niet te passen in de omschrijvingen van het Controleprotocol eID.

5. Het Controleprotocol eID dwingt af dat de aanbieder van het middel bij iedere authenticatie (van niveau substantieel of hoog) de gebruiker een bericht stuurt met daarin een melding van een authenticatiepoging bij een bepaalde dienstaanbieder. Deze eis is bedoeld om eventueel misbruik zichtbaar te maken voor de gebruiker. Echter, deze eis heeft — mogelijk onbedoeld — vergaande gevolgen voor de architectuur en de gegevensstromen bij het beoogde authenticatiemiddel. De aanbieder van het middel ziet door deze eis immers van elke gebruiker elke authenticatie(poging) bij elke dienstaanbieder.

   Hiermee wordt door het Controleprotocol eID afgedwongen dat de aanbieder van het authenticatiemiddel een *privacy hotspot* wordt. Dit is *non*-privacy by design. De aanbieder wordt gedwongen te registreren of een gebruiker bijvoorbeeld inlogt bij een slijter, of bij een psychiatrische kliniek. De aanbieder moet hiermee alle activiteiten van een gebruiker die authenticatie vereisen in kaart brengen en bouwt daarmee een gedetailleerd profiel van

de gebruiker op. De aanbieder van het middel kan deze uiterst gevoelige persoonsgegevens mogelijk combineren met andere (commerciële) activiteiten.

Voor deze verwerking van authenticatie-activiteiten hoeft de middelenaanbieder — dwz. voor de *privacy hotspot* rol — geen toestemming van de gebruiker te vragen. Immers, het Controleprotocol eID dwingt deze verwerking af, waardoor de middelenaanbieder zich kan beroepen op AVG art. 6 (c): de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting. Voor de combinatie van deze authenticatie historie met andere activiteiten van de middelenaanbieder is wel toestemming van de gebruiker nodig.

Vanuit het perspectief van privacybescherming ligt het meer voor de hand om af te dwingen dat een middelenaanbieder *niet* bijhoudt waar een gebruiker wanneer inlogt.

De voorgeschreven centralistische *privacy hotspot* rol is helemaal niet noodzakelijk. Bij IRMA vindt authenticatie rechtstreeks plaats tussen (de app van) de gebruiker en de dienstaanbieder. De decentrale architectuur van IRMA garandeert dat andere partijen, inclusief de stichting zelf, niet zien welke attributen een gebruiker aan wie dan ook onthult (*privacy by design*). De IRMA app houdt zelf een log bij waarin de gebruiker het eigen gebruik kan bekijken. Ook houdt de eerder genoemde herstel/anti-misbruik server bij op welk tijdstip het centraal opgeslagen deel van een persoonlijke cryptografische sleutel gebruikt wordt. De (bestaande 'MijnIRMA') inzage hierin geeft de gebruiker zicht op eventueel misbruik. Daaraan zou gekoppeld kunnen worden dat de gebruiker een bericht ontvangt bij ieder gebruik van het centraal opgeslagen deel van de eigen sleutel. Maar het gebruikte (*multi-party computation*) protocol van IRMA is zodanig ingericht dat de stichting of de herstel/anti-misbruik server niet kan registreren bij welke dienstaanbieder de gebruiker zich authenticeert. De stichting wil dat ook helemaal niet weten of bijhouden, juist om de privacy van gebruikers te beschermen — en wil ook geen onnodige wettelijke verplichting opgelegd krijgen om dat wel te doen.

6. Het Controleprotocol eID vereist dat de aanbieder van een authenticatiemiddel de mogelijkheid heeft tot intrekking en schorsing van het middel — en wel op korte termijn (24 uur). Ook dit is alleen mogelijk vanuit een centralistische architectuur met een privacy hotspot, waarbij de aanbieder van het middel feitelijke controle heeft over ieder middel. In een

privacy-vriendelijke decentrale architectuur kan de gebruiker zelf op ieder moment het eigen middel intrekken/schorsen (bij verlies of geconstateerd misbruik/disfunctioneren). Intrekken van specifieke (sets van) attributen is in principe ook mogelijk, door de uitgever van die attributen, en zelfs op een privacy-vriendelijke manier. Met deze meer verfijnde aanpak wordt niet het gehele middel buiten werking gesteld, zoals vereist in het Controleprotocol eID. Daardoor kan de gebruiker de niet-gecompromitteerde attributen blijven gebruiken. Dit draagt in belangrijke mate bij aan de gebruiksvriendelijkheid, zeker wanneer gebruikers eigenlijk niet zonder authenticatiemiddel kunnen functioneren.

De stichting Privacy by Design beoogt zonder winstoogmerk op transparante wijze (via open source software) en met gebruik van geavanceerde cryptografie zowel de privacy van gebruikers te beschermen als gebruikers flexibele en betrouwbare mogelijkheden te bieden voor authenticatie (en digitale ondertekening), met door de architectuur gegarandeerde regie over eigen gegevens. Daarbij kunnen dienstaanbieders gebruik maken van uitgebreide mogelijkheden, namelijk (1) een in principe onbegrensde verzameling van betrouwbare attributen van gebruikers; (2) digitale handtekeningen van gebruikers, bijvoorbeeld voor toestemmingsverklaringen zoals vereist onder de AVG. Het voorgestelde Controleprotocol eID is daarbij in de huidige vorm niet behulpzaam, zoals hierboven betoogd.

Bij deze wil de stichting Privacy by Design voorstellen dat het nu gepubliceerde Controleprotocol eID ingrijpend wordt herzien, waarbij de bovenstaande bezwaren en beperkingen worden weggenomen, met als doel om maximale ruimte te bieden voor nieuwe, alternatieve technieken met een hoog niveau van betrouwbaarheid en privacybescherming. Met name dringt de stichting er op aan dat: (1) inhoud en drager losgekoppeld worden en dat eisen onafhankelijk van een dergelijke (onnodige en beperkende) koppeling geformuleerd worden; (2) eisen die een centralistische architectuur afdwingen op een architectuur-neutrale wijze geherformuleerd worden.

De eIDAS-uitvoeringsverordening 1502, waar het hier bekritiseerde Controleprotocol eID zich op baseert, is heel generiek en architectuur-neutraal. Het kern-begrip daarin, *electronic authentication means*, wordt niet gedefinieerd; het zou een chipkaart kunnen zijn, of een app, of misschien zelfs een digitaal attribuut (op een chipkaart of app). Er wordt bijvoorbeeld heel in het algemeen geëist dat: *It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner*. Hiervoor wordt geen centralistische architectuur vereist. Er is ook geen eis dat gebruikers door de uitgever van het *means* direct

geïnformeerd worden over iedere authenticatiepoging bij een dienstaanbieder, en in het bijzonder wordt niet geëist dat dienstaanbieders registereren wie waar op welk moment inlogt. De stichting dringt er daarom op aan dat een Nederlandse leidraad voor de eIDAS-uitvoeringsverordening 1502 architectuur-neutraal is, zonder privacy hotspots, en in essentie niet afwijkt van de verordening via vergaande eigen dwingende interpretaties.

Waar mogelijk, gepast of gewenst wil de stichting een positieve rol spelen en bijdragen aan een modern eID in het algemeen, en aan het Controleprotocol eID in het bijzonder.

Prof. dr. B. Jacobs
Voorzitter stichting Privacy by Design.