Eric Verheul is een onafhankelijk cryptografisch adviseur en deeltijd hoogleraar aan de Radboud universiteit te Nijmegen. Hij geeft een master course in security management en doet onderzoek naar toegepaste cryptografie en privacy enhancing technologies. Dit artikel schrijft hij op persoonlijke titel. Eric is bereikbaar via eric.verheul@keycontrols.nl.

Toepassing privacy enhancing technology in het Nederlandse eID

Vanuit de Nederlandse overheid wordt hard gewerkt aan het beschikbaar krijgen van sterke (‘twee-factor’) vormen van authenticatie voor burger en bedrijven bij (publieke) dienstverleners. Belangrijke aspecten daarbij zijn beveiliging, privacy en gebruikersvriendelijkheid (ook voor de dienstverleners). Hoewel de volledige invulling nog niet bekend is, zijn wel verschillende deelproducten beschikbaar gemaakt. Dit artikel beschrijft deze deelproducten.

Op bsn-koppelregister.nl (1) staan de specificaties en decryptiesoftware (Java) voor de privacy enhancing technology (PET), voorzien binnen het Nederlandse eID-stelsel. Dit staat bekend als 'PEP' (Polymorphic Encryption and Pseudonimation). Het PEP-startpunt is – fundamenteel anders dan dat van bijvoorbeeld IRMA (2) – die van een gecentraliseerde opzet ('federatie'): de authenticatie vindt plaats bij een authenticatiedienst die het resultaat doorgeeft aan een dienstverlener.

Voor dit startpunt is gekozen, omdat ervaringen uit andere landen zoals Duitsland aangeven dat een gedecentraliseerde ('directe') benadering belastend is voor dienstverleners. Dit onder meer omdat dienstverleners dan specifieke protocollen moeten implementeren en specifieke helpdesks moeten inzetten. PEP beoogt evenwel de 'ontzorging' van een gecentraliseerde authenticatie-opzet te combineren met de privacy- en securityvoordelen van een gedecentraliseerde oplossing. Toepassing van PEP is authenticatietechnologie neutraal en kan worden gecombineerd met reguliere vormen van authenticatie (waaronder IRMA). In mei 2018 heeft PEP een securitybeoordeling door de universiteit van Birmingham glansrijk doorstaan. PEP wordt nu al toegepast voor het aanloggen vanuit Nederland in andere lidstaten en omgekeerd (eIDAS interoperabiliteit).

De cryptografische specificatie van PEP-eID staat in de subdirectory/pep-crypto-documentation/10-Reference. De specificatie start met de niet-technische achtergrond van PEP en de rationale voor de gekozen opzet. Daarnaast omvatten de specificaties ook innovatieve overheidstoepassingen die met PEP mogelijk worden zoals privacyvriendelijke gegevensuitwisseling in de zorg (3) en stemmen vanuit het buitenland. Dit wordt onderaan dit artikel verder toegelicht.

Het PEP-paradepaardje is DigiD Hoog, dat een fundamenteel privacyprobleem oplost in een gecentraliseerde opzet: in een standaard gecentraliseerde authenticatieopzet krijgt de authenticatiedienst zowel inzicht in de identiteit van de gebruiker als van de dienstverlener die deze wenst te bezoeken. Het bezoek aan sommige dienstverleners (bijvoorbeeld in de zorg) kan zelfstandig al als bijzonder persoonsgegevens worden bestempeld. DigiD Hoog lost dit privacy issue op door aanloggen anoniem te laten plaatsvinden. Dat wil zeggen: de (gecentraliseerde) authenticatiedienst DigiD verstrekt een gerandomiseerd, versleuteld BSN van een burger aan een dienstverlener zonder zelf inzage in te krijgen in het BSN of dit te kunnen linken. Doordat DigiD wel weet bij welke dienstverlener de burger wil aanloggen, kan deze wel worden beschermd tegen browser malware (`man-in-the-browser' malware). Daarmee is zowel hoge privacy als security mogelijk en hoeft hiertussen geen keuze te worden gemaakt zoals in andere landen wel is gedaan.

DigiD Hoog is gebaseerd op een eID-kaartapplicatie (Polymorphic Card Application of PCA) uitgegeven na 4 juni 2018. Het aanwezig zijn van PCA op een rijbewijs is te herkennen aan het 'ID'-logo (zie onder).

Vorig jaar is een succesvolle pilot uitgevoerd met DigiD Hoog. Als alternatief voor een separate kaartlezer konden gebruikers daarbij ook hun 'NFC-enabled'-telefoon gebruiken. Tot voor kort waren dat alleen Android-gebaseerde telefoons, maar recent zijn ook Apple-toestellen (iPhones) geschikt. November 2019 zijn ongeveer 3 miljoen rijbewijzen uitgegeven die geschikt zijn voor DigiD Hoog en dat aantal groeit met ongeveer 35.000 per week. Plaatsing van PCA op de Nederlandse identiteitskaart is later gepland (aanpassing Paspoortwet). De cryptografische werking van PCA maakt deel uit van de PEP-eID -specificaties. Een PCA-simulator kan worden gevonden op github.com (4).

PEP (en ook de eID-kaart) ondersteunt naast het BSN ook pseudoniemen zoals ook sterk geadviseerd in de Algemene verordening gegevensbescherming (AVG). Ter illustratie: de toepassing van het BSN in een attributenregister - waarin alleen wordt bijgehouden dat iemand ouder dan 18 lijkt - is niet in lijn met het AVG data minimization-beginsel. Zeker niet als de bevragende diensten (bijvoorbeeld zorg of goksites) privacygevoelig zijn. Bij gebruik van het BSN zouden de attribuutdiensten immers bij iedere bevraging inzicht krijgen

Met de toepassing van PEP ontstaat een krachtige securityinfrastructuur voor (toekomstige) Nederlandse overheid-toepassingen

wie de dienst bezoekt. Om vergelijkbare redenen hoeft ook een machtigingsregister niet het BSN van de gemachtigde te kennen; ook daar volstaat een pseudoniem.

Toepassing van pseudoniemen kan ook de beveiliging van registers enorm versterken. Een actueel voorbeeld zou een register zijn waarin de 'psychische (on)gezondheid' van burgers wordt vastgelegd ten behoeve van het afgeven van wapenvergunningen. Het gebruik van het BSN in een dergelijk register is ongewenst, omdat bij het compromitteren van een dergelijk register het leed niet te overzien is. Het gebruik van pseudoniemen mitigeert dit risico.

Naast de gebruikelijk eigenschappen hebben PEP-pseudoniemen ook bijzondere eigenschappen. Homomorfe cryptografie realiseert bijvoorbeeld dat een authenticatiedienst (zoals DigiD) de pseudoniemen vormt zonder er inzage in te krijgen; alleen de dienstverlener en betrokkene krijgen inzage. Doordat verder versleutelde BSN's en pseudoniemen digitaal getekend zijn (EC-Schnorr), kunnen zij ook end-to-end privacy en end-to-end security leveren zoals in een decentrale opzet. De eerste eigenschap betekent dat 'tussenliggende' partijen zoals makelaars geen inzage krijgen in de identiteiten (BSN's en pseudoniemen) en de tweede houdt in dat deze partijen de identiteiten niet kunnen manipuleren. PEP voorkomt daarmee dus ook het ontstaan van privacy hotspots waar in verleden discussie over was (de 'authenticatiepooiers' (5)).

Met de toepassing van PEP ontstaat een krachtige securityinfrastructuur voor (toekomstige) Nederlandse overheid-toepassingen die ook de AVG-beginselen 'data protection by design' en 'data minimization' ondersteunt. De ondersteuning van pseudoniemen maakt ook integratie mogelijk van publieke en private authenticatiediensten, hetgeen onderliggend is aan het Scandinavische eID-succes. Daarbij is sprake van één eID-infrastructuur voor zowel publieke als private dienstverleners. Bij private dienstverleners kan worden aangelogd onder pseudoniem en bij publieke dienstverleners onder BSN of pseudoniem. Een dergelijke opzet wordt al toegepast in andere landen zoals in Duitsland en Oostenrijk. Doordat pseudoniemen zijn afgeleid van het BSN zijn ze uniek per dienstverlener waarmee bijvoorbeeld ook Marktplaats-fraude en social media trolling zou kunnen worden gemitigeerd: een gebruiker kan dan immers maar een keer een eID verified (gepseudonimiseerd)-account aanvragen.

In de genoemde PEP-specificaties wordt de kracht van de eID-infrastructuur geïllustreerd aan de hand van twee voorbeeldtoepassingen: stemmen vanuit het buitenland en toepassing in het MedMij-initiatief (6).
Stemmen vanuit het buitenland gaat nadrukkelijk niet over digitaal stemmen voor iedereen, maar alleen voor de kleine groep Nederlanders die woonachtig zijn in het buitenland. Het huidige proces verloopt nu via de post (7) en staat daarmee onder meer op gespannen voet met het stemgeheim. De PEP-gebaseerde opzet vermijdt dit onder meer door gebruik van PEP-pseudoniemen. Medmij gaat over dataportabiliteit in de zorg: het ondersteunt dat patiënten hun medische gegevens vanuit zorgaanbieders naar gezondheidsomgevingen bij private dienstverleners kunnen onderbrengen. Dit levert patiënten controle over hun eigen gegevens en faciliteert zo bijvoorbeeld het vragen van second opinions. Door hun private aard mogen gezondheidsomgevingen niet het BSN verwerken. PEP-toepassing, waaronder diens pseudoniemen, kan een grote bijdrage kunnen leveren aan de beveiliging en privacy bescherming van burgers binnen Medmij. De Medmij-use case illustreert ook de voordelen van de integratie van publieke en private authenticatiediensten.

Referenties

(1) https://wiki.bsn-koppelregister.nl/display/DC/3.+Downloads
(2) https://privacybydesign.foundation/irma/
(3) www.medmij.nl
(4) https://github.com/CardContact/eID-sim/tree/PCA-sim
(5) https://pilab.nl/about%20pi%20lab/blog/privacy%20impact%20-assessement.html
(6) www.medmij.nl
(7) https://www.denhaag.nl/nl/bestuur-en-organisatie/verkiezingen/kiezers-buiten-nederland/permanente-registratie-voor-kiezers-buiten-nederland.htm