

Samenvatting

DigiD, dat staat voor Digitale Identiteit, is een authenticatievoorziening die door verschillende Nederlandse overheidsinstellingen gebruikt wordt bij de elektronische dienstverlening. Een dergelijk systeem kent grote uitdagingen en risico's op het gebied van privacy van de burger. Ook kan het leiden tot identiteitsroof. Aan de hand van een literatuurstudie en interviews met medewerkers van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, SURFnet en GBO.Overheid is onderzoek gedaan naar de mate waarin de privacy van de burger wordt gewaarborgd binnen DigiD. Bescherming van de privacy is in de Nederlandse Grondwet verankerd en nader uitgewerkt in de Wet Bescherming Persoonsgegevens. Deze laatste wet verplicht de verantwoordelijke tot het nemen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Technische maatregelen die kunnen worden ingezet ter bevordering van de privacy kunnen worden gebundeld onder de verzamelnaam Privacy Enhancing Technologies (PET). Er worden vier hoofdvormen van PET onderscheiden. In oplopende volgorde van effectiviteit zijn dit algemene PET-maatregelen, scheiden van gegevens, privacymanagementsystemen en anonimiseren van persoonsgegevens. De technische maatregelen die binnen DigiD zijn getroffen om te voorkomen dat onbevoegden toegang kunnen krijgen tot met behulp van DigiD verwerkte persoonsgegevens zijn algemene PET-maatregelen. Deze maatregelen zijn versleuteling van het opgeslagen wachtwoord, het over SSL tunnels van de communicatie tussen de burger en de DigiD server en het tekenen van de communicatie tussen de DigiD server en de overheidsdienst waarvoor authenticatie vereist is op basis van een gedeelde sleutel. Al in 1999 is kamerbreed een motie aangenomen waarin de regering onder andere wordt verzocht te bevorderen dat de overheid het voortouw zal nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens. Aan dit verzoek is onvoldoende gehoor gegeven bij de ontwikkeling van DigiD door geen gebruik te maken van één of meer effectievere hoofdvormen van PET-maatregelen, namelijk scheiden van gegevens, privacymanagementsystemen en anonimiseren.

Organisatorische maatregelen die binnen DigiD zijn getroffen om de privacy van de burger te waarborgen zijn het onderscheiden van verschillende zekerheidsniveaus, het controleren van de bij aanvraag van een DigiD opgegeven persoonsgegevens met behulp van de landelijk raadpleegbare deelverzameling en het per post versturen van een activeringscode.

Verder zijn maatregelen getroffen om het achterhalen van een gebruikersnaam en wachtwoord te bemoeilijken en mag een mobiel telefoonnummer maximaal aan één DigiD gekoppeld zijn. Tenslotte worden alle transacties met behulp van DigiD gelogd. Deze maatregelen bieden echter onvoldoende bescherming tegen identiteitsroof, omdat de huidige procedures voor aanvraag en activering geen garantie bieden dat de persoon die een DigiD heeft aangevraagd en geactiveerd ook daadwerkelijk de burger is met het sofinummer behorende bij deze DigiD. Bovendien kan uitsluitend op basis van een gebruikersnaam en wachtwoord een DigiD, worden uitgebreid met sms-authenticatie op een mobiel nummer naar keuze, indien de per post verstuurde activeringscode wordt onderschept. De extra zekerheid die het niveau midden zou moeten brengen, wordt hierdoor niet of nauwelijks geboden.

Een aanbeveling voor een extra technische maatregel om de privacy van de burger te waarborgen is gebruikmaking van de tweede hoofdvorm van PET-maatregelen, namelijk scheiding van gegevens. Hierbij wordt de burger binnen DigiD geïdentificeerd door een uniek, identificerend nummer dat niet bekend is bij de diverse overheidsdiensten die voor authenticatie gebruik maken van DigiD. In plaats hiervan worden deze diensten ingedeeld in verschillende sectoren, waarbij elke sector een eigen sectoraal identiteitsnummer gebruikt om een burger te identificeren. Per sector is er één vertrouwde partij die zowel het algemene identiteitsnummer als het identiteitsnummer behorende bij de eigen sector kent en in de communicatie tussen de overheidsdienst en DigiD als tolk fungeert. Uitsluitend de burger beschikt over alle sectornummers.

Ter verbetering van de organisatorische maatregelen wordt met name versterking van de procedures voor aanvraag en activering aanbevolen. De persoonsgegevens op basis waarvan men een DigiD kan aanvragen zijn te eenvoudig te achterhalen door derden en bieden daarom onvoldoende bescherming tegen fraude. In plaats van het sofinummer kan beter gekozen worden voor bijvoorbeeld de combinatie van het nummer van een paspoort, identiteitsbewijs, rijbewijs of verblijfsvergunning en de geldigheidsdatum van dit document. Ook de huidige activeringsprocedure biedt onvoldoende bescherming tegen identiteitsroof. Door de activeringscode niet langer per post te versturen, maar deze pas na legimitatie te overhandigen op het gemeentehuis, krijgt men meer zekerheid over de identiteit van de gebruiker van een DigiD. Wanneer ook bij wijziging of toevoeging van een mobiel telefoonnummer een activeringscode na legimitatie wordt overhandigd op het gemeentehuis, biedt een hoger zekerheidsniveau ook daadwerkelijk meer zekerheid over de identiteit van de gebruiker.