September 2018
Robin Oostrum

De Wereld van Authenticatie volgens SIVI

Authenticatie is, aangejaagd door steeds verder digitaliserende dienstverlening en nieuwe privacywetgeving, noodzakelijk voor het inrichten van online dienstverlening. Anno 2018 speelt moderne, veilige, vaak tweefactorauthenticatie daarbij een belangrijke rol.

De wereld van authenticatie is complex, en bovendien in beweging. Waar het jarenlang gebruikelijk was dat private dienstverleners hun eigen authenticatiemiddel gebruikten en de overheid één middel aanbood, zien we de vraag om breed gedragen middelen – over sectoren heen – steeds verder toenemen. Ondertussen ontstaan nieuwe uitdagingen, bijvoorbeeld rond authenticatie namens een derde persoon of organisatie.

Om de wereld van authenticatie te begrijpen is een opdeling in deeldomeinen nodig. In deze notitie geeft SIVI een overzicht van deze deeldomeinen. Daarnaast worden binnen elk deeldomein de kernpunten benoemd, die samen de SIVI-agenda voor 2018-2019 vormen.

- De wereld van authenticatie is complex en continu in beweging. Deze whitepaper geeft overzicht in deze wereld en in de huidige stand van zaken.
- Welke middelen hebben toekomst in de verzekeringsbranche? DigiD wordt doorontwikkeld, maar is alleen in het publieke domein te gebruiken. Private middelen, of samenwerkingen tussen overheid en private leveranciers, maken meer kans.
- Zakelijk was het Digitaal Paspoort decennialang *de facto* de branchestandaard, maar de continuïteit is nu onzeker. SIVI onderzoekt de toekomstscenario's.
- Verder duidt SIVI in 2018 de impact van de Wet Digitale Overheid en eIDAS-verordening, en onderzoekt relevante vraagstukken als machtigingen.

Inhoud

De waarde van vernieuwing

SIVI ontwikkelt en beheert standaarden voor digitaal zakendoen in de verzekeringsbranche. Onafhankelijk en deskundig. SIVI analyseert trends, onderzoekt de impact van nieuwe technologieën en inspireert alle ketenpartners om samen nieuwe stappen te zetten. Met de ambitie om digitaal verkeer voor de sector en de consument te laten werken. De consument, die steeds hogere eisen stelt aan gemak, zekerheid en veiligheid. En die 'vertrouwen' tegenwoordig met hoofdletters schrijft. Het succesvol bedienen van de digitale consument vraagt om de eenduidigheid van standaarden en de inspiratie van nieuwe mogelijkheden.

SIVI, standaard verandering

SIVI digitale toekomst verzekerd van standaarden

1. Introductie

Authenticatie cruciaal

De toename van online diensten impliceert een toename in het gebruik van privacygevoelige data, en een toename in het aangaan van verplichtingen. Misbruik en/of diefstal van identiteiten komt steeds vaker voor. Zowel binnen het particuliere als het zakelijke domein is authenticatie een essentieel onderdeel van online dienstverlening geworden.

Nieuwe privacywetgeving – zoals de GDPR en de Nederlandse afgeleide daarvan, de AVG – vormt bovendien een stevige aanjager voor moderne en sterke authenticatiemiddelen. Daarnaast stellen de aankomende eIDAS-verordening en Wet Digitale Overheid nieuwe eisen aan het implementeren van erkende, veilige middelen.

Los van wetgeving speelt ook het kostenplaatje een steeds belangrijkere rol. Enerzijds omdat de kosten simpelweg toenemen met het toenemend gebruik van (sterkere) authenticatiemiddelen. Anderzijds omdat ook het kostenmodel verschuift: waar voorheen de gebruiker betaalde, gaat nu ook de dienstverlener een bijdrage leveren aan het gebruik van moderne middelen. Het is zaak om hier rekening mee te houden en/of op in te spelen.

Onderverdeling in deeldomeinen

SIVI onderscheidt op hoofdlijnen twee domeinen binnen de wereld van authenticatie, met daarbinnen enkele deeldomeinen:

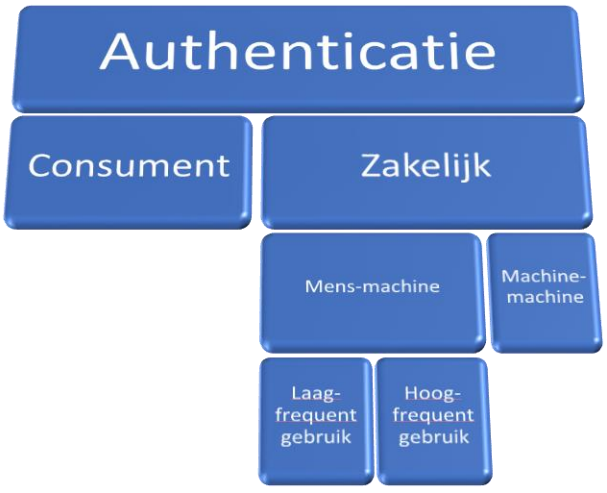
1. **Consument**: het authenticeren van een natuurlijk persoon, die een dienst wil afnemen voor hem/haar op persoonlijke titel. Dus bijvoorbeeld een burger die wil inloggen bij de Berichtenbox van de overheid, of een consument die online de dekking van haar reisverzekering wil aanpassen.
2. **Zakelijk**: het authenticeren van een organisatie. Onder te verdelen in mens-machine- en machine-machine-authenticatie:
    1. **Mens-machine**: authenticatie van een natuurlijk persoon namens een organisatie. Bijvoorbeeld een werkgever die wil inloggen op het werkgeversportaal van zijn pensioenadministratie, of een werknemer van een intermediairkantoor die verzekeringen wil vergelijken in een online tool.
    2. **Machine-machine**: authenticatie van een systeem namens een organisatie. Bijvoorbeeld een terminal die automatisch salarisbestanden verzendt naar een administratiekantoor.

Wat is authenticatie?
Authenticatie is het proces dat nagaat of een gebruiker daadwerkelijk is wie hij/zij beweert te zijn. Dat wil zeggen: daadwerkelijk de identiteit bezit die hij/zij opgeeft.

Deze vastgestelde identiteit bepaalt of de betreffende gebruiker gerechtigd is om een bepaalde handeling te verrichten of een service af te nemen; deze volgende stap noemen we **autorisatie**.

Authenticatie bestaat uit twee stappen. Bij de **registratiefase** wordt eenmalig een account gemaakt op basis van persoonsgegevens. Hoe grondig hierbij wordt gecontroleerd of de persoonsgegevens daadwerkelijk bij de betreffende persoon horen, bepaalt de betrouwbaarheid: face-to-face-controle met een paspoort bij een balie, leidt tot een hogere mate van betrouwbaarheid dan een gebruiker die online zijn/haar gegevens invoert.

Heeft de gebruiker eenmaal een account, dan kan hij/zij zich hier voortaan mee authenticeren. In deze **inlogfase** wordt vanaf nu alleen nog vastgesteld dat het om dezelfde gebruiker gaat als die ook de account aanmaakte. Ook hier hangt de betrouwbaarheid af van de mate waarin dit gecontroleerd wordt: enkel het invullen van een wachtwoord wordt als minder betrouwbaar verondersteld dan bijvoorbeeld een gezichtsscan of het invoeren van een extra code via de gsm van de gebruiker.



Figuur 1: de wereld van authenticatie in deeldomeinen

Binnen zakelijke mens-machine-authenticatie onderscheiden we tot slot authenticatie op laag-frequent gebruik tegenover authenticatie op hoog-frequent gebruik:

1. **Laag-frequent**: het beperkt gebruik van (zakelijke) authenticatiemiddelen, variërend van een keer per week tot enkele malen per jaar.
2. **Hoog-frequent**: het dagelijks, herhaaldelijk gebruik van authenticatiemiddelen in de zakelijke wereld. Op een werkdag van acht uur kan dit oplopen tot tientallen authenticaties.

Zie Figuur 1 op de vorige pagina voor een schematische weergave van de onderverdeling in deeldomeinen.

Opzet notitie

Deze notitie bespreekt elk van de hierboven genoemde deeldomeinen aan de hand van drie basisvragen:

1. Waar komen we vandaan?
2. Waar staan we nu?
3. Waar gaan we heen?

Met het beantwoorden van deze vragen voor elk van de domeinen wordt vervolgens de stap gezet naar de SIVI-agenda.

2. Consumentendomein

Waar komen we vandaan?

Binnen het consumentendomein is voor het grootste deel van de aanbieders van online diensten een login met gebruikersnaam en wachtwoord de standaard. Registratie en verificatie van persoonsgegevens gebeurt daarbij geheel online: de identiteit van de consument kan zo echter nooit met 100% zekerheid worden gegarandeerd. De Algemene Verordening Gegevensbescherming vereist security by design. Dat wil zeggen: systemen waarin persoonsgegevens omgaan, moeten volgens de als meest veilig geldende standaard zijn ontworpen. In die lijn kan tweefactorauthenticatie verstandig zijn bij authenticatie, zeker bij bijzondere persoonsgegevens.

Tweefactorauthenticatie
Authenticeren kan globaal op drie verschillende manieren: met iets dat je *weet*, iets dat je *hebt* en iets dat je *bent*. De methode van gebruikersnaam en wachtwoord is typerend voor iets dat je *weet*.

Tegenwoordig wordt daar vaak, om veiligheidsredenen, een tweede *factor* aan toegevoegd. Bijvoorbeeld een code die op je telefoon verschijnt (iets dat je *hebt*), een irisscan op een vliegveld (iets dat je *bent*) of een vingerafdrukscanner op een laptop (iets dat je *hebt* én iets dat je *bent*).

Wanneer bij één authenticatie van meerdere authenticatiemanieren gebruikgemaakt wordt, spreekt men van *multifactorauthenticatie*. Twee verschillende manieren wordt doorgaans als veilig beschouwd. Dit noemen we *tweefactorauthenticatie*.

Binnen de verzekeringsbranche heeft bijna iedere financieel dienstverlener nu een eigen online dienstverlening met een eigen authenticatievoorziening. Het belangrijke registratieproces vindt doorgaans plaats bij de financieel dienstverlener zelf. Dit gebeurt over het algemeen als een nieuwe klant een verzekeringsproduct afneemt of een bestaande klant – vaak op uitnodiging via brief of mail – toegang wil tot een mijnomgeving. Bij de registratie voor de mijnomgeving valideert de dienstverlener identificerende gegevens (bijvoorbeeld NAW, geboortedatum), waarna de consument een nieuw authenticatiemiddel ontvangt. Meestal ontvangt de consument per post of e-mail een wachtwoord, waarmee hij/zij in combinatie met een gebruikersnaam kan inloggen in de digitale omgeving. In de praktijk leidt dit aan de kant van de consument tot een veelheid aan accounts en combinaties van gebruikersnamen en wachtwoorden.

Waar staan we nu?

Binnen het consumentendomein zijn er nu drie groepen authenticatiemiddelen: publieke middelen, private middelen en publiek-private samenwerkingen. **Publieke authenticatiemiddelen** zijn ontwikkeld door – of in opdracht van – de overheid, en alleen inzetbaar binnen het BSN-domein (naast de overheid o.a. de collectiefpensioen- en zorgverzekeraars). Het bekendste publieke middel is DigiD. Om aan de nieuwste veiligheidsnormen te voldoen wordt DigiD doorontwikkeld naar hogere betrouwbaarheidsniveaus.

Private authenticatiemiddelen zijn authenticatiemiddelen die ontwikkeld zijn door private partijen. De voornaamste private optie is momenteel het door de Betaalvereniging opgezette iDIN. iDIN is herkenbaar en gebruiksvriendelijk dankzij de gelijkenis met het voor consumenten vertrouwde iDEAL. Verificatie van de consument gebeurt door middel van paspoortcontrole bij het aanmaken van een bankaccount, authenticatie is tweefactor. Naast gebruikersnaam en wachtwoord is altijd het bancaire inlogmiddel nodig. Bijvoorbeeld de TAN-codes van ING, de digipas van ASN of de random reader van de Rabobank. Groot voordeel hieraan is dat het merendeel van de consumenten dit middel al bezit: hier wordt immers ook gebruik van gemaakt bij iDEAL. De inzetbaarheid in het publieke domein is nog afhankelijk van de uniforme set van eisen[1] in de toekomstige Wet Digitale Overheid.

Mijnverzekeringenopeenrij
Op platform Mijnverzekeringenopeenrij.nl maken gebruikers eenvoudig hun eigen, online verzekeringsoverzicht. Registratie geschiedt eenmalig via iDIN: zo kan Mijnverzekeringenopeenrij op basis van de – door de banken gevalideerde – geboortedatum, naam en adres op een veilige en gecontroleerde manier de verzekeringsgegevens van de gebruiker bij verschillende verzekeraars tonen. Als alternatief kan ook via iDEAL worden geregistreerd, waarbij de naam wordt gevalideerd door de banken.

De gebruikte attributen worden opgeslagen in het profiel van de gebruiker, die vervolgens met gebruikersnaam en wachtwoord kan inloggen. Andere bankgegevens van de gebruiker blijven altijd onzichtbaar voor het platform.

Een derde optie is een **publiek-private samenwerking** tussen overheid en private partijen. Idensys is daarvan het bekendste voorbeeld. Idensys is een door de overheid geïnitieerd afsprakenstelsel, waarop erkende private partijen authenticatiemiddelen kunnen aanbieden. Dit leidt tot moderne, gebruiksvriendelijke middelen met sterke verificatie en – op het hoogste betrouwbaarheidsniveau – tweefactorauthenticatie. Idensys is inzetbaar in zowel het publieke als private domein en past uitstekend binnen de door de overheid beoogde multimiddelenstrategie. Begin 2018 zijn meerdere Idensys-pilots actief in zowel het publieke als private domein, maar van een brede uitrol is vooralsnog geen sprake.

Waar gaan we heen?

Voortbordurend op 2017 zal verder onderzocht worden welk authenticatiemiddel de meeste potentie/mogelijkheden heeft binnen de verzekeringsbranche: iDIN, Idensys of een ander middel. Onder meer NotarisID en self-sovereign identity-oplossingen, waarbij gebruikers zelf hun identiteit beheren, worden onderzocht. De overheid en de publieke ICT-dienstverlener Logius ontwikkelen ondertussen DigiD door naar een hoger betrouwbaarheidsniveau, waarmee DigiD voorlopig in het publieke domein het belangrijkste (dan wel enige) authenticatiemiddel lijkt. Bekeken moet worden of een – en zo ja, welk – privaat middel daar optimaal naast kan bestaan. Daarbij vormen de (transactie)kosten van het authenticatiemiddel een belangrijk punt. De mogelijkheid van een zogenaamde branche-inkoop zal daarom onderzocht moeten worden: kunnen de transactiekosten laag worden gehouden als met de hele verzekeringsbranche voor hetzelfde authenticatiemiddel wordt gekozen?

3. Zakelijk domein: mens-machine – laag-frequent gebruik

Waar komen we vandaan?

Net als in het consumentendomein, is binnen het zakelijke domein op laag-frequent gebruik over het algemeen gebruikersnaam en wachtwoord de standaard, soms in combinatie met een token. Daarbij is het voornaamste probleem dat geen honderd procent zekerheid kan worden gegeven over de identiteit van de werknemer en/of diens organisatie. Ook dienstverlening via een middle man-constructie is doorgaans niet ingebouwd: machtigingen dienen apart te worden vastgelegd en gekoppeld te worden aan gebruikersnamen.

Waar staan we nu?

Zeer beperkt wordt nu authenticatie met het **Digitaal Paspoort** (van Solera) gebruikt. Dit TLS/SSL-certificaat is relatief duur voor laag-frequent gebruik, zowel in aanschaf als beheer: de *cost of ownership* is zeker bij organisaties met veel werkplekken, die soms een of meer fte hieraan kwijt zijn, erg hoog. Het Digitaal Paspoort is in de praktijk bovendien niet strikt persoonsgebonden. Een alternatief als eHerkenning is dat wel, maar kent geen brede dekking in dit domein: hoewel vrijwel alle bedrijven een eHerkenningsmiddel hebben, geldt dit lang niet voor elke werknemer binnen een bedrijf. Zie de volgende alinea onder ‘waar gaan we heen’ voor meer over eHerkenning.

[1] Zie ook de whitepapers over iDIN en Idensys die SIVI eerder publiceerde: https://www.sivi.org/publicaties/klant-centraal/authenticatie

Waar gaan we heen?

Het verder verkennen van de opties rond het breed gebruik van **eHerkenning** binnen bedrijven is zinvol. eHerkenning is een open stelsel onder toezicht van de overheid, waarop – alleen door de overheid erkende – private leveranciers middelen mogen aanbieden. Voordelen hiervan zijn onder meer een hogere borging van continuïteit, keuzevrijheid tussen makelaars (geen vendor lock-in) en potentieel lagere kosten dankzij de daaruit voortvloeiende marktwerking. Bovendien is een eHerkenningsmiddel niet gebonden aan een werkplek: in tegenstelling tot het Digitaal Paspoort hoeven bij eHerkenning geen kopieën te worden gemaakt bij gebruik van het authenticatiemiddel in een andere browser of terminal.

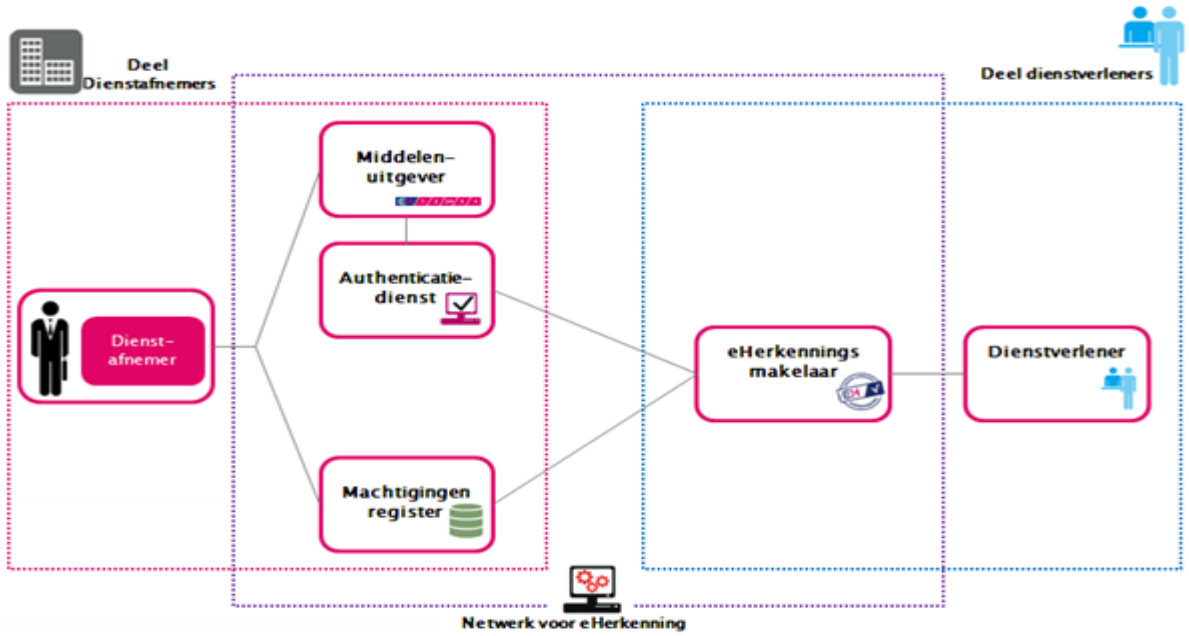
Aansluiting op eHerkenning gaat in twee delen. Enerzijds moeten gebruikers allemaal een eHerkenningsmiddel aanschaffen bij één van de eHerkenningsmakelaars in hun rol als middelenuitgever (zie ook Figuur 2). Dit is relatief eenvoudig. Anderzijds moeten dienstverleners aansluiten op het eHerkenningsstelsel, ook bij één van de makelaars – maar niet per se dezelfde. Hoewel de technische aansluiting eenvoudig is en kan worden uitbesteed, zit een uitdaging in het koppelen van nu bekende gebruikersgegevens aan de attributen die straks binnenkomen via eHerkenning. Bij succesvolle authenticatie krijgt de dienstverlener binnen eHerkenning altijd naam, geboortedatum, bedrijfsnaam en KvK-nummer. Het Digitaal Paspoort is echter gekoppeld aan een e-mailadres: er zit dan ook een uitdaging in het koppelen van gebruikers die nu het Digitaal Paspoort gebruiken en straks overstappen op eHerkenning.

Dienstverlening via middle man

Een belangrijke eis aan zakelijke authenticatiemiddelen is de mogelijkheid van een middle man-constructie. Hierbij machtigt een gebruiker een andere gebruiker namens hem/haar een bepaalde dienst af te nemen. Bijvoorbeeld een service provider die namens een intermediair inlogt bij een verzekeraar.

Bij het Digitaal Paspoort wordt deze constructie niet ondersteund. In de huidige situatie leent de gebruiker zijn/haar eigen Digitaal Paspoort uit – of verstrekt een kopie ervan – aan de middle man. Naast veiligheidsissues zorgt dit ook voor een gebrek aan herkenbaarheid: de dienstverlener denkt immers dat de gebruiker zelf inlogt, zonder gebruik te maken van een middle man.

Een mogelijke oplossing is een contractuele machtiging van de middle man. Intermediair, middle man en verzekeraar gaan een drie-partijen-overeenkomst aan, waarin de intermediair de middle man machtigt om namens hem transacties te doen bij de verzekeraar. Dankzij deze overeenkomst hoeft de verzekeraar niet de intermediair te authenticeren, en kan volstaan worden met de authenticatie van de middle man. Uiteraard dient daarbij wel gecontroleerd te worden of de middle man bevoegd is om namens de betreffende intermediair te handelen. Deze controle kan de verzekeraar intern en geautomatiseerd uitvoeren, door een machtigingsregister bij te houden.



Figuur 2: schematische weergave van het eHerkenningsstelsel (bron: eherkenning.nl)

Naast eHerkenning zal verder moeten worden geïnventariseerd naar het beste middel voor dit domein. Ook hier speelt de vraag om een machtigingenstructuur: vooral rond tussenpersonen die namens een dienstverlener transacties uitvoeren. Zie ook het kader over dienstverlening via middle man.

4. Zakelijk domein: mens-machine – hoog-frequent gebruik

Waar komen we vandaan?
Hierin is het Digitaal Paspoort (voorheen uitgegeven door ABZ, inmiddels overgenomen door Solera) de facto al twintig jaar de branchestandaard, een bedrijfsgebonden certificaat op basis van het TLS/SSL-protocol. Dit certificaat wordt lokaal geïnstalleerd in de browser van de werknemer.

Waar staan we nu?
Begin 2018 zijn ongeveer 33.000 **Digitaal Paspoort**-certificaten in omloop. Een Digitaal Paspoort is echter relatief eenvoudig te kopiëren en/of uit te lenen aan anderen binnen de organisatie en keten. Mede hierdoor zijn ze in de praktijk niet persoonsgebonden. Tevens zijn Digitaal Paspoort-certificaten niet geschikt voor dienstverlening via een middle man-constructie, zoals een service provider: in dergelijke gevallen wordt het Digitaal Paspoort nu uitgeleend aan de middle man, die zich als het ware voordoet als degene wiens belangen hij behartigt. Een eigen, persoonlijk authenticatiemiddel met een machtiging kan daar de oplossing bieden. Bij organisaties met veel werkplekken is, door het complexe beheer van TLS/SSL-certificaten, de *cost of ownership* bovendien erg hoog.

Naast het Digitaal Paspoort wordt nu dikwijls **eHerkenning** los gebruikt. Dit open stelsel is veilig, persoonsgebonden en breed inzetbaar. Single sign-on is nu geregeld via een tussenoplossing: zolang je als gebruiker van dezelfde herkenningsmakelaar (dus van hetzelfde authenticatiemiddel) gebruik maakt, hoef je nu (binnen een bepaalde tijd) niet opnieuw in te loggen. Idealiter wordt dit nog voor het hele eHerkenningsstelsel, los van welk authenticatiemiddel je gebruikt, geregeld. Zie voor meer info over eHerkenning het stuk hierboven onder ‘laag-frequent gebruik’.

De dienstverlening van ABZ wordt momenteel ondergebracht bij een dochteronderneming van Solera (Digidentity), wat leidt tot een nieuwe inrichting van diensten en services – waaronder ook het Digitaal Paspoort. Solera/Digidentity heeft eind 2017 aangegeven voornemens te zijn het gebruik van dergelijke SSL-certificaten anders in te richten. Dit roept de vraag op of dit nog wel de standaard is en/of andere opties moeten worden verkend. Tevens wordt het hiermee noodzakelijk om de gemaakte beveiligingsafspraken rondom zakelijke authenticatie opnieuw tegen het licht te houden, en zowel scenario’s als requirements op te stellen rond de uitfasering van het Digitaal Paspoort.

Waar gaan we heen?
Voor 2018 is de uitfasering van het Digitaal Paspoort een belangrijk onderwerp, in combinatie met de rol van eHerkenning of een ander authenticatiemiddel als nieuwe de facto branchestandaard. De voorgenomen uitfasering van het Digitaal Paspoort maakt het noodzakelijk om te anticiperen op alternatieve authenticatiemiddelen en om daar heldere, branchebrede requirements voor op te stellen. Als mogelijk onderdeel daarvan zal ook voor dit domein moeten worden onderzocht of behoefte is aan – en ruimte is voor – een branchebrede machtigingenstructuur.

5. Zakelijk domein: machine-machine

Waar komen we vandaan?
Binnen het gebied van machine-machine-authenticatie is het ABZ-bedrijfscertificaat (kortweg ABC) van Solera al twintig jaar de facto de branchestandaard. Dit is een bedrijfsgebonden TLS/SSL-certificaat gekoppeld aan het KvK-nummer.

Waar staan we nu?
Er zijn momenteel ca. 3000 ABC’s in omloop, waarlangs jaarlijks zo’n 50.000.000 transacties worden gerouteerd. Het TLS/SSL-protocol is bovendien nog steeds de belangrijkste, veiligste standaard en de standaardtechnologie voor afhandeling van webservices binnen gangbare platformen. De facto is ABC daarmee de standaard binnen de branche, al ontbreekt goede documentatie.

Waar gaan we heen?
Het ABC zal blijven moeten voldoen aan de nieuwste normen. Daarbij hoort bijvoorbeeld de doorontwikkeling van ABC naar TLS 1.3, en het verbeteren/uitbreiden van de documentatie.

6. SIVI-agenda

In het **consumentendomein** wordt onderzocht welk authenticatiemiddel de meeste potentie/mogelijkheden heeft binnen de verzekeringsbranche: iDIN, Idensys of een ander middel. Dit kan een privaat middel zijn of een publiek-private samenwerking, dat naast het voor het publieke domein doorontwikkelde DigiD kan bestaan. Ondertussen worden ontwikkelingen op het gebied van wetgeving in de gaten gehouden. Na de invoering van de AVG zijn nu de **Wet Digitale Overheid** (2019) en **eIDAS-verordening** (september 2018) op komst. Beide hebben naar verwachting grote impact op dienstverleners wat betreft eisen aan authenticatie en beveiliging.

Zakelijk wordt in het mens-machine-domein gekeken hoe de toekomst eruitziet rond het Digitaal Paspoort. Verschillende scenario's worden onderzocht en uitgediept, waaronder het grootschalig gebruik van het persoonsgebonden eHerkenning en mogelijke continuering van het Digitaal Paspoort. Deze scenario's worden getoetst aan de hand van opgestelde requirements voor zowel laag-frequent als hoog-frequent gebruik. Belangrijke issues hier zijn single sign-on op hoog-frequent gebruik en dienstverlening via een middle man. Voorts speelt natuurlijk de hoogte van de kosten, en wie daarvoor moet opdraaien, een belangrijke rol in de keuze voor een van de scenario's.

Algemeen ligt de vraag rond het instellen van een **machtigingenstructuur**. Zowel in het consumenten- als het zakelijke domein wordt gekeken hoe de rol van tussenpersonen kan worden gefaciliteerd binnen de wereld van authenticatie en autorisatie. Zowel vanuit de eisen rond toezicht (audit trails, fraudedetectie, etc.) en de toepassing van de Wft en AVG, als vanuit de wens om op ordentelijke wijze met authenticatiemiddelen om te gaan.

Voor vragen en reacties

Robin Oostrum
06-53398893
Robin.Oostrum@sivi.org