Beroepscertificaten en geattesteerde beroepskwalificaties

Vision paper

HOUSE OF TRUST

HOUSE OF TRUST

Inhoud

House of Trust is een uniek team van professionals dat in korte tijd een gekwalificeerde vertrouwensdienstverlener heeft ontworpen, opgezet en laten certificeren volgens de eisen van de eIDAS-verordening. Wij ondersteunen organisaties die vertrouwen in de digitale samenleving op het hoogste niveau willen implementeren. Onze aanpak is navolgbaar, verantwoordbaar en certificeerbaar, waardoor de dienst als 'gekwalificeerd' wordt aangemerkt conform de eIDAS-verordening.

Auteur: Koen Bonnet, Service Designer

Versiedatum: 28 augustus 2024

HOUSE OF TRUST

Samenvatting

In deze 'vision paper' beschrijven we onze visie op 'Integrale Beroepscertificaten'. Waar op dit moment beroepscertificaten een betrekkelijk statische weergave van een beperkt deel van de identiteit van een beroepsbeoefenaar is, is het Integrale Beroepscertificaat een combinatie van enerzijds een elektronisch certificaat voor ondertekening en authenticatie en anderzijds een dynamische set identiteitskenmerken, beroepskwalificaties en bevoegdheden.

In dit document zullen we de verschillende aspecten van beroepscertificaten en geattesteerde beroepskwalificaties verkennen. Eerst zullen we ingaan op de huidige stand van zaken rondom beroepscertificaten, inclusief hun rol en beperkingen. Hierna volgt een bespreking van kwalificaties en bevoegdheden en hoe deze digitaal vastgelegd kunnen worden.

Vervolgens behandelen we de relevante wetgeving, met name de eIDAS-verordening en haar implicaties voor digitaal vertrouwen. Tenslotte introduceren we het concept van Integrale Beroepscertificaten en onderzoeken we de voordelen en uitdagingen die gepaard gaan met hun implementatie.

Integrale Beroepscertificaten zijn elektronische certificaten die, beheerd via een mobiele applicatie - de Wallet -, niet alleen de identiteit van een beroepsbeoefenaar aantoont, maar ook aanvullende geattesteerde identiteitskenmerken bevatten in de vorm van Verifiable Credentials. Deze 'Integrale Beroepscertificaten' bieden een moderne en efficiënte manier voor professionals om hun identiteit, consent, kwalificaties en bevoegdheden te delen, terwijl ze voldoen aan zowel Europese als wereldwijde standaarden voor vertrouwen en veiligheid.

De nieuwe eIDAS-regelgeving biedt een solide basis voor de ondersteuning van Integrale Beroepscertificaten. Deze regelgeving zorgt ervoor dat digitale certificaten en geverifieerde identiteitskenmerken op een uniforme en betrouwbare manier kunnen worden gedeeld en vertrouwd binnen Europa. Echter, doordat sommige vertrouwensdiensten en aspecten van de regelgeving nieuw zijn, zijn er op dit moment ook nog onduidelijkheden die in de praktijk moeten worden uitgekristalliseerd.

Een belangrijke overweging voor (beroeps-)organisaties die met Beroepscertificaten willen werken, is of zij voor de uitgifte en het beheer van deze certificaten gebruik willen maken van een externe leverancier, of dat het voordeliger en efficiënter is om de benodigde infrastructuur

en organisatie zelf in te richten. Deze beslissing kan invloed hebben op de kosten, de controle over processen en de snelheid van implementatie.

Het is essentieel voor organisaties om deze factoren zorgvuldig af te wegen en te bepalen welke aanpak het beste aansluit bij hun behoeften en doelen.

House of Trust is een uniek team van professionals dat in korte tijd een gekwalificeerde vertrouwensdienstverlener heeft ontworpen, opgezet en laten certificeren volgens de eisen van de eIDAS-verordening. Wij ondersteunen organisaties die vertrouwen in de digitale samenleving op het hoogste niveau willen implementeren. Onze aanpak is navolgbaar, verantwoordbaar en certificeerbaar, waardoor de dienst als 'gekwalificeerd' wordt aangemerkt conform de eIDAS-verordening. Ons team staat klaar om toekomstige TSP's en QTSP's te ondersteunen met het implementeren en laten certificeren van hun diensten. Lees meer over onze diensten op www.eidas-vertrouwensdiensten.nl of neem contact met ons op via info@eidas-vertrouwensdiensten.nl.

Beroepscertificaten

Met beroepscertificaten kunnen beroepsbeoefenaren hun identiteit en lidmaatschap van hun beroepsgroep aantonen. Beroepscertificaten worden gebruikt in online omgevingen om artsen, notarissen, accountants, advocaten en zorgprofessionals te laten inloggen op systemen en elektronische handtekeningen te zetten.

De meeste beschermde beroepen hebben een vorm van een beroepscertificaat, zoals de UZI-pas in de zorg, de NOvA-pas in de advocatuur, het NBA Beroepscertificaat voor accountants en het beroepscertificaat binnen het notariaat dat gereguleerd wordt door de KNB.

Beroepscertificaten zijn persoonsgebonden en worden–net zoals alle elektronische certificaten met een hoge betrouwbaarheid– uitgegeven in een gecontroleerd uitgifteproces. In zo'n uitgifteproces wordt typisch de relatie gelegd tussen identiteitsbrongegevens zoals een paspoort, de beoogde houder van het elektronische certificaat en het persoonlijke 'token' waarmee de elektronische identiteit aangetoond kan worden. Zo'n token is vaak een USB-sleutel, een smartcard of, in toenemende mate, een smartphone.

Voor een beroepscertificaat wordt aan dit 'identity proofing'-proces een aspect toegevoegd, namelijk lidmaatschap van de beroepsgroep in kwestie. De uitgevende partij moet dan beschikken over (of alternatief toegang hebben tot) een betrouwbaar register, bijvoorbeeld van de beroepsorganisatie, waarin het ondubbelzinnig kan vaststellen dat de beoogde houder van de elektronische identiteit is opgenomen in dat register en dat er geen bezwaren bestaan tegen beroepsbeoefening.

De uitgifte van en controle op beroepscertificaten is in de praktijk een implementatie van een 'Public Key Infrastructure' (PKI). Dit is een set aan afspraken en standaarden om een sleutelpaar te genereren, waarbij de privé-sleutel onder beheer van de houder staat en met de publieke sleutel gecontroleerd kan worden dat de houder instaat voor ontvangen berichten, instemming, etc. Een hogere autoriteit staat in voor de betrouwbaarheid van de sleutels en de manier waarop die zijn uitgegeven. Dat vertrouwen is inzichtelijk en navolgbaar door ondertekening van de publieke sleutel door die hogere autoriteit.

Door gebruikmaking van deze standaarden is de manier waarop de identiteit en de wil van de houder wordt uitgedrukt gestandaardiseerd en daarmee ook de manier waarop dat te controleren is. Het is gestandaardiseerd hoe bijvoorbeeld de voornaam en achternaam van de houder gelezen kan worden uit het certificaat dat bij een handtekening hoort. Ook kan de 'hogere autoriteit' die instaat voor de betrouwbaarheid van de certificaten communiceren dat certificaten niet langer betrouwbaar zijn, bijvoorbeeld door verlies van de 'token'.

Terwijl een aantal basiskenmerken van de identiteit van de houder zijn gestandaardiseerd, zoals voornaam, achternaam en e-mailadres, is gebruik van identificerende kenmerken niet verplicht en is het aantal gestandaardiseerde kenmerken beperkt. Het is daarmee met elektronische certificaten van een enkele uitgever niet mogelijk om buiten het eigen 'ecosysteem' gestandaardiseerd aan te geven dat de houder specifieke kwalificaties of bevoegdheden heeft, zoals de kwalificatie 'kandidaat' in het notariaat of specifieke bevoegdheden in de zorg. Deze beperking wordt in de praktijk soms opgelost door voor grove opdelingen van de beroepsgroep verschillende groepen certificaten uit te geven waardoor aan de uitgever van het certificaat te herkennen is tot welke deelgroep de houder behoort. Dit is omslachtig en duur door de consequenties voor de inrichting van de Public Key Infrastructure en juiste herkenning en autorisatie op basis daarvan stelt eisen aan het gehele ecosysteem.

Praktisch genomen is het opnemen van identificerende kenmerken in een elektronisch certificaat wel een vorm van attribuut-attestatie, maar deze optie is beperkt omdat het een statisch geheel vormt. Bovendien voorziet de herziene eIDAS verordening niet direct in expliciete erkenning van deze aanpak onder de noemer Attribuut-attestatie (zie verderop).

HOUSE OF TRUST

Kwalificaties en bevoegdheden

Naast de identificatie van personen en beroepsbeoefenaren bestaat er ook behoefte aan het kunnen werken met digitale vastleggingen van kwalificaties en bevoegdheden. Dit laat zich het beste uitleggen aan de hand van voorbeelden uit de Nederlandse zorg. Naast dat zorgprofessionals zich als zodanig kunnen identificeren met behulp van de UZI-pas, bestaat er ook het BIG-register. Met behulp van het BIG-register kunnen geïnteresseerden vaststellen welke beroepstitel de zorgverlener mag dragen. Het CIBG houdt het register bij op basis van diploma's, criteria voor (her)registratie (zoals voldoende werkuren in het beroep) en de afwezigheid van beroepsbeperkende maatregelen.

In omgevingen met grote risico's voor de veiligheid worden beroepsbeoefenaren geacht continue training te volgen. Als training op onvoldoende peil is, dan kan de beroepsgroep, een werk- of opdrachtgever besluiten de beroepsbeoefenaar niet langer toe te laten op de opdracht. Dit is relevant in technische beroepen, waarbij bijvoorbeeld een lasser met onvoldoende of verouderde competenties niet toegelaten wordt tot opdrachten op een bouwplaats. Vergelijkbare eisen en maatregelen spelen in andere beroepsgroepen, zoals de zorg of luchtvaart.

Hoewel er een standaard bestaat voor het werken met digitaal vastgelegde kwalificaties en bevoegdheden, wordt die nog niet altijd gebruikt. Zo zijn veel beroepsregisters, zoals het BIG-

register, gebaseerd op een traditionele database en website met zoekmogelijkheden. De 'Verifiable Credentials' standaard wordt beheerd door W3C, de internationale organisatie die webstandaarden ontwikkelt en beheert. 'Verifiable Credentials' wordt vaak genoemd in de context van de 'Self-Sovereign Identity', omdat Verifiable Credentials zijn ontworpen met privacy als fundamenteel uitgangspunt.

Credly (nu onderdeel van Pearson) is een bekend platform waarmee opleidingsinstituten cursisten in staat stellen om het feit dat een competentie is verjaard te delen met belanghebbenden. Credly gebruikt (onder meer) Verifiable Credentials om dit te doen. Ook het Centraal Register Techniek is bezig om op deze manier van technisch personeel inzichtelijk te maken wie welke competentie heeft, zodat de juiste persoon aan de juiste klus op de bouwplaats wordt gekoppeld en fysieke veiligheid en verantwoording gewaarborgd is.

Dergelijke 'competentiepaspoorten' staan op dit moment nog altijd los van de gangbare opvatting over beroepscertificaten. Met de herziening van de Europese eIDAS-verordening, ook wel aangeduid als eIDAS2, ontstaat een geharmoniseerd model voor (beroeps-)certificaten in combinatie met geverifieerde identiteitskenmerken.

HOUSE OF TRUST

Digitaal vertrouwen verankerd in wetgeving

De eIDAS-verordening uit 2014 (Verordening (EU) nr. 2014/910) ziet erop toe dat digitaal vertrouwen in de wet verankerd wordt en is verplicht opgenomen in nationale wetgeving in heel Europa. Deze eerste eIDAS verordening introduceerde verschillende vertrouwensdiensten en drie niveau's van betrouwbaarheid waarop die aangeboden kunnen worden. Met name voor het hoogste betrouwbaarheidsniveau schrijft het eIDAS-stelsel, met inbegrip van de clausules voor en de implementatie van conformiteitsbeoordeling, gedetailleerde organisatorische en technische normen voor die door ETSI worden opgesteld en beheerd.

Dit hoogste betrouwbaarheidsniveau wordt behaald als de dienst en organisatie als "Gekwalificeerd" ("Qualified") wordt ingericht en ook zo wordt beoordeeld door het conformiteiten-beoordelingsinstituut. Wanneer we in deze vision paper praten over vertrouwensdiensten of vertrouwensdienstverleners, dan bedoelen we die telkens als Gekwalificeerd.

Door vertrouwensdiensten, zoals die voor de uitgifte van elektronische (beroeps)certificaten, in te richten op basis van deze ETSI-normen en dit te laten certificeren door een conformiteitsbeoordelingsinstituut, wordt de dienst opgenomen op de Europese vertrouwenslijst en door heel Europe beschouwd als 'betrouwbaar'. Dat betekent onder meer dat, in geval van een elektronische handtekening die werd gezet met een gekwalificeerd elektronisch (beroeps)certificaat, deze niet meer geweigerd kan worden alleen om het feit dat

hij digitaal is. Een gekwalificeerd geattesteerd identiteitskenmerk moet als net zo authentiek worden beschouwd als die kenmerken op papier met stempel en watermerk. Daarmee hebben dergelijke digitale wilsuitingen dezelfde rechtskracht als een 'natte' handtekening.

In 2023 is de eIDAS-verordening herzien via besluit 32024R1183. Belangrijke wijzigingen zijn dat 'attribuut-attestatie' als vertrouwensdienst is toegevoegd en de Europese Identity Wallet als concept is toegevoegd. De wijzigingen zorgen voor een nieuw mogelijk perspectief op identificatie door beroepsbeoefenaren, omdat er nu gereguleerde vertrouwensdiensten worden beschreven voor zowel authenticatie ondertekening met behulp van elektronische certificaten als het delen van geverifieerde identiteitskenmerken op basis van attribuut-attestatie. Door bovendien nu te beschrijven dat elektronische ondertekening kan plaatsvinden op basis van een op afstand beheerde privésleutel ('remote signing'), ontstaat de mogelijkheid om de gehele werking aan te bieden vanuit de zogenoemde 'EUID Wallet'.

Attribuut-attestatie is een vertrouwensdienst waarbij de bronbeheerder van identificerende kenmerken deze attesteert door elektronische ondertekening ervan en deelt met derden, idealiter de persoon waarop ze betrekking hebben. Omdat de gegevens ondertekend zijn op een navolgbare manier, kunnen de kenmerken verder gedeeld worden, waarbij de ontvanger ervan opnieuw kan vaststellen dat ze zijn geattesteerd door de authentieke bron.

Het CIBG kan gezien worden als bronbeheerder van zorgverleners en de disciplines waarin die werkzaam mogen zijn. Het RDW is bronbeheerder van personen en hun bevoegdheden om een motorvoertuig te mogen besturen. In de vertrouwensdienst 'Attribuut-attestatie' worden die gegevens als 'attributen' (identiteitskenmerken) door hen geattesteerd om volgens gedeeld te kunnen worden met belanghebbenden.

Het beoogde middel om dergelijke identiteitsgegevens mee te delen is de Wallet. Hiervoor zal de Europese Commissie 'implementation acts' uitvaardigen, maar dat is op dit moment nog niet gebeurd. Algemeen wordt aangenomen dat er gedoeld wordt op implementaties die een app op de mobiele telefoon implementeren die functioneert als schakelpunt voor gebruikers om gegevens fijnmazig te kunnen delen met door hen geselecteerde belanghebbenden. Er zijn inmiddels al initiatieven om een dergelijke Wallet te ontwikkelen, omdat wordt verwacht dat snelle toetreding tot de markt zal zorgen voor een groot marktaandeel en dat het platform-adagium 'The winner takes all' van toepassing zal zijn.

De traditionele wijze van distributie van (beroeps-)certificaten is lastig verenigbaar met de Wallet, omdat in die aanpak alle ondertekeningen (inclusief die van authenticatie) verzoeken via

de mobiele telefoon zouden moeten verlopen, wat een scala aan uitdagingen oplevert. De bijgewerkte eIDAS-verordening voorziet echter ook in de mogelijkheid van 'Remote Signing', waarbij de privésleutel waarmee getekend wordt centraal wordt beheerd door de vertrouwensdienstverlener en ondertekenverzoeken in de Cloud kunnen worden afgehandeld. Het geven van toestemming ('consent') op het gebruik van de privésleutel kan eenvoudiger verlopen via een app op de mobiele telefoon, hoewel eenvoud relatief is met het oog op de te hanteren ETSI-normen.

Integrale Beroepscertificaten

Een integraal beroepscertificaat bestaat op een elektronisch certificaat onder beheer van de beroepsbeoefenaar via de Wallet. Hierbij is de Wallet een app op de mobiele telefoon van de beroepsbeoefenaar. Maar het integraal beroepscertificaat wordt bovendien vergezeld door 'Verifiable Credentials', waarbij die worden geïmplementeerd als geattesteerde attributen in de zin van de regelgeving.

Integrate Beroepscertificaten zorgen voor een gebruiksvriendelijke manier voor beroepsbeoefenaren om zichzelf te identificeren en bovendien om fijnmazig gegevens te delen over kwalificaties en bevoegdheden. Door de verankering in Europese en nationale wetgeving kan vertrouwen grensoverschrijdend gegarandeerd worden en door gebruik te maken van beschikbare standaarden kan het vertrouwen wereldwijd ingebed worden in systemen.

Onderwerpen die speciale aandacht behoeven is de implementatie van praktisch en betrouwbaar 'Consent' bij toepassing van remote signing dan wel ondertekening op het mobiele apparaat. Dit is een overweging bij het ontwerp van de dienst waar goed stilgestaan moet worden bij de vereist exclusiviteit op beheer van de privésleutel, de noodzakelijkheid van die sleutel tijdens ondertekening, het gebruiksgemak en het certificeringsniveau van het mobiele apparaat als die als 'Qualified electronic Signature Creation Device' (QSCD) moet dienen.

Daarnaast is de regelgeving van de herziene eIDAS-verordening gedeeltelijk nieuw en zijn op dit moment de (ETSI-)normen nog niet vastgesteld voor de nieuwe vertrouwensdiensten. Hoewel de normen voor al bestaande vertrouwensdiensten enig houvast kunnen bieden, is de vertrouwensdienst voor attribuut-attestatie nog nooit geïmplementeerd en zijn ook de conformiteitsbeoordelaars er niet mee bekend. Hier moet rekening mee worden gehouden in het plannen van een implementatie van attribuut-attestatie.

Tenslotte is de Verifiable Credentials standaard ontworpen om de persoon waarop de identiteitskenmerken (kwalificaties en bevoegdheden) betrekking hebben de regie te geven in het delen. In de praktijk kunnen bronbeheerders ook de verantwoordelijkheid hebben om gegevens over die personen te delen met belanghebbenden. Delegatie van rechten is geen onderdeel van de Verifiable Credentials standaard, maar wel een essentiële mogelijkheid.

eIDAS beschrijft verschillende betrouwbaarheidsniveaus van de vertrouwensdiensten. Om op het hoogte niveau te opereren met zogenaamde “gekwalificeerde” vertrouwensdiensten moet een aanzienlijke set aan technische en organisatorische normen worden geïmplementeerd. Als gebruik gemaakt wordt van een leverancier voor deze diensten, dan is een deel van de nomen van toepassing op de leverancier en een deel van toepassing op de (beroeps-)organisatie die instaat voor de identiteitsgegevens. Daarnaast kan bij met name bij attribuut-attestatie de hoeveelheid transacties groot zijn waardoor kosten ook zullen toenemen. Dit zijn argumenten in de overweging of de (beroeps-)organisatie zelf de infrastructuur en processen inricht voor de uitgifte van Integrale Beroepscertificaten of dat ze worden betrokken van een leverancier.

HOUSE OF TRUST

Referenties

eIDAS EU-verordening

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

Besluit tot herziening eIDAS-verordening

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32024R1183

Verifiable Credentials Data Model:

https://www.w3.org/TR/vc-data-model/

Selective Disclosure -JSON WebToken Verifiable Credentials:

https://www.ietf.org/archive/id/draft-ietf-oauth-sd-jwt-vc-00.html