Connectis

Co-financed by the European Union
Connecting Europe Facility

Overzicht eIDAS en eHerkenning juli 2018

EH ontwikkelingen gerelateerd aan eIDAS

Werking van de eIDAS-keten

Diensten afnemen via de eIDAS-keten werkt globaal als volgt[1]. Een EU-burger bezoekt de website van een Nederlandse dienstverlener, klikt op de eIDAS- inlogknop en logt in met een erkend nationaal inlogmiddel. De Nederlandse dienstverlener stuurt een authenticatieverzoek naar de eHerkenningsmakelaar (hierna te noemen; makelaar). Dat verzoek gaat van de makelaar via de Berichtenservice en de eIDAS connector naar de buitenlandse authenticatiedienst.

Bij een positief authenticatieresultaat vraagt de Berichtenservice het BRPk de gegevens van de gebruiker te matchen met de BRP. BRPk levert (indien beschikbaar) het bijbehorende BSN versleuteld aan de Berichtenservice. De berichtenservice zet het versleutelde BSN door naar het BSNk. Vervolgens zorgt het BSNk voor versleuteling naar een (polymorf) pseudoniem en een versleutelde identiteit die uitsluitend door de beoogde dienstverlener is te ontsleutelen.
De Berichtenservice geeft het pseudoniem door (via de makelaar) aan de dienstverlener die het pseudoniem kan ontsleutelen en matchen met zijn eigen gegevens. Verder draagt het bij aan compartimentering binnen het stelsel en draagt daarmee bij aan het (AVG- compliant) waarborgen van de privacy van burgers. Per dienstverlener per middel wordt een ander pseudoniem gemaakt[2]. Zo is voor individuele dienstverleners niet zichtbaar wat de burger bij andere dienstverleners aan diensten afneemt. De gegevens over dienstverleners heen zijn niet op basis van de pseudoniem te aggregeren. Dit is een van de privacy beschermende maatregelen.

Er is een korte periode waarin de eIDAS-verordening van kracht is en er nog geen BSN-matching plaatsvindt. Eindgebruikers komen in die periode uit op een landingspagina met de volgende (strekking van de) boodschap: “Wij hebben uw middel kunnen lezen, maar op dit moment onvoldoende gegevens om de dienstverlening te starten.”
Na livegang van de gehele eIDAS-keten is BSN-matching voorzien en kan de eindgebruiker ook BSN-diensten afnemen, indien hij/zij beschikt over een BSN.

[1] In geval van een BSN-dienst, waarbij de gebruiker voor het eerst inlogt en de gebruiker een BSN heeft die wordt herkend.
[2] Het polymorfe pseudoniem is steeds hetzelfde. Dat wordt immers ook bij de Berichtenservice opgeslagen. Er wordt gebruik gemaakt van een (1) Versleutelde Identiteit (VI) voor een op het BSN gebaseerde dienstverlener specifieke sleutel en een (2) Versleuteld Pseudoniem (VP) voor een op het UID gebaseerde dienstverlener specifieke sleutel.

Releases 1.11 en Servicepack van de herkenningsmakelaar

De eIDAS-keten komt in twee stappen beschikbaar: (1) release 1.11 (sinds maart 2018 beschikbaar) en (2) Servicepack (vanaf eind juli 2018 beschikbaar). Deze releases hebben betrekking op (1) het koppelvlak tussen de makelaar en de dienstverlener en (2) een wijziging van het koppelvlak van de Berichtenservice en de makelaar[3].
Het koppelvlak tussen de Berichtenservice en het BSNk enerzijds en de Berichtenservice en het BRPk anderzijds zijn buiten scope van de makelaars. Die worden namelijk ontwikkeld door respectievelijk RVO (Berichtenservice), RVIG (BRPk) en Logius (BSNk)[4].

Bouwstenen van de eIDAS-infrastructuur

Een toelichting op de onderdelen van de eIDAS-keten:

- eIDAS knooppunt; iedere lidstaat heeft een eIDAS knooppunt; dit werkt als verbindingspunt tussen de lidstaten. Berichten van en naar Nederland gaan via het eIDAS knooppunt.
- Berichtenservice (RVO); de Berichtenservice heeft een koppeling met alle ketenpartners: het BRPk, het BSNk, de makelaars en het eIDAS knooppunt. Overige ketenpartners hebben vooralsnog geen directe koppeling met elkaar. Vanaf release 1.13 is er een koppeling tussen de makelaar en BSNk voor de uitgifte van het sleutelmateriaal voor dienstverleners.
- BRPk (RvIG); het BRPk controleert of de gebruiker bekend is met een BSN in het BRP. Indien dit het geval is, zorgt het BRPk voor het versleutelen van het BSN en levert dit aan de Berichtenservice.
- BSNk (Logius); het BSNk genereert op basis van het (versleutelde) BSN een pseudoniem en maakt van een PP-BSN een Versleutelde Identiteit en levert dit aan de Berichtenservice.
- Makelaar; de makelaars fungeren als tussenpersoon tussen de dienstverlener en de Berichtenservice. Zij ondersteunen de dienstverlener bij aansluiten.

[3] Het koppelvlak van RVO maakt berichtuitwisseling tussen de Berichtenservice en de herkenningsmakelaar mogelijk.
[4] RVO, RvIG en Logius noemen hun release na 1.11 ook Servicepack waardoor het lijkt alsof het om dezelfde release gaat (en van de eTD-makelaar afhankelijk is), maar dat is niet het geval.

Release 1.11

Vanaf het tweede kwartaal van 2018 kunnen dienstverleners aansluiten op het eIDAS compliant koppelvlak van hun makelaar. Met deze release kan de dienstverlener diensten aanbieden die geen BSN vereisen. Alle dienstverleners zijn met de implementatie van het 1.11 koppelvlak eIDAS-compliant. Deze release is vooral geschikt voor dienstverleners met diensten die geen BSN vereisen, dienstverleners die in stappen willen aansluiten, of dienstverleners die een van de andere nieuwe eTD functionaliteiten uit 1.11 willen gebruiken.

Servicepack[5]

De makelaars stellen vanaf eind juli 2018 het Servicepack beschikbaar. Het Servicepack voorziet in een nieuw koppelvlak tussen de makelaar en de Berichtenservice. Het koppelvlak tussen de makelaar en de dienstverlener wijzigt niet tussen 1.11 en Servicepack. Het vraagt van dienstverleners echter wel enige aanpassing in de configuratie(s). Deze release biedt dienstverleners de mogelijkheid om alvast de eigen systemen en processen gereed te maken om versleutelde identiteiten (naar een BSN) of versleutelde pseudoniemen (naar een pseudo van de uniqueness identifier) te kunnen ontsleutelen[6].

Vanaf eind oktober verstrekt de eIDAS-keten naar verwachting over dit koppelvlak de polymorf versleutelde identiteiten en/of pseudoniemen aan de dienstverlener als die daartoe verzoekt. Dat vraagt van de dienstverlener een implementatie om aan te kunnen geven of het gaat om een BSN-verplicht-, BSN-optioneel- of non-BSN- dienst en om de polymorf versleutelde identiteiten en/of pseudoniemen[7] te kunnen uitvragen, ontvangen, uitpakken en ontsleutelen.

In de periode tot september krijgen Duitsers die inloggen met hun nPA bij een aangesloten dienstverlener voor een BSN-dienst de melding dat inloggen is gelukt maar dat de dienst nog niet beschikbaar is. Deze melding wordt standaard gegeven door de Berichtenservice totdat de gehele eIDAS-keten in productie is[8].

Mijlpalen realisatie eIDAS

Hieronder zijn de drie mijlpalen van het eIDAS realisatie project samengevat:

[5] Voor het uitwisselen van het BSN moeten behalve het Servicepack ook het BRPk en de koppeling tussen de Berichtenservice en het BRPk gereed zijn. De gehele eIDAS- infrastructuur is in sep/okt gereed. Om die reden maakt het realisatieoverleg onderscheid tussen een fase waarin geen BSN en wel een BSN geleverd kan worden over het Servicepack koppelvlak. Voor de eTD-makelaar en dienstverlener is er technisch geen verschil in de koppeling, wél in de gegevens die zij ontvangen en de verwerking daarvan in hun eigen systemen.
[6] In een testomgeving zijn hiertoe mogelijk dummy BSN's beschikbaar.
[7] pseudoniem of BSN.
[8] Dit is nu in eerste instantie afgevangen doordat RVO (EB) een melding toont wanneer er een BSN ECTA wordt uitgevraagd.

Release	Gereed	Toelichting
1.11	Maart 2018	• Dienstverleners zijn na aansluiten *de jure* tijdig eIDAS compliant (en *de facto* voor niet BSN- diensten) • Dienstverleners ontvangen nog geen BSN • Dienstverleners ontvangen een unieke identifier van de EU-burger én de verplichte eIDAS attributen
Servicepack (1.12)	Juli 2018	• Dienstverleners zijn na aansluiten *de jure* tijdig eIDAS compliant • De eIDAS-keten biedt dienstverleners de gelegenheid zich voor te bereiden op het uitpakken van polymorfe identiteiten en/of pseudoniemen • Dienstverleners ontvangen nog geen BSN of een polymorfe identiteit en/of pseudoniem (daartoe moet de gehele eIDAS-keten gereed zijn)[9] • Dienstverleners ontvangen een unieke identifier van de EU-burger en de verplichte eIDAS attributen
1.13	Q4 2018	• Dienstverleners zijn na aansluiten *de facto* eIDAS compliant voor zowel niet als wel BSN-diensten • BSN via makelaars • Dienstverleners ontvangen een versleuteld polymorfe identiteit en/of pseudoniem dat in geval daarom is gevraagd, een BSN[10] kan zijn • De gehele eIDAS-keten is gereed op 31 oktober 2018

Uitgifte sleutels en ontsleutelsoftware

De uitgifte van sleutels is voorzien in release 1.13. BSNk (Logius) verzorgt de uitgifte van deze certificaten op basis van het OIN (per organisatie, per OIN). Een sleutel (lees: certificaat) is organisatie-specifiek en kan in zowel het burger- als het bedrijvendomein worden gebruikt. Dienstverleners kunnen een aanvraag indienen via een herkenningsmakelaar.

[9] Polymorfe pseudoniemen zitten wel in 1.12. Alleen is de flow nog niet helemaal geautomatiseerd, waardoor DV zelf decryptie keys moeten opvragen. De BSN flow werkt nog niet, maar wanneer een pseudoID wordt uitgevraagd, komt deze polymorfe ge-encrypt terug.

[10] Door de polymorfe identiteit en/of pseudoniem te ontsleutelen kan de dienstverlener attributen van deze persoon ophalen uit het BRP (via een webservice) of het interne dossier ophalen. Hiervoor moet de dienstverlener een cryptografische sleutel ontvangen van Logius en crypto software implementeren om de polymorfe pseudo te kunnen ontsleutelen.

De open source software om de sleutels te ontsleutelen is reeds beschikbaar via een openbare hyperlink[11]. Het implementeren van de ontsleutelsoftware kan voor kleinere organisaties redelijk eenvoudig. Grotere organisaties maken veelal gebruik van een HSM om digitale sleutels te bewaren. In die gevallen kan de implementatie soms iets complexer zijn. In alle gevallen geldt: de impact is afhankelijk van de inrichting van processen en systemen bij de dienstverlener. De herkenningsmakelaar kan de dienstverlener op verzoek ondersteunen bij de installatie van de software.

eIDAS-Inlogknop

De Beheerorganisatie eTD werkt aan een uniforme EU-inlogknop voor dienstverleners. Hiertoe wordt de online handreiking uitgebreid met kant-en-klaar materiaal waarin tekst en beeld zijn gespecificeerd. Doel is de herkenbaarheid voor eindgebruikers verhogen. Vanuit de EU worden deze materialen niet beschikbaar gesteld.

[11] https://github.com/BramvanPelt/PPDecryption.