Notitie

Aan:	Standaardisatieraad Edustandaard
Van:	Stuurgroep SION
Datum:	27 oktober 2014
Onderwerp:	Certificeringsschema Edukoppeling

Inleiding
Eind 2013 is binnen het Samenwerkingsplatform Informatie Onderwijs (SION) een certificeringsschema voor het gebruik van Edukoppeling door (cloud)leveranciers opgeleverd. Het certificeringsschema betreft enerzijds een afspraak over beveiligingsnormen waaraan een leverancier dient te voldoen en anderszijds een afspraak over de wijze waarop wordt toegezien of aan deze normen wordt voldaan.
Met het certificeringsschema wordt het mogelijk gemaakt om leveranciers die privacy gevoelige gegevens verwerken voldoende te kunnen vertrouwen op basis van aantoonbare maatregelen.

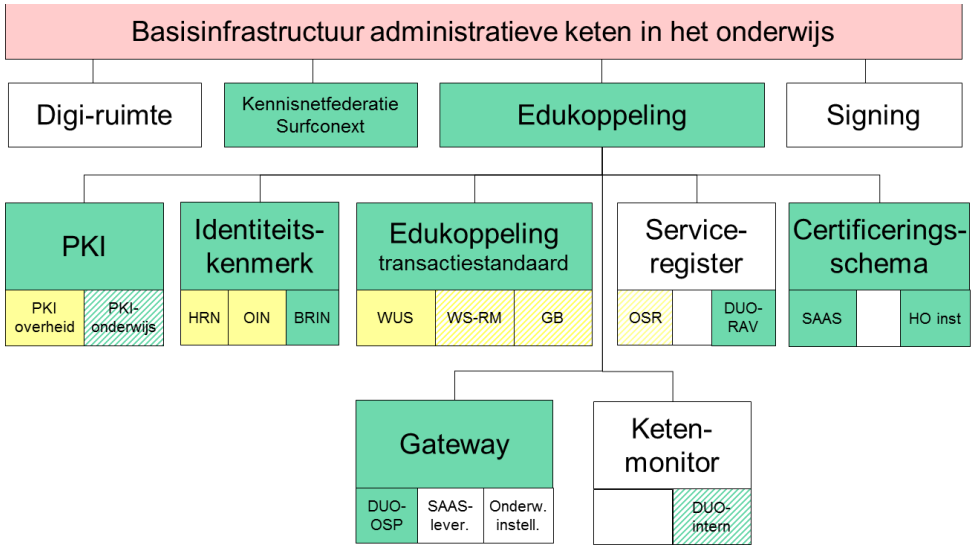
In deze notitie wordt het certificeringsschema toegelicht en de Standaardisatieraad gevraagd om een besluit te nemen over het beheer van de beveiligingsnormen die gesteld worden aan leveranciers als onderdeel van het certificeringsschema.

Scope
Het beheer van het certificeringsschema betreft niet het toezichtskader dat ook onderdeel uitmaakt van het certificeringsschema. Dit is het gedeelte waarin staat beschreven op welke wijze leveranciers worden gecontroleerd en gecertificeerd. De stuurgroep heeft besloten om het groeipad hiervoor komend jaar binnen SION te bepalen.

De beveiligingseisen in het certificeringsschema zijn niet bedoeld om na te gaan of een leverancier een technische of semantische standaard goed heeft geïmplementeerd, maar gaat om het afdekken van risico's die niet door deze standaarden kunnen worden afgedekt. Het gaat hierbij bijvoorbeeld om de scheiding van klantdata, het toegangsbeleid tot gegevens voor medewerkers, het vernietigen van data, etc.

Aanleiding
Aanleiding voor het certificeringsschema was om een eerste aanzet te geven voor de betrouwbaarheidseisen voor leveranciers die cloudoplossingen bieden voor het hergebruik van gegevens van DUO ten behoeve van het digitaal aanmelden in het MBO.
Deze manier van werken was nieuw voor alle betrokkenen en bood een basis voor samenwerking, omdat de betrouwbaarheid van de clouddienstverlening met dit schema voldoende was gewaarborgd.
Op 19 januari 2014 is DUO akkoord gegaan met het gebruik van het certificeringsschema Edukoppeling voor berichtenverkeer via cloudleveranciers in het kader van digitaal aanmelden. In haar goedkeuringsbrief heeft DUO een aantal randvoorwaarden gesteld, waaronder de uitgevoerde risico-analyse en de borging van het eigenaarschap en beheer van het schema.
Bij de tot standkoming van de nieuwe versie van het certificeringsschema is in nauwe samenwerking met DUO aan deze randvoorwaarden voldaan. DUO is voornemens om het schema ook toe te passen bij de projecten Doorontwikkelen Bron en Facet (een voorziening voor toetsen en examineren).

Positionering
Het certificeringsschema Edukoppeling maakt onderdeel uit van de basisinfrastructuur, die binnen de SION referentiearchitectuur onderwijs (genaamd ROSA 3.0) is onderkend en door de architectuurraad van Edustandaard is geregistreerd (zie figuur 1).



Figuur 1: Edukoppeling als onderdeel van de basisinfrastructuur voor het onderwijs

Een belangrijk onderdeel van het certificeringsschema is het gebruik van de Edukoppeling transactiestandaard die in het voorjaar van 2014 door Edustandaard in beheer is genomen en momenteel in een open werkgroep wordt doorontwikkeld. Deze (technische) standaard kan namelijk los van het certificeringsschema ook gebruikt worden voor andere processen waarin privacy gevoelige gegevens worden uitgewisseld.

Totstandkoming
Het certificeringschema is tot stand gekomen binnen de kerngroep ROSA, die onderdeel uitmaakt van SION. Hierin zijn vertegenwoordigers van de onderwijsraden, Kennisnet/SURF en OCW/DUO vertegenwoordigd. Daarnaast is er ook afstemming geweest met leveranciers in het MBO, met SURFnet, de werkgroep Informatiebeveiliging onderwijs (IBO) in het HO en de taskforce Informatiebeveiliging in het MBO.

Geconstateerd is dat het schema een verdere uitwerking en detaillering betreft van het SURF normenkader voor cloudservices in het HO en de toetsingskaders die momenteel voor het MBO wordt ontwikkeld. Voor deze kaders en voor het certificeringsschema is namelijk dezelfde internationale code voor informatiebeveiliging gebruikt, ISO 27001 en ISO 27002.

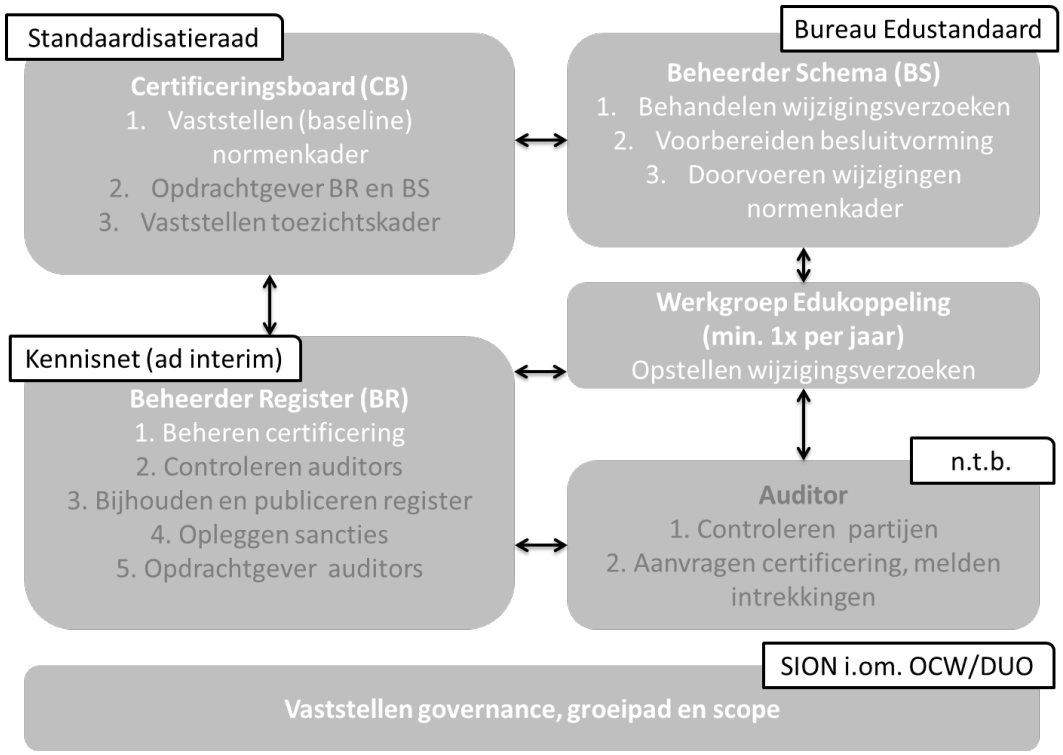
Het certificeringsschema is tenslotte afgestemd met de Architectuurraad van Edustandaard. Hieruit zijn tot nog toe geen vragen of opmerkingen naar voren gekomen.

Besluitvorming
De Standaardisatieraad wordt gevraagd om het gedeelte in het certificeringsschema dat gaat over de beveiligingsnormen waaraan leveranciers dienen te voldoen in beheer te laten nemen door Edustandaard (hoofdstuk 2 en bijlage A in het certificeringsschema). Dit beheer maakt onderdeel uit van de governancestructuur zoals deze door de SION stuurgroep is vastgesteld. Hierbij neemt Edustandaard de rol van Certificeringsboard en Beheerder Schema op zich. Zie bijlage voor verdere toelichting.

Doordat het beveiligingskader in beheer wordt genomen door Edustandaard kunnen de beveiligingsnormen binnen een open werkgroep met (vertegenwoordigers van) onderwijsinstellingen en leveranciers doorontwikkeld worden voor gebruik in verschillende ketenprocessen. De verwachting is dat een dergelijk schema de komende jaren voor steeds meer processen vereist zal worden in verband met regelgeving vanuit de EU.

Bijlage Governancestructuur Certificeringsschema Edukoppeling

Inleiding
De governancestructuur kent een viertal rollen: certificeringsboard, beheerder schema, beheerder register (of toezichthouder) en auditor (of uitvoerder), zie figuur 1. Hieronder worden deze rollen nader toegelicht. Uitgangspunt hierbij is dat certificering momenteel alleen plaatsvindt voor private cloudleveranciers in het kader van digitaal aanmelden MBO, maar in de nabije toekomst ook gebruikt gaat worden bij andere projecten, waaronder Facet en Doorontwikkelen Bron.



Figuur 1: Governance Certificeringsschema Edukoppeling
(witte tekst = belegd, grijze tekst = nog niet belegd)

Certificeringsboard
Het certificeringsboard is de inhoudelijke eigenaar van het schema. De eigenaar is verantwoordelijk voor het vaststellen van de inhoudelijke normen binnen het schema. Zij geeft opdracht aan de Beheerder Schema voor het onderhouden en doorontwikkelen van het normenkader.

In een later stadium kan de eigenaar ook verantwoordelijk worden voor het vaststellen van het toezichtskader, waaronder eventueel ook sancties. In die positie acteert het certificeringsboard ook als opdrachtgever voor de Beheerder Register (toezichthouder).

Voorgesteld wordt (zie besluitvorming) om de rol van Certificeringsboard te beleggen bij de Standaardisatieraad (SR) van Edustandaard. In de SR zitten vertegenwoordigers van relevante ketenpartijen die onderling afspraken maken over gegevensuitwisseling binnen de keten.

Beheerder Schema
De Beheerder Schema is verantwoordelijk voor het onderhouden van de inhoudelijke normen binnen het schema, zij evalueert deze en bereidt besluitvorming ten behoeve van het schema voor.

De beheerder adviseert en informeert de eigenaar van het schema. Daarnaast voert de beheerder wijzigingen in het schema door nadat hierover besluitvorming heeft plaatsgevonden. Voorgesteld wordt (zie besluitvorming) om de rol van beheerder te beleggen bij Bureau Edustandaard. Het bureau voert momenteel namens de SR het beheer over standaarden en afspraken binnen de onderwijsketen en biedt ondersteuning bij de implementatie hiervan.

In een structuur van werkgroepen wordt momenteel reeds binnen Edustandaard afspraken met betrokkenen opgesteld of wijzigingsvoorstellen voorbereid voor besluitvorming in de Standaardisatieraad.

Beheerder Register
De Beheerder Register beheert een register van gecertificeerde partijen. Daarbij controleert zij de verschillende uitvoerders. De Beheerder Register is verantwoordelijk voor het bijhouden en publiceren van het register en kan in een later stadium ook optreden als opdrachtgever richting de uitvoerders of hierin zelf een rol vervullen.

Voorlopig vervult Kennisnet (namens SION) ad-interim deze rol. Door de stuurgroep is besloten om deze rolverdeling voorlopig aan te houden en in 2015 over de definitieve invulling hiervan te besluiten. De invulling van deze rol is ook sterk afhankelijk van het groeipad naar meer externe toezicht, in het huidige schema is dit nog gebaseerd op zelfverklaringen van leveranciers.

De rol van Beheerder Register is zeer zeker niet vrijblijvend. Het kan deels betaald worden door de opdrachtgever, en deels betaald worden door de partijen die gecontroleerd dienen te worden. Binnen SION dient het tempo naar externe toezicht in overleg met leveranciers te worden bepaald.

Auditor
De auditor is verantwoordelijk voor het controleren van de leveranciers in de keten. De auditor controleert of partijen aan de gestelde kwaliteitseisen voldoen en verstrekt een goedkeuring hierover in de vorm van een certificaat. De uitvoerder informeert de Beheerder Register over nieuw verstrekte certificaten en intrekkingen van certificaten.

De rol van auditor wordt nog niet te beleggen, omdat dit nu nog niet nodig is. Momenteel wordt er nog gecertificeerd op basis van zelfverklaringen. In de toekomst – wanneer er externe toezicht vereist is - zou deze rol belegd kunnen worden bij marktpartijen, de rol kan echter ook belegd worden bij de Beheerder Register.