Edukoppeling

Transactiestandaard

Versie 1.2 (concept)

Edustandaard

Datum: juni 2015

Versie: 1.2

Inhoudsopgave

1. Inleiding

Doel en doelgroep

Dit document beschrijft de Edukoppeling Transactiestandaard (verder aangeduid als Transactiestandaard) en is onderdeel van de Edukoppeling Architectuur. De Transactiestandaard beschrijft op welke punten de Transactiestandaard afwijkt van de Digikoppeling WUS 3.0 profielen.

Het doel dat de Transactiestandaard hiermee nastreeft is het op een generieke manier kunnen uitwisselen van gegevens binnen de onderwijssector. Daarbij wordt, in tegenstelling tot Digikoppeling, zowel het model waarbij een school zijn administratiepakket zelf host, als waarbij de school deze diensten afneemt van een SaaS-leverancier, ondersteund. Dit document definieert de kaders voor de profielen om dit te bereiken.

Dit document is bedoeld voor ICT specialisten die betrokken zijn bij het ontwerpen en ontwikkelen van systeem-naar-systeem koppelingen en dient naast de Digikoppeling documentatie gebruikt te worden.

Leeswijzer

Hoofdstuk 1 bevat de inleiding en het doel en toepassingsgebied van de Edukoppeling standaard. In hoofdstuk 2 wordt de positionering van de transactiestandaard binnen de Edukoppeling architectuur beschreven. Hoofdstuk 3 werkt de transactiestandaard zelf verder uit met hierin de wijzigingen ten opzichte van de Digikoppeling profielen.

Historie

Versie	Auteur	Datum	Opmerking
0.93 / 1.0	Gerald Groot Roessink en Remco de Boer	06-12-2013	Goedgekeurd door Kerngroep RAO en ingediend bij Edustandaard
1.1	Gerald Groot Roessink en Remco de Boer	06-03-2014	Wijzigingen verwerkt n.a.v. openbare consultatieronde.
1.2	Werkgroep Edukoppeling	juni 2015	Op basis van discussie tijdens werkgroep van 27 januari en 1 april 2015 op een aantal punten aangescherpt. Wijzigingen in hoofdstuk 3, wsa:to en wsa:from vulling in tabel. Toevoeging paragraaf

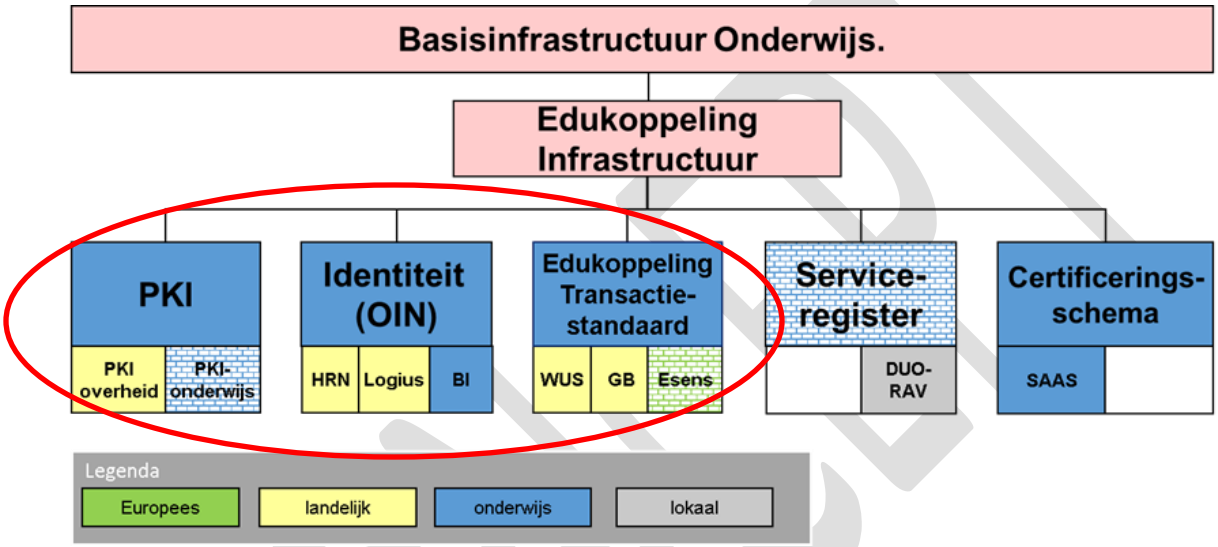
			Foutafhandeling en verwijdering E2E beveiliging Begrippenlijst bijgewerkt, termen ook vermeld in de Digikoppeling standaard zijn verwijderd

2. Positionering Edukoppeling Transactiestandaard

De Edukoppeling Transactiestandaard is onderdeel van de Edukoppeling Architectuur. In Figuur 1 wordt de relatie tussen de Transactiestandaard en overige bouwstenen van Edukoppeling weergegeven.

De Transactiestandaard sluit een aantal Digikoppeling profielen uit en ondersteunt alleen het gebruik van Digikoppeling WUS en Grote berichten profielen. Het beschrijft met name op welke punten er binnen de onderwijssector van de Digikoppeling WUS 3.0 profielen afweken wordt.

In het volgende hoofdstuk wordt inhoudelijk beschreven op welke punten de Edukoppeling WUS profielen verschillen met die van Digikoppeling.



Figuur 1- Edukoppeling Architectuur

3. Edukoppeling Transactiestandaard

Het aanbieden en afnemen van services op een servicebus tussen overheidsorganisaties is in detail uitgewerkt in de Digikoppeling standaard. Deze is verplicht gesteld door de Nederlandse overheid en dient als één ‘stopcontact’ wat hergebruik mogelijk maakt voor een veelheid van informatiestromen. Diezelfde overweging, een gemeenschappelijk elektronische snelweg of basisinfrastructuur, is ook gemaakt voor het onderwijs. Het resultaat hiervan is de Edukoppeling standaard. Hiermee wordt zoveel mogelijk aangesloten op de nationale standaard, maar er worden binnen het onderwijs wel een aantal afwijkende voorschriften geformuleerd. Dit hoofdstuk beschrijft deze afwijkende voorschriften. Verder geldt dat, buiten deze afwijkingen, de voorschriften volgens de Digikoppeling standaard toegepast dienen te worden.

Edukoppeling conformeert zich aan de Digikoppeling, maar wijkt op een aantal punten af, te weten:

1. **De Edukoppeling Transactiestandaard gebruikt het openbare internet, geen Diginetwerk of ander privaat netwerk.**
2. **De Edukoppeling Transactiestandaard past alleen Digikoppeling WUS profielen toe voor zowel bevragingen als meldingen. Daarnaast kan het profiel Grote Berichten toegepast worden wanneer dit meer bruikbaar is. De profielen WS-RM en ebMS worden niet toegepast.**
3. **De Edukoppeling Transactiestandaard staat het gebruik van PKI-ODOC en PKI-Overheid certificaten toe.**
4. **De Edukoppeling Transactiestandaard stelt specifieke eisen aan het gebruik van WS-addressing headers om formele (bv onderwijsinstellingen) en administratieve partijen (bv SaaS-leveranciers) te kunnen onderscheiden.**
5. **De Edukoppeling Transactiestandaard stelt specifieke eisen aan de foutafhandeling.**

Resulterend kan er worden gesteld dat Edukoppeling alle drie de WUS profielen ondersteunt, namelijk WUS 2W-be, 2W-be-S en 2W-be-SE. Deze profielen worden zowel gebruikt in het geval van SaaS-leveranciers als wanneer onderwijsinstellingen zelf de koppeling tot stand brengen. Hierna worden de aanvullende voorschriften nader toegelicht.

3.1 Gebruik van openbare internet

De partijen die deel uitmaken van de sector onderwijs maken nagenoeg zonder uitzondering gebruik van het openbare internet. Een privaat netwerk (zoals diginetwerk) daarvoor introduceren biedt (te) weinig meerwaarde en zou extra beheerslast met zich meebrengen.

3.2 Het WUS profiel wordt toegepast voor zowel bevragingen als meldingen

Voor betrouwbare gegevensoverdracht schrijft Edukoppeling een ander profiel voor dan Digikoppeling. Digikoppeling gebruikt hiervoor de WSRM en ebMS profielen. De onderwijssector wil geen complexe varianten introduceren die hetzelfde functionele doel hebben, maar biedt een architectuur die een end-to-

end reliable interactieproces mogelijk maakt (in plaats van dit alleen op protocolniveau te regelen zoals Digikoppeling WS-RM en ebMS).

Betrouwbare gegevensoverdracht wordt vaak gekoppeld aan een melding, de initiator van de gegevensuitwisseling wil een andere partij informeren over een gegevenswijziging. De initiator verwacht niet direct een real time resultaat, anders dan een bevestiging dat de gegevens zijn ontvangen. Op andere (business) niveaus is het in deze context vaak wel gewenst dat de verwerking van de gegevens of aanverwante resultaten worden teruggekoppeld. Deze patronen kunnen zeer complex zijn en hiermee ook de standaarden die dit soort patronen ondersteunen. Edukoppeling beperkt zich daarom tot de Digikoppeling WUS-standaard, de 2W-be, 2W-be-S en de 2W-be-SE profielen voor synchrone communicatie. Deze profielen kunnen daar waar nodig aangevuld worden met Digikoppeling Grote Berichten methodiek.

3.3 PKI-infrastructuur

De koppelvlakken die bij de gegevensuitwisseling gebruikt worden en de gegevens zelf tijdens transport moeten voldoende beveiligd zijn. Conform Digikoppeling[1] wordt hiervoor met een PKI-infrastructuur en certificaten gewerkt. Deze certificaten worden uitgegeven door CSP's. Een CSP is verantwoordelijk voor het controleren van de identiteit van de aanvrager en het opnemen van het identificerend gegeven dat voor deze aanvrager in het certificaat opgenomen moet worden. Voor Edukoppeling kunnen twee soorten certificaten toegepast worden, dit zijn:

1. PKI-Overheidscertificaten (Digikoppelingcertificaten)
2. PKI-ODOC

Een onderwijsinstelling en een SaaS-leverancier kunnen zowel een PKI-Overheidscertificaat als een PKI-ODOC certificaat gebruiken voor gegevensuitwisseling conform Edukoppeling.

PKI-Overheidscertificaten

PKI-Overheidscertificaten zijn certificaten die worden uitgegeven in het kader van PKI-overheid van Logius. PKI-overheid certificaten hebben als root (mastercertificaat) 'Staat der Nederlanden' en zijn beveiligd naar de laatste stand van techniek. Zodra deze techniek niet meer voldoende is, zal er een nieuw type certificaat met een sterkere encryptiemethode gebruikt moeten worden. Uitgegeven certificaten zijn maximaal 3 jaar geldig.

De certificaten worden uitgegeven door erkende CSP's. De PKI-overheidscertificaten zijn van het niveau STORK4. Bij de uitgifte hoort 'face-to-face' controle: de houder neemt het certificaat persoonlijk in ontvangst. Het identificerend kenmerk wordt conform Digikoppeling systematiek bepaald (zie identificatie). De CSP die het certificaat uitgeeft heeft de verantwoordelijkheid om de uniciteit van het

[1] Zie ook https://www.logius.nl/fileadmin/logius/ns/diensten/digikoppeling/aansluitdocumentatie/Digikoppeling_Gebruik_en_achtergrond_certificaten_v1_3_1.pdf

subject (service) te waarborgen en de identiteit te vermelden in het certificaat in het veld Subject.serialNumber.

Een Digikoppelingcertificaat is een specifiek PKI-overheidscertificaat. Bij de aanvraag hiervan moet men bij de CSP expliciet aangeven dat deze moet voldoen aan de specifieke Digikoppeling-eisen.

PKI-ODOC

DUO levert onderwijsinstellingen PKI-ODOC waarin de identiteiten conform deze nummersystematiek is opgenomen. DUO kan hiermee gezien worden als de Certificate Service Providers (CSP) voor onderwijsinstellingen.

Dit zijn certificaten die door DUO worden verstrekt in het kader van een wettelijke uitvoeringsregeling. Deze certificaten zijn technisch vergelijkbaar met PKI-Overheid. Het beveiligingsniveau is mede gebaseerd op de bestaande bekostigingsrelatie tussen DUO en onderwijsinstelling. De PKI-ODOC certificaten kunnen worden gebruikt voor ondertekening en encryptie zoals in Digikoppeling, maar ook voor het opzetten van het SSL/TLS protocol.

Identificatie & Authenticatie

Identificatie

Met een PKI-infrastructuur kan de identificatie en authenticatie van organisaties geregeld worden. Elke partij die via Edukoppeling de gegevensuitwisseling inricht, worden geïdentificeerd op basis van het unieke Overheids Identificatie Nummer (OIN), zie nummersystematiek Digikoppeling. De betreffende tabel wordt weergegeven in Figuur 2. Voor onderwijsinstellingen is een prefix van 00000007 gereserveerd. Marktpartijen zullen over het algemeen de HRN-variant van de nummersystematiek toepassen (prefix 00000001 of 00000003). Hierbij worden de nummers vastgesteld door de CSP, op basis van het door de aanvrager opgegeven KvK-nummer, dat door de CSP wordt gecontroleerd.

Prefix	Nummer	Suffix
00000001	Fi-nummer van Belastingdienst (9 posities). Dit wordt het RSIN uit het NHR.	"000"
00000002	RSIN of FI-nummer (9 posities)	Volgnummer (3 posities)
00000003	KvK nummer (8 posities)	Volgnummer "0000" (4 posities)
00000004	Nummer van Logius-beheerder (9 posities)	Volgnummer of "000" (3 posities)
00000005	Niet toegewezen	
00000006	Reservering (vestigingsnummer KvK)	
00000007	Niet toegewezen (BRIN)	
00000008 t/m 00000098 en vanaf 00000100	Nog niet toegewezen	
00000099	Reservering (9 posities)	Volgnummer (3 posities)

Figuur 2 - Digikoppeling nummersystematiek met reservering voor PKI-ODOC

Het zijn niet enkel de partijen die de verbinding voor de gegevens uitwisseling tot stand brengen die geïdentificeerd moeten worden, er zijn meerdere rollen te onderkennen. In de Edukoppeling Architectuur worden bij de gegevensuitwisseling de volgende rollen onderscheiden:

1. De eindorganisatie, heeft gegevens nodig voor zijn processen (school, DUO, inspectie etc)
2. De gegevensbewerker, is een organisatie die in opdracht van de eindorganisatie gegevens verzamelt, opslaat, berekeningen uitvoert, verstrekt en dergelijke.
3. De logistieke dienstverlener, is een organisatie die interoperabiliteitsfuncties uitvoert zoals, identificatie, authenticatie, autorisatie, routering, monitoring.

Deze rollen worden op verschillende wijze geïdentificeerd. De eindorganisatie wordt geïdentificeerd middels de WS-Addressing To en From headers. De gegevensbewerker (d.w.z. school met lokale applicatie, SaaS-leverancier, DUO etc) ondertekent het bericht met een XML-signature (op basis van een eigen PKI-certificaat met OIN). De logistieke dienstverleners kunnen middels de TLS verbinding geïdentificeerd worden op basis van het certificaat wat hierbij gebruikt is.

Authenticatie

Bij authenticatie wordt een aangegeven identiteit geverifieerd. De mate van betrouwbaarheid kan hierbij verschillen. Authenticatie levert als het ware de kwaliteit van de identificatie. De PKI-infrastructuur biedt een keten van vertrouwen (chain of trust), de identiteiten zijn met een vastgestelde mate van betrouwbaarheid opgenomen in de certificaten. De organisatie die de identiteit vaststelt (CSP) ondertekent het certificaat met zijn certificaat. Door het 'root' certificaat van de CSP te vertrouwen (en het certificaat is niet ingetrokken of verlopen) dan mag men op de inhoud vertrouwen.

De PKI-certificaten kunnen worden gebruikt bij de tweezijdige TLS-verbinding en voor de ondertekening en versleuteling van berichten zoals dit ook in Digikoppeling wordt toegepast. Op basis van het certificaat en dus ook de identiteit dat hierbij betrokken is kan de identiteit geauthenticeerd worden.

3.4 Identificatie via WS-addressing header

De formele partij waarvoor uitgewisseld wordt, is altijd opgenomen in de WS-Addressing:From en WS-Addressing:To veld, zowel in het geval van directe koppelingen met onderwijsinstellingen, als bij de inzet van SaaS-leveranciers. De WS-Addressing From en To headers identificeren altijd de formele partijen die met elkaar communiceren (onderwijsinstellingen, DUO etc). In onderstaande tabel is aangegeven hoe deze velden in het vraag- en antwoordbericht gevuld moeten worden.

Vraagbericht

Header	Verplicht	Vulling	Toelichting
To	Ja	Domein (of anonymous) & OIN	OIN van de formele partij die verantwoordelijk is voor de gegevens in het antwoordbericht (niet noodzakelijk de partij die de verbinding heeft opgezet).
Action	Ja	WSDL SOAPAction / WSA-Metadata binding request	Conform nationale standaard, t.b.v. aanduiding aangeroepen operatie
From	Ja	Domein (of anonymous) & OIN	Hierin wordt altijd het OIN opgenomen van de formele partijen die verantwoordelijk is voor deze

			gegevens (niet noodzakelijk de partij die de verbinding heeft opgezet).
ReplyTo	Nee		Conform nationale standaard (bevraging). Gezien de synchrone communicatie wordt aangenomen dat er naar zelfde client gecommuniceerd wordt
FaultTo	Nee		Conform nationale standaard (bevraging). Gezien de synchrone communicatie wordt aangenomen dat er naar zelfde client gecommuniceerd wordt, ook in het geval van fouten
MessageId	Ja	UUID (eigen waarde)	Conform nationale en standaard, hiermee kan dit bericht uniek geïdentificeerd worden
RelatesTo	Nee	UUID	Conform nationale standaard

Antwoordbericht

Header	**Verplicht**	**Vulling**	**Toelichting**
To	Ja	Domein (of anonymous) & OIN	OIN van de formele partijen die verantwoordelijk was voor de gegevens in het vraagbericht (niet noodzakelijk de partij die de verbinding heeft opgezet en vraagbericht heeft gestuurd).
Action	Ja	WSDL SOAPAction / WSA-Metadata binding response	Conform nationale standaard, t.b.v. aanduiding aangeroepen operatie
From	Ja	Domein (of anonymous) & OIN	Hierin wordt altijd het OIN opgenomen van de formele partijen die verantwoordelijk is voor de gegevens in het antwoordbericht (niet noodzakelijk de partij die de verbinding heeft opgezet).
ReplyTo	Nee		Conform nationale standaard (bevraging). Met antwoordbericht is aan de berichtuitwisseling een einde gekomen
FaultTo	Nee		Conform nationale standaard (bevraging). Met antwoordbericht is aan de berichtuitwisseling een einde gekomen
MessageId	Ja	UUID (eigen waarde)	Conform nationale en sectorstandaard, hiermee kan dit bericht uniek geïdentificeerd worden
RelatesTo	Ja	UUID (MessageID in requestbericht van service afnemer)	Conform nationale standaard, hiermee kan naar het ontvangen vraagbericht verwezen worden

Tabel 2. Vulling WSA-velden.

```
<soapenv: Header>
    <wsa:To>
```

```
            http://www.intermediairx.nl/services                /* het WSDL-adres */
            ?oin=00000001789455534530 /* OIN  */
        </wsa:To>
         <wsa:Action>
            http://www.intermediairx.nl/services/ontvangenLeerlinginformatie_V2
         /* de WSDL-operatie */
         </wsa:Action>
         <wsa:MessageID>
            550e8400-e29b-41d4-a716-446655440000     /* uniek bericht-id */
         </wsa:MessageID>
         <wsa:From><wsa:Address>
            http://www.w3.org/2005/08/addressing/anonymous   /* dummy */
            ?oin=000000079876 /* OIN */
         </wsa:Address></wsa:From>
         </soapenv: Header>
```

Voorbeeld OIN in WSA-header

3.5 Foutafhandeling

Digikoppeling stelt (nog) geen eisen aan de foutafhandeling, In het document ”Digikoppeling Best Practises WUS” en binnen de Gemeenschappelijke Afspraken Berichten (GAB)[2] zijn wel een aantal adviezen hierover opgenomen.

In de Edukoppeling Architectuur worden 5 soorten foutafhandeling en verwerking daarvan beschreven. Technische fouten zijn in lijn met de Digikoppeling (DK) afspraken, maar de lijst is voor Edukoppeling (EK) aangevuld.

Code	Omschrijving	S/C	Domein	Toelichting
1	Invalide envelop	Syntax	DK	Voldoet niet aan SOAP 1.1
2	Niet geautoriseerd	Syntax	DK	Niet beschikbaar voor onbevoegde.
3	Invalide soap-action	Syntax	DK	Action is niet gedefinieerd
4	Niet conform XSD	Syntax	DK	Inhoud niet valide
5	Wsa: to ontbreekt	Syntax	DK	Internetadres (URL)
6	Wsa: action ontbreekt	Syntax	DK	Naam van de operatie (URI)
7	Wsa: msgid ontbreekt	Syntax	DK	Unieke bericht id (UUID)
8	Wsa: relatesTo ontbreekt	Syntax	DK	Msgid uit request (UUID)
9	Niet conform utf-8	Syntax	DK	Bevat onverwachte tekens
10	Andere headers	Syntax	DK	Alleen edukoppeling profiel
11	Andere waarde in header	Syntax	DK	Niet in formaat (URL, URI, UUID)
20	Wsa: from ontbreekt	Syntax	EK	Afzender niet ingevuld
21	Wsa: from geen OIN	Syntax	EK	Moet OIN bevatten (20Numeriek)
22	Wsa: to geen OIN	Syntax	EK	Moet OIN bevatten (20Numeriek)
51	Service niet beschikbaar	Contract	DK	Service is gesloten

Conform de Digikoppeling standaard worden technische en functionele fouten doorgegeven in een soap:fault message. Een soap:fault is ingebed in de soap:body waar normaal de payload staat. Hieronder de structuur van een soap:fault (conform Soap 1.1).

```
<soap:Envelop>
    <soap:Body>
        <soap:Fault>
            <soap:Faultcode>
                <soap: Value>soap:Client</soap:Value>   /*value kan ook Server zijn */
            </soap:Faultcode>
            <soap:Faulstring>
                <soap:Text xml:lang=”nl”>
                    hier de fouttekst in het Nederlands
                </soap:Text >
```

[2] http://www.noraonline.nl/images/noraonline/b/bf/GAB_Voorstel_Foutafhandeling-20141202v1.5_definitief.pdf

```
            </soap:Faultstring>
            <soap:Detail>
                    Hier bij foutcode 4 informatie van de XSD-parser
            </soap:Detail>
        </soap:Fault>
    </soap:Body>
</soap:Envelop>
```

Het foutbericht wordt dus verpakt in het retourbericht onder dezelfde naam als het goedbericht. Er wordt daarmee geen gebruik gemaakt van een speciale WSDL-faultoperatie.

Bijlage A: Begrippenlijst

Onderwijsinstelling

De onderwijsgerelateerde organisatie die wordt geïdentificeerd met BRIN4.

Authenticatie

Het valideren van de identiteit van een organisatie die deelneemt aan Edukoppeling verkeer (‘ben jij wie je zegt dat je bent?’).

Autorisatie

Het bepalen of de service afnemer toestemming heeft voor de gevraagde dienst (‘mag jij wat je vraagt?’) of wat de het toegestane gegevensbereik voor de service afnemer is van de (‘waar mag je bij?’)

BRIN

Basisregister Instellingen. Register beheert door DUO met daarin alle bekostigde en aangewezen onderwijsinstellingen en gelieerde vestigingen. BRIN staat ook voor de identificatiecode van een instellingen van 4 posities.

Cloudleverancier

Leverancier van software 'in de cloud'. Zie ook SaaS.

Digikoppeling

Digikoppeling faciliteert gegevensuitwisselingen tussen overheidsorganisaties door standaardisatie van koppelvlakken (een overeengekomen set middelen en afspraken). Zie ook https://www.logius.nl/ondersteuning/digikoppeling/#c8445

Edustandaard

Edustandaard is een platform waar alle partijen binnen het onderwijsveld bij elkaar komen om afspraken te maken. Deze afspraken gaan bijvoorbeeld over het vindbaar maken van digitaal leermateriaal door middel van vastgestelde begrippen, of over het overbrengen van leerlinggegevens van het ene systeem naar het andere. Zie ook http://www.edustandaard.nl/.

Identificatie

Het relateren van een organisatie aan een registratie bij een identititeitsprovider. In het onderwijs is dat in veel gevallen BRIN, maar ook het NHR en Logius worden gebruikt.

ROSA

Referentie Onderwijssector Architectuur. Is de verbijzondering van de NORA voor de sector onderwijs. Voorheen: Referentie Architectuur Onderwijs (RAO).

SaaS

Software as a Service. Is een vorm van Cloud Computing. Veel toegepast in het onderwijs. De leerling, leraar of administratief personeel logt remote in op het systeem van de cloud- of SaaS-leverancier.

Webservice

Een webservice is een verbijzondering van een service waarbij het alleen services betreft die zijn gerealiseerd op basis van de W3C webservice specificatie (in de breedste zin van het woord, niet beperkt tot WS-*).