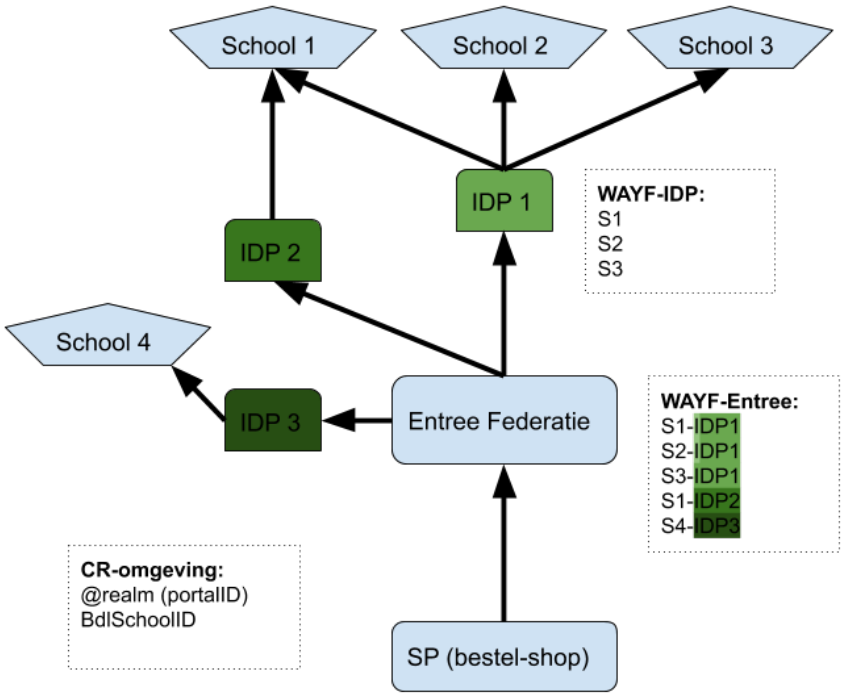
Oplossingsrichting Tussenschermen:

1) **Huidige situatie / werkwijze**

In de werkgroep “bestellen met ECK_iD” is o.a. in de sessie van 15 november stilgestaan bij het voorkomen van tussenschermen op de diverse IDP’s. Dit is primair ingestoken op de flow gezien vanuit een bestel-shop. De uiteenzetting vanuit Kennisnet (via Rick Oostmeijer) is weergegeven in onderstaande figuur 1.



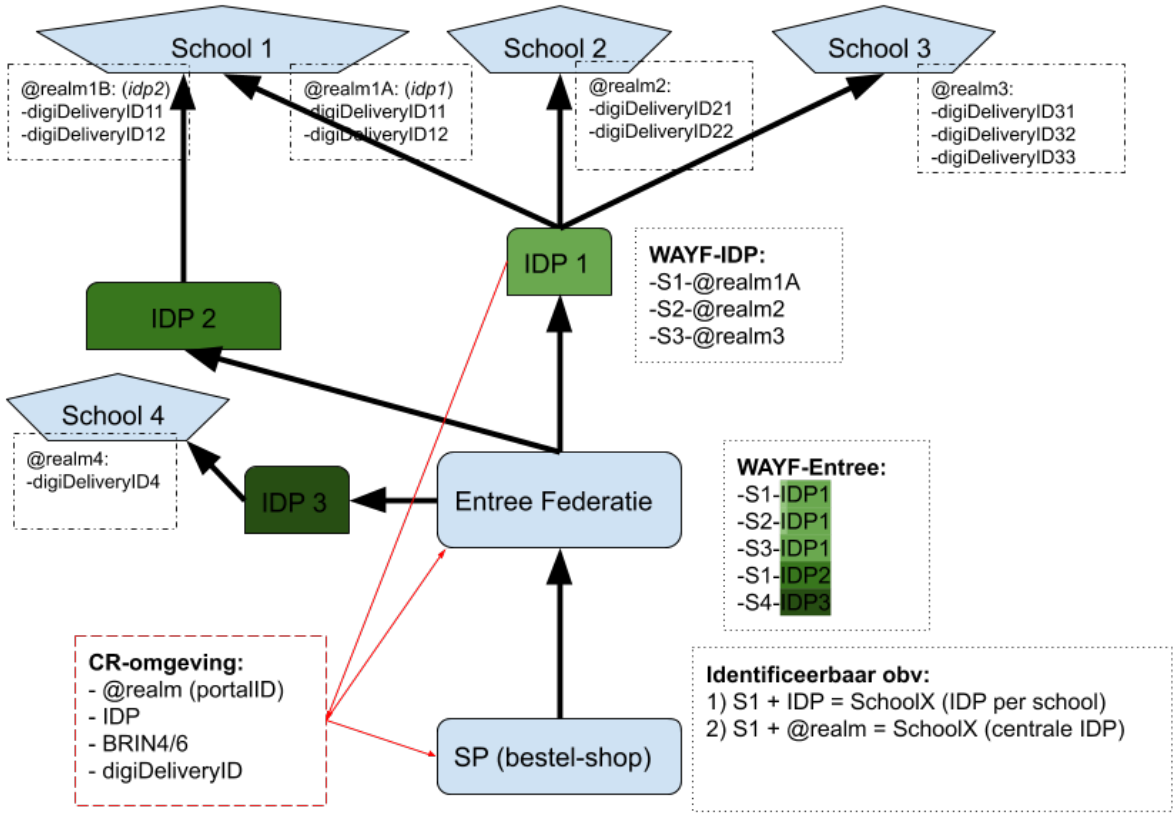
Figuur 1: huidige situatie en bekende gegevens

Tevens staat per schakel in de keten (SP, Entree en IDP van de school) beschreven welke gegevens er op dit moment bekend zijn. Gezamenlijk is geconstateerd dat er een aanvullend uniek kenmerk nodig is (**voorstel is het bestaande @realm kenmerk**) om vanuit een bestel-shop binnen een IDP de juiste school (afhankelijk van partij op instelling / vestigingsniveau) te kunnen identificeren zonder een tussenscherm. Het (nieuwe) unieke kenmerk @realm zorgt voor directe identificatie van de school, binnen een IDP die meerdere scholen bedient, en daarmee voor het kunnen overslaan van tussenschermen van zowel Entree als de diverse varianten van IDP’s

2) Voorstel nieuwe situatie / werkwijze

Voor het unieke aanvullende kenmerk is gekeken naar o.a. digiDeliveryID (=BdlSchoolID), Brin4 en @realm. Brin4 wordt al door It's Learning toegepast middels "brin-scoping" vanaf de Entree Federatie. Binnen de werkgroep is echter geconstateerd dat BRIN4 niet uniek genoeg is om een school uniek te identificeren en is als optie zodoende verder buiten beschouwing gelaten in de verdere analyse. Het overzicht in Figuur 2 toont alleen @realm en digiDeliveryID nog als mogelijkheden.

Tevens toont Figuur 2 aan dat binnen een @realm meerdere digiDeliveryID's kunnen vallen. Daarmee valt om dezelfde reden(en) als BRIN4 dit kenmerk af voor het kunnen overslaan van tussenschermen. Het voorstel is om het @realm kenmerk (reeds bekend binnen de CR-tooling) dat ontstaat binnen een IDP als uniek kenmerk te gebruiken.



Figuur 2: Aanvullende gegevens

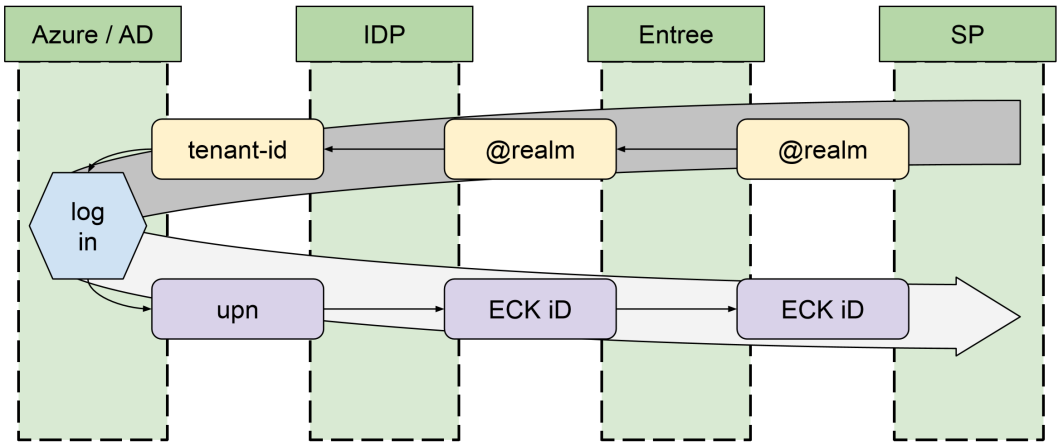
3) Processtappen om uniek kenmerk @realm te borgen in het bestelproces

Inrichting/configuratie in voortraject

1) IDP (of ELO) bepaalt het identificeerde unieke kenmerk. In dit voorbeeld uitgaande van @realm (bijv. som.gsf / UUID) om de school uniek te identificeren “achter” een centrale IDP.
2) IDP registratie bij Kennisnet. Dit gebeurt nu o.b.v. BRIN (4/6) aangevuld met gekoppelde IDP. In het geval van Somtoday is dat bijv. 00YH02 i.c.m. “somtoday.nl” als gekoppelde centrale IDP. Het @realm kenmerk dient aanvullend te worden meegegeven richting Kennisnet. Als controle achteraf wordt het kenmerk door Kennisnet uitgelezen vanuit de CR-tooling, zie punt 5.
3) Binnen het CR-proces wordt het registratierecord met het @realm kenmerk aangevuld met het digiDeliveryID, conform de volgende stappen:
    a) Distributeur door voorafgaand een crosscheck op de DUO-registratie.
    b) Uitvraag door distributeur aan coördinator DT, per school (= dienstverleningseenheid = digiDeliveryID).
    c) Distributeur beheert en controleert registratierecord per @realm en koppelt de onderliggende digiDeliveryID’s.
    d) Controle koppeling wordt uitgevraagd per registratierecord.
4) Bij de controle-koppeling wordt vanuit de ELO van de school via de IDP een registratie record bevestigd met daarin o.a. het @realm kenmerk.
5) De Entree Federatie leest de CR-omgeving uit om @realm te koppelen aan de reeds bekende gegevens (BRIN4/6 en IDP omschrijving) van een school. Dit om uiteindelijk het tussenscherm van de IDP’s over te slaan als het kenmerk binnenkomt vanuit de bestel-shop.
6) De bestel-shop (SP) leest ook de CR-omgeving uit om bij school selectie binnen de bestel-shop het @realm kenmerk mee te kunnen sturen richting de Entree Federatie.

Bestellen vanuit bestel-shop

1) Bij school selectie in de bestel-shop wordt richting Entree het @realm kenmerk meegestuurd (in het voorbeeld som.gsf)
2) Entree herkent het aangeleverde @realm kenmerk en stuurt deze direct door naar de relevante IDP (in het voorbeeld somtoday.nl)
3) Elke IDP kan aan de hand van het @realm kenmerk direct de relevante school identificeren zonder een herbevestiging (een tussenscherm) door de besteller. De selectie van de school heeft namelijk al plaatsgevonden binnen de bestel-shop en wordt in de nieuwe situatie via Entree meegeleverd naar de relevante IDP.



Figuur 3: Totale flow vanuit SP, heen en terug

Scoping berichten voor de flow (zie voor de flow Figuur 2:**):**
Bestelshop -> Entree Federatie -> IdP1 -> School1 met scoping o.b.v. "realm1a"

LET OP: de realm bevat geen @.

Stap 01:

Authenticatie verzoek met scoping van de Service Provider naar Entree Federatie.
Het authenticatie verzoek komt in dit geval van "https://bestelshop".
De scoping wordt gedaan op "realm1a" (behorend bij "School 1" en "IdP1").

```
<AuthnRequest Version="2.0"
        IssueInstant="2019-12-06T10:00:02Z"
        Destination="https://aselect.entree.kennisnet.nl/openaselect/profiles/saml2/sso/web
        AssertionConsumerServiceURL="https://bestelshop/saml2-acs.php"
        ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
 <Issuer>https://bestelshop</Issuer>
 <NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
               AllowCreate="true"/>
 <Scoping>
   <IDPList>
     <IDPEntry ProviderID="realm1a" />
   </IDPList>
 </Scoping>
</AuthnRequest>
```

Stap 02:

Op basis van de realm scoping stuurt Entree Federatie het authenticatie verzoek direct naar IdP 1. De gebruiker krijgt dus niet het WAYF scherm van Entree Federatie te zien.

Ook in dit authenticatie verzoek bevat het scoping element de waarde "realm1a".

Het RequesterID bevat het entityID van de Service Provider die het authenticatieverzoek met scoping heeft geïnitieerd.

```
<AuthnRequest AssertionConsumerServiceURL=
        "https://aselect.entree.kennisnet.nl/openaselect/profiles/saml2/sp/sso/web"
        Destination="https://idp1/sso"
        IssueInstant="2019-12-06T10:01:02Z"
        ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        ProviderName="Bestelshop"
        Version="2.0">
        <Issuer>aselect.entree.kennisnet.nl</Issuer>
        <Scoping>
          <IDPList>
           <IDPEntry ProviderID="realm1a" />
          </IDPList>
        <RequesterID>https://bestelshop</RequesterID>
        </Scoping>
</AuthnRequest>
```

Stap 03

De Identity Provider heeft op basis van de scoping op “realm1a” bepaalt dat het authenticatieverzoek voor een gebruiker van School 1 bestemd is. De gebruiker krijgt ook geen WAYF scherm van de Identity Provider te zien.

De Identity Provider verstuurt een authenticatie antwoord naar Entree Federatie

```
 <Response Version="2.0"
        IssueInstant="2019-12-06T10:03:15Z"
    Destination="https://aselect.entree.kennisnet.nl/openaselect/profiles/saml2/sp/sso/web">
        <Issuer>https://idp1</Issuer>
        <Signature>....</Signature>
        <Status>
        <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
        </Status>
        <Assertion Version="2.0"
        IssueInstant="2019-12-06T10:12:15Z">
        <Issuer>https://idp1</Issuer>
        <Signature>....</Signature>
        <Subject>
           <NameID SPNameQualifier="aselect.entree.kennisnet.nl"
                Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
               testleerling@realm1a</NameID>
        ....
        </Subject>
        <Conditions NotBefore="2019-12-06T10:02:45Z"
                NotOnOrAfter="2019-12-06T10:08:15Z">
        <AudienceRestriction>
        <Audience>aselect.entree.kennisnet.nl</Audience>
        </AudienceRestriction>
        </Conditions>
        <AuthnStatement AuthnInstant="2019-12-06T10:03:15Z"
                SessionNotOnOrAfter="2019-12-06T18:03:15Z">
        ....
        </AuthnStatement>
        <AttributeStatement>
        <Attribute Name="uid">
        <AttributeValue>testleerling@realm1a</AttributeValue>
        </Attribute>
        <Attribute Name="employeeNumber">
        <AttributeValue>20002</AttributeValue>
        </Attribute>
```

```
        <Attribute Name="givenName">
        <AttributeValue>Test</AttributeValue>
        </Attribute>
        <Attribute Name="eduPersonAffiliation">
        <AttributeValue>student</AttributeValue>
        </Attribute>
        <Attribute Name="sn">
        <AttributeValue>Leerling</AttributeValue>
        </Attribute>
        <Attribute Name="nlEduPersonHomeOrganizationId">
        <AttributeValue>99PP</AttributeValue>
        </Attribute>
        <Attribute Name="nlEduPersonHomeOrganization">
        <AttributeValue>School 1</AttributeValue>
        </Attribute>
        </AttributeStatement>
        </Assertion>
</Response>


<Response Destination="https://bestelshop"
        IssueInstant="2019-12-06T10:12:16.557Z"
        Version="2.0">
        <Issuer>aselect.entree.kennisnet.nl</Issuer>
        <Signature>
        ....
        </Signature>
        <Status>
        <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
        </Status>
        <Assertion IssueInstant="2019-12-06T10:12:16.557Z"
        Version="2.0">
        <Issuer>aselect.entree.kennisnet.nl</Issuer>
        <Subject>
        <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
                NameQualifier="aselect.entree.kennisnet.nl">
                50d9069cc1fe1ce1277b38c8149c3d23810ffc40@realm1a
        </NameID>
        ….
        </Subject>
        <Conditions NotBefore="2019-12-06T10:12:16.557Z"
                NotOnOrAfter="2019-12-06T10:13:16.557Z">
        <AudienceRestriction>
        <Audience>https://bestelshop</Audience>
        </AudienceRestriction>
        </Conditions>
        <AuthnStatement AuthnInstant="2019-12-06T10:12:16.557Z"
        SessionNotOnOrAfter="2019-12-06T20:12:16.511Z">
         <AuthnContext>
        ….
        <AuthenticatingAuthority> https://idp1</AuthenticatingAuthority>
        </AuthnContext>
        </AuthnStatement>
        <AttributeStatement>
        <Attribute Name="nlEduPersonHomeOrganizationId">
        <AttributeValue>99PP</AttributeValue>
        </Attribute>
        <Attribute Name="givenName">
        <AttributeValue>Test</AttributeValue>
        </Attribute>
```

```
        <Attribute Name="uid">
       <AttributeValue>50d9069cc1fe1ce1277b38c8149c3d23810ffc40@realm1a</AttributeValue>
        </Attribute>
        <Attribute Name="nlEduPersonHomeOrganization">
        <AttributeValue> School 1</AttributeValue>
             </Attribute>
        <Attribute Name="eduPersonAffiliation">
        <AttributeValue>student</AttributeValue>
        </Attribute>
        </AttributeStatement>
        </Assertion>
</Response>
```