Kennisnet

Bestellen voor meerdere gebruikers

Forced authentication in het bestelproces

Laat ict werken **voor het onderwijs**

Inhoud

1. Inleiding

Single Sign On zorgt ervoor dat een gebruiker met één account bij verschillende dienstaanbieders kan inloggen. Bovendien worden het aantal expliciete inlog momenten verminderd, doordat de gebruiker automatisch opnieuw geauthentiseerd wordt binnen een lopende SSO-sessie.

Waar herauthenticatie normaal gesproken extra gebruikersgemak oplevert, resulteert dit in het bestelproces binnen de educatieve content keten in een aantal gevallen tot problemen, wanneer bijvoorbeeld een ouder in één sessie voor twee of meer kinderen bestelt.

Om de kans op fouten in het bestelproces te verkleinen is het afgelopen schooljaar gebruik gemaakt van het 'cookie clear'-endpoint van Entree Federatie. Dit endpoint wordt door bestelportalen aangeroepen om de SSO-cookies te verwijderen. Hierdoor zal Entree Federatie de gebruiker niet automatisch herauthentiseren. De gebruiker moet opnieuw zijn Identity Provider (school) selecteren op het WAYF-scherm van Entree Federatie.

Dit scenario verkleint de kans op fouten in het bestelproces vooral wanneer verschillende Identity Providers in het bestelproces gebruikt moeten worden. Echter wanneer voor de bestellingen van beide kinderen dezelfde Identity Provider gebruikt moet worden is er nog steeds een aanzienlijke kans dat er een automatische herauthenticatie bij de Identity Provider plaatsvindt, aangezien deze nog een actieve sessie heeft.

Om ook in deze gevallen de kans op fouten te verkleinen, kan binnen het SAML-protocol gebruik gemaakt worden van de optionele forced authentication functionaliteit.

2. Forced authentication

Een authenticatieverzoek met de forced authentication optie moet beschouwd worden als een signaal aan de Identity Provider om gebruikersinteractie te initialiseren. De gebruiker wordt nogmaals gevraagd om actief in te loggen en dus wordt de gebruikelijke impliciete veronderstelling om de bestaande authenticatiestatus te hergebruiken door de Identity Provider genegeerd.

Forced authentication is hiermee een onderbreking van de normale Single Sign On flow en vermindert dan ook het gebruiksgemak. Het zou daarom ook alleen in specifieke use cases geïmplementeerd moeten worden. Het voorkomen van fouten in het bestelproces kan als zo'n use case bestempeld worden.

Voor de implementatie van forced authentication is nog één belangrijk aandachtspunt:
Forced authentication vraagt in principe om de herauthenticatie van de gebruiker die reeds bekend is in de SSO-sessie. Het is namelijk bedoelt als een *herbevestiging* van de identiteit van de gebruiker. Wanneer het antwoord van de Identity Provider de identiteit van een andere gebruiker bevat dan waarvoor de bevestiging is aangevraagd, zal dit in een standaard forced authentication flow tot een foutmelding leiden (AuthnFailed).

Deze foutmelding is echter te voorkomen wanneer de Service Provider eerst het 'cookie clear'-endpoint van Entree Federatie aanroept om de SSO-sessie cookies van Entree Federatie te verwijderen en pas daarna een forced authentication start. Mits juist geïmplementeerd in de keten zou forced authentication dan ook kunnen bijdragen aan het verminderen van het aantal fouten in het bestelproces.

In een forced authentication bericht van Entree Federatie naar de Identity Provider wordt meegegeven welke Service Provider het verzoek heeft geïnitieerd, bijvoorbeeld ProviderName="Entree - Referentie SP SAML forc. auth.". Het is echter niet aan te bevelen om als Identity Provider op basis hiervan te bepalen of er wel of niet om gebruikersinteractie wordt gevraagd.

Ten eerste is het in het authenticatieproces de bevoegdheid van de Service Provider om een forced authentication verzoek te starten. Alleen de Service Provider kan namelijk bepalen of dit voor zijn applicatie of onderliggende proces noodzakelijk is. Een Service Provider zou in dit geval er dan ook op moeten kunnen vertrouwen dat een forced authentication verzoek wordt afgehandeld zoals beoogd is.

Daarnaast zijn er buiten het bestelproces ook enkele Service Providers die gebruik maken van forced authentication, bijvoorbeeld voor het beheren van een online portemonnee. Eindgebruikers moeten er op kunnen vertrouwen dat ook in deze gevallen het authenticatieproces op juiste wijze wordt afgehandeld.

Ten slotte is de naam die wordt meegegeven niet persistent en het is daarom dus niet aan te bevelen om hier logica op te baseren.

3. Cookie clear functionaliteit

Let op: deze functionaliteit wordt alleen beschikbaar gesteld voor het bestelproces.

Voor het schooljaar 2019-2020 is het voor de bestelshops reeds mogelijk om de cookies van de Entree Federatie te verwijderen. Op de volgende pagina onder 3.3 staat een stuk voorbeeldcode die gebruikt kan worden om de functie te implementeren.

3.1. Monitoring

Met de bestelshops is afgesproken dat een herkenbare waarde wordt ingevuld voor "refererName" en deze wordt afgestemd met Kennisnet. Hiermee houdt Kennisnet bij waar de calls vandaan komen.

"refererName" komt in de URL voor die aangeroepen wordt en in de voorbeeldcode kan deze verwijzing gevonden worden bij:

var refererName = "**Name of your service**";

3.2. Testen van de functionaliteit

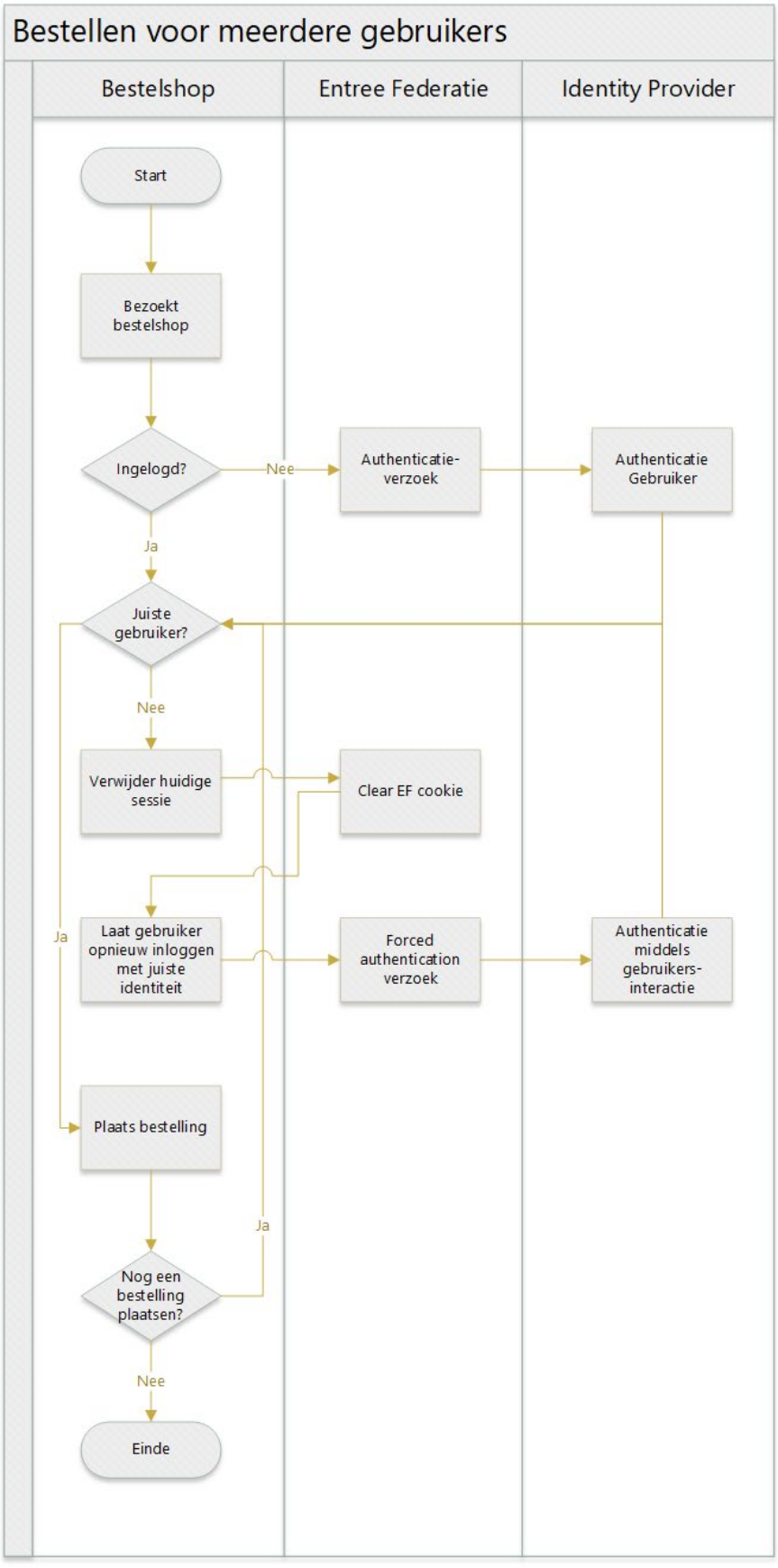
Het cookie clear endpoint is ook voor de staging omgeving beschikbaar. De URL die in de voorbeeldcode wordt aangeroepen verwijst naar onze productieomgeving. Voor de staging omgeving zal de URL veranderd moeten worden naar https://hub-s.entree.kennisnet.nl/openaselect/sso/cookie?domain=hub-s.entree.kennisnet.nl&referer=

3.3. Voorbeeldcode cookie clear functionaliteit

```
<!DOCTYPE html>
<html>
<head>
<title>Cookie clear - sample page</title>
</head>
<body>
<div>This page demonstrates the clear cookie functionality of Entree
Federatie.</div>
<button onclick="deleteEntreeCookies()">Clear cookies</button>
<p></p>
<div id="status"></div>
<script type="text/javascript">
    var refererName = "Name of your service";

    // Create a POST call to delete Entree Federatie cookies
    function deleteEntreeCookies() {
        var url =
"https://hub.entree.kennisnet.nl/openaselect/sso/cookie?domain=hub.entree.kennisnet
.nl&referer=" + refererName;

         // Check if jQuery is avaiable
        if (window.jQuery) {
            // Use jQuery to ask the Entree Federation to set a SSO Notification
            $.ajax({
                url: url,
                dataType: 'jsonp'
                }).always(function(data) {});
        } else {
            // This code can be used if no jQuery is available
            loadJSONP(url);
        }
    }

    // This function can be used if jQuery is not available
    function loadJSONP(url) {
        var script = document.createElement('script');
        script.type = 'text/javascript';
        script.src = url;

        // Setup handler
        window[name] = function(data) {
            callback.call((context || window), data);
            document.getElementsByTagName('head')[0].removeChild(script);
            script = null;
            delete window[name];
        };

        // Load JSON
        document.getElementsByTagName('head')[0].appendChild(script);
    }
</script>
</body>
</html>
```

4. Bestelscenario

Hieronder een schematische weergave van het bestelproces wanneer de gebruiker wil bestellen voor meerdere eindgebruikers.



5. Test scenario's

Hieronder eerst een scenario dat resulteert in een foutmelding en vervolgens het scenario waarin de forced authentication het gewenste resultaat heeft.

Voor het juist testen heb je twee accounts bij dezelfde Identity Provider nodig. Bij Entree Accounts kan je met behulp van verschillende email adressen meerdere accounts aanmaken. Entree Accounts ondersteunt forced authentication.

5.1. URL's

Voor de test scenario's die in dit document beschreven staan kunnen onderstaande URL's gebruikt worden.

- **Entree Federatie staging:**
  - Referentie Service Provider: https://kn.nu/refsp-s
  - Referentie Service Provider met forced authentication: https://referentie-s.entree.kennisnet.nl/saml/module.php/core/authenticate.php?as=RefSPSAMLfa
  - Cookie clear endpoint: https://kn.nu/cc-s
- **Entree Federatie productie:**
  - Referentie Service Provider: https://kn.nu/refsp
  - Referentie Service Provider met forced authentication: https://referentie.entree.kennisnet.nl/saml/module.php/core/authenticate.php?as=RefSPSAMLfa
  - Cookie clear endpoint: https://kn.nu/cc

5.2. Scenario 1 (resulteert in foutmelding bij de Service Provider)

1. Start de browser
2. Ga naar de Referentie Service Provider
3. Selecteer de school / Identity Provider op het WAYF-scherm van Entree Federatie
4. Log bij de Identity Provider in met het eerste account
5. Ga in dezelfde browser naar de Referentie Service Provider voor forced authentication
   Het authenticatie verzoek bevat *ForceAuthn="true"* om aan te geven dat de Service Provider forced authentication vereist.
6. Je wordt direct via Entree Federatie geredirect naar de Identity Provider waarmee je al was ingelogd.
   In het authenticatie verzoek van Entree Federatie naar de Identity Provider wordt ForceAuthn="true" gepropageerd. Bovendien bevat het bericht het *NameID* van het account waarmee de gebruiker al was ingelogd. Dit is namelijk het subject waarvoor een bevestiging gevraagd wordt:

```
<saml2:Subject>
   <saml2:NameID NameQualifier="https://entree-account-a.kennisnet.nl/idp">
      pluk@petteflet.nl
   </saml2:NameID>
   ...
</saml2:Subject>
```

7. Log bij de Identity Provider in met het tweede account. Het SAML response bevat het NameID van dit tweede account:

```
<saml:Subject>
   <saml:NameID SPNameQualifier="aselect-a.entree.kennisnet.nl">
      aagje@petteflet.nl
   </saml:NameID>
```

```
    ...
</saml:Subject>
```

8. Op de pagina van de Referentie Service Provider voor forced authentication krijg je een 500 foutmelding. Het SAML response bericht van Entree Federatie naar de Service Provider bevat de volgende status:

```
<saml2p:Status>
<saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
<saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed" />
</saml2p:StatusCode>
</saml2p:Status>
```

   De authenticatie is mislukt, omdat het ontvangen *NameID* niet overeenkomt met het *NameID* waarvoor een forced authentication is aangevraagd.

5.3. Scenario 2 (juiste implementatie voor ondersteuning van het bestelproces)

1. Start de browser
2. Ga naar de Referentie Service Provider
3. Selecteer de school / Identity Provider op het WAYF scherm van Entree Federatie
4. Log bij de Identity Provider in met het eerste account
5. Ga in dezelfde browser naar het 'cookie clear'-endpoint van Entree Federatie en verwijder de cookies. In dit testscenario is dit een handmatige actie, maar dit kan automatisch zoals dat nu al geïmplementeerd is door de bestelportalen.
6. Ga in dezelfde browser naar de Referentie Service Provider voor forced authentication.
   Het authenticatie verzoek bevat *ForceAuthn="true"* om aan te geven dat de Service Provider forced authentication vereist.
7. Selecteer opnieuw dezelfde school / Identity Provider op het WAYF scherm van Entree Federatie als in stap 3.
   Aangezien de SSO-cookies verwijderd zijn, kan Entree Federatie het forced authentication verzoek niet automatisch propageren. Het authenticatieverzoek van Entree Federatie naar de Identity Provider bevat wel *ForceAuthn="true"*, maar geen *NameID* waarvan de identiteit bevestigd moet worden.
8. Log bij de Identity Provider in met het tweede account.
9. Op de pagina van de Referentie Service Provider voor forced authentication ben je ingelogd met de gegevens van het tweede account.
   In tegenstelling tot het eerste scenario wordt er niet om de bevestiging van een gespecificeerde identiteit gevraagd middels een *NameID* en daarom ontstaat er ook geen foutmelding.