BRUIKBAARHEIDSRICHTLIJNEN VOOR AUTHENTICATIESCHERMEN

Richtlijnen voor Identity Providers aangesloten op SURFconext

Versienummer 1.2, juli 2012

Inhoud

1 Inleiding 3

1.1 Doel van dit document 3

1.2 Doelgroep van dit document 3

1.3 De leeswijzer 3

1.4 Minimale requirements 4

1.5 Bronnen 5

2 HTML & CSS 6

2.1 Gebruik van HTML 6

2.2 Gebruik van CSS 7

3 Functionaliteit en interactie 9

3.1 Flow 9

3.2 Afhandeling van storingen 10

3.3 Toetsenbord bediening 11

3.4 Cookies 12

3.5 Autocompletion 13

3.6 URL's 14

3.7 SSL 14

4 Vormgeving en schermindeling 16

4.1 Fluid design 16

4.2 Design voor kleine schermen 17

4.3 Identiteit 17

4.4 Fonts 19

5 Informatie & teksten 20

5.1 Labels 20

5.2 Overige informatie 21

5.3 Meertaligheid 22

1 Inleiding

1.1 Doel van dit document

Een groeiend aantal diensten voor hoger onderwijs en onderzoek gebruikt SURFconext als authenticatiemechanisme. Een aantal van deze diensten is geschikt voor gebruik op mobile devices. Helaas is een groot deel van de Identity Providers slecht of niet te gebruiken op mobile devices. Dit belemmert het gebruik van deze diensten.

Dit document bevat richtlijnen voor het ontwerpen en implementeren van authenticatieschermen. Als u de richtlijnen volgt dan krijgt u een gebruiksvriendelijk, veilig en betrouwbaar authenticatie-mechanisme geschikt voor toepassing in SURFconext. De richtlijnen zorgen ervoor dat uw inlogscherm geschikt is voor een breed publiek dat gebruik maakt van diverse browsers op uiteenlopende devices.

1.2 Doelgroep van dit document

Dit document is bedoeld voor automatiseerders die verantwoordelijk zijn voor authenticatie software bij instellingen aangesloten op SURFconext. Enige kennis van HTML en CSS is vereist om dit document te begrijpen en om de adviezen die hier beschreven worden, toe te kunnen passen.

1.3 De leeswijzer

De richtlijnen in dit document zijn gegroepeerd rondom een viertal thema's:

- **HTML & CSS:** over de opzet van de html en CSS en welke zaken u moet vermijden.
- **Functionaliteit & interactie:** over basisfunctionaliteit, de flow, URL's, certificaten, cookies, foutmeldingen, toetsenbordondersteuning en andere functionele zaken.
- **Vormgeving en schermindeling:** Richtlijnen en best practices die ervoor zorgen dat uw gebruikers de belangrijkste zaken als eerste zien en dat uw inlogschermen er in alle browsers herkenbaar en vertrouwd uitzien. Hier komen zaken als fonts, logo's en het maken van een schaalbaar ontwerp aan bod.
- **Informatie & teksten:** over hulp aan gebruikers, meertaligheid etc.

Bij dit document hoort een demo gemaakt met het open source authenticatie software pakket simpleSAMLphp (zie [8]) en een HTML demo die de richtlijnen illustreert. U kunt deze demo's relatief eenvoudig aanpassen voor uw eigen organisatie. In dit document zal regelmatig verwezen worden naar deze demo's en hoe u deze voor uw eigen situatie kunt aanpassen. U vindt deze demo's op **https://login.demo.surfconext.nl/**
U kunt inloggen met gebruikersnaam '*demo*' en wachtwoord '*demo*'.

Op **https://github.com/SURFnet/simpleSAMLphp-SURFnet** vindt u de theme bestanden welke u kunt kopiëren in uw eigen SimpleSAMLphp installatie. De SimpleSAMLphp installatie zelf kunt u downloaden op [8].

De richtlijnen zijn gegroepeerd in:

√ *Tips – Best practices, aan te raden in specifieke situaties*
! *Do's – Advies dat beter opgevolgd kan worden*
× *Dont's – Zaken die vermeden moeten worden*

Bij ieder van de richtlijnen staat hoe de richtlijn is toegepast in de demo, en indien van toepassing, hoe de demo is aan te passen naar uw situatie.

1.4 Minimale requirements

Het scala aan browsers en systemen is enorm. Wij hanteren de volgende minimale eisen die nodig zijn om in onze optiek te kunnen browsen met een device.

Device/browser eigenschap	**Requirement**
Bruikbare schermbreedte	320 pixels, minimum*
Ondersteuning Markup Language	XHTML Basic 1.1 [XHTML-Basic] aangeleverd als content type "application/xhtml+xml"
Character Encoding	UTF-8 [UTF-8]
Ondersteuning Image Format	JPEG GIF 89a PNG**
Kleur	256 kleuren, minimaal
Ondersteuning CSS	CSS Level 1 [CSS]. Met aanvullend, CSS Level 2 [CSS2] @media rule samen met "handheld" and "all" media types zie [5].
HTTP	HTTP/1.0 [HTTP1.0] of meer recent [HTTP1.1]
Script	Client side scripting in Javascript wordt ondersteund***

* = De W3C One Web richtlijn schrijft 120 pixels voor. In onze optiek is dit veel te weinig voor normaal internetgebruik.

** = De W3C One Web richtlijnen vereisen geen PNG. JPEG ondersteunt geen transparantie. GIF 89a ondersteunt maar een beperkt kleurenpalet. PNG heeft beide tekortkomingen niet en is dus in sommige situaties de meest geschikte. Bovendien ondersteunt een heel breed scala aan browsers dit format inmiddels.

*** = De W3C One Web richtlijnen vereisen geen Javascript. Voor serieuze toepassingen is het gebruik van Javascript soms onontbeerlijk.

1.5 Bronnen

[1] W3C One Web - http://www.w3.org/TR/mobile-bp/#OneWeb

[2] Android guidelines for web apps - http://developer.android.com/guide/webapps/overview.html

[3] W3C XHTML basic 1.1 - http://www.w3.org/TR/xhtml-basic/

[4] Screen resolutions reference, Spirit Light media - http://spirelightmedia.com/responsive-design-device-resolution-reference

[5] Mobile browser detection - http://detectmobilebrowsers.com/

[6] Media Queries - http://www.w3.org/TR/css3-mediaqueries/

[7] Veel gestelde vragen over de nieuwe cookie regels – http://www.opta.nl/nl/download/publicatie/?id=3595

[8] Support site SimpleSAMLphp - http://simplesamlphp.org/

2 HTML & CSS

2.1 Gebruik van HTML

√ *Gebruik de xhtml basic standaardversie 1.1*

Toelichting
De xhtml basic standaard wordt ondersteund door veel browsers. Door gebruik te maken van deze html is de kans groot dat uw inlogpagina op een juiste manier wordt weergegeven.
Advies
De xhtml basic standaard versie 1.1 is uitvoerig beschreven in [3].

× *Gebruik bij voorkeur geen tabellen voor lay-out doeleinden*

Toelichting
Tabellen werken niet goed op beperkte schermen en veroorzaken dat gebruikers vaak horizontaal moeten scrollen.

× *Gebruik geen iframes*

Toelichting
Veel mobile browsers ondersteunen het gebruik van iframes niet. Bovendien is de flow van webpagina's in SURFconext, van webservice naar WAYF, naar IDP en terug naar de webservice niet ingericht op het gebruik van iframes.

! *Definieer de viewport zo dat de browser op mobile devices de pagina niet onnodig verkleint*

Toelichting
Browsers op veel mobile devices verkleinen standaard alle pagina's zodat webpagina's die niet bedoeld zijn voor mobile devices, toch in totaal worden weergeven. Zij gaan bijvoorbeeld uit van een gebied van 960 pixels breed, terwijl zij in werkelijkheid maar een schermresolutie van 360 pixels breed hebben. Alle pagina's worden dan een factor 3 verkleind. Dat gebied van 960 pixels breed heet de **viewport** van de browser. Zonder aanvullende maatregelen passen dergelijke browsers de verkleining ook toe op een smal inlogscherm die deze verkleining niet echt nodig heeft.
Advies
Met metatags in de header kan de viewport van de browser beïnvloed worden. De volgende 2 metatags geven aan dat de pagina niet geschaald hoeft te worden.

```
<html>
   <header>
       <meta name="HandheldFriendly" content="true" />
       <meta name="viewport" content="width=device-width, initial-
             scale=1, maximum-scale=1">
   </header>
   <body>
   </body>
</html>
```

Meer informatie over het beïnvloeden van de viewport is te vinden in [2].

√ *Overweeg gebruik van specifieke html voor verschillende devices*

Toelichting
Het is ook mogelijk om server-side de HTML aan te passen voor specifieke devices. Zo kunnen delen in HTML bijvoorbeeld wel of niet aangeboden worden als dat niet of minder relevant is voor het opvragende device.
Advies
Device detectie gaat aan de hand van "user-agent" informatie, die aanwezig is in de http-header van een request, volgens de http1.1 standaard. Het probleem hierbij is dat alleen specifieke devices geadresseerd kunnen worden en bijvoorbeeld niet alle devices met een scherm resolutie kleiner dan een specifiek aantal pixels. Gelukkig zijn er wel libraries beschikbaar voor de meeste server-side script talen die bijvoorbeeld herkennen dat een device mobiel is. Deze libraries worden regelmatig geüpdatet zodat zij ook nieuwe devices herkennen. Zie bijvoorbeeld [5].

Verdere behandeling van deze techniek valt buiten de scope van dit document. Het is in de meeste gevallen eenvoudiger om gebruik te maken van CSS-media queries (zie volgende paragraaf).

2.2 Gebruik van CSS

√ *Maak gebruik van specifieke CSS voor verschillende schermresoluties*

Toelichting
De range aan schermresoluties van devices met internetbrowsers is enorm en loopt van 240 x 320 (QVGA) tot aan 2480 x 1536 (QXGA) zie [4]. Het is raadzaam om het ontwerp schaalbaar te maken (zie hoofdstuk 4), maar op kleine schermen met lage resoluties zal er wellicht ook informatie verborgen moeten worden.
Advies
Maak specifieke CSSvoor devices met een lage of juist hele hoge schermresolutie via @media-queries. In de SimpleSAMLphp-demo is media query toegepast om zaken te verbergen voor devices met een maximale schermresolutie van 480px.

Deze CSS overrulet dan de standaard CSS die voor normale devices geldt. Media queries kunnen als externe link aangeboden worden maar ook ge-embed worden in een andere CSS code in de header van de HTML.

Een voorbeeld met beide vormen:

```
<html>
   <header>
        <!—Normale stijl -->
        <link media="all" href=”all-device.css" type= "text/css"
              rel="stylesheet” />
        <!—Aanvullende externe stijl voor devices met kleine schermen -->
        <link media="screen and (max-device-width: 480px), handheld"
              href="small-device.css" type= "text/css" rel="stylesheet” />
        <style type="text/css”>
              /* Embedded CSS*/
              @media screen and (max-device-width: 480px) {
                /* aanvullende embedded stijl voor kleine schermen…*/
               }
        </style>
   </header>
   <body>
   </body>
</html>
```

Moderne mobile devices met hoge dichtheid schermen zoals de IPhone 4, of de Samsung Galaxy SII gebruiken meer scherm pixels voor 1 software pixel. Zij reageren op media queries alsof zij een normaal scherm hebben en hanteren de software pixel als uitgangspunt. Een IPhone 4 heeft bijvoorbeeld een resolutie van 960 pixels maar gebruikt 2 pixels voor 1 software pixel en reageert op media queries alsof hij maar 480 pixels heeft.

√ *Zorg voor een redelijke standaard en eenvoudige CSS*

Toelichting
Geavanceerde media-queries die ook maximale device breedte herkennen, worden pas ondersteund vanaf CSS3.
Advies.
Zorg dus altijd voor een redelijke standaard CSS. Oudere mobile browsers zullen ook media= “handheld” herkennen. Modernere browsers die wel om kunnen gaan met dit soort media queries zullen media type= “handheld” negeren. Meer informatie over media queries is te vinden in [6].

3 Functionaliteit en interactie

3.1 Flow

! *Geef duidelijke feedback over invoerfouten*

Advies

- Geef de feedback in de juiste taal.
- Noem de labels waar de foute invoer aanwezig is. Wees kort en bondig. Bij gebruikersnaam/wachtwoord authenticatie is het gebruikelijk om niet specifiek te vermelden welk gegeven onbekend is (gebruikersnaam of het wachtwoord).
- Zet de foutmelding boven aan het scherm zodat deze zeker zichtbaar is.
- Geef de foutmelding een afwijkende kleur (rood) zodat hij extra opvalt.
- Eventueel kunnen de velden ook een afwijkende kleur krijgen zodat de fout zeker opvalt.

Figuur 1. SimpleSAMLphp demo in landscape modus op een laag resolutie scherm na een foutmelding

! *Maak herstel van invoerfouten eenvoudig.*

Toelichting

Een vergissing is menselijk. Maak eenvoudig herstel mogelijk door het aantal noodzakelijke handelingen te minimaliseren.

Advies

Geef de terugkoppeling op dezelfde pagina als waar de invoer is gedaan. De gebruiker hoeft dan niet terug te navigeren. Gebruiksvriendelijk is het om de gebruikersnaam ingevuld te laten en het wachtwoord te verwijderen. De focus ligt dan op het wachtwoord. Een en ander wordt gedemonstreerd in de simpleSAMLphp demo[1].

[1] Op https://login.demo.surfconext.nl/ kan worden ingelogd met gebruikersnaam '*demo*' en wachtwoord '*demo*'.

! *Gebruik alleen meerdere stappen als u dit voor uw authenticatiemechanisme noodzakelijk is.*

Toelichting
In de meeste gevallen is het wenselijk om de gegevens voor de identificatie (gebruikersnaam) en de gegevens voor de authenticatie (wachtwoord) op een scherm te plaatsen zodat de invoer niet onderbroken hoeft te worden met het laden van een nieuwe pagina.
Uitzondering
In sommige gevallen biedt een IdP meerdere authenticatiemechanismen aan. De identificerende gegevens worden dan gebruikt om te bepalen welk authenticatiemechanisme van toepassing is voor de gebruiker. Alleen in zo'n geval vind authenticatie plaats in twee stappen.

3.2 Afhandeling van storingen

√ *Geef de gebruiker heldere terugkoppeling in geval van technische storing*

Toelichting
Geef aan, op een nette opgemaakte pagina met logo, dat inloggen (tijdelijk) niet mogelijk is. Storingen kunnen altijd voorkomen. Het vertrouwen in de kwaliteit van uw systeem wordt juist in die situaties bepaald.

Advies
Webservers als Apache, IIS en TOMCAT kunnen zo geconfigureerd worden dat zij een custom webpagina tonen in het geval dat de authenticatie software faalt. Richt deze pagina goed in.

- Vermeld eventueel contactinformatie voor het melden van de storing als deze langdurig aanhoudt.
- Vermijd het vermelden van technische details. Schrijf eventueel software die een ID van een log-item teruggeeft en communiceer deze op de storingspagina. De gebruiker kan deze ID melden aan een beheerder die vervolgens de details kan terugvinden in de logfiles.

In de simpleSAMLphp demo is een nette foutafhandeling volgens bovenstaand mechanisme uitgewerkt.

Figuur 2. Voorbeeld van een storingsscherm (in een desktop browser) zoals opgenomen in de SimpleSAMLphp demo.

3.3 Toetsenbord bediening

! *Zorg dat de tab-index klopt*

Toelichting
De tab-index dicteert de volgorde waarin een browser klikbare elementen op een web-pagina de focus geeft. De gebruiker kan met de tab-toets de cursor verplaatsen tussen deze elementen en hoeft hierbij geen muis te gebruiken. Veel mobile devices hebben op hun on-screen keyboard ook een voorziening om eenvoudig te navigeren tussen velden volgens de volgorde zoals gedicteerd door de tab-index.

Advies
Standaard hanteert de browser de volgorde in de HTML voor het tabben. Als de velden in de goede volgorde staan, zonder dat er andere aanklikbare elementen (zoals bijvoorbeeld link) in de HTML voorkomen, dan hoeft u niets te doen. Als dit niet het geval is, dan kan een afwijkende volgorde gedicteerd worden door gebruik te maken van het "tabindex" attribuut van de "<input>", "<select>" en "<textarea>" tags in de HTML.

√ *Zorg voor auto-focus op het eerste veld*

Toelichting
Een inlogscherm heeft één doel: inloggen. Het is dan ook gebruiksvriendelijk als de gebruiker direct kan beginnen met invoeren van de gevraagde gegevens.

Advies
Dit kan bereikt worden door het eerste veld de focus te geven nadat de pagina is geladen.

In de simplSAMphp demo[2] staat een voorbeeld hoe dat gedaan kan worden met een regel Javascript.

√ *Zorg er voor dat enter "inloggen" is*

Toelichting
Het is ook gebruikelijk en elegant dat de gebruiker de invoer submit en inlogt door middel van het drukken op Enter.
Advies
De meeste browsers voor desktops vertonen dit gedrag standaard als er een input element van het type "submit" gebruikt wordt voor het inloggen. Als er in een specifiek inlog-formulier geen submit button gebruikt kan worden, repareer dit dan door gebruik te maken van Javascript. De behandeling hiervan valt buiten scope van dit document, maar op internet zijn talloze voorbeelden te vinden.

3.4 Cookies

√ *Beperk het gebruik van cookies*

Toelichting
De wetgeving rondom het opslaan van informatie op devices van bezoekende gebruikers of het daar weer van afhalen, is op 5 juni 2012 aangescherpt. Gebruikers dienen in een groot aantal gevallen geïnformeerd te worden en expliciet toestemming te geven (zie [7]) .

Dergelijke informatie en opt-in interactie is op een inlogscherm niet wenselijk. Helemaal omdat in SURFconext het inlogscherm los staat van de feitelijke applicatie. Gebruikers kunnen denken dat de opt-in ook geldig is voor de toepassing die zij benaderen of juist niet. Pas dus bij voorkeur geen cookie-technieken toe op een authenticatiescherm waarvoor opt-in en informatieverstrekking nodig is.

Advies
Het gebruik van cookies is bij authenticatie via SURFconext onvermijdelijk. Zij worden gebruikt om Single Sign On mogelijk te maken. Dergelijk functioneel gebruik van cookies is volgens de wet toegestaan zonder toestemming van de gebruiker. Een andere toegestane toepassing is het gebruik van cookies ten behoeve van het vasthouden van een taalkeuze. Beperk het toepassen van cookies op inlogschermen tot deze zaken.

Een andere veel gebruikte toepassing, waarvoor wel toestemming nodig is, is het verzamelen van webstatistieken. Bedenk voordat u uw webstatistiekenpakket, zoals Google Analytics of Site Catalist, opneemt op uw authenticatie pagina of dit echt nodig is. Veel informatie die u verzamelt via een webstatistiekenpakket is ook al te halen uit de loggings van uw webserver. SURFnet verstrekt ook maandelijks rapportages over de hoeveelheid bezoeken van gebruikers binnen uw instelling aan diensten aangesloten op SURFconext. U vindt deze terug op https://dashboard.surfnet.nl.

[2] Op https://login.demo.surfconext.nl/ kan worden ingelogd met gebruikersnaam '*demo*' en wachtwoord '*demo*'.

Figuur 3. Het cookie control mechanisme op de SURFnet website bij gebruik van niet- functionele toepassingen van cookies zoals het verzamelen van webstatistieken

3.5 Autocompletion

√ *Denk na over toestaan van auto-completion*

Toelichting

Moderne browsers zoals Chrome, IE, Safari en Firefox hebben password management-voorzieningen waarmee gebruikers wachtwoorden kunnen opslaan in de browser. De gebruiker krijgt dan na het invoeren van een input veld met "type" "password" een melding of het wachtwoord onthouden moet worden. Hoe gebruiksvriendelijk ook, deze voorziening is alleen veilig als de beveiliging op het niveau van het device goed is geregeld en devices niet gemakkelijk onderling uitgewisseld worden. Voor sommige organisaties kan dit een reden zijn om een voorziening op te nemen die dit opslaan van wachtwoorden voorkomt.

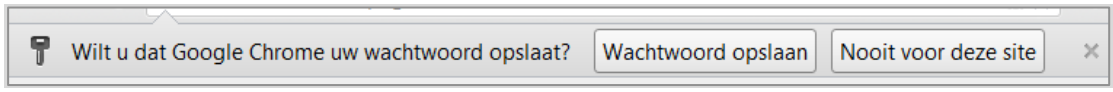
Advies

Er bestaat een eenvoudige methode voor het disablen van de password management voorziening voor specifieke formulieren. Deze maakt gebruik van een attribuut dat meegegeven kan worden aan een <input> en <form> HTML tag om autocompletion (automatisch invullen van herkende velden) uit te schakelen voor een specifiek veld. Dit attribuut is pas vanaf HTML 5 opgenomen in de HTML standaard en voldoet strikt genomen dus niet aan de XHTML basic standaard. De oplossing is dus niet 100% gegarandeerd, maar heel veel browsers herkennen het attribuut al heel lang.

Het gaat om het "autocomplete" attribuut. Als deze de waarde "off" krijgt dan zullen de meeste browsers het opslaan van het wachtwoord niet aanbieden. Onderstaand voorbeeld laat de HTML van een formulier zien waarvan zowel de gebruikersnaam als het wachtwoord niet worden onthouden.

```
<html>
   <header>
   </header>
    <body>
      <form autocomplete="off">
         <label></label><input type="text" name="gebruikersnaam" />
         <label></label><input type="password" name="wachtwoord" />
         <input type="submit" name="Login" />
      </form>
   </body>
</html>
```

Het attribuut kan ook in de <input> tag van het password worden gezet. De gebruikersnaam wordt dan wel onthouden, maar het wachtwoord niet.



Figuur 4. Melding van Chrome voor het opslaan van een wachtwoord bij een bepaald domein.

3.6 URL's

√ *Gebruik een korte herkenbare subdomein en domeinnaam*

Toelichting
De URL van uw inlogpagina lijkt wellicht niet zo belangrijk. Gebruikers worden immers altijd vanaf andere pagina's, al dan niet via SURFconext, doorverwezen naar deze pagina. De URL hoeft dus nooit handmatig ingevoerd te worden.

Toch is het belangrijk dat de URL van uw inlogpagina eenvoudig en herkenbaar is. Gebruikers moeten immers, voordat zij hun wachtwoord invoeren, wel herkennen dat de pagina de juiste is. De URL is hierbij erg belangrijk.

Advies
Plaats de inlogvoorziening altijd in een subdomein van het domein dat uw instelling communiceert als hoofddomein. Meestal is dat de naam of een afkorting van uw onderzoeks- of onderwijs-instelling. Geef het subdomein zelf geen cryptische naam die gebruikers niets zegt (afds, simplsaml. etcetara). Gebruik bijvoorbeeld de naam die het account heeft bij de gebruikers.

3.7 SSL

√ *Zorg voor een geldig en gecertificeerd server certificaat*

Toelichting
Authenticatie binnen SURFconext gebeurt altijd op een met SSL encripted verbinding. Zorg dat het server certificaat dat hiervoor nodig is:

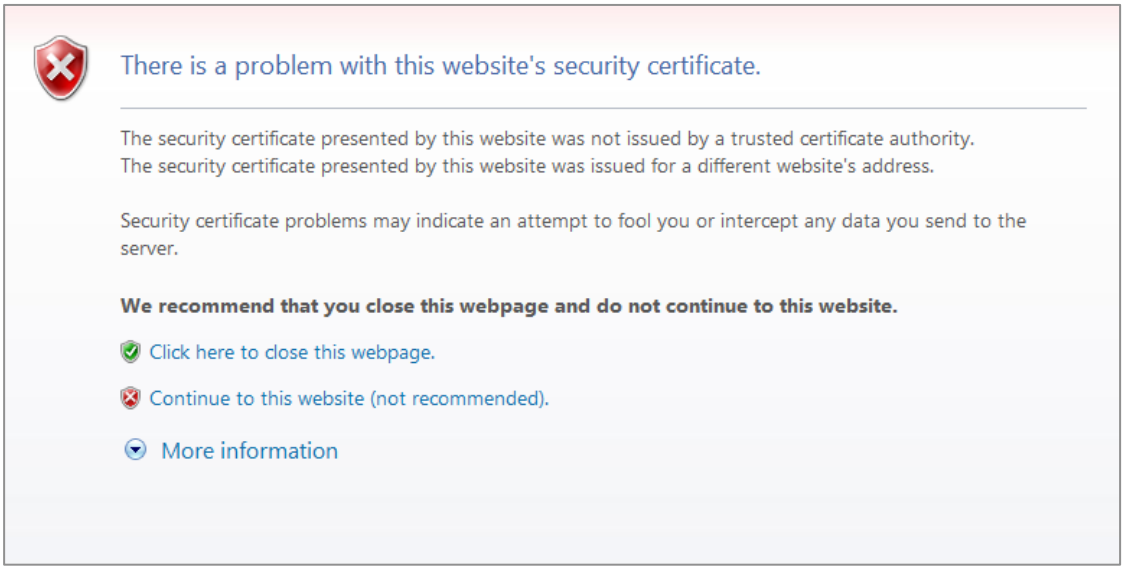
- verstrekt is door een Certificaat Autoriteit (CA)
- niet verlopen is

U kunt bijvoorbeeld gebruik maken van servercertificaten die door SURFnet geleverd worden. Zie voor meer informatie: http://www.surfnet.nl/surfcertificaten

Als aan een van beide zaken niet voldaan is, dan zullen gebruikers hierover een weinig subtiele waarschuwing krijgen en geadviseerd worden de pagina niet te gebruiken.

Advies

U kunt de geldigheid van uw certificaat laten bewaken door SURFopzichter (op http://opzichter.surfnet.nl/), de gratis monitoringsdienst van SURFnet.

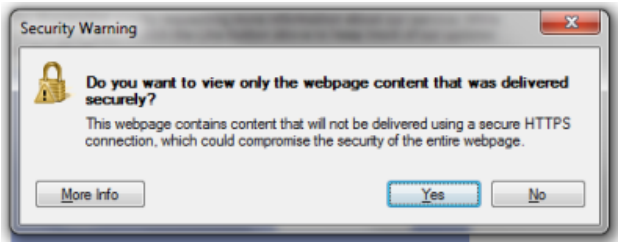


Figuur 5. Melding van IE dat de pagina die de gebruiker probeert te benaderen geen geldig certificaat heeft.

√ *Zorg dat alle afbeeldingen en andere bestanden via SSL te bereiken zijn*

Toelichting

Zorg dat **alle** onderdelen van uw loginpagina's via https worden opgehaald. Gebruikers krijgen anders een foutmelding of hun browser blokkeert de onderdelen die niet via SSL worden opgehaald. Denk bij het opzetten van uw authenticatieschermen aan afbeeldingen, externe CSS of javascript files, of http-connecties die opgezet worden door Javascript bijvoorbeeld ten behoeve van het vastleggen van webstatistieken. Alle communicatie moet via SSL verlopen.



Figuur 6. Melding van IE dat de pagina die de gebruiker probeert te benaderen onderdelen bevat die niet via SSL worden geladen.

Advies

De development tools van Internet Explorer 9 en Chrome of de Add-on "Firebug" voor Firefox hebben een networkmonitoring functie, waarmee u precies kunt zien welke files er geladen worden door uw authenticatiemechanisme en of hier SSL wordt gebruikt. Hiermee zijn spelbrekers snel te detecteren.

4 Vormgeving en schermindeling

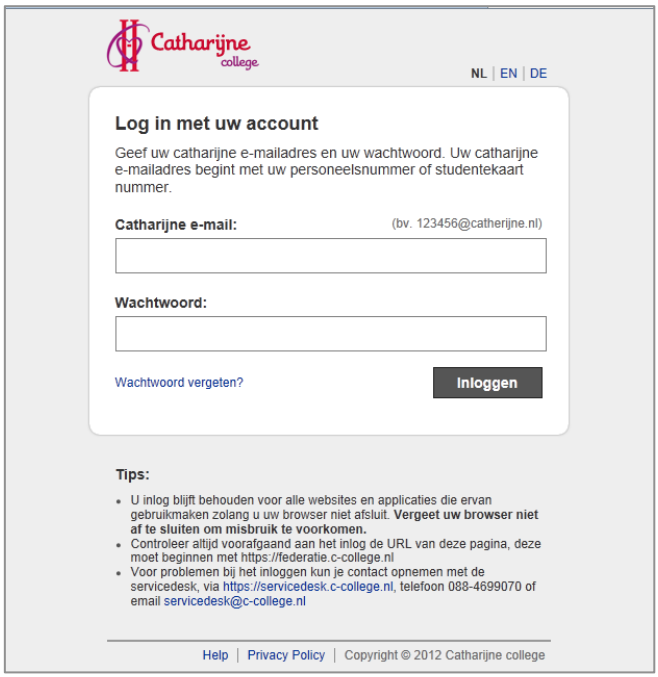
4.1 Fluid design

! *Beperk de afmeting van de pagina's en voorkom de noodzaak tot horizontaal scrollen*

Toelichting
Als u uw pagina inhoud te breed maakt, dan kunnen browsers deze op de kleinere schermen niet weergeven zonder horizontaal te scrollen of zonder de inhoud te verkleinen. Dit is niet wenselijk.
Advies
Hanteer **320 pixels** als ondermaat voor uw inlogscherm. De meeste devices die bruikbaar zijn voor het internet halen deze resolutie in landscape mode, een flink aantal zelfs in portrait en kunnen zo'n inlogpagina dus zonder verkleinen en of horizontaal scrollen weergeven.

! *Maak pagina's schaalbaar waar mogelijk, maar hanteer een bovengrens*

Toelichting
Het is dus belangrijk dat uw inlogpagina volledig zichtbaar is op kleine schermen. Maar de ondergrens van 320 pixels is wellicht wel wat beperkt als er meer pixels beschikbaar zijn. Het is dan ook raadzaam om de breedte van het inlogformulier en bijbehorende informatie groter te maken zodat er ook niet naar beneden gescrolled hoeft te worden. Beperk dit uitrekken echter wel. Tekst in te brede kolommen wordt onleesbaar.
Advies
In de demo is een maximale breedte van 480px gehanteerd. Behandeling van hoe dit schalen en maximeren te bereiken is met CSS, gaat te ver voor dit document. In de simplSAMLphp demo is een mogelijke oplossing uitgewerkt.



Figuur 7. SimplSAML demo in meest brede verschijning van maximaal 480 pixels breed.

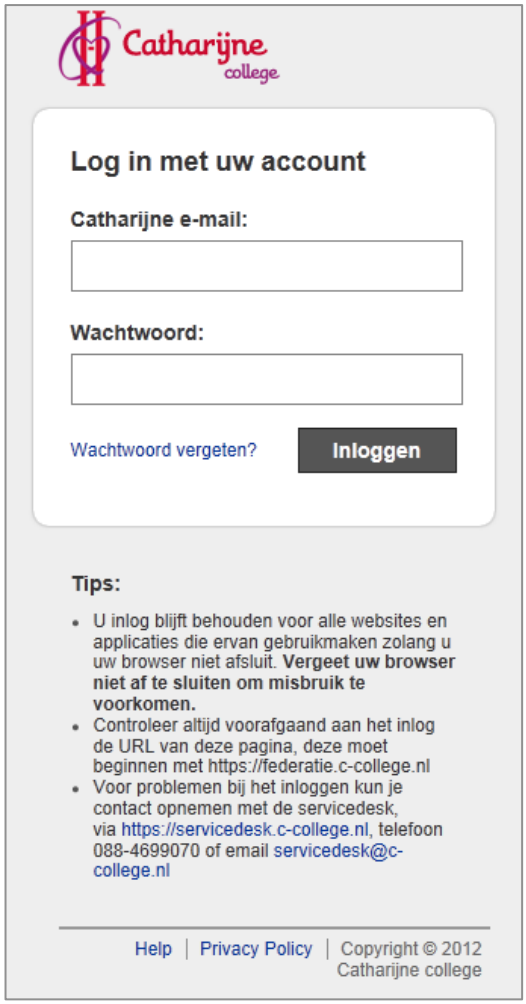
4.2 Design voor kleine schermen

√ *Verberg zaken die niet strikt noodzakelijke zijn op devices met kleine schermen*

Toelichting
Om schermruimte te besparen kunt u overwegen om onderdelen van uw inlogscherm te verbergen op schermen met een lage resolutie.

Advies
In de simpleSAMLphp demo worden de inleidende paragraaf en de taalswitch verborgen op devices met een maximale resolutie kleiner dan 480 pixels. Bovendien wordt het invulvoorbeeld verborgen als het scherm zo smal wordt dat het onder het label gaat vallen.

Onderdelen kunnen verborgen worden door speciale CSS te definiëren voor kleine devices (zie paragraaf 2.2 over media queries). Ook zou de HTML weggelaten kunnen worden middels devicedetectie (zoals aangegeven in paragraaf 2.1). Als laatste kunnen, door toepassing van floating, pagina-onderdelen onder andere onderdelen vallen waardoor ze verborgen worden.



Figuur 8. Demo scherm in portrait modus op een mobiel device waarbij de inleiding, de taal-switch en de invoerhulp zijn verborgen.

4.3 Identiteit

! *Toon het logo en de naam van uw instelling*

Toelichting
Herkenning is belangrijk bij authenticatie: 'Is de partij waar ik mijn wachtwoord opgeef inderdaad mijn instelling'. Een logo is een eenvoudige manier om de identiteit van uw instelling te communiceren. Voor andere stijlelementen als fotografie, fonts en zelfs een standaard paginastramien is vaak, vanwege andere requirements, geen ruimte.

Plaats uw logo altijd op het inlogscherm. Als de naam van uw instelling geen onderdeel uitmaakt van het beeldmerk, plaats deze dan naast het logo bovenaan het scherm.

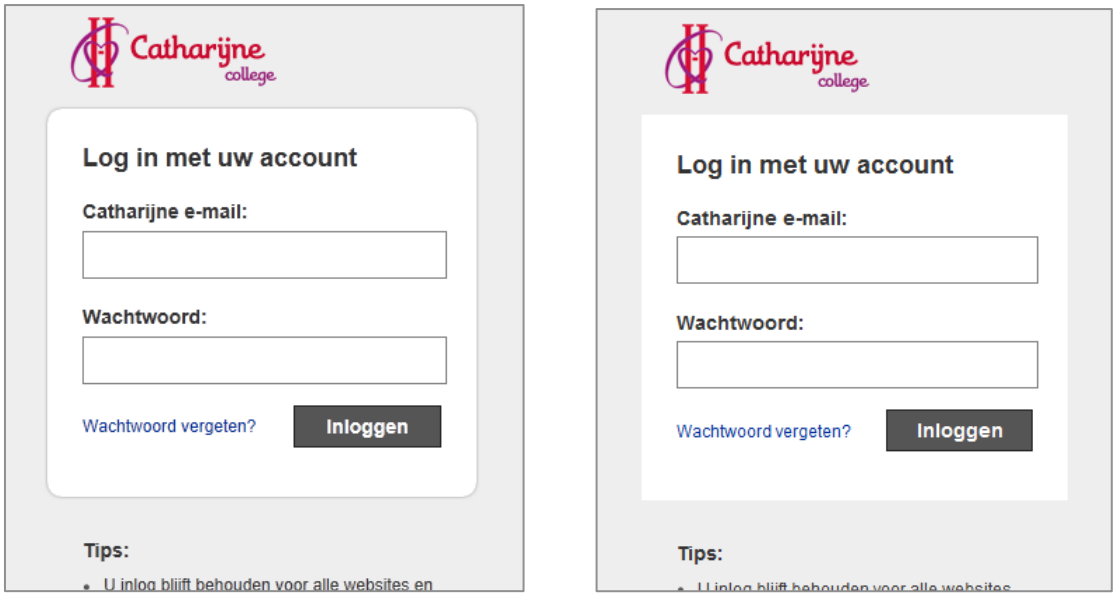
! *Beperk de afmeting en de resolutie van uw logo en kies een geschikt formaat*

Toelichting
Een duidelijk logo op uw inlogpagina is belangrijk voor de herkenning. Zorg dat de afmeting en de resolutie van deze afbeelding niet te groot zijn. Door een te groot logo bovenaan het scherm te plaatsen, verdwijnen de invoervelden op kleine schermen uit beeld en is de intentie van de pagina (voorziening om in te loggen) niet duidelijk.

Advies
Probeer de afbeelding van uw logo niet hoger te laten zijn dan 50 pixels. Kies het formaat GIF als uw logo weinig kleurverloop bevat (bijvoorbeeld zwart-wit). Als het logo kleurrijk is, kies dan PNG. Het is ongebruikelijk om JPEG te kiezen voor een logo. Dit formaat wordt eerder gebruikt voor foto's vanwege de goede compressie.

√ *Beperk het gebruik van afbeeldingen*

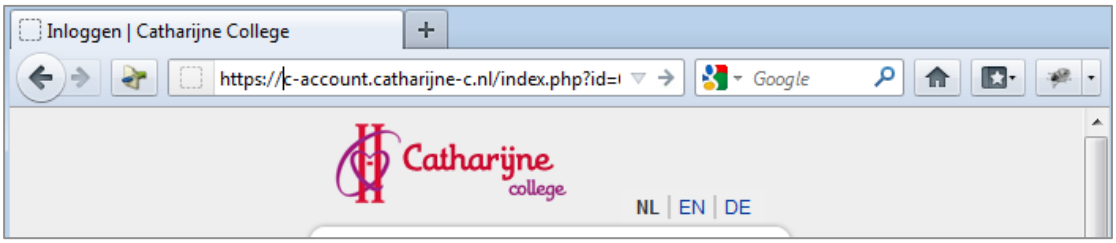
Toelichting
Vaak worden afbeeldingen gebruikt voor opmaak van de pagina. Probeer de toepassing hiervan te beperken. Zij vertragen het laden van uw inlogpagina, zeker bij mobiel gebruik.
Advies
Houd het design van uw inlogpagina rustig. CSS3 ondersteunt het toepassen van krommen en ronde hoekjes. Gebruik deze techniek in plaats van toepassing van afbeeldingen op de achtergrond. Deze laatste techniek werkt weliswaar in meer browsers maar vraagt om meer bandbreedte en geheugen van devices. Zorg wel dat bij gebruik van CSS3 stijlelementen het geheel leesbaar en overzichtelijk blijft.



Figuur 9. De demo in een browser met en zonder CSS3 support.

! *Geef uw inlogpagina een titel*

Toelichting
De HTML tag <title>die in de header van uw HTML pagina hoort te staan, wordt getoond op de tab van desktop-browsers. In alle browsers wordt deze titel vaak gebruikt in de history en in een overzicht van openstaande pagina's. Zorg dat deze titel correct gezet is. Dit komt beter over.
Advies
Neem de naam van uw instelling, of de naam van het account waarmee men moet inloggen op in de <title> tag. Verder is het doel van de pagina natuurlijk inloggen. Ook dat zou terug mogen komen in de titel. Stel uw account wordt e-account genoemd. Een goede titel is dan bijvoorbeeld "Inloggen – e-account".



Figuur 10. De naam in de <title> tag komt terug op de tab in de browser (hier Firefox)

4.4 Fonts

! *Gebruik websafe fonts*

Toelichting
Een aantal organisaties gebruikt een specifiek font in hun huisstijl. Het aantal fonts, beschikbaar op met name mobile devices, is beperkt. Grote kans dat uw font er niet bij zit. Er bestaan oplossingen waarmee non-native fonts toch gebruikt kunnen worden op websites (CSS @font-face, Google web-fonts, Typekit). Het gebruik van deze technieken heeft een aantal nadelen. De belangrijkste is dat het vaak ten koste gaat van de snelheid omdat er veel meer informatie opgehaald en verwerkt moet worden.

Advies
Gebruik een standaard font. De volgende fonts (font-families) zijn zowel aanwezig op Windows, OSX, Android, IPhone, Black Berry als Windows mobile[3]:
- Arial, Helvetica, sans-serif
- "Courier New", Courier, monospace
- Georgia, serif
- "Times New Roman", Times, serif
- "Trebuchet MS", Helvetica, sans-serif
- Verdana, Geneva, sans-serif

√ *Gebruik bij voorkeur relatieve font-sizes*

Toelichting
Als u de fontgroottes opgeeft in pixels, heeft u kans dat de letters erg klein worden op kleine schermen met hoge resolutie of grote schermen met lage resolutie.

Advies
Definieer de font-size in “em” of eventueel in “%” . De browser zal de fontgrootte dan zelf optimaal invullen. Een uitzondering kan gemaakt worden voor tekst in menu’s of tekst die in een container staat die volgens het design niet mogen schalen. In de demo is bijna alle tekst relatief gemaakt maar de taal-switch niet.

[3] Font-namen met spaties dienen tussen “” te worden opgegeven in CSS.

5 Informatie & teksten

5.1 Labels

√ *Zorg dat de labels zichtbaar zijn en duidelijk gerelateerd aan één veld*

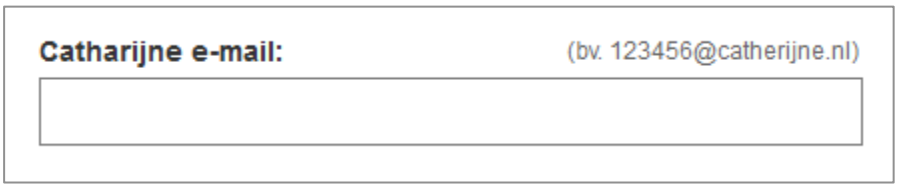
Toelichting
Veel mobile devices zoomen in op het invoerveld als de gebruiker deze selecteert om iets in te vullen. Het invoerveld wordt hierbij precies boven het "on screen keyboard" geplaatst. Labels die naast het veld staan verdwijnen. Labels boven het veld blijven meestal in beeld.
Advies
Plaats labels boven het veld en maak de afstand tussen label en gerelateerde input box kleiner dan de afstand tussen het label en een ander veld.

√ *Maak labels bij voorkeur zo specifiek mogelijk*

Toelichting
Instellingen hebben soms meerdere accounts welke zij verstrekken aan medewerkers. In deze situatie is het mogelijk niet helemaal triviaal welke gebruikersnaam/wachtwoord combinatie een gebruiker geacht wordt op te geven. Gebruik daarom voor de gebruikersnaam een specifiek mogelijke label. Gebruik niet de term "Gebruikersnaam" wanneer er een specifiekere term is. Specifiekere labels kunnen gebruikers helpen bij het herinneren van welke invoer wordt verwacht. Denk bijvoorbeeldaan collegekaart-nummer of e-mailadres.
Advies
Bedenk wel dat deze naam ook terug moet komen in eventuele foutmeldingen. Bij gebruik van een meertalige interface moet de term ook in alle aangeboden talen worden vertaald.

√ *Gebruik hulp voor de te verwachte invoer bij " gebruikersnaam"*

Toelichting
Geef, indien relevant, een voorbeeld van de invoer die verwacht wordt.
Advies
Stel dat de gebruikersnaam een e-mailadres is. Noem het veld dan e-mailadres. Als het om een specifiek e-mailadres gaat, noem die dan ook. Als de invoer aan een specifiek format moet voldoen, dan is het soms handig om een voorbeeld te geven. In de SimpleSAMLphp staat deze invulhulp boven het veld. Deze verdwijnt op schermen met een beperkte resolutie als de invoerhulp en het label over elkaar zouden vallen.



Figuur 11. Invoerhulp in de simpleSAMLphp demo waar om een specifiek e-mailadres wordt gevraagd.

! *Gebruik de <label> tag in formulieren*

Toelichting
Gebruik de <label> tag en gebruik het "for" attribuut om te verwijzen naar het bijbehorende veld. Als u de HTML op een dergelijke manier opzet, dan zal de browser beter in staat zijn om uw HTML op een juiste manier te interpreteren. Een aantal mobile browsers toont bijvoorbeeld bij beperkte ruimte het label in het veld.
Advies
Het relateren van een label aan een veld werkt als volgt:

```
<label for="password">Wachtwoord:</label>
<input type="text" name="password" id="password" />
```

5.2 Overige informatie

√ *Beperk de toelichting op het scherm zoveel mogelijk*

Toelichting
Een inlogscherm heeft een duidelijk doel en kan dus af met relatief weinig informatie. Beperk de getoonde informatie tot een minimum.
Advies
Enkele zaken die belangrijk zijn:

- Contactnummer, e-mailadres of website voor support in het geval inloggen niet lukt of er problemen zijn met het account.
- Indien aanwezig, een link naar een self service voorziening voor bijvoorbeeld het aanvragen van een account of het restten van een wachtwoord.

Enkele zaken die u kunt overwegen:

- Een inleiding die uitlegt welk account gebruikt moet worden om in te loggen[4].
- Een toelichting bij de Single Sign On voorziening en het belang van afsluiten van je browser.
- Een reminder aan de controle op de authenticiteit van de pagina. Zit de gebruiker wel echt bij de juiste URL.
- Linkjes naar achtergrondinfo als help en/of een privacy policy van uw instelling.

Plaats deze zaken altijd onder het scherm zodat deze niet te veel afleiden van het werkelijke doel en/of het snel gebruik op schermen met een lage resolutie belemmeren.

[4] Soms is de naamgeving van het label of de juiste titel voldoende.

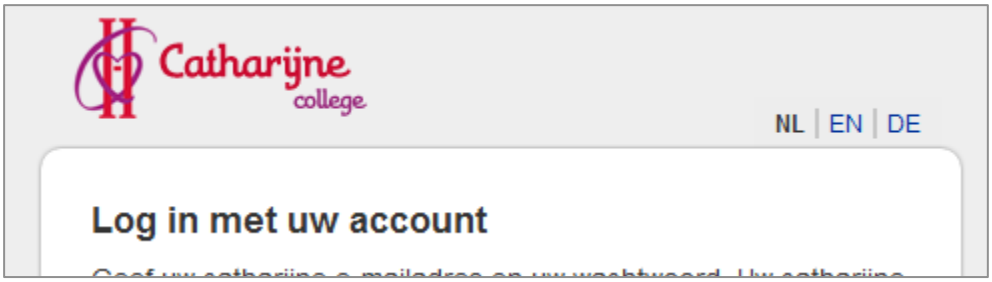
5.3 Meertaligheid

× *Bied niet meer talen aan dan noodzakelijk*

Toelichting
Het SimpleSAMLphp komt standaard met taalondersteuning voor meer dan 18 talen. Het is niet raadzaam om deze allemaal aan te bieden. Door het aanbod te beperken wordt de keuze veel overzichtelijker. Bovendien moet u alle teksten die u anders wilt dan dat ze in het template zitten, ook weer vertalen.

Bedenk goed welke gebruikers gebruik maken van de inlogfaciliteit en bedenk welke taal zij machtig zijn. Beperk de taalkeuze tot de grootste groep van uw gebruikerspopulatie. Ga er vanuit dat Engels in het hoger onderwijs verplicht is en dat de minderheid die een moedertaal heeft die niet tot de keuze behoort hier mee wel uit de voeten kan[5]. Bedenk ook: Het lijkt heel mooi en gebruiksvriendelijk om alle talen aan te bieden, maar wat is de taalondersteuning waard als je daarna bij een dienst terecht komt die de desbetreffende ondersteuning niet heeft.

Advies
Vaak is het voldoende voor Nederlandse onderwijsinstellingen om Engels en Nederlands aan te bieden. In de grensstreken kan soms Duits overwogen worden. Bij een beperkte keuze is het het duidelijkst om de taalmogelijkheden, al dan niet afgekort, als hyperlink aan te bieden waarbij de gebruikte taal bold wordt gemaakt. Gebruik bij voorkeur geen plaatjes van vlaggetjes. Vlaggetjes staan voor een land en een taal wordt vaak in meerdere landen gesproken.



Figuur 12. Taalswitch met afkortingen van de taal, zoals toegepast in de simpleSAMLphp demo

In de simpleSAMLphp demo wordt de taalswitch verborgen op devices met een lage resolutie. Het idee hierachter is dat deze mobile devices bijna altijd persoonlijk zijn en de taalinstelling van de browser doorgaans goed is ingesteld.

√ *Detecteer de taal van de browser en kies een slimme default als dit niet lukt*

Toelichting
Zorg dat bij het aanbieden van meerdere talen, de default taal goed is. Dit wekt vertrouwen in het systeem en de organisatie.

[5] Instellingen die in meerdere landen opereren hebben vaak een corporate taal, meestal Engels. Bijna altijd is het voldoende om die taal aan te bieden.

Advies
Taalinformatie wordt door de browser van de gebruiker meegegeven in het " accept-language" attribuut in een http request. Server-side script talen als PhP en Java kunnen deze informatie gebruiken om een goede taal aan te bieden. In de SimpleSAMLphp demo is dat op die manier gedaan.

Houd er rekening mee dat taaldetectie op die manier niet altijd lukt. Kies daarom altijd een goede hoofdtaal. Door het instellen van cookies kan de taal die eenmaal gekozen is, onthouden worden en voortaan voor die gebruiker als default worden aangeboden.