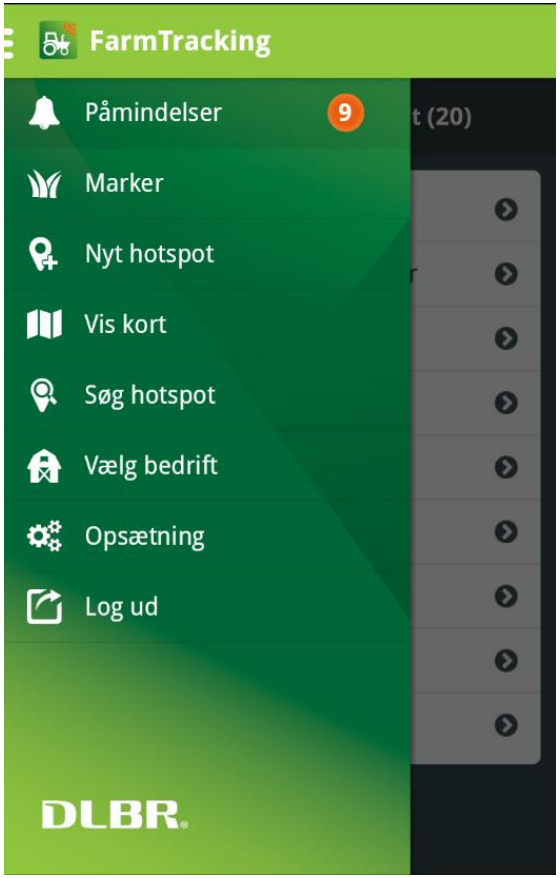
Tilpasning og modning af prototype på ”Farmtracking-grund-app”

Authentication and Web SSO



Authentication and Web SSO

- Web SSO requires the presence of the SSO cookie on the ADFS site, which is set during user authentication
- If the device browser is used for authentication, Web SSO will only work in the device browser, not in an in-app WebView
- If an in-app WebView is used for authentication, Web SSO will only work in this WebView

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

Authentication and Web SSO

- When everything runs in the device browser…
  - User can verify that he is not being phished
  - Transfer of access token to the native app becomes complex
    - Cross-platform protocol handlers
- When everything runs in an in-app WebView
  - Transfer of access token to the native app is relatively simple

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

Authentication and Web SSO

- Design decision: Authentication will be performed in an in-app WebView
  - Authentication is done using the WS Federation Passive protocol (based on browser redirects)
  - The WebView lets the user authenticate, and intercepts the token POST, storing the token in the app
- Sample code for this approach is available
  - For Windows Forms
  - For Xamarin.Forms / Xamarin.Auth / Android

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

WS-Fed flow

Following pages….

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

```
GET https://dev-www-aquaplan.vfltest.dk/ HTTP/1.1
Host: dev-www-aquaplan.vfltest.dk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.124 Safari/537.36
Accept-Encoding: gzip,deflate
Accept-Language: en,en-US;q=0.8,da;q=0.6
```

```
HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=utf-8
Location: https://si-idp.vfltest.dk/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fdev-www-
aquaplan.vfltest.dk%2f&wctx=rm%3d0%26id%3dpassive%26ru%3d%252f&wct=2014-10-06T08%3a26%3a57Z
Server: Microsoft-IIS/8.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 06 Oct 2014 08:26:57 GMT
Content-Length: 299

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="https://si-
idp.vfltest.dk/adfs/ls/?wa=wsignin1.0&amp;wtrealm=https%3a%2f%2fdev-www-
aquaplan.vfltest.dk%2f&amp;wctx=rm%3d0%26id%3dpassive%26ru%3d%252f&amp;wct=2014-10-
06T08%3a26%3a57Z">here</a>.</h2>
</body></html>
```

```
GET https://si-idp.vfltest.dk/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fdev-www-
aquaplan.vfltest.dk%2f&wctx=rm%3d0%26id%3dpassive%26ru%3d%252f&wct=2014-10-06T08%3a26%3a57Z
HTTP/1.1
Host: si-idp.vfltest.dk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.124 Safari/537.36
Accept-Encoding: gzip,deflate
Accept-Language: en,en-US;q=0.8,da;q=0.6



HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Mon, 06 Oct 2014 08:26:36 GMT
Content-Length: 5337

<login ui>
```

```
POST https://si-idp.vfltest.dk/adfs/ls/?wa=wsignin1.0&wtrealm=https%3a%2f%2fdev-www-
aquaplan.vfltest.dk%2f&wctx=rm%3d0%26id%3dpassive%26ru%3d%252f&wct=2014-10-06T08%3a26%3a57Z
HTTP/1.1
Host: si-idp.vfltest.dk
Connection: keep-alive
Content-Length: 1311
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.124 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Language: en,en-US;q=0.8,da;q=0.6

<user credentials>
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
(more headers)
Set-Cookie: MSISAuthenticated=MDYtMTAtMjAxNCAwODoyNjo0NQ==; path=/adfs/ls; secure; HttpOnly
Set-Cookie: SessionCookieKey=14187447-ed17-45cb-87ee-9f7426ec2565; path=/adfs/ls; secure;
HttpOnly
Date: Mon, 06 Oct 2014 08:26:45 GMT
Content-Length: 6174

<html><head><title>Working...</title></head><body><form method="POST" name="hiddenform"
action="https://dev-www-aquaplan.vfltest.dk/"><input type="hidden" name="wa"
value="wsignin1.0" /><input type="hidden" name="wresult"
value="&lt;t:RequestSecurityTokenResponse(<token>)/t:RequestSecurityTokenResponse>"
/><input type="hidden" name="wctx" value="rm=0&amp;id=passive&amp;ru=%2f"
/><noscript><p>Script is disabled. Click Submit to continue.</p><input type="submit"
```

```
POST https://dev-www-aquaplan.vfltest.dk/ HTTP/1.1
Host: dev-www-aquaplan.vfltest.dk
Connection: keep-alive
Content-Length: 6333
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.124 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip,deflate
Accept-Language: en,en-US;q=0.8,da;q=0.6

wa=wsignin1.0&wresult=%3Ct%3ARequestSecurityTokenResponse+xmlns%3At%3D%22http%3A%2F%2Fschem
as.xmlsoap.org%2Fws%2F2005%2F02%2Ftrust%22%3E%3Ct%3ALifetime%3E%3Cwsu%3ACreated+xmlns%3Awsu
%3D%22http%3A%2F%2Fdocs.oasis-open.org%2Fwss%2F2004%2F01%2Foasis-200401-wss-wssecurity-
utility-1.0.xsd%22%3E2014-10-
06T08%3A26%3A45.763Z%3C%2Fwsu%3ACreated%3E%3Cwsu%3AExpires+xmlns%3Awsu%3D%22http%3A%2F%2Fdo
cs.oasis-open.org%2Fwss%2F2004%2F01%2Foasis-200401-wss-wssecurity-utility-
1.0.xsd%22%3E2014-10-
06T09%3A26%3A45.763Z%3C%2Fwsu%3AExpires%3E%3C%2Ft%3ALifetime%3E%3Cwsp%3AAppliesTo+xmlns%3Aw
sp%3D%22http%3A%2F%2Fschemas.xmlsoap.org%2Fws%2F2004%2F09%2Fpolicy%22%3E%3Cwsa%3AEndpointRe
ference+xmlns%3Awsa%3D%22http%3A%2F%2Fwww.w3.org%2F2005%2F08%2Faddressing%22%3E%3Cwsa%3AAdd
ress%3Ehttps%3A%2F%2Fdev-www-
aquaplan.vfltest.dk%2F%3C%2Fwsa%3AAddress%3E%3C%2Fwsa%3AEndpointReference%3E%3C%2Fwsp%3AApp
liesTo%3E%3Ct%3ARequestedSecurityToken%3E%3Csaml%3AAssertion+MajorVersion%3D%221%22+MinorVe
rsion%3D%221%22+AssertionID%3D%22_404fbda7-00e0-4526-85a6-
4387a4f8e825%22+Issuer%3D%22http%3A%2F%2Fsi-
idp.vfltest.dk%2Fadfs%2Fservices%2Ftrust%22+IssueInstant%3D%222014-10-
06T08%3A26%3A45.778Z%22+xmlns%3Asaml%3D%22urn%3Aoasis%3Anames%3Atc%(<token>)%2Fsaml%3AAsser
tion%3E%3C%2Ft%3ARequestedSecurityToken%3E%3Ct%3ATokenType%3Eurn%3Aoasis%3Anames%3Atc%3ASAM
L%3A1.0%3Aassertion%3C%2Ft%3ATokenType%3E%3Ct%3ARequestType%3Ehttp%3A%2F%2Fschemas.xmlsoap.
org%2Fws%2F2005%2F02%2Ftrust%2FIssue%3C%2Ft%3ARequestType%3E%3Ct%3AKeyType%3Ehttp%3A%2F%2Fs
```

Securing calls to the Farmtracking Backend

- The FarmTracking backend consists of a set of services
- Services will be implemented using ASP.NET Web API
- Design decision: Service security will be based on OWIN Bearer token security (Microsoft.Owin.Security.OAuth package) using Base64-encoding (DLBR.CommonLogin.IdentityModel package)

DLBR
DANSK
LANDBRUGSRÅDGIVNING

AuthorizationConfig.cs

```
public void Configure(IAppBuilder app)
      {
          var audience =
FederatedAuthentication.FederationConfiguration.IdentityConfiguration.AudienceRestriction.AllowedAudienceUris.Single();
          var issuerNameRegistry = FederatedAuthentication.FederationConfiguration.IdentityConfiguration.IssuerNameRegistry;

          // Opting for deflate-free encoding, to make the job of the client side Javascript easier.
          var handler = new TokenHeaderEncodingSamlSecurityTokenHandler(new Base64TokenHeaderEncoder())
          {
              Configuration = new SecurityTokenHandlerConfiguration()
              {
                  AudienceRestriction =
                  {
                      AllowedAudienceUris = { audience }
                  },
                  SaveBootstrapContext = true,
                  CertificateValidator = X509CertificateValidator.None,
                  IssuerNameRegistry = issuerNameRegistry,

              }
          };
          app.UseTokenHandlerAuthentication(handler);
      }
```

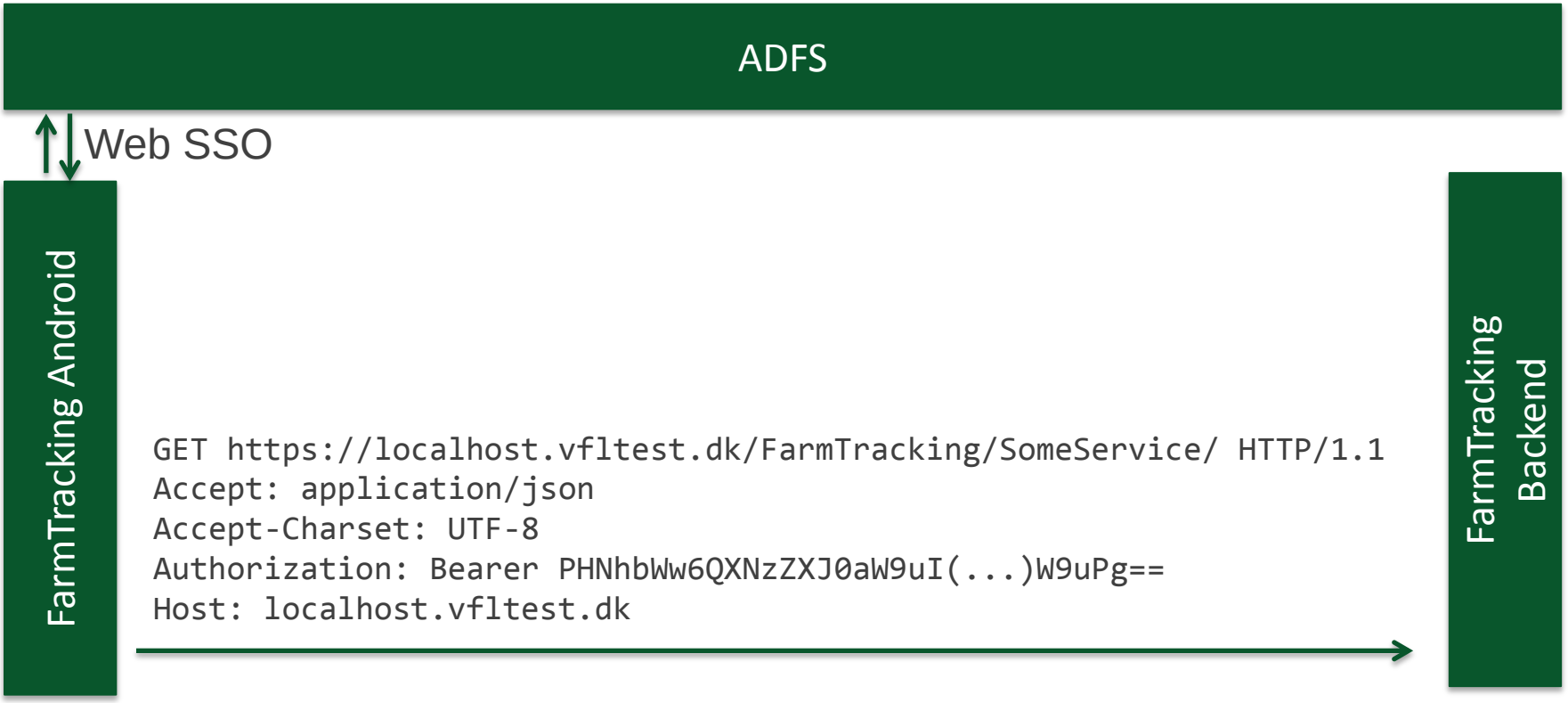
DLBR®
DANSK
LANDBRUGSRÅDGIVNING

Calling the backend from the frontend

- The Android app obtains a SAML token when the user authenticates
  - When the token expires, the Android app will ask the user to re-authenticate
- The OWIN middleware expects every call to the backend services to include an Authorization header with the value ”Bearer <encodedtoken>”
- <encodedtoken> is produced by base64 encoding the SAML token

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

Calling the FarmTracking backend



DLBR
DANSK
LANDBRUGSRÅDGIVNING

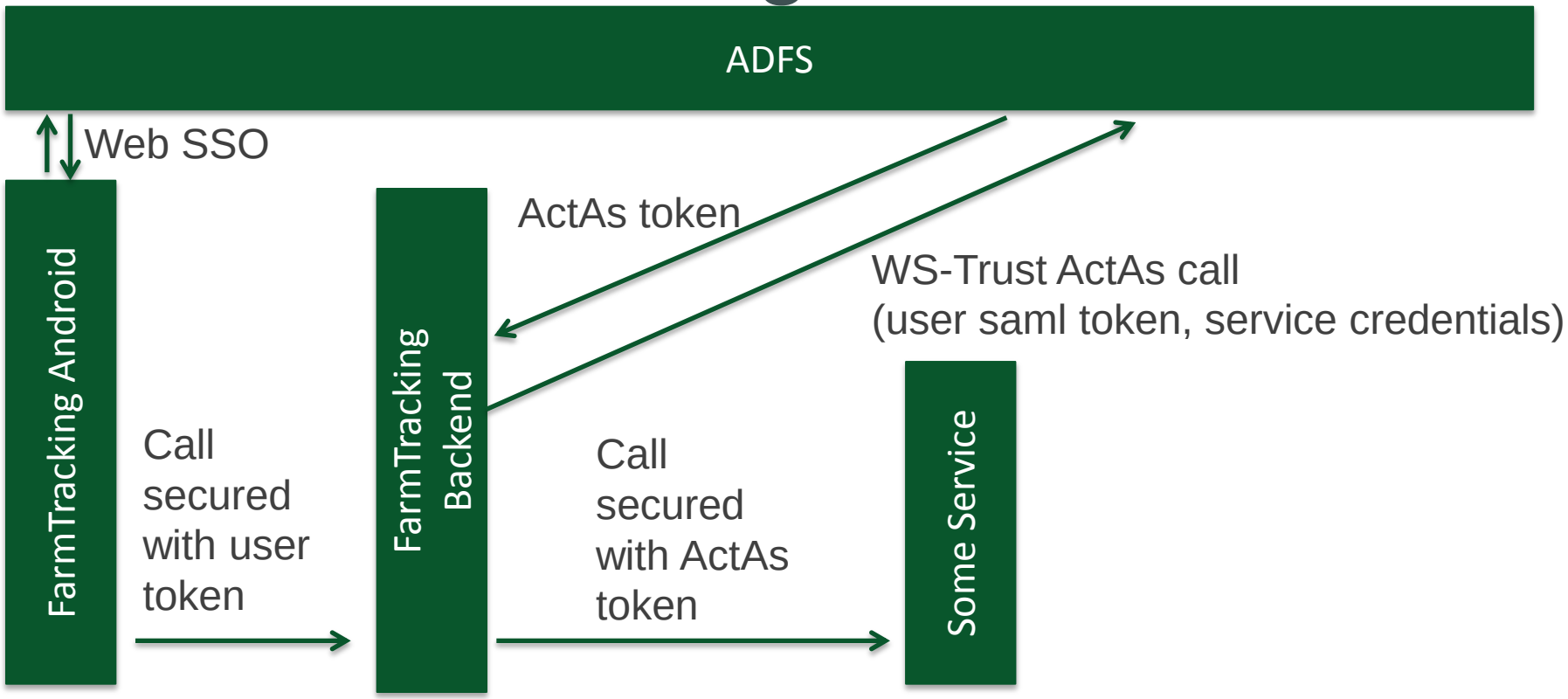
Call secured with user token

Calling other VFL services from the FarmTracking backend

- VFL runs a plethora of solutions based on securing backend calls using SAML access tokens obtained via Web Single Sign On
- Many of them have a web backend that exchange the user access token for a service backend specific ActAs token, using a system-specific account trusted for delegation
  - This exchange is done by the ADFS server
  - The resulting ActAs token contains the claims of the user, as wells as the claims of the system-specific account
  - This allows the service backend to verify the delegation chain (no ”double hop” issues)

DLBR®
DANSK
LANDBRUGSRÅDGIVNING

Calling other VFL services from the FarmTracking backend



DLBR
DANSK LANDBRUGSRÅDGIVNING