Ungedatabasen - integrationsvejledning

Indhold

Historik			
Dokumentid.	Dato	Udarb. af	Ændringer
<dok.id.>	24.11.2016	Tom Sørensen	Oprettet
	24.11.2016	Mikkel Brøndum	Reviewet
	03.02.2017	Tom Sørensen	Tilrettet vedr. STAR-end-point og sikerhedsmodel
	22.02.2017	Tom Sørensen	Apache CXF og .Net klienter inkluderet
	08-03-2017	Tom Sørensen	End-points i STILs test-miljø tilføjet
	29-03-2017	Tom Sørensen	Diverse tilføjelser - se afsnit 2
	15-05-2017	Tom Sørensen	Diverse rettelser og tilføjelser – se afsnit 2

1. Indledning og formål

Dette dokument har til formål at beskrive hvordan man som integrator kan sætte sig i stand til at integrere til Ungedatabasen og dermed gøre brug af dennes services til indberetning og efterfølgende modtagelse af informationer.

Dokumentet vil fokusere på de tekniske aspekter og henvise til dokumentet "Ungedatabasen – Snitfladebeskrivelse" for en mere detaljeret beskrivelse af de oplysninger som flyder frem og tilbage – og deres betydning.

I første omgang er dette dokument målrettet de pilot-integratorer, som vælger at samarbejde med STIL ift. at afprøve de endnu ufærdige services.

Dette dokument henvender sig til de integratorer, som benytter web services – der findes enkelte services, rettet mod grundskoler, hvor der i stedet tilbydes en FTP-grænseflade til overførsel af større filer.
FTP-grænsefladen er beskrevet i dokumentet "Ungedatabase – integrationsvejledning – FTP".

2. Status

Arbejdet med at implementere de services som udstilles er i gang og vil være det i nogle måneder. Status for den funktionalitet og features, som udstilles vil derfor ændre sig løbende. Dette afsnit beskriver på punktform hvad der i skrivende stund er med – og hvad der mangler.

Dato	Status
24.11.2016	8 af 8 services udstillet fra CGI udviklingsmiljø Udeståender: • Ingen underliggende forbindelse mellem udstillede services og UDBs funktionalitet – services giver derfor blot standardsvar • Sikkerhedsmodellen er implementeret, men kun demo-certifikat kan anvendes • FTP-baserede services til STAR og grundskoler er endnu ikke udstillet • HTTPS/TLS understøttes ikke endnu. Efter et par iterationer, vil services blive eksponeret via STILs testmiljø i stedet for via CGIs udviklingsmiljø, hvilket vil muliggøre HTTPS.
03.02.2017	Servicen HaendelserForUngeMedUddannelsespaalaeg omdøbt til HaendelserForSTAR – denne er tilgængelig fra 06.02.2017
	Mulighed for at bruge eget test-certifikat tilføjet – se afsnit 6.2
22.02.2017	Java/Apache CXF- og .Net-baseret klient vedlagt. Se afsnit 9
08.03.2017	End-points i STILs test-miljø tilføjet
29.03.2017	Ny certifikat-kæde beskrevet i det test-certifikater nu udstedes med anden kæde end tidligere. Nyt demo-certifikat tilføjet – udstedt via den nye kæde. Det nye demo-certifikat er nu inkluderet i SoapUI-projektet – se afsnit 7 Beskrivelse af certifikat-kæder til produktion tilføjet Beskrivelse af udfasning af TLS 1.0 og 1.1 – se afsnit 6.1 og 7 Snitfladeændring: Den tvungne struktur Modtager og deri indlejrede ModtagerSystemID og ModtagerSystemTransaktionsID tilføjet alle requests. Beslutningen om at indføre disse kommer centralt fra STIL integrationsplatform.

Dato	Status
15.05.2017	Fejl rettet ifbm. links til https-baserede adresser i CGIs miljø Produktions end-points tilføjet – som de forventes udstillet hos STIL Opdateret .Net-klient inkluderet – den håndterer nye felter (ModtagerSystemID og ModtagerSystemTransaktionsID) og inkluderer nyt validt FOCES-certifikat – det var gamle var udløbet.

3. Generelt

Ungedatabasen (UDB) udstiller en række SOAP-baserede web services, som kan opdeles i to grupper:

1. Indberetningsservices – som gør det muligt for systemer at indberette informationer om unges uddannelses- og beskæftigelsessituation. UDB gemmer, validerer og processerer disse oplysninger og danner på den baggrund en række hændelser, som efterfølgende stilles til rådighed for de eksterne systemer i form af notifikationer. Processeringen af de indberettede informationer er hovedsageligt asynkron, hvilket betyder at det kaldende system får en kvittering tilbage såfremt det indsendte request kan XML Schema valideres og hvis det lever op til kravene mht. sikkerhed (beskrevet senere). Den egentlige forretningsmæssige processering sker efterfølgende.
2. Notifikationsservices, som gør det muligt at hente de notifikationer der stilles til rådighed for det pågældende system.

Al kommunikation initieres af det eksterne system, som kalder UDB for indberette eller hente notifikationer.

4. Trin guide

Når et eksternt system ønsker at kommunikere med UDB, skal det pågældende system registreres i UDB.

Kommer senere – de udstillede pilot-services er pt. tilgængelige for alle og et demo-certifikat kan anvendes.

5. Services

Alle 8 SOAP-baserede services er i skrivende stund udstillet via CGIs udviklingsmiljø.
WSDL'erne for disse kan tilgås via disse adresser:

http://78.41.241.10:9000/services/AbonnementForUddannelsespaalaeg/?wsdl
http://78.41.241.10:9000/services/ForberedendeForloeb/?wsdl
http://78.41.241.10:9000/services/VideregaaendeUddannelse/?wsdl
http://78.41.241.10:9000/services/UngdomsUddannelse/?wsdl
http://78.41.241.10:9000/services/KontaktOgTilbudstid/?wsdl
http://78.41.241.10:9000/services/HaendelserForSTAR/?wsdl [1]
http://78.41.241.10:9000/services/HaendelserForUUCenter/?wsdl
http://78.41.241.10:9000/services/ValideringsSvarOgAdvis/?wsdl

Og via HTTPS på følgende adresser:

https://78.41.241.10/services/AbonnementForUddannelsespaalaeg/?wsdl

[1] Udstilles 6/2-2017

https://78.41.241.10/services/ForberedendeForloeb/?wsdl
https://78.41.241.10/services/VideregaaendeUddannelse/?wsdl
https://78.41.241.10/services/UngdomsUddannelse/?wsdl
https://78.41.241.10/services/KontaktOgTilbudstid/?wsdl
https://78.41.241.10/services/HaendelserForSTAR/?wsdl
https://78.41.241.10/services/HaendelserForUUCenter/?wsdl
https://78.41.241.10/services/ValideringsSvarOgAdvis/?wsdl

Pr. ultimo marts 2017 udstilles services i STILs test-miljø på følgende URLs:

https://ws01.ung.stil.dk/services/AbonnementForUddannelsespaalaeg/?wsdl
https://ws01.ung.stil.dk/services/ForberedendeForloeb/?wsdl
https://ws01.ung.stil.dk/services/VideregaaendeUddannelse/?wsdl
https://ws01.ung.stil.dk/services/UngdomsUddannelse/?wsdl
https://ws01.ung.stil.dk/services/KontaktOgTilbudstid/?wsdl
https://ws01.ung.stil.dk/services/HaendelserForSTAR/?wsdl
https://ws01.ung.stil.dk/services/HaendelserForUUCenter/?wsdl
https://ws01.ung.stil.dk/services/ValideringsSvarOgAdvis/?wsdl

STILs produktionsmiljø der etableres medio maj vil udstille sine services på følgende adresser:

https://ws03.ung.stil.dk/services/AbonnementForUddannelsespaalaeg/?wsdl
https://ws03.ung.stil.dk/services/ForberedendeForloeb/?wsdl
https://ws03.ung.stil.dk/services/VideregaaendeUddannelse/?wsdl
https://ws03.ung.stil.dk/services/UngdomsUddannelse/?wsdl
https://ws03.ung.stil.dk/services/KontaktOgTilbudstid/?wsdl
https://ws03.ung.stil.dk/services/HaendelserForSTAR/?wsdl
https://ws03.ung.stil.dk/services/HaendelserForUUCenter/?wsdl
https://ws03.ung.stil.dk/services/ValideringsSvarOgAdvis/?wsdl

6. Sikkerhed

6.1 Kryptering

Der anvendes HTTPS/TLS til transport-level kryptering af kommunikationen mellem parterne.
For services udstillet i CGIs udviklingsmiljø foregår krypteringen via et self-signed certifkat, som ikke matcher den anvendte URL.
Public-delen af dette certifikat kan hentes via denne adresse en af de ovennævnte https://78.41.241.10 WSDL-URLs hvorfra eksempelvis Internet Explorer kan downloade og installere certifikatet.

For services i STILs test-miljø foregår krypteringen via det certifikat, som STIL test-miljø udstiller.
Public-delen af dette certifikat kan hentes via denne adresse:

https://ws01.ung.stil.dk

Den kaldende part skal trust'e dette certifikat og den kæde, som validerer det, og den WS-client eller den infrastruktur, som de eksterne system anvender skal kunne håndtere TLS.

TLS 1.0, 1.1 og 1.2 understøttes pt. – dog vil services i STILs test og produktionsmiljø kun understøttes TLS 1.2.

6.2 Autentificering

Det eksterne system skal identificere sig overfor UDB vha. et OCES II funktionscertifikat.

I pilot- og test-fasen understøttes kun brugen af OCES testcertifikater, som skal være baseret på en af følgende certifikat-kæder:

- TRUST2408 Systemtest VII Primary CA
  - TRUST2408 Systemtest VII CA
- TRUST2408 Systemtest VII Primary CA
  - TRUST2408 Systemtest XIX CA

UDBs produktionsmiljø understøtter production-grade certifikater baseret på en af følgende certifkat-kæder:

- TRUST2408 OCES Primary CA
  - TRUST2408 OCES CA I
- TRUST2408 OCES Primary CA
  - TRUST2408 OCES CA II

Der er vedlagt et brugbart test-certifikat – se afsnit 7.

Pilot-integratorer kan benytte vedlagte demo-certifikat til at identificere sig – og vil dermed få adgang til alle til rådighed værende services og alle data, som udstilles derigennem. Det anbefales at integratorerne anskaffer eget test-certifikat – baseret på en af ovennævnte Systemtest certifikat-kæder. Når en integrator benytter eget test-certifikat, skal public key-delen af dette sendes til tom.sorensen@cgi.com samme med en liste af de service hvortil der ønskes adgang. Ungedatabasens integrationsplatformen vil da blive konfigureret i henhold til dette.
For en kort instruktion i hvordan man anskaffer sig et test-certifikat – se afsnit 8

Tilsvarende skal integratorer anskaffe sig production-grade certifikat og sende public-key delen af dette til tom.sorensen@cgi.com

Det eksterne system skal sikre, at SOAP requests til UDB indeholder følgende elementer:

- WSS Timestamp
- WSS Signature
- WSS UsernameToken

6.2.1 WSS Timestamp

Et WSS Timestamp element kan eksempelvis så ud som følger:

```
<soapenv:Header>
        <wsse:Security xmlns:wsse="http:… >
             <wsu:Timestamp xmlns:wsu="http:... >
                  <wsu:Created>2016-10-28T09:57:07.976Z</wsu:Created>
                  <wsu:Expires>2016-10-28T10:02:07.976Z</wsu:Expires>
               </wsu:Timestamp>
```

6.2.2 WSS Signature

Det eksterne system skal signere body-delen af requestet til UDB med sin private key og vedlægge public-delen af certifikatet.
Signatur-element skal indeholde følgende elementer:

- <ds:SignedInfo>: oplysninger om hvad der skal signeres. SOAP Body beskeden køres igennem en hash funktion, hvorved der dannes en hash værdi, kaldet for en ”message digest”.
- <ds:SignatureValue>: selve den digitale signatur, den dannede ”message digest” krypteret med afsenderens private key.
- <ds:KeyInfo>: skal indeholde en reference til X509v3 baserede offentlige nøgle. Den offentlige nøgle skal vedlægges som BST.

UDB dekrypterer den medsendte message digest med den vedlagte public key og verificerer dermed at den blev krypteret af afsenders private key – og dermed afsenderens identitet.

6.2.3 WSS UsernameToken

UDBs services har brug for at vide hvilken institution der afsender det pågældende request. Placer derfor institutionens institutionsnummer i UsernameToken/Username. Det er spiller ingen rolle hvad der angives som password – feltet må blot ikke være tomt.
Brugen af UsernameToken bidrager ikke i sig selv til at verificere, at det deri medsendte institutionsnummer er sandfærdigt.

7. SoapUI projekt

For at demonstrere hvordan requests til UDBs service kan se ud og hvordan sikkerhedssetuppet i praksis afspejles i requestet – findes vedlagte SoapUI projekt og tilhørende democertifikat.

UngeDBProject.zip

Projektet fungerer i v. 5.2.1 – og sikkert også i andre versioner af SoapUI.

I projektet er der importeret en WSDL fra en UDBs udstillede service – og der et defineret en sikkerhedsprofil kaldet ”Security”, som matcher det UDB forventer. Profilen anvender det vedlagte certifikat til signering.
Afhængigt at den JVM, som afvikler SoapUI, kan det være nødvendigt at tilføje flg. parameter for at sikre, at SoapUI understøtter TLS 1.2:

```
-Dsoapui.https.protocols=SSLv3,TLSv1.2
```

Det anbefales at tilføje denne i bin\Soap-5.2.1.vmoptions der hvor SoapUI er installeret.
Selve filnavnet vil variere ift. den valgte version af SoapUI.

8. Anskaffelse af certifikat

8.1 Test-certifikat

Sådan skaffer du et eller flere test-certifikater indeholdende et vilkårligt CVR-nummer:

1. Gå ind i test-miljøet hos NemId:
https://erhverv.pp.certifikat.dk/produkter/nemid_medarbejdersignatur/bestil_nemid/index.html?execution=e1s1

2. Find på et eksisterende CVR nummer – ligegyldigt hvilket - og gennemfør bestillingen.

3. Send en mail med til jeres certifikat-ansvarlige indeholdende CVR nummeret – han/hun vil så godkende det.

4. Efterfølgende kan man selv i den tilhørende selvbetjening udstede, spærre og ændre alle de funktionscertifikater indeholdende det anvendte CVR-nr., som man ønsker. Det er gratis.

8.2 Produktions-certifikat

Bestillingen af et produktions-certifikat indeholdende korrekte CVR-nr. skal ske via den person, som hos Nets/DanID er udpeget som virksomhedens certifikatadministrator – også kaldet LRA.

9. Eksempler til på WS-klienter

Der er konstrueret en to forskellige WS-klienter, som eksemplificerer hvordan et eksternt system kan implementere den WS-klient, som håndterer kaldet til UDBs services.

Klienterne er eksempler på hvordan en specifik UDB-service kaldes, og kan dermed kun anvendes direkte hvis man ønsker at kalde netop den eksemplificerede service.

9.1 Java / Apache CXF

Vedlagte klient til servicen ForberedendeForloeb kræver Java 1.8 og bygges med Maven.

udb-client.zip

9.2 Microsoft .Net

Vedlagte klient til servicen HaendelserForUUCenter er baseret på XUnit og indeholder en WCF CustomBinding, som matcher servicens sikkerhedsmodel.

HaendelserForUUCenter-signing-client.zip