DFDGs sikkerhedsmodel

Følgende beskriver den sikkerhedsmodel der er anvendt på DFDG's webservicesnitflade.

Alle webservices udstilles via SOAP-XML grænseflade og via HTTPS forbindelse. Alle webservices publiceres via WSDL filer. Aftagere skal anvende funktionscertifikater (FOCES). I metadata i SOAP headeren skal det angives hvilken myndighed kaldet foretages på vegne af, alt hvem aftager virker som databehandler for. Derudover skal angives hvilken bruger / medarbejder / applikationsproces (ved batch-processeringer) der foretager handlingen, uanset om det er en læse eller skriveoperation, for at dette kan logges.

Se også generelt om sikkerhed her: Sikkerhed

Metadata i SOAP Header

Sikkerhedsmodellen tager udgangspunkt i to overordnede SOAP request headers:

- ActiveOrganisationHeader - der anvendes til tjek af den grundlæggende sikkerhed, må denne databehandler behandle data for denne myndighed.
- RequestUserMetadata - anvendes primært til logning, så der sikres sporbarhed i forhold til, hvem det er, der anvender services, se elementerne i detaljer nedenfor. Elementet anvendes dog også til tjek af anden aktørs adgang til borger, tjek i forbindelse med gæsteadgang samt til tjek i forbindelse med sagsbehandlerlogin på Jobnet.

Undtaget fra disse er offentlige webservices, der kan udstilles uden sikkerhed.

Request Header

Følgende header-elementer angives i service-metodens requesttype, hvilket gøres ved at nedarve fra DFDG.Foundation.Core.Model.ServiceModel.BaseRequest class:

Request Class

```
public class BaseRequest
    {
  [MessageContract]
  public class BaseRequest
  {
         [MessageHeader(Namespace =
"http://rep.oio.dk/ams.dk/xml/schemas/2005/09/01/")]
      public ActiveOrganisationHeaderType ActiveOrganisationHeader {
get; set; }

   [MessageHeader(Namespace =
"http://service.bm.dk/RequestUserMetadata/2015/01/21/")]
   public RequestUserMetadataType RequestUserMetadataHeader { get;
set; }
     }
    }

 using DFDG.Foundation.Core.Model.ServiceModel;

    public class GetMyServiceExampleMethodRequest : BaseRequest
    {
        [MessageBodyMember(Name = "GetMyServiceExampleMethodRequest",
Namespace = "http://service.bm.dk/pjaktass/1/MyService", Order = 0)]
        public GetMyServiceExampleMethodRequestType
GetMyServiceExampleMethodRequest1 { get; set; }
    }
```

Feltnavn	Type	Detaljer	Forekomst	Beskrivelse
ActiveOrganisationHeader	ActiveOrganisationHeaderType		1	ActiveOrganisationHeader benyttes til angive hvilken myndighed kalderen udgiver (impersonate) sig for at være overfor DFDG.
- OrganisationTypeIdentifier	OrganisationTypeIdentifierType Base: Integer		1	Identificerer den type af organisation, som kaldet er foretaget på vegne af. Dette er en kodeliste, dog angives værdi som en integer af historiske årsager.
- OrganisationCode	String		1	Koden som identificerer organisationen. Det kan være jobcenternummer, et CVR nummer, en a-kassekode, en kommunekode, afdelingsnummer etc.

RequestUserMetadataHeader	RequestUserMetadataType		1	RequestUserMetadataHeader benyttes til at angive den kaldende myndighed overfor DFDG samt information om den kaldende bruger.
- RequestUserStructure	RequestUserStructureType		1	Struktur der indeholder beskrivelse af brugeren
- - UserFullName	UserFullNameType Base: String	Length: 1-140	1	Brugers fulde navn, ved systemkald angives systemets og jobbets navn her. Der skal oplyses konkret navn på medarbejder, når der er tale om Webservice kald foranlediget af sagsbehandleres læsning eller opdatering af oplysninger i DFDG eller STARs øvrige systemer.
- - RequestUserTypeIdentifier	RequestUserTypeIdentifierType Base: Integer		1	Kodeliste med brugertyperne: 1. Citizen - Borger, f.eks. i selvbetjeningsløsninger 2. CaseWorker - Sagsbehandler 3. System - En systemproces, som f.eks. et batchjob, eller noget andet automatiseret der ikke kan henledes til en brugerhandling. 4. CompanyEmployee - fx raskmelding foretaget medarbejder i en af virksomhed (via NemRefusion)
- - UserIdentifier	UserIdentifierType Base: String	Length: 1-255	1	Unik identifikation af brugeren, f.eks. en GUID, et medarbejder ID, system ID, bruger ID, certifikat ID, cpr-nummer, email (hvis den er unik) o.l. Afhængigt af RequestUserTypeIdentifier udfyldes feltet med: 1. Borgers CPR nummer eller et andet unikt ID, der identificerer borgeren 2. Sagsbehandler ID, der kan spores tilbage til brugeren, kan være en e-mail, et medarbejder id, eller lignende 3. System ID, unik identifikation af den proces eller batchjob der foretog handlingen.
- - UserEmail	EmailAddressIdentifierType String (E-mail)	Length: 2-256 Pattern: ([^>\(\)\[\]\\,;:@\s]{0,191}@[^>\(\)\[\]\\,;:@\s]{1,64})	0-1	Hvis der angives e-mail: Brugerens e-mail adresse skal angives, når der er tale om Webservice kald foranlediget af sagsbehandleres læsning eller opdatering af oplysninger.

- RequestOrganisationStructure	RequestOrganisationStructureType		1	Information om den organisation, som brugeren, der har foretaget kaldet, tilhører.
- - OrganisationTypeIdentifier	OrganisationTypeIdentifierType Base: Integer		1	Kodeliste. Identificerer den type af organisation, som brugeren hører til. Dette er en kodeliste, dog angives værdien som en integer af historiske årsager.
- - OrganisationCode	String		1	Koden som identificerer organisationen. Det kan være et jobcenternummer, CVR nummer, en a-kassekode eller en kommunekode.
- RegistrationDateTime	DateTime		1	Registreringstidspunkt i kaldende system

Fejlhåndtering

Når der kaldes tjekkes indholdet af felterne og rettighederne i forhold til kalder. Dette kan resulterer i følgende fejl, som skal håndteres på tværs af alle DFDG's webservicekald, der anvender sikkerhedsmodellen.

Fejlkoder

Fejlkode	Fejlbesked	Release
8173	OrganisationType is invalid according to the organisationTypeIdentifierCodeList.	2015-2
8174	UserType is invalid according to the requestUserTypeIdentifierCodeList.	2015-2
8232	The Soap request message is missing its required Soap header: ActiveOrganisationHeader	2015-2
8233	The Soap request message is missing its required Soap header: RequestUserMetadataHeader	2015-2
8234	Could not deserialize the Soap header: ActiveOrganisationHeader	2015-2
8235	Could not deserialize the Soap header: RequestUserMetadataHeader	2015-2

Udfyldelse af OrganisationTypeIdentifier og OrganisationCode felterne

Følgende beskriver, hvorledes sammenhængen er mellem organisationstypen og organisationskoden, derudover gennemgås, hvorledes de forskellige aktører forventes at kalde.

OrganisationType Identifier	Organisation	OrganisationCode Beskrivelse	Format	Eksempel
~~1~~	~~Arbejdsformidlingen~~			
2	A-kasse	A-kassekode	Integer - 2 cifre	15 Se Identifikator feltet i kodeliste: Get UnemploymentFundList
~~3~~	~~UdgaaetKommuner~~	~~Kommunekode~~	~~Integer - 3 cifre~~	~~101~~
4	Anden Aktør	CVR-nummer	Integer - 8 cifre	31299004

5	STAR	Afdelings-/systemnummer	Integer	0=Ikke specificeret (Udgår) 1=DFDG 2=Jobnet 3=LSS 4=BSM-Overvågning 5=Jobbing 6=MitJobkompas 7=EØS 8=VITAS 9=Planner 10=JobAG 11=JobKon 12=Jobservice Danmark 13=Borger.dk 14=IOM
6	Driftsselskab	Jobcenterkode	Integer - 5 cifre	10100 Se kodeliste: GetJobCenterList
7	Kommune	Kommunekode	Integer 3 cifre	101 Se kodeliste: GetMunicipalityList
8	JobCenter	Jobcenterkode	Integer - 5 cifre	10100 Se kodeliste: GetJobCenterList
~~9~~	~~Beskæftigelsesregion~~			
11	Uddannelsesinstitution	CVR-nummer	Integer - 8 cifre	32435465
12	Samarbejdspartner	CVR-nummer	Integer - 8 cifre	32435465
13	Sygehusregion	CVR-nummer	Integer - 8 cifre	32435465
14	Kriminalforsorgen	CVR-nummer	Integer - 8 cifre	32435465
15	Styrelsen for IT- og Læring	CVR-nummer	Integer - 8 cifre	32435465
16	Styrelsen for Videregående Uddannelser	CVR-nummer	Integer - 8 cifre	32435465
17	Fagforbund	CVR-nummer eller CPR-nummer [1)]	Integer 8/ string 10	32435465 / 0101714321
18	Udbetaling Danmark (UDK)	CVR-nummer	Integer - 8 cifre	32435465
19	Udlændinge, Integrations- og Boligministeriet (UIBM)	CVR-nummer	Integer - 8 cifre	32435465
20	Privat jobbank eller vikarbureau	CVR-nummer eller CPR-nummer 1)	Integer 8/ string 10	32435465 / 0101714321

Bemærk at der ikke er validering på at indberetninger med en given OrganisationCode indberetter jf. ovenstående formater.

1) Hvis der kaldes ind fra systemet, forventes RequestUserType sat til 3 - System og OrganisationCode er et CVR nummer. Derimod forventes kald fra borgervendt selvbetjeningsløsning at komme med RequestUserType 1 - Citizen og OrganisationCode: CPR-nummer.

Kommunalt Jobcenter sagsbehandlingssystem - KSS

Dette omhandler systemer som:

- KMD Momentum (Opera og Workbase)
- Schultz FASIT
- Andre jobcentersystemer

Der anvendes (mindst) ét FOCES certifikat pr. system. Metadata udfyldes ud fra følgende:

Feltnavn	Indhold
ActiveOrganisationHeader	OrganisationTypeIdentifier = 8 OrganisationCode = Jobcenterkode / 10100

RequestUserMetadataHeader	Hvis jobcentermedarbejder: • OrganisationTypeIdentifier = 8 • OrganisationCode = Jobcenterkode / 10100 Hvis Kommunalmedarbejder: • OrganisationTypeIdentifier = 7 • OrganisationCode = Kommunekode / 751 Hvis anden aktør medarbejder: • OrganisationTypeIdentifier = 4 • OrganisationCode = CVR nummer / 32435465

Hvis der skal laves sagsbehandling på en borger, der ikke ”ejes” af pågældende myndighed, skal myndigheden forinden overtage borgeren. Myndighedstilknytningen udledes via borgerens adresse, men den er selvstændig og kan ændres. Borgeren kan til enhver tid kun have én myndighedstilknytning.

Ydelsescentersystemer

Dette dækker systemer som:

- KMD-Aktiv og KOMBIT KY
- KMD eDagpenge og KOMBIT KSD
- Andre ydelsescentersystemer

Der anvendes (mindst) ét FOCES certifikat pr. system. Metadata udfyldes ud fra følgende:

Feltnavn	Indhold
ActiveOrganisationHeader	OrganisationTypeIdentifier = 7 OrganisationCode = Kommunekode / 751
RequestUserMetadataHeader	Hvis kommunal medarbejder: • OrganisationTypeIdentifier = 7 • OrganisationCode = Kommunekode / 751

A-kasse-sagsbehandlingssystemer

Der anvendes mindst ét FOCES cerfikat pr. a-kasse, også selv om disse anvender samme databehandler/system. Denne model har Datatilsynet accepteret på et møde om *a-kassernes* overgang til FOCES.

Feltnavn	Indhold
ActiveOrganisationHeader	OrganisationTypeIdentifier = 2 OrganisationCode = A-kassekode / 15
RequestUserMetadataHeader	Hvis a-kasse medarbejder: • OrganisationTypeIdentifier = 2 • OrganisationCode = A-kassekode / 15

Anden aktør sagsbehandlingssystemer

Anden Aktør opererer på vegne af en myndighed og det er derfor pågældende myndigheds ansvar, at Anden Aktør kun har den adgang, de må have. Anden aktør skal derfor anvende myndighedens certifikat. Vi kan via metadata se at det er AA der har foretaget registreringen, se eksempel senere i dokumentet.

I forhold til at have adgang til borger så validerer DFDG på om der foreligger en henvisning til borgeren for CVR nummeret for AA.

Feltnavn	Indhold
ActiveOrganisationHeader	OrganisationTypeIdentifier = 8 OrganisationCode = Jobcenterkode (det henvisende jobcenter) / 10100

RequestUserMetadataHeader	Hvis anden aktør medarbejder: • OrganisationTypeIdentifier = 4 • OrganisationCode = CVR nummer / 32435465

Se også: ExternalOperatorRegistrationService (Version 6)

STAR's systemer

Jobnet for jobkonsulenter

I forbindelse med at sagsbehandlerne kommer online på Jobnet via NemID erhverv, skal der i kommunikationen med DFDG stadig anvendes FOCES certifikatet. Medarbejderens myndighed fra NemID sendes som en del af metadata i dette tilfælde.

Jobcenter Planner

Jobcenter Planner skal anvende et FOCES certifikat, der har adgang til DFDG for den myndighed (kommune), der anvender Jobcenter Planner. Calender Provider (CP) kan stadig anvende et STAR certifikat.

Der kan evt. laves en direkte binding, da både DFDG og Jobcenter Planner er ejet af STAR og er på samme LAN. DFDG kan vælge at stole på, at Jobcenter Planner autentificerer brugerne. Dermed vil man skulle overføre data, der indeholder myndighedens identitet på en anden måde end FOCES. Afventer nærmere analyse.

Jobnet

Jobnet er et STAR system som fortrinsvis anvendes af borgerne. Jobnet bruger uafhængigt af borgers kommunetilknytning samme FOCES certifikat, og kalder med følgende:

Feltnavn	Indhold
ActiveOrganisationHeader	OrganisationTypeIdentifier = 5 OrganisationCode = 2
RequestUserMetadataHeader	Hvis borger: • OrganisationTypeIdentifier = 5 (* i mangel af en organisationkode for borgere) • OrganisationCode = 2 • RequestUserTypeIdentifier = 1 • UserIdentifier = CPR eller CV-number For sagsbehandlere kaldes med følgende, der dog kræver at Jobnet selv tjekker om sagsbehandler må få adgang til borger, enten via jobcentertilknytning, gæsteadgang eller henvisning. Hvis jobcenter sagsbehandler: • OrganisationTypeIdentifier = 8 • OrganisationCode = Jobcenterkode • RequestUserTypeIdentifier = 2 • UserIdentifier = Certifikat RID Hvis anden aktør sagsbehandler: • OrganisationTypeIdentifier = 4 • OrganisationCode = CVR number • RequestUserTypeIdentifier = 2 • UserIdentifier = Certifikat RID

Certifikater og testmiljøer

STAR stiller testcertifikater til rådighed som giver adgang til at agere som en eller flere myndigheder på et eller flere testmiljøer.

Serviceaftagers forpligtigelser

Web service aftageren skal etablere og opretholde fornødne sikkerhedsmæssige tiltag til sikring af, at meddelelser, der udveksles via

Webservices, ikke kommer til uvedkommendes kendskab, forvanskes eller går til grunde.

Det er web service aftagernes eget ansvar at sikre, at dennes IT-systemer er konfigureret og eventuelt tilrettet i nødvendigt omfang til at kunne få adgang til de i dette dokument beskrevne Web services.

Ligeledes er web service aftagernes ansvar at sikre, at der er knyttet forsvarlige sikkerhedsforanstaltninger til de applikationer og systemer, denne benytter for at kunne anvende de i dette dokument beskrevne Webservices.

Yderligere specifikation af de krav der stilles til webservice aftageren findes i tilslutningsaftalen.

Følgende beskriver de forpligtelser serviceaftageren påtager sig i forbindelse med en hver form for brug af de i dette dokument beskrevne services.

Serviceaftageren forpligter sig til følgende:

- Såfremt serviceaftageren tilgår webservices der kræver unik identifikation af hvilken medarbejder/sagsbehandler/bruger der har fortaget handlingen, skal aftager enten anvende en certifikatmodel, der understøtter dette eller specifikt anvende versioner af webservices, hvor der medsendes brugerid.
- Serviceaftager skal i webservices, hvor det er beskrevet, at der skal medsendes navn på den sagsbehandler, der er ansvarlig eller den sagsbehandler, der foretager læsning eller registrering af oplysninger, som minimum oplyse medarbejdernes for- og efternavn i servicekaldet, dvs.
    - der skal oplyses konkret navn på medarbejder, når der er tale om ws-kald foranlediget af sagsbehandleres læsning eller opdatering af oplysninger DFDG eller STARs øvrige systemer - der må i sådanne tilfælde ikke oplyses fx "Unknown" eller et systemnavn som navn på medarbejderen
    - angivelse af kun systemnavn er alene tilstrækkeligt, hvis ws-kald til DFDG er foranlediget af batchjob i det aftagende system
- Serviceaftageren er forpligtet til at logge de kvitteringer der returneres af servicen
- Serviceaftageren forpligter sig til at logge alle SOAP faults inkl. fejl koden som en del af deres fejl log.
- Serviceaftageren forpligter sig til, at reagere på de SOAP-falts som DFDG og STARs andre it-systemer returnerer ved forsøg på registrering i DFDG og STARs andre it-systemer

Krav til logging hos aftageren

Web service aftageren skal gennemføre en grundlæggende logging i forhold til kommunikationen med de i dette dokument beskrevne web services.

Web service aftageren skal opretholde en log med de kvitteringer der returneres til aftageren når serviceaftageren sender hændelser til de udstillede services.

Hvis der i kommunikationen opstår en fejl skal web service aftageren logge fejlen incl. allle fejl informationer der returneres fra servicen, samt den afsendte besked.

Web service aftageren skal som minimum også logge følgende indformationer:

- BrugerID – Unik identifikation af brugeren
- Den organisationstype brugeren repræsenterer f.eks. jobcenter eller a-kasse
- Den organisationskode der er knyttet til den organisation brugeren repræsenterer
- Timestamp

Hvis der indgår personoplysninger i applikationen skal logningen være i overensstemmelse med Bekendtgørelse nr 528 af 15/06/2000 - Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Se iøvrigt: Krav til logning i applikationer

Anvendelse af OrganisationType ved WSRM

Når der skal hentes beskeder over WSRM anvendes OrganisationType på følgende måde:

- Jobcenter medarbejdere kalder med OrganisationType=8
- Kommunale medarbejdere kalder med OrganisationType=7
- A-kassen kalder med OrganisationType=2

SAML og medarbejdercertifikater

Der er stadig behov for at have et SAML login i forbindelse med de administrative systemer: AMP, JCP, JN Administration, LSS, JobKon med videre.

AMPs sikkerhedsmodul (baseret på MOCES/nemid erhverv) fortsætter med at fungerer. Brugerdatabasen indeholder kun brugere, der anvender SAML løsningen. Denne løsning er separat fra webservices FOCES sikkerhedsmodel og beskrives derfor ikke yderligere her.