DATAFORDELER

Datafordelerens sikkerhedsmekanismer

Version: 1.0,
Juni 2016

DATAFORDELER

Indholdsfortegnelse

1. Indledning

Dokumentet beskriver det sikkerhedsmæssige setup omkring Datafordeleren. Dokumentet fokuserer på beskrivelse af den tekniske sikkerhed og omfatter ingen beskrivelse af oprettelse/fremskaffelse af f.eks. akkreditiver.
Dokumentet beskriver setup gældende fra august 2016.

2. Målgruppe for dokument

De primære målgrupper for dokumentet er dataanvendere, som vil kalde services på Datafordeleren for at tilgå grunddata samt dataleverandører, dvs. grunddataregistre, der skal levere grunddataopdateringer til Datafordelen.

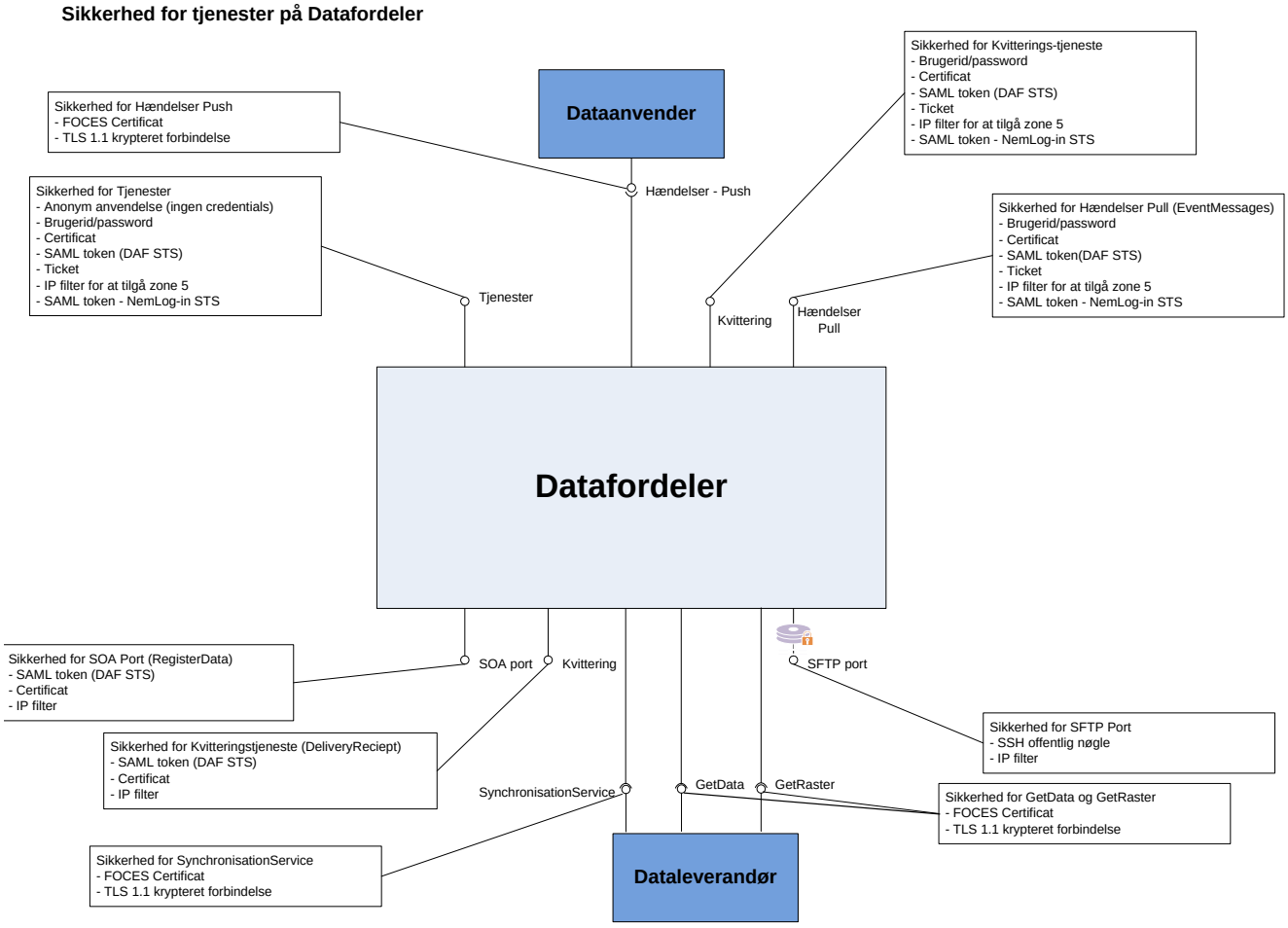
3. Generel sikkerhed omkring Datafordeler

Datafordeleren er opdelt i et antal sikkerhedszoner. For hver zone gælder et sæt af sikkerhedsmekanismer, og dermed vil sikkerhedsmekanismer for services variere, afhængig af hvilken zone services er udstillet i.

Navn	Beskrivelse	Adgangsbegrænsning
S5	Zone til opbevaring af personhenførbare, samt fortrolige data. Zonen indeholder systemkomponenter til udstilling og modtagelse af sådanne data. Alle registre sender deres data til systemet via replikeringskanaler i denne zone.	Zonen kan kun tilgås fra en på forhånd **godkendt** ip-adresse via internettet. Al web service kommunikation foregår over en TLS 1.1 (eller nyere) forbindelse til Tjenester og replikeringskanalens web-serviceport, der autentificeres med FOCES/VOCES certifikat. FTP-servere i zonen tilgås over SFTP fra en godkendt IP adresse, der autentificeres med en SSH nøgle.
S3	Systemkomponenter til konfiguration af systemet herunder oprettelse af systembrugere, administration af brugerrettigheder, start og stop af replikeringskanaler og konfiguration af tjenester.	Zonen kan kun tilgås fra en godkendt ip-adresse via internettet eller via MPLS(tilkøb). Al kommunikation foregår over TLS 1.1 (eller nyere).
S0	Zone til opbevaring af ikke-fortrolige data og brugerdata. Zonen indeholder systemkomponenter til udstilling af ikke-fortrolige eller personhenførbare data, oprettelse af brugere, bestilling af dataudtræk, oprettelse af abonnementer samt infrastrukturkomponenter til autentifikation og autorisation. De ikke-fortrolige eller personhenførbare data fra registrene modtages via replikeringskanaler i sikkerhedszone S5 (se beskrivelse af S5).	Adgang via internettet

4. Diagram over sikkerhed for Datafordeler

Nedenstående diagram viser et overblik for det sikkerhedsmæssige setup for dataanvendere og dataleverandører i forhold til tjenester og hændelser. De enkelte integrationspunkter for Datafordeleren er angivet, og for hvert af disse er opsummeret hvilke sikkerhedsmekanismer, der er gældende. Diagram i stor størrelse findes sidst i dokumentet.



5. Sikkerhed for dataanvendere

5.1 Generel sikkerhed for dataanvendere i Datafordelermiljøet.

Ip- filtrering (white listing). For dataanvendere kan adgang til Datafordelerportaler og zone 5 services kun ske fra ip-adresser, som er white listede, dvs. ip-adresser hvor der positivt er åbnet for adgang til Datafordeler. Kommunikation fra IP-adresser, der ikke er white listet, vil blive afvist.

5.2 Integrationspunkter for dataanvendere

Integrationspunkt	Beskrivelse og anvendelse	Sikkerhed
Tjenester	Service som kaldes fra dataanvendere for at hente data på datafordeleren	• Ip filter for white listed IP-adresse (for detaljer se ovenfor) Kan kaldes med en af følgende metoder til autentifikation • Brugerid/password (kun zone 0 tjenester) • SAML Token udstedt at Datafordeler STS • Certificat (eksempelvis FOCES eller tilsvarende) • Ticket udstedt af Datafordeleren (kun zone 0 tjenester) • SAML token udstedt af NemLog-in STS
Kvittering	Service, hvor dataanvendere skal kvittere for modtagelse af meddelelser fra Datafordeleren	• Ip filter for white listed ip-adresse (for detaljer se ovenfor) Kan kaldes med en af følgende metoder til autentifikation • Brugerid/password (kun zone 0 meddelelser) • SAML Token udstedt at Datafordeler STS • Ticket udstedt af Datafordeleren (kun zone 0 meddelelser) • SAML token udstedt af NemLog-in STS
Hændelser Pull	Service som kaldes fra dataanvendere for at hente hændelsesbeskeder som der abonneres på for den specifikke dataanvender	• Ip-filter for White listed ip-adresse (for detaljer se ovenfor) Kan kaldes med en af følgende metoder til autentifikation

		• Brugerid/password (kun zone 0 meddelelser) • SAML Token udstedt at Datafordeler STS • Ticket udstedt af Datafordeleren (kun zone 0 meddelelser) • SAML token udstedt af NemLog-in STS
Hændelser Push	Hændelser Push er en service, som dataanvenderen udstiller, og som kaldes fra Datafordeleren.	• Ip-filter for White listed ip-adresse (for detaljer se ovenfor) • Skal kaldes med FOCES certificat for kalderen, dvs. FOCES certificat for Datafordeleren. KMD fremsender FOCES certificat til Dataanvender, der udstiller en Hændelser Push service

6. Sikkerhed for dataleverandører

6.1 Generel sikkerhed for dataleverandører

Opdatering af data i Datafordeleren sker gennem zone 5, hvorfor følgende altid vil være gældende for opdateringer uanset om dette sker gennem en FTP eller SOA-port:

- Ipfiltrering (white listing). Adgang til Datafordeler som dataleverandør kan kun ske fra ip-adresser, som er white listede, dvs. ip-adresser hvor der positivt er åbnet for adgang til Datafordeler. Kommunikation fra ip-adresser, der ikke er white listet vil blive afvist.

6.2 Integrationspunkter for dataleverandører

Integrationspunkt	Beskrivelse og anvendelse	Sikkerhed
SOA Port	Anvendes som replikeringskanal mellem register og Datafordeler for opdatering af data som nær-realtidsopdateringer	• Ip-filter for White listed ip-adresse (for detaljer se ovenfor) • SOA port service kan i skrivende stund kun tilgås med et SAML token genereret af Datafordeler STS • Det forventes at SOA port i den nærmeste fremtid også vil understøtte certifikater
SFTP Port	Anvendes som replikeringskanal mellem Register og Datafordeler for opdatering af data ved anvendelse af fil-overførsel	• Ipfilter for White listed ip-adresse (for detaljer se ovenfor) • SSH offentlig nøgle. Der anvendes SSH autentifikation for at tilgå SFTP porten. Dataleverandør skal derfor sende den SSH-offentlige nøgle til Datafordeleren, således at signatur ved kald til SFTP-porten kan valideres • Det er dataleverandøren, der har ansvar for, at der generes et sæt SSH nøgle, og at den offentlige nøgle fremsendes til Datafordeleren.
Kvitteringstjeneste	Service, hvor register kan forespørge om status for dataleverancer. Servicenavn: DeliveryReciept	• Ip-filter for White listed ip-adresse (for detaljer se ovenfor) • Kan tilgås med et SAML token generet af Datafordeler STS • Det forventes at service i den nærmeste fremtid også vil understøtte certifikater som autentifikation
SynchronisationService	Service, hvor Datafordeler kan bestille en ekstraordinær synkronisering. Service udstilles af dataleverandøren. Servicenavn: SynchronisationService	• FOCES certificat sendes af KMD til dataleverandør • TLS 1.1 krypteret forbindelse
GetData	Service udstillet af register.	• FOCES certificat sendes af KMD til dataleverandør

	Anvendes ved den proaktive synkronisering som er indbygget i Datafordeleren. GetData er en service, hvor Datafordeler kan forespørge på udvalgte data og benyttes ved tabular data. Service udstilles af dataleverandøren. Servicenavn: GetData	• TLS 1.1 krypteret forbindelse
GetRaster	Service udstillet af register. Service, hvor Datafordeler kan forespørge på udvalgte data. Anvendes ved den proaktive synkronisering som er indbygget i Datafordeleren. Service anvendes ved filbaseret rasterdata. Service udstilles af dataleverandøren. Servicenavn: GetRaster	• FOCES certificat sendes af KMD til dataleverandør • TLS 1.1 krypteret forbindelse

6.3 Akkreditiver til tjenester (forskellige kategorier)

	Zone 0	Zone 5
Anonym bruger	Akkreditiver ignoreres	N/A
Kendt bruger	Username/password. Ticket (fra un/pw). FOCES/VOCES. System AD FS SAML-token. NemLog-in STS SAML-token (Primo August).	N/A
Begrænset adgang	Username/password. Ticket (fra un/pw). FOCES/VOCES. System AD FS SAML-token. NemLog-in STS SAML-token (Primo August).	FOCES/VOCES + IP-filter. NemLog-in STS SAML-token + IP-filter (Primo August). System AD FS SAML-token + IP-filter.
Replikeringstjenester	N/A	System AD FS SAML-token + IP-filter. FOCES/VOCES + IP-filter (Primo August). Kræver tjenestebruger med særlig autorisation.)

SAML-token fra System ADFS fås ved kald med VOCES/FOCES.

7. Diagram over sikkerhed for dataanvendere og dataleverandører