NSI Sikkerhedspolitik for Sign-on Service (STS)

Version 1.1
28. juni, 2011

Indhold

1 Introduktion

Sikkerhedspolitikken vedr. Sign-on Service indgår som en delpolitik i National Sundheds-ITs (NSI) informationssikkerhedspolitik og refererer til den overordnede sikkerhedspolitik for NSI.
Dette dokument fastlægger kravene til sikkerhed omkring driften af Secure Token Service (STS) komponenten.
Dokumentet følger i sin struktur internet standarden RFC 3647 som giver en skabelon for certifikat politikker. Da STS ikke fungerer som
Certification Authority (CA), men i stedet anvender OCES virksomheds-, funktions- og medarbejdercertifikater fra slutbrugerne til at udstede Single Sign On (SSO) tickets, er dele af denne skabelon dog ikke relevant, og de tilhørende punkter er udeladt af dokumentet.

Med anvendelse af den generelle indholdsfortegnelse fra RFC 3647, og med anvendelse af især Liberty Alliance projektets operationelle kriterier sikkerhedsniveau 3 og 4, har dokumentet potentiale til at kunne udbygges til en sikkerhedspolitik for hele National Sundheds It, med adressering af sikkerhedskrav og ansvar for brugere og tjenesteudbydere også. I denne første version er dokumentet dog målrette krav til driften af selve STS komponenten.

1.1 SOSI infrastrukturen

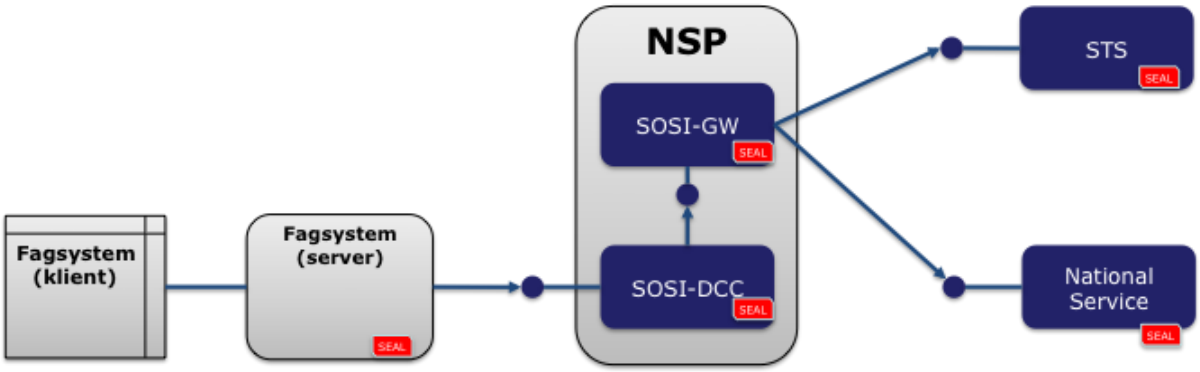
Secure Tokens Service (STS) komponenten er en central komponent i sundhedssektorens Service Orienteret System Integration (SOSI) infrastruktur.

STS'en autentificerer typisk slutbrugere, såsom læger og andet sundhedsfagligt personale, ved hjælp af OCES medarbejdersignatur. På baggrund af medarbejdersignatur og opslag i forskellige fagregistre, udstedes en SOSI (sessions) ticket, som kan anvendes af slutbrugerne til autentifikation overfor sundhedstjenester såsom Fælles MedicinKort (FMK) i en tidsafgrænset periode på f.eks. 8 timer.

ID Kort for (Subject name ID): 2606444917	
Kort udsteder: TDCHealth *Kort ID:AAATX* *Kort type (System el.medarbejder):user* *Kort version:1.0* *Kort autentifikationsniveau (1-4): 4*	*Udstedt: 01-06-2006 Kl. 07:53:00* *Gyldigt fra: 01-06-2006 Kl. 08:00:00* *Gyldigt til: 01-07-2006 Kl. 07:53:00*
IT-system oplysninger: *IT systemets ID:LægeSystemA*	*Organisationens ID:*079741 (ID format: medcom:ynumber) *Organisationens navn:* Lægehuset, Vandværksvej.
Evt. bruger oplysninger: CPR nummer: 2606444917 Stilling: Maskinarbejder Fornavn: Ole H. Efternavn: Berggren eMail: ohb@nomail.dk	Evt. autorisationsnummer: 24778 Bruger rolle: PRAKTISERENDE_LAEGE

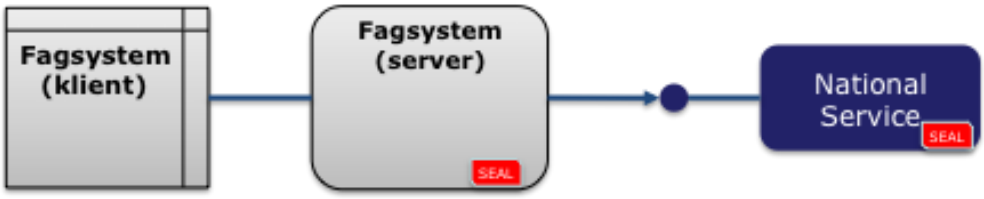
Figur 1 – Indhold af en SOSI ticket

SOSI komponenterne er placeret "imellem" fagsystemerne og STS'en hhv. de nationale services. Som det ses på Figur 2 nedenfor udstilles de fødererede nationale services igennem National Service Platform (NSP), idet SOSI dekoblingskomponenten DCC viderestiller kald til f.eks. FMK. Dette kan evt. ske igennem en gateway-komponent (SOSI-GW), såfremt NSP'en er implementeret i eget sikkerhedsdomæne.



Figur 2 – SOSI-komponenterne på NSP og anvendelse af en fødereret service

På Figur 3 ses et eksempel på direkte anvendelse af en ikke-fødereret national service, hvor et fagsystem kalder en national service direkte uden brug af SOSI-komponenterne.



Figur 3 – eksempel på direkte anvendelse af en ikke-fødereret national service

1.2 Sikkerhedsmål

STS'en er teknisk set opdelt i en central STS som drives af NSI driftsleverandøren og 5 regionale STS'er, som fysisk er placeret i driftscentre hos regionerne, men med overordnet driftsansvar liggende hos NSI driftsleverandøren.

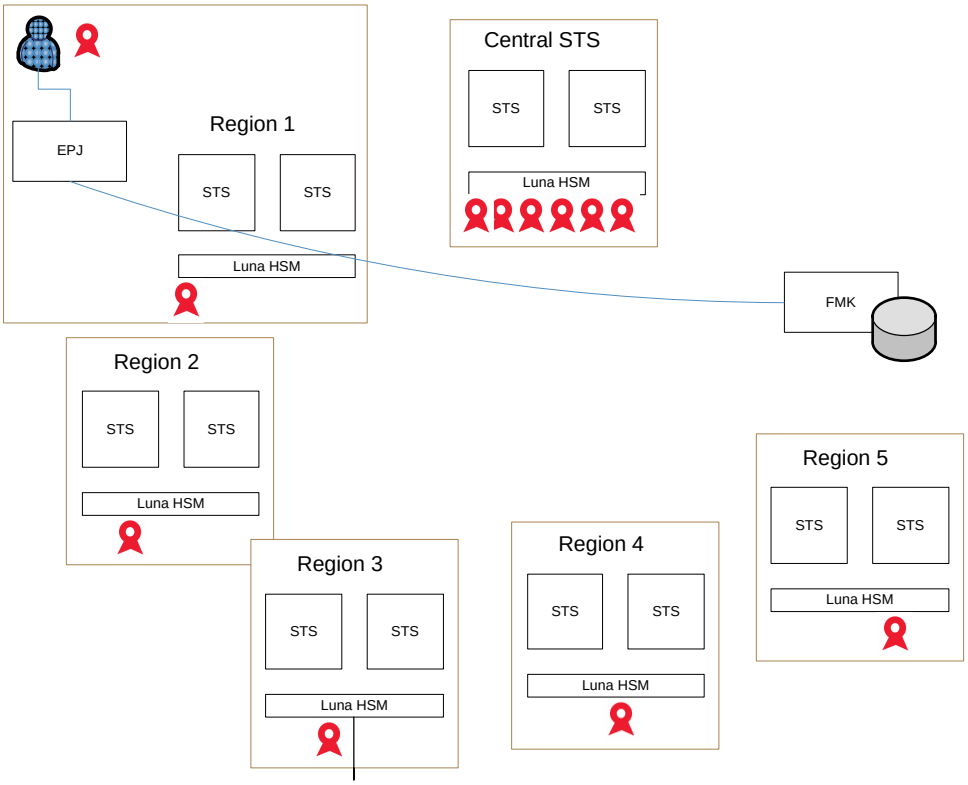


Fig. 4: Den centrale og de regionale STS'er

Sikkerhed af autentifikationsløsninger indplaceres ofte i forhold til det amerikanske "National Institute of Standards and Technologies", NIST standarden 800-63 "Electronic Authentication Guideline" [NIST 800-63].

Af andre anvendte referencer kan nævnes:

- IT- og Telestyrelsens (ITST) "Vejledning vedrørende niveauer af autenticitetssikring". [ITST aut]
- SOSI projektets "Sikkerhedsvejledning for SOSI serviceudbydere". [SOSI vejl]
- Liberty Alliance projektets operationelle kriterier for de fire niveauer i "Liberty identity assurance framework (LIAF)" [LIAF]

Disse standarder definerer og anvender fire forskellige niveauer af tillid til en brugers autentifikationsløsning.

De fire sikkerhedsniveauer er følgende:

- Niveau 1 - Lille eller ingen tiltro til påstået identitet
- Niveau 2 - Nogen tiltro til påstået identitet
- Niveau 3 - Høj tillid til påstået identitet
- Niveau 4 - Meget høj tillid til påstået identitet

Fig. 5: De fire niveauer som beskrevet af ITST

En autentifikationsløsnings niveau af sikkerhed kan vurderes indenfor fire områder (NIST):

1. Tokens (typisk en kryptografisk nøgle eller et password) for bevis af identitet
2. Procedurer for identifikation af bruger, udlevering og vedligeholdelse af tokens. (Politikker og praksisbeskrivelser)
3. Implementation af autentifikationsmekanismen, herunder protokol for bevis for besiddelse af token og andre identitetsoplysninger.
4. Fødereringsmekanisme, hvis der er behov for at viderekommunikere resultatet af en autentifikation til andre parter

Det er en grundlæggende målsætning, at SOSI infrastrukturen skal kunne understøtte sikkerhed af autentifikationen af slutbrugerne på NIST niveau 1 til 4.

Den samlede sikkerhed af SOSI ved autentifikation af brugerne afhænger af mange ting, herunder sikkerheden af signaturløsningen og binding af sessioner til slutbrugere. For at de samlede autentifikationsløsninger kan understøtte NIST niveau 3 og 4, er målsætningen at selve STS komponenterne som fødereringsmekanisme understøtter NIST niveau 4.

1.3 Dokument navn og identifikation

Dokumentets navn er "Sikkerhedspolitik for SOSI STS", med angivelse af versionsnummer som beskrevet på forside.

1.4 Deltagere og interessenter

1.4.1 Certificeringscentre

SOSI til NIST niveau 3 og 4 anvender som slutbrugerautentifikation OCES funktionscertifikater, virksomhedscertifikater og OCES medarbejdercertifikater udstedt af en dansk OCES CA.

1.4.2 Slutbrugere og lokale applikationer

Slutbrugere i SOSI føderationen er sundhedsfagligt personale, som skal autentificeres med henblik på at få adgang til IT ressourcer.

Slutbrugere tilgår SOSI infrastrukturen og nationale sundhedsservices såsom fælles medicinkort via forskellige lokale IT applikationer såsom EPJ systemer.

1.4.3 Fødereringstjenester (STS)

SOSI understøtter en distribueret fødereringstjeneste, som beskrevet I afsnit 1.1. Slutbrugerne kan tilsluttes forskellige af disse fødereringstjenester, alt efter hvor brugeren arbejder og hvilken lokal applikation brugeren anvender (såsom EPJ).

1.4.4 Tjenesteudbydere

Konsumenterne af SOSI tickets er de tjenesteudbydere, som har behov for at autentificere slutbrugere med henblik på at give adgang til sundhedsdata.

1.4.5 Andre deltagere

SOSI infrastrukturen understøttes af driftsorganisationer bag tjenester og.fødereringstjenester. Rollefordelingen bag driften af fødereringstjenesten er illustreret i Fig. 4: Den centrale og de regionale STS'er.

Dette dokument adresserer specielt "den centrale driftsleverandør", som dels hoster den centrale STS, dels har ansvaret for drift, overvågning af de decentrale STS'er, som er placeret i regionale driftsenheder.

De "regionale driftsenheder" er STS installationer placeret i den enkelte regions driftsmiljø, serviceret dels af lokalt driftspersonale, dels af driftspersonale fra den centrale driftsleverandør. For at minimere behovet for viden og uddannelse, er det en målsætning, at det regionale driftspersonale så vidt muligt ikke udfører sikkerhedskritiske opgaver.

1.5 Deltagernes ansvar

1.5.1 Certificeringscentres ansvar

Det er OCES certificeringscentrenes ansvar at autentificere slutbrugerne og udstede certifikater i henhold til den til enhver tid gældende OCES certifikat politik.

1.5.2 Slutbrugere og dataansvarlige for lokale applikationers ansvar

Den IT applikation, som i praksis videresender en SOSI ticket til en tjenesteudbyder på vegne af en slutbruger, benævnes her blot "den lokale applikation".

Det er slutbrugers ansvar at efterleve sikkerhedsbestemmelserne omkring anvendelse af OCES signatur jf. brugervilkår fra OCES certificeringscenteret.

Det er den dataansvarlig for de lokale applikation, der har ansvaret for at sikre, at den IT bruger, som modtager data eller IT ydelser fra en tjeneste på baggrund af en fremsendt SOSI ticket, er den retmæssige ejer af den pågældende SOSI ticket.

Efter at slutbrugeren har autentificeret sig med OCES certifikat, skal den lokale applikation kunne sikre slutbrugeren enekontrollen over den udstedte SOSI ticket.

1.5.3 Fødereringstjeneste (STS) ansvar

NSI er ansvarlig for fødereringstjenestens implementering og drift.

Fødereringstjenestens vigtigste opgave er at autentificerer slutbrugeren korrekt og sikkert ved hjælp af OCES signatur.

Det er desuden fødereringstjenestens opgave at sikre, at de udstedte tickets indhold er korrekt og valideret jf. autentifikation af slutbrugere og opslag i tilhørende databaser.

Endelig skal fødereringstjenesten drive sine services i henhold til denne sikkerhedspolitik.

1.5.4 Tjenesteudbyderes ansvar

Det er modtageren af en SOSI tickets (tjenesteudbyderens) ansvar at:

- Kontrollere, at en modtaget ticket ved kontroltidspunktet stadig er indenfor den angivne gyldighedsperiode
- Kontrollere at signaturen på en ticket er gyldig og herunder kontrollere, at alle certifikater i certifikat kæden op til OCES rodcertifikatet, eller andet godkendt tillidsanker, er gyldige og ikke revokerede.
- Afgøre hvorvidt den modtagne SOSI tickets attributter modsvarer den autorisation, som der behøves til den efterspurgte IT ydelse.
- Afgøre hvorvidt sikkerheden af brugerautentifikationen samlet set er passende i forhold til modtagerens behov

1.6 Administration af sikkerhedspolitik

Sikkerhedspolitikken administreres af

National Sundheds-IT (NSI)
CVR: 33257872
Islands Brygge 39
2300 København S

Kontakt: Sikkerhedsfunktionen

1.6.1 Godkendelsesprocedurer

Sikkerhedspolitikken og ændringer heraf skal godkendes af NSIs informationssikkerhedsudvalg (kan evt. delegeres til informationssikkerhedslederen).

2 Fysiske kontroller, ledelseskontroller og driftskontroller

Dette kapitel beskriver kravene til de organisationer og driftsinstallationer som skal drive STS komponenterne som udsteder SOSI tickets.

Der er forskellige krav til driftsmiljø og organisation hos den centrale driftsleverandør og driftsmiljøer og organisation hos de regionale driftsenheder.

Kravene adresserer specielt den fysiske indretning af driftslokaliteter, organisering af ledelsen for driftspersonale samt procedurer for personalets arbejde.

2.1 Fysiske kontroller

Fysiske kontroller er beskrevet i appendix A.

2.2 Proceduremæssige kontroller

Den centrale driftsleverandør skal have en sikkerhedspolitik, som er godkendt af ledelsen.

Den centrale og de regionale STS'er skal drives i overensstemmelse med en detaljeret driftshåndbog, som fastlægger, hvorledes alle kritiske driftsopgaver udføres, herunder hvilke roller der udfører dem, og hvorledes opgaveløsningen auditeres.

NSI skal vedligeholde en risikoanalyse for sin drift af infrastrukturen. Risikoanalysen skal opdateres årligt og godkendes af ledelsen. Risikoanalysen skal blandt andet behandle risikoen for:

- Sårbarhed overfor skadelig software
- Risici fra medarbejdere involveret i driften
- Risiko for svindel fra brugere og tjenester
- Sårbarhed overfor målrettet IT angreb og denial of service

2.2.1 Betroede roller

Medarbejdere som skal udføre sikkerhedskritiske opgaver hos den centrale driftsleverandør, skal have en skriftlig jobbeskrivelse, som beskriver deres rolle og ansvar I forhold til drift af STS.

2.2.2 Opgaver som forudsætter deltagelse af flere personer

Den centrale driftsleverandørskal have en driftshåndbog, som blandt andet fastlægger, hvilke opgaver der forudsætter deltagelse af flere medarbejdere.

2.2.3 Identifikation og autentifikation af medarbejdere.

IT adgangskontrolsystemer der anvendes af den centrale driftsleverandør, skal understøtte sikker identifikation af medarbejdere og disses roller, således at medarbejdere ikke kan tiltage sig rettigheder udover det autoriserede.

Den centrale driftsleverandør skal have dokumenterede procedurer for tildeling, vedligehold og fjernelse af adgangsrettigheder for medarbejdere.

Personale hos regionale driftsenheder skal udstyres med færrest mulige rettigheder, og skal understøttes med procedurer, organisation og uddannelse til at udføre de tilhørende opgaver korrekt og sikkert.

2.2.4 Funktions adskillelse

Den centrale driftsleverandør skal implementere funktionsadskillelse i drift, således at medarbejdere med de forskellige roller har færrest mulige privilegier og adgangsrettigheder under hensyntagen til de opgaver de skal løse.

2.2.5 Off-site backup

Databackup skal omfatte anvendelse af en ekstern backup lokation og planlægges i henhold til en konkret vurdering af risiko og konsekvens af et eventuelt datatab i henhold til klassifikation af de enkelte datatyper.

2.2.6 Change management

Ændringer i driftsmiljøet skal være underlagt change management procedurer, som sikrer, at funktionalitet der sættes i drift har gennemgået en tilstrækkelig kvalitetssikring samt at der er mulighed for at rulle tilbage til tidligere konfiguration. Change management procedurerne skal sikre, at ledelsen forestår prioriteringen og godkendelsen af planlagte ændringer.

2.3 Personale kontroller

2.3.1 Forudsætninger til kvalifikationer, erfaringer og sikkerhedsclearinger

Den centrale driftsleverandør skal kontrollere, at ledere og medarbejdere, der udfører betroede opgaver i eller for den centrale driftsleverandør, ikke er straffet for en forbrydelse, der gør dem uegnede til at bestride deres hverv.

Medarbejderstabene hos den centrale driftsleverandør og de regionale driftsenheder skal til enhver tid råde over tilstrækkelige faglige kompetencer til at udføre de tiltænkte opgaver og udfylde de tilhørende roller.

Dette skal sikres i rekruttering og gennem efteruddannelse.

2.3.2 Krav til underleverandører

Den centrale driftsleverandør skal sikre, at personalet hos underleverandører, som skal arbejde på den centrale STS, opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som den centrale driftsleverandørs egne medarbejdere i de funktioner, underleverandørens personale varetager for den centrale driftsleverandør.

Den centrale driftsleverandørskal med adgangsprocedurerne sikre, at personale fra underleverandører ikke kan arbejde u-overvåget hos den centrale driftsleverandør.

NSI skal ved aftale med de regionale driftsenheder sikre, at personalet hos underleverandører, som skal arbejde på den regionale STS installation, opfylder samme krav til uddannelse, erfaring og sikkerhedsklassifikation som den regionale driftsenheds egne medarbejdere i de funktioner, underleverandørens personale varetager for den regionale driftsenhed.

NSI skal ved aftale med de regionale driftsenheder sikre, at personale fra underleverandører ikke kan arbejde u-overvåget hos den regionale driftsenhed.

2.3.3 Krav til organisering

Den centrale driftsleverandør skal sikre, at dens administrative og ledelsesmæssige procedurer er tilstrækkelige og lever op til kravene til et "ledelsessystem for informationssikkerhed" som fastlagt i ISO-27001.

2.4 Audit log procedurer

2.4.1 Hændelser der logges

Den centrale driftsleverandør er ansvarlig for etablering af et datalagringssystem, der skal indeholde alle data, der er nødvendige for sikker drift af STS i overensstemmelse med denne sikkerhedspolitik.

Den centrale driftsleverandør skal desuden sikre, at

- alle sikkerhedskritiske aktiviteter samt aktiviteter, der kræver deltagelse af mere end én person, logges,
- Alle adgange og adgangsforsøg til områder, der skal beskyttes af adgangskontrol, logges,
- Der etableres billeddokumentation som dokumenterer fysisk adgang til den centrale driftslokation til brug for auditering.

2.4.2 Audit log backup procedure

Den centrale driftsleverandør skal sikre, at relevante loginformationer fra regionale driftsenheder konsolideres hos den centrale driftsleverandør og indgår i dennes audit log sikring, backup og arkivering.

Den centrale driftsleverandør skal sikre, at arkiveret information kan gøres tilgængelig i tilfælde af rejste forespørgsler, og at alt arkiveret materiale opbevares i mindst 6 måneder.

Logs indeholdende personfølsomme data behandles og slettes i henhold til persondataloven.

Logninger der indgår i sikkerhedsaudit opbevares indtil ekstern revision omfattende dette materiale er afsluttet og godkendt.

Den centrale driftsleverandør skal sikre, at

- al information beskyttes mod uretmæssig adgang,
- der er skriftlige regler for regelmæssig gennemgang af alle logs,
- alle audit-logs signeres elektronisk og tidsstemples,
- audit-logs behandles som fortroligt materiale,
- der foretages backup af audit-logs med regelmæssige mellemrum.
- at logs er beskyttet imod ændring og sletning, samt at der foreligger en sårbarhedsvurdering af audit log procedurer

2.5 Udskiftning af nøgler

Generering, udskiftning og backup af private nøgler, som anvendes til udstedelse af SOSI tickets, skal udføres af den centrale driftsoperatør med deltagelse af to personer med betroede roller i samarbejde.

2.6 Kompromittering og katastrofeberedskab

2.6.1 Procedurer for håndtering af sikkerhedshændelser

Den centrale driftsleverandørs driftshåndbog for STS skal beskrive håndteringen og rapporteringen af sikkerhedshændelser.

Rapporteringen skal sikre, at Den centrale driftsleverandørs ledelse regelmæssigt godkender håndteringen af sikkerhedshændelser.

2.6.2 Procedurer ved kompromittering af privat nøgle eller brugsret til privat nøgle

Ved mistanke om kompromittering af private nøgler til udstedelse af SOSI tickets, skal den centrale driftsleverandørs ledelse straks kontakte de ansvarlige for sikkerhedspolitikken jf. 1.6 for afklaring af hvorledes situationen skal håndteres og kommunikeres til interessenterne.

2.6.3 Business continuity

Den centrale driftsleverandør skal have en plan for videreførelse af STS driften i tilfælde af nedbrud eller udefra kommende katastrofer. Planen skal indgå i NSIs samlede risikoanalyse for driften af den centrale og de regionale STS'er. Planen skal operationaliseres og indøves i et omfang, som efterviser, at den centrale driftsleverandør og de regionale driftsenheder kan agere som planlagt i en katastrofesituation.

2.7 Nedlukning af STS

NSI skal have dokumenterede procedurer for nedlukning af hele STS infrastrukturen såvel som dele af denne.

Tjenesteudbydere og ejere af lokale applikationer som anvender de pågældende STS komponenter skal varsles om nedlukning og anvises anbefalede ændringer.

Efter nedlukning af STS infrastrukturen, eller dele af den, skal de tilhørende logfiler og forretningsdata være tilgængelige i løbende måned plus 6 måneder..

3 TEKNISKE SIKKERHEDSKONTROLLER

3.1 Generering og certificering af private nøgler til brug for SOSI tickets

3.1.1 Generering af nøglepar

Private nøgler til brug for udstedelses af SOSI tickets skal genereres og opbevares i kryptografiske moduler, der opfylder kravene opstillet i standarderne FIPS 140-2 level 3, CWA 14167-3, eller højere.

3.2 Beskyttelse af private nøgler og kryptografiske moduler

Aktivering af private nøgler på kryptografiske moduler skal indrettes således, at aktivering forudsætter deltagelse af to medarbejdere fra den centrale driftsleverandør med betroede roller.

3.2.1 Backup af private nøgler

Sikkerhedskopier af det kryptografiske modul må ikke kunne håndteres eller aktiveres af enkeltpersoner hos den centrale driftsleverandør, og skal opbevares på samme sikkerheds- og adgangskontrolniveau som kryptografiske moduler i drift.

Personale hos regionale driftsenheder må ikke have rettigheder til at kunne deltage i vedligehold, håndtering eller aktivering af kryptografiske moduler.

De kryptografiske moduler skal opbevares i henhold til kravene i afsnit 3.2.

Den centrale driftsleverandør skal sikre, at STS's private nøgler på den centrale såvel som de regionale STS'er ikke kompromitteres, og til stadighed bevarer deres integritet.

Lagring, sikkerhedskopiering og transport af STS's rodnøgler og andre private nøgler skal ske under overvågning af to personer med betroede roller fra den centrale driftsleverandør.

3.2.2 Arkivering/destruering af private nøgler

Private nøgler som anvendes i STS'er skal have en fastsat gyldighedsperiode. Efter udløb skal den private nøgle enten destrueres eller opbevares på en sådan måde, at den ikke kan genskabes og tages i brug igen.

Den centrale driftsleverandør skal sikre, at der, inden udløb af den private nøgle hos den centrale eller i regionale STS'er, genereres et nyt STS-nøglepar, der kan benyttes til udstedelse af SOSI tickets.

3.2.3 Opbevaring af private nøgler I Kryptografiske moduler

Den centrale driftsleverandør skal håndtere og opbevare kryptografiske moduler i henhold til kravene i afsnit 3.2 i hele de kryptografiske modulers levetid.

Den centrale driftsleverandør skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke er blevet kompromitteret inden installation.

Kryptografiske moduler må kun opbevares i særligt sikrede driftslokaler, hvortil der er oprettet sikker adgangskontrol, og fysisk beskyttelse jf. Appendix A.

Den centrale driftsleverandør skal sikre sig, at kryptografiske moduler til certifikat- og statusinformationssignering ikke bliver kompromitteret under brug.

Den centrale driftsleverandør skal sikre sig, at al håndtering af kryptografiske moduler til certifikat- og statusinformationssignering, hvad enten det er installeret hos den centrale driftsleverandør eller hos regionale driftsenheder, sker under medvirken af mindst to personer med hver sin betroede rolle hos den centrale driftsleverandør.

Den centrale driftsleverandør skal sikre sig, at nøgler, opbevaret i et kryptografisk modul til certifikat- og statusinformationssignering, destrueres i forbindelse med, at modulet kasseres.

3.3 Beskyttelse af delte hemmeligheder
Administratorer må ikke dele kodeord. Alle kodeord skal være valgt af den pågældende operatør og må kun være kendt af denne.

Den centrale driftsleverandør skal sikre sig, at driftspersonale på regionale driftsenheder til enhver tid kun har de nødvendige adgangsrettigheder og kodeord hørende til deres roller. Personale hos regionale driftsenheder må ikke kende kodeord, som anvendes af operatører hos den centrale driftsleverandør.

3.4 Netværks sikkerhedskontroller
Netværk sikkerhedskontroller er beskrevet I appendix B.

4 Compliance audit og andre sikkerhedsvurderinger
Compliance audit og andre sikkerhedsvurderinger er beskrevet i appendix B.

5 Andre juridiske og forretningsmæssige forhold
Den centrale driftsleverandør skal have en organisering og soliditet som modsvarer det ansvar den centrale driftsleverandør påtager sig.

5.1 Økonomisk ansvar
NSI er overordnet erstatnings ansvarlig efter dansk rets almindelige regler.

5.2 Fortrolighed af persondata
NSI skal sikre overensstemmelse med lovgivningen, herunder særligt lov om behandling af personoplysninger.

5.2.1 Forretningsvilkår
Tjenesteudbydere skal indgå tilslutningsaftale med NSI.

5.2.2 Ophør

5.3 Jurisdiktion
Kan en tvist ikke løses forligsmæssigt, kan enhver af parterne vælge at indbringe tvisten for de almindelige domstole. Værneting er København. Dansk ret er gældende.

5.4 Overholdelse af gældende lovgivning
NSI skal sikre overensstemmelse med gældende lovgivning.

Referencer

[ITST aut]: ” Vejledning vedrørende niveauer af autenticitetssikring, OIO Referencemodel for tværgående brugerstyring”, IT- og Telestyrelsen

[LIAF]: ”Liberty identity assurance framework (LIAF)”, v. 1.0

[NIST 800-63]: “National Institute of standards and technology, Electronic authentication guideline”, v. 1.0.2 April 2006

[SOSI vejl]: “Sikkerhedsvejledning for SOSI serviceudbydere”, 30/5 2007

6 Appendix A: Fysiske kontroller

6.1 Placering og konstruktion af driftslokaler

NSI skal tydeligt beskrive, på hvilke lokaliteter medarbejdere og datacentre i forbindelse med STS's virke er placeret.

De lokaler, hvor udstyr til nøglegenerering og SOSI ticket udstedelse er placeret, benævnes STS driftslokaler.

Opbevares eller behandles data på anden lokal lokalitet end STS driftslokalerne, skal NSI sikre, at dette sker under opfyldelse af samme krav til sikkerhed som krav til STS driftslokaler.

6.2 Fysisk adgang

NSI skal sikre, at alle lokaler har en perimeterbeskyttelse, som er passende i forhold til den samlede risikoanalyse for fødereringstjenesten.

NSI skal sikre, at der etableres vagt 24 timer i døgnet.

NSI skal sikre, at adgang til og ophold i de centrale driftslokaler dokumenteres med billedlogning.

NSI skal sikre, at fysisk adgang til driftslokaler er kontrolleret med adgangskontrol, som begrænser adgangen til autoriserede personer. Adgangsrettigheder til sikre områder skal gennemgås og ajourføres regelmæssigt.

6.3 Strøm og køling

Udstyr skal sikres mod forsyningssvigt i overensstemmelse med udstyrets betydning for kritiske forretningssystemer.

Driften af STS skal være robust overfor udfald af primær elektricitetsforsyning. Nødstrømsanlæg skal sikre en hensigtsmæssig nedlukning i tilfælde af strømudfald. Nødstrømsanlæg skal testes regelmæssigt.

Driftslokaler skal have et kølesystem med overvågning og alarmering, som tillader rettidig afhjælpning af eventuelle fejl.

6.4 Forebyggelse af oversvømmelse

Driftslokaler skal være beskyttet imod oversvømmelse.

6.5 Forebyggelse af brand

Driftslokaler skal være udstyret med flere uafhængige brand detekteringssensorer. Der skal være etableret automatisk branddæmpning f.eks. med Inergen anlæg.

6.6 Opbevaring af medier

Datamedier skal beskyttes imod uautoriseret eller utilsigtet brug, adgang, offentliggørelse eller beskadigelse og mod andre trusler såsom brand og vand.

6.7 Affaldshåndtering

Der skal anvendes procedurer for bortskaffelse af affald som forhindrer uautoriseret brug, adgang eller offentliggørelse af følsomme data.

7 Appendix B: Netværks sikkerhedskontroller og Complicance audit og andre sikkerhedsvurderinger

7.1 Netværks sikkerhedskontroller

7.1.1 Overvågning

Den centrale driftsleverandør skal implementere overvågning af IT systemer og alarmering af driftsvagt med henblik på forebyggelse af driftsnedbrud og sikkerhedshændelser..

7.1.2 Netværksbeskyttelse

Den centrale driftsleverandør skal anvende systemer til perimeterbeskyttelse i henhold til markedets bedste praksis. Perimeterbeskyttelse skal indgå i NSIs samlede risikoanalyse.
Alle installationer skal indgå som en del af sundhedsdatanettet og som sådan opfylde kravene hertil[1].

NSI har ansvar for, at de regionale driftsenheders perimeterbeskyttelse modsvarer de sikkerhedsbehov, der er hos de regionale driftsenheder.

7.2 Kontroller for systemadgang

Den centrale driftsleverandør skal implementere sikre rutiner for tildeling og fjernelse af systemadgang for betroede medarbejdere.

8 Compliance audit og andre sikkerhedsvurderinger

8.1 Hyppighed af audit

Den centrale driftsleverandør skal i forbindelse med den årlige IT sikkerhedsrevision indsende en revisionserklæring til NSI om den gennemført drift målt imod kravene til driften, som de er detaljeret i SOSI sikkerhedspolitikken (dette dokument) samt driftskontrakter.

Den centrale driftsleverandør skal have en intern auditør, som regelmæssigt kontrollerer driftens udførelse herunder håndteringen af sikkerheds incidents.

8.2 Kvalifikationskrav til auditor

Interne auditører skal have faglige kvalifikationer til at kunne vurdere drift og sikkerhedsrelaterede hændelser i henhold til ISO-27001.

Eksterne auditører skal have faglige kvalifikationer indenfor revision af IT systemer.

8.3 Auditørs tilhørsforhold til det auditerede

Den centrale driftsleverandør skal sikre, at personer med auditørfunktioner hos den centrale driftsleverandør ikke udsættes for interessekonflikter overfor sin ledelse under udøvelse af sin auditørfunktion og rapportering af resultaterne heraf.

8.4 Indhold af audit gennemgang

<Her indsættes indholdet af konkrete revisionserklæring som parterne årligt indsender (udestår)>

8.5 Offentliggørelse af audit resultater

Auditør funktionen hos den centrale driftsleverandør og de regionale driftsenheder skal på efterspørgsel stille rapporter , materiale og analyser til rådighed for NSI, eksterne auditører og andre interessenter godkendt af NSI.

[1] Se introduktion til sikkerhed på sundhedsdatanettet på http://www.medcom.dk/wm111781

Auditørfunktionerne skal opbevare informationer og resultater fra gennemførte audits i henhold til bogføringsloven. Disse informationer skal sikres mod efterfølgende ændringer og sletninger.