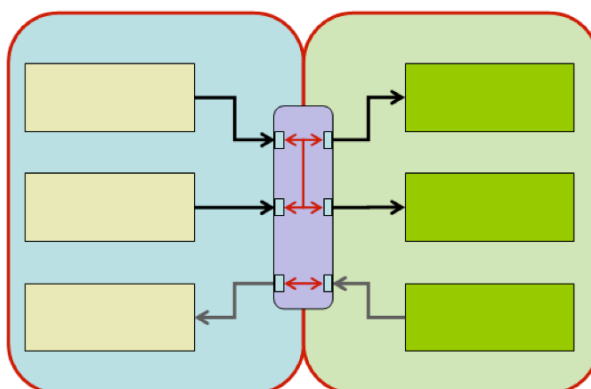


SOSI Gateway Komponenter (SOSI – GW)

- en security domain gateway



Version 1.2

Indledning

Region Syddanmark er udvalgt som pilotregion for projektet ”Det Fælles MedicinGrundlag”, og i den forbindelse arbejdes der intensivt med ideen om en infrastrukturkomponent. Denne komponent skal varetage nogle af de komplekse problemstillinger, der følger af LMS’ valg af autentifikationsniveau, specielt kravet om personlig digital signatur fra regionens EPJ-brugere, når der skal forespørges i og indberettes til ”Det Fælles MedicinGrundlag”.

Dette notat har til formål at skitsere ideerne bag infrastrukturkomponenten samt danne grundlag for en drøftelse af, om komponenten vil være nyttig for andre parter i ”Det Fælles MedicinGrundlag”/FAME og andre nationale integrationsprojekter.

Notatet er et relativt teknisk notat, idet infrastrukturkomponenten er teknisk af natur.

Baggrund

I Region Syddanmark (RSD) er de dele af regionsnettet, hvor kritiske servere er placeret, ekstra godt sikret mod ulovlig indtrængen og misbrug. Foruden fysisk sikring, er der høj netværksmæssig perimetersikkerhed, overvågning, gennemarbejdede beredskabsplaner etc. Regionen er samtidig i fuld gang med at ensrette brugeridentiteter, så både systemer og brugere inden for dette netværk er kendte, og regionen er ved at se på en fælles brugeradministrationsløsning (Identity Management løsning). Dette netværk udgør således et selvstændigt sikkerhedsdomæne, hvor man, pga. af alle disse tiltag og løsninger, ikke har samme behov for at etablere sikkerhedsløsninger som der er i forhold til de nationale tjenester.

Det ændrer dog ikke på, at behovet for at benytte nationale tjenester vil være stigende, og i et meget heterogent systemmiljø, som det i RSD, kan det blive en risikofyldt og bekostelig affære, at få alle systemer til at understøtte disse nationale sikkerhedskrav. Derfor kan der være gode argumenter for at etablere en regional ”passage” (en. gateway) som kan varetage flest muligt af disse sikkerhedskrav, f.eks.: .

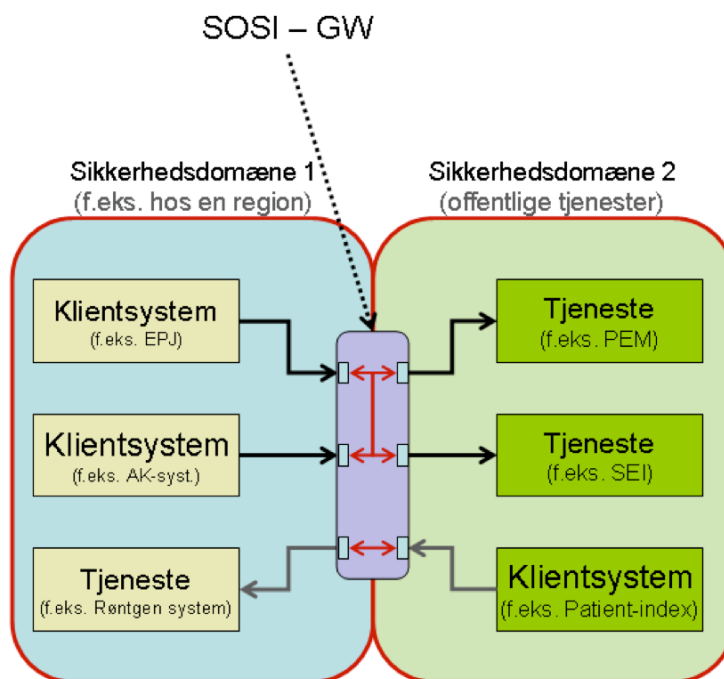
- Håndtering af SOSI ID-kort (rekvirering, lagring, fornyelse), således at håndtering af MOCES-certifikater ikke skal implementeres i alle klient-systemer.
- Håndtering af kommunikation med den nyetablerede identitetsservice (SOSI-STs’en)
- Central håndtering af ændringer i sikkerhedsmekanismer (f.eks. et kommende krav om message authentication), ændringer i standarder mv.
- Central håndtering af service metadata og UDDI integration (f.eks. til en kommende national UDDI infrastruktur).
- Konvertering af sikkerhedsniveauer fra interne forhold til eksterne krav (og omvendt)

Arkitekturoverblik

Gateway komponenten placeres konceptuelt lige på grænsen mellem regionens sikkerhedsdomæne og det sikkerhedsdomæne, som udgør de offentlige tjenester.

SOSI Gateway Komponenten

Forfatter: JRI – Lakeside A/S
Dato: 1 september 2008



Figur 1 – Konceptuel arkitektur

I RSD har man valgt at følge ”Den Gode Web Service” med sikkerhedsniveau 1 (dvs. beskeder indeholder ingen autentifikationsakkrediter) i integrationen mellem systemer inden for det sikre domæne. For at kunne ”konvertere” fra dette autentifikationsniveau til et højere niveau, f.eks. niveau 4 (personlig digital signatur), skal brugeren producere et ”bevis” for sin identitet. I det konkrete eksempel, skal brugeren digitalt underskrive en del af en digital besked, hvilket kræver temmelig meget af det system, der skal initiere underskriften (håndtering af OCES, XML digital signatur, installerede krypteringsalgoritmer mv.). Der er derfor god ræson i at forsøge at håndtere dette i komponenten.

En sidegevinst ved etablering af en sådan komponent, er, at der opnås ”single-sign-on” (SSO) til eksterne tjenester fra alle de systemer i regionen, der er integreret med komponenten. Når brugeren én gang har ”logget sig på” gateway’ en, kan hun shoppe rundt mellem de systemer i regionens systemkompleks, der er integreret med komponenten, uden at skulle logge på igen, når der skal benyttes eksterne tjenester. Hvor de eksisterende SOSI standarder og komponenter muliggør SSO mod flere offentlige tjenester, muliggør gateway komponenten SSO fra flere systemer. Dermed nærmer vi os en form for ”fælles login service” for web service tjenester i sundhedssektoren.

Den skitserede gateway har ligeledes til formål at centralisere kommunikationen med den eksterne nationale identitetsservice (SOSI-STS) og opbevare de udstedte digitale ID-kort på betryggende vis. Desuden centraliseres adgangen til Sundhedsdatanettet mht. web service tjenester. Dette muliggør en central overvågning kommunikationen på tværs af de to sikkerhedsdomæner, hvilket kan give god mulighed for at skride ind overfor driftsmæssige eller sikkerhedsmæssige nedbrud. Endelig udgør SOSI-GW komponenten også en logisk afkobling mellem regionens systemer og de nationale tjenester for så vidt angår sikkerhedsmekanismer. Skulle der i fremtiden komme tilføjelser eller

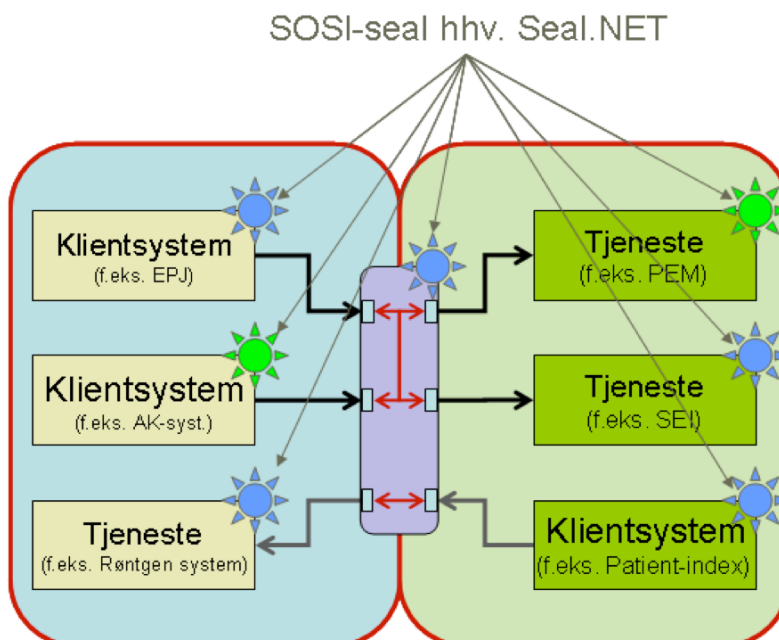
SOSI Gateway Komponenten

Forfatter: JRI – Lakeside A/S
Dato: 1 september 2008



ændringer til de nationale/internationale standarder, er der således etableret ét sted i regionen, hvor indsatsen skal fokuseres.

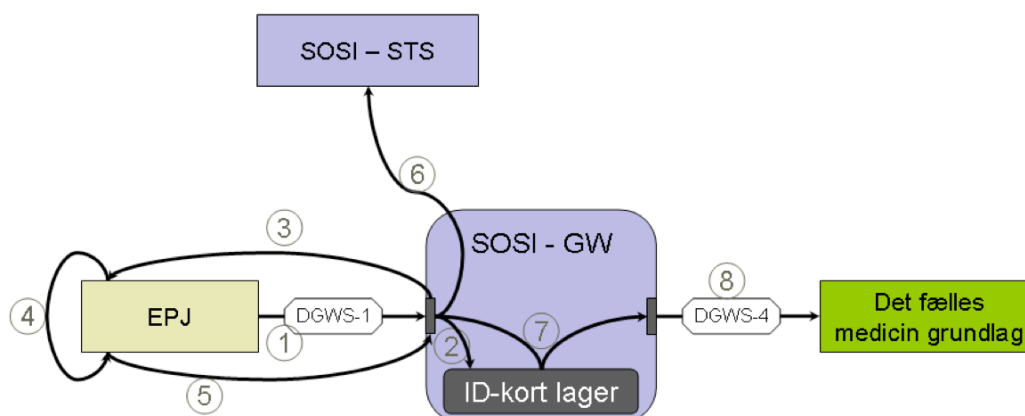
Det er værd at bemærke, at såvel SOSI-GW komponenten, klientsystemerne og tjenesteudbydere med fordel kan anvende de eksisterende biblioteker, der omgiver ”Den Gode Web Service” (SOSI-seal og Seal.NET). Klientsystemerne skal bruge bibliotekerne til at danne niveau 1 beskeder, hvilket performancemæssigt er meget nemt og effektivt, hvorimod SOSI-GW komponenten skal anvende de mere komplekse funktioner i SOSI biblioteket, herunder kontrol af føderationscertifikater, kontrol af digital signatur, håndtering af de nødvendige krypteringsalgoritmer etc. Dette virker som en fornuftig arbejdsdeling i heterogene miljøer.



Figur 2 - Bibliotekerne kan med fordel anvendes

Håndtering af DGWS-sikkerhedsniveau 4

Som ovenfor nævnt synes det ikke realistisk af få alle EPJ-systemer i Region Syddanmark til at understøtte digital-signatur, som en integreret del af EPJ systemet. Regionen ønsker derfor at flytte håndteringen af den digitale signatur ud af de pågældende EPJ-systemer og over til en central (regional) komponent. Dette kan opnås ved at etablere et ID-kort lager, som, i forbindelse med udstedelse af ID-kortet, beder brugeren om at underskrive ID-kortet med medarbejder OCES digital signatur, og derefter ”husker” ID-kortet så længe det er gyldigt. I nedenstående figur illustreres det, hvorledes arbejdsgangen mellem klientsystemet og SOSI-GW komponenten er, når der skal udstedes et nyt digitalt ID-kort:



Figur 3 – Bruger har ikke gyldigt ID-kort (komplekst flow)

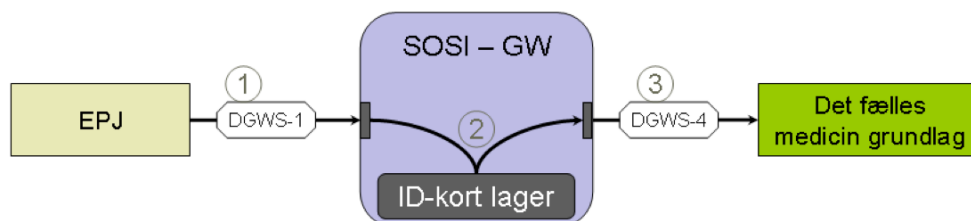
1. EPJ-systemet ønsker (f.eks.) at rekvirere det nyeste medicinkort fra ”Det Fælles Medicin grundlag”. EPJ-systemet danner derfor en web service besked (DGWS niveau 1) og kontakter SOSI-GW komponenten.
2. SOSI-GW kontrollerer ID-kort lageret og finder ikke noget (gyldigt) ID-kort for brugeren.
3. SOSI-GW komponenten adviserer EPJ systemet om, at der skal oprettes et nyt ID-kort, og EPJ-systemet indsender de fornødne informationer.
4. SOSI-GW returnerer de informationer, der skal digitalt signeres til EPJ-systemet, og EPJ-systemet iværksætter en digital underskrift.
5. EPJ systemet indsender de digitalt signerede informationer samt brugerens offentlige certifikat til SOSI-GW.
6. SOSI-GW danner en ”udsted ID-kort” forespørgsel til SOSI-STS’en (standard SOSI teknologi) og fremsender denne til STS’en. STS’en kontrollerer forespørgslen, brugerens digitale signatur og brugerens offentlige certifikat og hvis alt er OK, udstedes et digitalt ID-kort underskrevet af STS’en
7. SOSI-GW gemmer dette ID-kort i ID-kort lageret
8. SOSI-GW beriger det oprindelige kald (skridt 1) med det nye ID-kort, og fremsender det til ”Det fælles medicin grundlag”.

SOSI-GW vil tillade to måder, hvorpå EPJ systemet kan gennemføre skridtene 3,4 og 5:

- A. SOSI-GW klargør et ID-kort i en web-browser grænseflade (HTML) og returnerer en reference (URL) som EPJ systemet kan aktivere og derigennem lade brugeren signere ID-kortet (f.eks. vha. OpenOCES signeringsappletten)
- B. Alternativt klargør SOSI-GW et ID-kort og returnerer de fornødne informationer (bytes) til EPJ-systemet. EPJ-systemet overtager herefter selv kontrollen og iværksætter en signering ved brugerens hjælp.

Mulighed A (browsersignering) er meget teknologineutral, og stiller ikke mange krav til EPJ systemet. Til gengæld kan mulighed B meget bedre integreres i EPJ systemet (som det ses i SOSI pilotafprøvningen i Harmonie systemet).

Når ID-kortet er signeret og lagret hos SOSI-GW komponenten kan det genbruges ved fremtidige kald til offentlige tjenester, indtil ID-kortet udløber (24 timer) eller det afvises som ”for gammelt” hos en tjenesteudbyder. Kommunikationens flow kan illustreres således:



Figur 4 – Bruger har gyldigt ID-kort (simpelt flow)

Interfaces i gatewaykomponenten

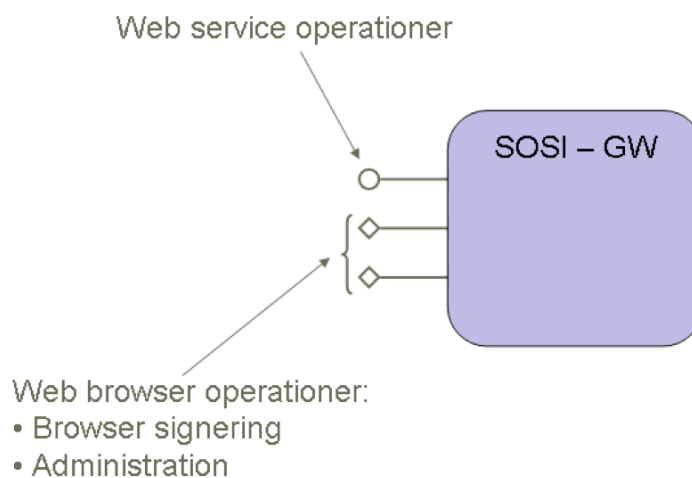
Gatewaykomponenten skal udvikles så gennemstillings-operationen er generisk. Dette kræver, at der i beskeden er referencer til det egentlige endepunkt (f.eks. en operation hos ”Det fælles medicin grundlag”). Disse informationer kommunikeres i nogle strukturer, der overholder den internationale standard WS-Addressing¹. Endvidere udstiller SOSI-GW enkelte andre services, der primært skal bruges i udstedelsessammenhæng:

1. Kald ekstern operation (gennemstillingsoperation)
2. Opret ID-kort til browser-signering (mulighed A ovenfor)
3. Opret ID-kort til klientsignering (mulighed B ovenfor)
4. Installer signerede ID-kort
5. Log-out (fjerner ID-kortet fra SOSI-GW lageret)

Alle disse services vil blive udstillet som web services. Derudover udstiller SOSI-GW komponenten det førnævnte web-baserede (HTML) interface til browser-signering (mulighed A) og et web-baseret administrationsinterface, hvor administratorer kan:

- Angive hvilke systemer, der er tillid til i sikkerhedsdomænet (white-list)
- Straksudelukke en bruger fra SOSI-GW komponenten
- Angive meta-informationer om de eksterne tjenester, herunder krævet sikkerhedsniveau mv.

¹ Adressering vha. WS-Addressing kan evt. tages med i en kommende version af DGWS



Figur 5 – Interfaces på SOSI-GW komponenten

Afslutning

Selvom gateway-komponenten tænkes etableret i arbejdet med at få EPJ-systemer til at håndtere data fra det fælles medicgrundlag, er ingen af de opstillede tekniske krav specifikke for dette projekt. Umiddelbart vil andre regioner også have mange af disse tekniske krav til integrationsopgaver knyttet til services i en fremtidig national infrastruktur. SOSI gateway komponenten er derfor en oplagt kandidat til en fælles regional infrastrukturkomponent på lige fod med SOSI-STS og SOSI-biblioteket.

I SOSI styregruppen er det blevet besluttet, at såfremt andre regioner finder komponenten anvendelig i deres miljøer, vil komponenten blive udviklet efter ”SOSI modellen”, dvs. som Open Source med ejerskab og ophavsret hos en central aktør i sundhedssektoren (i første omgang Danske Regioner), afprøvet i et pilotprojekt, publiceret på softwarebørsen etc.

SOSI Gateway Komponenten

Forfatter: JRI – Lakeside A/S

Dato: 1 september 2008



Dokumenthistorik

Dokumentplacering

Kilden til dette dokument vil blive placeret på www.sosi.dk

Revisionshistorik

Dato for denne revision: 1. september 2008	Dato for næste revision:
--	--------------------------

Revisionsnummer	Revisionsdato	Oversigt over rettelser	Rettet af	Rettelser markeret
0.9	13-06-2007	Udkast til styregruppen	JRI	(N)
0.95	27-06-2007	Redigeret oplæg til TSO	JRI	(J)
1.0	27-06-2007	TSO kommentarer indarbejdet. Afsendt til EDA	JRI	(N)
1.1	28-06-2007	Revideret af EDA	EDA	(N)
1.2	28-06-2007	Enkelte typografiske rettelser	JRI	(J)
