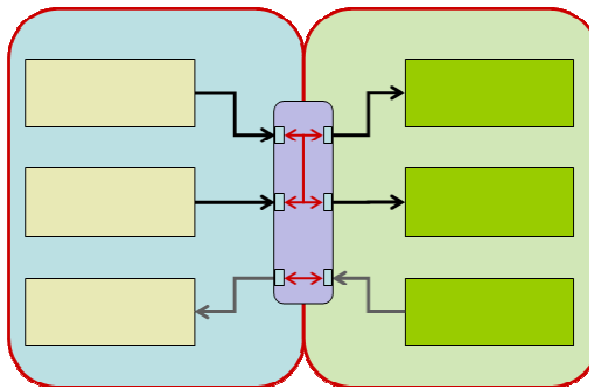


Kravspecifikation for SOSI-GW komponenten

Af: TSO/Lakeside

Version: 1.20



Indhold

Indhold	2
Baggrund.....	3
Overordnet teknisk beskrivelse.....	3
Om kravspecifikationen	5
Kravenes form.....	5
A Funktionelle krav til SOSI-GW	6
A.1 Generelle krav	6
A.2 WS: Kald ekstern service med påsat Id-kort.....	6
A.3 WS: Opret Id-kort til klient-signering.....	7
A.4 WS: Installer signeret Id-kort.....	8
A.5 WS: Opret Id-kort til browser-signering.....	8
A.6 WS: Logout	9
A.7 Browser adgang til Id-kort signering	9
A.8 Administrations interface	10
B Tekniske krav	10
C Quality of Service	11
D Leverance og test	12
Referencer	13

Baggrund

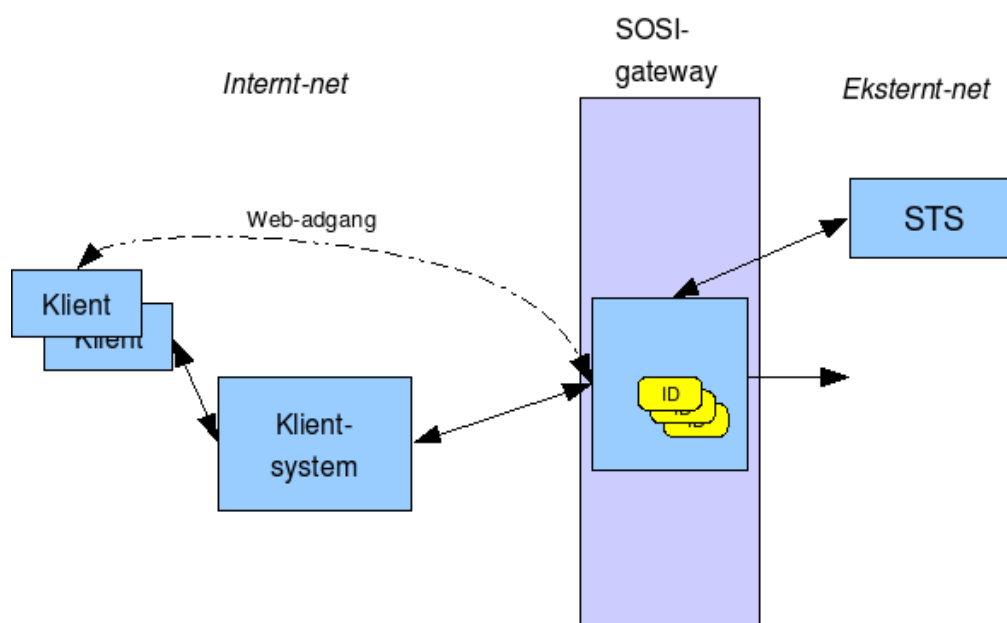
Når man anvender ”Den Gode Web Service” (DGWS) på niveau 3 og opefter, skal det SOSI Id-kort, der anvendes, være underskrevet med OCES digital signatur. Dette er en barriere for både applikationsleverandørerne og brugerne. En væsentlig del af formålet med SOSI-Gateway (SOSI-GW) er derfor at lægge en del af besværet ved at anvende digital-signatur ud i en fælles hjælpekomponent. For applikationsleverandørerne betyder det, at de hverken behøver at bekymre sig om signeringen, eller på hvordan det signerede Id-kort skal håndteres, og for brugeren betyder det, at man i en vis udstrækning opnår Single-Sign-On mod forskellige offentlige tjenester fra flere forskellige systemer.

Overordnet teknisk beskrivelse

SOSI-GW'ens funktion er at oprette, få signeret og opbevare Id-kort, som senere kan indsættes i DGWS kald. Når SOSI-GW'en bliver bedt om at oprette et Id-kort, præsenteres det for brugeren, som skal underskrive det med sin MOCES-signatur. Derefter huskes (caches) dette Id-kort så længe det er gyldigt. Når applikationer skal udføre et kald, der kræver anvendelse af Id-kort, kan de sende det via SOSI-GW'en, som så kan påklippe et underskrevet Id-kort.

SOSI-GW'en skal således være en servicekomponent, der varetager følgende opgaver:

- Oprettelse, signering og opbevaring af Id-kort
- Indsættelse Id-kort i DGWS kald og videresendelse af kaldet
- Validering af systemer der tilgår SOSI-GW'en



Figur 1: SOSI-GW i sammenhæng

Klientsystemer skal kommunikere med SOSI-GW'en via en række web-services.

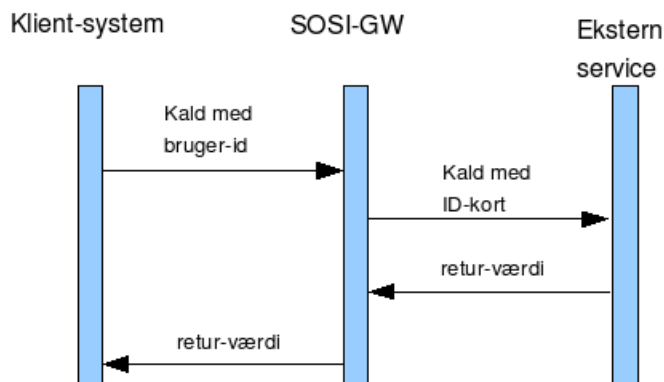
Den væsentligste service på SOSI-GW'en er at indsætte Id-kort i et DGWS request. Det vil sige omdanne et DGWS kald fra et niveau til et DGWS kald på et højere niveau (f.eks. fra niveau 1 med simpelt bruger-id til niveau 4 med bruger-signeret Id-kort). For at kunne gøre dette, skal der eksistere et gyldigt signeret Id-kort i SOSI-GW'ens cache, hvilket håndteres med de øvrige services.

SOSI-GW komponenten – kravspecifikation

IT-Staben – Strategi, arkitektur og sikkerhed

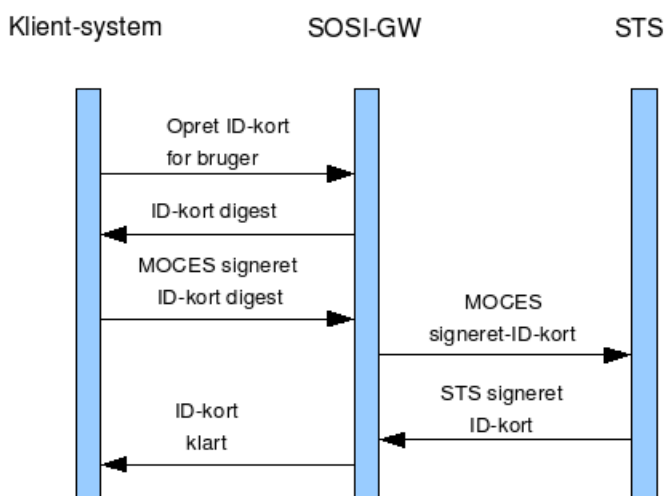
Dato: 22. august 2007

Dette scenarium er vist på figur 2.



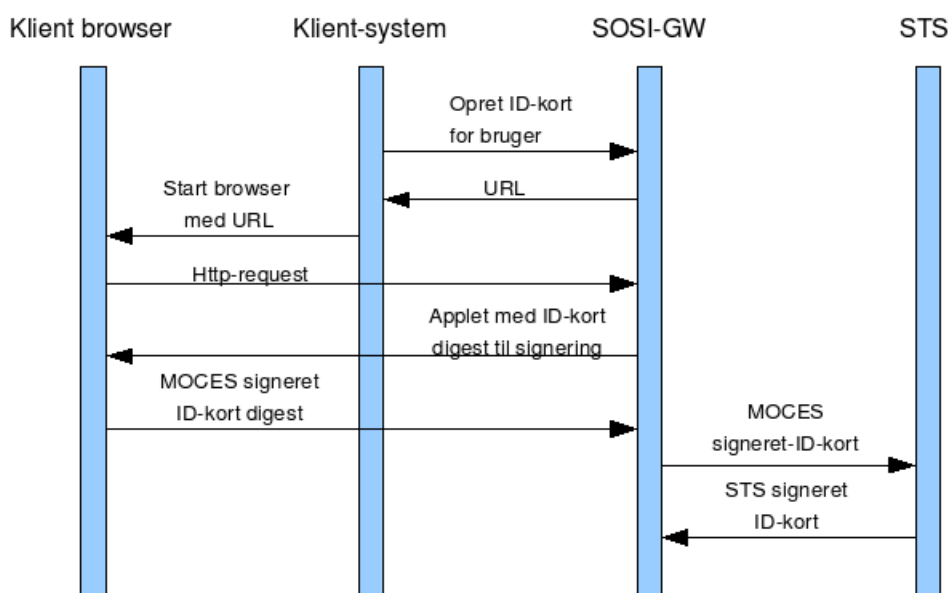
Figur 2: Omdan niveau-1 kald til niveau-4

Når der skal oprettes et Id-kort skal SOSI-GW'en give klientsystemet 2 muligheder. Den første mulighed, som ses skitseret på figur 3, kræver at klientsystemet selv integrerer MOCES signeringen i brugerdialogen.



Figur 3: Id-kort oprettelse med klientsystem signering

Hvis klientsystemet ikke selv kan varetage signeringen af Id-kort, kan den anden mulighed anvendes. Her starter klientsystemet en web-browser på brugerens maskine med en URL udleveret af SOSI-GW'en. Dette bringer brugeren i direkte kontakt med SOSI-GW'ens web-interface der nu gennem en *sign-applet* håndterer MOCES signeringen, hvorefter det færdige Id-kort kan gemmes i cachen.



Figur 4: Id-kort oprettelse med browser og signering

En forudsætning for at brugen af SOSI-GW er sikkerhedsmæssigt forsvarligt er, at der er en høj grad af perimetersikkerhed omkring applikationer og SOSI-GW. Hvis dette ikke er tilfældet er misbrug af den digitale signatur muligt.

En anden forudsætning er, at brugeren skal kunne identificeres entydigt. Til dette formål kan anvendes f.eks. CPR-nummer, et regionalt bruger-Id eller en kobling af system-id og system-specifikt bruger-id.

Om kravspecifikationen

Dette afsnit forklarer kravenes form og hvordan kravene tænkes at tilgodese kundens mål.

Kravenes form

Kravene er opdelt i kapitler efter deres art, fx kapitel A om funktionelle krav som systemet skal opfylde, kapitel B om tekniske krav, som systemet skal anvende osv. I hvert kapitel er kravene opstillet i afsnit, der vedrører en bestemt arbejdsopgave eller emne.

Kravene indeholder flg.:

- Kravnummer eller Optionsnummer
- Overskrift
- Beskrivelse
- (Info) Løsningsforslag
- (Info) Hyppighed
- (Info) Verificering
- (Info) Andre informationer (eksempel, kommentar ...)

De første tre punkter er obligatoriske og udgør selve kravet. Foruden disse punkter kan kravet foreslå en løsning, redegøre for hyppighed, hvordan kunden har tænkt sig at verificere kravet samt andre oplysninger. Disse oplysninger er ikke en del af kravet, men nogle nyttige informationer til

tilbudsgiver/leverandøren, der kan hjælpe eller guide mod den rigtige løsning.

Kravene har fortløbende unikke numre og kan således utvetydigt refereres til med deres kravnummer, f.eks. Krav 1 eller K1.

A Funktionelle krav til SOSI-GW

Følgende services/interfaces skal være til rådighed på SOSI-GW'en:

1. Kald ekstern service med påsat Id-kort
2. Opret Id-kort til klient-signering
3. Installer signeret Id-kort
4. Opret Id-kort til browser-signering
5. Check eksistens af Id-kort
6. Log-out (fjern cachet Id-kort)
7. Web-interface til signering af Id-kort
8. Interface til administration

A.1 Generelle krav

Krav 1: Check af *trusted* afsender

SOSI-GW'en skal have en *whitelist* over klientsystemer, der er tillid til, og skal for hvert kald kontrollere om klientsystemet har ret til at benytte SOSI-GW.

Tilbudsgiver bedes beskrive, hvorledes systemer identificeres samt hvorledes dette præcist repræsenteres i beskeden.

A.2 WS: Kald ekstern service med påsat Id-kort

Denne service er et gateway endpoint, og har således ikke nogen WSDL beskrivelse. Selve kaldet har den form som det skal have hos den endelige modtager, på nær SOAP-header informationen, som primært skal identificere brugeren og systemet unikt.

Krav 2: Gateway funktionalitet der ændrer niveau 1 kald til niveau 4 kald

Der skal laves gateway-funktionalitet som skitseret på figur 2. Det vil sige at den kan:

1. modtage et SOSI-kald
2. udskifte eller indsætte Id-kort
3. sende kaldet videre til endelig destination
4. modtage svar
5. returnere svar til den oprindelige afsender.

Når SOSI-GW'en modtager et kald med et "lav-niveau" Id-kort, der indeholder system-Id samt et *unikt bruger-id*, skal der kontrolleres:

1. om klientsystemet er i white-listen. Findes systemet ikke i white-listen, returneres en fejl.

2. hvis kaldet indeholder akkreditiver for det kaldende system, kontrolleres disse.
3. om SOSI-GW'en har et signeret Id-kort for brugeren. Findes et signeret Id-kort indsættes dette som erstatning for det medsendte Id-kortet, og kaldes sendes videre til det endelige system. Findes der ikke et signeret Id-kort returneres en fejl-kode til klientsystemet.

Tilbudsgiver bedes beskrive, hvorledes det unikke bruger-Id og system-Id repræsenteres i XML beskeden ved anvendelse af standarder, der ikke strider mod DGWS (Reference 3).

Krav 2a: Implicit oprettelse af Id-kort

Hvis SOSI-GW modtager et kald, som ikke kan behandles fordi SOSI-GW ikke har et gyldigt Id-kort for brugeren, skal det checkes, om der er tilstrækkelig information i "Lav-niveau" Id-kortet til at oprette et signeringsparat Id-kort. Hvis der er det, laves en *implicit Id-kort oprettelse*, og sammen med fejl-koden til klienten, sendes både digest til signering og URL til browser-baseret signering svarende til retursvar fra "WS: Opret Id-kort til klient-signering" og "WS: Opret Id-kort til browser-signering", som er beskrevet senere.

Klienten har herefter følgende muligheder:

1. Selv at håndtere signeringen af digest'et, og kalde "WS: installere signeret Id-kort", som er beskrevet i afsnit A.3
2. Starte en browser med den returnerede URL til browserbaseret signering
3. Undlade at gøre noget.

SOSI-GW skal specificere en timeout periode, som ikke må overskrides, hvis klienten vil anvende mulighed 1 eller 2. Efter denne timeout kan det oprettede men usignede Id-kort slettes.

Kommentar:

Ved at returnere både digest og URL undgår man at skulle konfigurere om forskellige klienter benytter den ene eller anden type signering.

Krav 3: Check af lovlig XML-struktur

Hvis kaldet ikke er lovlig XML, kan det afvises med en fejl-kode. Det er ikke et krav at Gateway'en checker kaldet udover den information gateway'en selv skal bruge, men det er frit for tilbudsgiver at beskrive andre passende kontroller.

Krav 4: Anvendelse af WS-Addressing

Kaldet mod SOSI-GW'en skal følge WS-Addressing specifikationen fra W3C (se referenceafsnittet), hvorved det endelige endpoint specificeres. WS-Addressing specificerer også hvordan retur- og fejl-koder skal tilbage til afsenderen. Er der ikke WS-Addressing information i kaldet returneres en fejl-kode.

Krav 5: Fjernelse af WS-Addressing informationer

WS-Addressing informationer skal fjernes fra kaldet inden den endelige destination kaldes, hvis denne ikke understøtter dette. Dette sættes op pr. destinations-endpoint gennem administrationsinterfacet (se senere).

Default er at sende WS-Addressing informationer videre.

A.3 WS: Opret Id-kort til klient-signering

Denne service bruges til at få SOSI-GW til at oprette et Id-kort for en angivet bruger. SOSI-GW'en

udfærdiger Id-kortet i det gældende format, og returnerer et Id-kort digest til klientsystemet, som er ansvarlig for at få dette signeret, jvf. forløb skitseret på figur 3.

Krav 6: Web-service interface til oprettelse af Id-kort til klient-signering

Der skal laves en web service, der kan oprette et usigneret Id-kort, udtrække det digest der skal signeres og returnere dette til klientsystemet.

Som input skal klientsystemet angive alle de informationer, der er nødvendige for at oprette et Id-kort jf. DGWS. Hvis klientsystemet medsender brugerens CPR-nummer skal dette medsendes til STS'en.

A.4 WS: Installer signeret Id-kort

Denne service bruges når en klient har fået signeret et Id-kort digest, og dette skal returneres til SOSI-GW'en. Her vil det signerede digest blive indsat i det genererede Id-kort, som derefter bliver installeret i SOSI-GW'ens cache.

Krav 7: Web-service interface til installering af signeret Id-kort

Der skal laves en web-service, der kan modtage et signeret Id-kort-digest, indsætte det i det tidligere genererede Id-kort, sende det til SOSI-STs'en og installere det af STS'en returnerede Id-kort i SOSI-GW'ens cache. For at kunne lave Id-kortet til STS-forespørgslen skal klientsystemet også medsende brugerens offentlige certifikat.

Krav 8: Verificering af Id-kort

Inden SOSI-GW'en installerer Id-kortet i dens cache, skal den kontrollere STS'en signatur. Hvis dette fejler, returneres fejl til klientsystemet.

A.5 WS: Opret Id-kort til browser-signering

Denne service bruges til at få SOSI-GW til at oprette et Id-kort for en angivet bruger, som skal underskrives via SOSI-GW'ens web-interface. SOSI-GW'en udfærdiger Id-kortet i det gældende format og gemmer dette i ikke signeret version. Herefter returneres en URL til klientsystemet, hvori en reference til en GUI præsentation af det usignede Id-kort er indkodet.

Krav 9: Web-service til klargøring af Id-kort til browserbaseret signering

Der skal laves en web-service, der kan oprette et usigneret Id-kort, som efterfølgende kan signeres via en web-browser. Id-kortet oprettes med samme parametre som ved kaldet: *Opret Id-kort til klient-signering*

Kaldet skal returnere en URL som vil bringe en browser til SOSI-GW'ens signeringsside.

Kommentar

Det er sandsynligt at SOSI-GW komponenten står på et lukket net, og at adgang fra en browser-klient derfor kun kan ske gennem en proxy eller lign. Det kan bl.a. betyde at host-navnet i URL'en til SOSI-GW komponentens browser-service må være en konfigurationsparameter.

Krav 10: Sikring mod URL-manipulation

Den returnerede URL skal indeholde en nøgle som kan bringe browseren direkte ind på siden der giver mulighed for at signere det netop oprettede Id-kort, men samtidig skal det sikres at man ikke ved simpel URL-manipulation kan få lov at signere en andens Id-kort. Den pågældende URL må kun kunne aktiveres inden for en periode på 30 sekunder (målt i SOSI-GW tid).

A.5a WS: Check eksistens af Id-kort

Denne service benyttes enten, hvis en klient ønsker at sikre sig at, der findes et gyldigt Id-kort, eller hvis klienten i forbindelse med at have startet en browser med henblik på browser-baseret signering, ønsker at vente på at Id-kortet er oprettet.

Krav 10a: Web-service til check af eksistens af Id-kort

Der skal laves en web-service, der kan checke, om der findes et gyldigt Id-kort for et specificeret bruger-id. Det skal i kaldet angives hvor længe klienten ønsker at vente på at et Id-kort eksisterer. Hvis ventetiden er 0, returneres med det samme en status på om gyldigt Id-kort findes.

Er ventetiden angivet større end nul, returnerer kaldet ved den først kommende af følgende to hændelser:

1. Der bliver modtaget et signeret Id-kort (enten via ”WS: Installer signeret Id-kort” eller via browser baseret signering). Kaldet returnerer at gyldigt Id-kort findes.
2. Ventetiden udløber, uden at et gyldigt Id-kort er modtaget. Kaldet returnerer at gyldigt Id-kort findes ikke.

A.6 WS: Logout

Denne service bruges til at få SOSI-GW til at fjerne et Id-kort for en angivet bruger fra cachen. Dette sikrer, at der ikke kan sættes Id-kort for den pågældende bruger på nye requests, før der er foretaget en signering af et nyt Id-kort.

Krav 11: Web-service til fjernelse af Id-kort fra cache

Der skal laves en service, der fjerner et Id-kort fra cachen ud fra et angivet *unik* bruger-ID.

A.7 Browser adgang til Id-kort signering

Krav 12: Web-side til signering af Id-kort

SOSI-GW'en skal have et web-interface som ved hjælp af f.eks. OpenOCES sign-appletten kan signere det Id-kort digest, der skal indsættes i det signerede Id-kort.

Web-siden skal præsentere de væsentligste elementer i Id-kortet, således at brugeren er informeret om, hvad der skrives under på. Det skal sikres at løsningen også sender brugerens offentlige certifikat med tilbage, således at det også kan indsættes i Id-kortet.

Når signeringen er afsluttet skal browser-vinduet lukkes, og det signerede Id-kort skal installeres i SOSI-GW'ens cache.

Kommentar

Det der skal signeres i forbindelse med Id-kort signering er binære data. Det betyder at brugeren reelt ikke har mulighed for at checke, hvad det er der underskrives, men må stole på, at det der præsenteres i klar-tekst stemmer med det binære digest der signeres. Denne tillid kan baseres på tilliden til den leverandør der har signeret appletten, og eventuelt også på kilden til web-siden, som kan checkes i browserens Location-felt.

Krav 13: sikring mod URL-hackning

Web-siden må kun tilgås med en gyldig URL returneret fra et kald af web-servicen: *Opret Id-kort til browser-signering*.

Hvis den anvendte URL ikke er lovlig eller er udløbet skal der vises en fejlbesked til brugeren.

A.8 Administrations interface

Der skal udvikles administrationsinterfaces, som benyttes til opsætning og ændring af konfigurationsparametre for SOSI-GW'en. Uanset hvilken type administrationsinterface der vælges, skal der laves simple brugergrænseflader, hvormed man kan lave den fornødne opsætning og konfigurerings.

Krav 14: Opsætning af whitelists

Der skal være et interface, hvormed man kan ændre, hvilke systemer der betegnes som *trusted* og dermed må anvende SOSI-GW'en. Sådanne ændringer skal kunne laves uden at SOSI-GW'en skal lukkes ned.

Krav 15: Opsætning af services der må kaldes

Det skal kun være muligt at få påsat Id-kort på kald til forud godkendte services.

Denne positivliste skal kunne vedligeholdes uden systemet lukkes ned.

For hver enkelt service skal man kunne specificere:

- Om servicen understøtter WS-addressing (eller om dette skal stripes af)
- Hvilket DGWS-niveau servicen kræver (default 4 i denne version)

Krav 16: Id-kort revocation

Det skal være muligt at tvinge SOSI-GW'en til at slette et Id-kort fra cachen, ud fra ejerens CPR-nummer.

Krav 17: Beskyttelse af administrationsinterface

Adgang til administrationsinterfacet skal beskyttes mod uautoriseret brug.

B Tekniske krav

Krav 18: Open Source Java komponent

Komponenten skal udvikles i JAVA under en af SOSI-projektet udpeget open-source licens.

Krav 19: Anvendelse af SOSI-biblioteket

Komponenten skal anvende SOSI-biblioteket. Såfremt dette afdækker problemer i SOSI-biblioteket vil disse blive rettet.

Krav 20: Standarder

Alle XML formater skal i videst muligt omfang følge de i "Den Gode Web Service" beskrevne standarder, herunder SOAP 1.2, WS-Security, XML-Signature, SAML etc. Desuden skal formater følge WS-addressing som tidlige beskrevet.

Hvis tilbudsgiver finder det nødvendigt at fravige dette, skal det eksplicit bemærkes og begrundes.

SOSI-GW komponenten – kravspecifikation

IT-Staben – Strategi, arkitektur og sikkerhed

Dato: 22. august 2007

Krav 21: Der skal foretages revokationskontrol af føderationcertificatet

Via de i SOSI-biblioteket indbyggede funktioner skal der foretages revokationskontrol af føderationcertificatet.

Krav 22: Logning

Alle gateway passerer og kald til SOSI-GW logges. I loggen skal der som minimum kunne findes flg. informationer:

- Tid for kald (til millisekund)
- Afsender system/bruger-id samt modtager service

Loggen skal rettes mod auditører og opbevares både fysisk og tidsmæssigt jf. gældende lovgivning.

Tilbudsgiver skal beskrive hvilken persistensmekanisme der forventes anvendt til logning, samt hvilke muligheder der er for at udtrække data fra loggen.

Krav 23: Afviklingsmiljø

SOSI-GW'ens skal som minimum kunne afvikles i et almindeligt java-miljø oven på en servlet 2.4 tomcat platform.

Det skal dokumenteres hvilke kodeændringer og konfigurationsændringer, der er nødvendige for at deployere komponenten i et Java-EE baseret applikations-server miljø.

C Quality of Service

Kravene i dette afsnit relaterer sig til kvaliteten af SOSI-GW'en. Kravene har til formål at sikre, at SOSI-GW'en fra begyndelsen udvikles med skalering, performance og robusthed for øje.

Krav 24: Operationelle krav

Den færdige service skal være til rådighed 24 timer i døgnet alle årets dage. SOSI-GW'en skal udarbejdes så den kan deployeres i et miljø, hvor det er muligt at vedligeholde servicen og det hardware servicen afvikles på uden at servicen tages ud af drift (rullende vedligeholdelse).

Leverandøren skal beskrive hvilket setup der kræves, hvis der ønskes rullende vedligehold.

Krav 25: Krav til kapacitet ved Id-kort udstedelser

I pilotafprøvningsperioden skal Id-kort udstedesservicen kunne udstede minimum 3000 Id-kort pr. døgn. I spidsbelastningstimer skal der kunne udstedes 1000 Id-kort i timen (= max kontinuerlig belastning). I spidsbelastning skal servicen kunne håndtere minimum 10 samtidige igangværende Id-kort udstedelser.

Ved browser baseret signering skal svartiden (målt fra ”kald af opret Id-kort til browsersignering” til hele http-strømmen inkl. applet er afleveret) være max 5sek ved 10 samtidige kald.

Krav 26: Kapacitet og svartider for gateway

Under kontinuerlig belastning skal gateway passagen (med simpel substitution af Id-kort) kunne klare minimum 10000 kald i timen med svartider på:

- Gennemsnitstid <0.5 sekund.
- 95 % fraktilen < 1 sekund.

- 99 % fraktilen < 4 sekunder.

Tiden måles fra det tidspunkt kaldet modtages i servicen til det er videresendt med signeret Id-kort. Kapaciteten skal kunne honoreres med beskeder på 4 kByte med en realistisk sammensætning af XML elementer.

Krav 27: Svartider på Administrations interface

Operationer der udføres mod administrations interfacet må ikke overskride 10 sekunder per operation. Hvis dette ikke kan overholdes for enkelte operationer, skal der være visuel tilbagemelding inden 5 sekunder samt løbende visning af reel aktivitet.

Krav 28: Dokumentation af tilstrækkelig hardware

Krav til hardware og driftsmiljø der er nødvendig for at opfylde de stille performancekrav skal dokumenteres.

Krav 29: Skalerbarhed

SOSI-GW'en skal udvikles så den kan køre parallelt i flere instanser, og disse forskellige instanser skal kunne benytte samme konfigurationsdata.

Krav 30: Dokumentation og adgang til dokumentation

De udstillede web-services skal dokumenteres, så en udenforstående udviklingsorganisation på baggrund af dokumentet umiddelbart kan integrere til servicen.

Verifikation:

Dokumentationen kvalitetssikres hos en uafhængig leverandør.

Krav 31: Sikkerhedsvejledning

Der skal udarbejdes en sikkerhedsvejledning over hvilke netværksmæssige krav, der skal opfyldes for at have et tilstrækkeligt trust-relation forhold mellem SOSI-GW'en og de systemer der anvender den.

D Leverance og test

Krav til form og tidsplan for leverancen beskrives i det følgende.

Krav 32: Løsningsbeskrivelse og pristilbud

Tilbudsgiver skal i forbindelse med aflevering af løsningsbeskrivelse med pristilbud også levere et estimat på forventet tidsforbrug specificeret på relevante funktionelle delelementer.

Løsningsbeskrivelsen skal afleveres senest 15.8.2007.

Krav 33: Delleverancer

Udviklingen af SOSI-GW'en skal foregå i delleverancer/iterationer, hvor kunden og andre projekter løbende kan følge med i fremdriften. Der er krav om flg. delleverancer:

Leverance 1 – Funktionel testversion:

Da SOSI-GW'en er en nøglekomponent i forbindelse med udvikling af EPJ-løsninger til Det Fælles Medicin grundlag skal en funktionel testversion være klar 1.11.2007.

Denne test version skal kunne:

- Udstede Id-kort, få dem signeret og cache dem

SOSI-GW komponenten – kravspecifikation

IT-Staben – Strategi, arkitektur og sikkerhed

Dato: 22. august 2007



- Videresende forespørgsler med påsat signeret Id-kort.

Leverance 2 – Stabiliseret fuld funktionel version:

En version hvor alle funktionelle krav er opfyldt skal være klar 1.12.2007, hvor integrationstesten af Det Fælles Medicin grundlag starter. Denne Integrationstest vil også være integrationstest af SOSI-GW'en.

Leverance 3 – Operationel version:

En fuld driftsklar version hvor alle drift, performance og logningskrav er opfyldt skal afleveres 1.2.2008, hvor Det Fælles Medicin grundlag går i pilot-drift.

Parallelt med pilot-driften laves en automatiseret performancetest, der indeholder:

- En skaleringstest der viser at SOSI-GW'en skalerer lineært indtil overbelastning
- En load/stresstest, der identificerer overbelastningspunktet og identificerer hvilke symptomer systemet udviser ved overbelastning og om eller hvornår systemet bryder sammen. Det skal påvises at systemet virker upåklageligt ved overbelastning, f.eks. at alle videre sendte forespørgsler med påsatte Id-kort er korrekte etc
- Endurancetest der viser at systemet ikke har ressourcelækager (CPU, RAM) ved længerevarende jævn belastning.

samt en almindelig afleveringstest af øvrige funktionelle og performancemæssige krav.

Testen gennemføres på et produktionslignende miljø. Krav til testmiljøer etc. skal dokumenteres i forbindelse med udarbejdelse af testplan.

Testen udføres i et samarbejde mellem leverandøren og repræsentanter for SOSI-projektet og resultaterne dokumenteres i et testdokument.

Leverance 4 – Endelig aflevering:

1.4.2008 skal hele projektet med kildekode og dokumentation være afleveret til SOSI-projektets ejere.

Referencer

WS-Addressing <http://xml.coverpages.org/ws-Addressing.html#Version200412>

Sign-applet <http://www.openoces.org/>

Den Gode Web Service <http://www.medcom.dk/wm110102>

Revisionshistorik

Dato for denne revision: 22. august 2007	Dato for næste revision:
--	--------------------------

Revisionsnummer	Revisionsdato	Oversigt over rettelser	Rettet af	Rettelser markeret
0.99	28-06-2007	Sendt til review til EDA	TSO	(N)
1.20	22-08-2007	Mindre tilføjelser af hensyn til øget usability	TSO	J