DIGITAL SUNDHED
SAMMENHÆNGENDE DIGITAL SUNDHED I DANMARK

SOSIGW

- **Administrationskonsol for SOSIGW 1.0**

Indeks

Version	Dato	Ansvarlig	Kommentarer
2	15-10-2009	jre	Layout og stavefejl rettet

Revisionshistorik

Version	Dato	Ændring	Ansvarlig
1	09/10/09	Initiel version af dokument	jre
2	15/10/09	Layout og stavefejl rettet	jre

Introduktion

Administration af et SOSI-GW cluster foretages via en webbaseret administrationskonsol. Grænsefladen er baseret på GWT (Google Web Toolkit). Administrationskonsollen indeholder flg. funktioner:

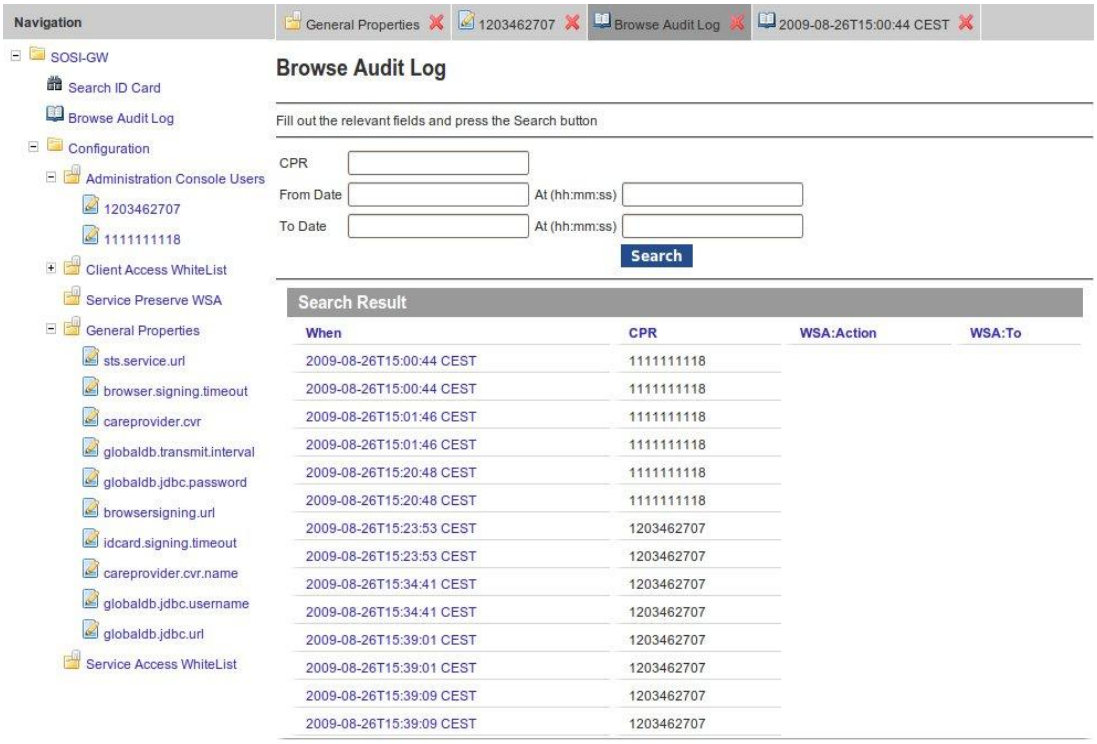
- Bootstrap mode, hvor gateway funktionalitet er slået fra, men hvor adgangsbegrænsning er baseret på filbaseret brugernavn/password. Dette mode benyttes kun under installationsprocessen.
- Opsætning af white lists, hvor tilladte klienter sættes op og identificeres.
- Opsætning af service positivliste, hvor services som må kaldes på vegne af klienter sættes op og identificeres.
- Id-kort revokering, hvilket giver mulighed for at fremsøge et id-kort på baggrund af et bruger id, og efterfølgende revokere dette, dvs. fjerne id-kortet fra den delte cache.
- Søgning i audit logs. Administrationskonsollen giver mulighed for at foretage simple søgninger i auditloggen, fx baseret på bruger-id og/eller tidsrum.
- Styre adgang til interfacet selv. Dette sker ved at give brugere adgang på baggrund af certifikater.
- Konfiguration af timeoutværdier
- Konfiguration af andre runtime-værdier

Administrationskonsollen

Administrationskonsollen tilgås via en normal browser på adressen http://<sosigw>/sosigw/console. Alt efter hvilken tilstand, serveren kører i, vil der blive krævet login via OpenSign-appletten. I development mode kræves der ikke login.

- Hvis der køres i test eller produktion, og der derfor kræves login, bliver der først spurgt om et cpr-nummer, der ønskes at logge ind med. Dette nummer skal være oprettet i systemet før login kan gennemføres, se afsnittet "Initiel konfiguration" nedenfor.
- Nu vises en OpenSign applet, som bruges til at validere en bruger. Vælg det rette certifikat og underskriv beskeden
- Efter validering af signaturen vises administrationskonsollen
- Vises konsollen ikke, eller fejler et af trinene, så se afsnittet omkring fejlfinding længere nede.

Generel brug af konsollen



Som vist ovenfor er administrationskonsollen er bygget op med en menu i en træstruktur i venstre side og indhold i højre side. Menuen kan navigeres ved at åbne og lukke knuder ved at trykke på + eller -. Vælg et menupunkt ved at trykke på det. Punkter åbnes i en række tabs, som ligger i toppen af skærmen, og som man kan skifte imellem ved at trykke på dem. De kan ligeledes lukkes ved at trykke på de røde krydser.

Alle ændringer foretaget i konsollen slår igennem umiddelbart, og det er ikke nødvendigt at genstarte serveren.

Bemærk dog, at hvis serveren kører i development mode, så persisteres konfiguration ikke, så ved næste genstart vil konfigurationen være nulstillet igen.

I det følgende er de enkelte funktioner i administrationskonsollen beskrevet.

Fremsøgning af ID-kort

Det er muligt at lave en søgning blandt alle de ID-kort, der eksisterer i clusteret. Det gøres under punktet “Search ID Card”. Fremsøgning sker på baggrund af CPR-nummer, som kan indtastes i søgefeltet. Hvis der eksisterer et ID-kort for brugeren, vil det blive vist i listen sammen med ID-kortets tilstand. Findes der ikke noget ID-kort vil listen være tom.

Det er ikke muligt at søge via wildcards.

Søgning i auditlog

Søgning i auditloggen sker via “Browse Audit Log”. Herfra er det muligt at se alle indgange i den globale auditlog – det er ikke muligt at søge i den lokale auditlog fra administrationskonsollen.

Søgning kan begrænses til et bestemt CPR-nummer for ID-kortet og et bestemt tidsrum. Hvis der ikke angives nogen begrænsninger, vises alle indgange i auditloggen.

Det er ikke muligt at bruge wildcards, men for tidsrum kan man nøjes med at udfylde dato-feltet og ikke angive noget tidspunkt.

Giv brugere adgang til administrationskonsollen

Admin-brugere skal eksplicit gives adgang til administrationskonsollen. Det gøres under punktet Configuration -> Administration Console Users. Brugere er identificeret via deres CPR-nummer, og CPR-nummeret skal matche det, der er tilknyttet det certifikat, der bruges til login.

Opret en ny bruger ved at vælge New. Som Name angives CPR-nummeret, og derudover skal fornavn, efternavn og emailadresse angives.

Adgangskontrol på SOSIGW

For at applikationer kan kalde ind igennem SOSIGW skal der gives adgang til disse applikationer. Adgangen sker primært på IP-adresse-niveau, men kan suppleres af en DGWS ClientAccessKey.

Listen af nuværende adgangsregler kan findes under Configuration -> Client Access WhiteList. Tilføj en ny ved at vælge New og udfyld følgende:

- Name: Internt navn der identificerer reglen
- IP-address: Klientapplikationens IP-adresse. Der matches på substrings, så som IP-adresse kan fx angives “10.0.0.”, hvilket vil matche alle IP-adresser der ligger i 10.0.0.x. Der kan ikke anvendes netmasks eller andre wildcards.
- Salt: Kan udfyldes med indholdet af DGWS ClientAccessKey, som så skal være til stede i alle requests. Fungerer som et shared secret mellem klient og SOSIGW.

Kontrol af WS-Addressing headers

Normalt fjerner SOSIGW alle WS-Addressing headers i proxy-requests, så de ikke sendes med i selve servicekaldet. Ønskes dette ikke, er det muligt at konfigurere hvilke WS-Addressing headers, der skal bevares. Dette gøres under Configuration -> Service Preserve WSA ved at vælge New og udfylde følgende:

- Name: Internt navn, der beskriver reglen
- WS-Addressing-to regexp: Regulært udtryk, der beskriver To-headeren.
- WS-Addressing-action regexp: Regulært udtryk, der beskriver Action-headeren.

Hvis et af felterne ikke udfyldes svarer det til et regulært udtryk, der matcher alle værdier.

Tillad proxy-requests til eksterne services

Når et proxy-request kommer ind fra en klient, checker SOSIGW hvorvidt der er tilladelse til at kalde den pågældende service eller ej. Alle eksterne services skal eksplicit konfigureres, hviket sker på baggrund af WS-Addressing headers. Det gøres under Configuration -> Service Access WhiteList, hvor der vælges New og følgende udfyldes:

- Name: Internt navn der beskriver reglen
- WS-Addressing-to regexp: Regulært udtryk der beskriver servicens To-header.
- WS-Addressing-action regexp: Regulært udtryk der beskriver servicens Action-header.

Hvis et af felterne ikke udfyldes svarer det til et regulært udtryk, der matcher alle værdier.

Øvrig opsætning

Under Configuration -> General Properties er der en række runtime-værdier, der kan justeres efter behov:

- sts.service.url: Endpoint-adresse for den STS, der skal bruges når ID-kort signeres.
- browser.signing.timeout: Antal sekunder, der max må gå mellem en signerings-URL sendes til en browser og resultatet er sendt tilbage til SOSIGW.
- browser.signing.url: Den URL, som browsere skal bruge ved signeringsrequests. I et clustered setup skal URLen pege på loadbalanceren.
- careprovider.cvr: CVR-nummer for organisationen. Skal matche det, der står i medarbejdercertifikaterne, og det skal desuden være registreret i STSen.
- careprovider.cvr.name: Systemets navn. Bruges i forbindelse med STS-registreringen.
- globaldb.transmit.interval: Antal millisekunder der går før lokale auditlogs sendes til den centrale logningsdatabase.
- globaldb.jdbc.username: Brugernavn til den globale logningsdatabase.
- globaldb.jdbc.password: Password til den globale logningsdatabase.
- globalgb.jdbc.url: JDBC URL til den globale logningsdatabase.

Fejlfinding i forbindelse med login

- **Authentication failed: cvr mismatch**: Det anvendte certifikat indeholder ikke det CVR-nummer, der er angivet i administrationskonsollen
- **Browser response handling failed: Authentication failed: cvrrid-cpr mismatch [CVR:xxx-RID:yyy,zzz]**: Det valgte CPR-nummer stemmer ikke overens med det, der er registreret på certifikatet.
- **Authentication failed: MOCES not in whitelist [CVR:25520041-SYSTEM:SOSITEST]**: Systemet er ikke tilføjet til STSens whitelist.

- Der sker ikke noget efter CPR-nummer er indtastet: Det indtastede CPR-nummer er ikke oprettet i systemet. Se afsnittet omkring initiel konfiguration.