**SOSI-Gateway**

Guide til anvendere

Indhold

[Formål 3](#_Toc454781867)

[Baggrund 3](#_Toc454781868)

[Hvorfor SOSI-GW? 3](#_Toc454781869)

[SOSI-GW kontekst 4](#_Toc454781870)

[NSP Gateway 4](#_Toc454781871)

[Netværkskomponent 4](#_Toc454781872)

[Security Token Service (STS) 4](#_Toc454781873)

[Afkoblingskomponent 5](#_Toc454781874)

[NSP services 5](#_Toc454781875)

[Decentral anvendelse 5](#_Toc454781876)

[Anvendelse af SOSI-GW 6](#_Toc454781877)

[Signering af id-kort i anvendersystem 6](#_Toc454781878)

[requestIdCardDigestForSigning 6](#_Toc454781879)

[signIdCard 6](#_Toc454781880)

[Browserbaseret signering 7](#_Toc454781881)

[requestIdCardDigestForSigning 7](#_Toc454781882)

[getValidIdCard 7](#_Toc454781883)

[Gateway Proxy 7](#_Toc454781884)

[proxy 7](#_Toc454781885)

[Anvendelse af implicit login 8](#_Toc454781886)

[Logge ud af SOSI-GW 8](#_Toc454781887)

[logout 8](#_Toc454781888)

[logoutWithResponse 8](#_Toc454781889)

[Fejlkoder 9](#_Toc454781890)

[Brug af SOSI-GW et delt miljø 9](#_Toc454781891)

[Brug af PassThrough-header 10](#_Toc454781892)

[Brug af signerede id-kort i proxy-kald 10](#_Toc454781893)

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Dato | Beskrivelse | Forfatter |
| 1 | 21-06-2016 | Første version, udarbejdet med udgangspunkt i ”programmers guide - SOSI-GW” | OBJ |

# Formål

Nærværende dokument udgør en guide til anvendere af SOSI-GW. Guiden er hovedsageligt målrettet eksterne anvendere af den centrale SOSI gateway som indgår i NSP platformen.

# Baggrund

En hyppigt forekommende eksempel på anvendelse af en NSP service er, når en privatpraktiserende læge ønsker at hente en borgers medicinkort fra Det Fælles Medicinkort (FMK). Dette vil i praksis ske igennem lægens eget lægepraksissystem, som skal foretage et webservicekald med SOAP-action ” http://www.dkma.dk/medicinecard/xml.schema/2015/01/01/E1#GetMedicineCard” til FMK for at hente medicinkortet.

FMK er blot en af mange NSP services. Overfor NSP er pågældende lægepraksissystem et af mange anvendersystemer.

NSP webservices er opbygget efter [Den Gode WebService](http://medcom.dk/standarder/webservice-standarder/den-gode-webservice) (DGWS), hvilket bl.a. betyder at der skal medsendes signerede id-kort i webservice-kald. I mange tilfælde er der krav om at anvende sikkerhedsniveau 4, hvor den enkelte bruger skal underskrive et id-kort med sin egen personlige digitale signatur. Hvis anvendersystemerne skulle kalde NSP webservices direkte, ville hvert enkelt system således være nødt til at håndtere signering af SOSI id-kort, og kende brugerens MOCES certifikat, hvilket kan være komplekst.

Det er her SOSI-GW kommer ind i billedet.

# Hvorfor SOSI-GW?

Formålet med SOSI¬GW er at flytte ansvaret for signering af SOSI id-kort fra de enkelte anvendersystemer til en central service. Denne service kan modtage requests og automatisk vedhæfte et signeret id-kort inden requests sendes videre til de endelige NSP service endpoints. Dermed behøver de enkelte anvendersystemer ikke at bekymre sig om at implementere signering af SOSI id-kort selv. I stedet håndteres dette af SOSI-GW.

Måden det foregår på er, at SOSI-GW gemmer selve id-kortet, men får en underskrift fra brugeren. Underskriften kan enten komme fra anvendersystemet eller via en browser-applet, der kan signere kortet via en normal browser. Anvendes browser-metoden, behøver anvendersystemet ikke at kende til brugerens certifikater eller signeringen af id-kort, men skal i stedet blot bekymre sig om at håndtere requests på den rette måde.

Der er dermed stadig er behov for, at brugeren selv signerer id-kortet. Men når et id-kort først er signeret, gemmes det i SOSI-GW indtil det udløber. Dette resulterer i, at NSP kan tilbyde Single Signon, da brugeren typisk kun bliver bedt om at signere id-kortet én gang i løbet af en normal arbejdsdag, selvom der foretages kald på tværs af NSP services.

# SOSI-GW kontekst

SOSI-GW anvendes i forskellige konfigurationer. I dette afsnit beskrives hovedsageligt anvendelse af central SOSI-GW, som den der står foran de centrale NSP miljøer (cNSP).

## NSP Gateway

Figur 1 illustrerer et centralt NSP setup med SSL overbygning, som f.eks. anvendes af kommunerne. I denne konfiguration er SOSI-GW placeret før afkoblingskomponenten (DCC).



Figur 1: Central SOSI-GW på NSP-platform (NSP-Gateway/NGW).

Der er etableret et antal centrale NSP miljøer med dette setup, både drift-, test- og uddannelsesmiljøer. Der henvises til [www.nspop.dk](http://www.nspop.dk) for mere information om NSP platform og miljøer.

### Netværkskomponent

Anvendersystemets kald foretages med HTTPS. Komponenten der kaldes sikrer at der kaldes med et korrekt SSL-klientcertifikat, og at anvendersystemet er whitelistet til at kalde den ønskede service. Hvis dette er i orden viderestilles til SOSI-GW.

### Security Token Service (STS)

Beskeden fra anvendersystemet kan i første omgang blot være et kald til en NSP service, som indeholder et sikkerhedsniveau 1 id-kort. SOSI-GW vil så undersøge sin id-kort cache for at se om der findes et gyldigt signeret niveau 4 id-kort. Hvis dette er tilfældet erstattes niveau 1 id-kortet i beskeden med det signerede niveau 4-kort, og der stilles videre gennem DCC.

Hvis der *ikke* findes et signeret id-kort, eller det signerede id-kort et udløbet, sendes en DGWSFault tilbage til anvendersystemet som svar. Svaret vil udover fejlkode også indeholde SOAP-headers med en digest samt en URL til en webside, som kan anvendes til at signere et id-kort med. Anvendersystemet kan så vælge en af to muligheder:

* Anvendersystemet starter en almindelig browser med pågældende URL, hvorefter brugeren kan signere id-kortet ved at anvende sit personlige MOCES certifikat. Dette er den simpleste løsning for anvendersystemet.
* Anvendersystemet dekoder og RSA-signerer den returnerede digest, og foretager derefter kald til SOSI-GW’s metode signIdCard kaldes.

SOSI-GW kalder i begge tilfælde STS for at få foretaget signering med føderationens certifikat. Hvis signeringen blev gennemført med succes, cacher SOSI-GW efterfølgende det signerede id-kort, som er gyldigt i et antal timer. Herefter kan anvendersystemet foretage kald igen, hvor der denne gang findes et signeret niveau 4 id-kort i SOSI-GW’s id-kort cache.

### Afkoblingskomponent

Som udgangspunkt kalder SOSI-GW videre til den relevante NSP service igennem en afkoblingskomponent kaldet DCC (Decoupling Component). Afkoblingskomponenten vil ud fra beskedens SOAP-action afgøre hvilket konkret endpoint, der skal kaldes. Eksempelvis vil DCC’en kalde Det Fælles Medicinkort (FMK) når SOAP action er GetMedineCard.

### NSP services

Den konkrete NSP service, f.eks. FMK, vil som nævnt oftest blive kaldt igennem DCC.

Såfremt beskeden fra anvendersystemet indeholder en WsAddressing SOAP-header, hvor ”To” er udfyldt, vil SOSI-GW kalde den pågældende URL direkte i stedet for at viderestille gennem DCC. Dette er illustreret på Figur 1 ved den stiplede pil fra SOSI-GW direkte til de forskellige NSP services.

## Decentral anvendelse

Det foregående afsnit beskriver en konfiguration hvor NGW står foran cNSP, hvilket i praksis betyder at SOSI-GW kaldes først, og typisk viderestiller gennem DCC.

SOSI-GW anvendes også decentralt, hovedsageligt af regionerne, hvor der er etableret systemintegration mellem NSP og regional IT. Dette setup adskiller sig bl.a. ved at DCC her står før SOSI-GW, som vist på Figur 2:



Figur : Decentral NSP (dNSP), med SOSI-GW placeret efter DCC

Anvendersystemet kan her f.eks. være en elektronisk patientjournal (EPJ). Afkoblingskomponenten afgør igen adressen på NSP service endpoint ud fra SOAP-action, og indsætter en WsAddressing SOAP-header med adresse i feltet ”To” og SOAP-action i feltet ”Action ”. Herefter kaldes videre til SOSI-GW. SOSI-GW vil så håndtere signering vha. STS som beskrevet i forrige afsnit, og efterfølgende kalde direkte til NSP servicen specificeret i ”To”.

Der henvises til [www.nspop.dk](http://www.nspop.dk) for mere information om NSP platform og miljøer.

# Anvendelse af SOSI-GW

For at kalde NSP services igennem SOSI-GW skal der anvendes webservice-kald som indeholder et gyldigt niveau 1 id-kort i SOAP-headeren.

Dette er krævet for *alle* kald til og gennem SOSI-GW. Det er også muligt at anvende højere niveau id-kort, se venligt afsnittet ”Brug af signerede id-kort i proxy-kald” for mere information om dette.

Signering af id-kort kan enten foretages af anvendersystemet, eller man kan overlade det til SOSI-GW ved at åbne en webside til signering i en browser. Hvilke metoder der skal kaldes for at anvende de 2 muligheder beskrives nærmere i dette afsnit.

## Signering af id-kort i anvendersystem

Hvis et anvendersystem selv ønsker at implementere signering af id-kort kan dette gøres ved at kalde følgende SOSI-GW operationer:

### requestIdCardDigestForSigning

Denne operation svarer til ”login”. Der returneres et digest som kan RSA-signeres med et certifikat.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#requestIdCardDigestForSigning

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

### signIdCard

Anvendes til signering af et id-kort.

Som input gives det RSA-signerede digest som der blev returneret til anvendersystemet af **requestIdCardDigestForSigning**, samt det certifikat som blev anvendt til signering.

Herefter vil SOSI-GW kalde STS, som signerer med føderationens certifikat, og lagre det resulterende signerede niveau 4 id-kort I sin cache.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#signIdCard

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

## Browserbaseret signering

Hvis man ikke ønsker at implementere signering af id-kort I anvendersystemet kan browserbaseret signering anvendes i stedet. Til dette kan følgende operationer anvendes:

### requestIdCardDigestForSigning

Denne operation svarer til ”login”. Svaret indeholder en URL som kan anvendes til at starte en browser-session.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#requestIdCardDigestForSigning

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

### getValidIdCard

Afgør om der findes et signeret id-kort.

Denne operation kan kaldes af anvendersystemet, f.eks. hvert sekund, mens brugeren signerer id-kortet i browseren.

Såfremt brugeren ikke signerer id-kortet alligevel, men f.eks. kommer til at lukke browseren ved en fejl, er det vigtigt at tillade at processen kan afbrydes, og at der kan foretages forsøg på signering påny.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#getValidIdCard

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

## Gateway Proxy

SOSI-GW’s gateway-operationen, som kaldes hver gang SOSI-GW skal viderestille til en NSP webservice, hedder **proxy**.

### proxy

Hvis der er et gyldigt, signeret id-kort I gateway’ens cache, vil denne metode viderestille til destinationen angivet i WsAddressing SOAP-headeren, eller til DCC, hvis informationen ikke findes i SOAP-headeren.

Hvis der ikke er et gyldigt signeret id-kort, vil en fejl blive returneret, indeholdende den samme information som returneres af **requestIdCardDigestForSigning**, dog placeret i en SOAP-header i response.

Bemærk at denne operation *ikke* findes i WSDL for SOSI-GW.

**Adresse** http://<host>:<port>/sosigw/proxy/soap-request

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1, 2, 3 eller 4

### Anvendelse af implicit login

Såfremt der anvendes browserbaseret signering er det også muligt helt at undlade at kalde **requestIdCardDigestForSigning**,

Hvis en NSP service forsøges kaldt igennem SOSI-GW med metoden **proxy** uden at der findes et signeret id-kort i SOSI-GW, vil der blive returneret en fejl i form af en DGWSFault. Denne indeholder fejlkoden "sosigw\_no\_valid\_idcard\_in\_cache", og der vil i svaret også findes en SOAP-header, som indeholder de samme data som **requestIdCardDigestForSigning** returnerer, blot i en header i stedet for i SOAP-body. Disse data kan anvendersystemet anvende til at åbne en browser, som beskrevet i afsnittet Browserbaseret signering.

Se venligst skemadefinition i "sosigw\_implicitLoginHeader.xsd" for en schemabeskrivelse for dette response.

## Logge ud af SOSI-GW

Ønskes at logge ud kan dette ske ved at fjerne signerede id-kort fra SOSI-GW’s id-kort cache. Følgende operationer kan anvendes:

### logout

Fjerner id-kort fra cache. Operationen kan kaldes når en bruger logger af et anvendersystem, og også ønsker at logge af SOSI-GW.

Vælges at kalde logout vil brugeren af anvendersystemet skulle logge på, dvs. signere id-kort igen, næste gang der foretages kald til NSP services.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#logout

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

### logoutWithResponse

Fjerner id-kort fra cache.

Denne operation er den samme som ovenfor, men der returneres ”ok” eller DGWSFault, afhængigt af om pågældende id-kort blev fjernet fra cachen eller ej.

**Adresse** http://<host>:<port>/sosigw/service/sosigw

**SOAP-action** http://sosi.dk/gw/2007.09.01#logoutWithResponse

**WSDL** sosigw.wsdl

**Namespace** http://sosi.dk/gw/2007.09.01

**SOAP-headers** DGWS id-kort sikkerhedsniveau 1

## Fejlkoder

Dette afsnit indeholder en liste med fejlkoder, som kan returneres fra SOSI-GW.

Bemærk at der også kan optræde andre fejlkoder I svar fra SOSI-GW, idet fejl fra STS og de NSP services der kaldes via **proxy** også returneres til anvendersystemet. Der henvises til dokumentationen for STS og øvrige NSP services såfremt der ønskes en komplet liste.

| Fejlkode | Beskrivelse |
| --- | --- |
| **sosigw\_no\_valid\_idcard\_in\_request** | Returneres hvis der mangler et UserIDCard i requestets SOAP-header. |
| **sosigw\_missing\_signinginfo\_in\_request**  | Retureneres hvis signeret digest eller certifikat mangler i kaldet til **signIdCard**. |
| **sosigw\_syntax\_error\_in\_request**  | Returneres når SOAP-headers ikke kan parses korrekt. |
| **sosigw\_awaiting\_signing** | Returneres af **getValidIdCard** når der er et id-kort i cachen, som endnu ikke er signeret. |
| **sosigw\_no\_valid\_idcard\_in\_cache** | Returneres når der ikke findes et id-kort i cachen som matcher nameID i input. |
| **sosigw\_internal\_error** | Generel fejlkode når der opstår uventede fejl. Se venligst serverens logfil for mere information.  |
| **sosigw\_proxy\_error** | Returneres hvis der opstår et problem med at kalde det ønskede endpoint gennem et **proxy** kald. |
| **sosigw\_access\_denied** | Kaldende klient eller service er ikke whitelistet. |

# Brug af SOSI-GW et delt miljø

SOSI-GW kan anvendes i et miljø som deles af mere end én organisation. I et delt miljø vil SOSI-GW og den omliggende infrastruktur[[1]](#footnote-1) partitionere id-kort cachen, hvilket sikrer at hver organisation kun har adgang til sin egen del af cachen.

Dette er implementeret på en måde, som ikke har indflydelse på det eksisterende SOSI-GW API og dennes dokumentation. Ligeledes er eksisterende brug af SOSI-GW upåvirket af dette.

## Brug af PassThrough-header

I et delt miljø går alle requests igennem SOSI-GW. Såfremt nogle requests skal videresendes af SOSI-GW uden ændringer, dvs. uden processering af request eller evaluering af id-kort, kan en ”PassThrough” SOAP header anvendes. Headeren indgår i SOSI-GW namespace (http://sosi.dk/gw/2007.09.01):

 <sosigw:PassThrough />

Requests med denne header vil få fjernet headeren, men vil ellers blive videresendt uændret af SOSI-GW til den specificerede destination.

## Brug af signerede id-kort i proxy-kald

Når alle kald går igennem SOSI-GW kan der være behov for at kalde Proxy med allerede signerede id-kort. Proxy interfacet er derfor blevet ændret, så beskeder indeholdende signerede id-kort sendes uændrede igennem SOSI-GW. Dette inkluderer niveau 2 id-kort (brugernavn og password), selvom disse teknisk set ikke er signerede.

SOSI-GW tillader nu alle id-kort niveauer, og proxy interfacet behandler de forskellige niveauer således:

Beskeder som videresendes *uden* udskiftning af id-kort:

* Requests med niveau 2 id-kort
* Requests med signeret niveau 3 og 4 id-kort

Øvrige beskeder behandles af SOSI-GW inden viderestilling:

* Requests med niveau 1 id-kort
* Requests med usigneret niveau 4 id-kort
1. Infrastrukturkomponenterne, der hentydes til her, indgår I NSP-operatørens nationale produktions- og test-miljøer. [↑](#footnote-ref-1)