

Stofmisbrugsdatabasen

Vejledning for opdatering af certifikat for systembruger v. NemLog-in

Version 1.5

Dato 07-01-2026

Esben Kramer v. Edora

Indhold

Introduktion	2
Modtagere	2
Baggrund	2
Overblik	2
Relevante koncepter	3
Mitld Erhverv og NemLog-in	4
Vejledning til udstedelse og opdatering af Systemcertifikat	4
Udstedelse af nyt Systemcertifikat	4
Udskiftning af certifikat for Systembruger v. NemLog-in	4
Opsætning af rullende skift til nyt certifikat og provisionering	4
Deploy af nyt Systembrugercertifikat	7
Koordinering	7
Hyppige spørgsmål	8

Introduktion

Alle begreber der er skrevet med stort, er forklaret i afsnittet Relevante koncepter.

Eksterne Systemer der kan sende data til Stofmisbrugsdatabasen (SMDB), skal kunne identificere sig overfor SMDB, som agerende på vegne af en organisation (som regel en myndighed) via NemLog-ins sikkerhedssystem, for at kunne indsende data for den myndighed. Som regel vil systembrugeren være oprettet af myndigheden.

NemLog-in systembrugere identificerer sig overfor SMDB med et Systemcertifikat, der udstedes via MitId Erhverv.

Systembrugeren og det tilhørende Systemcertifikat håndteres normalt af myndigheden, der bruger det eksterne system til at sende data til SMDB. Det er også muligt for leverandører af det Eksterne system at håndtere det via deres egen Systembruger, men det frarådes generelt, fordi de komplicerer relaterede sikkerhedselementer såsom fuldmagter fra andre myndigheder.

Dokumentet gennemgår hvordan der udstedes et Systemcertifikat, og en eksisterende NemLog-in Systembruger opdateres med certifikatet.

For information om hvordan en NemLog-in Systembruger oprettes og tildeles de nødvendige rettigheder, se da [Vejledning for Kommuner med Leverandør](#).

Modtagere

Modtagerne af dette dokument er MitId- og NemLog-in-ansvarlige i myndigheder, der bruger et eksternt system til at indberette data til SMDB.

Baggrund

Systemcertifikater udløber 3 år efter deres oprettelse. Derefter vil de ikke længere anses som gyldige, og de tekniske løsninger der beror på certifikatet, kan derefter ikke længere kommunikere sammen. Vejledningen antager at Eksterne Systemer benytter en Systembruger der udstedes og håndteres af myndigheden/organisationen selv, og ikke leverandøren af det Eksterne System.

Overblik

Processen ved udskiftning af Systemcertifikat kan overordnet nedbrydes til disse opgaver, der skal udføres i rækkefølge:

1. En ansvarlig hos myndigheden/organisationen anskaffer et nyt Systemcertifikat fra MitId. Leverandørerne af det Eksterne System bør kontaktes om at der skal foretages en fornyelse.
2. NemLog-in-administratoren angiver det nye Systemcertifikat som certifikatet der skal benyttes til Systembrugeren for Stofmisbrugsdatabasen.
3. Udviklings-ansvarlige for det Eksterne System integrerer det nye certifikat for Systembrugeren. Certifikatet skal overleveres fra Brugerorganisationens MitId-administrator, til firmaet der udvikler det Eksterne System.

Relevante koncepter

Her findes en liste over de begreber der bruges i vejledningen, med en tilhørende forklaring.

Brugerorganisation	Organisationen der i sidste ende anvender integrationen imod Stofmisbrugsdatabasen. Som regel vil både NemId og NemLog-in administratorer for organisationen være en medarbejder i denne organisation.
DST	Danmarks Statistik. Den ansvarshavende organisation for Stofmisbrugsdatabasen.
Eksternt System	Også kendt som <i>Fagsystem</i> . Her henvises til et system der kan sende og hente oplysninger til Stofmisbrugsdatabasen. Det dækker over en række forskellige programmer der bruges i bl.a. kommuner, til at indrapportere data til Stofmisbrugsdatabasen. Navnet dækker over, at det er et eksternt system for Stofmisbrugsdatabasen. Som eksempel dækker udviklerne af Eksterne Systemer over bl.a. KMD og Netcompany.
Integrationsmiljø	Test-specifikke versioner af Stofmisbrugsdatabasen og NemLog-in, der bruges i forbindelse med udvikling og verificering af tekniske løsninger. Som udgangspunkt kun relevant for udviklings-/drift-ansvarlige for et eksternt system.
MitId-administrator	Den ansvarlige for udstedelse af Systemcertifikater fra MitId Erhverv, på vegne af Brugerorganisationen.
NemLog-in-administrator	Ansvarlig for håndtering af bl.a. NemLog-in Systembrugere for et eksternt system. Hvor det eksterne system udvikles og driftes af en tredjepart, er det muligt at tredjeparten også varetager denne rolle via en fuldmagt. I dette tilfælde kan alle NemLog-in-specifikke opgaver udføres af tredjeparten.
NemLog-ins administration	NemLog-ins administrator-webportal
NemLog-in Systembruger	Type af bruger hos NemLog-in, særligt dedikeret til at sikre kommunikation fra et system til et andet (f.eks. fra et indberetningssystem til Stofmisbrugsdatabasen).
Privilegier	Specifikke rettigheder knyttet til Systembrugeren, der angiver hvilke muligheder et eksternt system har hos Stofmisbrugsdatabasen. Privilegier angives ved at anmode om dem via NemLog-in Administration, og tildeles endeligt efter godkendelse fra DST.
Produktionsmiljø	Den egentlige version af Stofmisbrugsdatabasen og NemLog-in. Adgang for Systembrugere til Stofmisbrugsdatabasens produktionsmiljø kan kun ske via NemLog-ins produktionsmiljø.
Systemcertifikat	MitId Erhverv-certifikat der repræsenterer et IT-system for en organisation. Det kan via NemLog-in knyttes til en NemLog-in Systembruger. Det erstatter funktionscertifikater i NemId.

MitId Erhverv og NemLog-in

Det er vigtigt at forstå forskellen på MitId Erhverv og NemLog-in. De to systemer håndterer i praksis to aspekter af samme overordnede sikkerhedsløsning, men har forskellige ansvarsområder.

MitId Erhverv står for at oprette brugere, der kan være både ansatte og systemer.

NemLog-in står for sikkerheden og omkring at logge ind på systemer med brugerne fra MitId.

I modsætning til MitId Erhverv for ansatte, håndteres rettigheder for en Systembruger i NemLog-in.

Eventuelle fuldmagter fra f.eks. en myndighed til et behandlingstilbud der skal agere på vegne af myndigheden, håndteres via MitId Erhverv.

Vejledning til oprettelse eller fornyelse af Systemcertifikat

Her gennemgås hvordan der helt konkret udstedes et nyt Systemcertifikat fra MitId, og det derefter opdateres for Systembrugeren i NemLog-in.

I MitId Erhverv oprettes der en certifikatprofil, der kan bruges til både at udstede eller forny et Systemcertifikat.

Fordi vejledningen hos MitId Erhverv kan skiftes uden at vi er opmærksomme på det, henviser vi til deres egne vejledninger, i stedet for at have en kopi direkte her i dokumentet.

Udstedelse af nyt Systemcertifikat

Udstedelsen skal foretages af MitId-administratoren.

Hvis det er første gang, f.eks. ved oprettelse af en ny NemLog-in Systembruger, er den mest opdaterede vejledning her:

<https://www.mitid-erhverv.dk/sadan-bruger-du-mitid-erhverv/administrer-certifikater/administrer-organisations-og-systemcertifikater/#bestilcert>

Fornyelse af eksisterende Systemcertifikat

Hvis du skal forny et eksisterende MitId Erhverv-certifikat, er vejledningen her:

<https://www.mitid-erhverv.dk/sadan-bruger-du-mitid-erhverv/administrer-certifikater/administrer-organisations-og-systemcertifikater/#fornycert>

Udskiftning af certifikat for Systembruger v. NemLog-in

Denne opgave skal foretages af NemLog-in-administratoren for brugerorganisationen, eller den tredjepart som har fået NemLog-in-administrator-rolle for brugerorganisationen via en fuldmagt.

Opsætning af rullende skift til nyt certifikat og provisionering

Rullende skift og provisionering er begreber i NemLog-ins Administration. De dækker over

Rullende skift: NemLog-in håndterer selv skift til et nyt Systemcertifikat når det gamle udløber.

Provisionering: Aktivisering af ændringer foretaget i NemLog-ins Administration.

Opsætningen udføres i NemLog-in Brugeradministration, hvor eksisterende Systembrugere findes via "IT-systemudbyder" i venstre side, og derefter i fanebladet "Systembrugere", som vist i Figur 1. Hvis der skal oprettes en Systembruger, benyttes linket "Tilføj systembruger", som kan ses nederst til venstre på Figur 1.



Figur 1: Visning af eksisterende Systembrugere i NemLog-ins Brugeradministration.

Trykkes der derefter på Systembrugeren der benyttes for Stofmisbrugsdatabasen, vises de tekniske detaljer for den valgte Systembruger, som vist på Figur 2. På denne side er det muligt at uploade/angive nye certifikater for integrations-/produktions-miljøerne, hvor det aktive certifikat efterfølgende automatisk vil blive udskiftet, så snart det eksisterende udløber.

Ændringerne lavet på denne side skal først gemmes via knappen "gem tekniske oplysninger", men vil derefter først blive aktive på henholdsvis integrations- og produktions-miljøet når der trykkes på de markerede links i venstre side ("Provisioner til integrationstest"/"Provisioner til produktion").

Vær opmærksom på at provisionerings-links i praksis fungerer som knapper, der starter provisionen med det samme efter de trykkes på, og altså ikke sender NemLog-in-administratoren videre til en anden side hvor det efterfølgende kan gøres. Sørg derfor for, at ændringerne er korrekte, før der provisioneres til produktion eller integration.

Som beskrevet i afsnittet Deploy af nyt Systembrugercertifikat, er det også nødvendigt for udvikleren af det Eksterne System at implementere det nye certifikat. **De skal derfor informeres om skiftet, og have det nye certifikat tilsendt.**

Det er også muligt at opdatere det gældende Systemcertifikat med det samme, ved at uploade dem under de aktive certifikater øverst i Figur 2, i stedet for under rullende skift.

Certifikaterne skal være af i formatet .cer for at kunne læses af NemLog-ins system.

NemLog-in/Administration

Sprog: Dansk English

Log ud

Hjem

Ventende opgaver

Hjælp

Hjem

EDORA A/S

Systembruger Detaljer

It-systemer

It-systemudbyder

It-leverandør

Løs opgaver

Provisioner til integrationstest

Provisioner til produktion

Anmod om adgang til webservice

Tekniske oplysninger

Navn

Test for Reference

Beskrivelse

Systembruger for WSC/WSP reference implementering.

Produktion

EntityId (Skal starte med https://wsc.)

https://wsc.saml.smdb.edora.dk

Signeringscertifikat

Vælg

Næste signeringscertifikat (rullende skift)

Mangler signeringscertifikat

Vælg

Sidste provisioneringsdato for produktionsmiljø

08-01-2020 12:56:17

Integrationstest

EntityId (Skal starte med https://wsc.)

https://wsc.saml.test.smdb.edora.dk

Signeringscertifikat

Vælg

Næste signeringscertifikat (rullende skift)

Mangler signeringscertifikat

Vælg

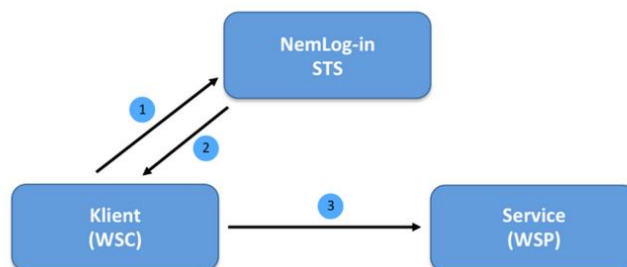
Sidste provisioneringsdato for integrationstestmiljø

04-02-2020 10:09:44

< Tilbage

Gem tekniske oplysninger

Figur 2: Tekniske oplysninger om Systembruger.



Figur 3: Service(WSP) er i dette tilfælde Stofmisbrugsdatasen, og Klient (WSC) er det Eksterne System.

Deploy af nyt Systembrugercertifikat

Denne opgave skal udføres af de udviklings-ansvarlige for det Eksterne System, da den præcise fremgangsmåde afhænger af hvordan certifikathåndteringen er implementeret. *Det er altså nødvendigt at kommunikere omkring certifikat-udskiftningen, med udviklerne af det Eksterne System.*

Medmindre det bliver relevant i samtalen med udviklerne, forventes det ikke at Brugerorganisationen selv (f.eks. kommuner), vil kunne bruge resten af dette afsnit direkte. Afsnittet er inkluderet for at lette kommunikationen omkring problemer med udviklerne af det Eksterne system, i tilfælde hvor det er relevant.

Hvis den oprindelige reference-implementationen stillet til rådighed via DST er benyttet som udgangspunkt for implementationen, vil certifikatet brugt for det eksterne system være importeret på servere/computere hvor det eksterne system afvikles, og være refereret fra konfigurations-filer i det eksterne system på en måde tilsvarende Figur 4.

```
<oiIdWSWcfConfiguration
  debugMode="true"
  stsEndpointAddress="https://SecureTokenService.test-nemlog-in.dk/SecurityTokenService.svc"
  tokenLifetimeInMinutes="5"
  wsbEndpointID="https://sts.saml.test.smbd.dst.dk/">
  <!-- The certificate used to identify the WSC. The issued token is based on this certificate. -->
  <!-- The consumer (WSC) application needs access to the private key of this certificate -->
  <clientCertificate
    storeLocation="LocalMachine" storeName="My"
    x509FindType="FindBySubjectName" findValue="CVR:34051178-FID:89344793" />
  <!-- The NemLog-in FOCES certificate used to verify the security token signature -->
  <stsCertificate
    storeLocation="LocalMachine" storeName="My"
    x509FindType="FindBySubjectName" findValue="CVR:34051178-FID:56940413" />
</oiIdWSWcfConfiguration>
```

Figur 4: Del af reference-implementering som henviser til fremsøgning af Systembruger, her kaldet "stsCertificate".

Vær opmærksom på at referenceimplementationen henter certifikatet ud fra Windows certifikatsystem, hvor det skal være importeret. Afhængigt af "subject" på det nye og gamle certifikat, kan det være nødvendigt at ændre "findValue" i konfigurationsfilen for det pågældende miljø. I sidste ende skal det nye Systembruger-certifikat være tilgængeligt for det Eksterne System og eventuelle referencer til certifikatet, hvis det ikke inkluderes eksplicit, skal være opdaterede.

Koordinering

Ved både manuel og rullende udskiftning af et fungerende certifikat, bør der koordineres imellem NemLog-in-administratoren og de ansvarlige for deploy af det nye certifikat, for at undgå unødvendig nedetid.

Hvis certifikatet udløber vil kommunikationen i trin 1 i Figur 3 **Fejl! Henvisningskilde ikke fundet.** fejle. Hvis certifikatet udskiftes i klienten før det udskiftes i NemLog-in STS, vil det også skabe fejl i trin 1. Ved kørende og fungerende systemer bør der tages højde for at minimere tiden imellem de forskellige punkter i opdateringsprocessen.

Hyppige spørgsmål

Her besvares nogle af de gængse spørgsmål, i forbindelse med udskitningen af Systembrugerens certifikat.

- Hvem skal i praksis bruge certifikatet?

Det nye certifikat skal kun bruges 2 steder:

1. *Det skal uploades til NemLog-in*
2. *Det skal udskiftes i det Eksterne System, der bruges til at sende og hente data til Stofmisbrugsdatabasen.*

DST har ikke brug for en kopi.

- Hvordan skiftes certifikatet i vores eget system?

Fordi der er mange forskellige måder systemerne kan være bygget på, kan en præcis fremgangsmåde ikke beskrives for alle. I nogle tilfælde kan det være nok at udskifte det gamle certifikat med det nye på serverne, og i andre tilfælde kan det kræve et nyt release med ændringer til systemet. Udviklerne af det Eksterne System vil kunne hjælpe med at definere og evt. foretage de nødvendige trin. Se Deploy af nyt Systembrugercertifikat.

- Hvorfor har vi ikke fået en advarsel omkring udløb af Systembrugerens certifikat?

I tilfælde hvor certifikatet for Systembrugeren ikke skal installeres på miljøer, men hvor det indgår direkte som del af et Eksternt System, vil certifikatets udløb som udgangspunkt ikke optræde på eventuelle alarmeringssystemer hos driftsafdelingen for systemet. Det kan overvejes at alligevel importere certifikatet i Windows Certificate Store eller lignende af den certifikat-ansvarlige, for at kunne se dets udløbsdato på samme vis som andre vigtige certifikater i organisationen.