Bilag 4: Blueprint om sikkerhed på sundhedsområdet

(Bilag til dagsordenspunkt 5: Arkitekturarbejdet på sundhedsområdet).

Signaturcentral

- Til anvendelse med EOJ

Version 0.95, oktober 2012

Udført af:

Signaturgruppen A/S
IT-huset
Åbogade 15
8200 Århus N.

Indholdsfortegnelse

1 Introduktion

Sektoren oplever, at stadig flere fællesoffentlige løsninger forudsætter anvendelse af medarbejdersignatur hos brugerne. Specielt indfasningen af fælles medicinkort (FMK) i Elektroniske Omsorgs Journals (EOJ) løsninger forventes at forøge antallet af brugere med medarbejdersignatur kraftigt.

Dette dokument beskriver integrationen af en brugervenlig og fleksibel medarbejdersignatur i EOJ løsningerne, således at medarbejdersignaturen ikke bliver en snublesten for ibrugtagning af FMK.

Ambitionen omkring en brugervenlig medarbejdersignatur som anvendes fleksibelt i forskellige arbejdssituationer er illustreret i nedenstående figur.

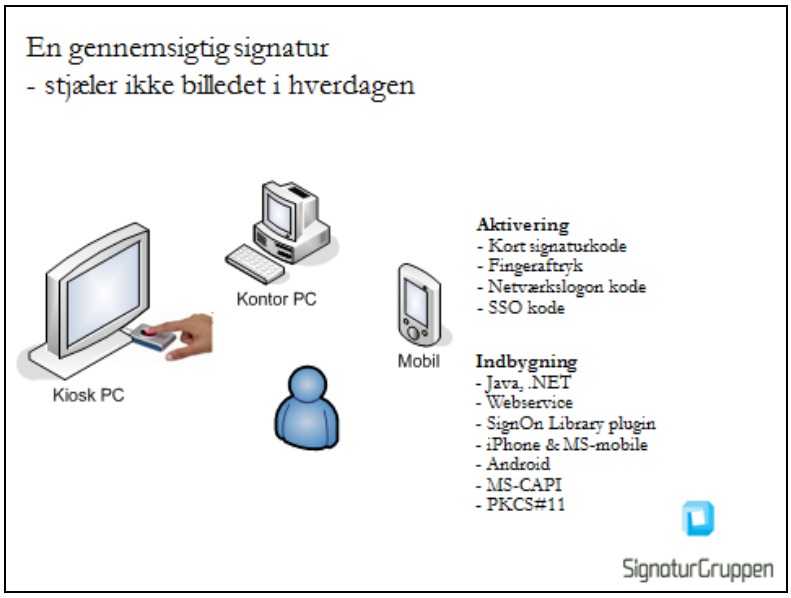

Fig 1: Anvendelse af samme medarbejdersignatur i forskellige arbejdssituationer

1.1 Den integrerede løsning set fra kunderne

EOJ med Signaturcentral kan opleves af kunderne som beskrevet herunder.

Nu hjælper EOJ dig både med fælles medicinkort oplysninger og en brugervenlig signaturløsning!

Det bliver nu muligt at få en brugervenlig medarbejdersignaturløsning integreret med EOJ.

Med Signaturcentralløsningen integreret i EOJ opnår I single sign on mellem EOJ og medarbejdersignaturen, således at hvad enten du skal anvende EOJ, og måske derigennem anvende medarbejdersignaturen til at læse fælles medicinkort, eller du anvender medarbejdersignaturen til at gå på sundhed.dk i en almindelig browser, så er det én og samme kode der giver adgang.

Den nye signaturløsning i EOJ tilvejebringer:

- *Medarbejdersignatur integreret i EOJ*
- *Automatisk fornyelse af medarbejdersignaturerne*
- *Automatisk backup af medarbejdersignaturer*
- *Administrators mulighed for at hjælpe ved glemt password hos brugeren*
- *Automatisk adgang til medarbejdersignatur fra alle arbejdspladser på lokalnettet hvor Signaturcentral klient softwaren er installeret (option)*
- *Automatisk adgang til medarbejdersignatur fra mobile enheder med EOJ applikationen (option)*

- *Automatiseret administration af medarbejdersignatur*
- *Mulighed for at anvende medarbejdersignatur i Citrix løsninger (option)*
- *Mulighed for at anvende medarbejdersignatur fra mobile devices*

1.2 Den integrerede løsning – fordele for EOJ leverandøren

Med integration af Signaturcentral får EOJ-leverandøren en ensartet grænseflade til at integrere og supportere medarbejdersignatur.

- Kunder, som har en Signaturcentral i forvejen, kan opgraderes til EOJ understøttelse. Det vil være enklest at anvende AD både til brugeradministration og autentifikation for både EOJ og signatur, da dette er situationen for de øvrige signaturbrugere hos kunden.
- Kunder, som har en anden medarbejdersignaturløsning, og ikke ønsker at anvende Signaturcentral generelt, kan vejledes i at indlægge medarbejdersignatur i Signaturcentral, således at EOJ har fuld kontrol over de brugere, som skal have adgang til fælles medicinkort. I dette scenarie kan man vælge enten EOJs interne brugeradministration/autentifikation eller AD.
- I alle tilfælde får EOJ en ensartet integrationsgrænseflade og brugerfunktionalitet, således at der er gennemsigtig understøttelse af EOJ på kontor computere, kiosk computere (flerbrugersystemer) og mobile devices med fuld roaming og samme medarbejdersignatur og passwords.
- Det er stadig muligt at opdele EOJ brugere i en gruppe som ikke behøver FMK adgang og en anden gruppe som skal have FMK adgang. De tilhørende brugeradministrationsløsninger skal i så fald kunne signalere/skelne dette i forhold til automatiseringen af signaturadministration.
- Anvendelse i Citrix understøttes transparent for brugerne.

2 Løsningsvarianterne EOJ DB og AD

Integrationen kan etableres i to forskellige hovedvarianter:

Én hvor brugeradministration og autentifikation foregår i EOJ og én hvor brugeradministration og autentifikation foregår i AD.

Såfremt kunden ønsker at anvende Signaturcentral generelt til alle medarbejdere, opnås den simpleste løsning og supportsituation, såfremt AD anvendes til brugeradministration og autentifikation.

Det opstillede design understøtter dog, at organisationer kan vælge at tilbyde sine brugere at anvende medarbejdersignatur i EOJ med EOJ bruger-ID og password og samtidig anvende samme signatur udenfor EOJ med AD bruger-ID og password.

Administrationen af brugerne er delt i to, for at understøtte at EOJ administratorer ikke alle steder også er LRA administrator for organisationen. Dermed kan man som LRA bulk-udtrække brugerændringer f.eks. én gang om dagen.

Herunder beskrives centrale flows i de forskellige varianter.

2.1 Separat administration af brugere i EOJ og på DanID LRA

Den helt afkoblede måde at administrere brugerne på anbefales ikke, på grund af fejlmuligheder og tilhørende support. Den kan dog teknisk godt lade sig gøre.

2.2 Med integration af brugeradministration i AD

Dette foregår analogt til beskrivelsen for EOJ herunder.

2.3 Med integration af brugeradministration i EOJ

Såfremt kunden anvender EOJ til administration af brugere, og gerne vil sammenkæde vedligeholdelsen af de tilhørende medarbejdersignaturer hermed, kan der etableres en ”Adm grænseflade” som beskrevet herunder.

Signaturcentral understøtter også en integration med brugeradministration i AD, således at oprettelser, ændringer og spærringer af medarbejdersignatur kan opstartes automatiseret herfra.

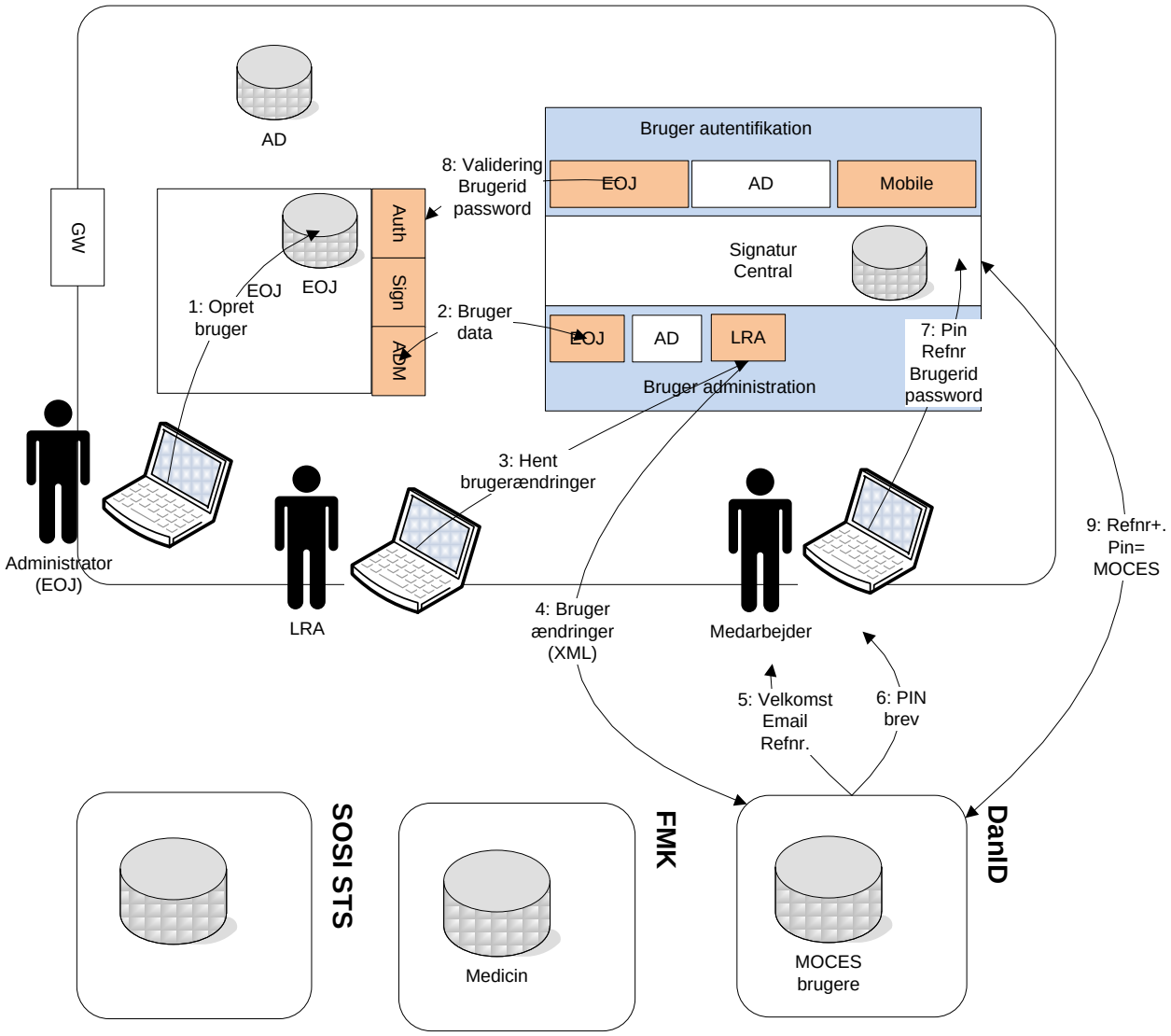

Fig 2: Oprettelse og udstedelse af signatur i lokal EOJ løsning

1. EOJ administrator opretter, ændrer eller spærrer medarbejder i EOJ brugerdatabasen med EOJ brugeradministrationsløsningen
2. EOJ sender brugerændringer til Signaturcentral. Signaturcentral sammenligner EOJ brugerdata med intern signaturstatus og forbereder bulk-ændringsfil (XML).
3. Organisationens LRA notificeres pr. mail om brugerændringer dagligt. LRA åbner browser og logger ind i Signaturcentral med (LRA) MOCES. LRA kan vælge om der skal laves straksudstedelse eller alm. PIN brevs udstedelse.
4. LRA og redirigeres til DanID med ændringsdata i XML fil.
5. Ved oprettelse af medarbejdersignatur sender DanID velkomst email til brugeren med referencenummer.
6. DanID sender PIN brev til brugeren. Alternativt vælger LRA straksudstedelse og får PIN koden oplyst på skærmen til overdragelse til medarbejderen.
7. Brugeren klikker på linket i velkomst emailen og åbner en webside på Signaturcentral, hvor der indtastes PIN kode fra pinbrevet samt EOJ brugernavn og password (Hvis organisationen både anvender EOJ og AD autentifikation til anvendelse af MOCES i EOJ og generelt, konfigureres løsningen således, at brugeren valgfrit kan angive bruger-ID og passwords for både EOJ og AD).
8. Signaturcentral validerer, at EOJ brugernavn og password er korrekt. (Hvis både EOJ og AD vælges af brugeren, valideres begge sæt brugernavne og passwords)

9. Signaturcentral genererer brugerens signaturnøgler og sender certifikat request til DanID sammen med referencekode og PIN kode. DanID returnerer certifikat.

2.4 Med integration til brugervalidering i AD

EOJ kunder som anvender AD til brugervalidering, kan også integrere Signaturcentral til AD og således opnå password synkronisering.

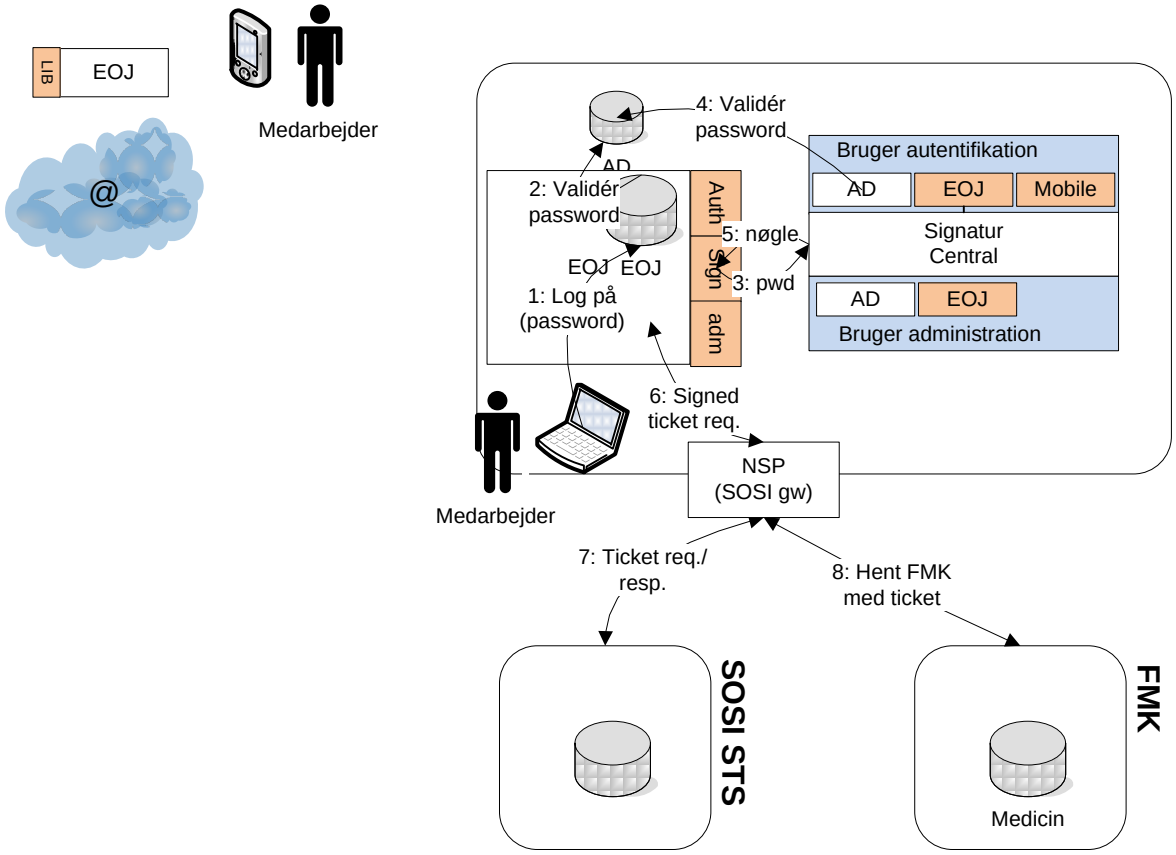

Fig 3: Anvendelse med EOJ autentifikation

1. Bruger indtaster AD password i EOJ klient (EOJ har kontrolleret i egen DB eller hos SC om certifikat fornyelsestekst skal vises for bruger ved logon)
2. EOJ validerer evt. selv AD password
3. EOJ anvender Sign lib til at sende signtext og brugerid samt password til signaturcentral
4. Signaturcentral validerer brugerid og password i AD
5. Signaturcentral returnerer PKCS#12 til signering af signtext
6. EOJ sender signtext og SOSI ticket request til SOSI gw
7. SOSI ticket udstedes
8. FMK data hentes

2.5 Med integration til brugervalidering i EOJ

EOJ kunder som anvender lokalt administreret brugernavn og password i EOJ til brugervalidering, kan også integrere Signaturcentral til EOJ og således opnå password synkronisering. Flowet er analogt til brugervalidering i AD, som beskrevet ovenfor.

2.6 Straksudstedelse

Der understøttes straksudstedelse af medarbejdersignatur, således at LRA kan vælge at få vist brugerens installationspinkode i sin browser-session mod DanID. Denne pinkode skal overdrages til slutbrugere på en sikker måde.

Af DanIDs vilkår for dette fremgår: ”*Såfremt koden udleveres direkte til medarbejderen, skal virksomheden sikre, at udleveringen sker på betryggende vis, og at medarbejderen kvitterer for modtagelsen. Virksomheden skal sørge for, at kvitteringen for modtagelse registreres/logges, og at der periodisk foretages audits heraf. Audits skal gennemføres af virksomhedens ledelse eller af en af ledelsen udpeget person (ikke administrator). Nets DanID kan til enhver tid bede virksomheden dokumentere at procedurerne følges, og at audits er gennemført.*”

Signaturcentral understøtter organisationen i at opfylde dette ved at:

- LRA inddaterer installationspinkode + brugerID på Signaturcentral
- Medarbejder logger ind på Signaturcentral udstedelsesside med brugerID og password
- Signaturcentral validerer brugerID og password og fremfinder på basis heraf referencenummer og installationspinkode som anvendes til certifikatudstedelse mod DanID
- Medarbejderen kvitterer for modtagelse af pinkode under selve certifikatudstedelsen på Signaturcentral
- Signaturcentral tilbyder en log over udstedelser på signaturcentral, som kan danne basis for ledelsens periodiske audits.

2.7 Brugere uden email

Det vurderes, at nogle organisationer har EOJ brugere, som ikke anvender email i deres arbejde. Der planlægges derfor også en registreringsløsning, som ikke forudsætter anvendelse af email adresse. Dette foregår i praksis som en straksudstedelse, hvor LRA efterfølgende inddaterer installationspinkode og bruger-id på brugeren i signaturcentral, hvorefter brugeren notificeres om at logge på signaturcentral udstedelsessiden og autentificere sig med bruger-id og password.

Velkomst email fra DanID sendes til en fælles postkasse, med brugernavnet indkodet i email adresse, således at Signaturcentral kan hente denne mail og parse referencenummeret ud herfra.

2.8 Certifikat udstedelse direkte i EOJ klient

Der stilles en webservice til rådighed på Signaturcentral, som muliggør at al brugerdialogen holdes i EOJ klienten, også selve certifikatudstedelsen hvor de nødvendige informationer fra brugeren vil kunne udveksles via webservice. Der er i så tilfælde behov for at vise accept af kundevikår samt certifikat indhold efter udstedelse i et EOJ GUI.
Dette kan muliggøre at nogle brugere f.eks. kun arbejder fra mobile terminaler og ikke er afhængige af at have en browser på LAN ved certifikatudstedelse.

2.9 Med understøttelse af mobile devices uden VPN adgang til LAN

Sikkerhedsløsningen vil omfatte en intiel registrering af mobil device hos kunden (ved hjælp af en registreringsapplikation som Signaturgruppen tilvejebringer), hvor der placeres en softwarenøgle på devicen. Signaturgruppen leverer et autentifikationsbibliotek til indbygning i forretningsapplikationerne, som kan signere en token omfattende brugerens indtastede brugernavn og password, således at autentifikationen omfatter noget man ved (brugernavn og password) og noget man har (mobil device med softwarenøgle). EOJ og Signaturcentral skal tilpasses til begge at kunne validere den udvidede brugerautentifikation af disse brugere.

Den initielle registrering af et device til den interne brugeridentitet omfatter følgende komponenter:

1) Device med Signaturgruppens SIB app/lib
2) SIB mobile device administration modul
3) Superbruger

Registreringen indeholder følgende trin:

1) Signaturgruppens SIB app/lib installeres på devices som ønskes godkendt til fjernadgang
2) Superbruger starter SIB app på device.
3) App’en registrerer, at devicet endnu ikke er sammenkædet og genererer en signeringsnøgle.

4) App'en indsender offentlig nøgle til SIB. (Og der vises en registrerings-pinkode på devicet (4-cifre) som superbrugeren aflæser).
5) Vha. en pc på det interne netværk logger Superbrugeren ind på SIB mobil device administrationsmodulet. Her vises en side med devices til godkendelse af sammenkædning. (Superbrugeren bekræfter sammenkædningen ved at indtaste pinkoden fra 4).

2.9.1 Anvendelse af device

Anvendelse af medarbejdersignatur fra en registreret device foregår som illustreret herunder:

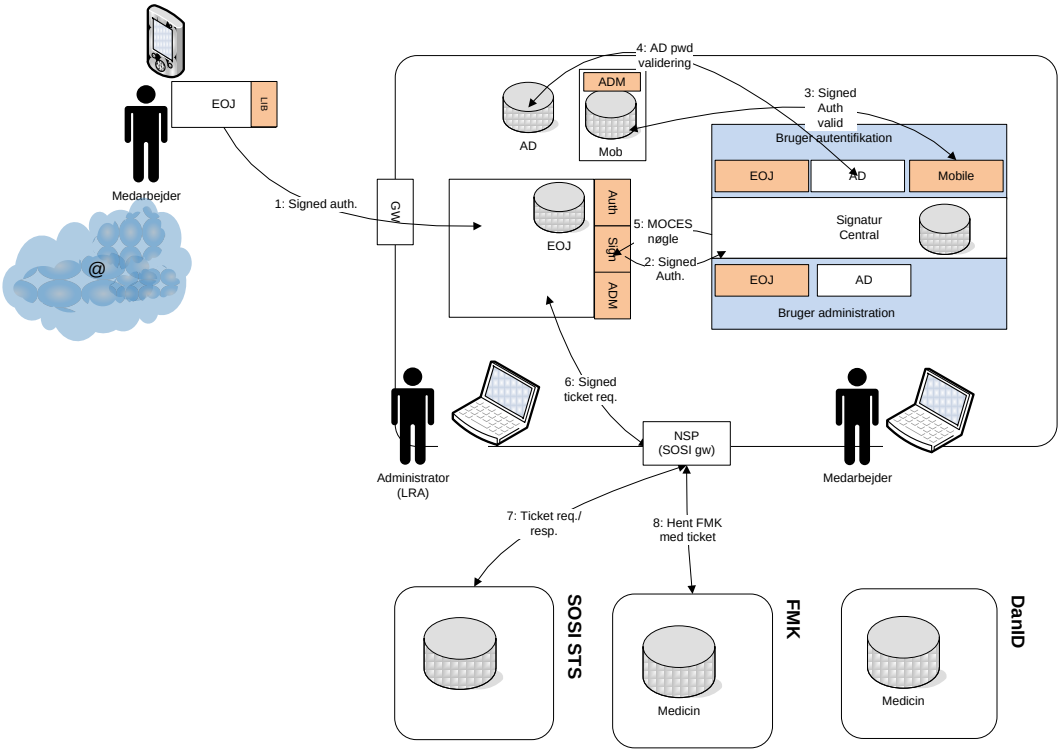

Fig 4: Anvendelse med mobile device uden VPN

2.9.2 Administration af devices

Devices administreres af medarbejdere og superbrugere.

Superbruger

- Registrér nyt device
- Spær device
- Se registrerede devices og historik

3 Leverancer fra Signaturgruppen i projektet

Signaturgruppen deltager med følgende leverancer:

1. Signaturcentral server og klient software.
2. Løsningsarkitektur (videreudvikling af dette dokument og tilhørende afklaringer).
3. Udvikling af EOJ integrationskomponenter til Signaturcentral.
4. (iOS, Android og Windows ? bibliotek til integration i EOJ applikation.)
5. Deltagelse i integration, aftestning og pilotprojekt

Forudsætninger til EOJ

1. (Webservice) grænseflade til at validere om en EOJ bruger ID og password er korrekt.
2. (Webservice) grænseflade til udtrække/notificere til Signaturcentral ved brugeradministration i EOJ
3. Implementering af procedurer ved administration af brugere, herunder reset af password etc. i henhold til certifikat politik krav om, at kun slutbrugeren kender password.
4. Evt. integration af løsning til mobil adgang fra Internet (uden VPN).

4 Appendix A: Usecases EOJ Signaturcentral.

Herunder gennemgås de forskellige usecases. Nedenstående figur giver et overblik over de forskellige interessenter og deres usecases.

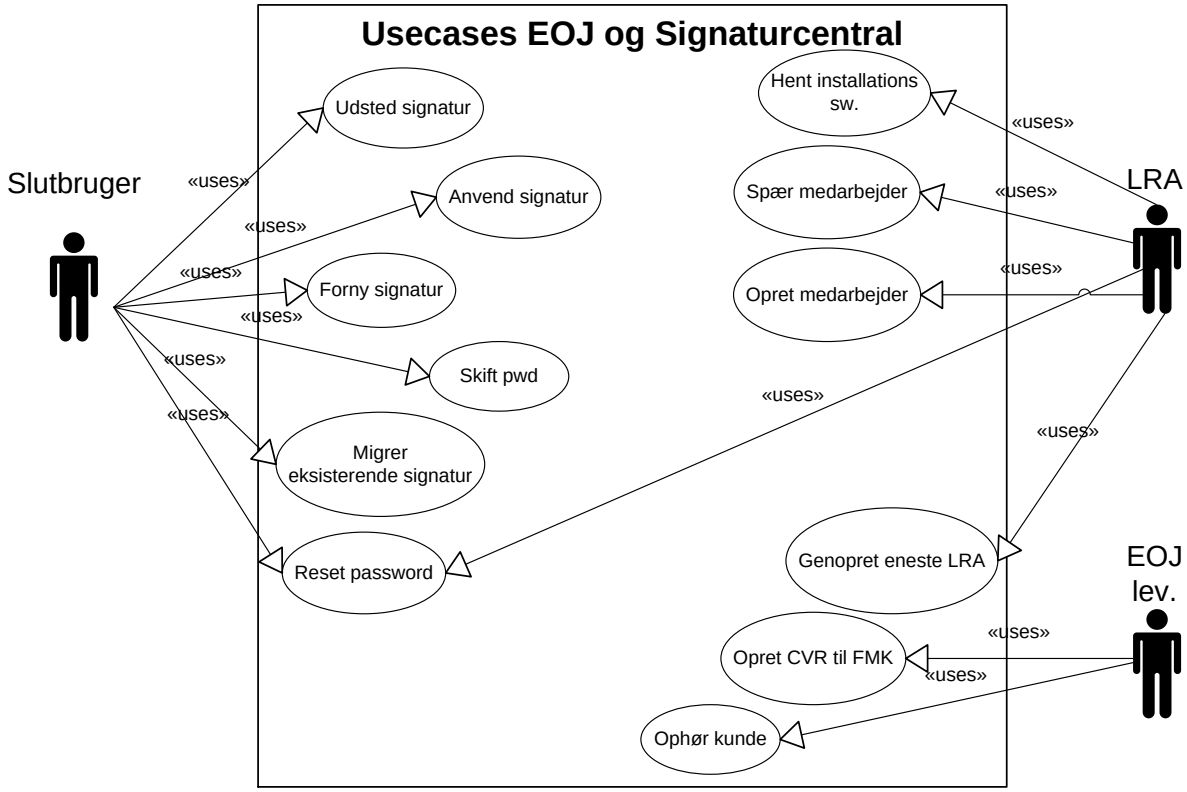

Fig 4: Usecases

4.1 EOJ lev.

4.1.1 Opret CVR til FMK

4.1.1.1 Brugeradministration og autentifikation i EOJ

Det forudsættes, at CVR enheden allerede har en LRA med en lokalt installeret signatur.

1. Administrator vejledes i at uploade LRA signatur til Signaturcentral, hvis den ikke allerede er der. Ved upload af LRA signatur indtaster administrator sin eksisterende kode til signaturen, og derudover den nye personlige kode i EOJ.
2. Signaturcentral verificerer den nye EOJ kode mod EOJ brugerbasen og indlægger herefter signatur i signaturcentral.

4.1.1.2 Brugeradministration og autentifikation i AD.

1. EOJ og Signaturcentral installeres hver for sig og konfigureres op mod AD.
2. Administrator vejledes i at uploade LRA signatur til Signaturcentral, hvis den ikke allerede er der. Ved upload af LRA signatur indtaster administrator sin eksisterende kode til signaturen, og derudover AD kode.
3. Signaturcentral verificerer AD kode og indlægger herefter signatur i signaturcentral.

4.1.2 Hent installations sw

Hjemmeside hvor administrator kan hente en Signaturcentral klient installationspakke. Dette er kun relevant såfremt brugerne skal anvende medarbejdersignaturen fra Signaturcentral generelt på websites.

4.1.3 Spær medarbejder

Luk bruger i EOJ/AD administration og initiér automatisk spærring af certifikat hos DanID via Signaturcentral.

4.1.4 Opret medarbejder

Se fig 2.

4.2 Slutbruger

4.2.1 Udsted signatur

1. Modtag velkomst email fra DanID
2. Modtag pinbrev fra DanID.
3. Log på Signaturcentral klient og indtast pinkode fra pinbrev samt EOJ eller AD brugerID+password til ny signatur

Se fig. 2

4.2.2 Anvend signatur

Som beskrevet i fig. 3

4.2.3 Forny signatur

Såfremt signaturen anvendes indenfor fornyelsesperioden fra en signaturcentral klient, opdager klienten at der skal ske fornyelse og prompter brugeren herfor i forbindelse med almindelig signaturanvendelse.

Fig 5: Eksempel på fornyelse dialog.
Kan også indbygges som et "afkrydsningsfelt" i den eksisterende brugerdialog ved logon.

Ved anvendelse af signaturen via EOJ klienten, bør GUI også prompte for fornyelse, hvis vi er indenfor fornyelsesperioden. EOJ leverandøren skal undersøge, hvorledes EOJ klienten kan detektere dette. Dette kan evt. være ved fremsøgning af certifikat eller ved anden (batch) opdatering af fornyelsestidspunkter jf. aktuelle certifikater.

4.2.4 Skift password

Slutbruger ændrer password via EOJ klient eller via AD.

4.2.5 Reset password

Reset af password skal indrettes således, at kun slutbrugeren kender den kode som kan aktivere digital signatur.

4.2.6 Importér sw signatur

1. Bruger vejledes i at uploade signatur til Signaturcentral. Ved upload af signatur indtaster bruger sin eksisterende kode til signaturen, og derudover den nye personlige kode til EOJ/AD.
2. Signaturcentral verificerer den nye EOJ kode mod EOJ/AD og indlægger herefter signatur i signaturcentral.
3. Alternativt kan der gennemføres en fornyelse, hvor den eksisterende signatur anvendes til at udstede en ny signatur til medarbejderen, som placeres på Signaturcentral. Dette er blevet den foretrukne metode i de fleste migreringer.