Teknisk beskrivelse af SmartSignatur

- og integration af NemID medarbejdersignatur

Version 3.0.1 - september 2016

SmartSignatur

Kontaktoplysninger

Liga Software ApS
International House
Center Boulevard 5
2300 København S

Telefon 35 36 95 05
Web www.smartsignatur.dk
Mail post@smartsignatur.dk

Kommentarer til dette dokument kan sendes til Bjarke Alling, ba@smartsignatur.dk

Indhold

Indledning

Afskaf password og gør hverdagen enklere

SmartSignatur hjælper medarbejdere med at kunne legitimere sig selv digitalt
Mere og mere lovgivning kræver, at medarbejdere legitimerer sig digitalt. Det er besværligt, hvis det skal gøres sikkert. Men SmartSignatur gør det let og sikkert på samme tid. Det skaber nye muligheder.

SmartSignatur gør det let for den person, der skal legitimere sig
Med nuværende, sikre løsninger skal man typisk logge ind med besværlige ekstrakoder hentet fra papkort, kodegenerator eller per SMS. Det er besværligt.

Afskaf passwords
Med SmartSignatur kan man nøjes med en simpel pinkode. På den måde sparer medarbejderne tid og besvær – uden at virksomheden går på kompromis med sikkerheden.

SmartSignatur holder en høj sikkerhed
Selv om SmartSignatur er enkelt og brugervenligt, går SmartSignatur ikke på kompromis med sikkerheden. Det kan lade sig gøre, fordi SmartSignaturs unikke løsning kobler virksomhedens eget brugersystem sammen med det danske NemID system til medarbejdersignaturer.

Den digitale hverdag for medarbejdere er kompleks. Hverdagen skal være både let, men samtidig sikker.

SmartSignaturs løsning overholder Digitaliseringsstyrelsens regelsæt for udstedelser og adgangskoder til medarbejdersignatur.

Åbne standarder
SmartSignatur Server er bygget på åbne internationale software standarder. Derved forhindres vendor lock-in og let tilpasning til fremtidige behov er sikret

SmartSignatur udsteder og vedligeholder automatisk de digitale medarbejdersignaturer
SmartSignatur er sammenkædet med virksomhedens eget brugersystem. Det giver en række fordele for virksomheden: Medarbejderne kan let identificere sig selv digitalt – også over for tredjepart uden for virksomheden.

Samtidig bliver brugeradgange og -rettigheder automatisk lukket, når medarbejdere fjernes fra det interne brugersystem. Tilsvarende bliver de opdateret, når medarbejderes navne, stamdata eller interne roller forandrer sig. Det sparer tid og kræfter både hos it-afdelingen og hos den enkelte medarbejder.

SmartSignatur overblik

SmartSignatur server gør livet lettere for medarbejderne - og øger sikkerheden for organisationen. SmartSignatur adskiller sig fra andre produkter ved at bygge på en mere robust og sikker it-arkitektur. Vi bygger på sikre standardkomponenter og tilpasser løsningen efter organisationens behov.

Det er administrativt dyrt og teknisk vanskeligt at håndtere NemID medarbejdercertifikater på enkeltstående computere. Derfor har vi skabt SmartSignatur server - en central signaturserver, som er integreret med Nets DanID og kundens øvrige it-infrastruktur.

SmartSignatur Card & Client er den decentrale, individuelle del af SmartSignatur, der sikrer en let, lokal håndtering af NemID medarbejdersignatur - eller andre digitale signaturer.

Med SmartSignatur på pc'en har den enkelte bruger altid NemID tilgængelig på sit enhed, for eksempel sin PC eller tablet, og det betyder, at man kan anvende sin NemID medarbejdersignatur uden at skulle bruge nøglekort eller central server opkobling.

SmartSignatur Mobile SDK er et udviklingsværktøj til Apple iOS programmører. Med dette værktøj er det ganske let, at udvikle yderst sikre iOS apps baseret på certifikater og tilhørende private nøgler læst fra smart cards via en tilsluttet smart card læser.

Digital signatur

En digital signatur er en elektronisk underskrift, som gør det sikkert for at sende fortrolige og følsomme oplysninger via internettet.

For kommuner, regioner og virksomheder kan anvendelse af digital signatur forøge service, kvalitet og sporbarhed i kommunikationen med den offentlige sektor og desuden gøre handel på internettet mere sikker.

Kilde: http://www.digst.dk/Loesninger-og-infrastruktur/Digital-signatur

En digitalt signatur har mange anvendelsesmuligheder

- Adgangskontrol & brugervalidering:
  - Browser adgang til offentlige og interne web systemer.
  - Windows- og netværkslogin til eksempelvis Cisco, Citrix, Terminal Service & VDI.
  - Fysisk bygningsadgang mv.
- Digital underskrift og attestering:
  - PDF filer & MS Office med kontrakter, afgørelser, tilladelser mv.
  - Fagapplikationer til godkendelse af bilag, journaler, tilsyn, recepter mv.
- Kryptering af data:
  - Harddiske, filer og emails.

Historien

Ideén med SmartSignatur begyndte tilbage i 2004 med forgængeren til SmartSignatur server, som hed ”Novell OCES Certificate Manager” (OCES betyder Offentlige Certifikater til Elektronisk Service) og senere blot LCES (Local Certificate Enrollment Service). LCES blev udviklet i samarbejde med det daværende Århus Amt, Novell (senere NetIQ), Cryptovision og TDC tilbage i 2005 og 2006.

I 2013 blev Liga ApS (mangeårig Novell/NetIQ/SUSE samarbejdspartner) opfordret til at videreudvikle og opgradere den gamle LCES løsning til den nye MOCES2 standard. I 2014 blev produktet SmartSignatur introduceret og alle de ”gamle” eksisterende kunder blev opgraderet til den nye SmartSignatur server version. I dag er SmartSignatur et produkt og varemærke i selskabet Liga Software ApS.

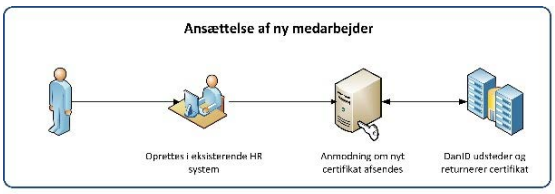
SmartSignatur produktet

I takt med den stigende digitalisering af den offentlige forvaltning stiger kravene til anvendelsen af medarbejdersignaturer også i erhvervslivet. Mange virksomheder tvinges imidlertid til at holde implementering samt brug af medarbejdercertifikatet på afstand, da det er vanskeligt at administrere og vanskeligt at anvende.

Virksomheder med behov for anvende certifikater vælger at minimere den medfølgende kompleksitet ved at implementere virksomhedscertifikater (VOCES), for så blot at løbe ind i andre problemer. Eksempelvis er virksomhedssignaturerne ikke personlige og kan derfor ikke anvendes i en række sammenhænge. Når et virksomhedscertifikat skal tilbagekaldes – f.eks. på grund af en sikkerhedsbrist - er det problematisk, at det vil påvirke alle brugere og ikke kun en enkelt person.

Se mere om de forskellige certifikattyper her: *http://www.nets.eu/dk-da/Produkter/Sikkerhed/Virksomhedssignatur/Pages/Ofte-stillede-spoergsmaal.aspx*

Nogle virksomheder vælger at implementere forskellige “gateway-løsninger” til certifikathåndtering i forbindelse med e-mail og andre funktioner, men det løser ikke problemet med adgang til certifikatet, der hvor brugeren og alle dennes applikationer er – nemlig på brugerens PC.

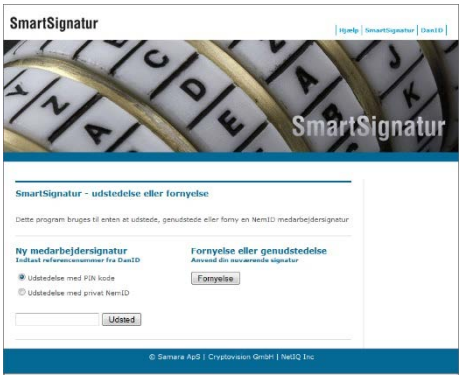


Automatiserer administration og letter anvendelsen af certifikater

Med SmartSignatur kan hele processen automatiseres, lige fra bestilling og udstedelse til opbevaring og installation. Ved at anvende Nets DanIDs SOAP interface kan en brugeroprettelse eller andre ændringer i et f.eks. Active Directory automatisk medføre en udstedelse af et medarbejdercertifikat. SmartSignatur kan også fungere uden SOAP ved hjælp af en manuel oprettelse af brugeren i selvbetjeningsportalen. Nets DanID forbereder herefter – som normalt -

selve certifikatudstedelsen og fremsender en personlig e-mail med referencenummer til certifikatudstedelsen, samtidigt med at den personlige PIN-kode fremsendes per post eller via straks aktivering via enten PIN kode eller med brugerens personlige NemID (dette kræver CPR tilknytning).

I SmartSignatur løsningen peger den medsendte URL ikke længere på Nets DanIDs hjemmeside, men i stedet for på den lokale SmartSignatur Server. Udgangspunktet er brugerens netværkslogon og enten den PIN-kode som brugeren har modtaget per post, fået overdraget eller brugerens personlige NemID. SmartSignatur Server kommunikerer herefter direkte med Nets DanID om udstedelse af medarbejdercertifikatet på samme måde, som det ellers vil foregå på manuel vis. Forskellen er, at i stedet for at medarbejdercertifikatet kun installeres på brugerens egen PC, bliver certifikatet i stedet bragt til en sikker og central opbevaring i den indbyggede database. Databasen er en specialiseret og sikker database der er særligt velegnet til opbevaring af certifikatet.



SmartSignatur server er en web baseret applikation som afvikles internt hos kunden.

Når brugeren fremover logger på en PC med sit netværkslogin, bliver det indtastede bruger-ID og password via SmartSignatur Client brugt til at give adgang til brugerens eget medarbejdercertifikat i databasen, hvorefter det automatisk kopieres til den aktuelle PC hvor brugeren og brugerens applikationer befinder sig. Samme service er ligeledes i stand til automatisk at fjerne medarbejdercertifikatet hvis det ønskes.

Sikkerhed og brugervenlighed er indbygget

SmartSignatur server letter anvendelsen af medarbejdercertifikater uden at gå på kompromis med sikkerheden. Adgangen til medarbejdercertifikatet sker med brugerens eget netværkspassword, som via en central passwordpolitik bringes i overensstemmelse med passwordkravene til certifikatet, og brugerens password til netværket vil fremover være det eneste password, der giver adgang til brugerens certifikat.

Medarbejdercertifikatet opbevares i databasen tilknyttet til det individuelle brugerobjekt, og ikke engang en administrator vil kunne ændre brugerens password for derefter at logge ind som brugeren og selv få adgang til certifikatet. Det er vigtigt for at overholdelsen af den Offentlige OCES-certifikatpolitik

Hvis virksomheden ønsker det, kan brugeren dog også sættes i stand til selv at skifte sit password eller måske modtage et passende ”password tip”, hvis brugeren har glemt sit password via SmartSignaturs password selfservice applikation.

Kan automatisere livscyklussen for både bruger-identiteter og certifikater

SmartSignatur server indeholder en brugerstyringskomponent, der muliggør en automatisering af brugeroprettelse og administration, som i realtid udsteder eller eventuelt tilbagekalde certifikater. Det hele afhængigt af virksomhedens politikker og medarbejdernes roller. Ved hjælp af en web-

baseret grafisk brugergrænseflade defineres virksomhedens processer, regler og sikkerhedspolitikker omkring bruger- og certifikatadministration, som efterfølgende automatisk omsætter dette til de tilsvarende brugeradministrative handlinger.

Med den indbyggede teknologi er det muligt for SmartSignatur server, at stille en komplet livscyklushåndtering af såvel bruger-identiteter som deres certifikater til rådighed. Løsningen kan således udvides til f.eks. at registrere en nyansættelse i et HR-system eller en brugeroprettelse i andre autoritative applikationer, til automatisk at oprette et bruger-ID på relevante applikationer og iværksætte en certifikatudstedelse. Når den pågældende medarbejder senere fratræder sin stilling, vil denne ændring igen blive afpsejlet i de samme autoritative systemer, som igen – automatisk - stopper for adgangen til den pågældende medarbejders certifikat.

Udfordringer ved NemID medarbejdersignatur manuel installation

- Certifikater er kun installeret på den enkelte PC.
- Eksport og import er muligt, men kræver en manuel proces som ofte ligger ud over kompetencen hos den almindelige slutbruger
- Malware kan stjæle medarbejdersignaturen fra den lokale PC via den indbyggede eksportfunktion
- Password på certifikat er forskelligt fra brugerens PC
- Genudstedelse af certifikat er påkrævet hvis password er glemt og medfører ventetid uden at brugeren har et certifikat
- Nets DanID selvbetjenings portal kræver, at virksomheden skal genindtaste alle bruger oplysninger
- Omkostningen til manuel administration af medarbejdercertifikater er typisk meget store. En supportmedarbejder til 400-600 certifikater.

Funktioner i SmartSignatur server

- Automatisk udstedelse/administration af certifikater
- Central og sikker opbevaring af certifikater – forhindrer uautoriseret adgang til et vilkårligt medarbejder certifikat
- Avanceret password administration, med mulighed for selvbetjening som overholder OCES certifikatpolitikkens passwordkrav
- Realtids integration til både Microsoft Active Directory og Micro Focus eDirectory
- Automatisk installation på Windows PC, Citrix, VDI eller på chip smartcard
- Indbygget overvågning og rapportering
- Tilgang til brugerens certifikater og nøgler via standard SOAP eller LDAP API
- Komplet livscyklus-styring af brugere og certifikater

Fordele i SmartSignatur server

- Inkluderer alle nødvendige softwarelicenser
- Muliggør fuldt automatiseret certifikatudstedelse, opbevaring og installation
- Sammenbygget med eksisterende brugersystem (Active Directory og eDirectory)
- Sikrer at brugerens certifikat altid er tilgængelig på den enhed brugeren anvender
- Muliggør single sign-on til både desktop og netværk
- Styrker virksomhedens passwordpolitik
- Første trin i en komplet afskaffelse af passwords i ens organisation
- Giver brugerne adgang til en selvbetjeningsportal for passwords
- Beskytter brugerens certifikater i henhold til OCES certifikatpolitikken
- Væsentlig tidsbesparelse i forhold til manuel administration
- Internationale it-sikkerhedscertificeringer (Common Criteria EAL3+ og FIPS 140-2)

Software komponenterne

SmartSignatur Server

Den centrale del af SmartSignatur Server er selve certifikat udstedelse og certifikat fornyelsen. Denne del er udviklet direkte af Liga Software og det er også denne del, som den enkelte bruger selv oplever i forbindelse med certifikat processen. Server komponenten er direkte integreret med Nets DanIDs webservices og kommunikerer i realtid med Nets DanID. Dette betyder at en bruger kan få sit certifikat udstedt når som helst i alle døgnets 24 timer.

Straksudstedelse af medarbejdersignatur kan ske med brugerens private NenID

SmartSignatur server håndterer alle Nets DanIDs metoder til udstedelse af en NemID medarbejdersignatur. Både den oprindelige metode med PIN kode brev samt de to nyere med enten straksaktivering via PIN kode eller via medarbejderens personlige NemID (NemID-POCES).

Fornyelsesprocessen er ligeledes automatiseret, så langt som den offentlige certifikat politik tillader.

Samtidig med enten udstedelse eller fornyelsen opdateres den bagvedliggende database med relevante oplysninger fra brugerens certifikat. Disse oplysninger kan efterfølgende benyttes af helpdesk funktionen til den overordnede certifikatadministration.

Når en medarbejdersignatur er udstedt, har SmartSignatur systemet ikke længere adgang til den pågældende medarbejders private certifikatnøgle. Dette er en meget vigtig funktion i SmartSignatur server. Det er kun brugeren som med sit personlige kodeord (altid det samme som vedkommendes netværkskodeord) der har adgang til den private nøgle. Hverken SmartSignatur server, helpdesk medarbejdere eller signaturadministrator har adgang til nøglen. I den offentlige certifikatpolitiks

punkt 6.2 fremgår det at certifikatindehaveren skal sikre, at certifikatholderen opfylder blandt andet disse betingelser:

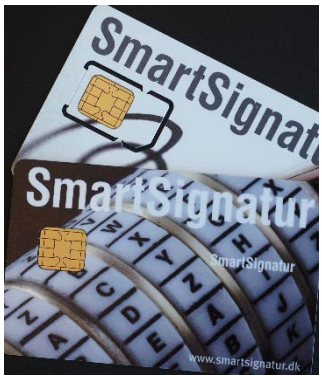
- at tage rimelige forholdsregler for at beskytte de sikkerhedsmekanismer, der sikrer den private nøgle, mod kompromittering, ændring, tab og uautoriseret brug
- at hemmeligholde adgangskoden, så andre ikke får kendskab til denne,omittering, ændring, tab og uautoriseret brug,

Kilde: https://www.nemid.nu/dk-da/digital_signatur/oces-standarden/oces-certifikatpolitikker/MOCES_Certifikatpolitik_version_5.pdf

SmartSignatur server betyder at organisationen har en sikker og stabil basis for brugeradminstration og sikrer en konstant synkronisering Nets DanID og NemID medarbejdersignaturen.

SmartSignatur Card

Et smart card er et plastickort hvor ens private nøgle er lagret på en sikker elektronisk chip. Et smart card kan udbygges med eID (electronic identification) faciliteter såsom billede, fingeraftryk, kontonummer, saldo med videre.



Et smart card er en ægte 2-faktor loginmetode. Kortets chip en mini computer og chippen er sikret mod at ens private nøgle aldrig kan kopieres. Adgang til kortet sker med en PIN kode. Den samme sikre metode anvendes på vores betalingskort.

Betalingskort som chipkort er væsentlig bedre sikret mod forfalskninger end magnetstribekort. De fleste kender chippen fra deres Dankort. Jf. Finansrådet er der aldrig blevet registreret forfalskninger af chip betalingskort.

Ved at placere en NemID medarbejdersignatur på et smart card, vil medarbejderen nu kunne bruge sin signatur fra flere maskiner og undgå ulemperne med at skulle genudstede ved reinstallation af PC og glemt kodeord.

Medarbejderen vil også opnå, at adgangskoden til certifikatet kan simplificeres ved brug af en 4-cifret pinkode, fremfor en adgangskode på minimum 8 bogstaver og tal og mindst 1 stort bogstav.

Smart card kan kombineres med velkendte adgangskort til bygninger. Disse kort indeholder både en chip og tilsvarende RFID og NFC komponenter. Kortet kan leveres med både Java Card (JCOP) PKI chip og Mifare RFID chip

Et smart card kan inkludere adskillige identifikation metoder. Både PKI chip, men også NFC og RFID. chip

SmartSignatur Card kan kombineres med andre sikkerhedselementer såsom to-faktor login til Windows, disk- og filkryptering, VPN eller single sign-on adgang til interne webtjenester og virker med Linux, Mac, Windows iOS, Android og Windows tablets.

SmartSignatur Client

Når brugeren logger på en PC, Citrix session eller Vmware VDI med sit netværkslogin, bliver det indtastede bruger-ID og password via SmartSignatur Client brugt til at give adgang til brugerens eget medarbejdercertifikat i databasen, hvorefter det automatisk kopieres til den aktuelle PC hvor brugeren og brugerens applikationer befinder sig. SmartSignatur Client fjerne automatisk medarbejdercertifikatet fra den lokale PC hvis det ønskes.

Medarbejdercertifikatet benytter standard Microsoft Windows CSP (Cryptographic Service Providers) på den lokale PC. Derved vil en enhver applikation kunne benytte medarbejdersignaturen og logning og styring af rettigheder kan kontroleres via standard Group Policy og SIEM værktøjer.

SmartSignatur Door

SmartSignatur Door er løsningen til integration med standard MIFARE RFID baserede dørsystemer. Løsningen aflæser MIFARE UID fra det enkelte kort og opdaterer automatisk det tilsluttede dørsystem. På samme måde deaktiveres også kort automatisk hvis en medarbejder fratræder. Løsningen kan udbygges til, at administre hvilke dører og lokaler en medarbejder skal have adgang til. Dette baseret på roller og automatik. Tilsvarende kan også fysisk print på adgangskort også indbygges.

Kombinationen af både fysisk og logisk adgang giver organisationen mange fordele. Eksempelvis kan en medarbejder kun være ét sted ad gangen når den digitale ID bæres på et fysisk smart card

Det er i udgangspunktet den enkelte medarbejder som selv administrere udstedelse og print på kort. Dog skal processer som genudstedelse, glemt kort med videre tilpasses den enkelte organisations procedure for dette. Metoden er meget lig metoden for password reset.

SmartSignatur Mobile SDK

SmartSignatur Mobile SDK er et udviklingsværktøj til Apple iOS programmører. Med dette værktøj er det ganske let, at udvikle yderst sikre iOS apps baseret på certifikater og tilhørende private nøgler læst fra smart cards via en tilsluttet smart card læser.

SmartSignatur Mobile SDK gør det nemmere for organisationer, kommuner, virksomheder eller app-udviklere at afskaffe brugernavn og passwords og erstatte dem med ægte digital identifikation på tablets og smartphones.

Med Mobile SDK kan man håndtere både kryptering og dekryptering af data og tilsvarende signering og verificering. Den private nøgle er opbevaret sikkert og kopibeskyttet på et smart card. Signering og verificering af tilfældigt dannede data kan bruges som bevis på at brugeren er i besiddelse af et smart card, men det kan også bruges til brugervalidering.

I den almindelige anvendelse af Mobile SDK vil den private nøgle *aldrig* forlade kortet. Dekryptering og signering sker ved hjælp af kortet og i kortets eget CardOS. Dette betyder at ingen ondsindet software kan få en kopi af den private nøgle.

SmartSignatur Mobile SDK taler med eID kortet via pkcs#11 standarden. SmartSignatur Mobile SDK anvender cv cryptovision pkcs#11 bibliotek og det er nødvendigt at anvende et Tactivo kortlæser cover fra Precise Biometrics.

SmartSignatur Mobile SDK består af et API og et bibliotek og en demonstrationsprogram. På Apple AppStore kan enhver hente SmartSignatur sample App til testformål.

SmartSignatur API

I alle organisationer er integration mellem fagapplikationer alfa og omega for organisationens digitale succes. SmartSignatur API er en løsning der gør, at enhver applikation kan benytte medarbejdersignaturen til signering, kryptering eller dekryptering uden at have direkte adgang til brugerens private nøgle. SmartSignatur API består af både en Windows C# klient, Java klient SOAP webservice og en LDAP service. Det står frit hvilken metode man ønsker at anvende.

Med SmartSignatur følger en standard integrationsklient til brug for signering af data med medarbejdercertifikatet. Denne klient anvendes blandt andet i forbindelse med integration til Fælles MedicinKort (FMK) og kommunale omsorgssystemer. Klienten kan også bruges til andre fagapplikationer.

I alle tilfælde skal brugerens brugernavn og adgangskode præsenteres. Kun på den måde sikres overholdelse af OCES-certifikatpolitiken.

Øvrige komponenter

Foruden de ovenfor omtalte komponenter indgår der også I SmartSignatur produkter fra Micro Focus, Cryptovision, MySmartLogon, Exceet Card Group AG og SwissSign AG. I takt med udviklingen af SmartSignatur bliver der løbende tilføjet nye komponenter til produkterne.

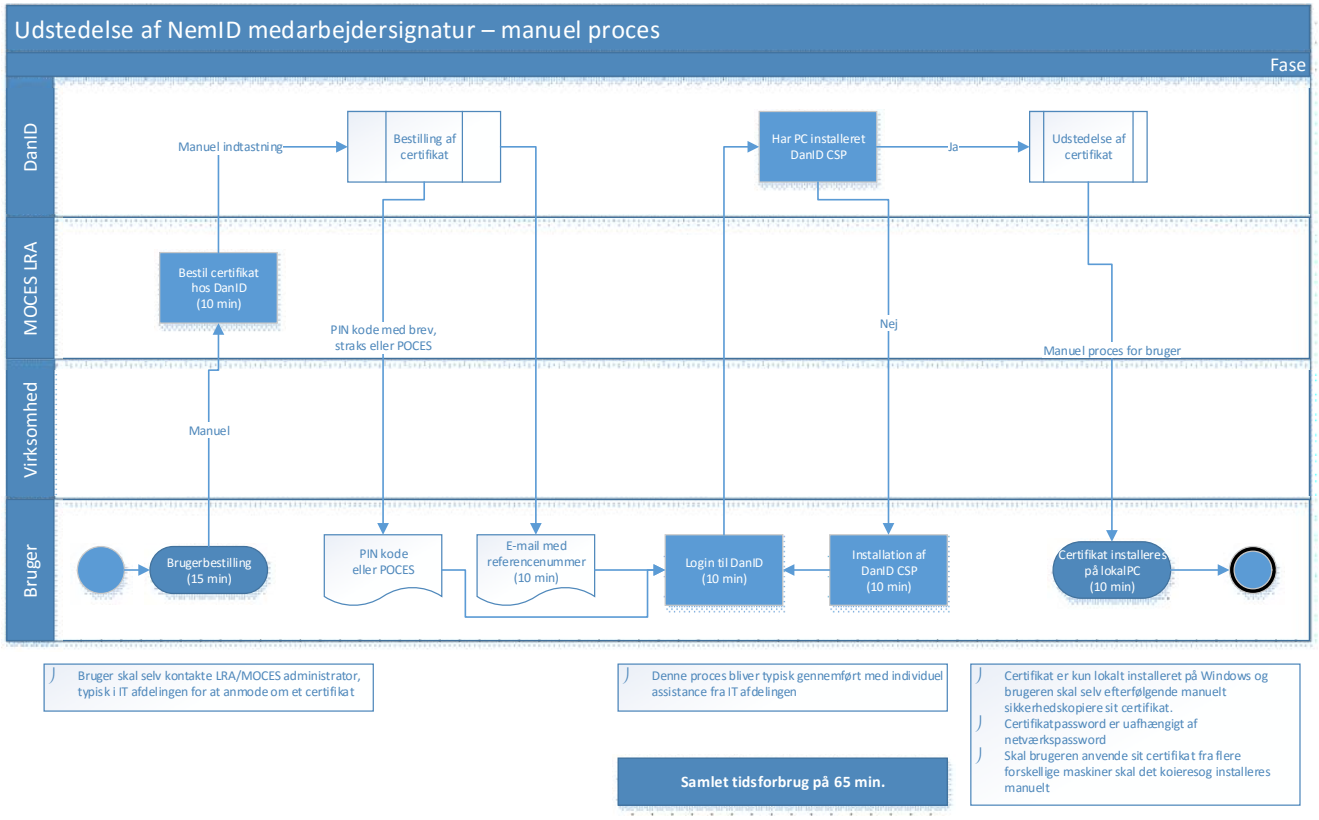
Udstedelsesproces og tidsforbrug

De næste 2 diagrammer vises dels en manuel proces for oprettelse af medarbejdercertifikater, dels den automatiserede proces ved anvendelse af SmartSignatur.

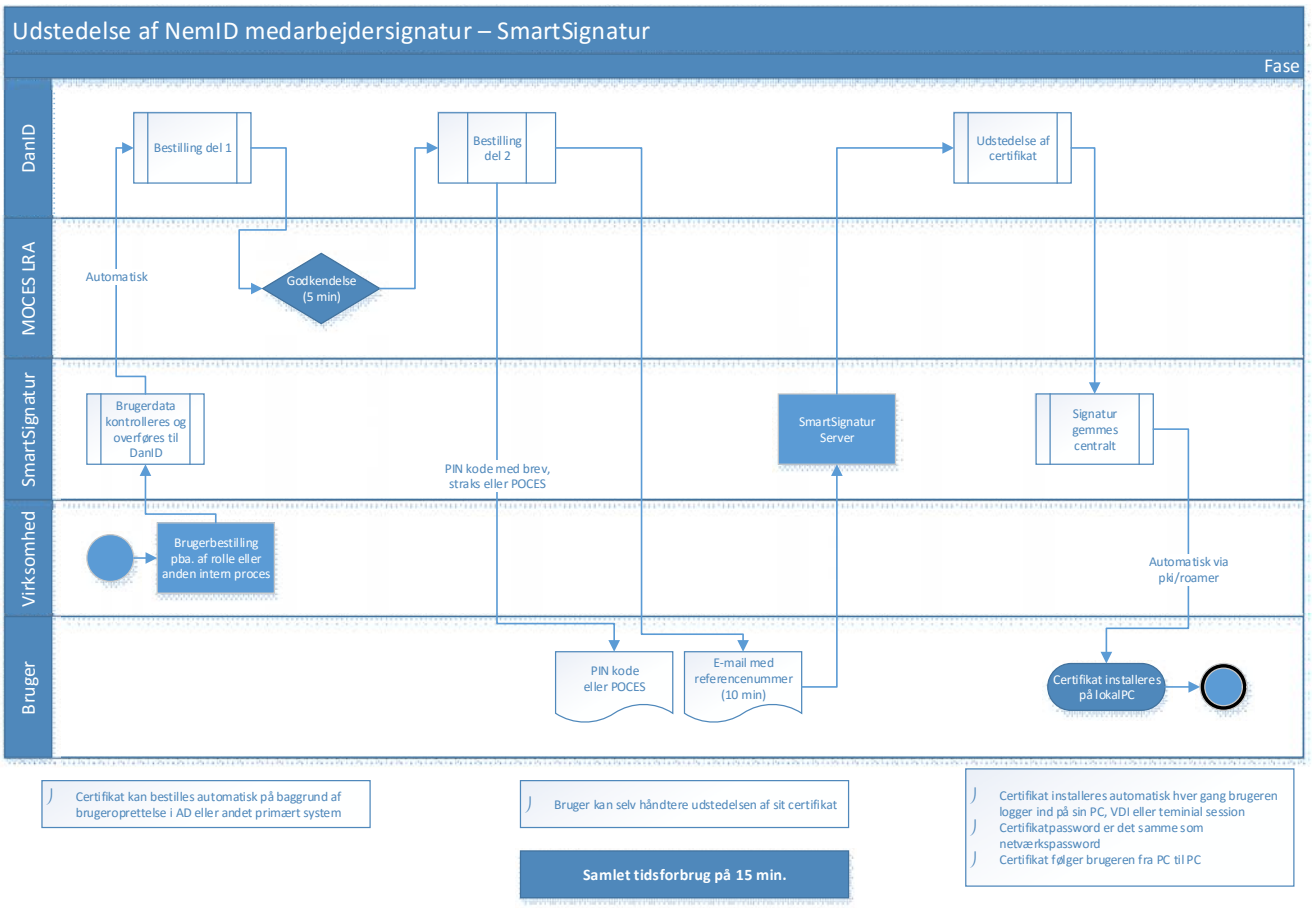
Tidsstudier har vist, at der kan være helt op til mellem tre kvarter og en time i besparelse for hver medarbejdersignatur, når der benyttes en automatiseret løsning som SmartSignatur

Dertil kommer, at certifikatet følger brugeren fra pc til pc. Dermed skal brugeren ikke spekulere på, om login foretages fra den samme arbejdsplads hver gang. Det finder SmartSignatur ud af. Endnu en kilde til effektivisering i en travl hverdag.

Udstedelse af NemID medarbejdersignatur – manuel proces



Udstedelse af NemID medarbejdersignatur – SmartSignatur



Arkitektur og software komponenter

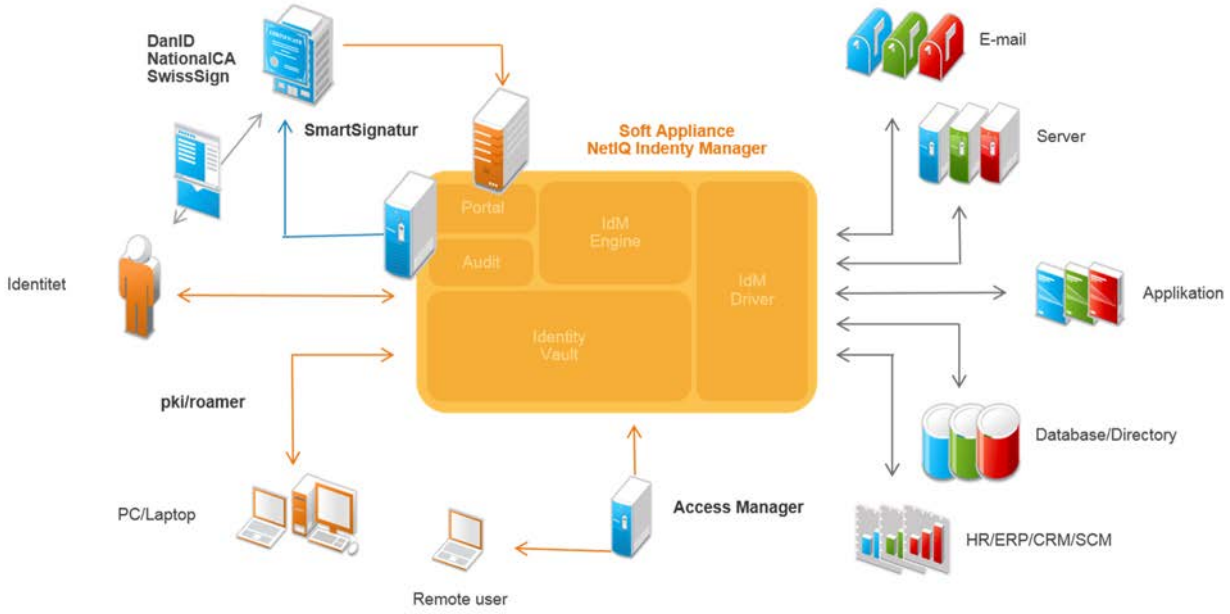
Software komponenter

- Suse Enterprise Server med Sun Java og Tomcat
- Suse Enterprise Server HA (option)
- Micro Focus eDirectory til identitets og certifikat opbevaring
- Micro Focus eDirectory for LDAPS access to certifikater
- Micro Focus eDirectory Instrumentation for Audit Logins and certifikat adgang
- Micro Focus Identity Manager,
    - Integration modules for Directories (Active Directory and eDirectory)
    - Utilities (SOAP integration med DanID)
    - EAS for Driver and object events
- LCES, til certifikat installation i Secret Store og integration til Nets DanID
- CryptoVision, pki/roamer og sc/interface til certifikat installation på brugerens Dekstops/laptops/Citrix….

Arkitekturplan

Nedenstående arkitekturplan beskriver dels elementerne i en standard SmartSignatur server installation, dels de udvidelsesmuligheder som løsningen også indeholder. Som udgangspunkt leveres integration til Active Directory samt til Nets DanID.

Hvis man allerede har en eksisterende Micro Focus IDM installation er det enkelt at udbygge med SmartSignatur funktionaliteten.



Den offentlige certifikatpolitik

I den offentlige certifikatpolitik (OCES-medarbejder certifikater CPen) er beskrevet, hvorledes NemID Medarbejdercertifikater skal håndteres.

Kilde: https://www.nemid.nu/dk-da/digital_signatur/oces-standarden/oces-certifikatpolitikker/MOCES_Certifikatpolitik_version_5.pdf

Det er væsentligt, at der skelnes mellem certifikatindhaver og certifikatholder.

(Fra CPen) - 4.4 Certifikatindehavere og certifikatholdere
Forud for udstedelse af medarbejdercertifikater indgår CA en aftale med certifikatindehaveren i egenskab af den virksomhed, der ønsker medarbejdercertifikater til sine medarbejdere. Den medarbejder, til hvem der efterfølgende udstedes et certifikat benævnes certifikatholder.

Password politik og håndtering

I forbindelse med med implemetering af SmartSignatur server er det nødvendigt at kunden samtidig implementere den offentlige password politik fra CPen. Kun på denne måde leveres der løsning til medarbejderne hvor de fortsat kun skal anvende et password til både netværket og deres medarbejdersignatur.

Af den offentlige certifikatpolitiks punkt 6.2 fremgår det at certifikatindehaveren skal sikre, at certifikatholderen opfylder blandt andet disse betingelser:

- at tage rimelige forholdsregler for at beskytte de sikkerhedsmekanismer, der sikrer den private nøgle, mod kompromittering, ændring, tab og uautoriseret brug
- at hemmeligholde adgangskoden, så andre ikke får kendskab til denne,omittering, ændring, tab og uautoriseret brug,
- omgående at ændre sin adgangskode eller spærre certifikatet, hvis der opstår mistanke om, at adgangskoden er kompromitteret,

Af punkt 7.3.1 afsnit ” Generering og installation af certifikatholders nøgler hos certifikatholder” fremgå det yderligere:

- den private nøgle er krypteret og beskyttet af adgangskoden,
- adgangskoden til aktivering af den private nøgle genereres og indtastes i forbindelse med nøglegenereringen
- den private nøgle er aktiveret, når certifikatholderen har angivet en adgangskode, der består af mindst 8 tegn og indeholder mindst et lille og et stort bogstav samt et tal.

Deaktivering

I tilknytning til password politik og håndtering skal der i forbindelse med fratrædelse af en medarbejder ske en omgående spærring af den pågældende medarbejder. Rutiner til overholdelse af dette krav er indbygget i SmartSignatur server

Af CPen fremgår det af punkt 6.2:

- indholdet heraf ikke er i overensstemmelse med de faktiske forhold,
- Såfremt certifikatholders tilknytning til certifikatindehaver ophører, skal certifikatindehaver omgående meddele CA dette og anmode om spærring af certifikatholderens certifikat.

FAQ til SmartSignatur

Hvad er et smartcard

Et smartcard er en lille computer med CPU kraft svarende til en 386 CPU. Denne lille computer vågner op når den får strøm fra en fysisk eller kontaktløs kortlæser. I denne computer kan der gemmes data med op til 80kb. I en del af dette memory område gemmes brugerens private nøgle/r. Disse er beskyttet med stærk kryptering og kræver brugerens hemmelige PIN kode for at kunne tilgås. Tastes PIN kode forkert mere end 3 gange bliver kortet automatisk spærret. Det sker i selve kortet. Selve PC'en som skal læse fra kortet kan kun tilgå kortet via et åbent standard API (PKCS11)

Hvad er et digitalt certifikat

Et digitalt certifikat er en elektronisk identifikation. Et digitalt certifikat kan udstedes til en person, en organisation, et computerprogram, eller en ting der har en unik identitet. Et digitalt certifikat indeholder blandt andet oplysninger om hvem der har udsendt certifitikatet og hvem det identificere men det indeholder også en offentlig kryperingsnøgle.

Smartcards er ikke sikre

Det er korrekt at der findes kort som regnes som usikre. Disse er typisk baserede på ældre RFID og tilsvarede teknologier og bør kun anvendes som simpel erstatning for fysiske nøgler. De kort som SmartSignatur benytter er sikre og her anvendes et langt mere avanceret kort med en indbygget mikroprocesser og kompleks kryptering. SmartSignaturs kort er EAL 4+ certificerede og anvendes over hele verdenen til eksempelvis PAS, nationale ID kort, bank betalingskort med videre.

Smartcards kan kopieres

Nej. Sammen som ovenfor. Det er kun simple RFID, Mifare og tilsvarende kort der kan kopieres. Et smartcard med en PKI chip kan IKKE kopieres.

Identitetskort går i stykker

Et billigt simpelt kort går lettere i stykker end et kraftigt og officielt kort. Et kort som skal bruges hyppigt skal produceres i god kvalitet og samtidig gives et officielt udseende. Det samme som med bank betalingskort. Disse holder normalt til daglig brug i mange år.

Identitetskort bliver glemt

Almindelige simple medarbejderkort er lette at glemme. Men et kort som er vigtigt for medarbejderen og som skal bruges ofte glemmes ganske sjældent. Det er på samme måde som med vores pung og betalingskort. Det er også sjældent for de fleste at glemme disse.

Skulle det ske alligevel er en erstatningskort let at udstede for medarbejderen og samtidig dekativeres det glemte kort.

Det bøvlet med udstedelse af fysiske kort

En bruger kan selv udstede et kort til sig selv via SmartSignatur selvbetjeningsløsning. Det kræver blot adgang til en PC med en kortlæser.

Mine brugere kan ikke huske deres PIN kode

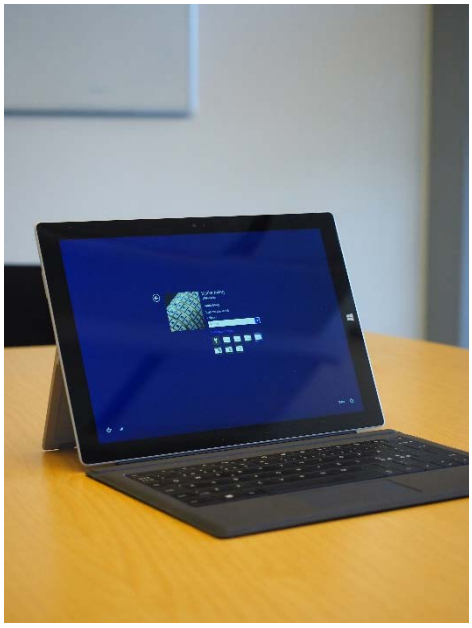
De fleste mennesker kan godt huske deres PIN kode hvis det er vigtigt. Med en SmartSignatur eID løsning vil brugeren anvende sit kort hyppigt. Skulle det alligevel hænde at en bruger enten glemmer sin kode eller taster forkert mere end 3 gange er det helt uproblematisk at udstede et nyt kort til brugeren. Denne kan selv gøre det via SmartSignatur selvbetjeningsløsningen.

Smartcards virker ikke som standard med Windows PC'ere

For at et kort virker med Windows skal maskinen have forhåndsinstalleret den nødvendige driver for at kortet kan læses. Det er ikke anderledes end med andre typer hardware. Microsoft Windows understøtter som standard alle funktioner med smartcards.

Det er så nemt med en SMS kode

Det er rigtigt. SMS koder er praktiske i mange sammenhænge. Brugeren har sin telefon med. SMS koder fungerer ikke godt hvis koden skal sendes mange gange i løbet af dagen, manglende dækning, manglende telefon osv. SMS koder har også et begrænset anvendelsesområde. De kan kun bruges til brugervalidering. Endeligt lider SMS koder af den svaghed at de skal leveres til brugerens telefon uden forsinkelse. Det hænder desværre at SMS afsendelse eller modtagelse er væsentligt forsinket.



Den meget populærer Surface Pro 3 fra Microsoft er en oplagt kandidant til at blive opgraderet til 2 faktor sikkerhed.

Kontaktoplysninger

Liga Software ApS
International House
Center Boulevard 5
2300 København S

Telefon 35 36 95 05
Web www.smartsignatur.dk
Mail post@smartsignatur.dk

Kommentarer til dette dokument kan sendes til Bjarke Alling, ba@smartsignatur.dk