Indledning

Dette dokument beskriver overordnet Signaturgruppens implementering af PAdES signaturer. Forinden gives en kort oversigt over de udfordringer, der opstår idet NemID ikke direkte understøtter PAdES.

NemID og PDF-signering

Når NemID anvendes til signering af dokumenter bliver resultatet et signeret XML-dokument. Der produceres et XML-dokument hver gang dokumentet underskrives. Det signerede PDF-dokument er indlejret i XML-dokumentet.

De producerede XML-dokumenter kan ikke læses af lægmand, og almindelige brugere kan dermed ikke afgøre, om signaturer er valide eller ej. Selve aftaleteksten er heller ikke umiddelbart tilgængelig.

I løsninger, hvor signerede dokumenter skal overdrages til en ikke-teknisk tredjepart, er disse forhold problematiske, og kan være hindrende for anvendelsen af digital signering i pågældende problem-domæne.

PAdES dokumenter

Mange leverandører på markedet forsøger at afhjælpe dette forhold ved at producere såkaldte PAdES (PDF Advanced Electronic Signatures) dokumenter. Disse er digitalt signerede PDF-dokumenter, hvor den digitale signatur indlejres i PDF-dokumentet. Dokumenterne kan umiddelbart læses i almindelige PDF-læsere (fx Adobe Reader), og PDF-læserne kan samtidig validere dokumenterne, og på enkel, letforståelig vis forklare bruger hvorvidt et dokument er signeret og om denne signatur er valid - og dermed om dokumentet har været manipuleret efter signering.

Dannelse af en PAdES signatur kræver direkte adgang til den private signerings-nøgle, og derfor kan PAdES signaturer kun vanskeligt dannes direkte med underskrivers NemID.

De forskellige signeringsløsnings-leverandører på markedet skrider derfor til en indirekte løsning: Dokumentet underskrives med NemID, og de resulterende XML-dokumenter indlejres i den færdige PDF som attachments sammen med forskellig meta-information såsom signeringscertifikat-status (dokumentation for at signeringscertifikatet ikke var spærret på underskriftstidspunktet) og tidsstempler fra 3. part.

Den færdige PDF udstyres også typisk med et summarisk underskriftsark, som ikke er en del af del oprindelige PDF-dokument, og signeres efterfølgende med et særligt dokument-signeringscertifikat udstedt til signeringsløsnings-leverandøren. PAdES signaturen skal derfor her betragtes som en afsluttende forsegling - en terminologi som flere af leverandørerne da også anvender.

Resultatet er meget brugervenligt: Modtager af dokumentet kan umiddelbart verificere, at forseglingen er ubrudt, idet Adobe Reader validerer PAdES signaturen når dokumentet åbnes. Bruger kan også i dokumentets underskriftsark læse hvem der har underskrevet dokumentet og hvornår. Bruger kan derimod ikke umiddelbart (med mindre hun er teknisk kyndig) kontrollere, at de indlejrede XML-signaturer er gyldige (eller var det på underskriftstidspunktet), og at disse svarer til de på underskriftsarket angivne underskrivere. Her må bruger umiddelbart stole på signeringsleverandøren. Hvis der opstår en juridisk tvist, hvor det bliver nødvendigt at redegøre indgående for de digitale underskrifter på dokumentet, er det derfor nødvendigt at foretage en mere dybdegående (teknisk) validering af dokumentet.

Teknisk validering af PAdES dokumenter

Valideringen består af følgende elementer:

1. Validering af de individuelle XML-signaturer
2. Validering af de tilhørende signeringscertifikater - evt. vha. gemte OCSP/CRL data
3. Kontrol af, at de under 1. signerede dokumenter er de samme
4. Kontrol af, at de under 1. signerede dokumenters juridiske indehold er det samme som indholdet i PAdES dokumentet
5. Validering af PAdES signaturen (forseglingen) på dokumentet
6. Validering af PAdES signeringscertifikatet - vha. online opslag hos certifikatudsteder.

Pkt. 3 sikrer, at alle underskrivere har underskrevet det samme dokument, og dermed er enige om indholdet i den juridiske aftale. Idet PAdES dokumentets indhold automatisk IKKE er identisk med det dokument, som underskriverne har set - bl.a. fordi PAdES dokumentet indeholder underskriftsarket, som først dannes efter alle parter har underskrevet dokumentet - er pkt. 4 nødvendigt.

Bemærk, at pkt. 4. kræver, at det dokument, som underskriverne har set på underskriftstidspunktet også er tilgængeligt på valideringstidspunktet. Nogle signeringsleverandører indlejrer ikke dette dokument i PAdES dokumentet, så en efterfølgende validering jf. pkt. 4 kræver altså at signeringsleverandøren kan udlevere dette dokument.

Signaturbeviser

Når der juridisk skal argumenteres for en digital signaturs gyldighed, fremføres beviser af to forskellige typer:

- Kryptografiske beviser
- Systembeviser

Et kryptografisk bevis er typisk et digitalt dokument med en digital signatur - eksempelvis et digitalt certifikat (dokumentsigneringscertifikatet ovenfor eller NemID certifikater) eller et signeret XML-dokument.

Et systembevis dokumenterer et systems opførsel på et givet tidspunkt. Et detaljeret systembevis omfatter fx en applikations source-kode og eventuelle logs samt opsamlede data - fx i en database. Systembevisers gyldighed kræver også en argumentation for, at systemet er drevet på sikker vis så eksempelvis en angriber ikke har kunnet manipulere med systemets opførsel eller data. Systembeviser accepteres derfor normalt kun for professionelle leverandører.

NemID PDF-signering - direkte og indirekte

NemID understøtter signering af PDF-filer. Metoden fungerer ved, at NemID klienten i underskrivers browser viser det dokument, der skal underskrives, hvorefter bruger skriver under. Dette kaldes i det følgende for direkte NemID PDF-signering.

Det er altså i denne situation alene NemID systemet, der styrer hvordan dokumentet vises for underskriver.

NemID PDF-signeringssystemet stiller - af tekniske grunde - høje krav til de PDF-dokumenter, der kan vises og dermed underskrives. Der er derfor flere leverandører på markedet, der anvender indirekte signering af PDF-dokumenter.

Processen er som følger: * Dokumentet, der skal underskrives, uploades til signeringsleverandørens system af

dokumentejer. * Underskriver logger på signeringsleverandørens system - fx via link sendt fra dokumentejer, eller via link i dokumentejers system * Signeringsleverandørens system viser dokumentet for bruger - fx ved download til Adobe Reader * Hvis bruger kan acceptere dokumentets ordlyd, underskrives en summarisk tekst med NemID

Den summariske tekst kan være noget i retning af:

```
Aftale mellem os.doc
EIC2P-Y01H0-KP3EN-OGAO8-YQ5AN-FEEBW
hash-værdi: 4086e75a09655865fb49b32efef4881ba4c4ca24fcae3d84314a378e035b8385
hash-algoritme: SHA-256
Jeg underskriver dokumentet:
- På vegne af DSB som adm. direktør
```

hvor værdien `EIC2P-Y01H0-KP3EN-OGAO8-YQ5AN-FEEBW` identificerer det relevante dokument ("Aftale mellem os.doc") entydigt hos signeringssystem-leverandøren.

Et almindeligt anerkendt paradigme ved digital signering af dokumenter er WYSIWYS - What You See Is What You Sign. Det er oplagt, at dette paradigme kun opfyldes indirekte ved ovennævnte, idet den underskrevne tekst netop ikke indeholder aftaleteksten.

Mere væsentligt er det, at en argumentation for den digitale underskrifts rigtighed kommer til at omfatte argumenter for opførslen af signeringsleverandørens system på underskrifttidspunktet: Viste systemet det rigtige dokument for bruger? Kan dokumentet sammenkædes korrekt til ovenstående summariske tekst ved genberegning af hash-værdierne? Findes det oprindelige dokument stadig? Denne bevisførelse falder i kategorien systembevis, som beskrevet ovenfor.

Anvendes direkte NemID signering af PDF-dokumenter, fjernes dette bagudrettede behov for at argumentere for signeringsleverandørsystemets opførsel, idet det alene er nødvendigt at knytte tillid til NemID komponenterne, når der argumenteres for PAdES dokumentets gyldighed.

En stærk PAdES signatur

Ovenfor har vi redegjort for, at PAdES/NemID kombinationen, som implementeret af signeringsleverandører på det danske marked, til dels udgør et kompromis mellem sikkerhed og brugervenlighed.

Hvis PAdES signaturer var direkte understøttet af NemID, ville der ikke være behov for at en 3. part (signeringsleverandøren) stempler og sammenkæder NemID- og PDF-signaturer, som beskrevet ovenfor.

Idet sammenkædningen er forskellig (og dermed proprietær) for hver enkelt leverandør, er det i vores optik langt fra ligegyldigt, hvilken leverandør, der vælges. I denne sammenhæng bør det indgå i overvejelserne, om der findes teknisk dokumentation, der beskriver hvordan PAdES dokumentet er opbygget, og hvorledes en validering - som omfatter de ovenfor beskrevne trin - kan foretages af uvildig 3. part.

Signaturgruppens implementation

Signaturgruppen har implementeret PAdES signaturer ved anvendelse af NemID PDF-signering - den ovenfor beskrevne direkte NemID PDF-signering. Hermed gøres signaturbevisførelsen så uafhængig som muligt af signeringsleverandøren (her Signaturgruppen).

Endvidere sikres det, at der alene ved argumentation for NemID sikkerheden, kan godtgøres hvilket dokument, underskriver blev præsenteret for ifm. afgivelse af NemID signatur.

Kontaktinformation

Email	support@signaturgruppen.dk
Tlf	+45 70256425
Hjemmeside	https://www.signaturgruppen.dk