Digitaliseringsstyrelsen

VALIDERING AF ELEKTRONISKE SIGNATURER

Version: 1.0

Forfatter: Digitaliseringsstyrelsen, Den Danske Stat TSP

Udgivelsesdato: Februar 2025

Den Danske Stat Tillidstjenester

Indholdsfortegnelse

Dokumenthistorik

Version	Dato	Forfatter	Status	Bemærkninger
1.0	25.02.2025	Den Danske Stat TSP	Endelig	Første version

1. Indledning

Dette er en vejledning i validering af elektroniske signaturer og elektroniske segl. Dokumentet skal give overblik til videre arbejde med at fastlægge, hvilke elektroniske signaturer og elektroniske segl en given modtagerpart[1] eller digital selvbetjeningsløsning skal understøtte. Dokumentet er således ikke en facitliste eller en konkret vejledning i, hvordan en sagsbehandler skal validere en specifik elektronisk signatur, da dette vil afhænge af en vedtagen politik for den enkelte organisation. Dokumentet kan derimod hjælpe med at fastlægge, hvilke elektroniske signaturer og/eller elektroniske segl organisationen ønsker at modtage.

Dokumentet er tiltænkt medarbejdere med ansvar for at indføre løsninger med anvendelse af elektroniske signaturer eller elektroniske segl. Det kan fx være en digitaliseringschef med ansvar for at digitalisere en eksisterende fysisk proces med underskrevne dokumenter. Det forudsættes ikke at læseren på forhånd er bekendt med teknologier og jura ift. elektroniske signaturer og elektroniske segl, men det anbefales, at personer med teknisk og juridisk domæneviden inddrages tidligt i en beslutningsproces. I det efterfølgende antages det, at en modtagerpart ønsker at modtage elektroniske signaturer og/eller elektroniske segl med henblik på at sikre og kunne bevise autenticitet og integritet af data fra en identificeret underskriver i et givet tidsrum efter signeringen.

Elektroniske signaturer eller log-in

Elektroniske signaturer adresserer typisk 3 behov:

- **Autenticitet** (hvem har signeret?)
- **Integritet** (er der ændret på data efter signeringen?)
- **Uafviselighed** (kan jeg bevise autenticitet og integritet over for tredjepart fx over for en dommer?)

En almindelig sikker forbindelse med et log-in adresserer typisk kun **autenticitet** og **integritet**, altså at leverede data ikke er manipuleret.

Man bør derfor ved forberedelse af en digital selvbetjeningsløsning indledningsvis vurdere og beslutte, om der er regulatoriske eller forretningsmæssige forhold, der kræver en elektronisk signatur eller et elektronisk segl, eller om et log-in via en sikret forbindelse kan dække behovet.

Anbefaling 0

Undersøg behovet for elektronisk signatur eller om et log-in via en sikret forbindelse vil dække behovet. Er der behov for uafviselighed?

Bemærk at anvendelsesscenariet for elektronisk signatur ofte ikke er uafviselighed over for en dommer, men en tredjepart der som modtagerpart har et behov for at validere data.

Elektroniske signaturer og elektroniske segl og retsvirkning

[1] Dette dokument anvender betegnelsen ”modtagerpart” svarende til det engelske begreb ”relying party”.

Inden det besluttes hvilke elektroniske signaturer eller elektroniske segl, man ønsker at understøtte i sin digitale selvbetjeningsløsning, er det væsentligt at have nogle begreber fastlagt.

EU-forordningen [eIDAS] og [eIDAS2] definerer elektroniske signaturer og elektroniske segl. Teknisk set er de to typer ens, men elektroniske signaturer er knyttet til en underskriver, der er en fysisk person i modsætning til elektroniske segl, der er knyttet til en juridisk enhed. Bemærk, at et elektronisk segl godt kan være initieret af en fysisk person, men at dette typisk ikke vil fremgå af seglet.

[eIDAS] definerer desuden en særlig klasse af elektroniske signaturer og elektroniske segl kaldet hhv. kvalificerede elektroniske signaturer og kvalificerede elektroniske segl. En række krav skal være opfyldt, før en signatur eller et segl kan betegnes som kvalificeret. Disse krav er ensartede i hele EU/EØS. Dvs. at hvis en elektronisk signatur opfylder kravene til en kvalificeret elektronisk signatur i ét medlemsland, opfylder den automatisk kravene til en kvalificeret elektronisk signatur i alle medlemsstater.

I forhold til juridisk gyldighed fastlægger [eIDAS] i artikel 25, at en elektroniske signatur ikke må nægtes retsvirkning og anerkendelse alene af den grund, at den er elektronisk eller, at den ikke er kvalificeret. Samtidig fastlægger [eIDAS] at en kvalificeret elektronisk signatur har samme retsvirkning som en håndskreven underskrift. Kvalificerede elektroniske signaturer anses i en række medlemslande at have en stærkere retsvirkning end ikke kvalificerede signaturer. I Danmark tillægges begge klasser af signaturer (kvalificerede og ikke kvalificerede) samme retsvirkning.

Det bemærkes, at et udvalg under Justitsministeriet i 2004 udgav en betænkning [Betænk1456] vedrørende elektroniske signaturers retsvirkninger. Udvalget fastslog, at retsvirkningerne af en elektronisk underskrift i princippet ikke adskiller sig fra retsvirkningerne af en håndskreven underskrift, idet det afgørende er, at begge typer af underskrifter tilkendegiver en vilje til at blive bundet. Der har således i Danmark i flere år været fastslået en teknologineutral tilgang til afgivelse af underskrifter og retsvirkningerne heraf.

2. Signaturformater

Der findes en række forskellige services og toolkits til generering af elektroniske signaturer/segl.

Nogle af disse følger standarder udstukket af EU Kommissionen gennem en implementeringsakt [Impl1506]. De standarder fra EU Kommissionens implementeringsakt har endelsen AdES fx PAdES (for signerede PDF-dokumenter) og XAdES (for signerede XML-dokumenter).

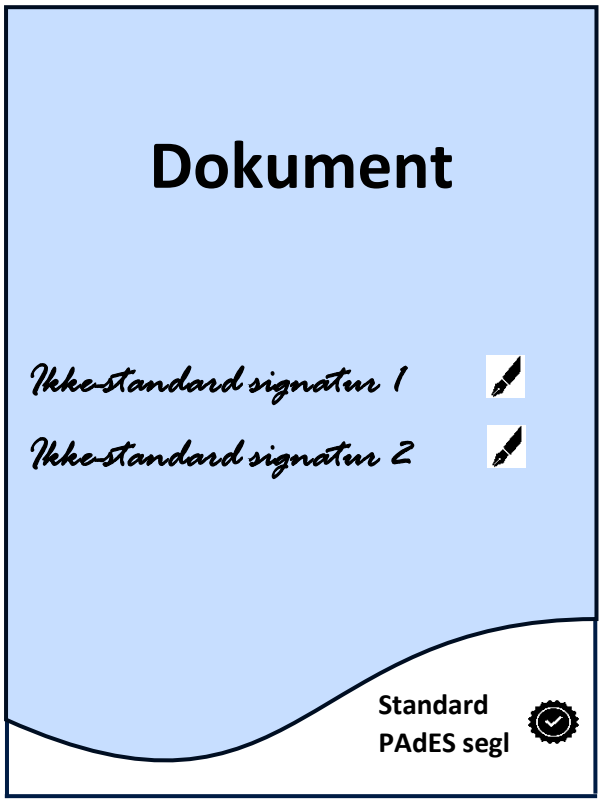
Hvis man som offentlig myndighed udbyder en digital selvbetjeningsløsning med krav om anvendelse af elektroniske signaturer, er man samtidig i medfør af [eIDAS] artikel 27 og artikel 37 forpligtet til at acceptere visse former for elektroniske signaturer, hvis de formatmæssigt er omfattet af [Impl1506].

Elektronisk signerede dokumenter i AdES-formaterne kan udover selve signaturen/seglet indeholde ekstra information, der understøtter validering af signaturen/seglet. AdES kan således inddeles i en række klasser:

- Et simpelt signeret dokument (*Basic Signature, B*) indeholder kun signaturen og det tilhørende certifikat
- Et dokument med tidsstempel (*Signature with Time, T*) indeholder et eller flere kryptografiske tidsstempler, der fx dokumenterer signeringstidspunktet
- Et dokument med alle certifikater til opbygning af en tillidskæde og certifikatstatus på signeringstidspunktet for de anvendte certifikater (*Signature with long-term validation, LTV*, og *Signature with long-term availability, LTA*)

LTV- og LTA-signaturer kan valideres over tid uafhængigt af certifikatudsteder og evt. signeringsservice, da de indeholder nødvendig information for at kunne gennemføre en validering.

Der findes en bred vifte af services (både kommercielle og ikke-kommercielle) til generering af elektroniske signaturer og elektroniske segl. Disse elektroniske signaturer kan være baseret på standardformater beskrevet ovenfor, ikke-standardiserede formater eller en kombination heraf. Der ses fx modeller, hvor underskriverne skriver under på et PDF-dokument i et ikke-standardiseret format, hvorefter integriteten af det endelige dokument sikres ved hjælp af et standardiseret elektronisk segl fra udbyderen af signeringsservicen.



3. Valg af accepterede signaturer og Validering

Fastlæggelse af accepterede elektroniske signaturer og segl

Det er op til den enkelte modtagerpart, hvilke elektroniske signaturer og/eller elektroniske segl, man ønsker at acceptere for hver brugsscenarie eller applikation, da dette vil afhænge af den konkrete kontekst. Ud fra et forretningsmæssigt og juridisk perspektiv bør det overvejes, hvilke af følgende muligheder en selvbetjeningsløsning skal anvende:

- Kvalificerede elektroniske signaturer
- Kvalificerede elektroniske segl
- Ikke-kvalificerede elektroniske signaturer eller segl baseret på såkaldte OCES-certifikater (fx udstedt gennem MitID Erhverv
- Ikke-kvalificerede og ikke-standardiserede elektroniske signaturer eller segl.

I overvejelserne bør følgende indgå

- Juridiske aspekter, herunder retsvirkning og bevisværdi,
- Forretningsmæssige aspekter (er det fx muligt at sikre, at underskriver er identisk med den part, som forventes at signere dokumentet),
- Tekniske aspekter (er det fx praktisk muligt for underskriver at generere signatur),
- Tidsmæssige aspekter (hvor lang tid, skal det være muligt at bevise gyldigheden af signaturen) og
- Internationale aspekter (skal signaturen fx have bevisværdi uden for DK)

Der kan være lovgivningsmæssige krav, der skal inkluderes i valg af understøttede elektroniske signaturer og segl. Bemærk, at offentlige myndigheder her særligt skal være opmærksomme på forpligtelserne i [eIDAS] artikel 27 og artikel 37.

Anbefaling 1
Undersøg eventuelle lovgivningsmæssige forpligtelser til at understøtte bestemte signaturformater.

Desuden bør man som modtagerpart beslutte, hvilken type en given signatur eller segl skal være for at blive accepteret. Som udgangspunkt anbefales det, at man stiller krav om LTV- eller LTA-format, da disse indeholder de nødvendige informationer til at kunne validere signaturen eller seglet over tid og giver en størst mulig uafhængighed af leverandører af signaturløsning.

Anbefaling 2
Sørg for at valgte signaturtype og signaturformat kan valideres i perioden, hvor signaturen skal have retsvirkning. Herunder vurder evt. afhængigheder af leverandører.

I forbindelse med fastlæggelse af elektroniske signaturer og segl bør der udover forretningsmæssige kompetencer involveres tekniske og juridiske domænekompetencer.

Anbefaling 3
Ved design af den digital selvbetjeningsløsning, hvor signering eller forsegling indgår, bør personer med teknisk og juridisk domæneviden inddrages.

Validering og sikring af elektroniske signaturer og segl over tid

Når modtagerparten har fastlagt hvilke typer af elektroniske signaturer og segl der ønskes accepteret i en given digital selvbetjeningsløsning, skal det fastlægges, hvordan signatur og/eller segl valideres, og hvordan signaturen eller seglet sikres i det tidsrum, hvor integritet og autenticitet af de signerede data er relevante.

For AdES standardformaterne kan valideringen ske jf. proces beskrevet i standarden ETSI TS 119 102-1. Man kan som modtagerpart enten selv udvikle en løsning til validering, eller man kan benytte en valideringstjeneste. Digitaliseringsstyrelsen stiller, på vegne af den danske stat, en valideringstjeneste til rådighed (se beskrivelse i afsnittet nedenfor om Den Danske Stats Valideringstjeneste).

For B (Basic) og BT (Basic/Timestamp) formerne af AdES bør man iværksætte ekstra tiltag for at sikre beviset i den tid signaturen skal have retsvirkning, mens LTV (Long Term Validation) og LTA (Long Term Availability) i en vis udstrækning har denne sikring for bevisværdi indbygget.

Hvis man ønsker at kunne validere et ikke-standardiseret signatur- og seglformat, bør man som modtagerpart indgå en dialog med udbyderen af den signeringsservice, der udsteder disse formater med henblik på at afgøre, hvordan signaturer/segl valideres og sikres over tid. Som modtagerpart bør man vurdere konsekvenserne, hvis det på sigt ikke er muligt at anvende udbyderens valideringstjeneste, fx hvis udbyderen lukker for løsningen, eller at validering bliver pålagt en uacceptabel licens/omkostning.

Ved anvendelse af enhver ekstern valideringstjeneste skal man sikre sig, at relevant lovgivning herunder GDPR overholdes.

Man bør fastlægge og kommunikere en politik for understøttede elektroniske signaturer og -segl til alle i organisationen, for hvem det er relevant. For systemer med automatisk validering skal specifikation indeholde krav til signaturer og/eller segl inklusiv evt. supplerende systembeviser der bringes i anvendelse for at sikre integriteten. For mere manuelle processer bør der udvikles guides til sagsbehandler i håndtering og validering af accepterede elektroniske signaturer og segl.

Anbefaling 4
Som organisationen bør man kommunikere politik for accepterede elektroniske signaturer og segl til relevante parter i organisationen evt. med guides til håndtering og validering.

Den Danske Stat Valideringstjeneste

Digitaliseringsstyrelsen udbyder på vegne af den danske stat en gratis tjeneste til validering af elektroniske signaturer og segl i digitale dokumenter. Det er muligt at uploade dokumenter til tjenesten, der efterfølgende vil forsøge at validere eventuelle elektroniske signaturer og segl i dokumenterne.

Valideringstjenesten kan anvendes til validering følgende formater:

- PAdES (B, T, LTV og LTA)
- XAdES (B, T, LTV og LTA)
- CAdES (B, T, LTV og LTA)
- ASiC

Begrænsninger:

- Tjenesten validerer kun kvalificerede elektroniske signaturer og segl, hvor certifikatudsteder er listet på EU's positivliste over kvalificerede certifikatudstedere (https://eidas.ec.europa.eu/efda/tl-browse) eller er udsteder af OCES-certifikater.
- Tjenesten validerer kun dokumenter med én signatur eller ét segl

Inden anvendelse af tjenesten skal man som dataansvarlig selv overveje eventuelle konsekvenser ift. GDPR, hvis de signerede dokumenter indeholder persondata. Det bemærkes, at Den Danske Stats Valideringstjeneste ikke lagrer de validerede data og alene gennemfører en automatiseret behandling, hvor dokumentet slettes umiddelbart efter den tekniske validering.

Bemærk, at hvis en kommerciel løsning er baseret på et ikke-standardiseret format for underskriverne og en efterfølgende forsegling med udbyderens segl, vil valideringstjenesten typisk validere seglet selvom seglet udelukkende er en sikring af dokumentets integritet. I dette tilfælde er det nødvendigt at kontakte udbyderen af signeringsservicen for yderligere indsigt i de indeholdte elektroniske signaturer genereret af de egentlige underskrivere, jf. beskrivelsen ovenfor.

4. Referencer

[eIDAS] "Europa-Parlamentets og Rådets forordning (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF".

https://eur-lex.europa.eu/eli/reg/2014/910/oj

Bemærk at denne forordning er opdateret med [eIDAS2].

[eIDAS2] ”Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet”.

http://data.europa.eu/eli/reg/2024/1183/oj

[Impl1506] ”Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market”.

https://eur-lex.europa.eu/eli/dec_impl/2015/1506/oj

[Betænk1456] Betænkning 1456/2004 ”e-signaturs retsvirkninger” ISBN 87- 601-9994-6

https://www.xn--betnkninger-c9a.dk/wp-content/uploads/2021/02/1456.pdf