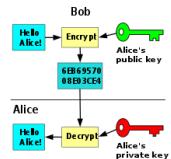


# **DIGITALE SIGNATURER – PAdES – XAdES - PDF/A**

## **PRESENTASJON – NORDIG – OKTOBER 2017**

*Erik Aaberg, eriaab@arkivverket.no*



# Utgangspunkt - elektronisk ID



Hjelp og veiledning > ID-porten > Slik skaffer du deg elektronisk ID

Søk

## Slik skaffer du deg elektronisk ID

Du kan velge mellom fem alternativer for elektronisk ID når du skal logge inn til offentlige tjenester:

**MinID** er en offentlig utstedt, personlig elektronisk ID som gir tilgang til offentlige tjenester på mellomhøyt sikkerhetsnivå, nivå 3. MinID utstedes av Direktoratet for forvaltning og IKT (Difi), og kan bestilles fra det året du fyller 13 år.

[Mer om registrering og innlogging med MinID.](#)

**BankID** er en personlig, elektronisk ID som gir tilgang til offentlige tjenester på høyeste sikkerhetsnivå, nivå 4. BankID utstedes av banken din, og kan bli utsendt til personer som er fylt 15 år, men bankene opererer med egne aldersgrenser.

[Mer om bestilling og innlogging med BankID.](#)

**BankID på mobil** er en personlig, elektronisk ID som gir tilgang til offentlige tjenester på høyeste sikkerhetsnivå, nivå 4. BankID på mobil utstedes av banken din. Husk at du må ha vanlig BankID med koder fra banken din før, og at du bare kan aktivere BankID på mobil fra banken som ga deg BankID.

[Mer om bestilling og innlogging med BankID på mobil.](#)

**Bypass ID** er en personlig, elektronisk ID som gir tilgang til offentlige tjenester på høyeste sikkerhetsnivå, nivå 4. Den utstedes av Bypass AS, og leveres som [Bypass ID på smartkort](#) og som [Bypass ID i mobil](#). Alle som har et smartkort fra Bypass, kan ta i bruk Bypass ID i mobil. Bypass ID opererer ikke med aldersgrense, men krever legitimering og personlig underskrift ved utstedelse.

[Mer om bestilling og innlogging med Bypass ID.](#)

**Commfides** er en personlig, elektronisk ID som gir tilgang til offentlige tjenester på høyeste sikkerhetsnivå, nivå 4. Commfides utstedes av Commfides Norge AS, og leveres som elektronisk ID på en sikker USB-pinne. Commfides opererer ikke med aldersgrense, men krever legitimering og personlig underskrift ved utstedelse.

[Mer om bestilling og innlogging med Commfides](#)

### ID-porten

- MinID

- BankID

- Bypass ID

- Commfides

- BankID på mobil

### Kjente feil og løsninger

### Sikkerhet og informasjonskapsler

Digital postkasse - spørsmål og svar

Oppdater kontaktinformasjon

Reservasjon

Opplæringsprogram

e-signering

Slett kontaktinformasjon



# De nye standarder PAdEs og XAdES

  
**WIKIPEDIA**  
The Free Encyclopedia

Main page  
Contents  
Featured content  
Current events  
Random article

Not logged in Talk Contributions Create account Log in

Article [Talk](#) Read Edit View history Search Wikipedia

## PAdES

From Wikipedia, the free encyclopedia

*For the Romanian commune, see [Pades](#).*

**PAdES** (PDF Advanced Electronic Signatures) is a set of restrictions and extensions to PDF and ISO 32000-1<sup>[1]</sup> making it suitable for Advanced Electronic Signature. This is published by ETSI as TS 102 778.<sup>[2]</sup>

  
**WIKIPEDIA**  
The Free Encyclopedia

Main page  
Contents  
Featured content

Not logged in Talk Contributions Create account Log in

Article [Talk](#) Read Edit View history Search Wikipedia

## XAdES

From Wikipedia, the free encyclopedia

**XAdES** (short for "XML Advanced Electronic Signatures") is a set of extensions to XML-DSig recommendation making it suitable for Advanced Electronic Signatures. W3C and ETSI maintain and update XAdES together.<sup>[1]</sup>

## ETSI

From Wikipedia, the free encyclopedia

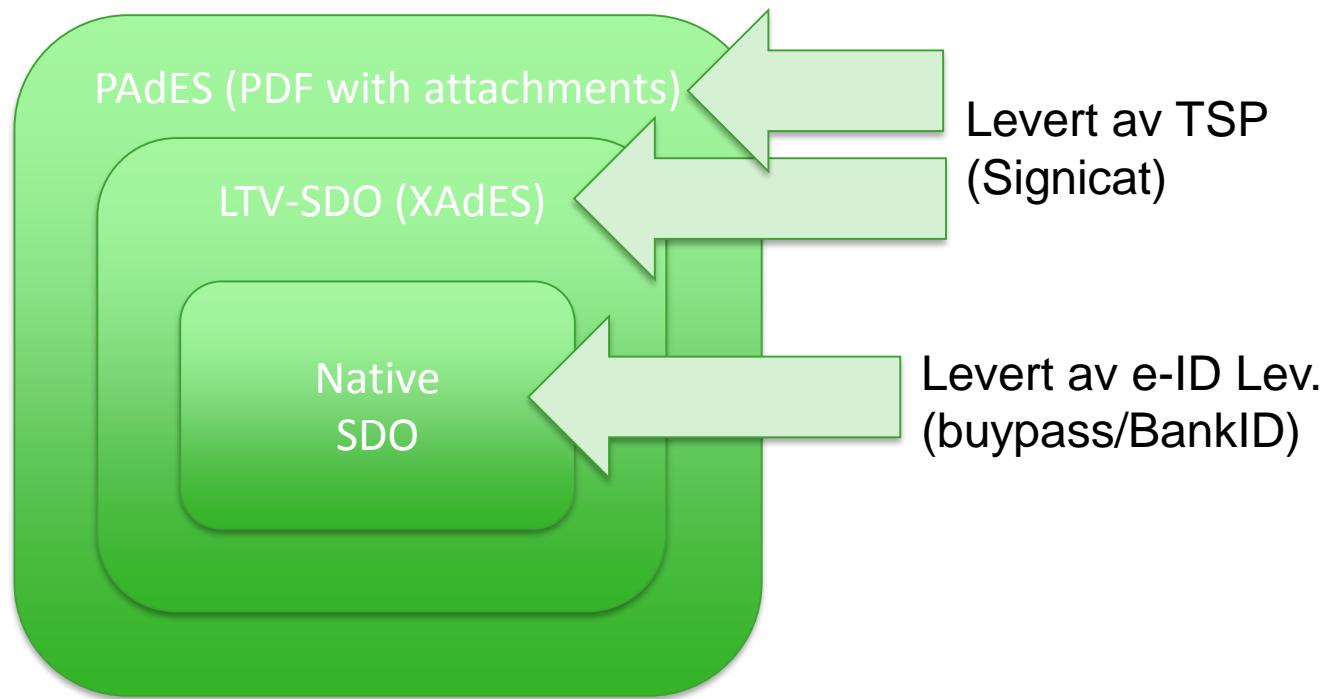
*Not to be confused with the ICAO code of the Ingolstadt Manching Airport.  
Not to be confused with Etsy.*

The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization





## PAdES løken

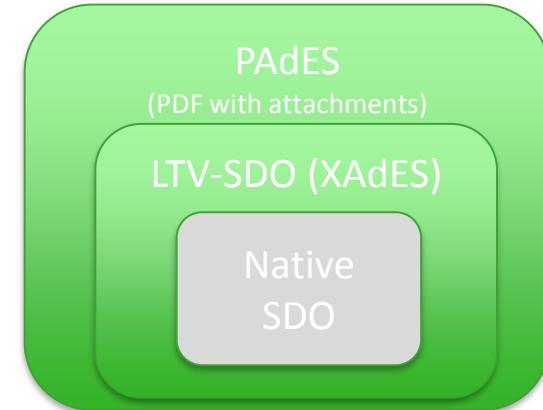


*TSP = Trusted Service Provider*



# Native SDO

- ▶ SDO = Signed Data Object
- ▶ Forskjellig innhold/format for hver e-ID leverandør
- ▶ BankID
  - ▶ Signeres med sluttbrukersertifikat
  - ▶ Forsegles med brukerstedssertifikatet
    - ▶ **Difi sitt sertifikat**
- ▶ Buypass
  - ▶ Signeres med sluttbrukersertifikat
  - ▶ Benytter ikke brukerstedssertifikater





LTV-SDO (XAdES)

Native  
SDO

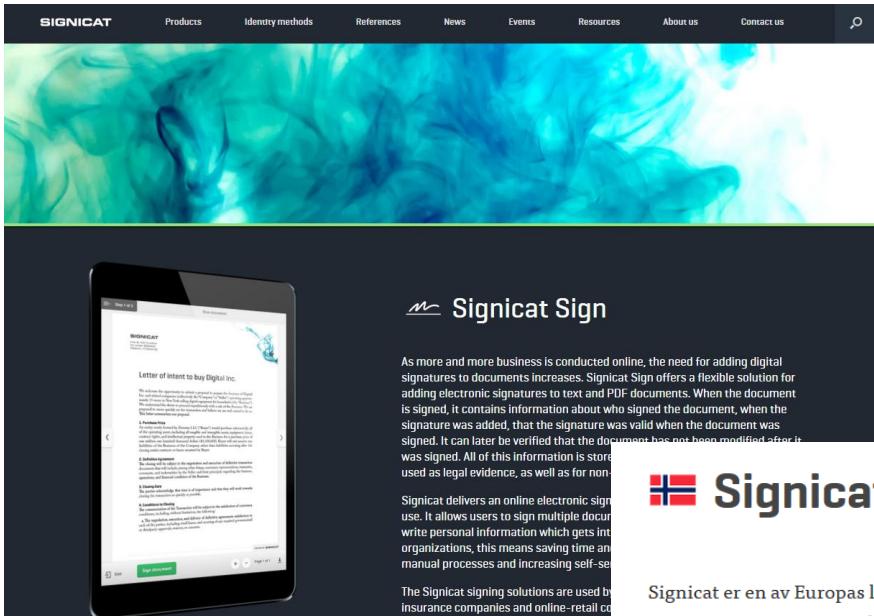
## LTV-SDO

- ▶ SDO = Signed Data Object
- ▶ LTV = Long Term Validation

- ▶ Pakker inn underliggende native SDO
- ▶ Tar høyde for forskjellige underliggende signeringsformater
- ▶ Sikrer at TTP-logg og andre nødvendige mekanismér for langtidsvalidering integritetssikres korrekt
- ▶ Pakketeres i henhold til Signicats packagin policy
  - ▶ <https://id.signicat.com/plugins/bankid-js/packagingpolicy/Packaging-Policy-BankID-NO-1.2.pdf>
  - ▶ <https://id.signicat.com/plugins/ltvso/Packaging-Policy-LTV-1.2.pdf>
- ▶ Forsegles av **Signicat** som har rollen som Trusted Service Provider (TSP)



# Signicat signerer - LTV-en



**Signicat Sign**

As more and more business is conducted online, the need for adding digital signatures to documents increases. Signicat Sign offers a flexible solution for adding electronic signatures to text and PDF documents. When the document is signed, it contains information about who signed the document, when the signature was added, that the signature was valid when the document was signed. It can later be verified that the document has not been modified after it was signed. All of this information is stored as legal evidence, as well as for non-

Signicat delivers an online electronic signature solution for both individuals and organizations. It allows users to sign multiple documents at once, write personal information which gets integrated into the document, and add a timestamp to the document. This means saving time and money on manual processes and increasing self-service levels.

The Signicat signing solutions are used by many companies, including insurance companies and online-retail companies.

PAdES  
(PDF with attachments)

LTV-SDO (XAdES)

Native  
SDO



## PAdES - PDF - dokumentet

PAdES  
(PDF with attachments)

LTV-SDO (XAdES)

Native  
SDO

- ▶ Kan åpnes og distribueres som en PDF i alle PDF-lesere
- ▶ Opprinnelig PDF er endre på følgende måte:
  - ▶ En forside med signeringsinformasjon
  - ▶ Vannmerke/signeringsinformasjon på hver side
  - ▶ Inkludert 2 vedlegg
- ▶ PAdES vedlegg
  - ▶ Visningsdokument med vannmerke og signeringsinformasjon
  - ▶ Forseglet LTV-SDO
- ▶ Hele dokumentet er forseglet og kan valideres



## PAdES – Varighet



- Det norske Arkivverket sjekker ikke gyldighet ved mottak
- "Uendelig" - ikke fordi signaturen har uendelig varighet, men bekreftelsen på at signaturen **var** ekte er "uendelig"



## PAdES – Kompatibilitet PDF/A

- ▶ XAdES er et XML attachment til PDF-en
- ▶ PDF/A-1 tillater ikke vedlegg - - -
- ▶ PDF/A-2 tillater vedlegg, men bare dersom de er PDF/A - -
- ▶ PDF/A-3 tillater alle vedlegg, men er ikke et foretrukket format
- ▶ Vår løsning:  
Vi godtar PAdES/XAdDES - PDF - dokumenter som er PDF/A-3, **forutsatt** at de med unntak av vedlegget er PDF/A-2 compliant