XAdES vs PAdES

Johannes Döring

CTO, INBATEK CO., LTD

CTO, ADDIVO GmbH

CEO, COM-STYLE

An overview about the history of signing with XML and PDF

Digital signatures

- An electronic signature is a paperless way to sign a document using a unique credential associated with a given person that is logically attached to or associated with the document
- Electronic signatures can be used to authenticate the signer as well as detect any changes made to the document after it was signed.
- Electronic signatures provide real benefits. For example, they promote the emergence of fully automated purchasing processes by enabling buyers and sellers to sign and approve transactions without the need for traditional “wet” (paper-based) signatures.

INBATEK
Intelligent Business & Technology

Legal overview

- Directive in force in every EU Member State about electronic signature: “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”
- Being deliberately neutral regarding
  - technology and security requirements
  - confers to all kinds of electronic signatures a potential legal validity
  - provided their authenticity is not contested.
- Advanced electronic signature (AdES)
- Qualified electronic signature (QES)

INBATEK
Intelligent Business & Technology

Requirements for AdES

- It is uniquely linked to the signatory.
- It is capable of identifying the signatory
- It is created in a way that the signatory can maintain sole control.
- It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Defined activities and services

- The definition of qualified cryptographic certificates
- What it takes for a smart card or token to become an SSCD
- The requirements that CSPs must meet
- How certificates are revoked
- How lists of CSPs and their qualified certificates that have been officially supervised/accredited by a government authority (Trust Status Lists) can be communicated across borders
- How to represent a digital signature as a data structure tied to the data or document being signed

INBATEK
Intelligent Business & Technology

Defined by

- Internet Engineering Task Force (IETF)
- International Standards Organization (ISO)
- European Telecommunications Standards Institute (ETSI)
- European Committee for Standardization (ECS)

- For example: Public-Key Infrastructure (X.509) (pkix)
  - ww.ietf.org/dyn/wg/charter/pkix-charter.html

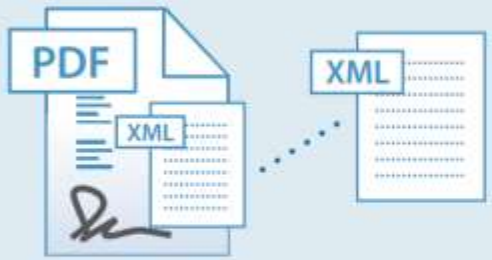
and Infrastructures (ESI) technical

- CAdES
- XAdES
- PAdES

- The biggest difference between PAdES, CAdES, and XAdES is that PAdES defines how software that is processing digital signatures in PDF documents should operate
- Various document workflows employing digital signatures are supported by standard off-the-shelf PDF software.

INBATEK
Intelligent Business & Technology

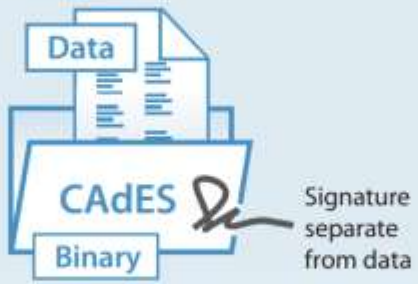
PAdES



Self-contained signature

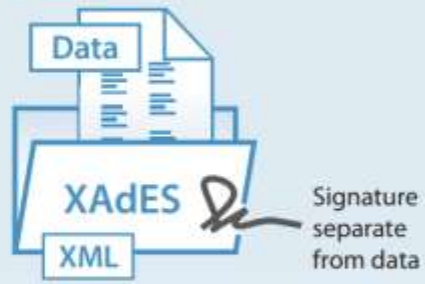
- Contains signatures within the PDF
- Supports XML data
- Included within the ISO PDF Standard
- Includes signing and verifying in PDF software—no customized programming required
- Supports serial form-fill and signatures for approval workflows
- Supports a visual signature appearance in the document
- Provides long-term validity

CAdES



- Enables signing of any data, including PDF
- Supports two signing methods:
  - Detached: the data being signed is separate from the signature (data and signature may be packaged together in some way)
  - Encapsulated: the data is wrapped within the signature structure
- Renders signature as binary data
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Appearance is up to the application to provide
- Provides long-term validity

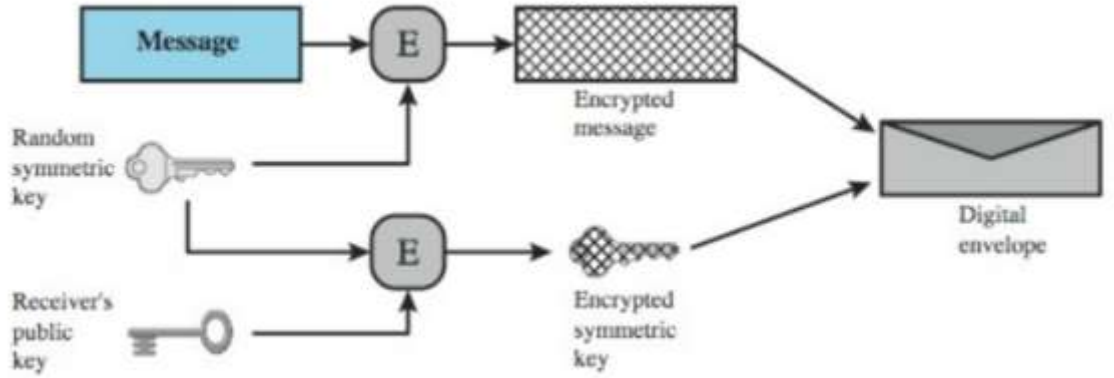
XAdES



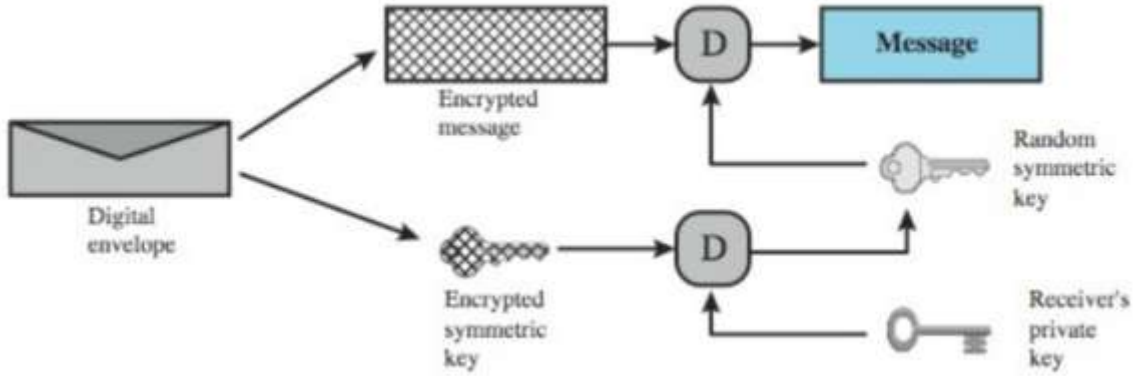
- Provides an all XML solution
  - Signs any data including PDF and binary
  - Supports XML package or separate files
- Often requires customization of applications or generic signing outside the application
- Supports multiple signatures applied in parallel, serial by repeated signing
- Supports a visual signature appearance, depending on the application
- Provides long-term validity

Signing always needs a container/envelope

- Digital signatures don’t modify the document they sign
- Equates to the same thing as a sealed envelope containing an unsigned letter



(a) Creation of a digital envelope



(b) Opening a digital envelope

INBATEK
Intelligent Business & Technology

So which envelope do we use then?

- In case of PDF, the PDF format is the container format
  - PDF can contain images
  - Fonts
  - PDF can even contain attachments
- Signing a PDF files, signs everything, also the e-tax invoice XML attachment
- Even versioning for workflows requiring multiple signatures is supported

INBATEK
Intelligent Business & Technology

Official PAdES CSPs (Adobe Approved Trust List members)

- https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html

- Applications from any country are welcome
- However CSPs have to follow these requirements:
- https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf
- An audit process will confirm, that the requirements are fulfilled

INBATEK
Intelligent Business & Technology

XML?

- XML is just a format to store data
- There is no difference, if something is data or an envelope
- There is no definition, how versioning would work

- XML Digital Signatures (XML-DSIG) define an XML syntax for digital signatures and is defined in the W3C recommendation XML Signature Syntax and Processing
- XAdES is built around the XML Digital Signatures (XML-DSIG) and adds more features
- No standard software exists for XAdES, since for XML it is not defined how to display the information to the end-user
- XAdES requires the users to build an own infrastructure of software and components, where in case of PDF applications and components already exist for many usecases

INBATEK
Intelligent Business & Technology

Example for XML-DSIG

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
       <Transforms>
       <DigestMethod>
       <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```


INBATEK
Intelligent Business & Technology

XAdES six profiles (forms)

- **XAdES** (also named **XAdES-BES** for "**Basic Electronic Signature**"), basic form just satisfying Directive legal requirements for advanced signature;
- **XAdES-T** (timestamp), adding timestamp field to protect against repudiation
- **XAdES-C** (complete), adding references to verification data (certificates and revocation lists) to the signed documents to allow off-line verification and verification in future (but does not store the actual data);
- **XAdES-X** (extended), adding timestamps on the references introduced by XAdES-C to protect against possible compromise of certificates in chain in future;
- **XAdES-X-L** (extended long-term), adding actual certificates and revocation lists to the signed document to allow verification in future even if their original source is not available;
- **XAdES-A** (archival), adding possibility for periodical timestamping (e.g. each year) of the archived document to prevent compromise caused by weakening signature during long-time storage period.

INBATEK
Intelligent Business & Technology

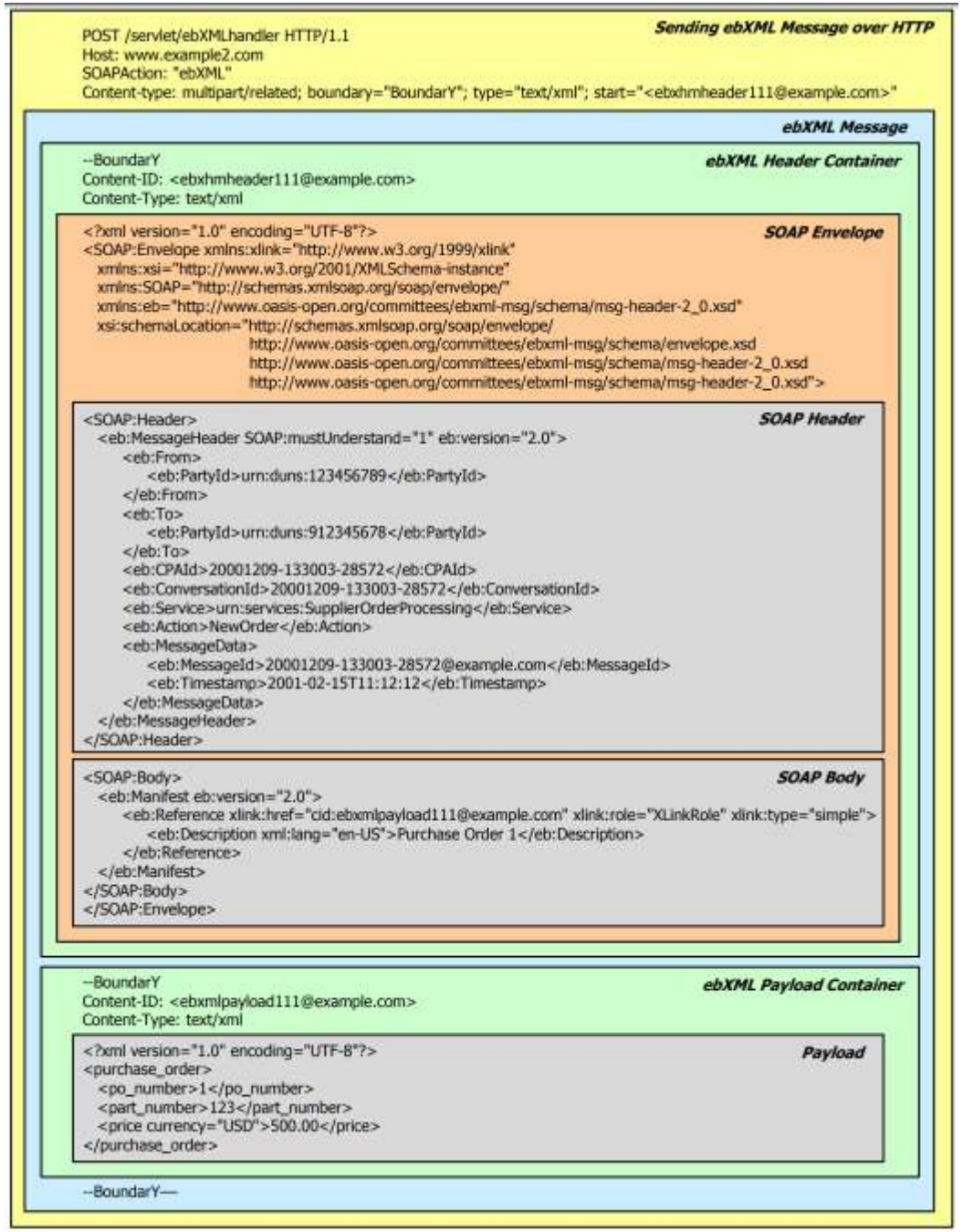
```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" Id="xmldsig-9417a92f-c32c-4ada-b8ab-
5c9ea22018e9">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    <ds:Reference Id="xmldsig-9417a92f-c32c-4ada-b8ab-5c9ea22018e9-ref0">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>LPNKwDiu5awG+TPd0dqYJuC7k4PBPY4LCI/O0LSpW1s=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference Type="http://uri.etsi.org/01903#SignedProperties" URI="#xmldsig-9417a92f-c32c-4ada-b8ab-
5c9ea22018e9-signedprops">
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
      <ds:DigestValue>KrfIQhXHcit8CBBEUpEgJGL+I7aP7AuGxm5/MKaY0fA=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue Id="xmldsig-9417a92f-c32c-4ada-b8ab-5c9ea22018e9-sigvalue">
    dZnEungCgdvI+PsiAY74uVnA3CNS/tZ7uAdiQg4V56CH3XdEm9Za70ZRkzYu3ZouvyzwQwYkrzE4
    iRtCLf49Km5XzITxuOIZTTrTs/XIkDGOx8JoloHF9x7SS6zV1QhelEKdkj+hEv0rCVErA8XXANSL
    GULuqmnGImCXlffXMJU=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>
        MIICh....PEM....XX4=
      </ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
```

….

INBATEK
Intelligent Business & Technology

```
 <ds:Object>
    <xades:QualifyingProperties xmlns:xades="http://uri.etsi.org/01903/v1.3.2#"
xmlns:xades141="http://uri.etsi.org/01903/v1.4.1#" Target="#xmldsig-9417a92f-c32c-4ada-b8ab-
5c9ea22018e9">
      <xades:SignedProperties Id="xmldsig-9417a92f-c32c-4ada-b8ab-5c9ea22018e9-signedprops">
        <xades:SignedSignatureProperties>
          <xades:SigningTime>2017-04-21T18:32:40.461+01:00</xades:SigningTime>
          <xades:SigningCertificate>
            <xades:Cert>
              <xades:CertDigest>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>yScwzjo9znhFNIxY7fl2gnK1UhFTFcjXJE8aGBgfzfk=</ds:DigestValue>
              </xades:CertDigest>
              <xades:IssuerSerial>
                <ds:X509IssuerName>CN=CA2-CP.02.01,OU=Testing,OU=Dod,O=U.S.
Government,C=US</ds:X509IssuerName>
                <ds:X509SerialNumber>8</ds:X509SerialNumber>
              </xades:IssuerSerial>
            </xades:Cert>
          </xades:SigningCertificate>
        </xades:SignedSignatureProperties>
      </xades:SignedProperties>
      <xades:UnsignedProperties>
        <xades:UnsignedSignatureProperties>
          <xades:SignatureTimeStamp>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            <xades:EncapsulatedTimeStamp>
              MIAGCSqGSIb3DQEHAqCAMIIVAgIBAzELMAkGBSsOAwIaBQAwggE3BgsqhkiG9w0BCRABBKCCASYE
              ggEiMIIBHgIAAAAAA==
            </xades:EncapsulatedTimeStamp>
          </xades:SignatureTimeStamp>
          <xades:CompleteCertificateRefs>
            <xades:CertRefs>
              <xades:Cert>
                <xades:CertDigest>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>6F5s4TtqSCTt+/C6kxSWxGiyQ/2uBQ/tQ2IFjNjna3U=</ds:DigestValue>
                </xades:CertDigest>
                <xades:IssuerSerial>
                  <ds:X509IssuerName>CN=CA1-CP.02.01,OU=Testing,OU=Dod,O=U.S.
Government,C=US</ds:X509IssuerName>
                  <ds:X509SerialNumber>7</ds:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
              <xades:Cert>
                <xades:CertDigest>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>YvyeUickj8O9yN2JXM991ULBr5v7aQnC0Dl5yNm6HnM=</ds:DigestValue>
                </xades:CertDigest>
                <xades:IssuerSerial>
                  <ds:X509IssuerName>CN=Trust Anchor,OU=Testing,OU=DoD,O=U.S.
Government,C=US</ds:X509IssuerName>
                  <ds:X509SerialNumber>6</ds:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
              <xades:Cert>
                <xades:CertDigest>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>3FPfkaoV1oQ0qvdahhmupFWYoIMIw0Aekh0eJz5BpH0=</ds:DigestValue>
                </xades:CertDigest>
                <xades:IssuerSerial>
                  <ds:X509IssuerName>CN=Trust Anchor,OU=Testing,OU=DoD,O=U.S.
Government,C=US</ds:X509IssuerName>
                  <ds:X509SerialNumber>99999</ds:X509SerialNumber>
                </xades:IssuerSerial>
              </xades:Cert>
            </xades:CertRefs>
          </xades:CompleteCertificateRefs>
          <xades:CompleteRevocationRefs>
            <xades:CRLRefs>
              <xades:CRLRef>
                <xades:DigestAlgAndValue>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>BxdjnMvJhUPD983q3SAF8rwz+xj9kig5cqMbuQlF3Y4=</ds:DigestValue>
                </xades:DigestAlgAndValue>
                <xades:CRLIdentifier>
                  <xades:Issuer>CN=CA2-CP.02.01,OU=Testing,OU=Dod,O=U.S. Government,C=US</xades:Issuer>
                  <xades:IssueTime>1999-01-01T12:01:00.000Z</xades:IssueTime>
                  <xades:Number>1</xades:Number>
                </xades:CRLIdentifier>
              </xades:CRLRef>
              <xades:CRLRef>
                <xades:DigestAlgAndValue>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>i1mVIJL63tU9nnIhbS1uxiOHYSrEtMsehOKLK2hDD8U=</ds:DigestValue>
                </xades:DigestAlgAndValue>
                <xades:CRLIdentifier>
                  <xades:Issuer>CN=Trust Anchor,OU=Testing,OU=DoD,O=U.S. Government,C=US</xades:Issuer>
                  <xades:IssueTime>1999-01-01T12:01:00.000Z</xades:IssueTime>
                  <xades:Number>1</xades:Number>
                </xades:CRLIdentifier>
              </xades:CRLRef>
              <xades:CRLRef>
                <xades:DigestAlgAndValue>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                  <ds:DigestValue>v4dIw4odnHNqHyAoHbc1l3C17kCF/F3Z2ii9v8n2TYA=</ds:DigestValue>
                </xades:DigestAlgAndValue>
                <xades:CRLIdentifier>
                  <xades:Issuer>CN=CA1-CP.02.01,OU=Testing,OU=Dod,O=U.S. Government,C=US</xades:Issuer>
                  <xades:IssueTime>1999-01-01T12:01:00.000Z</xades:IssueTime>
                  <xades:Number>1</xades:Number>
                </xades:CRLIdentifier>
              </xades:CRLRef>
            </xades:CRLRefs>
          </xades:CompleteRevocationRefs>
        </xades:UnsignedSignatureProperties>
      </xades:UnsignedProperties>
    </xades:QualifyingProperties>
  </ds:Object>
</ds:Signature>
```


INBATEK
Intelligent Business & Technology



DEMO TIME

- XAdES
- PAdES

INBATEK
Intelligent Business & Technology

For questions or inquiries contact us

About E-Tax-Invoice, our solutions shown here or any iText related topic including iText licensing and offers contact us at:

- INBATEK CO,.LTD
  - Johannes@inbatek.com,
  - Sujira@inbatek.com
  - +66-21074027
  - +66-9170 11159
  - English Skype: johannesdoering/ Thai Skype:nhing.phd
  - Whatsapp: +491713488981/Line: infinity001nhing

INBATEK
Intelligent Business & Technology

Thank you for your attention

บริษัทอินบาเทคจำกัด
INBATEK CO.,LTD
Intelligent Business & Technology

INBATEK
Intelligent Business & Technology