DOI: 10.15199/13.2015.3.20

Formats of electronic signature

(Formaty podpisu elektronicznego)

dr inż., MAREK HOŁYŃSKI, dr inż. prof. ndzw. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

One of the central problems that come up in the practical use of electronic signatures involves the compatibility of various applications and the constantly changing standards of electronic signature creation [1]. At present four such standards dominate the electronic signature market. These are: CAdES, XAdES, PAdES and ASiC; each has been described in the documents issued by ETSI (European Telecommunications Standards Institute). These standards describe the so-called advanced electronic signature, compliant with the requirements set out in Directive 99/93/EC.

Each electronic signature should contain essential information that identifies the signer, as well as its generation technique. It is also recommended that the certificate used to create the signature be attached to the document. The structure of the signature also contains references to the data that has been signed.

All this information will be used to verify the signature's validity. The verifying application must read the data contained in the signed file. Standardization and defining the location where the pertinent data would reside makes it possible for different applications to recognize the signature. For instance, it is necessary to provide information about the hash function employed (usually one from the SHA family [2]), and the signature algorithm (the one most commonly used at present is the RSA [2], with a key size of 2048 bits). Information contained in the certificate facilitates the building and validation of the certification path. It may also indicate the location where the certificate's validity can be checked by means of a CRL or the OCSP service. Standards that pertain to the XAdES and CAdES formats describe the correct approach to recording the information about the algorithms used, the signature itself, the signer, conditions to be met for signature verification to be valid, as well as other data that facilitate it (such as CRLs and OCSP responses). The basic form of the signature is BES (Basic Electronic Signature), which contains the minimum of necessary data. Additional information can be added to the structure of a BES signature.

– EPES – Explicit Policy-based Electronic Signature. Includes a signature-policy identifier
– T – TIME. A time-stamp is added to the EPES structure
– C – Complete. The following elements are added to the EPES structure: references to the full certification path, CRLs, certification paths for the CRLs.

The XAdES format

The XML Advanced Electronic Signature (XAdES), described in the ETSI standard TS 103 171, is an extension of the XMLDSIG structure designed by W3C. Its most basic form is XAdES-BES (Basic Electronic Signature). Below is shown the structure of an XML signature, which can be appended to the document being signed, or stored in a separate signature file:

```
<Signature ID>
     <SignedInfo>
       <CanonicalizationMethod/>
       <SignatureMethod/>
       (<Reference URI >
         (<Transforms>)
         <DigestMethod>
         <DigestValue>
       </Reference>)
     </SignedInfo>
     <SignatureValue>
    (<KeyInfo>)
    (<Object ID>)
</Signature>
```

XMLDSIG contains information about the technical means used in the creation of the signature, as well as references to the data that was signed. Additional content can be inserted into the DS: Object node. This element is used in the XAdES format for the incorporation of such information as, for instance:

– SigningTime – an attribute specifying the time when the signature was created
– CommitmentTypeIndication – an attribute indicating the purpose for which the signature was created, e.g. a statement of intent or non-repudiation.
– CounterSignature – an attribute containing a countersignature.

The first two attributes presented above as examples must be signed along with the data. The countersignature, on the other hand, is yet another signature, applied at a later date.

XAdES-EPES (Explicit Policy based Electronic Signature), an extension of the basic form, contains a signature policy identifier in the element <signedSignatureProperties>.

Electronic signatures conforming to the XAdES specification may also contain a time-stamp, confirming that the document was signed before a given date. This form is known as XAdES-T (Time). Its extended version is XAdES-C (Complete), which includes information necessary to verify the validity of the signer's certificate: references to the full certification path and the CRLs (A CRL contains the serial numbers of certificates that have been revoked or suspended, thus making it possible to determine whether the signer's certificate is still valid).

```
XMLDISG
<ds:Signature ID?>
  <ds: SignedInfo>
   <ds:CanonicalizationMethod/>
   <ds:SignatureMethod/>
  (<ds:Reference URI? >
    (<ds:Transforms>)?
    <ds:DigestMethod/>
    <ds:DigeetValue/>
   </ds: Reference>)
 </ds:SignedInfo>
 <ds:SignatureValue/>
(<de:KeyInfo>)?

<ds:Object>
      <SignedSignatureProperties>
      (SigningTime)?
      (SigningCert ificate)?
      (SignaturePolicyIdentifier)?
      (SignatureProductionPlace)?
      (SignerRole)?
    </SignedSignatureProperties>

    <SignedDataObjectProperties>
      (DataObjectFormat)*
      (ContnitmentTypelndication)*
      (AllDataObjectsTimeSCamp)*
      (IndividualDataObject8TimeStamp)
    </SignedDataObjectProperties>

    </SignedProperties>

    <UnsignedProperties>

      <UnsignedSignatureProperties>
        (Countersignature)*
        (SignatureTimeStarnp)+
        (CompleteCertificateRefs)
        (CompleteRevocationRefs)
        (AttributeCertificateRefs)?
        (AttributeRevocationRefs)?
      </UnsignedSignatureProperties>

     </UnsignedProperties>

  </QualifyingProperties>
 </ds:Object>
</ds:Signature>
```

XAdBS-BES(-EPES)
XAdES-T
XAdES-C

Fig. 1. Structure of XAdES-C format
Rys. 1. Struktura formatu XADES-C

The CAdES format

The structure of a CAdES signature conforms to the rules defined as part of the Cryptographic Message Syntax (CMS) standard [4]. The CMS is derived from PKCS#7, which was devised by RSA Laboratories in 1993, and it describes not only the implementation of electronic signatures, but also the encryption or authentication of data. In CMS information is encoded using ASN.1 (Abstract Syntax Notation One), in the form of 8-bit strings.

The specification for the CAdES format was described in ETSI TS 101733. Below follows an example structure that contains information about the signer, SignerInfo:

```
SignerInfo ::= SEQUENCE {
   version CMSVersion,
   sid SignerIdentifier,
   digestAlgorithm DigestAlgorithmIdentifier,
   signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
   signatureAlgorithm SignatureAlgorithmIdentifier,
   signature SignatureValue,
   unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }

 SignerIdentifier ::= CHOICE {
   issuerAndSerialNumber IssuerAndSerialNumber,
   subjectKeyIdentifier [0] SubjectKeyIdentifier }

 SignedAttributes ::= SET SIZE (1..MAX) OF Attribute

 UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute

 Attribute ::= SEQUENCE {
   attrType OBJECT IDENTIFIER,
   attrValues SET OF AttributeValue }

 AttributeValue ::= ANY

 SignatureValue ::= OCTET STRING
```

The CAdES format makes it possible to create a number of different versions of a signed file:

CAdES – BES – the simplest, basic form
CAdES – EPES – extended version, with a reference to the signature policy
CAdES – T – signature with a time-stamp
CAdES – C – like CAdES T, but with complete certificate and revocation references
CAdES – X Long – an extended form of CAdES C, containing the whole certificate path, the CRLs and OCSP responses
CAdES – X Type 1 and 2 – an extended version of CAdES C, with a time-stamp covering the signature (Type 1) or the complete certificate and revocation references only (Type 2)
CAdES X Long Type 1 and 2 – a combination of CAdES – X Long, and CAdES – X Type 1 or 2
CAdES – A – like CAdES X, with an added archive time-stamp
CAdES – LT – builds on any format among CAdES-T, CAdES-C, CAdES-X Long, CAdES-X Long Type 1/2 or CAdES-A, adding yet another time-stamp with full information about certification path and the suspension or revocation of certificates

The PAdES format

Electronic signatures in PAdES format (PDF Advanced Electronic Signature, ETSI TS 102 778) employ CAdES or PKCS#7 standards to describe data structures containing the signature. Because these structures are binary, they are relatively easy to insert into the document being signed. In a PDF file there is a specific location – a range of bytes – where the signature, once generated, is to be found.

When the file is being created the exact location of the electronic signature (with all the data it contains about the certificate's validity and time-stamping) will be defined. This space will be filled with 0 values until the signature is generated and embedded therein.

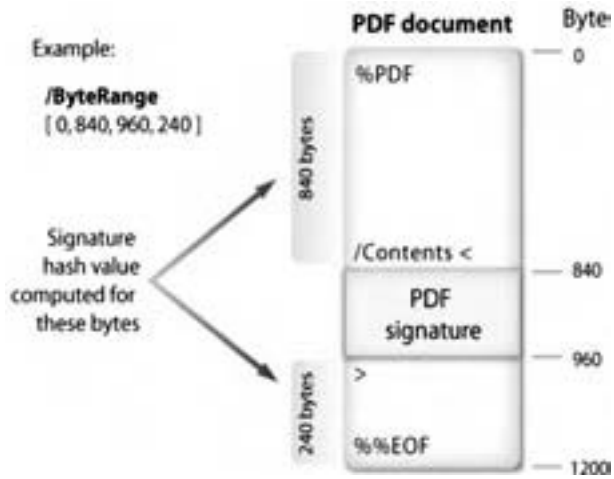

Fig. 2. Signature in a PDF file
Rys. 2. Lokalizacja danych podpisu w pliku PDF

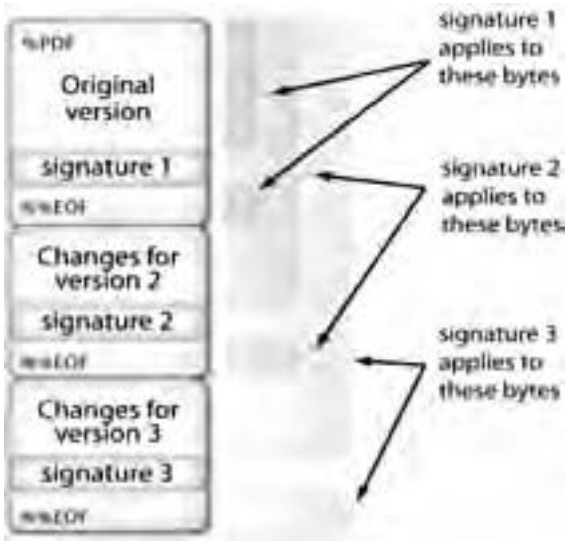

Fig. 3. Multiple signatures in PAdES
Rys. 3. Podpisy wielokrotne PAdES

In its basic form the PDF format allows only one signature to be applied to the document. Unfortunately, this approach is not inconvenient in those cases when a single document requires the signatures of more than one person. One way to circumvent this problem is to create special data structures, known as "signature dictionaries", to hold subsequent signatures. Each of these structures is assigned a specific range of bytes, defining the space where the next generated signature is to be placed.

If XML structures are embedded in the PDF file, XAdES signatures may also be placed within them.

The ASiC format

ASiC (Associated Signature Containter, ETSI TS 102 918) is the most recent electronic signature format. It involves the use of ZIP-based container forms to package signed data objects. The ZIP algorithm was chosen because it is the most popular container format, recognized by most operating systems. An ASiC data container includes two main folders. One – named "root" – is used to store the data that has been signed. The other – a sub-folder in the "root" folder – holds meta-data about the contents of the latter, including electronic signatures associated with the data objects stored therein.

There are two types of ASiC containers. One – ASiC-S (Simple) – can be used to hold a single data object and one or more signatures associated with it (multiple signatures must all be carried in a single signature structure). The second type is ASiC-E (Extended), capable of holding multiple data objects, each of which can have one or more signatures associated with it. Both ASiC-S and ASiC-E signature structures may consist of:

– a single CAdES signature, which in turn may contain parallel signatures, each of which can have a countersignature; or
– multiple XAdES signatures, each of which may also have a countersignature
– a single time-stamp.

It should be noted that the creators of the ASiC standard do not rule out the possibility of its being extended in the future, to enable support for other signature formats besides CAdES and XAdES.

Conclusion

There exists, therefore, more than one electronic signature format. Pursuant to the Regulation of the Council of Ministers of 7 August 2002 on the technical and organizational requirements for qualified entities providing certification services, certification policies for qualified certificates issued by those entities, and technical conditions for secure devices used to create and verify the electronic signature (Journal of Laws No. 128, item 1094) three electronic signature formats were accepted (PKCS#7 – KIR, CMS – Certum i XAdES – Signet). At the time of selection, in 2002, each company could present arguments to support its chosen format (CMS was the most mature, PKCS#7 – the most widely compatible, while XAdES was expected to become dominant); this decision, however, had a a strong negative effect on the market.

In 2006 the Senate of the Republic of Poland criticised the acceptance of multiple formats and the three Polish certification centres decided to set up a joint working group, tasked with the implementation of XAdES (ETSI TS 1010 903) for the purposes of Polish electronic signature standards. The work on regulating the situation, however, is still in progress.

References

[1] R. Poznański, K. Szacki, D. Wachnik, Ł. Stroiński: Przegląd formatów podpisu elektronicznego. Elektronika – konstrukcje, technologie, zastosowania,, nr 1/2014, str. 67-69
[2] http://www.itl.nist.gov/fipspubs/fip180-1.htm, http://www.ietf.org/rfc/rfc2437.txt
[3] http://www.w3.org/TR/xmldsig-core/
[4] RFC 3854
[5] RFC 2315
[6] ETSI TS 103 171
[7] ETSI TS 101 733
[8] ETSI TS 102 778
[9] ETSI TS 101 903, ETSI TS 102 918
[10] RFC 2437
[11] FIPS 180-1
[12] XML Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/)