Przegląd formatów podpisu elektronicznego

mgr inż. ROBERT POZNAŃSKI, mgr inż. KAROL SZACKI, mgr inż. DANIEL WACHNIK, inż. ŁUKASZ STROIŃSKI

Instytut Maszyn Matematycznych, Warszawa

Aktualnie na rynku podpisu elektronicznego uzyskują duże znaczenie cztery standardy definiujące w jaki sposób zapisać podpis elektroniczny. Są nimi CAdES, XAdES, PAdES oraz ASiC opisane w standardach wydawanych przez ETSI (*European Telecommu-nications Standards Institute)*. Są to standardy opisujące tzw. zaawansowany podpis elektroniczny, który wyróżnia się tym, że spełnia wymagania dotyczące takiego rodzaju podpisu zdefiniowane w Dyrektywie 99/93/WE.

W każdym podpisie elektronicznym muszą zostać zawarte podstawowe informacje identyfikujące podpisującego, oraz o przyjętej technice jego wygenerowania. Zalecane jest także załączenie certyfikatu użytego do złożenia podpisu. W strukturze samego podpisu zawierają się również odnośniki do danych, które są takim podpisem opatrzone.

Wszystkie te informacje są wykorzystywane w czasie procesu weryfikacji ważności podpisu. Aplikacja weryfikująca musi odczytać informacje zawarte w pliku z podpisem. Zestandaryzowanie oraz określenie miejsc w jakich się znajdują informacje, umożliwia rozpoznawanie podpisu pomiędzy aplikacjami. Dla przykładu, konieczne jest zawarcie informacji jaka została użyta funkcja skrótu, najczęściej jest to funkcja z rodziny SHA [1] oraz jaki jest algorytm podpisu, obecnie powszechnie stosowany jest algorytm RSA [2] z długością klucza 2048 bitów. Informacje zawarte w certyfikacie pozwolą na zbudowanie i zweryfikowanie ścieżki certyfikacji. Mogą także wskazywać miejsca w których jest możliwe sprawdzenie ważności certyfikatu za pomocą listy CRL lub usługi OCSP.

Normy odnoszące się do formatów XAdES oraz CAdES opisują w jaki sposób można zapisywać informacje dotyczące algorytmów, samego podpisu, podpisującego, warunków poprawności weryfikacji, a także informacje wspomagające weryfikację (np. listy CRL i odpowiedzi OCSP). Podstawową formą podpisu jest BES (*Basic Electronic Signature)* i zawiera on minimum niezbędnych danych. Do struktury podpisu BES mogą zostać dołączane dodatkowe informacje.

– EPES (*Explicit Policy-based Electronic Signature)*, dołączenie identyfikatora polityki podpisu,
– T – Time, czyli dodanie do struktury EPES znacznika czasu,
– C – Complete, dołączenie do struktury EPES następujących elementów: odnośników do pełnej ścieżki certyfikacji, listy CRL, odnośników do ścieżki certyfikacji listy CRL.

Format XAdES

XAdES – XML Advanced Electronic Signature został opisany w standardzie ETSI TS 103 171. Podstawową wersją podpisu XAdES jest XAdES-BES (*Basic Electronic Signature*). Bazą do stworzenia podpisu jest struktura XMLDSIG [3] opracowana przez W3C. Poniżej pokazana jest struktura XML podpisu, która dołączana jest do podpisy-wanego dokumentu, bądź zapisywana do osobnego pliku zawierającego podpis:

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

W XMLDSIG zawarte są informacje dotyczące środków technicznych wykorzystanych przy złożeniu podpisu, ale również odnośniki do danych, które zostały podpisane. Przewidziane jest również miejsce na dodanie dodatkowych informacji w polu DS:Object. Pole to zostało wykorzystane w formacie XAdES do umieszczenia informacji takich jak:

– SigningTime – atrybut wskazujący czas złożenia podpisu
– CommitmentTypeIndication – atrybut wskazujący cel złożenia podpisu np. oświadczenie woli, niezaprzeczalność
– CounterSignature – atrybut, który zawiera kontrasygnatę

Pierwsze trzy atrybuty z wymienionych przykładów są elementami, które jeśli dołączone, muszą zostać podpisane razem z danymi. Natomiast kontrasygnata jest kolejnym, złożonym w późniejszym czasie podpisem.

Rozwinięciem podstawowej formy jest XAdES – EPES (*Explicit Policy based Electronic Signature*), która w strukturze <signed-SignatureProperties> zawiera identyfikator polityki podpisu.

Podpis elektroniczny może także zawierać znacznik czasu, który potwierdza, że dokument został podpisany przed określoną datą. Taki format podpisu nazywany jest XAdES – T, (od Time). Jego rozszerzeniem jest XAdES – C, Complete. Zawiera on wskazanie na elementy, które są niezbędne do weryfikacji ważności certyfikatu podpisującego. Do takiego podpisu dołączone są: referencje do pełnej ścieżki certyfikacji oraz list CRL. Zawiera ona listę numerów seryjnych unieważnionych oraz zawieszonych certyfikatów. Dzięki temu można ustalić, czy certyfikat osoby podpisującej nie został unieważniony.

Format CAdES

Budowa podpisu w formacie CAdES oparta jest o zasady zdefiniowane w ramach standar-dów CMS – Cryptographic Message Syntax [4]. Standard CMS wywodzi się z PKCS#7 [5] opracowanego przez RSA Laboratories w 1993 roku i opisuje nie tylko implementację pod-pisów elektronicznych ale także szyfrowanie czy autentykację danych. Informacje w CMS zapisywane są w notacji ASN.1 w formie ośmiobitowych łańcuchów.

Rys. 1. Struktura podpisu XAdES-C
Fig. 1. Structure of XAdES-C

Specyfikacja formatu CAdES została opisana w ETSI TS101733. Poniżej przedstawiona jest przykładowa struktura opisująca informacje o podpisującym, 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
```

Format CAdES daje możliwość tworzenia wielu różnych postaci pliku z podpisem.
CAdES – BES – najprostsza, podstawowa wersja
CAdES – EPES – rozszerzona o odnośnika do polityki podpisu
CAdES – T – podpis ze znacznikiem czasu
CAdES – C – wersja T z dodanymi odnośnikami do pełnych informacji o ścieżce certyfikacji oraz o zawieszeniu lub unieważnieniu certyfikatów
CAdES – X Long – dodanie do wersji C pełnych informacji o ścieżce certyfikacji oraz o zawieszeniu lub unieważnieniu certyfikatów
CAdES – X – rozszerzenie formy C o dodanie znacznika czasu oraz pełnych informacji o ścieżce certyfikacji oraz o zawieszeniu lub unieważnieniu certyfikatów
CAdES – A – wersja X z dodanym znacznikiem czasu
CAdES – LT – może być stworzony na podstawie wersji C, X Long, X, A i polega na dodaniu kolejnego znacznika czasu wraz z pełnymi informacjami o zawieszeniu lub unieważnieniu certyfikatów

Format PAdES

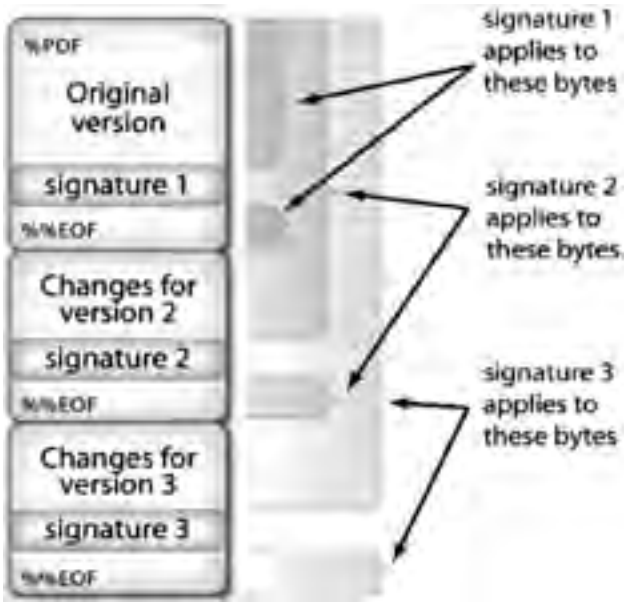
Podpis elektroniczny w formacie PAdES (PDF Advanced Electronic Signature, ETSI TS 102 778) wykorzystuje standardy CAdES lub PKCS#7 do opisu struktur danych zawierających podpis. Ponieważ są to formaty binarne, stosunkowo łatwym jest umieszczenie ich w podpisywanym dokumencie. Plik PDF ma określone miejsce – zakres bajtów, w których znaleźć się powinien wygenerowany podpis.

Rys. 2. Podpis w pliku PDF. Fig. 2. Signature in PDF file

Przy tworzeniu pliku określane jest miejsce na podpis elektroniczny wraz z zawartymi w nim danymi dotyczącymi informacji o ważności certyfikatu i znakowaniu czasem. Miejsce to zapełnione jest wartościami „0”, dopóki podpis nie zostanie wygenerowany i tam zapisany.

W podstawowej postaci format PDF pozwala na złożenie tylko jednego podpisu pod dokumentem. Niestety takie podejście nie jest wygodne w przypadku gdy jeden dokument wymaga podpisu kilku osób. Metodą obejścia tego problemu jest tworzenie zasobników, tzw. „signature dictionaries”, w których mogą zostać zapisane kolejne podpisy. Do każdego z tych zasobników przypisany jest indywidualny zasięg bajtów określający zakres, w którym zostanie umieszczony następny wygenerowany podpis.

W przypadku włączenia struktur XML do formatu PDF możliwe jest także dołączanie do nich podpisów w formacie XAdES.



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

Format ASiC

ASiC (*Associated Signature Containter*, ETSI TS 102 918) jest najnowszym formatem podpisu elektronicznego. Jest dedykowany do podpisywania danych, które są następnie umieszczane w kontenerze ZIP. Algorytm ZIP został wybrany ze względu na największą uniwersalność oraz rozpoznawalność przez różne systemy operacyjne. Plik ZIP formatu ASiC zawiera dwa foldery. Pierwszy, zwany „root" służy do przechowywania danych, które zostały opatrzone podpisem. W drugim folderze znajdują się metadane dotyczące folderu „root" oraz podpisy elektroniczne odnoszące się do danych z tego foldera.

Istnieją dwa typy formatu ASiC, pierwszym z nich jest ASiC-S (Simple). Służy on do przechowywania jednego zestawu danych oraz kilku powiązanych z nim podpisów, przy czym podpisy te muszą zwierać się w jednej strukturze. Drugim typem jest ASiC-E (Extended), który może przechowywać kilka zestawów danych. Każdej paczce danych może odpowiadać jeden lub wiele podpisów. Zarówno w przypadku ASiC-S, jak i ASiC-E podpisy zawarte w pliku mogą być:

– jednym podpisem CAdES, który może zawierać równoległe podpisy, dodatkowo do każdego z nich można dodać kontrasygnatę,
– wieloma podpisami XAdES, które również mogą zostać opatrzone kontrasygnatą,
– pojedynczym znacznikiem czasu.

Warto zaznaczyć, że twórcy normy ASiC dopuszczają rozszerzenie jej w przyszłości o dopuszczenie innych formatów podpisów poza CAdES i XAdES.

Literatura

[1] http://www.itl.nist.gov/fipspubs/fip180-1.htm
[2] 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 102 918
[10] RFC 2437
[11] FIPS 180-1
[12] XML Signature Syntax and Processing (http://www.w3.org/TR/xmldsig-core/)