pemi
stowarzyszenie

Podpis elektroniczny • Mobile • Internet

Podpis elektroniczny – Teoria i praktyka

Stowarzyszeni PEMI

Wisła, 2007

pemi
stowarzyszenie
Podpis elektroniczny • Mobile • Internet

Kim jesteśmy - misja i cele :

- **Celem Stowarzyszenia jest wspomaganie rozwoju gospodarczego, w tym rozwoju przedsiębiorczości oraz nauka i edukacja**

- **Stowarzyszenie swe cele realizuje poprzez:**
  - świadczenie usług informatycznych,
  - pomoc przy implementacji usług informatycznych,
  - promocję nowoczesnych technologii,
  - organizację szkoleń, seminariów, warsztatów,
  - prace badawczo-rozwojowe w dziedzinie IT,

- Stowarzyszenie PEMI jest instytucja NON PROFIT (nie prowadzi działalności gospodarczej)

Plan wystąpienia

- Wprowadzenie:
- Podstawy podpisu XML'owego:
  - Rodzaje podpisów
  - Najważniejsze cechy
  - Węzły XML używane w podpisie
- Zagadnienia zaawansowane:
  - Kontrasygnaty
  - Podpisy wielokrotne
  - XAdES-C – dlaczego trzeba czekać
  - Przechowywanie podpisów w długim okresie czasu
- Standaryzacja formatu podpisu

Wprowadzenie

- Wydawanie certyfikatów
  - kwalifikowanych
  - niekwalifikowanych
- Proces weryfikacji tożsamości użytkowników certyfikatów
  - Potwierdzanie danych zawartych w certyfikacie zgodnie z polityka certyfikacji
- Elektroniczne potwierdzanie ważności certyfikatu (OCSP,CRL)
  - Możliwe techniki weryfikacji
  - Zagrożenia związane z weryfikacja statusu certyfikatu

Wprowadzenie

- Omówienie najważniejszych formatów podpisu:
  - XMLDsig - XML Digital Signature,
  - XAdES - XML Advanced Digital Signatures ,
  - PKCS#7 - CMS Cryptographic Message Syntax Standard
- Porównanie najważniejszych cech poszczególnych formatów
  - elastyczność,
  - szybkość generowania podpisu,
  - otwartość,
  - łatwość wdrażania

Podstawy podpisu XML’owego

XAdES - podstawy

- Podstawy – XMLDSig
- Formaty podpisu:

Podstawowe

- XAdES-BES
- XAdES-EPES
- XAdES-T
- XAdES-C

Rozszerzone

- XAdES-X
- XAdES-X-L
- XAdES-A

XAdES - podstawy

- XML-Signature Core Syntax and Processing - podstawowe funkcjonalności związane z podpisywaniem kilku obiektów jednocześnie
- Wykorzystanie <Object> do zapisanie dodatkowych atrybutów

XAdES-BES – 1/2

- Format minimalny
- Nie nadaje się do przechowywania informacji w długim okresie czasu
- Spełnia wymagania dla podpisu elektronicznego określone w Dyrektywie Europejskiej

XAdES-BES – 2/2

- Certyfikat podpisującego MUSI być objęty podpisem
- Podpis może zawierać:
  - Czas złożenia podpisu
  - Informacje na temat podpisanego dokumentu
  - Definicja roli/funkcji podpisującego
  - Rodzaj składanego oświadczenia
  - Kontrasygnaty

XAdES-EPES

- Identyfikator polityki podpisu musi zostać objęty podpisem
- Polityka podpisu musi zostać wykorzystana do weryfikacji podpisu

XAdES-T

- Podpis zostaje ‘oznakowany’ czasem pochodzącym z zaufanego źródła
- Oznakowanie czasem w rozumieniu XAdES polega na:
  - wykorzystaniu węzła SignatureTimeStamp i umieszczeniu w nim znacznika czasu albo
  - skorzystaniu z usług Zaufanego Usługodawcy (TSP)

XAdES-C

- Zawiera kompletny zestaw odnośników do danych pozwalających zweryfikować podpis:
  - Odnośniki do cerytifikatów urzędów używanych do weryfikacji podpsiu
  - Odnośniki do informacji o ważności certyfikatów podpisującego i urzędów
  - Odnośniki do certyfikatów atrybutów i do informacji o ważności tych certyfikatów
- Użycie odnośników zmniejsza rozmiar podpisu

XAdES – przegląd węzłów – 1/5

- SignaturePolicyIdentifier – pozwala jednoznacznie określić politykę podpisu której użył składający podpis i którą powinien wykorzystać również weryfikujący podpis. Polityka m.in. precyzuje role i zakres oświadczenia składanego przez podpisującego

XAdES – przegląd węzłów – 2/5

- SigningCertificate – zawiera jednoznaczny odnośnik do certyfikatu podpisującego
- SigningTime – zawiera czas w którym podpisujący twierdzi, że złożył podpis
- DataObjectFormat – określa format danych które zostały podpisane. Szczególnie ważne w otwartych systemach

XAdES – przegląd węzłów – 3/5

- CommitmentTypeIndication – rodzaj ‘zobowiązania’; można definiować własne (w polityce podpisu); już zdefiniowane typy [TS 101 733]:
  - Proof of origin
  - Proof of receipt
  - Proof of delivery
  - Proof of sender
  - Proof of approval
  - Proof of creation
- SignatureProductionPlace - adres

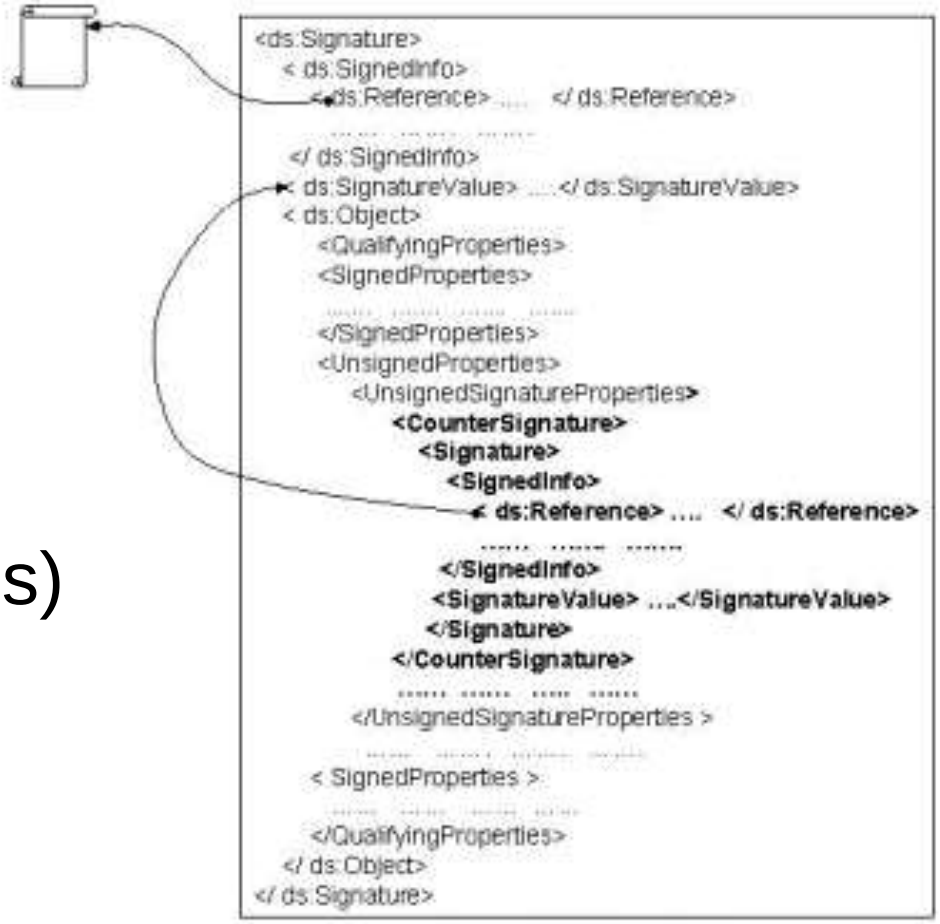
XAdES – przegląd węzłów – 4/5

- SignerRole – rola w której występuje podpisujący; może być podana wprost albo potwierdzona certyfikatem atrybutów
- CounterSignature - kontrasygnata; zdefiniowany w standardzie mechanizm pozwala na tworzenie łańcuchów podpisów (ale nie drzew)

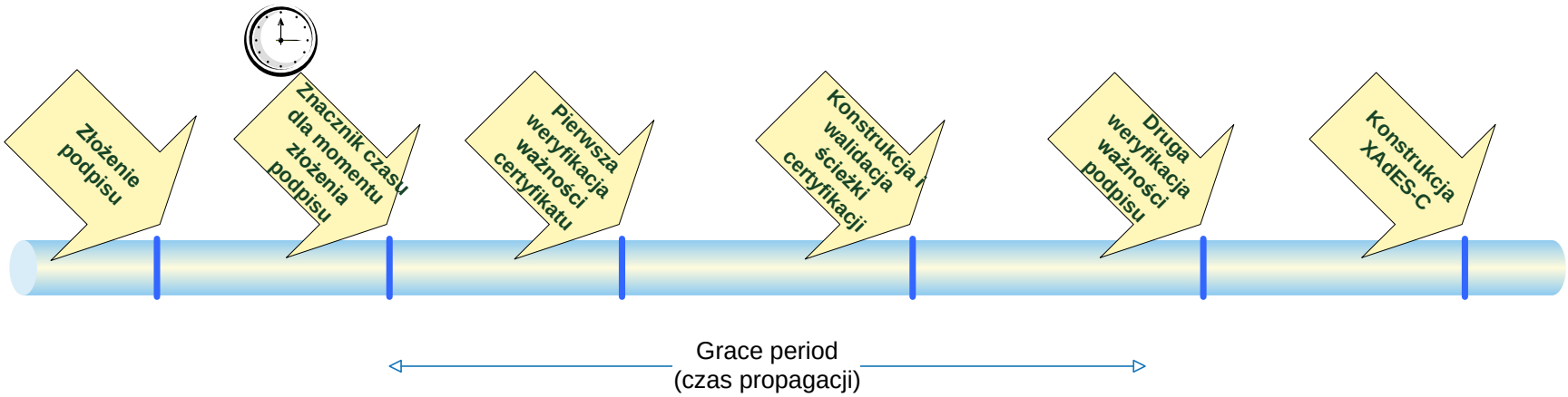
Zagadnienia zaawansowane

Kontrasygnaty

- Istnieją w XMLDsig
- Łańcuchy
- Są w części nie podpisanej (UnsignedProperties)



XAdES-C - dlaczego trzeba czekać



pemi
Podpis elektroniczny • Mobile • Internet

Przechowywanie podpisów przez długi okres czasu – 1/2

- Przechowywanie przez czas przekraczający okres ważności certyfikatów używanych do weryfikacji podpisu
- W tym czasie można również ‘złamać’ algorytmy
- Certyfikaty które mogą wygasnąć:
  - Certyfikat Podpisującego
  - Certyfikat CA Podpisującego
  - Certyfikat TSA (znaczniki czasu)

Przechowywanie podpisów przez długi okres czasu – 2/2

- W podpisie umieszczana jest cała ścieżka certyfikatów oraz informacje o ich ważności (CRLe albo odpowiedzi z OCSP)
- Znacznik czasu chroni te dane i jednocześnie potwierdza ich istnienie w danej chwili
- Co pewien czas tworzy się nowy znacznik chroniący wszystkie dane

pemi
stowarzyszenie
Podpis elektroniczny • Mobile • Internet

Wdrażanie podpisu w e-administracji

Przeszkody ……

- Brak decyzji związanych z „opieką” nad podpisem elektronicznym.
- Lobbing producentów
- Brak publicznej dyskusji oraz debaty związane z formatów i standardów
- Podpis w aktualnej „formie” stwarza więcej szkody niż pożytku.
- Systemy (administracji publicznej) wykorzystujące mechanizmy podpisu za każdym razem tworzą nowe autonomiczne rozwiązania (rozwiązania zamknięte) – Kilka razy płacimy za to samo
-

pemi
stowarzyszenie
Podpis elektroniczny • Mobile • Internet

Główne wyzwania stojące przed ……

- W Polsce nie ma problemu z podpisem elektronicznym …….. Ponieważ nikt z niego nie korzysta !!!
- Wymagane zmiany w istniejących aktach prawnych
- Ujednolicenie Formatu Podpisu
- Ujednolicenie Formatu dokumentu elektronicznego

Kontakt:

Mirosław Januszewski
Doradca Techniczny
mirek@pemi.pl

Stowarzyszenie PEMI
Podpis Elektroniczny Mobile Internet
ul. Stefana Bryły 3/582
02-685 Warszawa
KRS 0000213935

Materiały dodatkowe

- Znakowanie czasem
- Weryfikowanie statusu certyfikatów w trybie on-line
- Walidacja danych
- Poświadczenie odbioru i przedłożenia
- Poświadczenie depozytowe
- Poświadczenie rejestrowe i repozytoryjne