KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

POLITECHNIKA BIAŁOSTOCKA

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

Rozproszone systemy internetowe 2

Zaawansowane podpisy elektroniczne

„Podniesienie potencjału uczelni wyższych jako czynnik rozwoju gospodarki opartej na wiedzy”

Nr projektu: UDA-POKL.04.01.01-00-143/09-00

Dyrektywa Komisji Europejskiej
Community framework for electronic signatures

Podpis elektroniczny

(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.**

Dyrektywa Komisji Europejskiej

Community framework for electronic signatures

Zaawansowany podpis elektroniczny

Advanced electronic signature

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

XAdES - Ogólnie

- Podpisy XAdES bazują na podpisach XMLDSig
- Podpisy XAdES używają mechanizmu rozszerzeń XMLDSig (ds:Object)
- XAdES standaryzuje:
  - zestaw nowych własności, które pozwalają na umieszczenie informacji zgodnych z wymaganiami (ważność długookresowa, wyparcie się)
  - mechanizmy umieszczania tych własności w podpisie
  - definiuje tzw. formy (forms), które opisują podpisy z określonym zestawem własności

XadES - własności

- Własności mogą uwiarygadniać sam podpis, podpisywane dane lub podpisującego.
- Podpisujący może dołączyć własności do podpisu przed podpisaniem dokumentu i zabezpieczyć przez fakt podpisania (signed properties)
- Podpisujący, weryfikujący lub instytucja trzecia może dołączyć własności do podpisu po podpisaniu dokumentu (unsigned properties)

Signed Properties

- SigningCertificate:
  - Referencja do certyfikatu podpisującego oraz certyfikatów na ścieżce. Zawiera identyfikatory oraz skróty dla certyfikatów.
  - Zabezpiecza referencję do certyfikatu podpisującego.
- SignerRole
- CommitmentTypeIndication: proof of origin, receipt, delivery, sender, approval, creation

Signed Properties c.d.

- SignatureProductionPlace
- SigningTime
- Data object time-stamps
- Signature policy identifier

Unsigned Properties

- SignatureTimestamp – zapewnia, że podpis został złożony przed wskazanym czasem
- CompleteCertificateRefs – lista certyfikatów na ścieżce, które weryfikujący powinien sprawdzić
- CompleteRevocationRefs
- CertificateValues
- RevocationValues
- ArchiveTimeStamp

Formy podstawowe

- XAdES-BES – dołączony certyfikat
- XAdES-EPES – określona polityka
- XadES-T – znakowanie czasem

Formy rozszerzone

- XAdES-C - komplet odwołań: ścieżki certyfikacji, CRL, OCSP
- XAdES-X - XadES-C plus znakowanie czasem
- XAdES-X-L - komplet danych (a nie odwołań)
- XadES-A - XadES-X-L plus znakowanie czasem