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

Web Services Security: rozwinięcie

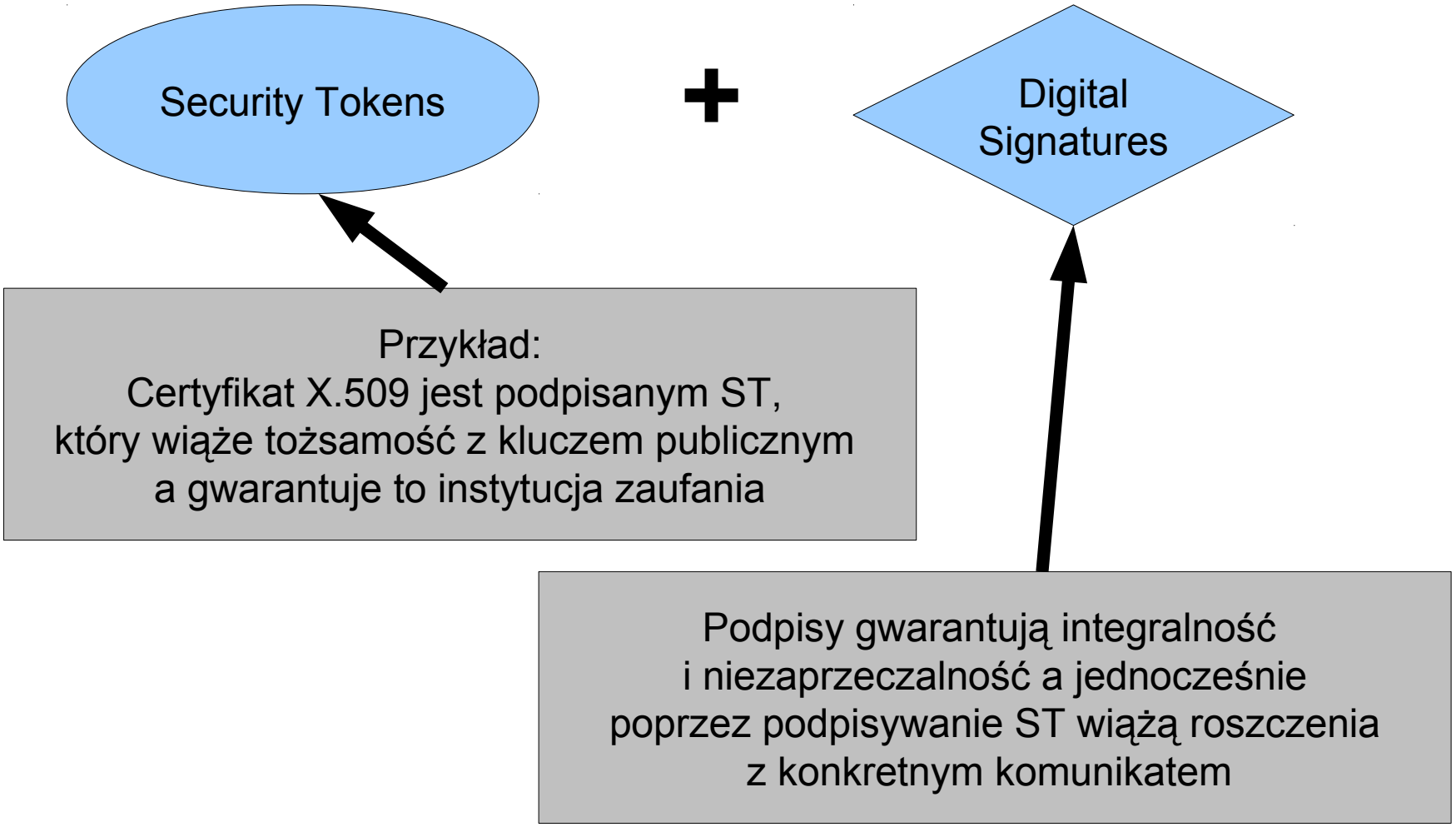
„Podniesienie potencjału uczelni wyższych jako czynnik rozwoju gospodarki opartej na wiedzy”

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

Wybrane pojęcia podstawowe

- **Claim** (roszczenie) – deklaracja złożona przez podmiot dot. nazwy,tożsamości, klucza, grupy, uprawnienia, możliwości
- **Security Token** – zbiór roszczeń
- **Signed Security Token** – ST, który został sprawdzony i podpisany
- **Trust** – informacja, że dany podmiot chce polegać na innym podmiocie w celu wykonania zbioru akcji lub przyjęcia założeń dot. zbioru obiektów

Model bezpieczeństwa dla komunikatu



Typy ST

USERNAME

<wsse:*UsernameToken* wsu:Id="...">

<wsse:*Username*>...</wsse:*Username*>

</wsse:*UsernameToken*>

BINARY SECURITY TOKEN

<wsse:*BinarySecurityToken* wsu:Id=...

EncodingType=...

ValueType=.../>

ENCRYPTED DATA TOKEN

Nie stanowi oddzielnego typu, jest sekcja

<xenc:EncryptedData/> ale referencje są odniesieniami do odkodowanej zawartości

Odniesienia do ST

<wsse:SecurityTokenReference wsu:Id="...">

<wsse:Reference URI="..." ValueType="..."/>

<wsse:KeyIdentifier wsu:Id="..." ValueType="..." EncodingType="...">

<wsse:Embedded wsu:Id="..."> ...</wsse:Embedded>

</wsse:SecurityTokenReference>

Postać kanoniczna

- C14n
  - Kodowanie (utf-8), końce linii, wartości atrybutów, encje, DTD, prolog, puste elementy, atrybuty domyślne itd. ...
- Exclusive c14n
  - Przestrzenie nazw są kopiowane podczas analizy fragmentów dokumentu a to może prowadzić do błędnego podpisu (uwaga! exc-c14n nie analizuje wartości atrybutów)

Zagadnienia dodatkowe

- Ataki typu „replay” - Timestamp, Expiration, Sequence Number, Message Corelation
- Privacy ?
- Które elementy wiadomości podpisywać i kiedy ?
- Zabezpieczenia dla kluczy, ST oraz stempli czasowych
- Duplikaty identyfikatorów