IBA GROUP

PI MON 2021

Дмитрий Манько,
специалист по интеграции,
IBA Group

XML “СИГИ”.
На земле и в облаках.

Еще раз о форматах

Зачем PAdES, CAdES, XAdES? (Advanced Electronic Signature)

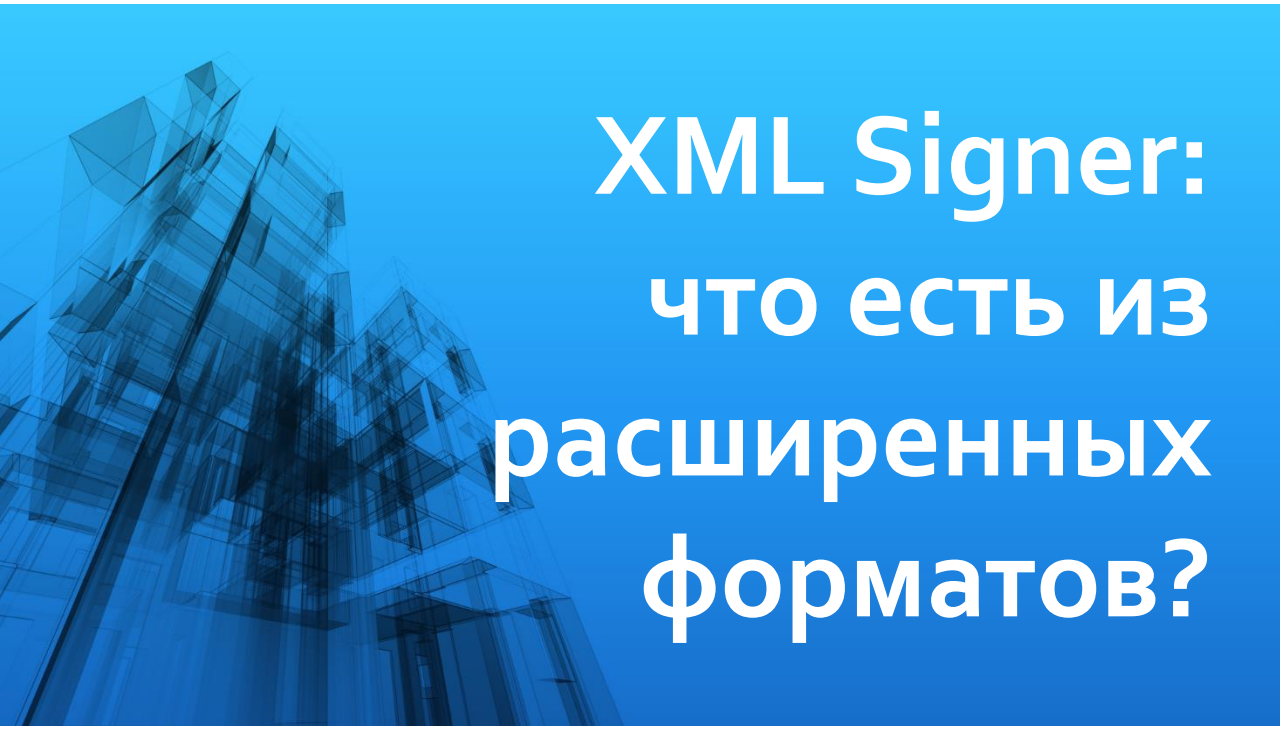
Что не так со стандартными форматами XML подписей?

XMLDSig, CMS, Open PGP, WS-Security… “-Давай по новой, Миша, всё не то” (с)

Недостатки стандартных форматов:

- НЕТ доверенных отметок времени создания подписи
- НЕТ доказательства подлинности сертификатов на момент подписания
- НЕТ возможности долгосрочного хранения подлинности подписи
- Отсутствие типа содержимого подписи (CMS)

_1 SAP CPI – Message Level Security



- CAdES-BES (PKCS#7/CMS)

https://www.etsi.org/deliver/etsi_ts/101700_101799/101733/02.02.01_60/ts_101733v020201p.pdf
(алгоритмы создания отпечатков и шифрования)
SHA512/RSA, SHA384/RSA, SHA256/RSA, SHA224/RSA, SHA/RSA, RIPEMD128/RSA, RIPEMD160/RSA, RIPEMD256/RSA, MD5/RSA, MD2/RSA, RIPEMD160andMGF1/RSA-ISO9796-2-2-3, SHAandMGF1/RSA-ISO9796-2-2-3, SHA256withDSA, SHA224withDSA, SHA/DSA.

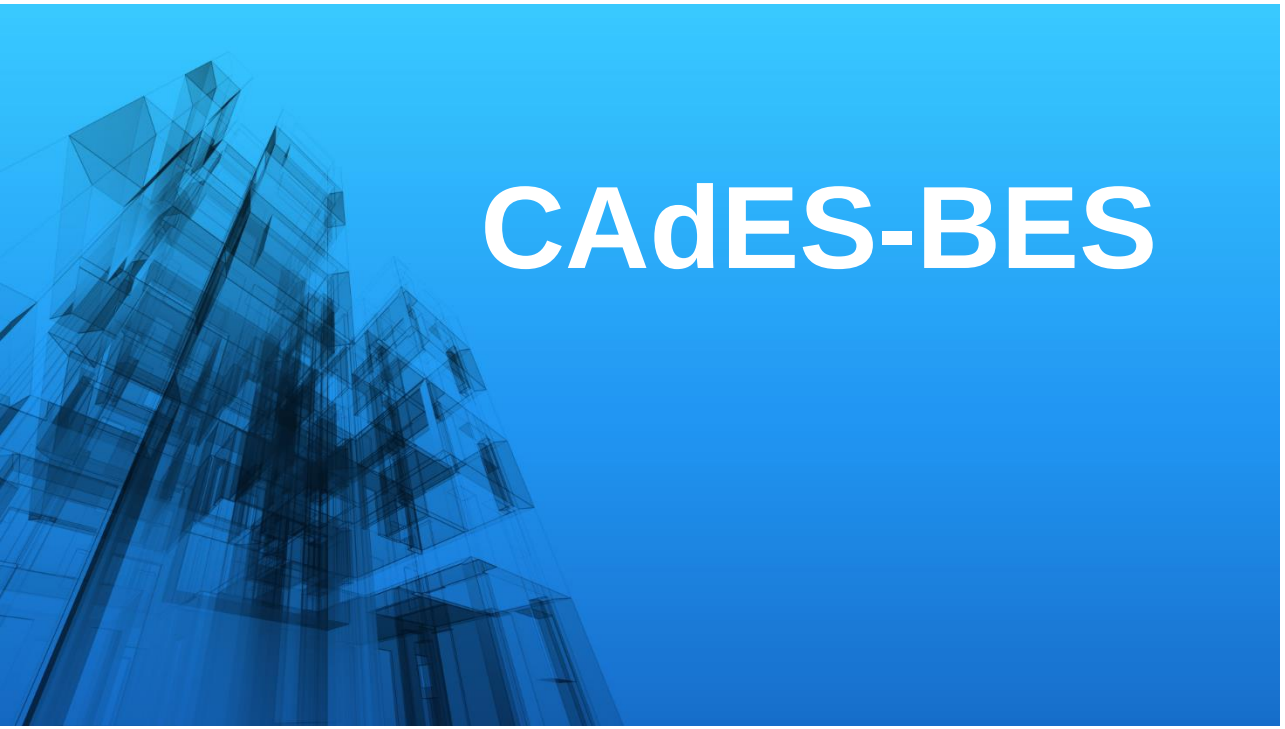
- XAdES-BES, XAdES-EPES

(алгоритмы шифрования)
DSA/SHA1, RSA/SHA1, RSA/SHA256, RSA/SHA384, RSA/SHA512

- Open PGP
- WS-Security

IBA GROUP

_2 SAP CPI - XML Signer



- Расширенная версия CMS подписей
- Обязательно подписываемые аттрибуты:

  •*content-type* (RFC 3852);
  •*message-digest* (RFC 3852);
  •*ESS signing-certificate* (RFC 2634)

- Дополнительно подписываемые аттрибуты:
  •*signing-time* (определен в CMS, RFC 3852);
  •*content-hints* (определен в ESS, RFC 2634);
  •*content-reference* (определен в ESS, RFC 2634);
  •*content-identifier* (определен в ESS, RFC 2634);
  •*commitment-type-indication* (определен в CAdES);
  •*signer-location* (определен в CAdES);
  •*signer-attributes* (определен в CAdES);
  •*content-time-stamp* (определен в CAdES);
  •*mime-type* (определен в CAdES).

IBA GROUP

_3 SAP CPI - XML Signer

Ограничения:
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/08d4522ca0f54bd1bbd22d4d2449a1f3.html

- No support for the QualifyingPropertiesReference element (see section 6.3.2 of the XAdES specification at http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf).
- No support for signature forms XAdES-T and XAdES-C.
- No support for the Transforms element contained in the SignaturePolicyId element contained in the SignaturePolicyIdentifier element.
- No support of the CounterSignature element; this implies that there is no support for the UnsignedProperties element.
- At most one DataObjectFormat element is supported.
- More than one DataObjectFormat element does not make any sense in the use cases supported by the Signer step, because only one signed data object is expected (the incoming message body to the XML signer).
- At most one CommitmentTypeIndication element is supported.
- More than one CommitmentTypeIndicationelement does not make any sense in the use cases supported by the Signer step, because only one signed data object is expected (the incoming message body to the XML signer).
- A CommitmentTypeIndication element always contains the AllSignedDataObjects element.
- The ObjectReference element within a CommitmentTypeIndication element is not supported.
- No support of the AllDataObjectsTimeStamp element (it requires a time a
- No support of the IndividualDataObjectsTimeStamp element (it requires a rity).

IBA GROUP

_4 SAP CPI - XML Signer

Message Headers

- **CamelXmlSignatureXAdESQualifyingPropertiesId**

Specifies the Id attribute value of the QualifyingProperties element.

- **CamelXmlSignatureXAdESSignedDataObjectPropertiesId**

Specifies the Id attribute value of the SignedDataObjectProperties element.

- **CamelXmlSignatureXAdESSignedSignaturePropertiesId**

Specifies the Id attribute value of the SignedSignatureProperties element.

- **CamelXmlSignatureXAdESDataObjectFormatEncoding**

Specifies the value of the Encoding element of the DataObjectFormat element.

- **CamelXmlSignatureXAdESNamespace**

Overwrites the namespace parameter value.

- **CamelXmlSignatureXAdESPrefix**

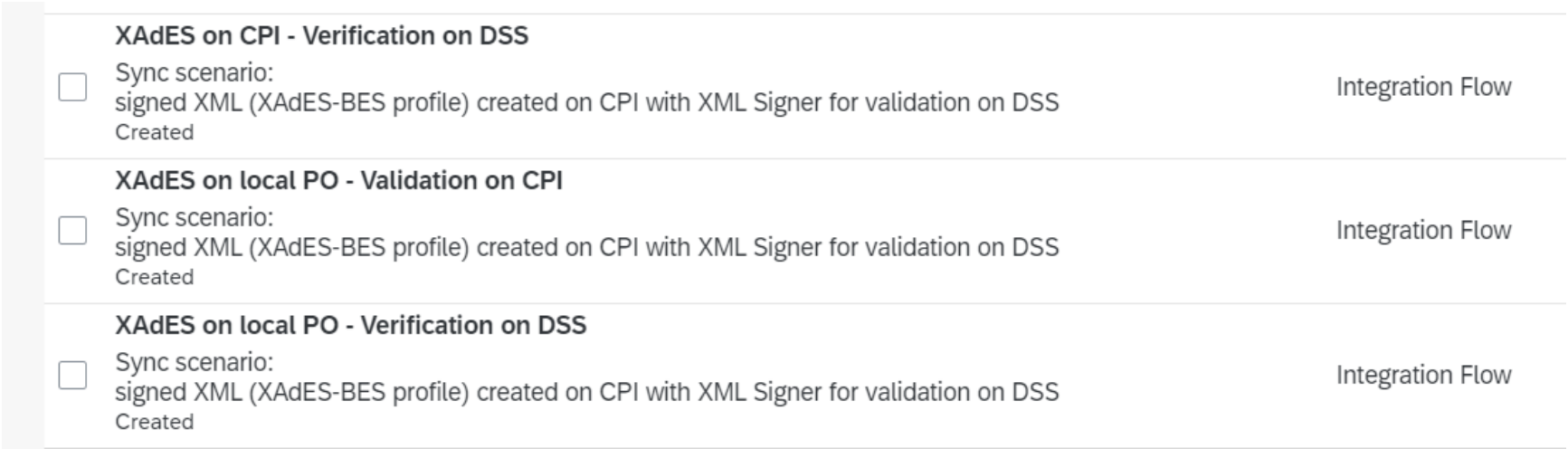
Overwrites the prefix parameter value.

IBA GROUP

_5 Время запускать СИГИ в облако!

Возможные сценарии:

- Подписываем на SAP PO (XAdES-BES) – валидируем на SAP CPI
- Подписываем на SAP PO – валидируем на внешнем сервисе (https://ec.europa.eu/cefdigital/DSS)
- Подписываем на CPI (XAdES-BES) – валидируем на DSS (или SAP PO)



IBA GROUP

_6 А как же ГОСТ-ские криптопровайдеры и шифры?

SAP PO/ CPI – не поддерживают российские алгоритмы подписей, шифрования и создания хешей (- Вы это серьёзно?)

КриптоПро CSP 5.0 (– Дайте два!)

Электронная подпись	ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001, ECDSA, RSA
Хэш-функции	ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, SHA-1, SHA-2
Шифрование	ГОСТ Р 34.12-2015 («Кузнечик» — начиная с 5.0 R2), ГОСТ 28147-89, AES (128/192/256), 3DES, 3DES-112, DES, RC2, RC4

IBA GROUP

_7 Что ж делать-то?

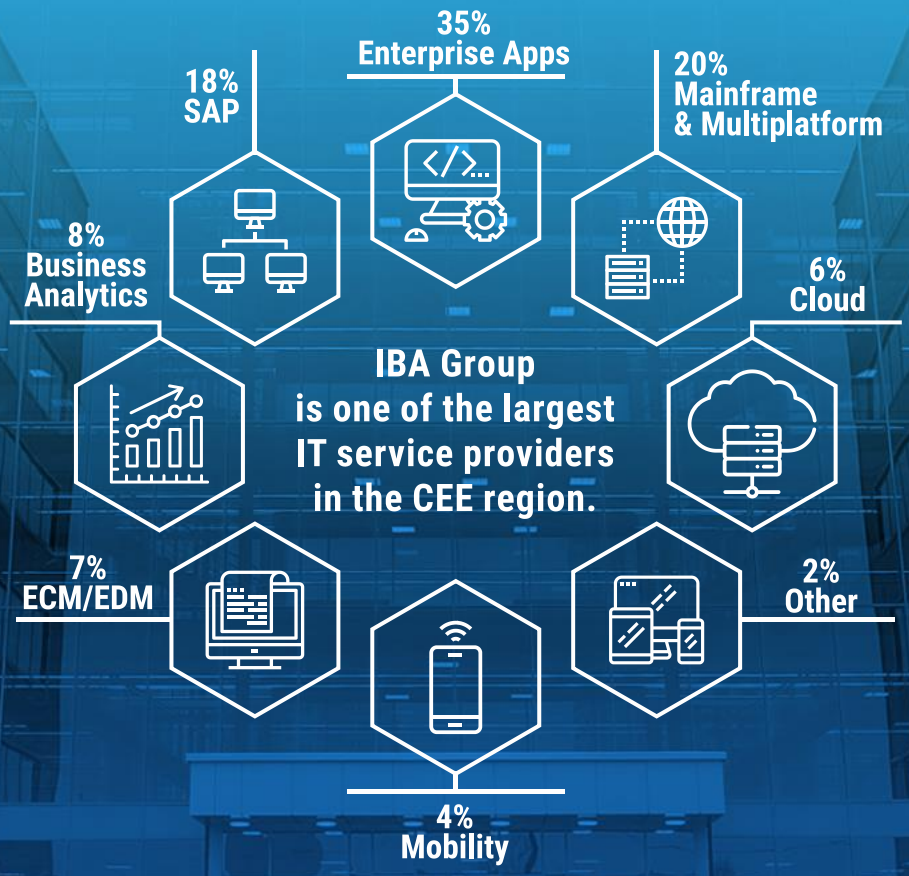
Внедрять CryptoPro JCP в SAP JVM ?
– Не вариант.

Ставим CryptoPro JCP (JCSP) на локальную машину.
Пишем сервис создания подписей
(+ шифрование, управление сертификатами и т.д.)

……
PROFIT!!!

IBA GROUP

Благодарю за внимание!



Дмитрий Манько
Специалист по интеграции
+375 29 5627970
dmanko@ibagroup.eu