Implementation of XML Digital Signatures on S1000D Data Modules

PREPARED FOR
S1000D User Forum & S-Day 2013
18 Sept. 2013

PRESENTED BY
Dr. Stergios ISAAKIDIS
Air Defence Programme
stergios.isaakidis@nspa.nato.int
Topics

- Data Modules distribution and integrity boundaries
- Digital signature benefits
- Signing concept
- Technical Implementation
  - Signature definition
  - How to get a certificate
  - Implementation effort
- References
Data Modules distribution and integrity boundaries
Digital Signature Benefits

- End-to-end data module integrity
- Authentication information about the originator of the data module
Signing concept

**Authoring**

- **Unsigned S1000D Data Module**
- **Certificate Store or Certificate Server**
- **XML Sign Tool**
- **Signed S1000D Data Module**

**End User**

- **Signed S1000D Data Module**
- **Distributed Certificate**
- **XML Verification Tool**
- **Verified Signed S1000D Data Module**
Technical Implementation: Signature definition

Specification:

```xml
<Signature ID/>
<SignatureValue>

<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (Reference URI?)? (Transforms)?
    <DigestMethod>
    <DigestValue>
    </Reference>)?
  </SignedInfo>
  <SignatureValue>
    <KeyInfo>?
    (<Object ID?>)*
  </SignatureValue>
</Signature>
```

Example:

```xml
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  - <SignatureValue>YvtbCMzVnfoNkL5wxxXwsj0P+Zw52ahd1NYEH3IjkOCggf6riZRhXHdkyuhTADsAQa</SignatureValue>
  - <SignatureValue>YvtbCMzVnfoNkL5wxxXwsj0P+Zw52ahd1NYEH3IjkOCggf6riZRhXHdkyuhTADsAQa</SignatureValue>
  - <X509Data>
    - <X509IssuerSerial>
      <X509IssuerName>CN=EDCA, DC=NSPA, DC=LU</X509IssuerName>
      <X509SerialNumber>127679794098451467206661</X509SerialNumber>
    </X509IssuerSerial>
  </X509Data>
</Signature>
```

Notes:

"?": zero or one occurrence

"+": one or more occurrences

"*": zero or more occurrences
Technical Implementation: Signature definition

```xml
<dmodule>
  <rdf:Description>
    <identAndStatusSection>
      <content>
        <Signature>
          Optional XMLDIGSIG signature section
        </Signature>
      </content>
    </identAndStatusSection>
  </rdf:Description>
</dmodule>
```
Technical Implementation: How to get a certificate

• Purchase a certificate from a trusted Certificate Authority
• Create a self-signed certificate
• Create a certificate using your Organization’s Certificate Authority (if exists)
Technical Implementation: Development Effort

- XML digital signature API’s and libraries are provided out-of-the-box by many development environments, e.g.:
  - Java:
    - Java XML Digital Signature API (javax.xml.crypto package)
    - Apache XML Security for Java (Apache Software Foundation)
  - C#, VB.NET, C++ (managed):
  - C++:
    - Apache XML Security for C++ (Apache Software Foundation)
  - Javascript:
    - Various open source implementations
- Easy to develop and integrate into existing applications
  - Our experience: less than 1000 lines of code (including unit tests)
References


• W3C, XML Signature Syntax and Processing (Second Edition),
  http://www.w3.org/TR/2008/REC-xmldsig-core-20080610