NATO SUPPORT AGENCY
AGENCE OTAN DE SOUTIEN

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

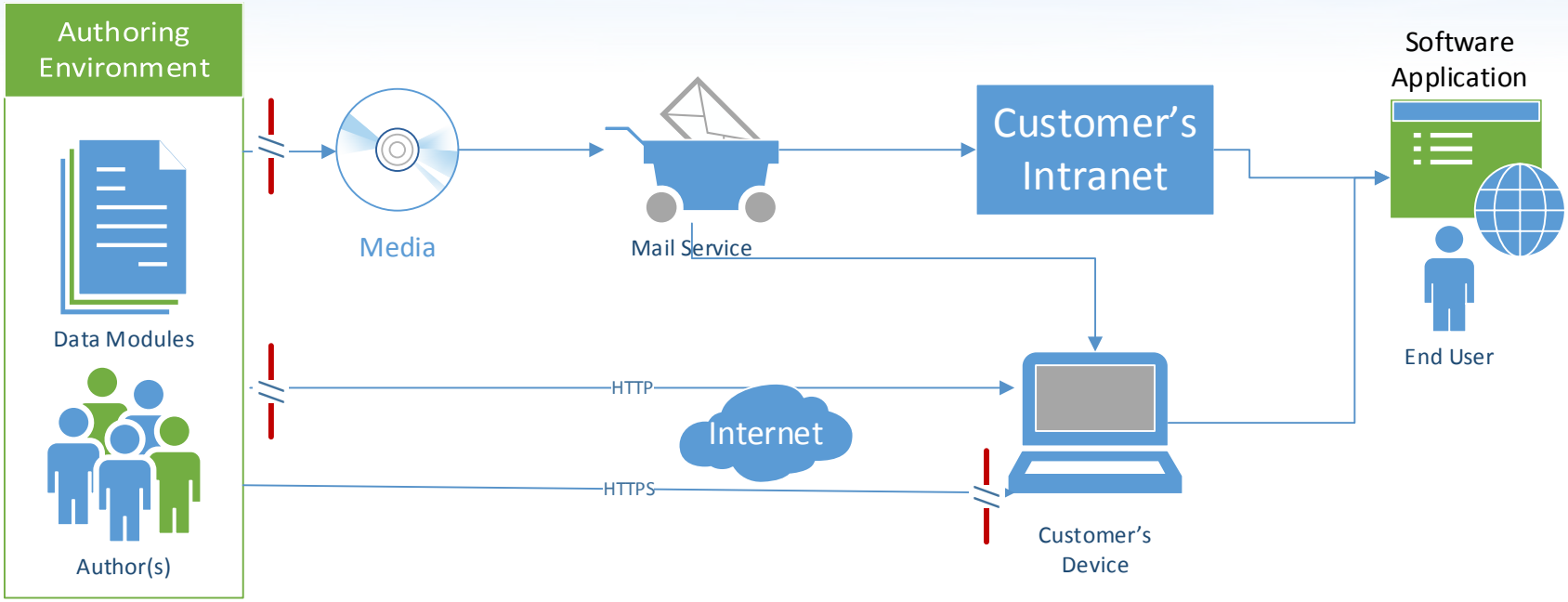
Air Defence Programme

stergios.isaakidis@nspa.nato.int

Topics

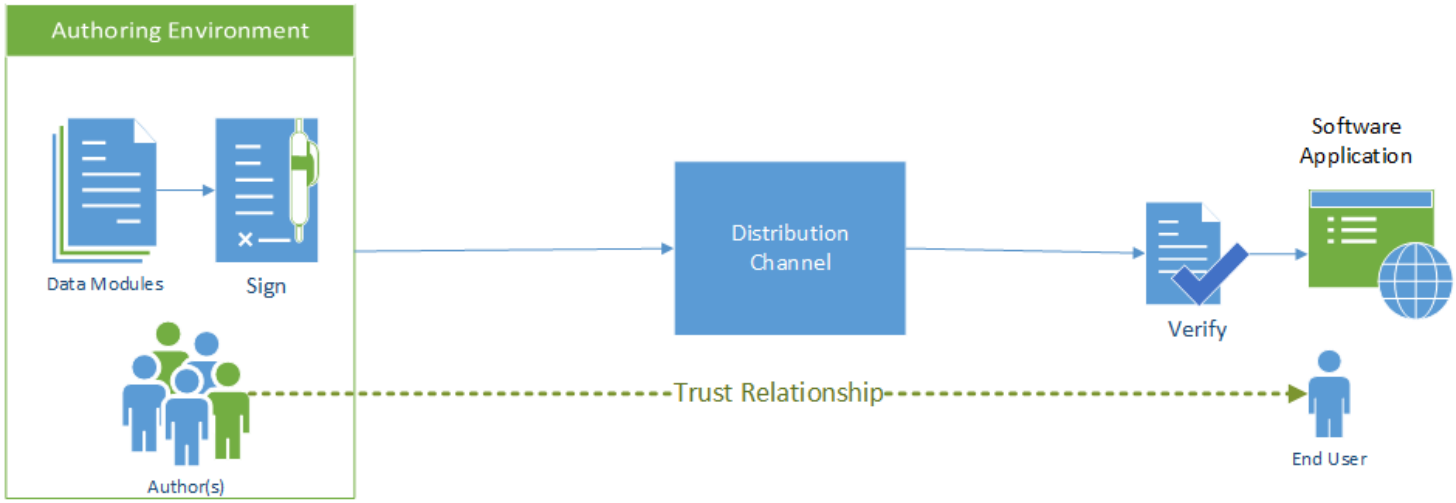
- Data Modules distribution and integrity boundaries
- Digital signature benefits
- Signing concept
- Technical Implementation
  - Signature definition
  - How to get a certificate
  - Implementation effort
- References

Data Modules distribution and integrity boundaries

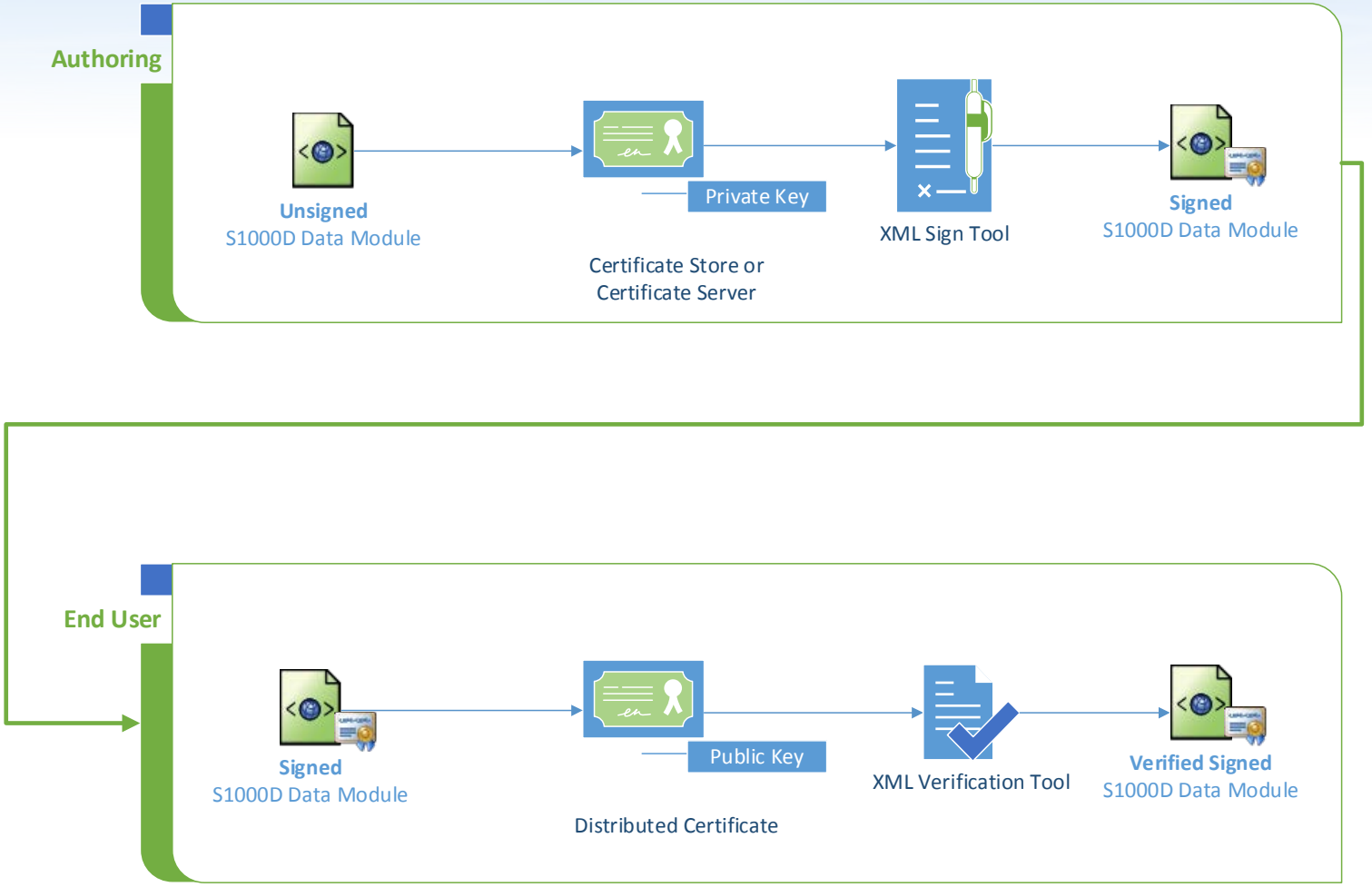


Digital Signature Benefits

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



Signing concept



Technical Implementation: Signature definition

Specification:

```
<Signature ID?>
   <SignedInfo>
     <CanonicalizationMethod/>
     <SignatureMethod/>
     (<Reference URI? >
       (<Transforms>)?
       <DigestMethod>
       <DigestValue>
     </Reference>)+
   </SignedInfo>
   <SignatureValue>
  (<KeyInfo>)?
  (<Object ID?>)*
 </Signature>
```

Example:

```
- <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    - <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      - <Reference URI="">
        - <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>SRrIgJXJAqWuFjUkUg/XqPp8hEI=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>YvtbCMzVnfoNkL5wxxXwsj0P+Zw52ahd1NYEH3IjkOCggf6riZRhXHdkyhuhTADsAQa
    - <KeyInfo>
        - <X509Data>
          - <X509IssuerSerial>
              <X509IssuerName>CN=EDCA, DC=NSPA, DC=LU</X509IssuerName>
              <X509SerialNumber>127679794098451467206661</X509SerialNumber>
            </X509IssuerSerial>
          </X509Data>
        </KeyInfo>
    </Signature>
</opunuwp>
```

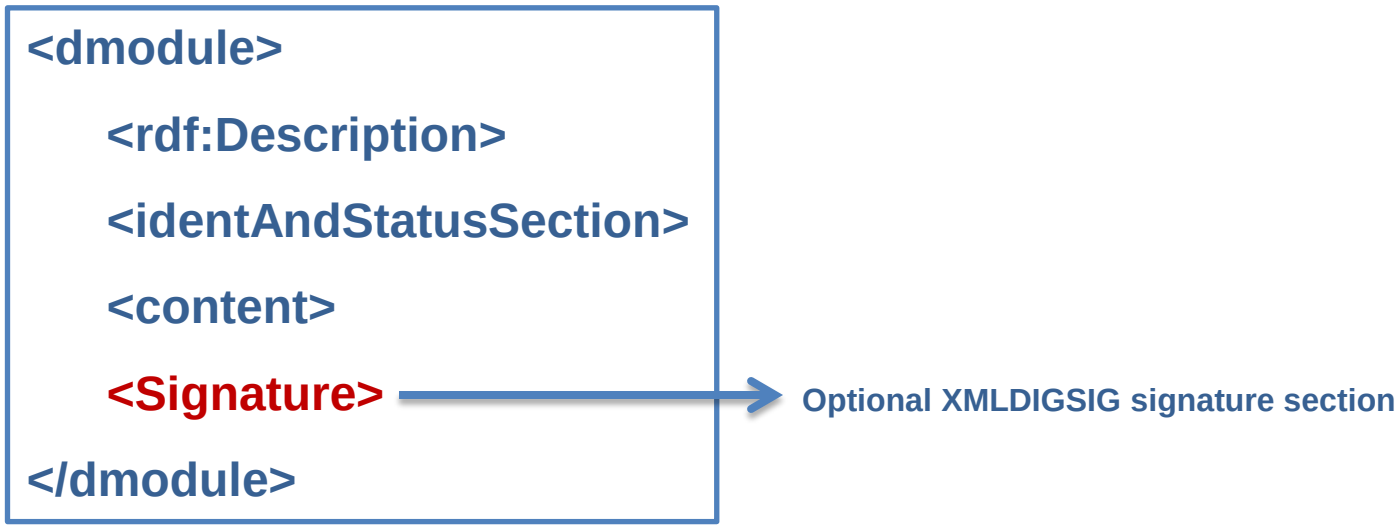
Notes:

“?”: zero or one occurrence

“+”: one or more occurrences

“*”: zero or more occurrences

Technical Implementation: Signature definition



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):
    - .NET Framework (System.Security.Cryptography.Xml namespace)
  - 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

- ITU-T X.509|ISO/IEC 9594-8: “Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”
- W3C, XML Signature Syntax and Processing (Second Edition), http://www.w3.org/TR/2008/REC-xmldsig-core-20080610

Dr. Stergios ISAAKIDIS | Senior Technical Officer
NSPA Logistics Operations | Air Defence Programme
11 rue de la Gare, L-8325 Capellen, Luxembourg
Tel: +352 3063 6248 | Fax: +352 3063 4800 | NCN: 2686248