Paper for Consideration by S100TSM9

Inconsistencies between XSD Schema and Part 15 - and missing instructions for when to use S100_SE_DigitalSignature, StandaloneDigitalSignature and S100_SE_SignatureOnData

Submitted by:	PRIMAR
Executive Summary:	There seems to be some inconsistencies between part 15 and the schema XSD file: https://staging.s100dev.net/schemas/S100/5.0.0/S100SE/20220728/Part15.xsd Explanatory text is needed for the use of S100_SE_DigitalSignature, StandaloneDigitalSignature and S100_SE_SignatureOnData.
Related Documents:	S-100 5.0.0 Part 15
Related Projects:	

Introduction / Background

In S-100 Part 15 some classes have inconsistencies in the name of the classes between part 15 and the schema. There also seems to be limited text explaining the use of the different classes. The confusion can also be a result of different notations between the part 15 text, missing protection scheme UML and different notation used in the part 15 XSD schema definition file.

Analysis/Discussion

1. In S-100 Part 15 15-8.8 the following example for additional digital signatures is used:

```
[datasetDiscoveryMetadata entry]
  <S100XC:signature id="s1" certificateRef="PROD1" dataStatus="Unencrypted">
     MEUCIQCplrd+/Bb436FwXQWxgwxdcj9BhMN+EiMmZD4/6khpWwIgfLy70alp7pZSEeR27zThhQCl
OVA/ST01C+75Ond1Pu0=
  </S100XC:signature>
  <S100XC:additionalSignature>
   <S100CE:signatureOnData id="s2" certificateRef="RENC1" dataStatus="Encrypted">
MEYCIQCg+OdfUcfGJUxUKd53NmtGJ9jVOTACrKTRQM96KE0yCgIhAJ35u1aQjej7absi/VllVOTS
DtKPUjxWAh+/DOWj+IOW
   </S100CE:signatureOnData>
  </S100XC:additionalSignature>
  <S100XC:additionalSignature>
   <S100CE:signatureOnSignature id="s3" certificateRef="DIST1" signatureRef="s2">
     MEUCIQCTGuSnqrbdQmO8ar4DdRGOjF8n5CI/9f/pGhDPeB2QhQIgMawaStd1wWJXiw1aDpz2JV/r
F9Hsx2txMN/3f2t8FIM=
   </S100CE:signatureOnSignature>
  </S100XC:additionalSignature>
```

In the schema XSD file the following names for those classes are:

```
<xs:element name="S100_SE_SignatureOnSignature" type="S100_SE_SignatureOnSi
<xs:element name="S100_SE_SignatureOnData" type="S100_SE_SignatureOnData" s
<!--  EXTENSION FOR SIGNATURES ON OTHER FORMS OF THE FILE (USUALLY UNENCRYP
<xs:complexType name="S100_SE_SignatureOnData">
▼<xs:annotation>
```

```
</xs:element>
  <!--  EXTENSION FOR SIGNATURES ON SIGNATURES  -->
 ▼<xs:complexType name="S100_SE_SignatureOnSignature">
   ▼<xs:annotation>
       <xs:documentation/>
```

- There seems to be a wrong naming of "S100CE:signatureOnData" in Part 15 example vs S100_SE_SignatureOnData in XSD.
- There seems to be a wrong naming of "S100CE:signatureOnSignature" in Part 15 example vs S100_SE_SignatureOnSignature in XSD.

The proposal would be to amend the example in Part 15-8.8 to align with schema XSD (or the opposite way) and ensure a complete review to ensure common notations are being used in the part 15 text and examples, UML diagram and XSD class definitions.

2. StandaloneDigitalSignature
There is an inconsistency between the XSD schema (for the class StandaloneDigitalSignature attribute signature) and Part 15 15-8.11.2

The Data Type S100_SE_DigitalSignature is used in the schema XSD:
https://staging.s100dev.net/schemas/S100/5.0.0/S100SE/20220728/Part15.xsd

```
▼<xs:complexType name="StandaloneDigitalSignature">
  ▼<xs:annotation>
     <xs:documentation>A single digital signature</xs:documentation>
  </xs:annotation>
  ▼<xs:sequence>
    ▼<xs:element name="filename" type="xs:string">
      ▼<xs:annotation>
         <xs:documentation>The filename of the content signed</xs:documentation>
      </xs:annotation>
    </xs:element>
    ▼<xs:element name="certificates" type="S100_SE_CertificateContainerType">
      ▼<xs:annotation>
         <xs:documentation>Any certificates required to authenticate the signature against the SchemeAdministrator</xs:documentation>
      </xs:annotation>
    </xs:element>
    ▼<xs:element name="digitalSignature" type="S100_SE_DigitalSignature">
      ▼<xs:annotation>
         <xs:documentation>A single digital signature</xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

Part 15 refers DigitalSignature:

15-8.11.2 StandaloneDigitalSignature

Role Name	Name	Description	Mult.	Data Type	Remarks
Class	StandaloneDigitalSignature	A single digital signature	-	-	-
Attribute	filename	The filename of the content signed	1	CharacterString	The filename of the resource signed
Attribute	certificates	Any certificates required to authenticate the signature against the SchemeAdministrator	1	S100_SE_CertificateContainer	
Attribute	signature	A single digital signature	1	DigitalSignature	The signature of the file resource

Proposal is to amend Part 15-8.11.2 to S100_SE_DigitalSignature, to be in alignment with the XSD Schema.

3. Part 15 XSD file defines classes S100_SE_DigitalSignature, StandaloneDigitalSignature, S100_SE_SignatureOnData without being explicit in S-100 Part 15 when they are going to be used. Except for the very limited description in 15-8.11.4 there are no further instructions of their use anywhere:

15-8.11.4 S100_SE_DigitalSignatureValue

The class S100_SE_DigitalSignatureValue is realized as one of either S100_SE_SignatureOnData (a digital signature of a particular identified resource) or an additional digital signature defined using the class S100_SE_AdditionalSignature, each of which is either a S100_SE_SignatureOnData or S100_SE_SignatureOnSignature element as described in clause 15-8.8. S-100 Part 17 metadata thus allows for multiple digital signatures, a single mandatory S100_SE_SignatureOnData and any number of additional signatures, either of the data or other signatures.

It is proposed that explanatory text is developed and added accordingly.

Conclusions
- Amend example in Part 15 15-8.8 to align with schema XSD.
- Conduct a complete review to ensure common notations are being used in the part 15 text and examples, UML diagram and XSD class definitions.
- Amend Part 15 15-8.11.2 to S100_SE_DigitalSignature, to align with schema XSD.
- Develop explanatory text for 100_SE_DigitalSignature, StandaloneDigitalSignature and S100_SE_SignatureOnData for when to be used.

Action Required of S100TSM9
The S100TSM is invited to:

Note the paper and discuss proposed changes.