1 Timestamp token

This section contains the definition of the timestamp token.

1.1 Schema Header and Namespace Declarations

The following schema fragment defines the XML namespaces and other header information for the timestamp token schema:

```
<xs:schema targetNamespace="urn:oasis-open:tc:names:dss:1.0:
 schema-v01"
 xmlns:dss="urn:oasis-open:tc:names:dss:1.0:schema-v01"
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified"
 attributeFormDefault="unqualified">
<xs:import namespace="http://www.w3.org/2000/09/xmldsig#"
 schemaLocation="http://www.w3.org/TR/2001/PR-xmldsig-core-
20010820/xmldsig-core-schema.xsd"/>
```

This schema imports definitions from the XML Digital Signature schema.

1.2 Element <tst>

The <tst> element represents a single timestamp token.

```
<xs:element name="tst" type="ds:SignatureType"/>
```

The <tst> element has the same type-definition as the **ds:SignatureType** definition. In this way, a timestamp can be created and validated by a conventional XML Digital Signature implementation.

The following sections define how the elements of the <ds:Signature> element MUST be used.

ds:Signature/KeyInfo/KeyName [Optional]

If present, the <KeyName> element SHALL contain a string representation of the TSA's name. In the case where the signature is verified by means of an X.509 certificate, the <KeyName> value SHOULD be the UTF-8 value from the TSA's signature-verification certificate Subject field.

ds:Signature/SignedInfo/Reference [Required]

The <Reference> element SHALL contain a barename URI identifying the <tst> element. It MUST also reference the document or documents that are timestamped.

ds:Signature/Object [Required]

The <tstInfo> element SHALL be contained in an <Object> element. Any extension elements that are not defined by this specification SHALL also be represented as <Object> elements.

1.3 Element <tstInfo>

A <tstInfo> element MUST be included in the <tst> element as a <ds:Signature/Object> element. The <tstInfo> element is of type **tstInfoType**.

```
<xs:element name="tstInfo" type="dss:tstInfoType"/>
```

1.4 ComplexType tstInfoType

This section contains the definition of the **tstInfoType** complex type.

```
<xs:complexType name="tstInfoType">
 <xs:sequence>
  <xs:element name="serialNumber" type="xs:integer"/>
  <xs:element name="creationTime" type="xs:dateTime"/>
  <xs:element name="policy" type="xs:anyURI" minOccurs="0"/>
  <xs:element name="accuracy" type="xs:duration" minOccurs="0"/>
  <xs:element name="ordered" type="xs:boolean" default="false"/>
 </xs:sequence>
</xs:complexType>
```

Defines the following elements (these could be represented as attributes).

`<SerialNumber>` [Optional]

This element SHALL contain a serial number produced by the timestamp authority. It MUST be unique across all the tokens issued by a particular TSA. Provided relying parties do not accept timestamp tokens from distinct TSAs that use the same name, the combination of the issuer name and the serial number will uniquely identify a timestamp token to a particular relying party. For these reasons, it is RECOMMENDED that the serial number be included.

`<Policy>` [Optional]

This element SHALL contain the policy under which the token was issued. If the corresponding element appears in the request, then this element MUST contain one of the values supplied in the request. Amongst other things, the TSA’s policy SHOULD identify the fundamental source of its time.

`<CreationTime>` [Required]

The time at which the token was issued. It SHALL be a time according to the local clock of the authority, no earlier than the time at which the request was completely received and no later than the time at which the signature process was started.

`<Accuracy>` [Optional]

The TSA’s estimate of the accuracy of its local clock.

`<Ordered>` [Default=”false”]

This element SHALL indicate whether or not timestamps issued by this TSA, under this policy, are strictly ordered according to the value and precision of the `<CreationTime>` value.

2 Timestamp verification procedure

We need to specify the steps by which a token is verified.

3 Example

[r01]

```
<tst xmlns="urn:oasis-open:tc:names:dss:1.0:schema-v01" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis-open:tc:names:dss:1.0:schema-v01 D:\MYDATA~1\Standards\dss\TSTV01~1\tst.xsd">
```

[r02]

```
  <ds:SignedInfo>
```

```
[r03]     <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
[r04]     <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
[r05]     <ds:Reference URI="#tst">
[r06]       <ds:Transforms>
[r07]         <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
[r08]       </ds:Transforms>
[r09]       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[r10]       <ds:DigestValue>A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D</ds:DigestValue>
[r11]     </ds:Reference>
[r12]     <ds:Reference Id="A1UdAQQ8MDqAEEVs">
[r13]       <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[r14]       <ds:DigestValue>4706816A 9CD0D89D A9993E36 BA3E2571 7850C26C</ds:DigestValue>
[r15]     </ds:Reference>
[r16]   </ds:SignedInfo>
[r17]   <ds:SignatureValue>IWijxQjUrcXBYoCf</ds:SignatureValue>
[r18]   <ds:KeyInfo>
[r19]     <ds:KeyName>DC="com" DC="AcmeCorp"</ds:KeyName>
[r20]   </ds:KeyInfo>
[r21]   <ds:Object>
[r22]     <tstInfo>
[r23]       <serialNumber>4758930295470847</serialNumber>
[r24]       <creationTime>2001-12-17T09:30:47-05:00</creationTime>
[r25]   <policy>urn:com:acme:timestamp:policies:policy1:v05:</policy>
[r26]       <accuracy>T00:00:01</accuracy>
[r27]     </tstInfo>
[r28]   </ds:Object>
[r29] </tst>
```

[r01-[r29] – The timestamp token.

[r05[- A reference to the timestamp token that results in the token information being included in the scope of the timestamp signature.

[r07] – The enveloped-signature transform that excludes the signature value from the signature calculation.

[r12] – A reference to the document that is timestamped.

[r17] – The signature value.

[r24] – The estimated time according to the TSA: 9:30 and 47 seconds AM Eastern Standard Time on 17th of December 2001.

[r25] – The identifier for the policy under which the timestamp was created.

[r26] – The TSA's estimate of its time accuracy: +/- 1s.

Note: the `<Ordered>` element is omitted. Its default value is False. Therefore, the relying party cannot assume the timestamps under this policy are strictly ordered.