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="http://www.oasis-
open.org/tc/dss/v1.0/timestamp-token/schema/wd/v02"
xmlns:dss="http://www.oasis-open.org/tc/dss/v1.0/timestamp-
token/schema/wd/v02" 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 token 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:KeyInfo/ [Required]`

The `<KeyInfo>` element SHALL identify the issuer of the timestamp and MAY be used to locate, retrieve and validate the timestamp token signature-verification key.

`ds:SignedInfo/Reference [Required]`

The `<Reference>` element SHALL contain a bare name XPointer reference to the `<tstInfo>` element. It MUST also reference the document or documents that are timestamped.

`ds: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:attribute name="serialNumber" type="xs:integer"/>
     <xs:attribute name="creationTime" type="xs:dateTime"/>
     <xs:attribute name="policy" type="xs:anyURI" use="optional"/>
     <xs:attribute name="errorBound" type="xs:duration"
use="optional"/>
     <xs:attribute name="ordered" type="xs:boolean"
default="false"/>
  </xs:complexType>
```

Defines the following attributes.

Attribute `serialNumber` [Required]

This attribute 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.

Attribute `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.

Attribute `policy` [Optional]

This attribute SHALL identify 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.

Attribute `errorBound` [Optional]

The TSA's estimate of the maximum error in its local clock.

Attribute `ordered` [Default="false"]

This attribute 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` attribute value.

2 Timestamp verification procedure

If any one of these steps results in failure, then the timestamp token SHOULD be rejected.

1. Locate and verify the signature-verification key corresponding to the `ds:KeyInfo/` element contents.
2. Verify that the signature-verification key is authorized for verifying timestamps.
3. Verify that the signature-verification key conforms with all relevant aspects of the relying-party's policy.
4. Verify that all digest and signature algorithms conform with the relying-party's policy.
5. Verify that the signature-verification key is consistent with the `ds:SignedInfo/SignatureMethod/@Algorithm` attribute value.
6. Verify that there is a `ds:SignedInfo/Reference/@URI` attribute whose value is "#tstInfo".
7. Verify that there is a `ds:SignedInfo/Reference/@` attribute that correctly identifies the timestamped document.
8. Verify that the `tstInfo/@policy` attribute value is acceptable.
9. Establish a maximum acceptable error bound value and verify that the `tstInfo/@errorBound` attribute value is less than or equal to this value.
10. Verify all digests and the signature.

11. If comparing the `tstInfo/@creationTime` attribute value to another time value, first verify that they differ by more than the maximum acceptable error bound value.

3 Example

```
[e01]  <?xml version="1.0" encoding="UTF-8"?>
[e02]  <tst xmlns="http://www.oasis-open.org/tc/dss/v1.0/timestamp-token/schema/wd/v02"
       xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
       instance" xsi:schemaLocation="http://www.oasis-open.org/tc/dss/v1.0/timestamp-token/schema/wd/v02
[e03]  D:\MYDATA~1\Standards\dss\TSTV02~1\tst.xsd">
[e04]      <ds:SignedInfo>
[e05]          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
       20010315"/>
[e06]          <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
[e07]          <ds:Reference URI="#tstInfo">
[e08]              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[e09]              <ds:DigestValue>A9993E36 4706816A BA3E2571 7850C26C
       9CD0D89D</ds:DigestValue>
[e10]          </ds:Reference>
[e11]          <ds:Reference Id="A1UdAQQ8MDqAEEVs">
[e12]              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[e13]              <ds:DigestValue>4706816A 9CD0D89D A9993E36 BA3E2571
       7850C26C</ds:DigestValue>
[e14]          </ds:Reference>
[e15]      </ds:SignedInfo>
[e16]      <ds:SignatureValue>IWijxQjUrcXBYoCf</ds:SignatureValue>
[e17]      <ds:KeyInfo>
[e18]          <ds:KeyName>DC=com, DC=AcmeCorp</ds:KeyName>
[e19]      </ds:KeyInfo>
[e20]      <ds:Object>
[e21]          <tstInfo serialNumber="4758930295470847" creationTime="2001-12-17T09:30:47-05:00"
       policy="urn:com:acme:timestamp:policies:policy1:v05" errorBound="T00:00:01"/>
[e22]      </ds:Object>
[e23]  </tst>
```

[e02]-[e26] – The timestamp token.
[e07] - A reference to the timestamp token information that results in the token information being included in the scope of the timestamp signature.
[e11] – A reference to the document that is timestamped.
[e16] – The signature value.
[e18] – The issuer of the timestamp.
[e21] – The timestamp token information, comprising: the serial number, the estimated time according to the TSA: 9:30 and 47 seconds AM Eastern Standard Time on 17th of December 2001, the identifier for the policy under which the timestamp was created and the TSA's estimate of its time error: +/- 1s.
Note: the `Ordered` attribute is omitted. Its default value is False. Therefore, the relying party cannot assume that timestamps under this policy are strictly ordered.