A. Santoni
Actalis S.p.A.
Internet Draft
Intended status: Informational
Expires: September 2008
March 19, 2008

Syntax for binding documents with time stamps

draft-santoni-timestampeddata-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document describes a syntax which can be used to bind a generic document (or any set of data, not necessarily protected by means of cryptographic techniques) to one or more time-stamp tokens obtained for that document, where "time-stamp token" has the meaning defined in RFC 3161. Additional types of temporal evidence are also supported.

This document proposes a simple syntax based on the Cryptographic Message Syntax (RFC 3852).

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [KWORDS].

Table of Contents

1. Introduction

Digital time stamping has become the standard technique for proving the existence of a document before a certain point in time. Several digital signature legislations around the world embrace the concept and provide for time-stamping services as an approved means for attesting the signing time and/or for extending the validity of signed documents beyond the expiry date of the signer's certificate.

However, while digital time stamping enhances digital signature, its value does not depend on this latter. It can obviously be useful to time-stamp a document even if this is not signed. And it can also be useful, or even mandatory in some cases, to time-stamp a document in its entirety, regardless of how many signatures it contains.

When a time-stamp is related to a digital signature, there already exist a way to keep the two pieces together: RFC 3161 describes how one or more TimeStampTokens can be included in a SignerInfo structure as unsigned attributes. On the other hand, when time-stamps are not related to a digital signature, there is no standard way to keep together the time-stamped document and the related time-stamps.

In such cases two approaches are typically being adopted:

- time-stamps are kept as separate files (keeping track of what time-stamps belong to what documents is up to the user);

- an ad hoc solution is adopted for specific applications, like e.g. a ZIP archive or a proprietary "envelope" of some kind.

Both solutions impede interoperability, the objective of this memo.

This document proposes a simple syntax for bundling one document (actually, any kind of file) to the corresponding temporal evidence, this latter being typically represented by one or more RFC 3161 TimeStampTokens. Additional types of temporal evidence, like e.g. an RFC 4998 EvidenceRecord, are also supported via an "open" syntax. However, for the sake of interoperability, the emphasis is given to TimeStampTokens.

The proposed syntax is broadly based on the Cryptographic Message Syntax (CMS) defined in RFC 3852 [CMS].

2. Syntax for TimeStampedData

The proposed data structure is called TimeStampedData and it is based on the ContentInto envelope defined in [CMS]:

```
ContentInfo ::= SEQUENCE {
   contentType ContentType,
   content [0] EXPLICIT ANY DEFINED BY contentType }
```

```
ContentType ::= OBJECT IDENTIFIER
```

While CMS defines six content types (data, signed-data, enveloped-data, digested-data, encrypted-data, and authenticated-data), this memo defines an additional content type, timestamped-data, identified by the following specific contentType OID:

```
id-timestamped-data OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs7(7) 9 }
```

This particular OID signals that the content field of the ContentInfo has the following syntax:

```
TimeStampedData ::= SEQUENCE {
   version        INTEGER { v1(1) },
   fileName       UTF8String,
   mimeType       PrintableString,
   content        OCTET STRING,
   evidence       Evidence
}

Evidence ::= CHOICE {
   timeStamps        [0] SET (SIZE(1..MAX)) OF TimeStampToken,
   evidenceRecord    [1] EvidenceRecord
   -- additional evidence types to be registered with the IETF
}
```

The version field contains the version number of the TimeStampedData syntax. The initial version number is 1.

The fileName field contains the original filename of the document which was time-stamped and whose content was inserted into the TimeStampedData structure.

The mimeType field contains a MIME media type and subtype for the bundled file (e.g. "text/rtf"), according to RFC 2045 [MIME]. It is an advisory information which may help decide how to open or deal with the file after having "detached" it from the TimeStampedData structure, regardless of the filename extension (which could be missing or unknown).

The content field carries the entire content, in its original format, of the file which was time-stamped. The file need not be a document in the strict sense; it can be any kind of file (e.g. an executable, a database, etc).

The evidence field carries the evidence that the content data existed before a certain point in time. The TimeStampedData syntax allows for different types of evidence (like e.g. an EvidenceRecord according to RFC 4998). However, this document mandates support for one type only: a non-empy set of RFC 3161 TimeStampToken's [TSP].

Additional types of evidence may be used after having registered them (and having had a distinguishing tag assigned to them) with the IETF. A suitable registration procedure should be defined for that purpose.

3. Compliance requirements

Compliant applications MUST support the RFC 3161-based type of evidence (i.e. the timeStamps CHOICE).

Compliant applications MUST always populate the mimeType field of TimeStampedData structure with a valid MIME type/subtype string according to RFC 2045 [MIME]. A valid example is "application/pdf". An invalid example is "whatever". An empty string is not allowed.

4. Recommended processing

When generating the TimeStampedData structure, applications are supposed to behave like follows:

- populate the version field with the integer value v1(1);

- populate the fileName field with the real name of the file;

- populate the mimeType field with an appropriate MIME type/subtype string, preferably, or at least with "application/octet-stream";

- populate the content field with the entire contents of the file in its original format and encoding;

- add the necessary evidence (e.g. one or more TimeStampTokens);

- insert the TimeStampedData into a ContentInfo structure, with the id-timestamped-data OID in the contentType field;

- BER-encode the ContentInfo structure and save it with the same name of the time-stamped file, but with the file extension recommended in section 5.

When parsing an existing TimeStampedData structure, applications are supposed to behave like follows:

- check that the contentType field of the ContentInfo structure has the expected value (id-timestamped-data) in its contentType field; then, extract the inner TimeStampedData structure and continue processing;

- check the version field (it should be v1);

- check the fileName field and keep it for later use;

- check the mimeType field and keep it for later use;

- read the content field and prepare to save it in a separate file and/or show it to the user (or otherwise deal with it);

- check that the evidence field not be empty; extract the inner data and prepare to show them to the user and/or save them to separate files;

- validate the evidence data (e.g. in case of timeStamps: check that each TimeStampToken does indeed contain the hash of the document and it was signed by a trusted TSA);

- depending on the application, show the evidence data to the user;

- depending on the application, show the time-stamped document to the user, possibly by activating a suitable external "viewer" based on the fileName extension and the mimeType field;

- depending on the application, save the content field into a separate file with the name specified by the fileName field (see Security Considerations) or let the user specify the desired filename.

5. Recommended file extensions

A file containing a TimeStampedData structure SHOULD bear the .tsd extension. Example: "patent123.tsd"

6. Security Considerations

Any consumer of TimeStampedData should validate the entire filename (carried in the filename field of the TimeStampedData structure) according the rules of its local filesystem and its intended usage before using some or all of the name to store the data.

7. IANA Considerations

This document defines one object identifier under the pkcs7 arc:

```
id-timestamped-data OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs7(7) 9 }
```

8. References

[KWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[TSP] Adams, C., Cain, P., Pinkas, D. and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001. http://www.ietf.org/rfc/rfc3161.txt

[CMS] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004. http://www.ietf.org/rfc/rfc3852.txt

[MIME] Borenstein, N., and N. Freed, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996. http://www.ietf.org/rfc/rfc2045.txt

[ERS] Gondrom, T., Brandner, R., and Pordesch, U., "Evidence Record Syntax (ERS)", RFC 4998, August 2007. http://www.ietf.org/rfc/rfc4998.txt

Author's Addresses

Adriano Santoni
Actalis S.p.A.
Via Taramelli 26
I-20124 Milano

Phone: +39-02-68825.1
Email: adriano.santoni@actalis.it

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.