LTANS
Internet-Draft
Intended status: Informational
Expires: January 13, 2011

T. Gondrom
S. Fischer-Dieskau

July 12, 2010

Validation and long term verification data for Evidence Records and signed documents
draft-ietf-ltans-validate-03

Abstract

Digitally signed documents and data in a LTANS service receive the signature renwal procedures and non-repudiation services. As documents can be stored for very long (theoretically inifinite) times, it is very important to understand which data is and will be necessary for the verification of the contained digital signatures and the applied timestamps and the evidence records. This document shall describe various pieces of information which SHOULD and MUST be provided to effectively verify evidence records and their protected data and signatures.

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 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 13, 2011.

Copyright Notice

Table of Contents

1. Introduction

Data and documents stored in a Long term archiving services may contain digitally signed or encrypted data and their integrity may be assured with the use of timestamps and archivetimestamps as specified in ERS and XMLERS. As such data and it's proof of existence and non-repudiation may be verified at a point in time very far in the future, it is important to analyse and understand what information may be needed for this verification and what controls need to be implemented to ensure the availability and integrity of this data.

2. Terminology

Archived data object: Data unit that is archived and has to be preserved for a long time by the Long-term Archive Service.

Archived data object group: A multitude of data objects, which for some reason belong together. E.g. a document file and a signature file could be a archived data object group, which represent signed data.

Archive Timestamp: Is a timestamp and lists of hash values, which allows to verify the existence of several data objects at a certain time.

Evidence: Information that may be used to resolve a dispute about various aspects of authenticity of archived data objects.

Evidence record: Collection of evidence compiled for one or more given archived data objects over time. An evidence record includes all Archive Timestamps (within structures of Archive Timestamp Chains and Archive Timestamp Sequences) and additional verification data, like certificates, revocation information, trust anchors, policy details, role information, etc.

Long-term Archive Service(LTA): A service responsible for preserving data for long periods of time, including generation and collection of evidence, storage of archived data objects and evidence, etc.

hash-tree: a hash tree as decribed by Merkle in [MER1980] is a list of sorted hash values ordered in a tree where the child nodes are combined and hashed to generate the father nodes up to one top node. This hash-tree can also be reduced to a list as decribed in ERS.

Timestamp: A cryptographically secure confirmation generated by a Time Stamping Authority (TSA) [RFC3161] specifies a structure for timestamps and a protocol for communicating with a Time-stamp Authority (TSA). Besides this, other data structures and protocols may also be appropriate, e.q., such as defined in [ISO-18014-1.2002], [ISO-18014-2.2002], [ISO-18014-3.2004], and [ANSI.X9-95.2005].

Trust Center: A Trust Center may be operated as a Trusted Third Party (TTP) service (as also specified in RFC 3161), though other operational models may be appropriate. Depending on local laws and criteria the services of a trust center may include to provide certificates, OCSP responses and CRL for a guarantted period of time. The Trust center can also function as the Trusted Third party connecting (and guaranteeing the identity of the owner of a certificate with a certain person.

3. General Considerations

3.1. Basic assessment of environment of verification data

Due to the lack of a common, international wide applicable understanding of terms used in respect of digital signature related objects some basic assessments have to be presumed and are discussed in this section.

3.2. Types of trust centers (fully trusted - partially trusted)

Depending on local laws and authorities trust centers can be of different levels of trust which can have impact on the verification data needed for a later verification of the digital signatures, time stamps and ERS.
Typically two types of trust centers can be envisioned:

3.2.1. Fully trusted trust center

A trust center that has been accredited by a local government authority or a private office declared as competent from such, the accreditation saying that all relevant requirements to ensure a certain security level are fulfilled (as typically done in most of the European countries) can be classified as a fully trusted at least in the national context. In case of multinational mutual acceptance agreements this trust can be extended to regions or globally. Based on the accreditation and the national interest in these trust centers it can be assumed that it would be publicly known that and when a private key of such a trust center was compromised.

3.2.2. Partially trusted Trust Center

Partially trusted centers could e.g. be private organizations which function as a kind of common notary but whose security and protection is not accredited by a government authority. This usually means that the validity and availability of the verification data can not be guaranteed. This implies that the LTA (Long term archive) has to ensure at least the availability and usually also the integrity of the data itself including all OCSP responses and or CRLs.

3.2.3. Layer model versus chain model

Typically a signature depends on other instances that issue a certificate which again have their certificates issued by another instance. E.g. a person could get his certificate issued by a local (or company) trust center, which in turn gets its own certificate issued by a government authority of fully trusted trust center. So for verifiying a signature it is necessary to verify all certificates up to the root which must be trusted if the signature shall be verified positively.

This raises the question if it is necessary that all certificates up to the roof have to be valid at the time of signing (layer model), or if it is sufficient that only the latest signature is not yet expired at the time of signing and all signature algorithms used in the chain are still considered secure (chain model).

Both models have pros and cons regarding the consequences occurring from different scenarios. As the layer model is established on the international level more respected and accepted point of view.

Based on discussion in the working group the layer model is necessary for verifying a chain of certificates when you verify a signature.

This would mean that all signatures in the certificates must be valid at the time of signing. This means all used algorithms must still be secure and none of them must have been revoked. (note: both cases would mean that the chain could have been compromised at this level and below and which means the final signature can not be trusted.)

Note: the layer model for the validity of the signatures in the certificates does not imply that all certificates have not been expired. In the contrary, concerning the expiry dates of certificates this means only you need to verify that the last certificate has not been expired when the signature has been done. It is of no interest whether certificates in the chain have already been expired as long as they have been valid at the time when they were used to sign (issue) the lower certificates.

4. Verification data for Evidence Records

4.1. List of verification data

Evidence Records contain hashtrees secured with time stamps. The security and verification of the hashtrees themselves only depend on the used hash algorithm and its possible parameters. Despite the generally available list of algorithms and their validity period (which could be documented in a general policy) no further external verification data is necessary to validate the integrity of the hashtrees.

The time stamps used in the Evidence Record are based on digital Signatures. To validate these signatures in respect of their authenticity additional verification data like certificates of all parties involved in the issuance of the time stamp certificate, Certificate Revocation Lists (CRLs) and/or OCSP responses are needed.

To correctly verify the time stamps in the Evidence Record an expert needs to verify that the used private key has not been compromised when it has been used. The time information provided by a trusted time stamp authority allows to determine the reference date to which the used private key had to be valid.

Additionally to fully evaluate the certificate used in respect of the time stamp signature the correct chain of issuers of all certificates up to the root need to be checked.

Knowing the reference date the verifier needs an OCSP response or a CRL to verify that the used certificate has not been revoked at the moment of signature creation. Note: OSCP responses are not needed when a misuse of the certificate can be excluded before its owner has obtained it, as could be the case with accredited time stamp authorities.

In cases where a specially accredited authority is the trusted time stamp authority (refer to 2.1.1 a) fully trusted trust center), it could be assumed that the compromise of used keys would have so much impact that it would be publicly known even without directly checking the CRL or OCSP status of the used certificate. This situation can justify that it is only necessary to store all certificates but no CRL or OCSP response with the time stamp used in the Evidence Record. Additionally based on the accreditation criteria it can also be the case that certain availability of verification data is guaranteed by the local government. (E.g. in Germany for 30 years).

4.2. Location to store verification data

All verification data necessary for the verification of the time stamp has to be stored in a non-repudiation system as long as a later verification may be needed. And as this verification data contain electronic signatures which used algorithms may expire further renewals of these electronic signatures may be necessary[S2]. E.g. in RFC3161 time stamps the verification data can be directly integrated into the time stamp, and is by this integrated, protected and automatically renewed with the ERS using the time stamp.

4.3. Verification Data retrieved from an SCVP server

The necessary verification data can also be stored separately in an SCVP server an be retrived from there. This relieves the archiving party from integrating all evidence right at the time of archival right into the document. The system can only store the data and some subset of the verification data, e.g. only the end entity certificates into the documents and their signatures and leave it to an SCVP server to store and protect the remaining required verification data. The SCVP server can provide this data and their according protecting evidence recprds via ERS/SCVP [LTANS-ERS-SCVP].

5. Verification data for the signed documents secured by the Evidence Records

5.1. List of required verification data

In respect of the verification data needed to secure a long term validation of the electronic signature all the above mentioned requirements are applicable. The only differences refer to the fact that the signature is not issued by a time stamp authority as owner of the certificate but a person.

Therefore a special reference time regarding the validity of the certificate at the time of signature creation is needed to verify that the used private key has not been compromised before it has been used.

With reference to the above the correct chain of issuers of all certificates up to the root need to be verified to fully evaluate the certificate used in respect of the signature. A CRL is needed to verify that the used certificate has not been revoked at the moment of signature creation. To verify the authenticity of the CRL the issuer of it has to be checked by verifying the signature of the CRL. Therefore the correct chain of issuers of all certificates up to the root needs to be verified.

5.2. Location / structure to store verification data

All verification data necessary for the verification of the time stamp have to be stored in a non-repudiation system as long as a later verification may be needed. As these verification data contain electronic signatures which algorithms may expire further renewals of these electronic signatures may be necessary.

This explicitly includes OCSP or CRL data and all certificates (including the complete chains for the used signatures.

6. Validation policy

To validate signatures, time stamps and evidence records it is useful for a validation authority to define and apply a verification policy. In this policy the verifier defines which algorithms are considered valid and secure in which time frames. A policy is defined in "Data Structure for Security Suitabilities of Cryptographic Algorithms" [LTANS-DSSC]

Basically the policy simply contains the algorithm identifier and the two dates valid from and expires. With this information the verifier can check that all algorithms have only been used at the time when they have been considered secure. Any deviation from this in the historic time line of an Evidence Record or a signature SHOULD lead to the failure of the verification.

Following examples should lead to a failure of the verification:

1. a signature of time stamp used an algorithm which has been secure at the time of application but is no longer considered secure (i.e. expired in the policy) and has not been protected by more secure time stamps in an applied ERS SHOULD fail to be verified

2. an ERS with a timestamp in the latest structure that is not considered secure SHOULD fail to verify.

3. Whenever in the structure of an ERS a later ArchiveTimestamp is applied after the algorithm in the timestamp of the preceding ArchiveTimeStamp is expired (as defined per policy) the verification MUST fail.

4. Whenever in the structure of an ERS a ArchiveTimeStampChain is applied after the hash algorithm of the preceding ArchiveTimeStampChain is no longer secure (as defined in the verification policy) the verification MUST fail.

7. Security Considerations

Long term availability and integrity of verification data

The verification data has to be stored and available including non-repudiation for all verification data.

8. References

8.1. Normative References

[ANSX995] American National Standard for Financial Services, "Trusted Timestamp Management and Security", ANSX X9.95-2005, June 2005.

[I180141] ISO/IEC JTC 1/SC 27, "Time stamping services - Part 1: Framework", ISO ISO-18014-1, February 2002.

[I180142] ISO/IEC JTC 1/SC 27, "Time stamping services - Part 2: Mechanisms producing independent tokens", ISO ISO-18014-2, December 2002.

[I180143] ISO/IEC JTC 1/SC 27, "Time stamping services - Part 3: Mechanisms producing linked tokens", ISO ISO-18014-3, February 2004.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", RFC 2026, 1996.

[RFC2119] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, 1997.

[RFC3126] Adams, C., Pinkas, D., Ross, J., and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC 3126, 2001.

[RFC3161] Adams, C., Cain, P., Pinkas, D., and R. Zuccherato, "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, August 2001.

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

8.2. Informative References

[ETSI2003]
European Telecommunication Standards Institute (ETSI), Electronic Signatures and Infrastructures (ESI);, "Algorithms and Parameters for Secure Electronic Signatures", ETSI SR 002 176 V1.1.1, March 2003.

[LTANS-DSSC]
IETF, "Data Structure for Security Suitabilities of Cryptographic Algorithms (DSSC)", October 2007.

[LTANS-ERS-SCVP]
IETF, "Using SCVP to Convey Long-term Evidence Records", November 2007.

[MER1980] Merkle, R., "Protocols for Public Key Cryptosystems, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA)", pages 122-134, April 1980.

[REQ2004] Wallace, C., Brandner, R., and U. Pordesch, "Long-term Archive Service Requirements", I-D ???, 2005.

Authors' Addresses

Tobias Gondrom
Munich
Germany

Email: tobias.gondrom@gondrom.org

Stefanie Fischer-Dieskau