Requirements for Certification Services
draft-ietf-ltans-notareqs-01.txt

Abstract

This document establishes the goals and requirements for protocols and data structures for use with services that provide additional means for users to ensure and prove the validity of data, especially digitally signed data, in a common and reproducible way. It
establishes the need for components to be used in addition to long-term archive services. It provides some use cases and scenarios, and establishes technical requirements for protocols and data structures to support them.

Table of Contents

1. Introduction .......................................................... 3
2. General Requirements ............................................... 3
3. Use cases .............................................................. 3
4. Specific workflows .................................................. 5
   4.1 Record transactions .............................................. 5
5. Technical Requirements ............................................... 6
6. Operational Considerations ......................................... 7
7. Security Considerations ............................................ 7
8. Acknowledgements ................................................... 7
9. Informative References ............................................. 7
    Authors’ Addresses .................................................. 7
A. Previous ‘Technical Requirements’ section ......................... 8
   A.1 Enable submission, retrieval and deletion ...................... 8
   A.2 Provide services ................................................. 9
   A.3 Support Demonstration of Service Integrity and Trust ....... 9
   A.4 Operation ....................................................... 9
   A.5 Data confidentiality ............................................ 10
Intellectual Property and Copyright Statements .................... 11
1. Introduction

[NOTE: This document contains comments by the editors, delimited in square brackets, primarily to note areas for subsequent discussion in the LTANS working group.]

In many scenarios, users need to be able to ensure and prove the existence and validity of documents and data, including digitally signed data, in a common and reproducible way, over a long period of time. A long-term archive service[1] may provide assurances about the integrity of data and past validity of digital signatures. However, additional mechanisms are required, in real workflows, to provide the technical means to satisfy user requirements.

Usually, these mechanisms involve a trusted third party who is willing, over a period of time, to accept data and validate it, or witness events, and subsequently make assertions about those events or data. In many legal jurisdictions, a ‘notary’ is a person with credentials, recognized by that jurisdiction to perform these services, in a way that gives their certification a special legal standing. Indeed, some types of transactions may require an official certification by someone with specific notary credentials.

This document establishes the goals and requirements for protocols and data structures for use with services that provide additional means for users to ensure and prove the validity of data, especially digitally signed data, in a common and reproducible way. It provides some use cases and scenarios, and establishes technical requirements for protocols and data structures to support them.

2. General Requirements

It is desirable that the protocols and data structures established be usable by an official notary to provide appropriate assertions for electronic documents. Of course, nothing in a technical document can provide for legal standing of any such assertions.

Requirements for data certification services may vary widely across different processes and jurisdictions. For this reason, the technical standards for data certification should provide a common base of mechanisms, useful across jurisdictions and work processes, and the means for extending these to support particular additional workflows.

3. Use cases

This section gives some examples workflows where data certification services and assertions by trusted third parties might be used, as a
way of motivating the subsequent requirements.

record transactions: In the case of an agreement between two (or more) parties, a trusted third party records the transaction, and the fact that all of the parties agreed to the final documents and that all of the necessary information has been provided to all of the involved parties. The trusted third party acts as a witness to the agreement at the time it is made, and, at a later date, may be called upon to attest to the validity of the agreement. This kind of service might be used for a contract between individuals, e.g., a private transfer of ownership of private property, or a public transfer of ownership of land.

negotiation support: In some cases, a trusted third party is used during the negotiation of a complex agreement in order to support the mechanisms of coming to the agreement. For example, a trusted third party might gather and store the documents during the course of a negotiation, making it impossible for any party to delete the document or repudiate a partial agreement; there might be time deadlines established for submitting information or approvals, or information may be held back from release until a particular time. For example, this kind of service might be used for the awarding of public contracts based on private bids.

certification of copies and conversions: In many cases, a trusted third party or service is used to certify the validity of a transformation or translation of a document from one form to another. Classically, a notary might attest to the validity of a paper copy of a document. The ability to attest to the validity of a wide variety of transformations are important, including the transformation of documents from one electronic format to another, or possibly the validity of conversion between paper and electronic forms. The third party should be able to attest that one document contains the same information as another and the validity of all contained digital signatures and the identity of the signers.

record events: In this case, a trusted third party or service is used to document and later provide proof that a certain event has happened. Initially, the service identifies the involved entities and verifies that all necessary preconditions are met. After this, an event or ceremony is held; during the event, the service ensures that all entities understood and received all appropriate information about the event and its consequences. After the event, a record of the event is issued to all of the entities; additional copies are retained for later documentation.

administering of oaths: In some cases, the ‘event’ being recorded is the performance, by an individual, of a particular agreement or ‘oath’. The trusted third party is used to document and later provide proof that an individual has made a particular statement or agreement, in a specified ceremony or event.
4. Specific workflows

This sections describes some concrete scenarios based on the use cases introduced in the previous section. [LMM: This section was added without working group discussion; please review. We’re expecting more than one of these.]

4.1 Record transactions

The following example will show the additional benefits of a certification service in the case of private transactions. We start with a basic protocol that achieves, upon completion, a state of mutual non-repudiation between two parties, A and B. Suppose, A wants to offer an electronic contract (contract_A) to B, where "contract_A" means that A has digitally signed the contract with her private key. This is sent as an offer to B:

contract_A -> B

B, after receiving and accepting contract_A, counter-signs the contract and sends it back to A as an acceptance of A’s offer:

(contract_A)_B -> A

Now, A has to confirm reception of the acceptance. He signs (contract_A)_B and sends it back to B:

((contract_A)_B)_A -> B

After that, both parties have a document with at least two signatures, and neither party can succeed in repudiating the validity of the contract.

Now let’s see what happens when we put a certification service N as a trusted third party between A and B. When B gets the contract from A and accepts it, he signs the contract and sends it to N:

(contract_A)_B -> N

The certification service confirms receipt of the contract with a signature and sends it to both A and B:

((contract_A)_B)_N -> A, B

After that, both parties have a document signed by A, B, and N. Since N is trusted, A and B can be sure that the other party has a contract which is signed by both. We have the same level of trust as in the scenario without the certification service. However, an additional benefit of using a certification service in this case can be the archiving of the contract, as may be required by the law for certain types of contracts.

In order to allow for N to provide documentation that all necessary
information has been provided to both parties, the scenario can be extended as follows:

When A and B get the confirmation \(((\text{contract}_A)_B)_N\) from N, both A and B send an acknowledgement to N:
ack_A \rightarrow N \text{ ack}_B \rightarrow N

After N received the two acknowledgements he sends a notification to both A and B that confirms that the transaction is completed:
not_N \rightarrow A, B

For both ack_A/B and not_N it suffices to contain (sufficiently secure) hash values of the pertaining original documents, and the same is true for the third message sent from the notary in the protocol above, but not for the second one, if the contract is to be archived by the notary.

The utility of notary services in these generic scenarios is twofold: They can accomplish the fulfillment of technical requirements, e.g., archiving of transaction records, which may in turn be entailed by legal requirements. And they can be instrumental in the fulfillment of genuine legal requirements, like documentation that all necessary information has been provided to all involved parties.

5. Technical Requirements

This section describes some of technical requirements associated with certification services. [LMM: Note that currently the previous contents of ‘technical requirements’ have been moved to Appendix A].

The primary technical requirement is for a data structure that can represent the assertion, by the certification service, that a particular service has been performed. The data structure should include the identity (as known) of the participants, the credentials of the certification service and its operator, the date and time that the service was performed, and other information relevant to the acknowledgement of the service. The data structure should be signed by the certification service.

Secondarily, there should be protocols for requesting services, monitoring the progress of the service, participating in services that require contemporaneous participation, cancelling ongoing services.

Some services also require the certification service to maintain a long-term archive of records of events that it has certified; the users of a certification service may request operations that cause archived certificates to be accessed, forwarded, or possibly even
6. Operational Considerations

A certification service must be able to work efficiently even for large amounts of data objects and requests.

In order to limit expenses and to achieve high performance, the involvement of other trusted third parties should be minimized.

7. Security Considerations

[LM: This section should contain a threat analysis for certification services, and the ways in which those threats can be guarded against.] Trust is the principal asset of a certification service. The implementation of such a service must be very careful so that no data integrity can be lost or manipulation of the system can be done.

8. Acknowledgements

Thanks to members of the LTANS mailing list for review of earlier drafts and many suggestions.

9 Informative References

Appendix A. Previous ‘Technical Requirements’ section

[LMM: For the record, this was the previous content of ‘technical requirements’; it’s been temporarily moved to the appendix, while the working group figures out the requirements based on the use cases above.]

This section describes a (technical) system delivering notary services. Possible services MUST support at least one use case completely but NEED NOT support all possible use cases for notary systems and services. This way one can have a self-contained system for each separate task.

A.1 Enable submission, retrieval and deletion

A notary service must permit entities to perform the following basic operations:
- submit data
- retrieve data
- delete data (if the notary services is authorised to allow deletion at a given point in time)

Users must be able to request a specific service they want to access, and receive an attestation (possibly a digitally signed document) after the completion of the service. The format for the acknowledgements must allow the identification of the notary service provider; in specific cases also the identity of the individual human notary. The acknowledgement of a successful execution of the notary
service should permit the submitter to verify that the correct data was received by the service and the correct kind of service was executed.

All requests to a notary service MUST be authenticated.

Following submission, the service must start a workflow to enable the human notary to fulfill and supervise its work. If supervision or a response within a given timeframe is not possible the service must report an error to the user.

After submission and before completion of the service the user SHOULD always be able to receive information about the status of the process. The access to the status information MUST only be accessible to authorised entities.

Deletion requests also MUST be authorised and additionally there MUST be a kind of authorisation policy which controls that the notary service does not delete information that must be kept.

It must be possible to authenticate requests and responses. This may be accomplished using transport security mechanisms.

A.2 Provide services

All services must be well documented and the notary service MUST create reports whose authenticity can be verified by an initial client and any other interested authorised party, for a long time after the creation of the report.

Depending on the kind of service online interaction between the participants MUST be possible.

A.3 Support Demonstration of Service Integrity and Trust

A notary service MUST be able to demonstrate that the clients and users can trust it. For this evaluation records by other trusted parties (e.g. government authorities), the identity of members of the notary office and further documentation MUST be easily accessible to the client. For every user and client it MUST be obvious if systems have been tampered with or manipulated.

A.4 Operation

The operation of the notary service must be under the complete and unconditional control of the notary office. It MUST be impossible to manipulate the system without the human notaries from the office noticing it.
A.5 Data confidentiality

The notary service MUST allow to respect the confidentiality requirement of a particular procedure to be executed.

If information is deployed on systems outside the direct supervision of the notary office it is MANDATORY to encrypt the information with maximum security. If encryption becomes weak due to improvements in cryptography, the notary office has to be informed and all information has to be re-encrypted with better algorithms.

All communications with a notary service MUST be encrypted. (e.g. SSL) Traditional standardized encrypting methods and formats, e.g. CMS, should be supported.
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 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 Internet Society (2004). 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.