Notary Services requirements
draft-ietf-ltans-notareqs-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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.

This Internet-Draft will expire on January 12, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

Notary services are available today in a wide variety for paper based processes and documents. To define the needs, requirements and future world for notary services in the electronic world, this document describes use cases and scenarios as base for further discussion and work of the LTANS WG in this area.
Table of Contents

1. Introduction ................................................. 3
2. Terminology .................................................. 5
3. Use cases ..................................................... 6
4. Technical Requirements ....................................... 7
5. Operational Considerations ................................. 12
6. Security Considerations ....................................... 13
7. Acknowledgements ............................................ 14
8. References ..................................................... 14
   Authors’ Addresses .............................................. 14
   Intellectual Property and Copyright Statements ............. 17
1. Introduction

The office of notary dates back to the Roman Empire. Since about 2000 years trustworthy persons act as notaries to approve that they have witnessed something.
A Notary in common law jurisdictions is a qualified lawyer.
The office of a notary is always commissioned by the state.
Traditionally, notaries recorded matters of judicial importance as well as private transactions or events where an officially authenticated record or a document drawn up with professional skill or knowledge was required. Specifically, the functions of notaries include the attestation of documents and certification of their due execution, administering of oaths, witnessing affidavits and statutory declarations, certification of copy documents, noting and protesting of bills of exchange and the preparation of ships’ protests.

Significant weight attaches to documents certified by notaries. Documents certified by notaries are sealed with the notary’s seal and are recorded by the notary in a register maintained by him/her. These are known as "notarial acts". Notarial acts and certificates are recognised by some countries without the need for any further certification from the respective Foreign Ministry or foreign diplomatic missions. (In countries subscribing to the Hague Convention Abolishing the Requirement for Legalisation for Foreign Public Documents only one further act of certification is required, known as an apostille). (source: wikipedia.org)

A notary service should support and enable a human notary to fulfill his tasks with electronic documents as well as he already does with paper based documents and processes.

Notary services might be located at a government facility, at the office of a civil notary or a lawyer or other places that are honored by the trust of the public.

In the the different countries the characteristics of a trusted notary and their "notarial acts" can vary widely so a computer based notary service has to meet their individual concerns and requirements.

Examples of notary service usage by submitters include:

- an entity (person or company) wants a notary to function as a witness for the existence of a document or the closing of a contract
- entities need a trusted third party to gather and store documents, making it impossible for them to delete the document, or taking care, that some information has to be submitted by a sender until a certain time and also guaranteeing that the recipient doesn't receive the document before a giving time. (an important requirement for awarding contracts by public authorities)
- format transformations
  Classically, virtually the only "format conversion" exerted by notaries is the exemplification of attested copies of documents. Besides this paper-to-paper transformation, with electronic documents three other format changes become possible: paper-to-electronic, electronic-to-paper, and most importantly electronic-to-electronic format transformations.
- verification and testation of the legal validity of signed documents
- ...

In parallels to the document "Long term archive service requirements" draft-ietf-ltans-reqs-01.txt, which aims to identify the technical requirements for a long-term archive service, this document tries to identify possible use cases and technical requirements for notary services.
2. Terminology

Notary: a person or institution which is trusted by the public and other involved parties.

Seal: The sign of a notary set to certify a notarial act.

User: Person or institution that needs the service of a notary or other trusted third party.

Notary service: electronic service that supports a human notary to provide his/her services on electronic based processes and documents. An electronic notary service cannot function without the trust earned by the human behind it and the fact that the human notary has absolute control over the machine.
3. Use cases

3.1 record transactions:
The notary service has to record private transactions, e.g. transactions of ownership. Additionally to the recording it MUST be able to guarantee and provide documentation that all necessary information has been provided to all involved parties.

3.2. record events:
The notary service has to document and proof that a certain event has happened. At first the service has to identify the involved entities and verify that all necessary preconditions are met. After this the event or ceremony can be held. During which the notary service has to ensure that all entities understood and received the whole information and consequences of the event. After the event an officially authenticated record has to be issued to all entities and one copy kept for later documentation. (events might be e.g. marriage, Å )

3.3. certification of copy documents
The notary service must 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. With this the transformation of one document format into another can be achieved.

3.4. administering of oaths
One Service can be that the administering of oaths can in the future be documented electronically instead of applying the seal of a notary on a piece of paper. E.g. the client can visit the office of a notary (maybe even only virtually), take an oath and the notary can record that with an electronic document, like a digital signed document.

3.5. attestation and certification of documents and events
The notary can attest and certify the correctness and existence of a document and all contained signatures as the notary service took part in the creation and signing of the document and by this ensured the integrity of the environment for all participants.
4. Technical Requirements

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.

4.1 Enable submission, retrieval and deletion

4.1.1 Functional Requirements

A notary service must permit entities to perform the following basic operations:

- submit data
- retrieve data,
- delete data (if the notary service 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 their 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.
4.2 Provide services

4.2.1 Functional Requirements

All services must be well documented and the notary service MUST create reports whose authenticicity 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.

4.3 Support Demonstration of Service Integrity and Trust

4.3.1 Functional Requirements

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 MUST be obvious if systems are tempered or manipulated.

4.4 Operation

4.4.1 Functional Requirements

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.

4.5 Data confidentiality

4.5.1 Functional Requirements

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 encrypted with better algorithms again.

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

A notary 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.

6. Security Considerations

Trust is the principal asset of a notary service. Concerning that 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.
7. Acknowledgements

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

Authors’ Addresses

Tobias Gondrom
IXOS Software AG
Bretonischer Ring 12
85630 Grasbrunn / Munich
Germany

Fax: +49 (89) 4629-33-1816
eMail: tobias.gondrom@ixos.de
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgment

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