This document describes those features of a service which processes signed documents which must be present in order for that service to constitute a "technical non-repudiation" service. A technical non-repudiation service must permit an independent verifier to determine whether a given signature was applied to a given data object by the private key associated with a given valid certificate, at a time later than the signature. The features of a technical non-repudiation service are expected to be necessary for a full non-repudiation service, although they may not be sufficient.

This document is intended to clarify the definition of the "non-repudiation" service in RFC 2459. It should thus serve as a guide to when the nonRepudiation bit of the keyUsage extension should be used and to when a Certificate Authority is required to archive CRL’s.
RFC 2459 [1] specifies a bit within the KeyUsage extension called the nonRepudiation bit which is "asserted when the subject public key is used to verify digital signatures used to provide a non-repudiation service which protects against the signing entity falsely denying some action, excluding certificate or CRL signing." Extensive discussions in the PKIX WG have revealed that the description of the non-repudiation service contained in this passage is not widely enough understood or agreed upon to characterize any given service as providing or not providing a non-repudiation service. Two major categories of service have been proposed as potentially providing a non-repudiation service: the technical non-repudiation service, which this draft attempts to define with greater precision, and a full non-repudiation service which is intended to prevent all possible repudiations of a signed object or document. Since a full non-repudiation service is required to meet all the requirements of this technical non-repudiation service as a prerequisite, the technical non-repudiation service’s definition is necessary for both.

1.1 Definitions

Signing Certificate: A certificate containing the key pair whose private key was used to create the signature being verified.

Signer: The party who created the signature being verified. It is outside the scope of these requirements to distinguish between the actual signer and the holder of the signing certificate.

Relying Party: The party who received the signature being verified, and initially verified it.

Verifier: An entity independent of both the signer and the relying party who is verifying that the supplied signature, data object, and certificate are consistent with each other.

1-way NR: A service in which the relying party preserves sufficient evidence to permit the verifier to perform a verification, and may submit it for verification by his or her own action.

2-way NR: A service in which the relying party submits sufficient evidence to permit the verifier to perform a verification o a third party, known as the "escrow holder".

Escrow holder: The party responsible for preserving signature evidence in 2-way NR. The escrow holder may also be, but need not be, the verifier.

Escrow package: The data submitted from the relying party to the escrow holder, in 2-way NR. The escrow holder may add certain auditing and tracking information to this package before storage.

NR service: The technical nonRepudiation service referenced above.

keyUsage extension: A standard extension within X.509v3 certificates with object identifier { 2 5 29 15 }, consisting of a series of enumerated bits.

NR bit: The nonRepudiation bit (offset 1) of the keyUsage extension.
1.2 Scope and caveats

The NR service is expected to provide evidence that a given object was signed by the private key corresponding to a given certificate which was valid at the time of signature. It is not anticipated that the use of the NR service will ordinarily constitute execution of a contract, or acceptance of any other legal obligation. It is anticipated that the use of this service in accepting legal obligations will be the subject of legislation or judicial decision in various jurisdictions, which are likely to lay additional technical burdens upon the provision of such a service to such an extent as to constitute another, larger service which need not be the same in all jurisdictions. It is outside the scope of the definition of this service to provide evidence that the signer and the holder of the signing certificate are the same, that the signer has been adequately informed of the content which is signed, that the signer is not acting under duress, etc.

2 Requirements for both 1-way and 2-way NR

2.1 The signer must submit, with the signature, the signing certificate or an unambiguous identifier of that certificate. Unambiguous identifiers of certificates include the combination of a certificate serial number with an issuer name.

2.2 The signer must submit, with the signature, the content being signed or an unambiguous reference to that content. It is explicitly contemplated that a URI constitutes an unambiguous reference to its content.

2.3 The signer must include, in the base over which the signature is calculated, the time at which the signature was created.

2.4 The relying party must, before accepting the signature, verify that the signing certificate is valid. This verification should include a CRL check.

2.5 The relying party must, before accepting the signature, verify the signature of the data object being submitted.

3 Requirements for 1-way NR

3.1 The relying party must save a copy of the content being signed.

3.2 The relying party must save the identity of the signing certificate, along with the content of the signature.

3.3 The relying party must check that the signing certificate contains a keyUsage extension. If the extension is not present or does not contain the nonRepudiation bit, and the version of the certificate is v3 or higher, the submission must be rejected.

4 Requirements for 2-way NR

4.1 The relying party must submit to the escrow holder a copy of the content being signed, the identity of the signing certificate, and the signature.

4.2 The relying party must sign the submission to the escrow holder. The relying party SHOULD include, in the base over which that signature is calculated, the current time. This time will be between the time
when the signer submitted the signature and the time when the package is submitted. The signed object submitted is known as the escrow package.

4.3 The relying party must check whether or not the signing certificate contains a keyUsage extension. If the keyUsage extension is present and the nonRepudiation bit is not set the submission must be rejected.

5 Copyright

Copyright (C) The Internet Society (date). 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 assigns.

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.

6 References

[2] X.509(97)

7 Author’s Address

Thomas Gindin
IBM Corporation
800 North Frederick Ave.
Gaithersburg, MD 20879
USA

Email: tgindin@us.ibm.com

Internet-Draft  Technical Requirements for a non-Repudiation Service Expires: 28 February 2000