1. Abstract

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 set and to when a Certificate Authority is required to archive CRL’s.

2. Introduction

RFC 2459 [2] 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

Gindin Informational - November 2000

Technical Requirements for a non-Repudiation Service Nov. 2000

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.

2.1 Definitions

Signing Certificate: A certificate containing the public key component of a 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 subject 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. This service is not expected to be extended in such a way that it may be used as a basis for legal agreements.

2-way NR: A service in which the relying party submits sufficient evidence to permit the verifier to perform a verification to a third party, known as the "escrow holder". Either the relying party or the signer may request that this data be submitted for verification. Future extensions of this service would be necessary to permit it to serve as a basis for legal agreements.

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.


NR bit: The nonRepudiation bit (offset 1) of the keyUsage extension.

2.2 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 any use of this service in accepting legal obligations would 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 subject 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.

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 [4].

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

3.1 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 and the combination of issuer name, subject name, and subject key identifier.

3.2 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.

3.3 The signer MUST include, in the base over which the signature is calculated, the time at which the signature was created. There is no obligation that this time be verified with an independent authority.

3.4 The signer MUST include, in the base over which the signature is calculated, the content being signed or the message digest of that content. This object therefore includes all those fields which are both mandatory and variable on a per-object basis within a Non-
repudiation of origin token using asymmetric keys according to ISO 13888[5].

3.5 The relying party MUST, before accepting the signature, verify that the signing certificate is valid. This verification SHOULD include a CRL check or other online certificate verification using such mechanisms as OCSP[6] or SCVP.

3.6 The relying party MUST, before accepting the signature, verify the signature of the data object being submitted.

3.7 The validity of the signer’s certificate is considered to have been finally judged once a validation has been performed in which the effective time of the certificate status is no earlier than the later of the signing time and the relying party’s time. There is no need to check for a later revocation with an invalidityDate CRL Entry extension prior to the signature, because that extension’s value is purely advisory and not validated by anyone other than the certificate subject. In the case where a certificate status is derived from a CRL, the effective time of the certificate status is the value of the "thisUpdate" field of the CRL. In the case where a certificate status is represented by a basic OCSP response, the effective time of the certificate status is the value of the "thisUpdate" field of the status for that certificate.

4. Requirements for 1-way NR

4.1 The relying party MUST save a copy of the content being signed.

4.2 The relying party MUST save the identity of the signing certificate, along with the signature itself and any signature attributes. If the relying party has verified the certificate using a server supporting a "signed-status-response" protocol such as OCSP or SCVP, the relying party MUST store the status responses with the data submitted. If the relying party has verified the certificate using a CRL, the relying party MAY store that CRL with the data submitted. The relying party MAY also include the chain of issuer certificates back to his (or her) trusted root.

4.3 The relying party MUST check that the signing certificate contains a keyUsage extension and an extendedKeyUsage extension. If the keyUsage extension is not present or does not contain the nonRepudiation bit, unless the extendedKeyUsage extension is present and contains a specific key purpose involving non-repudiation or the version of the certificate is lower than v3, the submission MUST be rejected.

4.4 The relying party SHOULD create, and save with the data submitted by the signer, a package containing a current time stamp signed by an independent authority, which may be a Time Stamp Authority. This package signed by the independent authority SHOULD include the time stamp, the identity of the signing certificate, and at least one of the following: a countersignature created by the
relying party, a copy of the "signature block" of the submitted
document, or the entire submitted document.

4.5 The relying party MAY return a receipt to the signer. This
receipt, if it exists, SHOULD contain the package time stamped and
signed by an independent authority referred to in the preceding
subsection. The relying party SHOULD sign the receipt and include
both the current time and an unambiguous identifier of his (or her)
signing certificate or that certificate itself. The relying party
MAY include an identifier specifying the non-repudiation policy which
is being followed during this transaction. This receipt therefore
includes all those fields which are both mandatory and variable on a
per-object basis within a Non-repudiation of delivery token using
asymmetric keys according to ISO 13888[7].

4.6 The relying party SHOULD, at various fixed intervals (not
herein defined) after the acceptance of the package, perform
certificate verifications for the purpose of finding a revocation of
the signing certificate, especially one having a revocation date
which is no earlier than the later of the originator’s time (see
section 3.3) and the independent authority’s time (see section 4.4).
If such a revocation is found evidence of the revocation MUST be
preserved with the package. Such evidence SHOULD be in the form of a
CRL or a signed response from a certificate verification service.
Once a CRL is found with an effective time no earlier than the later
of the relevant times above, the status is final and the CRL MUST be
preserved with the package. Once a status response is found with an
effective time no earlier than the later of the relevant times above,
the status is final and the status response MUST be preserved with
the package.

4.7 If either the issuer of the submitter’s certificate or the
third party which signed the package in 4.4 ceases operation and the
public key which they used can no longer be obtained from a source
independent of the relying party, the transaction is considered to be
unverifiable. If one or more of them cease operation, but their
public keys can still be obtained from independent sources, the
transaction does not become unverifiable. If the key of the
independent third party is compromised, the transaction becomes
unverifiable.

5. Requirements for 2-way NR

5.1 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. If the relying party has verified the certificate
using a server supporting a "signed-status-response" protocol such as
OCSP or SCVP, the relying party MUST include the status responses in
the escrow package. If the relying party has verified the
certificate using a CRL, the relying party MAY include that CRL in
the escrow package. The relying party SHOULD also include the chain
of issuer certificates back to his (or her) trusted root.

5.2 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 and the identity of the signing certificate. 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.

5.3 The relying party MUST check whether or not the signing certificate contains a keyUsage extension and an extendedKeyUsage extension. If the keyUsage extension is present and the nonRepudiation bit is not set, unless the extendedKeyUsage extension contains a specific key purpose involving non-repudiation the submission MUST be rejected. Larger services extending this one MAY dispense from this requirement by explicit statements in their service definition.

5.4 The relying party MAY return a receipt to the signer. This receipt, if it exists, SHOULD contain the "signature block" of the escrow package. The relying party MAY include an identifier specifying the non-repudiation policy which is being followed during this transaction. This receipt therefore includes all those fields which are both mandatory and variable on a per-object basis within a Non-repudiation of delivery token using asymmetric keys according to ISO 13888[8].

5.5 The escrow holder SHOULD, at various fixed intervals (not herein defined) after the acceptance of the package, perform certificate verifications for the purpose of finding a revocation of the signing certificate, especially one having a revocation date which is no earlier than the later of the originator’s time (see section 3.3) and the time at which the escrow holder received the escrow package(see section 5.2). If such a revocation is found, the relying party SHOULD be informed, and evidence of the revocation MUST be preserved with the escrow package. Such evidence SHOULD be in the form of a CRL or a signed response from a certificate verification service. Once a CRL is found with an effective time no earlier than the later of the relevant times above, the status is final and the CRL MUST be preserved with the package. Once a status response is found with an effective time no earlier than the later of the relevant times above, the status is final and the status response MUST be preserved with the package.

6. Security Considerations

Most of this memo deals with security mechanisms. All messages exchanged between identified parties consist mainly of signed components.

7. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.
8. Acknowledgments

I would like to thank Tony Bartoletti, Ed Gerck, Steve Kent, Aram Perez, Andreas Schmidt, and John Wray for their many suggestions for revisions to earlier versions of this document.

9. Author’s Addresses

Thomas Gindin
IBM Corporation
6710 Rockledge Drive
Bethesda, MD 20817

Gindin      Informational - November 2000                   6

Technical Requirements for a non-Repudiation Service Nov. 2000

USA
Email: tgindin@us.ibm.com

Full Copyright Statement

"Copyright (C) The Internet Society (2000). 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."