INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.813

(10/96)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

Security

Information technology – Open Systems Interconnection – Security frameworks in open systems: Non-repudiation framework

ITU-T Recommendation X.813

(Previously "CCITT Recommendation")

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

PUBLIC DATA NETWORKS	X.1-X.199
Services and facilities	X.1-X.19
Interfaces	X.20-X.49
Transmission, signalling and switching	X.50-X.89
Network aspects	X.90-X.149
Maintenance	X.150-X.179
Administrative arrangements	X.180-X.199
OPEN SYSTEM INTERCONNECTION	X.200-X.299
Model and notation	X.200-X.209
Service definitions	X.210-X.219
Connection-mode protocol specifications	X.220-X.229
Connectionless-mode protocol specification	X.230-X.239
PICS proformas	X.240-X.259
Protocol Identification	X.260-X.269
Security Protocols	X.270-X.279
Layer Managed Objects	X.280-X.289
Conformance testing	X.290-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
General	X.300-X.349
Satellite data transmission systems	X.350-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
Networking	X.600-X.629
Efficiency	X.630-X.649
Naming, Addressing and Registration	X.650-X.679
Abstract Syntax Notation One (ASN.1)	X.680-X.699
OSI MANAGEMENT	X.700-X.799
Systems Management framework and architecture	X.700-X.709
Management Communication Service and Protocol	X.710-X.719
Structure of Management Information	X.720-X.729
Management functions	X.730-X.799
SECURITY	**X.800-X.849**
OSI APPLICATIONS	X.850-X.899
Commitment, Concurrency and Recovery	X.850-X.859
Transaction processing	X.860-X.879
Remote operations	X.880-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999

For further details, please refer to ITU-T List of Recommendations.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. Some 179 member countries, 84 telecom operating entities, 145 scientific and industrial organizations and 38 international organizations participate in ITU-T which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the Members of ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, 1993). In addition, the World Telecommunication Standardization Conference (WTSC), which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of ITU-T Recommendation X.813 was approved on 5th of October 1996. The identical text is also published as ISO/IEC International Standard 10181-4.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

CONTENTS

Summary

This Recommendation | International Standard defines a general framework for the provision of non-repudiation services. The goal of the Non-repudiation service is to collect, maintain, make available, and validate irrefutable evidence regarding identification of originators and recipients involved in data transfers.

Introduction

The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. The Non-repudiation service can be applied in a number of different contexts and situations. The service can apply to the generation of data, the storage of data, or the transmission of data. Non-repudiation involves the generation of evidence that can be used to prove that some kind of event or action has taken place, so that this event or action cannot be repudiated later.

In an OSI environment (see CCITT Rec. X.800 and ISO 7498-2) the Non-repudiation service has two forms:

– Non-repudiation with proof of origin which is used to counter false denial by a sender that the data or its contents has been sent.

– Non-repudiation with proof of delivery which is used to counter false denial by a recipient that the data or its contents (i.e. the information that the data represents) has been received.

Applications which make use of OSI protocols may require other forms of the Non-repudiation service which are specific to particular classes of applications. For example, MHS (ITU-T Rec. X.402 | ISO 10021-2) defines the Non-repudiation of submission service, while the EDI Messaging System (see Recommendation X.435) defines the Non-repudiation of retrieval and Non-repudiation of transfer services.

The concepts in this framework are not limited to OSI communications but may be interpreted more broadly to include such uses as creation and storage of data for later use.

This Recommendation | International Standard defines a general framework for the provision of a Non-repudiation service.

This framework:

– expands upon the concepts of Non-repudiation services described in CCITT Rec. X.800 and ISO 7498-2 and describes how they may be applied to Open Systems;

– describes alternatives for the provision of these services; and

– explains the relationship of these services to other security services.

Non-repudiation services may require:

– adjudicators who will arbitrate disputes that may arise as a result of repudiated events or actions; and

– Trusted Third Parties who will assure the authenticity and integrity of the data to be used for the verification of evidence.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS IN OPEN SYSTEMS: NON-REPUDIATION FRAMEWORK

1 Scope

This Recommendation | International Standard addresses the application of security services in an Open Systems environment, where the term "Open Systems" is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) which are used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

This Recommendation | International Standard:

– defines the basic concepts of Non-repudiation;

– defines general Non-repudiation services;

– identifies possible mechanisms to provide the Non-repudiation services;

– identifies general management requirements for Non-repudiation services and mechanisms.

As with other security services, Non-repudiation can only be provided within the context of a defined security policy for a particular application. The definitions of security policies are outside the scope of this Recommendation | International Standard.

The scope of this Recommendation | International Standard does not include specification of details of the protocol exchanges which need to be performed in order to achieve Non-repudiation.

This Recommendation | International Standard does not describe in detail the particular mechanisms that can be used to support the Non-repudiation services nor does it give details of the supporting security management services and protocols.

Some of the procedures described in this framework achieve security by the application of cryptographic techniques. This framework is not dependent on the use of a particular cryptographic or other algorithm or on particular cryptographic techniques (i.e. symmetric or asymmetric) although certain classes of Non-repudiation mechanisms may depend on particular algorithm properties. Indeed it is likely, in practice, that a number of different algorithms will be used. Two entities wishing to use cryptographically-protected data must support the same cryptographic algorithm.

[| NOTE – Although ISO does not standardize cryptographic algorithms, it does standardize the procedures used to register them in ISO/IEC 9979.]

A number of different types of standard can use this framework including:

1) standards that incorporate the concept of Non-repudiation;

2) standards that specify abstract services that include Non-repudiation;

3) standards that specify uses of a Non-repudiation service;

4) standards that specify the means of providing Non-repudiation within an open system architecture; and

5) standards that specify Non-repudiation mechanisms.

Such standards can use this framework as follows:

- standards of type 1), 2), 3), 4) or 5) can use the terminology of this framework;
- standards of type 2), 3), 4) or 5) can use the facilities defined in clause 7; and
- standards of type 5) can be based upon the classes of mechanism defined in clause 8.

2 Normative references

The following Recommendations and International Standards contain provisions, which through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*
- ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

3 Definitions

3.1 Basic Reference Model definitions

This Recommendation | International Standard builds on concepts developed in ITU-T Rec. X.200 | ISO/IEC 7498-1 and makes use of the following term defined in it:

(N)-entity.

3.2 Security Architecture definitions

This Recommendation | International Standard builds on the concepts developed in CCITT Rec. X.800 and ISO 7498-2 and makes use of the following terms defined in it:

- access control;
- audit (also security audit);
- authentication;
- channel;
- cryptographic checkvalue;
- cryptography;
- data integrity (also integrity);
- data origin authentication;
- decipherment;

- digital signature (also signature);
- encipherment;
- key;
- key management;
- notarization;
- repudiation;
- security audit trail (also audit trail, log);
- threat.

3.3 Security Frameworks Overview definitions

This Recommendation | International Standard builds on the concepts developed in ITU-T Rec. X.810 | ISO/IEC 10181-1 and makes use of the following terms defined in it:

- certification authority;
- digital fingerprint;
- hash function;
- one-way function;
- private key;
- public key;
- revocation list certificate;
- seal;
- sealed;
- secret key;
- security certificate;
- security domain;
- security token;
- trusted third party.

3.4 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.4.1 **compromised evidence**: Evidence that was, at one time, satisfactory but which no longer has the confidence of the Trusted Third Party or adjudicator.

3.4.2 **counter-signature**: A digital signature appended to a data unit which has already been signed by a different entity (e.g. a TTP).

3.4.3 **evidence**: Information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute.

3.4.4 **evidence generator**: An entity that produces Non-repudiation evidence.

NOTE – This entity may be the Non-repudiation service requester, the originator, the recipient or multiple parties working in conjunction (e.g. a signer and co-signer).

3.4.5 **evidence subject**: The entity whose involvement in an event or action is established by evidence.

3.4.6 **evidence user**: An entity that uses Non-repudiation evidence.

3.4.7 **evidence verifier**: An entity that verifies Non-repudiation evidence.

3.4.8 **message authentication code**: A cryptographic checkvalue that is used to provide data origin authentication and data integrity.

3.4.9 Non-repudiation service requester: An entity that requests that Non-repudiation evidence be generated for a particular event or action.

3.4.10 notary: A Trusted Third Party with whom data is registered so that later assurance of the accuracy of the characteristics of the data can be provided.

3.4.11 originator: In the context of data transfer, an entity that originates the data in an action that is subject to a Non-repudiation service.

3.4.12 recipient: In the context of data transfer, an entity that receives the data in an action that is subject to a Non-repudiation service.

NOTE – In the logical model of Non-repudiation, other entities may be considered. E.g. the owner is the entity that makes an original message and a transfer agent is the entity that transfers the message; in this context, entities are modeled as originators or recipients.

4 Abbreviations

OSI	Open Systems Interconnection
CA	Certification Authority
TTP	Trusted Third Party
MAC	Message Authentication Code

5 General discussion of Non-repudiation

5.1 Basic concepts of Non-repudiation

The Non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Disputes cannot be resolved unless the evidence has been previously recorded.

The purpose of the Non-repudiation service described in this framework is to provide evidence about a particular event or action. Non-repudiation services may be requested by entities other than those involved in the event or action. Examples of actions which may be protected with a Non-repudiation service are:

- sending an X.400 message;
- inserting a record in a database; and
- invoking a remote operation.

When messages are involved, to provide proof of origin, the identity of the originator and the integrity of the data must be confirmed. To provide proof of delivery, the identity of the recipient, and the integrity of the data must be confirmed. In some cases, evidence concerning the context (e.g. date, time, location of the originator/recipient) may also be required.

The service provides the following facilities which can be used in the event of an attempted repudiation:

- generation of evidence;
- recording of evidence;
- verification of generated evidence;
- retrieval and re-verification of the evidence.

Disputes may be settled between parties directly through inspection of the evidence. However, a dispute may have to be resolved by an adjudicator who evaluates the evidence and determines whether or not the disputed action or event occurred. Adjudication can only be provided effectively if the parties to the dispute accept the authority of the adjudicator. For the evidence provided to be accepted by the adjudicator, it must usually be assured by one or more Trusted Third Parties. The adjudicator can optionally be the Trusted Third Party that assures the evidence. Non-repudiation mechanisms use a number of types of Trusted Third Parties and forms of evidence.

5.2 Roles of a Trusted Third Party

One or more Trusted Third Parties may be involved in the Non-repudiation service.

Trusted Third Parties which support Non-repudiation without being actively involved in each use of the service are known as Off-line Trusted Third Parties. A TTP which is actively involved in the generation or verification of evidence is known as an On-line TTP. An On-line TTP which acts as an intermediary in all interactions is known as an In-line TTP.

A Trusted Third Party may be required to record and/or gather evidence as well as being required to vouch for the validity of the evidence. There may be a number of Trusted Third Parties involved acting in various roles (e.g. Notary, Time Stamping, Monitoring, Key Certification, Signature Generation, Signature Verification, and Delivery Authority roles). A single Trusted Third Party may act in one or more of these roles.

In an Evidence Generation role, a TTP cooperates with a Non-repudiation service requester to generate evidence.

In an Evidence Recording role, a TTP records evidence that can later be retrieved by an evidence user or an adjudicator.

In a Time Stamping role, a TTP is trusted to provide evidence which includes the time when the time stamping request was received.

In a Monitoring role, a TTP monitors the action or the event and is trusted to provide evidence about what was monitored.

In a Key Certification role, a TTP provides Non-repudiation certificates related to an evidence generator in order to assure the validity of a public key to be used for Non-repudiation purposes.

In a Key Distribution role, a TTP provides keys to the evidence generators and/or the evidence verifiers. It may also place constraints on the use of the keys, in particular when symmetrical techniques are used.

In a Signature Generation role, a TTP is trusted to provide evidence in the form of a digital signature on behalf of the evidence subject.

In an Evidence Verification role, a TTP verifies evidence at the request of an entity.

In a Signature Verification role, a TTP is trusted by the evidence user to verify evidence in the form of a digital signature.

NOTE – The Signature Generation role is a particular case of the Evidence Generation role. The Signature verification role is a particular case of the evidence verification role.

In a Notary role, a TTP provides assurance about the properties of the data (such as its integrity, origin, time or destination) that are communicated between two or more entities and that have been previously registered with the TTP.

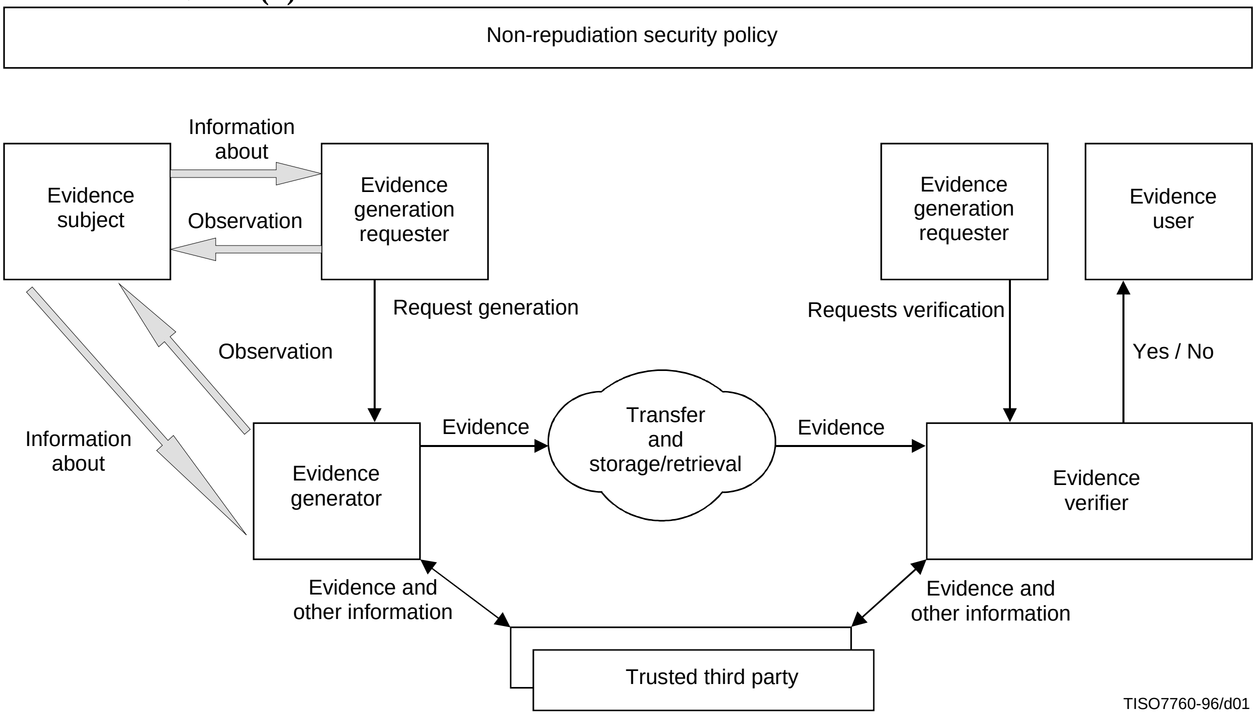
In a Delivery Authority role, a TTP interacts with the intended recipient of data and attempts to release the data to the recipient. It then provides evidence that the data was delivered, that the data was not delivered, or that delivery was attempted but that no confirmation of receipt was received. In the last case, the evidence user cannot determine whether the data was received by the intended recipient or not.

5.3 Phases of Non-repudiation

Non-repudiation is composed of four distinct phases:

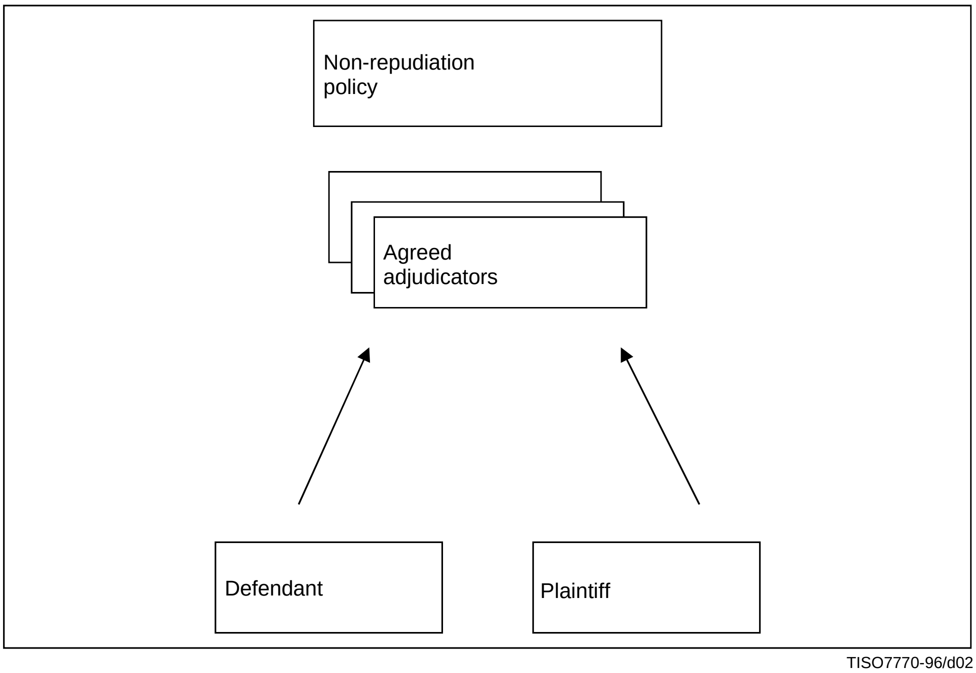
- evidence generation;
- evidence transfer, storage and retrieval;
- evidence verification; and
- dispute resolution.

Figure 1 illustrates the first three phases; Figure 2 illustrates the fourth phase.



NOTE – This figure is illustrative, not definitive.

Figure 1 – Entities involved in the generation, transfer, storage/retrieval and verification phases



NOTE – This figure is illustrative, not definitive.

Figure 2 – Dispute Resolution phase of a Non-repudiation process

5.3.1 Evidence Generation

In this phase, the Evidence Generation Requestor requests the Evidence Generator to generate evidence for an event or action. An entity whose involvement in the event or action is established by the evidence is known as an Evidence Subject. Different groupings of these entities are possible: an Evidence Subject and an Evidence Generator may be the same entity as may the Evidence Subject, the Evidence Generation Requestor and the Evidence Generator; the Evidence Generation Requestor and the Trusted Third Party; the Evidence Generator and Trusted Third party; and the Evidence Generation Requestor, the Evidence Generator and Trusted Third party. Depending on the type of Non-repudiation service, the evidence may be generated by the evidence subject, perhaps in conjunction with the services of a Trusted Third Party, or by a Trusted Third Party alone.

NOTE – Depending on the context of the Non-repudiation service, relevant evidence will typically include the identities of the entities involved, the data, and the time and date. Additional information such as mode of transfer (e.g. OSI communication; database storage and retrieval); location of entities involved; distinguishing identifier; and the “owner”/creator of the data, could also be included.

5.3.2 Evidence Transfer, Storage and Retrieval

During this phase, evidence is transferred between entities or to or from storage (see Figure 1).

5.3.3 Evidence Verification

In this phase, the evidence is verified by an evidence verifier at the request of an evidence user. The purpose of this phase is for an evidence user to gain confidence that the supplied evidence will indeed be adequate in the event of a dispute arising. Trusted Third Party services may additionally be involved for providing information to verify the evidence. The evidence user and the evidence verifier may be the same entity.

5.3.4 Dispute Resolution

In the dispute resolution phase, an adjudicator has the responsibility of resolving disputes between parties. The disputing parties are sometimes known as the plaintiff and the defendant. The dispute resolution phase is depicted in Figure 2.

When the adjudicator resolves disputes, it collects evidence from the disputing parties and/or the Trusted Third Parties. The process used by an adjudicator to resolve disputes is outside the scope of this Recommendation | International Standard.

This phase is not always needed. If all interested parties agree that an event or action occurred (or agree that it didn't occur) then there is no dispute to resolve. Furthermore, even if a dispute arises, it can sometimes be resolved directly between the parties without the need for an adjudicator. For example, if one of the parties to the dispute is honest but mistaken, then they may realize that they are wrong when they are shown the other party’s evidence.

Although this phase is not always needed for every instance of the Non-repudiation service, all Non-repudiation mechanisms must support the dispute resolution phase. That is, they must enable disputes to be resolved if they occur.

5.4 Some forms of Non-repudiation services

There are many forms of Non-repudiation services. Among the many forms, the Non-repudiation service associated with the transfer of data is one that is frequently considered.

The transfer of a message involves at least two entities, namely the originator and the recipient. Potential disputes concerning the event include the following:

- disputes in which the originator’s involvement in the event is disputed e.g. the alleged originator claims that the message was either forged by the recipient or forged by a masquerading attacker.
- disputes in which the recipient’s involvement in the event is disputed e.g. the alleged recipient claims the message was either not sent, lost in transit, or only received by a masquerading attacker.

For messaging, Non-repudiation services may be classified according to the kind of dispute they can help resolve.

The transfer of messages from an originator to a recipient may be regarded as being a sequence of separate events:

- the transmission of the message from the originator to a transfer agent;
- the transmission of the message between transfer agents (if more than one transfer agent is involved); and
- the transmission of the message from a transfer agent to the recipient.

For each of these events there are forms of the Non-repudiation service which provide evidence concerning that event. Accordingly, the following additional Non-repudiation services are identified:

- the Non-repudiation with proof of submission service is used to protect against a transfer agent's false denial of having accepted a message for transmission (either from the originator or from another transfer agent).
- the Non-repudiation with proof of transport service is used to protect against a transfer agent's false denial of having transmitted a message (either to the recipient or to another transfer agent).

NOTE – The Non-repudiation with proof of submission and Non-repudiation with proof of transport services do not provide evidence that an entity is responsible for the message or has understood the information that the message contains.

5.5 Examples of OSI Non-repudiation evidence

Depending on the OSI Non-repudiation services invoked, particular forms of evidence are needed for each type of event or action as illustrated below.

5.5.1 For Non-repudiation of origin

The evidence must include the following (which can be either signed or notarized):

- the distinguishing identifier of the originator;
- the data sent, or a digital fingerprint of the data.

The evidence may also include the following:

- the distinguishing identifier of the recipient;
- the date and time that the data was sent.

5.5.2 For Non-repudiation of delivery

The evidence must include the following (which can be either signed or notarized):

- the distinguishing identifier of the recipient;
- the data received, or a digital fingerprint of the data.

The evidence may also include the following:

- the distinguishing identifier of the originator;
- the date and time when the data was received.

When a Delivery Authority is used, the evidence may also include the following (which can be either signed or notarized):

- the distinguishing identifier of the Delivery Authority;
- the date and time when the delivery was first attempted by the Delivery Authority;
- the date and time when a ready to receive was obtained from the recipient;
- the date and time when the delivery was performed by the Delivery Authority;
- the date and time when the Delivery Authority was unable to perform the delivery;
- the probable cause of the non-delivery conditions (e.g. communications channel broken);
- an indication of the handling requirements that were met when delivering the message.

6 Non-repudiation policies

A Non-repudiation policy may include the following:

- Rules for the generation of evidence e.g. specifications of the classes of activity for which Non-repudiation evidence should be generated; specifications of the TTPs to be used to generate evidence; the roles in which those TTPs may act; the procedures that entities must follow when generating evidence.
- Rules for the verification of evidence e.g. specifications of the TTPs whose evidence is acceptable; for each TTP, the forms of evidence that will be accepted from that TTP.
- Rules for the storage of evidence e.g. the means to be used to ensure the integrity of stored evidence.

- Rules for the use of evidence e.g. specification of the purposes for which evidence may be used.

  NOTE – With some Non-repudiation mechanisms it may be difficult to prevent unauthorized use of evidence.

- Rules for adjudication e.g. specification of the agreed adjudicator(s) that may settle a dispute.

Each of these sets of rules may be defined by a different authority. For example, the rules for generation of evidence could be defined by the owner of a system, while the rules for adjudication could be defined by the law of the country in which the system exists.

If different parts of the policy are inconsistent, then the Non-repudiation service may fail to operate correctly e.g. by allowing an event which did in fact occur to be successfully denied during the dispute resolution phase.

The Non-repudiation policy itself may be used by the adjudicator when resolving a dispute. For example, the adjudicator might refer to the Non-repudiation policy to determine whether the rules for generation of evidence have been complied with.

Security policies can be explicitly stated, or implicitly defined by implementations. An explicit statement of the Non-repudiation policy (e.g. a natural language document) can help detect conflicts between different parts of the policy and can also aid the adjudicator.

Non-repudiation policies also deal with cases in which evidence has been compromised or in which the keys used to generate the evidence have been compromised or revoked.

Non-repudiation policies for interactions between security domains may result from agreements between independent security domains or may be imposed by a super-domain.

7 Information and facilities

7.1 Information

Information that can be used to resolve a dispute is known as evidence. Evidence may be stored locally by an evidence user or may be stored by a Trusted Third Party. Particular forms of evidence are digital signatures, secure envelopes and security tokens. Digital signatures are used with public key techniques while secure envelopes and security tokens are used with secret key techniques. Examples of information that can constitute evidence include:

- An identifier of the Non-repudiation security policy.
- The distinguishing identifier of the originator.
- The distinguishing identifier of the recipient.
- A digital signature or Secure Envelope.
- The distinguishing identifier of the evidence generator.
- The distinguishing identifier of the evidence generation requestor.
- The message, or a digital fingerprint of the message.

  NOTE – When the digital fingerprint is used in place of the message, an indicator is required to identify the method used in the derivation.

- The message identifier.
- An indication of the secret key needed to validate the security token.
- An identification of the particular public key needed to validate the digital signature (e.g. the distinguishing identifier of the Certification Authority and certificate serial number).
- The distinguishing identifier of the notary, time stamping TTP, In-line TTP, etc.
- A unique identifier for the evidence.
- The date and time that the evidence was deposited or recorded.
- The date and time the digital signature or security token was generated.

7.2 Non-repudiation facilities

This subclause identifies a number of Non-repudiation facilities that may be used to generate, send and validate evidence or to deposit evidence with a TTP.

7.2.1 Management-related facilities

Non-repudiation management-related activities may involve distribution of information, passwords or keys (using key management) to entities required to perform Non-repudiation. This may involve use of a protocol between communicating entities and other entities providing Non-repudiation services. Non-repudiation management may also involve the revocation of the keys used to produce evidence.

The Non-repudiation management facilities allow a user to obtain, modify and delete information which is necessary for the provision of Non-repudiation. In broad terms these facilities are:

- install management information;
- modify management information;
- delete management information;
- list management information.

The following management-related actions may be required in support of Non-repudiation services:

- recording the event in the audit trail;
- recording of the results of dispute arbitration;
- local reporting of the event;
- remote reporting of the event.

The specific action to be taken for each event is dependent on the security policy in operation.

7.2.2 Operation-related facilities

7.2.2.1 Generate Evidence

This facility is used to generate evidence. Evidence may be generated directly by the evidence subject (without involving a TTP), by one or more TTPs acting on behalf of the evidence subject, or by the evidence subject and one or more TTPs acting together.

Candidate inputs include:

- the Non-repudiation policy;
- the distinguishing identifier of the evidence subject;
- the distinguishing identifier of the Non-repudiation service requester;
- the data, or a digital fingerprint of the data;
- the distinguishing identifier of the TTP that will be used to generate the digital signature, the security token, or other evidence.

Candidate outputs include:

- evidence (e.g. a digital signature or a security token);
- the distinguishing identifier of the TTP that generated the digital signature, the security token, or other evidence.

7.2.2.2 Generate Time Stamp

This facility is used to generate time stamps.

Candidate inputs include:

- the distinguishing identifier of the entity requesting the time stamp;
- the distinguishing identifier of the TTP in the Time Stamping role;
- the data (e.g. signed message; acknowledgment;) or a digital signature or a digital fingerprint of the data.

Candidate outputs include:

- counter-signature computed by the TTP;
- an identification of the method and/or cryptographic algorithm used to generate the counter-signature (which secondarily indicates if the data or a digital fingerprint of the data is used);
- the distinguishing identifier of the Time Stamping Service;
- the date and time when the time stamping request was received;
- the date and time when the counter-signature was generated;
- a signed message which includes a time stamp and a digital fingerprint of the input data.

7.2.2.3 Generate Notarized Evidence

This facility is used to deposit evidence with the TTP.

Candidate inputs include:

- the distinguishing identifier of the evidence generation requestor;
- the evidence (e.g. a digital signature or security token);
- the distinguishing identifier of the evidence generator;
- the distinguishing identifier of the Non-repudiation policy.

Candidate outputs include:

- the recording number of the evidence;
- the date and time of evidence recording.

7.2.2.4 Validate Evidence

This facility is used to validate evidence.

Candidate inputs include:

- evidence;
- the distinguishing identifier of the evidence subject;
- the distinguishing identifier of the evidence user;
- the identifier of the key to be used for evidence verification;
- an indication of the intended use of the evidence (so that an assessment can be made to determine if the evidence is appropriate for this use under the Non-repudiation policy).

Candidate outputs include:

- the result of the verification (i.e. valid or invalid);
- the distinguishing identifier of the evidence subject;
- the distinguishing identifier of the evidence generator;
- the distinguishing identifier of the evidence verification requestor;
- the distinguishing identifier of the TTP that verified the digital signature or security token;
- the data or the digital fingerprint of the data.

7.2.2.5 Generate evidence for data transfers via an in-line TTP

Instead of sending data and/or acknowledgements between an originator and a recipient directly, data may be transferred through a TTP, so that Non-repudiation evidence may be assured by the TTP. This facility may also be used when it is suspected that a recipient could claim communication channel failure to deny delivery of the data.

To use this facility the following must be presented to the In-line TTP:

- the data;
- the distinguishing identifier of the recipient,

In addition, the following may be presented:

- a digital fingerprint of the data;
- the distinguishing identifier of the originator;
- a digital signature;
- the distinguishing identifier of the In-line TTP;
- the non-repudiation policy.

Candidate outputs from the In-line Trusted Third Party include:

- the distinguishing identifier of the In-line Trusted Third Party;
- the distinguishing identifier of the recipient;
- the recording number of the evidence;
- the date and time of the recording;
- the data, or a digital fingerprint of the data.

8 Non-repudiation mechanisms

The Non-repudiation service may be provided through the use of mechanisms such as digital signatures, encipherment, notarization and data integrity mechanisms, with support from other services such as time stamping. Both symmetric and asymmetric cryptographic algorithms can be used for Non-repudiation. The Non-repudiation service can use a combination of these mechanisms and services as appropriate to satisfy the security requirements of the application in question.

This clause describes mechanisms that can be used to provide Non-repudiation service and describes some of the threats to those mechanisms.

8.1 Non-repudiation using a TTP security token (secure envelope)

In this scheme, Non-repudiation evidence consists of a security token, sealed with a secret key known only to a TTP. The TTP generates the security token at the request of the evidence generation requestor and can subsequently verify it for the evidence user or the adjudicator. In this case the TTP is the evidence generator and the evidence verifier.

An evidence generation requestor transmits to the TTP, the data or a digital fingerprint of the data, along with a request to generate a security token. This request must be integrity-protected (e.g. using a seal), and may also be confidentiality-protected (e.g. using encipherment). Integrity-protected security tokens are sometimes known as secure envelopes.

Candidate inputs used in the generation of the security token include:

- an identification of the method and/or cryptographic algorithm used to ensure the integrity of the security token;
- an identification of the method and/or cryptographic algorithm used to ensure the confidentiality of the security token;
- the distinguishing identifier of the evidence subject;
- the distinguishing identifier of the evidence generation requestor;
- the non-repudiation policy applicable;
- the date and time of the event or action;
- data describing the event or action.

Candidate outputs include:

- a security token;
- the date and time the security token was generated.

8.2 Non-repudiation using security tokens and tamper-resistant modules

In this scheme, Non-repudiation evidence consists of a security token, sealed with a secret key which is stored within tamper-resistant cryptographic modules which are possessed by the evidence generator, the evidence verifier and the adjudicator. The tamper-resistant modules restrict the operations which may be performed with the secret key, and prevent the value of the key from being revealed outside the module.

The evidence generator's module permits the secret key to be used to create a sealed token, while the modules possessed by the evidence verifier and the adjudicator only permit token verification. All parties involved must trust that the secret keys have been installed correctly in the tamper-resistant cryptographic modules so that the same secret key can only be used by one entity for evidence generation but by other entities only for evidence verification.

If a dispute arises, the evidence user presents the sealed token to the adjudicator, and argues that it must have been created using the evidence generator's module, as the other modules which contain the same key are not capable of security token generation.

8.3 Non-repudiation using a digital signature

In this scheme, Non-repudiation evidence consists of a digitally signed data structure. Signature generation uses a signing key and signature verification uses a verification key.

Depending on the security policy, time information may be required. This may be included in the digital signature provided by an entity and/or provided by a TTP acting as a time stamping authority. When this is not provided by a TTP, this is not necessarily trusted by other entities. If the adjudicator needs a time stamp and/or the contextual information to resolve disputes, this information must be obtained from trusted sources (e.g. TTPs).

The evidence verifier and the adjudicator must be able to obtain the verification key in order to verify the evidence. If it cannot be guaranteed that the adjudicator will know the evidence generator's public key by other means, then the evidence must also include a security certificate for this key.

The digital signature may be generated by the evidence subject or generated by a TTP in a Signature Generation role.

A digital signature which is generated by the evidence subject is known as a direct digital signature. A digital signature mechanism which is generated by a TTP on behalf of the evidence subject is called a mediated digital signature.

Digital signatures alone are not sufficient to settle disputes when the certificate used to verify the signature has been revoked. In order to settle such disputes it is necessary, in addition, to provide the adjudicator with evidence about the revocation of the certificates (e.g. Certificate Revocation Lists – CRLs) that shows that the certificate was still valid at the time the digital signature was generated. However, this scheme does not allow settlement of disputes when the owner of the private key voluntarily uses an incorrect time, or when an attacker compromises the private key used to generate the signature. In order to settle such disputes it is necessary, in addition, to use a trusted time reference or a counter-signature from a TTP in its Time Stamping Role (see Annex E).

An evidence verifier may use a Directory Service to obtain information (such as security certificates) needed for the verification process. The evidence verifier must obtain the public key of the evidence generator. This key may be contained within a security certificate stored in the Directory. More than one certificate may be needed. To ensure a certificate is valid, it is also necessary to request the revocation certificate list that may apply. This is necessary for every Certification Authority which appears in a certification path (see ITU-T X.509 | ISO/IEC 9594-8).

An evidence user may seek the assistance of a TTP acting in a Signature Verification role to validate a digital signature. In this role the TTP verifies the relationship between the original message (or, if used, a digital fingerprint of the message) and the digital signature.

In this case the role of the TTP is to relieve the evidence user of the complexity of the signature verification process and to maintain the results of prior verification requests in the interest of optimizing responses to future verification requests. In order to do this, the TTP may require some interaction with a Directory. It is expected that the TTP acting in a Signature Verification role holds the public key of at least one Certification Authority. The TTP also takes into account the trust relationships that exist between different Certification Authorities.

8.4 Non-repudiation using Time Stamping

When a trusted time reference is needed and when the clock provided by the entity that produces the digital signature or security token cannot be trusted, it is necessary to rely on a Trusted Third Party to provide Time Stamping. Time Stamping can be used to establish that a message was signed before the signature key was compromised, and hence that the message is not a forgery. In a Time Stamping role the Trusted Third Party will provide a digital signature or security token to establish when the request was received. Time Stamping may be requested by the evidence generator, the Non-repudiation service requester, the evidence user or the evidence verifier.

Time Stamping adds the time and date and a seal or digital signature to data. Time Stamping does not require authentication of the entity that requested the time stamp. The evidence verifier must determine if the time stamps are within an acceptable range as dictated by the security policy.

Time Stamping may be combined with Signature Generation or Token Generation. If the entity that generates the digital signature includes a reliable and trusted clock, a counter-signature may not be required.

8.5 Non-repudiation using an in-line Trusted Third Party

In-line Trusted Third Party facilities can be explicitly requested for a particular event or action or may be provided implicitly. The In-line TTP then acts as an intermediary in all interactions for which the Non-repudiation service is requested and may provide evidence to an evidence user (such as an adjudicator). The In-line TTP will, in all cases, relay the data and monitor the event or action.

The TTP is trusted to keep records for future resolution of disputes. The data, or a digital fingerprint of the data, can be evidence if kept by the TTP.

8.6 Non-repudiation using a Notary

In the OSI model, a notarization mechanism provides assurance about the properties of data communicated between two or more entities, such as its integrity, origin, time and destination. A notary is trusted by the entities involved to hold the necessary information required to provide assurance in a testifiable manner and to keep records for future resolution of disputes. Digital Signature, Encipherment and Integrity mechanisms may be used, as appropriate, in support of the service being provided by the notary.

In an Evidence Generation role, the notary will record evidence to assure the properties of the data. In addition, a recording number may be used to identify this evidence.

In an Evidence Verification role, the notary will confirm the validity of the evidence.

8.7 Threats to Non-repudiation

No Non-repudiation mechanism is completely invulnerable to all threats. A mechanism which involves a TTP may not be secure if the TTP does not behave in a way which it is supposed to behave. This may happen either as the result of an accidental failure or as the result of an attack carried out by an insider. The consequences of this threat may be significant but are not discussed further in this Recommendation | International Standard. Non-repudiation mechanisms vary with respect to the consequences of TTP misbehaviour, and with respect to how easy it is for a TTP to cause protocol failures. An assessment must be made of which threats are likely and which have significant consequences in a particular environment, in order to choose a selection of mechanisms which keep the total risk within acceptable limits. Some examples of these threats, together with possible countermeasures, are discussed below.

8.7.1 Compromise of keys

8.7.1.1 Comprise of entity's generation key

In the period between the compromise of a key and the detection of this compromise by the legitimate owner of the key, there is a risk that an attacker might use the compromised key to generate evidence which an evidence user will accept as being valid. The Non-repudiation mechanism cannot recover from any damage that has been caused by such misuse of an evidence generation key. However, it is possible to determine the extent of the damage by using an evidence generation authority (e.g. a Signature Generation Authority) which may then keep an audit trail of generated evidence and hence make it possible to discover which evidence has been generated and when it was generated. It is also desirable to advertise as widely as possible the fact that the key has been misused but it will not always be possible to reach all the recipients who received evidence built using the compromised generation key.

As soon as this key compromise is detected by the legitimate owner of the key, the generation key needs to be revoked. If the generation key is a private key, then the corresponding public key certificate needs to be revoked. This can be done using Certificate Revocation Lists as defined in ITU-T Rec. X.509 | ISO/IEC 9594-8. However this is not sufficient, since this does not prevent some misuse of the key. Possible ways of countering this threat include using a Non-repudiation mechanism in which the generation of evidence requires the cooperation of a TTP as well as the evidence subject. For example, the use of either mediated digital signatures or counter-signatures from a Time-Stamping Authority can protect against this form of threat. In the later case, the Non-repudiation policy specifies that the evidence is valid only if correctly counter-signed by a Time-Stamping Authority (see Annex E).

Key compromise can also be deliberate. If the Non-repudiation policy specifies that an evidence subject will not be held responsible for misuse of their key between the time the key is compromised and the time this compromise is detected, then the evidence subject can take advantage of this to claim that its key has been compromised, and hence repudiate an action or event which actually took place. This threat may be countered by defining a maximum time delay that is allowed before reporting the compromise of a key. Under this policy, if an evidence user fails to declare the compromise of their key within this time limit, then the evidence subject is held responsible for any consequences of the misuse of their key. Evidence verifiers can then make sure that the delay allowed for the declaration of a key compromise has expired before accepting any evidence.

8.7.1.2 Compromise of TTP's generation key

When the compromise of a TTP's key has been detected, the key must be revoked. If the generation key is a private key, then the corresponding public key certificate needs to be revoked. This can be done using Certificate Revocation Lists as defined in ITU-T Rec. X.509 | ISO/IEC 9594-8. In order to deal with evidence previously generated with the (possibly) compromised key, it is necessary that the TTP keeps an audit trail of every use of its key. If the TTP's key is compromised, the audit trail can then be used to settle disputes.

8.7.1.3 Substitution of entity's verification key

This is the threat that an evidence user/verifier is fooled into believing that they have valid evidence. However, when a dispute needing adjudication arises, it is discovered that the evidence is invalid. That is, the evidence user looses, because they acted in good faith on the basis of apparently valid evidence, but the adjudicator finds against them. Possible ways of countering this threat include the use of strong procedures to make sure that the right entity is associated with the right verification key. Should a substitution occur, the wrong verification key must be removed as soon as the substitution is detected.

8.7.1.4 Substitution of TTP's verification key

If the verification key is a public key used by a TTP to directly verify evidence, the TTP can be tricked into accepting falsified evidence by falsifying whatever conveys the verification key to the adjudicator (e.g. paper documents, a certificate chain). A particular example of this is when the adjudicator's copy of a public key is substituted by an attacker.

When an attack of this kind has been detected, the substitution should be advertised as widely as possible but it should be noted that it will not always be possible to reach all the evidence users who used evidence that could have been verified using the substituted key. It is possible to determine which evidence was verified before the warning of the substitution by using an evidence verification authority (e.g. a Signature Verification Authority) which may then keep an audit trail of verified evidence. In this way it is possible to know which evidence was verified before, and which evidence was verified after, the warning.

If the verification key is a public key used by evidence users to directly verify certificates, then it should be changed as soon as detected.

8.7.2 Compromise of evidence

Information which was at one time acceptable as evidence may cease to be acceptable. Such information is known as compromised evidence.

8.7.2.1 Unauthorized modification or destruction of evidence

In this case, the action or event did happen, but the party with an interest in repudiating the event manages to modify or destroy the stored evidence. That party may then successfully repudiate an event which, in fact, occurred. This threat can be protected against by employing appropriate security mechanisms to prevent the modification or destruction of the evidence (e.g. redundant storage). The use of a TTP to store evidence can provide improved protection against this threat, as storage media kept by a TTP may be better protected than storage media kept by the evidence user.

8.7.2.3 Destruction or invalidation of evidence

This is the threat that the evidence stored by the TTP is destroyed. This threat can arise if the TTP is not sufficiently careful, and the TTP has not made adequate arrangements for backup. This threat can be protected against by using Non-repudiation mechanisms in which all the evidence needed to resolve disputes is stored by the evidence user. The evidence user can then ensure that the evidence will not be destroyed even if a TTP is malicious or careless.

8.7.3 Falsification of evidence

8.7.3.1 Falsification of evidence by outsider

In this case, a disputed event did not happen, but an outsider penetrates the system and creates false evidence that it did happen. This case may happen when a notary is involved. Cryptographic mechanisms may be used to protect stored evidence against forgery or modification by an intruder.

8.7.3.2 False verification of evidence

In mechanisms where a TTP is used to verify evidence, there is a threat that the TTP will tell the evidence user that it has validated the evidence, when the evidence is actually invalid. If a dispute arises, the evidence user will be unable to convince the adjudicator that the disputed event occurred. This threat can be protected against by using a Non-repudiation mechanism in which the evidence verifier can verify the evidence directly, without using a TTP.

8.7.3.3 Falsification of evidence by Trusted Third Party

This is the threat that a Trusted Third Party might forge evidence for an event which never occurred. If the TTP is trusted by the adjudicator, the adjudicator would accept the falsified evidence and hence be tricked into making an incorrect decision. This threat can be protected against by using a Non-repudiation mechanism in which it is difficult for TTPs to falsify evidence, or by ensuring that the TTPs used are trustworthy as well as being in a position of trust. In general, it is difficult to provide irrefutable evidence as to the trustworthiness of an entity.

9 Interactions with other security services and mechanisms

This clause describes how other security services can be used to support Non-repudiation. The use of Non-repudiation to support other security services is not discussed here.

9.1 Authentication

When interacting with a Trusted Third Party, entities may need to prove their identity by using an Authentication Service. Subsequent exchanges may need to be assured by the use of a Data Origin Authentication service. For example, when a TTP is used for signature generation, it may be required to authenticate the evidence subject before generating a signature.

9.2 Access Control

An Access Control service may be used to ensure that information stored by a TTP, or service offered by a TTP, is made available only to authorized entities.

9.3 Confidentiality

Confidentiality services may be required to protect the data from unauthorized disclosure (including, in some cases, unauthorized disclosure by or to a TTP) and also to protect against unauthorized disclosure of evidence.

9.4 Integrity

Integrity services will be required to ensure the integrity of the evidence.

With Non-repudiation with proof of Origin or Non-repudiation with proof of Delivery the integrity of the data must also be assured so that the data transferred between an originator and a recipient cannot be modified without detection.

9.5 Audit

An evidence user may use the audit recorder function to store evidence for use if a dispute arises later.

A notary or In-line TTP may use the audit recorder function to record the contents, origin, destination and time of the messages.

9.6 Key Management

A key Management service may be used to provide keys for use in evidence generation and evidence verification. The key Management service may be required to provide keys for evidence verification even though the corresponding key used for evidence generation has ceased to be valid or available.

Annex A

Non-repudiation in OSI Basic Reference Model

(This annex does not form an integral part of this Recommendation | International Standard)

A.1 Non-Repudiation with Proof of Origin

The Non-repudiation with Proof of Origin service provides the recipient of data with proof that protects against any attempt by the sender to falsely deny sending the data or its contents. This may be achieved when the evidence generator (usually the sender of the data, but possibly a TTP) delivers to the evidence verifier (usually the recipient of the data but possibly a party representing the recipient), evidence that the data was sent by the sender.

When a signature mechanism is used, the evidence is a digital signature of the data or a digital fingerprint of the data. Non-repudiation with Proof of Origin depends upon a previously agreed scheme for the provision of validated evidence. It has the following phases:

1) the Non-repudiation service requester generates evidence, or obtains evidence from a TTP and appends the evidence to the data;

2) the evidence is made available to the evidence user;

3) in the event of a dispute, the data and the evidence are produced by the evidence user; the adjudicator verifies the data against the evidence.

A.2 Non-repudiation with Proof of Delivery

The Non-repudiation with Proof of Delivery service provides the sender of the data with proof that protects against any subsequent attempt by the recipient to falsely deny receiving the data or its contents. This may be achieved when the evidence generator (usually the recipient of the data, but also possibly a TTP) delivers to the evidence verifier (usually the sender of the data but also possibly a party representing the originator, or a TTP) evidence that the data was delivered.

This service depends upon the return, by the recipient of the data, of an acknowledgement containing evidence. The acknowledgement will contain confirmation of receipt in the form of a digital signature on the original message (or a digital fingerprint of the original message) at the time of receipt.

When a signature mechanism is used, a signed acknowledgment is required as evidence.

Two cases of this service may be considered according to whether or not a TTP, acting in the role of a Delivery Authority, is involved in supporting this service.

Annex B

Non-repudiation Facilities Outline

(This annex does not form an integral part of this Recommendation | International Standard)

Security Facilities Outline		Element	Entity: Evidence Subject, Evidence Generator, Evidence Verifier, Evidence User, Non-repudiation-TTP, Adjudicator		
			Info Object: Evidence		
		Goal of Entity: To collect, maintain, make available and validate irrefutable evidence			
ACTIVITY	Entity	TTP, Security Authority			
	Function	(Not defined)			

	Management related activity	– install;
		– modify;
		– delete;
		– list.			

	Entity	Evidence generator	Evidence verifier	NR-TTP	Adjudicator
	Function	(Not defined)	(Not defined)	(Not defined)	(Not defined)
	Operational related activity	– Generate Evidence; – Generate notarized Evidence.	– Generate Evidence; – Generate notarized Evidence.	– Generate Time Stamp; – Transfer via TTP,	(Not defined)

INFORMATION	Input/Output Data element managed by SDA	– Management information, e.g. password or keys;
		– Information type;
		– Non-repudiation policy.			

	Information type used in operation	– Evidence;
		– digital signature;
		– security token;
		– security certificate;
		– time stamp.			

	Control Information	Recording of the event in the audit trail and the results of dispute arbitration; reporting of the relationship between entities.			

Annex C

Non-repudiation in store and forward systems

(This annex does not form an integral part of this Recommendation | International Standard)

In a store and forward system, a message is transferred between its originator and its recipient by one or more intermediaries, known as *transfer agents*. In such systems, the transmission of a message involves not only communication between the originator and the recipient, but also communication between the originator and a transfer agent, communication between the recipient and a transfer agent, and communication amongst transfer agents. The Non-repudiation service may be applied separately to each of the steps that are carried out in transporting the message to its ultimate destination.

The *Non-repudiation with proof of origin* service protects against a sender's false denial of sending the message or its contents. Either the recipient or the transfer agents may use the evidence collected by this service.

The *Non-repudiation with proof of delivery* service protects against a recipient's false denial of having received a message or its contents. Either the originator or the transfer agents may use the evidence collected by this service.

The *Non-repudiation with proof of submission* service is used to protect against a transfer agent's false denial of having accepted a message for transmission (either from the originator or from another transfer agent). The originator or other transfer agents may use the evidence collected by this service.

The *Non-repudiation with proof of transport* service is used to protect against a transfer agent's false denial of having transmitted a message (either to the recipient or to another transfer agent). The originator is the user of the evidence collected by this service.

The *Non-repudiation with proof of transfer* service is used to protect against a transfer agent's false denial of having accepted responsibility for delivering a message. This service is used when more than one transfer agent is involved in the delivery of a message. When the transfer agent which first accepted the message passes it on to a second transfer agent, the second transfer agent may provide the first with evidence that it has accepted responsibility for the message. When more than two transfer agents are involved, this service may also be used between the second and the third agent, and so on.

The use of these different forms of the Non-repudiation service is summarized in the following table:

Name of service	Protects against	Used by
Proof of origin	Originator	Recipient, transfer agent
Proof of submission	Transfer agent	Originator
Proof of transport	Transfer agent	Originator
Proof of transfer	Transfer agent	Transfer agent
Proof of delivery	Recipient	Originator, transfer agent

These additional forms of the Non-repudiation service (proof of submission and proof of transport) can be provided by viewing the system at a different level of granularity, and then using mechanisms that provide more fundamental forms of the Non-repudiation service (proof of origin and proof of delivery). For example, proof of transport can be implemented by refining the transmission of a message from an originator to a recipient into a sequence of message exchanges, one of which is an acknowledgement of delivery from a transfer agent to the originator, and then using the proof of origin service to protect this acknowledgment.

Annex D

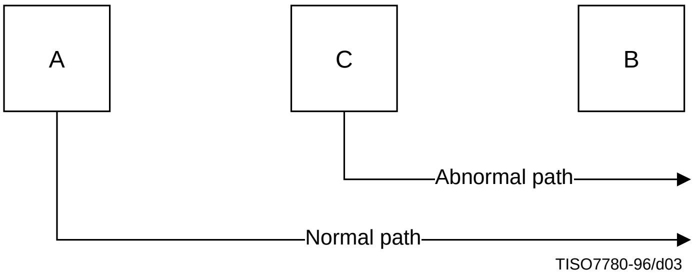
Recovery in a Non-repudiation service

(This annex does not form an integral part of this Recommendation | International Standard)

Security recovery deals with situations that should not occur under normal circumstances. However, the reality of computer security is that abnormal circumstances do occur and it is best to prepare for such an eventuality.

Specifically, many Non-repudiation mechanisms are dependent on cryptographic keys and the secrecy needed to protect them. The loss or exposure of a cryptographic key should be anticipated with a recovery plan being available to be put into effect immediately.

The following situation could occur when private cryptographic keys are used for a Non-repudiation service:



Data signed by a dishonest party (C), using the compromised private key from A, may be given to an honest participant (B). At some point in time it can be assumed that B will have cause to seek out A as a result of an action (or inaction) related to the unauthorized message, presenting the signed message as justification for the action. A will claim to have lost the related private key and cite a public declaration to that effect.

If brought to the attention of a judge or adjudicator, the liability of A will likely be determined as a result of comparing the time difference between the public declaration of the compromised key and the unauthorized, signed message. A will more than likely be held liable if the message pre-dates the declaration of the key compromise. Therefore if C has effectively pre-dated the message, A will be held responsible, unless some care has been taken to deal with this case.

In order to recover from such a situation, it is necessary to be able to know when exactly the message was signed. As the time put in the message by C cannot be trusted, it is necessary to invoke a TTP, to register formally the message by either:

- copying the message and signature in a suitable security audit trail (i.e. using a notary); and/or
- applying a counter-signature on the message which includes the date and time of the registration, obtained from an independent trusted party (i.e. Time Stamping Service).

By following this procedure, a dishonest participant would inadvertently document the real date and time of the signature. An adjudicator could then render an opinion of liability to the injured party (A) dependent on the following:

first, a comparison between the date/time of the message and the date/time of the counter-signature which must be within a small enough time window (e.g. 24 hours);

second, a comparison between the date/time of the message and the formal notification of the lost or compromised key.

In this manner the effective misuse of a lost or compromised cryptographic key will be reduced to the time window allowed for the registration of data by the Time Stamping Service.

The liability of party A in the event of a key compromise depends on the security policy in force. Breaches of security are not always detected immediately. Thus, even if party A notifies the TTP as soon as they become aware of the compromise, it can be possible for party C to forge messages after compromising A’s private key and before the detection of the compromise by A.

In resolving disputes, both of the following times can be relevant:

- The time at which A reported the compromise – A will repudiate all messages that can be shown to be signed after this time. (A should stop using the private key as soon as A becomes aware that it has been compromised).
- A time which A claims to be before the compromise of the key – A will not repudiate messages that can be shown to have been signed before this time. This time may not exist: A may have discovered the compromise, but be unsure as to when it actually took place.

Annex E

Interaction with the Directory

(This annex does not form an integral part of this Recommendation | International Standard)

A digital signature may be verified using an appropriate public key. When the public key is contained in a user certificate placed in the Directory, the correctness of the key may be verified provided the public key of the Certification Authority is known.

As the Certification Authority which has issued a certificate may have changed its public key since the certificate was prepared, it is necessary to have a means to verify the correctness of an "aged" public key. As the only key normally known is the current public key of a CA, there needs to be a link between the current public key and aged public keys. As a recipient is not aware of CA key changes, it is the responsibility of the different Certification Authorities to provide a way to verify their "old" certificates. This may be accomplished in two ways:

- by certifying every aged CA public key by the CA current public key; or
- by certifying every aged CA public key by the next CA public key.

In the former case, it is possible to verify directly the validity of the old CA public key corresponding to the private key used by the Certification Authority to issue the original certificate.

In the latter case, it is necessary to be able to collect a chain of certificates, to verify step by step the validity of the old CA public key. This will be accomplished by first looking for the certificate with a validity period corresponding to the date/time of the signed message and then recursively looking for a certificate with an overlapping but more recent validity period to find the value of the previous CA public key.

NOTE – In case of the possibility of the compromising of an old CA public key, the former method is preferable, because, with the second method, the chain of certificates towards older CA public key would be broken and thus older public keys of the CA would become implicitly invalid.

In the Directory, the Certification Authority does not keep track of the revocation list certificates of the other Certification Authorities or of their users for certificates when they are no longer valid. Therefore, an evidence user or a TTP has to gather all the necessary information (i.e. including revocation lists, even if empty) while it is still available, to prove that a given public key was valid at some point of time.

A revocation list certificate contains the date when it has been issued by the authority. It may also contain another date which can help to resolve disputes for some cases: the date when the user was still sure that his key was not compromised. All signatures issued by the user before this date will be recognized by the user as valid. Without this date, assuming the worst case, all signatures issued during the validity period of the security certificate would be considered as invalid. In a commercial environment it may be very important for a user that a signed document is still recognized as valid even in the case when the key used to sign the message has been lost. While this date is optional within a revocation list certificate, it will be required if the key of the corresponding certificate is used for a Non-repudiation service.

Trust relationships may vary with time. For example, an adjudicator can trust a CA today but not necessarily tomorrow. This kind of trust has to be made available so that it is possible for a recipient to know whether or not a potential dispute can be solved to his advantage. What kind of trust relationships a given adjudicator recognizes must be expressed. These trust conditions may be modeled using the following trust expressions:

- the CAs fully trusted and for which current public key value is known;
- the CAs trusted to issue both CA certificates and user certificates;
- the CAs only trusted to issue user certificates (but not CA certificates).

This information has to be made freely available to the evidence user. They may take the form of a security certificate which includes a validity period. Two forms of security policy certificate are defined: security policy certificates where it is the responsibility of the adjudicator to keep track of them and security policy certificates where it is the responsibility of the recipient to keep track of them.

Annex F

Bibliography

(This annex does not form an integral part of this Recommendation | International Standard)

– ITU-T Recommendation X.402 (1995) | ISO/IEC 10021-2:1996, *Information technology – Message Handling Systems (MHS): Overall Architecture*.

– CCITT Recommendation X.435 (1991), *Message handling systems: Electronic data interchange messaging system*.

– ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework*.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Telephone network and ISDN
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media
Series H	Transmission of non-telephone signals
Series I	Integrated services digital network
Series J	Transmission of sound-programme and television signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound-programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminal equipments and protocols for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks and open system communication**
Series Z	Programming languages