ISO/IEC JTC 1 N 9927

2009-12-01

ISO/IEC JTC 1
Information Technology

Document Type:	**New Work Item Proposal**
Document Title:	**Proposal for a new work item on Anonymous entity authentication.**
Document Source:	**SC 27 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 27 Secretariat**
Action ID:	**Act**
Due Date:	**2010-03-01**
No. of Pages:	**33**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1/SC 27 N8207

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for Proposed NP Ballot

TITLE: **Proposal for a new work item on Anonymous entity authentication**

SOURCE: SC 27 Secretariat

DATE: 2009-11-06

PROJECT: NP

STATUS: In accordance with Resolution 7 (contained in SC 27 N8299) of the 39th SC 27/WG 2 meeting held in Redmond, WA, USA, 2nd - 6th November 2009, this document is being circulated to the SC 27 National Bodies for a 3-month NWI letter ballot and to JTC 1 for a concurrent review.

P-Members of SC 27 are requested to submit their votes on this document via the ISO e-balloting application by **2010-02-25.**

ACTION ID: LB

DUE DATE: **2010-02-25**

DISTRIBUTION: P- and L-Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 7

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

New Work Item Proposal

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2009-11-06	Proposer: ISO/IEC JTC 1 SC 27
Secretariat: ISO/IEC JTC 1/SC27 DIN, Germany	**ISO/IEC JTC 1/SC 27 8207**

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title: Information technology – Security techniques – Anonymous entity authentication

Scope:

This ISO/IEC standard specifies anonymous entity authentication mechanisms. These mechanisms are used to corroborate that an entity is legitimate, i.e. it is the entity possesses the claimed attributes. The entity to be authenticated provides evidence that she/he has knowledge of a secret, without revealing her/his identifier to any unauthorized entity. The mechanisms are defined as exchanges of information between entities.

This standard provides

- a general anonymous entity authentication model;
- a variety of mechanisms that provide an anonymous entity authentication service.

For each mechanism, this standard specifies

- the requirements for and constraints on the mechanism;
- the cryptographic keys used by the mechanism;
- the contents of the information exchanges between entities.

Purpose and justification:

Authenticating the identifiers of communicating partners is one of the most important cryptographic services. Much research has been done into creating cryptographic mechanisms supporting this service, e.g., the entity authentication mechanisms specified in ISO/IEC 9798 and the digital signature mechanisms specified in ISO/IEC 9796 and ISO/IEC 14888.

The idea of anonymous communications is to hide the identifier of an authenticated entity to its communicating partner and/or to a third party, but to maintain the property that only an authentic entity can pass an authentication service. Practical requirements for anonymous communications have been growing very fast. Much research has been performed on the design of entity authentication mechanisms supporting anonymity, which have been targeted to meet a variety of requirements. Some of these mechanisms have been implemented by the computing industry and are widely available in computer platforms.

SC 27 started a NWI 29191 on the requirements for a certain type of anonymous communications and initiated a WG 2 Study Period on cryptographic mechanisms supporting anonymity in October 2008. After a one year investigation, it has been established that anonymous entity authentication is a sufficiently mature area of cryptography to allow standardisation by ISO/IEC.

Thus it is proposed to develop a new international standard concerned with mechanisms providing anonymous entity authentication. The new standard would be expected to contain a small number of mechanisms chosen for their efficiency and security, together with guidance on their use.

The study period has also proposed the development of another relevant new international standard, to be entitled anonymous digital signatures. This issue is addressed in a separate NWI proposal.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?
____ a single International Standard
____ more than one International Standard (expected number: .....)
__X_ a multi-part International Standard consisting of 2 parts
_____ an amendment or amendments to the following International Standard(s) .....
_____ a technical report , type .....

And which standard development track is recommended for the approved new work item?

_X_a. Default Timeframe

___b. Accelerated Timeframe

___c. Extended Timeframe

Relevant documents to be considered

IS 9798, IS 9796, IS 14888, WD 29191

Co-operation and liaison

Preparatory work offered with target date(s)

Target dates

WD 2010-05 CD 2011-05 FDIS 2012-10 IS 2013-05

Signature: DIN, German NB of ISO/IEC JTC 1/SC 27

Will the service of a maintenance agency or registration authority be required: No
- If yes, have you identified a potential candidate?
- If yes, indicate name

Are there any known requirements for coding? No

-If yes, please specify on a separate page

Does the proposed standard concern known patented items? Patents unknown
- If yes, please provide full information in an annex

Are there any known accessibility requirements and or dependencies (see: http://www.jtc1access.org)? No..........
- If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? No.....
- If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC27- attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:
It is proposed to assign this new item to JTC 1/SC 27

Voting on the proposal - Each P-member of the ISO/IEC/JTC 1/SC 27 has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:	**Closing date for voting:**	**Signature of Secretary:**
2009-11-24	2010-02-25	Krystyna Passia Secretariat JTC 1/SC27

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		
A.1 Market Requirement	Essential _X_ Desirable ____ Supportive ___	There is a generally accepted need for improved security in digital communications.
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive _X_ Not Relevant __	This standard might be used by evaluation facilities performing ISO/IEC 15408 security evaluations in support of regulatory requirements. E.g. legal frameworks for digital signatures.
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No _X_	
B.2 Commitment to other organization	Yes ___ No _X_	
B.3 Other Source of standards	Yes ___ No _X_	
C. Technical Status		
C.1 Mature Technology	Yes _X_ No ___	Schemes are known which have mathematical proofs of security, and which have been published for some years.
C.2 Prospective Technology	Yes __ No _X_	
C.3 Models/Tools	Yes __ No _X_	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes ___ No _X_	
D.2 Interoperability	Yes _X_ No __	Adoption of the schemes should improve interoperability of security products.
E. Adaptability to Culture, Language, Human Functioning and Context of Use		

E1. Cultural and Linguistic Adaptability	Yes ___ No _X_	
E.2 Adaptability to Human Functioning and Context of Use	Yes ___ No _X_	
F. Other Justification		

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for a external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. Adaptability to Culture, Language, Human Functioning and Context of Use

NOTE: The following criteria do not mandate any feature for adaptability to culture, language, human functioning or context of use. The following criteria require that if any features are provided for adapting to culture, language, human functioning or context of use by the new Work Item proposal, then the proposer is required to identify these features.

E.1 Cultural and Linguistic Adaptability. Indicate here if cultural and natural language adaptability is applicable to your project. If so, indicate how it is addressed in your project

plan. ISO/IEC TR 19764 (Guidelines, methodology, and reference criteria for cultural and linguistic adaptability in information technology products) now defines it in a simplified way:

“ability for a product, while keeping its portability and interoperability properties, to:

- be internationalized, that is, be adapted to the special characteristics of natural languages and the commonly accepted rules for their se, or of cultures in a given geographical region;

- take into account the usual needs of any category of users, with the exception of specific needs related to physical constraints”

Examples of characteristics of natural languages are: national characters and associated elements (such as hyphens, dashes, and punctuation marks), writing systems, correct transformation of characters, dates and measures, sorting and searching rules, coding of national entities (such as country and currency codes), presentation of telephone numbers and keyboard layouts. Related terms are localization, jurisdiction and multilingualism.

E.2 Adaptability to Human Functioning and Context of Use. Indicate here whether the proposed standard takes into account diverse human functioning and diverse contexts of use. If so, indicate how it is addressed in your project plan.

NOTE:

1. Human functioning is defined by the World Health Organization at **http://www3.who.int/icf/beginners/bg.pdf as:**
   <<In ICF (International Classification of Functioning, Disability and Health), the term functioning refers to all body functions, activities and participation.>>

2. 2. Content of use is defined in ISO 9241-11:1998 (Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability) as:
   <<Users, tasks, equipment (hardware, software and materials), and the physical and societal environments in which a product is used.>>

3. 3. Guidance for Standard Developers to address the needs of older persons and persons with disabilities).

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here

ISO/IEC JTC 1/SC 27 N8207 Annex 1

Date:2009-11-03

ISO/IEC XXXXX-1

Supporting document for NWI proposal

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Information technology — Security techniques — Anonymous entity authentication — Part 1: General

Technologies de l'information — Techniques de sécurité — Authentification d'entité Anonyme — Partie 1: Général

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

C:\Documents and Settings\liqun\My Documents\ISO\mechanisms supporting anonymity\NWI proposals\support_doc_anonymous_authentication_part1_20091103.doc STD Version 2.1c2

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC XXXXX-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *JTC*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC XXXXX consists of the following parts, under the general title *Information technology — Security techniques — Anonymous entity authentication*:

Part 1: General

Part 2: Mechanisms based on anonymous signature schemes.

Further parts may follow.

Introduction

Authenticating the identifiers of communicating partners is one of the most important cryptographic services. There are a wide variety of cryptographic mechanisms supporting this service, e.g., the entity authentication mechanisms specified in ISO/IEC 9798 and the digital signature mechanisms specified in ISO/IEC 9796 and ISO/IEC 14888.

The concept of anonymous communications is to hide the identifier of an authenticated entity to its communicating partner and/or to a third party, but to keep the property that only an authentic entity can pass an authentication service. Practical requirements for anonymous communications have been growing very fast. Anonymous entity authentication mechanisms are designed to support such anonymous communications. Some of these mechanisms have been implemented by the computing industry and are widely available in computer platforms.

This ISO/IEC standard specifies a general model and a number of mechanisms for anonymous entity authentication.

Information technology — Security techniques — Anonymous entity authentication — Part 1: General

1 Scope

This part of ISO/IEC XXXXX specifies a general model, general requirements and constraints for anonymous entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is legitimate, as claimed. The entity to be authenticated provides evidence that s/he has knowledge of a secret without revealing her/his identifier to any unauthorised entity. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC XXXXX, but in the following parts of this multipart International Standard.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC XXXXX (all parts), *Information technology – Security techniques – Anonymous digital signatures*.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
entity authentication
the corroboration that an entity is the one claimed

3.2
mutual authentication
entity authentication which provides both entities with assurance of each other's identity

3.3
sequence number
a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

3.4
time stamp
a time variant parameter which denotes a point in time with respect to a common reference

3.5
time variant parameter
a data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp

3.6
token
a message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique

3.7
unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

3.8
anonymous entity authentication

3.9
anonymous (digital) signature

4 Symbols (and abbreviated terms)

5 General requirements

This clause specifies the general requirements of anonymous entity authentication mechanisms, for instance,

- Each entity involved in a mechanism should be able to access to domain public parameters.
- In an anonymous entity authentication mechanism based on an anonymous signature, each entity involved in the mechanism should be able to access to an authentic copy of the public verification key(s).
- Etc…

6 General model

This clause specifies the general model of anonymous entity authentication mechanisms. A couple of figures each indicating a type of communication approaches between entities in the mechanisms are given.

7 Options for unilateral authentication and mutual authentication

This clause specifies the definitions of unilateral authentication mechanisms and mutual authentication mechanisms which support anonymity.

8 Options for the aid of a trusted third party

This clause specifies how a trusted third party is involved in anonymous entity authentication mechanisms specified in this standard.

Annex A
(informative)

Security properties of anonymous entity authentication mechanisms

This annex provides informative information of security properties and use guidelines of anonymous entity authentication mechanisms.

Bibliography

ISO/IEC JTC 1/SC 27 N8207 Annex 2

Date:2009-11-03

ISO/IEC XXXXX-2

Supporting document for NWI proposal

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Information technology — Security techniques — Anonymous entity authentication — Part 2: Mechanisms based on anonymous digital signature schemes

Technologies de l'information — Techniques de sécurité — Authentification d'entité Anonyme — Partie 2: Des mécanismes basés sur des schémas de signature numérique anonyme
search

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

C:\Documents and Settings\liqun\My Documents\ISO\mechanisms supporting anonymity\NWI proposals\support_doc_anonymous_authenticaton_part2_20091103.doc STD Version 2.1c2

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC XXXXX-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *JTC*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC XXXXX consists of the following parts, under the general title *Information technology — Security techniques — Anonymous entity authentication*:

Part 1: General

Part 2: Mechanisms based on anonymous digital signature schemes

Further parts may follow.

Introduction

Authenticating the identifiers of communicating partners is one of the most important cryptographic services. There are a wide variety of cryptographic mechanisms supporting this service, e.g., the entity authentication mechanisms specified in ISO/IEC 9798 and the digital signature mechanisms specified in ISO/IEC 9796 and ISO/IEC 14888.

The concept of anonymous communications is to hide the identifier of an authenticated entity to its communicating partner and/or to a third party, but to keep the property that only an authentic entity can pass an authentication service. Practical requirements for anonymous communications have been growing very fast. Anonymous entity authentication mechanisms are designed to support such anonymous communications. Some of these mechanisms have been implemented by the computing industry and are widely available in computer platforms.

This part of ISO/IEC XXXXX specifies a number of anonymous entity authentication mechanisms which follow the general model specified in ISO/IEC XXXXX-1. Every mechanism makes use of an anonymous digital signature mechanism, as specified in ISO/IEC XXXXX (anonymous digital signature mechanisms).

The mechanisms specified in this document use a collision resistant hash-function to hash the entire message. ISO/IEC 10118 specifies hash-functions.

Information technology — Security techniques — Anonymous entity authentication — Part 2: Mechanisms based on anonymous digital signature schemes

1 Scope

This part of ISO/IEC XXXXX specifies entity authentication mechanisms using anonymous digital signature mechanisms, as specified in ISO/IEC XXXXX (anonymous digital signature mechanisms).

The mechanisms specified in this part of ISO/IEC XXXXX use time variant parameters such as time stamps, sequence numbers, or random numbers to prevent valid authentication information from being accepted at a later time or more than once.

This part of ISO/IEC XXXXX provides

- a general description of an anonymous entity authentication mechanism using an anonymous signature;
- a variety of mechanisms that provide an anonymous entity authentication service.

For each mechanism, this part of ISO/IEC XXXXX specifies

- the requirements for and constraints on the mechanism;
- the cryptographic keys used by the mechanism;
- the contents of the information exchanges between entities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 10118 (all parts), *Information technology – Security techniques – Hash-functions*.

ISO/IEC XXXXX (all parts), *Information technology – Security techniques – Anonymous digital signatures*.

ISO/IEC XXXXX-1, *Information technology – Security techniques – Anonymous entity authentication – Part 1: General*.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
collision-resistant hash-function
hash-function satisfying the following property:

- it is computationally infeasible to find any two distinct inputs which map to the same output

[ISO/IEC 10118-1]

3.2
hash-code
string of bits which is the output of a hash-function

[ISO/IEC 10118-1]

3.3
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

- for a given output, it is computationally infeasible to find an input which maps to this output;
- for a given input, it is computationally infeasible to find a second input which maps to the same output

[ISO/IEC 10118-1]

3.4
message
string of bits of any length

3.5
parameter
integer or bit string or function

3.6
signature
one or more data elements resulting from the signature process

3.7
signature key
set of private data elements specific to an entity and usable only by this entity in the signature process
NOTE Sometimes called a private signature key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-7.

3.8
signature process
process which takes as inputs the message, the signature key and the domain parameters, and which gives as output the signature

3.9
signed message
set of data elements consisting of the signature, the part of the message which cannot be recovered from the signature, and an optional text field

3.10
verification key
set of public data elements which is mathematically related to an entity's signature key and which is used by the verifier in the verification process

NOTE Sometimes called a public verification key in other standards, e.g. ISO/IEC 9796-2, ISO/IEC 9796-3 and ISO/IEC 9798-7.

3.11
verification process
process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid

3.12
security strength

a number associated with the amount of work (that is the number of operations) that is required to break a cryptographic algorithm or system

NOTE Security strength is specified in bits and is a specific value from the set {80, 112, 128, 192, 256}

3.13
group key

3.14
group manager (also called group issuer)

3.14
signer credential

3.15
entity authentication
the corroboration that an entity is the one claimed

3.16
mutual authentication
entity authentication which provides both entities with assurance of each other's identity

3.17
sequence number
a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period

3.18
time stamp
a time variant parameter which denotes a point in time with respect to a common reference

3.19
time variant parameter
a data item used to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp

3.20
token
a message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique

3.21
unilateral authentication
entity authentication which provides one entity with assurance of the other's identity but not vice versa

3.22
anonymous entity authentication

3.23
anonymous (digital) signature

4 Symbols (and abbreviated terms)

5 General model and requirements

This clause specifies the general model and requirements of the anonymous entity authentication mechanisms specified in this part of the standard. Some contents in this clause are recalled from the general part of this standard. The references to the general part are given here, and specific requirements on the mechanisms using an anonymous digital signature mechanism are addressed.

6 Options for signer traceability

This clause gives a high level description of two options regarding how a signer can be traced from a signature created by this signer. They are called signer-controlled traceability and manager-controlled traceability. The definitions of these two options and differentiation between them are addressed.

7 Mechanisms with signer-controlled traceability

This clause specifies a small number of entity authentication mechanisms with signer-controlled traceability.

8 Mechanisms with manager-controlled traceability

This clause specifies a small number of entity authentication mechanisms with manager-controlled traceability.

Annex A

(normative)

ASN.1 module

This annex specifies the ASN.1 module for all the mechanisms specified in this part of the standard.

Annex B
(informative)

Security guidelines for anonymous entity authentication mechanisms

This clause provides security and usage guidelines for the anonymous entity authentication mechanisms which are specified in this part of the standard. It also provides some information on how to choose a mechanism suitable for particular applications.

Annex C
(informative)

Use of text fields

This clause specifies a variety of text fields, which are used in the mechanisms specified in this part of the standard.

Bibliography