ISO/IEC JTC 1/SC 27 N8208

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 digital signatures**

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 N8208**

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 digital signatures

Scope:

This ISO/IEC standard specifies anonymous digital signature mechanisms, in which given a signature, an unauthorised entity cannot discover the signer's identifier. However the mechanisms still have the property that only a legitimate signer can provide such a signature.

This standard provides

- a general description of an anonymous digital signature mechanism;
- a variety of mechanisms that provide anonymous digital signatures.

For each mechanism, this standard specifies

- the process for generating private signing keys and public verification keys;
- the process for producing signatures;
- the process for verifying signatures.

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 keep 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 done into designing digital signature mechanisms supporting anonymity, which are targeted to meet a variety of requirements. Some of the 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 signatures are 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 digital signatures. 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 titled anonymous entity authentication. 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 9796, IS 14888, IS 9798, 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 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 N8208 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 digital signatures — Part 1: General

Technologies de l'information — Techniques de sécurité — Anonyme signatures numériques — 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_signature_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 digital signatures*:

Part 1: General

Part 2: Mechanisms using a group public key

SC27/WG2 note: If a business need for the development of ring signatures is discovered, then a new part of the standard can be added, possibly to be called:

- Part 3: Mechanisms using multiple public keys.

However, work on this part should not start before the business need is established.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity. A digital signature mechanism satisfies the following requirements.

- Given either or both of the following two things:
  - the verification key but not the signature key,
  - a set of signatures on a sequence of messages that an attacker has adaptively chosen,

  it should be computationally infeasible for the attacker:
  - to produce a valid signature on a new message,
  - to produce a new signature on a previously signed message, or
  - to recover the signature key.
- It should be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE – Computational feasibility depends on the specific security requirements and environment.

Anonymous digital signature mechanisms are a special type of digital signature mechanism. In an anonymous digital signature mechanism, given a digital signature, an unauthorised entity cannot discover the signer's identifier. However the mechanism still has the property that only a legitimate signer can provide such a signature.

As is the case for ordinary digital signature mechanisms, anonymous digital signature mechanisms are based on asymmetric cryptographic techniques, and involve three basic operations.

- A process for generating private signature keys and public verification keys.
- A process that uses the signature key, called the signature process.
- A process that uses the verification key, called the verification process.

One of the major differences between an ordinary digital signature and an anonymous digital signature is the nature of the public keys used to perform the signature verification. To verify an ordinary digital signature, the verifier makes use of a single public verification key, which is bound to the signer's identifier. To verify an anonymous digital signature, the verifier makes use of either a group public key or multiple public keys, which are not bound to an individual signer. The level of anonymity depends upon the size of the group and the number of public keys.

The security of digital signature mechanisms depends on problems believed to be intractable, i.e. problems for which, given current knowledge, finding a solution is computationally infeasible, such as the integer factorization problem and the discrete logarithm problem in an appropriate group. The mechanisms specified in this standard are based on one of these two problems.

The mechanisms specified in this standard use a collision resistant hash-function to hash the entire message. ISO/IEC 10118 specifies hash-functions. Ordinary digital signature mechanisms are specified in ISO/IEC 9796 and ISO/IEC 14888.

Information technology — Security techniques — Anonymous digital signatures — Part 1: General

1 Scope

ISO/IEC XXXXX specifies anonymous digital signature mechanisms for messages of arbitrary length.

This part of ISO/IEC XXXXX contains general principles and requirements for anonymous digital signatures. It also contains definitions and symbols which are used in all parts of ISO/IEC XXXXX.

A variety of means are available for obtaining a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of ISO/IEC XXXXX. For further information, see ISO/IEC 9594-8 [4], ISO/IEC 11770-3 [3] and ISO/IEC 15945 [5].

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*.

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}

4 Symbols (and abbreviated terms)

5 General requirements

This clause specifies the general requirements of anonymous digital signature mechanisms, for instance,

- Each entity involved in a mechanism should be able to access to domain public parameters.

- In an anonymous signature mechanism using a group public key, each entity involved in the mechanism should be able to access to an authentic copy of the public key.

- In an anonymous signature mechanism using a group public key, an authentic channel should be required between a signer and a group manager (or an issuer) during the process of generating a credential of a signer's signature key.

- Etc…

6 General model

This clause specifies the general model of anonymous digital signature mechanisms. Generally speaking, an anonymous digital signature mechanism is defined by the specification of the following processes: key generation process, signature process, and verification process. Some mechanisms also need a signer tracing process, a revocation process and so on.

7 Options for group verification keys and multiple verification keys

This clause specifies the definitions of two categories of anonymous digital signature mechanisms specified in this standard. The first category is using a group verification key and the second one is using multiple verification keys.

8 Key generation

This clause specifies the procedures of a key generation process, such as

- generating domain parameters,

- generating the group manager's (or issuer's) private key and public key,

- generating a signer's signature key and the corresponding credential.

9 Signature process

This clause specifies the procedures of a signature process.

10 Verification process

This clause specifies the procedures of a verification process. In some mechanisms, the verification process includes a signer tracing process and/or a revocation process. The clause also specifies the meaning of the signer tracing process and revocation process.

Annex A
(informative)

Security properties of anonymous digital signatures

This annex provides informative information of security properties and use guidelines of anonymous digital signature mechanisms.

Bibliography

ISO/IEC JTC 1/SC 27 N8208 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 digital signatures — Part 2: Mechanisms using a group public key

Technologies de l'information — Techniques de sécurité — Anonyme signatures numériques — Partie 2: Mécanismes utilisant un groupe de clé publique

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_signature_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 digital signatures*:

Part 1: General

Part 2: Mechanisms using a group public key

SC27/WG2 note: If a business need for the development of ring signatures is discovered, then a new part of the standard can be added, possible to be called:

- Part 3: Mechanisms using multiple public keys.

However, work on this part should not start before the business need is established.

Introduction

Digital signature mechanisms can be used to provide services such as entity authentication, data origin authentication, non-repudiation, and data integrity. A digital signature mechanism satisfies the following requirements.

- Given either or both of the following two things:
  - the verification key but not the signature key,
  - a set of signatures on a sequence of messages that an attacker has adaptively chosen,

  it should be computationally infeasible for the attacker:
  - to produce a valid signature on a new message,
  - to produce a new signature on a previously signed message, or
  - to recover the signature key.
- It should be computationally infeasible, even for the signer, to find two different messages with the same signature.

NOTE – Computational feasibility depends on the specific security requirements and environment.

Anonymous digital signature mechanisms are a special type of digital signature mechanism. In an anonymous digital signature mechanism, given a digital signature, an unauthorised entity cannot discover the signer's identifier. However the mechanism still has the property that only a legitimate signer can provide such a signature.

As is the case for ordinary digital signature mechanisms, anonymous digital signature mechanisms are based on asymmetric cryptographic techniques, and involve three basic operations.

- A process for generating private signature keys and public verification keys.
- A process that uses the signature key, called the signature process.
- A process that uses the verification key, called the verification process.

One of the major differences between an ordinary digital signature and an anonymous digital signature is the nature of the public keys used to perform signature verification. To verify an ordinary digital signature, the verifier makes use of a single public verification key, which is bound to the signer's identifier. To verify an anonymous digital signature, the verifier makes use of either a group public key or multiple public keys, which are not bound to an individual signer. The level of anonymity depends upon the size of the group and the number of public keys.

This part of ISO/IEC XXXXX specifies a number of anonymous digital signature mechanisms which make use of a group verification key for verifying a signature. The corresponding private key is owned by a group manager, also called the group issuer.

The security of digital signature mechanisms depends on computational problems believed to be intractable, i.e. problems for which, given current knowledge, finding a solution is computationally infeasible, such as the integer factorization problem and the discrete logarithm problem in an appropriate group. The mechanisms specified in this part of ISO/IEC XXXXX are based on one of these two problems.

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 digital signatures — Part 2: Mechanisms using a group public key

1 Scope

This part of ISO/IEC XXXXX specifies anonymous digital signature mechanisms, in which a verifier makes use of a group public key to verify a digital signature.

This part of ISO/IEC XXXXX provides

- a general description of an anonymous digital signature mechanism using a group public key;
- a variety of mechanisms that provide such anonymous digital signatures.

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

- the process for generating private signing keys and public verification keys;
- the process for producing signatures;
- the process for verifying signatures.

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-1, *Information technology – Security techniques – Anonymous digital signatures – 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

4 Symbols (and abbreviated terms)

5 General model and requirements

This clause specifies the general model and requirements of the anonymous digital signature mechanisms specified in this part of the standard. Some contents in this clause are recalled from the general part of this standard. So references to the general part are given here, and specific requirements on the mechanisms using a group public key are addressed.

6 Options for signer traceability

This clause gives a high level specification 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 digital signature mechanisms with signer-controlled traceability. This type of digital signatures is also called Direct Anonymous Attestation (DAA).

8 Mechanisms with manager-controlled traceability

This clause specifies a small number of digital signature mechanisms with manager-controlled traceability. This type of digital signatures is also called group signatures.

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 the anonymous signature mechanisms

This clause provides security and usage guidelines for the anonymous signature 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)

Numerical examples

This clause provides numerical examples for each digital signature mechanism specified in this part of the standared.

Bibliography