INTERNATIONAL STANDARD

ISO/IEC 9796-2

Second edition
2002-10-01

AMENDMENT 1
2008-01-15

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 2: Integer factorization based mechanisms

AMENDMENT 1

Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message —

Partie 2: Mécanismes basés sur une factorisation entière

AMENDEMENT 1

Reference number
ISO/IEC 9796-2:2002/Amd.1:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

Amendment 1 to ISO/IEC 9796-2:2002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Information technology — Security techniques — Digital signature schemes giving message recovery —

Part 2:
Integer factorization based mechanisms

AMENDMENT 1

Add the following text after page 46.

Annex E
(normative)

ASN.1 module

E.1 Formal definition

```
MessageRecoverySignatureMechanisms {
   iso(1) standard(0) signature-schemes(9796) part(2) asn1-module(1)
      message-recovery-signature-mechanisms(0) }
DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

   HashFunctions
      FROM DedicatedHashFunctions {
         iso(1) standard(0) hash-functions(10118) part(3)
            asn1-module(1) dedicated-hash-functions(0) };


SignatureWithMessageRecovery ::= SEQUENCE {
   algorithm  ALGORITHM.&id({MessageRecovery}),
   parameters ALGORITHM.&Type({MessageRecovery}{@algorithm}) OPTIONAL
}

MessageRecovery ALGORITHM ::= {
   dswmr-mechanism1A      |
   dswmr-mechanism2A      |
   dswmr-mechanism3A      |
   dswmr-mechanism1N      |
   dswmr-mechanism2N      |
   dswmr-mechanism3N      |
   dswmr-mechanism1A-sha1 |
   dswmr-mechanism2A-sha1 |
   dswmr-mechanism3A-sha1 |
   dswmr-mechanism1N-sha1 |
   dswmr-mechanism2N-sha1 |
   dswmr-mechanism3N-sha1,

   ...   -- Expect additional signature scheme objects --
}

dswmr-mechanism1A ALGORITHM ::= {
   OID mechanism1A PARMS HashFunctions
}

dswmr-mechanism2A ALGORITHM ::= {
   OID mechanism2A PARMS HashFunctions
}

dswmr-mechanism3A ALGORITHM ::= {
   OID mechanism3A PARMS HashFunctions
}

dswmr-mechanism1N ALGORITHM ::= {
   OID mechanism1N PARMS HashFunctions
```

```
}

dswmr-mechanism2N ALGORITHM ::= {
   OID mechanism2N PARMS HashFunctions
}

dswmr-mechanism3N ALGORITHM ::= {
   OID mechanism3N PARMS HashFunctions
}

dswmr-mechanism1A-sha1 ALGORITHM ::= { OID  mechanism1A-sha1 }

dswmr-mechanism2A-sha1 ALGORITHM ::= { OID  mechanism2A-sha1 }

dswmr-mechanism3A-sha1 ALGORITHM ::= { OID  mechanism3A-sha1 }

dswmr-mechanism1N-sha1 ALGORITHM ::= { OID  mechanism1N-sha1 }

dswmr-mechanism2N-sha1 ALGORITHM ::= { OID  mechanism2N-sha1 }

dswmr-mechanism3N-sha1 ALGORITHM ::= { OID  mechanism3N-sha1 }

-- Cryptographic algorithm identification --

ALGORITHM ::= CLASS {
   &id    OBJECT IDENTIFIER  UNIQUE,
   &Type  OPTIONAL
}
  WITH SYNTAX { OID &id [PARMS &Type] }

-- Message recovery signature mechanisms --

OID ::= OBJECT IDENTIFIER  -- Alias

signatureMechanismA OID ::= {
   iso(1) standard(0) signature-schemes(9796) part2(2) mechanism(0) alternate(0)
}

mechanism1A OID ::= { signatureMechanismA mechanism1(0) }

mechanism2A OID ::= { signatureMechanismA mechanism2(1) }

mechanism3A OID ::= { signatureMechanismA mechanism3(2) }

signatureMechanismN OID ::= {
   iso(1) standard(0) signature-schemes(9796) part2(2) mechanism(0) normal(1) }

mechanism1N OID ::= { signatureMechanismN mechanism1(0) }

mechanism2N OID ::= { signatureMechanismN mechanism2(1) }

mechanism3N OID ::= { signatureMechanismN mechanism3(2) }

-- Combined signature scheme and hash-function mechanisms --

mechanismA-Hash OID ::= {
   iso(1) standard(0) signature-schemes(9796) part2(2)
      mechanismHash(2) alternate(0) }

mechanism1A-sha1 OID ::= { mechanismA-Hash mechanism1-SHA1(0) }
```

```
mechanism2A-sha1 OID ::= { mechanismA-Hash mechanism2-SHA1(1) }

mechanism3A-sha1 OID ::= { mechanismA-Hash mechanism3-SHA1(2) }

mechanismN-Hash OID ::= {
   iso(1) standard(0) signature-schemes(9796) part2(2)
      mechanismHash(2) normal(1) }

mechanism1N-sha1 OID ::= { mechanismN-Hash mechanism1-SHA1(0) }

mechanism2N-sha1 OID ::= { mechanismN-Hash mechanism2-SHA1(1) }

mechanism3N-sha1 OID ::= { mechanismN-Hash mechanism3-SHA1(2) }

END  -- MessageRecoverySignatureMechanisms --
```

E.2 Use of subsequent object identifiers

Each of the signature schemes uses a hash-function, a sequence containing a hash algorithm identifier and any associated parameters. Therefore, the signature scheme object identifier may be followed by one of the dedicated hash-function algorithm identifiers specified in ISO/IEC 10118-3 and any associated parameters.

Using the ASN.1 XML value notation, a value of type SignatureWithMessageRecovery using normal signature processing mechanism 1 defined in this Standard and the SHA-1 hash-function defined in ISO/IEC 10118-3 would be represented as:

```
<SignatureWithMessageRecovery>
   <algorithm> 1.0.9796.2.0.1.0 <algorithm>
   <parameters>
      <HashFunctions>
         <algorithm> 1.3.14.3.2.26 <algorithm>
         <parameters/>
       <HashFunctions>
   </parameters>
</SignatureWithMessageRecovery>
```

A value of type SignatureWithMessageRecovery using the combined object identifier for normal signature processing mechanism 1 and the SHA-1 hash-function has the simpler form:

```
<SignatureWithMessageRecovery>
   <algorithm> 1.0.9796.2.2.1.0 <algorithm>
</SignatureWithMessageRecovery>
```