

INTERNATIONAL STANDARD ISO/IEC 29150:2011 TECHNICAL CORRIGENDUM 1

Published 2014-03-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION

• MEЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

• ORGANISATION INTERNATIONALE DE NORMALISATION

INTERNATIONAL ELECTROTECHNICAL COMMISSION

• MEЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ

• ORGANISATION INTERNATIONALE DE NORMALISATION

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Signcryption

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Signcryptage RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 29150:2011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Page 28, A.1 Formal definition

Replace the current text of A.1 with the following:

A.1 Formal definition

```
Signcryption {
  iso(1) standard(0) signcryption(29150)
      asn1-module(0) signcryption-mechanisms(0) version(1)
}
  DEFINITIONS EXPLICIT TAGS ::= BEGIN

IMPORTS

HashFunction, KeyDerivationFunction
  FROM EncryptionAlgorithms-2 {
    iso(1) standard(0) encryption-algorithms(18033) part(2)
      asn1-module(0) algorithm-object-identifiers(0) };
```

ICS 35.040

Ref. No. ISO/IEC 29150:2011/Cor.1:2014(E)

ISO/IEC 29150:2011/Cor.1:2011(E)

```
SigncryptionAlgorithmIdentifier ::=
                  AlgorithmIdentifier {{ SigncryptionMechanism }}
SigncryptionMechanism ALGORITHM ::= {
   { OID signcryption-mechanism-dlsc
                                       PARMS SCparameters } |
   { OID signcryption-mechanism-ecdlsc PARMS SCparameters } \mid
   { OID signcryption-mechanism-ifsc PARMS SCparameters } |
   { OID signcryption-mechanism-ets
                                      PARMS SCparameters },
   ... -- Expect additional signcryption mechanisms --
}
SCparameters ::= SEQUENCE {
   kdf KeyDerivationFunction,
   hash HashFunction
-- Cryptographic algorithm identification --
OID ::= OBJECT IDENTIFIER -- Alias --
is29150 OID ::= { iso(1) standard(0) signcryption(29150) }
mechanism OID ::= { is29150 mechanisms(1) }
signcryption-mechanism-dlsc OID ::= { mechanism dlsc(1) }
signcryption-mechanism-ecdlsc OID ::= { mechanism ecdlsc(2) }
\verb|signcryption-mechanism-ifsc| & \verb|OID| ::= \{ | mechanism | ifsc(3) | \} \\
signcryption-mechanism-ets
                             OID ::= { mechanism ets(4) }
AlgorithmIdentifier { ALGORITHM: IOSet } ::= SEQUENCE {
   algorithm ALGORITHM.&id({IOSet}),
   parameters ALGORITHM.&Type({IOSet}{@algorithm}) OPTIONAL
}
ALGORITHM ::= CLASS {
   &id OBJECT IDENTIFIER UNIQUE,
   &Type OPTIONAL
  WITH SYNTAX { OID &id [PARMS &Type] }
END -- Signcryption --
```