International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 2

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 2

ITU-T Recommendation X.509 (2005) – Technical Corrigendum 2

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	
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 SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	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	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	**X.500–X.599**
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
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 and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399

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

INTERNATIONAL STANDARD ISO/IEC 9594-8
ITU-T RECOMMENDATION X.509

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 2

Source

Corrigendum 2 to ITU-T Recommendation X.509 (2005) was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under ITU-T Recommendation A.8 procedure. An identical text is also published as Technical Corrigendum 2 to ISO/IEC 9594-8.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

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.

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 2

1) Correction of the defects reported in defect report 326

a) *Add a new paragraph to the end of 18.1.1*

Annex J provides a suggested algorithm to be used for protected passwords.

b) *Add Annex J and renumber subsequent annexes:*

Annex J

Use of Protected Passwords for Bind operations

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

The protected component of **SimpleCredentials** specifies an **OCTET STRING** to be hashed. This annex provides information about how this octet-string may be constructed. It also proposes some suggested associated procedures.

In its simple form, the octet-string is constructed as the DER encoding of the following:

```
SEQUENCE {
        name        DistinguishedName,
        time1       GeneralizedTime,
        random1     BIT STRING,
        password    OCTET STRING }
```

The **name** component is the distinguished name of the sender and the **password** component is the password of the sender.

The sender generates the two other values as follows:

a) The **time1** value should specify the time after which the authentication should fail. This time should be "closely" after the current time.

b) The **random1** value is a new random number generated for each authentication attempt. The value should be sufficiently large to prevent the same number to be generated frequently.

The same pair of **time1** and **random1** should never be used more than once.

The same value of **name**, **time1** and **random1** shall be supplied in the **SimpleCredentials** data type of the Bind.

NOTE 1 – The hashing algorithm is also transferred.

The receiver of a Bind request/result will perform the authentication as follows:

a) If the value in **time1**, as supplied in the **SimpleCredentials**, is less than the current time seen by the recipient, the authentication already fails here. Also, the time value should be different from recently received time values.

b) If the value in the **random1**, as supplied in the **SimpleCredentials**, is equal to a value received in a recent Bind request/response, the authentication also fails.

c) If **time1** and **random1** appear to be valid, the **name**, **time1** and **random1** included in the Bind request/result, together with the local copy of the password, are used to generate a copy of the message digest using the algorithm indicated.

d) If the generated message digest is equal to the message digest received in the Bind request/result, the authentication is positive, otherwise it fails.

The above procedure allows the password to be protected during transfer and it prevents replay of the transmission sequence. If the attempted reply is done early, the random number will cause the authentication to fail. If the reply is attempted sometime later, the random number may be accepted, but the authentication will fail due to the time value.

The scheme above may be extended by using the following sequence.

```
SEQUENCE {
    f1          OCTET STRING,     -- hashed octet string from above
    time2       GeneralizedTime,
    random2     BIT STRING }
```

The DER encoding of this data type is then used as the octet-string in the **SimpleCredentials**.

In this case, also the **time2** and **random2** have to be included in **SimpleCredentials**.

The hashing algorithm used for producing the **f1** component shall be the same as used for the hashing, as indicated within the **HASH** data type within **SimpleCredentials**.

NOTE 2 – This Directory Specification does not give any recommendation as to how values for **time2** and **random2** are selected.

2) Correction of the defects reported in defect report 330

a) In clause 7, in the paragraph starting with "The **extensions** *field allows..", replace the existing text:*

"If the criticality flag is **TRUE**, unrecognized extensions shall cause the structure to be considered invalid, i.e., in a certificate, an unrecognized critical extension would cause validation of a signature using that certificate to fail. When a certificate-using implementation recognizes and is able to process an extension, then the certificate-using implementation shall process the extension regardless of the value of the criticality flag. Note that any extension that is flagged non-critical will cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension and will ignore it.

If unknown elements appear within the extension, and the extension is not marked critical, those unknown elements shall be ignored according to the rules of extensibility documented in 12.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5."

With the following text:

"If the criticality flag is **TRUE**, unrecognized extensions shall cause the structure to be considered invalid, i.e., in a certificate, an unrecognized critical extension would cause validation of a signature using that certificate to fail. When a certificate-using implementation recognizes and is able to fully process an extension, then the certificate-using implementation shall process the extension regardless of the value of the criticality flag. When a certificate-using implementation recognizes and is able to partially process an extension for which the criticality flag is **TRUE**, then its behaviour in the presence of unrecognized elements is extension specific and may be documented in each extension. However, the default behaviour, when not specified specifically for an extension, is to treat the entire extension as unrecognised. If unrecognized elements appear within the extension, and the extension is not marked critical, those unrecognized elements shall be ignored according to the rules of extensibility documented in 12.2.2 in ITU-T Rec. X.519 | ISO/IEC 9594-5.

Note that any extension that is flagged non-critical will cause inconsistent behaviour between certificate-using systems that will process the extension and certificate-using systems that do not recognize the extension and will ignore it. The same may be true for extensions that are flagged critical, between certificate-using systems that can fully process the extension and those that can partially process the extension, depending upon the extension."

b) *In clause 7 replace the following paragraph:*

"A validation engine has two possible actions to take with respect to an extension:

i) it can ignore the extension and accept the certificate (all other things being equal);

ii) it can process the extension and accept or reject the certificate depending on the content of the extension and the conditions under which processing is occurring (e.g., the current values of the path processing variables)."

with:

"A validation engine has three possible actions to take with respect to an extension:

i) if the extension is unrecognized and is marked non-critical, the validation engine shall ignore the extension and accept the certificate (all other things being equal);

ii) if the extension is unrecognized and marked critical, the validation engine shall reject the certificate;

iii) if the extension is recognized, the validation engine shall process the extension and accept or reject the certificate depending on the content of the extension and the conditions under which processing is occurring (e.g., the current values of the path processing variables)."

3) Correction of the defects reported in defect report 331

In the Scope clause replace:

The schema components, including object classes, attribute types and matching rules for storing PKI and PMI object in the Directory, are included in this Recommendation | International Standard.

with:

The schema components (including object classes, attribute types, and matching rules) for storing PKI and PMI objects in the Directory are included in this Recommendation | International Standard.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009