International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# X.893

**Corrigendum 1**

(10/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

OSI applications – Generic applications of ASN.1

## Information technology – Generic applications of ASN.1: Fast infoset security

## Technical Corrigendum 1

Recommendation ITU-T X.893 (2007) – Technical Corrigendum 1

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 (1) | X.1100–X.1199 |
| CYBERSPACE SECURITY | X.1200–X.1299 |
| SECURE APPLICATIONS AND SERVICES (2) | X.1300–X.1499 |
| CYBERSECURITY INFORMATION EXCHANGE | X.1500–X.1599 |
| CLOUD COMPUTING SECURITY | X.1600–X.1699 |
| QUANTUM COMMUNICATION | X.1700–X.1729 |

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

**INTERNATIONAL STANDARD ISO/IEC 24824-3**
**RECOMMENDATION ITU-T X.893**

# Information technology – Generic applications of ASN.1: Fast infoset security

## Technical Corrigendum 1

## Summary

This technical corrigendum to ITU-T Rec. X.893 | ISO/IEC 24824-3 provides corrections to the informative annexes and bibliography removing references to the obsolete triple DES algorithm.

## Source

Corrigendum 1 to ITU-T Rec. X.893 (2007) was approved on 2019-10-14 by ITU-T Study Group 17 (2017-2020) under the Recommendation ITU-T A.8 procedure. An identical text is also published as Technical Corrigendum 1 to ISO/IEC 24824-3.

## History

| Edition | Recommendation | Approval | Study Group | Unique ID[*] |
|---|---|---|---|---|
| 1.0 | ITU-T X.893 | 2007-05-29 | 17 | 11.1002/1000/9113 |
| 1.1 | ITU-T X.893 (2007) Cor. 1 | 2019-10-14 | 17 | 11.1002/1000/14041 |

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## 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 not 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 – Generic applications of ASN.1: Fast infoset security

# Technical Corrigendum 1

*Conventions used in this corrigendum: Original, unchanged, text is in* normal font. *Deleted text is struck-through, thus:* ~~deleted text~~. *Inserted text is underlined, thus:* inserted text.

## 1 Clause A.3.2.6

*Replace clause A.3.2.6 with:*

**A.3.2.6** The encrypting application selects that the ~~triple DES~~ AES 256 algorithm (see [~~ANSI X9.52~~FIPS 197]) will be used for encrypting the **n:payment element** information item (and content). This results in the production of the **xenc:EncryptionMethod element** information item associated with the encrypted type information (see the **xenc:EncryptedData element** information item).

## 2 Annex C

Replace:

```
<soap:Body wsu:Id="TheBody">
  <xenc:EncryptedData wsu:Id="EncryptedBodyContents"
           Type="urn:fastinfoset:element">
       <xenc:EncryptionMethod
             Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
       <xenc:CipherData>
           <xenc:CipherValue>...</xenc:CipherValue>
       </xenc:CipherData>
  </xenc:EncryptedData>
</soap:Body>
```

with:

```
<soap:Body wsu:Id="TheBody">
  <xenc:EncryptedData wsu:Id="EncryptedBodyContents"
           Type="urn:fastinfoset:element">
       <xenc:EncryptionMethod
             Algorithm="http://www.w3.org/2001/04/xmlenc#~~tripledes~~aes256-cbc"/>
       <xenc:CipherData>
           <xenc:CipherValue>...</xenc:CipherValue>
       </xenc:CipherData>
  </xenc:EncryptedData>
</soap:Body>
```

## 3 Bibliography

Replace bibliography with:

[ITU-T X.509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

~~[ANSI X9.52] ANSI X9.52: *Triple Data Encryption Algorithm Modes of Operation*, 1998.~~

[FIPS 180-2] FIPS PUB 180-2, *Secure Hash Standard*, U.S. Department of Commerce/National Institute of Standards and Technology, 2002.

[FIPS 197] FIPS PUB 197, *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology (NIST) 2001.

[IETF RFC 2045] IETF RFC 2045 (1996), *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*.

[IETF RFC 3447] IETF RFC 3447 (2003), *Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1*.

[WSS] OASIS *Web Services Security (WSS): SOAP Message Security 1.1 (WS-Security 2004)*.

[WS-I] WS-I *Basic Security Profile 1.0*.

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | Tariff and accounting principles and international telecommunication/ICT economic and policy issues |
| 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 | Environment and ICTs, climate change, e-waste, energy efficiency; 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 | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling, and associated measurements and tests |
| 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, next-generation networks, Internet of Things and smart cities |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2019