

ISO/IEC 24824-3:2008-05 (E)

Information technology_ - Generic applications of ASN.1: Fast infosec security

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references	1
2.1 Identical Recommendations International Standards	1
2.2 Additional references	1
3 Definitions	2
3.1 Imported definitions	2
3.2 Additional definitions	2
4 Abbreviations	2
5 Notation	2
6 Canonical Fast Infosec algorithms	3
6.1 Requirements on canonical Fast Infosec algorithms	3
6.2 Requirements on canonical XML algorithms for use by a canonical Fast Infosec algorithm	3
6.3 Restrictions when serializing an XML infosec to a canonical fast infosec document	3
6.4 Canonical Fast Infosec algorithms	4
7 W3C XML Signature and Fast Infosec	4
8 W3C XML Encryption and Fast Infosec	5
8.1 Application-level extensions for encryption	5
8.2 Generation of a complete XML infosec from part of an XML infosec	5
8.3 Application-level extensions for decryption	6
Annex A Examples of signing and encrypting an XML infosec	7
A.1 Introduction of examples	7
A.2 Signing and verifying the SOAP message infosec	7
A.3 Encrypting and decrypting the SOAP message infosec	10
Annex B – Signed SOAP message infosec	12
Annex C – Signed and encrypted SOAP message infosec	13
Bibliography	14