z/OS

Change version

2.4.0

Show full table of contents

Filter on titles

BDT
Encryption Facility for z/OS
EREP
GDDM
HLASM
IBM HTTP Server - Powered by Apache, Version 9.0
IBM Z Multi-Factor Authentication
IBM Tivoli Directory Server for z/OS
IBM Z System Automation
IBM z/OS Management Facility
IBM Open Data Analytics for z/OS
ICKDSF
Infoprint Server and Transforms, PSF for z/OS - APS
ISPF
Knowledge Center for z/OS
REXX Alternate Library

	Non-FIPS				FIPS						
Algorithm	**Sizes**	**System SSL software**	**Direct calls to CPACF**	**Support through ICSF[1]**	**Sizes**	**System SSL software**	**Direct calls to CPACF**	**Support through ICSF (zEC12, zBC12, z13, z13s, z14, z14 ZR1)**			
								Software	**CPACF**	**CEXnA**	**CEXnP**
3DES	168	X	X		168	X	X				
AES	128 and 256	X	X		128 and 256	X	X				
AES-GCM	128 and 256			X	128 and 256				X		
Brainpool Curves - ECC, ECDH, ECDHE	160-512			X							
DES	56	X	X								
DH, DHE	512–2048	X			2048			X		X - Key agreement	
DSA	512–2048	X			1024-2048	X					
MD5	48	X									
NIST Curves - ECC, ECDSA, ECDH, ECDHE	192-521			X	192-521			X			X - ECDSA signature generate, ECDH/ECI key agreemer

IIC TECHNOLOGIES

- S-100 doesn’t use “pluggable” (dynamic) algorithms because they need to be fixed for ECDIS OEMs
- S-100 Part 15 uses DSA because it was used by S-63 and familiar
- Blowfish was replaced by AES
- US FIPS standard (186-5) is the main normative reference (reflects origins of S-63).

- Key lengths were increased by S-100 Edition 5.0.0 following observations by SECOM community. Other algorithms were added (to the S-100 schema enumeration) by S-100 (but not implemented)

- A change of schema would be possible (without change to S-100 schemas) but is currently unexplored. The only impact is
  - Size of signatures and CATALOG.XML (CATALOG.SIGN) files.
  - There is an impact on implementers though

- DSA will disappear from FIPS, and SSH (remains in SSL for now)

4 The Digital Signature Algorithm (DSA)

Prior versions of this standard specified the DSA. This standard no longer approves the DSA for digital signature generation. However, the DSA may be used to verify signatures generated prior to the implementation date of this standard. See FIPS 186-4 [7] for the specifications for the DSA.

Notably, FIPS 186-5 removes DSA as an approved digital signature algorithm “due to a lack of use by industry and based on academic analyses that observed that implementations of DSA may be vulnerable to attacks if domain parameters are not properly generated. DSA is retained only for the purposes of verifying existing signatures.”

To facilitate a transition to the new standard, FIPS 186-4 will remain in effect alongside FIPS 186-5 for a period of one year. During the transition period (02/03/2023 – 02/03/2024) vendors may elect to comply with FIPS 186-4 or FIPS 186-5. After the one-year transition period vendors must comply with the new FIPS 186-5 standards.

IIC TECHNOLOGIES