

IBM Servers with Cryptographic Coprocessor(s)

The chart below is provided as a quick reference for the number of actual CMOS Cryptographic Coprocessors are available per model on each of the IBM Server machines listed. There are additional caveats for availability of the Cryptographic Coprocessor during recovery situations that are listed due to complexity and variation.

Included under the Features column are all cryptographic features available since initial announcement on the machine. Some of these feature codes are no longer available due to packaging changes.

Exportable feature codes for the Crypto Licensed Internal Code authorize the use of 512-bit RSA keys for symmetric key distribution, use of 56-bit DES keys for data privacy, and 1024-bit RSA keys for digital signature generation.

Feature codes authorizing use of Triple-DES (T-DES) also authorize the use of 56-bit DES. The key lengths for cryptographic usage are selected by the application issuing the Application Programming Interface from OS/390's or z/OS's Integrated Cryptographic Service Facility (ICSF) component.

Server	Models	# Cryptos	Features ¹
2003 - Multiprise 2000² (withdrawn) FIPS 140-1 Level 4	102, 103, 104, 105, 106, 107, 115, 116, 124, 125, 126, 135, 1C5, 136, 202, 203, 204, 205, 206, 207, 215, 216, 224, 225, 227, 2C5, 237	1	0800, 0808 0801, 0802, 0803 0804, 0805, 0806 0809, 0810, 0807⁶
	146, 156, 246, 247, 257	2	0811 ⁶ , 0812 ⁶ , 0813 ⁶
3000 - Application StarterPak 3000 (withdrawn) FIPS 140-1 Level 4	A10, A20	1	0800, 0808, 0814, 0815, 0806, 0809 0810, 0807 , 0811 ⁶ 0812 ⁶ , 0813 ⁶
7060 - Multiprise 3000² FIPS 140-1 Level 4 (TDES)	H30 ⁵ , H50 ⁵ , H70 ⁵ , P30 ⁵	1	0003 ⁵ , 0005 ⁵ , 0007 ⁵ 0008 ⁵ , 0800, 0808, 0804, 0805, 0824, 0825, 0866, 0869 0807⁶ , 0806, 0809 0811 ⁶ , 0812 ⁶ , 0813 ⁶
9672 - Generation 3² (withdrawn) FIPS 140-1 Level 4	R14, RA4, RB4, R24, RC4, R34	1	0800, 0808, 0804 0805, 0806, 0809
	R44, R54, R64, R74, R84, R94, RX4, RY4(C04 is a coupling facility and has no Crypto Coprocessors)	2	0810, 0807⁶ , 0811 ⁶ 0812 ⁶ , 0813 ⁶
9672 - Generation 4 FIPS 140-1 Level 4 (TDES)	RA5, R15, RB5, R25, RC5, R35	1	0800, 0808 ⁶ , 0814, 0815, 0834, 0835 0806, 0809, 0810
	R45, R55, R65, R75, R85, R95, RX5, RY5 (C05 is a coupling facility and has no Crypto Coprocessors)	2	0866, 0869 , 0807 ⁶ 0811 ⁶ , 0812 ⁶ , 0812 ⁶ 0813 ⁶

IBM Servers with Cryptographic Coprocessor(s)

9672 - Generation 5 FIPS 140-1 Level 4 (TDES)	T16, RA6, R16, Y16	1 ³	0800, 0814, 0815 0834, 0835
	T26, RB6, R26, RC6, Y26		0866, 0869, 0860
	R36, RD6, R46, R56, R66, R76, R86, R96, RX6, Y36, Y46, Y56, Y66, Y76, Y86, Y96, YX6	2 ⁴	0806, 0809, 0810 0807 ⁶ , 0811 ⁶ , 0812 ⁶ 0813 ⁶
9672 - Generation 6 FIPS 140-1 Level 4 (TDES)	X17, Z17	1 ³	0800, 0808, 0814, 0815
	X27, X37, X47, X57, X67, X77, X87, X97, XX7, XY7, XZ7, Z27, Z37, Z47, Z57, Z67, Z77, Z87, Z97, ZX7, ZY7, ZZ7	2 ⁴	0834, 0835 , 0806 0809, 0810, 0860 0864, 0865, 0866 0869
2064 - z900 FIPS 140-1 Level 4 (TDES)	101, 1C1, 2C1	1 ³	
	102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 1C2, 1C3, 1C4, 1C5, 1C6, 1C7, 1C8, 1C9, 2C2, 2C3, 2C4, 2C5, 2C6, 2C7, 2C8, 2C9, 210, 211, 212, 213, 214, 215, 216	2 ⁴	0800, 0808, 0844, 0845, 0861, 0862 0864, 0865, 0866 0869, 0874, 0875 0876, 0879
2066- z800² FIPS 140-1 Level 4 (TDES)	0A1, 0B1, 0C1, 001	1 ³	0800, 0808, 0861
	0A2, 002, 003, 004	2 ⁴	0862, 0865, 0866 0869, 0876, 0879 0875

¹ The below is the description of each feature code. Note that the feature code is listed without its preceding zero.

0800 - Crypto Coprocessor (CCF) Hdw installed	0808 - Crypto Coprocessor (CCF) Hdw not installed
0003 ⁵ - Processor 7060 Model H30 with crypto	0005 ⁵ - Processor 7060 Model H50 with crypto
<u>0007⁵ - Processor 7060 Model H70 with crypto</u>	<u>0008⁵ - Processor 7060 Model P30 with crypto</u>
0801 - CDMF with Exportable PKA (config)	0802 - DES with Exportable PKA (config)
0803 - DES with Exportable PKA and TKE (config)	
0804 - DES with PKA (config)	0805 - DES with PKA and TKE (config)
0806 - TKE Hardware (Token-Ring) Connection	0809 - TKE Hardware (Ethernet) Connection
0807 ⁶ - Optional Priced Smart Card Reader (4754)	0810 - TKE Hardware (WAN) Connection (N/A)
- 3 Personal Security Cards are included with	0811 ⁶ - CDMF with Exportable PKA
<u>0812⁶ - DES with Exportable PKA (config)</u>	<u>0813⁶ - DES with Exportable PKA and TKE (config)</u>
0814 - DES with PKA (config)	0815 - DES with PKA and TKE (config)
0824 - T-DES with PKA on M3000 (config)	0825 - T-DES with PKA & TKE on M3000 (config)
0832 - T-DES with Exportable PKA (config)	0833 - T-DES with Exportable PKA & TKE (config)
<u>0834 - T-DES with PKA G5/6 CCF (config)</u>	<u>0835 - T-DES with PKA and TKE G5/6 CCF (config)</u>
0874 - T-DES w/PKA for z900 CCF (config)	0875 - TDES w/PKA & TKE for z900/z800 CCF (config)
0866 ⁷ - TKE Hdw 2000 (Token-Ring) Connection	0869 ⁷ - TKE Hdw 2000 (Ethernet) Connection
0860 - PCICC Hdw Feature for G5 and G6	0861 - Dual PCICC Hdw Feature for z900/z800
0864 - PCI T-DES w/Exportable PKA (config)	0865 - PCI T-DES with PKA (config)
Requires 0834 or 0874	Requires 0835 or 0875
0862 - PCI Crypto Accelerator (PCICA) Hdw Feat.	

US Export laws have relaxed such that most companies outside the US and Canada are generally approved for triple-DES full key length support and 1024-bit length for Public Keys protecting Symmetric keys during key distribution. If these options are not selectable, contact your countries' IBM ERO office for information.

IBM Servers with Cryptographic Coprocessor(s)

² The machines so indicated do not have the US standard no-charge crypto support. These machines have a fee charged against the Enablement Diskette. Other geographies may charge fees for features differently than in US.

³ There are 2 Cryptographic Coprocessors installed on these models but only 1 is available for usage.

⁴ Loss of Crypto sparing capability (via Twin-tail) may occur on some models depending on number of ICFs.

⁵ These feature codes are associated with the M3000 models that have Crypto installed. Feature codes also exist for each model indicating no crypto; 0013, 0015, 0017, and 0018.

⁶ This code may appear with earlier processor models or with models based on country export laws but is no longer associated with these models or has been withdrawn. Some codes, like 0808, may never appear on some models.

⁷ TKE 2000 Workstation features are enhanced and provide support for PCICC features.

Codes shown are from the US configurator for the specific processors are in **bold blue text** and may not be selectable in some countries during the ordering process. Contact your countries' IBM ERO office for information.

Abbreviations:

CDMF	Commercial Data Masking Facility	PKA	Public Key Algorithm
DES	Data Encryption Standard (FIPS-46)	T-DES	Triple-DES
ERO	Export Regulation Office	TKE	Trusted Key Entry
FIPS	Federal Information Processing Standard	WAC	Wide Area Connection
LIC	Licensed Internal Code		