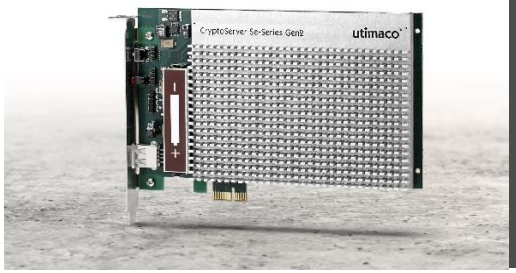


SecurityServer Se-Series Gen2 LAN V5 Benchmarks (PKCS#11 R2)

1 Environment

Benchmarks below have been measured on a server with Intel Xeon Dual Core (2.33 GHz), 2 GB RAM running under Debian 8 (64 bit).

The benchmark program communicates with the SecurityServer Se-Series Gen2 LAN V5 HSM through PKCS#11 interface, running a single thread and a single session. RSA signing operations received minimal input data, thus hashing overhead is negligible; performance for RSA decryption can thus be assumed to be the same as for RSA signing.

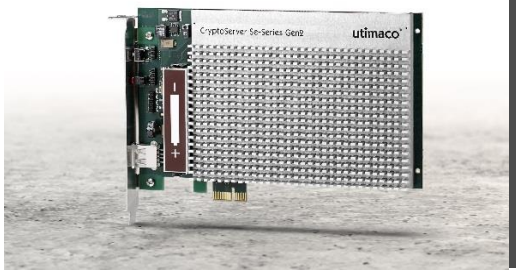
Measurements do not include overhead for session setup (login), but they include communication time through the PCIe bus respectively Ethernet network. The figures thus show the effective performance that a single-threaded application with strictly sequential function calls will achieve.

Applications spawning multiple threads for processing high loads on an HSM may achieve considerably higher performance, depending on the number of threads, algorithm and key sizes. As such multi-threading scenarios may be very diverse, please contact us with your specific requirements for discussing performance estimations.

Note:

- Performance for CryptoServer LAN may vary considerably depending on network architecture and network latency.
- Performance for CryptoServer plug-in cards may vary depending on server architecture, CPU frequency and Operating System, especially for short commands and encryption of short data blocks.

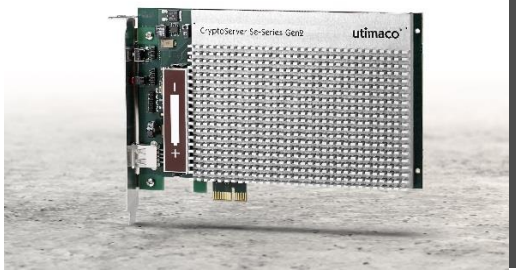
.



SecurityServer Se-Series Gen2 LAN V5 Benchmarks (PKCS#11 R2)

2 Symmetric algorithm: Triple DES 112 bit key size

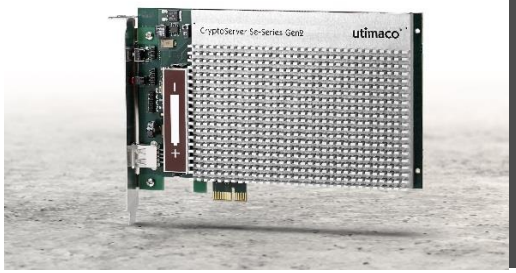
Triple DES 112 bit	Se12 PCIe	Se52 PCIe	Se500 PCIe	Se1500 PCIe	Se12 LAN	Se52 LAN	Se500 LAN	Se1500 LAN
Key generation	900 / s	900 / s	900 / s	900 / s	900 / s	900 / s	900 / s	900 / s
Encryption 128 byte	1000 / s	4000 / s	4000 / s	4000 / s	1000 / s	2600 / s	2600 / s	2600 / s
Encryption 512 byte	1000 / s	2800 / s	2800 / s	2800 / s	1000 / s	1900 / s	1900 / s	1900 / s
Bulk encryption 8 Kbyte	0,8 MB/s	2,9 MB/s	2,9 MB/s	2,9 MB/s	0,8 MB/s	2,9 MB/s	2,9 MB/s	2,9 MB/s
Bulk encryption 64 Kbyte	0,8 MB/s	2,9 MB/s	2,9 MB/s	2,9 MB/s	0,8 MB/s	2,9 MB/s	2,9 MB/s	2,9 MB/s



SecurityServer Se-Series Gen2 LAN V5 Benchmarks (PKCS#11 R2)

3 Symmetric algorithm: AES 128 and 256 bit key sizes

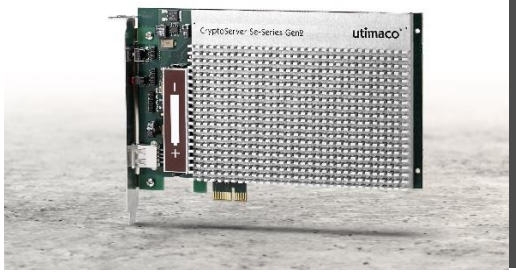
AES 128 bit	Se12 PCIe	Se52 PCIe	Se500 PCIe	Se1500 PCIe	Se12 LAN	Se52 LAN	Se500 LAN	Se1500 LAN
Key generation	1000 / s	1100 / s	1100 / s	1100 / s	1000 / s	1100 / s	1100 / s	1100 / s
Encryption 128 byte	1000 / s	4000 / s	4000 / s	4000 / s	1000 / s	2800 / s	2800 / s	2800 / s
Encryption 512 byte	1000 / s	3200 / s	3200 / s	3200 / s	1000 / s	2200 / s	2200 / s	2200 / s
Bulk encryption 8 Kbyte	1,1 MB/s	4,7 MB/s	4,7 MB/s	4,7 MB/s	1,1 MB/s	3,9 MB/s	3,9 MB/s	3,9 MB/s
Bulk encryption 64 Kbyte	1,1 MB/s	4,7 MB/s	4,7 MB/s	4,7 MB/s	1,1 MB/s	4,3 MB/s	4,3 MB/s	4,3 MB/s
AES 256 bit								
Key generation	460 / s	460 / s	460 / s	460 / s	460 / s	460 / s	460 / s	460 / s
Encryption 128 byte	1000 / s	4100 / s	4100 / s	4100 / s	1000 / s	2800 / s	2800 / s	2800 / s
Encryption 512 byte	1000 / s	3200 / s	3200 / s	3200 / s	1000 / s	2200 / s	2200 / s	2200 / s
Bulk encryption 8 Kbyte	1,1 MB/s	4,7 MB/s	4,7 MB/s	4,7 MB/s	1,1 MB/s	3,8 MB/s	3,8 MB/s	3,8 MB/s
Bulk encryption 64 Kbyte	1,1 MB/s	4,7 MB/s	4,7 MB/s	4,7 MB/s	1,1 MB/s	4,2 MB/s	4,2 MB/s	4,2 MB/s



SecurityServer Se-Series Gen2 LAN V5 Benchmarks (PKCS#11 R2)

4 Asymmetric algorithm: RSA 1024, 2048, 3072 and 4096 bit key sizes

RSA		Se12 PCIe	Se52 PCIe	Se500 PCIe	Se1500 PCIe	Se12 LAN	Se52 LAN	Se500 LAN	Se1500 LAN
Key generation 1024 bit		1,8 / s	8,4 / s	11,0 / s	12,0 / s	1,8 / s	8,4 / s	11,0 / s	11,0 / s
Key generation 2048 bit		0,2 / s	1,0 / s	3,5 / s	4,2 / s	0,2 / s	1,0 / s	3,5 / s	4,2 / s
Key generation 3072 bit		0,05 / s	0,3 / s	0,8 / s	1,0 / s	0,05 / s	0,3 / s	0,8 / s	1,0 / s
Key generation 4096 bit		0,02 / s	0,1 / s	0,3 / s	0,5 / s	0,02 / s	0,1 / s	0,3 / s	0,5 / s
Signature generation 1024 bit	Single signing Bulk signing	100 / s 105 / s	450 / s 520 / s	1300 / s 6500 / s	1600 / s 9500 / s	100 / s 105 / s	420 / s 520 / s	1000 / s 6000 / s	1200 / s 8600 / s
Signature generation 2048 bit	Single signing Bulk signing	16 / s 16 / s	80 / s 85 / s	640 / s 2200 / s	900 / s 3500 / s	16 / s 16 / s	75 / s 80 / s	560 / s 2100 / s	750 / s 3300 / s
Signature generation 3072 bit	Single signing Bulk signing	5 / s 5 / s	26 / s 26 / s	160 / s 390 / s	260 / s 630 / s	5 / s 5 / s	25 / s 25 / s	160 / s 380 / s	250 / s 630 / s
Signature generation 4096 bit	Single signing Bulk signing	2 / s 2 / s	11 / s 11 / s	100 / s 230 / s	160 / s 370 / s	2 / s 2 / s	11 / s 11 / s	100 / s 220 / s	150 / s 370 / s
Signature verification 1024 bit		800 / s	2300 / s	1600 / s	2000 / s	800 / s	1600 / s	1300 / s	1600 / s
Signature verification 2048 bit		390 / s	1400 / s	1100 / s	1500 / s	390 / s	1100 / s	1000 / s	1200 / s
Signature verification 3072 bit		210 / s	850 / s	850 / s	1200 / s	210 / s	750 / s	800 / s	1000 / s
Signature verification 4096 bit		130 / s	560 / s	650 / s	920 / s	130 / s	500 / s	600 / s	800 / s



SecurityServer Se-Series Gen2 LAN V5 Benchmarks (PKCS#11 R2)

5 Asymmetric algorithm: Elliptic Curves secp224r1, secp256r1, secp384r1 and secp521r1

Elliptic Curve		Se12 PCIe	Se52 PCIe	Se500 PCIe	Se1500 PCIe	Se12 LAN	Se52 LAN	Se500 LAN	Se1500 LAN
Key generation secp224r1		45 / s	200 / s	230 / s	260 / s	33 / s	190 / s	220 / s	250 / s
Key generation secp256r1		26 / s	170 / s	240 / s	270 / s	26 / s	160 / s	230 / s	260 / s
Key generation secp384r1		11 / s	85 / s	150 / s	170 / s	11 / s	85 / s	140 / s	160 / s
Key generation secp521r1		5 / s	40 / s	75 / s	90 / s	5 / s	40 / s	75 / s	80 / s
Signature generation secp224r1	Single signing Bulk signing	140 / s 160 / s	860 / s 1300 / s	1200 / s 2200 / s	1400 / s 3300 / s	140 / s 160 / s	740 / s 1300 / s	940 / s 2000 / s	1100 / s 3200 / s
Signature generation secp256r1	Single signing Bulk signing	115 / s 130 / s	760 / s 1100 / s	1300 / s 2500 / s	1500 / s 3800 / s	115 / s 130 / s	650 / s 1100 / s	1000 / s 2400 / s	1200 / s 3700 / s
Signature generation secp384r1	Single signing Bulk signing	50 / s 50 / s	400 / s 480 / s	900 / s 1500 / s	1100 / s 2300 / s	50 / s 50 / s	370 / s 480 / s	780 / s 1500 / s	940 / s 2300 / s
Signature generation secp521r1	Single signing Bulk signing	22 / s 22 / s	200 / s 220 / s	500 / s 730 / s	650 / s 1200 / s	22 / s 22 / s	180 / s 220 / s	480 / s 710 / s	620 / s 1100 / s
Signature verification secp224r1		60 / s	390 / s	500 / s	580 / s	60 / s	360 / s	450 / s	540 / s
Signature verification secp256r1		45 / s	320 / s	560 / s	680 / s	45 / s	300 / s	500 / s	610 / s
Signature verification secp384r1		20 / s	150 / s	360 / s	420 / s	20 / s	150 / s	330 / s	400 / s
Signature verification secp521r1		9 / s	70 / s	180 / s	210 / s	9 / s	70 / s	170 / s	210 / s