1 General Performance Tests

The general performance tests are all measured inside the CryptoServer with a special benchmark firmware module.

Command/Action	CryptoServer CS10	CryptoServer CS50
(1) Maximum number of Commands per second	1000	18000
(2) TDES Throughput ECB	1.95 MBytes/sec.	8.8 MBytes/sec.
(3) TDES Throughput CBC	1.95 MBytes/sec.	8.75 MBytes/sec
(4) AES, 16 Bytes Key, ECB	7.28 MBytes/sec.	54.25 MBytes/sec
(5) AES, 16 Bytes Key, CBC	7.15 MBytes/sec.	52.11 MBytes/sec
(6) AES, 32 Bytes Key, ECB	6.93 MBytes/Sek.	41.05 MBytes/sec
(7) AES, 32 Bytes Key, CBC	6.87 MBytes/sec.	39.57 MBytes/sec
(8) RSA Verify, 1024 Bit	2.5 ms	0.1 ms
(9) RSA Sign, 1024 Bit	105 signatures/second	540 signatures/second
(10) RSA Sign, 2048 Bit	16 signatures/second	83 signatures/second
(11) RSA Key Generation 1024 Bit	450 ms (average)	100 ms (average)
(12) RSA Key Generation 2048 Bit	3,8 sec (average)	870 ms (average)
(13) Generation of high quality (“true”) random numbers	8.7 kBytes/sec	8.7 kBytes/sec
(14) Generation of pseudo random numbers	15.8 MBytes/sec	15.8 MBytes/sec
(15) SHA-1 Hash	65 MBytes/sec	65 MBytes/sec
(16) SHA-512 Hash	9.2 MBytes/sec	9.2 MBytes/sec
(17) RIPEMD-160 Hash	66 MBytes/sec	66 MBytes/sec
(18) ECDSA Sign, 160 Bit	220 signatures/second.	2200 signatures/second.
(19) ECDSA Sign, 256 Bit	110 signatures/second.	1170 signatures/second.

Details:

to (1): The theoretical maximal amount of commands per second (sequential).

to (8): RSA encryption with public key (as used for encryption of secret data)

to (9)+(10): RSA encryption with private key (i. e. as used for signatures), using Short-Cut algorithm (Chinese Remainder Theorem).

to (13): True random number generator (TRNG), where the “output” of a hardware noise generator is mathematically post-processed and online-tested to guarantee the quality of the generated random numbers.
In the sense of the BSI specification AIS 31, http://www.bsi.de/zertifiz/zert/interpr/ais31e.pdf, this TRNG belongs to (the highest possible) class P2.

to (14): The CryptoServer pseudo random number generator (PRNG) is implemented according to FIPS 186-2, Appendix 3, and complies to ANSI X9.31, Appendices A.2.1. and A.2.2. It uses the SHA-1 hash algorithm as internal transition function. In the sense of the BSI specification AIS 20,

http://www.bsi.de/zertifiz/zert/interpr/ais20e.pdf, this PRNG belongs to (the highest possible) class K4. It can be used for generation of session keys, padding bits, etc.

2 Performance of the CSI – API

In this chapter the performance of the CSI interface of the CryptoServer is shown. The host system used for testing was a 3.00 GHz Pentium 4 System with 2 GB RAM running Microsoft Windows XP Professional SP2. The source code performing these benchmarks is provided within the csi_demo.c file on the SecurityServer Product CD.

2.1 DES

Function	Calls/sec
CS 50 PCI card	
Key Generation (16 Bytes)	672
Key Generation (24 Bytes)	450
3DES Encipher of 8 Bytes	15857
3DES Encipher of 64 Bytes	12807
3DES Encipher of 1024 Bytes	5842
3DES Encipher of 1 MBytes	4
CS 50 LAN	
Key Generation (16 Bytes)	542
Key Generation (24 Bytes)	418
3DES Encipher of 8 Bytes	2205
3DES Encipher of 64 Bytes	2130
3DES Encipher of 1024 Bytes	1330
3DES Encipher of 1 MBytes	3.4
CS 10 PCI card	
Key Generation (16 Bytes)	673
Key Generation (24 Bytes)	453
3DES Encipher of 8 Bytes	1000
3DES Encipher of 64 Bytes	1000
3DES Encipher of 1024 Bytes	1000
3DES Encipher of 1 MBytes	1,5
CS 10 LAN	
Key Generation (16 Bytes)	529
Key Generation (24 Bytes)	418
3DES Encipher of 8 Bytes	1000
3DES Encipher of 64 Bytes	1000
3DES Encipher of 1024 Bytes	888
3DES Encipher of 1 MBytes	1.4

2.2 RSA

Function	Calls/sec
CS 50 PCI card	
Keypair generation (512 Bits)	52
Keypair generation (1024 Bits)	12
Keypair generation (2048 Bits)	1.3
Keypair generation (4096 Bits)	0.1
Sign (1024 bit keys)	266
CS 50 LAN	
Keypair generation (512 Bits)	48
Keypair generation (1024 Bits)	9.5
Keypair generation (2048 Bits)	1.2
Keypair generation (4096 Bits)	0.1
Sign (1024 bit keys)	235
CS 10 PCI card	
Keypair generation (512 Bits)	9.2
Keypair generation (1024 Bits)	2.5
Keypair generation (2048 Bits)	0.16
Keypair generation (4096 Bits)	0.015
Sign (1024 bit keys)	86.5
CS 10 LAN	
Keypair generation (512 Bits)	11.3
Keypair generation (1024 Bits)	2.6
Keypair generation (2048 Bits)	0.21
Keypair generation (4096 Bits)	0.015
Sign (1024 bit keys)	83.4

2.3 AES

Function	Calls/sec
CS 50 PCI card	
Key Generation (16 Bytes)	673
Key Generation (24 Bytes)	450
Key Generation (32 Bytes)	336
AES Encipher (16 Bytes) of 16 Bytes	12807
AES Encipher (16 Bytes) of 64 Bytes	12807
AES Encipher (16 Bytes) of 1024 Bytes	5842
AES Encipher (16 Bytes) of 1 MByte	7.1
CS 50 LAN	
Key Generation (16 Bytes)	476
Key Generation (24 Bytes)	418
Key Generation (32 Bytes)	312
AES Encipher (16 Bytes) of 16 Bytes	2286
AES Encipher (16 Bytes) of 64 Bytes	2130
AES Encipher (16 Bytes) of 1024 Bytes	1558
AES Encipher (16 Bytes) of 1 MByte	5.3
CS 10 PCI card	
Key Generation (16 Bytes)	673
Key Generation (24 Bytes)	450
Key Generation (32 Bytes)	336
AES Encipher (16 Bytes) of 16 Bytes	1000
AES Encipher (16 Bytes) of 64 Bytes	1000
AES Encipher (16 Bytes) of 1024 Bytes	1000
AES Encipher (16 Bytes) of 1 MByte	3,7
CS 10 LAN	
Key Generation (16 Bytes)	525
Key Generation (24 Bytes)	417
Key Generation (32 Bytes)	312
AES Encipher (16 Bytes) of 16 Bytes	1000
AES Encipher (16 Bytes) of 64 Bytes	1000
AES Encipher (16 Bytes) of 1024 Bytes	1000
AES Encipher (16 Bytes) of 1 MByte	3.1