



16-Bit Security Controller with Memory Management and Protection Unit

32-Kbytes EEPROM

1100-Bit Advanced Crypto Engine

112-Bit / 192-Bit DDES-EC2 Accelerator

dKey is a SATA HTS security solution based on a cryptographic token equipped with a smartcard reader.

The token has a standard chip which manages RSA public and private key.
The token has both the function of encryption chip and smartcard reader.

The encryption chip consists of a microprocessor which elaborates the RSA algorithm (up to 2048 bit).

The encryption is performed by dedicated APIs as PKCS#11 and Microsoft CAPI.

The device is also available with integrated flash memory (**dKey Flash**, 512MB up to 4GB).



Specification:

- Full-speed USB 2.0 host interface (transmission rate up to 12 Mbps)
- CCID compliant for easy plug & play (no additional USB driver is required if operating system supports CCID)
- PC/SC drivers are available for all major operating systems

Certification:

- Microsoft WHQL2 - EMV3 2000 Level 1
- ISO 7816
- HBCI

Operating System:

- Windows® 98/Me/2000/XP/CE 3.0/CE.NET (depending on hardware)/Vista
- Linux®
- Mac® OS X

DKEY are compliant with all relevant smart card standards, offering highest interoperability and excellent performance. Regardless of whether high speed serial, USB connectivity is required.

16-Bit Security Controller with MMU - 32-Kbyte EEPROM 1100-Bit ACE and 112-Bit / 192-Bit DDES-EC2 Accelerator

Features

- 16-bit microcomputer in 0.22 μm CMOS technology
- Instruction set opcode compatible with standard SAB 8051 processor
- Enhanced 16-bit arithmetic
- Additional powerful instructions optimized for chip card applications
- Dedicated, non-standard architecture with **execution time 6 times faster (18 times by PLLmax)** than standard SAB 8051 processor at same external clock
- **134 Kbytes User ROM** for application programs
- Additional 2 Kbytes reserved ROM for Resource Management System (RMS+ Superslim) with intelligent E² write/erase routines
- **32 Kbytes Superslim-EEPROM**
- **4Kbytes XRAM**, 256 bytes internal RAM, 700 bytes Crypto RAM.
- **Memory Management and Protection Unit (MMU)**
- **Dual Key Triple DES (DDES) and EC2 GF (2n) Accelerator**
- **Advanced Crypto Engine for up to 2048 bit RSA computation**
- **Certified RSA 2048 library** available (refer to product brief)
- CRC Module
- Interrupt Module
- **PLL** up to 15 MHz
- Two 16-bit Autoreload Timer
- Power saving sleep mode
- **Ext. Clock freq. 1 to 7.5 MHz for int. Clock £ 15 MHz @ 2.7V-5.5V**
Ext. Clock freq. 1 to 5 MHz for int. Clock
£ 11 MHz @ 1.62V-5.5V
- **UART for handling serial interface** in accordance with ISO/IEC 7816 part 3

supporting transmission protocols T=1 and T=0

- I/O routines realized in software executable
- Supply voltage range: 1.62 to 5.5 V
- Current consumption
< 10 mA @ 5.5 V
< 6 mA @ 3.3 V
< 4 mA @ 1.98 V
- Temperature range: -25 to +85°C
- ESD larger than 6 kV

Superslim-EEPROM

- Reading and programming byte by byte
- Flexible page mode for 1 to 64 bytes write/erase operation
- 32 bytes security area (OTP)
- Fast personalization mode 0.63 ms @15MHz
- Erase + Write time < 4.0 ms @15MHz
- **Minimum of 500.000 write/erase cycles at 25°C**
- Data retention for a minimum of 10 years
- EEPROM programming voltage generated on chip

Memory Management and Protection Unit

- Addressable memory up to 1 MByte
- Separates OS (system mode) and application (user mode)
- System routines called by traps
- OS can restrict access to peripherals in application mode
- Code execution from XRAM possible

Security Features

Operation state monitoring mechanism

- Low and high voltage sensors

- Frequency sensors and filters
- Light Sensor
- Glitch Sensor
- Temperature Sensor
- Life Test Function for Sensors

Testmode

- Irreversible Lock - Out of testmode

Anti Snooping

- HW-countermeasures against SPA/DPA-, Timing- and DFA-attacks (differential fault analysis – DFA)
- CRC – Module
- Non standard dedicated Smart Card CPU – Core
- Active Shield with automatic and user controlled attack detection

Support

- HW-& SW-Tools (Emulator, ROM Monitor, Card Emulator, Simulator, Softmasking)
- Application notes

Supported Standards

- ISO/IEC 7816
- EMV 2000
- GSM 11.11, 11.12, 11.18
- ETS I TS 102 221

Memory Security

- 16 bytes security PROM, hardware protected
- Unique chip identification number for each chip
- MED - memory encryption/decryption device for XRAM, ROM and EEPROM
- True Random Number Generator with Firmware test function
- Security optimised layout and layout scrambling

Performance Advanced Crypto Engine

Operation	Modulus	Exponent	Calculation Time		
			5MHz	10MHz	15MHz
Modular Exponentiation RSA Encrypt / RSA Signature Verify	1024 bit 2048 bit	17 bit 17 bit	20 ms 630 ms	11 ms 315 ms	7 ms 210 ms
Modular Exponentiation RSA Decrypt / RSA Signature Generate	1024 bit	1024 bit	820 ms	410 ms	273 ms
Modular Exponentiation using CRT RSA Decrypt / RSA Signature Generate	eq. 1024 bit eq. 2048 bit	eq. 1024 bit eq. 2048 bit	250 ms 1840 ms	125 ms 920 ms	83 ms 614 ms
DSA Signature Generate	512 bit	160 bit	97 ms	49 ms	32 ms
DSA Signature Verify	512 bit	160 bit	117 ms	59 ms	39 ms
DSA Signature Generate	1024 bit	160 bit	438 ms	219 ms	146 ms
DSA Signature Verify	1024 bit	160 bit	711 ms	356 ms	237 ms

Performance DDES-EC2 Accelerator

Operation	Data Block Length	Encryption Time for an 8-Byte Block incl. Data Transfer		
		5MHz	10MHz	15MHz
56-bit Single DES Encryption	64 bit	23 μ s	11 μ s	8 μ s
112-bit Triple DES Encryption	64 bit	35 μ s	17 μ s	12 μ s
	Operand Length	Calculation Time		
		5MHz	10MHz	15MHz
Elliptic Curves GF(2n) EC-DSA Signature Generate	192 bit	285 ms	142 ms	95 ms
Elliptic Curves GF(2n) EC-DSA Signature Verify	192 bit	540 ms	270 ms	180 ms

Important: Further information is confidential and on request. Please contact:

Sata HTS Hi-Tech Services SpA in Udine, Italy,

Tel +39 - (0)432 499860

Fax +39 - (0)0432 499831

E-Mail: info@sata-hts.com

Published by Sata HTS Hi-Tech Services SpA,

Via Sinalunga 57, I-00138 Roma

© Sata HTS Hi-Tech Services SpA 2007

All Rights Reserved.

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.