NXP MIFARE SAM™ AV2

Embed security in your smart card system

The NXP MIFARE SAM™ AV2 hardware solution is the ideal add-on for reader devices offering additional security services. Supporting TDEA, AES and RSA capabilities, it offers secure storage and secure communication in a variety of infrastructures.

Key benefits

- Secure storage of keys in hardware
- Simpler reader design
- Improved application performance with direct connection to reader IC

Key features

- Supports MIFARE Ultralight™, MIFARE Ultralight™ C, MIFARE 1 K, MIFARE 4 K, MIFARE Plus™, MIFARE DESFire™, MIFARE DESFire™ EV1
- Supports MIFARE Crypto1™, TDEA (Triple DES encryption algorithm), RSA and AES cryptography
- Simultaneous multiple card support (up to 4 parallel sessions)
- Flexible key diversification options
- Secure download and storage of keys
- 128 key entries for symmetric cryptography and 3 RSA key entries for asymmetric cryptography
- Support ISO 7816 baud rates
- Support high speed baud rates up to 1.5 Mbit/s
- Available in wafer, PCM 1.1 module, or HVQFN package

Applications

- Public transport
- Access management
- Loyalty programs
- Micro payment

The NXP MIFARE SAM AV2 solution lets developers of smart card applications meet the needs of ever-changing security standards.

Unlike other products in the field, MIFARE SAM AV2 has proven interoperability with all of NXP's broad card portfolio, (MIFARE Ultralight, MIFARE Ultralight C, MIFARE 1 K, MIFARE 4 K, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1 and SmartMX solutions), making it the most versatile and secure SAM solution on the market today.

Secured communication

When used in combination with a reader IC supporting innovative "X" features, MIFARE SAM AV2 provides a significant boost in performance to the reader along with faster communication between reader and module. The "X" feature is a new way to use the SAM in a system, with SAM connected to the microcontroller and the reader IC simultaneously.
The connection between the SAM and the reader is performed

NXP founded by Philips

using security protocols based on either symmetric cryptography (TDEA and AES) or PKI RSA asymmetric cryptography. The protocols comply with the state-of-art standards and thereby ensure data confidentiality and integrity.

The MIFARE SAM AV2 solution offers the following functionality :

- Up to four logical channels; simultaneous multiple card support
- Support for DESFire and MIFARE Plus authentication (with related secure messaging and session key generation)
- Secure Host ↔ SAM and back end ↔ SAM communication with symmetric cryptography 3 pass authentication for confidentiality and integrity
- Secure Host ↔ SAM and back end ↔ SAM communication with RSA based cryptography
- TDEA and AES based key diversification
- Secure storage and updating of keys (key usage counters)
- Offline cryptography
- RSA cryptography
- True random number generator (TRNG)

The MIFARE pedigree

NXP MIFARE is the leading technology platform for contactless ticket, card, and reader solutions. It is a proven and reliable technology that represents the largest installed based worldwide, with more than 20 million core reader components, 1 billion cards, and 800 million smart tickets sold.

Compliant with the ISO 14443A international standard, MIFARE ensures that today's infrastructure can easily be upgraded. It lets service providers expand their transportation networks and integrate additional services – such as payment systems for taxi fares, cinema and theatre tickets, loyalty programs, access management and parking – while reducing the total costs of operations.

MIFARE evolves. NXP's latest innovations in MIFARE such as the MIFARE Ultralight C, MIFARE Plus and MIFARE DESFire EV1, bring your application to the next level of security, performance and convenience.

Product features	MIFARE SAM AV2
Memory	
EEPROM size [byte]	80 K
Write endurance [cycles]	up to 500.000
Data retention [years]	up to 25
Organization	128 key entries for symmetric cryptography and 3 RSA key entries for PKI cryptography
RF-Interface	
Acc. to ISO 14443A	ISO 7816, T=1
Frequency [MHz]	1 to 10
Baud rate [kbit/s]	9.6 to 1500
Security	
SHA-1, SHA-224, SHA-256	For hash computation and RSA signature support
Unique serial number [bytes]	7
Random number generator	Yes
Access keys	128 symmetric key entries, 3 RSA key entries, 16 key usage counters
MIFARE Classic security	Supported
DES & TDEA security	MACing / Encipherment / SAM communication / Offline cryptography
AES 128 / AES 192	MACing / Encipherment / SAM communication / Offline cryptography
RSA cryptography	Signature generation and verification, RSA decryption for symmetric key updates
Packaging	
Delivery type: wafer	P5DF081UA
Delivery type: PCM1.1 module	P5DF081X0
Delivery type: HVQFN32	P5DF081HN
Connection	
X-functionality	Yes

MIFARE.net

www.nxp.com

founded by PHILIPS

Date of release: October 2009
Document order number: 9397 750 16829
Printed in the Netherlands