NXP®
MIFARE SAM AV2

Embed security in your contactless system

The 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 FEATURES

- Supports MIFARE Ultralight® C, MIFARE Classic®, MIFARE Plus®, MIFARE® DESFire®, MIFARE® DESFire® EV1 (MIFARE Plus® EV1 and MIFARE® DESFire® EV2 are supported in backward compatible mode)
- Supports Crypto1, TDEA (Triple DES encryption algorithm), AES and RSA 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
- Supports ISO 7816 baud rates
- Supports high speed baud rates up to 1.5 Mbit/s
- X-mode interface connecting SAM directly with NXP reader IC
- Available in wafer, PCM 1.1 module, or HVQFN package

TARGET APPLICATIONS

- Public transport
- Access management
- Loyalty programs
- Micropayment

KEY BENEFITS

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

The 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 NXP's contactless IC portfolio, making it a versatile and secure SAM solution.

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 the SAM connected to the microcontroller and the reader IC simultaneously.

The connection between the SAM and the reader is performed 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 FUNCTIONALITIES:

- Up to four logical channels; simultaneous multiple card support
- Support for MIFARE 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)

FEATURES

Product features	MIFARE SAM AV2
Memory	
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

ORDERING INFORMATION

Packaging	MIFARE SAM AV2
Delivery type: Wafer	P5DF081UA
Delivery type: PCM1.1 module	P5DF081X0
Delivery type: HVQFN32	P5DF081HN

www.nxp.com

Date of release: June 2018
Document Number: MIFARESAMAV2 REV0

www.MIFARE.net