NXP®
MIFARE SAM AV3

Secure your IoT connections by enhancing cryptographic performance in devices

This third-generation MIFARE Secure Access Module (SAM), designed for flexible performance in today's IoT, secures keys and protects assets. It offers built-in support for MIFARE ICs and NXP's "DNA" range of products from the NTAG, ICODE, and UCODE families. It is an ideal add-on for edge computing nodes and end nodes such as reader and POS terminals, toll gates, and door locks.

KEY FEATURES

▶ Compatible with MIFARE SAM AV2

▶ Supports latest security features of MIFARE® DESFire® EV2, MIFARE Plus® EV1, and MIFARE Ultralight® EV1

▶ Supports UCODE® DNA, ICODE® DNA, and NTAG® DNA

▶ Supports Crypto 1, TDEA (112, 168), AES (128, 192, 256), RSA, and ECC

▶ Flexible key diversification

▶ Secure download and storage of keys

▶ 128 key entries for symmetric cryptography, 3 key entries for RSA, and 8 key entries for ECC asymmetric cryptography

▶ Programmable functionality for customized commands and logic

▶ ISO/IEC 7816 interface with extended baud rates up to 1.5 Mbit/s

▶ I²C slave host interface in HVQFN package only

▶ X-mode for direct pass through connection with NXP reader IC

▶ Common Criteria EAL6+ (HW) + Security Certification for MIFARE (SW)

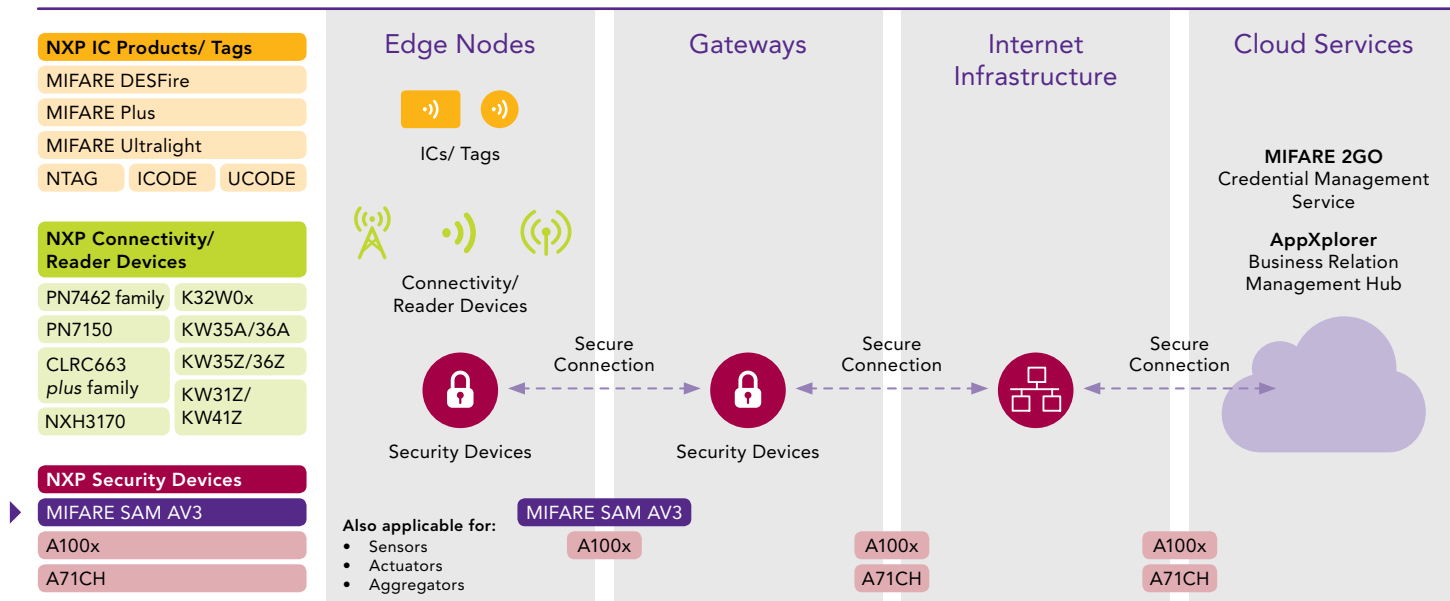▶ Available in wafer, PCM 1.5 module, or HVQFN package

TARGET APPLICATIONS

▶ Public transport

▶ Access management

▶ Loyalty programs

▶ Micropayment

▶ Road tolling

▶ Electronic vehicle identification

▶ Originality and security protection for IoT devices

KEY BENEFITS

▶ Strongest protection of highly sensitive keys (e.g. Master Keys)

▶ Faster, leaner design of edge computing nodes

▶ Higher application performance in direct pass through X-mode

▶ Customizable flow, executable with one command

IoT Architecture and NXP Solutions

NXP IC Products/ Tags		
MIFARE DESFire		
MIFARE Plus		
MIFARE Ultralight		
NTAG	ICODE	UCODE

NXP Connectivity/ Reader Devices	
PN7462 family	K32W0x
PN7150	KW35A/36A
CLRC663 *plus* family	KW35Z/36Z
	KW31Z/
NXH3170	KW41Z

NXP Security Devices
▶ MIFARE SAM AV3
A100x
A71CH

Edge Nodes

ICs/ Tags

Connectivity/ Reader Devices

Security Devices

Also applicable for:
- Sensors
- Actuators
- Aggregators

MIFARE SAM AV3
A100x

Secure Connection

Gateways

Security Devices

A100x
A71CH

Secure Connection

Internet Infrastructure

A100x
A71CH

Secure Connection

Cloud Services

MIFARE 2GO
Credential Management Service

AppXplorer
Business Relation Management Hub

The MIFARE SAM architecture, now in its third generation, extends functionality to include support for NXP's DNA range of the NTAG, ICODE, and UCODE families beyond MIFARE ICs. Optimized for use with the product types in these families that offer Transaction Message Authentication Codes (TMACs), the MIFARE SAM AV3 secures keys and protects assets in the latest IoT applications.

The MIFARE SAM AV3 raises the bar on flexibility by supporting programmable logic, too, so you can integrate a proprietary algorithm for key diversification or implement a full business flow that executes with just one call. Support for programmable logic also lets you develop your own code while re-using the intrinsic cryptography functions of the MIFARE SAM AV3.

To simplify the development of customized logic – a process that requires eligibility, tool investment, and specialized skills – NXP partners with design houses that offer code development and other services tailored to the MIFARE SAM AV3.

The MIFARE SAM AV3 offers an easy way to add security to all of today's more important IoT applications, and helps to create faster, leaner designs of edge computing nodes.

The efficient X-mode configuration allows direct communication with RF-frontend ICs without using the SAM as a cryptographic coprocessor to achieve higher application performance.

Taken as a whole, the flexibility and simplicity features of the MIFARE SAM AV3 make it an ideal choice for securing IoT connections.

FEATURES

Product features	MIFARE SAM AV3
Memory	
Number of symmetric key entries	128
Number of asymmetric key entries	3 RSA 8 ECC 24 EMV CA
Interfaces	
ISO/IEC 7816	T=1 protocol for contact communication, 9.6 up to 1500 kbit/s data throughput
I^{2}C host interface (in HVQFN package only)	Supports fast mode up to 400 kbit/s
Security	
Symmetric crypto	Crypto 1, TDEA-64-128-169, AES-128-192-256
Asymmetric crypto	RSA (2048 bits), ECC (256 bits)

ORDERING INFORMATION

Packaging	Part Type
Delivery type: wafer	MF4SAM3U15
Delivery type: PCM 1.5 module	MF4SAM3X84
Delivery type: HVQFN32	MF4SAM3HN

www.MIFARE.net