AN10957

Generic Access Control Data Model

Rev. 1.1 — 7 March 2011 | Application note
196811 | Public

Document information

Info	Content
Keywords	MIFARE Plus, MIFARE DESFire EV1, MIFARE SAM AV2, SmartMX
Abstract	This application note provides a generic approach for physical access control applications.

Revision history

Rev	Date	Description
1.1	20110307	More clarification added.
1.0	20100701	Initial version.

Contact information

For additional information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. Introduction

1.1 Scope

This application note achieves a common data model that can be supported across card and reader manufacturers to provide interoperability between the card and reader on a physical access system.

1.2 Applicable Products

Contact and contactless PCD and PICC devices

1.3 Abbreviations

The following table lists abbreviations used throughout this document**.**

Table 1. Abbreviations

Abbreviations	Meaning
APDU	Application protocol data unit
ATR	Answer to reset
BCD	Binary Coded Decimal
ASCIIZ	ASCII zero delimited string
APPMK	Application Master Key
APPVK	Application Validation Key
OCPSK	Originality Cloning Protection System Key
PACS	Physical Access Control System
IV	Initial Vector?
CMAC	Cipher based Message Authentication Code
RID	Random IDentifier
UID	Unique IDentifier
P1-P2	Parameter bytes (inserted for clarity, the dash is not significant)
PCD	Proximity coupling device
PICC	Proximity integrated circuit card
RFU	Reserved for future use
SW1-SW2	Status bytes (inserted for clarity, the dash is not significant)
TLV	Tag, Length, Value
VCD	Vicinity coupling device
VICC	Vicinity IC card

2. Card Definition

The card application shall be defined as an application that contains two objects, the card identifier object and the PACS data object, depends on the technology used, they can be two different files or sectors. In case of file structure, file Id 0x01 and 0x02 shall be used respectively and of sector structure, MAD (MIFARE Application Directory) shall be used.

The application identifier shall be 0xf532fN, where the default value of N is 0. in case of multiple applications/sites, other values of N (‘1’ to ‘F’) can be used. The implementation in terminal (either locked to one application or scanning the card for the right application) is out of the scope of this application note. Each site shall have the ability to use different keys for that site and therefore allow for site independence.

The card setting should allow scanning the application identifier installed in the card.

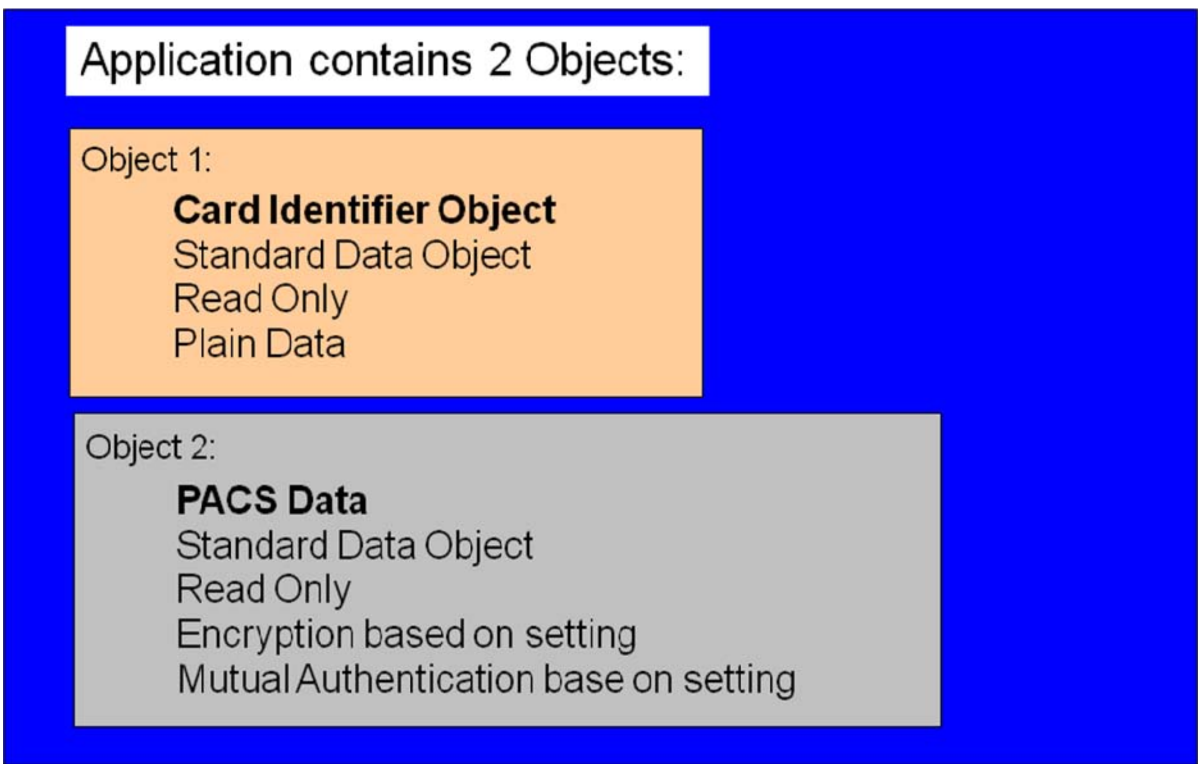


Fig 1. Card Definition

3.Data Model

3.1 PACS Data Object

The PACS data object contains a standard implementation for physical access control. This data object will be populated during card personalization and locked before issuance. All data fields must be present in the object but optional fields are not required to be populated. The encryption method used on the data is defined in the Card Identifier Object.

Any optional value if not used, shall be set to 0 (RFU).

Table 2. PACS Data Object

Field Name	Field Type	Length (Bytes)	Mandatory Optional
Version – Major	Binary	1	Mandatory
Version – Minor	Binary	1	Mandatory
Customer / Site Code	BCD	5	Mandatory
Credential ID	BCD	8	Mandatory
Reissue Code	BCD	1	Optional
PIN Code	BCD	4	Optional
Customer Specific Data	Binary	20	Optional
Digital Signature	Binary	8	Mandatory

3.1.1 Version – Major

Field Type – Binary data

Length – 1 byte

Mandatory

Usage – This field is used for the major version number of the data model. This value shall be set to 0x01.

3.1.2 Version – Minor

Field Type – Binary data

Length – 1 byte

Mandatory

Usage – This field is used for the minor version number of the data model. This value shall be set to 0x00.

3.1.3 Customer / Site Code

Field Type – Binary Coded Decimal

Length – 5 bytes

Mandatory

Usage – This field contains a 10 digit numerical BCD data representation of the customer / site code.

Example – 0x0000001234 would represent a customer /site of 1234

3.1.4 Credential ID

Field Type – Binary Coded Decimal

Length – 8 bytes

Mandatory

Usage – This field contains a 16 digit numerical BCD data representation of the customer ID.

Example – 0x1122334455667788 would represent a customer ID of 1122334455667788

3.1.5 Reissue Code

Field Type – Binary Coded Decimal

Length – 1 byte

Optional

Usage – This optional field contains a 2 digit numerical BCD data representation of the reissue code.

Example – 0x01 would represent a reissue code of 01.

3.1.6 Pin Code

Field Type –Binary Coded Decimal

Length – 4 bytes

Optional

Usage – This field contains a 8 digit numerical BCD data representation of the pin code.

Example – 0x00001234 would represent a pin code of 00001234.

3.1.7 Customer Specific Data

Field Type – Binary

Length – 20 bytes

Optional

Usage -Customer Specific Data shall be a binary scratch pad defined by the end user. The data in this field will be customer specific.

Example – This is where a binary wiegand representation of the card information can be stored for the access control reader. The access control reader would be able to read this data and output the data without interpreting the data.

3.1.8 Digital Signature

Field Type – Binary

Length – 8 bytes

Mandatory

Usage - A cryptographic signature of all data in this object not including the digital signature. Please see Digital Signature section of this document.

3.2 Card Identifier Object

The card identifier object contains information that can be used in the discovery phase of the card.

Any optional value if not used, shall be set to 0 (RFU).

Table 3. Card Identifier Object

Field Name	Field Type	Length (Bytes)	Mandatory Optional
Manufacturer	ASCIIZ	16	Optional
Mutual Authentication Mode	Binary	2	Mandatory
Communication Encryption	Binary	1	Mandatory
Customer ID	BCD	4	Optional
Key Version	BCD	1	Optional
Digital Signature	Binary	8	Optional

3.2.1 Manufacturer

Field Type – ASCIIZ

Length – 16 bytes

Optional

Usage – This data field contains the ASCII representation of the Card Personalization / Manufacturer of the card. This can also be used to store the end user.

3.2.2 Mutual Authentication Mode

Field Type – Binary

22Length – 2 bytes

Mandatory

Usage – This data field contains 2 bytes consisting of several setting of the mutual authentication method. The first byte contains the Mutual Authentication type, Key Diversification algorithm, encryption Algorithm and if a random or unique Identifier is returned during anti-collision. Random or Unique ID will be important for key diversification. The second byte defines the key length. If bit seven is set, this signifies that the key length is proprietary. Bits 6 – 0 have an adder effect.

Example: 0xC103 signifies ISO-7816 Mutual Authentication, Unique ID, Standard ISO DES Algorithm, using a key length of 192 bits. Since each key in the DES operation is 8 bytes in length, this would signify 3 key triple DES. For 2 key triple DES, the value would be 128 bits.

Table 4. Mutual Authentication Mode Settings

Bit	Description
15	1 – ISO 7816-4 Authentication
	0 – Proprietary Authentication
14	1 – Standard ISO Algorithm
	0 – Proprietary
13	1 – Random ID returned during anti-collision
	0 – Unique ID returned during anti-collision
12	RFU - set to 0
11-10	10 – Key Diversification AES
	01 – Key Diversification DES
	00 – Key Diversification Proprietary
9 - 8	10 – Encryption AES
	01 – Encryption DES
	00 – Encryption Proprietary Algorithm
7	1 – Proprietary bit length
6	RFU – set to 0
5	RFU – set to 0
4	RFU – set to 0
3	1 - 512 bit
2	1 - 256 bit
1	1 - 128 bit
0	1 - 64 bit

3.2.3 Communication Encryption

Field Type – Binary

Length – 1 byte

Mandatory

Usage – This data field sets the security of the data streams for reading the data streams between the reader and the card

Table 5. Communication Encryption Settings

Value	Cryptographic Mode
0x00	Plain Communications
0x01	Plain Communications secured by CMAC
0x02	Fully Enciphered Communications
0xFF	Proprietary

3.2.4 Customer ID

Field Type – Binary Coded Decimal

Length – 4 bytes

Optional

Usage – This field contains a 8 digit numerical BCD data representation of the Customer ID.

Example – 0x00001234 would represent a Customer ID of 00001234.

3.2.5 Key Version

Field Type – Binary Coded Decimal

Length – 1 byte

Optional

Usage – This field contains a 2 digit numerical BCD data representation of the application verification key version.

Example – 0x01 would represent a key version of 01.

3.2.6 Digital Signature

Field Type – Binary

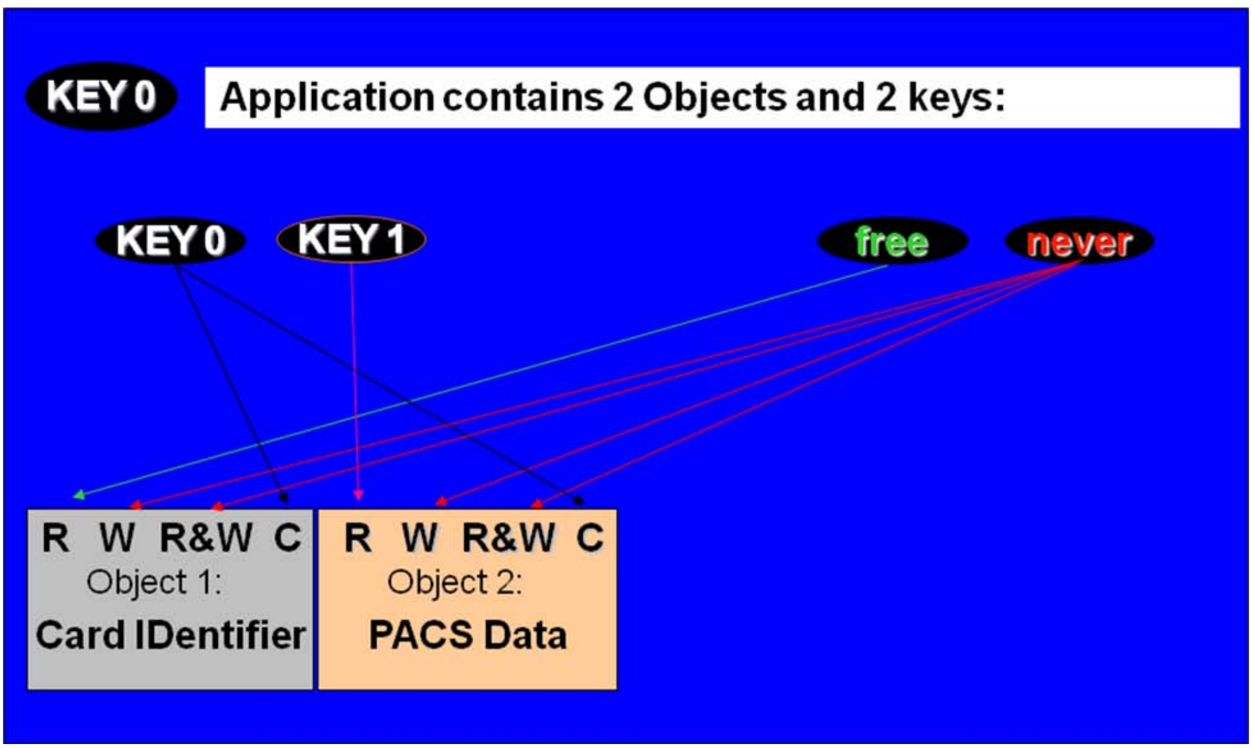
Length – 8 bytes

Optional

Usage - A cryptographic signature of all data in this object not including the digital signature. Please see Digital Signature section of this document.

4. Key Management

There shall be three basic keys per site that will be used with this application. Each key, except the general mutual authentication key, shall be diversified by the described algorithm in this document. The three keys shall be an Application Master key, application validation key, general mutual authentication key and a originality and cloning protection system key. If a random Identifier is returned during anti-collision, the application will have to query the card for a unique identifier after using the general mutual authentication key for authentication. The layout of the application and keys are illustrated below.



(1) Key 0 – Application Master Key

(2) Key 1 – Application Validation Key

Fig 2. Key Management Diagram

4.1 Application Master Key (APPMK – Key 0)

UID based diversified key that is stored on the card. The master key is stored on the backend system. This key is only used for personalization and administration of the data objects.

4.2 Application Validation Key (APPVK – Key 1)

UID based diversified key that is stored on the card. The master key is stored on the backend system. This key is only used for validation / authentication of the data objects.

4.3 Originality and cloning protection System Key (OCPSK)

UID based diversified key that is used for the calculation of the digital signature in each of the data objects. This key is not stored on the card.

4.4 General Mutual Authentication Key (GMAK)

This key is used for general mutual authentication when a random identifier method is used during anti-collision. Each card shall have a method to retrieve a unique, non changing identifier that shall be used for key diversification and originality check.

4.5 Key Diversification

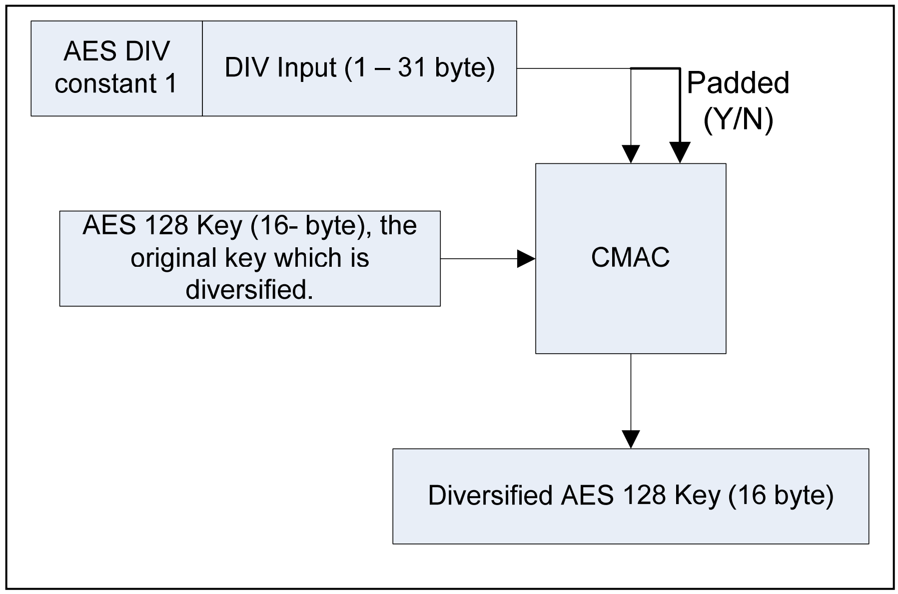
All keys, except the General Mutual Authentication Key (GMAK) shall be diversified, based on the UID of the card. Therefore, the secret keys are unique to every card in the system.

Key diversification mechanisms are explained in NXP application note “AN10922”, available at http://www.nxp.com/documents/application_note/AN10922.pdf

As the preferred crypto algorithm is AES-128, the AES-128 key diversification is explained once again in the following section using a different example.

4.5.1 Diversification of AES-128 keys

The following diagram shows the 16-byte AES key diversification scheme.



AES DIV constant 1: 0x01
DIV Input: Message with length of 31 bytes. This DIV input contains the AES DIV constant, UID of the card and padding, if necessary.

Example:

Secret Key : 0xf3f9377698707b688eaf84abe39e3791
UID : 0x04deadbeeffeed
Div Constant : 0x01

Step 1: Generate subkeys

Generate K0:
K0 = CIPHK(0b). Encrypt 0s using Secret Key.
Here K0 = 0x6704a3af8af3d920a0a7594f5cebf9fd

Generate K1:
If MSB(K0) = 0, then K1 = K0 << 1;
Else K1 = (K0 << 1) XOR 0x00000000000000000000000000000087;
Shift K0 one bit left. If Most Significant Bit of K0 is not 0, XOR shifted result with 0x00000000000000000000000000000087.
Here K1 = 0xce09475f15e7b241414eb29eb9d7f3fa

Generate K2:
If MSB(K1) = 0, then K2 = K1 << 1;
Else K2 = (K1 << 1) XOR 0x00000000000000000000000000000087.
Shift K1 one bit left. If Most Significant Bit of K1 is not 0 XOR shifted result with 0x00000000000000000000000000000087

Here K2 = 0x9c128ebe2bcf6482829d653d73afe773.

Step 2 : Create Div Input
Div Constant + UID + Padding
0x0104deadbeeffeed800000000000000000000000000000000000000000000000

Step 3 : XOR string
Since padding occurred, K2 will be XOR'd with Div Input
Result –
0x0104deadbeeffeed80000000000000009c128ebe2bcf6482829d653d73afe773

Step 4: Encrypt the above result with Secret Key
Result –
0x901789466c3d5fb6c885ab59139e132f0bb408baff98b6ee9f2e1585777f6a51

Step 5: Diversified Key would be the last 16 byte block (Block 2) of the encryption result.
Diversified key is 0x0bb408baff98b6ee9f2e1585777f6a51

5. Digital Signature / Originality Check

The signature of the data will be defined by a computed cryptographic message authentication coding (CMAC) that will authenticate that the data has not been altered or manipulated. The system will be able to compute the digital signature and compare it to the stored signature. The OCPSK key will only be known by the system and not stored on the card.

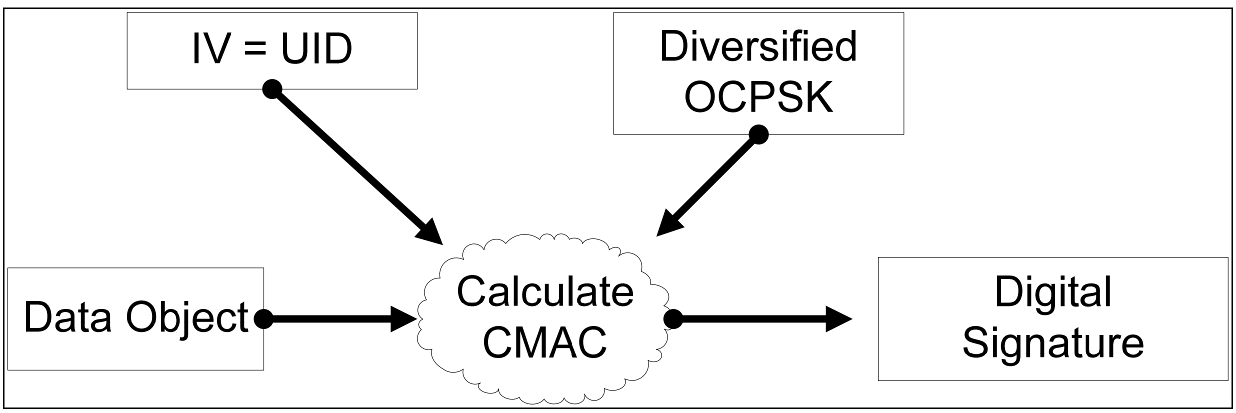


Fig 3. Digital Signature / Originality Check

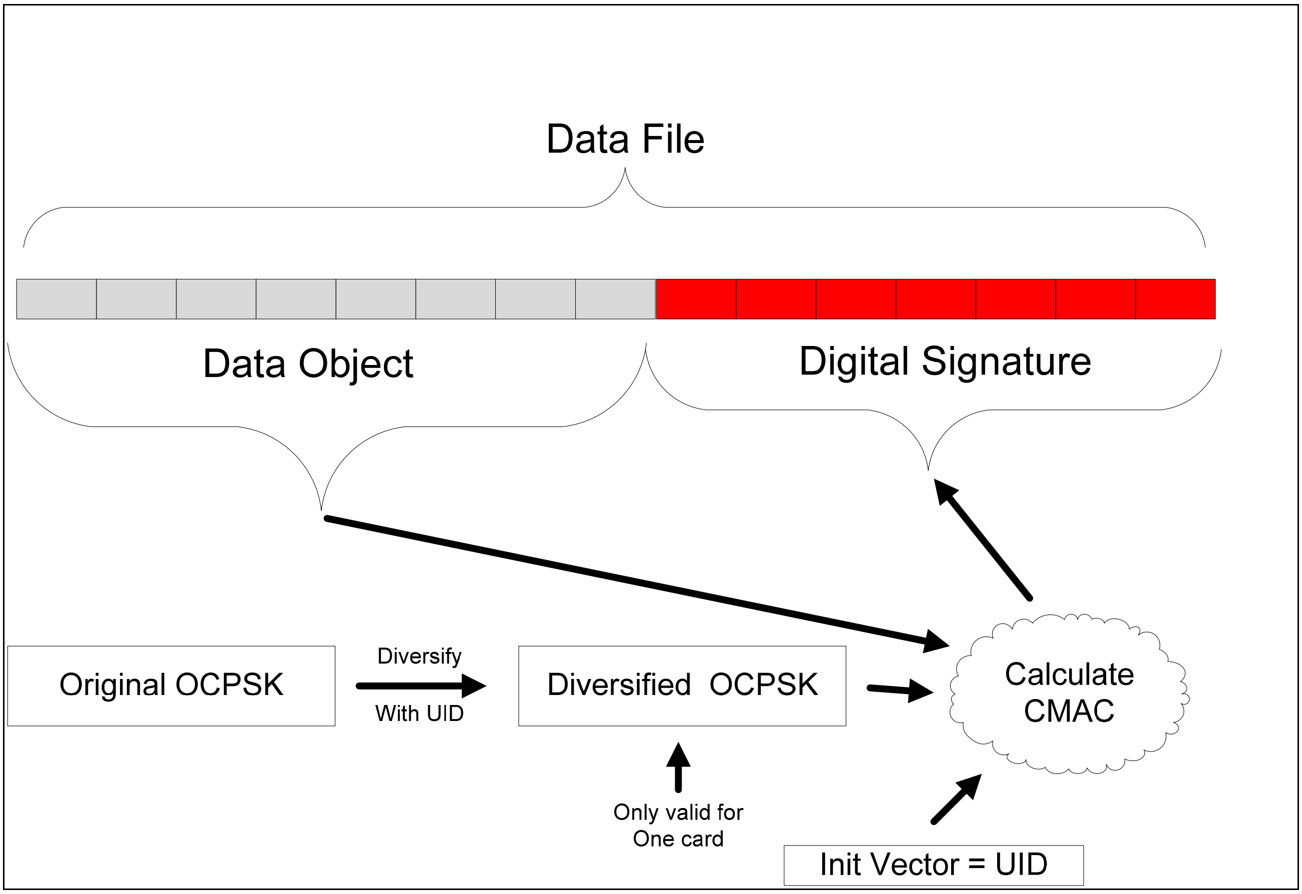


Fig 4. Data Construction of Digital Signature

Example: Based on AES – 128 key

PACS Data Object:

Version Major - 0x01

Version Minor - 0x00

Site Code - 0x00 00 00 11 22

Credential ID - 0x00 00 00 00 00 06 55 30

Reissue Code - 0x00

Pin Code - 0x00 00 00 00

Customer Data – 0x00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99

Original OCPSK - 0xf3f9377698707b688eaf84abe39e3791

UID : 0x04deadbeeffeed

AES DIV constant 1: 0x01

Signature data – 0x01 00 00 00 00 11 22 00 00 00 00 00 06 55 30 00 00 00 00 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99

Generate OCPSK Diversified Key

Step 1 :Generate subkeys

Generate K0:
K0 = CIPHK(0b). Encrypt 0s using Secret Key.
Here K0 = 0x6704a3af8af3d920a0a7594f5cebf9fd

Generate K1:
If MSB(K0) = 0, then K1 = K0 << 1;
Else K1 = (K0 << 1) XOR 0x00000000000000000000000000000087;
Shift K0 one bit left. If Most Significant Bit of K0 is not 0, XOR shifted result with 0x00000000000000000000000000000087.
Here K1 = 0xce09475f15e7b241414eb29eb9d7f3fa

Generate K2:
If MSB(K1) = 0, then K2 = K1 << 1;
Else K2 = (K1 << 1) XOR 0x00000000000000000000000000000087.
Shift K1 one bit left. If Most Significant Bit of K1 is not 0 XOR shifted result with 0x00000000000000000000000000000087
Here K2 = 0x9c128ebe2bcf6482829d653d73afe773.

Step 2 : Create Div Input

Div Constant 1 + UID + Padding
0x0104deadbeeffeed800000000000000000000000000000000000000000000000

Step 3 : XOR string

Since padding occurred, K2 will be XOR'd with Div Input
Result –
0x0104deadbeeffeed80000000000000009c128ebe2bcf6482829d653d73afe773

Step 4: Encrypt the above result with Secret Key
Result –
0x901780466c3d5fb6c885ab59139e132f0bb408baff98b6ee9f2e1585777f6a51

Step 5 : Diversified Key would be the last 16 byte block (Block 2) of the encryption result.
Diversified key is 0x0bb408baff98b6ee9f2e1585777f6a51

Generate Digital Signature using standard CMAC with Init Vector set to UID.

Init Vector 0x04deadbeeffeed8000000000000000000000
Diversified Key 0x0bb408baff98b6ee9f2e1585777f6a51
Signature data – 0x01 00 00 00 00 11 22 00 00 00 00 00 06 55 30 00 00 00 00 00 11 22 33 44 55 66 77 88 99 00 11 22 33 44 55 66 77 88 99

Digital Signature is 0x8FB0EF8EB12AC1F3

6. Legal information

6.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

6.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

6.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

6.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE — is a trademark of NXP B.V.

MIFARE Plus — is a trademark of NXP B.V.

MIFARE Ultralight — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

7. Contents

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an please send an email to: salesaddresses@nxp.com

Date of release: 7 March 2011
196811

Document identifier: AN10957