**Document information**

<table>
<thead>
<tr>
<th>Info</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords</td>
<td>Conditional, Access, Management, Control</td>
</tr>
<tr>
<td>Abstract</td>
<td>First document before implementing access control architecture</td>
</tr>
</tbody>
</table>
1. Introduction

1.1 Access Management basics

NXP offers a set of applications and a set of proven commercial hardware that customers may adopt to implement an access management/access control architecture.

Access Management System or Conditional Access system is an end-to-end infrastructure which objective is to implement physical and/or logical access control. In other words, it would allow the entrance or access of authorized entity/person to a restricted location or virtual area (“cloud”). In case of physical access, there is often a turnstile or door gate, preventing non-identified people to enter in such restricted areas. In case of logical access, there is a firewall preventing unauthorized access. An access management system is commonly organized as a star network, in which each node contains an interface to external world, and all nodes communicate to a central body.

![Common Access Management System](image)

**Fig 1.** Common Access Management System

1.1.1 Access Management typical architecture

An end-to-end access control systems typically includes:

1) Cards or portable objects (keyfobs): it stores user credentials, is normally carried by people in their pocket; when approaching a physical gate (turnstile, door or other kind of admittance hall), person conveys such credentials to electronic interface placed on
infrastructure, by approaching one to the other. In case of magstripe cards or contact smartcards, such contact is physical; in case of RFID contactless technology, it happens via electromagnetic interaction.

2) Reader controller: local part of infrastructure able to collect person’s electronic credentials from the card or portable object and conditionally dispatch them to back office/back end control center.

3) Back end/back office: it collects data coming from each single reader unit. In the case of RFID contactless technology, every reader is polling for the presence of card in every access gate or building turnstile, so that more than one user can authenticate his/her presence and enter the building (typical employee badging system).

Fig 2. End-to-end access control system minimum configuration

1.1.2 Document contents and purpose

The core of this application note is to show how to deploy a scalable end-to-end RFID based access control system starting from one single interface reader which interacts with a card. Also, explanation will be given on all available software and hardware tools which integrators or developers might use to implement their own access control system (where & how to request/retrieve basic building blocks and respective configuration instructions).

1.1.3 High level specifications and customer profiles

Often, access management public tender participants are system integrators who add value by delivering end-to-end tested system which is:

1) ready to issue virgin cards to be personalized with new users’ credentials

2) properly initialized in each individual reader-equipped turnstile and ready to poll for contactless cards

3) ready to record employee’s proof of presence in a time-stamped log file, and organize all time stamps in monthly reports.

On the other hand, Reader-controller OEM suppliers are companies that add value by delivering a self-standing block, the so-called embedded reader controller, which will be supplied in tenths/hundred units to the system integrator, who is responsible for final integration and entire test.

System integrator will receive all Reader controller units, all back office building blocks and will:
1) execute acceptance incoming test on each hardware block;
2) execute acceptance test on all complementary units delivered by third parties or
design houses (e.g. HSM - Host Secure Module boards, SAM - Secure Application
Modules, back office server boards, monitoring software, badge personalization software,
badging printing/issuing machines, mechanical turnstiles, etc).
3) assemble and test whole infrastructure.

System integrator is often interested in qualifying OEM suppliers by checking their
functionality and equipment quality against a requirement list. This check list includes
digital interface requirements, since data/digital output log transactions will be delivered
by each individual reader block. Both partners need to know how to implement and read
a so called Generic access control data model [4] in order to be able
interpret/encapsulate/extract and exchange data from badging readers to/from Back
office, using suitable protocol and applying proper security recommendations [5]. [6].

1.2 Security levels on Access control systems
There are several access control architectures which can be chosen by integrators of
access control systems, ranging from very simple and low security to complex and high
security. Main characteristics can be found in coming paragraphs.

1.2.1 Embedded reader storing keys in MCU

Communication is secured by symmetric key encryption both in card as well in reader,
which hosts keys in MCU flash.
This reader architecture although very cheap, simple and straight forward has the lowest
security because at any moment MCU box could be stolen and keys could be retrieved
by reverse engineering. Reader antenna assembly shall be built in a robust tamper-free
container, with mechanical protection which might delete MCU FW immediately after
break-in. In addition, the reader itself might be placed inside the area to secure, while the
RFID antenna is place outside of this area (for example on the other side of the wall),
with wire connection.
1.2.2 Reader keys stored in SAMs: turnstile model

The SAM builds a “second fortress wall around” the reader, so that complete communication will be secure. The secret credentials cannot be obtained from the SAM, even by tampering. In case SAMs are stolen, it is impossible to retrieve system keys. In case SAMs are replaced within a reader, some additional authentications are mandatory to operate the system again.
1.2.3 SAM connected to host computer

Same security level as 1.2.2, slightly longer transaction time.

Fig 5. SAM connected to host computer

1.2.4 SAM in X-mode connection

Same security level as in 1.2.2 and 1.2.3, this architecture presents fastest performance in terms of transaction speed. Ideal architecture for fare collection/access management systems containing keys stored in only one SAM; such architecture makes full benefit from I2C connection available in SAM AV2 and in many NXP chip readers.

Fig 6. SAM in X-mode connection

2.1 Access Management principles

NXP has elaborated a list of recommendations and best practices aiming to steer customers towards suitable choices both from practical point of view (fulfillment of customer needs in terms of security) as well as considering cost-effectiveness and easy-to-deploy architectures. This specific knowledge will be presented taking into account technical assumptions (e.g. compliance to standards and security level requirements) and will gradually cover from less complex, less secure to most powerful, most secure solutions. This will allow customers to choose the best suitable architecture given their initial requirements and budget.

2.1.1 Literature and available documents

The access management support package currently includes following documents:

3rd party whitepapers:


[3] - OpenCashFile micro payment specification (based on MIFARE DESFire) – issue by consortium Common Smartcard; [www.nxp.com/redirect/common-smartcard.org/](http://www.nxp.com/redirect/common-smartcard.org/). This specification is only available for consortium members, and available in German only. An English version will be available shortly.

NXP documents and recommendation papers:


2.1.2 Hardware content list

Next to abovementioned document list, NXP is providing a list of hardware electronic blocks, reference designs and related software, useful to quickly deploy access management pilots, which can be re-scaled up, with simple HW modifications and extensions in Software/Firmware.

2.1.2.1 NXP available HW:

1) Pegoda reader (CLRD701, CLRD710)

MFEV710,599  12NC: 9352 941 66599

Pegoda reader bundles include gerber files and libraries; Access Management demo software (MAMD) (see chapter 3) is provided separately to deploy an easy conditional access pilot, including source code.

Fig 7. MAMD user interface
2) Embedded Reference design PREV601

Fig 8. PREV601 Demoboard

Such reference design can be ordered via NXP distributors or via extranet, PREV601M - 12NC: 9352 998 73699.

Core Documentation:

<table>
<thead>
<tr>
<th>Item no</th>
<th>Item</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>219311</td>
<td>Datasheet</td>
<td>PR601, Integrated reader module, objective datasheet</td>
</tr>
<tr>
<td>219211</td>
<td>Datasheet</td>
<td>PRH601, Integrated reader module, objective data sheet</td>
</tr>
<tr>
<td>243910</td>
<td>Application note</td>
<td>Quick Start Up Guide PREV601 Demo Board</td>
</tr>
</tbody>
</table>

Further Documentation:

<table>
<thead>
<tr>
<th>Item no</th>
<th>Item</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AN11022</td>
<td>Application Note</td>
<td>CLRC663 Quickstart Guide</td>
</tr>
<tr>
<td>AN11019</td>
<td>Application Note</td>
<td>CLRC663, MFRC631, MFRC630, SLRC610 Antenna Design Guide</td>
</tr>
<tr>
<td>AN11020</td>
<td>Application Note</td>
<td>CLRC663, MFRC631, MFRC630, SLRC610 Matching Calculations</td>
</tr>
<tr>
<td>AN11020</td>
<td>Calculation tool</td>
<td>CLRC663, MFRC631, MFRC630, SLRC610 Directly Matched Antenna design – advanced user</td>
</tr>
<tr>
<td>AN11145</td>
<td>Application Note</td>
<td>CLRC663, MFRC630, MFRC631, SLRC610 PC-Serial RS232 and low power card detection Quick Start Guide</td>
</tr>
<tr>
<td>AN11021</td>
<td>Application Note</td>
<td>CLRC663, MFRC631, MFRC630, SLRC610 Software Design Guide for NXP RDLib</td>
</tr>
</tbody>
</table>

All above documentation is available on:


PREV601 software examples can be downloaded from NXP public website:
http://www.nxp.com/demoboard/PREV601.html
3) Embedded reference designs ready to be attached to an LPCXpresso board:
PNEV512B and CLEV663B

CLEV663B embedded reference designs based on CLRC663 (and derivatives) and
PNEV512B (based on PN512) - You can access following NXP links containing
examples for Cortex MCU’s from NXP:

http://www.nxp.com/demoboard/CLEV663B.html#showall
http://www.nxp.com/demoboard/PNEV512B.html#showall
3. Access Management Demo Software

3.1 MAMD - MIFARE Access Management Demo

The first Software package to be described is Windows-pc based MAMD which consists of an access management application related to a reader block, and a webserver which simulates a Back office center.

3.1.1 MAMD Supported hardware

The Demonstrator supports following readers:

- NXP Pegoda CLRD701 + PC-Built-in ISO7816-readers or external PC/SC-usb commercial contact readers, to host the SAM
- NXP Pegoda CLRD710 with SAM AV2 installed in respective ISO/IEC-7816 slot

In general all readers could be added if they are included in the NXP Reader Library.

3.1.1.1 MAMD NXP SAM-connection Supported Modes:

<table>
<thead>
<tr>
<th>Reader</th>
<th>SAM Mode</th>
<th>SAM AV2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD701</td>
<td>No SAM</td>
<td>SAM in External contact reader</td>
</tr>
<tr>
<td>RD710</td>
<td>No SAM</td>
<td>SAM in External contact reader (see next table)</td>
</tr>
<tr>
<td>RD701</td>
<td>SAM Non-X</td>
<td>SAM in External contact reader</td>
</tr>
<tr>
<td>RD710</td>
<td>SAM Non-X</td>
<td>SAM inside RD710 slot (see next table)</td>
</tr>
<tr>
<td>RD710</td>
<td>SAM X</td>
<td>SAM inside RD710 slot (see next table)</td>
</tr>
</tbody>
</table>

3.1.1.2 NXP Reader RD710 hardware settings:

Switch positions of the RD710:

<table>
<thead>
<tr>
<th>SW1</th>
<th>SW2</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>OFF</td>
<td>No SAM in reader slot; SAM can be connected to a separate contact reader</td>
</tr>
<tr>
<td>ON</td>
<td>OFF</td>
<td>SAM in Non-X-mode connection</td>
</tr>
<tr>
<td>OFF</td>
<td>ON</td>
<td>SAM in X-mode</td>
</tr>
</tbody>
</table>

For more information on NXP-reader <-> SAM connection please read: [8]

For more information on NXP readers (RD701 and RD710) please read: [7], [8], [9]
3.1.2 MAMD Introduction and tutorial

A complete MAMD tutorial can be found in Docstore (MIFARE ICs > Application Notes > Access Management). Both documentation and software are delivered to NXP by a third party (FH JOANNEUM Gesellschaft Germany). It includes several use cases. Each use case comes along with a setup where certain components of the whole system are used.

The tutorial can be found in the zip file: MAMD-SDK_V1.10.x documentation.zip

After you have unzipped it, you will find all tutorial documents.

![MAMD Tutorial documents](image)

3.1.3 MAMD server installer

MAMD server installer can be found in Docstore (MIFARE ICs > Application Notes > Access Management) and it is delivered in this executable file: MAMD-Setup_V1.10.x.exe.

Make sure you have at least 360Mbytes free space on your hard disk for SW installation, and PC/Laptop with 800x600 minimum screen resolution. Make sure you have administrator rights, then double click on previous executable; you will get:

![Select language](image)
Press ok; then you will get:

![Fig 12. Installation dialogue](image)

Fig 12. Installation dialogue

![Fig 13. License agreement dialogue](image)

Fig 13. License agreement dialogue

After you press "Next", you'll get:
Fig 14. Installation directory on your hard disk

Press next:
Fig 15. Selection of type of installation

Press Next:

Fig 16. Start Menu folder choices
Press next.

![Fig 17. Ready to Install dialogue](image)

Press install and wait until installation is finished:
Press “finish” button. You will find following directories in your C: driver and three tabs in Windows Start Menu:

Fig 19. Directories installed on C:\ and Start menu after installation of MAMD server installer
In order to check if the demo software is running, click on Start MAMD Launcher; you will see this window. You may need to run this program as an administrator.

![Start MAMD Launcher](image)

**Fig 20. Start MAMD Launcher**

### 3.1.4 Understanding MAMD Launcher

As explained in `01_MAMD_Tutorial.docx`, once launcher is running, you have to start the servers first. After you have pressed start server, you will read message "servers running". Once the servers (web and database servers) are started, you will be able to start other components:
Fig 21. MAMD server status user interface

3.1.4.1 (Access) Controller Component

Physically it is the reader unit, in this case represented by Pegoda reader. After you have pressed "start" any component "button", you will see the respective component window popping up.

In case you press “start controller” (under Components), and you have no reader connected to PC, you'll get this error message:

Fig 22. Error message
On the other hand, if you have previously connected a Pegoda (CLRD701) to your pc you will see:

![MAMD controller user interface](image)

**Fig 23. MAMD controller user interface**

If you choose to have a SAM, it will be possible to select a pc-built-in contact reader where SAM (Secure Application Module) might be plugged to allow MAMD to retrieve keys for symmetric cryptography (MIFARE Crypto1, 3kDES, AES):
Fig 24. MAMD contact reader selection

In order to simplify this quick start,
- assume there is a SAM in NON-X, insert the SAM in a card reader, select the right reader in the drop list and click connect;
- alternatively, if you don’t have a SAM car, select ‘no SAM’

then you will see the controller display:

Fig 25. MAMD controller including Grant/Deny status
The Controller is a program which manages several readers. It can either gather its access decision by connecting with the back end or by accessing access control list files. From now onwards, you may continue to read 01_MAMD_Tutorial.docx from page 5 onwards.

In the MAMD launcher, press “stop” button on right side of “controller”, and check that previous window disappeared.

3.1.4.2 (Card) Personalization Component

In order to personalize cards which will be used by people to get access to your Access control system, on Launcher window, press button “start” on right side of keyword “Personalization”; you will see following window popping up:

Select the right contactless reader, select ‘no SAM’ and press ‘Connect’. Place a virgin MIFARE DESFire EV1 card on Pegoda reader and press “New User” button; you will see following window:
After you have added new data to all fields and established badge expiration date, press save. You will then notice a new entry in previous list:
Although, information now is in the backoffice, the card has neither been personalized nor issued yet.

Press the button connect, click with mouse the person you want to personalize the card, and press button "write to card":

![MAMD personalization card interface](image)

**Fig 29. MAMD personalization card interface**

Once the person is registered in the system, the card will be recognized as personalized and its UID will be shown in the back end system ("Users & Cards").
Stop the personalization component and restart controller component, then press button “read card”. As soon as the card is put on the reader, the controller will show its data and also whether access is granted or denied.
In this case, the answer is “Deny” because personalization did not make use of SAM keys. Next chapter will show how to set keys in SAM so that Personalization component can retrieve them during card personalization.
3.1.5 SAM Manager component

On MAMD launcher, press “start” SAM Manager; you will see this window; choose appropriate ISO7816 reader and write proper Host key; choose Key entry number and write proper key to respective key entry. Keys by default are assumed to be AES 128 bit key length (see document 05_MAMD_Security_Measures.docx)

In this case, we are choosing Host key 0x0000….. 00, 16 bytes (128 bits key), since we assume the SAM AV2 card manager has default key 0x0000….. 00, (16 bytes)

![SAM Manager window](image)

Fig 32. MAMD SAM manager user interface

Select the key entry number 02, which you can freely choose. Beware the system will not remember the last key you have set, so write its value in a backup file. There is absolutely no possibility to read back the key out of the SAM. In our case, we will choose default key 02 = 0x0000….. 00, 16 bytes.

Then you can personalize a virgin MIFARE DESFire EV1 card, using any Backoffice individual data, provided that you choose the key number to be retrieved during personalization:
Fig 33. MAMD personalization user interface

Afterwards, stop Personalization component, restart Controller and place card over reader; you will see “access granted”.

If you attempt to run Pegoda reader both when Personalization component and Controller component are running, then you will get this error message:

![Error message](image)

**Fig 35.** Error message

**Fig 34.** MAMD is granting access to personalized card
In order to understand the other components, please continue reading other tutorials from 02 to 09 in the MAMD Document list.

### 3.1.6 MAMD reader source code

The third package you will receive is the Reader controller software; this file MAMD-SDK_V1.10.15.zip can be retrieved in Docstore (Doc n°; Box net location link)

After you have unzipped it, you will find following files and directories:

![MAMD Reader controller directory structure](image)

In each directory you will find source files for each component which can be a valid start point for porting the functionality into your embedded platform.
4. Legal information

4.1 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 to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

4.2 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 competent 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.

4.3 Licenses

ICs with DPA Countermeasures functionality

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

4.4 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.
5. List of figures

<table>
<thead>
<tr>
<th>Fig</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fig 1</td>
<td>Common Access Management System</td>
<td>3</td>
</tr>
<tr>
<td>Fig 2</td>
<td>End-to-end access control system minimum configuration</td>
<td>4</td>
</tr>
<tr>
<td>Fig 3</td>
<td>Embedded reader storing keys in MCU</td>
<td>5</td>
</tr>
<tr>
<td>Fig 4</td>
<td>Turnstile model</td>
<td>6</td>
</tr>
<tr>
<td>Fig 5</td>
<td>SAM connected to host computer</td>
<td>7</td>
</tr>
<tr>
<td>Fig 6</td>
<td>SAM in X-mode connection</td>
<td>7</td>
</tr>
<tr>
<td>Fig 7</td>
<td>MAMD user interface</td>
<td>9</td>
</tr>
<tr>
<td>Fig 8</td>
<td>PREV601 Demoboard</td>
<td>10</td>
</tr>
<tr>
<td>Fig 9</td>
<td>Blueboards</td>
<td>11</td>
</tr>
<tr>
<td>Fig 10</td>
<td>MAMD Tutorial documents</td>
<td>13</td>
</tr>
<tr>
<td>Fig 11</td>
<td>Select language</td>
<td>13</td>
</tr>
<tr>
<td>Fig 12</td>
<td>Installation dialogue</td>
<td>14</td>
</tr>
<tr>
<td>Fig 13</td>
<td>License agreement dialogue</td>
<td>14</td>
</tr>
<tr>
<td>Fig 14</td>
<td>Installation directory on your hard disk</td>
<td>15</td>
</tr>
<tr>
<td>Fig 15</td>
<td>Selection of type of installation</td>
<td>16</td>
</tr>
<tr>
<td>Fig 16</td>
<td>Start Menu folder choices</td>
<td>16</td>
</tr>
<tr>
<td>Fig 17</td>
<td>Ready to Install dialogue</td>
<td>17</td>
</tr>
<tr>
<td>Fig 18</td>
<td>MAMD installation complete window</td>
<td>18</td>
</tr>
<tr>
<td>Fig 19</td>
<td>Directories installed on C:\ and Start menu after installation of MAMD server installer</td>
<td>18</td>
</tr>
<tr>
<td>Fig 20</td>
<td>Start MAMD Launcher</td>
<td>19</td>
</tr>
<tr>
<td>Fig 21</td>
<td>MAMD server status user interface</td>
<td>20</td>
</tr>
<tr>
<td>Fig 22</td>
<td>Error message</td>
<td>20</td>
</tr>
<tr>
<td>Fig 23</td>
<td>MAMD controller user interface</td>
<td>21</td>
</tr>
<tr>
<td>Fig 24</td>
<td>MAMD contact reader selection</td>
<td>22</td>
</tr>
<tr>
<td>Fig 25</td>
<td>MAMD controller including Grant/Deny status</td>
<td>22</td>
</tr>
<tr>
<td>Fig 26</td>
<td>MAMD personalization user interface</td>
<td>23</td>
</tr>
<tr>
<td>Fig 27</td>
<td>Personalization entry</td>
<td>24</td>
</tr>
<tr>
<td>Fig 28</td>
<td>MAMD personalization list</td>
<td>24</td>
</tr>
<tr>
<td>Fig 29</td>
<td>MAMD personalization card interface</td>
<td>25</td>
</tr>
<tr>
<td>Fig 30</td>
<td>MAMD server status user interface</td>
<td>26</td>
</tr>
<tr>
<td>Fig 31</td>
<td>MAMD server status user interface</td>
<td>27</td>
</tr>
<tr>
<td>Fig 32</td>
<td>MAMD SAM manager user interface</td>
<td>28</td>
</tr>
<tr>
<td>Fig 33</td>
<td>MAMD personalization user interface</td>
<td>29</td>
</tr>
<tr>
<td>Fig 34</td>
<td>MAMD is granting access to personalized card</td>
<td>30</td>
</tr>
<tr>
<td>Fig 35</td>
<td>Error message</td>
<td>30</td>
</tr>
<tr>
<td>Fig 36</td>
<td>MAMD Reader controller directory structure</td>
<td>31</td>
</tr>
</tbody>
</table>
6. Contents

1. Introduction ......................................................... 3
   1.1 Access Management basics............................... 3
   1.1.1 Access Management typical architecture .......... 3
   1.1.2 Document contents and purpose ..................... 4
   1.1.3 High level specifications and customer profiles .. 4
   1.2 Security levels on Access control systems ......... 5
   1.2.1 Embedded reader storing keys in MCU .......... 5
   1.2.2 Reader keys stored in SAMs: turnstile model.... 6
   1.2.3 SAM connected to host computer .................... 7
   1.2.4 SAM in X-mode connection ......................... 7
2. Access Management Product Support
   Package ................................................................ 8
   2.1 Access Management principles.......................... 8
   2.1.1 Literature and available documents ............... 8
   2.1.2 Hardware content list .................................. 9
   2.1.2.1 NXP available HW: ..................................... 9
3. Access Management Demo Software .............. 12
   3.1 MAMD - MIFARE Access Management Demo. 12
   3.1.1 MAMD Supported hardware ....................... 12
   3.1.1.1 MAMD NXP SAM-connection Supported
                      Modes: ....................................................... 12
   3.1.1.2 NXP Reader RD710 hardware settings:........... 12
   3.1.2 MAMD Introduction and tutorial .................... 13
   3.1.3 MAMD server installer: ......................... 13
   3.1.4 Understanding MAMD Launcher ..................... 19
   3.1.4.1 (Access) Controller Component ................. 20
   3.1.4.2 (Card) Personalization Component ............. 23
   3.1.5 SAM Manager component............................ 28
   3.1.6 MAMD reader source code ......................... 31
4. Legal information .............................................. 32
   4.1 Definitions .................................................. 32
   4.2 Disclaimers .................................................. 32
   4.3 Licenses ...................................................... 32
   4.4 Trademarks .................................................. 32
5. List of figures ..................................................... 33
6. Contents ............................................................. 34