ASSA ABLOY

Aperio RFID Technologies

1 Table of Contents

2 Revision History

Revision	Date	Changed by	Description
PA1	2012-05-30	Hector Hernandez Gomez	The purpose of this document is to explain the different RFID technologies supported by Aperio. It is based on the AAID_025_Aperio_RFID_Technologies_RevA document.
A	2012-06-26	Jörgen Frejd	Updated to rev A. after internal review.
PB1	2013-04-11	Fredrik Einberg	Updated with V2 SE support.
PB2	2013-04-15	Tomas Stragnemyr	Updated with Legic support
PB3	2013-04-15	Jörgen Frejd	Updated with some minor changes and textual updates
PB4	2013-04-16	Jörgen Frejd	Updated after further internal review
B	2013-04-18	Jörgen Frejd	Updated and set to rev B after review and approval
PC1	2013-07-09	Fredrik Einberg	Clarifications and corrections regarding DESFire and MIFARE Plus support across platform versions.
C	2013-08-21	Jörgen Frejd	Approved after review.
PD1	2015-07-29	Jörgen Frejd	Draft update, adding Aperio V3 specific changes and specified support.
PD2	2016-03-09	Jörgen Frejd/Niclas Herlin	Updated after internal review. Added chapters for Elite and Mobile Credentials as well as added a security level in the initial support table
PD3	2016-03-17	Jörgen Frejd/Niclas Herlin	Updated after further internal review.
D	2016-04-13	Jörgen Frejd/ Niclas Herlin	Updated after internal review and input from HID on the security level classification.

3 Introduction

3.1 Purpose

The purpose of this document is to explain the different RFID technologies supported by Aperio.

3.2 Definitions and abbreviations

Expression	Description
UID	Unique Identification Number
Sector Data	User data stored in none volatile memory in the RFID card.
EAC	Electronic Access Control
AES	Advanced Encryption Standard
2KDES	2 Key Data Encryption Standard
3KDES	3 Key Data Encryption Standard.
NFC	Near Field Communication
SIO	Secure Identity Object
MAC	Message Authentication Code. Cryptographicj checksum on data to ensure integrity and authenticity of data.

3.3 References

[1]	www.nxp.com
[2]	www.hidglobal.com
[3]	www.waazaa.org

4 RFID Technologies in Aperio

4.1 Overview

The RFID Technologies supported by Aperio are divided into two major groups, high frequency - HF and low frequency – LF. Different lock hardware is used for HF and LF.

The table below shows an overview of the Aperio RFID, the main features of each technology and the support across platform generations. Further information about these technologies is given in the next chapters.

RFID TECHNOLOGY		SECURITY LEVEL	PLATFORM
HF			
iCLASS	- **2kbits, 16kbits, 32kbits**	**1**	**V2/V2SE/V3**
ISO14443b UID	- **4 or 7 bytes UID**	**0**	**V2/V2SE/V3**
MIFARE Classic	- **4 or 7 bytes UID** - **Sector data** - **1kbytes or 4kbytes cards**	**0 (UID ONLY)** **1 (SL1)** **3 (SL3)**	**V2/V2SE/V3**
MIFARE plus	- **4 or 7 bytes UID** - **Sector data in security level 1 & 3** - **2kbytes or 4kbytes cards**	**0** **1** **1**	**V2/V2SE/V3**
MIFARE DESFire	- **DESFire 0.6 & DESFire EV1** - **4kbytes or 8kbytes cards**	**0 (UID ONLY)** **3**	**V2/V2SE/V3**
MIFARE Ultralite	- **CSN only**	**0**	**V3**
Rijkspas	- **Special DESFire EV1 format**	**3**	**TBD**
iCLASS Seos	- **Highest security** - **NFC card emulation** - **SIO enabled**	**4**	**V2SE/V3**
MIFARE DESFire SE	- **SIO enabled**	**2**	**V2SE/V3**
iCLASS SE	- **SIO enabled**	**2**	**V2SE/V3**
Legic	- **Prime** - **Advant**	**1**	**V2/V3 LEGIC**
LF			
HID Prox	- **HID Prox reader compatibility**	**0**	**V2LF/V3**
EM Prox	- **Raw data output**	**0**	**V2LF/V3**
EM4450 CSN	- **Raw data output**	**0**	**V2/V3**

The security levels are to be interpreted like below in this table:

Security level	Interpretation
0	"None" - there is no protection from cloning or creating new identities, as the identity is used in an unprotected form and it is considered trivial to copy it or spoof it.
1	"Weak" - there is a weak protection of the data on the card which is known to be broken (algorithm is weak), and it allows to read or modify the data, so that new identity can be created with some effort.
2	"Clonable" - there is a weak protection of the data from unauthorised reading (or replay), but the method used for the protection is known to be broken and the attack is publically available; however, new identity cannot be created as there is a signature protecting the integrity of the data which prevents the data modification.
3	"Tracable" - there is a strong protection of the data on the card from unauthorised reading or replay and this protection is currently not considered to be broken. However, it is possible to track the owner of the card through some other means such as static UID or other static data stored on the card which allow tracking the card holder.
4	"Secured" - there is no known way <(for an unauthorised actor)> to read any data from the card and there is no way to track the card holder, as the card has no static data which would be readable, so the holder cannot be tracked.

4.1.1 iCLASS

iCLASS employs ISO15693 communication protocol and HID proprietary security protocol.

The use of iCLASS does not require any configuration by the user since the Aperio iCLASS firmware will automatically read up to 144 bits from the HID Access Control ID field of the HID Access Control Application.

The data read by Aperio is identical to the data that an iCLASS standard reader would read.

4.1.2 ISO14443B UID

Some RFID technologies such as Calypso, Atmel CryptoRF, Pico Pass and others use the ISO/IEC 14443B communication protocol. Aperio supports the reading of the UID for cards using this technology.

Early versions of Calypso employ what is called Innovatron protocol, also known as ISO14443(B'). Aperio does not support this protocol.

Pico Pass can use either ISO14443B or ISO15693. The UID reading in ISO15693 is not currently supported.

4.1.3 MIFARE Classic

This RFID technology is compliant to ISO14443A-3 and makes use of a NXP proprietary security protocol for authentication and ciphering.

The Aperio platform supports the reading of 4 and 7 bytes UID.

Aperio also supports sector reading; the user must configure the sector containing the desired information as well as the key assigned to this sector. Only one configuration per lock is supported and therefore multiple sector reading is not supported.

The platform supports all NXP MIFARE Classic manufactured cards (1K/4K), Infineon MIFARE cards (also known as IFX MIFARE) and NFC MIFARE Classic implementations for mobile phones.

MIFARE Classic memory is organized in sectors. These sectors are divided into blocks of 16 bytes each. MIFARE Classic 1k cards have 16 sectors of 4 blocks, whereas 4k cards have 32 sectors of 4 blocks and 8 sectors of 16 blocks. Aperio can read up to 48 bytes of data from any sector.

Every sector contains a trailer block where key A and B are stored. There are also 4 bytes access bits. Depending on these access bits, card reading/writing can be allowed by using key A, key B or both. MIFARE keys are 6 bytes long. Aperio supports usage of key A or B for reading sector data.

In order to read sector data, the Aperio lock needs to be configured via the PAP tool. The following parameters need to be set: sector number, the index where the information starts, the data length, use of key A or B and the key value.

As an example, imagine we want to read the user data shown in the figure below: 17 10 19 80. Assuming we want to use Key A and the value is 001122334455, the lock configuration parameters become:

Sector: 14, index: 17, length: 4, key: A, key: 001122334455

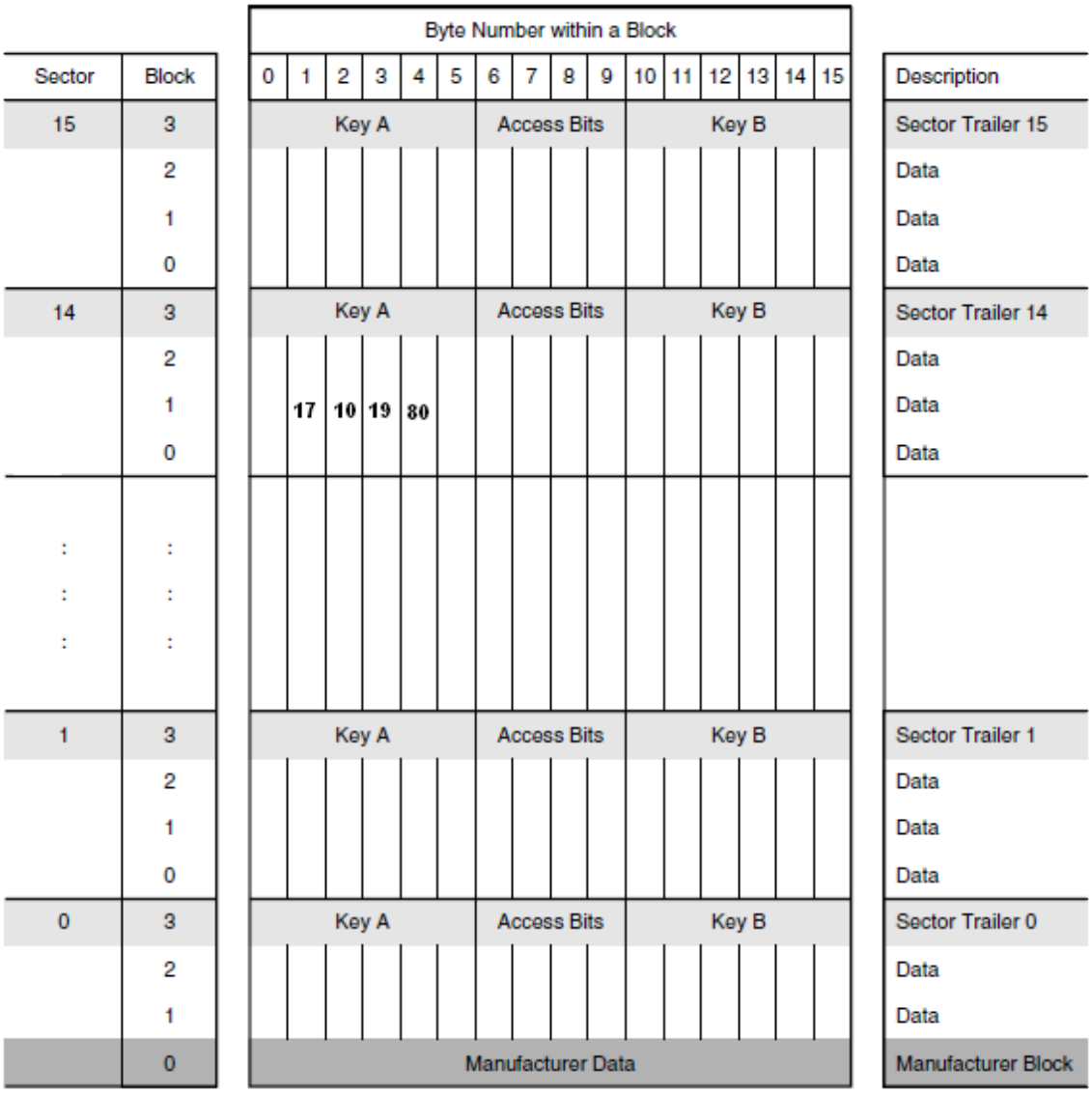

Fig. 1

4.1.4 MIFARE Plus

MIFARE Plus cards can be used in security level (SL) 1, 2 and 3. Aperio supports the use of security level 1 and 3 only.

Security Level 1 is backwards compatible with MIFARE Classic, the use and configuration of this mode is identical to MIFARE Classic. This mode is adequate for migrations from MIFARE Classic to MIFARE Plus where both credentials can be used in the same installation. The optional AES authentication support in security level 1 is not supported. For higher security, please use security level 3.

Security Level 3 uses AES cryptography for authentication, data integrity and confidentiality. In order to read data from the sector, the user must configure a 16 bytes AES key.

Aperio can handle 4 and 7 bytes UIDs as well as 2K and 4K cards.

The memory organization is identical to MIFARE Classic with the exception of 2K cards which have 32 sectors instead of 16. Therefore, the configuration parameters are the same as for MIFARE Classic with the exception of the key length in SL3. The MIFARE Plus key length in SL3 is 16 bytes (AES-128 bit).

There are 2 types of MIFARE Plus cards, S and X. SL1 operation is identical. In SL3, MIFARE Plus S cards lacks the support for data encryption in SL3, only MAC is supported to ensure integrity. MIFARE Plus X cards support data encryption (and MAC) in SL3. It is possible to configure a MIFARE Plus X card (the access rights) to behave as a MIFARE Plus S card, i.e. to allow reading of plain data protected via MAC only.

In SL3, Aperio supports MIFARE Plus S and X cards differently depending on platform version.

V2 specific: MIFARE Plus S and X cards are handled in the same way meaning plain mode access of data is used (MAC only). X cards has to be configured to allow plain mode reading of data.

V2SE/V3 specific: The highest possible security is used for each card. For MIFARE Plus S cards, plain mode is used. For X cards, full encryption is used. No configuration is needed for this. The lock determines type of MIFARE Plus cards and acts accordingly meaning read data in plain for S cards, read encrypted data for X cards. Note, X cards shall be configured to only allow encrypted read access to increase security. It is possible to configure X cards to allow both plain and encrypted read access.

4.1.5 MIFARE DESFire

MIFARE DESFire communication protocol complies to part ISO14443-4. Depending on the configuration of the card, several cryptography standards can be applied.

Aperio platform supports MIFARE DESFire 0.6 and MIFARE DESFire EV1. MIFARE DESFire 0.6 is discontinued by NXP for security breach reasons. MIFARE DESFire EV1 is recommended for all new installations. Depending on the card configuration, a 2KDES, 3KDES or AES key will be required; also the user must know the application identifier and file identifier where the data is located.

2K, 4K and 8K cards are supported.

Regarding UID length, it is 7 bytes for MIFARE DESFire. However, MIFARE DESFire cards can be configured to use a 4 byte random ID (RID) during anti-collision. Such cards are handled differently depending on platform version, see below.

MIFARE DESFire cards do not have a fix memory structure. The user can define the memory organization. The card can be divided into applications (up to 28) and these applications contain up to 32 files. Each application can have up to 14 keys.

In order to read MIFARE DESFire data, the Aperio lock needs to be configured via the PAP tool. The following parameters need to be set: Application identifier, the file identifier, the key including: key value, key type and key number, and the start index and length of the data to be read within the file.

V2 specific:

Both MIFARE DESFire 0.6 and MIFARE DESFire EV1 are supported.

The maximum supported data lengths is 30 bytes.

Random ID cards are not supported.

V2SE/V3 specific:

Only MIFARE DESFire EV1 is supported.

The maximum supported data lengths is 48 bytes.

Random UID cards are supported where 3 of the 7 bytes UID are reported as zeroes. The RUID shall not be used for any access decisions.

Example:

As an example, imagine a MIFARE DESFire card application as given by the figure below and we want to read the data 17 10 19 80.

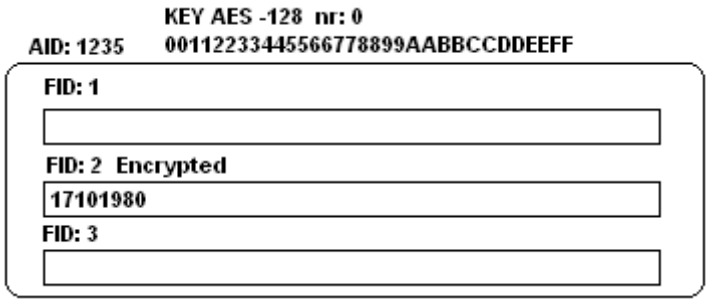

Fig. 4

The following parameter values would need to be set in the Aperio lock:

Application identifier - AID: 1235, file identifier – FID: 2

Protection level: Encrypted

Key type: AES-128, key number = 0, key value: 001122...EEFF

Start index: 0, length: 4,

4.1.6 Rijkspas

Rijkspas is a card format based on MIFARE DESFire EV1 cards. It does not require a PAP configuration; however the configuration is performed by using Rijkspas configuration cards. The Aperio lock is delivered in factory mode, the end user will be able to present a configuration card which gives the lock all the MIFARE DESFire configuration parameters including the key.

Due to some restrictions in the HID library handling the MIFARE DESFire code, Rijkspas is fully firmware implemented and therefore the SAM AV1 is not used.

Future Rijkspas specification requires the storage of the keys in a SAM module as well as a specific way to perform a key diversification defined in SAM AV2 datasheets. Aperio version 2.x current hardware is not able to satisfy this requirement.

4.1.7 Secure Identity Object (SIO) – SE credentials

Secure Identity Object (SIO) is a portable credential methodology developed by HID Global. The SIO adds an additional security layer to any RFID or smart card technology. In short, the credential data (access control data) to be protected is wrapped in an encrypted data container – the SIO. The SIO is then programmed to the card. The RFID reader (the Aperio lock) retrieves the SIO using the underlying card security protocol (e.g. iCLASS or MIFARE Classic). Then, checks the authenticity of the SIO and decrypts it to get the credential data which is then handled (sent to EAC).

The SIOs are generated and distributed by HID Global's Trusted Identity Platform™ (TIP). All physical cards using SIOs are purchased via HID Global. Mobile phone credentials using SIOs are supported by the HID Seos platform.

SIO enabled credentials are typically suffixed with SE (SIO Enabled), e.g. iCLASS SE. An exception to this rule is the iCLASS Seos credential which is a newly developed credential with built-in SIO support from the start.

Two types of keyset security schemes are available for SE credentials and readers, Standard and Elite. Standard is the default universal keyset (same for all readers and cards) that maximize interoperability and simplifies integration. Elite offers a customer/site unique keyset to increase the security level. The reader must be configured to use the Elite keyset via configuration cards. Elite readers do not read Standard SE cards.

The Aperio V2 SE and Aperio V3 platform supports SIO enabled credentials, V2 do not. For physical SE credentials, no configuration is needed. For all supported SE credentials, all keysets are pre-loaded. By default, the *Standard* keysets are used.

To provide easy migration, credential data retrieved a SIO enabled card is currently reported to the EAC using the underlying credential format, i.e. data read from an iCLASS SE card is reported to the EAC using Aperio's iCLASS credential format. This may change at a later time though.

4.1.8 iCLASS SE

This is a SIO enabled iCLASS credential. From a user and integration perspective, spec is the same as for the iCLASS credential.

4.1.9 MIFARE DESFire SE

This is a SIO enabled MIFARE DESFire credential. Compared to standard MIFARE DESFire, no configuration of the lock is needed to read this credential. The Aperio MIFARE DESFire credential format is used to report the data retrieved from the SIO. This format has a byte sized length field. A constraint with this is that non-even 8 bit data sizes cannot be reported precisely. Such data formats will be reported with trailing bits padded with zeroes. I.e. a 26-bit data format will be reported as 4 bytes (32 bits) of data with the trailing 6 bits set to 0. If possible, it is recommended to select a data size of even 8 bit size when using this credential.

4.1.10 iCLASS Seos

iCLASS Seos is a high-end standards based smart card technology developed by HID Global. The RFID technology used is ISO/IEC 14443, smart card commands follows the ISO/IEC 7816 protocol.

Multiple applications (data files) are supported and data is structured using object oriented constructs. Security is state of the art meeting NIST and NSA Suite B requirements.

The design of iCLASS Seos enables software only java card emulation in NFC phones. When emulating iCLASS Seos in NFC phones there is no need for proprietary encryption hardware (as needed for MIFARE).

Aperio supports reading SIO data from iCLASS Seos credentials using ISO/IEC 14443A RFID technology. Encryption and authentication used is AES-128. The maximum data size is 384 bits. The UID is random and not reported to the EAC.

For physical credentials, no lock configuration is required by the user, all encryption keys are pre-loaded. A separate configuration is needed to use mobile phone credentials, as different keysets are used. At the time of writing it has not been determined if this configuration is to be done in the field or production (as physical Elite), in development.

Physical cards are available from HID Global and ordered the same way as iCLASS cards. Mobile phone credentials are supported and will be available via the ASSA ABLOY SEOS platform in development at the time of writing.

4.1.11 Elite Credentials

As mentioned in previous chapters Elite credentials are supported for iCLASS, Seos and SE credentials. Elite is a customer specific key set different from the standard key set which is the default in the readers. The Elite credentials are created by HID and the Elite keys need to be applied to the Aperio reader via configuration cards.
Depending on the product and region, Aperio readers may be configured by the customer (installer/system integrator) or be pre-configured for Elite in the factory.

4.1.12 Mobile Credentials

With Aperio V2SE and V3 we can support mobile credentials via NFC/HCE. The technology used is iCLASS Seos which allows for soft emulation of cards in mobile phone supporting NFC.
As with Elite the key set is different from the standard and needs to be applied via configuration cards. The HID Mobile Access portal and mobile application can be used to create, administrate and use the mobile credentials.

4.1.13 Legic

Aperio supports:

- Legic Prime MIM22, MIM256 and MIM1024 credentials
- Legic Advant ISO14443A and ISO15693 credentials

A Legic credential consists of a UID (4, 7, 8 or 10 bytes) one or several data segments, the data segment are identified using a segment number, search string and segment type.

In order to read Legic data segments, the Aperio lock needs to be configured via the PAP tool. The following parameters are configurable:

- Search string (optional, if not set, the search string is ignored)
- Segment type (optional, if no type is set the segment type is ignored)
- Start segment for searching (mandatory, i.e. first, second, third etc)
- Start address and length of the data to be read within the segment (mandatory)
- CRC Consistency check (optional, can be used on segments including checksum protection)

Aperio can read up to 45 bytes of segment data.

Aperio supports the LEGIC Master-Token System Control (MTSC) meaning it can be launched with a Master-Token SAM 63 contactless smart card which contains a unique genetic code. This genetic code ensures the secure connection of cards and readers.

4.2 Low Frequency

4.2.1 HID Prox

This HID 125 kHz card technology supports formats up to 85 bits; however the most common format is 26 bits Wiegand output.

The data read by Aperio is identical to the data that an HID Prox standard reader would read.

HID Prox uses FSK modulation.

4.2.2 EM Prox (EM41xx/EM4450CSN)

This card operates at 125 kHz. Aperio reads out 40 bits (EM41xx) or 32 bit CSN (EM4450) from the card and sends them to the EAC in a raw format; therefore, the data in the card is not previously processed.

EM Prox uses ASK modulation.