MORPHOACCESS

DES*Fire* terminals

Two new MorphoAccess terminals, the MA221D and OMA221D, were introduced in early March 2005. Both terminals include the possibility to detect fake fingers and function solely in verification mode. The MA221 D is an indoor terminal whereas the OMA221 D can be used both indoors and outdoors. MA221D and OMA221D are designed to read DESFIRE contactless smart cards.

DESFIRE is a technology that complies with the ISO14443-A standard for contactless smart cards. This technology improves the level of security of the communication between card and reader. The security relies on the use of a 3-DES encryption algorithm. Communication between card and reader requires first a mutual authentication and the establishment of a session key. This session key is used to encrypt all the data exchange between card and reader.

Another improvement comes from the data management on the card. Data is no longer stored in blocks and sectors as was case with MIFARE. DESFIRE introduces the notion of “application” and an “application” may require several files, each of them possibly protected by keys.

DESFIRE technology is implemented on the MA/OMA 221D as a biometric application managing one file.

Our solution contains communication protection of both the card/terminal and the terminal/host.

1 MA221D & OMA221D operating mode

These terminals only operate in verification mode. Multi-factor authentication is possible when combining card, fingerprint and password (or PIN). MA/OMA221D provides the possibility to return the ID through a secure encrypted TCP/IP-based communication protocol. However, the standard set of MA interfaces remains but is not secure: Wiegand, Data & Clock and RS.422. This standard relay can be activated if needed.

2 Key Management

Overall, five keys are required to manage the card/terminal and terminal/host communication.

Regarding the card, these keys are:

- The badge master key (PICC_MASTERKEY)
- The application master key (APPLICATION_MASTERKEY)
- The biometric file master key (BIO_FILE_READ_MASTERKEY)

It is important to note that the biometric file master key is not directly used to read the biometric file on the badge. Indeed, the badge serial number and the BIO_FILE_READ_MASTERKEY are used to derive the effective key that controls the reading of the badge. Thus even if a badge is compromised, the file master key remains valid.

Regarding the terminal, these keys are:

- The MorphoAccess master key
- The MorphoAccess network key
- The biometric file master key (BIO_FILE_READ_MASTERKEY)

The MorphoAccess master key is used to renew some keys such as the network key.
The MorphoAccess network key is used to secure the communication between the host and the terminal.

The biometric file read master key is needed to read the biometric file on the card. When the MA is installed for the first time, default transport keys are used to communicate with the terminal. This gives users the possibility to replace the transport key.

The key management is performed through a service called “Service Safe”. “Service Safe” manages the base key and the network key required to communicate with the MA. The BIO_FILE_READ_MASTERKEY master key management should be transferred from this service to the MA. A DLL is supplied to load the key in “Service Safe”.

3. Communication with MA terminals

The host communicates with the MA through an encrypted TCP/IP communication. Each communication requires mutual authentication between host and terminal as well as session key establishment. In addition, all the data exchanged is 3DES encrypted. Two communication channels exist. The server channel is used to manage the MA terminal from the host. The client channel is used by the MA terminal to return the ID to the host.