AUTEC - UPDATE

Highest security of badge data:
Key diversification

Dear Sirs,

With the “Key diversification” feature of XMP BABYLON the access control security can be increased in substantial way. Currently, this feature is available in connection with Mifare ® DESFire and UHF badges. Each project identification card is equipped with an individual (derived / diversified) key, which is spontaneously calculated by the system to realize the authentification process to get access on card memory. The use of this function presupposes a preceding encoding of the badge with an appropriate key on the basis of an adequate computation algorithm.

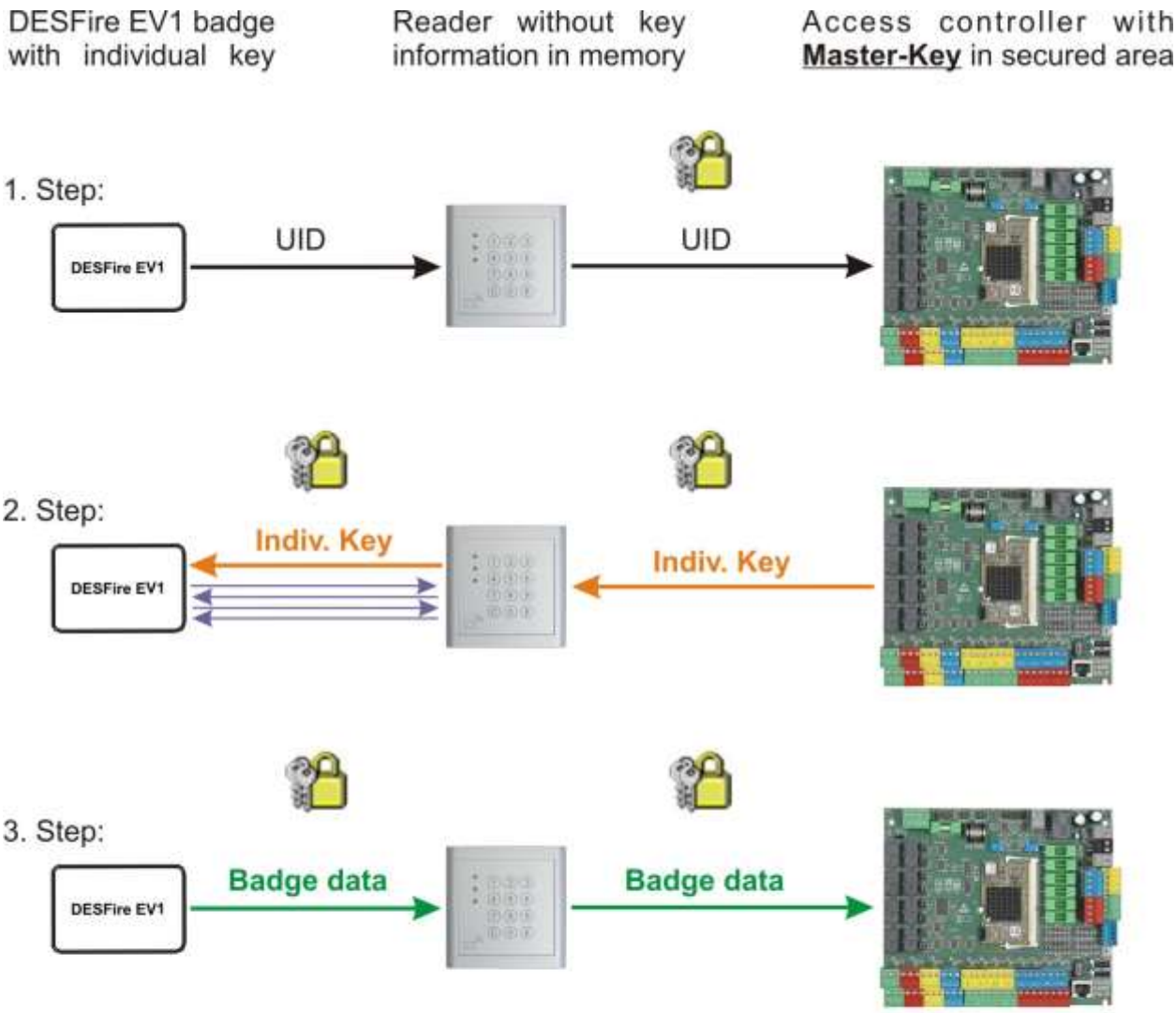
This option protects the project as a whole if possibly the safety key of a single badge was found out by not authorized „third parties“. In this case the respective badge must be removed from project. The project as a whole, however, remains uninfluenced because the knowledge of this one key is insignificant for other project badges.

A substantial advantage of this feature consists of the fact that the safety keys must not be loaded into the card reader – as in the standard case - but are transmitted from door control unit to the card reader during the encrypted communication process.

The diversified (derived) key is calculated by the door control unit on basis of the badge UID and a project master key. This project master key can be provided only with a special security dongle. This security dongle is also required to load the project master key into the respective door controllers or into the TMC3500 card readers. After having finished the download the security dongle must be deposited in a secured range of the customer (safe or security container).

AUTEC Gesellschaft für Automationstechnik mbH | Bahnhofstraße 57 – 61 b | D-55234 Framersheim
Phone: +49 6733 9201-0 | Fax: +49 6733 9201-91 | E-Mail: verkauf@autec-gmbh.de | Internet: www.autec-gmbh.de
Managing Director: Dr. Hartmut Stärke | Amtsgericht Mainz, HRB 32164 | Steuernr: 08/666/0614/6
Bank details: Deutsche Bank Alzey | BLZ: 545 700 94 | Kto-Nr: 3540101 SWIFT: DEUTDESM545 | IBAN: DE64 5457 0094 0354 0101 00

Schematic diagram of the Key Diversification:



= Encrypted communication (AES/SecuCrypt)

UID = Unique Identifier (Serial number)

Indiv. Key = Individual Key

AUTEC Gesellschaft für Automationstechnik mbH | Bahnhofstraße 57 – 61 b | D-55234 Framersheim
Phone: +49 6733 9201-0 | Fax: +49 6733 9201-91 | E-Mail: verkauf@autec-gmbh.de | Internet: www.autec-gmbh.de
Managing Director: Dr. Hartmut Stärke | Amtsgericht Mainz, HRB 32164 | Steuernr: 08/666/0614/6
Bank details: Deutsche Bank Alzey | BLZ: 545 700 94 | Kto-Nr: 3540101 SWIFT: DEUTDESM545 | IBAN: DE64 5457 0094 0354 0101 00

Order number	Functions
 XMP-NT-140	**ID/NT Badge layout software.** Badge encoding and/or Badge layouts and employee's photographs are processed **in standard BMP/GIF/JPG format.**
 XMP-NT-141	**Dongle for Key Diversification.** Definition of the Master-Key and download into the access controller / reader (Mifare ® DESFire and UHF badges)
 XMP-K12-F13	**Software extension of the Key Diversification for K12** (Mifare ® DESFire and UHF badges)
 XMP-K32SX-F13	**Software extension of the Key Diversification for K32SX** (Mifare ® DESFire and UHF badges)
 XMP-K32-F13	**Software extension of the Key Diversification for K32** (Mifare ® DESFire and UHF badges)
 XMP-TMC3500-F13	**Software extension of the Key Diversification for TMC3500** (Mifare ® DESFire and UHF badges)

If you have any further questions, please do not hesitate to contact us.

Yours sincerely,

Your AUTEC - Team

AUTEC Gesellschaft für Automationstechnik mbH | Bahnhofstraße 57 – 61 b | D-55234 Framersheim
Phone: +49 6733 9201-0 | Fax: +49 6733 9201-91 | E-Mail: verkauf@autec-gmbh.de | Internet: www.autec-gmbh.de
Managing Director: Dr. Hartmut Stärke | Amtsgericht Mainz, HRB 32164 | Steuernr: 08/666/0614/6
Bank details: Deutsche Bank Alzey | BLZ: 545 700 94 | Kto-Nr: 3540101 SWIFT: DEUTDESM545 | IBAN: DE64 5457 0094 0354 0101 00