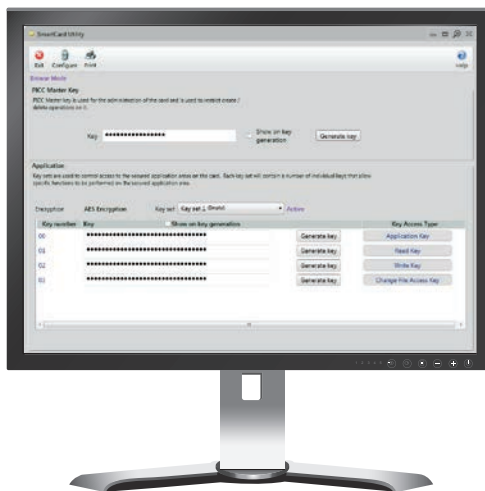


AC2000 Smartcard Utility User Defined Keys



Key Features

- AC2000 Smart card key management utility
- Advanced Encryption Standard (AES)-128-bit
- Random & Manual Key generator
- Create, encode and manage user defined AES-128-bit Keysets
- Seamless smartcard encoding/enrolment process
- Option for both Private Secure Number (PSN) or Public Unique Identifier (UID) card number encoding
- Hardcopy printout for 3rd party system compatibility
- Key rolling provision for extra level of security redundancy
- Minimal impact on day to day operations
- Organisations obtain full ownership of key management functions
- Convenient approach to key management; no requirement for configuration cards
- Auditable system logs

The AC2000 Smartcard Utility is a dedicated, Advanced Encryption Standard (AES)-128-bit, key management application.

The Smartcard Utility allows users to securely define, manage, and encode card reader and blank DESfire EV1/EV2 smartcards with user defined encryption keysets. Keysets are then downloaded via a secure Ethernet network to all CEM readers.

A fail-safe solution is also provided in the form of the "AC2000 Key Rolling" feature. AC2000 key rolling involves the CEM Smart Card Utility providing an additional secondary Keyset, which is also encoded during the smartcard encoding/enrolment process.

The secondary/redundant keyset, with its own unique encryption keys, can be implemented (Key rolled) via the AC2000 smart card utility application. All CEM connected readers will be updated via the secure Ethernet network to begin utilising the secondary keysets encryption keys.

The CEM smartcard utility allows organisations to take full ownership of their smartcard personalisation process; independently of third party card manufacturers.

Organisations will also be offered a convenient approach to smartcard key management, without the need for configuration cards. If the organisation's encryption keys become compromised, this flexible approach to smart card key management and encryption key updates insures minimal impact to day-to-day operations.

Key set generation

A keyset template is provided within the AC2000 smart card utility. System administrators can manually enter the encryption keys or use a randomised key generator. All keys will be generated or manually entered in hexadecimal format. Each keyset is made up the following keys:

PICC/Master Key – 16 Character Hex Number (64 bits) – Access to the DESfire EV1/EV2 smartcard, is managed via the PICC/Master key. Used for administration of all operations on the card.

Application Key – 32 Character Hex Number (128 bits) – Used to authenticate access to an application area on a DESfire EV1/EV2 card.

Read Key – 32 Character Hex Number (128 bits) – Used for authentication before reading the Private Secure Number (PSN) or Unique Identifier number (UID)

Write Key – 32 Character Hex Number (128 bits) – Used for Authentication before writing PSN to an application area

Change File Access Key – 32 Character Hex Number (128 bits) – for future use

Key Rolling

The AC2000 Smart card utility encodes two keysets into the blank DESfire EV1/EV2 smart card during the encoding/ enrolment process. Only one keyset will be active at any one time. The secondary keyset will remain dormant. If keyset one becomes compromised, system administrators can then use the smart card utility to update the CEM connected readers to begin using the second keyset on the DESfire EV1/EV2 smart cards.

Card encoding/enrolment

The AC2000 smart card utility encoding process, involves AC2000 creating two unique application areas within the blank DESfire EV1/EV2 smart cards. Both application areas are secured using unique AES-128-bit keysets. Within each secure application area, a 32-bit PSN will be written to a secure file area. Each application area will have the same 32-bit PSN.

Prior to card enrolment/encoding, administrators must choose the card number they would like to validate against the cardholder. Administrators will have a choice to validate either a UID, sometimes known as the card serial number (CSN), or the PSN.

Once a selection has been made, all cardholders will be enrolled against either the PSN or UID. All blank DESfire EV1/EV2 cards will be encoded /enrolled via the HID Omnikey 5422 encoder.

There are two options available for third party systems to utilise the customer specific DESfire EV1/EV2 smart cards.

Option One – Shared public card number (UID)

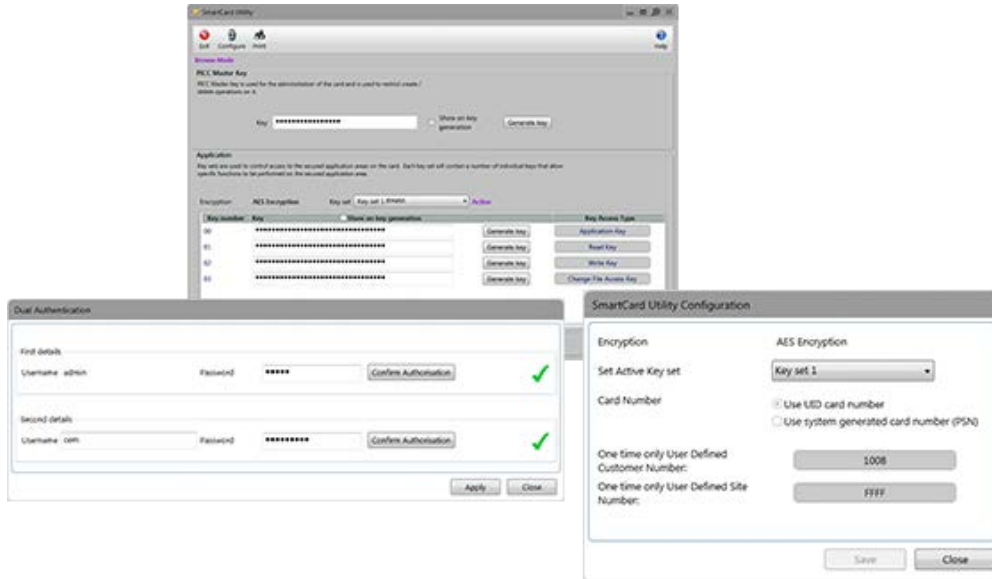
This option can be used if the UID option was chosen as the validation number, prior to card enrolment using the AC2000 smart card utility. The CEM access control readers will use AES-128-bit authentication before reading the UID from the DESfire EV1/EV2 smart card. Third party readers would read the DESfire EV1/EV2 smart card UID without any encryption. This option would typically be used by third party biometric readers, where the risk of card cloning is minimal due to biometric authentication.

Option Two – Private system card numbers (PSN)

Third party systems will be able to access the customer specific DESfire EV1/EV2 smartcards, if authorised to do so by the customer. To access the DESfire EV1/EV2 smart cards memory, third party systems would need to have authorised access to the PICC/Master Key. Customers will be provided with a keyset report/print option to share keysets with third parties if they wish to do so. This option is only available via dual authorisation. Once third part systems have access to the DESfire EV1/EV2 smart cards PICC/Master key, they will then have the ability to create their own application folders. This option would typically be used by third party cashless vending or secure printing systems.

Dual Authentication

Any changes to the AC2000 SmartCard Utility will require two system administrators with an authorisation level of four; to enter their username and passwords before the changes will take place.



Requirements

- AC2000 v7.0 upwards
- AC2000 Airport v7.0 upwards
- HID Omnikey 5422 DESFire EV2 Smartcard encoder/validation reader
- Blank DESfire EV1/EV2 Smart Cards 4K Bytes

(If future Applications are required Recommended 8K Byte Smart Cards)

Ordering Information

Product Code	Description
SW-SCUTILITY	AC2000 Smart Card Utility (User defined keys)
RDR/015/422	HID Omnikey 5422 DESFire EV2 Smartcard encoder/validation reader

Related Products



AC2000
AC2000 Airport



emerald
MiFare/
DESfire



S610f
MiFare/
DESfire



sPass DESFire smart card reader
sPass DESFire smart card reader with keypad

About Johnson Controls

Johnson Controls is a global diversified technology and multi-industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat.

For additional information, please visit www.cemsys.com or follow CEM Systems on LinkedIn and Twitter.

© 2020 Johnson Controls. All rights reserved. Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

CEM/B/356 Rev C

The power behind **your mission**

