

PREVENT CLONING AND REPLICATION



Security risks

Cloning - anyone can quickly copy RFID cards or fobs that have not been securely encoded. Cloning kits, including hand-held RFID reader/writers, are readily available from familiar online retail and auction sites for the price of a take-away pizza!

Replication - access cards of commonly used default formats can be purchased online without even needing an original to copy.

RFID door access systems that rely on card UID/CSN, or cards that use off-the-shelf formats without custom encoding, are vulnerable to these attacks.



Solution

Organisations need their own, well secured, custom RFID encryption keys that are used to encode their access cards and configure their card readers - protecting access controls from card cloning and replication attacks.

Key-ID Encoder is the secure DESFire card encoding solution that makes it easy, and cost-effective, for organisations to set and control private RFID encryption keys.

Multi-location card encoding and enrolment is supported by Key-ID Encoder. Hardware key store SAMs allow encryption keys to be shared without compromising security.

Key-ID Encoder features/specifications

Contactless RFID technologies supported	DESFire EV1, EV2 (MIFARE Classic and Ultralight options on request)
Key storage options	Software templates (plaintext and encrypted, with single password) NXP SAM AV2 (with user and admin passphrase security)
Card configuration options	Set/change card master key Set application ID and set/change application key Set file key number, file number and set/change file key
Credential encoding options	Industry-standard 26-bit format (8 bit facility code, 16 bit card number) 32 bit binary format (for backwards compatibility with CSN) Other formats available on request
Functions available	Create software template Create hardware (SAM) key store Random key generator Encode sequential cards Read, encode, revert single card

Key-ID Encoder compatibility

Operating systems	Windows 7, 8, 10
Licensing options	By reader serial number or embedded SAM license.
Smartcard reader / writers	Contactless (for DESFire card encoding) – most PC/SC desktop contactless readers, including Omnikey 502x, 5427, Identiv uTrust 3700 and 4701, ACS ACR1252 and ACR1222L (with LCD display and 3 SAM slots). Contact (for SAM reading/writing) – most PC/SC contact SIM readers.
Access control readers	Cards created with Key-ID Encoder have been tested for use on STID Architect range of secure DESFire door access readers, HID iClass readers with custom DESFire option, Aperio locks, and will work on most other readers capable of reading and decoding a DESFire card, due to the flexible configuration options available.
Other software	Key storage SAMs created with Key-ID can be used with Read-a-Card for secure DESFire card reading, keyboard wedge and PC/web application integration without risk of exposing security information. Key-ID encoded cards can be used with most enterprise pull-printing solutions such as PaperCut, with suitably-configured readers.

KEY-ID

Simple solutions for securing
identity-based access

www.key-id.com

UK HQ (Worldwide coverage)

+44 (0)1428 685 861

US Office (Northern and Latin America)

+1 562-262-9642

© 2019 Dot Origin Ltd.

