

# easyPAKS



- **Key generation**
- **Key administration**
- **SAM personalisation**
- **Key backup**
- **Key template administration**



## easyPAKS

easyPAKS implements a hierarchical key management system where the MSM is the core. It provides a simple handling system for PRO-TOS SAM's and is a core product with basic functionality to be extended easily on demand.

All keys are maintained inside the MSM and distributed with end-to-end security to SAMs and UserCards. The MSM serves as the main security nucleus in a background system. SAMs and UserCards may be personalized in accordance to user defined templates.

## Features

### Key Management (KM)

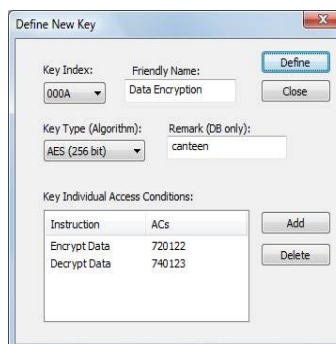
- Key generation
- Key backup
- Key restore
- Key deletion
- Key import (plain /encrypted)
- SAM template definition (define SAM type individual key sets for personalisation)

### SAM Personalisation (SP)

- Load keys
- Manual personalisation
- Mass personalisation (option.)
- View personalised SAMs
- Delete SAM from administration
- Test SAM
- Reset SAM

## Technical data

- The application design is based on a standard Windows MFC application written in C++
- Access rights to the application are verified (access card PIN verification)
- After start an empty application window is presented with a menu bar (Key Management, SAM Personalisation, Card Personalisation)
- MS Access database/ODBC
- All keys stored in the database for backup are encrypted



Define New Key

Key Index: 000A Friendly Name: Data Encryption

Key Type (Algorithm): AES (256 bit) Remark (DB only): canteen

Key Individual Access Conditions:	
Instruction	ACs
Encrypt Data	720122
Decrypt Data	740123

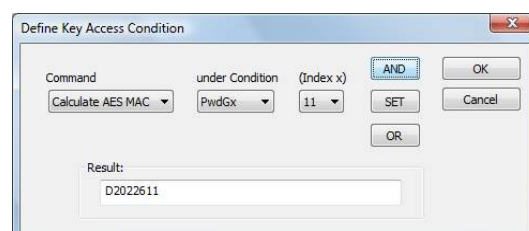


Enter Mental Key

Please enter first part of MTK

Input Hex Values (e.g. a0b1c3...):

Confirm Input:



Define Key Access Condition

Command: Calculate AES MAC under Condition: PwdGx (Index x): 11

Result: D2022611