SmartPGP

Peter Benčík

Marek Vančík

Jakub Martinka

Improvements

1) In place encrypt/decrypt

- Input and output buffer may be the same
- Better readability
- Performance – no useless copy

Improvements

2) Fill transient memory with random data

- Zeros → random data
- Better practice
- No memory separation (“000” blocks)

Improvements

3) Double checks on critical conditions

- Fault induction protection

Improvements

4) Random delay on crpyto-related parts

- Before sensitive operations
- Naive but modular implementation

Improvements

5) Tests (simulator)

- Verify PINs
- Set & Change PIN
- Set attributes (AES, RSA)
- Generate RSA keys
- AES Encrypt & Decrypt

POSSIBLE improvement

6) ALG_TRNG instead of ALG_SECURE_RANDOM

- Current kit: JC 3.0.4
- ALG_SECURE_RANDOM deprecated since JC 3.0.5
- Not changed - backward compatibility

Card compatibility problems and limits

No card support for JC 3.0.4

- Support for JC 3.0.3
- *signPreComputedHash()* since 3.0.4
- Result: can’t test or measure **sign** procedure

Performance testing

Results

Instruction	Time [ms]
0xCA - Get data	16.5
0xCC - Get next data	11.7
0x20 - Verify	66.7
0x24 - Change reference data	75.4

Performance testing

Results

Instruction	Time [ms]
0xDA - Put data	66.2
0x47 - Generate asymmetric key pair (2048 b)	19 649
0x2A - Security operation (Encrypt)	16.7
0x2A - Security operation (Decrypt)	16.9
0x2A - Security operation (Sign)	NA

Performance testing

Results

Instruction	Time [ms]
0x84 - Get challenge	19.1
0xE6 - Terminate DF	19.8
0x44 - Activate file	189

Summary

1) In place encrypt/decrypt

2) Fill transient memory with random data

3) Double checks on critical conditions

4) Random delay on crpyto-related parts

5) Tests (simulator)

6) Possible - ALG_TRNG