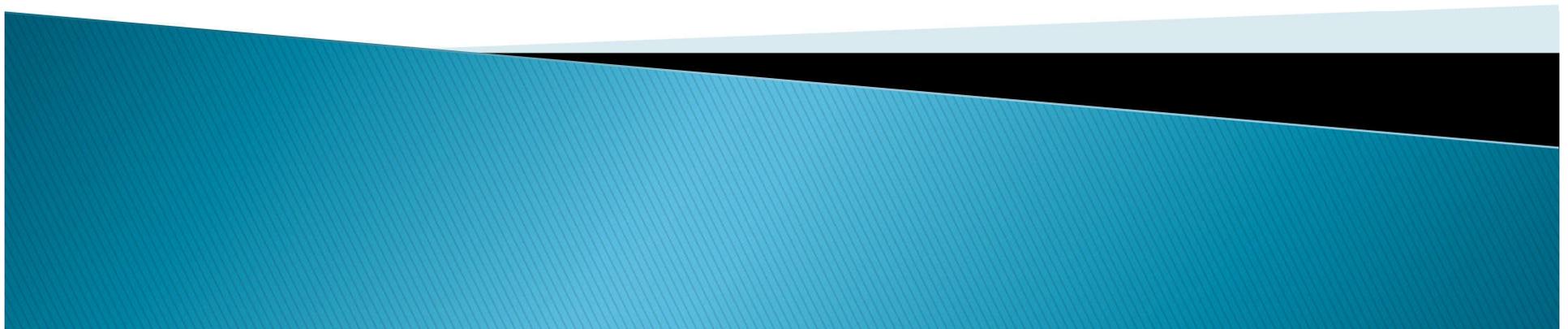


SmartNppCrypt

Matej Evin, Matej Kušnier, Simon Nespešný



Source Application

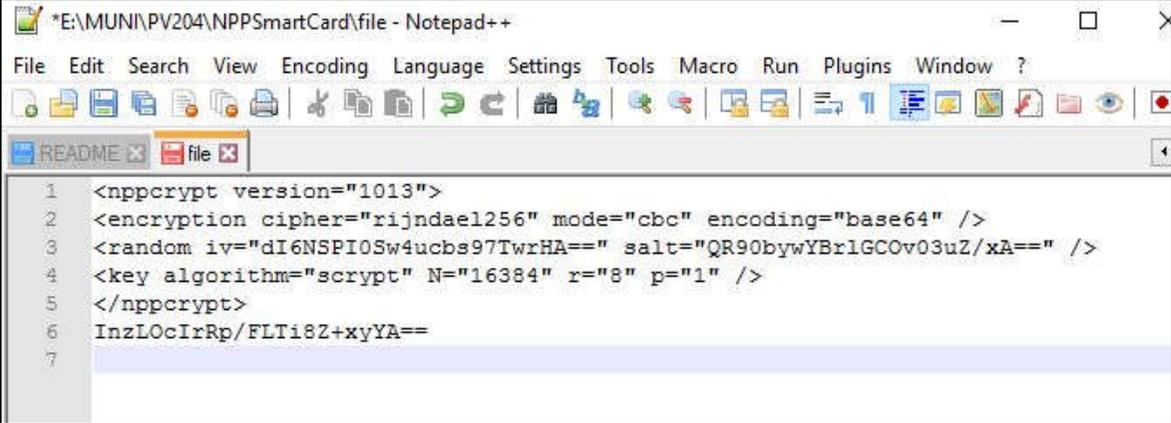
- ▶ <https://github.com/jeanpaulrichter/nppcrypt>
- ▶ Crypto plugin for Notepad++
- ▶ Functionality invoked by password
- ▶ Offers:

Symmetric file encryption/decryption

Various encoding options

Hash functions

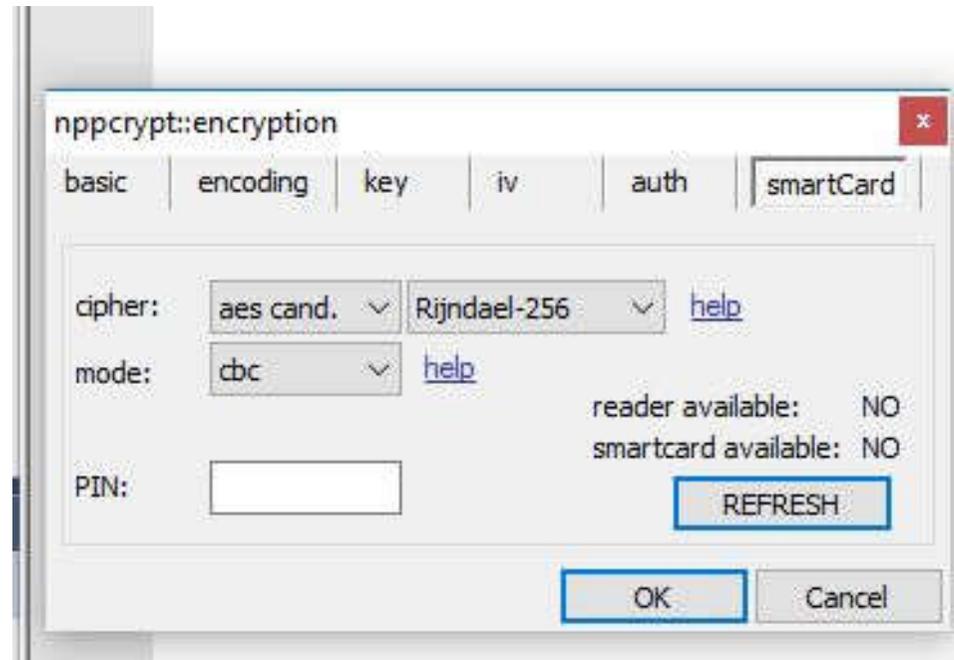
RNG



```
*E:\MUNI\PV204\NPPSmartCard\file - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
1 <nppcrypt version="1013">
2 <encryption cipher="rijndael1256" mode="cbc" encoding="base64" />
3 <random iv="dI6NSPI0Sw4ucbs97TwrHA==" salt="QR90bywYBr1GCOv03uZ/xA==" />
4 <key algorithm="scrypt" N="16384" r="8" p="1" />
5 </nppcrypt>
6 InzLOcIrRp/FLTi8Z+xyYA==
7
```

SmartNppCrypt plugin

- ▶ <https://github.com/gimlly/SmartNPPCrypt>
- ▶ JavaCard extension for NppCrypt
- ▶ Adds extra level of security
- ▶ NppCrypt retains crypto functionality
- ▶ Invoked by PIN
- ▶ Card stores KEK

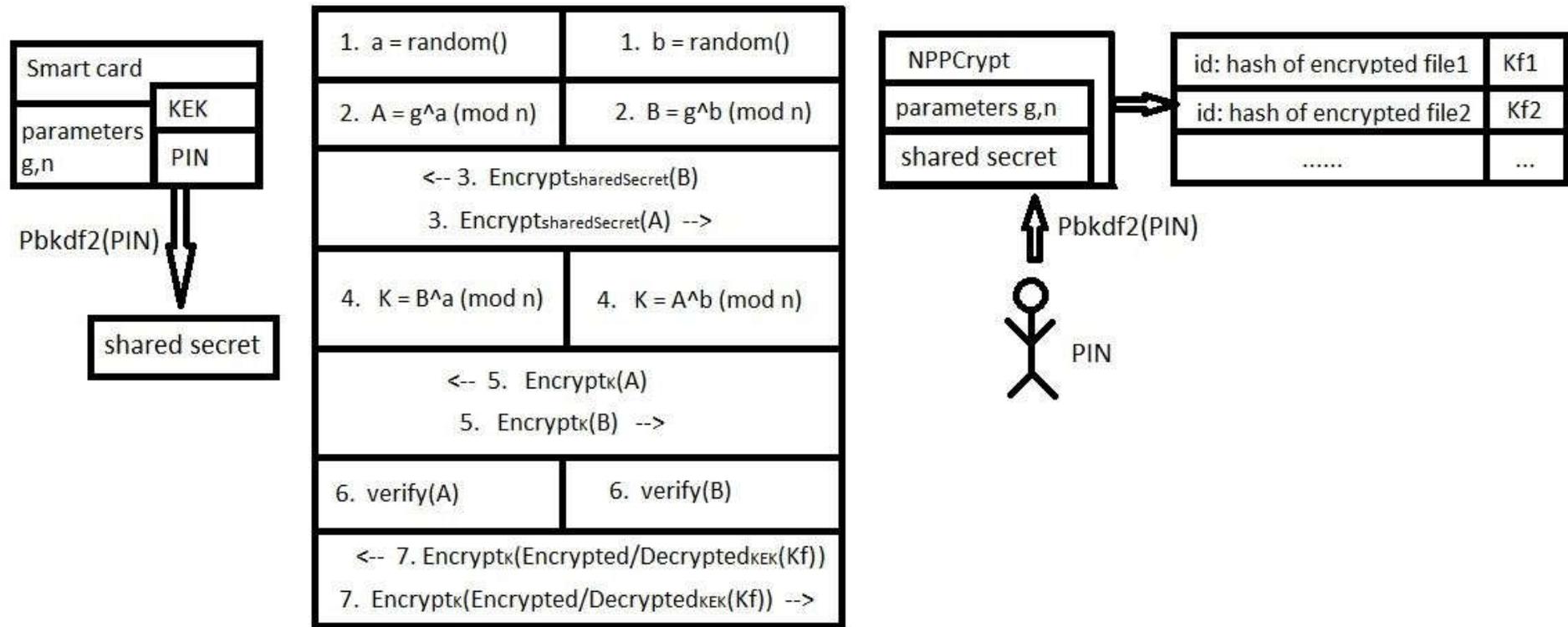


Secure Channel

- ▶ NppCrypt plugin is not in safe environment
- ▶ JavaCard is safe environment
- ▶ Pre-shared secret: PIN, $H(\text{PIN})$
- ▶ Session Key establishment: Diffie-Hellman (using RSA), public generator/modulus
- ▶ Channel security verification – PIN check



Secure Channel



JavaCard applet

- ▶ Establish secure channel
 - SecureRNG
 - RSA 1536
 - AES 128 CBC
 - SHA 256
- ▶ Encrypt/Decrypt using 128bit KEK
- ▶ Change PIN (up to 16 bytes)



Thank you for your attention

