OWASP #30
Authentication topic

Teemu Simonen
11.10.2016

FUJITSU
shaping tomorrow with you

Authentication factors

- Something the user knows
- Something the user has
- Something the user is

- Combined when need authentication
  - Web, Mobile, Users, Devices, Servers

Authentication Solutions

- Something the user knows
  - Username & Password
  - Smart Card PIN
- Something the user has
  - OTP list, PKI, Mobile devices, Token devices, Smart Cards
  - Biometrics
- Something the user is
  - Biometrics

Terveydenhuollon ammattihenkilö
Yrkesutbildad person inom hälso- och sjukvården
Voimassa 16.4.2009
Giltigt 16.4.2014
12345678912
Mallikorttilainen-Testaushenkilö
Saija-Maria
Proviisori
Provisor

Biometrics basics

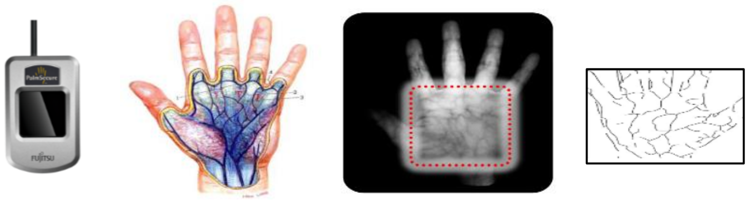
- FAR (false accept rate)
- FRR (false reject rate)
- Registration
- 1 to 1 verification
- 1 to N identification

Use case: Biometric authentication to web applications

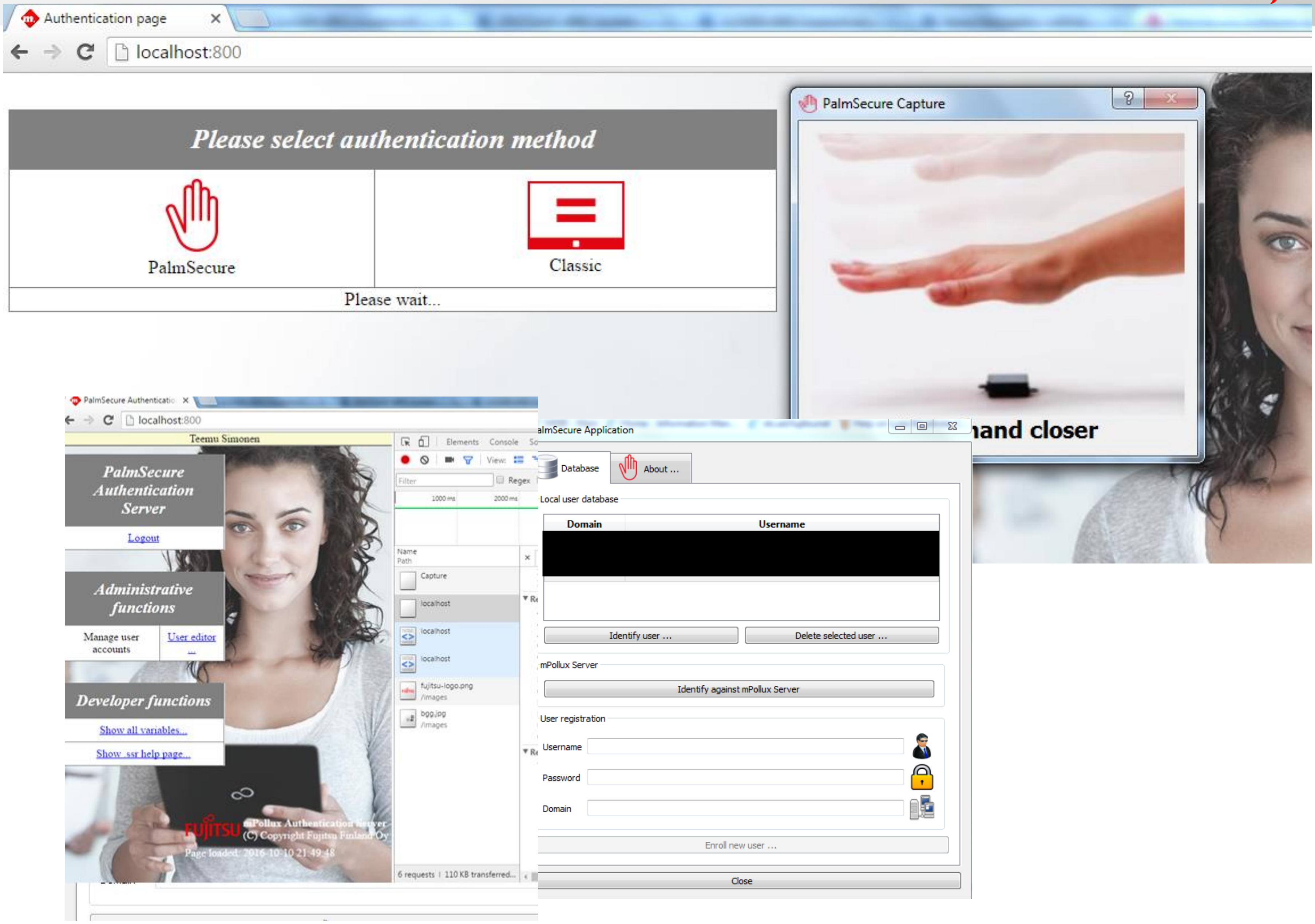
- Registration
  - Capture biometric data
  - Transform image into pattern data
  - Save data as biometric authentication template
- Authentication
  - Compare captured data against the saved template

Use case: Biometric authentication to web applications

- Demo: Using palm vein authentication (mPollux PalmSign with PalmSecure)
  - Web application
  - Log-in to desktop



Use case: Biometric authentication to web applications



Authentication page

localhost:800

Please select authentication method

PalmSecure	Classic
Please wait…	

PalmSecure Capture

…hand closer

PalmSecure Authenticatio…

localhost:800

Teemu Simonen

PalmSecure Authentication Server

Logout

Administrative functions

Manage user accounts	User editor …

Developer functions

Show all variables…

Show ssr help page…

mPollux Authentication Server
(C) Copyright Fujitsu Finland Oy
Page loaded: 2016-10-10 21:49:48

…almSecure Application

Local user database

Domain	Username
[redacted]	

mPollux Server

User registration

Username

Password

Domain

Use case: Biometric authentication to web applications

- PalmSecure®
  - Palm Vein Authentication based on vascular pattern recognition
  - Capture near-infrared image of unique palm vein pattern
  - FAR (false accept rate) 0.00001%
  - FRR (false reject rate) 1.0% F Pro sensor: 0.01% (one retry)
  - The maximum number for 1 to N identification authentication is 10,000 palms (5,000 persons if both hands enrolled)
  - http://www.fujitsu.com/us/solutions/business-technology/security/palmsecure/palmsecuresso/

Comparison FAR and FRR

- PalmSecure®
  - Palm Vein Authentication based on vascular pattern recognition
  - Capture near-infrared image of unique palm vein pattern
  - FAR (false accept rate) 0.00001%
  - FRR (false reject rate) 1.0% F Pro sensor: 0.01% (one retry)
- Apple fingerprint Touch ID
  - FAR (false accept rate) 0.002% (1 in 50,000)
  - FRR (false reject rate) unknown
  - https://support.apple.com/en-us/HT204587
- 4 digit PIN code guessing
  - FAR (false accept rate) 0.01% (1 in 10,000

Use case: Biometric authentication to web applications

- PalmSecure® Sensors:

	V2	F Pro (new model)
Temperature	0°C-60°C	-40°C-85°C
Sunlight	Max. 3,000 lux	Max. 80,000 lux
		Ability to correct hand movements

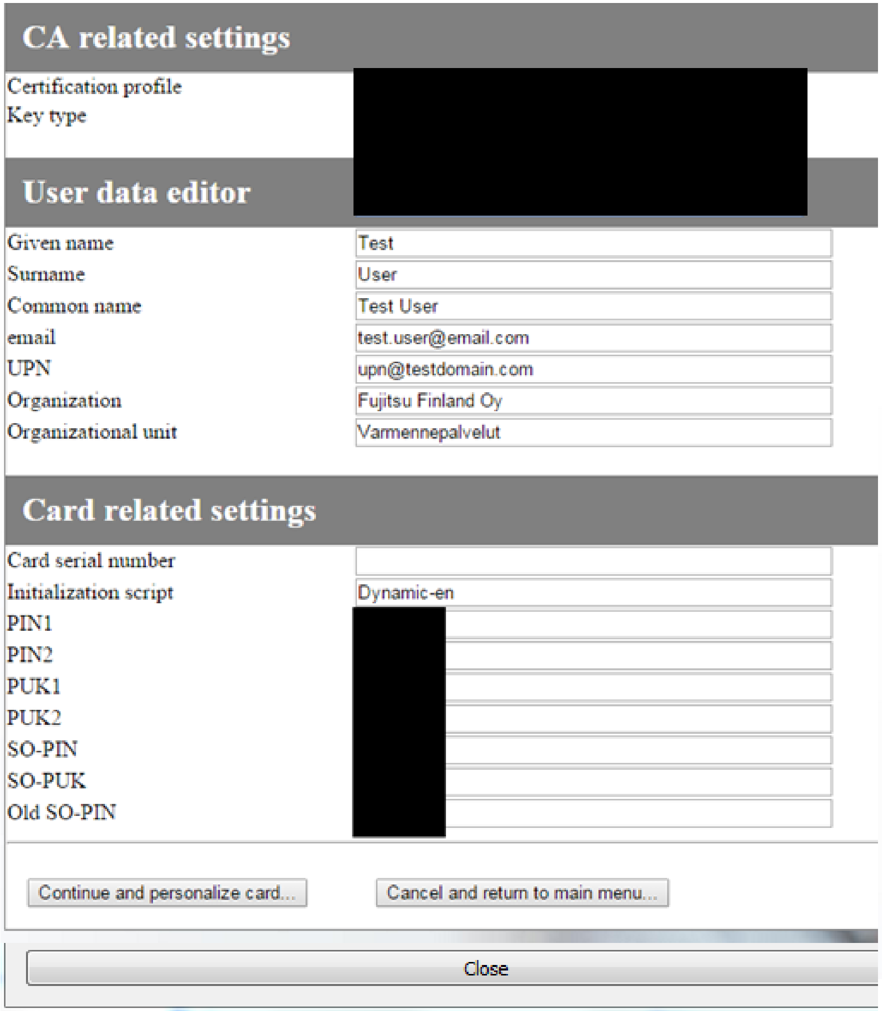
PalmSecure Sensor V2
(35mm×35mm×27mm)

PalmSecure-F Pro
(29mm×29mm×13mm)

http://www.fujitsu.com/global/about/resources/news/press-releases/2016/0912-01.html

Use case: PKI authentication in web application context can be easy

- Demo: Smart card personalization self-service



CA related settings

Certification profile	[redacted]
Key type	

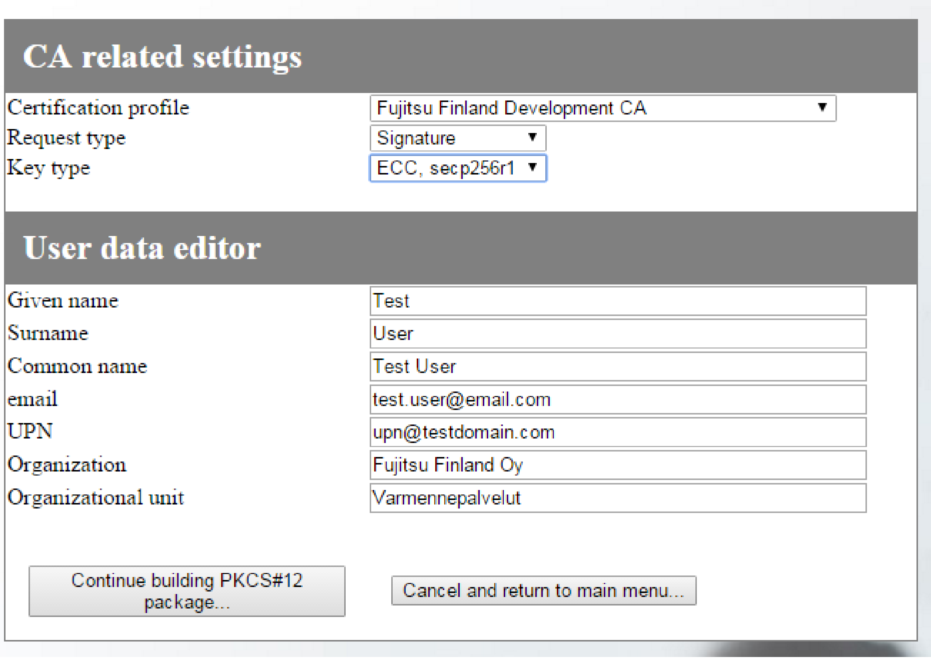
User data editor

Given name	Test
Surname	User
Common name	Test User
email	test.user@email.com
UPN	upn@testdomain.com
Organization	Fujitsu Finland Oy
Organizational unit	Varmennepalvelut

Card related settings

Card serial number	
Initialization script	Dynamic-en
PIN1	[redacted]
PIN2	
PUK1	
PUK2	
SO-PIN	
SO-PUK	
Old SO-PIN	

Continue and personalize card...
Cancel and return to main menu...
Close



CA related settings

Certification profile	Fujitsu Finland Development CA ▼
Request type	Signature ▼
Key type	ECC, secp256r1 ▼

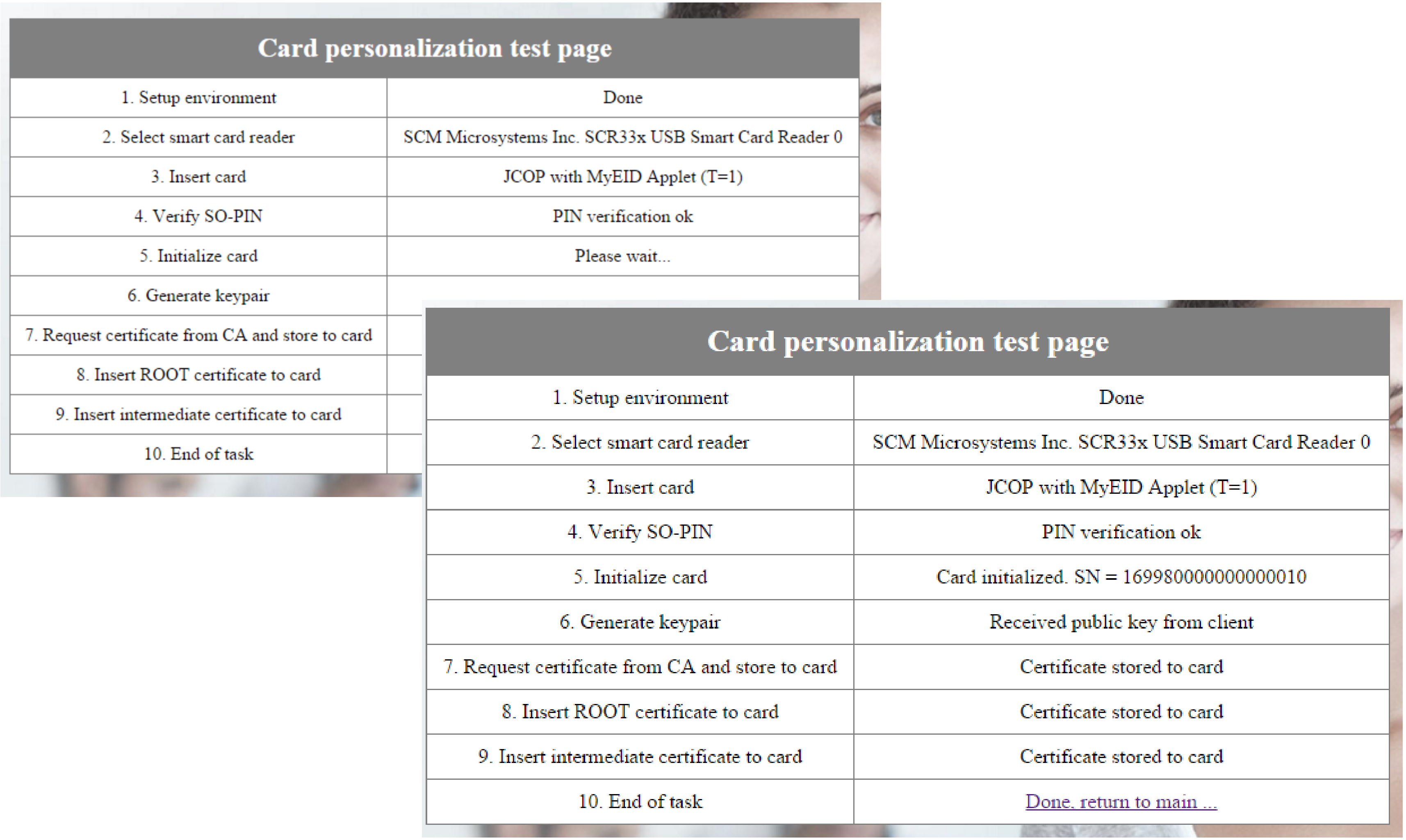
User data editor

Given name	Test
Surname	User
Common name	Test User
email	test.user@email.com
UPN	upn@testdomain.com
Organization	Fujitsu Finland Oy
Organizational unit	Varmennepalvelut

Continue building PKCS#12 package...
Cancel and return to main menu...

Use case: PKI authentication in web application context can be easy

- Demo: Smart card personalization self-service



Card personalization test page

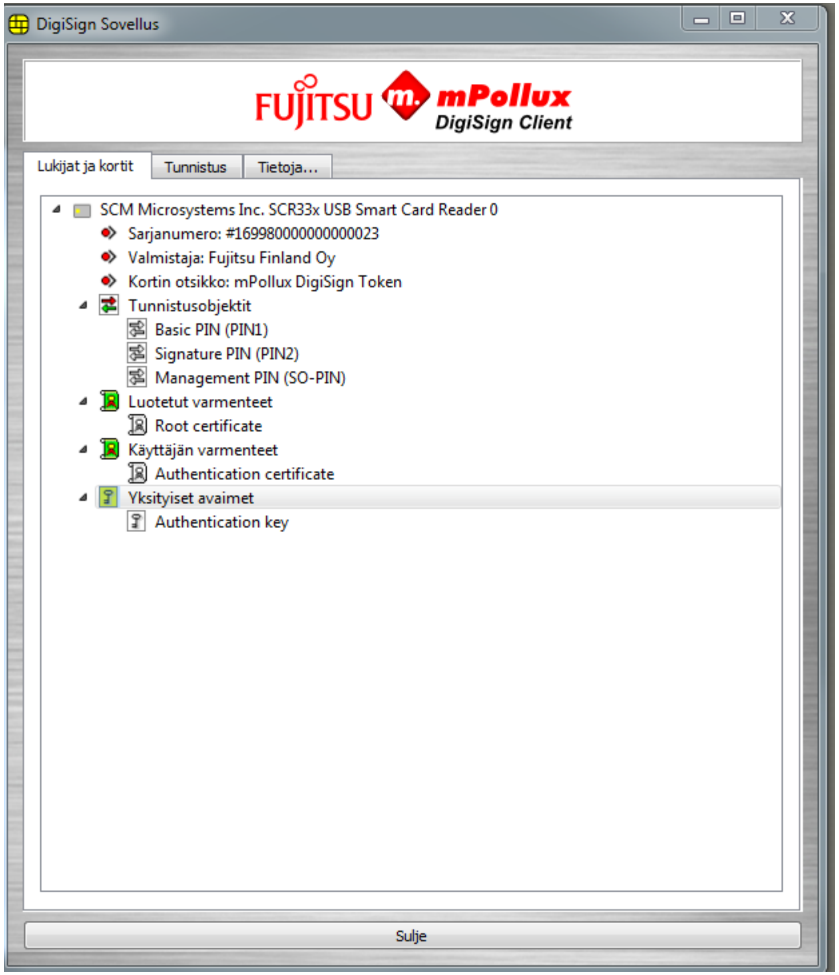
1. Setup environment	Done
2. Select smart card reader	SCM Microsystems Inc. SCR33x USB Smart Card Reader 0
3. Insert card	JCOP with MyEID Applet (T=1)
4. Verify SO-PIN	PIN verification ok
5. Initialize card	Please wait...
6. Generate keypair	
7. Request certificate from CA and store to card	
8. Insert ROOT certificate to card	
9. Insert intermediate certificate to card	
10. End of task	

Card personalization test page

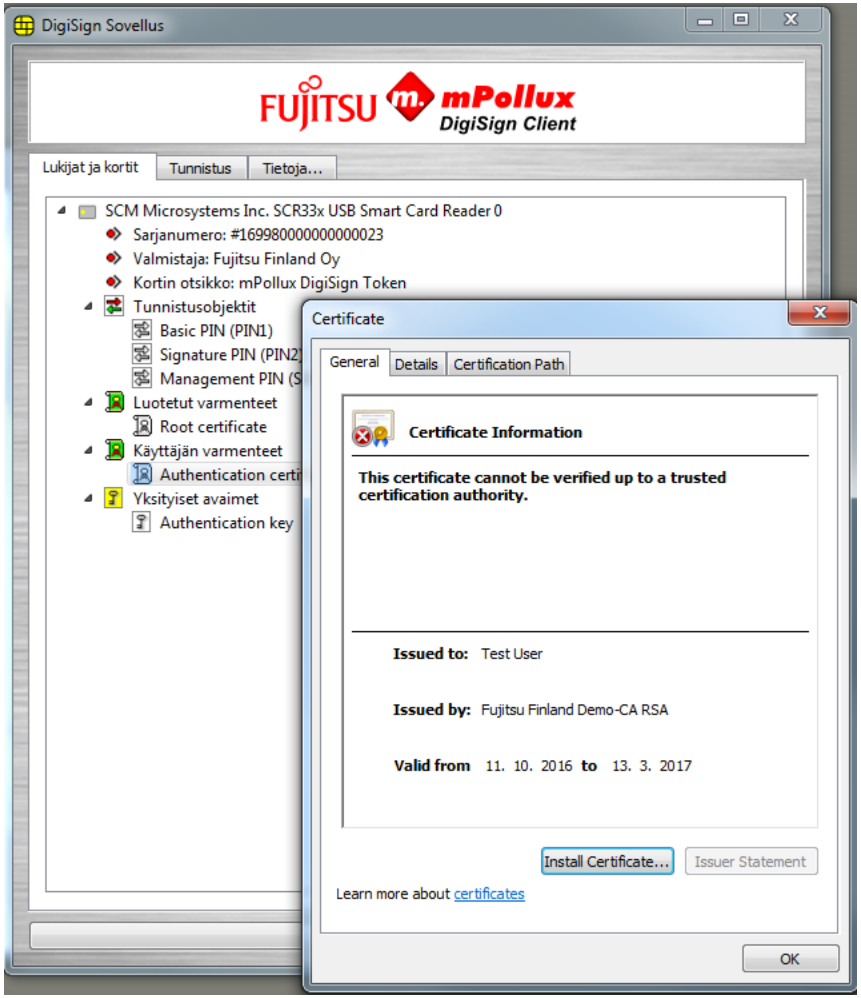
1. Setup environment	Done
2. Select smart card reader	SCM Microsystems Inc. SCR33x USB Smart Card Reader 0
3. Insert card	JCOP with MyEID Applet (T=1)
4. Verify SO-PIN	PIN verification ok
5. Initialize card	Card initialized. SN = 1699800000000000010
6. Generate keypair	Received public key from client
7. Request certificate from CA and store to card	Certificate stored to card
8. Insert ROOT certificate to card	Certificate stored to card
9. Insert intermediate certificate to card	Certificate stored to card
10. End of task	Done, return to main ...

Use case: PKI authentication in web application context can be easy

- Demo: Smart card personalization self-service



SCM Microsystems Inc. SCR33x USB Smart Card Reader 0
- Sarjanumero: #1699800000000000023
- Valmistaja: Fujitsu Finland Oy
- Kortin otsikko: mPollux DigiSign Token
- Tunnistusobjektit
  - Basic PIN (PIN1)
  - Signature PIN (PIN2)
  - Management PIN (SO-PIN)
- Luotetut varmenteet
  - Root certificate
- Käyttäjän varmenteet
  - Authentication certificate
- Yksityiset avaimet
  - Authentication key



SCM Microsystems Inc. SCR33x USB Smart Card Reader 0
- Sarjanumero: #1699800000000000023
- Valmistaja: Fujitsu Finland Oy
- Kortin otsikko: mPollux DigiSign Token
- Tunnistusobjektit
  - Basic PIN (PIN1)
  - Signature PIN (PIN2
  - Management PIN (S
- Luotetut varmenteet
  - Root certificate
- Käyttäjän varmenteet
  - Authentication certi
- Yksityiset avaimet
  - Authentication key

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: Test User

Issued by: Fujitsu Finland Demo-CA RSA

Valid from 11. 10. 2016 **to** 13. 3. 2017

Learn more about certificates

Document information & history

Title	Biometric authentication for web applications
Customer/Project	Fujitsu
Owner	Teemu Simonen
Classification	Unclassified

Date / Version	Author	Status	Reviewed by	Changes
10.10.2016	Teemu Simonen			First version
12.10.2016	Teemu Simonen			Added comparison FAR and FRR and certificate image

FUJITSU

shaping tomorrow with you