SKS – Secure Key Store
KeyGen2 – Token Provisioning Protocol
Executive Level Presentation
The Token Enrollment Enigma

Certificate Enrollment
- CMP
- SCEP
- CMC

Cryptographic APIs
- JCE
- PKCS #11
- CryptoAPI

Enrollment Using Browsers
- `<keygen>`
- “CertEnroll”

Smart Card Middleware
- “MiniDriver”
- OpenSC
- PKCS #11

Smart Card Standards
- GlobalPlatform
- PKCS #15
- PIV
- EMV
- ISO7816
- SIM
- JavaCard
- ICCD
- CCID
- .NET Card

Token Containers
- Mobile Devices
- Discrete Smart Cards
- Networked Devices

Other Requirements
- End-To-End Security
- PIN Deployment
- Etc.

Non-PKI Credentials
- OTP “Seeds”
- Information Cards
- Etc.

Q: How can you make this work?
A: By using tons of time, money and professional services!

There simply must be a better way…
Unified Token Provisioning

Issuer (CA)

KeyGen2 – Token Provisioning Protocol

Enhanced mobile device with embedded **SKS-compliant** security hardware

**SKS-compliant** smart card or USB memory stick

**SKS-compliant** networked device (router, switch, etc.)

Security tokens come in many “form factors”
**Universal Authentication Technology Support**

**PKI (Public Key Infrastructure)**
The current gold standard for strong authentication

**OTP (One Time Password)**
Excellent alternative to static passwords for accessing moderately critical services from arbitrary computers

**Information Cards**
Powerful way dealing with federated logins by for example providing the attributes (claims) required for accessing a resource rather than the user’s identity

Why select when you can have them all using a single enrollment process?
• Compatible with Existing Applications
• Dedicated Provisioning Scheme

Applications Using Cryptographic Keys

Issuer (CA)

KeyGen2
End-To-End Security (E2ES) protocol where the issuer and the SKS exploit a cooperatively created shared secret

SKS - Secure Key Store

- Device Certificate
- Attestation Private Key
- Credential Database
- Crypto Engine

Protocols and APIs:
- PKCS #11
- JCE (Java)
- SKS Native API
- CryptoAPI

Client Platform

• Networking
• JSON Processing
• Content Aggregation
• User Interaction

Embedded or Connected Device
For more information....

http://webpki.org/auth-token-4-the-cloud.html

The separation between authentication and payment solutions is only due to historical reasons, using SKS “a key is a key” 😊