SKS – Secure Key Store

KeyGen2 –Token Provisioning Protocol

Executive Level Presentation

WEBPKI
.ORG

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 ICCD
SIM JavaCard 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!*

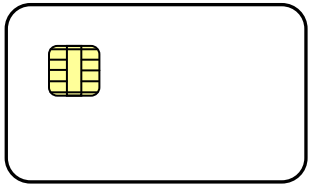
*There simply **must** be a better way…*

Unified Token Provisioning

Issuer (CA)

KeyGen2 – Universal Token Provisioning Protocol

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



SKS-compliant smart card

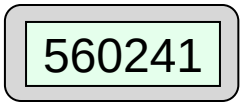
SKS-compliant USB memory stick or USB token

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

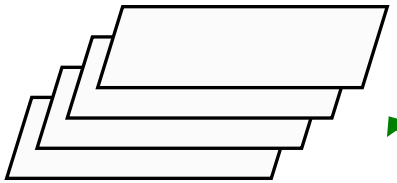
Powerful way dealing with federated logins by for example providing the attributes (claims) required for accessing a resource rather than the user's identity

Why select when you can have them all using a single enrollment process?

- Compatible with Existing Applications
- Dedicated Provisioning Scheme

Issuer (CA)

Applications Using Cryptographic Keys



JCE (Java)

CryptoAPI

PKCS #11

KeyGen2

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

Provisioning Proxy

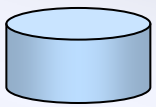
SKS Native API

- Networking
- XML Decoding
- XML Encoding
- Content Aggregation
- User Interaction

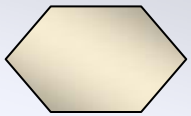
SKS - Secure Key Store

Device Certificate

Attestation Private Key



Credential Database



Crypto Engine

Embedded or Connected device

Client Platform

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" ☺