



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# PKCS#11 and Mac OS X Keychain Integration

Work in Progress

Ron DiNapoli

Cornell University, CIT/ATA



# Why Is This Needed?

- ◆ Apple Keychain Services is the recommended method (by Apple) for performing certificate based operations.
- ◆ The Keychain is the *only* mechanism through which certificate based operations can occur in Apple's native apps

Mail.app

Safari



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# What Does it Provide?

- ◆ Keychain/PKCS#11 integration allows any PKCS#11 device to be used via Keychain Services under Mac OS X (Tiger only)
- ◆ Operations currently supported (by infrastructure):
  - Signing operations
  - Encryption/Decryption
  - Changing PIN



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Why Doesn't Apple Provide This?

- ◆ Apple wants the user to simply “plug the token in and have it work”
- ◆ PKCS#11 doesn't quite have this experience
  - User would need to specify a PKCS#11 library to be dynamically loaded for the token in question



# How Does it Work?

- ◆ Beginning in Mac OS X v10.4 (Tiger) Apple added a component called *TokenD* to their security architecture
  - Used to handle hardware tokens
  - Some cards/tokens “supported” out of the box:
    - BELPIC, CAC, MuscleCard
  - OpenDarwin project available to let anyone define (program) their own TokenD



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# A Customized Tokend

- ◆ To add support for a new token:
  - Take existing Tokend project (OpenDarwin) and modify it.
  - Name resulting executable something different.
  - Place in `/System/Library/Security/tokend/`



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# How Many Tokends?

- ◆ Any system may have multiple Tokends
  - Installed in `/System/Library/Security/tokend/`
  - When token inserted, each tokend is launched and a standard method is called to determine if a given tokend should handle the inserted token



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Talking to the Token

- ◆ Once a Token has control, it may communicate with the token in any of the following ways:
  - Using built in methods and ISO-7816 commands
  - Using other libraries which handle communicating with the token, such as:
    - PKCS#11
    - OpenSC libraries



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# How Is PKCS#11 Used?

- ◆ PKCS#11 usually involves a shared library loaded at run time.
- ◆ How does Tokend know what PKCS#11 library to load?
  - Implemented a System Preference Pane
  - Manages a preferences file
  - The custom Tokend consults the preferences file to find out the name(s) of the available PKCS#11 libraries



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Preferences Pane

PKCS11

◀ ▶ Show All 🔍

Please specify up to three PKCS#11 libraries you'd like to use with tokend:

PKCS#11 Library #1:

Token ID String #1:

---

PKCS#11 Library #2:

Token ID String #2:

---

PKCS#11 Library #3:

Token ID String #3:

Turn on debugging  Show icon in Dock when tokend runs



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# What Is “In” the “Distribution”?

- ◆ Custom tokend daemon (tokend.PKCS11)
  - Installed in /System/Library/Security/tokend/
- ◆ Tokend/PKCS11 System Preferences Pane
  - Installed in /Library/PreferencePanes/
- ◆ Preferences file (tokend.PKCS11.prefs)
  - Installed in /Library/Preferences/



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Demonstration

Using `tokend.PKCS11`



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Limitations

- ◆ **No support for key generation**
  - Limitation of Tokend infrastructure
  - Enhancement request submitted (4479978)
- ◆ **No support for multiple certificates on a single token**
  - Still investigating where the problem lies
- ◆ **Limited vendor support for PKCS#11 (Mac OS X)**
  - Aladdin today
  - SafeNet (iKey) Q3 2006
  - OpenSC today



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

# Where Can I Get It?

- ◆ <http://ata.cit.cornell.edu/cit/ata/Project-PKI.cfm>
- ◆ Look for “Mac OS X PKCS#11 Token” in the sidebar.
- ◆ Source will be available
  - Pending Cornell’s deployment of SourceForge
  - Will require you have installed darwinbuild



Cornell Information Technologies  
ADVANCED TECHNOLOGY & ARCHITECTURES

Q&A

Any Questions?