

# Secure Lightweight Activation and Lifecycle Management

Nick Stoner  
Senior Program Manager

05/07/2009

**Actividentity™**

DIGITAL IDENTITY ASSURANCE

# Agenda

- Problem Statement
- Secure Lightweight Activation and Lifecycle Management Conceptual Solution
  - CMS Accessibility
  - The Secure Token
  - Versatile Authentication and LWA Service
- Sample Architecture
- Reduction in the Total Cost of PIV Card Deployments While Maintaining Security

# Problem Statement

- Activation of PIV cards generally must occur at “Full” enrollment or activation stations
  - Approximately 20% of Federal Employees must travel more than 25 miles to reach a full activation station
  - Activation stations must have middleware, matching software, drivers, and the appropriate readers to support card activation
- A Card Management System (CMS) is generally deployed within an isolated network
  - For standalone deployments on a single network, this is less problematic
  - For managed services, this prevents most users from being able to access CMS
  - Making CMS accessible outside isolated networks has large security and service availability concerns



## Problem Statement (continued)

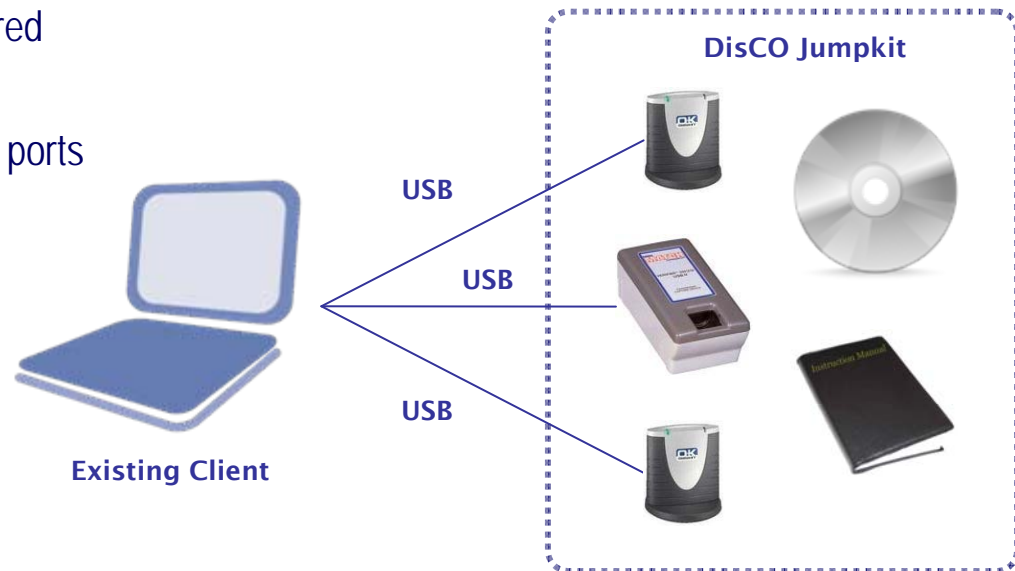
- The ability to perform biometric authentication as a means to begin activation is limited
  - Biometric fingerprint as a primary means of authentication is not always supported
  - Username / Password, Security Questions, Temporary PIN used instead
  - Support of alternative biometrics is very limited or non-existent
- These issues also apply to the card's lifecycle
  - Post-issuance updates, card unblock, certificate renewal, card renewal, suspend / resume, etc.
  - Some lifecycle use cases can be supported via help desk calls, which carry additional costs

# What is Needed to Solve These Problems?

- Make CMS accessible outside of isolated network
  - Must maintain level of security
  - Must provide serviceability
- A portable and secure mechanism for card activation and lifecycle events
  - Integration of all necessary activation and lifecycle management components into a small and portable package
  - Should not require installation of additional software on the client
  - Devices must support standards based secure communication channels
  - Device must be trusted and resistant to tampering
- Server to perform authentication and activation orchestration
  - Fingerprint biometrics as primary means of authentication
  - Tight integration with CMS to perform card activation and other lifecycle events
  - Provide a pluggable framework for use of other biometric types in the future
  - Support of standards based secure communication channels

# CMS Accessibility

- Standalone deployments will have less accessibility issues
- Managed Service Offering Distributed Card Operations (DisCO) Project
  - MSO CMS services to be publicly accessible
    - Proof of concept complete
    - Production deployment forthcoming
  - Remaining Challenges
    - Username / password still required
    - Jumpkit portability
    - Requires several available USB ports
    - Software must be installed
    - Untrusted client environment
    - Serviceability management



## The Client and Secure Token

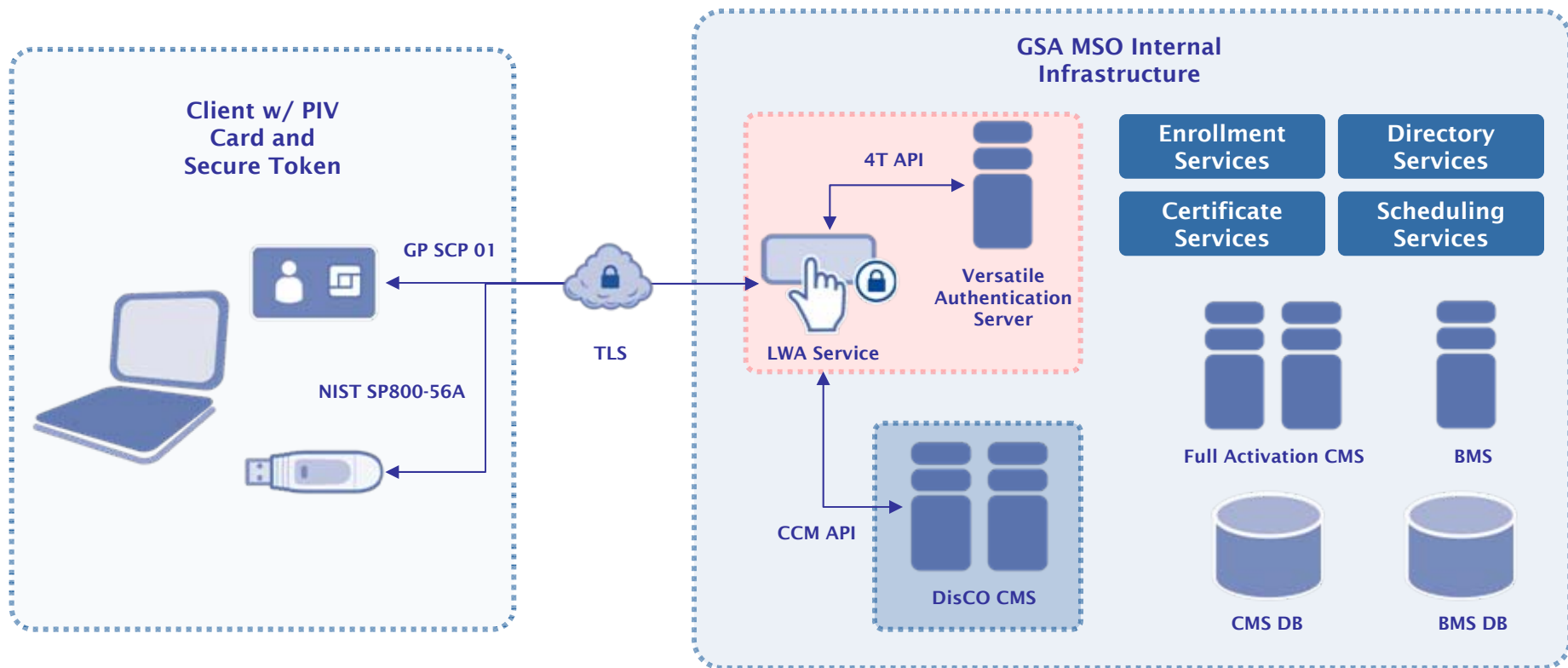
- Small, portable device with single USB interface
- Integrates
  - Secure, tamper resistant activation environment (FIPS 140-2 Level 2)
  - Biometric swipe sensor
  - Zero installation – activation and lifecycle management software resides on the token
- Client requires middleware and smart card reader (which would be needed to use the card anyways)
- Versatile Authentication Server is the only system that can access the token
  - Tokens are pre-provisioned from server
  - Protected by NIST SP800-56A compliant, 2048-bit PKI secure channel



## Versatile Authentication Server and LWA Service

- A Versatile Authentication Server provides a multi-channel authentication framework capable of supporting authentication via a variety of technologies
  - Username / password
  - Digital Certificates
  - One Time Passwords
  - Biometrics (fingerprint, voiceprint, etc.)
- Deployed alongside CMS and includes a service that orchestrates card activation and lifecycle management
- Establishes a secure channel with token for passing of biometric data
- Biometric matching occurs on the server
  - Prints are not stored on token or client
  - Service leverages prints from CMS database
- Leverages HSM for securing of keys

# Secure Lightweight Activation and Lifecycle Management Sample Architecture



# Reduce the Total Cost of PIV Card Deployment While Maintaining Security

- Reduce impacts to productivity
  - Cardholders are not required to travel to a full activation station
  - No need to install additional software on each client
- Reduce help desk calls
  - User can authenticate with biometrics
  - No need for out-of-band security questions or temporary PINs
- Leverage a single, portable device – the Secure Token
- Provide the ability to manage serviceability
- Implement a pluggable authentication framework to support alternative biometric types
- FIPS 140-2 Level 2 secured client environment
- Secure communication channel for all transactions

# Questions?

Nick Stoner

Email: [nick.stoner@actidentity.com](mailto:nick.stoner@actidentity.com)

Phone: 407- 927- 6695

**Acti**identity™

DIGITAL IDENTITY ASSURANCE