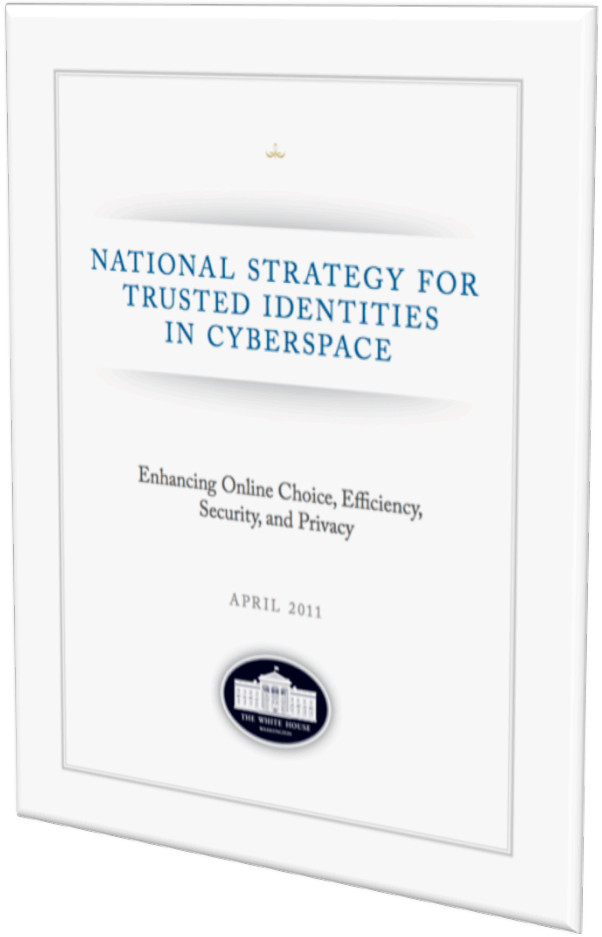
NSTIC Key Team AuthentID Solution: Eliminating Passwords via Strong Authentication

Exponent | HID Global | Gemalto

October 21, 2013

National Strategy for Trusted Identities in Cyberspace (NSTIC)

- What is NSTIC?
  - White House initiative to improve the privacy, security and convenience of sensitive online transactions
  - Goal of NSTIC is to create an identity ecosystem to authenticate presented credentials
  - Move away from the current practice of password-based authentication
  - Managed through the National Program Office (NPO) at NIST



Key Team Members

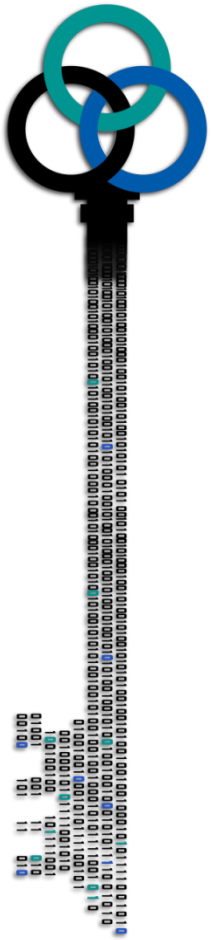
Pilot Partners

Supporting Partners

STANFORD COMPUTER SCIENCE

Experian™

Key Team Responsibilities



- Exponent®
  - Serve as the Team lead
  - Provide independent evaluation of the system and its interoperability
- HID®
  - Develop and deploy device management including mobile phone and computer components for PAD usage.
  - Deploy identity provider solutions to allow the use of authentication device credentials with relying parties
- gemalto security to be free
  - Provide secure elements and their identity applications, and will support software deployment to mobile network operators

NSTIC AuthentID Solution

- Our solution leverages two key concepts:
  - GICS, a Generic ID Card Command Set that allows widespread interoperability
  - OPACITY, a generic, standard, authentication and key agreement protocol optimized for fast contactless connections
- The proposed system consists of four major elements:
  - a device (a mobile phone or a wearable personal device) that contains a secure credential for a user,
  - a client that accesses and uses the device,
  - an authenticator that can verify credentials, and
  - a relying party that wishes to verify an element of the identity of a user.

Smartphone Recognition

- Detects watch
- Prompts for PIN
- Unlocks
- Locks

Laptop Recognition

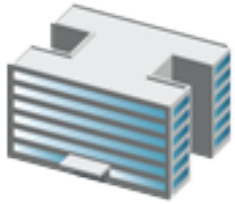
- Detects watch
- Prompts Fingerprint scan
- Account access privileges

Other Authentication Uses

- Office security
- Age identity
- Social media apps

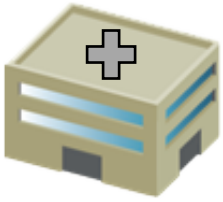
System Architecture

- Authentication Device
  - Container for a secure credential
- Client
  - Accesses and uses the secure credential
- Authenticator
  - Verifies authenticity of credential
- Relying Party
  - Entity needing verification of identity



Social

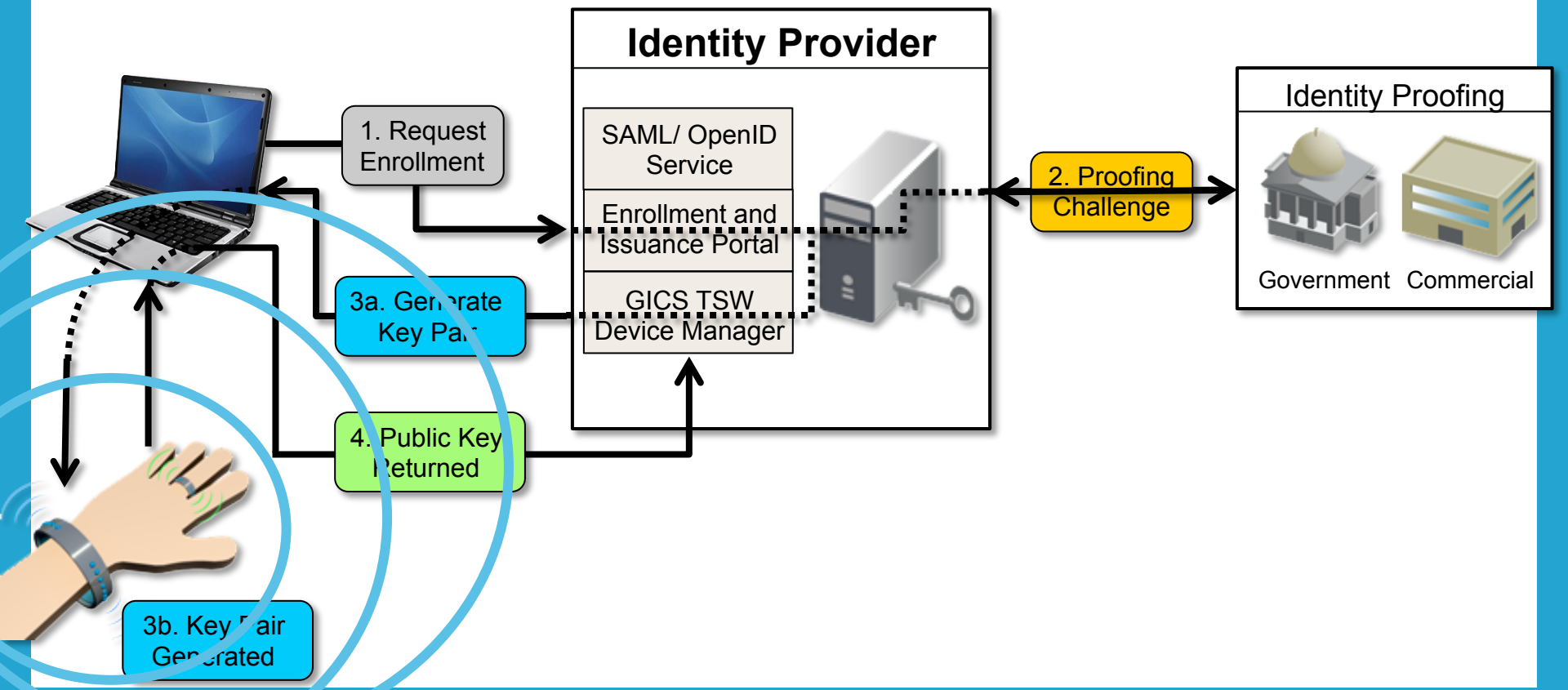
Government



Medical

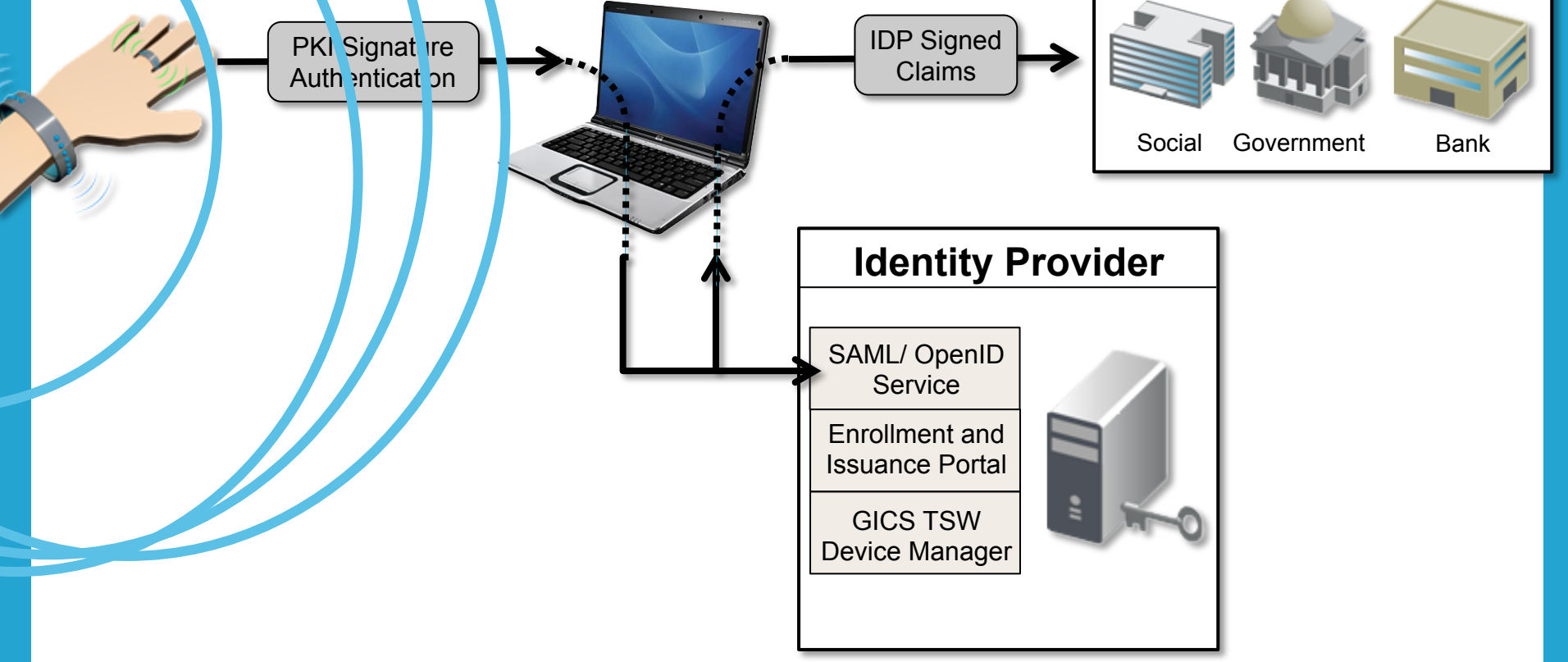
System Architecture

Credential Issuance Process



System Architecture

Authentication Process



Three Pilot Projects

- Government Pilot: Demonstrating NST
  FICAM Compatibility and Elevation o
  Trust from Derived Credentials

- Social Media Pilot: Strong Authentication with a Portable Identity Credential

- Healthcare Pilot: Strong Portable Credentials for Doctors

Use Cases

- **Social Media**
  a) Device: Mobile Phone
  b) Client: Mobile handset and browser,
  c) Credential: PKI
  d) Authentication: PKI to IDP and SAML to RP
  e) Provisioning: Win sync client over NFC + card emulation

Use Cases *(Cont'd)*

- **Healthcare**:
  a) Device: PAD w/ GICS container
  b) Client: Windows ActivClient
  c) Credential: PKI
  d) Authentication: PKI winlogon to MS domain
  e) Provisioning: Win sync client over NFC

Use Cases *(Cont'd)*

- **DMDC**:
  a) Device: Mobile GICS container
  b) Client: Mobile handset and browser
  c) Credential: PKI derived from CAC card
  d) Authentication: PKI to IDP and SAML to RP
  e) Provisioning: Win sync client over NFC or Mobile client (TBD)

Government: DMDC

- Current Status
  - DMDC and HID have demonstrated how CAC cards may be used with NFC enabled mobile platforms
  - Relying on OPACITY, a secure Contactless protocol
- Issues
  - User experience concerns still exists with the proposed implementation
    a) Frequent usage of NFC may impact the battery life of the phone
    b) Keeping the CAC card in contact with the phone for a lengthy period of time and frequently may not result in the best user experience
  - Finalizing OPACITY specs in FIPS 201-2 and availability of a reliable NFC stack on a critical number of phone platforms.

Government: DMDC *(Cont'd)*

- Specific Use Cases
  1. Tap your CAC card to your phone to enable the derived credential
  2. Use your phone derived credential to access a medium level protected web site
  3. When a web site is set to require higher level of Assurance, demonstrate that the end user is prompted to TAP the CAC card for that specific transaction
  4. Show that the derived credential does not work after a predetermined period of time (and another CAC Tap in is required)
  5. User disabling a derived credentials

     (tap or reset)

Summary

- The Team will deploy a standards-based identity authentication system that provides individuals with a portable identity credential that interacts with the system through a user-friendly process
- The guiding principles that drive our program include:
  - Privacy
  - Security
  - Interoperability
  - Convenience
- We're excited to develop our 3 pilots and provide lessons learned to the NSTIC community