

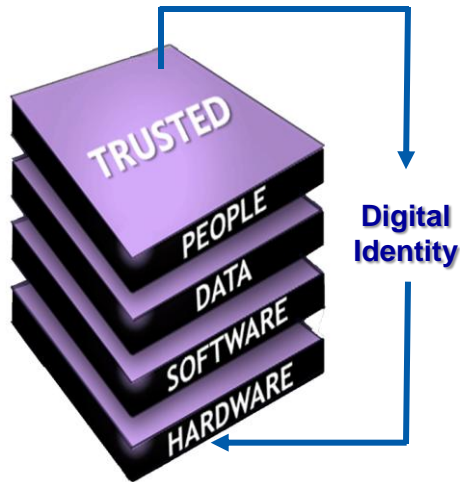
# Interagency Advisory Board

*Meeting Agenda, April 27, 2011*

---

1. **Open Remarks** (*Mr. Tim Baldrige, IAB Chair*)
2. **FICAM Plan for FIPS 201-2** (*Tim Baldrige, IAB Chair and Deb Gallagher, GSA*)
3. **NSTIC Cross-Sector Digital Identity Initiative** (*Keith Ward, Northrup Grumman*)
4. **FiXs, Helping Meet the OMB 11-11 Directive** (*Warren Blosjo, 3Factor*)
5. **Legal Implementation Challenges for NSTIC: Emerging Virginia Solutions for Credential Issuer Liability, Trademarks, and Remote Notarization** (*Tim Reiniger, FutureLaw*)
6. **Closing Remarks** (*Mr. Tony Cieri*)

# ***National Strategy for Trusted Identities in Cyberspace (NSTIC)***



## ***Cross-Sector Digital Identity Initiative***

May 2011

Keith Ward

*Northrop Grumman Information Systems – Defense Systems  
Director Enterprise Security & Identity Management  
Transglobal Secure Collaboration Program (TSCP) Vice Chairman*

# Overview

- **The National Strategy for Trusted Identities in Cyberspace (NSTIC)** identifies a set of guiding principles for accelerating the use of trusted digital identity credentials.
- **Solutions should be:**
  - ✓ Secure and resilient
  - ✓ Interoperable
  - ✓ Privacy enhancing and voluntary for the public
  - ✓ Cost-effective and easy to use
- **Deploying a system** that reflects these principles can help secure transactions on the Internet, improve the public's awareness and control of personal information, and stimulate the growth of online commerce.
- **It is prudent** to first create one or more Proofs of Concepts (POCs) in controlled settings to expose and close critical gaps before expanding to more ambitious trials that include real transactions with real people.

# Cross-Sector Digital Identity Project

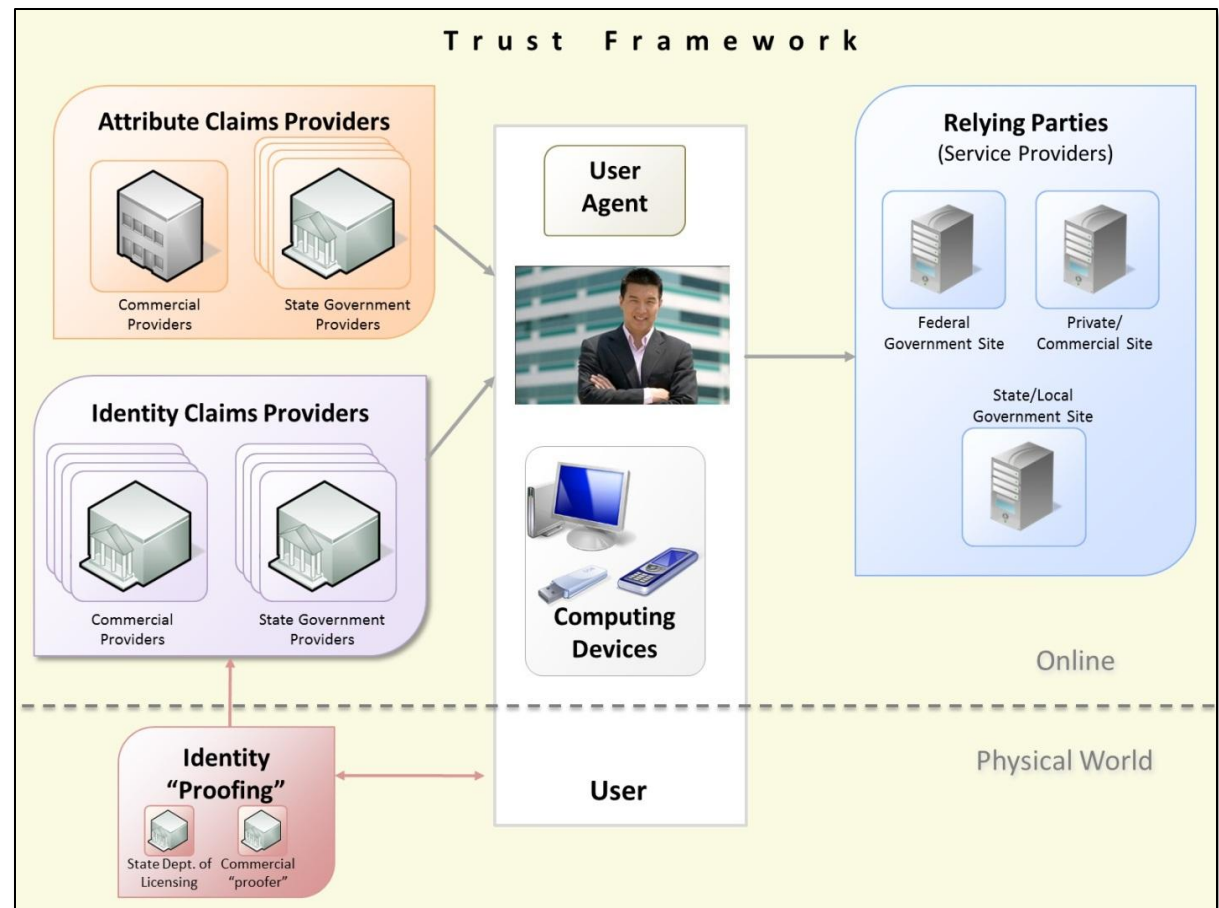
- **The Cross-Sector Digital Identity Project brings together** private and public sector participants to demonstrate, within those POCs, key NSTIC concepts and to identify barriers to adoption across technical, political, social and economic domains.
- **The goal of this POC** is to learn how to mature and optimize the architecture for a future pilot and eventual broad-scale production deployment. The analysis will investigate the readiness of technology, maturity of business models, social acceptance, policy coverage and usability.
- **Questions that will be addressed** by the POC include:
  - **Technical:** Is the feature set complete? Is the implementation sufficiently robust? Is the interface simple enough for the average user?
  - **Political:** Are existing policies and laws mature and comprehensive enough to enable high valued transactions? For example, can an online business meaningfully assess the risk of relying on a 3rd party identity claim?
  - **Economic:** Are the emerging business models compelling enough for ecosystem participants to enter the marketplace?
  - **Social:** Can new technology and public policy work together to help people feel more confident that they can control their information and that it will be used appropriately?

The proposed architecture focuses on empowering users to better protect their privacy. A key element is a User Identity Agent that provides a user with visibility and control over the flow of information between Claims Providers and Relying Parties. The agent can also help the user combine claims from multiple Claims Providers and present them to a Relying Party.

## Key Components

The POC will build a *user-centric identity ecosystem* consistent with NSTIC principles. The development of the POC will include:

- ❖ **Identity Proofer:** Verify the identity and/or attributes of a person
- ❖ **Claims Providers:** Issue verified identity and/or attribute claims
- ❖ **Relying Parties:** Rely on verified identity and/or attribute claims (e.g., a web service)
- ❖ **User Identity Agent:** Helps the user control the flow of their personal information
- ❖ **Technology Providers:** Provide key components to enable the ecosystem
- ❖ **System Integrators:** Help connect components together



## The POC will focus on these use cases:

- **A private sector Claims Provider (e.g., a bank)** issues claims to a user that are subsequently relied upon by a private sector Relying Party (e.g., an online commerce website) in order to perform a commercial transaction such as an online purchase of wine where the buyer must be at least 21 years old.
- **A private sector Claims Provider (e.g., a bank)** issues claims to a user that are subsequently relied upon by a public sector Relying Party (e.g., a state agency) to perform an e-government transaction such as a permit for a new business.
- **A public sector Claims Provider (e.g., a state agency)** issues claims to a resident that are relied upon by a public sector Relying Party (e.g., a state healthcare department) to qualify the resident to receive services.
- **A public sector Claims Provider (e.g., a state agency)** issues claims to a user that are relied upon by a private sector Relying Party (e.g., a bank web site to enable a banking transaction).

## ➤ **Looking for Partnerships**

# ***NORTHROP GRUMMAN***



Contact:

Keith Ward

Director Enterprise Security & Identity *Management*

Phone: 703.945.9863

Email: [k.ward@ngc.com](mailto:k.ward@ngc.com)