Cross-Sector Digital Identity Initiative (CSDII):
Overview

Philippe Guiot
CSDII Principal Investigator
AAMVA

Work described in this presentation was supported by the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office and the National Institute of Standards and Technology (NIST).

The views in this presentation do not necessarily reflect the official policies of the NIST or NSTIC, nor does mention by trade names, commercial practices, or organizations imply endorsement by the U.S. Government.
NSTIC Opportunity

- On Sept. 20, 2012, NIST awarded more than $9 million for pilot projects in support of NSTIC
- Five U.S. organizations will pilot identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information
- The CSDII Consortium is one of the five from more than 180 applicants
- The pilot projects intend to:
  - Advance the NSTIC vision, objectives and guiding principles; and
  - Demonstrate innovative frameworks that can provide a foundation for the Identity Ecosystem, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized
CSDI I Consortium

Private and public sector Individuals, Relying Parties, Identity Providers, Identity Proofers, Attribute Verifiers and Attribute Providers, and Credential Service Providers to include:
Objective

- increase confidence in end-user identity by leveraging DMV in-person proofing to strengthen the authentication events while maintaining user privacy when accessing on-line services
Challenges

- Identify Trust Framework model to meet CSDII business needs
- Bind self-assured credential to user without impacting IdP
- Leverage DMV in-person proofing on remote authentication events
- Create composite claim set with privacy enhanced attributes
Milestones and Timeline

- **10/1/2012 - 2/1/2013**: Initiation
- **2/1/2013 - 3/1/2014**: POC
- **3/1/2014 - 3/31/2015**: Pilot

**POC – Proof of Concept**
**TF – Trust Framework**
**RP – Relying Party**

- 8/19: Strong Authentication
- 6/28: TF v1.1
- 11/12: TF v2.0
- 12/27: Stronger Credential (enrollment)
- 2/6: Consolidated Claim
- 4/1: RP Deployment
- 9/30/2014: Year Two End
• Business
  • Completed Trust Framework (TF) v1.1
  • Established Governing Board
  • Solicited interest from Health IT Provider RP
  • Defined Health IT Provider Use Cases
  • Defined Value Proposition Approach and Cost Model Principles
Progress to date (Cont.)

- Technical
  - Integrated “Strong Authentication” Capability (i.e. Verify Attributes)
  - Integrated “Stronger Authentication” Capability (i.e. 2\textsuperscript{nd} / Multi Factor)
  - Defined User Interface / User Experience Flow
CSDII:
Walkthrough & Demonstration

Michael P Farnsworth Jr
CSDII Technical Lead
Virginia Department of Motor Vehicles
Logical Architecture

- **Relying Party**
- **User Services Business Requirements**
- **PETP: MSFT (CPIM)**
- **Trust Framework Policy Enforcement Claim Consolidation**

**IdP:** Commercially Available

**AV: AAMVA (Drivers License Data Verification)**

**AP: VA DMV**

**CSP Multi Factor: BioSig-ID**

**CSP 2nd Factor: Phone Factor**

**CSP 2nd Factor: CA**

**SELF-ASSERTED + STRONG + STRONGER**

**Attribute / Credential Authentication & Verification**
RP’s utilize the CSDII ecosystem for authentication and attribute verification in support of delivering business services to their users.
RP’s utilize the CSDII ecosystem for authentication and attribute verification in support of delivering business services to their users.
Logical Architecture

IDPs create, maintain, and manage identity information for principals and provides principal authentication to other services.
AVs serve as the gateway to one or more Attribute Providers in a specific community of interest.
Logical Architecture

APs serve as the authoritative source of information that can be used to validate against.

User Services
Business Requirements

Trust Framework Policy Enforcement
Claim Consolidation

IdP: Commercially Available

AV: AAMVA (Drivers License Data Verification)

AP: VA DMV

CSP
Multi Factor: BioSig-ID

CSP
2nd Factor: Phone Factor

CSP
2nd Factor: CA

Attribute / Credential Authentication & Verification

SELF-ASSERTED + STRONG + STRONGER
Logical Architecture

CSPs provide and validate tokens and credentials authentication events.
Logical Architecture

The PETP enforces the trust framework and offers privacy protection between participants of the ecosystem.
CSDII Demonstration

DMV uses CSDII to protect your privacy and secure access to your records.


Please log in using one of your existing IDs:

- Google account
- Microsoft account

©CSDII 2013 – Privacy Policy – About CSDII – For 24/7 help call CSDII support: +1 (804) 555-4877
Philippe Guiot: CSDII Principal Investigator  
+1.703.908.8289 / pguiot@aamva.org

Michael P Farnsworth Jr: CSDII Technical Lead  
+1.804.385.4877 / michael.farnsworth@dmv.virginia.gov

Jennifer Behrens: CSDII Operations Manager  
+1.434.906.1171 / jennifer.behrens@vita.virginia.gov