Assurance Implementation Example - Virginia Tech

Table of Contents

Contact and Profile Information

Name of Organization: Virginia Tech

Name of Contact: Mary Dunker

Email Address: dunker at vt dot edu

Would you be willing to be contacted for more details? yes

Profile(s), Version and Method of Determination(s) of Conformance:
_x_ Bronze (1.1) - Audited
_x_ Silver (1.1) - Audited

Certification Date: September 10, 2012

Why is Assurance important to your organization? Include the service providers with which you'd like to federate under this Program.

Virginia Tech has long recognized the importance of mapping the level of assurance needed to access our online services with the credential that corresponds to that LoA. A Standard for Personal Digital Identity Levels of Assurance was created in 2010, and this standard reflected guidance from NIST 800-63. However, since NIST publications are designed with the federal government in mind, it was a welcome development when the InCommon Identity Assurance Profiles were established, with a focus specifically on higher education. These profiles allowed Virginia Tech to verify and strengthen our existing identity assurance program and credential technology based on a standard for higher education. In addition to using Bronze and Silver assurance profiles to access external services that require those levels, Virginia Tech services will also have the option to request/require Bronze or Silver from our local users.

A few Virginia Tech research faculty members have already federated with the CILogon service, which is currently accepting InCommon Bronze and Silver credentials in production. Further use is anticipated by the Office of Sponsored Programs for grant submissions. It is hoped that Virginia Tech financial aid officers will be able to use their Silver credentials to access services offered by the Department of Education and National Student Clearing House. NSFand NIH may have other services that will require Bronze or Silver credentials, so Virginia Tech will be ready when those services are available.

Who/what department led the Assurance Project? With whom did you engage during the process?

Mary Dunker, Director of Secure Enterprise Technology Initiatives (SETI) and Karen Herrington, Director of Identity Management Services (IMS) served as co-leaders for the "InCommon Silver for Virginia Tech" project. Both departments are within the Information Technology (IT) organization. Formal project management processes were followed, with IT's Associate Director for Project Planning as the designated project manager. Technical support and software development tasks were handled by the developers in the Middleware and Secure Information Exchange Services (SIES) units in SETI.

The InCommon Silver for Virginia Tech team interacted with the Virginia Tech Payroll and Human Resources offices to gain a good understanding of the identity information that is collected and entered into the ERP system when an employee is hired. Staff in the Hokie Passport Office confirmed identity proofing procedures used to obtain the university's ID card. The Director for Policy and Planning, the IT Security Office, the Office of Sponsored Programs, Student Network Services, and Internal Audit were all involved in the project and were kept informed of status through a project wiki space. The level of engagement with Internal Audit was high, including a pre-project briefing with the Director of Internal Audit, weekly meetings with the IT Auditor assigned to collect information and perform the verification, and working with the the Associate Director of Internal Audit to create the audit summary that was submitted to InCommon.

What specific steps did you take to address the functional areas?

4.2.1 Business, Policy and Operational Criteria

Scope

Legal agreements required to join InCommon.

Gap Analysis

No gaps were identified.

Management Assertion

Virginia Polytechnic Institute and State University is a legal entity that is an InCommon Participant in good standing, and has the organizational structures and processes to comply with the provisions of this IAP.

Evidence of Compliance

InCommon Participation Agreement, Participant Operational Practices, and PO number for most current membership payment. Virginia Tech's InCommon Administrative contacts acknowledged and agreed to perform their responsibilities to comply with this section of the IAP. IT organizational documentation at www.it.vt.edu.

4.2.2 Registration and Identity Proofing

Scope

The project was scoped to achieve InCommon Silver for faculty/staff only - not students. Thus, the registration and identity proofing applies only to employees. Registration is handled by the Token Administration System (TAS). TAS is a locally developed system for the management and issuance of Personal Digital Certificates on smart devices. These cerrificates are issued by the Virginia Tech User Certificate Authority.TAS interfaces with the Enterprise LDAP directory component of oVirginia Tech's Identity Management System. In-person identity proofing is performed by Registration Authority Administrators using TAS to retrieve information about employees with an existing relationship to the university. TAS also records the required registration information in its database.

Gap Analysis

Action item (identify section and sub-section)	Who (Univ. unit)	Type (documentation, infrastructure, procedure, Token Administration System)	Effort (Major, moderate, minor, complete)

4.2.2.3 Registration Records – the record of the facts of registration needs to be modified to include issuer of document; i.e., Drivers license is currently recorded. The issuer (State /country of issuance) is not captured.	SETI SIES, SNS, Software Dist.	TAS or procedure	Minor if issuer is entered in existing comment field by TAS operator; moderate if TAS is modified to enforce entry of issuer. Resolution: Change TAS, providing all acceptable document types in pulldown menus, and to require entry of the issuer.
4.2.2.4 Identity Proofing – Details about payroll and departmental procedures and documentation are unknown, so it is possible that changes could be required to meet the IAP. If graduate students who are not employees remain eligible for Silver LoA PDCs, it might be necessary to review initial identity proofing procedures for them.	Meet with representatives from Payroll and HR to determine procedures.	Documentation, procedure	minor if documentation exists and procedures do not need to change. Resolution: documentation exists for payroll, HR, I-9 hiring procedures. No changes to procedures required.
4.2.2.4.1 Existing relationship - TAS should record the person's eligible affiliation(s) at the time the certificate was issued.	SETI SIES	TAS	minor Resolution: TAS was changed to record eligible affiliations.
4.2.2.4.2 In-Person proofing - determine if any changes are needed based on conversations addressing 4.2.2.4. Item 3 under 4.2.2.4.2 is N/A. We will require that addresses match. Update October 27, 2011 - Since the only government issued photo ID that contains an address seems to be the driver's license, we will ensure we have a process for address confirmation according to one of the options in 4.2.2.5	Project leads, SETI SIES if TAS changes are needed.	Documentation, procedure, TAS, Enterprise Directory	moderate Resolution: TAS workflow, registration screens, and recording enhanced to ensure criteria met.
4.2.2.5 Address of record confirmation - need to add this to TAS registration process.	SETI Middleware, SIES; IMS, TAS RAAs	TAS	Moderate Resolution: electronic address verification added to workflow in TAS.

Management Assertion

Virginia Tech asserts that identity proofing in this IAP is based on a government issued ID and that information verified at the time of employment is used to create a record for the Subject in Virginia Tech's Identity Management System.

Evidence of Compliance

The Token Administration System is documented in a TAS User Guide, to which the auditors were given access. Requirements for RA administrators, who access TAS using a Silver-level eToken, are documented in the Virginia Tech User CA Certification Practice Statement. Since we based the registration on an existing relationship with the university, we consulted with HR, payroll, and the Bursar's office, and then provided the auditors with documentation of the procedures used to verify a person's identity during the hiring process. The auditor observed the TAS registration procedures by obtaining a Virginia Tech eToken from the RA Administrators in the Student Network Services office.

4.2.3 Credential Technology

Scope

Virginia Tech employees will use an X.509 personal digital certificate on the SafeNet 64K USB eToken Pro device as their credential for InCommon Silver.

Gap Analysis

Action item (identify section and sub-section)	Who (Univ. unit)	Type (documentation, infrastructure, procedure, Token Administration System)	Effort (Major, moderate, minor, complete)
4.2.3 Credential Technology – This section does not apply to multifactor credentials. Documentation will be produced to show how Virginia Tech's credential technology meets or exceeds IAP requirements. Where guidance is needed, we will refer to NIST 800-63.	IMS, SETI	Documentation	moderate Resolution: See management assertion and evidence of compliance.

Management Assertion

The Virginia Tech User Certification Authority issues an X.509 personal digital certificate (PDC) onto a SafeNet 64K USB eToken Pro device. The eToken is activated using a password. Public-private key exchange (client SSL) is used to perform authentication. This is not a typical "Shared Authentication Secret" form of Identity Credential, but the institution asserts that this multi-factor credential meets or exceeds the requirements of the IAP. Additional guidance is provided in NIST 800-63.

Evidence of Compliance

See Sample Management Assertions under multi-factor Excample 2 at the CIC Multi-factor Working Group page.

4.2.4 Credential Issuance and Management

Scope

Data retention policy (User CPS) and procedures. Registration Authority Administrator (RAA) procedures (User CPS and TAS User Guide), RAA training.

Gap Analysis

Action item (identify section and sub-section)	Who (Univ. unit)	Type (documentation, infrastructure, procedure, Token Administration System)	Effort (Major, moderate, minor, complete)

4.2.4.2 Credential revocation or expiration – item #1 specifies the IdPO shall revoke Credentials or Tokens within 72 hours of being notified that a credential is invalid or compromised. We must document this in CPS and publish/enforce procedures.	SIES for draft language, PMA for approval	Documentation, procedure	minor Resolution: CPS changed, administrators alerted.
4.2.4.4 Credential issuance records retention – IdPO shall retain records of credential issuance and revocation for minimum of 180 days beyond expiration of the credential. VT User CPS states VTCA retains audit logs for 1 year.	PMA, SIES	documentation, Infrastructure, TAS	minor Resolution: CPS changed, Retention requirement communicated.

Management Assertion

The authentication Credential is bound to the physical Subject and to the IdMS record pertaining to the Subject.

Evidence of Compliance

The authentication credential is bound to the Subject during credential issuance according to procedures that are described in the Virginia Tech User Certification Authority CPS. These procedures are carried out by the RA and CA Administrators who use TAS to register the subjects and issue certificates onto eTokens. The process requires the RAA to verify the person's identity in person, comparing information from the required government-issued photo IDs with information in the IdMS and comparing the photo with the pysical appearance of the Subject. Unique attributes associated with the Subject in the IdMS are included in the X.509 certificate. Revocation requests are taken by the Help desk and offices that issue eTokens. The revoked certificate serial numbers are included in the CRL, which is published at least once every 24 hours. Certificates are issued for a period of two years, and upon expiration or revocation, the Subject must appear in person to receive a new public-private key pair and certificate using the same procedures as for initial personal digital certificate issuance on the eToken. The tAS audit logs (records of issuance & revocation) and archives are retained for three years. Auditors confirmed compliance by observing the credential issuance process.

4.2.5 Authentication Process

Scope

Central Authentication Service (CAS), Shibboleth, eToken Usage Agreement.

Gap Analysis

No gaps were identified.

Management Assertion

Virginia Tech's IdP authentication implementation allows the Subject to interact with the IdP in a manner that proves he or she is the holder of a Credential, thus enabling the subsequent issuance of Assertions.

Evidence of Compliance

CAS is the authentication handler for Virginia Tech's Shibboleth implementation. CAS contains functionality to resist replay attacks. SSL provides secure communication and resistance to eavesdropper attacks. Proof of possession is provided via the requirement for the user to possess a hardware eToken whose private key can only be unlocked using a password which is known only to the Subject. The CAS protocol specification requires entropy in session ids and cryptographic techniques to ensure that sessioins are at least as resistant to attach as initial authentication. The risk of sharing credentials is mitigated by the requirement for the Subject to use two-factor authentication. The Subject is required to read and digitally sign that he/she will comply with the eToken Usage Agreement before the device is given to the Subject.

4.2.6 Identity Information Management

Scope

Policies and procedures of the Virginia Tech Identity Management Services office within Information Technology. Policies and procedures described in the Virginia Tech User Certification Authority CPS and governed by the Virginia Tech PKI Policy Management Authority.

Gap Analysis

No gaps were identified

Management Assertion

Subject Records are managed appropriately so that Assertions issued by the IdP are valid. IdPO management practices are summarized below.

Evidence of Compliance

Subject records exist in the Enterprise Directory and in the Virginia Tech Certificate Authority's (VTCA) Public Key Infrastructure (PKI). The management of the Enterprise Directory is done in accordance with policies and procedures developed by the Identity Management Services (IMS) office within Information Technology. The VTCA PKI is managed in accordance with policies and procedures for the Virginia Tech User CA described in the User CPS. The VTCA is governed by the Virginia Tech PKI PMA. Subject records from the Enterprise Directory are used for eligibility and identity proofing during registration to enroll for a Virginia Tech PDC on an eToken. Some of the attribute information comprising attributes of the PDC is retrieved from the Subject's Person record in the Enterprise Directory, thus linking the subject records from the Enterprise Directory with those in the VTCA PKI.

The eToken PDCs have a validity period of two years from the date of issuance. The PDC Usage Agreement requires eTokens to be returned at the end of employment or enrollment, and employee Separation Notice assigns departmental responsibility for collecting them. Supervisors are instructed to return any eTokens they collect to the nearest eToken issuance location, where the certificates will be revoked. (See PDC FAQ.)The certificate revocation list is checked during CAS authentication, and authentication is denied if the certificate has been revoked.

To enroll for an eToken PDC, the Subject presents all required credentials (including a valid current government-issued photo ID containing the subject's full name, date of birth, picture, and either an address or nationality) to the TAS operator. If the Subject proves to be eligible for a Silver PDC,TAS issues PDC on eToken with the "medium silver" Object Identifier (OID) as defined in the Virginia Tech User CPS. All other eToken PDCs are issued with "medium bronze" OID. Users wishing to access services that require the InCommon Bronze or Silver profile must authenticate to CAS using the eToken PDC. At authentication time, the CAS login handler recognizes the "medium silver" or "medium bronze" OID in the PDC, and passes information to Shibboleth that is used to determine if this person has authenticated with a credential that meets the Silver or Bronze profile. If the person qualifies, the Shibboleth IdP will then assert the applicable "silver" or "bronze" IAQ for this person to the SP. The SP will use InCommon metadata associated with the Virginia Tech entity id to determine whether or not Virginia Tech is certified to assert Bronze and/or Silver.

4.2.7 Assertion Content

Scope

Banner ERP system, Enterprise Directory, CAS, Shibboleth.

Gap Analysis

No gaps were identified.

Management Assertion

Processes are in place at Virginia Tech to ensure that information about a Subject's identity conveyed in an Assertion of identity to an SP is from an authoritative source.

Evidence of Compliance

The Identity Attributes on the eToken PDC are based on information retrieved from the VT Enterprise Directory. These attributes are:

- User unique UID
- User Legal (Banner) Name
- eMail Address

While the SunGard Banner system is the authoritative source for most of the attributes related to people in the Enterprise Directory, the Enterprise Directory is the authoritative source for person affiliations, which are mapped to eduPersonScopedAffiliation.

Until the time at which the Virginia Tech IdP is certified by InCommon to assert an Identity Assurance Qualifier (IAQ), the IdP will only assert IAQs appropriate for testing, such as http://id.incommon.org/assurance/silver-test or http://id.incommon.org/assurance/bronze-test.

Communication between CAS and Shibboleth components of the IdP is achieved using a secure channel. XML digital signatures and encryption provide for non-repudiation and security, respectively, of messages sent from the IdP to service providers.

4.2.8 Technical Environment

Scope

VTCA infrastructure components (EJBCA), Shibboleth IdP, and the communication channels between these components

Gap Analysis

No gaps were identified.

Management Assertion

Virginia Tech's IdMS Operations are managed to resist various potential threats such as unauthorized intrusions and service disruptions that might result in false Assertions of Identity or other erroneous communications.

Evidence of Compliance

The Virginia Tech User CA Certification Practice Statement describes controls for the VTCA software (EJBCA), its maintenance, and security in sections 6.6.1 and 6.6.2. Section 6.7 specifies that Network Security Controls must be implemented to protect against known network attacks. Controls include up to date patching of operating system and application software, appropriate network boundary controls, turning off unused network ports and services, restricting installed software to that which is required to operate the CA. Login access to EJBCA and TAS requires the use of the eToken, issued at the Silver level. Audit logs and archives are maintained, with restricted access to those logs. Separation of duties for PKI roles is required and enforced through data base roles, and secured channels are used for all network communication.

Hardware for the VTCA and IdP is located in the Information Systems Building data center. All access to the building is monitored with video cameras, with entry doors requiring swipe cards. Additional biometric access is provided for machine room entry. Machine room visitors are required to have an escort and sign a log book. Fire suppression systems are installed, and cooling and other environmental factors are monitored. Power is backed by UPS and generator, with sufficient redundancy to provide a reliable operating environment.

Daily backups are of all components of the IdMS are stored at a secure offsite location which can only be accessed by authorized personnel. The servers are scanned daily by the Information Security Office. Disaster recovery plans are documented and tested.

EJBCA operates such that a failure will result in the certificate not being issued rather than a certificate that contains inaccurate information.

The Shibboleth IdP is configured in a high availability environment to minimize system failures, but the database is a single point of failure. Should a failure occur, the result should be unavailability, not an inaccurate assertion.

Did you use Alternative Means? If yes, describe briefly the process.

Virginia Tech used alternative means for the Credential Technology, IAP section 4.2.3. Virginia Tech's credential is a personal digital certificate (PDC) stored on the multi-factor SafeNet 64K USB eToken PRO and eToken 5100 devices. The Shared Authentication Secret is the Private Key component of the X.509 certificate. The Private Key is generated onboard the eToken, and cannot be exported off the device. Access to the Private Key is activated using a password that meets the requirements for "strong" resistance to guessing Authentication Secrets outlined in section 4.2.3.3. Virginia Tech asserts that the PDC on the eToken meets or exceeds the criteria outlined in section 4.2.3.

The process for submitting for certification using this alternative means first involved providing the auditor with evidence that the SafeNet eToken device would meet or exceed each of the criteria in IAP section 4.2.3. Details supporting our assertion are provided under Sample Management Assertions at the CIC Multi-factor Working Group page.

The initial audit report contained a description of the eToken solution and an opinion that Virginia Tech met the criteria in Section 4 of the IAP. After receiving the report, the InCommon Assurance Advisory Committee (AAC) asked questions about our alternative means. Mary Dunker participated in a conference call with the AAC to answer their questions, and followed up with answers in writing. Ultimately, the following information was included in the audit summary.

- Explicit Management Assertion that the multi-factor alternative meets or exceeds the effect of the requirments in section 4.2.3 of the IAP
- Description of the basis on which management is making that assertion
- Auditor's explicit concurrence and positive attestation to management's assertion that the multifactor alternative meets or exceeds the effect of the rquirements in 4.2.3

As a result of this first submission for certification using an alternative means, InCommon has worked with the AAC to develop more explicit criteria for documenting alternative means. More guidance regarding information to be included in the audit summary will be published at Join.

What did the auditors do during the audit?

Virginia Tech's Internal Auditors were involved with the project from the beginning and were given full access to the project wiki space. When the audit phase began, the auditor assigned to the project met weekly with the project leads to gather information and ensure that project status was well communicated. During initial meetings, the scope of each IAP section was discussed and a list of references was compiled, including documentation and technical personnel who would be interviewed. The auditors read the referenced policy documents and interviewed technical personnel who explained their technical controls and, where applicable, how the policies were implemented and enforced in technology and software. Auditors performed vulnerability scans and examined configuration files. The auditors obtained eTokens and observed the procedures for identity proofing, registration, and certificate issuance. Certificates were examined to verify the Object identifier in each certificate that corresponds to a Bronze or Silver credential.

Internal Audit used a modified version of their standard audit template to submit the report to InCommon. The report included:

- Auditor qualifications
- Evidence of auditor independence through direct reporting line to the governing Board of Visitors
- Outline of audit methodology, including
    - background on identity assurance
    - identification of the departmental services being audited, and a brief description of the VTCA.
    - audit objectives (the criteria categories identified by the InCommon Identity Assurance Profiles Bronze and Silver)
- Scope
- Multifactor alternative
- Opinion (positive attestation that the IdPO is in compliance with and meets the requirements for all criteria)

Provide any lessons learned for those just starting.

- Secure sponsorship from a person in a high place. Our Vice President for Information Technology and CIO sponsored the project, and we had buy-in from Internal Audit.
- Collaborate with other institutions working to achieve InCommon Silver. Participation in the CIC Silver project helped early on.
- Manage the project with specific target milestone dates, and meet those deadlines. A deadline for the audit to begin helped us align priorities with other projects.
- Obtain a clear understanding of the information InCommon expects to see in the audit summary, particularaly if an alternative means is being used to satisfy one or more criteria in the IAP.

What resources (templates, documents, planning tools, URLs, etc) where especially helpful during this process?

The following resources were helpful during the "InCommon Silver for Virginia Tech" process:

- InCommon Assurance Specification and Program site
- Community Toolkit / Auditor Toolkit
- Gap Analysis Templates
- Password Entropy Calculators
- Management Assertion Templates
- Community Contributions
- Service Provider Behavior
- Identity Provider Behavior
- Shibboleth documentation on Session Initiator
- Shibboleth documentation on Configuring User Authentication