CIC InCommon Silver Project: Phase I Report

July 2010

C·I·C COMMITTEE ON INSTITUTIONAL COOPERATION

Contents

1. Introduction

Headquartered in the Midwest, the Committee on Institutional Cooperation (CIC) is a consortium of the Big Ten universities plus the University of Chicago. For more than half a century, these 12 world-class research institutions have advanced their academic missions, generated unique opportunities for students and faculty, and served the common good by sharing expertise, leveraging campus resources, and collaborating on innovative programs.

In 2009 the CIC initiated an Identity Management program area whose steering body identified several initial program objectives and chartered corresponding implementation project teams. One of these objectives is for all CIC institutions to achieve InCommon Silver by Fall 2011. Achieving that objective is the task of the CIC Silver project team.

InCommon Silver is an identity assurance profile (IAP) developed by the InCommon Federation. The InCommon Silver profile is fundamentally a set of best practices for identity and access management aligned with the recommendations in NIST 800-63 for Level of Assurance 2 (LoA

2). Being "Silver compliant" will ensure that an institution's conforming authentication assertions will be accepted by relying parties at LoA 2.

The Silver IAP imposes requirements of several different types which the CIC Silver project team has divided into the following three general categories:

1. documentation of policies and procedures and standard operating practices
2. strength of authentication and shared secrets
3. registering identity subjects and issuing credentials

The work is being tackled in three phases, one for each of these categories. Each phase begins with an initial period of evaluation and level-setting on interpretation and understanding of the InCommon Identity Assurance Profile requirements for that particular phase. Following this group work, the schools each conduct a Gap Analysis to identify areas needing to be addressed for each campus as well as commonalities which lend themselves to collaboration and partnerships among the CIC schools.

The CIC Silver project team picked up two additional partners during its initial phase. Both the University of Washington and Virginia Tech were in a similar state of preparation for Silver implementation, and project participants decided it would be good to share our experiences and plans as the project progresses.

This report is released with the completion of Phase I of the CIC Silver project. It is the project's first public deliverable.

"The CIC Universities are implementing InCommon Silver to be able to support LoA 2 by Fall 2011." That statement leads to a great deal of deep discussion, careful analysis, and difficult choices by all parties concerned: the IT people who must make it happen, their Auditors who must figure out how to audit the Silver IAP for the first time, and the InCommon Technical Advisory Committee who produced the Silver IAP and who are responsible for providing a path to LoA 2 that is achievable by the R&E sector in the US. The perspectives of each of these three constituencies, as they have evolved over the course of Phase I of the CIC's Silver project, are reported below.

2. Perspectives of the IT Implementers

Upon completion of Phase I each participating school was asked to respond to a survey covering the key areas of deep discussion & analysis and tough choices they each are making. Here's what they had to say.

2.1. Groups of people to be supported for Silver

Most are targeting faculty & staff (or employees), some also students or just graduate students. The smallest scope is researchers and others as needed. Some intend that all of the pieces of their Silver implementation will fall into place only for people in those categories with a need to access a sensitive service. For example, one school will require in-person identity proofing and so will omit remote people, at least initially. Another school's assertion of Silver for a specific

login will be contingent on the user's password having been changed recently enough, and by taking this approach are avoiding the policy debate of whether or not whole swaths of their people should be required to comply with mandatory password age limits.

In several cases a school's thinking about the population they'd target for Silver support has changed along the way. Several originally felt that they would start out by only supporting people with a specific need and use a specially-crafted process to verify the identity of and issue credentials to those people. They decided to target a larger population instead either because they felt that Silver-needing services would soon enough require it, or that the enhancements to existing processes needed for the larger scope weren't that much more compared to the smaller scope.

2.2. Current or anticipated services motivating campus Silver project

Specifically-mentioned external services include NIH, NSF, TeraGrid, and the National Student Clearinghouse. More generally, several schools anticipate the need to support other research oriented services, and at least one anticipates the need to support outsourced services related to payroll and benefits.

Notably, several schools report that internal services are the leading or a major motivator. In one case Silver will help to implement an existing data classification policy by providing higher level of assurance for access to restricted information. In another, having a Silver-compliant identity verification procedure will help to meet a requirement for an eLoan service.

2.3. IT systems in scope for campus Silver project

2.3.1. Authentication-related systems

All schools consider their shibboleth IdP and the authentication service which supports it to be in scope. LDAP, Active Directory, Kerberos, CAS, Cosign, or Pubcookie fills this need in most cases. One school will extend an existing end-user PKI for their Silver implementation.

One aspect of trust that a substantial part of the Silver IAP deals with is the ability of the IdP to limit the opportunity to guess passwords online. Systems that handle passwords that are in scope must have controls limiting exposure of passwords to online guessing sufficient to meet a specified standard. Some schools interpret that to refer just to their shibboleth IdP and its associated authentication service, the one that actually verifies user credentials when a Silver assertion might be made. Others are proceeding on the basis of limiting exposure of passwords to online guessing wherever they might be used. For these, all authentication contexts are in scope.

2.3.2. Other IdM-related systems

Many schools have identified as in scope the systems they use for managing identities and issuing credentials: the databases in which basic identifiers and attributes are stored, including those needed to manage conditional expression of Silver assurance, as well web sites involved in user account issuing, password reset, etc.

A few worry that their scope may creep outward from there to core business systems that supply basic information about constituents to the IdM system.

A few schools plan to leverage in-person vetting of their ID Card operation or strong authentication token issuing process. Those management systems are also in scope.

2.4. Enhancements needed for IT systems and operations

Most schools find their documentation of process and policy to need work, and some also note need to improve or extend change management, business continuity, or risk management plans to cover their IdP operation (perhaps inclusive of the encompassing IdM operation). Concern has also been raised about Silver's specification pertaining to data center exit logs, although most believe they have acceptable compensating controls such as video surveillance of exits.

Meeting technical requirements for entropy of Silver passwords and limiting ability to guess them online is not an issue, at least for schools adopting a narrow scope of their authentication systems. Others have more work to ensure that encrypted tunnels protect passwords in more contexts, for example.

There has been special concern around the use of Active Directory and ability to protect passwords. It is not possible to configure a Domain Controller to require LDAP BINDs to occur over an encrypted channel. A variety of legacy circumstances can require the remediation of NTLM or MS-CHAP based authentication. And NTLMv2 and MS-CHAPv2 might not meet the specifications of the current Silver IAP (but see the section on the InCommon Technical Advisory Committee below for more on this issue).

These concerns have led at least two schools to wonder whether they will need to provide separate credentials and operate a separate authentication service just for Silver to avoid these issues.

2.5. Business processes in scope for campus Silver project

The Silver IAP addresses Subject registration, identity vetting, and credential issuance and re-issuance processes. Most schools that plan to extend Silver support to employees also plan to rely on identity vetting already carried out by their HR operation. The process that links people so vetted with the credentials issued to them is in scope, and in some cases may need enhancement. But the CIC Silver project hasn't yet spent substantial time on this aspect of campus Silver implementation.

2.6. Silver IAP specifications of special concern

Phase I of the CIC Silver project focused on Silver IAP specification sections 4.2.1, 4.2.6, and 4.2.8, though discussions have ranged beyond those sections to some extent. Following is a compendium of particular concerns that have been aired with particular specifications.

Silver IAP Reference	Concern
4.2.1.*	The amount and types of documentation required (though all feel they will meet documentation requirements).
4.2.1.8	The nature and scope of this audit is unspecified. Most schools don't have an established standard or practice to audit against. See the section on auditors' perspectives below.
4.2.1.10	The volume of authentication events makes it difficult to keep logs for 6 months, at least for schools that broadly interpret which authentication systems are in scope.
4.2.2.3.3	No school has as yet determined how they can perform remote credential issuance or re-issuance in a manner that meets this specification, though that wasn't a focus of Phase I.
4.2.5.2	Schools that run Active Directory and that broadly interpret which authentication systems are in scope may not be able to comply.
4.2.5.11	The specifications make it hard to determine which authentication protocols can be used without the protection of an encrypted tunnel, if any
4.2.6.1	Concern over how reliably attributes are maintained over time.
4.2.8.1	Which systems are subject to change management is unclear. Logging of all software and configuration changes is challenging.
4.2.8.3	Egress logging is an uncommon practice and raises personal safety concerns.

2.7. The single hardest aspect of the implementation, so far

- Creating and maintaining documentation and validating its currency over time.
- The need to establish a new and widely distributed in-person identity proofing process.
- Gaining acceptance of a password policy sufficient to meet entropy requirements.
- Bi-annual audits of the IdP operation, and even establishing what their objective should be.
- Remediation of legacy Windows authentication protocols.
- Gaining understanding and support across the university community.

2.8. What would make the process easier?

- An IAP with a clearer set of definitions, goals, scope, and prescribed actions.
- More staff dedicated to this project.
- Someone else to have already gone through this!

3. Perspectives of the Auditors

3.1. General Comments

The Internal Audit (IA) CIC group is excited by the CIC Silver project's progress. We also appreciate being asked to participate in the early stages of the project.

The IA CIC group recognizes that Federated IDs are critical to our institution's success beyond the scope of communicating and interacting with federal agencies. The IA CIC group believes there are many processes within our individual organizations where the availability and use of trusted federated identities will be a valued strategic initiative.

The work being performed by the project will better position our organizations to obtain InCommon Silver identity assurance designation. IA CIC group believe the process is helping many of our organizations think about and improve the control processes associated with their central identity management and user authentication functions. The project is helping IT management define the control assertions (i.e., basis of trust) that need to be made to In-Common along with a better understanding and greater confidence in the control processes associated with these systems.

The IA CIC group appreciates the opportunity to learn from and work with the CIC Silver project team. We believe this interaction prepares us to assist our individual organizations to meet the Silver IAP requirements. Our intent is to be a valued resource for the CIC Silver project team and assist when needed to accomplish the goals of adequate controls with minimum additional investment.

3.2. Possible process for future auditor involvement

Representatives from IA CIC group are interested and willing to work with/assist the project team on future phases of the project.

3.2.1. For each phase of the project

Project staff may want to meet with the IA CIC group to discuss the scope or any change in scope, (i.e. what population of users is included). Then discuss the assessment factors and how these factors have been interpreted.

Once the gap analysis is completed, it may be worthwhile to have a discussion with the IA CIC group to explain the gaps and resolution. Compensating controls to resolve a gap will be open to discussion with the CIC Silver group as a whole to reach consensus that the proposed compensating control will meet Silver IAP requirements.

3.2.2. Validation process

The IA CIC group will work on reaching consensus on the minimum requirements for the Identity Assurance Profile audit. The IA CIC group will work to reach consensus on how the validation process will be performed and basic wording for the validation report. The expected date of the report along with distribution list will be determined in consultation with CIC Silver project team.

3.3. Questions/Discussion items raised by the project team or amongst the IA CIC group

3.3.1. Key components requiring validation

It appears that the validation process includes 2 components which are:

The identity process:

4.2.1 Business, Policy and Operational Factors

There is some testing in this section, but nothing extensive, it is mostly verifying adequate documentation exists.

4.2.2 Registration and Identity Proofing

This section will require the auditor to select a sample of users to verify proper procedures were followed when credentials were issued.

4.2.3 Digital Electronic Credential Technology

This section requires the auditors to validate all user ID's are unique, and that passwords can be reset by the user in a manner that is compliant with the institutions password policy for the Silver certified ID's, and the reset tool enforces compliance with this policy.

4.2.4 Credential Issuance and management

This section requires auditors to validate:

How the IdP maintains credentials and they only authenticate active ID's.

IdPs maintain 99% uptime (inclusive of scheduled down time) the ability to verify the status of credentials so that revoked credentials cannot authenticate, and active credentials can.

IdPs identify and appropriately respond to potential brute force attacks.

Credentials are revoked timely upon notification of compromise or that the credential is no longer needed.

4.2.5 Security and Management of Authentication Events

This section requires the auditors to validate:

Secure (encrypted) end-to-end communication.

Stored secrets are encrypted at rest.

4.2.6 Identity Information Management

There is no validation/testing required in this section, only verification of adequate documentation.

4.2.7 Identity Assertion Content

There is no validation/testing required in this section, only verification of adequate documentation.

Supporting infrastructure:

4.2.8 Technical Environment

This section requires the auditor to verify:

Change Control process is in place for IdP systems and is working.

Physical security controls are in place and operating as intended.

Documented Disaster Recovery plan exists, or Silver certified staff knows there is not a documented DR plan.

3.3.2. Who can do validation?

Based on the InCommon Identity Assurance Assessment Framework (IAAF), one option that an institution could exercise for completing the validation process is to request their internal auditors to complete an assessment of the integrity of management control assertions. The material from InCommon does not suggest that individuals outside of the organization applying for "Silver accreditation" need to be involved in the validation work or drafting of the validation report. The IA CIC group however believes that the validation process needs to be conducted/lead by a person(s) who does not have IT management responsibilities within the organization (i.e., the person must be independent). It is important to remember that management's control assertions and the validation report is being constructed for InCommon which is ultimately responsible for determining if the institution is eligible for "Silver accreditation".

3.3.3. How validation will likely occur with some comments about some of the steps

- Management makes control assertions
    - Management may want to ask their auditors to consult on possible assertions they want to make discuss other assertions that management may be able to make based on previous audit work/knowledge of the institution
- IT support staff collect supporting evidence for the control assertions
- Valuator's (e.g., internal audit) determine what assertions require sample testing
- Validator completes assessment, including management's control assertions, and issues an opinion on the validity of control assertions made by management

3.3.4. Frequency of validation

The IA CIC group understanding is that the general approach requires an initial assessment, and then periodic reassessments. Assessment factor 4.2.1.8 requires an Institutional Audit of the IdM operation at least every 24 months. Audit's concern is that there may not be sufficient audit resources and/or other pressing audit priorities that would prevent the Internal Audit function from performing these requirements. The IA CIC group recommends regular contact between the Chief Audit Executive and the Chief Information Officer to work out a balance between the periodic assessments needs with the audit plan. This may require the engagement of external auditors.

3.3.5. Process to prioritize areas requiring management assertions and validation work

The eight assessment areas that have 43 factors cover a wide area of identity assurance control activities. To enhance the gap analysis and implementation plan process the IA CIC group would encourage the emphasis of specific control assertions, i.e. a priority of those factors causing greatest concern. The IA CIC group also suggest establishment of a process to consider compensating controls that would include a means to reach consensus that the control will meet or exceeds Silver IAP requirements.

3.3.6. Some basic questions for refinement of expectations

How to define what components are key to include in the assessment (e.g., if an institution is using their university issued ID card issuing process to support that individuals with Silver status have provided University management with a copy of their government ID, do controls over the Ucard system need to be included in the assessment). Some auditors believe the answer to be yes, unless the ID card issuing process has been reviewed within the last 12 months and there have been no material changes with the process. There may be other situations like this that need to be considered on an ad hoc basis.

What will the CIC consider good enough (e.g., control of entry to the data center but not egress from the data center)?

The Silver IAP and IAAF leave room for interpretation and subjective judgment on the part of the independent auditors in terms of what is an acceptable control. The auditors would prefer that there is consensus on what appropriate minimum level of compliance and acceptable compensating controls. If this doesn't happen, there is the risk that one institution could have less control in a particular area than other institutions. Interpretation and subjective judgment also brings the risk of InCommon not agreeing with our interpretation or subjective judgment when the audit report is issued. An audit report suggesting the institution meets or exceeds the InCommon criteria doesn't guarantee Silver approval.

4. Perspectives of the InCommon Technical Advisory Committee

The InCommon Technical Advisory Committee (TAC) is a group of mostly volunteers from the higher education community that range from the "Fathers of Federating" to those who have

deep stakes in the ground running entire systems based on federating. The TAC's work originates from many directions including the InCommon Steering Committee, new services, higher education members, services providers and other federations. The CIC Silver project is being co-led by two of the TAC's members which provides a direct and natural path for elevating concerns and recommendations regarding the implementation of the Silver IAP in real campus environments.

The TAC has been trying to find a balance between the concerns and requests for clarification presented by the CIC schools, the intent of the Silver IAP specifications, and the need to align the Silver IAP with NIST SP800-63 and with ICAM (the Identity, Credential, and Access Management program of the US Federal Government).

Thus far, the TAC has received feedback from the CIC Silver project in the form of a formal letter asking for clarification to address questions and concerns centered on 4.2.4.5, 4.2.5.2, 4.2.5.6, and 4.2.5.11, and numerous other concerns (essentially all of those detailed in section 2.6 above) that have been communicated to the TAC by the liaisons as part of TAC's normal agenda.

In response to the CIC letter, the TAC made some changes to wording in relevant Silver IAP sections (as yet unpublished, though included in the TAC's Silver IAP submission to ICAM). More generally, the issues raised by the CIC Silver project and the many discussions those have engendered have led the TAC to make two key observations:

- The Silver IAP uses a mixture of goal-oriented and implementation-oriented language that can produce ambiguous or divergent interpretations of its meaning.
- InCommon originally expected it would play a very modest role in the process by which a campus receives the authority to produce Silver authentication assertions, but that process, and that role, may need to be rethought.

Regarding that first observation, the TAC has decided that it will make corresponding changes to Silver IAP specifications as needed to clarify how the Silver IAP addresses issues raised by the CIC Silver project. Work on those changes will start after the CIC Silver project has completed its review of all of the Silver IAP requirements and communicated the results to the TAC.

5. Summary and Next Steps

The CIC Project IT implementers, the InCommon TAC, and the Internal Audit CIC group have developed a working relationship and collaboration that is relatively unique and will benefit identity federations and the adoption of identity assurance profiles. It is the balance of the intent of the InCommon Silver Profile as conceived by InCommon with the comparable requirements and audit of compliance by the IA CIC group as well as the assessment and changes of process and management of identity provider infrastructure by IT implementers that will assure this project's success.

There is a lot yet to work through within this identified framework over the next year. Two fundamental questions about the IAP have arisen. The first is what' s meant by the term "IdP" in the IAP and who is responsible for the definition? Is it narrow, is it the IdM operation, or is it

the entire university? Different parts of the IAP may require or appear to require different interpretations to make sense in the higher education community.

The second fundamental question centers on who is authoritative for whether a given campus has met the requirements of the Silver IAP. The InCommon TAC conceived the IAAF and IAP with the expectation that a campus could conduct an objective review of its IdM practices, determine whether they are sufficient to warrant Silver, and notify InCommon of the result. Early experience with the CIC Silver project indicates the possibility that either the IAAF or IAP must be somehow modified to support that approach, or that InCommon may need to play a role in assessing the results of objective campus review to determine if Silver requirements are met.

By being the first to test the process of achieving Silver, the feedback and insight provided by CIC Silver project participants will have an impact on the IAP and IAAF. Clarifying these fundamental questions and addressing some of the more specific concerns that are raised will help InCommon establish and refine a process and practice by which many further institutions in the R&E sector in the US can expect to successfully achieve Silver.

The decision by the CIC to have an entire cohort proceed together has been highly beneficial. Having a venue in which to air, share, and explore what each campus might do and what obstacles they see is extremely helpful. Furthermore, we've found that some campuses share similar technologies or approaches, and that they can share related documents and solutions and so help each other along that much faster.

Other existing associations of R&E institutions should also consider a cohort-facilitated approach to Silver adoption. And because so many institutions do not have that opportunity, we think InCommon would greatly expedite Silver adoption, and relieve the anxiety independent adopters feel as they examine their operations in detail, by providing a way for cohorts of Silver implementers to be assembled.

The CIC Silver project was designed to be accomplished in three phases, each focused on one of three categories of Silver IAP specifications. The plan has been to initiate each phase with a gap analysis of campus practices against the requirements in the corresponding category. We now realize that, although the phases make sense as implementation steps, there should be a single gap analysis up front against all of the IAP's specifications. That makes it likelier that all of the substantial issues are discovered early in the process, allowing more time to determine how to handle them.

With the start of Phase II of the CIC Silver project, we will complete a comprehensive gap analysis of the Silver IAP relative to the practices of participating campuses. That information will be given to the InCommon TAC as soon as it is gathered so that they too can anticipate as early as possible what the issues are likely to be, and what they might do to increase the chance of successful campus outcomes.

6. Appendix A - IdM Project Participants

Ron Thielen
University of Chicago
rthielen@uchicago.edu

Tom Barton
University of Chicago
tbarton@uchicago.edu

Ken Rowe
University of Illinois
kenrowe@uillinois.edu

Michael Grady
University of Illinois
m-grady@illinois.edu

Jacob Farmer
Indiana University
jpfarmer@indiana.edu

Nick Roy
University of Iowa
nicholas-roy@uiowa.edu

Chris Pruess
University of Iowa
chris-pruess@UIOWA.EDU

Liz Salley
University of Michigan
salley@umich.edu

Luke Tracy
University of Michigan
ltracy@umich.edu

Jim Green
Michigan State University
jfgreen@msu.edu

Anne Hopkins
University of Washington
annehop@u.washington.edu

Matt Kolb
Michigan State University
mk@msu.edu

Don Ries
Michigan State University
riesd@msu.edu

Arash Forouhari
University of Minnesota
foro0004@umn.edu

Greg Niemeyer
Ohio State University
niemeyer.8@osu.edu

David Pike
Ohio State University
pike.58@osu.edu

Renee Shuey
Pennsylvania State University
rshuey@psu.edu

Jerry Mihaly
Pennsylvania State University
jsm@psu.edu

Rob Stanfield
Purdue University
rob@purdue.edu

Stefan Wahe
University of Wisconsin-Madison
smwahe@wisc.edu

Steve Devoti
University of Wisconsin-Madison
devoti@WISC.EDU

Mary Dunker
Virginia Tech
dunker@vt.edu

Karen Herrington
Virginia Tech
kmherrin@vt.edu

Jean Plymale
Virginia Tech
vplymale@exchange.vt.edu

7. Appendix B - CIC Participating Auditors

Gene Fruit
University of Illinois
gfruit@uillinois.edu

Gary Grgurich
Penn State University
GJG13@psu.edu

Kevin Keough
Indiana University
kkeough@indiana.edu

Steve Kurncz
Michigan State University
kurncz@msu.edu

Chad Sharp
University of Iowa
chad-sharp@uiowa.edu

Dennis Skovsted
University of Minnesota
skovs001@umn.edu