

# IDENTITY MANAGEMENT AND STUDENT RECORDS

Andrea Beesing, Cornell University  
Jeff von Munkwitz-Smith, University of Connecticut  
Ann West, EDUCAUSE/Internet2/InCommon

AACRAO Tech - July 19, 2009

1

---

---

---

---

---

---

---

---

## Agenda

- Why Should We Care About Identity Management?
- Identity Management 101
- Federated Identity
- Break
- Discussion
- Resources and Next Steps

AACRAO Tech - July 19, 2009

2

---

---

---

---

---

---

---

---

## Why Should We Care About Identity Management?

The short answer is that we've  
always cared.

AACRAO Tech - July 19, 2009

3

---

---

---

---

---

---

---

---

## Directions to Prospective Students

Connecticut Agricultural College, 1917

- Write for the formal application blank, answer the questions it contains, and mail it as early as possible to the President in order to facilitate dormitory and dining room arrangements.
- Check trunks and send express packages to Willimantic. Address freight to Eagleville. Be sure to tag all packages and baggage with your name and correct destination.

AACRAO Tech - July 19, 2009

4

---

---

---

---

---

---

---

---

- Write to the Secretary of the Connecticut Agricultural College stating the date and time of your arrival.
- Upon arrival at the College, call at the office of the Registrar for registration and directions.
- Read carefully announcements on the bulletin board.

AACRAO Tech - July 19, 2009

5

---

---

---

---

---

---

---

---

## More Recently

- Movement from personal knowledge of individuals to physical identifiers (i.e., ID cards).
- Creation of pins and passwords for early touchtone registration and on-line access systems.
- Creation and maintenance of multiple IDs and passwords as services expanded (registration, email, course management systems, etc.) = Identity Management on a system-by-system basis!

AACRAO Tech - July 19, 2009

6

---

---

---

---

---

---

---

---

## Why Should We Care *More* Now?

- The old models are not scalable.
- Students, faculty, and others need access to more services, sooner, and often remotely, than ever before.
- We may never even see the people using our services.

AACRAO Tech - July 19, 2009

7

---

---

---

---

---

---

---

- We aren't always the provider of the service, but may still need to authenticate the users.
- There are heightened concerns for individual privacy.
- We may have contractual obligations to outside providers.

AACRAO Tech - July 19, 2009

8

---

---

---

---

---

---

---

- Developing and maintaining service-by-service mechanisms to managing identity is expensive.
- For individuals, managing multiple IDs and passwords for our institutions is a burden and often leads to weaker passwords or poor practices.
- Transitions from role to role or even within roles create problems unless they are managed well.

AACRAO Tech - July 19, 2009

9

---

---

---

---

---

---

---

## And Finally

There are more regulatory requirements than ever before:

- Family Educational Rights and Privacy Act (FERPA) - 1974
- Health Insurance Portability and Accountability Act (HIPAA) - 1996
- Gramm-Leach-Bliley Act (GLB) - 1999
- "Red flags Rule" – 2009
- Revised FERPA regulations - 2009

AACRAO Tech - July 19, 2009

10

---

---

---

---

---

---

---

---

## What's New with FERPA?

A few highlights:

- Authentication
- "Direct control" standard
- Access control
- Recommendations for Safeguarding Education Records

AACRAO Tech - July 19, 2009

11

---

---

---

---

---

---

---

---

## Authentication

"The regulations in § 99.31(c) require educational agencies and institutions to use reasonable methods to identify and authenticate the identity of parents, students, school officials and other parties to whom the agency or institution discloses personally identifiable information from education records. The use of widely available information to authenticate identity, such as the recipient's name, date of birth, SSN or student ID number, is not considered reasonable under the regulations." – Department of Education analysis of regulations, December 2008

AACRAO Tech - July 19, 2009

12

---

---

---

---

---

---

---

---

## “Direct Control” Standard

“An agency or institution must ensure that an outside party providing institutional services or functions does not use or allow access to education records except in strict accordance with the requirements established by the educational agency or institution that discloses the information.” – Department of Education analysis of regulations, December 2008

AACRAO Tech - July 19, 2009

13

---

---

---

---

---

---

---

---

## Access Control

“The regulations in § 99.31(a)(1)(ii) will require an educational agency or institution to use reasonable methods to ensure that teachers and other school officials obtain access to only those education records in which they have legitimate educational interests....An educational agency or institution that chooses not to restrict access to education records with physical or technological controls, such as locked cabinets and role-based software security, must ensure that its administrative policy for controlling access is effective and that it remains in compliance with the legitimate educational interest requirement.” – Department of Education analysis of regulations, December 2008

AACRAO Tech - July 19, 2009

14

---

---

---

---

---

---

---

---

## Safeguards

- “Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information.” – Department of Education analysis of regulations, December 2008

AACRAO Tech - July 19, 2009

15

---

---

---

---

---

---

---

---

### Resources on Safeguarding Education Records - Department of Education

- The National Institute of Standards and Technology (NIST) 800–100, “Information Security Handbook: A Guide for Managers”
- NIST 800–53, “Information Security”
- Office of Management and Budget May 22, 2007 memorandum on safeguards to protect personally identifiable information
- Federal Register / Vol. 73, No. 237 / Tuesday, December 9, 2008 / Rules and Regulations

AACRAO Tech - July 19, 2009

16

---

---

---

---

---

---

---

---

### Identity Management 101

AACRAO Tech - July 19, 2009

17

---

---

---

---

---

---

---

---

### What is Identity Management (IdM)?

Identity management is the term used to describe the business processes, standards, practices, and technologies which enable people to take full advantage of online resources in a way which balances the need for functionality with the need for data security and privacy. It is built upon the three cornerstones of policy, process and IT infrastructure.

AACRAO Tech - July 19, 2009

18

---

---

---

---

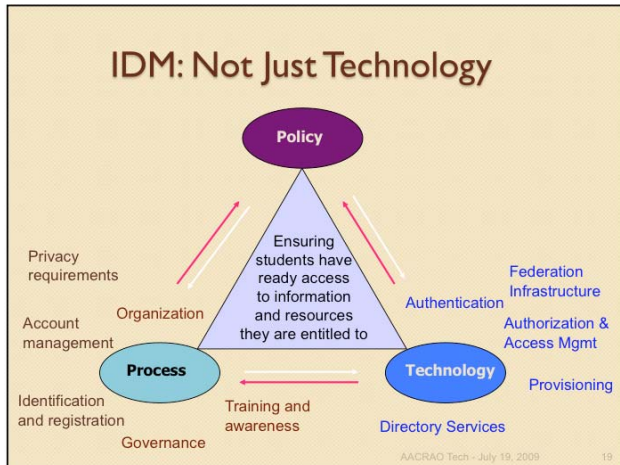
---

---

---

---

## IDM: Not Just Technology




---

---

---

---

---

---

---

---

## Policy & Identity Management

“Cornell's policies connect the university's mission to the everyday actions of its community, clarify the institution's expectations of its individual members, mitigate institutional risk, enhance efficiency, and support the university's compliance with laws and regulations.”

- Policy is a key driver in determining how identity management is implemented.

AACRAO Tech - July 19, 2009

20

---

---

---

---

---

---

---

---

## University Policies

4.4 Access to Cornell Alumni Affairs Information

4.6 Ethical Conduct



4.5 Access to Student Information

4.12 Data Stewardship and Custodianship

AACRAO Tech - July 19, 2009

21

---

---

---

---

---

---

---

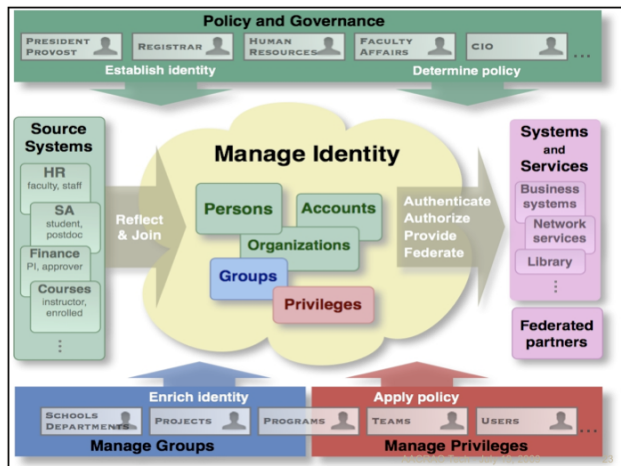
---

## Process & Governance

- The role of process
  - Means of implementing policy and University mission
  - Guidelines, standards, procedures
  - Education and awareness
  - Informs technical implementations
- The role of governance
  - Decision-making for issues affecting the entire institution
  - Focus on areas of highest priority to the institution
- All of above = campus IdM infrastructure
- Requires high level of collaboration between IT and business units to do it right

AACRAO Tech - July 19, 2009

22



## Case Study: Secure Access to Services

An important goal of identity management is secure user access. Secure user access means that there is a high level of assurance that the people accessing the service are who they claim to be (authentication) and that they are entitled to use the service (authorization) based on their relationship with the institution.

AACRAO Tech - July 19, 2009

24



## IDM Balancing Act

- Deliver value and functionality to student service area
  - Easy access to the right information at the right time from anywhere
  - Agile, cost-effective
- Assume only acceptable risks
  - Authorized access only
  - Combination of technical controls and user behavior
- Ensure privacy while enabling service delivery

AACRAO Tech - July 19, 2009

25

---

---

---

---

---

---

---

---

## Start with Policy: Data Classification

- Define types of data – keep it simple!
  - Confidential
  - Restricted
  - Public
- All data associated with University business defaults to restricted unless explicitly made public
- Enumerate confidential data elements & focus more resources on protecting those
- Key area of focus is identity level of assurance (LoA)

AACRAO Tech - July 19, 2009

26

---

---

---

---

---

---

---

---

## Cornell Confidential Data

- Social security numbers
  - Credit card numbers
  - Driver's license numbers
  - Bank account numbers
  - Patient treatment information
- “This set may expand based on future regulatory requirements or designations made by the appropriate university data steward (as defined in University Policy 4.12). Future additions will be reviewed by an appropriate governance body before they are incorporated here.”

AACRAO Tech - July 19, 2009

27

---

---

---

---

---

---

---

---

## Authorized Access

Authentication – “The process by which you prove your identity to another party...” (Cornell University)

Authorization – “The process of determining a user's right to access a resource.” (the MAMS project - Australia)

Credential – “An object that is verified when presented to the verifier in an authentication transaction.” (Webopedia, OMB)

AACRAO Tech - July 19, 2009

28

---

---

---

---

---

---

---

---

## Authorized Access: Authentication

- Not just the credential—NetID and password for example
- Processes matter—beware the weak link!
  - ID proofing
  - Record maintenance
  - Distribution of initial password
  - User awareness – managing user behavior
  - The parent challenge/re-credentialing

AACRAO Tech - July 19, 2009

29

---

---

---

---

---

---

---

---

## Authorized Access: Authentication

- Robust, centralized infrastructure is also key
  - One NetID for life
  - Integrates with variety of applications
  - Password resistance to guessing/cracking
  - When and where is dual-factor authentication needed?
- Effectively managing risk vs. avoiding impacting user experience
- Standards documents valuable reference
  - NIST
  - InCommon Bronze & Silver

AACRAO Tech - July 19, 2009

30

---

---

---

---

---

---

---

---

## All of Above = Level of Assurance

- Level of Assurance (LoA) – “Describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity.” (NMI-EDIT)
- Standards documents are valuable reference
  - NIST Special Publication 800-63
  - InCommon Bronze & Silver Identity Assurance Profile

AACRAO Tech - July 19, 2009

31

## Technology: Resistance to Guessing Shared Secret

### InCommon Federation – Bronze and Silver Identity Assurance Profile – Assessment Checklist

Requirements	Suggested Evidence of Compliance	Procedures to Test Compliance	Evidence Gathered
<b>§ 4. Strong resistance to guessing shared secret</b>			
The PIN (numeric-only) or password, and the controls used to limit on-line guessing attacks shall ensure that an attacker targeted against a selected user's PIN or password shall have a probability of success of less than $2^{-14}$ (1 chance in 16,384) over the life of the PIN or Password.	Documented procedures and mechanisms that define a method of providing a mathematically adequate level of resistance.	Examine the procedures and mechanism that allow a user to change their shared secret.	
The PIN (numeric-only) or password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker faces to guess the most commonly chosen password used in a system) to protect against untargeted attack. <ul style="list-style-type: none"> <li>• Refer to NIST SP 800-63 Appendix A, and the NIST Shared Secret Entropy Spreadsheet to calculate min-entropy and resistance to online guessing.</li> </ul>	Use of NIST Entropy Spreadsheet to show sufficient token strength.	Request a temporary token be established. Use this temporary token to test with inadequate PINs or passwords to determine the process is working as documented.	

AACRAO Tech - July 19, 2009

32

## Process: Confirmation of Delivery

### InCommon Federation – Bronze and Silver Identity Assurance Profile – Assessment Checklist

Requirements	Suggested Evidence of Compliance	Procedures to Test Compliance	Evidence Gathered
<b>§ 3. Confirmation of Delivery</b>			
If the credential issuance process is a separate transaction from registration, these processes must be tied together to ensure that the credential is issued to the registered person. This may be done using a temporary secret provided at registration time in person, or sent to the subject by means of: <ul style="list-style-type: none"> <li>• Postal address of record such as that used for delivery of sensitive personal communications to that individual; or</li> <li>• Cell phone or telephone number of record.</li> </ul>	Documentation of the credential issuance process.	Examine the documentation	

AACRAO Tech - July 19, 2009

33

## Process Drill-down: ApplicantID vs. NetID

- Differing business needs
  - Temporary (use once & delete) vs. assigned for life
  - Volume and cost of providing the service
    - 38,000 undergraduate applicants (ApplicantIDs)
    - 3,800 matrics (NetIDs)
- Differing risks based on data accessed
- Processes and technologies will probably differ
  - Distribution of initial password: email vs. U.S. mail
  - Stronger authentication technologies: single vs. dual -factor

AACRAO Tech - July 19, 2009

34

---

---

---

---

---

---

---

---

## Authorized Access: Authorization

- Risk plays a role here too
- Authorization based on
  - Relationship to the University
  - Role
  - Assurance of identity
  - Combination of above
- Role: "Collection of common requirements, tasks and business functions performed by individuals using an application support "system". Based upon these common requirements, specific common services can be allocated." (Indiana U.)

AACRAO Tech - July 19, 2009

35

---

---

---

---

---

---

---

---

## IDM Support for Authorized Access

- Centralized access management solutions with shared operational responsibility
  - IT implements and maintains group and privilege management infrastructure
  - Business units use them to assign access based on established policy
- Governance is result of collaboration between IT and business units
  - Establishes authority for deciding who has access
  - Assists in operational reflection of institutional decisions

AACRAO Tech - July 19, 2009

36

---

---

---

---

---

---

---

---

## Application Access

- IT staff are data custodians—can implement access but not determine (defined in policy 4.12)
- Process defined for access requests decisions
  - Template to be filled out by customer with help from Data Administration staff
  - DA staff works with data stewards to obtain decision

AACRAO Tech - July 19, 2009

37

---

---

---

---

---

---

---

---

### File>>Properties>>Title: Requestname Data Access Request/Agreement

This document describes a request and subsequent agreement between the requester and data steward(s) for approved access to the data in a manner that is specified herein. This document is specific to a singular business process and service delivery mechanism.

This agreement may be reexamined at the discretion of the data steward(s) to ensure:

- adherence to relevant University Policies,
- business application consumption of the service is accurate and appropriate,
- authentication and authorization mechanisms are adequately maintained,
- delivery mechanisms are adequately secured, and
- other considerations have not compromised the original intent of the approved request.

#### TOC

<a href="#">I. Request Contact Information</a>	2
<a href="#">II. Provisions</a>	2
<a href="#">III. Signature Page</a>	3
<a href="#">IV. Request Description</a>	4
<a href="#">V. Security</a>	5

AACRAO Tech - July 19, 2009

38

---

---

---

---

---

---

---

---

### IV. Request Description

#### Business Case:

The staff of the Messaging team handle escalated cases from the Help Desk concerning email, calendaring, and related matters. Often the resolution of the problem requires research into the end user's status and entitlements, some of which are not visible to my staff. With the release of different email systems for students and for faculty and staff, distinctions of status are even more a part of problem resolution. The Help Desk staff can view this information through the HelpHero application, however this has not been available to the Messaging group.

Problem resolution would be greatly speeded and made more accurate if the Messaging staff can see the same information about user status as the Help Desk. As it currently stands, answers to some questions require several back-and-forth exchanges of information, which could be short-circuited by access to this tool. It is appropriate for the backline support staff to have access to at least the same level of diagnostic information that the frontline staff does.

#### Application Name and Description:

CET HelpHero

Request Date of Availability of the Data (MM/DD/YYYY):

ASAP

#### Related Web Services:

N/A

#### Data Delivery mechanism:

Web Page

#### Data Requirements:

Provide overview of the data that will be retrieved from each system that will be accessed. Specify batch or real-time access. Specify one-time or on-going.

AACRAO Tech - July 19, 2009

39

---

---

---

---

---

---

---

---

**Data Input:**

Field	
Need	

**Data Output:**  
Specify the number of occurrences of the data that are expected.  
One per request

**The constituency populations of output data to be delivered:**  
Specify the constituency populations:  
Staff, Students, Alumni, Sponsored Exceptions, Affiliates

**NB** Employee home address & phone are data elements that, while not deemed "confidential" according to policy, are treated with nearly the same restrictions --- regardless of the employee's individual election to suppress or not.

**For All Populations:**

Field	Public	Business Definition	Source System / Service	Currency	Cardinality	Display/Update
NetID						
Name						
EmpID						
FERPA election						
HideHomeAddress & Phone						
HideName						
CampusAddress & phone						
Home Address & phone						
Local Address & phone						

AACRAO Tech - July 19, 2009 40

---

---

---

---

---

---

---

---

## Access for Individuals

- Point-to-point access management works for application access case and for some large, centralized services like Banner, PeopleSoft
- But many distributed systems are managed by many staff in many units
- Distributed model with governance needed
  - Common set of access management tools
  - Distributed and shared responsibility for daily operations

AACRAO Tech - July 19, 2009 41

---

---

---

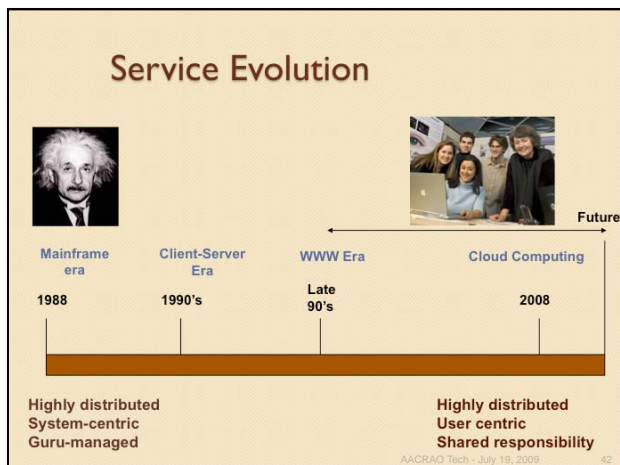
---

---

---

---

---




---

---

---

---

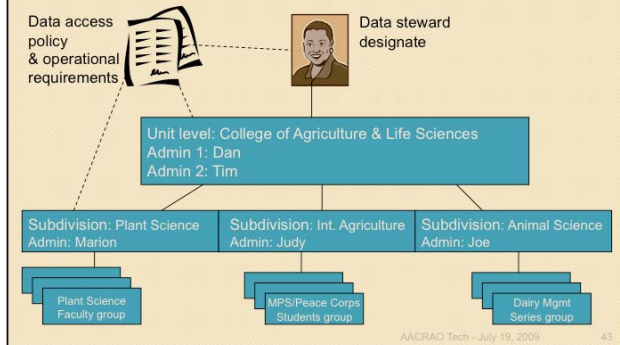
---

---

---

---

## Group Management Example: Shared Responsibilities




---

---

---

---

---

---

---

---

## Group Management Example: Shared Responsibilities

Data access policy  
& operational  
Requirements



Data steward  
designate



Cornell implementation:

- University Policy 4.12 Data Stewardship and Custodianship
- "IT Security Requirements for Confidential Data"
- Requirements addressing access management to be developed

Cornell proposal:

- IT Security Council Rep or
- IT Managers Council Rep

AACRAO Tech - July 19, 2009

44

---

---

---

---

---

---

---

---

## Federated Identity Management: Off-campus Services

AACRAO Tech - July 19, 2009

45

---

---

---

---

---

---

---

---



## Bedtime Story

It's 3:00 am and Bianca is sitting in a 24 hour Starbucks in the spring semester of her senior year, working on her Physics 456 homework. In a browser, she clicks on the link to the course management system, logs in with her University web single sign-on userid and password, and starts viewing the course information.

Next, she clicks on the homework link hosted by a third-party provider and "Welcome Bianca" appears along with her new homework assignment for that class. After finishing that, she decides to check her loan status and surfs to the web site of her financing agent. She clicks "Access your record" and is presented with an aggregation of her loan liability without having to identify herself or login.

In April, Bianca graduated. One day she was a student and the next, an alumna. She noticed her access changed too. She now could get to an alumni networking service where she put out a query about apartments in the Bay Area. Her loan status had changed on the financing agent's site. She now was out in the wide world of opportunity and responsibility.

AACRAO Tech - July 19, 2009

46

---

---

---

---

---

---

---

---

## The Problem

- How many off-campus applications do you have?
- How do these service providers
  - Verify the identity of your students?
  - Know who's eligible to access the service?
  - Know the student is active and hasn't left school?
- How comfortable are you with the security and privacy of the identity data?

AACRAO Tech - July 19, 2009

47

---

---

---

---

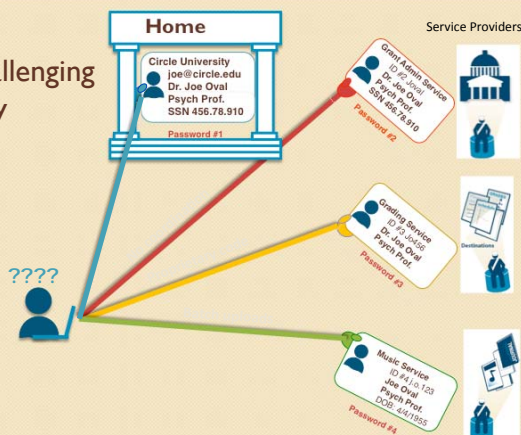
---

---

---

---

## The Challenging Way



AACRAO Tech - July 19, 2009

48

---

---

---

---

---

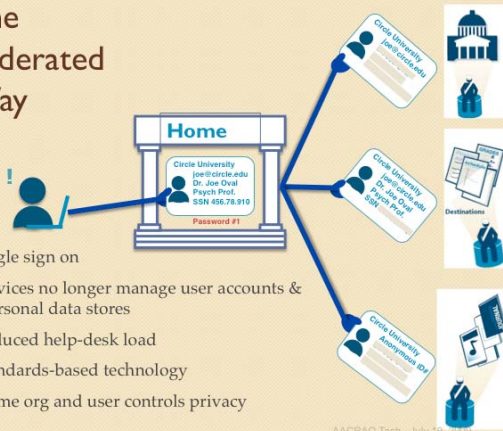
---

---

---



## The Federated Way



1. Single sign on
2. Services no longer manage user accounts & personal data stores
3. Reduced help-desk load
4. Standards-based technology
5. Home org and user controls privacy

AACRAO Tech - July 19, 2009

49

---

---

---

---

---

---

---

---

## SAML and Shibboleth

### Security Assertion Markup Language (SAML)

- Standard for the formation and exchange of authentication, attribute, and authorization data as XML.

### Shibboleth Single Sign-on and Federating Software

- Open source software uses SAML to perform this exchange across boundaries

AACRAO Tech - July 19, 2009

50

---

---

---

---

---

---

---

---

## Shibboleth In Action

AACRAO Tech - July 19, 2009

51

---

---

---

---

---

---

---

---

### The Role of the Federation

1. Agreed upon attribute vocabulary & definitions:  
member of, role, unique identifier, courses, ...
2. Criteria for identity management practices (user accounts, credentialing, etc.), privacy stewardship, interop standards, technologies
3. Trusted "notary" for all universities and partners
4. Trusted exchange of participant information

AACRAO Tech - July 19, 2009 52

---

---

---

---

---

---

---

---

### Federations: Who's Using This Approach?

- Higher-Education Systems
  - U of TX, U of CA, U of MD...
- Network Providers
  - NJEdge, MCNC (North Carolina), Great Plains Network...
- National
  - UK, Switzerland, The Netherlands, Sweden, Norway, Denmark, France, Germany, Australia... and US

AACRAO Tech - July 19, 2009 53

---

---

---

---

---

---

---

---

### Federations: Why?

- Minimizing distribution of PII
  - Pass only what's needed for access
  - Privacy can be maintained
- Service tied to role and affiliation status
  - Changes affect access: Security
- Ease of use
  - SSO for on- and off-campus services
  - Timely access
- Time and money savings
  - Use of the same technologies and standards for each service partner

AACRAO Tech - July 19, 2009 54

---

---

---

---

---

---

---

---

## InCommon Federation

- US Research and Education Federation
  - [www.incommon.org](http://www.incommon.org)
  - LLC operated by Internet2 with separate governance
- 159 participants representing over 3 million individuals.
- Agree to a common participation rules that allows each to inter-operate with the others
  - Sets basic practices for identity providers and service providers

AACRAO Tech - July 19, 2009

55

## InCommon Identity Assurance

- Specifies criteria used to assess the credential strength of identity providers:
  - InCommon Bronze and Silver Identity Assurance Profiles
- Provides initial practices for authentication processes and technology
- Based on Foundational Government Standard: NIST 800-63 Electronic Authentication Guideline

AACRAO Tech - July 19, 2009

56

## InCommon Activities

- Collaboration
  - InC-Library, InC-Student, InC-NIH, InC-Research, InC-Apple, Dreamspark
- National and International standards
  - Co-wrote SAML spec
  - Involved in VVS-Fed, OASIS, Terena, ISOC, and Liberty Alliance and other standards and federation organizations
  - Working with PESC
- Development Work
  - Interfederation, Privacy and Consent, Evolution of Federations

AACRAO Tech - July 19, 2009

57

## FERPA Impacts on Federations

- Only available for services institution would otherwise provide
- “A contractor (or other outside service provider) that is given access to education records under this provision must be under the direct control of the disclosing institution and subject to the same conditions on use and redisclosure of education records that govern other school officials.”

-- DOE Section-by-Section Analysis of Final Rule (12/08)

AACRAO Tech - July 19, 2009

58

---

---

---

---

---

---

---

---

## FERPA Impacts on Federations

- Sharing student data attributes to enable federated identity management may implicate FERPA and other privacy laws – it all depends on who’s giving what to whom
- If you’re only passing directory information, fine except
  - Opt outs
  - Caution against widespread directory information disclosures

AACRAO Tech - July 19, 2009

59

---

---

---

---

---

---

---

---

## FERPA Impacts on Federations

- Confirming directory information with SSN etc. supplied by requester, is a disclosure of education records
- If non-directory information, need:
  - Consent
  - School official with LEI (contract) – but limited by nature of service at issue
  - Exemption for sharing records with school in which student is enrolled/plans to enroll, for purposes related to enrollment – limited
- If data shared is not personally identifiable, OK
  - E.g., “X is an enrolled student at IU”
  - To not be PII, data alone or in combination with other data out there reasonably would not allow one in the school community w/o special knowledge of circumstances, to identify student
  - PII if reasonably believe that requester knows who student is

AACRAO Tech - July 19, 2009

60

---

---

---

---

---

---

---

---

## BREAK

AACRAO Tech - July 19, 2009

61

---

---

---

---

---

---

---

---

## RESOURCES

AACRAO Tech - July 19, 2009

62

---

---

---

---

---

---

---

---

## AACRAO Resources

### Publications

*A Few Things You Should Know About Identity Management*  
[http://www.aacrao.org/identity/articles/A\\_Few\\_Things.pdf](http://www.aacrao.org/identity/articles/A_Few_Things.pdf)

*The Electronic FERPA: Access in the Digital Age – Identity and Access Management for Student Records Professionals.* C&U Journal, 85(1), 2009. (Pending publication.)

*Building an Identity Management Governance Process: A Case Study.* C&U Journal, 84(3), 2009.

*Identity and Access Management: Technological Implementation of Policy.* C&U Journal, 80(2), 2004.

AACRAO Tech - July 19, 2009

63

---

---

---

---

---

---

---

---

## AACRAO Resources

### Upcoming Events

Watch for upcoming AACRAO Webinar on  
Distribution of Remote Credentials

AACRAO Annual Conference –  
Identity Management Sessions

### Proceedings

AACRAO Identity Management Workshop

<http://www.aacrao.org/identity>

CAMP: Delivering, Sourcing, and Securing Services  
Throughout the Student Identity Life Cycle

[www.educause.edu/camp091](http://www.educause.edu/camp091)

AACRAO Tech - July 19, 2009

64

---

---

---

---

---

---

---

---

## AACRAO Tech Sessions

### Sunday

- 3:45 pm - 5:00 pm - Identity Management and the Student Life Cycle

### Monday

- 8:00 am - 9:15 am - The Student Identity Life Cycle
- 1:30 pm - 2:45 pm - Former Student Authentication, Temporary Credentials, and Online Transcript Requests: Save Time and Provide Exceptional Service
- 3:15 pm - 4:30 pm - Federating the Student Identity: A Case Study
- 5:00 pm - 6:00 pm - Roundtable: Identity and Access Management Issues

### Tuesday

- 8:00 am - 9:00 am - Security, Privacy, and Identity Management Plenary

AACRAO Tech - July 19, 2009

65

---

---

---

---

---

---

---

---

## Cornell Resources

IT Security Requirements for Confidential  
Data:

<http://www.cit.cornell.edu/security/depth/requirements/confidentialdata.cfm>

Computer Security at Cornell:

<http://www.cit.cornell.edu/catc/security/>

Cornell Policy Site:

<http://www.policy.cornell.edu/>

IT Policy Framework:

<http://www2.cit.cornell.edu/policy/framework/chart.html>

AACRAO Tech - July 19, 2009

66

---

---

---

---

---

---

---

---

## Federation Resources

NIST Special Publication 800-63:

<http://www.cio.gov/eauthentication/>

InCommon Federation:

<http://incommonfederation.org>

InCommon Identity Assurance:

<http://www.incommonfederation.org/assurance/>

AACRAO Tech - July 19, 2009

67

---

---

---

---

---

---

---

---

## Federation Case Studies

Dreamspark Student Verification Through InCommon

[www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_Dreamspark\\_2008.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_Dreamspark_2008.pdf)

Apple, InCommon Complete Pilot to Federate iTunes U

[www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_iTunes\\_2008.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_iTunes_2008.pdf)

Small Colleges Benefit from Federated Services

[www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_SmallCollege\\_2008.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_SmallCollege_2008.pdf)

Federating WebAssign Saves Time, Effort

[www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_PSU\\_WebAssign\\_2007.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_PSU_WebAssign_2007.pdf)

Federating Simplifies Access to Symplicity Career Services

[www.incommonfederation.org/docs/eg/InC\\_CaseStudy\\_PSU\\_Symplicity\\_2007.pdf](http://www.incommonfederation.org/docs/eg/InC_CaseStudy_PSU_Symplicity_2007.pdf)

AACRAO Tech - July 19, 2009

68

---

---

---

---

---

---

---

---

## Contacts

Andrea Beesing  
Cornell University  
amb3@cornell.edu

Jeff von Munkwitz-Smith  
University of Connecticut  
jvon@uconn.edu

Ann West  
EDUCAUSE/Internet2/InCommon  
awest@internet2.edu

AACRAO Tech - July 19, 2009

69

---

---

---

---

---

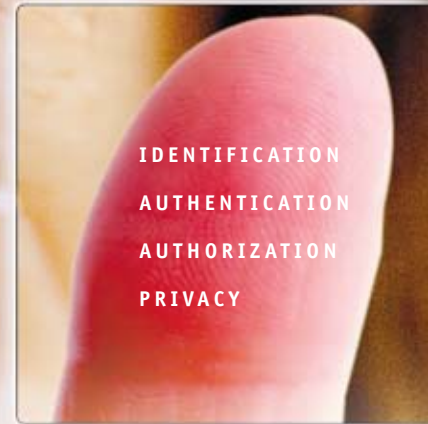
---

---

---



IDENTITY MANAGEMENT  
PARTNERS



IDENTIFICATION  
AUTHENTICATION  
AUTHORIZATION  
PRIVACY

## A Few Things You Should Know About Identity Management

### WHAT IS IDENTITY MANAGEMENT?

Identity and access management (IdM) ensures that the right people access the right services. In the past, this was implemented system by system with duplicate identity data distributed across campus and among third-party providers. Add another service and you add the identity infrastructure to go with it. Now try to manage the distributed security issues associated with these duplicate identity stores and you have your hands full. The solution is to use the same identity information service for all your applications.

Identity information about a person is collected from authoritative sources such as the human resources, payroll, student information, and other systems of record and is securely maintained in a registry. This information is then used to grant, change or rescind access to services based on a person's roles or affiliations with the institution. Identity Management includes the policy, administrative processes, and technical systems involved in online identity services and access management.

### WHY SHOULD REGISTRARS CARE?

There are several reasons why registrars should care about well-run identity services:

- **SECURITY**—Centralized management of identity information gets sensitive personal information such as SSNs out of localized departmental databases. It concentrates



1. Security
2. Enhanced Service
3. Save Money

the resources on supporting a single, secure, centralized identity repository and ensures compliance with regulations by improving auditability. Reducing the number of login ids and passwords that people manage will also reduce the number of credential-related sticky notes on monitors.

- **REDUCES DUPLICATE IDENTITY INFORMATION**—Because IdM consolidates identity and related identifiers, it helps to reduce or eliminate the instance of individuals having duplicate identifiers across campus applications.
- **SEAMLESS SERVICES**—New students experience faster access to new services as they move through their relationship life cycle from applicant to enrolled student to alumni. Role-based information from multiple sources is consolidated in the central IdM repository, and service providers can determine what populations they choose to serve (grant access) based on role and/or affiliation and attribute criteria.
- **CONSISTENT APPLICATION OF POLICY**—IdM provides a central point for the application of access-related policy. Technical staff support is reduced when resolving problems because of the existence of a common directory for which there is documentation and mapping of roles and services.
- **SAVE TIME AND MONEY**—IdM saves money by reducing redundancy in supporting multiple identity databases. Faster provisioning of new services to the campus community reduces calls from confused customers when they don't yet have expected access.
- **POSITIONING FOR THE FUTURE**—In today's electronic environment, new opportunities will continue to surface to conduct business on-line. A robust IdM system will enable new ways for providing on-line services in a secure fashion as well as enabling seamless access to third-party applications.

Ensuring *privacy* of student data  
is at the core of a registrar's mission.

### WHY SHOULD REGISTRARS BE INVOLVED?

Ensuring privacy of student data is at the core of a registrar's mission. The registrar can provide a strong role in the governance of an IdM system and the use of student personal data as well as determining the "need to know" for data access requests. The Registrar is not only a source of student information and authority on student roles, but also in touch with federal and state regulations related to the privacy and protection of student records. The Registrar will likely serve in partnership with Human Resources, and various campus service providers, as well as central campus information technology.

### WHAT'S NEXT?

If you're interested in getting IdM going on your campus, consider the following steps:

- Take information back to your campus and begin educating and stirring interest.
- Reflect how an IdM system would affect your institution and your office.
- Think about a governance process and who should participate in implementing and supporting an IdM system. See the University of Wisconsin – Madison case study for more ideas.
- Consider budgetary implications.

Have more questions? Contact AACRAO for what's going on in identity management.

Identity Management will allow us to appropriately define and change roles as students progress through their academic careers and will enable us to extend secure authenticated services such as online transcript ordering throughout our students' lifetimes.

*Karen Schultz,  
University Registrar  
The Pennsylvania State  
University*



### ◀ A BEDTIME STORY FOR STUDENT SERVICES ▶

It's 3:00 am and Bianca is sitting in a 24 hour Starbucks in the spring semester of her senior year, working on her Physics 456 homework. In a browser, she clicks on the link to the course management system, logs in with her University web single sign-on user and password, and starts viewing the course information.

Next, she clicks on the homework link hosted by a third-party provider and "Welcome Bianca" appears along with her new homework assignment for that class. After finishing that, she decides to check her loan status and surfs to the web site of her financing agent. She clicks "Access your record" and is presented with an aggregation of her loan liability without having to identify herself or login.

She takes a deep breath, wondering if any of those job applications had yielded an interview. She clicks on her shortcut to the job placement service and again is presented with the status of her applications, without having to identify herself. One company is requesting an interview, so Bianca purchases a cheap airline ticket offered by an online service that sells only to students. In the past, she had to provide proof of enrollment, but now the technology handles this in the background.

Bianca occasionally wonders what the institution is giving out to other service providers like the financial aid, job placement, and other companies on her behalf. She cares about her information and doesn't like her address and cell number available. She decides to check how this is done and clicks on the "Control your information" link provided on the web single sign-on page. She is presented with the campus information release policy that includes the policy and specific information about online transactions. Bianca knows that each of the transactions she has completed tonight implied that the institution was passing identity information on her behalf to the other sites so they could authorize her to access her information there. She opens the list of sites that she has visited and reviews the type of information that is sent. "No, that all looks okay to me." She notices that there's a music site that her institution has an agreement with, but she doesn't use. She clicks the "do not pass information" box, knowing she now can't access the service, but that they won't know anything about her either.

In April, Bianca graduated. One day she was a student and the next, an alumna. She noticed her access changed too. She now could get to an alumni networking service where she put out a query about apartments in the Bay Area. Her loan status had changed on the financing agent's site. She now was out in the wide world of opportunity and responsibility.

- What are the important policy, process and technology elements in the story?
- What important relationships exist?
- Is this an exciting vision?
- What does this story imply for governance on campus?
- What resources from AACRAO, EDUCAUSE or Internet2 might be useful?



# IdM Briefs

ARTICLE #0708

# Identity and Access Management: Technological Implementation of Policy

- Navigating the multiple processes for accessing ever-multiplying campus information systems can be a daunting task for students, faculty, and staff. This article provides a brief overview of Identity and Access Management Services. The authors review key characteristics and components of this new information architecture and address the issue of why a campus would want to implement these services. Implementation issues, particularly those where technology and policy intersect, are also discussed.

by Jeff von Munkwitz-Smith and Ann West

*Jeff's in his office and the telephone rings. The display gives him the number; it's one he recognizes. "Hi Dave, what can I do for you," he says. Dave is the director of First Year Programs and they speak pretty often. "Hi, Jeff! Some of the students in my Peer Mentoring classes are registered for the wrong sections. What's the best way to fix it?," Dave asks. "Send me a list," he replies. A few minutes later, he receives an e-mail message with a list of students to move to different sections. He gives the list to one of the staff in the Enrollment Services section of his department and a while later can let Dave know that the students are now in the correct sections.*

*Later a student knocks on his door. She's dressed in a suit and she's in tears. "Can you help me? I was in your class a few years ago." She asks. "Sure, Jennifer, I remember you. What do you need?" "I lost my purse and I need a transcript for an internship interview and I can't get a transcript without my ID card, what can I do?" "No problem, I know who you are," he tells her and informs the appropriate staff person that it's ok to give Jennifer her transcript.*

What do these two situations have in common? In both, the transactions depended on the identities of the people involved, Jeff's ability to verify their identities (and his staff members' ability to verify his identity), and the appropriateness of the transactions they requested to their roles.

Clearly, it works on an occasional basis, since we do it all the time. However, it doesn't scale. Many of the nearly two thousand faculty and 26,000 students like their problems solved promptly, but Jeff likes to sleep at night and take the occasional day off!

## Identity and Access Management

Automated approaches to these problems are not new. Access is typically managed differently in each system and then aug-

mented in an *ad hoc* fashion by people like the examples above. This wasn't a big problem years ago, when the number of systems that a person might use was limited. Now, a person might be granted access and authorities for e-mail, voice-mail, the student information system, the human resources system, the financial system, the course management system, the library system, an electronic portfolio, a campus portal, a data warehouse or data mart or two, a local area network, and who-knows-what-other campus resources. All of these might require separate applications for access, customization profiles, and IDs and passwords. Navigating the multiple processes for gaining access can be a daunting task for any new student, employee, or faculty member.

Enter the identity and access management services. This new information infrastructure has several key characteristics.

- It integrates all the pertinent information about people from multiple authoritative source systems such as those listed above. This reconciles the accounts we all have in these systems and joins our identities together under one campus unique identity. Using such a system, an application in the library, for instance, might use a person's library system ID to look up that person's e-mail address, campus address, and role at the institution to generate a message that a recalled book was being sent, print a label to use to send the book through the campus mail system, and verify the person's role at the institution to determine a due date for the book, extracting information from separate systems with separate identifiers.
- It processes and transforms information about people including their affiliations with the institution, employment status, and resource access. It then pushes out and stores the information where it can be of use to applications. For example, a campus advising system resource on study habits and the college transition is only licensed for freshmen on campus. The resource needs class standing

to verify access, but the student information system only stores credit information. This piece of information could be computed and stored in the identity management infrastructure.

And let's say ten applications written by different developers wanted to use this same information. Each of them would need to contact someone regarding the algorithm: How would someone know if they've done it correctly? How would the developers know if there are changes in the computation? Computing class standing once and making it available to applications increases likelihood of data accuracy and security and reduces development time. If the student drops out of school in the middle of the term, his or her class standing changes and access is no longer granted.

- It acts as a focus for implementation of policies concerning visibility and privacy of identity information and entitlement policies across the systems. In many cases, it's difficult to implement a privacy service that allows individuals to set higher levels of privacy in some instances (such as a request from outside the institution) than others. Having a central place for management of identity allows the individual to set a privacy profile based on policy governing the types of information being released and under what conditions. This in turn can be used by application developers across the institution.

## Components of Identity Management

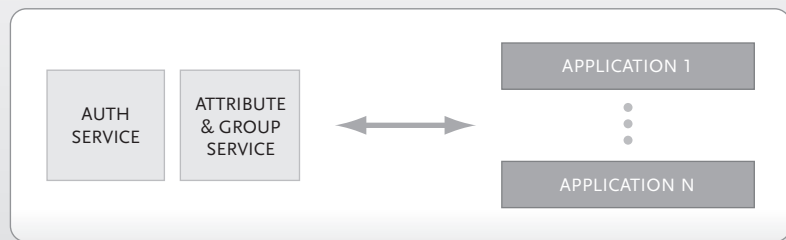
The key components of Identity Management can be summarized by four questions:

- Who are you? (Identification)
- How do we know? (Authentication)
- What services and transactions are available to you? (Authorization)
- Is the information about you secure? (Privacy)

"Identity" is the set of attributes about, and identifiers referring to, an individual. The question "Who are you?" is usually answered by a username or ID that uniquely identifies an individual user. It might be an identifier already associated with an individual, such as the SSN. It might be system-assigned, as is the case with many of our administrative sys-



**Stovepipe (or silo):** Each application performs its own authentication and consults its own database for authorization and customization attributes.



**Integrated:** Suite of applications refer authentication to and obtain attributes for authorization and customization from common infrastructure services.

(Graphic courtesy of Thomas J. Barton, University of Chicago.)

FIGURE 1: COMPARATIVE SERVICE ARCHITECTURES

tems. Or it might be user-assigned, as is the case with most commercial services we access via the Web.

"Authentication" is the process used to verify that individual's, or "subject's," association with an identifier. The most common form of authentication used by our system is a password. Identity cards, often used in combination with a password or personal identification number are also common, particularly with financial transactions. A less common method of authentication, outside of the movies, is biometric identification using a unique physical characteristic, such as a fingerprint, voiceprint, or retinal pattern. The most secure authentication would use a combination of these forms. Identification and authentication link the electronic identity to the physical individual.

"Authorization" is the process of determining if policy permits an intended action to proceed. For individual systems—online library resources, for example—the authorization for access might be all or nothing. For other systems the authorization might be group-based or role-based. An example of this access might be one where all employees have access to view their own payroll information, but only payroll staff are able to update that information. In other cases, the authorization could be controlled at the transaction and field level, with the individual being able to process certain types of transactions for a limited range of data, such as the chair of



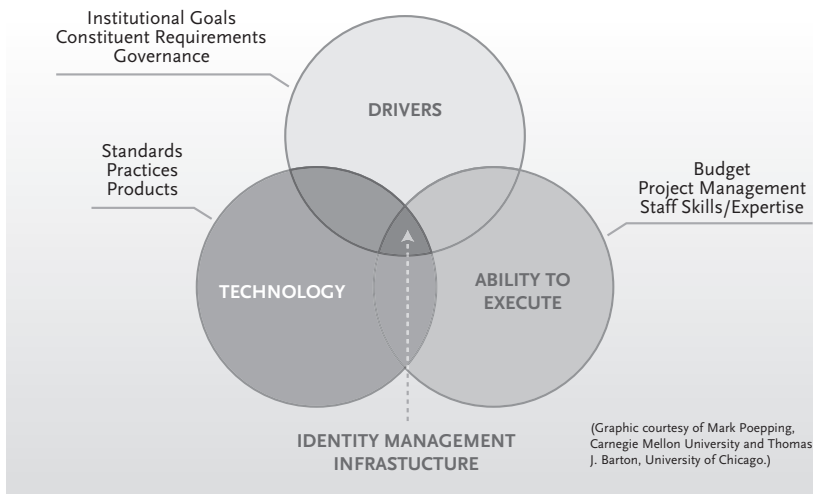


FIGURE 2: IDENTITY MANAGEMENT FACTORS

history department being the only member of that department allowed to update course instructors. Electronic authorization is, ideally, the technical manifestation of institutional policy. Its efficacy is limited by the availability of subject attributes and by how faithfully policy is incorporated in the infrastructure or application.

### Why would your campus want one?

Besides the obvious opportunities for making existing services more convenient to use and for developing new services not easily possible using older systems for authorization and authentication, there are six reasons why an institution ought to consider implementing an identity and access management system.

- **Reduced overhead of service management**—In typical application delivery models, each service maintains its own user identity store and related authentication (and authorization) services. Simplifying the authentication model by having the applications use the same shared identity and access infrastructure not only reduces the staff and resulting overhead required to manage each application, but also achieves substantial economies of scale for the service providers and results in time and system cost savings. Having consolidated systems and business processes for authentication services also reduces the cost and time to deploy new applications. Since these services do not need to be created for each new application, the cost and time of doing so, and the recurring cost of independently maintaining those services are mitigated. (See Figure 1.)
- **Increased security**—Security and privacy issues are not new to higher education. After all, we've operated under FERPA (Family Educational Rights and Privacy Act) since 1974. With the growth of identity theft there is a greater awareness and, as we discuss below, the regulatory requirements have become more stringent. Consolidating the

identity and access services for separate applications means that related policies can be supported in one protected place by the same group of staff. Because the same user credential is presented to all integrated services, all system and application log files reference the same identifier. This enables a consolidated approach to logging which assists in the investigations of alleged cases of abuse. In reduced sign-on instances, users need to remember fewer credentials. They may therefore employ less creative password memory-jogging mechanisms, and are more likely to remember them. For those campuses with a distributed model that provide password feeds to departments to simulate a single-password environment, having the applications instead

access a consolidated authentication service reduces the likelihood of password theft and the chance the department password data is corrupted.

- **Simplified network and online service access**—Consolidated authentication can enable unified identity verification for many online services, so our constituents need only to provide a reduced set of credentials, with user ID/password pairs being the most common. Because of the integration with Web-based applications, solutions to common service issues like self-service password resetting and management are enabled using a common infrastructure.
- **Contractual requirements**—Campuses must be able to prove that resources are being used by the subjects licensed to do so. This could be due to a specific library or course-resource contract or because of funding agency requirements and access to restricted research findings. For example, a faculty member working on a classified project might need to provide funding and employment status—information currently stored in two different administrative systems—for access to online resources. Another illustration includes an e-procurement site that might want information on the employment status, title, and department in order to make a decision to process an individual's order. Contractual obligations, such as those restricting access to licensed electronic resources to people affiliated with our institutions, also play a role. When we charge users fees—either directly or as part of a general student fee—for use of specific resources, such as student recreational facilities, we may want to ensure that only the group that pays has access to those resources.
- **Legal pressures**—Institutions are required to restrict access to health, financial, and academic records. And while FERPA requires us to keep student information private, both the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB) include requirements that we have plans

## MORE INFORMATION ON IDENTITY AND ACCESS MANAGEMENT SYSTEMS

The NMI-EDIT Consortium (Enterprise and Desktop Integration Technologies–EDIT) Consortium, part of the NSF Middleware Initiative (NMI), comprises Internetz, EDUCAUSE, and the Southeastern Universities Research Association (SURA). The Consortium offers practice documents, software, tools, and architectures to facilitate inter-institutional resources sharing and collaboration. For more information on the components in an identity management system, review the following:

- NMI-EDIT offers half-day and full-day workshops for CIOs, technical architects, and project managers, covering basic and advanced topics in

identity and access management and related topics. Visit the NMI-EDIT Web site at [www.nmi-edit.org](http://www.nmi-edit.org) for locations, topics, and dates.

- For additional information and networking opportunities with experienced architects and management, consider attending the Campus Architectural Middleware Planning (CAMP) sessions. Check the NMI-EDIT, EDUCAUSE, or Internetz Web sites for details.
- For a current list of tools, documents, software and schemas available from NMI-EDIT relating to identity management components, visit the

Releases section of the NMI-EDIT Web site or the Internetz Middleware Initiative site at <http://middleware.internetz.edu>.

- To discuss Identity Management with your colleagues, subscribe to the EDUCAUSE Middleware Constituent Group at [www.educause.edu/cg/middleware.asp](http://www.educause.edu/cg/middleware.asp).
- For more information on the NSF Middleware Initiative, visit <http://nsf-middleware.org>. For questions concerning identity management tools and resources, contact Ann West at [awest@educause.edu](mailto:awest@educause.edu) or [awest@internetz.edu](mailto:awest@internetz.edu).

in place for maintaining security of the covered information. It is no longer sufficient to merely not release private information; we also have an obligation to keep the information secure.

- **Business and ethical stewardship**—Institutions must also consider the requirements of doing business including safeguarding confidential information and intellectual property, and other strategic information. This includes ensuring appropriate access to tenure committee communications, salary and review information, institutional planning, and archive information, to name a few. The institution also has an ethical obligation to protect information that can be, for example, used for identity theft. A very concrete example of this is restricting access to and use of social security numbers in states where no legislation exists to protect them.

### Implementation Issues

While not minimizing the effort involved in implementing the technology pieces, the issues related to policy tend to be the stickiest ones to resolve, requiring the collaboration of numerous campus participants. (See Figure 2.)

#### INTERDEPENDENCY: WE'RE ALL IN THIS TOGETHER

Tying together the access to our applications so their use can be updated, enabled, or disabled quickly is a powerful thing. However, what we do on a daily basis affects may people we're unaware of and small, uncommunicated changes can make for unforeseen consequences.

For example, a new, temporary policy allows returning students to pay their bills a week late. This grace period begins, and the Bursar's Office hasn't received Bob's bill and doesn't update his active status in the SIS system. And as usual, every half hour, the identity management system checks the active status, updates its information, and, in this case, removes the contents of the attributes used in authorizing Bob's access to the library service, health service, course management sys-

tem, e-mail, and departmental accounts. At 7:30 a.m., Bob tries to log on and read e-mail and can't, contrary to the new policy. In this case, the operating policy consequences ripple out to the applications served by the infrastructure and the student is confused.

#### TRADEOFFS: RISK AND SERVICE DELIVERY

A critical part of the identity and access management function is an accompanying security policy that highlights the goals and levels of trust the systems will support. From this (and other things), the technology and procedures are derived. For instance, providing access to a course resource site might require a different security level, than, say, an application that changes a student's financial aid. Looking further, to reset one's password in the first scenario might require answering two predefined questions online and, in the second, visiting a particular office in person.

So what if there's a mismatch between the level of security supported by the infrastructure and that required by the application? Or vice versa? Coupled with increased security is increased cost and decreased risk, but how important is the new application to the institution, and who will pay this increased cost? Is it worth it? And who makes the decisions regarding the tradeoffs? This is where a well developed governance process comes into play.

#### GOVERNANCE: COMMUNICATION IS CRITICAL

Data stewardship policies and ongoing interpretations of them are classic examples of the need for governance. Setting up a definition of stewardship, the responsibilities of the steward as well as the user of the data (application developers) is important for those using the identity management system. The stewardship of the identity management system should be discussed as well. Usually it's a combined management of IT (for the service), data stewards (for the data), and the policy stewards. Additional players including the risk managers and auditors, online service providers and resource managers, application champions, and system users.

A classic example of a problem that the technologists typically receive, but should be considered at policy level is that of a faculty member who wants to give a colleague at another institution access to an online course he is teaching. They are collaborating on research on pedagogy in their field, and he believes that it would be helpful for his colleague to view what's happening in the course. It would require little effort to create an affiliate ID in the identity management system for the colleague and to give her access to the online course and the identities of the students and their grades. However, this raises potential FERPA issues. Would the person processing the request for an affiliate ID know enough to ask the right questions?

Communication and education about the challenges and issues that we each face on a daily basis is crucial. In the most successful implementations, policy examination and interpretation is an integral part of the process and an on-going, rather than a one-time, event. It is critical that all of the groups—data and policy stewards, technology staff, and others—understand both policy and technology issues well enough to identify potential problems as they arise and know how to get them resolved.

## Conclusion

In general, we're all trying to accomplish similar things, such as transitioning to self-managed services for faculty, staff, students, parents, alumni and any constituent the institution wants to maintain a relationship with. In fact, we want contact with more people, earlier in their affiliation with us, wherever they are, and for life. Beyond that, we want these services to work and we want a degree of trust that only those we want to access them do so. Beyond that, we hear rumors of government-sponsored electronic services that are reliant on our campus ability to vouch that a student or faculty member is who they say they are. All this can't be done cost effectively or reliably without an identity management system.

*This material is based in whole or in part on work supported by the National Science Foundation under the NSF Middleware Initiative—NSF 02-028, Grant No. ANI-0123937. Thanks are extended to Mark Bruhn of Indiana University and Michael Gettes of Duke University for their ideas and contributions.*

## ABOUT THE AUTHORS

**Jeff von Munkwitz-Smith, Ph.D.** is the University Registrar at the University of Connecticut.

**Ann West** has a joint appointment with EDUCAUSE and Internet2 to lead the outreach activities of their National Science Foundation Middleware Initiative Award.

*This article originally appeared in the Fall 2004 (Volume 80, No. 2) issue of College & University, and is being reproduced/ distributed with the permission of the American Association of Collegiate Registrars and Admissions Officers. Copyright 2004.*



# **File>>Properties>>Title: Requestname Data Access Request/Agreement**

This document describes a request and subsequent agreement between the requester and data steward(s) for approved access to the data in a manner that is specified herein. This document is specific to a singular business process and service delivery mechanism. This agreement may be reexamined at the discretion of the data steward(s) to ensure:

- adherence to relevant University Policies,
- business application consumption of the service is accurate and appropriate,
- authentication and authorization mechanisms are adequately maintained,
- delivery mechanisms are adequately secured, and
- other considerations have not compromised the original intent of the approved request.

## **TOC**

<b><u>I. Request Contact Information</u></b>	<b>2</b>
<b><u>II. Provisions</u></b>	<b>2</b>
<b><u>III. Signature Page</u></b>	<b>3</b>
<b><u>IV. Request Description</u></b>	<b>4</b>
<b><u>V. Security</u></b>	<b>5</b>

## I. Request Contact Information

**Sponsor Name – Title:**

**Contact/Designer Name – Title:**

**CIT Analyst Name – Title:**

**Developer Name – Title:**

## II. Provisions

**The Requester** agrees to Data Steward(s) discretionary review of this agreement.

**The Requester** acknowledges adherence to all relevant University Policy, and in particular:

**University Policy 4.12, DATA STEWARDSHIP AND CUSTODIANSHIP**, (<http://www.univco.cornell.edu/policy/DA.for.html>), including the **Access to University Data Agreement** (<http://www.univco.cornell.edu/forms/policy/daagreement.doc>)

**University Policy 5.4, SECURITY OF INFORMATION TECHNOLOGY RESOURCES**, (<http://www.univco.cornell.edu/policy/SEC.for.html>)

**University Policy 4.5, ACCESS TO STUDENT INFORMATION**, (<http://www.univco.cornell.edu/policy/ASI.for.html>)

As necessary, Authentication and Authorization and will utilize University approved mechanisms, including CUWebLogin (<http://aads.cit.cornell.edu/authentication/index.html>).

In the case of web service access to data, our delivery mechanism will be required to utilize an application-specific Kerberos SRVTAB to be provided upon preliminary approval from the data steward(s).



### III. Signature Page

**Request Sponsor** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

**Request Sponsor** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

**Data Steward** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

**Data Steward** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

**Data Steward** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

**Data Steward** \_\_\_\_\_ **Date** \_\_\_\_\_  
Name – Title

## IV. Request Description

**Business Case:**

**Application Name and Description:**

**Request Date of Availability of the Data (MM/DD/YYYY):**

**Related Web Services:**

**Data Delivery mechanism:**

### **Data Requirements:**

Provide overview of the data that will be retrieved from each system that will be accessed. Specify batch or real-time access. Specify one-time or on-going.

**Data Input:**

<i>Field</i>

**Data Output:**  
Specify the number of occurrences of the data that are expected.

**The constituency populations of output data to be delivered:**  
Specify the constituency populations

*For All Populations:*

Specify the number of occurrences of the data that are expected.

**The constituency populations of output data to be delivered:**  
Specify the constituency populations

*For All Populations:*

**The constituency populations of output data to be delivered:**  
Specify the constituency populations

*For All Populations:*

**Specify the constituency populations**

*For All Populations:*

**For All Populations:**

[illegible]


## V. Security

**This request is for Self Service and Proxy/Admin (see *Authentication / Authorization below*)**

**Authentication will be set up for access to this data, if delivered via an application, in the following manner:**

**Authorization will be set up for access to this data, if delivered via an application, in the following manner:**

NIST Special Publication 800-63  
Version 1.0.2

**NIST**  
**National Institute of  
Standards and Technology**  
Technology Administration  
U.S. Department of Commerce

# Electronic Authentication Guideline

*Recommendations of the  
National Institute of  
Standards and Technology*

**William E. Burr**  
**Donna F. Dodson**  
**W. Timothy Polk**

## I N F O R M A T I O N   S E C U R I T Y

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

***April 2006***



### **U.S. Department of Commerce**

*Donald L. Evans, Secretary*

### **Technology Administration**

*Robert Cresanti, Under Secretary of Commerce for Technology*

### **National Institute of Standards and Technology**

*William Jeffrey, Director*



## **Reports on Computer Systems Technology**

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

## Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

**National Institute of Standards and Technology Special Publication 800-63, 64 pages  
(April 2006)**

Certain commercial entities, equipment, or material may be identified in the document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose.

## **Abstract**

This recommendation provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.

**KEY WORDS:** Authentication, Authentication Assurance, Credentials Service Provider, Cryptography, Electronic Authentication, Electronic Credentials, Electronic Transactions, Electronic Government, Identity Proofing, Passwords, PKI, Public Key Infrastructure, Tokens.

## **Acknowledgments**

The authors, Bill Burr, Tim Polk and Donna Dodson of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

## Executive Summary

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network, for the purpose of electronic government and commerce. This recommendation provides technical guidance to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system. This guidance addresses only traditional, widely implemented methods for remote authentication based on secrets. With these methods, the individual to be authenticated proves that he or she knows or possesses some secret information. NIST expects to explore other means of remote authentication (for example using biometrics, or by extensive knowledge of private, but not truly secret, personal information) and may develop additional guidance on the use of these methods for remote authentication.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [\[OMB 04-04\]](#) that defines four levels of authentication Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, the document states specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,
- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

A summary of the technical requirements for each of the four levels is provided below.

**Level 1** - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing

the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

**Level 2** – Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. It allows any of the token methods of Levels 3 or 4, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

**Level 3**– Level 3 provides multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish

two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

**Level 4** – Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

## Table of Contents

1. Purpose.....	1
2. Authority .....	1
3. Introduction.....	1
4. Definitions and Abbreviations .....	4
5. E-Authentication Model.....	9
5.1. Subscribers, RAs and CSPs .....	10
5.2. Tokens.....	11
5.3. Electronic Credentials .....	12
5.4. Verifiers .....	13
5.5. Assertions.....	13
5.6. Relying Parties .....	14
6. Tokens.....	15
6.1. Token Threats .....	16
6.2. Token Levels.....	16
7. Registration and Identity Proofing.....	19
7.1. Registration Threats .....	19
7.1.1. Threat Model.....	19
7.1.2. Resistance to Registration Threats.....	20
7.2. Registration Levels .....	20
7.2.1. Registration and Identity Proofing Requirements.....	21
7.2.2. Records Retention Requirements.....	25
7.3. Mapping FPKI Certificate Policies to Registration Levels.....	25
8. Authentication Protocols.....	26
8.1. Authentication Threats.....	26
8.1.1. Authentication Protocol Threats .....	26
8.1.2. Resistance to Protocol Threats.....	27
8.1.3. Other Threats .....	29
8.2. Authentication Mechanism Requirements.....	30
8.2.1. Level 1 .....	31
8.2.2. Level 2 .....	32
8.2.3. Level 3 .....	34
8.2.4. Level 4 .....	37
9. Summary of Technical Requirements by level.....	38
9.1.1. Relationship of PKI Policies to E-authentication Assurance Levels .....	41
10. References.....	43
10.1. General References .....	43
10.2. NIST ITL Bulletins .....	43
10.3. NIST Special Publications .....	44
10.4. Federal Information Processing Standards .....	45
10.5. Certificate Policies .....	45



Appendix A: Estimating Password Entropy and Strength..... 46

    A.1 Randomly Selected Passwords..... 47

    A.2 User Selected Passwords..... 47

    A.2 Other Types of Passwords..... 51

    A.3 Examples..... 51

Appendix B: Errata ..... 54

    Appendix B.1: Errata for Version 1.0.1 ..... 54

    Appendix B.2: Errata for Version 1.0.2..... 54

## 1. Purpose

This recommendation provides technical guidance to agencies in the implementation of electronic authentication (e-authentication).

## 2. Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

## 3. Introduction

Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. E-authentication presents a technical challenge when this process involves the remote authentication of individual people over a network. This recommendation provides technical guidance to agencies to allow an individual person to remotely authenticate his/her identity to a Federal IT system.

This technical guidance supplements OMB guidance, *E-Authentication Guidance for Federal Agencies*, [OMB 04-04] that defines four levels of assurance Levels 1 to 4, in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with criteria for determining the level of e-authentication assurance required for specific electronic transactions and systems, based on the risks and their likelihood of occurrence.

This document states specific technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,
- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

The overall authentication assurance level is determined by the lowest assurance level achieved in any of the four areas listed above.

This technical guidance covers remote electronic authentication of human users to Federal agency IT systems over a network. It does not address the authentication of a person who is physically present, for example for access to buildings, although some credentials and tokens that are used remotely may also be used for local authentication. While this technical guidance does, in many cases, establish requirements that Federal IT systems and service providers participating in authentication protocols be authenticated to subscribers, it does not specifically address machine-to-machine (such as router-to-router) authentication, nor does this guidance establish specific requirements for issuing authentication credentials and tokens to machines and servers when they are used in e-authentication protocols with people.

The paradigm of this document is that individuals are enrolled and undergo an identity proofing process in which their identity is bound to an authentication secret, called a token. Thereafter, the individuals are remotely authenticated to systems and applications over an open network, using the token in an authentication protocol. The authentication protocol allows an individual to demonstrate to a verifier that he has or knows the secret token, in a manner that protects the secret from compromise by different kinds of attacks. Higher authentication assurance levels require use of stronger tokens (harder to guess secrets) and better protection of the token from attacks. This document covers only authentication mechanisms that work by making the individual demonstrate possession and control of a secret.

It may also be practical to achieve authentication by testing the personal knowledge of the individual (referred to as knowledge based authentication). As this information is private but not actually secret, confidence in the identity of an individual can be hard to achieve. In addition, the complexity and interdependencies of knowledge based authentication systems are difficult to quantify. However, knowledge based authentication techniques are included as part of registration in this document.

Biometric methods are widely used to authenticate individuals who are physically present at the authentication point, for example for entry into buildings. Biometrics do not constitute secrets suitable for use in the conventional remote authentication protocols

addressed in this document. In the local authentication case, where the claimant is observed and uses a capture device controlled by the verifier, authentication does not require that biometrics be kept secret. The use of biometrics to “unlock” conventional authentication tokens and to prevent repudiation of registration is identified in this document.

NIST is continuing to study both the topics of knowledge based authentication and biometrics and may issue additional guidance on their uses for remote authentication of individuals across a network.

This document identifies minimum technical requirements for remotely authenticating identity. Agencies may determine based on their risk analysis that additional measures are appropriate in certain contexts. In particular, privacy requirements and legal risks may lead agencies to determine that additional authentication measures or other process safeguards are appropriate. When developing e-authentication processes and systems, agencies should consult *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* [[OMB 03-22](#)]. See the *Guide to Federal Agencies on Implementing Electronic Processes* for additional information on legal risks, especially those that related to the need to satisfy legal standards of proof and prevent repudiation [[DOJ 2000](#)].

## 4. Definitions and Abbreviations

Active Attack	An attack on the authentication protocol where the attacker transmits data to the claimant or verifier. Examples of active attacks include a man-in-the-middle, impersonation, and session hijacking.
Address of Record	The official location where an individual can be found. The address of record always includes the residential street address of an individual and may also include the mailing address of the individual. In very limited circumstances, an Army Post Office box number, Fleet Post Office box number or the street address of next of kin or of another contact individual can be used when a residential street address for the individual is not available.
Attack	An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possess a claimant's token.
Attacker	A party who is not the claimant or verifier but wishes to successfully execute the authentication protocol as a claimant.
Approved	FIPS approved or NIST recommended. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation. Approved cryptographic algorithms must be implemented in a crypto module validated under FIPS 140-2. For more information on validation and a list of validated FIPS 140-2 validated crypto modules see <a href="http://csrc.nist.gov/cryptval/">http://csrc.nist.gov/cryptval/</a> .
Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol.
Asymmetric keys	Two related keys, a public key and a private key that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
Authentication	The process of establishing confidence in user identities.
Authentication protocol	A well specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.
Authenticity	The property that data originated from its purported source.
Bit	A binary digit: 0 or 1.
Biometric	An image or template of a physiological attribute (e.g., a fingerprint) that may be used to identify an individual. In this document, biometrics may be used to unlock authentication tokens and prevent repudiation of registration.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Certificate Revocation	A list of revoked public key certificates created and digitally signed by

List (CRL)	a Certification Authority. See <a href="#">[RFC 3280]</a>
Challenge-response protocol	An authentication protocol where the verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier. The verifier knows the shared secret and can independently compute the response and compare it with the response generated by the claimant. If the two are the same, the claimant is considered to have successfully authenticated himself. When the shared secret is a cryptographic key, such protocols are generally secure against eavesdroppers. When the shared secret is a password, an eavesdropper does not directly intercept the password itself, but the eavesdropper may be able to find the password with an off-line password guessing attack.
Claimant	A party whose identity is to be verified using an authentication protocol.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Credentials Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass Registration Authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cryptographic key	A value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification. For the purposes of this document, keys must provide at least 80-bits of protection. This means that it must be as hard to find an unknown key or decrypt a message, given the information exposed to an eavesdropper by an authentication, as to guess an 80-bit random number. See also Asymmetric keys, Symmetric key.
Cryptographic strength	A measure of the expected number of operations required to defeat a cryptographic mechanism. For the purposes of this document, this term is defined to mean that breaking or reversing an operation is at least as difficult computationally as finding the key of an 80-bit block cipher by key exhaustion, that is it requires at least on the order of $2^{79}$ operations.
Cryptographic token	A token where the secret is a cryptographic key.
Data integrity	The property that data has not been altered by an unauthorized entity.
Digital Signature	An asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature. Digital signatures provide authentication and integrity protection.
Electronic Credentials	Digital documents used in authentication that bind an identity or an attribute to a subscriber's token. Note that this document distinguishes between credentials, and tokens (see below) while other documents may interchange these terms.
Entropy	A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. See

	otherwise stated no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking...) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party).
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Off-line attack	An attack where the attacker obtains some data (typically by eavesdropping on an authentication protocol run, or by penetrating a system and stealing security files) that he/she is able to analyze in a system of his/her own choosing.
On-line attack	An attack against an authentication protocol where the attacker either assumes the role of a claimant with a genuine verifier or actively alters the authentication channel. The goal of the attack may be to gain authenticated access or learn authentication secrets.
On-Line Certificate Status Protocol (OCSP)	An on-line protocol used to determine the status of a public key certificate. See [RFC 2560].
Passive attack	An attack against an authentication protocol where the attacker intercepts data traveling along the network between the claimant and verifier, but does not alter the data (i.e. eavesdropping).
Password	A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings.
Possession and control of a token	The ability to activate and use the token in an authentication protocol.
Personal Identification Number (PIN)	A password consisting only of decimal digits.
Practice Statement	A formal statement of the practices followed by an authentication entity (e.g., RA, CSP, or verifier); typically the specific steps taken to register and verify identities, issue credentials and authenticate claimants.
Private key	The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.
Proof of Possession (PoP) protocol	A protocol where a claimant proves to a verifier that he/she possesses and controls a token (e.g., a key or password)
Protocol run	An instance of the exchange of messages between a claimant and a verifier in a defined authentication protocol that results in the authentication (or authentication failure) of the claimant.
Public key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.
Public key certificate	A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the

	certificate has sole control and access to the private key. See also <a href="#">[RFC 3280]</a>
Pseudonym	A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.
Registration	The process through which a party applies to become a subscriber of a CSP and an RA validates the identity of that party on behalf of the CSP.
Registration Authority (RA)	A trusted entity that establishes and vouches for the identity of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP, but it has a relationship to the CSP(s).
Relying party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.
Salt	A non-secret value that is used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.
Security Assertion Markup Language (SAML)	A specification for encoding security assertions in the XML markup language. See: <a href="http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security">http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security</a>
Shared secret	A secret used in authentication that is known to the claimant and the verifier.
Subject	The person whose identity is bound in a particular credential.
Subscriber	A party who receives a credential or token from a CSP and becomes a claimant in an authentication protocol.
Symmetric key	A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and web servers. TLS is defined by <a href="#">[RFC 2246]</a> and <a href="#">[RFC 3546]</a> . TLS is similar to the older Secure Socket Layer (SSL) protocol and is effectively SSL version 3.1.
Tunneled password protocol	A protocol where a password is sent through a protected channel. For example, the TLS protocol is often used with a verifier's public key certificate to (1) authenticate the verifier to the claimant, (2) establish an encrypted session between the verifier and claimant, and (3) transmit the claimant's password to the verifier. The encrypted TLS session protects the claimant's password from eavesdroppers.
Verified Name	A subscriber name that has been verified by identity proofing.
Verifier	An entity that verifies the claimant's identity by verifying the claimant's possession of a token using an authentication protocol. To do this, the verifier may also need to validate credentials that link the token and identity and check their status.
Verifier impersonation attack	An attack where the attacker impersonates the verifier in an authentication protocol, usually to learn a password.



## 5. E-Authentication Model

In accordance with [OMB 04-04] e-authentication is the process of establishing confidence in user identities electronically presented to an information system. Systems can use the authenticated identity to determine if that individual is authorized to perform an electronic transaction. In most cases, the authentication and transaction take place across an open network such as the Internet, however in some cases access to the network may be limited and access control decisions may take this into account.

E-authentication begins with *registration*. An *applicant* applies to a *Registration Authority (RA)* to become a *subscriber* of a *Credential Service Provider (CSP)* and, as a subscriber, is issued or registers a secret, called a *token*, and a *credential* that binds the token to a name and possibly other attributes that the RA has verified. The token and credential may be used in subsequent authentication events.

The subscriber's name may either be a *verified name* or a *pseudonym*. A verified name is associated with the identity of a real person and before an applicant can receive credentials or register a token associated with a verified name, he or she must demonstrate that the identity is a real identity, and that he or she is the person who is entitled to use that identity. This process is called *identity proofing*, and is performed by an RA that registers subscribers with the CSP. At Level 1, since names are not verified, names are always assumed to be pseudonyms. Level 2 credentials and assertions must specify whether the name is a verified name or a pseudonym. This information assists *relying parties*, that is parties who rely on the name or other authenticated attributes, in making access control or authorization decisions. Only verified names are allowed at Levels 3 and 4.

In this guidance, the party to be authenticated is called a *claimant* and the party verifying that identity is called a *verifier*. When a *claimant* successfully demonstrates possession and control of a token in an on-line authentication to a *verifier* through an *authentication protocol*, the verifier can verify that the claimant is the subscriber. The verifier passes on an assertion about the identity of the subscriber to the relying party. That assertion includes identity information about a subscriber, such as the subscriber name, an identifier assigned at registration, or other subscriber attributes that were verified in the registration process (subject to the policies of the CSP and the needs of the application). Where the verifier is also the relying party, the assertion may be implicit. In addition, the subscriber's identifying information may be incorporated in credentials (e.g., public key certificates) made available by the claimant. The relying party can use the authenticated information provided by the verifier/CSP to make access control or authorization decisions.

Authentication simply establishes identity, or in some cases verified personal attributes (for example the subscriber is a US Citizen, is a student at a particular university, or is assigned a particular number or code by an agency or organization), not what that identity is authorized to do or what access privileges he or she has; this is a separate decision.

Relying parties, typically government agencies, will use a subscriber's authenticated identity and other factors to make access control or authorization decisions. In many cases, the authentication process and services will be shared by many applications and agencies, but the individual agency or application is the relying party that must make the decision to grant access or process a transaction based on the specific application requirements. This guidance provides technical recommendations for the process of authentication, not authorization.

In summary, an individual applicant applies first to an RA. The RA identity proofs that applicant. As the result of successful identity proofing, the applicant becomes a subscriber of a CSP associated with the RA, with a credential and a secret token registered to the subscriber. When the subscriber needs to authenticate to perform a transaction, he or she becomes a claimant to a verifier. The claimant proves to the verifier that he or she controls the token, using an authentication protocol. If the verifier is separate from the relying party (application), the verifier provides an assertion about the claimant to the relying party, which uses the information in the assertion to make an access control or authorization decision. If the transaction is significant, the relying party may log the subscriber identity and credential(s) used in the authentication along with relevant transaction data.

### ***5.1. Subscribers, RAs and CSPs***

In the conceptual e-authentication model, a claimant in an authentication protocol is a subscriber to some CSP. At some point, an applicant registers with an RA, which verifies the identity of the applicant, typically through the presentation of paper credentials and by records in databases. This process is called identity proofing. The RA, in turn, vouches for the identity of the applicant (and possibly other verified attributes) to a CSP. The applicant then becomes a subscriber of the CSP.

The CSP establishes a mechanism to uniquely identify each subscriber and the associated tokens and credentials issued to that subscriber. The CSP registers or gives the subscriber a token to be used in an authentication protocol and issues credentials as needed to bind that token to the identity, or to bind the identity to some other useful verified attribute. The subscriber may be given electronic credentials to go with the token at the time of registration, or credentials may be generated later as needed. Subscribers have a duty to maintain control of their tokens and comply with the responsibilities to the CSP. The CSP maintains registration records for each subscriber to allow recovery of registration records.

There is always a relationship between the RA and CSP. In the simplest and perhaps the most common case, the RA/CSP are separate functions of the same entity. However, an RA might be part of a company or organization that registers subscribers with an independent CSP, or several different CSPs. Therefore a CSP may have an integral RA, or it may have relationships with multiple independent RAs, and an RA may have relationships with different CSPs as well.

Section 7 provides recommendations for the identity proofing and registration process.

## 5.2. Tokens

Tokens generically are something the claimant possesses and controls that may be used to authenticate the claimant's identity. In e-authentication, the claimant authenticates to a system or application over a network. Therefore, a token used for e-authentication is a secret and the token must be protected. The token may, for example, be a cryptographic key, that is protected by encrypting it under a password. An impostor must steal the encrypted key and learn the password to use the token.

Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a voice print or other biometric)

Authentication systems that incorporate all three factors are stronger than systems that only incorporate one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, consider a hardware device that holds a cryptographic key. The key might be activated by a password or the hardware device might include a biometric capture device and uses a biometric to activate the key. Such a device is considered to effectively provide two factor authentication, although the actual authentication protocol between the verifier and the claimant simply proves possession of the key.

The secrets are often based on either *public key pairs* (asymmetric keys) or *shared secrets*. A *public key* and a related private key comprise a public key pair. The *private key* is used by the claimant as a token. A verifier, knowing the claimant's public key through some credential (typically a *public key certificate*), can use an authentication protocol to verify the claimant's identity, by proving that the claimant has control of the associated private key token (*proof of possession*).

Shared secrets are either *symmetric keys* or passwords. In a protocol sense, all shared secrets are similar, and can be used in similar authentication protocols; however, passwords, since they are often committed to memory, are something the claimant knows, rather than something he has. Passwords, because they are committed to memory, usually do not have as many possible values as cryptographic keys, and, in many protocols, are vulnerable to network attacks that are impractical for keys. Moreover the entry of passwords into systems (usually through a keyboard) presents the opportunity for very simple keyboard logging or "shoulder surfing" attacks. Therefore keys and passwords demonstrate somewhat separate authentication properties (something you know rather than something you have). Passwords often have lesser resistance to network attacks. However, when using either public key pairs or shared secrets, the

subscriber has a duty to maintain exclusive control of his token, since possession and control of the token is used to authenticate the subscriber's identity.

Biometrics are unique personal attributes that can be used to identify a person. They include facial pictures, fingerprints, DNA, iris and retina scans, voiceprints and many other things. In this document, biometrics are used in the registration process to be able to later prevent a subscriber who in fact registered from repudiating the registration, to help identify those who commit registration fraud, and to unlock tokens. Biometrics are not used directly as tokens in this document.

As defined in Section 6, this guidance recognizes four kinds of claimant tokens: hard tokens, soft tokens, one-time password device tokens and password tokens.

### ***5.3. Electronic Credentials***

Paper credentials are documents that attest to the identity or other attributes of an individual or entity called the subject of the credentials. Some common paper credentials include passports, birth certificates, driver's licenses, and employee identity cards. The credentials themselves are authenticated in a variety of ways: traditionally perhaps by a signature or a seal, special papers and inks, high quality engraving, and today by more complex mechanisms, such as holograms, that make the credentials recognizable and difficult to copy or forge. In some cases, simple possession of the credentials is sufficient to establish that the physical holder of the credentials is indeed the subject of the credentials. More commonly, the credentials contain biometric information such as the subject's description, a picture of the subject or the handwritten signature of the subject that can be used to authenticate that the holder of the credentials is indeed the subject of the credentials. When these paper credentials are presented in-person, authentication biometrics contained in those credentials can be checked to confirm that the physical holder of the credential is the subject.

Electronic identity credentials bind a name and perhaps other attributes to a token. This recommendation does not prescribe particular kinds of electronic credentials. There are a variety of electronic credential types in use today, and new types of credentials are constantly being created. At a minimum, credentials include identifying information that permits recovery of the records of the registration associated with the credentials and a name that is associated with the subscriber. In every case, given the issuer and the identifying information in the credential, it must be possible to recover the registration records upon which the credentials are based. Electronic credentials may be general-purpose credentials or targeted to a particular verifier. Some common types of credentials are:

- X.509 public key identity certificates that bind an identity to a public key;
- X.509 attribute certificates that bind an identity or a public key with some attribute;
- Kerberos tickets that are encrypted messages binding the holder with some attribute or privilege.

Electronic credentials may be stored as data in a directory or database. These credentials may be digitally signed objects (e.g., X.509 certificates), in which case their integrity may be verified. In this case, the directory or database may be an untrusted entity, since the data it supplies is self-authenticating. Alternatively, the directory or database server may be a trusted entity that authenticates itself to the relying party or verifier. When the directory or database server is trusted, unsigned credentials may simply be stored as unsigned data.

#### **5.4. Verifiers**

In any authenticated on-line transaction, the verifier must verify that the claimant has possession and control of the token that verifies his or her identity. A claimant authenticates his or her identity to a verifier by the use of a token and an authentication protocol. This is called *Proof of Possession (PoP)*. Many PoP protocols are designed so that a verifier, with no knowledge of the token before the authentication protocol run, learns nothing about the token from the run. The verifier and CSP may be the same entity, the verifier and relying party may be the same entity or they may all three be separate entities. It is undesirable for verifiers to learn shared secrets unless they are a part of the same entity as the CSP that registered the tokens. Where the verifier and the relying party are separate entities, the verifier must convey the result of the authentication protocol to the relying party. The object created by the verifier to convey this result is called an assertion.

#### **5.5. Assertions**

Assertions can be used to pass information about the claimant or the e-authentication process from the verifier to a relying party. Assertions contain, at a minimum, the name of the claimant, as well as identifying information that permits recovery of registration records. A relying party trusts an assertion based on the source, the time of creation, and attributes associated with the claimant.

Examples of assertions include:

- SAML assertions, specified using a mark up language intended for describing security assertions, can be used by a verifier to make a statement to a relying party about the identity of a claimant. SAML assertions may optionally be digitally signed.
- Cookies, character strings placed in a web browser's memory, are available to websites within the same Internet domain as the server that placed them in the web browser. Cookies are used for many purposes and may be assertions or may contain pointers to assertions.<sup>1</sup>

Assertions may be stored as directory or database objects. Where assertions are digitally signed objects (e.g., signed SAML assertions), their integrity may be verified.

---

<sup>1</sup> There are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.

Alternatively, the directory or database server may be a trusted, authenticated entity. When the server is trusted, unsigned assertions may be accepted based on the source.

### ***5.6. Relying Parties***

A relying party relies on results of an on-line authentication to establish the identity or attribute of a subscriber for the purpose of some transaction. The verifier and the relying party may be the same entity, or they may be separate entities. If they are separate entities, the relying party normally receives an assertion from the verifier. The relying party ensures that the assertion came from a verifier trusted by the relying party. The relying party also processes any additional information in the assertion, such as personal attributes or expiration times.

## 6. Tokens

This guidance recognizes four kinds of claimant tokens for e-authentication. Each type of token incorporates one or more of the authentication factors (something you know, something you have, and something you are.) Tokens that provide a higher level of assurance incorporate two or more factors. The four kinds of tokens are:

- *Hard token* – a hardware device that contains a protected cryptographic key. Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall:
  - require the entry of a password or a biometric to activate the authentication key;
  - not be able to export authentication keys;
  - be FIPS 140-2 validated:
    - overall validation at Level 2 or higher,
    - physical security at Level 3 or higher.
- *Soft token* – a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token key shall be encrypted under a key derived from some activation data. Typically, this activation data will be a password known only to the user, so a password is required to activate the token. For soft tokens, the cryptographic module shall be validated at FIPS 140-2 Level 1 or higher, and may be either a hardware device or a software module. Each authentication shall require entry of the password or other activation data and the unencrypted copy of the authentication key shall be erased after each authentication.

Some “mobility solutions” also allow keys to be stored on servers and downloaded to subscriber systems as needed. Other mobility solutions employ key components generated from passwords with key components stored on servers for use in split signing schemes. Such solutions may provide satisfactory soft tokens, provided that a subscriber password or other activation data is required to download and activate the key, that the protocol for downloading the keys block eavesdroppers and man-in-the-middle attacks, and the authentication process produces Approved digital signatures or message authentication codes. These mobility solutions usually present what appear to relying parties to be ordinary PKI digital signatures, and may be acceptable under this recommendation provided they meet the PKI cross certification requirements. This cross certification will require a detailed analysis of the implementation of the specific mobility scheme.

- *One-time password device token* - a personal hardware device that generates “one time” passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by

using an Approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a nonce to generate a one-time password. The nonce may be a date and time, a counter generated on the device, or a challenge from the verifier (if the device has an entry capability). The one-time password typically is displayed on the device and manually input to the verifier as a password (direct electronic input from the device to a computer is also allowed). The one-time password must have a limited lifetime, on the order of minutes, although the shorter the better.

- *Password token* – a secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings, however some systems use a number of images that the subscriber memorizes and must identify when presented along with other similar images.

### **6.1. Token Threats**

If an attacker can gain control of a token, they will be able to masquerade as the token's owner. Threats to tokens can be categorized into attacks on the three factors:

- *Something you have* may be stolen from the owner or cloned by the attacker. For example, an attacker who gains access to the owner's computer might copy a software token. A hardware token might be stolen or duplicated.
- *Something you know* may be disclosed to an attacker. The attacker might guess a password or PIN. Where the token is a shared secret, the attacker could gain access to the CSP or verifier and obtain the secret value. An attacker may install malicious software (e.g., a keyboard logger) to capture this information. Finally, an attacker may determine the secret through off-line attacks on network traffic from an authentication attempt.
- *Something you are* may be replicated. An attacker may obtain a copy of the token owner's fingerprint and construct a replica.

There are several complementary strategies to mitigate these threats:

- *Multiple factors* raise the threshold for successful attacks. If an attacker needs to steal a cryptographic token *and* guess a password, the work factor may be too high.
- *Physical security mechanisms* may be employed to protect a stolen token from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- *Complex passwords* may reduce the likelihood of a successful guessing attack. By requiring use of long passwords that don't appear in common dictionaries, attackers may be forced to try every possible password.
- *System and Network security controls* may be employed to prevent an attacker from gaining access to a system or installing malicious software.

### **6.2. Token Levels**

Password authentication is easy to implement and familiar to users, so many systems rely only on a password for authentication. In this case impersonation of an identity requires



only that the impersonator obtain the password. Moreover, the ability of humans to remember long, arbitrary passwords is limited, so password tokens are often vulnerable to a variety of attacks including guessing, dictionaries of commonly used passwords, and simple exhaustion of all possibilities. There are a wide variety of password authentication protocols that differ significantly in their vulnerabilities, and many password mechanisms are vulnerable to passive and active network attacks. While some cryptographic password protocols resist nearly all direct network attacks, these techniques are not at present widely used and all password authentication mechanisms are vulnerable to keyboard loggers and observation of the password when it is entered. Experience also shows that users are vulnerable to “social engineering” attacks where they are persuaded to reveal their passwords to unknown parties, who are basically “confidence men.”

Impersonation of an identity using a hard or soft token requires that the impersonator obtain two separate things: either the key (token) and a password, or the token and the ability to enter a biometric into the token. Therefore both hard and soft tokens provide more assurance than passwords by themselves normally provide. Moreover, a hard token is a physical object and its theft is likely to be noticed by its owner, while a soft token can sometimes be copied without the owner being aware. Therefore a hard token offers more assurance than a soft token.

One-time password device tokens are similar to hard tokens. They can be used in conjunction with a password or activated by a password or a biometric to provide multifactor authentication, however one-time password devices do not result in the generation of a shared session authentication key derived from the authentication.

This recommendation requires multifactor authentication for authentication assurance Levels 3 and 4 and assigns tokens to the four levels corresponding to the OMB guidance as follows:

- Password tokens can satisfy the assurance requirements for Levels 1 and 2.
- Soft cryptographic tokens may be used at authentication assurance Levels 1 to 3, but must be combined with a password or biometric to achieve Level 3.
- One-time password devices are considered to satisfy the assurance requirements for Levels 1 through 3, and must be used with a password or biometric to achieve Level 3.
- Hard tokens that are activated by a password or biometric can satisfy assurance requirements for Levels 1 through 4.

The above list is a general summary of the assurance levels for tokens. Specific requirements, however, vary with respect to the details of the authentication protocols. Levels 3 and 4 require two-factor authentication. Typically this means that for Level 3 or 4 a password or biometric is used to activate a key. Alternatively, a password protocol may be used in conjunction with a soft token, hard token, or one-time password token to

achieve two-factor authentication. Detailed level by level token requirements are described in conjunction with protocol requirements in Section 8.

## 7. Registration and Identity Proofing

In the registration process an applicant undergoes identity proofing by a trusted registration authority (RA). If the RA is able to verify the applicant's identity, the CSP registers or gives the applicant a token and issues a credential as needed to bind that token to the identity or some related attribute. The applicant is now a subscriber of the CSP and may use the token as a claimant in an authentication protocol.

The RA may be a part of the CSP, or the RA may be a separate and independent entity; however a trusted relationship always exists between the RA and CSP. Either the RA or CSP must maintain records of the registration. The RA and CSP may provide services on behalf of an organization or may provide services to the public. The processes and mechanisms available to the RA for identity proofing may differ as a result. Where the RA operates on behalf of an organization, the identity proofing process may be able to leverage a pre-existing relationship (e.g., the applicant is employee or student.) Where the RA provides services to the public, the identity proofing process is generally limited to confirming publicly available information and previously issued credentials.

The registration and identity proofing process is designed, to a greater or lesser degree depending on the assurance level, to ensure that the RA/CSP knows the true identity of the applicant. Specifically, the requirements include measures to ensure that:

1. A person with the applicant's claimed attributes exists, and those attributes are sufficient to uniquely identify a single person;
2. The applicant whose token is registered is in fact the person who is entitled to the identity;
3. The applicant cannot later repudiate the registration; therefore, if there is a dispute about a later authentication using the subscriber's token, the subscriber cannot successfully deny he or she registered that token.

An applicant may appear in person to register, or the applicant may register remotely. Somewhat different processes and mechanisms apply to identity proofing in each case. Remote registration is limited to Levels 1 through 3.

### **7.1. Registration Threats**

There are two general categories of threats to the registration process, impersonation and either compromise or malfeasance of the infrastructure (RAs and CSPs). This recommendation concentrates on addressing impersonation threats. Infrastructure threats are addressed by normal computer security controls (e.g., separation of duties, record keeping, independent audits, etc.) and are outside the scope of this document.

#### *7.1.1. Threat Model*

While some impostors may attempt to register as any subscriber in the system and other impostors may wish to register as a specific subscriber, registration threats can be categorized as follows:

- Impersonation of a claimed identity – An applicant claims an incorrect identity, supporting the claim with a specific set of attributes created over time or by presenting false credentials.
- Repudiation of registration – A subscriber denies registration, claiming that he/she did not register that token.

#### ***7.1.2. Resistance to Registration Threats***

Registration fraud can be deterred by making it more difficult to accomplish or increasing the likelihood of detection. This recommendation deals primarily with methods for making impersonation more difficult, however it does prescribe certain methods and procedures that may help to prove who carried out an impersonation. At each level, methods are employed to determine that a person with the claimed identity exists, the applicant is the person who is entitled to that identity and the applicant cannot later repudiate the registration. As the level of assurance increases, the methods employed provide increasing resistance to casual, systematic and insider impersonation.

### **7.2. Registration Levels**

The following sections list the NIST recommendations for registration and identity proofing for the four levels corresponding to the OMB guidance. As noted in the OMB guidance, Levels 1 and 2 recognize the use of anonymous credentials. When anonymous credentials are used to imply membership in a group, the level of proofing should be consistent with the requirements for the identity credential of that level. Explicit requirements for registration processes for anonymous credentials are not specified, as they are unique to the membership criteria for each specific group.

At Level 2 and higher, records of registration shall be maintained either by the RA or by the CSP, depending on the context. Either the RA or the CSP shall maintain a record of each individual whose identity has been verified, and the steps taken to verify his/her identity, including the evidence required in the sections below. The CSP shall be prepared to provide records of identity proofing to relying parties as necessary. The identity proofing and registration process shall be performed according to a written policy or practice statement that specifies the particular steps taken to verify identities.

If the RA and CSP are remotely located, and communicate over a network, the entire registration transaction between RA and CSP shall be cryptographically authenticated using an authentication protocol that meets the requirements for the assurance level of the registration, and any secrets transmitted shall be encrypted using an Approved encryption method.

The CSP shall be able to uniquely identify each subscriber and the associated tokens and the credentials issued to that subscriber. The CSP shall be capable of conveying this information to verifiers and relying parties. At Level 1, the name associated with the subscriber is provided by the applicant and accepted without verification. At Level 2, the

name associated with the subscriber may be pseudonymous but the RA or CSP must know the actual identity of the subscriber. In addition, pseudonymous Level 2 credentials must be distinguishable from Level 2 credentials that contain meaningful names. At Level 3 and above, the name associated with the subscriber must be meaningful. At all levels, personal identifying information collected as part of the registration process must be protected from unauthorized disclosure or modification.

The following subsection, Section 7.2.1, establishes registration and identity proofing requirements specific to each level. Records retention requirements for each level are specified in Section 7.2.2.

#### *7.2.1. Registration and Identity Proofing Requirements*

The following text establishes registration requirements specific to each level. There are no level-specific requirements at Level 1. Both in-person and remote registration are permitted for Levels 2 and 3. Explicit requirements are specified for each scenario in Levels 2 and 3. Only in-person registration is permitted at Level 4.

At Level 2 and higher, the applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other individual identifying information. Detailed level-by-level identity proofing requirements are stated in Table 1 below.

**Table 1. Identity Proofing Requirements by Assurance Level**

	<b>In-Person</b>	<b>Remote</b>
<b>Level 2</b>		
<b>Basis for issuing credentials</b>	Possession of a valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport)	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number (e.g., checking account, savings account, loan or credit card) with confirmation via records of either number.
<b>RA actions</b>	<p>Inspects photo-ID, compare picture to applicant, record ID number, address and DoB. If ID appears valid and photo matches applicant then:</p> <ol style="list-style-type: none"> <li>If ID confirms address of record, authorize or issue credentials and send notice to address of record, or;</li> <li>If ID does not confirm address of record, issue credentials in a manner that confirms address of record.</li> </ol>	<ul style="list-style-type: none"> <li>Inspects both ID number and account number supplied by applicant. Verifies information provided by applicant including ID number or account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.</li> <li>Address confirmation and notification: <ol style="list-style-type: none"> <li>Sends notice to an address of record confirmed in the records check or;</li> <li>Issues credentials in a manner that confirms the address of record supplied by the applicant; or</li> <li>Issues credentials in a manner that confirms the ability of the applicant to receive telephone communications or e-mail at number or e-mail address associated with the applicant in records.</li> </ol> </li> </ul>
<b>Level 3</b>		
<b>Basis for issuing credentials</b>	Possession of verified current primary Government Picture ID that contains applicant's picture and either address of	Possession of a valid Government ID (e.g. a driver's license or passport) number and a financial account number

	<b>In-Person</b>	<b>Remote</b>
	record or nationality (e.g. driver's license or passport)	(e.g., checking account, savings account, loan or credit card) with confirmation via records of both numbers.
<b>RA actions</b>	<p>Inspects Photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compare picture to applicant, record ID number, address and DoB. If ID is valid and photo matches applicant then:</p> <ol style="list-style-type: none"> <li>If ID confirms address of record, authorize or issue credentials and send notice to address of record, or;</li> <li>If ID does not confirm address of record, issue credentials in a manner that confirms address of record</li> </ol>	<ul style="list-style-type: none"> <li>Verifies information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual.</li> <li>Address confirmation: <ol style="list-style-type: none"> <li>Issue credentials in a manner that confirms the address of record supplied by the applicant; or</li> <li>Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.</li> </ol> </li> </ul>
<b>Level 4</b>		
<b>Basis for issuing credentials</b>	In-person appearance and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a new recording of a biometric of the applicant at the time of application	Not Applicable
<b>RA actions</b>	<ul style="list-style-type: none"> <li><i>Primary Photo ID:</i> Inspects Photo-ID and verify via the issuing government agency,</li> </ul>	Not applicable

	<b>In-Person</b>	<b>Remote</b>
	<p>compare picture to applicant, record ID number, address and DoB.</p> <ul style="list-style-type: none"> <li>• <i>Secondary Government ID or financial account</i> <ol style="list-style-type: none"> <li>a) Inspects Photo-ID and if apparently valid, compare picture to applicant, record ID number, address and DoB, or;</li> <li>b) Verifies financial account number supplied by applicant through record checks or through credit bureaus or similar databases, and confirms that: name, DoB, address other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.</li> </ol> </li> <li>• <i>Record Current Biometric</i> Record a current biometric (e.g. photograph or fingerprints to ensure that applicant cannot repudiate application.</li> <li>• <i>Confirm Address</i> Issue credentials in a manner that confirms address of record.</li> </ul>	

At Level 2, employers and educational instructors who verify the identity of their employees or students by means comparable to those stated above for Level 2 may elect to become an RA or CSP and issue credentials to employees or students, either in-person by inspection of a corporate or school issued picture ID, or through on-line processes, where notification is via the distribution channels normally used for sensitive, personal communications.

At Level 2, financial institutions subject to the supervision of the Department of Treasury's Office of Comptroller of the Currency may issue credentials to their customers via the mechanisms normally used for on-line banking credentials and may use on-line banking credentials and tokens as Level 2 credentials provided they meet the provisions of Section 8.

In some contexts, agencies may choose to use additional knowledge-based authentication methods to increase their confidence in the registration process. For example, an applicant could be asked to supply non-public information on his or her past dealing with the agency that could help confirm the applicant's identity.



### ***7.2.2. Records Retention Requirements***

A record of the facts of registration (including revocation) shall be maintained by the CSP or its representative. The minimum record retention period for registration data for Level 2 credentials is seven years and six months beyond the expiration or revocation (whichever is later) of the credential. CSPs operated by or on behalf of executive branch agencies must also follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities. A minimum record retention period for registration data is:

- For Levels 2, and 3, seven years and six months beyond the expiration, and
- For Level 4, ten years and six months beyond the expiration.

### ***7.3. Mapping FPKI Certificate Policies to Registration Levels***

The identity proofing and certificate issuance processes specified in the Federal PKI Certificate Policies [FCBA1, FBCA2, FBCA3] may be mapped to the Registration levels specified in the preceding section. These mappings are as follows:

- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Citizen and Commerce Class policies [FBCA2] are deemed to meet the identity proofing provisions of Level 2.
- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Basic Certificate Policy [FBCA1] are deemed to meet the identity proofing provisions of Levels 2 and 3.
- The identity proofing and certificate issuance processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Medium, Medium-HW, or High Assurance Certificate policies in [FBCA1] or Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies in [FBCA3] are deemed to meet the identity proofing provisions of Levels 2, 3, and 4.

However, agencies are not limited to relying upon only those certificates by CAs cross-certified with the Federal Bridge CA at Levels 1 and 2. At these levels, agencies may choose to rely on any CA that has been determined to meet the identity proofing and registration requirements stated in the General Requirements, Section 7.2.1. At Levels 3 and 4, PKI credentials must be issued by a CA cross-certified<sup>2</sup> with the Federal Bridge CA under one of the certificate policies identified above, or a policy mapped to one of those policies.

---

<sup>2</sup> Note that bi-directional cross-certification is not required; it is sufficient that a valid certificate path exist from the Bridge CA to the issuing CA. The reverse certificate path need not exist.

## 8. Authentication Protocols

An authentication protocol is a defined sequence of messages between a claimant and a verifier that enables the verifier to verify that the claimant has control of a valid token to establish his/her identity. An exchange of messages between a claimant and a verifier that results in the authentication (or authentication failure) of the claimant is a protocol run.

### **8.1. Authentication Threats**

Threats can be divided into those threats that involve attacks against the actual authentication protocol itself, and other attacks that may reveal either token values, or compromise confidential information. In general, attacks that reveal the token value are worse than attacks that simply compromise some information, because the attacker can then use the token to assume a subscriber's identity.

#### *8.1.1. Authentication Protocol Threats*

Registration Authorities, CSPs, verifiers and relying parties are ordinarily trustworthy (in the sense of correctly implemented and not deliberately malicious). However, claimants or their systems may not be trustworthy (or else their identity claims could simply be trusted). Moreover, while RAs, CSPs and verifiers are normally trustworthy, they are not invulnerable, or could become corrupted. Therefore, protocols that expose long-term authentication secrets more than is absolutely required, even to trusted entities, should be avoided.

Protocol threats include:

- Eavesdroppers observing authentication protocol runs for later analysis. In some cases the eavesdropper may intercept messages between a CSP and a verifier, or other parties rather than between the claimant and the verifier. Eavesdroppers generally attempt to obtain tokens to pose as claimants;
- Impostors:
  - impostor claimants posing as subscribers to verifiers to test guessed tokens or obtain other information about a specific subscriber;
  - impostor verifiers posing as verifiers to legitimate subscriber claimants to obtain tokens that can then be used to impersonate subscribers to legitimate verifiers;
  - impostor relying parties posing as the Federal IT system to verifiers to obtain sensitive user information;
- Hijackers who take over an already authenticated session to then:
  - pose as subscribers to relying parties to learn sensitive information or input invalid information;
  - pose as relying parties to verifiers to learn sensitive information or output invalid information.

Eavesdroppers are assumed to be physically able to intercept authentication protocol runs; however, the protocol may be designed to render the intercepted messages

unintelligible, or to resist analysis that would allow the eavesdropper to obtain information useful to impersonate the claimant. Subscriber impostors need only normal communications access to verifiers or relying parties. Impostor verifiers may have special network capabilities to divert, insert or delete packets, but, in many cases, such attacks can be mounted simply by tricking subscribers with incorrect links in e-mails or on web pages, or by using domain names similar to those of relying parties or verifiers, and therefore the impostors need not necessarily have any unusual network capabilities. Because of their ubiquitous use, and the way they are implemented, users of web browser clients are particularly vulnerable to impostor verifiers in password protocols. Hijackers must be able to divert communications sessions, but this capability may be comparatively easy to achieve today when many subscribers use wireless network access.

Specific attack mechanisms on authentication protocols include:

- Eavesdroppers who listen passively to the authentication protocol exchange, and then attempt to learn secrets, such as passwords or keys.
- Active on-line attacks against authentication mechanisms including:
  - In-band attacks where the attacker assumes the role of a claimant with a genuine verifier. These include:
    - Password guessing attacks, where an impostor attempts to guess a password in repeated logon trials and succeeds when he/she is able to log onto a system. A targeted guessing attack is an attack against the password of a selected user whose name is known.
    - Replay attacks, where an attacker records and replays some part of a previous good protocol run to the verifier.
  - Out-of-band attacks where the attacker alters the authentication channel in some way such as:
    - Hijacking sessions after authentication is complete;
    - Verifier impersonation attacks where the attacker impersonates the verifier and induces the claimant to reveal his secret token. Because of the functional complexity of web browsers, the complexity of their user interfaces, and the control they give servers over what users see, users of web browsers are likely to be vulnerable to password verifier impersonation attacks, even when using or “apparently using” secure protocols (e.g. TLS) that authenticate verifiers;
    - Man-in-the middle attacks where the attacker inserts himself in the path of an authentication exchange, to obtain secret tokens. Because of the functional complexity of web browsers, the complexity of their user interfaces, and the control they give servers over what users see, users of web browsers are likely to be vulnerable to man-in-the-middle attacks on passwords, even when using or “apparently using” secure protocols (e.g. TLS) that are intended to block such attacks;

### *8.1.2. Resistance to Protocol Threats*

This section defines the meaning of resistance to specific protocol threats.

- *Eavesdropping resistance*: An authentication protocol is resistant to eavesdropping attacks if an eavesdropper who records all the messages passing between a claimant and a verifier or relying party finds that it is impractical to learn the private key, secret key or password or to otherwise obtain information that would allow the eavesdropper to impersonate the claimant. Eavesdropping resistant protocols make it impractical<sup>3</sup> for an attacker to carry out an off-line attack where he/she records an authentication protocol run then analyses it on his/her own system for an extended period, for example by systematically attempting to try every password in a large dictionary, or by brute force exhaustion.
- *Password guessing resistance*: An authentication protocol is resistant to password guessing attacks if it is impractical for the attacker, with no *a priori* knowledge of the password, to find the password by repeated authentication attempts with guessed passwords. Both the entropy of the password and the protocol itself contribute to this property. Password authentication systems can make targeted password guessing impractical by requiring use of high-entropy passwords (see [Appendix A](#)) and limiting the number of unsuccessful authentication attempts, or by controlling the rate at which attempts can be carried out. To resist untargeted password attacks, a verifier may supplement these controls with network security controls.
- *Replay resistance*: An authentication protocol resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message.
- *Hijacking resistance*: A property of both the authentication protocol and the subsequent session protocol used to transfer data. An authentication and transfer protocol in combination is resistant to hijacking if the authentication is bound to the transfer in a manner that prevents an adversary capable of inserting, deleting, or rerouting messages from altering the contents of any information sent between the claimant and the relying party without being detected. This is usually accomplished by generating a per-session shared secret during the authentication process that is subsequently used by the claimant and the relying party to authenticate the transfer of all sensitive information.
- *Verifier impersonation resistance*: In a verifier impersonation attack, the attacker poses as a legitimate verifier. It may be comparatively easy to impersonate a verifier by “name spoofing,” or some more advanced network attack may be required (wireless LAN access today makes these “advanced” network attacks relatively easy for attackers in many circumstances). An authentication protocol is resistant to verifier impersonation if the impersonator does not learn the value of any token when acting as the verifier. However, even secure protocols can sometimes be bypassed by fooling the claimant into using another protocol or

---

<sup>3</sup> “Impractical” is used here in the cryptographic sense of nearly impossible, that is there is always a small chance of success, but even the attacker with vast resources will nearly always fail. For off-line attacks, impractical means that the amount of work required to “break” the protocol is at least on the order of  $2^{80}$  cryptographic operations. For on-line attacks impractical means that the number of possible on-line trials is very small compared to the number of possible key or password values.

overriding security controls (for example by accepting unverified server certificates).

- *Man-in-the-middle resistance*: In a man-in-the-middle attack on an authentication protocol, the attacker interposes himself between the claimant and verifier, posing as the verifier to the claimant, and as the claimant to the verifier. The attacker thereby learns the value of the authentication token. Authentication protocols are resistant to a man-in-the-middle attack when both parties (e.g., claimant and verifier) are authenticated to the other in a manner that prevents the undetected participation of a third party. However, even secure protocols can sometimes be bypassed by fooling the claimant into using another protocol or overriding security controls (for example by accepting unverified server certificates).

### 8.1.3. Other Threats

Attacks are not limited to the authentication protocol itself. Other attacks include:

- Malicious code attacks that may compromise authentication tokens;
- Intrusion attacks that obtain credentials or tokens by penetrating the subscriber/claimant, CSP or verifier system;
- Insider threats that may compromise authentication tokens;
- Out-of-band attacks that obtain tokens in some other manner, such as social engineering to get a subscriber to reveal his password to the attacker, or “shoulder-surfing;”
- Attacks that fool claimants into using an insecure protocol, when they think that they are using a secure protocol, or trick them into overriding security controls (for example, by accepting server certificates that cannot be validated);
- Intentional repudiation by subscribers who deliberately compromise their tokens.

Malicious code could be introduced into the claimant’s computer system for the purpose of compromising the claimant’s authentication token. The malicious code may be introduced by many means, including the threats detailed below. There are many countermeasures (e.g. virus checkers and firewalls) that can mitigate the risk of malicious code on claimant systems. General good practice to mitigate malicious code threats is outside the scope of this document. Hardware tokens prevent malicious software from extracting and copying the authentication secret token from the token. However, malicious code may still misuse the token, particularly if activation data is presented to the token via the computer. Similarly, the cryptographic tokens at least make it difficult to trick a user into verbally giving away his authentication secret, making social engineering more difficult, while many kinds of passwords are readily expressed over the telephone.

Insider threats are a major concern in many IT systems; however, good security, personnel, and auditing practices may mitigate these risks. General good practice to mitigate insider threats is outside the scope of this document.

From a protocol perspective, shared secrets must be closely held and carefully protected by CSPs. In general, at assurance Levels 2, 3 and 4 independent verifiers must not be

given long-term shared secrets by CSPs, as this increases exposure to insider attacks. Independent verifiers may be given one time challenge-response information, provided that the shared secret is a cryptographic key<sup>4</sup>. If the shared secret is a password, challenge-response mechanisms are vulnerable to insider or penetration attacks.

Network intrusion attacks are similar in many ways to insider threats, and are a risk for all on-line IT systems. Much information is available on the use of preventive measures such as firewalls, system configuration, and intrusion detection to mitigate the risks of network intrusion attacks (see sections 10.2 and 10.3 for some helpful references). Note that subscriber/claimant systems are also subject to network intrusion attacks, but appropriate authentication mechanisms are one defense against such attacks.

The most serious consequence of a network intrusion attack is that it might allow an attacker to gain possession or control of tokens used in authentication protocols. A general treatment of methods for mitigating intrusion attacks is outside the scope of this document. However, as with insider threats, some elements of the design of an authentication service can increase or mitigate penetration risks to the authentication service itself. Hardware tokens and cryptographic modules provide protection for keys and passwords against penetration attacks, due to the constrained environment that holds the keys. Other authentication mechanisms may be vulnerable to an attacker who has access to or can penetrate the claimant's system. However, shared secret mechanisms are potentially subject to penetration attacks against the verifier or CSP as well, where the attacker may find files of many shared secrets. Public key mechanisms are usually less vulnerable to attacks against verifiers or CSPs. Encryption of files containing long-term shared secrets reduces the risks of a successful penetration attack.

Subscribers may intentionally compromise tokens to repudiate authentication. A full discussion of repudiation is outside the scope of this document; typically, however, safeguarding the authentication protocol against other threats will also help to restrict repudiation. A variety of measures will reduce the risk of repudiation, including periodic confirmations that a user has complied with security requirements, confirmations of transactions through a separate channel (such as electronic mail), and reminders to users that delegation of tokens is prohibited. Additional discussion appears in DOJ 2000.

## ***8.2. Authentication Mechanism Requirements***

This section covers the mechanical authentication process of a claimant who already has registered a token. Identity proofing and registration are dealt with separately in Section 7. The authentication process shall provide sufficient information to the relying party to

---

<sup>4</sup> Cell phone systems commonly employ such shared secret challenge-response authentication mechanisms. A shared secret key is maintained on the cell phone and at the home service provider's "home location register." When a user roams and registers with a base station of another host provider, the home service provider generates a challenge and a reply and sends it to the host service provider to be used to authenticate the roaming user. If the shared secret keys have sufficient entropy, insider offline attacks at the host service provider are impractical.

uniquely identify the registration information provided by the subscriber and verified by the RA in the issuance of the credential.

Four assurance levels are defined, numbered 1 to 4. Level 4 provides the highest level of authentication assurance, while Level 1 provides the least assurance. The technical requirements for authentication mechanisms (tokens, protocols and security protections) are stated in this section.

#### *8.2.1. Level 1*

Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and permits the use of any token methods of Levels 2, 3 or 4. Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token.

Plaintext passwords or secrets shall not be transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline analysis by eavesdroppers. For example, password challenge-response protocols that combine a password with a challenge to generate an authentication reply satisfy this requirement although an eavesdropper who intercepts the challenge and reply may be able to conduct a successful off-line dictionary or password exhaustion attack and recover the password. Common protocols that meet Level 1 requirements include APOP [RFC 1939], S/KEY [SKEY], and Kerberos [KERB]. Since an eavesdropper who intercepts such a protocol exchange will often be able to find the password with a straightforward dictionary attack, and this vulnerability is independent of the strength of the operations, there is no requirement at this level to use Approved cryptographic techniques.

At Level 1, long-term shared authentication secrets may be revealed to verifiers.

##### *8.2.1.1. Credential Lifetime, Status or Revocation*

There are no stipulations about the revocation or lifetime of credentials at Level 1.

##### *8.2.1.2. Assertions*

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or
- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

##### *8.2.1.3. Protection of Long-Term Shared Secrets*

Files of shared secrets used by verifiers at Level 1 authentication shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords; typically they contain a one-way hash or “inversion” of the password. In

addition, any method allowed for the protection of long-term shared secrets at Levels 2, 3 or 4 may be used at Level 1.

#### *8.2.1.4.Password Strength*

For password (or PIN) based Level 1 authentication systems, the probability of success of a targeted on-line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed  $2^{-10}$  (1 in 1024), over the life of the password. There are no min-entropy requirements for Level 1. Appendix A contains information about estimating the entropy of passwords.

#### *8.2.1.5.Example Implementations*

A wide variety of technologies should be able to meet the requirements of Level 1. For example, a verifier might obtain a subscriber password from a CSP and authenticate the claimant by use of a challenge-response protocol.

### *8.2.2. Level 2*

Level 2 allows a wide range of available authentication technologies to be employed and permits the use of any of the token methods of Levels 3 or 4, as well as passwords. Successful authentication requires that the claimant shall prove, through a secure authentication protocol, that he/she controls the token. Eavesdropper, replay, and on-line guessing attacks shall be prevented. Approved cryptography is required to prevent eavesdroppers.

#### *8.2.2.1.Credential and Token Lifetime, Status or Revocation*

CSPs shall provide a secure mechanism, such as a digitally signed revocation list or a status responder, to allow verifiers or relying parties to ensure that the credentials are still valid. Verifiers or relying parties shall check to ensure that the credentials they use are valid. Shared secret based authentication systems may simply remove revoked subscribers from the verification database.

CSPs shall revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid or a token is compromised to ensure that a claimant using the token cannot successfully be authenticated. If the CSP issues credentials that expire automatically within 72 hours (e.g. issues fresh certificates with a 24 hour validity period each day) then the CSP is not required to provide an explicit mechanism to revoke the credentials. CSPs that register passwords shall ensure that the revocation or de-registration of the password can be accomplished in no more than 72 hours and that the use of that password in authentication shall fail.

CAs cross-certified with the Federal Bridge CA at the Basic, Medium, High, Citizen and Commerce Class, or Common Certificate Policy levels are considered to meet credential status and revocation provisions of this level.

#### *8.2.2.2.Assertions*

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or



- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

Assertions generated by a verifier shall expire after 12 hours and should not be accepted thereafter by the relying party.

#### *8.2.2.3. Protection of Long-term Shared Secrets*

Long term shared authentication secrets, if used, shall never be revealed to any party except the subscriber and CSP (including verifiers operated as a part of the CSP), however session (temporary) shared secrets may be provided by the CSP to independent verifiers.

Files of shared secrets used by CSPs at Level 2 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall not contain the plaintext passwords or secret; two alternative methods may be used to protect the shared secret:

1. Passwords may be concatenated to a salt and/or username and then hashed with a Approved algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file.
2. Store shared secrets in encrypted form using Approved encryption algorithms and modes and decrypt the needed secret only when immediately required for authentication. In addition any method allowed to protect shared secrets at Level 3 or 4 may be used at Level 2.

#### *8.2.2.4. Password Strength*

For password based Level 2 authentication systems, the probability of success of an on-line password guessing attack by an attacker who has no *a priori* knowledge of the password, but knows the user name of the target, shall not exceed  $2^{-14}$  (1 in 16,384), over the life of the password. Level 2 passwords shall have at least 10 bits of min-entropy.

[Appendix A](#) contains information about estimating the entropy of passwords.

#### *8.2.2.5. Example Implementations*

A wide variety of technologies can meet the requirements of Level 2. For example, a verifier might authenticate a claimant who provides a password through a secure (encrypted) TLS protocol session (tunneling). This prevents eavesdropper attacks, but generally does not adequately block not man-in-the middle attacks or verification impersonation attacks because common web browser clients offer many avenues to fool or trick users. After a successful authentication, the verifier then puts a security assertion for the claimant in a secure server, and sends a “handle” for that assertion to a relying party in an HTTP referral.

### 8.2.3. Level 3

Level 3 authentication is based on proof of possession of a cryptographic key using a cryptographic protocol. Level 3 authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token (a secret key or a private key) against compromise by the following protocol threats defined in section 8.1.1: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. Level 3 also requires two factor authentication; in addition to the key, the user must employ a password or biometric to activate the key.

Three kinds of tokens described below may be used to meet Level 3 requirements:

- *Soft cryptographic token*: a cryptographic key stored on a general-purpose computer. Hardware tokens validated at FIPS 140-2 Level 1 or higher may also be used to hold the key and perform cryptographic operations. The claimant shall be required to activate the key before using it with a password or biometric, or, alternatively shall use a password as well as the key in an authentication protocol with the verifier. If a password is employed to unlock the soft token key, the key shall be kept encrypted under a key derived from a password meeting the requirements for Level 2 authentication, and decrypted only for actual use in authentication. Alternatively, if a password protocol is employed with the verifier, the use of the password shall meet the requirements for Level 2 authentication assurance.
- *Hard token*: a cryptographic key stored on a special hardware device. Tokens must be validated at FIPS 140-2 Level 1 or higher overall. The claimant shall be required to activate the key before using it with a password or biometric, or, alternatively, shall use a password as well as the key in an authentication protocol with the verifier. The authentication mechanism used to authenticate the claimant to unlock token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2. Alternatively, if a password protocol is employed with a verifier, the use of the password shall meet the requirements for Level 1 authentication assurance.
- *One-time password device tokens*: the authentication depends on a symmetric key stored on a personal hardware device that is a cryptographic module validated at FIPS 140-2 Level 1 or higher overall. The device combines a nonce with a cryptographic key to produce an output that is sent to the verifier as a password. The password shall be used only once and is cryptographically generated; therefore it needs no additional eavesdropper protection. The one-time password output by the device shall have at least  $10^6$  possible values. The verifier must be authenticated cryptographically to the claimant, for example using a TLS server. To protect against the use of a stolen token, one of the following measures shall be used:
  - The authentication mechanism used to authenticate the claimant to the token shall be validated as meeting the operator authentication requirements for FIPS 140-2 Level 2.

- The claimant sends the verifier a personal password meeting the requirements for (E-authentication) Level 1 with the one-time password.

Authentication requires that the claimant shall prove through a secure authentication protocol that he or she controls the token. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP, however session (temporary) shared secrets may be provided to verifiers by the CSP. Approved cryptographic techniques shall be used for all operations.

Each of the three token types has somewhat different utility and security properties. Soft token solutions are easily realized in “thin clients” with TLS and client certificates. Moreover this solution allows not only initial authentication of claimants, but also allows the entire session, or as much of it as is security critical, to be cryptographically authenticated by a key created during the authentication process. Hard token solutions provide the additional assurance of a physical token, and users should know if their token has been stolen. Like soft tokens, hard tokens allow not only initial authentication of claimants, but also allows the entire session, or as much of it as is security critical, to be cryptographically authenticated by a key created during the authentication process. One-time password device token systems are commercially available, portable and work easily with any browser client. Like hard tokens, one-time password device tokens have the security advantage that the token is a tangible, physical object. Subscribers should know if their token is stolen, and the key is not vulnerable to network, shoulder-surfing or keyboard sniffer attacks. Unlike soft tokens or hard tokens, a session key is not created from the authentication process to authenticate subsequent data transfers.

All three token types present the eavesdroppers with similar strong cryptographic protection. Each has its advantages and disadvantages against various types of attacks. All three offer considerably greater strength than Level 2 solutions. Application implementers with specific Level 3 authentication requirements, who need to select a particular technology should chose the one that best suits the functional needs and risks of their application.

#### *8.2.3.1. Credential/Token Lifetime, Status or Revocation*

CSPs shall provide a secure mechanism to allow verifiers or relying parties to ensure that the credentials are valid. Such mechanisms may include: revocation lists, on-line validation servers, and the use of credentials with short life-times or the involvement of CSP servers that have access to status records in authentication transactions. Shared secret based authentication systems may simply remove revoked subscribers from the verification database. Verifiers shall check to ensure that the credentials they use are valid.

CSPs shall have a procedure to revoke credentials and tokens within 24 hours. The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the Basic, Medium, High or Common Certificate Policy levels are considered to meet credential status and revocation provisions of this level.

Verifiers shall ensure that the tokens they rely upon are either freshly issued (within 24 hours) or still valid.

#### 8.2.3.2. *Assertions*

Relying parties may accept assertions that are:

- digitally signed by a trusted entity (e.g., the verifier); or
- obtained directly from a trusted entity (e.g. a repository or the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. TLS) that cryptographically authenticates the verifier and protects the assertion;

Assertions generated by a verifier shall expire after 2 hours and should not be accepted thereafter by the relying party.

#### 8.2.3.3. *Protection of Long-term Shared Secrets*

Files of long-term shared secrets used by CSPs or verifiers at Level 3 shall be protected by discretionary access controls that limit access to administrators and only those applications that require access. Such shared secret files shall be encrypted so that:

1. The encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.
2. Shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module.
3. Shared secrets are split by a cryptographic secret sharing method between  $m$  separate verifier systems, so that the cooperation of  $n$  (where  $2 \leq n \leq m$ ) systems in a secure protocol is required to perform the authentication and an attacker who learns  $n-1$  of the secret shares, learns nothing about the secret (except, perhaps, its size).

Temporary session authentication keys may be generated from long-term shared secret keys by CSPs and distributed to third party verifiers, in an appropriate protocol, but long-term shared secrets shall not be shared with any third parties, including third party verifiers. Session authentication keys are typically created by cryptographically combining the long term shared secret with a nonce challenge, to generate a session key. The challenge and session key are securely transmitted to the verifier. The verifier in turn sends only the challenge to the claimant, and the claimant applies the challenge to the long-term shared secret to generate the session key. Both claimant and verifier now share a session key, which can be used for authentication. Such protocols are permitted at this level provided that all keys preserve at least 80-bits of entropy and approved cryptographic algorithms (e.g., AES, SHA-1, SHA256, HMAC) are used for all operations.

#### *8.2.3.4.Example Implementations*

Level 3 assurance can be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key certificates. Other protocols with similar properties can also be used. Level 3 authentication assurance can also be met by tunneling the output of a one-time password device and a Level 1 personal password through a TLS session.

#### *8.2.4. Level 4*

Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant shall prove through a secure authentication protocol that he or she controls the token. The protocol threats defined in section 8.1.1 above (eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks) shall be prevented. In addition, the token shall protect the secret from compromise by the malicious code threat as described in section 8.1.3 above. Long-term shared authentication secrets, if used, shall never be revealed to any party except the claimant and CSP; however session (temporary) shared secrets may be provided to verifiers or relying parties by the CSP. Strong, Approved cryptographic techniques shall be used for all operations. All sensitive data transfers shall be cryptographically authenticated using keys derived in the authentication process.

##### *8.2.4.1.Credential/Token Lifetime, Status or Revocation*

CSPs shall provide a secure mechanism to allow verifiers or relying parties to ensure that the credentials are valid. Such mechanisms may include: revocation lists, on-line validation servers, and the use of credentials with short life-times or the involvement of CSP servers that have access to status records in authentication transactions. Shared secret based authentication systems may simply remove revoked subscribers from the verification database. Verifiers shall check to ensure that the credentials they use are either freshly issued or still valid.

CSPs shall have a procedure to revoke credentials within 24 hours. Verifiers or relying parties shall ensure that the credentials they rely upon are either freshly issued (within 24 hours) or still valid. The certificate status provisions of CAs cross-certified with the Federal Bridge CA at the High and Common Certificate Policies shall be considered to meet credential status provisions of Level 4. [[FBCA1](#)].

At this level sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process. All temporary or short-term keys derived during the original authentication operation shall expire and re-authentication shall be required after not more than 24 hours from the initial authentication.

#### *8.2.4.2. Protection of Long-term Shared Secrets*

Files of long-term shared secrets used by CSPs or verifiers at Level 4 shall be protected in the same manner as long-term shared secrets for Level 3 (specified in section 8.2.3.3 above.)

#### *8.2.4.3. Example Implementations*

Level 4 assurance can be satisfied by client authenticated TLS (implemented in all modern browsers), with claimants who have public key hard tokens. Other protocols with similar properties can also be used.

## **9. Summary of Technical Requirements by level**

This section summarizes the technical requirements for each level in tabular form. Table 2 shows the types of tokens that may be used at each authentication assurance level. Table 3 identifies the protections that are required at each level. Protections are defined in section 8.1.2 above. Table 4 summarizes the requirements for the resistance of passwords to on-line password guessing attacks. Table 5 identifies the types of authentication protocols that are applicable to each assurance level. Table 6 identifies additional required protocol and system properties at each level.

**Table 2. Token Types Allowed at Each Assurance Level**

<i>Token type</i>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

**Table 3. Required Protections**

<i>Protect against</i>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
On-line guessing	√	√	√	√
Replay	√	√	√	√
Eavesdropper		√	√	√
Verifier impersonation			√	√
Man-in-the-middle			√	√
Session hijacking				√

**Table 4. Minimum Online Password Guessing Resistance**

<i>Attack Type</i>	<b>Level 1</b>	<b>Level 2</b>
<i>Targeted Attack:</i> Maximum chance of an attacker guessing the password of a selected user over the life of the password with no <i>a priori</i> knowledge other than the username	one in $2^{10}$ (1/1024)	one in $2^{14}$ (1/16384)
<i>Untargeted Attack:</i> min-entropy	-	10-bits

**Table 5. Authentication Protocol Types**

<b><i>Protocol Type</i></b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Tunneled or Zero knowledge password	√	√		
Challenge-response password	√			

**Table 6. Additional Required Properties**

<b><i>Required Property</i></b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>	<b>Level 4</b>
Shared secrets not revealed to third parties by verifiers or CSPs		√	√	√
Multi-factor authentication			√	√
Sensitive data transfer authenticated				√



### 9.1.1. Relationship of PKI Policies to E-authentication Assurance Levels

Agencies are, in general, issuing certificates under the policies specified in the Common Policy Framework [FBCA3] to satisfy FIPS 201. Table 7 summarizes how certificates issued under these policies correspond to the E-authentication assurance levels. Note that the *Card Authentication* and *Common Device* policies are not listed; these policies support authentication of a system or a cryptographic module rather than a person.

**Table 7. E-authentication Assurance Levels and the Common Policy Framework**

E-auth Level	Selected Policy Components			Overall Equivalence
	Identity Proofing	Token	Status Reporting	
Level 2	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies
Level 3	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies
Level 4	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies	Common-Auth, Common-HW, and Common-High Certificate Policies

Agencies that were early adopters of PKI technology, and organizations outside the Federal government, issue PKI certificates under organization specific policies instead of the Common Policy Framework. The primary mechanism for evaluating the assurance provided by public key certificates issued under organization specific policies is the policy mapping of the Federal Policy Authority to the Federal Bridge CA policies. These policies include the Rudimentary, Basic, Medium, Medium-HW, and High assurance policies specified in [FBCA1] and the Citizen and Commerce class policy specified in [FBCA2]. Table 8 below summarizes how these certificate policies correspond to E-authentication assurance levels. At Level 2 agencies may use certificates issued under policies that have not been mapped by the Federal policy authority, but are

determined to meet the Level 2 identify proofing, token and status reporting requirements.

**Table 8. E-authentication Assurance Levels and PKI Certificate Policy Mappings**

<b>E-auth Level</b>	<b>Selected Policy Components</b>			<b>Overall Equivalence</b>
	<b>Identity Proofing</b>	<b>Token</b>	<b>Status Reporting</b>	
Level 2	Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy or other policies that meet level 2 ID proofing requirements	Rudimentary, Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy, any cert with at least 1024-bit RSA key & SHA1 or equivalent.	Basic, Citizen and Commerce Class, Medium, Medium-HW or High Certificate Policy or certs. issued by other CAs with a 72 hour or smaller CRL or revocation cycle	Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy or other policies that meet all level 2 requirements
Level 3	Basic, Medium, Medium-HW, or High Certificate Policy	Rudimentary, Basic, Citizen and Commerce Class, Medium, Medium-HW, or High Certificate Policy	Basic, Medium, Medium-HW, or High Certificate Policy	Basic, Medium, Medium-HW, or High Certificate Policy
Level 4	Medium, Medium-HW, or High Certificate Policy	Medium-HW or High Certificate Policy	Medium, Medium-HW, or High Certificate Policy	Medium-HW or High Certificate Policy

The Federal PKI has also added two policies, Medium Commercial Best practices (Medium-CBP) and Medium Hardware Commercial Best practices (MediumHW-CBP) to support recognition of non-federal PKIs. In terms of e-Authentication levels, the Medium CBP and MediumHW-CBP are equivalent to Medium and Medium-HW, respectively.

## 10. References

### 10.1. General References

- [DOJ 2000] Guide to Federal Agencies on Implementing Electronic Processes (November 2000), available at: <http://www.usdoj.gov/criminal/cybercrime/ecommerce.html>
- [OCC] Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks. Office of the Comptroller of the Currency, 12 CFR Part 21. May 2003. Available at: <http://www.fdic.gov/regulations/laws/federal/03joint326.pdf>
- [OMB 04-04] OMB Memorandum M-04-04, E-Authentication Guidance for Federal agencies, December 16, 2003, available at: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- [OMB 03-22] OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003 available at: <http://www.whitehouse.gov/omb/memoranda/m03-22.html>.
- [KERB] Neuman, C., and T. Ts'o, Kerberos: An Authentication Service for Computer Networks, IEEE Communications, vol. 32, no.9, 1994.
- [RFC 1939] IETF, RFC 1939, Post Office Protocol - Version 3, May 1996, available at: <http://www.ietf.org/rfc/rfc1939.txt>
- [RFC 2246] IETF, RFC 2246, *The TLS Protocol, Version 1.0*. January 1999, available at: <http://www.ietf.org/rfc/rfc2246.txt>
- [RFC2560] IETF, RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, available at: <http://www.ietf.org/rfc/rfc2560.txt>
- [RFC 3280] IETF, RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, available at: <http://www.ietf.org/rfc/rfc3280.txt>
- [RFC 3546] IETF, RFC 3546, Transport Layer Security (TLS) Extensions, June 2003, available at: <http://www.ietf.org/rfc/rfc3546.txt>
- [SKEY] IETF, RFC 1760, The S/KEY One Time Password System, February 1995, available at: <http://www.ietf.org/rfc/rfc1760.txt>

### 10.2. NIST ITL Bulletins

NIST ITL Bulletins are available at: <http://csrc.nist.gov/publications/nistbul/index.html>. The following bulletins may be of particular interest to those implementing systems of applications requiring e-authentication.

[ITL Dec02] ITL Bulletin, *Security of Public Webservers*, Dec. 2002

- [ITL July02] ITL Bulletin, *Overview: The Government Smartcard Interoperability Specification*, July 2002
- [ITL Jan02] ITL Bulletin, *Guideline on Firewalls and Firewall Policy*, January 2002
- [ITL Feb00] ITL Bulletin, *Guideline for Implementing Cryptography in the Federal Government*, February 2000
- [ITL Dec99] ITL Bulletin, *Operating System Security: Adding to the Arsenal of Security Techniques*, December 1999
- [ITL Nov99] ITL Bulletin, *Acquiring and Deploying Intrusion Detection Systems*, November 1999
- [ITL Sep99] ITL Bulletin, *Securing Web Servers*, September 1999
- [ITL May99] ITL Bulletin, *Computer Attacks: What They Are and How to Defend Against Them*, May 1999

### **10.3. NIST Special Publications**

NIST 800 Series Special Publications are available at:  
<http://csrc.nist.gov/publications/nistpubs/index.html>. The following publications may be of particular interest to those implementing systems of applications requiring e-authentication.

- [SP 800-31] NIST Special Publication, 800-31, *Intrusion Detection Systems (IDS)*, November 2001
- [SP 800-32] NIST Special Publication, 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
- [SP 800-33] NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001
- [SP 800-40] NIST Special Publication 800-40, *Procedures for Handling Security Patches*, September 2002
- [SP 800-41] NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002
- [SP 800-42] NIST Special Publication 800-42, *Guideline on Network Security Testing*, draft
- [SP 800-43] NIST Special Publication 800-43, *Guide to Securing Windows 2000 Professional*, November 2002
- [SP 800-44] NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002
- [SP 800-47] NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002

- [SP 800- 52] NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security Implementations, draft.

#### **10.4. Federal Information Processing Standards**

FIPS can be found at: <http://csrc.nist.gov/publications/fips/>

- [FIPS 46-3] Federal Information Processing Standard Publication 46-3, *Data Encryption Standard (DES)*, NIST, October 25, 1999
- [FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001
- [FIPS 180-2] Federal Information Processing Standard Publication 180-2, *Secure Hash Standard (SHS)*, NIST, August 2002.
- [FIPS186-2] Federal Information Processing Standard Publication 186-2, *Digital Signature Standard (DSS)*, NIST, June 2000.
- [FIPS 197] Federal Information Processing Standard Publication 197, *Advanced Encryption Standard (AES)*, NIST, November 2001.
- [FIPS 198] Federal Information Processing Standard Publication 198, *Keyed-Hash Message Authentication Code (HMAC)*, NIST, March 2002.

#### **10.5. Certificate Policies**

These certificate policies can be found at: <http://www.cio.gov/fpkipa/policies.htm>.

- [FBCA1] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.1 January 12, 2006. Available at [http://www.cio.gov/fpkipa/documents/FBCA\\_CP\\_RFC3647.pdf](http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf)
- [FBCA2] *Citizen & Commerce Certificate Policy*, Version 1.0 December 3, 2002. Available at [http://www.cio.gov/fpkipa/documents/citizen\\_commerce\\_cp1.pdf](http://www.cio.gov/fpkipa/documents/citizen_commerce_cp1.pdf)
- [FBCA3] *X.509 Certificate Policy for the Common Policy Framework*, Version 2.4 February 15, 2006. Available at <http://www.cio.gov/fpkipa/documents/CommonPolicy.pdf>

## Appendix A: Estimating Password Entropy and Strength

Claude Shannon coined the use of the term “entropy”<sup>5</sup> in information theory. The concept has many applications to information theory and communications and Shannon also applied it to express the amount of actual information in English text. Shannon says, “The entropy is a statistical parameter which measures in a certain sense, how much information is produced on the average for each letter of a text in the language. If the language is translated into binary digits (0 or 1) in the most efficient way, the entropy  $H$  is the average number of binary digits required per letter of the original language.”<sup>6</sup>

Entropy in this sense is at most only loosely related to the use of the term in thermodynamics. A mathematical definition of entropy in terms of the probability distribution function is:

$$H(X) := - \sum_x P(X=x) \log_2 P(X=x)$$

where  $P(X=x)$  is the probability that the variable  $X$  has the value  $x$ .

Shannon was interested in strings of ordinary English text and how many bits it would take to code them in the most efficient way possible. Since Shannon coined the term, “entropy” has been used in cryptography as a measure of the difficulty in guessing or determining a password or a key. Clearly the strongest key or password of a particular size is a truly random selection, and clearly, on average such a selection cannot be compressed. However it is far from clear that compression is the best measure for the strength of keys and passwords, and cryptographers have derived a number of alternative forms or definitions of entropy, including “guessing entropy” and “min-entropy.” As applied to a distribution of passwords the guessing entropy is, roughly speaking, an estimate of the average amount of work required to guess the password of a selected user, and the min-entropy is a measure of the difficulty of guessing the easiest single password to guess in the population.

If we had a good knowledge of the frequency distribution of passwords chosen under a particular set of rules, then it would be straightforward to determine either the guessing entropy or the min-entropy of any password. An attacker who knew the password distribution would find the password of a chosen user by first trying the most probable password for that chosen username, then the second most probable password for that username and so on in decreasing order of probability until the attacker found the password that worked with the chosen username. The average for all passwords would be the guessing entropy. The attacker who is content to find the password of any user would follow a somewhat different strategy, he would try the most probable password with every username, then the second most probable password with every username, until he found the first “hit.” This corresponds to the min-entropy.

---

<sup>5</sup> C. E. Shannon, “A mathematical Theory of Communication,” *Bell System Technical Journal*, v. 27, pp. 379-423, 623-656, July, October 1948, see <http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html>

<sup>6</sup> C. E. Shannon, “Prediction and Entropy of Printed English”, *Bell System Technical Journal*, v.30, n. 1, 1951, pp. 50-64.

Unfortunately, we do not have much data on the passwords users choose under particular rules, and much of what we do know is found empirically by “cracking” passwords, that is by system administrators applying massive dictionary attacks to the files of hashed passwords (in most systems no plaintext copy of the password is kept) on their systems. NIST would like to obtain more data on the passwords users actually choose, but, where they have the data, system administrators are understandably reluctant to reveal password data to others. Empirical and anecdotal data suggest that many users choose very easily guessed passwords, where the system will allow them to do so.

### **A.1 Randomly Selected Passwords**

As we use the term here, “entropy” denotes the uncertainty in the value of a password. Entropy of passwords is conventionally expressed in bits. If a password of  $k$  bits is chosen at random there are  $2^k$  possible values and the password is said to have  $k$  bits of entropy. If a password of length  $l$  characters is chosen at random from an alphabet of  $b$  characters (for example the 94 printable ISO characters on a typical keyboard) then the entropy of the password is  $b^l$  (for example if a password composed of 8 characters from the alphabet of 94 printable ISO characters the entropy is  $94^8 \approx 6.09 \times 10^{15}$  – this is about  $2^{52}$ , so such a password is said to have about 52 bits of entropy). For randomly chosen passwords, guessing entropy, min-entropy, and Shannon entropy are all the same value. The general formula for entropy,  $H$  is given by:

$$H = \log_2 (b^l)$$

Table A.1 gives the entropy versus length for a randomly generated password chosen from the standard 94 keyboard characters (not including the space). Calculation of randomly selected passwords from other alphabets is straightforward.

### **A.2 User Selected Passwords**

It is much more difficult to estimate the entropy in passwords that users choose for themselves, because they are not chosen at random and they will not have a uniform random distribution. Passwords chosen by users probably roughly reflect the patterns and character frequency distributions of ordinary English text, and are chosen by users so that they can remember them. Experience teaches us that many users, left to choose their own passwords will choose passwords that are easily guessed, and even fairly short dictionaries of a few thousand commonly chosen passwords, when they are compared to actual user chosen passwords, succeed in “cracking” a large share of those passwords.

#### **A.2.1 Guessing Entropy Estimate**

Guessing entropy is arguably the most critical measure of the strength of a password system, since it largely determines the resistance to targeted, in band password guessing attacks.

In this guidance, we have chosen to use Shannon's estimate of the entropy in ordinary English text as the starting point to estimate the entropy of user-selected passwords. It is a big assumption that passwords are quite similar to other English text, and it would be better if we had a large body of actual user selected passwords, selected under different composition rules, to work from, but we have no such resource, and it is at least plausible to use Shannon's work for a "ballpark" estimate. Readers are cautioned against interpreting the following rules as anything more than a very rough rule of thumb method to be used for the purposes of E-authentication.

Shannon conducted experiments where he gave people strings of English text and asked them to guess the next character in the string. From this he estimated the entropy of each successive character. He used a 27-character alphabet, the ordinary English lower case letters plus the space.

In the following discussion we assume that passwords are user selected from the normal keyboard alphabet of 94 printable characters, and are at least 6-characters long. Since Shannon used a 27 character alphabet it may seem that the entropy of user selected passwords would be much larger, however the assumption here is that users will choose passwords that are almost entirely lower case letters, unless forced to do otherwise, and that rules that force them to include capital letters or non-alphabetic characters will generally be satisfied in the simplest and most predictable manner, often by putting a capital letter at the start (as we do in ordinary English) and punctuation or special characters at the end, or by some simple substitution, such as \$ for the letter "s." Moreover rules that force passwords to appear to be highly random will be counterproductive because they will make the passwords hard to remember. Users will then write the passwords down and keep them in a convenient (that is insecure) place, such as pasted on their monitor. Therefore it is reasonable to start from estimates of the entropy of simple English text, assuming only a 27-symbol alphabet.

Shannon observed that, although there is a non-uniform probability distribution of letters, it is comparatively hard to predict the first letter of an English text string, but, given the first letter, it is much easier to guess the second and given the first two the third is easier still, and so on. He estimated the entropy of the first symbol at 4.6 to 4.7 bits, declining to on the order of about 1.5 bits after 8 characters. Very long English strings (for example the collected works of Shakespeare) have been estimated to have as little as .4 bits of entropy per character.<sup>7</sup> Similarly, in a string of words, it is harder to predict the first letter of a word than the following letters, and the first letter carries about 6 times more information than the 5<sup>th</sup> or later letters<sup>8</sup>.

An attacker attempting to find a password will try the most likely chosen passwords first. Very extensive dictionaries of passwords have been created for this purpose. Because users often choose common words or very simple passwords systems commonly impose rules on password selection in an attempt to prevent the choice of "bad" passwords and

---

<sup>7</sup> Thomas Schurmann and Peter Grassberger, "Entropy estimation of symbol sequences," <http://arxiv.org/ftp/cond-mat/papers/0203/0203436.pdf>

<sup>8</sup> *ibid.*



improve the resistance of user chosen passwords to such dictionary or rule driven password guessing attacks. For the purposes of this guidance we break those rules into two categories:

1. dictionary tests that test prospective passwords against an “extensive dictionary test” of common words and commonly used passwords, then disallow passwords found in the dictionary. We do not precisely define a dictionary test, since it must be tailored to the password length and rules, but it should prevent selection of passwords that are simple transformations of any one word found in an unabridged English dictionary, and should include at least 50,000 words. There is no intention to prevent selection of long passwords (16 characters or more based on phrases) and no need to impose a dictionary test on such long passwords of 16 characters or more.
2. composition rules that typically require users to select passwords that include lower case letters, upper case letters, and non-alphabetic symbols (e.g.:: “~!@#\$%^&\*()\_-=+{ }[]\|;’,<,>./1234567890”).

Either dictionary tests or composition rules eliminate some passwords and reduce the space that an adversary must test to find a password in a guessing or exhaustion attack. However they can eliminate many obvious choices and therefore we believe that they generally improve the “practical entropy” of passwords, although they reduce the work required for a truly exhaustive attack. The dictionary check requires a dictionary of at least 50,000 legal passwords chosen to exclude commonly selected passwords. Upper case letters in candidate passwords converted to lower case before comparison.

Table A.1 provides a rough estimate of the average entropy of user chosen passwords as a function of password length. Estimates are given for user selected passwords drawn from the normal keyboard alphabet that are not subject to further rules, passwords subject to a dictionary check to prevent the use of common words or commonly chosen passwords and passwords subject to both composition rules and a dictionary test. In addition an estimate is provided for passwords or PINs with a ten-digit alphabet. The table also shows the calculated entropy of randomly selected passwords and PINs. The values of Table A.1 should not be taken as accurate estimates of absolute entropy, but they do provide a rough relative estimate of the likely entropy of user chosen passwords, and some basis for setting a standard for password strength.

The logic of the Table A.1 is as follows for user-selected passwords drawn from the full keyboard alphabet:

- the entropy of the first character is taken to be 4 bits;
- the entropy of the next 7 characters are 2 bits per character; this is roughly consistent with Shannon’s estimate that “when statistical effects extending over not more than 8 letters are considered the entropy is roughly 2.3 bits per character;”
- for the 9<sup>th</sup> through the 20<sup>th</sup> character the entropy is taken to be 1.5 bits per character;

- for characters 21 and above the entropy is taken to be 1 bit per character;
- A “bonus” of 6 bits of entropy is assigned for a composition rule that requires both upper case and non-alphabetic characters. This forces the use of these characters, but in many cases these characters will occur only at the beginning or the end of the password, and it reduces the total search space somewhat, so the benefit is probably modest and nearly independent of the length of the password;
- A bonus of up to 6 bits of entropy is added for an extensive dictionary check. If the attacker knows the dictionary, he can avoid testing those passwords, and will in any event, be able to guess much of the dictionary, which will, however, be the most likely selected passwords in the absence of a dictionary rule. The assumption is that most of the guessing entropy benefits for a dictionary test accrue to relatively short passwords, because any long password that can be remembered must necessarily be a “pass-phrase” composed of dictionary words, so the bonus declines to zero at 20 characters.

For user selected PINs the assumption of Table A.1 is that such pins are subjected to at least a rule that prevents selection of all the same digit, or runs of digits (e.g., “1234” or “76543”). This column of Table A.1 is at best a very crude estimate, and experience with password crackers suggests, for example, that users will often preferentially select simple number patterns and recent dates, for example their year of birth.

### **A.2.2 Min Entropy Estimates**

Experience suggests that a significant share of users will choose passwords that are very easily guessed (“password” may be the most commonly selected password, where it is allowed). Suppose, for example, that one user in 1,000 chooses one of the 2 most common passwords, in a system that allows a user 3 tries before locking a password. An attacker with a list of user names, who knows the two most commonly chosen passwords can use an automated attack to try those 2 passwords with each user name, and can expect to find at least one password about half the time by trying 700 usernames with those two passwords. Clearly this is a practical attack if the only goal is to get access to the system, rather than to impersonate a single selected user. This is usually too dangerous a possibility to ignore.

We know of no accurate general way to estimate the actual min-entropy of user chosen passwords, without examining in detail the passwords that users actually select under the rules of the password system, however it is reasonable to argue that testing user chosen passwords against a sizable dictionary of otherwise commonly chosen legal passwords, and disallowing matches, will raise the min entropy of a password. A dictionary test is specified here that is intended to ensure at least 10-bits of min entropy. That test is:

- Upper case letters in passwords are converted to entirely lower case and compared to a dictionary of at least 50,000 commonly selected otherwise legal passwords and rejected if they match any dictionary entry, and
- Passwords that are detectable permutations of the username are not allowed.

This is estimated to ensure at least 10-bits of min entropy. Other means may be substituted to ensure at least 10 bits of min-entropy. User chosen passwords of at least 15 characters are assumed to have at least 10-bits of min-entropy. For example a user might be given a short randomly to character randomly chosen string (two randomly chosen characters from a 94-bit alphabet have about 13 bits of entropy). A password, for example might combine short system selected random elements, to ensure 10-bits of min-entropy, with a longer user-chosen password.

## **A.2 Other Types of Passwords**

Some password systems require a user to memorize a number of images, such as faces. Users are then typically presented with successive fields of several images (typically 9 at a time), each of which contains one of the memorized images. Each selection represents approximately 3.17 bits of entropy. If such a system used five rounds of memorized images, then the entropy of system would be approximately 16 bits. Since this is randomly selected password the guessing entropy and min-entropy are both the same value.

It is possible to combine randomly chosen and user chosen elements into a single composite password. For example a user might be given a short randomly selected value to ensure min-entropy to use in combination with a user chosen password string. The random component might be images or a character string.

## **A.3 Examples**

The intent of this guidance is to allow designers and implementers flexibility in designing password authentication systems. System designers can trade off password length, rules and measures imposed to limit the number of guesses an adversary can attempt.

The approach of this recommendation to password strength is that it is a measure of the probability that an attacker, who knows nothing but a user's name, can discover the user's password by means of "in-band" password guessing attack. That is the attacker attempts to try different passwords until he/she authenticates successfully. At each level given below, the maximum probability that, over the life of the password, an attacker with no *a priori* knowledge of the password will succeed in an in-band password guessing attack is:

1. Level 1-  $2^{-10}$  (1 in 1024)
2. Level 2 -  $2^{-14}$  (1 in 16,384)

Consider a system that assigns subscribers 6 character passwords, randomly selected from an alphabet of 94 printable keyboard characters. From Table A.1 we see that such a password is considered to have 39.5 bits of entropy. If the authentication system limits the number of possible unsuccessful authentication trials to  $2^{39.5}/2^{14} = 2^{25.5}$  trials, the password strength requirements of Level 2 are satisfied. The authentication system could, for example, simply maintain a counter that locked the password after  $2^{25.5}$  (about

forty-five million) total unsuccessful trials. An alternative scheme would be to lock out the claimant for a minute after three successive failed authentication attempts. Such a lock out would suffice to limit automated attacks to 3 trials a minute and it would take about 90 years to carryout  $2^{25.5}$  trials. If the system required that password authentication attempts be locked for one minute after three unsuccessful trials and that passwords be changed every ten years, then the targeted password guessing attack requirements of Level 2 would be comfortably satisfied. Because the min-entropy of a randomly chosen password is the same as the guessing entropy, the min-entropy requirements of level two are met.

Consider a system that used:

- a minimum of 8 character passwords, selected by subscribers from an alphabet of 94 printable characters,
- required subscribers to include at least one upper case letter, one lower case letter, one number and one special character, and;
- Used a dictionary to prevent subscribers from including common words and prevented permutations of the username as a password.

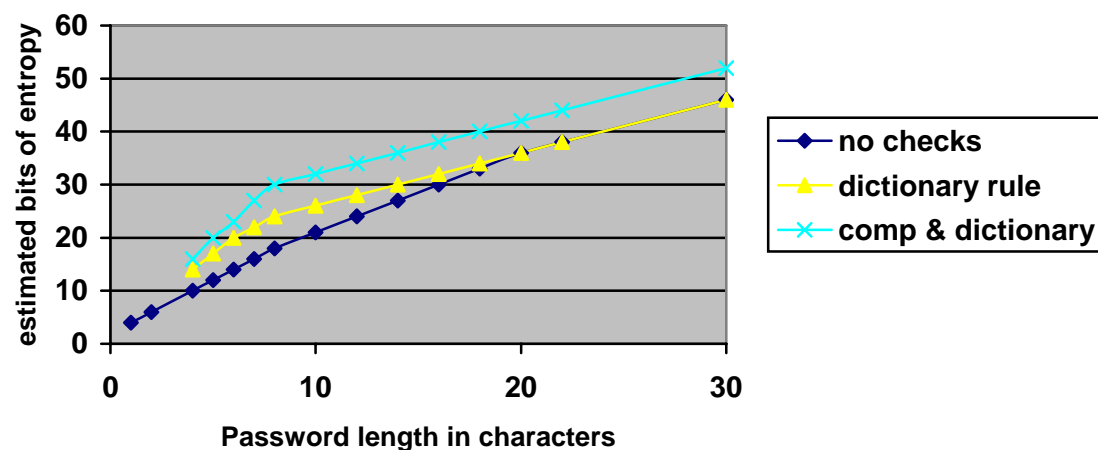
Such a password would meet the composition and dictionary rules for user-selected passwords in Appendix A, and from Table A.1 we estimate guessing entropy at 30 bits. Any system that limited a subscriber to less than  $2^{16}$  (about 65,000) failed authentication attempts over the life of the password would satisfy the targeted guessing attack requirements of Level 2. For example, consider a system that required passwords to be changed every two years and limited trials by locking an account for 24 hours after 6 successive failed authentication attempts. An attacker could get  $2 \times 365 \times 6 = 4,380$  attempts during the life of the password and this would easily meet the targeted attack requirements of Level 2. Because of the dictionary test, this would also meet the min-entropy rules for Level 2.

It will be very hard to impose dictionary rules on longer passwords, and many people may prefer to memorize a relatively long “pass-phrases” of words, rather than a shorter, more arbitrary password. An example might be: “IamtheCapitanofthePina4”.

As an alternative to imposing some arbitrary specific set of rules, an authentication system might grade user passwords, using the rules stated above, and accept any that meet some minimum entropy standard. For example, suppose passwords with at least 24-bits of entropy were required. We can calculate the entropy estimate of “IamtheCapitanofthePina4” by observing that the string has 23 characters and would satisfy a composition rule requiring upper case and non-alphabetic characters. Table A.1 estimates 45 bits of guessing entropy for this password.

**Table A.1 – Estimated Password Guessing Entropy in bits vs. Password Length**

Length Char.	User Chosen			Randomly Chosen		
	94 Character Alphabet			10 char. alphabet		94 char alphabet
	No Checks	Dictionary Rule	Dict. & Comp. Rule			
1	4	-	-	3	3.3	6.6
2	6	-	-	5	6.7	13.2
3	8	-	-	7	10.0	19.8
4	10	14	16	9	13.3	26.3
5	12	17	20	10	16.7	32.9
6	14	20	23	11	20.0	39.5
7	16	22	27	12	23.3	46.1
8	18	24	30	13	26.6	52.7
10	21	26	32	15	33.3	65.9
12	24	28	34	17	40.0	79.0
14	27	30	36	19	46.6	92.2
16	30	32	38	21	53.3	105.4
18	33	34	40	23	59.9	118.5
20	36	36	42	25	66.6	131.7
22	38	38	44	27	73.3	144.7
24	40	40	46	29	79.9	158.0
30	46	46	52	35	99.9	197.2
40	56	56	62	45	133.2	263.4

**Figure A.1 - Estimated User Selected Password Entropy vs. Length**

## Appendix B: Errata

### ***Appendix B.1: Errata for Version 1.0.1***

1. Cover page: Changed Version number from 1.0 to 1.0.1.
2. Cover page: Changed date from June 2004 to September 2004.
3. Page vii: Clarified text to indicate Level 3 authentication may be supported using one-time passwords, but not reusable passwords.
4. Definition of “Approved” revised to include FIPS 140-2 validation of cryptographic modules and include a URL pointing to the list of validated modules.
5. Page 26: Clarified meaning of “cross-certification” with the Federal Bridge CA by adding a footnote to explicitly state that cross-certification with the Federal Bridge CA need not be bi-directional for the purposes of this guideline.
6. Page 40, Table 2: Clarified that PINS, a form of passwords, are allowed at Levels 1 and 2.

In addition, minor editorial changes (e.g., capitalization, spelling, and punctuation) have been made throughout, and some links have been fixed.

### ***Appendix B.2: Errata for Version 1.0.2***

1. Cover page: Changed Version number from 1.0.1 to 1.0.2.
2. Cover page: Changed date from September 2004 to April 2006.
3. Cover page: Specified William Jeffrey as NIST Director and Robert Cresanti as Department of Commerce Under Secretary for Technology
4. Page 25: Updated mapping of FPKI Certificate Policies to 800-63 registration levels to reflect changes in FBCA Basic Assurance Level and incorporate three new FPKI certificate policies (FBCA Medium Hardware policy, Common Authentication, and Common-High). FBCA Basic was upgraded by the Federal PKI Policy Authority to meet Level 3 registration requirements; the new policies satisfy Level 4 Registration requirements.
5. Page 41: A new Table 7 was inserted to clarify the relationship of the certificate policies in the Common Policy Framework with the E-Authentication Assurance Levels. New introductory text associated with this table explains that the Card Authentication and Common Device policies are excluded from consideration, since these policies support authentication of devices.
6. Page 42: Table 8 (Table 7 in version 1.0.1) was updated to reflect the modifications in the Basic certificate policy, which now satisfies Level 3. The new Medium-HW certificate policy, which satisfies Level 4, was also added to this table. Certificate policies from the Common Policy Framework were deleted from this table, since they are specified in the new Table 7.
7. Page 45: URLs for FPKI certificate policies have been updated.

## What is the InCommon Federation?

*Providing a framework of trust for the safe sharing of online resources*

---

### What is InCommon?

Increasingly, far-flung faculty members, universities and service providers work together online. Collaboration groups require user IDs and passwords for their protected online resources. As passwords proliferate, users fill notebooks or add more and more sticky notes around their computer monitors to remember which credentials go with which resource. Security and intellectual property nightmares ensue.

As off-campus resource accounts proliferate, so does personal identity data, which is retained by a multitude of service partners, increasing the likelihood of data spills and misuse that cannot be controlled by campus policies. Furthermore, service providers are forced to provision and maintain large user account systems instead of focusing on their real mission: providing online resources.

InCommon eliminates this need for multiple, password-protected accounts and simplifies access for the end user, minimizing support calls for everyone. Online service providers no longer need to maintain their own databases of identity information for access control.

And best of all, federated access scales. Once an institution or higher-education partner is a participating member, setting up a new relationship can take as little as a few minutes.

### How Does it Work?

InCommon's value is based on federated identity management. A user of a resource clicks on a service partner's resource. Once the user is authenticated by his or her home institution, the campus infrastructure releases only enough identity data to allow the service partner to make an access decision.

The user's institution takes responsibility for authentication and controls the release of personal information. The service partner uses the minimal identity information to control access to its resources.

End users simply use their campus user ID and password to access off-campus online resources.

InCommon's role in this is simple: It provides a framework of shared policies trust-establishing processes, and technology standards for universities and service partners to follow. This greatly streamlines collaboration with multiple organizations. For example, institutions and service providers could spend time establishing operating principles, technology hooks, and agreed-upon data exchange elements with each partner, or they could do it once by joining InCommon and then leveraging these common elements for many relationships.

### InCommon Benefits

- InCommon supports Web-based distributed authentication and authorization services, such as controlled access to protected content resources.
- Participants exchange information in a standardized format, reducing or removing the need to repeat integration work for each new resource.
- Access decisions and user privacy controls are decided on a case by case basis for each resource, providing higher security and more granular control.
- Institutions experience reduced account management overhead by eliminating the need for separate accounts to access particular resources.
- Campus and company IT professionals provide protected content to multiple organizations using a single authentication framework.
- The home institution controls when an identity is disclosed, and how much information is revealed.

### Who can join InCommon?

Any accredited two-and four-year higher education institution can join InCommon. Additionally, higher education participants can sponsor their online service providers that make resources available to individuals or groups. For more information, and a list of participants, see [www.incommonfederation.org](http://www.incommonfederation.org).

10/12/2008



# **Identity Assurance Profiles Bronze and Silver**

11/04/2008  
Version 1.0



## Executive Summary

Identity Assurance Profiles, as described in the InCommon Identity Assurance Assessment Framework, define the specific requirements that Identity Providers must meet in order to be eligible to include InCommon Identity Assurance Qualifier(s) in identity assertions that they offer to Service Providers. The reader is assumed to be familiar with the InCommon Identity Assurance Assessment Framework.

This document defines criteria used to assess Identity Providers that wish to qualify for InCommon Silver or Bronze identity assurance designation. These profiles are intended to be at least compatible with the Federal NIST Special Publication 800-63 "Level 2" and "Level 1" identity assurance levels. The requirements are directly applicable to Identity Providers that use shared secret models for identity credentials but stronger credentials, as defined in [SP 800-63], could be used as well.

InCommon Bronze designation requires that an Identity Provider support at least basic userID/password credentials with reasonably hard to guess passwords. Identity assertions may include a unique identifier for each identity Subject that should be usable in access control lists but further identity information may be not well known. InCommon Silver designation requires credentials with very hard to guess passwords and better credential management, reasonably verified personal information about each Subject, unique Subject identifiers that are never reassigned, and secure business and operational processes.

An identity provider that qualifies under Silver automatically also qualifies under Bronze. Identity providers that meet or exceed either of these qualifications are identified as compliant in the InCommon Identity Provider metadata and may include the appropriate Identity Assertion Qualifier(s) in identity assertions they provide.

# Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>2</b>	<b>SCOPE.....</b>	<b>1</b>
<b>3</b>	<b>TERMINOLOGY .....</b>	<b>3</b>
<b>4</b>	<b>CRITERIA .....</b>	<b>4</b>
4.1	SUMMARY OF ASSESSMENT FACTORS .....	4
4.2	DESCRIPTION OF ASSESSMENT FACTORS .....	6
4.2.1	<i>Business, Policy and Operational Factors.....</i>	<i>6</i>
4.2.2	<i>Registration and Identity Proofing .....</i>	<i>8</i>
4.2.3	<i>Digital Electronic Credential Technology .....</i>	<i>11</i>
4.2.4	<i>Credential Issuance and Management .....</i>	<i>13</i>
4.2.5	<i>Security and Management of Authentication Events .....</i>	<i>16</i>
4.2.6	<i>Identity Information Management .....</i>	<i>19</i>
4.2.7	<i>Identity Assertion Content .....</i>	<i>20</i>
4.2.8	<i>Technical Environment.....</i>	<i>21</i>
<b>5</b>	<b>REFERENCES.....</b>	<b>23</b>
<b>6</b>	<b>DOCUMENT HISTORY .....</b>	<b>23</b>

## 1 INTRODUCTION

This document is part of InCommon's defined identity assurance service. Please refer to the InCommon Identity Assurance Assessment Framework (IAAF) for an overview.

Additional information can be found at <http://www.incommonfederation.org>

This Identity Assurance Profile (IAP) document contains criteria used to assess Identity Provider (IdP) operators that wish to qualify for InCommon Silver or Bronze identity assurance designation. An IdP operator is an organization that registers identity Subjects, issues and manages digital identity credentials, maintains an identity information database or directory, and provides certain identity information to Service Providers (SPs) on behalf of the identity Subject. This type of IdP is called "assertion-based" because an identity Subject authenticates to the IdP and then the IdP provides identity information regarding the Subject to one or more SPs in identity assertion messages. InCommon's certification that an IdP operator meets the requirements of an IAP gives the SP a basis for trusting the identity assertion.

IdP operators that wish to qualify for Silver or Bronze certification must undertake an initial assessment against the requirements in this IAP and then engage an independent qualified auditor to review and attest to that assessment. IdP operators qualified under this IAP must undergo a re-assessment and audit at least every 24 months to ensure the organization's policies, procedures and practices remain consistent with the IAP.

## 2 SCOPE

The scope of this assessment profile includes issues regarding the nature of the IdP operator's organization, the process for Subject registration with the IdP operator, the type of the digital credential they are given, the handling of identity information about the Subject, and the identity assertion given to SPs. This IAP covers only how identity credentials and associated identity information for Subjects that are natural persons are issued and managed. A full description of the role and scope of an IAP document is contained in the InCommon IAAF.

In any assertion-based system, the identity Subject must be given one or more digital credential(s) with which to authenticate to their IdP. A common form of credential is a "UserID" and a "shared secret" (e.g., password) to be used for local authentication of the Subject to the IdP. This IAP assumes that sufficiently robust passwords are adequate for the purposes of these identity assertions. Stronger forms of digital identity credentials such as Kerberos or PKI certificates should satisfy the credential requirements of these profiles as well.

A password is the secret that a claimant keeps confidential and enters on-line only to verify ownership of his or her digital identity credential. Passwords are typically character strings and may vary in robustness against guessing by an unauthorized party. Passwords also encompass Personal Identification Numbers (PINs), which are considered a special form of password consisting of only decimal digits. This IAP defines requirements for the nature and handling of passwords used for authentication to the IdP.

If stronger forms of digital credentials are used, e.g., Kerberos or PKI certificates, the password provisions of this IAP may not apply. For example, a PKI certificate on a hardware token must have a PIN to protect it but this IAP does not define the strength of that PIN nor any requirement for certificate revocation in case the device is lost or the PIN compromised. Therefore, in these cases the IdP operator and independent auditor must use professional judgment in determining whether the stronger credentials meet or exceed the requirements in section 4.2.3 *Digital Electronic Credential Technology*. Examples include:

- Password-based systems that employ specialized client software for the password authentication protocol and access management to the SP;
- Systems that use passwords in conjunction with hardware tokens or specialized software;
- Systems where PINs are used in conjunction with physical tokens or specialized software.

This IAP **may not** apply to:

- PKI or other token-based systems where the relying party (SP) expects to directly verify the Subject's possession of her or his credential; or
- Systems that require an independent SP to know the Subject's "shared secret" (see section 4.2.5.6); or
- Other types of IdP services such as authorization assertions.

InCommon Bronze criteria are a subset of InCommon Silver criteria. These two IAPs may have different requirements for the same criterion, for example password or token strength. In this case, meeting the Silver requirement will also satisfy the Bronze requirement but not *vice versa*. InCommon Federation metadata will designate Identity Provider (IdP) operators that are Federation Participants and that meet or exceed the requirements of the Bronze IAP as qualified to assert the Bronze Identity Assurance Qualifier (IAQ) as part of identity assertions. Identity Provider operators that meet the requirements of the Silver IAP will be designated as qualified to assert both Bronze and Silver IAQs, as appropriate, as part of identity assertions.

A given IdP operator may support a diverse community of Subjects and may have different identity management processes and services for subsets of that community. For example, a campus IdP operator might support a basic level of identity assurance for most students and staff and support enhanced identity assurance for faculty and for staff that perform in roles that require it. A campus IdP operator might support "guest accounts" for visitors for which there is no formal identity assurance and hence assertions for those Subjects would not conform even to the Bronze IAP. It is also possible for a given Subject to have more than one type of credential with which to authenticate to the campus's IdP and the particular credential used might affect the relevant IAQ. An InCommon IdP operator that is certified by InCommon to provide identity assertions under more than one IAP must be able to associate the appropriate IAQ(s), if any, with each identity assertion it makes based on how the assertion Subject's identity has been managed with respect to the criteria in each IAP.

### 3 TERMINOLOGY

This document relies on terminology defined in NIST Special Publication 800-63 "*Recommendations for Electronic Authentication*", and the Federal OMB "*Guidance for E-Authentication for Federal Agencies*" as well as terms defined by InCommon. See the References section of the IAAF for bibliographic details. The IAAF, Appendix A: Glossary, provides definitions of terms used in this document.

000001

## 4 CRITERIA

The criteria outlined below are organized by assessment topic, and will be applied cumulatively as discussed in Section 2, Scope. These criteria apply to the organization's IDP and its relevant functional unit, not to a parent organization directly.

### 4.1 Summary of Assessment Factors

This table summarizes all of the assessment factors defined for Bronze and Silver IAPs. Cells that are shaded gray do not apply to the particular profile. Each factor is described and defined in the sections following.

Assessment Area	Factors	Bronze	Silver
<b>4.2.1 Business, Policy and Operational Factors</b>	.1 Established legal entity		
	.2 Designated authority for IdMS and IdP services		
	.3 General Disclosures to identity Subjects		
	.4 Documentation of policies and practices	n/a	
	.5 Appropriate staffing	n/a	
	.6 Outsourced components	n/a	
	.7 Helpdesk	n/a	
	.8 Audit of IdMS operations		
	.9 Risk Management plan	n/a	
	.10 Logging of operations events	n/a	
<b>4.2.2 Registration and Identity Proofing</b>	.1 Identity Verification Process disclosure	n/a	
	.2 Retention of registration records	n/a	
	.3 Identity proofing	n/a	
	.3.1 Existing relationship with the organization	n/a	
	.3.2 In-person proofing	n/a	
	.3.3 Remote proofing	n/a	
<b>4.2.3 Digital Electronic Credential Technology</b>	.1 Unique credential identifier		
	.2 Subject modifiable shared secret		
	.3 Resistance to guessing shared secret		n/a
	.4 Strong resistance to guessing shared secret	n/a	
<b>4.2.4 Credential Issuance and Management</b>	.1 Unique Subject identifier		
	.2 Credential status		
	.3 Confirmation of delivery	n/a	
	.4 Credential status verification	n/a	
	.5 Suspected or attempted credential compromise	n/a	
	.6 Credential revocation	n/a	
	.7 Credential renewal or re-issuance	n/a	

Assessment Area	Factors	Bronze	Silver
<b>4.2.4.7 Security and Management of Authentication Events</b>	.1 Secure channel		n/a
	.2 End-to-end secure communications	n/a	
	.3 Proof of possession		
	.4 Session authentication		
	.5 Stored secrets		
	.6 Protected secrets	n/a	
	.7 Mitigate risk of sharing credentials		
	.8 Threat protection 1		
	.9 Threat protection 2	n/a	
	.10 Authentication protocols 1		n/a
	.11 Authentication protocols 2	n/a	
<b>4.2.6 Identity Information Management</b>	.1 Identity status management	n/a	
<b>4.2.7 Identity Assertion Content</b>	.1 Identity attributes		
	.2 Identity Assertion Qualifier		
	.3 Cryptographic security		
<b>4.2.8 Technical Environment</b>	.1 Configuration Management	n/a	
	.2 Network Security	n/a	
	.3 Physical Security	n/a	
	.4 Continuity of Operations	n/a	

## 4.2 Description of Assessment Factors

The assessment criteria and suggested evidence of compliance are presented below for each of the factors in each assessment area. The suggested evidence is not an absolute requirement; assessors should create an assessment program appropriate to the IdP operator to be assessed. Assessors may use subjective judgment if the suggested evidence for a particular criterion is not readily available but other relevant evidence might be substituted. In such a case, the assessor should provide a brief justification for such a decision.

In the tables that follow, ⑥ indicates the criterion applies to the Bronze IAP;  
⑦ indicates the criterion applies to the Silver IAP.

### 4.2.1 Business, Policy and Operational Factors

These are factors that indicate the identity service provider's readiness to support and operate a reliable operational service.

#### 4.2.1.1 ⑦ ⑥ Established legal entity and identity management services

1. The institution responsible for the IdP operator shall be a valid legal entity.
2. The operational identity management system (IdMS) and IdP service(s) will be assessed as they stand at the time of the Assessment. Planned but not yet implemented upgrades or modifications are not to be considered during the assessment.

##### **Suggested Evidence of Compliance**

1. Articles of incorporation, Organizational Charter, Affidavit, etc.
2. Site visit to the IdP operator management and operational facilities.

#### 4.2.1.2 ⑦ ⑥ Designated authority for IdMS and IdP services

The IdP operator shall be designated by executive management of the responsible institution to perform this service as required by the institution's policies.

##### **Suggested Evidence of Compliance**

Institution's organization documentation and either relevant policy or delegation memo from executive office responsible for the IdP function.

#### 4.2.1.3 ⑦ ⑥ General disclosures to Identity Subjects

The IdP operator shall make available to the intended Subject community the terms and conditions under which it issues accounts, as well as the privacy policy which governs the release of identity attribute information for its identity Subjects.

##### **Suggested Evidence of Compliance**

1. Terms, Conditions, and Privacy policies posted on Website or equivalent.
2. Documentation describing how IdP operator will do this.

#### 4.2.1.4 ⑦ Documentation of policies and practices

1. The IdP operator shall have all security related policies and procedures documented that are required to demonstrate compliance.
2. Undocumented practices will not be considered evidence.



**Suggested Evidence of Compliance**

Copies of or on-line links to policies

**4.2.1.5 ⓘ Appropriate staffing**

1. The IdP operator shall have sufficient numbers and levels of staff to operate its services and supporting infrastructure according to its stated policies and procedures.
2. The staff who operate the IdP services shall have the appropriate skills and abilities for their roles.

**Suggested Evidence of Compliance**

Roles and responsibilities defined in job descriptions for each staff member.

**4.2.1.6 ⓘ Outsourced components**

1. Components of an IdP's services may be provided by third parties but all such arrangements that might impact these assurance profiles must be covered by a written binding contract.
2. Any contract for outsourced components of the IdP services shall have clear, appropriate and monitored requirements, where the agreement stipulates critical policies and practices that bear upon the assurance profile of the IdP services.
3. Contractor responsibilities that are not stipulated in their agreements will not be considered reliable during the assessment.

**Suggested Evidence of Compliance**

The existence of supporting contracts and agreements.

**4.2.1.7 ⓘ Helpdesk**

A helpdesk shall be available for identity Subjects to resolve issues related to their credentials during the IdP operator's regular business hours, minimally 8 hours per day, Monday through Friday.

**Suggested Evidence of Compliance**

The existence and proper staffing of a help desk function.

**4.2.1.8 ⓘ ⓘ Institutional Audit of IdMS operations**

The IdP operator shall be audited by an independent internal or external auditor at least every 24 months to ensure the operation's practices are consistent with the institution's policies and procedures for services of this type. At the time of the required assessment for conformance with these IAPs, the most recent institutional audit shall have been performed within the last 12 months.<sup>1</sup>

**Suggested Evidence of Compliance**

A copy of latest audit results and IdP response.

**4.2.1.9 ⓘ Risk Management plan**

The IdP shall demonstrate a risk management methodology that adequately identifies and mitigates risks related to the IdP operations. These considerations should include at a minimum:

- background checks on staff in sensitive positions;

---

<sup>1</sup> This is a separate requirement from the audit for compliance with this IAP. The two audits may be combined.

- controls on access and changes to critical data;
- strong digital credentials for access to critical systems;
- separation of duties where appropriate.

### **Suggested Evidence of Compliance**

Risk Assessment documentation

#### **4.2.1.10 ⓘ Logging of operations events**

The IdP operator shall log date, time, nature and outcome of all significant events related to identity management (e.g., issuance, vetting, revocation, reactivation, successful and failed authentication events, etc.) and retain such logs securely for at least 6 months after the date of the last entry.

### **Suggested Evidence of Compliance**

The existence of logs and a retention policy.

## **4.2.2 Registration and Identity Proofing**

Identity proofing is the process by which an identity service provider associates a specific identity Subject with the correct record in the IdP operator's IdMS or creates a new record. If a new record is created it must be seeded with basic information for that Subject that will help re-establish the Subject's association with that record if required at some time in the future, e.g. the credential has expired or there is a gap in the Subject's association with the IdP operator.

#### **4.2.2.1 ⓘ Identity Verification Process (IVP) disclosure**

1. The identity proofing and registration process shall be performed according to a written policy or practice statement that specifies the particular steps taken to verify identities.
2. The practice statement shall address primary objectives of registration and identity proofing, including:
  - Ensuring a person with the applicant's claimed attributes does exist, and those attributes are sufficient to uniquely identify a single person within the IdP operator's range of foreseeable potential Subjects;
  - Ensuring the applicant whose identity information is registered is in fact the physical person who is entitled to the claimed identity;
3. Personal identifying information collected as part of the registration process must be protected from unauthorized disclosure or modification.
4. The IdP operator shall publish its IVP and evidentiary requirements, to the extent necessary to indicate compliance with these IAP criteria. That is, the IdP operator is not *de facto* required to disclose all of its IVP processes and details. Rather, only enough information is required for the Assessment Team and Auditor to make an informed decision.

### **Suggested Evidence of Compliance**

Documentation of procedures and requirements

#### **4.2.2.2 ⓘ Retention of registration records**

1. A record of the facts of registration shall be maintained by the IdP operator or its representative (e.g., Registration Authority). This information should help re-establish the Subject's correct association with his or her IdMS entry if necessary at some future time.
2. The record of the facts of registration, shall, as a minimum, include:
  - Identity proofing document numbers;
  - Full name as shown on the documents;
  - Date of birth;
  - Current address of record (see IAAF glossary).
3. Records also must include revocation or termination of registration.
4. The minimum record retention period for registration data is seven years and six months beyond the expiration or revocation (whichever is later).
5. IdP operators also must conform with any corporate records retention policies, whatever laws apply to the corporate entity, and any state or Federal records retention requirements.
6. At a minimum, credentials shall include identifying information that permits recovery of the records of the registration associated with the credentials and a personal name that is associated with the identity Subject. In every case, given the issuer and the identifying information in the credential, it must be possible to recover the registration records upon which the credentials are based.

#### **Suggested Evidence of Compliance**

The records and logs obtained and kept

##### **4.2.2.3    ©   Identity proofing**

For each identity proofing mechanism employed by the IdP operator or its Registration Authority, one or more of the following three criteria must be met:

##### **4.2.2.3.1   Existing Relationship**

Employers and educational institutions which verify the identity of their employees, students or other affiliates by means comparable to those stated for In-person Proofing or Remote Proofing may be designated an RA by the IdP operator. The IdP operator shall confirm that the applicant is a person with a current relationship to the organization, record the nature of that relationship and verify that the relationship is in good standing. If the IdP operator's IdMS directory or database is separate from the institution's or RA's database, the IdP operator shall confirm that the applicant's name and address are consistent in both places.

#### **Suggested Evidence of Compliance**

The records of identity proofing.

##### **4.2.2.3.2   In Person Proofing**

1. The IdP operator's Registration Authority (RA) shall establish the applicant's IdMS registration identity based on possession of a valid current Government Picture ID that contains applicant's picture, and either an address or nationality (e.g., driver's license or passport)

2. RA inspects photo-ID, compares picture to applicant, records ID number, date of issuance and expiration, address if available, and date of birth. If ID appears valid and photo matches applicant then:
  - a. If ID confirms the address of record,<sup>2</sup> authorize or issue credentials and send notice to the address of record; or
  - b. If ID does not confirm the address of record,<sup>3</sup> issue credentials in a manner that confirms the address of record.

#### **Suggested Evidence of Compliance**

The existence of a standard documented process done by competent trained individuals.

#### **4.2.2.3.3 Remote Proofing**

1. The RA shall establish the applicant's IdMS registration identity based on possession of at least one valid Government ID number (e.g. a driver's license or passport) and either a second Government ID number or
  - a student or employee ID number; or
  - financial account number (e.g., checking account, savings account, loan or credit card); or
  - a utility service (e.g., electricity, gas, or water) account number.
2. RA verifies other information provided by applicant using both of the ID numbers above through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual.
3. Address confirmation and notification:
  - a. RA sends notice to an address of record confirmed in the records check and receives a mailed or telephone reply from applicant; or
  - b. RA issues credentials in a manner that confirms the address of record supplied by the applicant, for example by requiring applicant to enter on-line some information from a notice sent to the applicant; or
  - c. RA issues credentials in a manner that confirms ability of the applicant to receive telephone communications at a telephone number or e-mail at an e-mail address associated with the applicant in existing records. Any secret sent over an unprotected channel shall be invalidated upon first use.

#### **Suggested Evidence of Compliance**

Documentation of the policy and process, and samples of records.

---

<sup>2</sup> See definition in section 4.2.2.2 above.

<sup>3</sup> Ibid.

### 4.2.3 Digital Electronic Credential Technology

These InCommon IAPs allow the use of "shared secret" forms of identity credentials; stronger credentials<sup>4</sup> may be used as well to authenticate the Subject to the IdP. The most common form of shared secret credentials is the traditional userID and password but other types exist as well. The basic model is that a Subject must enter a secret that only he or she knows and that can be used by the IdP's credential verification system to confirm that the subject of the credential is in fact offering the credential.

#### 4.2.3.1 ⑤ ⑥ Unique credential identifier

1. Each identity Subject shall self-select or be given at registration time a token (e.g., credential UserID) that is unique across all such elements in use by the IdP operator.
2. An identity Subject can have more than one token, but a given token can only map to one identity Subject.

##### **Suggested Evidence of Compliance**

The documented mechanism in place to ensure uniqueness.

#### 4.2.3.2 ⑤ ⑥ Subject modifiable shared secret

1. Each identity Subject shall self-select or be given a shared secret, e.g., PIN or password, that must be presented by a claimant asserting the credential. Such secret must meet the applicable requirements for resistance to guessing.
2. The identity Subject must be able to change his or her shared secret if the credential is still valid and the current secret has not been compromised. The new secret must meet the applicable requirements for resistance to guessing. If the Subject can not provide the current shared secret, the credential renewal procedure must be followed per section 4.2.4.7.

##### **Suggested Evidence of Compliance**

A documented process and mechanisms to accomplish this.

#### 4.2.3.3 ⑥ Resistance to guessing shared secret

The PIN (numeric-only) or password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a given identity Subject's PIN or password shall have a probability of success of less than  $2^{-10}$  (1 chance in 1,024) success over the life of the PIN or password.

Refer to NIST [SP 800-63], Appendix A, and the NIST Shared Secret Entropy Spreadsheet to calculate resistance to online guessing.

##### **Suggested Evidence of Compliance**

1. Documented procedures and mechanisms that define a method of providing a mathematically adequate level of resistance.
2. Use of NIST Entropy Spreadsheet to show sufficient token strength.

#### 4.2.3.4 ⑤ Strong resistance to guessing shared secret

1. The PIN (numeric-only) or password, and the controls used to limit on-line guessing attacks shall ensure that an attack targeted against a selected user's PIN or password

---

<sup>4</sup> See NIST [SP 800-63]

shall have a probability of success of less than  $2^{-14}$  (1 chance in 16,384) over the life of the PIN or Password.

2. The PIN (numeric-only) or password shall have at least 10 bits of min-entropy (a measure of the difficulty that an attacker faces to guess the most commonly chosen password used in a system) to protect against untargeted attack.

Refer to NIST [SP 800-63], Appendix A, and the NIST Shared Secret Entropy Spreadsheet to calculate min-entropy and resistance to online guessing.

#### **Suggested Evidence of Compliance**

1. Documented procedures and mechanisms that define a method of providing a mathematically adequate level of resistance.
2. Use of NIST Entropy Spreadsheet to show sufficient token strength.

#### 4.2.4 Credential Issuance and Management

How electronic identity credentials are issued and managed is critical to the assurance of identities that may be asserted by an IdP later. The credential represents the binding between the physical identity Subject and the IdMS database or directory record describing that entity.

##### 4.2.4.1 ⑤ ⑥ Unique Subject identifier

At the time of credential issuance, the IdP operator shall assign a unique identifier to the Subject's IdMS record. This identifier may be included in identity assertions that require a specific identifier for this Subject. This identifier must:

- a. be unique among all such identifiers previously issued by the IdP operator;
- b. never be reassigned to a different person.

This identifier need not be persistent, that is, the particular identifier for a given Subject could be changed if necessary.

##### **Suggested Evidence of Compliance**

The IdP operator's documentation of the procedures and mechanisms to achieve and ensure this uniqueness.

##### 4.2.4.2 ⑤ ⑥ Credential status

IdP operator shall maintain record of the status of credentials and not authenticate credentials that have been revoked.

##### **Suggested Evidence of Compliance**

Documentation of mechanism in place to accomplish this

##### 4.2.4.3 ⑤ Credential Issuance Process

If the credential issuance process is a separate transaction from registration, these processes must be linked together to ensure that the credential is issued to the registered person. For simple passwords and where the credential is issued in person, this may be accomplished by observing the Subject make use of it. In the case of remote issuance, it may be accomplished by requiring the Subject to provide a secret phrase to the RA at the time s/he applies for a credential and then entering that phrase after entering his/her password for the first time. This also may be done by requiring subsequent entry of a temporary secret provided at registration time in person, or sent to the subject by way of:

- a. Postal address of record such as that used for delivery of sensitive personal communications to that individual; or
- b. Cell phone or telephone number of record.

##### **Suggested Evidence of Compliance**

Documentation of the credential issuance process.

##### 4.2.4.4 ⑤ Credential status verification

IdP operator shall provide a secure automated mechanism to allow the credential verifier to determine credential status during authentication of the claimant's identity. Acceptable mechanisms for credential status verification include, but are not limited to:

- Database lookup;
- Digitally signed revocation list;
- Status Responder.

In addition, IdP operator must ensure that credential status is available to verifier at least 99% of the time, inclusive of scheduled downtime,

#### **Suggested Evidence of Compliance**

Documentation of mechanism as implemented; system logs of down time for credential verifier.

#### **4.2.4.5 ⓘ Suspected or attempted credential compromise**

1. If some type of compromise of a Subject's password is suspected, the IdP must not include the Silver IAQ as part of identity assertions for that Subject until the password has been reset successfully by the identity Subject.

The identity Subject must be notified of this event as soon as possible.

The IdP may include the InCommon Bronze IAQ during the period between suspected compromise and shared secret reset.

2. If a credential verifier detects 10 or more successive failed attempts to submit an authentication secret for a given credential within 10 minutes, this could indicate a brute force attack on the Subject's credential.<sup>5</sup> In this case the IdP must take at least one of the following steps:

A. The IdP's credential verifier shall insert a 30 second delay before acting on password submission from that IP address until a verification is successful. If the failed attempts continue for more than 48 hours, the Subject shall be notified and required to reset her or his password; or

B. The IdP shall not include the Silver IAQ as part of identity assertions for this Subject until the Subject resets her or his password (the Bronze IAQ still may be included); or

C. Lock out use of this Subject's account until the Subject resets her or his password.

#### **Suggested Evidence of Compliance**

Documentation of processes and mechanisms to effect and demonstrate this.

#### **4.2.4.6 ⓘ Credential revocation**

1. The IdP operator shall revoke credentials and tokens within 72 hours after being notified that a credential is no longer valid or is compromised to ensure that a claimant using the credential cannot successfully be authenticated by the IdP.
2. If the IdP operator issues credentials that expire automatically within 72 hours or less then the IdP operator is not required to provide an explicit mechanism to revoke the credentials.

#### **Suggested Evidence of Compliance**

Documentation of the mechanism in place to effect and demonstrate this.

---

<sup>5</sup> A slower rate of such an attack would take far too long to complete. See [SP 800-63], Appendix A, Section A.3



#### **4.2.4.7 ⑤ Credential renewal or re-issuance**

Appropriate policy and process must be in place to ensure that any new credential and/or authentication secret, e.g., password, is provided only to the actual credential subject should it be necessary to renew an authentication secret, e.g., due to suspected compromise or the Subject having forgotten the secret, or to reissue a credential due to expiration. This process must be at least as trustworthy as the process used for initial issuance of the credential.

Proof-of-possession of an unexpired current authentication secret shall be demonstrated by the Claimant prior to the IdP allowing renewal or re-issuance. If the Claimant can not supply the current authentication secret, supplying answers to pre-registered personalized questions can suffice. If this "question and answer" method is used it must meet the requirements for shared secrets described in section 4.2.3 (strong resistance to guessing, etc).

Authentication secrets shall not be recovered; new secrets shall be issued. All interactions shall occur over a protected channel such as SSL/TLS.

After expiration of the current credential or authentication secret, renewal and re-issuance shall require the Subject be vetted again as described in section 4.2.2.

#### **Suggested Evidence of Compliance**

Documentation of the mechanism in place to effect and demonstrate this.

## 4.2.5 Security and Management of Authentication Events

An authentication event occurs when a Subject ("claimant") offers his or her credential to a credential verifier and proves the right to that identity binding. Such an event might occur at the time an identity assertion is needed or some amount of time before that point if the verifier supports a "single sign-on" stateful mechanism.

### 4.2.5.1 ② Secure Channel

Any secret used by a claimant during the authentication event supporting an identity assertion shall be encrypted if transmitted across any shared network that is not managed by the IdP operator or, if applicable, its parent organization.

#### Suggested Evidence of Compliance

Policy statement and mechanism to demonstrate this.

### 4.2.5.2 ③ End-to-end secure communication

Under this IAP, cryptographic operations are required between claimant and verifier in order to ensure an end-to-end secure communications channel.

#### Suggested Evidence of Compliance

Documentation of procedures and mechanisms to properly encrypt the communications.

### 4.2.5.3 ③ ② Proof of Possession

The authentication protocol shall prove the claimant has possession of the authentication password or token. For simple passwords, this should be accomplished by successful entry of the shared secret as determined by the verifier. For one-time passwords, the ability to enter a valid "next password" is sufficient. For PKI credentials, the ability of the Subject to prove possession of the private key would be sufficient. Other types of credentials may accomplish this in different ways.

#### Suggested Evidence of Compliance

Technical documentation and mechanism to demonstrate this.

### 4.2.5.4 ③ ② Session Authentication

Session tokens shall be cryptographically authenticated. For example, session cookies must be encrypted, digitally signed, or contain a Hash-based Message Authentication Code. NIST approved cryptographic and or hash standards must be used.

#### Suggested Evidence of Compliance

Technical documentation and mechanism to demonstrate this.

### 4.2.5.5 ③ ② Stored Secrets

Secrets such as passwords or PINs shall not be stored as plaintext. Access to encrypted stored secrets and to decrypted copies shall be protected by discretionary access controls that limit access to administrators and applications that require access (see also 4.2.5.6).

Three alternative methods may be used to protect the shared secret:

1. Passwords may be concatenated to a salt and/or username and then hashed with an Approved Algorithm so that the computations used to conduct a dictionary or exhaustion attack on a stolen password file are not useful to attack other similar password files. The hashed passwords are then stored in the password file; or
2. Store shared secrets in encrypted form using Approved Encryption Algorithms and modes and decrypt the needed secret only when immediately required for authentication; or
3. Any method protecting shared secrets at NIST [SP 800-63] Level 3 or 4 may be used.

#### **Suggested Evidence of Compliance**

Documentation of the policy, procedure and mechanisms used to accomplish this, including documentation of implementation and testing.

##### **4.2.5.6 ⑤ Protected secrets**

Any secret (e.g., password, PIN, key) involved in authentication shall not be disclosed to third parties by verifier or IdP, with the following exceptions:

- Sharing of session (temporary) shared secrets may be provided by the IdP to independent systems that must verify the secret;
- Long-term secrets and session (temporary) secrets can be shared with infrastructure elements controlled by the IdP operator or managed by an entity with which the IdP operator has a contract or other written agreement that defines adequate controls to mitigate risk of inappropriate disclosure of those secrets.

#### **Suggested Evidence of Compliance**

Documentation of mechanism in place to demonstrate and ensure this.

##### **4.2.5.7 ⑤ ⑥ Mitigate risk of sharing credentials**

Measures shall be taken to reduce the risk of an identity Subject intentionally compromising his/her token to repudiate authentication. These should include one or more of the following, as appropriate:

- Periodic confirmations that identity Subjects understand and will comply with security policy requirements;
- Confirmations of sensitive on-line transactions through a separate channel (such as electronic mail);
- Reminders to identity Subjects that sharing of credential tokens is prohibited.

#### **Suggested Evidence of Compliance**

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

##### **4.2.5.8 ⑤ ⑥ Threat protection 1**

The authentication protocol must resist:

- On-line guessing – passwords or other authentication secrets must meet or exceed the required entropy and min-entropy criteria as determined using the NIST Password Entropy spreadsheet for the assurance profile being asserted.

- Replay – ensure that it is impractical to achieve successful authentication by recording and replaying a previous authentication message.

**Suggested Evidence of Compliance**

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

**4.2.5.9 ⓘ Threat protection 2**

The authentication protocol must resist an eavesdropper attack. Any eavesdropper who records all the messages passing between a claimant and a verifier or relying party must find that it is impractical (see IAAF Glossary) to learn the password or to otherwise obtain information that would allow the eavesdropper to impersonate the claimant.

**Suggested Evidence of Compliance**

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

**4.2.5.10 ⓘ Authentication protocols 1**

Authentication protocol types allowed under this IAP are:

- *Challenge-response password* – verifier sends the claimant a challenge (usually a random value or a nonce) that the claimant combines with a shared secret (often by hashing the challenge and secret together) to generate a response that is sent to the verifier.
- Any protocol allowed by the Silver IAP.

**Suggested Evidence of Compliance**

Documentation of the mechanism as implemented.

**4.2.5.11 ⓘ Authentication protocols 2**

The authentication protocol types allowed under this IAP are:

- *Tunneled password* – claimant who provides a password does so through a secure (encrypted) TLS protocol session (tunneling).
- *Zero knowledge-base password* – claimant who provides password does not tell receiver anything about the password the receiver does not already know.

**Suggested Evidence of Compliance**

Documentation including the policy, procedures and description of the mechanisms to accomplish this.

Documentation of the operational IdP system.

## 4.2.6 Identity Information Management

Identity is the set of information correctly associated with an identity Subject. Identity assurance profiles attempt to reassure a Relying Party that identity information offered by an IdP can be trusted to a known degree. The Relying Party must decide for itself whether this reassurance is sufficient for its own purposes.

### 4.2.6.1 ⑤ Identity status management

If the IdP operator is an independent service organization, identity attributes required by this IAP must be re-confirmed at a minimum frequency of every 2 years, or when notified by the identity Subject of a change.

If the IdP operator is part of a larger organization that is maintaining a continuing relationship with the identity Subject, identity attributes required by this IAP that are developed as part of that relationship and must be maintained reliably as part of the business processes for managing that continuing relationship with the Subject are assumed to be valid. Otherwise the requirement above for this factor applies.

#### **Suggested Evidence of Compliance**

Documentation of any reviews and audits to support the reliability of the identity attributes the IdP will offer to a Relying Party.

## 4.2.7 Identity Assertion Content

An identity assertion is the critical message that an IdP service sends to a Relying Party. It must be formed from reliable information and sent securely to the Relying Party. Some 'real time' information may be required in an assertion, e.g. details of the authentication event.

### 4.2.7.1 ⑤ ⑥ Identity Attributes

Identity attributes as used by InCommon are described on the InCommon Federation Attribute Overview web page. Specific attributes recommended for use by all IdPs and SPs are described on the InCommon Federation Attribute Summary web page. The actual meaning of any attribute values identified as attributes recommended for use by InCommon Participants **must** be consistent with definitions in the most recent Attribute Summary document.

#### Suggested Evidence of Compliance

Documentation of the IdP operator's service and identity management descriptions.

### 4.2.7.2 ⑤ ⑥ Identity Assertion Qualifier (IAQ)

An IdP operator may be certified by InCommon to be able to include one or more InCommon IAQs as part of identity assertions. The IdP **must not** include an InCommon IAQ that it has not been certified by InCommon to assert and **must not** include an IAQ if that identity assertion does not meet the criteria for that IAP.

#### Suggested Evidence of Compliance

IdP's documentation regarding how the IdP operator has been certified for each IAQ and how IAQs are assigned to assertions.

### 4.2.7.3 ⑤ ⑥ Cryptographic security

Cryptographic operations are required between an IdP's assertion provider and any Relying Party. Cryptographic operations shall be done in compliance with cryptographic techniques that are specified or recommended by NIST.

The identity assertion must be either:

- Digitally signed by the verifier; or
- Obtained directly from the trusted entity (e.g. the verifier) using a protocol where the trusted entity authenticates to the relying party using a secure transmission channel (e.g., TLS or SSL) that cryptographically authenticates the verifier and protects the assertion.

#### Suggested Evidence of Compliance

Documentation of the system as implemented, or a statement from the software provider or developer regarding implemented cryptographic standards.

## 4.2.8 Technical Environment

The server and database platforms used by an IdP service must be configured to resist unauthorized intrusions and disruptions. Robust or redundant platforms help ensure continuity of service. Change management helps ensure that the state of all service platforms is known at any point in time.

### 4.2.8.1 ⑤ Configuration Management

The IdP operator shall demonstrate a Configuration Management methodology that includes at least:

- a. Version control for software system components;
- b. Timely identification and installation of all applicable patches for any software used in managing or provisioning of the IdP service;
- c. Logging of all software and configuration changes.

#### Suggested Evidence of Compliance

Documentation including CM logs and other documents.

### 4.2.8.2 ⑤ Network security

1. The IdP operator shall protect their internal communications and systems with appropriate measures if such internal communications are transmitted across any shared network where the active components are not managed by the IdP operator or, if applicable, its parent organization. Such measures should mitigate against threats including eavesdropper, replay, verifier impersonation, DNS hijacking and man-in-the-middle attacks (See NIST [SP 800-63], section 8.1.1)
2. Appropriate network intrusion detection and prevention measures should be in place.

#### Suggested Evidence of Compliance

Documented protection measures for communications systems.

### 4.2.8.3 ⑤ Physical security

The IdP operator shall employ physical access control mechanisms to ensure access to sensitive areas, including areas such as leased space in remote data centers, is restricted to authorized personnel. Access logs should document both entrance and exit of individuals.

#### Suggested Evidence of Compliance

Documentation of policy, procedures and mechanisms that provide physical access controls, including:

- Lock types and key distribution and retrieval
- Access lists and logs
- Procedures for guest or one-time entry

### 4.2.8.4 ⑤ Continuity of Operations

1. The IdP operator shall employ mitigation techniques to ensure system failures do not result in false positive authentication errors.
2. The IdP operator should have a Continuity of Operations Plan (COOP) that covers disaster recovery and resilience of the IdP Subject authentication and identity

assertion service. Priority should be given to serving existing Subjects rather than registering new Subjects. If no COOP for this service exists, Subjects should be made aware of this fact.

*NOTE: Service level agreements with Subjects are not assessment criteria for this factor; they are contractual arrangements between the parties.*

**Suggested Evidence of Compliance**

1. Documentation of procedures and mechanisms that provide resistance to false positives
2. Documentation of Continuity of Operations / Disaster Recovery plan and the results from the last test of the plan or equivalent documents.



## 5 REFERENCES

For a Glossary and Acronym definitions, see the [IAAF].

[IAAF] InCommon "**Identity Assurance Assessment Framework**", version 1.0,  
September 2008

[eAuth CAP] Federal E-Authentication "**Password Credential Assessment Profile**",  
Release 2.0.0, March 16, 2005.

[SP 800-63] "**Electronic Authentication Guidelines**" NIST Special Publication 800-63-1

[Entropy spreadsheet] NIST "**PIN and Password Evaluation Spreadsheet**", version  
2.0.0 <http://www.cio.gov/eauthentication/documents/CommonCAP.xls>

[InC-Attr-Ovr] "**InCommon Federation Attribute Overview**"  
<http://www.incommonfederation.org/attributes.html>

[InC-Attr-Sum] "**InCommon Federation Attribute Summary**"  
<http://www.incommonfederation.org/attributesummary.html>

[eduPerson] "**eduPerson Object Class**"  
<http://www.educause.edu/eduPersonObjectClass/949>

## 6 DOCUMENT HISTORY

This document was developed initially by the InCommon Federation Technical Advisory Committee. The overall concept was derived from the Federal e-Authentication "Password Credential Assessment Profile" Release 2.0.0 and NIST Special Publication 800-63-1.

### Editors

David Wasley	Steven Carmody	RL "Bob" Morgan
John Krienke	Renee Shuey	Tom Barton
Karl Heins	Virginia Luke	David Walker

Status	Release	Date	Comments	Audience
Public	1.0	4 Nov 2008	First full release for implementation	Open

## Microsoft Provides Students with a Sweet Suite

*DreamSpark design and development tools available through InCommon.*



What's not to like about free software?

Particularly when it

includes professional developer tools from industry giant Microsoft? Microsoft has made its DreamSpark™ suite of software available to any college or university student in the world. Students can receive professional development and design tools at no cost. DreamSpark includes Visual Studio, Expression Studio, Windows Server and xna Game Studio.

For Microsoft, the program places key tools in the hands of young developers likely to create the next generation of applications. For students, particularly those in engineering, computer science, and other technology-driven curricula, essential software provided at no cost – well, it is better than free pizza for a month.

The key question in the process: how to verify student status in a low-cost and scalable way. The key answer turned out to be InCommon.

### The Problem

Microsoft saw value in distributing developer software, free of charge, to college students. But with thousands and thousands of students eligible for free downloads, how would the company verify enrollment in a college or university? According to Microsoft's Scott Blackwell, "This program poses the problem of identifying students in a low-overhead fashion. Some existing [Microsoft] programs work through various academic channels, but don't have the scope or consistency needed for this program."

### The Solution

For a solution, Microsoft turned to InCommon and, subsequently, other federations around the globe. Through InCommon and the use of privacy-preserving attributes, colleges and universities could verify enrollment without releasing personally identifying information about individuals. By using InCommon and attributes, Microsoft could leverage university identity management systems to determine whether a potential downloader is a student.

"We saw the emergence of global federations in higher education as a great opportunity to leverage campus

services for student-affiliation verification," Blackwell said. "We're committed to supporting federation in our own products, so it's a direction we want to promote. We worked first with our U.S. colleagues in InCommon, then with many others worldwide."

Rather than dealing with thousands of universities in the U.S. and abroad, Microsoft joined InCommon and 14 other federations, working through the policy and contract issues. The company worked with InCommon to determine which information would need to be exchanged, all the while looking to ensure a smooth and successful user experience.

*"We saw the emergence of global federations in higher education as a great opportunity to leverage campus services for student-affiliation verification."*

*Scott Blackwell,  
Microsoft DreamSpark  
Global Program  
Manager*

### The Result

Microsoft was pleased with the trust services and scalability provided by InCommon. According to Blackwell, "The success of this scheme depends on the scaling and assurance we get from working with national-level federations rather than individual campuses. We had a tremendous reaction when we launched the service. It has received a lot of attention within Microsoft and in higher education."

Microsoft has learned a lot through the process of joining and using InCommon, says Blackwell. "As seamless as the technology is, there are still lots of human relationships involved in providing a great service. Some of the technical elements are still evolving and we're working with the federations and campuses on improving practices for the next generation of the service."

### About InCommon

You can read more about InCommon on the back of this page and at [www.incommonfederation.org](http://www.incommonfederation.org).

## iTunes U: Apple is InCommon-ly Good for Universities

### *Pilot program tests iTunes U protected access through InCommon.*

Several universities and Apple have completed a successful pilot, using Shibboleth® Single Sign-on and Federating Software and the InCommon Federation, to provide federated access to iTunes U. A federated iTunes U provides universities with an ideal platform for offering online course content to students around the globe.

The goal of the pilot was to develop a standards-based, vendor-neutral approach to authenticate and authorize users of iTunes U. And leveraging a university's identity management system means only students enrolled in a specific course can access the materials.

Professors and students love iTunes U. Students can revisit a lecture and view other multi-media content made available by the professor. Professors record lectures and add related audio and video content to provide examples, background information or context for a course. Students can then listen or view the podcasts from a computer, iPod or iPhone.

Students sign on with their university ID, access iTunes U and go to school!

#### The Problem

iTunes U has proven to be a very good tool for students and faculty. Universities, however, needed a scalable solution for authentication and authorization, ensuring that only those registered for a course can gain access to materials distributed via iTunes U.

Apple provides a proprietary transfer script that allows students to authenticate with their university credentials; a script that released only the information needed to provide access. However, with more than 100 universities now members of InCommon – each potentially working with a number of service providers – the issue became one of scalability. How many vendor-specific implementations can one IT shop support?

Federating through InCommon and Shibboleth also provides an elegant solution for universities using iTunes U to provide online courses for their own students and for students from other universities.

As an example, in 2007, Penn State produced more than 3,500 podcasts for 300 courses, and that number grows every year. "We are seeing growth even without

much of a marketing effort," says Renee Shuey of Penn State's information technology services. "That's why we knew we needed the scale that InCommon brings to the university community."

"The demand is growing," said Bill Corrigan of the University of Washington. "At this point, there are a lot of students expressing desire to get more course materials online."

This growth means that any solution has to scale.

#### The Solution

Apple and the universities agreed to operate a pilot program, using InCommon and Shibboleth, to federate iTunes U. The pilot developed a way to use the standard authentication and authorization process involved with Shibboleth and federated identity, rather than Apple's transfer script, for those universities that are members of InCommon.

*"With iTunes U now supporting federated identity, we can now take next steps towards making this service the place for secure rich media digitally delivered for teaching and learning."*

*Cole Campese,  
Director of Educational  
Technology Services,  
Penn State University*

Through the use of the InCommon Federation, universities can use Shibboleth to authenticate their students, releasing only the necessary information to provide access to the course materials, and Apple will authorize access to the appropriate iTunes U content.

#### The Result

For those universities conducting the pilot, it is full steam ahead with federated iTunes U. The pilot reached its goal of successfully using InCommon and Shibboleth for the authentication and authorization of users for iTunes materials.

With this successful pilot complete, universities can now use their InCommon participation, and Shibboleth, to integrate with iTunes U.


#### About InCommon

You can read more about InCommon on the back of this page and at [www.incommonfederation.org](http://www.incommonfederation.org).

## Simplifying Career Services for Students

*InCommon provides a smart career choice*

### Penn State and Symplicity

 Symplicity provides software applications to manage many facets of college recruiting, from career fairs to on-campus interviewing. The company works with 600 institutions providing an end-to-end career service management suite.



Pennsylvania State University has thousands of students

using career services at any given time. For Penn State's 24 locations across the state, the sheer size and complexity of offering quality, unified services can be daunting.

### The Problem

Rather than develop its own system for on-line job posting and on-campus interviewing, Penn State conducted an extensive review of various vendors. The university chose Symplicity and used the company's software for a year without federated single sign-on.

During that year, every student received a user name and password – separate from their existing Penn State ID and password – to access the career services system.

"Our office was constantly receiving phone calls from students who couldn't log in to Symplicity," said Larry Kolbe, a programmer/analyst with Penn State's career services office. "We wanted to eliminate the assignment of yet another user name and password to students."

### The Solution

Penn State was already an InCommon participant, using federated identity management for other campus applications. "We were asked to investigate and implement a way to integrate access to Symplicity's system with Penn State's log-in," Kolbe said. "Because Symplicity did not, at that time, work with Shibboleth®, we worked closely with their developers to make this happen."

"Penn State approached us about a federated single sign-on system, so we Shib-enabled our applications," said Symplicity's Brent Franks. "Since then, we have started working with the University of Maryland-Baltimore County toward using InCommon and have just opened talks with NYU."

Franks said this is part of a process he has seen with other institutions. "A typical scenario is that a school will deploy Symplicity software and, after it has been up and running, begin discussion of a federated single sign-on system."

### The Result

For Penn State, the result has been a streamlined authentication and authorization system. "For the year that we used Symplicity prior to implementing this solution, we were constantly fielding phone calls from students,"

Kolbe said. "The office no longer receives these types of calls, which has resulted in significant savings in staff time."

As a service provider, Franks said it all comes down to customer satisfaction.

"Ultimately it comes down to making our customers happier, which in turn helps create sales opportunities," he said. "InCommon and Shibboleth provide a great SSO solution and make it much easier for students to use our software while allowing career services staff to concentrate on what is most important; helping students rather than troubleshooting technology issues."

### About InCommon

You can read more about InCommon on the back of this page. InCommon is operated by Internet2 and managed by an independent steering committee representing the higher education and research community. For more information visit [www.incommonfederation.org](http://www.incommonfederation.org)

*"InCommon and Shibboleth provide a great SSO solution and make it much easier for students to use our software while allowing career services staff to concentrate on what is most important..."*

*—Brent Franks, Symplicity*

## Making the Grade with InCommon

*WebAssign gives the Federation high marks.*

**WebAssign** operates a homework delivery system that has become increasingly popular with professors around the country. By harnessing the power of the Internet, WebAssign provides faculty members with the tools to create assignments from a database of textbook questions, or write and customize their own exercises. Instructors enjoy a streamlined system for making homework assignments, communicating due dates and providing feedback to students.

### The Problem

WebAssign typically works with individual professors, not with university IT departments. Professors can sign up for their own WebAssign accounts and begin using the service almost immediately. As a result, the company could have hundreds of accounts on a single campus, with no coordination of information.

In addition, the individual faculty member has responsibility for entering and updating roster information as students drop and add classes.

"The primary problem was how to enter student and roster information, including passwords, and then disseminate that information," said Brian Marks, chief technology officer at WebAssign. "What was needed was a secure, standard method of sharing such information with an external entity in a trusted way."

### The Solution

WebAssign joined InCommon as a service provider and installed Shibboleth federating software. This allowed WebAssign to stop managing user accounts and focus, instead, on the company's applications.

"The solution to sharing the information ended up being the integration of Shibboleth and InCommon with WebAssign," Marks said.

"The role of InCommon was to provide the trust layer so that institutions would feel comfortable sharing student information with us," Marks said.

That trust layer results from InCommon's federated approach, in which organizations agree on a set of privacy-preserving user attributes, technologies,

processes and policies to exchange selected user information. Users receive single sign on convenience, using the user ID and password from their home institution.

### The Result

WebAssign's InCommon university partners no longer need to upload and update rosters and other information. Students and faculty members also have Single SignOn convenience.



For example, **Penn State's** physics department help desk

saw a 70 percent drop in calls once the university installed federating software. Those calls had little to do with physics help and everything to do with forgotten passwords.

WebAssign has also seen measurable benefits from their InCommon participation, including customer confidence with the online experience.

"A primary benefit of being a member of InCommon is that the trust mechanism is already in place when another institution expresses interest in integrating their class rosters," Marks said.

*"The role of InCommon was to provide the trust layer so that institutions would feel comfortable sharing student information with us."*

—Brian Marks, WebAssign

This scalability means that WebAssign and Penn State can interact with many more organizations, using multiple applications, with relative ease.

### About InCommon

You can read more about InCommon on the back of this page. InCommon is operated by Internet2 and managed by an independent steering committee representing the higher education and research community. For more information, visit <http://www.incommonfederation.org>.



## Federation Not Small Stuff for Small Colleges

*Lafayette federates several applications; Carleton on the way.*

The benefits of federation are not limited to research universities with large IT staffs. Using InCommon and federating software, small colleges can also extend their reach and the services they provide.

### LAFAYETTE

Lafayette College has several federated applications, allowing

for both on- and off-campus access to protected resources, including library applications JSTOR and RefWorks, the open-source course management system Moodle, an internally developed DHCP application, and University Tickets.

### Carleton College

Carleton College has federated a career services application from Symplicity and is

looking at federating with a library database vendor and an emergency services provider.

#### The Problem

Lafayette continues to add online services at the behest of stakeholders, including the library, as well as faculty wishing to collaborate with their colleagues from other institutions. Providing additional services, however, could lead to a proliferation of user IDs and passwords. John O'Keefe, Lafayette's director of academic technology and network services, also wanted an uncomplicated way to provide off-campus access to services, using single sign-on technology.

Carleton College faced a similar situation when considering NACELink, a career services resource from Symplicity, as well as other online resources. Joel Cooper, director of information technology services, says, "We have other systems where students have silo passwords and there are multiple resources that require new credentials." Cooper wanted to continue to provide access to multiple protected resources without growing the number of IDs and passwords that users need to maintain.

#### The Solution

Lafayette used its InCommon membership and Shibboleth® Single Sign-on and Federating Software to provide access to protected resources. With this solution, the college was able to offer single sign-on convenience for its users and provide off-campus access to third-party applications. In the case of

Moodle, this solution also allows access for appropriate outside users.

InCommon membership allowed Carleton to federate career services resource NACELink. "Our IT staff member was looking for a career services resource compatible with our architecture and he had installed Shibboleth," Cooper said. "NACELink had all of the tools the career center wanted."

#### The Result

Lafayette's O'Keefe said, "[Shibboleth] has become our de-facto application to solve authentication issues with third-party apps, as well as internally hosted apps. Everyone is pleased that campus network IDs can be used to access more resources."

At Carleton, federating NACELink has simplified things for users — college IDs provide access to the resource. This success has caused Carleton to consider federating other protected resources. "We're actively looking at others, particularly library resources," Cooper said. "We are looking to use Shib for internal web authorization, as well."

*"InCommon provides a way for us to expand our services through third-party providers, rather than use valuable and scarce staff resources to add or maintain services."*

*Joel Cooper,  
Carleton College*

Cooper also said that federating can help a college or university strategically outsource services without consuming scarce resources.

"InCommon provides a way for us to expand our services through third-party providers, rather than use valuable and scarce staff resources to add or maintain services. Federating enables outsourcing while making it secure and transparent for our users. We can take advantage of services and applications that already exist, without having to worry about managing a different set of user accounts."

#### About InCommon

You can read more about InCommon on the back of this page and at [www.incommonfederation.org](http://www.incommonfederation.org).