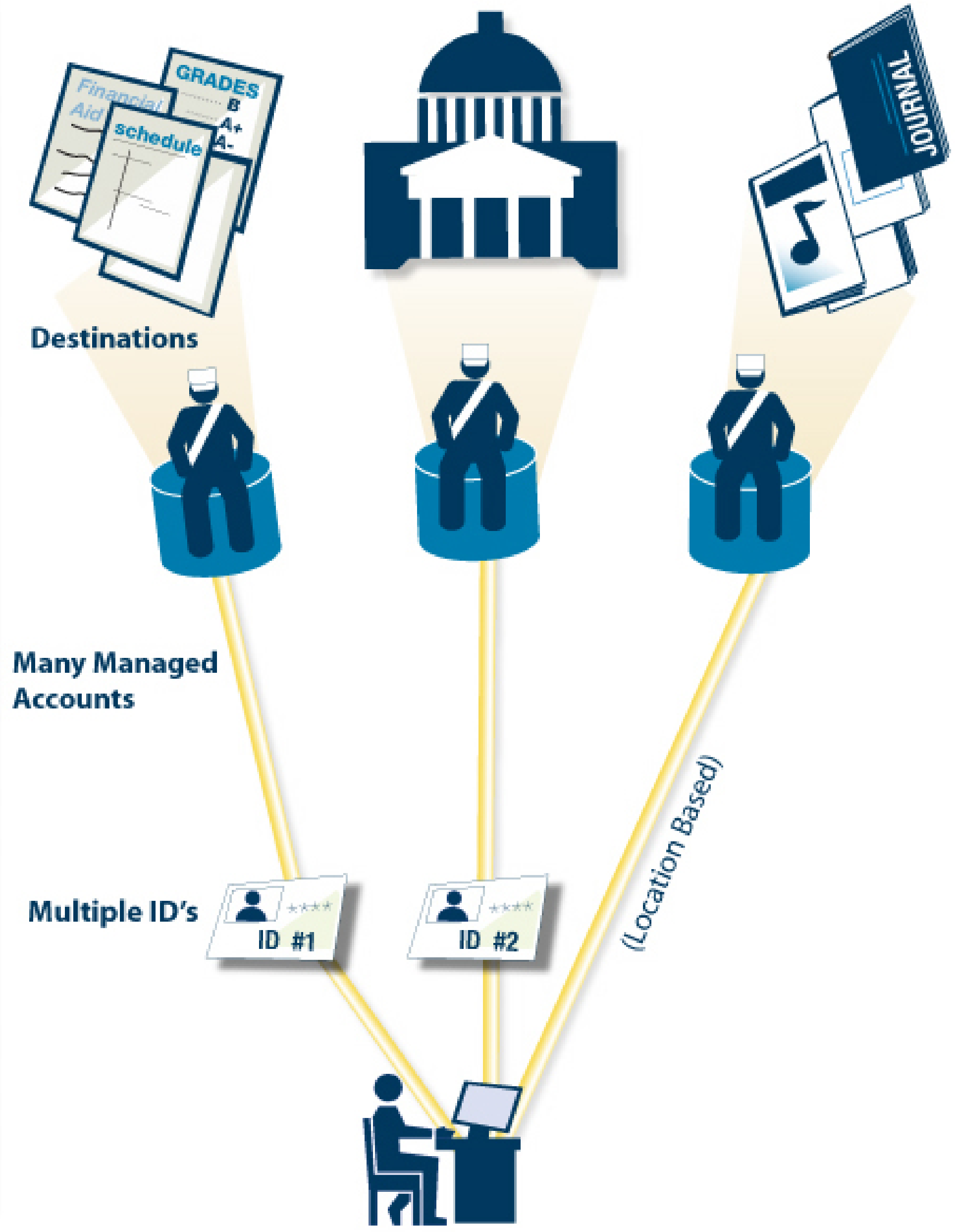
InCommon
Federated Identity Management

www.incommon.org

The Problem

- Growing number of applications – on-campus and outsourced or hosted
- All of these service providers must:
  - Verify the identity of users (faculty, staff, students, others)
  - Know who’s eligible to access the service
  - Know the student is active and hasn’t left school
- The increase in outsourced or external cloud services raises concerns about the security and privacy of the identity data by both providers and universities.



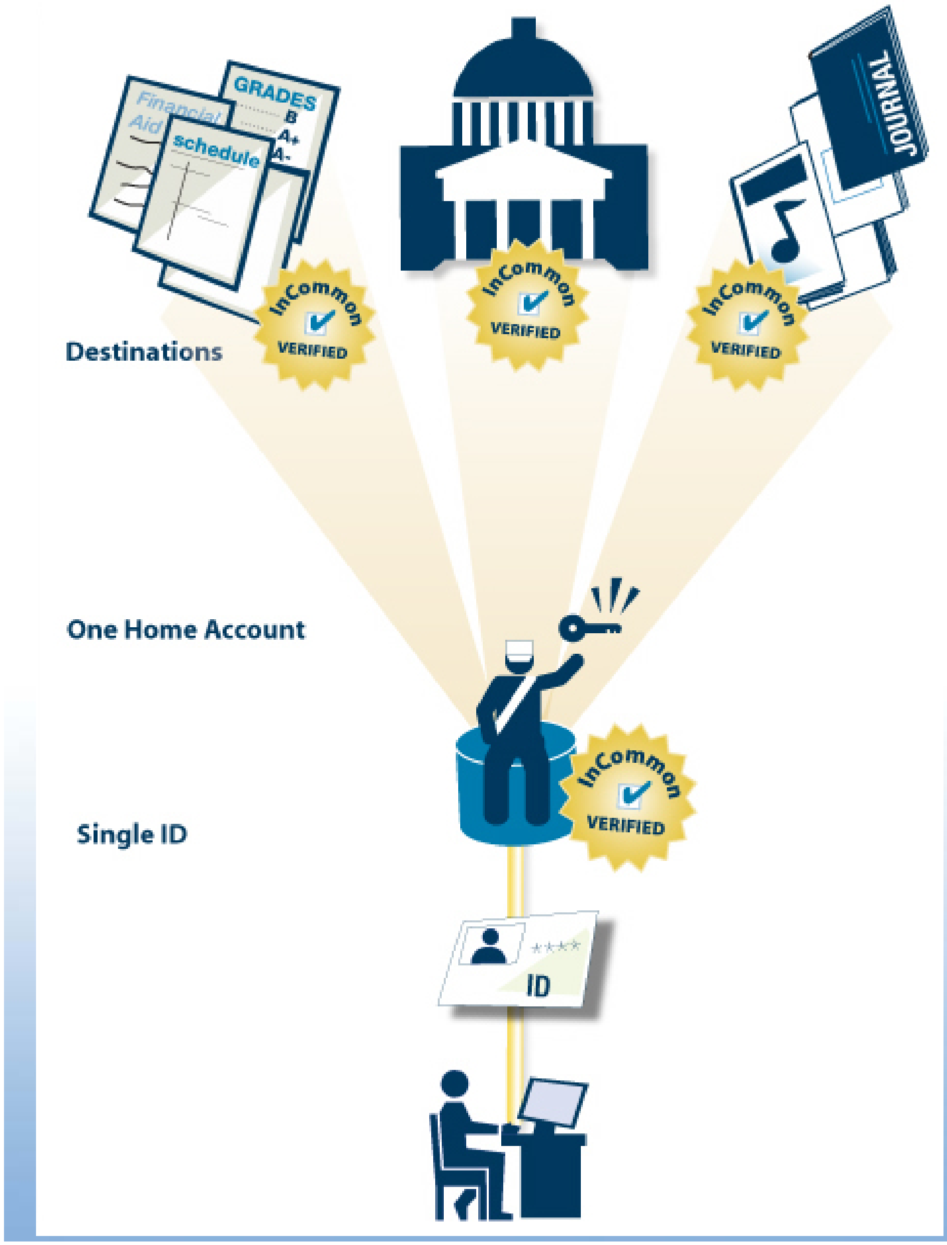
Without Federated ID

1. Users have many accounts to access needed resources
2. Access is based on user identity or location
3. Different login process at each resource
4. Many different passwords
5. Each resource provider must manage accounts / passwords
6. Lack of standards for password complexity, resets, format, etc.

The Solution: **InCommon** Federation

InCommon Federation was developed by higher education to meet our needs by:

1. **Define contractual rules:** We have developed a contract that universities and service providers agree too as members.
2. **Technical architecture:** The reference architecture for operation and interchange of **Attributes** – agreed upon data elements.
3. **Governance:** How we evolve over time to meet new requirements and opportunities.



With Federated ID

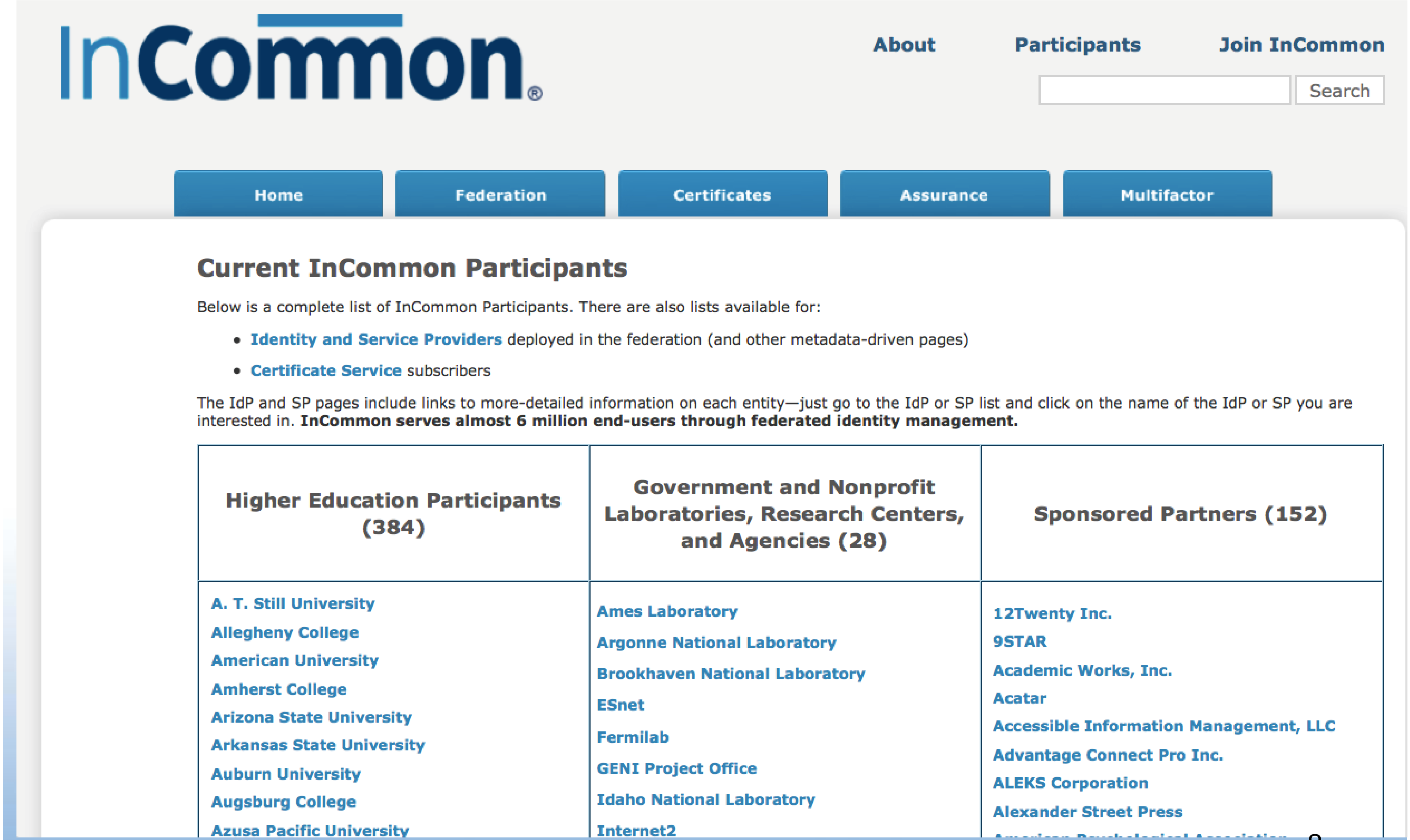
- Users have single account to access the resources they need
- Access is based on trusted credentials from user' institution
- No overhead requirement for resource provider to manage accounts / passwords
- Private Information from user institution can be passed to resource as needed rather than having resource store it

InCommon

- **InCommon is:**
  - A wholly owned not-for-profit LLC of Internet2 created to support federated authentication with a board from higher ed.
  - Based on open international standards (SAML).
  - Focused on higher education institutions and service providers working with higher education institutions.
  - Working closely with the Federal government to provide government services to universities.
- **InCommon isn't:**
  - A vendor.
  - Focused on services outside the mission of research & education.

InCommon Facts

- Fact: InCommon has more than 7 million higher education users across its members.
- Fact: InCommon membership has increased by 50% yearly for several years and now is at 550 participants.
- Fact: InCommon higher education members include institutions of all sizes, including community colleges, research universities, and small liberal arts colleges.
- Fact: InCommon technology is based on standards being adopted globally by over 30 countries.



Current InCommon Participants

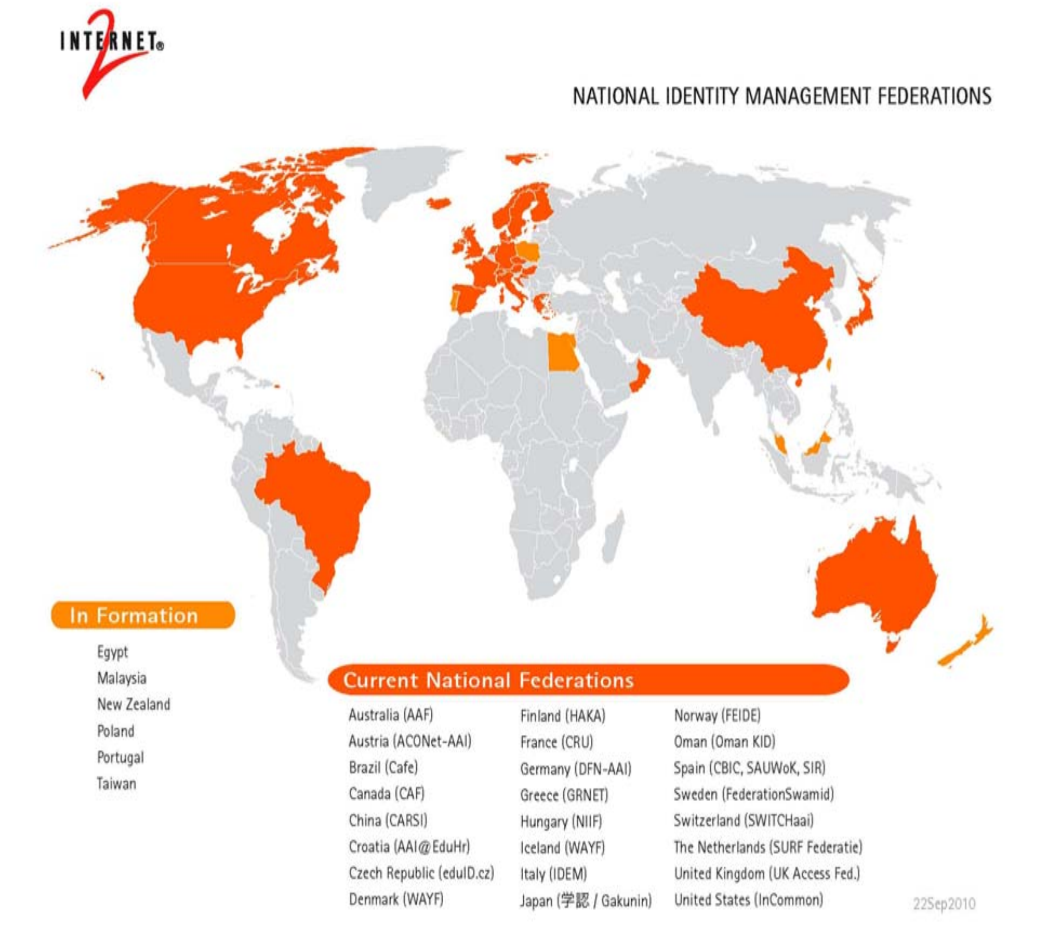
Below is a complete list of InCommon Participants. There are also lists available for:

- **Identity and Service Providers** deployed in the federation (and other metadata-driven pages)
- **Certificate Service** subscribers

The IdP and SP pages include links to more-detailed information on each entity—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in. **InCommon serves almost 6 million end-users through federated identity management.**

Higher Education Participants (384)	Government and Nonprofit Laboratories, Research Centers, and Agencies (28)	Sponsored Partners (152)
A. T. Still University	Ames Laboratory	12Twenty Inc.
Allegheny College	Argonne National Laboratory	9STAR
American University	Brookhaven National Laboratory	Academic Works, Inc.
Amherst College	ESnet	Acatar
Arizona State University	Fermilab	Accessible Information Management, LLC
Arkansas State University	GENI Project Office	Advantage Connect Pro Inc.
Auburn University	Idaho National Laboratory	ALEKS Corporation
Augsburg College	Internet2	Alexander Street Press
Azusa Pacific University		American Psychological Association

Federations Worldwide



INTERNET2®

NATIONAL IDENTITY MANAGEMENT FEDERATIONS

In Formation

Egypt
Malaysia
New Zealand
Poland
Portugal
Taiwan

Current National Federations

Australia (AAF)
Austria (ACONet-AAI)
Brazil (Cafe)
Canada (CAF)
China (CARSI)
Croatia (AAI@EduHr)
Czech Republic (eduID.cz)
Denmark (WAYF)

Finland (HAKA)
France (CRU)
Germany (DFN-AAI)
Greece (GRNET)
Hungary (NIIF)
Iceland (WAYF)
Italy (IDEM)
Japan (学認 / Gakunin)

Norway (FEIDE)
Oman (Oman KID)
Spain (CBIC, SAUWoK, SIR)
Sweden (FederationSwamid)
Switzerland (SWITCHaai)
The Netherlands (SURF Federatie)
United Kingdom (UK Access Fed.)
United States (InCommon)

22Sep2010

Future Proofing Access

- The world is changing:
  - Federal initiatives such as FICAM that seek to address 3rd party access to federal resources.
  - Public-private partnerships such as NSTIC that seek to create standards in other sectors.
  - New requirements for security, such as second factor requirements.
  - Increasing concern over user privacy.

InCommon Initiatives

- **Assurance:** FICAM certification for universities to access federal resources.
- **NSTIC:** We actively participate and share our work with NSTIC.
- **Multi-Factor:** We now have support for institutionally-defined multi-factor support using a variety of devices, including your cell phone!
- **Privacy:** 2 million NIST grant to develop advanced user privacy controls into InCommon.

InCommon Resources

- Overview – http://incommon.org/
- Particpants – http://incommon.org/participants
- Assurance – http://incommon.org/assurance
- Multi-factor: http://incommon.org/multifactor
- Certificates – http://incommon.org/certificates

Other Resources:

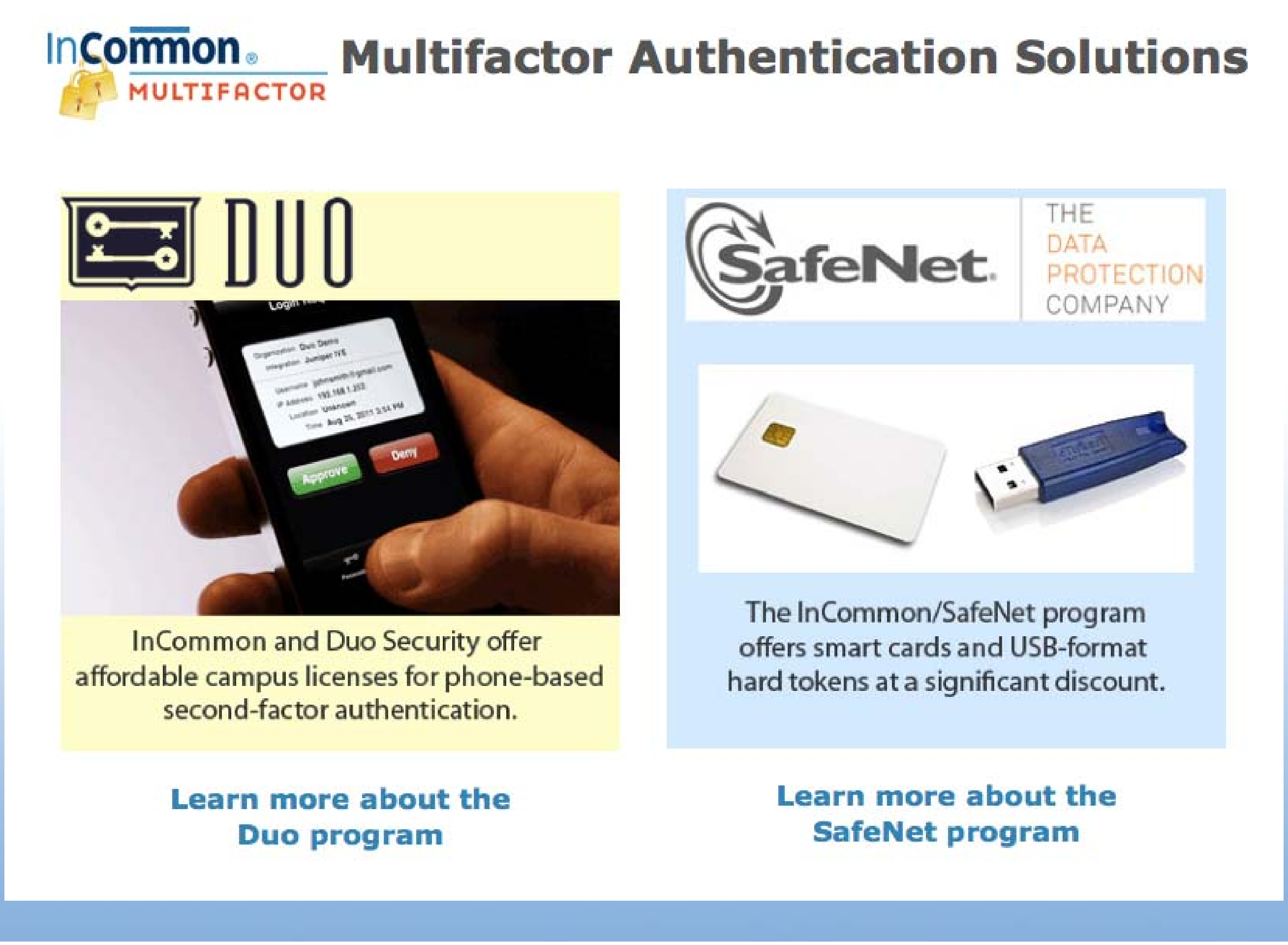
- NSTIC – http://www.nist.gov/nstic
- IDESG – http://idecosystem.org/

InCommon and Federated Identity Management

www.incommon.org

info@incommon.org

Multi-Factor



Multifactor Authentication Solutions

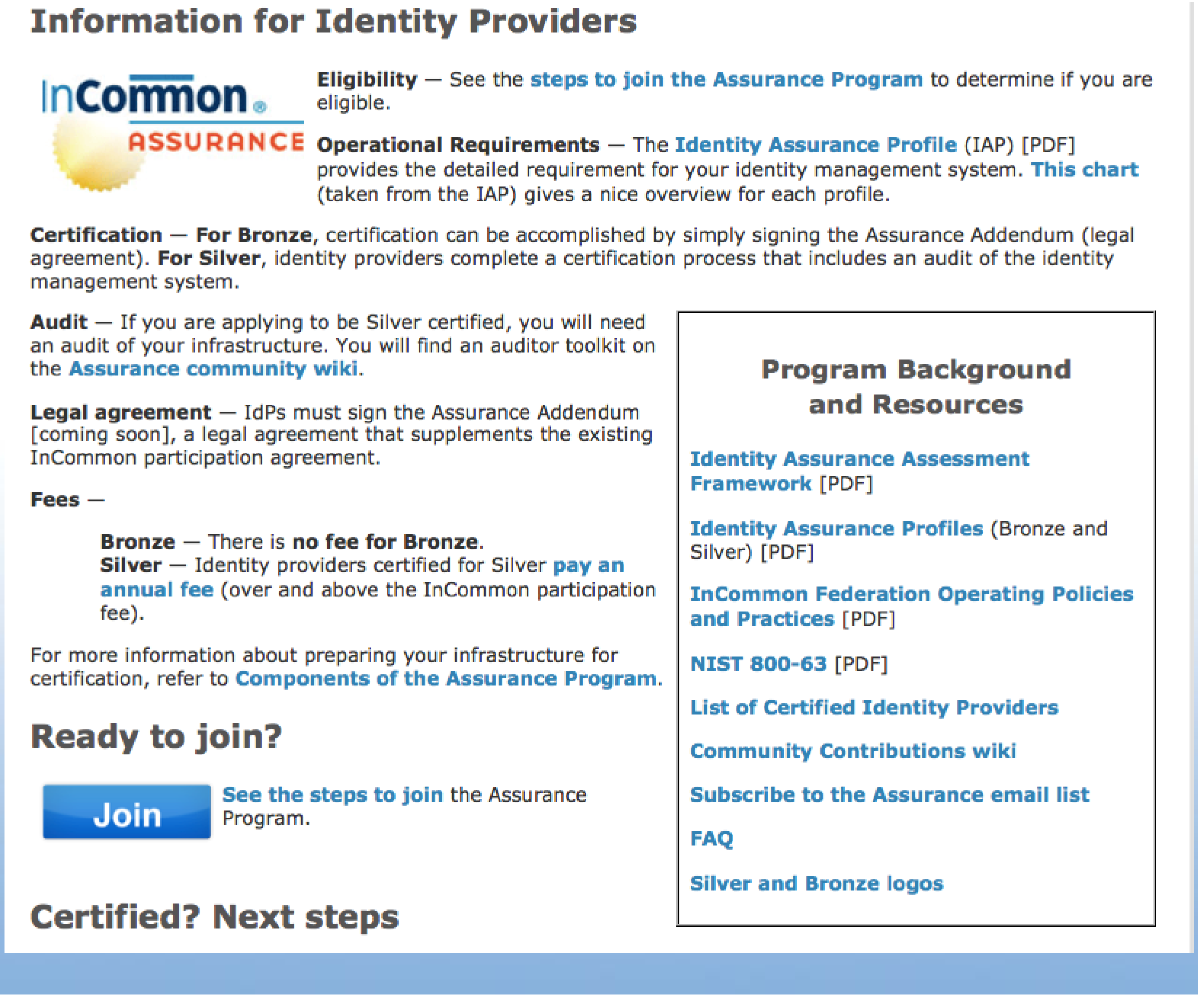
InCommon and Duo Security offer affordable campus licenses for phone-based second-factor authentication.

The InCommon/SafeNet program offers smart cards and USB-format hard tokens at a significant discount.

Learn more about the Duo program

Learn more about the SafeNet program

Assurance



Information for Identity Providers

Eligibility — See the **steps to join the Assurance Program** to determine if you are eligible.

Operational Requirements — The **Identity Assurance Profile** (IAP) [PDF] provides the detailed requirement for your identity management system. **This chart** (taken from the IAP) gives a nice overview for each profile.

Certification — **For Bronze**, certification can be accomplished by simply signing the Assurance Addendum (legal agreement). **For Silver**, identity providers complete a certification process that includes an audit of the identity management system.

Audit — If you are applying to be Silver certified, you will need an audit of your infrastructure. You will find an auditor toolkit on the **Assurance community wiki**.

Legal agreement — IdPs must sign the Assurance Addendum [coming soon], a legal agreement that supplements the existing InCommon participation agreement.

Fees —

> **Bronze** — There is **no fee for Bronze**.
> **Silver** — Identity providers certified for Silver **pay an annual fee** (over and above the InCommon participation fee).

For more information about preparing your infrastructure for certification, refer to **Components of the Assurance Program**.

Program Background and Resources

Identity Assurance Assessment Framework [PDF]

Identity Assurance Profiles (Bronze and Silver) [PDF]

InCommon Federation Operating Policies and Practices [PDF]

NIST 800-63 [PDF]

List of Certified Identity Providers

Community Contributions wiki

Subscribe to the Assurance email list

FAQ

Silver and Bronze logos

Ready to join?

See the steps to join the Assurance Program.

Certified? Next steps

NIST NSTIC

NSTIC Animated Video

National Strategy for Trusted Identities in Cyb...