

The InCommon Federation

The U.S. Access and
Identity Management Federation

www.incommon.org

Value of Federation

- Participants exchange information in a standardized format.
- Once an organization is a participating member, setting up a new relationship can take as little as a few minutes.
- Community-based collaboration and support.
- Use of a common authentication and authorization software provides single sign-on convenience.
- Interchange of agreed upon attributes hides the underlying complexity or differences between software systems at each location.

Federation Example - InCommon

- InCommon uses SAML-based authentication and authorization systems (such as Shibboleth®) to enable scalable, trusted collaborations among its community of participants.
- Several open-source and vendor products support SAML and interoperate including those offered by Internet2 (Shibboleth), IBM (Tivoli), Oracle, Sun, and CA (Siteminder).

The Challenging Way



Fire District

joe@district1.g

Dr. Joe Oval
Badge No.
SSN 456.78.910

Homeland Security
ID #2 Joval
Dr. Joe Oval
Badge No.
SSN 456.78.910
Password #2

Service Providers



Chemical Spill
ID #3 Jo456
Dr. Joe Oval
Chem. Engr
Password #3



No coordination

Proprietary code

Batch uploads

EMT Protocols
ID #4 j.o.123
Joe Oval
Badge No.
DOB: 4/4/1955
Password #4



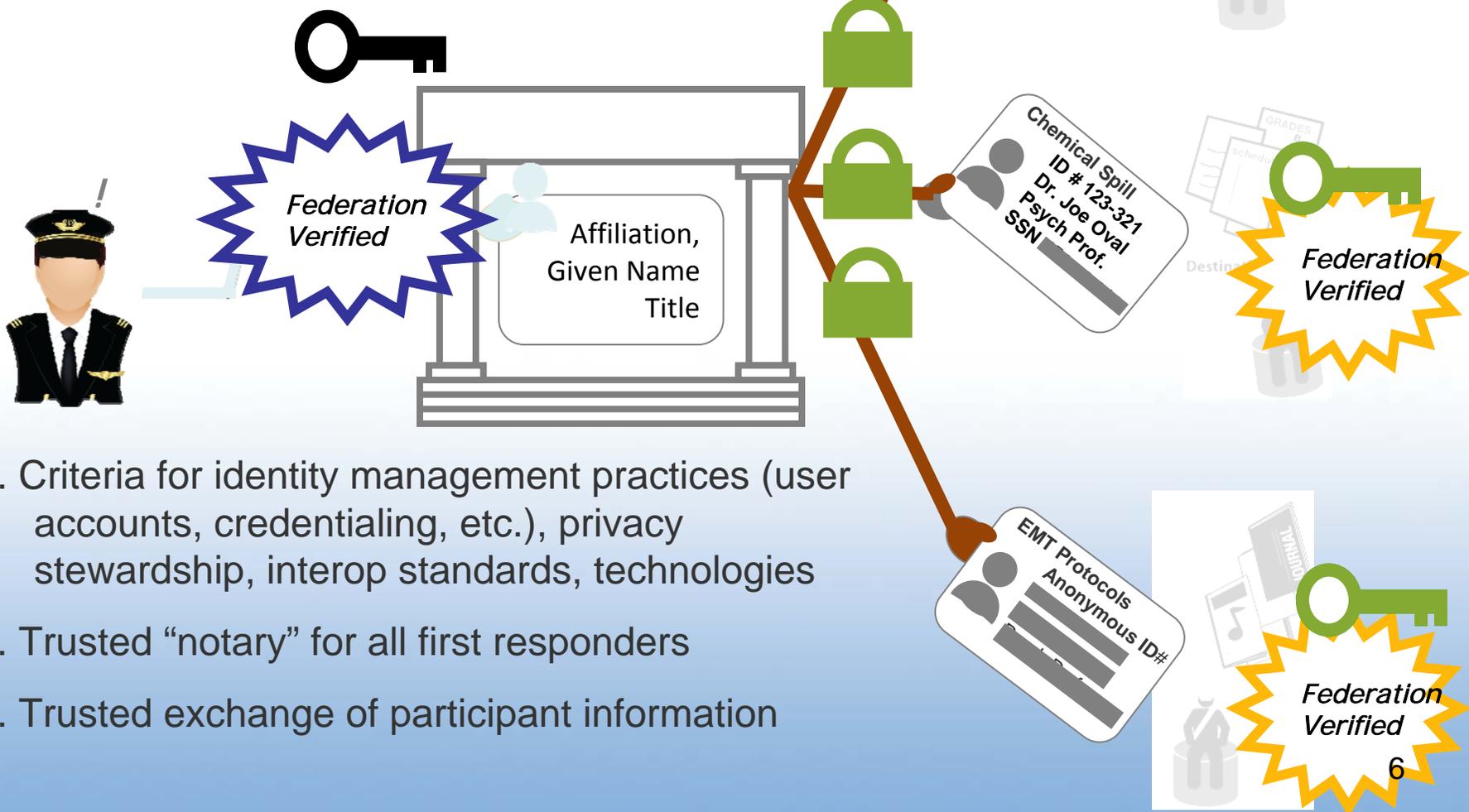
The Federated Way



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

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 first responders
4. Trusted exchange of participant information

Federated Access in 30 seconds

4. If attributes are acceptable to resource policy, access is granted!

3. Authorization: Privacy-preserving exchange of agreed upon attributes

2. Federation-based trust exchange to verify partners and locations

1. Authentication: single-sign-on at home institution



Online Resource

Attributes: Anonymous ID, Staff, Student, ...

Metadata, certificates, common attributes & meaning, federation registration authority, Shibboleth



Home District – user signs in

InCommon and the Federal Government

- Worked closely with GSA to provide feedback on the new federal trust framework.
 - GSA
 - Federal CIO Council (FCIOC)
 - Information Security and Identity Management Committee (ISIMC)
 - Program oversight by Identity, Credential and Access Management Subcommittee (ICAMSC)
- Can leverage trust framework based on OMB's M-04-04 (risk management) and NIST 800-63 (electronic authentication guidelines).