

Safeguarding Digital Identity: The SPICI (Sharing Policy, Identity, and Control Information) Approach to Negotiating Identity Federation and Sharing Agreements

Deborah Bodeau
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730
1-781-271-8436
dbodeau@mitre.org

ABSTRACT

To perform key business functions, organizations in critical infrastructure sectors such as healthcare or finance increasingly need to share identifying and authorization-related information. Such information sharing requires negotiation about identity safeguarding policies and capabilities, as provided by processes, technologies, tools, and models. That negotiation must address the concerns not only of the organizations sharing the information, but also of the individuals whose identity-related information is shared. SPICI (Sharing Policy, Identity, and Control Information) provides a descriptive and analytic framework to structure and support such negotiations, with an emphasis on assurance.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: Security and protection

General Terms

Security

Keywords

Identity Management, Identity Federation, Information Sharing, Credentials

1. INTRODUCTION

To perform key business functions, organizations in critical infrastructure sectors such as healthcare or finance

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or to publish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IDTrust 2009, April 14-16, 2009, Gaithersburg, MD, U.S.A.
Copyright© 2009 ACM 978-1-60558-474-4...\$5.00

increasingly need to share identifying and authorization-related information. Thus, organizations increasingly need to negotiate agreements for identity federations or other sharing of identifying and/or authorization-related information. Such negotiations cover, among other topics, identity safeguarding policies and capabilities required to implement policies, provide agreed-upon functionality, and thus meet business needs while managing risks.¹

Negotiations that lead to contractual or other documented agreements to share identity-related information must address the concerns not only of the organizations sharing the information, but also of the individuals whose identity-related information is shared. A common framework for assessing potential harms – to the partnering organizations that share and rely upon identifying information and to the identified individuals – facilitates agreement on a risk-appropriate level of assurance.

The SPICI (Sharing Policy, Identity, and Control Information) approach is being developed under the Institute for Information Infrastructure Protection (I3P) Safeguarding Digital Identity project [1]. SPICI is intended to help organizations identify the capabilities they need, and to negotiate how they will provide those capabilities via technologies and business processes, so that they can share identity and supporting information in a way that protects individual privacy as well as organizational interests. Thus, SPICI complements, and provides a usage context for,

¹ Identity safeguarding capabilities are organizational abilities to create, protect, share, use, and manage identity and/or authorization-related information in a way that safeguards individual privacy and protects organizational interests, using a combination of processes, technologies, tools, and models. For brevity, the term “capabilities” is used.

automated negotiation systems that can implement organizational agreements [2, 3].

SPICI provides a structure in which

- The concerns of stakeholders, including organizational users of identity information, individuals, and oversight bodies, are expressed as overarching goals and objectives for sharing identity and credential information in an appropriately protected manner.
- Identity safeguarding capabilities that organizations can use to manage and share identity, policy, and control information (particularly as represented by digital credentials) in a protected way are defined. These capabilities are motivated by related to the overarching goals of Unambiguous Identification, Assured Authentication, Accurate Authorization, Privacy Protection, and Accountable Trust and to the more specific objectives that derive from those goals.
- Four levels of assurance are defined for capabilities specifically related to sharing identity and credential information. The recommended identity safeguarding capability assurance level depends on organizational and privacy concerns.

More specifically, SPICI consists of a descriptive framework, an analytic framework, and a process. The SPICI descriptive framework identifies five goals for sharing identifying and authorization-related information (and the policy and control information needed to support that sharing), a set of objectives for technologies and/or business processes used for such sharing, and a set of capabilities which can be implemented in IT products and/or via business processes to achieve those goals. The SPICI descriptive framework also defines four capability levels (weak, basic, strong, and enhanced); these levels can be achieved by business processes and/or technologies (e.g., prototype tools, IT products). The SPICI analytic framework also defines levels of potential harms associated with sharing identifying and authorization-related information, and maps those levels of harm to capability levels. The SPICI process uses the descriptive and analytic frameworks to support negotiation of identity federation agreements, or of agreements for other forms of sharing identifying and authorization-related information.

2. BACKGROUND

Sharing of identity information, particularly in the form of easily propagated digital credentials, raises privacy as well as business concerns. The consequences to individuals of privacy violations range from minor embarrassment or inconvenience to identity theft, misdelivery of medical services leading to injury or death, or misapprehension by law enforcement. Sharing of identity and credential information also raises concerns for the organizations that

handle such information. Consequences to organizations can include damage to reputation or business relationships, as well as legal liability or financial costs associated with identity fraud or error.

To address these concerns, organizations must share more than identity or authorization-related information. They must also communicate their associated policies for using and protecting that information. For example, an organization that provides identity information might communicate its retention policy: how long shared identity information may be retained. To enable policy enforcement, the organization also needs to share control information (e.g., start date for the allowable retention period). Credentials can include policy and control information (e.g., period of validity), or such information can be shared using another mechanism.

Via negotiation, organizations determine what capabilities they will use to share identity- and authorization-related, and supporting policy and control, information. The set of technologies for managing identity information and credentials is large and growing. These are increasingly supported by technical, architectural, or assurance frameworks intended to facilitate specification and assessment of capabilities. However, these frameworks were not designed to facilitate analysis and negotiation. Furthermore, as discussions with stakeholder organizations have repeatedly highlighted, technical problems are frequently overshadowed by the challenges of establishing trust among organizations, by aligning policies and business processes.

SPICI takes into consideration the findings and recommendations of the Identity Theft Prevention and Identity Management Standards Panel (IDSP, [4]). SPICI is informed by existing identity management and identity federation frameworks, in particular the E-Authentication Guidance [5, 6], the Liberty Identity Assurance Framework (LIAF, [7]) and the framework [8] produced by the Focus Group on Identity Management (FG IdM) of the International Telecommunications Union – Telecommunication Standardization Sector (ITU-T).

The IDSP, E-Authentication, Liberty, and FG IdM work all define or rely upon an identity life cycle. The life cycle for identity and credential information defined by SPICI builds upon these high-level life cycles. However, SPICI considers identity- and authorization-related information (and supporting policy and control information) solely in digital form. Hence, SPICI does not consider issuance of foundational documents (e.g., birth certificates) or subsequent credentials in physical form (e.g., drivers licenses).

3. NEGOTIATING IDENTITY FEDERATION AGREEMENTS

Organizations that negotiate identity federation agreements (or other identity information sharing agreements, such as a Circle of Trust in the Liberty model or a simple bilateral agreement) need to address such topics as:²

- **Identity Assurance:** How confident can or should the federation or information sharing partners be that identified individuals actually exist and are distinctively identified; that credentials are correctly and securely managed and delivered; that attributes are meaningful and correct; and that identity and credential information is protected and accountable?
- **Trust Relationships:** How much trust does a given federation or sharing partner have in its credential service provider, in the federation as a trusted third party for the organizations in the federation, in another federation partner, in other federations in which the given organization participates, and in other federations in which other federation partners participate? To what extent do trust relationships depend on the business model and business rules (e.g., rules for compliance monitoring or auditing)?
- **Attributes:** What attributes are needed to make authorization-related decisions about identified individuals? What are the semantics of those attributes? How confident can or should the federation partners be in the quality (e.g., timeliness, correctness) of shared attributes?
- **Privacy and the Use of Personally Identifiable Information (PII):** How are the Fair Information Practice Principles³, as they apply to identifying or authorization-related information, interpreted within the federation or among the partners in identity information sharing? What legal and/or regulatory requirements apply to the identifying or authorization-related information? How confident are federation or sharing partners that these principles and regulatory requirements are interpreted and met consistently?
- **Technologies and Terminology:** What technical standards are used for identity data representation, for

policy representation and enforcement, for control data representation and use, and for communications between partner systems? What terminology is common to federation or other sharing partners, for roles and responsibilities; for identity and authorization-related attributes, policies, and control information; for information sensitivity and criticality; and for potential harms and corresponding risk mitigations?

- **Business Models and Business Rules:** How does the identity information sharing or identity federation relate to the business processes and models of the federation or sharing partners? In the case of a federation, how are the costs of operating the federation recovered? What service level agreements (SLAs) related to shared identifying or authorization-related information are needed to support the business processes of federation or sharing partners? What transparency standards apply, and how are they implemented (e.g., by sharing or review of audit trails)? What liability is accepted or disclaimed, and what enforcement procedures are implemented?

Answers to questions in these areas constrain the choice of technical solutions. The SPICI process uses the SPICI descriptive and analytic frameworks to provide a starting point for negotiating agreements in a way that makes explicit the concerns that drive or constrain the choice of technical solutions.

4. THE SPICI PROCESS

SPICI provides a descriptive and an analytic framework that organizations looking to form, join, or evolve an identity federation can use to identify issues about capabilities that they will need to negotiate, and to frame the discussion of those issues. The following paragraphs sketch the process for using SPICI to support analysis and negotiation. The process takes the form of a facilitated discussion, in five stages.

1. **Describe Business Process Needs.** Organizational representatives – typically the business process owners, and the technologists who support them – briefly describe the *business processes* that require sharing identifying or authorization-related information. They characterize or describe the *identifying or authorization-related* information they need or plan to share with each other. They indicate how they intend to *use* federated or shared identity or credential information. Examples of uses include: to identify an individual, to authenticate an asserted identity, to decide whether to provide a restricted service to an authenticated individual, to personalize the individual's interactions with their services, to market additional services to the individual, and to track an individual's

² This list of topics is derived from the Internet2 Federation Soup report [9], the Liberty Alliance legal framework for a Circle of Trust [10], and published examples of federation agreement templates.

³ Fair Information Practice Principles are “widely-accepted principles regarding the collection, use, and dissemination of personal information” [11]. While many different versions have been articulated, the principles usually address notice, consent or choice, access and redress, and security.

use of their services (for purposes of charging, to provide additional dynamic personalization, for auditing and compliance). They identify the types of other organizations with which they expect to *share* the information. They might also indicate how they plan to *protect* the information as it is sent to them, as they send it to another organization, and/or in storage. They might also indicate their expectations and plans about *accuracy or data quality*. (Thus, to a large extent, they answer the questions that would arise if they were drafting a Privacy Notice for the identity- and/or authorization-related information.)

2. **Assess Concerns or Potential Harms.** Organizational representatives then identify and assess the potential harms associated with the identity- or authorization-related information they provide to and/or get from the federation. Business process owners identify and assess potential harms related to their business processes; other organizational stakeholders identify and assess other potential harms. For example, a Chief Privacy Officer (CPO) might address the harms related to identified individuals, while a representative of the organization's Legal department might consider the harms related to unauthorized disclosure and to possible civil and criminal violations, and an organizational risk manager might consider financial and reputational harms. They might capture those assessments in table form, or using a spreadsheet or database. (Under the I3P project, a spreadsheet tool has been prototyped.) They could structure and normalize their assessments using the sets of threats and harms provided in the SPICI report. Note that harms can be assessed for different groupings of identity or authorization-related information; for example, if only one field in a credential is highly sensitive, it could be described and assessed separately from the rest of the credential. This lays the foundation for selective application of capabilities and technologies.
3. **Review Recommended Capabilities.** Based on these assessments, each organization will have a profile of recommended capabilities and levels. Many of those capabilities are defined by the LIAF. However, some capabilities are related specifically to the *sharing* of identifying or authorization-related information. SPICI defines six such capabilities, and (via the framework of goals, objectives, and capabilities discussed below) explains how they and the LIAF capabilities relate. The non-technical organizational representatives check that the recommendations make sense, and fine-tune the description or assessment as they deem appropriate to reflect their organizations' risk appetite.
4. **Negotiate Capability Implementation.** The technologists among the organizational representatives are now well positioned to start talking about how they

can implement (and assure their partners in the federation that they provide) the recommended capabilities. The definitions of the different assurance levels for the six SPICI-value-added capabilities can help guide those discussions, and help identify areas for more detailed negotiation and planning. In addition, SPICI identifies (but does not define assurance levels for) other capabilities; the negotiation can result in definitions of, and recommendations for, agreed-upon assurance levels of those additional capabilities.

5. **Negotiate Additional Considerations.** The organizational representatives must also define shared or cross-organizational processes (e.g., data correction, dispute resolution), legal and financial risk management, and (in the case of a federation) the federation business model. This negotiation, while crucial, is not the focus of SPICI.

5. SPICI DESCRIPTIVE FRAMEWORK

SPICI defines five overarching goals for sharing policy, identity, and control information:

- **Unambiguous Identification:** A user of identity or credential information (more specifically, a service provider, i.e., an entity that provides a service to individuals, such as an organization, a system, an application, or a Web service) should be able to distinguish one individual from another well enough to make decisions regarding and establish accountability for actual or attempted uses of services.
- **Assured Authentication:** A user of identity or credential information should be able to determine the identity or authorization-relevant attributes of an individual with assurance appropriate to the potential harms of misdelivered services.
- **Accurate Authorization:** A user of identity or credential information should be able to determine whether an individual is authorized to use that service with assurance appropriate to the potential harms of misdelivered services.
- **Privacy Protection:** A user of identity or credential information should handle the information regarding an individual that it maintains or uses with care sufficient to protect the individual's privacy. Privacy protection can be characterized in more detail by using the Fair Information Practice Principles.
- **Accountable Trust.** Identified individuals, and organizational providers and users of identifying and authorization-related information, should be able to explain defensibly (i.e., to give an account of) why they trust one another to the extent that they do.

Based on these goals, and on information life cycle models, SPICI defines a set of objectives, and capabilities

for achieving those objectives. Capabilities defined by other frameworks and initiatives (in particular, the LIAF) fit into this framework. SPICI currently defines six capabilities which are not addressed by other frameworks but are crucial to achieving the objectives.

For ***Unambiguous Identification***, the *objectives* and capabilities are:

- ***Identity Specification***: Within the scope of the identification problem, each individual can be uniquely characterized. Capabilities: Assignment of Subject Identifier / Attributes, Assignment of Service Provider Identifier / Attributes. These capabilities are well addressed by the LIAF.
- ***Identity Resolution*** : The unique characterization of an individual can be constructed (or reconstructed) from identifying and/or authorization-related information. Capabilities: Identity Attribute Correlation. As defined in SPICI, this is the capability to determine, to a specified or calculable degree of confidence, that presented credentials or sets of presented identifying information correspond to the same individual by correlating or matching presented values with known attributes, possibly by relying upon credentials issued using the LIAF.
- ***Initial Identity / Attribute Verification***: The association of identifying and/or authorization-related information with an individual is verified. Capabilities: In-Person Verification, Remote Evidence-Based Verification. These capabilities are well addressed by the LIAF.

For ***Assured Authentication*** (which could be more precisely called Assured Credential Authentication), the *objectives* and capabilities are:

- ***Credential Binding***: The credential is bound to the individual and/or to the transaction that the individual requests. Capabilities: Individual Binding, Transactional Binding.
- ***Credential Property Validation***: The expected properties of the credential are validated. Capabilities: Conditional Property Validation, Procedural Property Validation.
- ***Credential Status Validation***: The status of the credential (in particular, whether or not it has been revoked) can be determined. Capabilities: Conditional Status Validation, Procedural Status Validation.

For ***Accurate Authorization***, the *objectives* and capabilities are:

- ***Authorization Attribute Comprehensibility***: The intended meaning of attributes used to make authorization decisions can be discerned; the attributes cannot easily be misconstrued. Capabilities: Common Vocabulary, Mutual Understanding via Common

Attribute Syntax and Semantics. As defined in SPICI, Mutual Understanding is the capability to use syntactic and semantic rules (e.g., policy interpretation rules, rules for combining attributes) to provide a common understanding of well-founded uses of authorization-related information.

- ***Authorization Attribute Quality***: The quality (e.g., accuracy, currency) of attributes used to make authorization decisions can be determined. Capabilities: Attribute Quality Specification, Attribute Quality Assurance.
- ***Authorization Attribute Validation***: The validity of attributes used to make an authorization decision can be assessed in the context of the decision. Capabilities: Conditional Identity/Attribute Validation, Internal Attribute Validation. As defined in SPICI, Conditional Identity / Attribute Validation is the capability to validate, and make authorization decisions based on, authorization-related information using conditions that involve information not in the credential (e.g., history-based conditions such as Chinese Wall, location-based conditions, time-based conditions, conditions asserted by credential issuers).

For ***Privacy Protection***, the *objectives* and capabilities are:

- ***Notice and Consent***: Identified individuals are provided with notice of the intended and expected uses of identifying information, and are given the opportunity to consent to uses as appropriate. Capabilities: Notice, Consent.
- ***Usage Restriction***: Uses of identity and credential information are restricted to those to which identity information providers and identified individuals consent. Capabilities: Agreement on Terms of Use, Conditional Use. As defined in SPICI, Agreement on Terms of Use is the capability to validate agreement to the terms of use for shared identity and authorization-related information as a precondition for sharing it.⁴
- ***Disclosure / Exposure Restriction***: Identity and credential information is disclosed, or exposed to observation, only in accordance with restrictions to which credential providers and identified individuals consent. Capabilities: Selective Disclosure/Retrieval

⁴ *Terms of use* for information are statements about restrictions and obligations applicable to any individual or organization that handles the information. Terms of use can include how the information may or may not be used (e.g., for what purposes, in combination with what other information, for how long), with whom else the information may or may not be shared, how the information must be protected, and what accountability for using or sharing the information is needed.

Protection, Onward Transfer Restriction, Transmission Protection. As defined in SPICI, Selective Disclosure / Retrieval Protection is the capability to provide in, or derive from, credentials only such identity or authorization-related information as is required for agreed-upon business processes.

- *Retention Restriction*: Retention of identity and credential information is restricted to the duration and conditions to which credential providers and identified individuals consent. Capabilities: Conditional Retention Restriction, Procedural Retention Restriction.

For *Accountable Trust*, the *objectives* and capabilities are:

- *Policy Specification and Enforcement*: The policies related to the collection, use, sharing, retention, maintenance, and destruction of identity-related information are transparent and effective. Capabilities: Policy Specification, Policy Enforcement.
- *Trust Specification*: Users of identity and credential information are able to state the extent to which they can or wish to trust its source. Capabilities: Trust Designation, Trust Assessment, Trust Accreditation.
- *Accountability*: Organizations and individuals are accountable for their handling and use of identity and credential information. Capabilities: Accountability for Creation/Collection, Accountability for Use, and Accountability for Disclosure/Sharing, which is the capability to provide accountability for the onward transfer⁵ of identity or authorization-related information.
- *Recourse*: Organizations that handle or use identity or credential information provide recourse processes to individuals and/or oversight bodies. Capabilities: Access/Correction Process, Violation/Non-Compliance Recourse.

SPICI defines assurance levels for the six capabilities it defines (Identity Attribute Correlation, Mutual Understanding, Conditional Identity/Attribute Validation, Agreement on Terms of Use, Selective Disclosure/Retrieval Protection, and Accountability for Disclosure/Sharing). Higher levels give greater confidence that the corresponding goals and overarching objectives will be achieved. SPICI capability levels are defined consistent with existing frameworks, including the LIAF and the E-

⁵ Onward transfer is the transfer or disclosure of personal information to an additional party that did not collect or create that information and that is not acting on behalf of the party that collected or created that information. [12]

Authentication Guidance.⁶ The SPICI-defined capabilities complement those defined by other frameworks, and thereby fill some gaps in those frameworks related to sharing. The SPICI-defined capabilities do not fill all gaps; however, SPICI is easily extensible to include additional capabilities.

6. SPICI ANALYTIC FRAMEWORK

SPICI identifies potential harms associated with sharing identity or credential information, consistent with the E-Authentication Guidance. Based on the level of harm (minimal, moderate, substantial, or high),⁷ SPICI recommends capability assurance levels. This is illustrated for Identity Attribute Correlation, i.e., for the capability to determine an individual's identity based on identifying or authorization-related attributes, which may come from different credentials. This capability involves either correlation and aggregation of identity and credential information or reliance on a unique identifier [14]. This capability is needed when credential tokens are validated, information from them is extracted, and local stores of shared identity or credential information are updated, so that the individual can be identified unambiguously. The four levels of assurance for this capability are:

- **Weak**: A service provider (i.e., an entity that provides goods or services to an individual) can have little or no confidence that shared identity and/or credential information refers to a specific individual. Shared identity and/or credential information is associated with information that the service provider maintains based on a single attribute that can frequently be confused or conflated, e.g., name.
- **Basic**: A service provider can have some confidence that shared identity and/or credential information refers to a specific individual. Shared identity and/or

⁶ The E-Authentication Guidance and the LIAF define assurance levels that apply to both Unambiguous Identification and Assured Authentication, and maps potential harm levels to assurance levels. Community acceptance of this lack of granularity is possible largely because of a relatively large common experience in the use of credential processes. However, less experience has been captured, and less consensus can be expected, regarding the set of capabilities that enable *sharing* of identity or credential information. Thus, SPICI provides more granularity: levels are defined for different capabilities, and potential harms are mapped not to a bundle of capabilities but to each capability.

⁷ These levels of harm are largely identical to those in the E-Authentication Guidance. SPICI provides additional detail for harms to individuals. When those harms are associated with unauthorized disclosure of personal information, the SPICI definitions of moderate, substantial, and high levels of harm are consistent with the examples of low, moderate, and high confidentiality impacts in the draft NIST guide [13].

credential information is associated with information that the service provider maintains based on multiple attributes (e.g., name plus phone number, name plus account identifier), or on a single attribute that is intended to be unique (e.g., SSN, driver’s license number).

- Strong: A service provider can have high confidence that shared identity and/or credential information refers to a specific individual. Shared identity and/or credential information is associated with information that the service provider maintains based on multiple attributes that comply with an agreed-upon specification, or on a single attribute that the service provider and the entity that shared the information accept as unique (e.g., identity credential supplied by an agreed-upon Assurance Level 3 Credential Service Provider).
- Enhanced: A service provider can have very high confidence that shared identity and/or credential information refers to a specific individual. Shared identity and/or credential information is associated with information that the service provider maintains based on selective retrieval or evaluation of multiple attributes that comply with an agreed-upon specification (e.g., age range rather than date of birth), based on rigorous methods (e.g., statistical methods), or on a single attribute that the service provider and the entity that shared the information have very high confidence in as unique (e.g., identity credential supplied by an agreed-upon Assurance Level 4 Credential Service Provider).

Table 1 presents the mapping from levels of potential harm to the recommended level for Identity Attribute Correlation. For example, if an organization’s potential harm from unauthorized release of sensitive information, due to misidentifying an individual and granting them more privileges than they are entitled to, is high, then the recommended level of Identity Attribute Correlation is Strong. If the potential physical harm to an individual, for example due to medical mistreatment based on misidentification associated with an incorrect attribute, is substantial, then the recommended level is Enhanced. The overall recommended level is the maximum of the recommendations across all stakeholders.

Identity attribute correlation or matching that does not rely upon a unique identifier is an active research area at the Enhanced level [15, 16, 17].

7. CONCLUSION

Organizations that share identity or credential information can use SPICI as part of their process of negotiating identity federation or other identity information sharing agreements. The organizations can determine which capabilities are relevant to their joint and separate

business processes, assess their respective concerns, and determine what capability levels they require or can achieve. The organizations can thus reach agreement on how they each provide the relevant capabilities – on the processes and mechanisms they will use to achieve the five objectives. Under the I3P project, a spreadsheet tool has been prototyped.

Table 1. Recommended Level of Identity Attribute Correlation

| Potential Harm to Service Provider | Level of Harm | | | | |
|---|---------------|------------|------------|------------|-------------|
| | <i>N/A</i> | <i>Min</i> | <i>Mod</i> | <i>Sub</i> | <i>High</i> |
| Inconvenience, distress or damage to standing or reputation | Weak | Weak | Basic | Strong | Enh. |
| Financial loss or liability | Weak | Weak | Basic | Strong | Enh. |
| Harm to organizational programs or interests | Weak | Weak | Basic | Strong | Enh. |
| Sensitive information breach | Weak | Weak | Weak | Basic | Strong |
| Civil or criminal violations | Weak | Weak | Basic | Strong | Enh. |
| Potential Harm to Individual | <i>N/A</i> | <i>Min</i> | <i>Mod</i> | <i>Sub</i> | <i>High</i> |
| Social harms | Weak | Weak | Basic | Strong | Enh. |
| Physical harm or distress | Weak | Basic | Strong | Enh. | Enh. |
| Financial harms | Weak | Weak | Weak | Basic | Strong |

In addition, an organization that handles identity or credential information can use SPICI to manage risks, by identifying gaps in current or planned capabilities vis-à-vis recommended assurance levels. An identity management or federation solution provider can use SPICI to profile product capabilities. Finally, researchers can use SPICI to identify capability gaps as research areas. The work being performed or leveraged as part of the I3P Safeguarding Digital Identity project aligns with the six capabilities currently defined in SPICI, and in general will produce enhanced capabilities:

- A service—VeryIDX [15]—that facilitates trust negotiations across organizations that wish to share digital identities, and an attribute trust framework [18], which address Identity Attribute Correlation and Conditional Identity / Attribute Validation.
- Minimum-Disclosure Credentials [19], Attribute-Based Messaging [20], Attribute-Based Encryption [21, 22],

Zero-Knowledge Identity Federation [23] and Privacy-Preserving Distributed Queries address Selective Disclosure / Retrieval Protection in a variety of contexts.

- Enabling Web Services for Federated Digital Identities (integrated into a demonstration being developed under the I3P project) address Identity Attribute Correlation and Mutual Understanding via Common Attribute Syntax and Semantics.

The SPICI analytic framework is extensible; future versions of SPICI could include definitions of, and recommendations for, additional capabilities. For example, Trust Calculus [24], also being developed under the I3P project, addresses Trust Assessment.

8. ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the author and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

9. BIBLIOGRAPHY

- [1] I3P, Safeguarding Digital Identities Overview, 2008, <http://www.thei3p.org/docs/research/idmgmtoverview.pdf>
- [2] Bhargav-Spantzel, Abhilasha, Squicciarini, Anna C., Bertino, Elisa, Trust Negotiation in Identity Management, *IEEE Security and Privacy*, March/April 2007.
- [3] Gateau, B., Feltus, C., Aubert, J., Incoul, C., An agent-based framework for identity management: The unsuspected relation with ISO/IEC 15504, in *Research Challenges in Information Science, 2008*. ISBN: 978-1-4244-1677-6. DOI: 10.1109/RCIS.2008.4632091
- [4] American National Standards Institute-Better Business Bureau (ANSI-BBB) Identity Theft Prevention and Identity Management Standards Panel (IDSP), Final Report Volume I: Findings and Recommendations, 31 January 2008, <http://publicaa.ansi.org/sites/apdl/ID%20Theft%20Prevention%20and%20ID%20Management%20Standards%20Pa/IDSP%20Final%20Report%20-%20Volume%20I%20Findings%20and%20Recommendations.pdf>
- [5] Office of Management and Budget (OMB), E-Authentication Guidance for Federal Agencies, OMB Memorandum 04-04, 13 December 2003, <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- [6] National Institute of Standards and Technology (NIST), Electronic Authentication Guideline, NIST Special Publication (SP) 800-63, Version 1.0.2, April 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf and Draft Revision 1, December 2008, <http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63-Rev.%201>
- [7] Liberty Alliance Project, Liberty Identity Assurance Framework, Version 1.1, June 2008, <http://www.projectliberty.org/liberty/content/download/4315/28869/file/liberty-identity-assurance-framework-v1.1.pdf>
- [8] ITU-T FG IdM, Report on Identity Management Framework for Global Interoperability, Study Group 17 Temporary Document 0297 (FG IdM Doc 196), <http://wftp3.itu.int/fgidm/Deliverables/0297-att-1.doc>
- [9] Internet2, Federation Soup: An Assembly of Ingredients, Proceedings of the Federation Soup Workshop, held 2-4 June 2008 in Seattle, WA, 7 September 2008, http://middleware.internet2.edu/fedsoup/docs/internet2-fed_soup_report-200809.pdf
- [10] Liberty Alliance Project, Liberty Alliance Contractual Framework Outline for Circles of Trust, March 2007, <http://www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf>
- [11] Federal Trade Commission (FTC), Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, May 2000, <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>
- [12] Connolly, K. *Law of Internet Security and Privacy (2004 Edition)*, Aspen Publishers Online, ISBN 0735542732, 9780735542730
- [13] NIST, Guide to Protecting the Confidentiality of Personally Identifying Information (PII) (DRAFT), NIST SP 800-122 (Draft), <http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf>
- [14] National Alliance for Health Information Technology (NAHIT), Safety in Numbers: Resolving shortcomings in the matching of patients with their electronic records, Point of View Paper #1, December 2007, <http://www.nahit.org/images/pdfs/PatientIdentifierPointofView.pdf>

- [15] Bhargav-Spantzel, A., Jungha Woo, Bertino, E. Receipt Management- Transaction history based receipt management, *Workshop On Digital Identity Management, Proceedings of the 2007 ACM workshop on Digital identity management*, November 2007, pages: 82 – 91, <http://homes.cerias.purdue.edu/~bhargav/pdf/ReceiptDIM07.pdf>
- [16] Language Resources and Evaluation Conference, *Proceedings of the 2008 Workshop on Resources and Evaluation for Identity Matching, Entity Resolution and Entity Management*, 31 May 2008, <http://www.lrec-conf.org/proceedings/lrec2008/>
- [17] Hatakeyama, Makoto, Shima, Shigeyoshi. Privilege federation between different user profiles for service federation. *Proceedings of the 4th ACM workshop on Digital identity management*, November 2008. DOI=<http://doi.acm.org/10.1145/1456424.1456432>
- [18] Mohan, A., and Blough, D. "AttributeTrust: A Framework for Evaluating Trust in Aggregated Attributes via a Reputation System," *Proceedings of the Conference on Privacy, Security, and Trust*, 2008.
- [19] Bauer, D., Blough, D., and Cash, D. "Minimal Information Disclosure with Efficiently Verifiable Credentials." *Proceedings of the 4th ACM Workshop on Digital Identity Management*, November 2008.
- [20] Bobba, R., Fatemeh, O., Khan, F., Gunter, C., and Khurana, H. Using Attribute-Based Access Control to Enable Attribute-Based Messaging, *IEEE Annual Computer Security Applications Conference (ACSAC '06)*, Miami, FL, December 2006.
- [21] Goyal, V., Pandeyy, O., Sahaiz, A., and Waters, B. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. *Proceedings of the ACM conference on Computer and Communications Security*, 2006.
- [22] Bethencourt, J., Sahai, A., and Waters, B. 2007. Ciphertext-Policy Attribute-Based Encryption. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy* (May 20 - 23, 2007). SP. IEEE Computer Society, Washington, DC, 321-334. DOI=<http://dx.doi.org/10.1109/SP.2007.11>
- [23] Bhargav-Spantzel, A., Squicciarini, A. C., and Bertino, E. 2006. Establishing and protecting digital identity in federation systems. *J. Comput. Secur.* 14, 3 (May 2006), 269-300.
- [24] Huang, J. and Nicol, D. 2009. A Calculus of Trust and Its Applications to PKI and Identity Management. *Proceedings of IDtrust 2009*, April 2009.