

1
2
3
4 **Developing Trust Frameworks to**
5 **Support Identity Federations**
6

7 David Temoshok
8 Christine Abruzzi
9
10
11
12
13
14

Developing Trust Frameworks to Support Identity Federations

David Temoshok
*Applied Cybersecurity Division
Information Technology Laboratory*

Christine Abruzzi
*Deloitte & Touche LLP
Rosslyn, VA*

October 2016



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

56

57

58

National Institute of Standards and Technology Internal Report 8149

59

33 pages (October 2016)

60

61

62

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

63

64

65

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

66

67

68

69

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at <http://csrc.nist.gov/publications>.

70

71

72

Public comment period: *October 3, 2016* through *November 1, 2016*

73

National Institute of Standards and Technology

74

Attn: Applied Cybersecurity Division, Information Technology Laboratory

75

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

76

Email: trustframeworks@nist.gov

77

78

All comments are subject to release under the Freedom of Information Act (FOIA).

79

80
81

Abstract

82 When supported by trust frameworks, identity federations provide a secure method for the
83 leveraging of shared identity credentials across communities of similarly-focused online service
84 providers. This document explores the concepts around trust frameworks and identity federations
85 and provides topics to consider in their development.

86

87

Keywords

88 Identity; identity federation; trust frameworks; identity management; multilateral agreements;
89 credential service providers; authentication; relying parties; secure online transactions; NSTIC;
90 interoperability, information security; cybersecurity; identity proofing.

91

92

Acknowledgements

93 The authors would like to thank Ryan Galluzzo, Amanda Patino, Ellen Nadeau, and Kaitlin Boeckl for
94 their contributions to this report.

Table of Contents

95			
96	1	Introduction.....	1
97	1.1	Purpose & Scope.....	2
98	1.2	Audience	2
99	2	Identity Federation & Trust Frameworks.....	3
100	2.1	Identity Federations.....	4
101	2.2	Trust Frameworks	4
102	3	Roles & Responsibilities.....	5
103	3.1	Federation Administrators	5
104	3.2	Credential Service Providers	6
105	3.3	Relying Parties	6
106	3.4	Users	7
107	4	Trust Framework Components.....	7
108	5	System Rules	9
109	5.1	Registration/Enrollment.....	9
110	5.2	Identity Proofing.....	10
111	5.3	Credential management	11
112	5.4	Privacy requirements	12
113	5.5	Security requirements.....	13
114	5.6	Data handling requirements	13
115	5.7	Technical Specifications	13
116	6	Legal Structure	13
117	6.1	Trust Framework Legal Rules.....	14
118	6.2	Risk and Liability Allocation.....	14
119	6.3	Multilateral Agreements	15
120	7	Establishing Conformance	16
121	7.1	Self-assessment	16
122	7.2	3 rd -party assessment	17
123	7.3	Audit.....	17
124	8	Recognizing & Communicating Conformance.....	18
125	8.1	Registries & Listing Services	19
126	8.2	Compliance Marks.....	20

127 8.3 Trustmarks21

128 8.4 Digital Certificates..... 22

129 9 Conclusion & Other Considerations..... 22

130 Appendix A – Glossary..... 24

131 Appendix B – Reference Documents..... 26

132

133

1 Introduction

It's difficult to overstate the impact the internet has had on modern life. Our ability to connect with people and organizations online presents virtually unlimited opportunities for delivering services and conducting business. But, as many organizations and businesses have discovered, doing business with people over the internet presents its own particular challenges, not the least of which is being able to identify with whom they are interacting.

In traditional environments, if an organization needed to verify with whom it was doing business, it could require its clients and customers to show up in person and present proof of their identity. For obvious reasons, though, online service providers have had to devise other means of identifying who is accessing their systems. More often than not, this involves having their users register and create individual accounts for use in accessing their services. This means that now, instead of being able to focus on delivering the best possible services and products they can, providers must also devote resources to creating and managing users' login credentials.

Online service providers are not the only ones that face additional challenges from this model. Most consumers are all too familiar with the ubiquitous sign-in screen requiring them to enter their username and password. While widely-known best practices state that usernames and passwords should not be shared between services, maintaining an ever growing list of logins creates friction for individuals and employees from virtually all walks of life. In many cases, users would rather risk having their identities compromised than go through the trouble of creating separate login credentials for each and every website with which they do business.¹

To address these challenges, communities and organizations that share a common user base and transaction type have built the means to allow users to sign on and access multiple services through common login and authentication processes. This is known as federated identity management; that is, users are enabled to "federate" their identity through common, shared authentication processes and access multiple online organizations and services. Federated identity management is based on trust. Organizations must trust the federated identity management processes in order to allow access to users that were authenticated by another entity. The "rules" for federated identity management are known as "**trust frameworks**" and the organizations that agree to follow such rules and participate are known as "**identity federations.**"

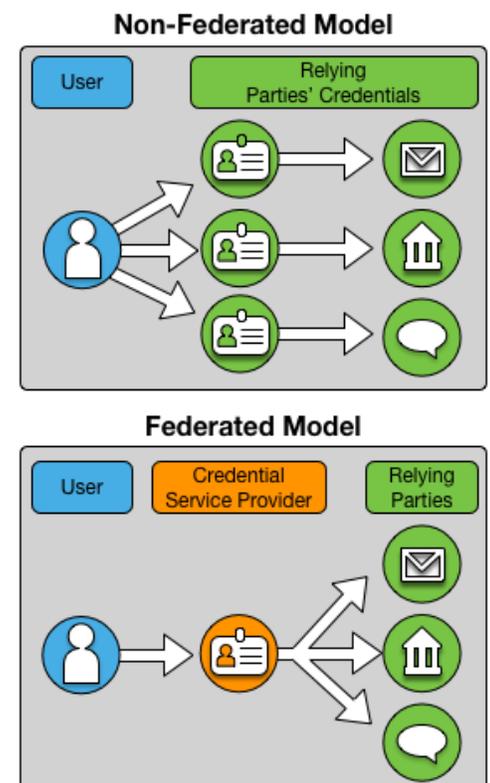


Figure 1: Federated v. Non-Federated Identity

¹ A recent report from Telesign that surveyed 2,000 consumers in the U.S. and the U.K. notes that 73% of respondents used duplicate passwords. Further corroborating this result, the study also found that consumers have an average of 24 online accounts, but only 6 unique passwords to protect them.

(<https://www.telesign.com/wp-content/uploads/2015/06/TeleSign-Consumer-Account-Security-Report-2015-FINAL.pdf>)

170 These identity federations serve as clearinghouses that can provide a basis for individuals to prove
171 their identity or attributes when necessary to any online service provider without compromising
172 their individual privacy or increasing the risk of catastrophic data breaches. In time, an inter-
173 federation of clearinghouses can ensure that services that will be available to all individuals for their
174 online transactions both with government and across the global commercial marketplace.

175 1.1 Purpose & Scope

176 This document provides considerations for communities interested in pursuing federated identity
177 management when establishing the multilateral agreements that make up a Trust Framework. It
178 examines the various roles involved in an identity federation, what to consider from a legal
179 standpoint, and the issues of establishing and recognizing conformance.

180 More broadly, this publication will serve as an educational document to spread the knowledge of
181 identity federations and trust frameworks to a more general audience. Additionally, NIST seeks to
182 increase standardization of the language around identity federation and trust frameworks and to set
183 a broad, common understanding of the concepts in order to facilitate their widespread adoption.

184 While this document explores some elements for consideration when forming an identity federation
185 and trust framework, it is not intended to be a how-to guide that gives specific instructions or
186 templates for their development. NIST believes that this is best left to the experts who are familiar
187 with the needs of their specific community. Also, this does not represent a technical guide for the
188 protocols and interfaces needed to exchange information in a federation.

189 1.2 Audience

190 NIST created this publication for organizations that provide online services and who seek to minimize
191 the cost and administrative burden of operating stand-alone identity management systems for their
192 online users. The document is written for organizations and individuals that could benefit from
193 assistance in forming an identity federation with other online service providers and focuses on the
194 administrative aspects for building trust frameworks to support identity federation and online trust.
195 Typically, identity federations are formed among organizations that have a common, or largely
196 overlapping, user base and that provide similar, or complementary, types of online services and
197 applications.



198

199 The diversity of various industries and sectors imply diverse needs and challenges, but in identity
200 NIST continues to find a large degree of common ground and overlapping requirements in

201 information technology. In this document we hope to demonstrate that trust frameworks can
202 provide a foundation for trust in federated identity among many communities of interest and also
203 present the range and scope of options available to organizations when developing trust
204 frameworks to address the needs of their particular communities.

205 **2 Identity Federation & Trust Frameworks**

206 In an identity ecosystem that supports secure and convenient access to online services, trust
207 frameworks play a vital role by laying the foundation upon which the various participants can trust
208 each other. Put simply, trust frameworks aim to move from expensive and resource intensive
209 bilateral agreements toward streamlined, efficient, and reliable multilateral arrangements that still
210 meet the needs of all participants.

211 *A **trust framework** is developed by a community whose members have similar goals
212 and perspectives. It defines the rights and responsibilities of that community's
213 participants in the Identity Ecosystem; specifies the policies and standards specific to
214 the community; and defines the community-specific processes and procedures that
215 provide assurance. A trust framework considers the level of risk associated with the
216 transaction types of its participants; for example, for regulated industries, it could
217 incorporate the requirements particular to that industry. Different trust frameworks
218 can exist within the Identity Ecosystem, and sets of participants can tailor trust
219 frameworks to meet their particular needs. In order to be a part of the Identity
220 Ecosystem, all trust frameworks must still meet the baseline standards established
221 by the Identity Ecosystem Framework.²*

222 From the perspective of an online service provider, there are many reasons to participate in an
223 identity federation. Some of the benefits to doing so include:

- 224 • Increased efficiency and cost savings from not having to manage login information for its
225 users,
- 226 • Risk management through the use of multilateral agreements,
- 227 • Improved system design decision criteria based on defined security expectations aligned
228 with the community being served, and
- 229 • Customer convenience and reduced risks associated with having to manage fewer discrete
230 credentials.

² **National Strategy for Trusted Identities in Cyberspace** – Enhancing Online Choice, Efficiency, Security, and Privacy, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

231 2.1 Identity Federations

232 **Federated Identity Management** is a means to enable users to
 233 access the systems and applications of multiple organizations
 234 using the same login credentials. It allows users to choose a
 235 **credential service provider (CSP)** (for example an email or social
 236 media provider). Users register once with their selected CSP and
 237 establish online credentials to be managed by that CSP for
 238 authentication. When a user wants to access a **relying party**
 239 **(RP)** service or application (for example a bank or online
 240 retailer), that user is redirected to the selected CSP for
 241 authentication using the credentials established with that CSP.
 242 The CSP then presents the status of the authentication to the RP
 243 so that the user may be granted access to the service or
 244 application they wish to use. In this way, users do not need to
 245 register or establish login credentials with each service they
 246 want to access and they only need to provide their credentials
 247 to their selected CSP rather than to each service they want to
 248 access.

249 In the simplest terms, identity federations consist of CSPs and
 250 RPs that have agreed to participate in a specific federated
 251 identity management arrangement. CSPs register, establish
 252 credentials, authenticate users, and assert user authentication
 253 status to federation RPs. RPs consume identity assertions
 254 provided by the CSPs and use the authentication status
 255 information to authorize user access to online services and applications. **Trust amongst members of
 256 an identity federation is foundational to its operation and is established through the set of
 257 agreements and associated rules that are specific to that community.** Such rules for a federated
 258 identity management arrangement are known as its trust framework.

259 2.2 Trust Frameworks

260 As defined above, a trust framework is the set of rules and policies that govern how the federation
 261 members will operate and interact, including:

- 262 • Conducting identity management responsibilities,
- 263 • Sharing identity information,
- 264 • Using identity information that has been shared with them,
- 265 • Protecting and securing identity information,
- 266 • Performing specific roles within the federation, and
- 267 • Managing liability and legal issues.

268 Trust frameworks serve as the basis for the multilateral agreements among all of a federation’s
 269 members that enable the trust and governance of a federation’s operations.

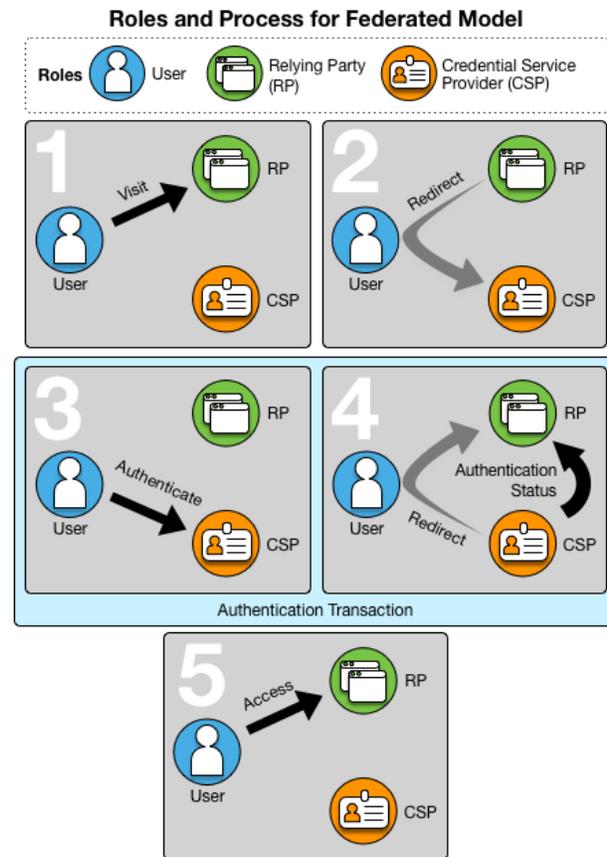
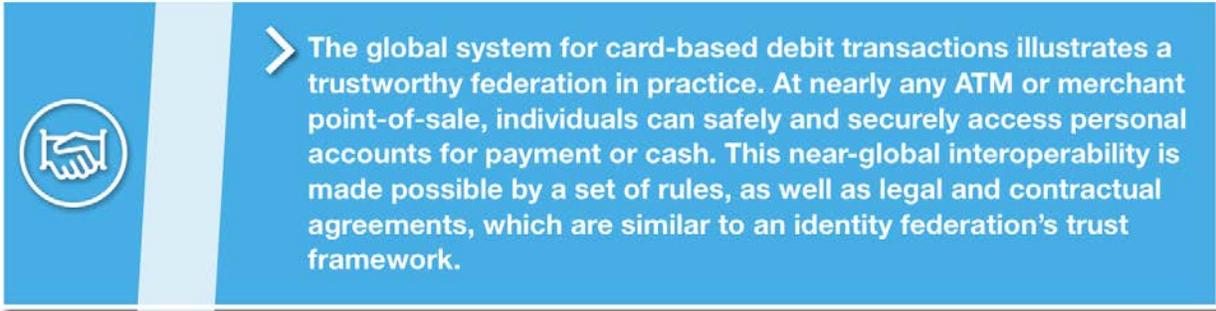


Figure 2: Roles and Processes in a Federated Model



270

271

3 Roles & Responsibilities

272

3.1 Federation Administrators

273

Role description

274

275

276

277

278

279

280

Federation administrators are responsible for the governance of an identity federation. They are organizations, often set-up by their constituent members, to administrate the activities associated with operating an identity federation.³ The structure of this organization may vary, depending on the nature of the community, the level of risk an identity federation seeks to address, and whether or not it is driven by regulatory or other such considerations. For example, federation administrators may take the form of government programs, corporate entities, not-for-profit membership organizations, or industry associations.

281

In this way, federation administrators act as policy clearinghouses for digital identity services.

282

Responsibilities

283

Federation administrators:

284

285

286

287

288

289

- Establish the trust framework rules and requirements,
- Develop and manage the documentation,
- Manage membership and participation,
- Manage member conformance to the trust framework's rules,
- Maintain, promote and evolve the federation, and
- Oversee the smooth operation of the federation.

290

³ While federation administrators are also commonly called trust framework providers or trust framework operators, for the purposes of this document we will only refer this role as “federation administrators.”

291 3.2 Credential Service Providers

292 Role description

293 Credential service providers (CSPs) issue and maintain the electronic credentials that individuals use
294 to access online services.⁴ For example, some email providers act as CSPs when they allow users to
295 use their credentials to log into other vendor's services, as do some social media sites. CSPs may
296 specialize in managing identities for the specific community served by a trust framework, or may
297 offer a more broad-based identity service, of which some users fit the profile targeted by the
298 framework. In the latter scenario, a CSP may operate in multiple trust frameworks, in effect
299 providing a single user identity service in multiple communities, such as in both healthcare and
300 banking.

301 In this way, CSPs act as technical clearinghouses for digital identity services.

302 Responsibilities

303 CSPs:

- 304 • Register/enroll users,
- 305 • Perform identity proofing,
- 306 • Manage credentials, and
- 307 • Perform user authentication and authentication status assertion.

308 See [Section 5, System Rules](#), of this document for a more detailed explanation of these activities.

309 3.3 Relying Parties

310 Role description

311 Online service providers operating within a federation are known as relying parties (RPs) and are
312 organizations that offer services, applications, and information that require restricted access.
313 Examples of RPs include a retail bank's online services and online retailers. Relying parties accept
314 (rely upon) user authentication status assertions from federation CSPs, rather than operate separate
315 identity management systems of their own. They must be able to trust the identity information they
316 receive from a CSP about a user's identity in order to make decisions about whether or not to allow
317 that user access to their online services or products. RPs may still maintain some account
318 information, especially if it is core to its business, such as a retailer keeping browsing and purchase
319 history for a user and perhaps shipping and payment information. In such a case, the RP may simply
320 outsource the authentication of the user to the CSP, subject to the rules of the federation.

321 In this way RPs can achieve their goal of providing their online service without bearing the cost of
322 managing identity services that are neither core to their business nor their core competency.

⁴ Other commonly used terms for CSPs include identity providers (IdPs) and identity service providers (ISPs).

323 **Responsibilities**

324 RPs:

- 325 • Consume the identity information provided by the CSPs, and
- 326 • Authorize access to users, in accordance with the rules of the federation.

327 **3.4 Users**328 **Role description**

329 As consumers of the services offered by the RPs, end users (users) are not formally members of an
330 identity federation. However, they typically bear certain responsibilities depending on the nature of
331 the trust framework.

332 By having credentials that are accepted under trust frameworks, users can have a consistent
333 experience in which their credentials are accepted and their data treated in the same manner
334 regardless of provider.

335 **Responsibilities**

336 Users:

- 337 • Protect their identities and digital credentials from fraud and misuse,
- 338 • Use their credentials in the manner for which they are intended, and
- 339 • In some cases, undergo some manner of identity proofing, as explained later in this
340 document.

341 **4 Trust Framework Components**

342 Identity federations consist of different types of organizations; some provide
343 identity management operations for the federation (CSPs) and other
344 organizations that consume identity information from CSPs in order to allow
345 users access to their online systems, applications and transactions (RPs). If
346 there are only a few members in the identity federation, it would be
347 manageable to establish bilateral agreements among the members to define
348 their roles and responsibilities. However, identity federation is intended to
349 scale to large online communities and trust frameworks are the means to
350 scale and enable identity federation to work for these communities.

351 In an identity federation's trust framework, the individual components define
352 how federation members will interact with each other. By defining the
353 expectations members have of each other, a federation is able to support the
354 trusted transactions for which it was created. For the purposes of this
355 document, we have identified four components that characterize an identity
356 trust framework:

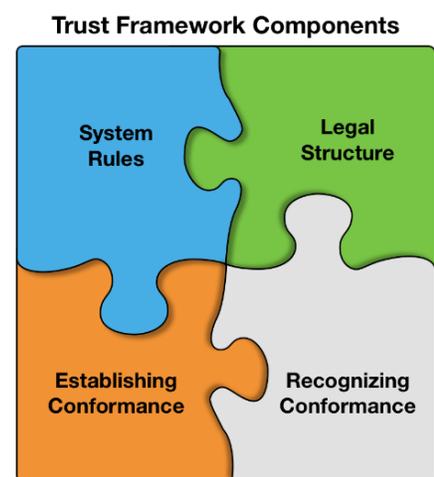


Figure 3: Trust Framework Components

- 357 • **System Rules**, which govern the interactions between members,
- 358 • **A Legal Structure**, which identifies the rights, responsibilities, and liabilities associated with
- 359 participation in the federation,
- 360 • A way of **Establishing Conformance** across its members, and
- 361 • A way of **Recognizing that Conformance**.
- 362

363 The following sections, explore these concepts further and explain how these components fit
364 together to support an identify federation.

365 **Risk Management and trust**

366 Mutual trust among federation members is crucial for identity federation to work. Trust is typically
367 generated through experience and reputation. For example, based on experience, we trust that we
368 can use our debit cards in virtually any ATM and reliably and safely conduct financial transactions in
369 any location. Our interactions have taught us that debit transactions are executed in a reliable and
370 secure manner and when errors do occur they are handled according to established rules and
371 processes. We generally recognize and make risk evaluations in differing environments, such as
372 when something does not seem right with a retailer or an ATM and we choose not to hand over our
373 card.

374 Identity federations aim to reach similar levels of trust and expectation among members and users.
375 However, it will take some time to build similar experience with online federated systems. To build
376 trust now, identity federations need to identify potential risks and manage those risks. Identity
377 federations have accomplished this by clearly articulating the roles and responsibilities of all
378 members and how those responsibilities will be met. Trust frameworks are the means to present
379 those expectations, typically in the form of rules and agreements.

380 Because each community operates its online transactions at a unique level of risk, the elements that
381 go into a trust framework should be selected to address the specific needs of its members. Risk
382 management always involves balancing the costs of risk mitigation and risk tolerance. So trust
383 framework development should be considered as a process that involves fulfilling expectations
384 through risk analysis, risk management, risk tolerance, performance, and experience. Accordingly,
385 identity federations will need to analyze risks to the types of online services that they offer, identify
386 ways to manage those risks, determine the most effective and efficient solutions, and incorporate
387 those solutions in their trust framework.

388 Fortunately, there are several methodologies available for use in identifying the risk profile of their
389 members and determining appropriate rules, legal documentation, and conformance processes for
390 their trust framework. Whichever framework is used, however, the core set of risk management
391 practices must reflect a federation's participants' understanding of their risk environment, and the
392 specific components must be chosen to mitigate these risks – be they technical, legal, or business.
393 The following sections present components that are typically addressed in trust frameworks.



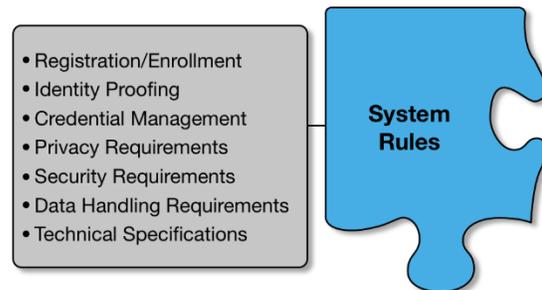
> Risk Management Frameworks & Methodologies include:

- NIST's "Risk Management Framework" (specifically SPs 800-37-1 & 800-53-4)
- ISO 31000:2009, "Risk Management – Principles and Guidelines"
- NIST's "Digital Authentication Guideline" (SP-800-63-3)
- ISO/IEC 29115:2013, "Entity Authentication Assurance Framework"
- Control Objectives for Information and Related Technologies (COBIT)

394

395 5 System Rules

396 A fundamental purpose for building trust frameworks is to define the
 397 identity management operations and technical requirements needed
 398 to support the identity federation and to clearly assign responsibility
 399 for performing those operations. Since federation members expect
 400 and need to trust those identity management operations, the identity
 401 management operations of the federation are typically presented as
 402 requirements or rules. The federation members responsible for
 403 performing specific operations are expected to demonstrate
 404 conformance with the rule set specific to their role.



405 5.1 Registration/Enrollment

406 What is registration?

407 Registration, or enrollment, is the process of creating an identity record within an **identity**
 408 **management system (IDMS)** and associating it with attributes specific to a particular User. Each
 409 identity record within an IDMS should be unique, such that there is enough information about a User
 410 to distinguish them from other users managed by the system.

411 In many cases, ID proofing and registration are closely linked and may occur in the same session. For
 412 instance, for registration processes that require an applicant user to appear in-person in front of a
 413 registration agent, the identity documents required for ID proofing may be scanned into the system
 414 and associated with the user's identity record.

415 Why should registration be included in a trust framework?

416 Members of a federation must know what processes and procedures were followed when creating
 417 an identity record, including what types of systems were used to capture the results of the ID
 418 proofing and how those results are associated with, or bound, to a user.

419

420 Registration options, based on risk

421 For lower risk transactions, registration or enrollment may be as simple as asking a new user to
422 create a username and password. Depending on the nature of the services supported by the
423 federation, additional information may be requested, such as mailing addresses, phone numbers,
424 and email addresses. Other factors that may affect registration process requirements include
425 whether an identity federation allows for pseudonymous identities.

426 Federations that operate to mitigate higher levels of risk often require the organizations that
427 perform the enrollment process (often referred to as Registrars or Registration Agents) to meet
428 certain requirements before they can be authorized to perform their role, including minimum skills or
429 experience levels and/or the completion of training on the system. For the highest risk environments,
430 potential Registrars may even be required to pass a background check before they can be “certified”
431 to register users in a system.

432 Additionally, the amount and types of information captured and associated with a user may vary,
433 depending on the degree of rigor applied within a federation. On the lower end of the spectrum,
434 username and password or unverified demographic information (e.g., mailing addresses, phone
435 numbers, email addresses) may be included in identity records. Where a moderate level of risk is
436 being addressed, that information may need to be validated against authoritative sources. For the
437 highest risk transactions, additional data, such as scanned documentation or biometrics, may be
438 collected during in-person ID proofing. In any case, the only information that should be collected and
439 maintained is the information that is needed for enrollment and subsequent identity proofing
440 processes.

441 As in other aspects of an identity federation’s trust framework, decisions must be made and included
442 in the documentation as to the amount of rigor, commensurate with a risk profile, its members must
443 apply while performing their roles.

444 5.2 Identity Proofing

445 What is Identity Proofing?

446 Identity proofing is the process by which a CSP collects and verifies information about a person for
447 the purposes of issuing credentials to that person. In other words, it’s how CSPs require applicants
448 to prove they are who they claim to be.

449 Why should ID proofing be included in a trust framework?

450 By defining baseline requirements for ID proofing, identity federations set a foundation for their
451 members to trust that users have been vetted to an appropriate level prior to being issued a
452 federation credential. Depending on the level of risk associated with a federation, required ID
453 proofing activities can be as simple as verifying an email provided by a user, or as complicated as
454 requiring a user to appear in person in front of a trusted agent with one or more identity documents.

455

456 ID proofing options, based on risk

457 Identity federations should choose an identity proofing methodology to include in their Rules, based
458 on the amount of risk associated with its community's transactions.

- 459 • **Self-assertion/no identity proofing:** For transactions with the lowest associated risks, a CSP
460 can issue an identity credential based on an unverified statement that an individual is who
461 they claim to be. Self-assertion of an identity is appropriate when the resultant credentials
462 consist of a simple user name and password, issued for the purposes of identifying a user
463 across multiple sessions. Identity proofing is also not required for **anonymous** and
464 **pseudonymous** transactions.
- 465 • **Remote identity proofing:** Remote identity proofing is appropriate for moderate-risk
466 environments and requires a User to provide additional evidence in support of their asserted
467 identity. Options for remote proofing include knowledge-based challenges, which involve
468 checking information provided by an applicant against an authoritative data source, and
469 sending one-time codes to an applicant's email address or cell phone.
- 470 • **In-person identity proofing:** In-person proofing is the most rigorous proofing method and is
471 appropriate for higher levels of risk. In-person proofing involves an applicant appearing in
472 person, with supporting evidence of their identity, in front of an authorized agent for the
473 identity service.



474

> More information about registration & enrollment can be found in:

- NIST's "Digital Authentication Guideline" (SP-800-63-3)
- ISO/IEC 29115:2013, "Entity Authentication Assurance Framework"
- ISO/IEC 24760, "A Framework for Identity Management"

475 5.3 Credential management

476 What is credential management?

477 Credentials are issued as the result of the registration or enrollment activity and are what users
478 actually use, or assert they are, in order to gain access to online systems and services. Credentials
479 consist of an identifier, which points to a user's unique record in an IDMS; an authenticator, or the
480 mechanism by which a user is verified as being the same person who was registered; and any bound
481 attributes, or information about the identity, which may be transmitted by the CSP to an RP. In many
482 cases, the process of issuing a credential is transparent to the user, who simply knows they were
483 asked to provide some information about themselves and then created, or were provided with, a
484 user name to use when logging into the system.

485 Credential management, then, is the set of processes a CSP follows during the lifecycle of an identity.
486 Depending on the requirements of a particular identity federation, lifecycle stages may include any
487 or all of the following: credential issuance, updates, renewal, expiration and revocation.

488 **Credential management options, based on risk**

489 Trust frameworks can define minimum requirements for any stage of the credential lifecycle,
490 depending of the level of risk mitigation that needs to be achieved. Trust framework system rules
491 may include specific expectations for some or all of the lifecycle stages, as listed above. Higher levels
492 of risk generally include stricter requirements that involve higher costs and effort on the part of the
493 members; however, many identity federations believe this extra burden is warranted in order to
494 maintain the integrity of the identities and support a high level of trust.



495

496 5.4 Privacy requirements

497 Protecting a user's privacy goes beyond a single transaction or identity service. Through federated
498 technologies, an IDP could have insight into a range of transactions a user is conducting online
499 across a variety of RPs, building a narrative about a user that she never anticipated, or wanted, the
500 IDP to have.

501 Thus, trust framework developers should consider including requirements that serve to protect a
502 user's privacy, including the use of policy and technical controls. An example of a technical control is
503 a double-blind architecture, which prohibits a CSP from seeing which RPs a user is accessing, and
504 prohibits an RP from seeing which CSP a user is leveraging. While a double-blind architecture could
505 benefit a user's privacy using federated login, it also could help companies to ensure that a CSP is
506 not, for instance, harvesting an RP's customer list, which is a valuable business asset.

507 In order to select the appropriate controls, a trust framework may also require privacy risk
508 management practices in identifying and managing privacy risks in an information system. Some
509 trust frameworks build these privacy-enhancing features into their overall requirements, while
510 others address privacy in its own separate document. Either way, a trust framework's policy around
511 protecting privacy should be clearly articulated in its membership agreements and policy documents,
512 using plain language that is easily accessible to users. Those trust frameworks that place user privacy
513 as a primary concern may even consider including it explicitly in their vision statements and
514 operating rules.

5.5 Security requirements

IT system security is an essential component of any risk reduction and management scheme and trust framework developers can use the traditional three pillars of IT security model (i.e., confidentiality, integrity, availability) to inform their security-related policies and requirements. Setting expectations of its participants to protect the confidentiality, integrity, and availability of their services sets a foundation for trusted transactions between the parties. As with the other components, the level of risk and potential harm should drive the amount of attention paid to security requirements.

5.6 Data handling requirements

Data handling and usage requirements establish what identity data can be transmitted amongst member organizations and how that data must be used, managed, and protected. Identity federations should consider setting guidelines and requirements about how their members protect the identities themselves, as well as any attributes associated with those identities. Generally, the less identity data exchanged and stored, the better.

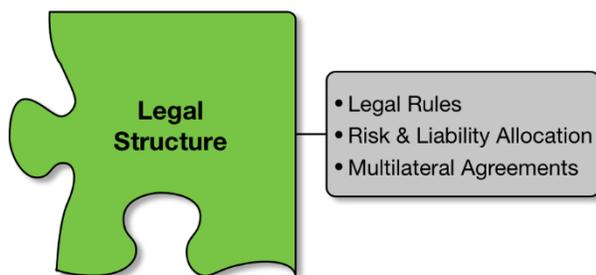
5.7 Technical Specifications

By identifying a common set of technical protocols and standards, trust frameworks promote the seamless exchange of authentication assertions and identity information amongst its members. To achieve the greatest level of interoperability, identity federations are encouraged to adopt open standards, which are often more cost-effective and flexible than proprietary solutions.

At a minimum, a trust framework's systems rules should define protocols and standards for handling the exchange of authentication data and for assessing the strength or validity of an asserted authentication.

6 Legal Structure

Trust frameworks present the operational and technical requirements for federated Identity management, and must also provide the legal basis to bind those requirements to federation members. Identity federation members voluntarily agree to participate in the federation and follow the trust framework rules. While there are varying means to bind members to federation rules, the most straightforward and common method is through contract or agreement. Members become legally bound to the trust framework rules through signed agreements to comply with the operational and technical rules as well as the legal rules, rights, and obligations of federation members. Therefore, trust frameworks and associated member agreements form a contract-based legal structure which applies to all federation members. This legal obligation is critical for providing the assurance and trust for the federated identity system.



551 6.1 Trust Framework Legal Rules

552 Trust frameworks are created within the framework of public laws that apply within the jurisdiction
553 of federation operations. Public law established through statutes, regulations, and common law will
554 apply to federated management operations and systems that operate within their jurisdiction;
555 applicable general laws include contract law, tort law, business law, etc. Some public laws regulate
556 activities that will directly apply to identity management systems. For example, public law regulating
557 information privacy and data protection of personal information will apply to identity management
558 systems and operations (e.g., Federal Trade Commission Act, Fair Credit Reporting Act, and the
559 European Union Data Protection Directive). Public law and rules may also apply to specific types of
560 federation communities and transactions; examples include:

- 561 • The Child Online Privacy Protection Act (COPPA) regulates privacy protections for online
562 service providers directed to children under 13 years of age;
- 563 • The Financial Services Modernization Act (Gramm-Leach-Bliley Act) regulates the collection,
564 use and disclosure of financial information for financial institutions such as banks, securities
565 firms and insurance companies, and to other businesses that provide financial services and
566 products.
- 567 • The Health Insurance Portability and Accountability Act regulates medical information and
568 applies broadly to health care providers, data processors, pharmacies and other entities that
569 come into contact with medical information.

570 Trust framework administrators need to be aware of and understand the impacts of applicable
571 public laws on federation members and operations when creating trust framework rules and on an
572 ongoing basis. Obviously, trust framework rules must be in compliance with applicable existing and
573 emerging public law. This is particularly important given the scope of online commerce and services
574 and the potential for international, cross-jurisdictional business and identity federation.

575 Legal rules serve to bind federation members to all trust framework rules and requirements, and
576 present responsibilities and obligations of all members to each other and clarify any administrative or
577 legal aspects involved in their participation in the federation. These may include any warranties for
578 goods and services, compliance requirements beyond the operational and technical and operational
579 requirements, and enforcement mechanisms for non-compliance. Trust framework legal rules also
580 typically provide means and processes for dispute resolution in order to try to resolve disputes
581 between federation members through administrative processes, rather than court action.

582 6.2 Risk and Liability Allocation

583 A consideration for trust framework legal rules is the allocation of risk and liability of federation
584 members. Authentication transactions involve data exchange among a user, an RP, and a CSP. There
585 are potential risks to the successful execution of these transactions and subsequent access
586 authorizations that may present risks to any of the parties involved. For example, the CSP may have
587 erred in the enrollment information or credentialing of the user, users may be denied service due to a
588 disruption in system services, relying parties may have allowed unauthorized access to protected
589 resources due to identity theft or fraud. The result of any of these circumstances is that a federation
590 member or user may feel that they have suffered a loss (e.g., financial, exposure of personal

591 information, exposure of relying party protected resources). Any of the federation operations may
592 present risks that something may go wrong which introduces risks or, possibly, actual losses to any
593 of the federation members.

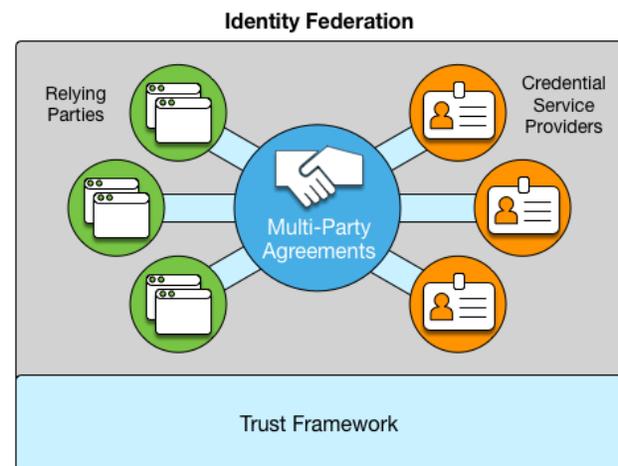
594 The general rule is that the party affected by the loss will bear the loss, unless the liability for the loss
595 is allocated to another party.⁵ However, liability losses are a zero-sum equation; that is, allocating
596 liability does not defer the loss, it simply allocates responsibility to a particular party. Trust
597 framework administrators may create legal rules to allocate risk and liability for various reasons;
598 typically risk and liability allocation has been used to ensure equitable allocation of risk and liability
599 among federation members.

600 Furthermore, the objective of the allocation of risk and liability may be to ensure the participation or
601 protection of a class or category of system participants critical to the federation. An Industry
602 example of such risk and liability allocation is the limitation on personal account liability for losses
603 occurring through electronic funds transfer in which liability may be allocated to the card issuing
604 financial institution under certain circumstances (i.e., Electronic Funds Transfer Act, Federal Reserve
605 Regulation E). Prior to this arrangement, uncertainty existed across multiple parties and the least
606 cost avoider lacked incentive to mitigate risk, in some ways stifling the market.

607 6.3 Multilateral Agreements

608 The principal purpose of trust framework legal
609 rules is to bind the applicable operational,
610 technical and legal rules and requirements to all
611 federation members. Federation trust and
612 reliance on identity management operations will
613 not be achieved without clear commitment of all
614 members to comply with trust framework rules.
615 This commitment is achieved through executing
616 legally binding agreements among all federation
617 members. Separate bilateral agreements could
618 be executed between the parties in federations
619 with few members, but this would be
620 cumbersome and costly and may jeopardize
621 federation trust since there is no assurance of binding all members to the same rules and
622 requirements if separate agreements among parties are executed; this would defeat the purpose of
623 the identity federation.

624 Common multilateral agreements typically bind federation members to the applicable operational,
625 technical and legal rules of the federation. Multilateral agreements present the same terms, rules
626 and requirements for all federation members. The specific requirements and responsibilities for
627 credential service providers and relying parties are applicable to those specific roles, but are clearly
628 presented for all members. Multilateral agreements streamline the process, allow the federation to

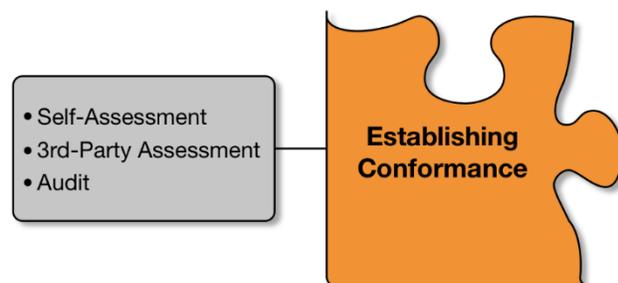


⁵ **The Vocabulary of Identity System Liability**, The Open Identity Exchange/Edwards Wildman Palmer LLP, by Thomas J. Smedinghoff, Mark Deem, and Sam Eckland.

629 scale, and enable each participant to easily see and understand the roles, responsibilities, and
 630 obligations of the other federation members. Multilateral agreements will also provide assurance
 631 that all members are bound to the same common enforcement mechanism of a legally binding
 632 agreement with common terms. The multi-party agreement should incorporate all relevant rules and
 633 requirements either directly or by reference if presented in a separate document(s).

634 7 Establishing Conformance

635 Establishing and enforcing conformance amongst its members
 636 to its set of agreements and operating rules is vital to an
 637 identity federation's functioning. Conformance is the degree to
 638 which a federation member has implemented, and is adhering
 639 to, the rules of the federation. The amount of rigor, and
 640 therefore burden, an identity federation requires of its
 641 participants in demonstrating conformance to its trust
 642 framework should be commensurate with the degree of risk it is
 643 designed to address. Frameworks that accommodate different
 644 kinds of transactions, with differing amounts of risk, may choose to offer multiple levels of
 645 conformance based on a graduated set of rules and requirements. This section provides options a
 646 Federation Administrator may consider when defining how they will establish conformance amongst
 647 its members.



648 7.1 Self-assessment

649 What is a self-assessment?

650 A self-assessment is the process by which a member organization (CSP or RP) evaluates its processes
 651 and systems against the stated requirements of a trust framework and is the simplest way for a
 652 member to demonstrate conformance within an identity federation. Used primarily in low-risk
 653 environments, self-assessments can often be completed using in-house resources and, therefore,
 654 impose a lower administrative burden on the member organization.

655 Trust frameworks often have a process by which its members can conduct their self-assessments and
 656 may set requirements for the degree to which all its requirements must be met in order operate
 657 within the parameters of the federation.

658 Upon completion of the assessment against requirements and standards, the trust framework may
 659 require member organizations to attest to their assessed conformance to the requirements of the
 660 trust framework.

661 When should they be used?

662 Self-assessment is an effective and efficient means to provide assurance that federation members
 663 conform to the rules and requirements of the trust framework. Self-assessment should be
 664 considered when federation members expect or require greater assurance than a signed agreement

665 in order to build trust amongst all its members. Self-assessment processes require assignment of
666 staff resources, but since the resources are internal to the organization, the assessment processes
667 can be planned and executed efficiently to minimize overall impact. Efficiency and higher assurance
668 are key considerations for establishing self-assessment conformance requirements.

669 7.2 3rd-party assessment

670 **What is a 3rd-party assessment?**

671 For federations that require higher levels of trust amongst their members, 3rd-party assessments
672 provide the means for members to demonstrate their adherence to the federation's operating rules.
673 As the name indicates, 3rd-party assessment arrangements involve independent entities trained and
674 certified to perform assessments of requirements for a specific community or trust framework.
675 Federation members employ certified assessors to evaluate their systems and services against the
676 framework's requirements and assessment criteria. It is typical for 3rd-party assessors to provide a
677 notice, or attestation of conformance, to the trust framework's rules on behalf of the service
678 provider.

679 **When should they be used?**

680 Independent, 3rd-party assessments are required when a higher level of assurance is needed to
681 demonstrate conformance among federation members, or when there is little tolerance for
682 operational risk. As with most risk mitigation strategies, higher assurance and lower risk will result in
683 higher burdens. The planning, contracting and execution of 3rd-party assessments will result in higher
684 costs than self-assessments, so the need and member expectations for greater assurance must be
685 justified. Third-party assessments must meet established federation standards and the results can be
686 relied upon with a higher level of assurance.

687 7.3 Audit

688 **What are audits?**

689 Audits are a standardized method for evaluating conformance to federation or industry
690 requirements. Auditors are typically certified to meet established requirements of audit
691 organizations. Independent audits may be required to ensure an identity federation member is
692 conforming, often both technically and procedurally, to a trust framework when high assurance and
693 low risk tolerance are needed and the federation does not provide for the certification of 3rd-party
694 assessors. A framework that requires audits as a means of acknowledging and enforcing
695 conformance often defines the specific roles and responsibilities associated with the auditors and
696 the auditees and identifies consequences should the responsibilities not be met.

697 In addition to defining how audits must be conducted, identity federations may include in their
698 framework documentation when and how often members should be audited in order to ensure their
699 continued conformance to the framework's rules and requirements.

700 As noted for 3rd-party assessments, it is typical for auditors to provide a notice or attestation of
701 conformance to the trust framework rules on behalf of the audited service provider.

702 **When should they be used?**

703 Identity federations that require their members to undergo audits usually do so because the
704 federation operates within an industry that is subject to regulatory or statutory oversight. The
705 burden on its members is high, but so is the potential harm associated with either not complying
706 with the requirements, or with a compromise of users' privacy or security. In fact, in many cases,
707 industries that are subject to these conditions will often form an identity federation to provide a
708 standardized method for its members to meet the requirements.

709

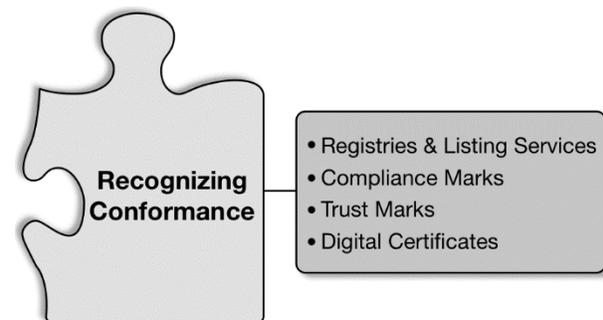
710

711 **8 Recognizing & Communicating Conformance**

712 Conformance recognition is the process by which identity
713 federations enable their participants to communicate alignment
714 with the technical rules and legal stipulations of the framework. It
715 is done only after completion of the selected conformance
716 testing process.

717 It is not enough for federation participants to simply establish
718 their conformance; they must also be able to communicate that
719 conformance to other federation members. In addition to
720 establishing cross-boundary trust, enabling discovery of
721 approved services and entities, and—in some cases—promoting a competitive service market, trust
722 frameworks must also be able to support mechanisms for the communication and recognition of
723 conformance. There are many ways this can be achieved, ranging in complexity from a simple
724 registry or listing service, to trustmarks and digital certificates. There are even emerging approaches
725 that seek to express federation conformance through dynamic and machine readable mechanisms to
726 allow for real time federation and inter-federation

727 Not all mechanisms are appropriate or necessary for every community, and they are not mutually
728 exclusive. As with most aspects of trust framework development, the selection of an appropriate
729 conformance recognition program and mechanism requires close coordination with community
730 members and a sound understanding of constituent needs. When considering which mechanism is



731 the most appropriate for an emerging trust framework it is important to take into account the
732 following considerations:

- 733 • The scalability and cost of implementing a recognition mechanism,
- 734 • The size of federation membership and amount of churn amongst members,
- 735 • The technical maturity of framework participants and the federation operator,
- 736 • The sensitivity and security requirements associated with the operating environment,
- 737 • Alignment with rigor of conformance evaluation, and
- 738 • Governance and management capabilities of the community.

739 8.1 Registries & Listing Services

740 What are registries and listing services?

741 The most basic and straightforward of recognition mechanisms, Registries and Listing Services offer
742 a scalable and easily implemented solution for communities and federation administrators to
743 communicate and discover services which have been deemed compliant with rules and
744 requirements. These may be as straightforward as a hosted website with approved services and
745 information about their conformance. The sophistication of the implementation, level of detail
746 provided on the listed service providers, and search and discovery capabilities are all easily tailored
747 based on the needs of the identity federation. Likewise, the cost and resources required to build and
748 stand-up such a service are relatively limited and directly tied to the sophistication required to meet
749 community needs.

750 Along with the limited cost of implementation and high scalability, there are some additional
751 considerations for the use of registries to present compliant services. Discovery requires framework
752 participants, especially RPs, to play an active role in seeking out and identifying compliant services.
753 This could limit the growth of federated services due to the effort required for each new service an
754 RP must discover and actively integrate with. Registries may offer listed organizations only limited
755 opportunity to market and advertise framework compliance since the format and content is often
756 standardized. Aside from pointing to the registration service through (ideally) approved messaging,
757 there are limitations for services to directly convey compliance from their own properties. As with
758 the discovery issues addressed above, this also requires RPs or potential users to actively seek out
759 the registry and confirm the services listed status.

760 When should they be used?

761 Registries for compliant organizations can be used for any type of federation, but are most typically
762 used where self-declaration or self-assessment is used to determine compliance with federation
763 rules. In this way, compliant services can be publicly listed for all federation members and for the
764 public in a simple, straightforward manner. There should be alignment between the rigor of the
765 compliance evaluation process and the type of conformance recognition mechanism or program that
766 is put in place. Registries, when used independently, are most appropriate for programs that
767 implement low cost and self-assessed processes. Similarly, registries offer a scalable, low cost means

768 to convey compliant organizations with low overhead and maintenance for the federation
769 administrator.



> There are many different examples of existing frameworks in both identity and cybersecurity that leverage registries and listing services:

- Identity Ecosystem Framework Registry, from the Identity Ecosystem Steering Group (IDESG)
- OIXNet, from the Open Identity Exchange (OIX)
- CSA STAR from the Cloud Security Alliance

770

771 8.2 Compliance Marks

772 What are compliance marks?

773 Often used to augment a registry listing to make marketing and discovery of compliant services
774 more effective, a compliance mark is a visually recognizable mark that can be placed on the web
775 properties and communication materials of complaint framework participants. These can—and in
776 most cases should—be further supported by electronic verification capabilities.

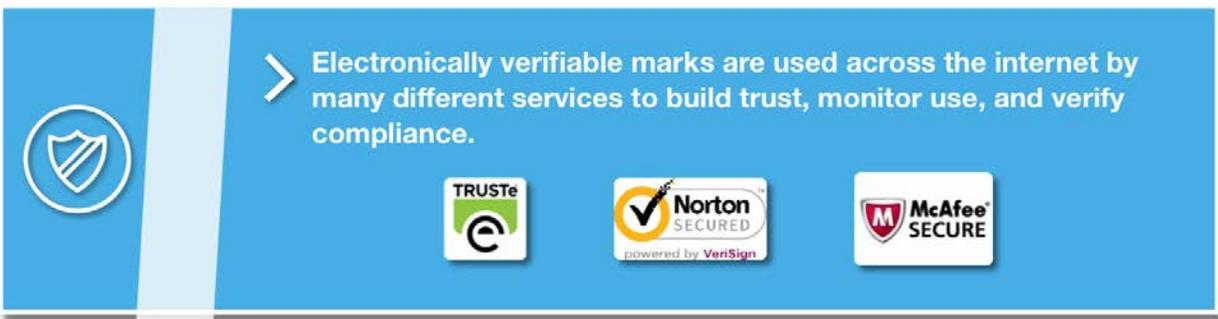
777 When should they be used?

778 Implementing compliance marks carries very little technical burden for framework participants
779 because, even when augmented by electronic verification, it requires little more than adding an
780 image and URL to a website, yet they do carry an overhead burden for the federation administrators.
781 Compliance marks are trademarked and legally protected images that require appropriate
782 documentation to be put in place by the federation administrator to ensure that they are registered
783 with responsible national or international authorities (e.g., U.S. Patent and Trademark Office) and
784 that the terms for their use are properly documented and agreed to by all participants.

785 Establishing terms of use and ensuring proper compliance mark registration are short term, typically
786 one-time tasks. However, to protect the integrity of the mark and the reputation of the framework,
787 the federation administrator or other delegated authority will need to maintain the capability to
788 monitor the mark's use, detect fraudulent or inappropriate applications, and initiate action to
789 remediate any infractions. While internal framework misuse, for example a framework participant
790 posting a modified or incorrect mark, can often be handled through the core legal and enforcement
791 mechanisms described in Section 5 of this document, addressing external misuse presents far
792 greater challenges. In addition to establishing processes to detect misuse (e.g., reporting
793 capabilities, web-crawling applications), the federation administrator would also need to have the
794 capability to take appropriate legal action against parties fraudulently using a mark (i.e., legal
795 counsel).

796 Electronically verifiable marks, for example those that have an imbedded URL linked to a registry or
797 listing, make the management and protection of compliance marks easier and enable users to more

798 effectively detect fraudulent representations. This can enhance trust and improve discovery in a
799 framework by enabling a community's participants to more easily identify approved service
800 providers.⁶



801

802 Generally speaking, the discovery and marketing value compliance marks bring to the table makes
803 them very valuable to frameworks and their participants—as long as the Trust Framework
804 Administrator is sufficiently able to institute and protect its compliance mark.

805 8.3 Trustmarks

806 What are trustmarks?

807 Like compliance marks, trustmarks are a visual indication that a service provider is compliant with a
808 federation's requirements.

809 Trustmarks comprise a very specific subset of compliance marks. In addition to being electronically
810 verifiable, these logos or seals are backed by rigorous third party validation, assessment, or auditing.
811 Certification of conformance and associated trustmarks may be issued by the assessor, the
812 federation, or a separate certifying body on behalf of the federation. The key point is that
813 certification trustmarks result from independent 3rd- party assessments and both the assessing and
814 the certifying organizations stand behind the certifications with their own brand name and
815 reputation. Therefore, trustmarks serve as a reliable and high assurance means to convey
816 compliance with federation rules.

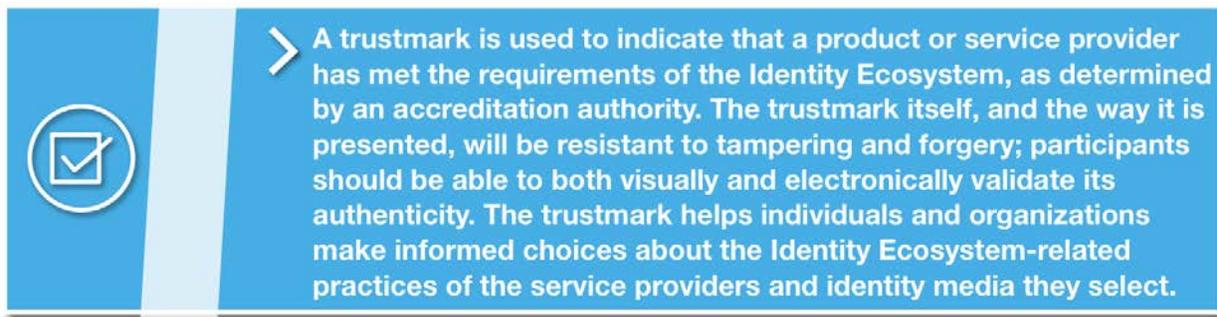
817 When should they be used?

818 The integrity of a trustmark is absolutely essential, both to promote widespread confidence among
819 framework participants and their customer base and to ensure the security of transactions. For this
820 reason, the trustmark must inherently be electronically verifiable and the method by which
821 electronic verification is conducted must be sufficient to prevent spoofing or modification of the
822 trustmark or the mechanisms by which it is verified.

823 For communities that support high risk transactions, which require rigorously verified identity
824 solutions, and support a strong certification program, trustmarks enable a broad but secure

⁶ The graphic provides several common examples of the many electronic verifiable marks & logos in use today. It is not exhaustive in nature.

825 recognition of compliant services. However, the degree of rigor and technical requirements for
826 properly instituting these marks makes them unnecessary for emerging or lower assurance
827 frameworks.



828

829 8.4 Digital Certificates

830 What are digital certificates?

831 Digital certificates are a specific type of electronic credentials that are issued and managed by a
832 centralized authority. Identify federations that employ an infrastructure that supports certificates,
833 called Public Key Infrastructures (PKIs), do so to meet their members' needs for a high-degree of
834 trust within the federation. In these situations, the Federation Operator serves not just to govern
835 and develop the framework, but also as the technical root of trust—also known as a Certificate
836 Authority (CA)—for all participants, issuing cryptographically signed certificates to members of the
837 community. These are, in turn, used to sign credentials issued to individuals and organizations
838 participating in the framework.

839 When should they be used?

840 Because of their high overhead (cost and procedural rigor), PKIs are generally only used in
841 environments that require a high-degree of assurance in the identities being exchanged within
842 closed communities, such as industry supply chains, organizations doing business with a government
843 entity, or research communities.

844 9 Conclusion & Other Considerations

845 This document provides a foundation for understanding identity federations and the trust
846 frameworks that underpin them. It is not intended to be a comprehensive how-to guide for creating
847 such a Federation, and only touches on many of the factors that contribute to one's success. For
848 organizations and communities to transition from planning and designing to building an operational
849 Federation, communities should consider additional elements, such as:

- 850 • **Governance.** Governance addresses how an Identity Federation, at its Trust Framework, is
851 managed and maintained across its life cycle. It defines how are decisions made, and by
852 whom.

- 853 • **Enforcement.** It may be necessary to enforce a federation’s rules and agreements, and
854 identity federations should define how this will be handled, and who will be responsible for
855 managing violations and adjudicating complaints.
- 856 • **Technical Protocols & Support.** An Identify Federation should decide what role it should play
857 in enabling the technical exchanges between its participants. This is done through identifying
858 standards, protocols, and technologies to support interoperability among its members.

859 Ultimately, identity federations enable communities and organizations to manage user identities and
860 identity data more efficiently by enabling interoperability between participants. Trust frameworks
861 provide the glue that binds these participants together—defining the rules for how they interact,
862 laying out roles and expectations, providing clear liability and legal processes, and enabling
863 determinations of conformance with Federation requirements. From supply chain risk management
864 to retail environments, the benefits of identity federations are substantial:

- 865 • The ability to consistently manage and understand risk across multiple organizations,
- 866 • The ability to limit organizational costs associated with managing individual identities,
- 867 • Streamlined user experience due to fewer credentials,
- 868 • The ability to scale and expand customer bases,
- 869 • The ability to provide more online services, and
- 870 • Increased ease of access to shared resources.

871 Furthermore, establishing identity federations can have impacts that extend well beyond the
872 boundaries of a single community or organization. By creating unified structures for managing and
873 understanding trust, the entire identity and security market will be better able to understand the
874 state of practices and processes, identify cross sector commonalities, and eventually break down
875 barriers (real or perceived) between sectors and markets. Eventually the expansion of federations
876 could support the overall health and security of the ecosystem, promoting more efficient practices,
877 and enabling consumers and citizens to more effectively access the services they both want and
878 need. While certainly not a silver bullet, trust frameworks and the federations they support
879 represent a shift towards a more consistent and extensible model for trust than more traditional
880 identity management with efficiencies that extend to all parties including users.

881 For more information on identity federations and trust frameworks, please take a look at the
882 “References Section” which includes references to several documents that go into greater detail on
883 deploying identity federations.

884

885 **Appendix A – Glossary**⁷

- 886 **Authentication** - The process of establishing confidence in the identity of users or information
887 systems. (NIST SP 800-63-3)
- 888 **Certificate Authority (CA)** – A trusted entity that issues and revokes public key certificates.
889 (NIST SP 800-63-3)
- 890 **Credential** - An object or data structure that authoritatively binds an identity (and optionally,
891 additional attributes) to an authenticator possessed and controlled by a subscriber.
892 (NIST SP 800-63-3)
- 893 **Credential Service Provider (CSP)** – A trusted entity that issues or registers subscriber authenticators
894 and issues electronic credentials to subscribers. (NIST SP 800-63-3)
- 895 **Federated Identity Management** – A means to enable users to access the systems and applications
896 of multiple organizations using the same login credentials; a process that allows for the conveyance
897 of identity and authentication information across a set of networked systems. (NIST SP 800-63-3,
898 referred to as *Identity Federation*)
- 899 **Federation Administrators** – Those responsible for the governance of an identity federation.
- 900 **Federation Credential Service Provider** – See Credential Service Provider.
- 901 **Identity** – A set of attributes that uniquely describe a person within a given context.
902 (NIST SP 800-63-3)
- 903 **Identity Ecosystem** – An online environment where individuals can choose from a variety of
904 credentials to use in lieu of passwords for interactions conducted across the internet. (NSTIC)
- 905 **Identity Federation (n.)** – The organizations that agree to follow the rules of a trust framework in
906 order to participate in an identity federation.
- 907 **Identity Management System (IDMS)** – Identity management system comprised of one or more
908 systems or applications that manages the identity verification, validation, and issuance process. (NIST
909 FIPS 201-2)
- 910 **Identity Proofing** – The process by which a CSP and a Registration Authority (RA) collect and verify
911 information about a person for the purpose of issuing credentials to that person. (NIST SP 800-63-3)
- 912 **Identity Provider (IdP)** – See Credential Service Provider.
- 913 **Identity Service Provider (ISP)** – See Credential Service Provider.
- 914 **Multi-Factor Authentication** – A characteristic of an authentication system or an authenticator that
915 requires more than one authentication factor. (NIST SP 800-63-3)

⁷ In this glossary, definitions not marked with a source were taken from the text of the document.

- 916 **Public Key Infrastructure (PKI)** – A set of policies, processes, server platforms, software and
917 workstations used for the purpose of administering certificates and public-private key pairs,
918 including the ability to issue, maintain, and revoke public key certificates. (NIST SP 800-63-3)
- 919 **Registrar** – Also known as a Registration Agent, a person who performs the enrollment process.
- 920 **Registration** – The process through which an applicant applies to become a subscriber of a CSP and
921 an RA validates the identity of the applicant on behalf of the CSP. (NIST SP 800-63-3)
- 922 **Registration Authority** – A trusted entity that establishes and vouches for the identity or attributes
923 of a subscriber to a CSP. The RA may be an integral part of a CSP, or it may be independent of a CSP,
924 but it has a relationship to the CSP(s). (NIST SP 800-63-3)
- 925 **Relying Party (RP)** – An entity that relies upon the subscriber’s authenticator(s) and credentials or a
926 verifier’s assertion of a claimant’s identity, typically to process a transaction or grant access to
927 information or a system. (NIST SP 800-63-3)
- 928 **Trust Framework** - The “rules” underpinning federated identity management, typically consisting of:
929 system, legal, conformance, and recognition.
- 930 **Trust Framework Operators** – See Federation Administrators.
- 931 **Trust Framework Providers** – See Federation Administrators.
- 932 **User** – A consumer of the services offered by an RP.

933 Appendix B – Reference Documents

934

935 NIST Publications & Programs

936 **FIPS 200: Minimum Security Requirements for Federal Information and Information Systems**, March
937 2013, <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>.

938 **FIPS 201-2: Personal Identity Verification (PIV) for Federal Employees and Contractors**, August
939 2013, <http://dx.doi.org/10.6028/NIST.FIPS.201-2>.

940 **SP 800-63-3 [DRAFT]: Digital Authentication Guideline**, [https://www.nist.gov/itl/nstic/special-](https://www.nist.gov/itl/nstic/special-publication-800-63-3)
941 [publication-800-63-3](https://www.nist.gov/itl/nstic/special-publication-800-63-3).

942 **The National Strategy for Trusted Identities in Cyberspace (NSTIC)**, <https://www.nist.gov/itl/nstic>.

943 **NIST Cybersecurity Framework**, <https://www.nist.gov/cyberframework>.

944 **NIST Risk Management Framework (RMF)**, <http://csrc.nist.gov/groups/SMA/fisma/framework.html>.

945

946 Identity and Risk Related Standards

947 **ISO/IEC 29115:2013: Entity authentication assurance framework**. Provides a framework for managing
948 entity authentication assurance in a given context. <http://www.iso.org/>.

949 **ISO/IEC 24760 Parts 1 – 3: A Framework for Identity Management**. Explores core concepts of identity
950 and identity management and their relationships and is applicable to any information system
951 that processes identity information. <http://www.iso.org/>.

952 **ISO 31000:2009: Risk management principles and guidelines**. Provides principles, framework and a
953 process for managing risk. <http://www.iso.org/>.

954 **ISO/IEC WD 29003: Identity Proofing and Verification**. Currently under
955 development. <http://www.iso.org/>.

956

957

958 **Trust Frameworks**

959

960 **The CertiPath Public Key Infrastructure (PKI) Bridge** enables cross organizational trust for its
961 member PKIs, including PIV-I providers. <http://www.certipath.com/FederatedTrust.html>.

962 **The Federal Bridge Certification Authority (FBCA)** allows US federal agencies to operate their own
963 PKIs and to interoperate with the PKIs of other agencies. <https://www.idmanagement.gov/>.

964 **FICAM Trust Framework Solutions (TFS) Program** is the federated identity framework for the U.S.
965 Federal Government. <https://www.idmanagement.gov/>.

966 **IdenTrust** provides trusted identity solutions for its corporate clients, across a wide range of
967 business sectors. <https://www.identrust.com/>.

968 **Incommon** is operated by Internet2, and provides a trust framework for use for by research and
969 higher education organizations, and their partners, in the United
970 States. <https://www.incommon.org/>.

971 **The Kantara Initiative** fosters identity community harmonization and interoperability across a range
972 of public and private organizations. <https://kantarainitiative.org/>.

973 **Minors Trust Framework (MTF)** is focused on children's identity and parental consent within the
974 context of complying with the Children's Online Privacy Protection Act (COPPA) and emerging
975 international policies. <http://www.generationalltrustalliance.org/minors-trust-framework/>.

976 **The National Identity Exchange Federation (NIEF)** is a collection of agencies in the U.S. that have
977 come together to share sensitive law enforcement information. <https://nief.org/>.

978 **The Open Identity Exchange (OIX)** is a non-profit trade organization which promotes trusted online
979 transactions across competing business sectors. <http://openidentityexchange.org/>.

980 **SAFE Bio-Pharma** was created by the biopharmaceutical industry and its regulators to support
981 identity trust for cyber-transactions in biopharmaceuticals and healthcare. [http://www.safe-](http://www.safe-biopharma.org/)
982 [biopharma.org/](http://www.safe-biopharma.org/).

983 **Transglobal Secure Collaboration Program (TSCP)** is a government and industry partnership that has
984 created a framework for the secure electronic transmission and sharing of sensitive information
985 internationally. <https://www.tscp.org/about-tscp/>.