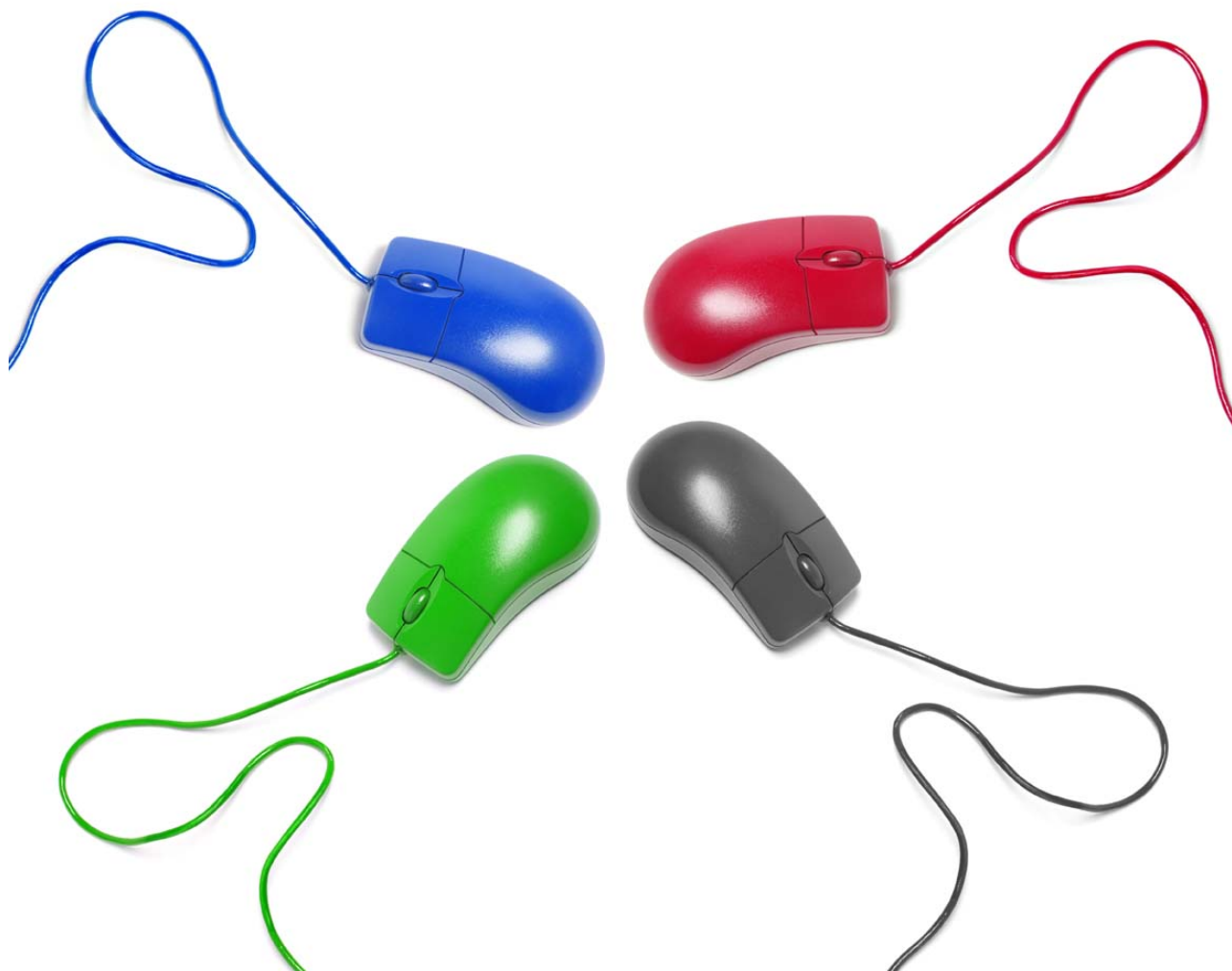


Identity Federation governance
Catalyst for the Identity Ecosystem



Contents

1.	Identity federation governance: Catalyst for the Identity Ecosystem	1
2.	Identity federation terms	2
3.	The case for identity federation	4
3.1	Value and benefits of federation	4
3.2	Identity federation trends and drivers	5
3.3	Risks and challenges	6
3.4	Need for governance	7
4.	Federal government role in Identity Federation governance	9
5.	Elements of Identity Governance: Trust framework implementation	10
5.1	Organizational governance	10
5.2	Technical and operational governance	11
5.3	Business and legal governance	12
6.	How Deloitte can help	15
7.	Contacts	16

1. Identity federation governance: Catalyst for the Identity Ecosystem

Today's identity and secure credential market can be compared to the bank card industry over the last 50 years. In the 1960s, the major credit card companies served their own member card issuers and participating retailers to provide credit transaction services at the point of sale (POS). Similarly, in the early 1970s, banks served only their own customers through proprietary Automated Teller Machine (ATM) networks. Several decades later, credit card customers (as well as other card providers) can perform transactions at the same retail POS terminals at retailers nationwide. Likewise, debit cardholders from most financial institutions can use most ATMs to withdraw cash, regardless of which banks operate them. Furthermore, cardholders can use both their debit and credit cards in ATMs and POS terminals. It is the federation scheme implementations of major credit card companies that established the universal retail electronic funds transfer (EFT) infrastructure. Years later, having leveraged this EFT infrastructure and governance model, the development of Electronic Benefits Transfer system in the mid-1990s took only approximately five years from design to implementation.

Similarly, over the last decade, governments and various organizations have implemented identity and credential schemes for secure access to their applications. Because of Homeland Security Presidential Directive-12 (HSPD-12) of 2004, which mandated secure identities and credentials for the federal government, the development and exchange of secure credentials originated in the government sector; and related policies, particularly around strong credentials even for commercial entities, historically have aligned with these government standards. Even as governments and companies continue to require highly secure transactions for sensitive applications (e.g., defense applications), they are also looking to authenticate at lower levels of assurance for both government and commercial applications. In order to avoid the high costs and inefficiencies of duplicative proprietary systems, these participants are working to leverage their infrastructures by aligning around a federated model. Over the last decade, various federations have been established that serve industry communities.

This paper shows how governance schemes that have been built around federated trust frameworks are being formulated to provide the needed structure for identity federations. Although in the secure identity and credential market, we still see large Identity Providers in the commercial sector that set their own rules to electronically collaborate with their business partners (e.g., supply chains), companies and organizations that need to collaborate outside their immediate environment have aligned to federation trust frameworks. This paper will focus primarily on secure identity and credentials; however, to the extent that nonsecure credential schemes illustrate the migration toward identity federation, these examples will be referenced.

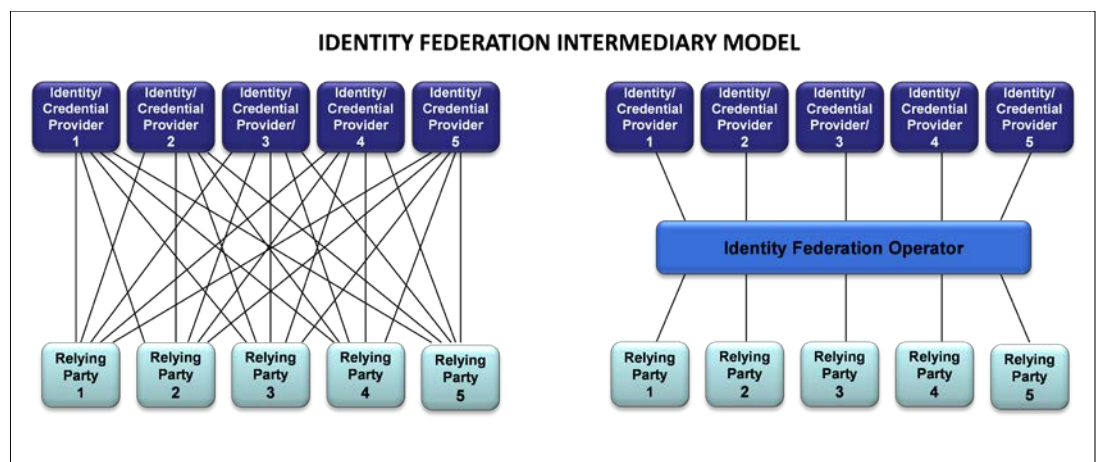
The target audiences for this paper are 1) companies and organizations considering participation in an identity federation to facilitate the use of secure credentials, 2) companies and organizations looking to stand up and operate an identity federation, and 3) government entities that operate applications requiring secure authentication.

2. Identity federation terms

The key concepts covered in this paper are defined below:

Identity federation. Identity federation is an interoperability model by which multiple Identity Providers agree to associate to allow their users to employ a single set of identification data, managed by the user’s “home” enterprise, to access the networks or specific applications of all entities in the association. The participants are responsible for authenticating their users and for vouching for the validity of their identities. Federation is achieved through the use of common standards, specifications, policies, and procedures to achieve uniformity and trust, which are enforced through governance.

Secure credentials and authentication. Users are issued secure credentials for the purpose of secure authentication to networks and applications. Secure credentials are issued at various levels of assurance. At a minimum, a secure credential is based on some degree of identity proofing. Examples include username/password (with identity proofing), username/password plus one or more attributes, software digital certificate, smart card, secure key fobs, username/code with biometric, etc. In a federated model, there has to be some standardization and agreement on what constitutes various levels of secure or assured credentials and the processes of authentication. In the federal government community, standards have been developed for secure identity credentials, i.e., Personal Identity Verification (PIV for government employees) and PIV-Interoperability (I) for government contractors and business partners. The federal government has also established four levels of assurance associated with credential types from Level of Assurance 1 (LOA-1 — lowest) to LOA 4 (highest). Both schemes have been adopted by companies and organizations that conduct business with the federal government and require access to government networks, applications, and/or data. Alternatively, a nonsecure credential may likely be a username/password without identity proofing of the user, for example, a social media or browser username and password because no identity proofing is performed as a prerequisite for issuance.



Intermediary model. The intermediary model refers to an identity federation scheme in which a federation operator serves as the link between the Identity Providers (and credential issuers) and Relying Parties. Each Identity Provider and Relying Party needs only to integrate to the

federation operator; the federation operator facilitates the authentication process between the Identity Providers and Relying Parties. In this way, identity can be dissociated from authentication, and likewise, Identity Providers are dissociated from Relying Parties. Individuals have the choice of what types and how many credentials they will maintain and to what Identity Providers they choose to entrust their sensitive identity information. An example of an intermediary model is the Federal Public Key Infrastructure (FPKI) bridge. In the bank card analogy, an example would be a credit card network's operating entity acting as the transaction intermediary. Relying Parties are able to extricate themselves from the issuance and maintenance of thousands of identities, usernames, and passwords or maintaining links to multiple third-party issuers.



3. The case for identity federation

The development of several federations and various identity trust frameworks in recent years demonstrates how companies and governments that collaborate to share information see the value in authenticating identities across domains for secure access. The section that follows describes the benefits, trends, and drivers associated with identity federation and how governance can help address several of these risks and challenges.

3.1 Value and benefits of federation

For entities that require secure collaboration or seek to have a diverse set of users access data they want to protect, identity federation represents several benefits, which include:

- **Single point of integration and policy enforcement.** In a federation model, all participants integrate to the federation operator using common standards, which also provides a single point for governance and policy enforcement.
- **Roles distinction.** In a federated model, the role of the Identity Providers is to manage the identity and credential and the Relying Party is responsible for authentication; their roles and responsibilities are defined and distinct. The responsibility for vetting, proofing and protecting, and securing a user's identity lie with the Identity Provider. In a federation, a user typically has one Identity Provider.
- **Reduced risk.** As a result of roles distinction, the Identity Provider is responsible only for the user's identity data and to validate for authentication; Relying Parties no longer need to establish and manage identities and be at risk for handling a user's privacy data. The risk is clearly defined and limited to the roles associated with each party.
- **Increased speed to market.** When operating through an intermediary model, each party needs only to integrate to the federation operator as opposed to each party in the association. This enables all parties to more quickly bring services and applications to market and enables users to access a broader set of services and applications.
- **Assured identities for Relying Parties.** Relying Parties are able to rely on the validity of the credentials they accept, that they are current, and that they are associated with identities that have had some degree of vetting and proofing.
- **Preemptive security solution.** Because of the ability to validate identities and credentials, a federation model represents a preemptive solution to secure access (letting legitimate people in) as opposed to a reactive one (keeping the wrong people out).
- **Privacy protection.** Only identity data required for authentication is passed to the Relying Party. Users no longer need to divulge extraneous data at multiple Relying Party sites, which preserves the integrity and confidentiality of the user's personal information.
- **Enhanced user experience.** The user needs to maintain fewer accounts and passwords while being allowed to access multiple resources and have their personal data protected.
- **Reduced operational costs.** Although the migration to federation involves up-front costs, in the longer term, it provides reduced account overhead through simplified password management, better provisioning and deprovisioning and less integration work associated with each Relying Party application and multiple Identity Providers as a result of standard interfaces.

- **Efficiency in governance.** Federation participants are able to execute a single multilateral agreement with the federation operator as opposed to bilateral agreements with multiple Identity Providers or Relying Parties.

3.2 Identity federation trends and drivers

Because of the lessons learned from the financial services industry and the leadership role taken by the federal government, the case for federation has gained momentum in the marketplace. Effective identity federation would mean a critical mass of individuals who could use a variety of credentials selected from the Identity (and credential) Providers of their choice for authentication to a variety of online applications unrelated to the credential issuers. The federal government refers to this environment as the Identity Ecosystem. Although the realization of an Identity Ecosystem has had a slow start, what trends and drivers can be expected to mobilize the migration?

Introduction of an intermediary model. Much like the bank card industry, the Identity Ecosystem will start to get traction when an intermediary model is adopted, whereby identity validation is dissociated from authentication, and likewise, Identity Providers are dissociated from Relying Parties. An example of where the intermediary model is being implemented is the federal government's Federal Cloud Credential Exchange (FCCX). (See highlighted box on p. 10). Another example is Transglobal Secure Collaboration Program, which is expanding its existing infrastructure from a Public Key Infrastructure (PKI) bridge to add a credential exchange for lower-level credentials and allow members to join as Relying Parties only.

Need to securely collaborate with business partners. The initial motivation for identity federation started with the need for business partners to securely authenticate into one another's applications and infrastructures for secure collaboration in an environment that will decrease the risk of security breaches. Examples include large companies collaborating with their supply chains and the federal government collaborating with its contractors. Historically, it has been the large and dominant entities that dictate the framework and requirements for secure credentials on the Relying Party side. Nonetheless, these frameworks and requirements served as the starting point for many of the third-party trust frameworks that exist today.

Maturing governance structure. For the last eight years we have seen the development of trust frameworks and interoperability guidance across the identity space. More recently, federations with maturing governance structures and governance bodies have started to emerge — often aligned to the federal government's Federal Identity, Credential, and Access Management (FICAM) trust framework — that produce and publish technical specifications and operating rules that standardize Identity Providers and Relying Party requirements and responsibilities.

Several organizations have established trust frameworks, i.e., Trust Framework Providers. Examples include the Kantara Initiative and Open Identity Exchange. Another example is the federal government's FICAM trust framework. These organizations have set up trust frameworks and processes by which Identity Providers and Relying Parties agree to trust and exchange credentials within their community of interest; entities that agree to participate in the framework are trust framework adopters. Although trust framework providers offer guidance on interoperability, exactly how the participants implement and technically interoperate is up to them and may be formalized through bilateral agreements.

Growth of operational federations. An operational federation not only has a trust framework, but also interoperability technical specifications with a bridge or credential exchange service and infrastructure that enable the actual exchange of credentials and secure authentication. The relationship is formalized through a multilateral agreement executed by Identity Providers and

Relying Parties with the federation bridge or exchange operator. Examples of operational federations that have taken root over the last five years are FPKI, InCommon, SAFE-BioPharma and TSCP.

Early development of business model. Because the migration to an intermediary model is still in the early stages, the prevailing model is still one in which Relying Parties issue credentials to access their applications, i.e., Identity Providers and Relying Parties are one and the same. Under these circumstances, there is no need for a business or liability model. When identity and credential holders start to use their business or third-party credentials to perform commercial and retail applications, normal business practices imply that the Relying Party may likely expect the Identity Provider to accept liability in the event the credential is used fraudulently and damages result.

Today, Identity Providers cover their credential issuance and management costs. When acting as Relying Parties, they also cover their enablement costs; and federation operators typically cover the costs of operating the federation services through membership dues and fees. As the intermediary model is established, Identity Providers and Relying Parties are looking for a business case to justify the costs of credential exchange. Extending the usage of secure credentials into the commercial and retail sectors further dissociates the Identity Provider's business case from the Relying Party's business case. The costs will have to justify the value.

3.3 Risks and challenges

As with the introduction of a new business structure, there are several risks and challenges that need to be addressed and resolved. For identity federation to be effectively implemented in the marketplace, some of the risks and challenges to be addressed are as follows:

Need for executive support. Today, there are early identity federation schemes in which the “big” players established the rules and smaller business partners participate accordingly. The establishment of third-party federations, with the requirements of participants to work across domains (and often with competitors), means that the participants' interests have to be met and legal agreements need to be signed. Often, it may require that additional controls be put into place to protect proprietary information. Naturally, this requires a much higher degree of participating company commitment, executive support, and legal review.

Undefined business model. While the business case for federation in the aggregate is compelling, the details of the business case and model are not yet defined. Although there are many business benefits to participating in an identity federation, it is often difficult to isolate and

FICAM/ICAM:

Government Federated Identity Trust Framework

Since 2004, the federal government has collaborated with industry to develop a trust framework and promote the adoption of the common Personal Identity Verification (PIV) and FICAM standards and specifications. The General Services Administration (GSA) has established a methodology so that commercial and other government identity partners can participate in a federated environment, commonly known as the ICAM program. ICAM addresses design requirements for digital identity, credential, and access management and promotes interoperability and consistency for implementing ICAM programs. The ICAM program components include:

- Federal ICAM (FICAM) Roadmap & Implementation Guidance
- Personal Identity Verification (PIV) Credential Issuance
- Personal Identity Verification Interoperability for Non-Federal Issuers (PIV-I)
- Federal Public Key Infrastructure (FPKI)
- Trust Framework Providers Adoption Process (TFPAP)
- Trust Framework Solutions (TFS) Program
- FICAM Scheme & Technical Profiles Adoption Process
- Certification of Identity Providers

Together, the complete body of governance documents covers the four levels of assurance credential strengths. Initially developed for interoperability across the federal government, the FICAM trust framework has been extended for the benefit of the government's external partners and their credentials.

identify the cost savings within a specific organization and also requires an up-front investment. The following questions will need to be answered: In an intermediary model, who pays what to whom and under what circumstances? How are Identity Providers compensated? Will Relying Parties pay fees? If so, how much?

Effectiveness dependent on critical mass. Achieving critical mass is essential for the effectiveness of identity federation. Much like the bank card example, unless there are many issuers and acquirers participating, the benefits of a shared and leveraged infrastructure are not achieved and costs are not distributed or lowered. In the interim, there have to be enough participants willing to shoulder the burden until critical mass is reached.

Partially standardized credentials and processes. The identity federation landscape consists of groups that cater to particular industry segments that have either adopted common standards and processes or created their own. In the secure credential market outside of PIV/PIV-I (using PKI), there is no uniformity yet in credential formats and strengths and authentication processes.

3.4 Need for governance

Identity federations have established and follow rules and specifications that enable interoperability, trust, and governance within a particular community of interest or domain. Identity federations facilitate the validation of identity credentials between trust domains using an intermediary model leverage common infrastructures and commonly accepted policies and specifications.

Effective federations are built around trust and a trust framework, which is a set of rules, requirements, and agreements that enable Identity Providers and Relying Parties to conduct identity verification transactions in a secure environment that protects the privacy of credential holders. Operational federations not only follow a trust framework, but also establish a governance structure to ensure that the elements of the trust framework are implemented.

Federation governance leads to the expectation that interoperating system participants will follow the same processes and procedures when validating identities for enabling access. The foundation for governance is based on some key principles:

- Governance starts with the policies or even laws that establish the requirements for identities, credentials and access transactions.
- To enable the policies to be operationalized, standards, specifications and rules are derived from them.
- Each network or system establishes a federation trust framework that incorporates these standards and defines the rights, responsibilities, and requirements for participants to

NSTIC Identity Ecosystem Framework: Mobilizing the Identity Ecosystem

The federal government is looking to extend secure Internet access and transactions to the public at large, i.e., businesses and individuals. Toward that end, in 2011 the federal government released the National Strategy for Trusted Identities in Cyberspace, commonly known as NSTIC. In this strategy, the concept of the “Identity Ecosystem” was introduced. The vision is to establish a secure online environment for conducting transactions across the Internet and leverage components that are already in use to achieve identity portability across participation systems while protecting users’ privacy.

A key concept of NSTIC is to enable individuals to use secure credentials that either have already been issued to them, or they procure on their own, in order to conduct online transactions in lieu of depending on credentials issued by each Relying Party.

To jump start and coordinate this initiative, the NSTIC National Program Office was established by the National Institute of Standards of Technology (NIST), Department of Commerce, which in turn set up a Steering Group composed of commercial sector participants whose task it is to administer the process of developing the trust framework and governance documents.

operate within that system, in addition to their own policies and requirements (e.g., bank-specific ATM withdrawal limits).

- Checks and balances need to be established in the form of accreditation authorities to validate that participants are abiding by the rules.
- In order to reposition identity federation from concept to an operational business, the business and legal issues need to be addressed. Except in the case of a legal mandate, parties to identity federation transactions need to build a business case to justify the investment and operational costs; in other words, can the parties achieve revenues, cost savings, enhanced security, and/or brand reputation protection? What are the liabilities and how are they allocated? The business liability model needs to be documented as part of the governance scheme in the form of a liability allocation and fee structure.
- A governance body needs to be established to maintain and enforce governance.



4. Federal government role in Identity Federation governance

Over the last 10 years, since the announcement of HSPD-12, the federal government has issued policies, standards, and specifications related to identities, credentials, access management, and information sharing both for government agencies and for entities that interact and interoperate with the federal government.

Over this time period, the federal government has developed an infrastructure of identities, credentials, and authentication systems. In the interest of economy and efficiency, the federal government seeks to leverage the credentials already issued and used by its industry partners rather than issue separate credentials for use on government networks. In the United States, the federal government has taken a lead role in establishing and promoting standards and specifications for identity federation in order to:

- Facilitate interoperability across the federal government;
- Promote interoperability across its government and commercial partners; and,
- Extend secure authentication and access to the public at large.

The major federation initiatives within the federal government that have advanced the exchange of identities within and external to government agencies are FICAM (including the FPKI), the National Strategy for Trusted Identities in Cyberspace (NSTIC) Identity Ecosystem Steering Group (IDESG), and the FCCX. These initiatives are described in the highlighted boxes.

FCCX:

Operational Government-Citizen Federation

The federal government is in the process of developing an operational federation that will allow individuals to conduct secure transactions over the Internet when accessing government-sponsored programs using their own credentials. The system being developed is called the Federal Cloud Credential Exchange — FCCX. It will enable citizens to access online government services, for example, health benefits, student loan information, and retirement benefit information, using various commercially issued credentials. The FCCX operator is the U.S. Postal Service. The governance around FCCX is being managed by GSA.

In most cases, citizens currently need to establish a username and password to authenticate and access each agency application. In addition, the agencies have to then manage and protect these identities. Thus, the agencies act in both the role of Identity Provider and Relying Party in the current model. The introduction of FCCX, which will be a federation operator, will enable agencies to accept a user's commercial credentials, alleviating the need for agency-issued credentials. The FCCX operator will maintain the connections to all the participating issuers, which will enable agencies to maintain a single connection to FCCX. If agencies wanted to accept commercial credentials in the absence of FCCX, they would have to maintain connections to all commercial issuers from whom they accept credentials. In addition to streamlining and increasing the security of their applications and lowering costs, FCCX is expected to improve the user experience.



5. Elements of Identity Governance: Trust framework implementation

While the identity and authentication infrastructure and technical specifications are critical to the foundation of federated systems, these federation schemes cannot be effective without supporting governance structures. Federations operate within an established governance structure that is memorialized in a series of governance documents. Governance can be categorized into three areas: organizational, technical/operational, and business governance. Each is described in the sections that follow.

5.1 Organizational governance

Organizations that operate in a federated environment typically make use of several governance documents to establish:

- how the federation entity and its participants will operate;
- how decisions will be made;
- who in the organization will perform what duties/responsibilities;
- how members or participants will be bound to the federation; and,
- how adherence to the federation rules and requirements will be validated.

The organizational policies and processes consist of foundational documents, federation agreements, and the accreditation process. Though not directly related to the operation of a federated system, the foundational documents — the charter and bylaws — are important for establishing the fundamental requirements for participation and decision making, in other words, organization governance. Through agreement to the bylaws, members bind themselves to the decisions made by the representatives who have been voted in to make these decisions.

Organizational governance polices and processes		
Foundational Documents	Charter	Grants authority to the federation organization; defines its purpose, function, rights, obligations and privileges; and establishes the governance body.
	Bylaws	Establishes membership and participation requirements, how the governance body will be selected and structured, and how decisions will be made for the organization. Describes the roles and responsibilities of the federation and its members for the governance of the federation.
Participation Agreements	Membership Agreement	Defines terms and obligations for membership in the federation and participation in governance of the federation. Describes the requirements of the federation as an entity and its members and binds them to the organization bylaws.
	Federation Participation Agreement	Either all or a subset of members participate in the operational federation for the exchange of credentials; these members sign a multilateral bridge federation services agreement in which the technical/operational governance documents are incorporated by reference.

Organizational governance polices and processes		
	Service Agreements	Document whereby members agree to perform in accordance with their trust framework roles. Agreement(s) for those companies or vendors that provide technical services for the operation of the federation, e.g., bridge service operator, third-party services for attribute exchange.
Certification and Accreditation Process	Certification and Accreditation	Process that verifies that the design and implementation of a participant's system meets trust requirements established by the federation, e.g., credential issuance process, authentication process, business practices, policies and procedures, key life cycle management, security controls, and environmental controls.

The participation agreements bind the parties to their responsibilities and obligations as participants in the federation. The federation organization is responsible for ensuring that all the participants comply with its policies and standards, and that every participant can rely on the fact that all other participants are playing by the rules, which requires an accreditation process. A federation organization or framework provider normally establishes an accreditation process to which participants are required to periodically submit.

In some cases, a federation organization may even establish a trustmark, which is a logo or symbol on their application website that indicates a participant's compliance and participation in the federation, as determined by an accreditation authority.

5.2 Technical and operational governance

A participant's level of interoperability is dependent on the type or types of credentials it issues or accepts. In the case of strong LOA 4 credentials, the participant (Identity Provider or Relying Party) must cross-certify to a PKI bridge, normally through an established bridge service. In addition or alternatively, the participant can agree to exchange non-PKI lower levels of credentials through a credential exchange. Note that the Certificate Policy (CP), Certification Practice Statement (CPS), and Criteria and Methodology for Cross-Certification (C&M) relate to PKI for those organizations that issue and transact using highly secure credentials, particularly at a LOA 4. The Technical Specifications and Common Operating Rules apply both to PKI and non-PKI credentials.

A federation's operations are based on interoperability through a set of policies, standards, and technical requirements that are embodied in the operational governance documents. Assuming a federation operates in both a PKI and non-PKI environment, the primary technical and operational governance documents include CP, CPS, C&M, Technical Specifications, and Common Operating Rules.

Technical and operational governance documents		
PKI	Certificate Policy (CP)	Set of rules that identifies the applicability of a certificate to a community or domain and/or class of application with common security requirements, defined independently of the specific operating environment. Maintained by the Policy Management Authority, it defines the standards, policies, and procedures for processing certificates across the federation community.
	Certification Practice Statement (CPS)	Statement of the practices employed by a Certificate Authority in managing PKI's certificates in accordance with its organizational structure, operating procedures, facilities, and computing environment of the operating entity. Describes how the CP is interpreted in the context of the system architecture and operating procedures of its members.

Technical and operational governance documents		
	Criteria and Methodology for Cross Certification (C&M)	Identifies the criteria for eligibility for cross-certification and defines the methodology for implementing and maintaining cross-certification with the federation's Operator Bridge by external entity PKIs and PKI bridges.
PKI and Non-PKI	Common Operating Rules	States and consolidates operational requirements and processes that allow all parties to understand "who does what to whom." Includes sections on issuance, authentication, transaction processing, and security and privacy requirements. May also include general liabilities across the operational components. Incorporated by reference into the participation agreement.
	Technical Specifications	Requirements that define standards to be followed and specifications for interfaces and formats for credentials and interoperable authentication transactions as expressed in the Common Operating Rules.

¹Non-PKI credentials at LOA 1-2 can include Personal Identification Numbers, user names, and passwords; LOA 3 may be a password or biometric factor in combination with a hardware token, software token, or one-time password device token.

5.3 Business and legal governance

Over the next several years, the expectation is that the identity access market will start to see the:

- Use of secure government and company-issued credentials for business and sensitive commercial applications (e.g., banking and medical records), and
- Use of standard Internet credentials (e.g., browser/social media usernames and passwords) for applications requiring lower levels of assurance.

Similar to how the card networks incorporate the requirements of the Electronic Funds Transfer Act and related laws and regulations into their governance frameworks, the identity federations have incorporated the body of government policies related to identity and credentials largely because up until now, even these corporate and commercial credentials have largely been used in government programs. In order to extend this enhanced secure functionality into the commercial and retail sectors, there are important factors that shape the governance around federation: the legal framework, the liability model, and the business model. For the commercial market, there are at least three major considerations:

- Protecting a user's private information;
- Ensuring that in the event something goes wrong with the transaction, someone is holding the liability if damages result; and,
- Offsetting the costs of managing and transacting with the credentials, and potentially earning revenue.

Legal and policy framework. Governance starts with the policies or even laws that establish the requirements for identities, credentials, and access transactions. For example, the salient policies related to identity credentials and federated identity for the federal government are:

- HSPD-12, PIV, and PIV-I policy
- Federal Information Processing Standards Publications and special publications related to information security published by the NIST, U.S. Department of Commerce
- GSA/Office of Management and Budget and Department of Defense external credential policies

- DoD identity and Common Access Card policies
- GSA and DoD PKI and non-PKI credential and interoperability policies

The requirements of these policies are incorporated into the governance documents for the federal government. The federal government’s business partners and trust framework providers have incorporated PIV-I policies into their governance documents.

Similarly, identity federations that are dedicated to specific communities of interest incorporate policies associated with their industries, e.g., financial services, aerospace and defense, pharmaceuticals, etc.

Liability model. Because the PIV program and levels of assurance for identities and credentials are inherently governmental and the federal government does not accept liability, the terms of liability around identity and credential transactions are relatively immature. Overall, the perspective is that the proofing, vetting, and credential checking behind PIV, PKI, and LOA3 credentials are much more secure than using usernames and passwords — which are still largely used for most applications — so Relying Parties should be willing to accept them without provisions for liability against the Identity Providers. In general, for these credentials, each party accepts liability for its reliance on the credential.

In the commercial environment, however, when using PIV-I or similar company credentials in conducting business, liabilities are assigned and allocated in the event one of the members fails to operate in compliance with the governance requirements and damages result. Although we are starting to see retail and commercial applications accepting Internet

(insecure) credentials, for the most part, they issue their own credentials, i.e., users are issued usernames and passwords, which are managed by companies and retailers; under these circumstances, there is no need for a liability model. For Relying Parties that accept Internet credentials, liabilities are either established by agreement with the Identity Providers or the retailer assumes the risk based on the perceived benefit of accepting a credential whose identity has been at least minimally established by a known Identity Provider.

When employees start to use their business credentials to perform retail applications, Relying Parties likely will expect the Identity Provider to accept liability in the event the credential is used fraudulently and results in damages. At a minimum, if the Identity Providers are unwilling to

FCCX:

Operational Government-Citizen Federation

The federal government is in the process of developing an operational federation that will allow individuals to conduct secure transactions over the Internet when accessing government-sponsored programs using their own credentials. The system being developed is called the Federal Cloud Credential Exchange — FCCX. It will enable citizens to access online government services, for example, health benefits, student loan information, and retirement benefit information, using various commercially issued credentials. The FCCX operator is the U.S. Postal Service. The governance around FCCX is being managed by GSA.

In most cases, citizens currently need to establish a username and password to authenticate and access each agency application. In addition, the agencies have to then manage and protect these identities. Thus, the agencies act in both the role of Identity Provider and Relying Party in the current model. The introduction of FCCX, which will be a federation operator, will enable agencies to accept a user’s commercial credentials, alleviating the need for agency-issued credentials. The FCCX operator will maintain the connections to all the participating issuers, which will enable agencies to maintain a single connection to FCCX. If agencies wanted to accept commercial credentials in the absence of FCCX, they would have to maintain connections to all commercial issuers from whom they accept credentials. In addition to streamlining and increasing the security of their applications and lowering costs, FCCX is expected to improve the user experience.

accept any liability, an agreement should be in place that states as much, and the Relying party should agree to not sue for damages.

Business model. Today, each party to identity and authentication transactions covers its own costs — issuance, enablement, management, and operations, as applicable. The extension of company or third-party credential usage into commercial and retail applications and the adoption of an intermediary model will require Identity Providers and Relying Parties to separately justify the costs of credential exchange by way of a business case.

For example, Relying Parties can claim a benefit or value if they can accept secure credentials in lieu of issuing and managing lower levels of credentials to access their own applications. Issuers, on the other hand, may expect to be compensated for the use of their strong credentials in commercial and retail applications, particularly if they are expected to accept liability; and federation operators — bridge services and credential exchanges — may likely also expect to be compensated for providing the infrastructure and services that enable interoperability between the issuers and Relying Parties. Although there are successful models from which to baseline a business case for identity federation, a viable model has yet to be adopted in the secure credential space. In the government world, use of secure credentials can be mandated. In the commercial world, there has to be a business case. While some of the nonsecure Internet identity providers (e.g., social media websites) allow their credentials to be used on other websites to learn more about their customers' on-site activity, no such benefit is yet established in the secure credential market.



6. How Deloitte can help

Similar to the evolution of bank card systems in the United States, governments and organizations that host proprietary identity-based access systems have started to leverage their investments and extend access through federation. Extending interoperability to the degree necessary to establish a vibrant and operational Identity Ecosystem requires an effective and standardized governance structure — organizational, technical, and business governance — that is adopted by a majority of the participants.

Effective development and implementation of an identity federation governance model require a diverse set of capabilities. Deloitte has strong experience in developing governance models and supporting policy; along with the corresponding enforcement and assessment and implementation:

- **Federation trust framework.** Advises customers in developing the organizational, technical, and business governance structure required for participants to trust the identity credentials and parties for authentication within an identity federation.
- **Federation governance policies and processes.** Provides the experience to develop and produce the policy and process documents required to support the governance structure for an identity federation for PKI and non-PKI transactions. Governance documents include, but are not limited to, Charter, Bylaws, Membership Agreements, Federation Participation Agreements, CP, CPS, C&M, Common Operating Rules, and Technical Specifications.
- **Certification and accreditation process.** Assists customers in the development of a process to compare the design and implementation of a participant's system against the trust requirements established by a federation, e.g., credential issuance process, authentication process, business practices, policies and procedures, key life cycle management, security controls, and environmental controls.
- **Trust partner applications.** Assists customers in the application process for identity partner relationships with the federal government, specifically organizations seeking to become cross-certified to the Federal Bridge Certification Authority or to become a Trust Framework Provider.
- **Trust framework requirements and specifications development.** Assists in the development of requirements and specifications that will define a trust framework's policies, procedures, and requirements for identities, security, data, privacy, and interoperability and the roles and responsibilities of each party.
- **Trust framework system design and architecture.** Provides the experience to define the architecture, components, interfaces, and data for the systems and networks to fulfill the requirements of the trust framework specifications and requirements.



7. Contacts



Gordon Hannah

Principal

Federal Technology Risk
Deloitte & Touche LLP
+1 571 882 5930

Chris Goodwin

Principal

Federal Technology Risk
Deloitte & Touche LLP
+1 571 882 6923

Rick Siebenaler

Principal

Technology Risk Midwest
Deloitte & Touche LLP
+1 312 486 4137

Iana Bohmer

Senior Manager

Federal Technology Risk
Deloitte & Touche LLP
+1 571 882 5406

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

