



## **Tier 2 Business Guidelines: 401K Scenario**

## **Introduction to the Abstract**

This whitepaper focuses on one specific Liberty Alliance-enabled application area: 401K servicing, provisioning, and support.

As a tier 2 document, this paper moves beyond a basic discussion of what Liberty does and how it operates into actual business issues and models with regards to the 401K scenarios.

This paper is targeted to audiences on all sides of the 401K arena including corporations that offer them to their employees, the organizations that manage and sell them and potential business partners whose equities and funds might be offered and traded through these plans.

### **Editors**

Deidre Sullivan

Darren Calman

### **Company**

Phaos Technology

Phaos Technology

### **Contributors**

Jennifer Schlapak

Frank Kaupa

Jeff Palmeri

Diana Heutmaker

Ravikanth Erramilli

Bob Arndt

Andrew Shikiar

Yvonne Lee

### **Company**

Fidelity

American Express

American Express

American Express

American Express

American Express

Sun Microsystems

Sun Microsystems

## **401K and Employee Benefits Account Access**

Today a number of *Fortune* 100 companies are deploying solutions based on federated identity standards that provide employees with individual IDs and passwords to securely access external records, retirement funds, and other employee benefit resources via a single portal.

In this new model, a consumer or business only enters their password once and is able to move to trusted sites without re-keying their identity information. This is an example of identity federation.

A federated identity model enables every business or HR department to manage their own data distribution versus relying on a central authority like a certificate provider.

By deploying new federated network identification standards, organizations address the security issues around:

- transmitting confidential information
- assuring identity / mapping of identities
- balancing authentication risk and liability among trading partners

This model also enables HR executives to better manage the employee lifecycle process. HR, for example, can enable a new hire with immediate resource access or revoke all privileges of a terminated employee. They can limit access levels via different networked devices (laptop, cell phone etc...) and can also create an audit trail in case of security breach—an important consideration in light of all the new breach disclosure legislation.

For employees, the benefits are significant. A unified view of total employee compensation eases navigation through benefit plans (most of which currently rely on external providers) and improves morale. By aggregating all resources in one portal, employees can also see the true and full value of their compensation.

## **The Factors Driving Adoption**

A number of factors are driving large enterprise organizations and their financial services partners together to embrace the 401K federated applications model.

Enterprise organizations are seeking ways to establish:

- an employee self service model
- single portal for all benefits and key company information
- a secure pipe to large resource providers
- a more balanced risk management model
- improved employee relations through better technology deployment and ease of use
- compliance with privacy regulations

401K Providers are looking for ways to:

- securely connect to their corporate customers' employees
- enhance their protection from fraud
- enable new types of online business
- differentiate their offerings from their competition's
- address regulatory requirements
- obtain information of customer's employees in a simpler and quicker fashion

## **Understanding the Impact of Federation in the 401K Application Space**

Over the past several years, technological innovation has dramatically opened up what is possible in terms of using identity to create a range of different kinds of trusted relationships with employees, business partners and customers. Today's most forward thinking organizations are looking beyond the tactical issues of single sign-on, application provisioning, and core trading relationship communications security and are beginning to explore how digital identity can actually change their business models.

For example, instead of simply looking to secure B2B, B2C, and B2E transactions, these organizations are considering the possibilities of relationship models like B2B2E where identity facilitates trading relationships between/among partners and extends those relationships to each partners' representatives (employees). In a sense, this allows technology to mimic a traditional contractual trading relationship between firms where authorized employees execute the contractual terms and conditions day-to-day.

In this new world, if a trading partner has strong identity management and authentication technology in place, then that organization is understood as having reached a certain threshold in the marketplace. This threshold can be leveraged to provide a level of assurance to others in multiple untapped markets.

For instance if organization "A" authenticates and authorizes a principal in organization "B," and if organization "B" authenticates and authorizes a principal in organization "C" by exactly the same rules, then organization "A" should be able to accept transactions from organization "C" without going through a separate authentication process. As we will see, this can enable new business opportunities.

The 401K application is an ideal scenario for federated identity that will provide short-term gains in organizational efficiency while also positioning the company to expand their business models.

## **Learning from Early Adopters about Security and Deployment**

A number of Fortune 100 companies have 401K Liberty-enabled implementations up and running. Their experience has taught the marketplace to:

- Carefully evaluate proprietary solutions versus standards-based ones and how the choice impacts moving towards federation. Question all "quick and dirty" solutions. If something sounds too good to be true, it probably is.
- Deploy extensible components that can be leveraged both internally and externally.
- Establish guidelines around passwords, access and employee behavior (see addendum A). This "human element" represents persistent areas of risk.
- Educate key constituencies on what it means to be a service provider and an identity provider.
- Continually evaluate new levels of risk. Ask the hard question: does the enterprise want to assume this burden?

## **Technology Standards Creates Business Flexibility and Opportunity**

Not every trading partner or individual will have the resources to install their own large-scale identity management solution or technology, nor will it be necessary. The critical enabler for this expansion is the deployment of standards-based interfaces and technologies. In the simplest terms, smaller and medium-sized enterprises need to be able to "plug and play."

An organization's smallest partners should be able to interact under the same rules as the largest. This approach provides:

- Consistency of business policies and procedures
- Economies of scale
- Equal protection and/or services for all clients – whether it's the average small investors represented by large firms or high net worth individuals represented by boutique financial services advisors
- New business opportunities
- Relationship loyalty between trading partners
- Cost savings by distributing identity management logistics to trading partners
- Liability distribution by having trading partners assume appropriately shared liability for transactions

### **The Liberty Alliance's Contribution to the 401K Application Arena**

The Liberty Alliance was established in December 2001 and is the only open, global organization working to address the business, technical and policy aspects of federated identity management. Consisting of over 150 members across multiple industries, the Alliance develops open standards for federated identity and identity-based web services.

Senior executives from the world's leading financial services organizations and systems providers count themselves as a driving force behind the Alliance. Their contributions have helped to ensure that Liberty's technical, business and policy output address the specific needs of consumers, financial organizations, and regulators in the financial arena.

The Liberty Alliance is unique among standards-setting organizations. While other forums are producing technology platforms for building web services, only the Liberty Alliance is devoting attention to not only building standards but providing the business and policy best practices that allow those standards to work across industries, across the globe and in a privacy and security-enhancing manner.

### **Introducing Specifications in Phases**

Liberty's specifications have been introduced in phases. The Phase One Specifications, introduced in July 2002, focused on enabling interoperability between technology systems to make it easy for businesses to provide opt-in account linking and simplified sign-on functionality to partners, customers and employees.

Phase Two, released in November 2003, represents a Web Services Framework that provides organizations with an open, standards-based way of delivering identity-based web services that can enable new revenue opportunities, cut internal IT costs and make web services more secure and private. Because the Liberty specifications are built on existing open industry standards such as SAML, SOAP, XML and WS-Security, they can be deployed and supported in any environment and maximize an organizations investment in non-proprietary standards.

Future Phases of the Alliance's specifications will focus on actual web service interface specifications. For example, calendar, contact book, billing and location services. The Alliance's open architecture allows for development of vertical-specific services (hypothetically, an 401k rollover service) that could adhere to the Liberty architecture and plug in seamlessly to a Liberty-enabled identity deployment.

Collectively, the Liberty specifications can enable deployment of a "Circle of Trust". A "Circle of Trust" is a group including at least one service provider and at least one identity provider that have both technology and business agreements in place for interactions based on linked identities. Once a user has been authenticated by a Circle of Trust identity provider, that individual can be easily recognized and take part in targeted services from other service providers within that Circle of Trust without needing to re-authenticate for each provider and service. It should be noted that this concept of 'trust-based relationships' between organizations and their individual or joint customers has existed in the offline business world for years; two common examples would include travel alliances and affiliate business partnerships, and the Circle of Trust automates such relationships through federated identities.

### **Understanding the Elements of a Liberty 401K Application**

There are two critical application providers in a 401K scenario: the Identity Provider and the Service Provider.

#### **The Role of 401K Identity Provider**

A Liberty-enabled Identity Provider is an organization recognized by the members of a circle of trust as the entity responsible for users' (or "principals") digital information and identity. Identity providers enter into partnerships with service providers and provide services that follow agreed-upon practices set by all parties. By offering services that adhere to the Liberty Alliance specifications, businesses can off-load the management of digital identities to Identity Providers and offer online services at lower cost per customer, employee or partner. Within the context of the 401K application offering, the Identity Provider is most often the enterprise looking for ways to manage HR information of their employees.

#### **The Role of the 401K Service Provider**

A Service Provider is an entity that provides services/goods to principals. In the context of a Liberty-enabled deployment, a service provider needs to be able to accept and process authentication information it receives from an identity provider so that it may then provide the services to the principals. The Service Provider must also follow agreed-upon business practices set by all parties. Within the context of the 401K application offering, the service provider is a financial services company that offers 401K plans.

#### **Identity Provider Benefits**

- Extensibility: Once the architecture is built, it is reusable to other areas within the organization as well as to access resources at other service providers within a circle of trust.
- Improved depth of the offering to employees by providing secure access to different services such as advice on funds, education and any other 401K embedded information.
- Allows the entity that is potentially the most intimate (knowledgeable) with the principal to authenticate their identity.

### **Service Provider Benefits**

- Unique cross selling and new product development opportunities: Service providers have the opportunity to bundle their offering with another organization's. For example via federation, a 401K provider could bundle a brokerage service together for their corporate clients.
- Quickly allows a service provider to add additional clients and their employees (cost savings).
- Mitigation of risk and liability. Individual authentication is being handled by the identity provider.
- Minimize investment in authentication infrastructure and services

### **Business Guidelines Overview**

The Liberty Alliance is developing and delivering technical standards that enable wide-scale identity federation. Enterprise customers, vendors, and service providers are in the process of implementing these standards. To efficiently enable wide-scale federated identity deployment, Liberty is also defining technology and business guidelines for creating inter-linked circles of trust between business partners and publishing scenarios and case studies as they become known or available. The following is a high-level overview of the Business Requirements that need to be considered during a large-scale deployment

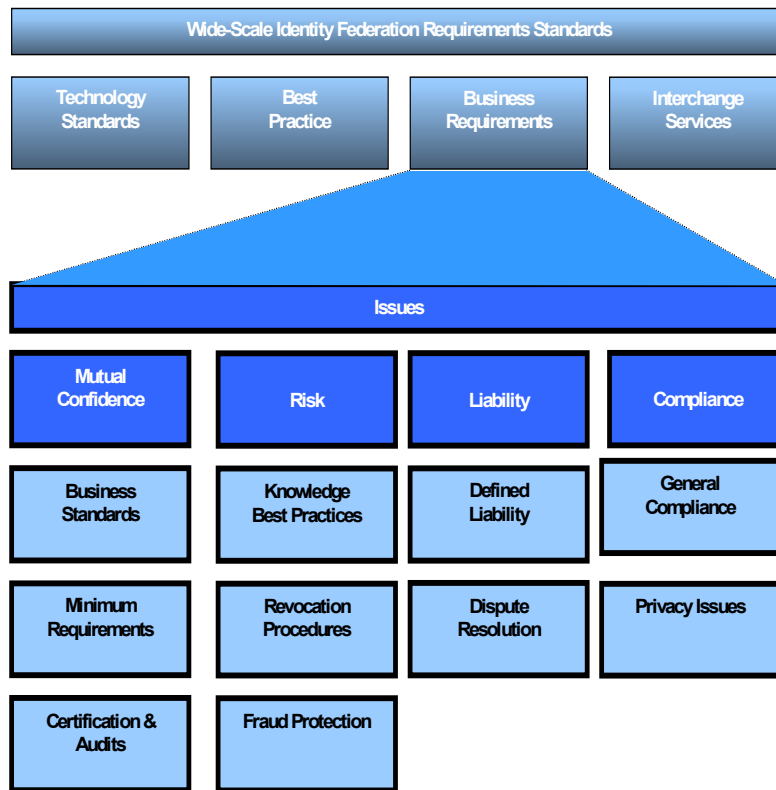


Figure 1: Positioning the Liberty Business Guidelines in the Federated Identity Business Requirement Framework

### Mutual Confidence

Business and individuals must be able to fully rely on the integrity of identity assertions and identity related information exchanged among members of a federation.

Within the context of federated identity, mutual confidence refers to the measures and tasks that circle of trust members must undertake or adopt together to enforce rules for compliance and manage the risks of exposure.

In face to face transactions, mutual confidence is often taken for granted. On the Web, it must be explicitly set forth.

Establishing mutual confidence is one of the core objectives associated with any implementation of federated identity architecture. To establish mutual confidence on the Web, a number of factors must be considered.

- Legal agreements among parties
- Business standards associated with policies and practices, e.g. agreement on authentication context meanings and interpretations, agreement on meaning of any attributes shared, agreement on administration procedures, agreement on business

rules/security policy to be implemented, agreement on account 'setup' such as whether to use bulk federation or not, agreement on how to keep accounts up to date at the Service Provider.

- Minimum requirements for implementation, ensuring consistent application of the Liberty specifications
- Enforcement and compliance mechanisms: certifications and audits
- Other deployment considerations such as the legal structure of the federation (circle of trust) defining the obligations and rights of its participants, and risk management are dealt with in separate sections.

With mutual confidence in place, the 401K environment represents both unique opportunities and challenges for the coordination of authentication architectures and single sign-on.

There are a number of key security risks and questions to consider. Please see addendum A for questions around enterprise authentication and controls.

### **Business Standards**

Business Standards are the set of rules, conventions and guidelines that participating members of a circle of trust need to abide by. The business standards that will be most critical in creating a circle of trust related to identity transactions include:

- Legal structure of circle of trust, relationships amongst participants
- Technical standards and associated levels of performance
- Security and Privacy standards
- Accreditation standards and guidelines
- Trade standards for vertical and cross-vertical transactions
- Adoption and alignment with legal standards (such as HIPAA and privacy law)

Federation governance provides the frameworks for the definition, development, implementation, and enforcement of these standards. A governance framework is one of the measures that can be used by circle of trust members to demonstrate how the risk of federating identity is managed, and how regulatory compliance is achieved. It drives the legal structure of the circle of trust and the relationships amongst its participants. Regulatory considerations include how membership in the trust circle is determined and managed, member service pricing, and avoidance of anti-trust exposure.

Business standards related to information privacy and customer information management are also material for both practical business and regulatory reasons.

Monitoring and enforcement of minimum acceptable standards for all members of a federation (or a circle of trust) is necessary to ensure that no weak link creates exposures for the participants. Additionally, liabilities may be incurred by lapses in adherence to the standards.

### **Minimum Requirements**

These are the service delivery quality control measures that need to be articulated and enforced in order to mitigate operational performance risks:

- Internal controls
- Service Level achievement against controls and technical standards
- Employees' integrity/certification requirements
- Audit

Each member of a circle of trust needs to assert that they can and will adhere to a minimum level of standards and requirements. In addition, each member must have the ability to confirm and validate that these standards are being adhered to (see Certification & Audits).

Furthermore, recourse must be defined for both lapses in achievement of minimal requirements, as well as disqualification of any participant. It is likely that the federation will need to provide for continual improvement in the level of minimum requirements in order to ensure the quality of the services delivered over time.

The 401K environment poses a number of unique challenges which must be addressed in the form of minimum requirements. Factors to be addressed include:

- Privacy issues, including
  - How to protect data not related to employee's current employer (in the scenario where the employee worked for a previous employer with benefits administered by the 401K vendor)
  - Personal financial data, should it be aggregated or accessible from the 401K site
  - Other benefits information, like health care
  - Will joint account information (such as from a spouse) be accessible from the 401K vendor
- How to best implement consumer friendly options, like opting in or out of the service and providing visible privacy protection without alarming the employee
- How to best navigate a network of providers
  - Multiple federations all entwined, with the 401K provider being the SP for the client and IdP for several related vendors
- What is the fiduciary responsibility of the employer? Need to consider employee's benefit above their desire to use a certain technology
- What will be the impact on members of a COT from the addition of a new member? Do all members of a COT have to 'approve' and establish agreements with the new member?

### **Certification & Audits**

Certification is the act of certifying or confirming that certain facts are true, and that the levels of performance and conformance are maintained. Factors to be considered include:

- Authentication Contexts – how are the different authentication contexts to be certified for consistency across the federation. Service providers rely upon the veracity of the authentication context when applying their own local acceptance policy to an authentication assertion.
- Identity Proofing – certification of identity providers processes to ensure compliance with minimal identity proofing, and revocation requirements
- Legal Conformance – right of independent third parties to audit members conformance to legal and business process obligations
- Audit logs – requirements to maintain transaction audit trails for troubleshooting and non-repudiation

Certifications and accreditations are measures that can be used by the circle of trust members to validate the effectiveness of their policies, and ensure ongoing mutual confidence vis-à-vis managing risks and complying with regulatory requirements.

Certification can be achieved by self-assertion of facts by a party, notification of compliance by accepted third parties such as external auditors, statement of compliance from an accredited testing organization, or by examination by representatives of the federation. It is possible for various methods to be adopted depending on the category and maturity of the policy and the criticality of the requirement.

## **Risk Management**

The challenges inherent in the 401K environment require a comprehensive risk management strategy to minimize potential costs and legal exposures.

Risk management mechanisms should include considerations such as:

- Federal and state laws and regulations.
- Competition regulations (e.g. in terms of Circle of Trusts, issues of limiting the inclusion of additional parties by boycott, etc.) *Note: Circles of Trust neither enhance nor take care of legal/competition problems!*
- The code of conduct/practice within the 401K industry, possibly utilizing existing agreements and other business contracts.
- A process to deal with actual or attempted fraud or identity theft , including responsibilities of each party
- Process for identity revocation, revocation of issued assertions, and notifications of affected parties
- Process and standards for financial liabilities associated with revoked credentials
- Risk assessments & mitigation procedures (technical & otherwise)
- Security Audits

All entities face risk in the form of potential exposure to financial injury or loss. Within the context of a federated identity, risk can manifest itself as actual losses due to fraudulent use of an identity, loss or exposure of identities or attribute information, and loss of business integrity due to insecure processes and data. Both the identity user and the service provider are subject to financial loss as well as loss of personal or business reputation (such as in the case of identity theft and fraud), but all parties in the circle of trust are exposed to the risks pursuant to insecure processes and data. Federations can manage risk through disseminating knowledge of best practices, revocation procedures, and fraud protection measures.

## **Disseminating Knowledge of Best Practices**

The deployment of federated technologies and application of associated business models is still in its infancy. Risks will change as technology, and business models evolve. The most effective way to keep current on these risks, design deterrents, and upgrade requirements and specifications will be to employ the best practices of the industry.

Best practices are particularly critical in the areas of: sources of attacks, methods of attacks, sources of detection and safeguards. There are also a number of best practices that must be established in the area of compliance, which is detailed later in this document.

## **Revocation Procedures**

Revocation is the process of suspending the access rights of a principal, and is also a powerful potential tool to mitigate risk. This could be the result of a mutual agreement between the principal and one or more members of the circle of trust; or it could be the result of breach or a dispute between the parties.

The following set of federated procedures can be defined and integrated into the operational delivery environment:

- Credential revocation
- Identity suspension
- Confidence lowering of a type of interaction (e.g. risk scoring)
- Affected party notifications
- Transaction revocation, cancellation, or reversal
- Fees and costs for these procedures, if any.

### **Fraud Protection Measures**

One area for particular consideration in the identity space is the fraudulent use of an identity following identity theft. This can entail the creation and use of invalid identities, a user's repudiation of a legitimate transaction, or a service providers' use of a networks capabilities without legitimate users behind its transactions. Each of these forms of fraud requires specific protections, and constant vigilance, actions and alerts. This implies the need for active management and oversight of operations, procedures, data, and pooled information.

In order to address identity theft, companies issuing identities may want to consider delivering a clear statement to their end users. Service providers need to do the same for the users of their services. The goal here is to inform the end user of the scope and responsibilities of the different entities.

Any identity federation will find that it must constantly battle abuse of the system through its use of pooled data, and that it will need to continually respond to nascent approaches of fraud and threats through new methods of detection and intervention.

### **Liability**

Liability results from failures to satisfy obligations and requirements established in the legal structure (contracts) of the federation. The risk management measures described above attempt to reduce the practical liability exposure in various scenarios. Liability is a function of the legal structure, business standards, and risk management measures. Liability can be limited by mutual agreement in the contracts, as well as originating from the failure to meet contractual obligations.

### **Defined Liability**

It is important to identify and define areas of potential liability, and address each within an appropriate context (contracts, business standards, risk management, etc.). Liability areas to consider include:

- Service Level Problems (i.e., the identity federation not working successfully)
  - One result: user can not be authenticated
- Identity misrepresentation by another individual
  - By theft of device, username/pwd, etc.
  - By failure to adequately identity proof the principal before issuing credentials
  - By failure to revoke fraudulent or compromised credentials on a timely basis
  - By failure to detect fraudulent use through appropriate fraud management practices
- Illegal or illicit activities over the network
  - e.g., money laundering
- Ramifications of breakdown in specific services;

- e.g., person-to-person money transfer failure can lead to domino effect of failed payments

Predetermined dispute resolution needs to be in place to address these and other issues:

- Assessing which federation member will bear costs associated with an identity network failure
- Source and amount of liability in case of fraudulent commercial activities
- Physical damages
- Failure to meet service level assurances to relying parties

Failure to mitigate risk or to execute obligations as defined in an agreed upon process or specification can result in liability in the form of money damages or requirements to repair damages to another party in the event a) of an accident where the right of a principal (individual consumer or a company) was compromised; b) where laws or standards have been violated. In networked environments, there are potential liabilities to all parties, including providers, agents, and the network, based on agreements and expectations related to rules and performance.

Identifying in the contracts who will bear what losses, and in what circumstances, (minimum standards not being met, processes being omitted or shortcut, etc.) can help limit unnecessary frustration and expenses. Over time, the web services and identity federation industry will likely evolve customary practices for assessing and determining the allocation of liability between parties in a business relationship. In the absence of allocation of risk by private contract, recourse will be made to other less preferable methods of dispute resolution.

### **Dispute Resolution**

Identifying agreed-upon processes for dispute resolution can help minimize or eliminate the need for parties to resort to traditional, and often time-consuming and costly, means of resolving conflicts.

For example, if a customer of an online brokerage firm is unable to perform a critical trade because of a problem related to shared authentication, who is at fault? Who is financially liable? What is the individual recourse? What are the efficient and timely procedures for resolving the incident?

Traditional means of dispute resolution include mediation, arbitration, or recourse to appropriate legal or regulatory authorities. The agreed upon means of resolving disputes should be specified in contracts.

Dispute Resolution methods tend to be human resource intensive and may not be appropriate for the high-volume and automated environment of web-services. Parties should consider the extent to which mediation or arbitration options can be adapted for the online environment.

One approach might be to put more into an end-user agreement (sort of a use at your own risk clause.)

### **Compliance**

Compliance with legal, business, technical and operational requirements and standards are essential to achieving a practical level of mutual confidence to enable an identity federation. Beyond the specific identity-related (e.g. Liberty standards) compliance issues, there are a host of other mutually interdependent compliance requirements that need to be identified and ensured. These standards, policies and procedures may be governed by contract – be they unilateral, bi-lateral or multi-lateral.

These include compliance with:

- ERISA (Employee, Retirement, Income, Security Act of 1974) It is the primary federal law governing pensions, health and welfare arrangements created by private employers. It has a set of disclosure and reporting obligations as well as trust, accountancy, and audit requirements.
- applicable privacy laws
  - HIPAA
  - Digital signature directive
  - Graham-Leach-Bliley
  - Breach Disclosure Laws

Other key areas where best practices in compliance should be established are:

- “As-ofs” where an error occurs in the trading or transmission of an investment
- Disclosure requirements. There are different disclosure rules around retail financial services and 401K. For example, there are no rules around whether an account holder should get a quarterly or a yearly statement. Having additional clarity around these rules to insure timeliness and consistency around the end user experience would be helpful.
- Protocols and rules around rolling over accounts from one provider to another
- SAS 70: Safety and Soundness reviews.

### **Privacy Issues**

Information privacy standards address the interest of an individual (Principal) or a company (presumably a member in the identity federation) in controlling, or at least significantly influencing the handling of sensitive data associated with that entity.

The 401K arena holds unique challenges in this regard that must be addressed. Specifically, it is not clear where privacy rights are held since the provider of a 401K plan works through its enterprise client to the client’s employees. Therefore it is not a direct retail relationship and it is unclear who owns the employees’ data and how that data can be used.

To address this issue, some of the nation’s leading 401K providers, including Fidelity, Magellan and T. Rowe Price, have established policies that they use with their clients. It is important to address and set forth parameters around this issue during the discovery phase of a relationship.

Within the context of a federated identity, there are a number of privacy compliance regulatory issues that needs to be considered from the perspective of:

- Applicable privacy law
- Privacy interest of the consumer, their personal information, as well as service history (buying preferences, services used, amount spent, etc.)
- Privacy interest of the business
- Privacy interest of employees

Within a deployed federated identity system, necessary information should be provided in order to be compliant with local privacy requirements. It is assumed that any member of the federation will comply with applicable laws (see Business Standards). Adherence to any new legislation enacted on the national or local level should be considered a requirement for all participants.

Privacy policy within the identity federation includes local policies for accepting an authentication request from a service provider, for accepting an identity assertion from an identity provider, and accepting an identity attribute request from a service provider. Such privacy policies need to define the circumstances under which these requests or assertions will be honored. The Liberty

standards provide the protocols for communicating these semantics, not the local policies to be employed in determining which ones to grant and under which circumstances.

## **Addendum A**

### **Enterprise Authentication and Controls: Key Questions to Consider**

What authentication method will be used as the basis for the integrated sign on?

Are the authentication methods consistent across all employees and access methods to include remote access?

What policies exist regarding the authentication method used for integrated sign on?

Do credentials need to be reset periodically?

Are there rules regarding password construction complexity, authentication credential expiration and renewal and default password change requirements?

What is the strike out policy?

Can authentication credentials be stored locally for reuse (e.g. password savers)?

What are the reset processes for employees who do not remember their passwords or otherwise need to have their authentication credentials reset?

Are reset procedures automated or do they require manual intervention?

What safeguard mechanisms are in place to ensure that only the authorized individual can reset their credential(s)?

Who has access to the authentication credential store?

What access do system administrators have to the access credentials? What actions can they perform on behalf of employees?

How long do authentication credential sessions last?

How are new accounts established for employees within the identified authentication store for SSO?

Does the account requestor have to show up in person anywhere and show credentials such as an identity card?

How are remote, work-at-home employees handled? Employees in foreign countries, especially when there is little/no local manager or HR presence.

What about contingent workers (contractors, temps etc.)

What is done to prevent one user from sharing ID/credentials with another user?

Are there segregated production and non-production authentication stores?

What is the method by which terminated employees are removed from access?

Will there be established criteria for authorizing employees to use the SSO functionality?

How are IDs ensured to be unique - are IDs ever reused?

Will shared IDs such as group IDs be eligible for SSO?

What auditing and logging functionality exist in the defined authentication method?

What methods are available to scan the voluminous amount of audit/log data and quickly detect anomalies?

What sorts of anomalies are included in the checks?

What procedures are in place to deal with invalid authentication, intrusion activity, system administrator activity logging and alerts derived from logging?

How might SP application sessions enable access beyond termination of login session at the IDP?

What are the IDP and SP session termination practices?

What caching might impact or delay session termination?

Once the user has been authenticated, what is he/she authorized to do?

Who sets the rules regarding authorization?

Who provides the data upon which authorization decisions are made?

How are the semantics of the data used for authorization mapped between SP and IDP?

Where are the Policy Enforcement Points and Policy Decision Points for different levels of authorization (high level vs low level (data level) access control.)

Who does the security policy administration (e.g. Authorization specification) – is any of it delegated?

What are the procedures around authorizing the folks who do the security policy administration?