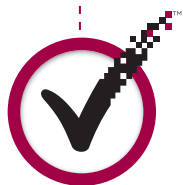




WHITE PAPER

Trusted Federated Identity Solution Architecture Business Requirements





WHITE PAPER



CONTENTS

+ Who Should Read	3
+ Identity Federation	3
Federation Scenarios	3
Trust	7
Transactional Confidence	8
+ IBM-VeriSign Solution Overview	8
VeriSign Solution Components	8
IBM Solution Components	10
+ Conclusions	11



Where it all comes together.™

Who Should Read

This white paper is an introduction for the Trusted Federated Identity Solution Architecture White Paper and is intended to provide an overview of the business drivers, justifications, and requirements for Federated Identity Solutions. It is targeted at business managers and executives who want more background on the well-documented reasons why federated identity will help improve resource allocation, IT spending costs, and user experience for many common business processes.

This paper will present an overview of the joint VeriSign-IBM solution, but for more detailed technical information, please reference the full Trusted Federated Identity Solution Architecture White Paper.

Identity Federation

In any business transaction, access to resources such as applications and information systems must be controlled. This control is enforced by evaluating whether or not a subject, described by a set of attributes including an identity, is authorized to access the requested resource.

As businesses open their infrastructure and extend their networks and applications to include customers, business partners, and suppliers, a fundamental disconnect is exposed: there is no standardized way, with today's environments, to "trust" or broker identities belonging to partners and other external users.

The lack of interoperable trust management and identity brokering infrastructures means that businesses must redundantly manage attributes for both internal and external users. This approach results in significant identity management costs for the company, increasing the cost of integrating businesses across business units and with partners. It also requires users to maintain multiple identities for each possible business interaction, resulting in poor user experience and the associated risk with multiple sign-on systems.

Federated identity management solutions address these issues. Federated identity solutions provide a standardized means for allowing businesses to directly provide services for trusted third-party users or users they don't directly manage. It refers to the ability of one enterprise to associate with one or more others in a federation, such that the users from one enterprise domain (or Identity Provider) are granted access to the

services of another enterprise (or Service Provider) based on federated identities and attributes. These solutions will allow companies to share identities and attributes in a trusted fashion. This, in turn, will enable rich sets of business interactions for users and business processes.

Federated identity solutions must manage the complete user lifecycle, within and across enterprises. This means user and account creation, account linking, authentication, access control, and account termination:

- **User and account creation:** How and under what legal structure a new user is given an account at all required parties
- **Account linking:** How users establish a means of mapping existing accounts across business providers (sometimes called "federation") to allow for cross-application behavior
- **Authentication:** How a user proves his/her identity and attributes to various parties, either through direct authentication to an Identity Provider or single-sign-on to associated Service Providers
- **Access control:** How a user's behavior is controlled across enterprises
- **Account termination:** How a user's account linking is "broken" between identity and Service Providers, without necessarily destroying a user's account itself sometimes referred to as "de-federation" or "de-referencing."

Once identity federation is contemplated, it is necessary to evaluate what will be done with a federation, who is going to participate, how it will be managed, and what types of risks must be assumed by federation participants. The remainder of this paper addresses these issues.

+ Federation Scenarios

Federation use cases fall into one of three broad categories: Business-to-Consumer (B2C), Business-to-Business to Employee (B2B2E), and Business-to-Business (B2B). These categories can extend to both the public and private sector, with the U.S. federal government serving as potentially the largest relying party in the world. Each one of the use cases has the same set of federation-level actors. These are:

• Identity Provider

An entity that is responsible for validating a user's authentication credentials and "vouching for" the user in the scope of a single-sign-on relationship. When vouching for a user, the Identity Provider will issue trusted single-sign-on credentials that are used to identify the user to a

federation partner. The Identity Provider may also issue the credential and be responsible for the identity proofing prior to issuance and therefore assuming certain liability for the credential.

• **Service Provider**

An entity that provides services within a federation. This entity acts as the recipient of a single-sign-on event from an Identity Provider. Based on the trust relationship with the Identity Provider, a Service Provider is able to validate Identity Provider-provided single-sign-on credentials for a user.

• **User (or Delegate Agent)**

The end user, or an agent acting on the user's behalf, who participates in the federation, using services from both the Identity Provider and the Service Providers, while directly authenticating only to the Identity Provider.

Each of these federation use cases exposes these actors to the following issues:

• **Fraud exposure**

Fraud is considered with respect to inappropriate actions, usually based on the incorrect identification of a user. Fraud may affect all federation actors, but is especially sensitive to the end user in a B2C scenario.

• **Liability**

Each actor in a scenario has a level of liability that may be assumed. Different scenarios apportion liability to different actors.

• **“Lifecycle critical”**

Lifecycle issues, such as replacement of their account or credential, are generally managed by a user's Identity Provider, but they impact all actors. If lifecycle issues are not managed correctly, users will have a bad user experience, reducing their desire to participate in a federation.

• **Frequency**

The frequency of a transaction must be taken into account when describing a federation scenario.

• **Identity “mapping”**

Identity mapping issues impact all federation actors but are, if handled correctly, only managed by the Identity and Service Provider.

These issues, taken together, characterize a federation use case scenario, and the risks associated with that scenario. If, for example, the risk of fraud exposure is high, then the federation actors may require that additional safeguards be put in place to provide assurance against fraud, such as users needing to use strong authentication for single-sign-on.

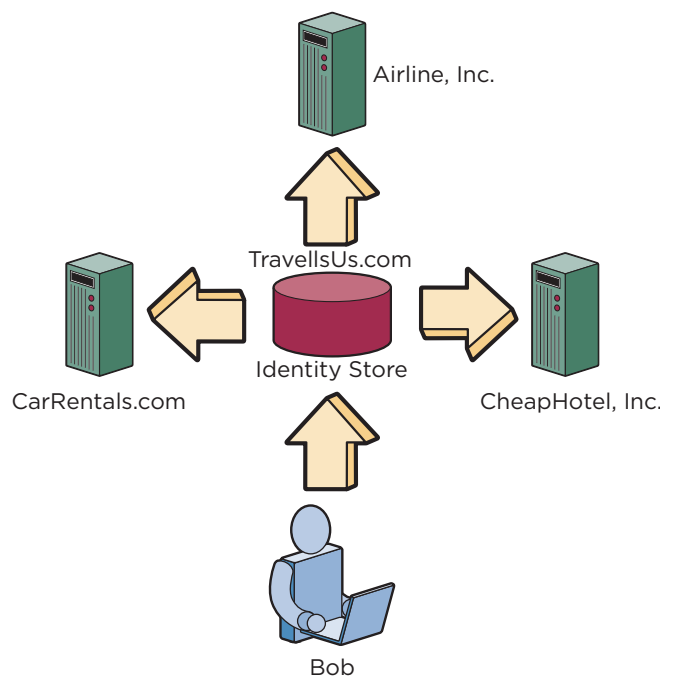
In the following sections we provide brief examples of common federation use case scenarios.

B2C: Travel Industry Example

The travel industry provides a commonly used application of federated identity solutions in a B2C setting. This example involves an airline, a car rental company, and a hotel chain. These parties are all part of a business relationship that allows them to share identities and provide users with a single-sign-on experience across providers. Within this business relationship, also known as a federation and sometimes referred to as a circle of trust, there will be one party that is able to act as the user's Identity Provider.

Consider the following typical scenario involving Bob. Bob wishes to book a vacation and so he goes to his favorite airline's Web site. He authenticates to the airline and books an airplane ticket for Boston. Once he has finished making his travel arrangements, he needs to book accommodations. Following a link on the airline's Web page, he is redirected without reauthenticating to the hotel chain's Web site, where he can book his accommodations.

Figure 1



There are several models as to whom will act as the Identity Provider in this type of scenario. The two most common variants are that Bob's Internet Service Provider will act as his Identity Provider in these types of B2C scenarios, or that a federation specific Identity Provider, such as "TravellsUs.com," will act as an Identity Provider within this travel-related federation.

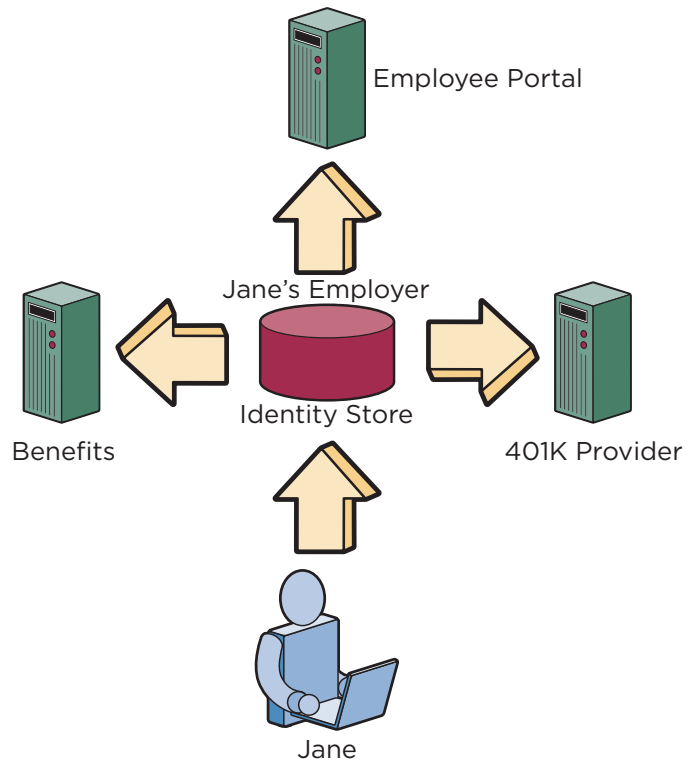
In general, the transactions in a B2C scenario are:

- **Fraud exposure—minimal**
While the value of Bob's purchases within "TravellsUs.com" may be of high value to Bob, the potential for long-term, high-value fraud in this use case is minimal. It is easy to detect (even long after the fact) theft of information from the hotel chain; the ability to retire to Tahiti with the proceeds of fraudulent purchases is minimal.
- **Liability—low**
Bob's purchases are typically insured by his credit card company. The liability associated with an incorrect transaction is typically negligible.
- **"Lifecycle critical"—no**
The linking of accounts across this federation is mostly for the convenience of the end user and does not normally imply financial liability to the Identity Provider.
- **Frequency—low**
This type of transaction will most likely will be driven by a consumer at low to moderate frequency.
- **Identity "mapping"—one-to-one**
In this scenario, the mapping is one-to-one as Bob is engaging in a transaction that must be uniquely identifiable to him.

B2B2E: Employer/Employee and Third-Party Benefits
A common application of federated identity solutions to B2B2E environments is that of an employer with outsourced benefits such as medical, dental, and retirement savings plans and federal and state tax management. These parties are all part of a business relationship that allows them to share identities and provide users with a single-sign-on experience across providers. Within this business relationship, the employer acts as the Identity Provider, authentication credential issuer (to the employee/user), and single-sign-on credential issuer (to federation partners on behalf of the employee).

Consider the following typical scenario involving Jane. Jane is a new employee and so must be provisioned with both her internal employer-system accounts and accounts at all of the benefits providers. When Jane wishes to manage her retirement savings plan contributions, she is transferred to the retirement plan provider in a single-sign-on fashion from her employer's site. Five years later, when Jane retires, the account linking between the employer and the benefits providers may need to be "broken." Jane can no longer single-sign-on from her employer but she can still access her retirement plan account, but with the benefit provider now being the identity provider and the service provider.

Figure 2



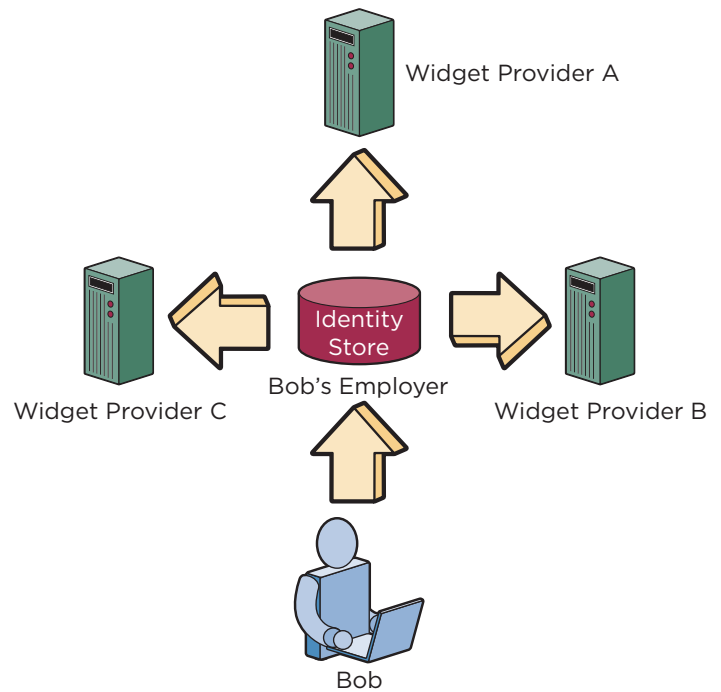
In general, the transactions in a B2B2E scenario have the following characteristics:

- **Fraud exposure—medium**
Significant, but not of the highest value and not a huge motivation for fraud. The value associated with these transactions is often associated with intangible aspects of a relationship, such as user confidence or privacy, as opposed to the dollar value of the transaction itself.
- **Liability—medium**
The liability associated with an incorrect transaction is often associated with intangible aspects of a relationship, such as user confidence or privacy, as opposed to the dollar value of the transaction itself.
- **“Lifecycle critical”—yes**
Transactions within this type of federation are bound to a user’s employment—Jane’s accounts at the benefits provider are referred to as “sponsored accounts.” Jane’s ability to single-sign-on to these resources is intimately bound to Jane’s status as an employee and there needs to be a way to migrate direct to the benefits provider after she retires.
- **Frequency—medium**
The transactions will occur in medium frequency and most likely will be performed by more technically savvy end users.
- **Identity Mapping—one-to-one**
The identity mapping in this scenario is one-to-one as the transactions must be uniquely identifiable and bound to the individual employee.

B2B: Supply Chain Management: Service Aggregators
A common application of federated identity solutions in B2B environments is that of a supply chain management (SCM) or a customer relationship management (CRM) scenario. In some scenarios, this supply chain may involve competitive interests where secure control of information is paramount. Participants within a B2B federation are all part of a business relationship that allows them to share identities and provide users with a single-sign-on experience across providers. Within this business relationship, it is not uncommon for each participant to act as both an Identity Provider and a Service Provider. This allows a business to act as the Identity Provider for its employees within the scope of the supply chain and to act as a Service Provider to users from other federation partners.

Consider the following typical scenario involving Bob. Bob is a purchasing agent who needs to place a large order for widgets. Bob’s company does not have any one preferred widget supplier, but sources widgets from one of several suppliers based on cost, delivery schedules, etc. Bob will locate an appropriate supplier from a set of suppliers managed through a widget aggregator.

Figure 3



There is only one entity who will act as the Identity Provider in this scenario: Bob's employer.

In general, the transactions in a B2B scenario are:

- **Fraud exposure—high**
Even when the maximum individual order value is relatively small, aggregate order values often reach millions of dollars. Corporate embezzlement is often committed by relatively low-level employees buying personal items using company funds or directing contracts through front companies controlled by the employee.
- **Liability exposure—medium**
While there is a liability associated with this transaction, it is usually possible to undo the transaction for a penalty.
- **“Lifecycle critical”—high**
Depending on Bob's status with his employer, his ability to participate in the federation is allowed or disallowed. Bob should not have ANY access to the federation partners outside of the scope of his employer's relationship.
- **Frequency—high**
The transactions will occur frequently by trained, technically savvy end users.
- **Identity mapping—many-to-one**
In this scenario, Bob's identity is required more for audit purposes than for individual transactional verification.

Transactional verification is based on Bob's role, where Bob may be one of many individuals who may assume that role.

B2B: Financial Industry: Electronic Trading

Another common application of federated identity solutions for B2B environments is a financial industry scenario for electronic trading between business partners. Participants within a B2B federation are all part of a business relationship that allows them to share identities and provide users with a single-sign-on experience across providers. Within this business relationship, there are typically several Identity Providers and a single Service Provider. This implies that the Service Provider has multiple independent relationships, one with each Identity Provider.

Consider the following typical scenario involving Jane. Jane is a trader for a large mutual fund company. Her company uses the services of a large trading exchange for executing all of its trades. Jane's trades are all high volume and time sensitive—having a trade filled five minutes after it is placed may cost Jane's firm millions of dollars of lost revenue.

In general, the transactions in a B2B scenario are:

- **Fraud exposure—high**
It is not uncommon for order values of the millions of dollars to be handled.
- **Liability exposure—high**
There are large performance and liability implications for transactions that are incorrectly executed or delayed. Thus the amount of processing applied to the transaction at the Service Provider side needs to be minimized.
- **“Lifecycle critical”—yes**
Depending on Jane's status with her employer, her ability to participate in the federation is allowed or disallowed. Jane should not have ANY access to the federation partners outside of the scope of her employer's relationship.
- **Frequency—high**
Transactions will be performed frequently by highly trained, technically savvy end users.
- **Identity mapping—many-to-one**
In this scenario, Jane's identity is required more for audit purposes than for individual transactional verification. Transactional verification is based on Jane's role, where Jane may be one of many individuals who may assume this role.

+ Trust

Day-to-day business operations are based on the assurance that business partners will appropriately honor transactions. This is easily seen from the previous examples, where participants in the federation must consider the risk associated with fraud and liability exposure. In other words, a business must have some degree of assurance that losses due to fraud and exposure will be minimized when participating in a federation.

Within the context of business relationships, trust in a partner results from the assurance of good behavior by those partners. This trust is based on the assurance that a partner's business follows the appropriate legal, statutory, and regulatory requirements; implements the appropriate technology infrastructure to support the relationship; and so on.

Assurance in a business partner is represented through trust relationships. Management of the trust relationship between federation partners is a fundamental prerequisite to the participation in federation and federated identity management. Within a federation, trust and trust relationships must be represented through technical artifacts. Common practice is to represent a trust relationship through cryptographic techniques, such as encryption and digital signatures.

+ Transactional Confidence

All of the use cases described in the previous section require transactional confidence. Transactional confidence is the assurance that can be placed in a specific request, including the user identity associated with a request.

Transactional confidence is achieved by:

- **Transaction Appropriate Authentication Mechanisms**
Stronger authentication methods for end-users facilitate stronger transactional confidence, which includes identity proofing and credential type.
- **Enforceable and traceable trust models**
This would include authentication and accreditation of the entities (businesses) that participate in any federation.
- **Next-generation identity management**
Secure, federated identity lifecycle management is required to facilitate transactions, regardless of the confidence level.

Depending on the characteristics of a federation, including the value and liability associated with requests, different levels of transactional confidence are required. For example, high-value, high-liability transactions, such as those found in the B2B space, require a high degree of transactional confidence and would require high assurance solutions.

Transactional confidence places several requirements on a federation's partners. Federation partners must trust each other, which includes trust at the business level as well as trust at the technology level. This trust must be appropriately managed through a federation lifecycle, including the bootstrapping of a trust relationship. Federation partners must trust that users are appropriately managed by an Identity Provider. User authentication mechanisms used by an Identity Provider must be sufficient to enforce transactional confidence. Federation partners must also trust that users are appropriately managed through the user lifecycle, including the appropriate revocation of user credentials when appropriate.

IBM-VeriSign Solution Overview

Together, IBM and VeriSign provide a complete solution for federated identity management, including strong authentication techniques, full user lifecycle management, and a Trust Authority and Accreditation broker functionality. IBM's Federated Identity Management solutions focus on the management and runtime implementation of federation solutions, including federated lifecycle management and single-sign-on. VeriSign's strong authentication and trust accreditation services work with the IBM solutions to provide a comprehensive solution architecture for federation scenarios, including the ability to manage the risk associated with the federation.

A high-level solution architecture, including who does what, is shown below. The figure shows a solution overview for the combined IBM-VeriSign Federated Identity offerings. The major components for the joint offering are described in the next section. For a more detailed discussion of the solution components, please refer to the Solution Architecture white paper.

+ VeriSign Solution Components

VeriSign solutions play in both the authentication services and federation services aspects of federation management.

Authentication Services

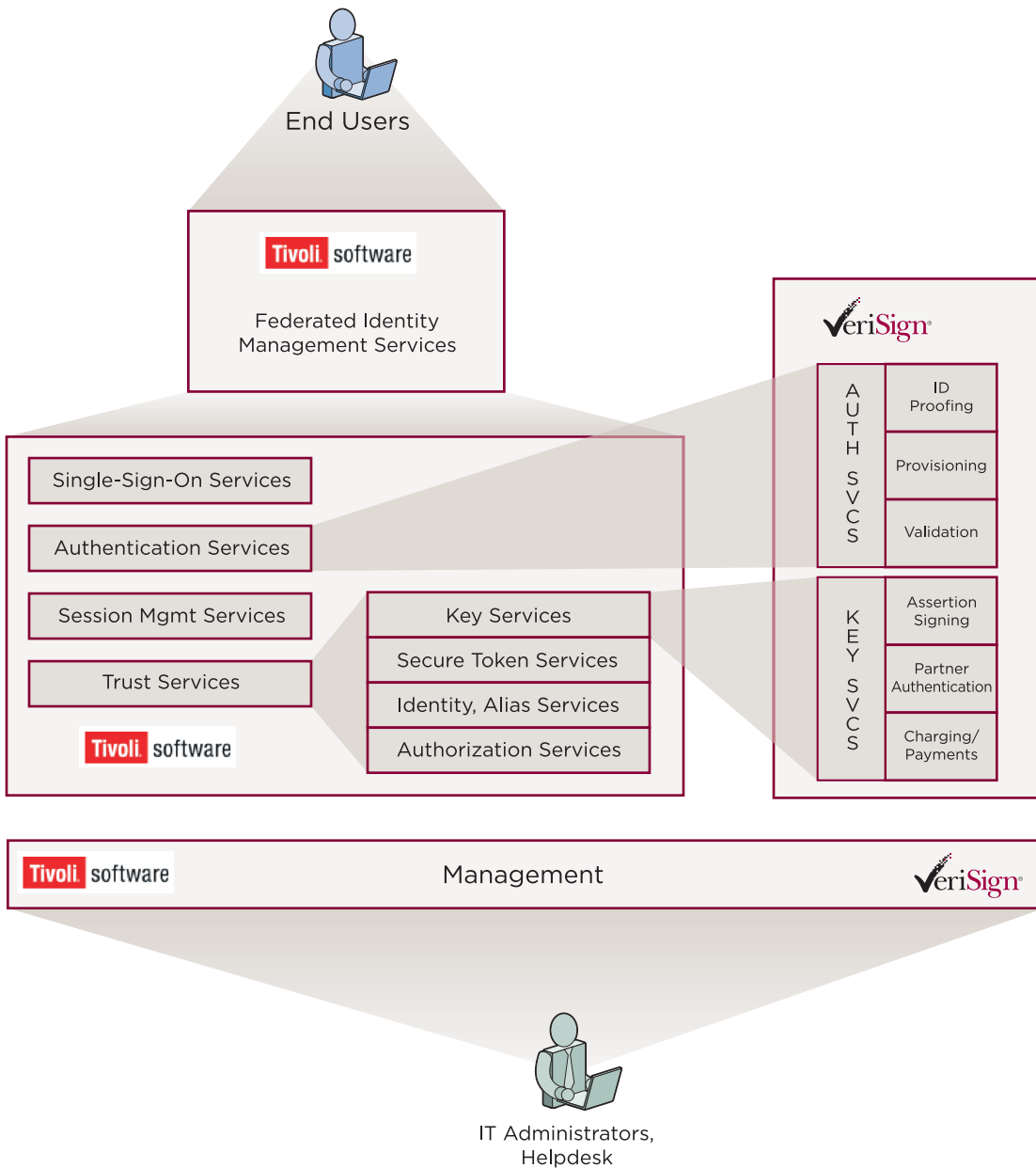
VeriSign offers a full range of authentication services that are easily extended into federated environments, including:

- **Identity Proofing Services**
Spanning from non-intrusive identity verification, interactive queries to in-person proofing services, VeriSign Identity Proofing (e.g., Consumer Authentication Service) services provide outsourced options for vetting consumer, healthcare, or business identities.
- **Unified Authentication (UA) Platform**
One of the most flexible, strong authentication platforms available, including hard (token protected) and soft PKI and OTP credentials all managed from the same management platform. UA integrates closely with federation identity management infrastructure, like directories and gateways, to provide an easily deployed authentication engine.

Transactional validation is available through VeriSign's global validation engine built upon the ATLAS infrastructure, the same system used to power the ubiquitous DNS infrastructure for the Internet. Validation enables basic audit trail functions necessary for non-repudiation and is offered in a way that is economical for large deployments that may also require global servicing.

Also, to create custom authentication modules, VeriSign will provide a complete integration SDK (C and Java). The SDK will be used by the VeriSign/IBM professional services team to create custom validation modules across specific terminal server systems and servers when these systems do not have built-in PKI or RADIUS validation capabilities.

Figure 4



Federation Services

VeriSign has been a leader in the business authentication services since 1995 when it launched its market-leading SSL Certificate offering, which became the baseline trust network for e-commerce and business-to-business transactions around the world. VeriSign has authenticated and issued certificates to almost a half a million businesses. This offering will provide the foundation of trust for federated identity environments.

Business Authentication and Accreditation Services

VeriSign's Business Authentication Service provides federation hubs, a streamlined, integrated outsourced service to vet corporate identities of Service Providers wishing to join a federation. This service is based upon the same infrastructure that authenticates SSL customers and provides the flexibility to include federation-specific components into the vetting process, which is a mix of querying available online data sources and telephone and Internet verification processes.

Federation (Assertion Signing) Certificates

These certificates will allow quick and easy trust enablement between businesses within a federation. Similar to SSL and browser, VeriSign roots of trust will be embedded within gateways sending and receiving signed assertions. These roots will provide the trust mechanism to enable assertion sharing among federation nodes. The certificates will enable organizational signing of the assertions that will provide authentication, non-repudiation, and essential audit functions.

Federation Services

VeriSign's extensive consulting organization, which has helped hundreds of organizations set up authentication infrastructure systems, including developing Certification Practices Statements (CPS) with the CSO, will help enterprises with their risk assessment and policy development when setting up federations.

Other federation services include root-signing and cross-certification services, which enable the interoperability within and among other linked federations.

Payment Services Platform

VeriSign's Payment Services platform enables transactional economics to occur seamlessly. The Payment Services platform, currently servicing one-third of all of North America's e-commerce transactions, will provide federations with a transaction engine to facilitate payments for the use of shared credentials and other fees associated with doing business within a federation. The Payflow SDK can easily integrate

into most B2B middleware that will serve as the economic engine for federations.

+ IBM Solution Components

IBM's Federated Identity Management solutions build on the Tivoli Identity Management suite, which includes award-winning products such as Tivoli Access Manager for e-business, Tivoli Identity Manager, Tivoli Directory Service and Tivoli Directory Integrator. Each of these components provides stand-alone solutions that are integrated as part of a federation solution to provide a complete solution for enterprise-level and federation-level identity management.

Tivoli Access Manager for e-business provides direct authentication of users, session management, and access control functionality. TAMEb supports the use of external authentication services, including strong authentication techniques as offered by the VeriSign Unified Strong Authentication platform. TAMEb, when integrated with FIM, will provide session management functionality, so that there is no change to the edge of an enterprise architecture. TAMEb is configurable to support Identity Provider, Service Provider, or combined Identity/Service Provider functionality.

Tivoli Identity Manager supports workflow-based management of users, providing complete user lifecycle management within an enterprise. When integrated with FIM, it will support user lifecycle management across enterprises within a federation. This will allow an Identity Provider to centralize the user lifecycle management of a user within a federation.

IBM Directory Services provide the necessary data repository for user information, including both user authentication information and user attributes. FIM solutions will leverage both LDAP-based data repositories, such as IDS, as well as pluggable JNDI and JDBC accessible data repositories.

Federation Solutions

In addition to requirements on transaction confidence, FIM solutions will not be adopted if they impose architectural constraints and prerequisites on an existing environment. The IBM Tivoli FIM solution is designed to be modular and composable, minimizing the effort required to integrate the solution into an existing environment. The basic pattern of a FIM architecture is shown Figure 4.

The FIM functionality provides federated identity management solutions based on SAML, WS-Federation, and Liberty ID-FF. The FIM functionality also implements a trust infrastructure, functionality that may be bootstrapped with VeriSign-issued Federation Assertion Signing certificates.

Conclusions

In time, the business world might realize the vision of “frictionless capitalism,” a business environment in which every transaction takes place automatically in a medium that is entirely mediated by software agents. Even though an environment of this kind is unlikely to become a universal goal, let alone a universal reality, it is entirely practical for many real-world business transactions (e.g., the ordering of office supplies). The key to realizing this goal is trust, the ability to quantify and thus the ability to manage risk. IBM and VeriSign provide the tools necessary to realize these goals.

For more detailed technical information, please reference the full Trusted Federated Identity Solution Architecture White Paper.

Visit us at www.Verisign.com for more information.