VeriSign®

WHITE PAPER

Trusted Federated Identity Solution Architecture

VeriSign®

WHITE PAPER

CONTENTS

Where it all comes together.™

Who Should Read

This white paper is a technical discussion of the joint IBM/VeriSign Trusted Federated Identity Solution Architecture. It is intended to provide an overview and discussion of the components included within the joint solution and the integration present between the two offerings. It is intended for a more technical audience or business/IT managers interested in learning more about the joint solution details.

Please consult the Business Requirements White Paper if you want background details on why federated identity will help improve resource allocation, lower IT spending costs, and enhance user experience for many common business processes.

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 many 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 participants. 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 federation participants 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 participants, 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 participants.
- **"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 participants. If lifecycle issues are not managed correctly, a user 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 participants 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 participants 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.

+ 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 business entities 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. The rest of this paper will outline the various components that enable transactional confidence and achieving real-world federation.

Transaction Appropriate User Authentication

Identity federation is intended to reduce the cost of identity management for all parties in the federation. However, this also means that companies are now relying on another entity to follow the appropriate procedures and practices in authenticating the end user. Note that these procedures and practices must not drive up the cost of identity management within a federation.

Federation participants need to agree on a priori when establishing the federation—what minimum authentication methods and processes will be for all participants. As fraud and liability exposure increase, the demand for strong authentication will increase. There is already movement in the industry to standardize on a set of authentication levels. Among the pioneers of this work are NIST (Special Publication 800-63, *http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf*) and the EAP/ Electronic Authentication Partnership (*http://www.eapartnership.org/*).

There are two components that constitute an authentication level:

- Initial Identity proofing and Verification techniques
- Online credentials, bound to an identity and used on an ongoing basis

These components are described in more detail below.

+ Identity Proofing

Identity proofing is the process of verifying the physical identity of an individual before enabling that person to conduct online transactions. Various forms of identity proofing techniques and processes can be used, including:

- Self-assertion
- Leverage an existing customer or employee relationship
- Confirmation of electronic or postal address
- Knowledge-based authentication utilizing authoritative databases
- Business license verification, e.g., doctors, lawyers
- In-person verification using a government issued photo-ID

The result of the identity proofing process is a long-term identity. This identity can be changed should a new identity be required. If a new identity is required, then the identity proofing process must be re-enacted.

+ Online Authentication Credentials

Once the identity proofing process has been completed, a user is typically issued an online authentication credential. An online authentication credential is "something" unique that is bound to a user identity and is known only by the user and the party to performing the authentication. A user presents her online authentication credential as part of the process of proving that she is the entity that is bound to the associated identity as determined by the identity proofing process. Typically, the "something" of an authentication credential is based on one of three basic principles:

- Something you know—a password or a PIN
- Something you carry—a smartcard or hardware token
- Something you are—a biometric measurement such as a fingerprint

A username and password are an example of an online credential. In this case, the username is assigned as part of the identity proofing process. The password is then bound to the username to create the online authentication credential. The password may be initially assigned as part of the identity proofing process, but may also be re-defined as part of the user's overall identity lifecycle. For example, password reset does not require a re-enactment of the identity proofing process.

Any one online credential provides single-factor authentication. Authentication based on username and password is an example of single-factor authentication techniques. Two-factor authentication mechanisms combine two online credentials, one each from the set of something you know/carry/are, to provide greater security. For example,

authentication based on a hardware token that is activated by a PIN number provides for two-factor authentication.

While two-factor authentication techniques are seen as stronger/better than single-factor authentication, in many cases they are considered impractical or too costly. However, as the risks associated with online transactions, including risk of fraud and the liability associated with fraud increase, two-factor and similar strong authentication techniques are gaining acceptance and wider deployment.

Common Authentication Methods

User authentication today is dominated by password-based systems. Password policies are used to define password attributes such as number of repeated characters, mix of alphabetic and numeric characters, and password lifetime before it must be "reset". Passwords are sometimes differentiated based on the strength of these password policies. However, there are many well-known disadvantages of password-based authentication systems such as:

- Vulnerability of passwords to discovery through social engineering.
- Inability to assert non-repudiation of password-based authentication.
- High support costs associated with password management, such as the reset of forgotten passwords.
- Limited password sample set due to reuse of passwords, selection of passwords with "meaning," etc.

The main reason that passwords still dominate the market, despite these well-known disadvantages, is their user perceived ease of use and low-cost to initially deploy. However, this ease-of-use advantage is quickly offset by the sheer number of usernames and passwords that a user must remember. To cope with this complexity, a user often ends up choosing an easy-to-remember password or reusing the same password at multiple sites.

Two-factor authentication mechanisms include certificates, smartcards with certificates, hardware tokens, biometric devices, and one-time password devices. These authentication credentials provide stronger authentication than password-based authentication mechanisms primarily because authentication based on these mechanisms cannot be easily stolen "off the wire" and replayed. For all of these mechanisms, if the certificate, Smartcard, hardware token, etc., is stolen, then impersonation of a user is possible. But, impersonation of an identity is not as simple when strong authentication mechanisms are employed.

Figure 1: Generic Hardware Token Dongle

Hardware-based authentication mechanisms are less widely deployed than passwords due to perceived start-up costs such as the cost of deploying hardware tokens. The cost and complexity of hardware tokens typically has been prohibitive for any large-scale deployments. Hardware tokens have been deployed to a certain extent by enterprises, especially to secure remote access applications like VPNs and SSL VPNs. There has been some deployment of strong authentication in Europe/Middle East/Africa for consumer banking in extremely large deployments or where demanded for legislative compliance. Despite the costs of hardware-based authentication mechanisms, newer consumer applications are now being tested. These strong authentication techniques are slowly expanding into new markets where loss due to fraud has become an inhibitor to business.

Strong authentication techniques also benefit the end user. A prime deterrent to participation in online activities, including federations, is the fear of identity theft. Identity theft is made easier by the use of weak passwords and other easily replayed authentication credentials. For example, online techniques for identity theft such as "phishing" attacks are becoming more and more routine. These types of attacks typically involve presenting a user with a rogue Web site that visually looks like the real e-commerce Web site. The purpose of this rogue Web site is to collect a user's personal information including username and passwords. These usernames and passwords can then be replayed at the real Web site to hijack the user account. Strong authentication techniques such as one-time passwords and digital certificates reduce this risk of identity theft by reducing these threats back to the level of physical theft threats. Online techniques (such as phishing) are no longer sufficient to accomplish identity theft as they do not result in an easily replayed authentication credential.

Strong Credentials in a Federated World

With federation scenarios, using an appropriate authentication mechanism becomes even more important. Third-party Service Providers are now relying on one entity to evaluate a user's identity (identity proofed) and associated authentication credential. If a user's authentication credential is based on a password, then these third-parties must now rely on the Identity Provider's password policies to ensure the

strength of the user's password. Service Providers will require authentication credentials that satisfy their internal policies on authentication strength. These policies, in turn, must be based on the required transactional confidence. Despite the password management policies that may be imposed, passwords are still vulnerable to the weaknesses described above. Transactional confidence amongst the federation participants can be increased by leveraging strong authentication, particularly for those transactions that require higher levels of assurance

Federated identity deployments will now require and encourage the use of strong authentication techniques. In a federated environment, the Identity Provider is able to assume the management of the strong authentication process on behalf of the federation participants. Note that the Identity Provider may well pass on a portion of the cost of managing this strong authentication environment to its partners thereby amortizing the cost across all participants. Strong authentication schemes will no longer be restricted to an enterprise's internal applications based on infrastructure costs.

The use of strong authentication also decreases the liability of the Identity Provider to its partners and may serve to increase acceptance by relying partners. Strong authentication techniques allow Service Providers to place greater assurance in the security tokens (including credentials) received from Identity Providers. This means that the Service Provider has increased transactional confidence within the federation without assuming the full cost of a strong authentication environment.

Partner Authentication and Trust Assurance

Federation appropriate user authentication mechanisms are required to ensure transactional confidence at the user level; likewise partner appropriate authentication engenders the trust required to ensure transactional confidence at the partner level. Before a Service Provider can trust an Identity Provider to appropriately authenticate end users, the Service Provider must trust the Identity Provider. Trusting a federation partner is, in turn, based on the ability to authenticate a partner.

Authentication of a federation partner has two facets—one a priori and one runtime. A priori authentication of federation partner is used to determine information such as "is there a legitimate business with the stated name?" A priori partner authentication is the result of the partner identity proofing process combined with the accreditation and reputation evaluation of the partner. If a priori authentication fails, then it is not possible to implement a runtime-based trust relationship, including runtime authentication of a partner.

Runtime authentication of a partner is the process of ensuring that a given request has in fact been made by the claimed partner. Runtime authentication of a partner includes the authentication of a request made by a partner.

+ A Priori Partner Authentication

A priori partner authentication has three main steps:

- Partner Identity Proofing
- Partner Accreditation
- Partner Reputation Evaluation

All three of these steps must be completed as part of the a priori authentication of a partner. Once these steps have been successfully completed, a business has sufficiently evaluated the risk of doing business with a partner and is able to enter into a trust relationship with that company.

Partner Identity Proofing

Partner identity proofing is the process of verifying the physical identity of a prospective federation partner both before entering into an online business relationship with that partner and when engaged in runtime transactions with the partner. Part of the partner identity proofing process involves verification of the physical identity of the business—who is the business?

- Is there a legitimate business with the stated name?
- Is this the party making the request?
- Is the specific employee making the request authorized?

Once the physical identity has been verified, some form of online token is issued to the business partner and then bound to the physical identity of the business.

Various forms of partner identity verification techniques and processes can be used, including:

- Self-assertion
- Leverage an existing relationship
- Confirmation of electronic or postal address
- Credit agency, business bureau ratings
- Business license or articles of incorporation
- As the name suggests, identity verification

Partner Accreditation

Partner accreditation addresses the question "what do we know about the company?" and more specifically, "what do we expect of this company?" Accreditation is based on a well-defined policy that defines the criteria that a company must satisfy. A company that wishes to enter into a federation may publish a policy that defines the criteria that prospective partners must match. Likewise, a partner wishing to enter into a federation may publish a policy that defines the criteria that it satisfies (a policy describing its own features). Evaluating the fit of these two policies is an action that is undertaken by a trusted party specializing in business accreditation.

Examples of the types of characteristics that are evaluated as part of the accreditation process include:

- Is the company credit worthy?
- Is the company considered a reputable business?
- Is the company approved by relevant professional/trade bodies?
- Is the company accredited as part of the federation?
- Has the company authenticated and issued credentials in a standardized trustworthy fashion?

Traditional forms of accreditation are not sufficient for an online business relationship. The accreditation process must also consider operational security accreditation and privacy accreditation.

An operational security accreditation is used as part of the assessment of transactional confidence that can be assumed with a partner. Some questions that are addressed as part of an operational security assessment include:

- Are the end points secured correctly?
- Has the assertion been signed by a trusted hierarchy?
- Was an appropriate form of authentication used based on the required transactional confidence? (e.g., strong authentication for medium and high transactional confidence?)
- Does the subject and associated underlying service hold a relevant security audit accreditation (e.g., SAS70, Web Trust, EAP)?

A privacy accreditation addresses issues such as:

- Does the subject comply with relevant legislative requirements?
- Does the subject agree to comply with relevant confidentiality agreements?

Partner Reputation Evaluation

Reputation is an alternate means of knowing additional qualitative information about a business. The primary difference between a reputation service and accreditation is that reputation typically is measured on an ongoing basis using behavioral information about the business or an individual. Another difference is that reputation is typically measured by an independent entity and typically does not involve the participation of the business or individual being measured. The reputation service may develop an automated framework for measuring reputation based on transactional visibility. Alternatively, a more explicit feedback-based mechanism is used. The reputation service will usually assign a simple score that is derived using a well-defined procedure and is easy to understand.

For identity federations, concepts of partner identity verification, accreditation, and reputation will coexist as the fundamental trust brokering mechanisms. Each mechanism makes sense depending on the type of federation (banking versus supply chain), as well as the type of identity (business versus individual).

For example, it is likely that an Identity Provider will be identity verified, accredited, and have a reputation rating. On the other hand, an individual user identity is unlikely to be accredited, but a reputation rating such as a credit score could help a Service Provider in making authorization decisions on specific transactions.

TA&AA Brokers

The a priori authentication of a partner requires the functionality of a new type of component: a trust assurance and accreditation authority (TA&AA) broker. TA&AA brokers are responsible for providing the operational due diligence required to facilitate federation relationships. One example of the functionality provided by a trust broker is the functionality provided by a credit rating agency. A report from a credit rating agency allows the seller to assess the probability that a customer will pay for goods purchased on credit. A credit report may also be used by the buyer to assess the probability that a supplier will meet their commitments; a poor credit rating may indicate that the company is unable to pay its suppliers.

Businesses assess the risk involved in a transaction. These assessments draw on past experience of doing business with a company as well as information provided by various types of TA&AA brokers. It is quite unlikely that two strangers would meet through the Internet and immediately complete a transaction that involves a very large value and extreme risk on the assessment of a TA&AA broker alone. A TA&AA

broker providing a general assessment of the reputation of a business is no substitute for due diligence. A company would be unwise to place a large order for critical parts with a previously unknown supplier without the usual process of obtaining references, personal meetings and a personal inspection of the supplier's factory. But even in this situation a TA&AA broker can play an essential part in pre-qualifying tenders. There is no point in traveling half way around the world to sell to a customer who is likely to become insolvent.

TA&AA Portal

Acting as a TA&AA broker on a global scale creates new issues. How is a global TA&AA broker infrastructure implemented and managed? How do independent trust brokers evaluate each others ratings? National credit rating agencies have existed for many years, but international agencies are another matter. How do we know how a "VIb" credit rating from Meng (Xian) Reporting Agency, Inc., corresponds to a four-star rating issued by a U.S. agency? Even if both agencies use a rating scheme that awards up to five stars, the result is meaningless without some standard means of evaluating the criteria applied to the awarding of these stars.

Additionally, the business and reputation elements of the business are now coupled with other ancillary data that do not necessarily exist in an existing data source, i.e., audit reports, vulnerability assessments, etc. Each of these sources can be represented by simple, machine representable formats or may exist in the form of reams of audit paperwork. In general, how does one correlate all this data and make it useful at the transactional level where the decision to trust someone is actually made?

This issue points to a need for an additional type of TA&AA broker known as a TA&AA broker portal. A TA&AA broker portal is responsible for assessing and correlating information obtained from multiple disparate sources. The TA&AA broker portal allows companies to establish a basis for comparison of information from these sources and distills the various sources of data into a usable format to help enable federations.

+ Runtime Partner Authentication

Once the a priori authentication/due diligence of a prospective partner has been completed, it must be possible to represent this process in a technology-appropriate manner. This is accomplished by implementing a runtime-based process for partner authentication and binding the results of this process to the priori authenticated partner identity.

Runtime partner authentication is based on cryptographic techniques, such as digital signatures. These techniques require that some form of cryptographic elements, such as digital signature verification keys and certificates, be distributed to partners within a federation, which introduces a requirement for bootstrapping.

Trust Assurance & Accreditation

Higher transactional confidence scenarios must rely on trust relationships based on out-of-band legal, business, and liability agreements. This requires that partners issuing/serving high-value transactions leverage existing trust relationships.

Regardless of transactional confidence requirements, all trust models have a bootstrapping requirement. This is the process whereby initial trust is established as it is the backbone on which federation partner authentication is based. Bootstrapping can be accomplished out-of-band, using time-honored traditions of face-to-face meetings and lengthy discussions. Or, as an alternative, a Trust Assurance and Accreditation Authority can be used to simplify the bootstrapping process.

A Trust Assurance and Accreditation Authority (TA&AA) will provide two essential services: authentication of federation nodes, both Identity and Service Providers, and accreditation of federation nodes according to advertised and registered network policies.

Authentication of federation nodes establishes the offline, or physical, identity of each node. This process is similar to the Registration Authority (RA) functionality of the PKI world. Based on this authentication process, a federation node is the issued a bootstrap credential by the TA&AA. The result of this process is that an Identity Provider has a bootstrap credential that can be used to identify and authenticate the Identity Provider to Service Providers as part of a federated transaction. This bootstrap credential may also be used to sign assertions between the Identity Provider and all Service Providers within that federation. This Federation (Assertion Signing) Certificate will be issued in a structure similar to SSL, which is used to secure e-commerce on the Internet. These bootstrap credentials will be offered in several classes depending on the type of assurance level for the transaction and will have dynamic extensions that can be used to help facilitate federation specific decisions.

The TA&AA's accreditation trust services are then used to certify federated nodes against the specific policy (including liability) of the federated network. Federation nodes are able to evaluate the claimed adherence of a partner to a network policy based on a policy accreditation certificate issued by the TA&AA. This certificate may be used by both Identity and Service Providers to sign policy elements based on WS-Policy

of a Web services transaction, on a transaction-by-transaction basis. This signed policy element will be verified by a validation utility provided by the TA&AA. Trust in the policy accreditation certificate, and the signatures from which they are based, are in turn implied by the TA&AA's accreditation services and may be loosely or tightly coupled to the TA&AA's federation bootstrap credential.

Federations requiring a high level of transactional confidence will make certification by a TA&AA a prerequisite to joining a federation. There will be general characteristics for certain levels of assurance as provided by a TA&AA-issued Assertion Certificate. Dynamic policy certificates defining specific policy requirements may also be issued. This overall TA&AA functionality allows a federation, and the partners within a federation, to specify the level of transactional confidence required and ensure that these requirements are met.

Next-Generation Identity Management

Next-generation identity management solutions integrate trust models and federated identity management solutions to enable online business solutions. These solutions provide complete user lifecycle management solutions across trusted federation partners. These solutions go beyond simple solutions that enable direct authentication to an Identity Provider and then under-the-covers, single-sign-on to trusted Service Providers. Next-generation identity solutions must manage the complete user lifecycle within and across enterprises in a manner that enforces transactional confidence.

+ Federated Identity Management

Federated identity management (FIM) provides a standardized mechanism for simplifying identity transformation and identity management across company boundaries. FIM approaches based on Liberty ID-FF and WS-Federation are designed to support runtime-based federation identity management activities. Both approaches are designed to support day-to-day activities regarding the management of users within a federation relationship. The result of this functionality is that users are able to seamlessly access resources provided by multiple federation partners.

Within a federation relationship, the bulk of the traditional user management will be retained by the federation partner acting as the Identity Provider. An end user's Identity Provider is responsible for the identity lifecycle management of this user including account creation, user provisioning, password management, and general account management. Having one federation partner act as a user's Identity Provider relieves the remaining partners of the burden of managing equivalent data for the user. These non-Identity Provider partners act as Service Providers. Service Providers will leverage their trust relationships with an Identity Provider to accept and trust (vouch-for) information provided by an Identity Provider on behalf of a user, without the direct involvement of the user. This enables businesses/Service Providers to offload identity and access management costs to business partners within the federation.

A Service Provider may still manage local information for a user, even within the context of a federation. For example, entering into a federated identity management relationship does not mean that a Service Provider must hand all identity management control to an Identity Provider. It does mean that a Service Provider may hand over as much identity management functionality to the Identity Provider as it can to minimize its identity management requirements while still enabling full Service Provider functionality.

The sharing of user information across federation partners is based on the secure exchange of tokens, or assertions, referring to a user, their attributes, privileges, etc. This requires trust models to support the secure exchange of this information. This implies that it is not sufficient to simply establish a trust relationship between partners. This trust relationship is used within FIM protocols to demonstrate the continuance of the trust relationship. FIM solutions in isolation are not sufficient to provide transactional confidence. FIM solutions must be layered over a trust relationship between federation partners.

+ Federation Trust Services

The main barriers to the deployment of FIM solutions are often due to the differences in trust semantics rather than differences in protocol. Trust, in the form of confidentiality and integrity, is demonstrated by the encryption and signing of information. Federation trust services provide the runtime demonstration of trust relationships by implementing the appropriate encryption and signing of information exchanged between federation partners as part of a FIM protocol.

Federation trust relationships must be established before FIM can be implemented. These trust relationships can be determined based on out-of-band techniques, including face-to-face meetings, email, etc., or can leverage services offered by a TA&AA as described earlier. TA&AA services will allow federation partners to bootstrap a trust relationship based on a TA&AA-issued federation/assertion signing certificate.

A trust infrastructure is required to ensure that the user lifecycle management is implemented in an environment consistent with the requirements for transactional confidence. If the user lifecycle process is not managed appropriately, then transactional confidence cannot be satisfied.

Federation trust services are used to issue, validate, and exchange mutually trusted assertions (also known as tokens) exchanged between federation partners. These trusted tokens are transferred between partner sites and are used to authenticate and vouch for users as part of a single-sign-on process. For example, an Identity Provider will authenticate a user through traditional means such as username and password or strong authentication techniques. When a user attempts to access a resource at a Service Provider, the Identity Provider will issue the appropriate assertion required by the Service Provider. If this assertion is not understood by the Service Provider, the Service Provider may request that the Identity Provider exchange this for a different assertion.

+ Next-Generation Identity Management Services

Next-generation identity management (NextGen ID Mgmt) requires the integration of current enterprise Web presence enablement solutions and federated identity management and the underlying trust infrastructure over which these integrated solutions are implemented. In this section, we briefly define and describe the services required to support a next-generation identity management solution.

Authentication Services

Authentication services are required to support direct authentication of users. An authentication service is able to evaluate user-presented authentication credentials. Authentication services commonly support username and password type authentication credentials.

To fully support NextGen ID Mgmt, an authentication service must also support strong authentication techniques, such as hardware-token-based authentication credentials, and two-factor authentication techniques, such as a PIN-enabled hardware tokens.

Within a federated model, each user will have one federation partner that acts as that user's Identity Provider. The Identity Provider is responsible for authenticating the user and vouching for that user to federation partners. The Identity Provider maintains a user's authentication credentials. Once a user has been authenticated, the Identity Provider will be able to provide trusted tokens on the user's behalf to trusted federation partners, validating, or vouching-for, the user to the Service Provider.

Session Management Services

Session management services implement session creation and deletion functionality as well as the management of an existing session. Session management services often incorporate authentication services as a logical component to allow for session creation based on successful authentication.

Session creation is normally the result of a successful authentication. Within a NextGenIdMgmt solution, session creation must be possible in response to a successful authentication as reported by an Authentication Service and by successful single-sign-on as reported by a Federated Identity Management Service (see below).

Session deletion is a response to activities such as an explicit user logout, session inactivity timeout, or an administrator-forced session deletion. Within a NextGen ID Mgmt solution, session deletion may also be in response to a single logout request, that is, in response to a logout request that is brokered by a third party on behalf of a user.

Authorization Services

Authorization services are already a part of many enterprises' Internet presence. When a user requests a Web-enabled resource or Web service, authorization must be applied to the Web services to see if the user has permission to use the resource in the requested manner (for example, read, write, etc.). As part of the management of a user's session, a session management service may invoke an authorization service to request authorization decisions. This will allow the session management service to act as an Access Enforcement Point while the authorization service implements an Access Decision Point (according to ISO-7498).

Federated Identity Management Services

Federated identity management services provide the user lifecycle functionality required to support a user's participation in a federated relationship. The most obvious functionality required is the single-sign-on functionality that allows a user to authenticate to an Identity Provider and then single-sign-on to one or more Service Providers.

In addition to single-sign-on, FIM services are required to support functionality that allows a user to link their accounts at different federation partners to enable single-sign-on, to break this linkage if desired, and to implement single logout (allowing one logout request to delete all sessions within a federation). For a Service Provider, a FIM service implementation must also be able to determine where to request single-sign-on from for each given user. This additional functionality is best described as "Where are you from?" functionality.

FIM services must integrate with existing session management services in several ways. A session management service must support a FIM service as an authentication service to allow for single-sign-on. A session management service must also support a FIM service as a means of providing a session deletion request.

FIM services themselves must also include/support services. These services may be implemented as logical services within a FIM service infrastructure, or they may exist as stand-alone or pluggable services. These FIM services include:

- **Protocol Services**
  A FIM protocol service implements the runtime services (protocols) required to implement user session and lifecycle management. These runtime services include single sign-on, single-sign-off, account linking, account de-linking and "Where are you from?" functionality.
- **Assertion Services**
  While some federation protocols restrict the type of assertions that are passed between partners, other protocols allow for a customizable assertion about a user. This implies that some form of assertion or token service is required to evaluate the contents of an assertion within, for example, a single-sign-on request. Assertions contain information such as user aliases, which are used in place of user identities such as email or username, and attributes about a user/their session attributes at the Identity Provider.
- **Alias Management Services**
  Within a federation protocol, there is often the need to uniquely refer to a user in some manner that does not reveal information about the user; these techniques use aliases to provide a common, unique identity for a user that is opaque with respect to the user's local identity. Alias management services provide support for the creation, deletion, storage, and retrieval of these alias values.
- **Attribute Transformation Services**
  As part of a federation protocol, a partner may include attributes about a user that provide information for the other partner. As these attributes may not be globally identified, the attributes values may need to be transformed (mapped, retrieved, etc.) to locally valid attributes. An attribute transformation Service Provider provides this functionality.
- **Provisioning Services**
  Provisioning services allow a Service Provider to rely on an Identity Provider for complete user lifecycle management, from account creation to account deletion, as opposed to session creation to deletion. Federation provisioning allows a Service Provider to initiate the creation of a local user record, with a set of attributes, in response to a provisioning trigger from a Service Provider where no account or attributes previously existed.

Trust Services

Trust services provide the trust infrastructure over which federated identity management solutions are implemented. This includes the management of trust information, such as signing and encryption keys and certificates used by federation participants. Trust services provide the means of managing the trust relationships by providing an additional binding of partner identity to trust assertion information such as federation assertion signing credentials issued by a TA&AA. This binding is then used as additional proof of the authenticity of a partner (not user) acting within a federation relationship. For example, a trust service will use a TA&AA issued assertion signing certificate as part of the evaluation of a partner's signature placed on an assertion. Note that this assertion does not refer to the partner, but a user that has been authenticated by the partner.

+ Integrating NextGen ID Management Solutions

Next-generation identity management solutions must also include a trust infrastructure and management of the appropriate trust relationships.

Support of NextGen ID Mgmt solutions must be integrated into an existing partner's infrastructure. This means that support for FIM solutions must integrate with existing authentication, access control and identity management systems as well as interoperate with other partner's federation solutions. An Identity Provider will continue to directly authenticate users but must now add the ability to complete a single-sign-on request for that user to a trusted Service Provider. A Service Provider may no longer directly authenticate users and must be able to initiate a single-sign-on request for a user as well as build an authenticated session for the user in response to a single-sign-on response. Finally, participation in a federation should not force a partner into a single role of only a Identity Provider or Service Provider.

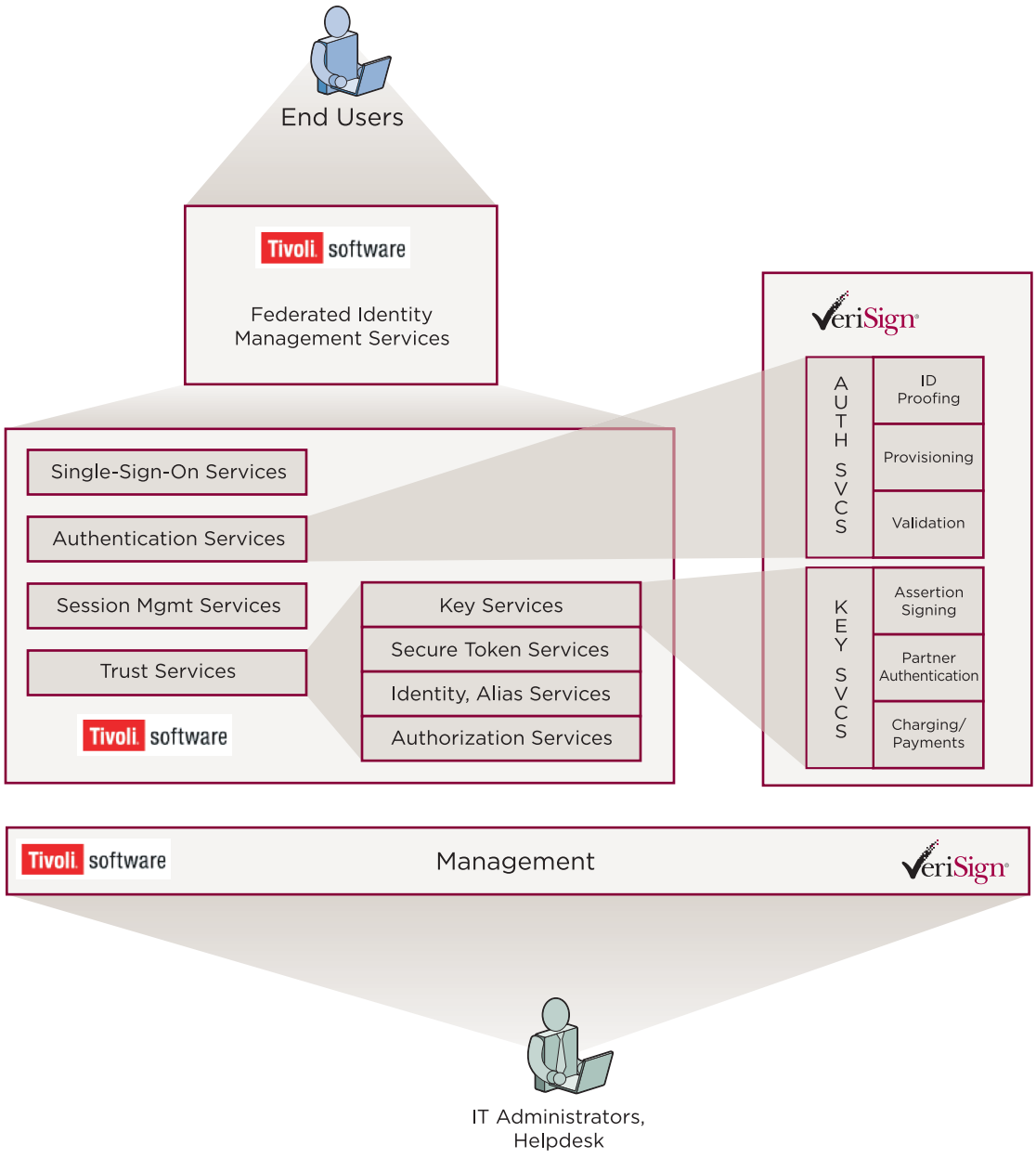
Interoperability with a federation partner requires agreement on the federation protocol to be used and on the means of transferring information between partners.

Federated identity management protocols, such as Liberty ID-FF and WS-Federation, describe the protocol used to communicate single-sign-on information. Thus the protocol itself and the format of the single-sign-on information must be agreed upon. As FIM protocols are simply a means of communicating information, agreeing on the protocols to be used is a relatively simple task.

FIM techniques do not provide a complete NextGen ID Mgmt solution. As was mentioned earlier, in practice, the main barriers to deployment are differences in trust semantics rather than differences in protocol. Note that these solutions require a trust infrastructure that must be bootstrapped and possibly brokered as described above. A trust infrastructure is required to ensure that the user lifecycle management is implemented in an environment consistent with the requirements for transactional confidence. If the user lifecycle process is not managed appropriately, then transactional confidence cannot be satisfied.

NextGen ID Mgmt leverages standards-based and public FIM specifications, such as those defined by the Liberty Alliance Identity Federation Framework and the Web Services Security Roadmap and WS-Federation specification. Identity

Figure 2



Providers and Service Providers may be required to support these and other federation protocols as part of participation in a federation. A customer or supplier with a very strong market position, such as a leading retailer or automobile manufacturer, may be able to impose protocol standards on its partners, but few enterprises enjoy such a position. The partners of such enterprises are likely to find themselves required to support multiple specifications.

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 TA&AA 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, as shown in Figure 2. The figure shows a solution overview for the combined IBM-VeriSign Federated Identity offerings. The major components for the joint offering are described in this section.

+ 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.

The UA solution enables certificate- and token (OTP)-based authentication in a Tivoli Access Manager deployment and will support PKI validation using CRLs or OCSP, and OTP validation.

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 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.

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 Server, 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 in Figure 2.

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.

In Figure 2, the IBM Tivoli FIM functionality is required to integrate with the Point of Contact and possibly with a local user registry. This architecture has been designed to minimize the impact and integration requirements on an existing environment.

- **Browser**
  A browser provides an interface between the end user and the infrastructure. In order to participate in FIM protocols, the browser must be capable of supporting redirects and/or automatic forwarding (POST) of requests (via Javascript or ActiveX).
- **WAP Browser**
  A WAP browser, that is a browser used by a mobile device, may have limitations not found with Internet-based browsers, such as query-string size limitations. Specific techniques to address WAP uses cases exist for FIM functionality and are described in more detail below.
- **Tivoli Access Manager**
  Implements Authentication Services, Session Management Services, Authorization Services, and Identity Service functionality. It is also able to invoke (when required) Single-Sign-On Services as part of the implementation of federation identity management functionality.
- **FIM Functionality**
  IBM Tivoli FIM functionality implements the Single-Sign-On Services required to implement federated

identity management. As a black box, this also includes Trust Services, as used by the SSO Services. FIM also includes Identity Service functionality, allowing this functionality to integrate with external user datastores as part of user identity and attribute management.

- **User Registry**
  IBM Tivoli FIM functionality requires some form of user registry/data store for maintaining the CUID-local identity mapping. This user registry may be implemented as an internal, private FIM registry that is used by FIM only (minimizing integration requirements with local user registries). IBM Tivoli FIM functionality may also leverage existing user registries. Levering an existing user registry allows the FIM components to access additional (partner maintained) user attributes that may be required as part of the user's CUID-local identity mapping. This user registry/data store is accessed by an Identity Service, which provides an implementation independent means of access this data store.

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 and the ability to cost effectively manage the inherent risk associated with it.

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

00017877