Enterprise Identity Management: Beyond PKI into Federation

An Exostar whitepaper

July 2005

Developed by:

Exostar, LLC
13530 Dulles Technology Dr., Ste 200
Herndon, VA 20171
USA

TABLE OF CONTENTS

Executive Summary

Secure collaboration makes trusted e-business possible.

Authoritative digital identities are the foundation for trusted e-business. They provide assurance that the parties you're doing business with online are in fact who they claim to be. Consequently, digital identities are the basis for security, control, auditing, compliance, and customer service within today's online economy. With ever-increasing corporate governance and regulatory hurdles, the management of these identities introduces new business compliance issues. Enterprises are deploying IdM infrastructures to address growing privacy, compliance, legal, and regulatory requirements.

Identities pervade all aspects of modern e-business. Digital identities drive the provisioning and management of accounts for access to essential business services, such as e-mail, local area networks, and virtual private networks. Unfortunately, many enterprises have established IdM "silos" or "stovepipes" within their internal and external networking environments. These IdM silos impede organizations' ability to automatically create, manage, and terminate accounts across diverse applications. IdM silos also contribute to suboptimal user experience, since people must often log in separately to various applications (rather than avail themselves of the single sign-on experience of a truly unified IdM environment). In addition, IdM silos contribute to high costs of administering user accounts, passwords, and credentials, due to the need for help desk personnel to manually handle such mundane functions as resetting forgotten passwords (a function that could be automated securely within a unified IdM environment).

> PKI is an important component of Identity infrastructure, but it doesn't address account provisioning, authentication and access management.

PKI is an important component of a unified, end-to-end IdM environment, but it's not the only critical trust and security infrastructure. Enterprises in the A&D industry have invested heavily in PKI to support strong assurance on the authentication process, which ensures that person presenting credentials to an online application or other resource is in fact who they claim to be.

However, PKI does not adequately address the problem of linking an authoritative digital identity with an e-mail, local area network (LAN), enterprise resource planning (ERP), or other application accounts—a function known as "account provisioning."

In addition, PKI digital certificates don't provide sufficient information that applications need for authorization—in other words, to determine whether a particular user should be granted access to enterprise resources, such as applications, documents and data records.

Furthermore, PKIs haven't been universally deployed and integrated with all applications, platforms, and devices. Among other issues, it's quite difficult to set up and administer all of the requisite trust relationships among PKIs in use through a heterogeneous, multinational, B2B supply chain.

Consequently, traditional PKI-based trust infrastructures are not yet up to the challenge of managing complex B2B environments. Federated IdM is an emerging industry best practice for dealing with the heterogeneous, dynamic, loosely coupled trust relationships that characterize companies' external and internal supply chains. Federated IdM enables strong authentication, Web single sign-on (SSO), role-based access control (RBAC), and other trust-enabled security services across diverse identity, security, and application domains.

Federated IdM addresses these challenges by providing a standardized way to manage user identities within and between organizations. A federated business model enables an enterprise to share selected identity information about their users with a trusted partner. This enables the partner company to make access management decisions without having to administer distinct identity accounts for the third-party user within the company.

Federation is a relatively new approach to distributed identity and security, but it's by no means a "bleeding edge" approach. In fact, it has rapidly become the predominant approach in new IdM deployments over the past few years, especially since the industry ratification of the Security Assertion Markup Language (SAML) standard in late 2002. Vendors such as BMC, Computer Associates/Netegrity, Entrust, Entegrity, HP, IBM, Microsoft, Novell, Oracle/Oblix, RSA Security and Sun have made standards-based federation the core of their IdM, security, policy, and trust infrastructure strategies going forward. There are a growing range of federated IdM deployments in most industries throughout the world. Not surprisingly, federated IdM has begun to take hold in production and pilot deployments in the aerospace and defense (A&D) industry.

The value proposition of federated IdM is clear-cut. Federated IdM environments enable delivery of e-business services and solutions that are functional, secure and cost-effective. Enterprises realize return on investment (ROI) from federated IdM in three principal areas: tightened security, reduced costs, and improved user experience. These benefits can be realized across diverse trading partners in a B2B environment, or within a single, diversified organization implementing federated IdM among its various business units. We discuss these federated IdM ROI components in greater detail in this whitepaper.

> Federated identity environment enable delivery of secure e-business that reduces costs, mitigates risk and improves user experience.

The roadmap to federated B2B IdM demands coordination of various business, technical, and policy issues among partner companies, organizations, and business units. Federated IdM leverages existing trust relationships among organizations, which are, in turn, built upon a solid track record of mutually satisfactory and productive business relationships. Within the PKI world, organizations establish trust relationships that are predicated among all partners publishing their respective enterprise "certificate policies" and "certificate practice statements." These documents describe how an organization manages digital certificates throughout their lifecycles, all the way from proofing and enrollment to certificate issuance, validation, and revocation.

This same approach can and should be applied within the federated IdM world. Organizations that have implemented federated IdM should publish their IdM policies and practices in a standard syntax, such as the Federated IdM Policy and Practice Statements (FIdPPS) framework being proposed by Exostar. An FIdPPS describes an organization's policies and practices governing the following functions:

- Identity and account provisioning across distributed environments;
- Identity proofing and vetting;
- Credentials issuance and management;
- Token, session, and claim lifecycle management;
- Identity repository management;
- Auditing and logging; and
- Facility management.

Vertical industry sectors should strongly consider defining standard FIdPPS formats and rules that are applicable to all firms doing business in those markets. Furthermore, vertical sectors should consider relying on TTPs to vet and certify organizations' published FIdPPSs for compliance with accepted standards. In this way, all trading partners in a particular industry might be able to rely more thoroughly on the trustworthiness of each others federated IdM "claims," "tokens," or "assertions," knowing that all participants' federated IdM procedures have been certified to a common standard.

A&D industry should standardize industry federation profiles and seek the services of a Trusted Third Party to certify enterprise policies enabling an efficient and scalable solution.

The A&D industry should institute sector-wide FIdPPS standards and rely on a sector-wide TTP to vet, certify, and vouch for the equivalence of all A&D companies' compliance with these standards. In pursuing such an approach, the A&D industry would be ensuring that any FIdPPS-compliant company is eligible to participate in the A&D industry's federated IdM community. For example, the FiDPPS standard might prescribe mandatory identity and account management policies, procedures, and practices rules applicable to export/import control throughout the multinational B2B A&D supply chain. Similarly, the A&D-wide FIdPPS standard might specify minimum privacy-protection safeguards that all companies would need to meet in order to pass regulatory muster in all participating nations. From an efficiency perspective, a TTP such as Exostar's proposed "Trust Enabler" should certify A&D companies' compliance with FIdPPS standards. In this way, this A&D "Trust Enabler" environment can perform a function analogous (and complementary) to the bridge certificate authorities of the PKI world.

In conclusion, Federated IdM—when implemented in conjunction with PKI—allows organizations to provide secure application services to external, trusted users whose identities they do not manage directly. TTPs can provide federated IdM certification services based on industry-wide standards. In this way, TTPs, such as the proposed "Trust Enabler," would enable more secure B2B collaboration.

Introduction

In this whitepaper, Exostar examines the issues of federated identity management (IdM) in general, placing special emphasis on its applications of that technology within the aerospace and defense (A&D) industry. Nevertheless, the lessons learned from federated IdM deployments in the A&D sector are applicable to all industries.

Federated IdM environments are foundation for trustworthy, productive, flexible e-business. They allow your enterprise to tighten security while also controlling operational costs and improving users' quality of experience. They are a critical component of ensuring that your organization complies with regulations such as Sarbanes-Oxley (Section 404, specifically), Gramm-Leach-Bliley, and HIPAA.

> Federated identity management delivers mitigate risk, reduce costs, and improved user experience throughout the B2B supply chain.

The intended readers of this whitepaper are enterprise architects, chief security officers, chief technology officers, and chief information officers within the A&D industry. The paper provides a perspective on the identity, security, and trust challenges facing the A&D sector. It describes federated IdM as an approach for addressing these challenges. And it recommends a new federated IdM service--called "Trust Enabler"—for establishing trust environments throughout the business-to-business (B2B) supply chain and leveraging companies' identity management infrastructure investments.

The A&D industry is continuing to make major investments in the area of federated IdM, recognizing the need for an infrastructure solution that is available across multiple programs. At the same the industry needs to meet regulatory mandates when collaborating across organizational boundaries. In implementing federated IdM, the A&D industry is driven by the requirements of major customers the defense departments of various nations, especially the US Department of Defense (DoD) and the UK Ministry of Defense (MoD). The US DoD has recognized the need for stronger authentication credentials and is issuing Common Access Cards (CAC) to its personnel to meet this objective. In addition, under the auspices of the General Services Administration (GSA), the U.S. government has established a Federal PKI Bridge Certificate Authority (FBCA) to improve interoperability among public key infrastructure (PKI)-based communities of trust.

To connect to this expanding government-sponsored PKI trust environment, the A&D industry plans to implement a PKI Bridge Certificate Authority managed by CertiPath, which is a joint venture of ARINC, EXOSTAR and SITA. CertiPath's mission is similar to FBCA, but with the additional requirement of providing a trusted credential that is interoperable with the existing US Federal PKI communities and future international government PKI initiatives. Major A&D industry participants are working with the DoD and the MoD under the Transatlantic Secure Collaboration Program (TSCP) to implement industry wide secure collaboration solution.

Under the TSCP, A&D firms and the US and UK defense departments have identified the need to extend PKI infrastructures to meet the requirements of access management and strong authentication requirements. TSCP has identified federated IdM as a key enabler of secure B2B and multinational collaboration among diverse organizations. TSCP has also identified trusted third parties (TTPs), such as Exostar, as playing a critical role in enabling more robust B2B trust that leverages federated IdM and PKI.

Secure e-business: PKI critical, but not enough

Authoritative digital identities enable security, control, auditing, compliance, and customer service within distributed network application infrastructures. Digital identities can best be managed within a general-purpose, online trust management infrastructure. Every e-business relationship is a trust relationship that must be codified in diverse agreements, policies, and procedures binding on all partners, and reflected in a broad range of credentials.

In general, applications depend on multiple attributes about a user's identity in order to support such critical security functions as authentication and authorization. These critical identity attributes fall into the following general categories:

- ***Authentication attributes*:** These are any attributes or data structures that are bound to the core identity (such as the userID) and are used to authenticate the security principal (also known as a "user"). They are also referred to as "credentials." PKI X.509v3 certificates are a type of credential. Passwords, personal identification numbers (PINs), and biometric patterns are other credentials, which, when used to log into applications, may also be referred to as "authentication factors."
- ***Authorization attributes*:** These are attributes that define privileges, permissions, rights, roles, or entitlements associated with a particular identity. For example, roles are a type of authorization attribute. Authorization attributes are often used by applications as part of access control decisions at the transactional level.
- ***User profile attributes***: These are any attributes that don't support authentication or authorization decisions. For example, a user's e-mail or postal address may be stored in a directory but not be used for login or access control.

PKI is backbone of any enterprise identity, trust, and security environment.

In essence, a PKI X.509 digital certificate is an assertion by a trusted authority—usually referred to as a "certificate authority" (CA)--about an identity and about other attributes—such as an e-mail address--that are cryptographically bound to that identity. The PKI digital certificate's cryptographic binding enables a PKI-relying party—such as the recipient of a signed or encrypted document--to verify with assurance that a document was indeed signed and/or encrypted by its purported originator. Generally, PKI digital certificates and their corresponding private keys enable the following fundamental security services within network environments:

- ***Authentication***: server authentication and/or client or end-entity authentication, by means of Secure Sockets Layer (SSL) and other PKI-reliant protocols;
- ***Confidentiality***: content encryption and/or session confidentiality, via SSL, Secure Multipurpose Internet Mail Extensions (S/MIME), XML Encryption, and other PKI-reliant protocols, formats, and interfaces;
- ***Integrity and tamper proofing***: digitally signed messages, documents, and other objects, via XML Signatures and other PKI-reliant protocols, formats, and interfaces;
- ***Non-repudiation***: sender and/or recipient non-repudiation of message origination, delivery, and/or receipt, via PKI-reliant digital signatures and/or trusted timestamps applied to message contents and/or to message delivery and receipt notifications

Clearly, PKI is a critical component of every organization's trust management environment. PKIs provide the core environment for registering, issuing, storing, transmitting, validating, verifying, and revoking public key certificates. PKI is used universally to provide e-business security in critical infrastructure services, such as Web server authentication and session confidentiality

(which leverages SSL) and virtual private networks (which leverage PKIs to provide session confidentiality in many organizations' intranets and extranets).

However, PKI digital certificates don't address authorization requirements. The PKI industry recognized this issue and defined PKI attribute certificates. However, PKI attribute certificates are a concept that has seldom been implemented in the real world. The reason for this is that applications in general have historically stored most identity attributes in directories and databases, which support dynamic attribute updates and modifications, rather than in relatively static cryptographic objects such as PKI certificates.

PKI digital certificates don't play into most authorization decisions, beyond the initial decision to authenticate a user login based on presentation of an X.509 certificate and other credentials. Likewise, PKI certificates do not address the need to provision the necessary user identity attributes such as roles, in application accounts.

> Authorization - who can access what resource - is critical component of B2B secure collaboration and is entirely separate from PKI.

Consequently, PKI is critical to B2B security, but it's not sufficient, especially where role based access management and account provisioning are concerned.

For example, two companies might establish a PKI-based trust relationship. Under that relationship, the companies cross-certify their respective PKIs, so that each firm's employees can use their certificates to access the other's applications. As part of this relationship, each firm might also provision the other's employees with identities, accounts, and roles on the requested applications (in addition to whatever identities, accounts, and roles those people also have on their employers' internal systems).

One big risk of this arrangement is that an individual's internal roles on their employer's systems might change without those changes being propagated immediately to the trading partner's systems. As a consequence, one firm might inadvertently grant the employees of its trading partners an inappropriate level of access on its own applications and data.

Federated identity management: the key to trustworthy e-business

To enable truly trustworthy e-business, organizations must implement comprehensive IdM environments that leverage and extend their PKI investments. IdM infrastructures allow organizations to tighten security, cut costs, improve user productivity, manage risks, and ensure continuous compliance with legal and regulatory mandates. Federated IdM provides an environment wherein trust, identity, account, and role provisioning can be managed effectively on an end-to-end basis across organizations, over and above what's possible with PKI.

> Federation enables standards-based account provisioning and single sign-on across organizations.

Directories are the first step toward general-purpose, comprehensive IdM environments that can be leveraged across all applications, both internal and external. In the past few years we have seen many enterprises start to centralize user identity and account management into directories, thereby streamlining IdM lifecycle costs. Typically, enterprises have migrated towards a centralized directory model that implements LDAP. Much of the information needed by an application to make authorization decisions resides in centrally managed directories, which provide authoritative repositories for user accounts.

Organizations everywhere, and in all sectors, are migrating toward integrated IdM infrastructures. Administration of users, groups, passwords, digital certificates, roles, and other identity information must be centralized within secure, general-purpose, client-agnostic infrastructures. Without an integrated, pervasive, general-purpose IdM environment, organizations can't consistently enforce strong authentication, enterprise SSO, and other policies across their distributed environments. A general-purpose IdM environment ensures that the right people have authorized access to appropriate online resources--and that all others are kept out. Yesterday's application- or platform-specific IdM "adhocracies" must give way to scalable, standards-based infrastructures that span applications, platforms, and organizational trust boundaries.

Increasingly, trust relationships are being defined, enforced, and monitored in IdM environments. At the heart of IdM environments sit one or more identity repositories—such as corporate directories—that designate who may access various resources under various conditions. Companies are always under pressure to provide a broader set of users with ready access to a broader range of new e-business applications and corporate information assets. Consequently, the trust boundaries grow ever blurrier and virtual, and the business risks grow ever more acute. IdM environments allow organizations to control the resource access of external personnel—such as contractors--as closely as they control access by corporate employees.

Within complex, heterogeneous IdM environments, such as those associated with B2B supply chains, the emerging best practice is called "federation." Federated IdM refers to an architecture, protocols, policies, and practices that support account provisioning, SSO, RBAC, strong authentication, and other security services across two or more autonomous organizations or identity, security, policy, trust, and application domains.

Federation is a potent term, deriving from the ancient Latin word for "trust." In the modern world of distributed network services, federation refers to the need for trust relationships among decentralized domains. It requires that an organization trust each of its partners to authenticate their respective users' identities and also vouch—in the form of secure, structured message exchanges--for successful authentications. Essentially, Security Assertion Markup Language (SAML), Liberty Alliance, WS-Federation, and other IdM standards describe various approaches

for structuring the message exchanges among federated domains. All the above standards depend upon exchanging identity attributes information after initial authentication process with federated partner companies. This information is digitally signed using the private key that is cryptographically bound to the public key that is asserted by the X.509 certificate of the user's company. The digital certificate is used to verify the integrity of the information and protect against repudiation by the issuing company.

Federated IdM enables account linking, SSO, and RBAC across diverse network and application environments. It is enabled through standards, technologies, and agreements that allow organizations to interchange and validate identities, attributes, roles, and permissions across autonomous domains. Within a federated IdM environment, a user can log into his or her company's domain and then leverage that authentication to access resources transparently in external domains, such as those managed by customers or suppliers, subject to various policies defined by local and external administrators.

> Federated identity management refers to the set of business agreement, technical agreements and policies that enable companies to effectively manage identity lifecycle costs while improving user experience

Federated IdM environments define what amounts to an abstraction layer over the legacy identity and security environments of diverse domains. Each domain maps its local identities and attributes to the agreed-upon schemas and syntaxes. Federated IdM environments generally leverage and interface a broad range of existing, heterogeneous infrastructure services. Consequently, domains can retain their internal directory, meta-directory, account provisioning, and PKI services, as long as their external IdM interfaces implement a common federated IdM standard such as SAML.

Federation allows autonomous domains to maintain control over their respective users' identities, as well as over the resources that they allow internal and external users to access. In a federated environment, identity information need not be replicated or synchronized across diverse federated domains. Instead, identities and other attributes can continue to be stored, managed, and controlled locally by the administrators of the domain in which they are registered. In this way, federated IdM allows B2B trading partners to deal with the risks outlined above, in terms of propagating identities, accounts, roles, permissions, and attributes automatically, in keeping with bilateral policies, across distributed environments.

Federated IdM is well-suited to the heterogeneous, decentralized, loosely coupled fabric of modern e-commerce. In the real world, no one administrator has responsibility for registering all users, activating all accounts, and granting all access privileges in B2B environments, or in many large, multidivisional companies. At the same time, though, administrators of the various domains don't want to give up local control and storage of identity information. Consequently, federated IdM may be regarded as a mechanism for enterprises to address the authorization challenge, while not taking on the burden of third-party user account management.

A real world example of federation is the universally accepted bank automated teller machine (ATM) networks—such as Cirrus. These multi-institution ATM networks allow users to login remotely to their bank accounts from any federated institution's machines. Users enter their identities (account numbers and PINs) at a federated bank's machine, which routes that information securely to the bank that granted and administered those credentials, and that provides the user's account. If the user authenticates successfully from the federated ATM machine and has requested a sum of money that is within their current bank balance, their home

bank authorizes the federated bank to dispense the money. The federated institutions handle all the authentication, authorization, routing, reconciliation, and settlement behind the scenes, within their network, and appear, from the user's point of view, as a seamless money-dispensing environment.

Federated identity can be implemented with various standard protocols and specifications.

Within federated IdM environments, organizations aim for a similar degree of seamlessness in handling strong authentication, SSO, RBAC, and other distributed security transactions. The functional model for federated IdM revolves around the following principal functional infrastructure nodes in the various domains (various underlying IdM protocols can be used to implement these architectural concepts). Please note that the end user would generally interact with this infrastructure through a presentation front-end such as a Web portal, or through applications that were written to access the strong authentication, enterprise SSO, and other features provided by the federated IdM environment. The following functional architecture might rely on a Web services environment, but it can just as readily be implemented in a heterogeneous identity, trust, and security environment involving both Web and legacy protocols:

- ***Identity provider (IdP)***: IdPs create, register, manage, and authenticate identities, credentials, roles, permissions, and other network identity attributes associated with users. Typically, the IdP provides a capability for users to log in to the federated collaborative space. An IdP will usually have an associated presentation interface, authentication service, and user directory. After authenticating user credentials against a trusted authentication service, the IdP transmits authentication and attribute assertion messages to service providers who control access to the resources that users are requesting. The authentication and attribute assertion messages vouch for user login and various user attributes (such as roles, groups, and citizenships) managed by that IdP. The user's credentials—such as passwords or PKI certificates—never flow outside the IdP's domain.
- ***Service provider (SP)***: As noted above, SPs provides content, applications, and other resources to users. Typically, an SP is another portal or application platform (managed separately from the IdP) that controls resources to which users require authenticated access. The SP will usually have an associated presentation interface, authorization service, and policy rulebase. The SP relies on authentication and attribute assertion (i.e., voucher) messages transmitted from IdPs when authorizing a user to access a requested resource.

Figure 1 provides a graphical overview of a basic federated IdM environment, noting the principal assertion messages or data structures interchanged among various functional components. Note the difference between functional components (such as principals, authentication authorities, attribute authorities, policy decision points, policy repositories, policy enforcement points, and resources), data structures (such as authentication assertions, attribute assertions, and authorization decision assertions), and supporting technologies (such as LDAP directories, RADIUS servers, Kerberos key distribution centers, relational databases, and portals).

This figure provides an abstract functional model that is largely agnostic to the underlying "plumbing" of the federated IdM environment, in terms of such enabling protocols as WS-Security, SAML, Liberty Alliance Identity Federation Framework (ID-FF), and WS-Federation. Also note that this diagram primarily describes the functional components necessary for federated SSO and RBAC, but doesn't show the necessary components for federated account provisioning across domains.

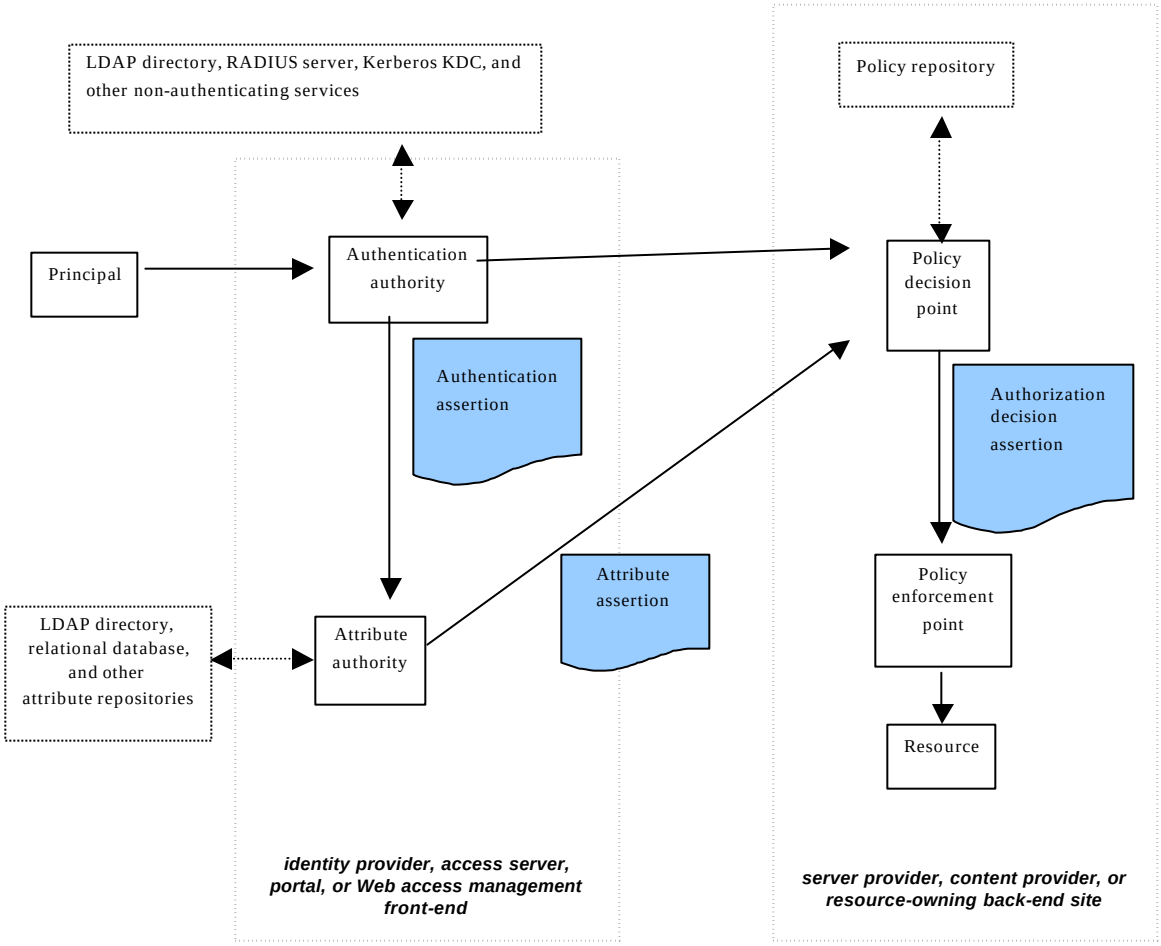

Figure 1: Federated IdM environment

For example, a typical Assertion-based Web SSO use-case involves browser-based users logging into their home domain IdPs through authentication techniques such as ID/password (over Secure Sockets Layer (SSL)) against an LDAPv3 directory or PKI digital certificate authentication using client authentication SSL. The home domain's IdP portal is configured as a SAML "authentication authority." The IdP, after successfully validating the user's ID, password, and any other credentials, then vouches for that event by creating an "authentication assertion" message that it transfers to a "policy decision point" configured into the SP, thereby enabling the user to log transparently into the SP and access the requested resource. All of this protocol interaction takes place transparently to users, who only see the initial login challenge screen and the browser redirects taking them to their requested application or data.

> Federation is rapidly becoming mainstream approach to enterprise Web SSO and other security services.

Much of this federation terminology may be new or unfamiliar to traditional IT directory and security professionals. However, federation is not a bleeding-edge approach to distributed security. In fact, it has rapidly become the predominant approach in new IdM deployments over

the past few years, especially since the industry ratification of the SAML standard in late 2002. Vendors such as BMC, Computer Associates, Entrust, Entegrity, HP, IBM, Microsoft, Novell, Oracle, RSA Security and Sun have made standards-based federation the core of their IdM, security, policy, and trust infrastructure strategies going forward.

Federation isn't the only approach for enabling diverse IdM domains to interoperate, but it is well-suited to the security requirements of today's decentralized B2B environments. Traditional IdM interoperability approaches—such as meta-directories, delegated directory administration, and directory lookups--usually require that domains copy some or all of their directory information to external domains. At a minimum, traditional approaches allow external domain administrators some degree of access and visibility into the identity information that is managed and owned by others. Under these older approaches, the original custodian of identity data surrenders some control over the data. That loss of control creates an increased risk of fraud, security breaches, privacy issues, and legal liabilities for the owner of the identity data.

Another disadvantage of traditional IdM interoperability approaches is that they require tighter protocol and schema integration between domains. Furthermore, they usually require that additional firewall ports be opened for cross-domain directory synchronization and administration.

> Federation isn't the only approach for IdM interoperability, but it is the only efficient and scalable approach

Due to these limitations and risks, traditional IdM interoperability approaches have been implemented primarily inside enterprises, rather than in B2B environments. Lastly, the complex data sharing scenarios of traditional approaches limit their scalability. Meta-directories and firewall configuration changes can't scale to support millions of identities and hundreds or thousands of partner relationships. The amount of configuration this point-to-point scenario represents is beyond the administrative capacity of both the firewall and meta-directory software as well as the IT departments of any organization.

Enterprises' ROI from federated IdM is in three principal areas: tightening security, reducing costs, and improving user quality of experience. In various ways, as compared with meta-directories and other approaches to distributed security, federated IdM has the advantage. We now discuss each of these advantages in detail.

Securing a distributed, heterogeneous application environment is no easy feat. Typically, identity information is administered by many people, stored in many repositories, and used by many applications and services. The more complex the application environment, the less likely it is that authoritative digital identities and credentials will get propagated, administered, and deprovisioned promptly and reliably across all connected systems.

This IdM fragmentation--typical of many large enterprises—creates the potential for errors, omissions and redundancies in identity data across systems. It calls into question the accuracy and completeness of identity information that exists on systems. It creates the risk that unauthorized users—such as those recently terminated—will gain access to critical systems. When an employee leaves an organization for whatever reason or even has a significant change in role, a significant liability exists for the employer, due to the fact this user's accounts will remain active or will have associated with them privileges greater than those to which their current role entitles them.

A general-purpose IdM infrastructure ensures that all applications are leveraging a common, up-to-date set of authoritative identities, attributes, permissions, roles, credentials, and security policies. Deploying a common IdM infrastructure provides a single point of control, and also facilitates enforcement, tracking, and auditing of security-sensitive interactions for regulatory-

compliance purposes. Federation of this infrastructure enables inter-enterprise SSO without requiring that autonomous domains disclose any local user identity information, thereby strengthening security. And use of strong, multifactor, device-agnostic authentication within this infrastructure provides greater assurance that resources are being accessed by the right people, as opposed to someone who stole or hacked an insider's password.

In addition, federated IdM environments are inherently more privacy-friendly and robust than one of their principal alternatives: identity aggregation services, such as that provided by MSN's Passport. In an identity aggregation service, network identity and user information is kept in a single repository, under centralized control, providing a single point of failure for a network security environment and providing a substantial honeypot for identity thieves. Federated approaches, by contrast, disperse identity information across separate domains under separate control, making it more difficult for any party to aggregate and correlate a significant amount of information on any individual. By the same token, federation reduces the likelihood of single points of failure within in the distributed IdM environments, though access to data and resources in the other federated domains.

Reduce costs

Typically, IT staff members spend too much time tending manually to mundane IdM chores, such as registering new user accounts in diverse applications, reconfiguring roles and Sun have forgotten, and deprovisioning accounts for terminated users. In addition, directory IT administrators must often expend considerable resources transferring and synchronizing redundant identity information among diverse directories, databases, and other repositories. Organizations have invested a lot of money and time in implementing and administering the heterogeneous directories, authentication systems, and other components of their existing IdM infrastructure. For their part, users spend a lot of time waiting for new accounts to be created for them, signing into multiple applications every day, and contacting IT helpdesks over accounts, passwords, and other quotidian matters.

Federated IdM environments reduce the cost and personnel requirements of everyday IdM administration. They also simplify and expedite IdM user support, thereby allowing employees to be more productive and not get distracted from their core jobs. Finally, application developers can work more efficiently, because they can interface to the IdM infrastructure rather than write custom authentication, access control, and other IdM services into their code.

Improve user quality of experience

A typical user might have to remember dozens of ID/password combinations in order to access all systems and applications on which they have accounts. The usability burden grows when systems' ID/password syntax policies vary widely. Users' frustration mounts when they're challenged for IDs, passwords, and other credentials continually throughout their workday, and when they've forgotten the precise ID/password combination for some mission-critical application.

IdM features such as enterprise SSO and federated identity reduce the number of separate ID/password combinations that a user might have to present to diverse systems. At the very least, integrated IdM systems reduce the syntactic heterogeneity among the diverse passwords that users must remember. Many integrated IdM systems also provide users with the ability to register mnemonic IDs and passwords, and to easily recover forgotten passwords through responses to personal questions such as "what was your first pet's name?" An added benefit of many IdM systems is support for personalization, location, and privacy profiles, which allow people to tailor portal user interfaces to their individual preferences.

These are all important applications and benefits for federated IdM. However, bear in mind that the conditions for truly universal, mature IdM federation haven't yet emerged. The principal issues in this regard are:

- The Web services standards for SSO and other security services have not yet been implemented universally in e-business infrastructures, though these standards—such as WS-Security 2004, SAML 1.0, and Liberty Alliance Identity Federation Framework (ID-FF) 1.1—are being implemented widely. Others, such as WS-Federation and SAML 2.0, have not yet been adopted broadly within commercial solutions or real-world enterprise or service provider deployments.
- No B2B communities have implemented the necessary standards-based, third-party-hubbed environment for federated "trust enablement," which would facilitate seamless mapping and equivalency of contractual agreements, information access permissions, credentials issuance and management practices, and other policies with suppliers, distributors, customers, and other trading partners.

Nevertheless, federated IdM has taken hold in the A&D industry. In addition to its coming implementation within Exostar's SecurePass initiative, federated IdM is a big component of the security roadmaps of major A&D companies. At the time that article was published, Boeing, for example, is implementing SAML-based identity federation for both internal and business-to-business SSO, but in phases.

Trust Enabler: critical to trusted B2B federation

As noted above, federated IdM environments revolve around functional entities known as IdPs, which vouch for authenticated logins and various attributes associated with authenticated user sessions. SPs rely upon (i.e., trust) the assertion messages (i.e., vouchers) that IdPs create and transmit. Based on these assertions, SPs authorize—or deny--user access to requested resources.

One critical piece of information that these assertion messages might contain is a description of the assurance level—such as two-factor authentication—associated with a particular login. The SP would use this information in determining whether authentication had been done at a high enough assurance level for the requested resource (such as a highly sensitive operational database). Ideally, an SP should also have visibility into the policies, practices, and controls implemented at the IdP. This knowledge would enable the SP to determine whether the IdP has issued its assertions pursuant to sound, secure operating practices. The more trustworthy the IdP's policies and practices, the more trustworthy the assertions issued by that IdP.

In the PKI world, an X.509 certificate authority often documents its operational controls in the form of a Certificate Policy (CP) definition and Certification Practice Statement (CPS). The Internet Engineering Task Force has defined a standard framework—RFC 3647—for creating CPs and CPSs. In PKI, trust is established through the visibility of CPs and CPSs. The standardized format for CP/CPS documents eases evaluation of different CAs policies and practices for the purpose of determining their equivalence, which is an important component of bilateral trust between CAs. By the same token, CP/CPS mapping around a common security policy standard is the basis for multilateral trust through certificate bridge CAs, such as the US Federal Bridge CA (FBCA) or the proposed commercial bridge, CertiPath.

> Federated trust requires that identity providers certify their policies and practices to common standards.

However, in the world of federated IdM, there are as yet no equivalent standard formats within which an IdP might document its own policies and practices. Exostar is proposing a draft policy framework under which IdPs can describe their federated IdM policies and controls. Under this framework, IdPs would describe their domain's IdM policies in a plain-text document format. IdPs would publish these Federated IdM Policy and Practice Statements (FIdPPS) to collaborative partners when setting up trust and federation relationships with those domains. In its FIdPPS, each IdP would describe its policies and practices governing identity and attribute vetting; identity and account provisioning; credential management (PKI certificates policies and practices will referenced via the CP/CPS); attribute, token, session, and claim lifecycle management; identity repository management; auditing and logging; and facility management.

Of course, it's not enough for an organization to simply assert that it complies with particular IdM policies. For other organizations to fully rely on a particular FIdPPS, an IdP would first have had to gain certification from a TTP that had investigated and vetted that IdP's internal procedures and controls. The TTP—also known as a "Trust Enabler"--would then issue a digital signing certificate which the IdP will use to digitally sign identity assertions, confirming the IdP's adherence to a particular established and published IdM federation policy. The TTP might, within its FIdPPS-compliance assertion, also vouch for the mapping or equivalence between the IdP's FIPPS and those of the relying firm, or the standard FIdPPS for a particular vertical market, nation, or community. Other domains would be able to rely on those TTP-issued FIdPPS compliance and equivalence assertions when deciding whether to trust that IdP's authentication and attribute assertions. In this way, through Trust Enablers, federated IdM environments can

establish multilateral trust for strong authentication, SSO, RBAC, and other services. Consequently, the Trust Enabler becomes the hub of a federated B2B "community of trust," providing the critical services of IdP FIPPS policy definition, vetting, mapping, certification, and vouching.

Figure 2 shows Exostar's vision of the Trust Enabler, anchoring a B2B supply chain community of trust.

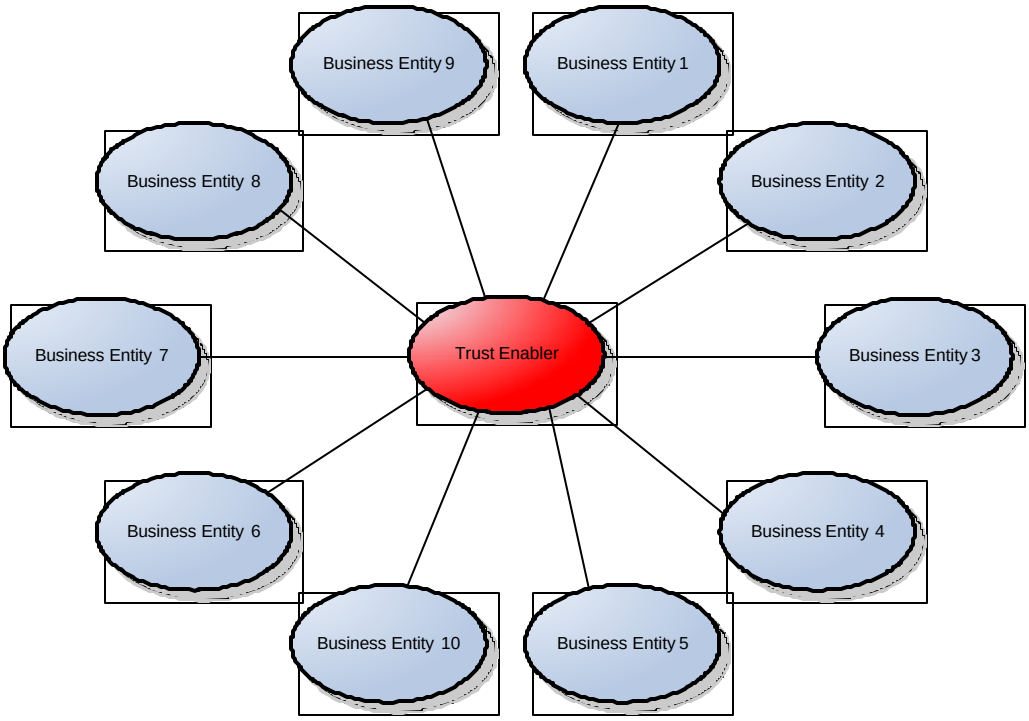

Figure 2: Federated IdM with Trust Enabler

It's important to stress that trust is built on solid business and legal relationships, not on technical protocol plumbing. Trust is nothing without productive business relationships, common goals and policies, well-wrought contractual agreements, and an equitable sharing of risks and liabilities. Organizations that choose to federate their IdM, security, and policy infrastructures—whether bilaterally or through a TTP--must do so within a supportive business context.

Federated trust infrastructures, no matter how sophisticated and well engineered, can't work miracles. They can't magically create trust among trading partners. They can only leverage pre-existing trust relationships into productive collaborations throughout the value chain.

Recommendations

Federated IdM has become a strategic imperative for organizations everywhere, and in particular for the A&D industry in the area of collaboration with partners.

Federated IdM environments are foundation for truly trustworthy, productive, flexible e-business. They allow your enterprise to tighten security while also controlling operational costs and improving users' quality of experience. They are a critical component of ensuring that your organization complies with regulations such as Sarbanes-Oxley (Section 404, specifically), Gramm-Leach-Bliley, and HIPAA.

Within federated IdM environments, strong authentication is the first line of defense against identity spoofing and fraud. As you implement enterprise SSO, account provisioning, and other IdM features across your enterprise and B2B value chains, you'll be creating new security vulnerabilities everywhere if you're not, at the same time, also requiring multifactor user authentication with identity proofing and trustpath validation.

When planning, acquiring, and deploying federated IdM environments, enterprise IT professionals should follow these recommendations:

- Identify the desired organizational return on investment in federated IdM, based on some combination of security improvements, cost reductions, and administrative and user productivity enhancements;
- Implement a general-purpose federated IdM environment that provides a consistent set of authentication, access control, and other services across all internal applications, platforms, and data;
- Define the range of IdM functions to be supported throughout the federated infrastructure, including registration, provisioning, discovery, authentication, authorization, meta-directory, account provisioning, virtual directory, user management, permission management, credentials management, password management, context management, personalization, tracking, auditing, compliance analysis, and administration;
- Assess commercial IdM solutions based on the following criteria:
    - Ability to provide all or most of these functions within an integrated IdM product set;
    - Ability to integrate easily with existing, best-of-breed IdM solutions in which you've invested, via open industry standards, especially those under the growing Web services framework;
    - Ability to leverage and extend your organization's PKI investments;
    - Support for the range of users, clients, applications, operating systems, directories, authentication technologies, and application servers across which you will be implementing enterprise SSO, or, at the very least, reduced sign-on;
    - Support for the assurance levels that will be required for user authentication to applications of varying sensitivity throughout your IdM environment;
    - Support for the roles, permissions, and attributes that will be necessary for multilevel access control to applications throughout your IdM environment;
    - Support for control, tracking, analysis, and reporting features necessary to ensure continued compliance with regulatory requirements;
    - Support for integration and extension via open APIs and industry standards, especially those under the growing Web services arena; and

- Packaging or customization to the particular needs of your vertical market and business process.

- Define and publish standards- based FIdPPS documents that describe your IdPs' policies and practices governing identity and attribute vetting; identity and account provisioning; identity, certificate, password, attribute, token, session, and claim lifecycle management; identity repository management; audit and logging; and facility management.
- Participate in B2B communities hubbed by TTPs that certify your FIdPPS for compliance with established, industry-wide IdM federation policies, so as to enable multilateral trust among you and your B2B trading partners grounded in mapping and equivalence among your respective policies.

For further information contact:

United States:
Exostar, LLC.
13530 Dulles Technology Dr., Ste 200
Herndon, VA 20171
USA
Toll-free Phone: 1-866-239-6782
Toll-free Fax: 1-866-981-7827
Email: customerservice@exostar.com

United Kingdom:
Toll-free Phone: 0800-917-2485
Fax: +1 703-793-1763
Email: customerservice@exostar.com

Worldwide:
Phone: +1 703-561-0500
Fax: +1 703-793-1763
Email: customerservice@exostar.com

Glossary

- ***Account provisioning***: automating registration, publishing, updating, and termination of identity-specific access to applications, services, databases, systems, and other resources;
- ***Administration***: managing the repositories that contain identities and credentials, permissions, roles, and other attributes
- ***Assurance***: the ability of an entity to ascertain, resolve, and verify each other's identities that is consistent with the entity risk profile, and refrain from or repudiate interactions in which such verification is lacking
- ***Attribute authority***: any node that processes an authentication assertion message, retrieves attribute information from a repository (such as an LDAP directory or database) associated with the security principal, and issues a message or data structure (often called an "attribute assertion") vouching for the association between the principal and certain attributes
- ***Authentication***: verifying the identity of a principal for the purpose of gaining access to a resource;
- ***Authentication authority***: any node that passes the credentials of a requestor (a "principal," in IdM parlance) to an authenticating service (such as an LDAP directory or RADIUS server), determines whether a successful authentication has taken place, and issues a message or data structure (often called an "authentication assertion") vouching for the occurrence of that event;
- ***Authentication factors***: devices and/or credentials necessary to authenticate users, including ID/password, smartcard, USB token, and biometrics
- ***Authorization***: controlling an authenticated principal's access to particular applications, data, and other resources;
- ***Compliance tracking***: monitoring the progress of identity-based transactions associated with identities and analyzing historical data on completed and terminated transactions;
- ***Credentials management***: requesting, issuing, distributing, storing, retrieving, validating, synchronizing, mapping, and revoking credentials—such as passwords, PINs, X.509 digital certificates, and biometric patterns--associated with authentication of identities, sessions, and/or objects;
- ***Digital rights management (DRM)***: the ability to encapsulate the resource along with its access and usage policies in a distributable package that persistently enforces those policies throughout the resource's life;
- ***Directory***: any repository of identity information, such as those that support Lightweight Directory Access Protocol (LDAP) lookups; generally, directories enable centralized registration, retrieval, storage, and administration of identities, groups, roles, attributes, passwords, digital certificates, and other IdM-relevant information and objects; directories also frequently import and map identity information from external repositories, such as application-specific databases;
- ***Discovery***: searching for and retrieving the identities of users, groups, applications, databases, customers, suppliers, distributors, and other entities;
- ***Federation*** : any environment within which interoperability spans two or more autonomous administrative domains, such as when two or more independent organizations interoperate within a business-to-business (B2B) value chains, or among different business units within a large enterprise; a domain may be regarded as autonomous if it supports unilateral administration of its own users, resources, and policies, independent of other domains; federated domains choose to interoperate in accordance with business agreements, trust relationships, interoperability arrangements, and their respective local policies; typically, federated domains honor each others' decisions within well-defined spheres of operation.

- ***Meta-directory***: any node that supports the ability to query, retrieve, aggregate, synchronize, join, update, and manage identity information across two or more directories, databases, and other repositories.
- ***Orchestration engine***: any node that automates the policy-driven flow of meta-directory, account provisioning, enterprise SSO, and other IdM interactions between diverse applications, platforms, administrators, users, and other nodes.
- ***Password management***: enforcing password quality standards, enabling self-service or delegated user password resets, and/or synchronizing passwords across domains or applications;
- ***Permission management***: granting to a principal the permission, right, or entitlement to perform a particular action on a resource to which it has gained authenticated access;
- ***Personalization***: the ability to tailor the retrieval, aggregation, and presentation of data and other resources to a user's identity, roles, locations, and other attributes;
- ***Policy decision point***: any node that processes authentication and attribute assertion messages; evaluates the assertions against policies maintained in a repository; and issues messages or data structures (often called "authorization decision assertions") that contain references to valid authentications and attributes;
- ***Policy enforcement point***: any node that processes authorization decision assertions and enforces policies governing access to particular resources.
- ***Policy repository***: any node that maintains a store of permissions, rules, and other policies governing authenticated, authorized access to resources;
- ***Registration***: enrollment, creation, and issuance of digital identities, user attributes, permissions, roles, credentials, and other information into directories or other authoritative identity repositories;
- ***Resource***: an instance of information, services, or capabilities requested by and delivered to principals online, subject to authentication and authorization controls.
- ***Role-based access control (RBAC)***: the ability to control access to resources based on the role attributes of various requesters and permissions associated with requested resources;
- ***Single sign-on (SSO)***: the ability to enable authentication to multiple applications controlled by one or more authentication authorities, based on a single client-side user-login event; enterprise SSO sometimes relies on IdM infrastructure components that cache user credentials and present them to relying parties; enterprise SSO may also rely on identity federation, an approach under which one authentication authority authenticates its own users' logins and issues assertion messages that vouch for those logins to external relying domains;
- ***Strong authentication***: the ability to provide more certain verification of a principal's identity through presentation of two or more unique authentication factors, such as ID/password (i.e., something only the principal knows), digital certificate and smartcard (i.e., something only the principal holds), and voice and fingerprint recognition (i.e., something only the principal embodies);
- ***Trust management***: approaches, disciplines, processes, environments, infrastructures, and/or tools for registering, issuing, storing, transmitting, validating, verifying, and revoking public key certificates, federated IdM policies and practices statements, and other credentials instrumental to establishment and maintenance of trust relationships among various entities;
- ***User management***: creating, managing, and revoking user accounts, identities, roles, permissions, and other attributes;
- ***Virtual directory***: any nodes that supports query and retrieval of identity information from multiple directories, databases, and other repositories; aggregation of this information; and tailoring of the logical view of this aggregated information to each user or client application.
- ***Web access management (WAM)***: authentication, SSO, authorization, and other IdM functions through browser-oriented portals