realtimepublishers.com™

The Definitive Guide™ To

Identity Management

SafeNet®
The Foundation of Information Security

Archie Reed

Copyright Statement

Chapter 5: Identity Management Standards

Chapter 1 provided an introduction to Identity Management standards—this chapter delves into the fundamental Identity Management standards that you should evaluate as you define your requirements for and plan an Identity Management implementation. As with many areas of focus, a significant amount of effort by many individuals and organizations has been devoted to defining and implementing standards around Identity Management. Standards defined by recognized groups and authorities provide key levels of interoperability and might be formally published and mandated or adopted through common use.

Although there has been an undue amount of duplication as well as contention between the standards bodies that are creating potentially proprietary solutions, this behavior appears to be diminishing. There is increased participation from organizations that actually use the resulting solutions as opposed to vendors who need to solve a specific interoperability problem.

The goal throughout this chapter is to determine which standards solve the challenges of your environment and are well supported. Let’s begin by exploring the relevant standards bodies.

Relevant Standards Bodies

Over time, the dynamics of the following standards bodies might change, with equal potential for mergers or splits and new organizations being formed. Table 5.1 details the roles and responsibilities of each organization according to its own definitions as well as the key standards they “own” or “develop” as they relate to Identity Management.

A majority of the organizations listed here maintain some relationship to the concept of Web services. Therefore, following this standards organization review, we will discuss the key Web services model as it applies to Identity Management, then review the details of the key Identity Management standards that were referenced.

Standards Body	Role and Responsibilities
The Organization for the Advancement of Structured Information Standards (OASIS) at http://www.oasis-open.org/	OASIS is a private worldwide organization focused primarily on XML-based standards. A non-profit organization that has a large membership and has driven a number of popular and essential standards, including: Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), Directory Services Markup Language (DSML), and Service Provisioning Markup Language (SPML).
Web Services Interoperability (WS-I) at http://www.ws-i.org/	WS-I states that it is “an open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages.” The key standard managed by WS-I is the Simple Object Access Protocol (SOAP).
The World Wide Web Consortium (W3C) at http://www.w3.org/	W3C is responsible for the Web Services Description Language (WSDL) specification.
Internet Engineering Task Force (IETF) at http://www.ietf.org/	IETF is a loose affiliate of individuals and organizations aimed at defining, maintaining, and evolving standards to support the Internet. The IETF is not a traditional standards organization, although many specifications produced become standards. Of particular interest to identity management-related activities is the Lightweight Directory Access Protocol (LDAP) standard.
The Open Group at http://www.opengroup.org/	The Open Group sponsors several sub-groups for identity management-related activities. Beyond the messaging and the mobile management forums are those relevant to identity management: the Directory Interoperability Forum (DIF) and the Security Forum (SF).

National Institute of Standards and Technology (NIST) at http://csrc.nist.gov/	NIST is responsible for a wide variety of activities; specifically related to identity management are the Cryptographic Standards and Applications and Security Research/Emerging Technologies - Authorization Management and Advanced Access Control Models (AM&AACM). The NIST RBAC model is recognized as being one of the few standards initiatives of its type. A related standard around biometrics known as the Common Biometric Exchange File Format (CBEFF) is managed by the NIST Information Technology Laboratory (ITL) in conjunction primarily with the US National Security Agency (NSA) amongst other bodies. Derived and incorporating several biometric standards efforts.
International Standards Organization (ISO) at http://www.iso.ch/ and ITU Telecommunication Standardization Sector (ITU-T) at http://www.itu.int/ITU-T/	ISO is responsible for many standards world-wide as it is a standards network for 145 countries. The technical work of ISO is highly decentralized and based in more than 2800 technical committees, subcommittees, and working groups that have already published more than 12,000 standards. In relation to identity management, ISO with the ITU-T is well known for the X.xxx-based standards. Of particular interest to the identity management market are the X.500 through X.586 directory-related standards. Most PKI implementations rely on the X.509 standard.
The BioAPI Consortium at http://www.bioapi.org/	The BioAPI Consortium was formed in 1998. The most prevalent biometric standard outside governments is the BioAPI, which defines an open API for developers to integrate with biometric mechanisms in a standard way.

Table 5.1: Standards bodies relevant to Identity Management.

Directory Services

Considered the core of most Identity Management solutions, directory services enable many of the previously listed standards. The key standards are X.500 and related standards, LDAP, and DSML. Although X.500 remains popular in large global organizations, government, and educational environments, LDAP remains the core for most Identity Management solutions that rely on directory services. There are many places to review the X.500 Directory, X.509 Public Key Infrastructure (PKI), and LDAP standards, but fewer resources available regarding DSML.

DSML

Originally defined in 1999, DSML v1 defined an XML-based document type for publishing directory schemas and exchanging directory data over any transport protocol. Unfortunately, DSML v1 did not find much success as it competed with LDAP Data Interchange Format (LDIF), a widely understood and widely adopted protocol. In addition, DSML v1 didn't offer any advances in functionality or suitability. However, accessing LDAP directories through firewalls and within secure environments has proved a limiting factor in directory deployments.

Despite the lukewarm adoption of DSML v1, version 2 was developed by OASIS and approved as a standard in May 2002. DSML v2 addresses most of the deficiencies of the first version and maps LDAP v3 operations to SOAP schemas. As a result, there is now explicit support for transports such as HyperText Transfer Protocol (HTTP), which for the time being allows for directories to be more easily accessed through secure firewalls.

However, even now, version 2 has seen little market momentum. Because of the lack of security inherent in the protocol, vendors have been slow to adopt this new standard. Therefore, in spite of the DSML and XML relationship, DSML appears stalled while other Identity Management–related standards have gained popularity.

Web Services

Web services are a business service provided by a software component and accessed through standard protocols and over public and/or private networks. The goal of Web services is to provide for loosely coupled communication between heterogeneous platforms, applications, and systems as well as allow for the dynamic assembly of new applications and services. For example, Web services help to enable the following types of data and process integration scenarios:

- Stock quotes and stock charting
- Credit card verification and payment processing
- Integrated travel planning
- Request for Quote (RFQ), bid process, auctions
- Moving data for a federated Identity Management solution

Table 5.2 provides a guide to the core Web services standards that relate to Identity Management from a protocol standpoint.

Area	Standard
Universal Data Format (UDF)	XML
Transport	HTTP(S)
Network	TCP/IP
Service invocation	SOAP
Service descriptions	Web Services Description Language (WSDL)
Publish and find services	Universal Description, Discovery and Integration (UDDI)
Authentication and authorization	SAML
Access controls	XACML
Provisioning	SPML
Web Services Security	WS-Security (WSS)

Table 5.2: Identity Management-related Web services standards.

Table 5.2 shows the basic Identity Management–related Web services standards, although there are many other supporting standards and components. The core of Web services functionality is based on the model that Figure 5.1 shows.

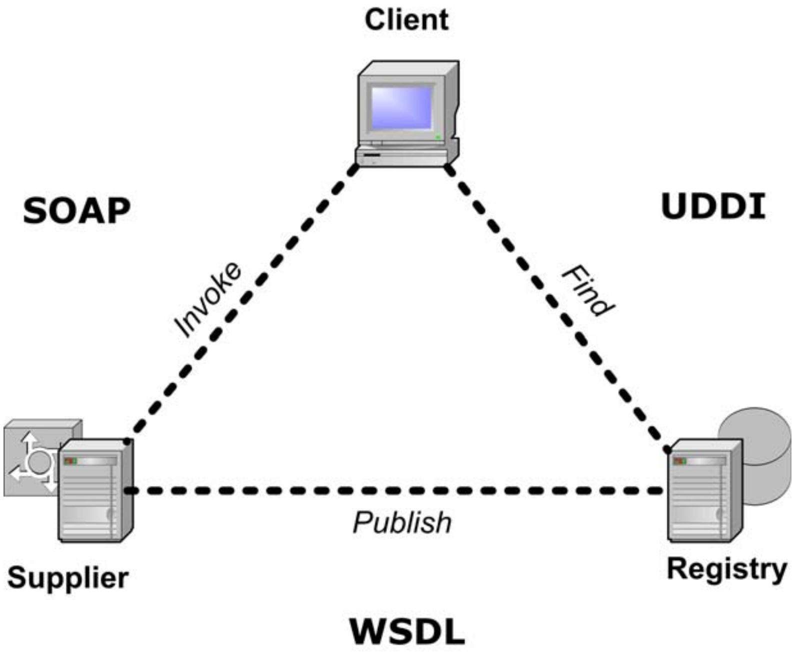

Figure 5.1: Basic Web Services model using SOAP, WSDL, and UDDI.

At the base, SOAP, WSDL, and UDDI make up the foundation of Web services architectures. Let’s summarize these standards before we discuss the rest of the Identity Management standards.

SOAP

SOAP is a standard for transporting XML-based messages. Using TCP/IP and HTML as the basis, SOAP is a representation for remote procedure calls (RPCs—call and response). SOAP is a standard originally defined by Microsoft, and now maintained by the W3C. The SOAP specification defines a method for encoding data into an XML format and focuses on an envelope with headers and a body with message content. SOAP can be used with different transports, including HTTP(S). Figure 5.2 illustrates the basic SOAP document structure.

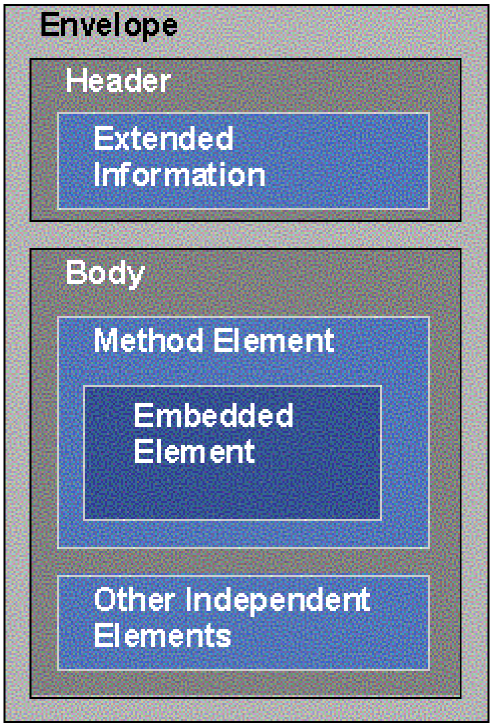

Figure 5.2: Basic SOAP document structure.

There are numerous SOAP extensions, some of which do not deal with Identity Management directly:

- XML Signature and XML Encryption—Draft proposal for public key–based signing and encryption.
- WSS—Defines how to attach signature and encryption headers to SOAP messages to provide quality of protection through message integrity, message confidentiality, and single message authentication. WSS also describes how to attach security tokens, including binary security tokens, allowing for interoperability with common existing security solutions.
- WS-Attachments defines a method for dealing with non-XML content in SOAP. Direct Internet Message Encapsulation (DIME) provides a mechanism for packaging pieces of data together. WS-Attachments then defines how DIME can be used to include attachments with SOAP messages and how to refer to those attachments within the realm of the DIME package.

- WS-Policy—Will describe the capabilities and constraints of the security (and other business) policies on intermediaries and end points (for example, required security tokens, supported encryption algorithms, privacy rules).
- WS-Trust—Will describe a framework for trust models that enables Web services to securely interoperate.
- WS-Privacy—Will describe a model for how Web services and requesters state privacy preferences and organizational privacy practice statements.
- WS-Coordination—Describes an extensible framework for providing protocols that coordinate the actions of distributed applications. Such coordination protocols are used to support several applications, including those that need to reach consistent agreement on the outcome of distributed transactions.
- WS-Routing—A simple, stateless, SOAP-based protocol for routing SOAP messages in an asynchronous manner over a variety of transports such as Transmission Control Protocol (TCP), UDP, and HTTP. With WS-Routing, the entire message path for a SOAP message (as well as its return path) can be described directly within the SOAP envelope. It supports one-way messaging, two-way messaging (such as request/response and peer-to-peer conversations), and long-running dialogs.

There are numerous other extensions being defined on top of SOAP, but this list should provide some clarity to the flexibility of SOAP as a basic solution for interoperability.

WSDL

WSDL descriptions express the programming interface and location of a service. Publication of a service is really any action that makes the WSDL document available to a potential requester. For example, emailing a WSDL (or a URL pointer to a WSDL) to a developer is publishing. So is advertising a WSDL in a UDDI registry for many developers. Figure 5.3 shows the basic WSDL document structure.

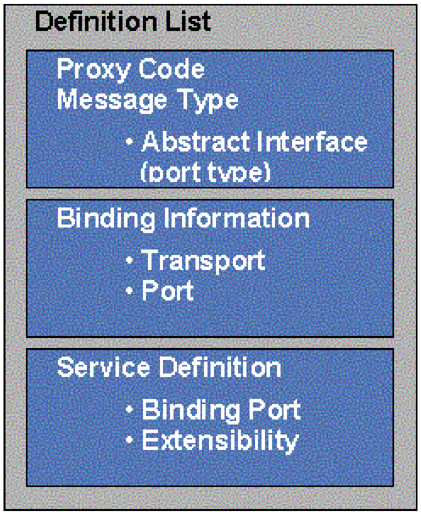

Figure 5.3: The basic WSDL document structure.

Likewise, discovery of a service is any action that gives the service requester access to WSDL for a service. The action might be as simple as accessing a file or URL containing the WSDL or as complex as querying a UDDI registry and using WSDL file(s) to select one of many potential services. Note the lack of specific security or validation around these activities, however. Listing 5.1 shows a simplified sample of a WSDL document.

```
<message name="getUserDataRequest">
       <part name="term" type="xs:string"/>
</message>

<message name="getUserDataResponse">
   <part name="value" type="xs:string"/>
</message>

<portType name=“UserData">
  <operation name="getUserData">
      <input message=" getUserDataRequest"/>
      <output message=" getUserDataResponse"/>
  </operation>
</portType>

<binding type=“UserData" name="b1">
<soap:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation>
    <soap:operation
     soapAction="http://example.com/getUserData"/>
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
  </operation>
</binding>
```

Listing 5.1: A simplified WSDL document sample.

UDDI

UDDI registry provides a standard way to publish and find information about Web services:

- Find services by searching or by using a unique identifier
- Publish and find services using browser-based and SOAP-based interfaces

UDDI registries contain information about businesses, services, and service bindings as well as additional metadata for categorization purposes (Figure 5.4 shows high-level UDDI interactions). A Web service listing is created using WSDL and then sent to a UDDI registry. UDDI registries organize this information in a manner similar to most directory and phone book concepts (using "colored pages" as the basis). The UDDI business registry has the following three components:

- White pages—Business information including business name, address, and contact information
- Yellow pages—Service categorization (that is, categories based on standard taxonomies)
- Green pages—Technical information (that is, technical specifications and references such as interfaces and URL locations); when requesting a service, you use WSDL to electronically interact with the Green Pages section of that service's listing

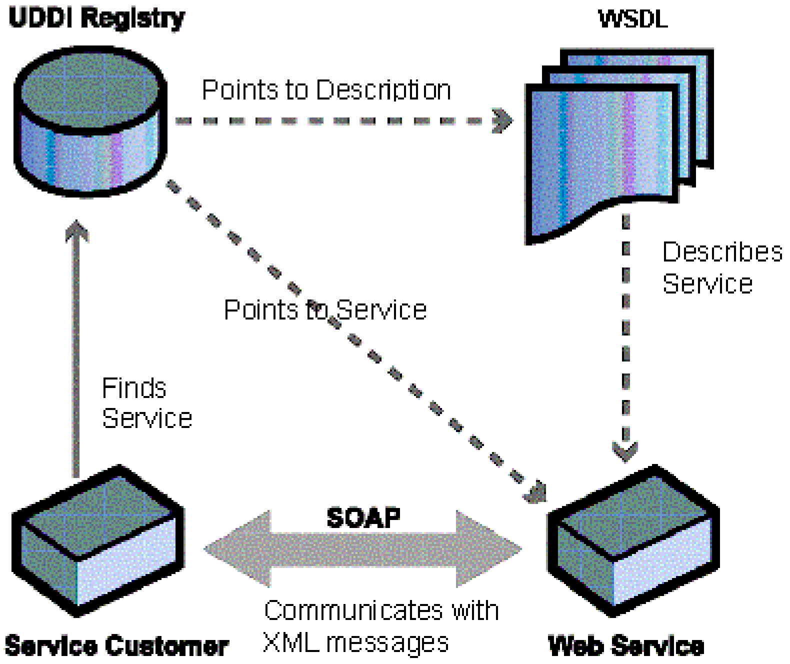

Figure 5.4: High-level UDDI interactions.

UDDI was originally developed by IBM, Microsoft, and Ariba, and is now managed by OASIS. With the stewardship for the standard having been moved to OASIS, work is now progressing on the next release.

📖 You can find information about UDDI versions 1, 2 and 3; supporting WSDL service interface descriptions; and tModel overview documents at http://uddi.org/specification.html.

tModel

Although the interface descriptions are important when looking for a service, perhaps more important is the concept of a tModel. A tModel is the technical fingerprint used to describe these interfaces. tModels provide a binding template, which allows you to determine whether you are compatible with a given service based on interface, behavior, or some other concept.

Free, public, interconnected UDDI servers are deployed today by Microsoft, IBM, SAP, and NTT. In addition, there are test registries you can use to develop and test deployments against. Companies such as Novell, Sun Microsystems, and Computer Associates are working on UDDI support in their directory products, and BEA WebLogic 7.0 includes an LDAP-enabled UDDI server that will allow for private or intra-organizational registries, supporting the goals of code reuse as well as full service access within an organization.

📖 For information about the LDAP schema for UDDI, check out the Internet draft on the IETF Web site at http://www.ietf.org.

Security

In the area of security, there are a couple of Identity Management–related solutions. In the following sections, we'll explore SAML and WSS.

SAML

SAML delivers an XML-based authentication solution for Web services. SAML is designed to support the exchange of authentication and authorization information between disparate systems from Web access management to broader security solutions, leveraging the Web services standards that we discussed earlier (such as XML and SOAP). The goal is to allow transactions to be securely distributed across multiple organizations and Web services, while mitigating the complexities of differing authentication and authorization schemes.

In some cases, such solutions will have significant impact because the simple act of authentication and authorization is quite arduous; in other cases, authentication and authorization is only a small part of the problem. That is not to say that solving this problem is not important, but that authentication is not always the only problem being faced. Consider a company that partners with many third-party organizations and providers to offer a consolidated store-front for the purchasing of many different items and services. To initiate this arrangement, there is a significant amount of work to integrate the sign-on and back-end shopping processes. Being able to move customers from one site to another without requiring that they log on to every one of those sites is critical to the seamless shopping experience, but this ability assumes that all the work takes place at the first logged onto site. It is the back-office coordination of deliveries, packaging, and returns that must be considered in addition to authentication and authorization. Thus, the goal of SAML (and the Liberty Alliance Project) is to allow for easier integration of systems, enabling organizations to quickly develop basic but strategic alliances.

SAML is comprised of three parts:

- Assertions—There are three assertions: authentication, attribute, and authorization
    - Authentication assertion validates a user's identity
    - Attribute assertion contains specific information about a user
    - Authorization assertion identifies what the user is authorized to do
- Protocols define how SAML asks for and receives assertions
- Binding defines how SAML message exchanges are mapped to SOAP exchanges; SAML can utilize multiple protocols including HTTP, Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and SOAP.

However, SAML is not a provisioning solution. There is an implicit assumption in the protocol that the correct accounts have been registered (that is, the identities have been established for all parties—source and destination) or that the initiation of SAML will call into play some dynamic registration. This then presupposes that Identity Management provisioning is in play. As such, there is also work on provisioning standards, the most prominent of which is SPML, which we will discuss shortly.

For reference, many Identity Management companies currently support SAML, including:

- Sun Microsystems
- Baltimore
- Oblix
- OpenNetwork
- RSA Security
- Crosslogix
- OverXeer
- ePeople
- Sigaba
- Entegrity

Many others have announced support and will likely introduce it to their products in 2003.

OpenSAML is a set of open-source libraries in Java and C++ that you can use to build, transport, and parse SAML messages. OpenSAML is able to transform the individual information fields that make up a SAML message, build the correct XML representation, and unpack and process the XML before handing it off to a recipient. OpenSAML fully supports the SAML browser/POST profile for Web sign-on, and supports the SOAP binding for exchange of attribute queries and attribute assertions. It does not currently support the browser/artifact profile or other SAML messages involving authorization decisions. You can download the OpenSAML code at http://www.opensaml.org/.

Another resource is the SourceID Single Sign-On Toolkit. Although it doesn't directly offer identity storage, retrieval, authentication, or authorization logic, it provides well-documented plug-in points with which the tool kit user can write short Java classes that bridge existing systems to the SourceID SSO kernel. You can download the toolkit at http://www.sourceid.org/.

WSS

WSS, sometimes referred to as the Web Services Security Language, specifies enhancements to the SOAP protocol and is intended to enhance message confidentiality and integrity through the definition of how and where to place security information in a SOAP message envelope. For example, SAML definitions could be incorporated into the WSS model, and the standard specifically calls out PKI, Kerberos, and Secure Sockets Layer (SSL).

Initiated by IBM, Microsoft, and VeriSign, WSS is now managed by the WS-I. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination, and WS-Transaction.

Federated Identity and Standards

We examined the concept of federated identity in previous chapters. The rise of new distributed computing models has driven the adoption of federated identity and Web services solutions. This rise of the Internet has forced organizations to play in the wider arena of interoperability across organizations in order to optimize their value chains. This cross-organizational push has forced the adoption of proprietary solutions over time; however, the concept of federated identity allows for a standards-based solution to be developed that allows individuals or systems to better interoperate securely across organizational boundaries currently protected by security systems, primarily firewalls and virtual private networks (VPNs).

Because interoperability has historically been perceived and addressed as a data-level issue, the consideration of how access is gained and who or what has access has almost always been hard coded (that is, developers or vendors have predefined access control within the application by, for example, providing only administrator, manager, and user definitions). To create fluid and efficient interoperability requires that the security or identity components be automated too. Thus, the need to continue to build and manage internal processes around Identity Management are just as, if not more, critical than solving the federated identity problem. The bigger issue remains around policies, repudiation, and related aspects. Although PKI has driven many of these discussions already, the solutions available today do little to address privacy policies and trading-partner agreements that are essential to creating trust relationships. The difference is that with the experience gained from the PKI initiatives, new solutions and standards are making trust relationships easier to establish.

On the standards front, there are a number of efforts initiated to support the requirements of federated identity. Because these initiatives are moving fast, I'll briefly discuss them, then quickly move on to how you can determine which is best for you.

The Liberty Alliance Project

As introduced in Chapter 1, the Liberty Alliance Project (http://www.projectliberty.org/) "is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way."

Although the Liberty Alliance Project intends to solve multiple issues around authentication, authorization, and the related policy issues, the first release addresses the following requirements:

- Opt-in account linking—Enables a choice to link accounts across disparate organizations regardless of business type
- Simplified sign-on for linked accounts—Provides the ability to authenticate using a single account and navigate to other sites without authenticating again, utilizing linked accounts as required
- Authentication context—Enables organizations to designate authorization levels for specific customers, defining what the customer can see and do at a site
- Global log out—Provides the capability for customers to log out of all linked sites through logging out of the initial logon site
- Liberty Alliance Project client feature—Provides a client component for fixed and wireless devices that facilitates the use of Liberty version 1.0

> 🕮 Sun Microsystems has released an "Interoperability Prototype for Liberty" that you can download from http://wwws.sun.com/software/sunone/identity/ipl/index.html.

Microsoft Passport

Microsoft Passport, now know as the .NET Passport, was introduced in 1999 and, as noted by Microsoft, "is a suite of Web-based services that help make using the Internet and purchasing online easier and faster." .NET Passport is delivered as part of the .NET Services, which is a broad swath of services designed to provide the building blocks for the efficient development of user-centric applications. As the Microsoft Web site notes ".NET Passport provides users with single sign-in (SSI) and fast purchasing capability at a growing number of participating sites, reducing the amount of information users must remember or retype."

Passport is delivered as a Web service, allowing developers to use the Microsoft managed authentication service instead of implementing their own. This factor is an important consideration in that while you might maintain local identity information for any reason, some subset of that identity data is held outside your control.

The areas most concerning both supporters and detractors are around liability, privacy, ownership, and regulation of the identity data. Microsoft has faced the European Union on these specific issues as related to the Passport design, and was forced to make changes. Although this situation has not significantly affected partners using Passport at this time, the issue of being able to meet your own organizations' current and future compliance requirements bears careful consideration against any potential upside gained by using a widely available solution such as Passport. Although you cannot predict every future possibility, consider the introduction of HIPAA, which we've discussed in previous chapters.

As we've explored, HIPAA has driven many organizations to change the way in which they deal with privacy issues, often resulting in systems being removed or radically changed to support the mandatory requirements around patient data management and access. If you no longer own some of the data, this exercise becomes even more excessive. However, if you partner with Microsoft or implement solutions using .NET and Internet Information Server (IIS), you should consider integrating security access with Passport as well as maintaining your own data.

> 🕮 Microsoft has released an SDK that allows you to integrate Passport into your own applications. The .NET Passport SDK is available as part of the developer resources on Microsoft's Web site (http://www.microsoft.com).

Liberty, Passport, Both, or Something Else?

One of the questions that will likely arise is whether to use the Liberty Alliance Project solutions, Passport, both, or something else? At a base level, these "standards" attempt to solve the identity requirement for authorization and to differing degrees, authorization. The goal of all the solutions is to enable federation of Identity Management for organizations, from internally integrated solutions to cross-organizational resource access, by minimizing the need to exchange sensitive data, but still securely share relevant data.

In theory, these solutions should allow for a single identity to be used for sign-on across all relevant applications, services, and resources. The logical end is seamless interoperability; however, as mentioned earlier, there is still a potential need to support registration across the disparate applications, services, and resources.

As noted, both the Liberty Alliance Project solutions and Passport are well suited to support consumer solutions; however, these solutions might be more than an organization requires. The Liberty Alliance Project has based a lot of their initial solution on the SAML specification, so while there are additional specifications by the Liberty Alliance Project, perhaps SAML is all that is needed for your situation.

For example, OpenSAML offers a basic SAML implementation through open source licensing. Alternatively, the Shibboleth Project (http://shibboleth.internet2.edu/), which is sponsored by Internet2, uses OpenSAML to advance its solution of "developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of Web resources subject to access controls. In addition, Shibboleth is developing a policy framework that will allow inter-operation within the higher education community."

The Shibboleth project's goals are very similar to the goals of the Liberty Alliance Project, and thus, require consideration especially if you do not plan to extend into commercial applications immediately. The common use of SAML provides some level of mitigation for interoperability in the future.

Although developing your own solution is one option, it is likely that vendors will provide comprehensive and interoperable support for the various standards around Identity Management, in particular those related to security. For example, the first company to demonstrate an interoperable solution using both the Liberty Alliance Project's solution and SAML was OpenNetwork.

OpenNetwork’s solution works as follows:

1. As Company A’s user signs into a DirectorySmart-protected Web service with their Passport credentials, they might want to access a second Web service hosted by a trusted business partner using SAML.
2. As the user attempts to access this SAML-based service, DirectorySmart passes on the required authentication and authorization information in SAML to the trusted partner, Company B.
3. The partner then uses this information to determine authentication and authorization to Web services, eliminating the need for an additional logon for the user.
4. Company A is then able to deliver a seamless user Web experience by joining Passport and SAML through the DirectorySmart interoperability bridge.

This solution is a good example of the need for and implementation of interoperability.

Trust

We have touched on the issue of trust several times. In the case of Passport, trust must be placed in Microsoft not only to manage and protect the data, but also to maintain the service availability. In the case of the Liberty Alliance Project, there is less of this concern, but the authentication service must still be available to work or there must be processes in place to deal with a failure of any of these areas. Because these considerations must often be enforced outside the automatic confines of system interoperability, they require out of band or manual process, legally binding companies to certain support levels and remediation processes.

At this point, organizations such as PingID become valuable. Aiming to provide a visa-like network of trust through standard and legal agreements, PingID is made up of members who want to trust for Identity Management purposes. Organizations such as the Liberty Alliance Project and Microsoft offer some protections, whereas SAML, of course, as a standard, provides none of this support. Furthermore, the level to which the Liberty Alliance Project solution and Passport offer such protections is not as great as PingID.

The example given by PingID is of Automated Teller Machine (ATM) agreements between banks. These machines would not allow non-bank customers to withdraw cash without some form of legal agreement and standards that all the banks can rely on and fall back on in the event of some failure or challenge. This agreement defines the processes, bounds, and limits for transactions, as well as the agreed upon processes for remediation.

Visa International operates their member network in a similar way. A member organization that wants to allow visa card-holders to make purchases or payments at their establishment agrees to the terms and conditions of the network, and gains the benefits associated with that network from access and validation to the similar remediation policies. The danger is that many of these types of affiliations arise, creating too many standards.

Workflow

There are many workflow solutions available, some of which can help you in your Identity Management implementation. The question is, do workflow standards actually help you? When looking at internal development or third-party solutions, consider that workflow is required to ensure the right processes are followed; however, it is very rare for systems to interoperate at the workflow level. As such, the need for a solution to support a workflow standard is less important than being able to expose the workflows in a way in which you can easily manage and monitor them.

If you want to understand the level of interoperability available, you could consider reviewing the Workflow Management Coalition (WfMC—http://www.wfmc.org/) who "promote and develop the use of workflow through the establishment of standards for software terminology, interoperability, and connectivity between workflow products." Alternatively, in line with the relentless drive toward XML, you might be looking for BPML or Business Process Execution Language (BPEL). For more information about BPML, see http://www.bpmi.org/bpml.esp.

BPEL

Published in August 2002, BPEL is an update and replacement for IBM's Web Services Flow Language (WSFL) and Microsoft's XLANG specification. BPEL is a specification for a programming language that enables a task to be accomplished using a combination of Web services, possibly involving more than one company. As noted at http://xml.coverpages.org/bpel4ws.html "BPEL allows companies to describe business processes that include multiple Web services and standardize message exchange internally and between partners."

For example, a BPEL program could be used to describe a business protocol between travel agents and tour operators such that each can automate the process by which they will exchange order and confirmation information, and more importantly, how to deal with exceptions. Perhaps most important is the definition of the order in which steps are processed and if they are parallel or serial. How those things are processed at each step of the transaction is left to the Web service definitions.

BPEL is seeing uptake especially by its original developers, Microsoft, IBM, and BEA Systems. However, BPEL has not achieved widespread use.

📖 For more information about BPEL, see http://www-106.ibm.com/developerworks/webservices/library/ws-bpel/.

Provisioning

Standards in the provisioning space are minimal. There have been several efforts to provide standards-based provisioning solutions. The workflow standards provide methods to ensure that provisioning takes place in the correct order, and importantly allow for the specification of what to do if something fails. The only provisioning-specific standard worth discussing at this time is SPML.

SPML

SPML is a proposed specification through OASIS, which has been working on the development of the specification since late 2001. The development has some way to go before it reaches the level of sophistication of SAML, but the first version of SPML is due for release in mid 2003.

SPML requests are intended to facilitate the creation, modification, activation, suspension, enablement, and deletion of data on managed Provisioning Service Targets (PSTs). OASIS has been working on SPML since late 2001, and it has some way to go to reach the level of SAML; however, this version is due for 1.0 release in mid 2003.

To understand SPML, we must review the Web services model that we discussed earlier in this chapter. In that model, there is a networking layer, on top of which is an XML-based messaging layer. This layer, which is based on SOAP, makes communications possible between Web services and their clients. SPML will specify the provisioning or subscribing function of the Web services. SPML will determine the provisioning (for example, to add, create, delete, modify, or query) of provisioning service points (PSPs) and provisioning service targets (PSTs). SPML will make this determination based on a formal submittal from the Requesting Authority (RA). In certain situations, the PST might be an RA that is requesting access to a service on another PSP.

As we discussed earlier, security is one a key factor in Web services solutions. Such being the case, we can see a relationship between the protocol/API and security solutions, one of which is SPML:

- HTTP—HTTP over SSL
- SOAP—Signed requests and/or reliance on HTTPS for secure channel
- SPML—WSS

Thus, you can see that SPML is being developed to address the severe demands of today’s e-businesses, which include security management and quality of service management.

Biometric Standards

Biometrics provides automated mechanisms for identifying a person based on physiological or behavioral characteristics. We discussed this idea in Chapter 1 as "something you are." Examples of biological aspects that could be used in biometrics are:

- Deoxyribonucleic Acid (DNA)
- Fingerprints
- Facial recognition
- Handwriting analysis
- Retinal and iris scanning
- Voice recognition

The biometrics arena is growing quickly. However, this market has many considerations that need to be addressed, including the definition of biometric information and more esoteric and moral factors. Many in this market are working to address such unresolved issues.

The media often shows clever individuals that can easily fool biometric solutions (for example, by wearing a latex glove and powder or stick-on fingerprints to dupe a palm scanner or by using a recording to trick a voice-recognition solution). Thus, one of the key challenges of using biometrics is that if the definition of the biometric challenge is held in a central place and the scanner used to gain the biometric scan and feed it through the verification process remains in a fixed position, there is the possibility for impersonation due to the assumption that the actual input mechanism is foolproof. This factor will always be an issue; however, vendors of biometric solutions now have the technology to deploy the scanner (the input mechanism) with the actual biometric signature, which can minimize the ability of interception of the biometric data. For example, SafeNet offers iKey that has a fingerprint scanner built-in to the actual device. This configuration ensures that the biometric signature stays within the device and can never be intercepted.

> 📖 For more information about biometrics and the evolution of this market, check out http://www.biometrics.org/. This Web site provides a definition of biometrics as well as the current issues being addressed in this market.

BioAPI

The most prevalent biometric standard outside governments is the BioAPI, which defines an open API for developers to integrate with biometric mechanisms in a standard way. Originally approved by ANSI in February 2002, NIST and the NSA and the U.S. Biometric Consortium sponsored a unification meeting in March of 1999 in which the ANSI Human Authentication API (HA-API) working group (originally sponsored by the U. S. Department of Defense, which published the high-level biometric API in 1997) agreed to merge their activities with the BioAPI Consortium. The HA-API is a high-level API that was published in November 1997.

The BioAPI still has a ways to go to make the standard broadly interoperable, specifically in terms of support for definition of matching agreements, wherein the standard needs to define the levels of accuracy to be agreed or required between technologies using the BioAPI. The BioAPI organization plans to release a new version in 2004.

📖 Current BioAPI-compliant products are listed on the BioAPI organization's home page at http://www.bioapi.org/BioAPI_products/products.htm.

X9.84—Biometric Information Management and Security for the Financial Services Industry

The X9.84 Biometric Information Management and Security for the Financial Services Industry standard defines the security and management of biometric data, including secure transmission and storage, and security of the surrounding hardware. Essentially, X9.84 helps secure the authenticity and integrity of biometric data using digital signatures. To do so (and unlike the BioAPI at the time of this writing), X9.84 defines recommendations around false match rates for verification and identification. As the title suggests, this standard is driven by the financial services industry and is being shepherded by ANSI.

XML Common Biometric Format

Developed to consolidate and enhance interoperability through the use of Web services–based solutions, the XML Common Biometric Format (XCBF) is an initiative under the OASIS banner.

This consolidation exercise is taking the BioAPI and X9.84 specifications and providing a common XML format using a common schema. Eventually XCBF would also become a format supported by CBEFF.

The main dilemma with the BioAPI and X9.84 specifications are that they are binary constructs. This type of representation allows for minimal memory waste and is critical when dealing with resource-constrained devices such as smart cards and tokens. However, while it appears that the drive towards XML-based standards seems to be trying to replace every existing standard, using XML representations makes them easier to read and use in Web services models and sometimes easier to transport.

CBEFF

As previously noted, CBEFF was the result of consolidated work by NIST and the BioAPI consortium (see Table 5.1). The goal of the exercise was to provide a "technology-blind biometric file format that would include all modalities of biometrics and would not bias, encourage, or discourage any particular vendor or biometric technology from another. It would not attempt to translate among different biometric technologies, but would identify them and facilitate their co-existence." NIST published the "Common Biometric Exchange File Format (CBEFF)" on January 3, 2001 as NISTIR 6529.

Incorporating a method to encapsulate payloads of biometric data in a standard format, CBEFF currently "recognizes" two standards, the BioAPI and X9.84. As a result, CBEFF smoothes the interoperability issues between the two.

📖 For more information about CBEFF, check out http://www.itl.nist.gov/div895/isis/bc/cbeff/.

Smart Card Standards

Although the standards we've discussed so far cover the main Identity Management components, you can check out the Smart Card Industry Association's Web site for more information. This site contains information on related Identity Management standards, industry events, and newsletters related to smart card technology.

> 📖 For more information about smart cards and the related standards, check out http://www.smartcardalliance.org/.

Summary

Many Identity Management–related standards have existed for some time, but this area is still rapidly evolving and as such, expectations must be set around the level of real interoperability these standards will supply. Efforts by the involved forums and groups that were mentioned in this chapter as well as those of vendors will help these efforts maintain a progressively smoother level of integration.

The standards keep rolling forward, ranging from loose to tight affiliations with the requirements of Identity Management. The key is to look for those that solve your challenges and are well supported.

In Chapter 6, we will look at the organizations that can help you plan and implement your Identity Management initiative, and finally take a look at where this market is going. The rapid developments alluded to make Identity Management an interesting and dynamic space with massive potential to improve productivity and value in your organization.