IBM Framework for e-business

Security

Mike Schlosser
Senior Software Engineer
IBM, Software Group

01 November 1999

This paper reviews the business requirements for e-business security, and then discusses how these requirements are addressed by the technologies and products that comprise the security services for the IBM Framework for e-business.

The Framework for e-business architecture provides a full range of services for developing, deploying, and managing e-business applications. This paper focuses on the security services, which are a key component of the Framework's Network Infrastructure. For information on the other aspects of the architecture, refer to the IBM Framework for e-business - Architecture Overview paper.

Introduction

In today's marketplace, across all industry segments, businesses are realizing that transformation to e-business (the integration of traditional Information Technology (IT) with technology that
supports the Internet) is required to remain competitive. As enterprises around the world undergo transformations, they are increasingly leveraging Internet technologies to:

- Broaden their markets by extending their reach globally at minimal additional expense and enticing new prospects to become customers
- Enter new business areas through collaborations or expanded services made possible with Web-based interactions
- Increase employee productivity by providing easier access to corporate information and services
- Reduce costs through improved operations that integrate Web access and traditional IT systems
- Achieve operating efficiencies by reducing the number of people making routine decisions, by decreasing turnaround time, by managing reduced inventories, etc.
- Combine faster response times, continuous availability, and an ability to deal with complexity through the use of e-business applications to enable business opportunities that couldn't be made profitable in a manual implementation

Not only is the e-business transformation changing the competitive landscape, it is also changing the way companies must identify and deal with new threats and vulnerabilities to their business assets. Business procedures and IT policies need to be updated to account for these new business risks. The basic issues of security have not changed for IT groups, but the technologies available for IT groups to integrate security into e-business solutions have changed.

A wealth of data supports the point that security is the primary concern of IT managers when moving to e-business. But for e-business to take place successfully, the role that security plays must change from being solely a preventive measure to being an enabling force as well. Marlo Kosanovich, META Group's program director of Service Management Strategies and Global Network Strategies, asserts: "IT organizations can no longer view security as a burden. Rather, security must be viewed as an enabler, and security policies must become an integral part of IT as businesses continue to expose themselves and collaborate with key partners, customers, and employees." (Source: META Group press release, 15 March 1999: "META Group unveils enterprise security issues; research reveals that third-party access will drive increase in external security breaches.")

**Security requirements**

Security requirements really haven’t changed -- security has always been about risk management. Managing risk is a business decision based on a cost/benefit analysis. How much security you implement is based on your assessment of the risks involved in not providing it as compared with the benefit you achieve when you do. Your decision to apply security to your e-business application will involve a series of decisions and policies, not a binary declaration to "do" security or not. Which, and how many, of the security mechanisms described in this paper you use will depend in part on the nature of the application you're working with and the business value of the transactions you're supporting. Usually the amount of money you spend on technology to protect
your assets, coupled with the cost of managing and maintaining that technology, must be less than the values of your assets for you to stay in business.

The security requirements for e-business include:

• **Authorization.** How do you ensure that users are who they claim to be? How do different elements in the system locate and determine whether to trust one another? How do you enable new customers or business partners to access existing systems without major changes to existing security infrastructure? Whose identity should be used to determine authorization: the end user, the server, or some other entity?Â

• **Asset Protection.** Can you keep data confidential and private when it's stored and when it's traveling across relatively untrusted networks? How can you be sure that the data doesn't change while it's stored or in transit?

• **Accountability.** How can you can tell who did what when? How can you ensure, and prove, that requests and results are not altered, inadvertently or maliciously?Â

• **Administration.** Can you define the security policy? Can you ensure that policies are consistent across all elements of applications, systems, platforms, and networks?

• **Assurance.** Can you convince yourself that the system keeps its security promises? How can you ensure that the infrastructure and application resources -- including systems, networks, and data -- are not presently under attack?

• **Availability.** How do you prevent attacks on elements of the system that cause disruptions in service? How do you design for fault tolerance and ensure that applications and data are restored in the event of a serious failure? How can you keep the system up and running 7 X 24 and also make needed modifications to the application, the systems, and the enterprise network?Â

The services provided by the Framework for e-business allows you to deal effectively with these requirements.

**Framework environment**

The IBM Framework is not something you buy -- it's an approach you use to create and deploy e-business applications that are based on open systems standards, that provide support for multiplatform heterogeneous environments, that are server centric and scalable, and that use and extend existing systems. This section provides a general description of the Framework environment, or model, that you use to design and develop applications.

The Framework is based on a Web-oriented style of network computing that has evolved from traditional client/server computing, and incorporates the 3-tier application elements of presentation services, Web-centered business logic, and data storage. A key element of the Framework is integrating a company's existing business systems, applications, and data to provide a complete e-business solution.

The design principles for secure e-business are defined in the Framework's System Model. We will focus on two design principles here. We begin with the design principle that the business logic of a Web application runs on the server and not on the client. The Web application server is used
to integrate access to resources (databases, etc.), which simplifies application design, improves scalability, and provides greater security of the resources. This design principle is implemented using the Framework’s Model/View/Controller (MVC) based Web Application Programming Model.

Another design principle is structuring your e-business application to protect the Web application server by using network filters called "firewalls." A good design protects the Web server (providing presentation services) behind an outer firewall, and the remaining servers (supporting business logic) behind a second, inner firewall. This structure is known as a demilitarized zone, or DMZ.

While we will discuss the security services that are used to implement the protection in the DMZ later, the application design must first be structured to permit it to operate across a DMZ. In most cases, a Web server sits alone in the DMZ, handling requests from the Web and passing them along to the secure intranet network. The Web server contains the logic and data necessary to construct the user interface of the e-business application and the ability to convert protocols (IIOP, MQ, etc.), and little else. The Web application server and internal business systems behind the inner firewall contain all the remaining business logic and data of the application.

This separation of roles has implications for how you structure your applications and how the various parts communicate, especially when using objects. You must also consider trade-offs in your design between the performance of your application and risk. One important tradeoff to evaluate is the degree to which you will exploit the performance benefit you can attain by caching frequently requested data inside the DMZ rather than retrieving it from back-end systems each time it is requested. In any case, machines in the DMZ are known to be at higher risk and are managed accordingly.

Up to now, we have focused on the aspects of security addressed by the basic Framework computing environment and structure. The next section will define the set of security services and mechanisms that are used to enable and deliver e-business applications built on the model and structure we have defined.
Security services

The IBM Framework for e-business provides many services for developing, deploying, and managing e-business applications. This section lists the security services of the Framework.

Authorization

Only authorized users should be able to gain access to systems, applications, data and services, no matter where they are located. There are two essential and interrelated aspects to authorization—authentication and access control. Authentication is the process of proving that a user or other entity is authorized to use a particular system privilege. Access control is the act of checking whether an authenticated user's privileges permit the execution of a particular operation on a particular protected resource.

Authentication

An important step in building secure e-business applications is to define who can run the application, and then ensure that users are who they claim to be. This was not a priority during the initial stages of Internet enablement, because the information posted on the Web was there for all to see and use, while intranets were available only to employees inside the enterprise boundary. But e-business is different. You need to authenticate the consumers who buy your products or services, employees who access internal systems from remote locations via the public Internet, or business partners who are tightly integrated into your supply chain and ERP systems. Non-repudiation is also required. Non-repudiation is the ability to provide proof of the origin or delivery of data to protect the sender against a false denial by the recipient that the data has been received— or to protect the recipient against false denial by the sender that the data has been sent.

There are many types of authentication mechanisms. The extensible security architecture provided by the Framework can accommodate a range of mechanisms that match the authentication strength required for the application. These mechanisms include user ID and password, one-time passtokens, digital certificates, and biometrics. Because Public Key Infrastructures (PKIs) are emerging as one of the technologies for trusted e-business applications, it is IBM's direction to implement and increasingly rely on PKI for e-business solutions. Here's a look at the key authentication mechanisms supported by the Framework.

- **PKI** capabilities help create and manage asymmetric cryptographic keys or public/private key pairs required by applications. The following major PKI components provide the necessary capabilities to establish, maintain, and protect trusted relationships.
  - The **Certification Authority (CA)** creates and signs digital certificates, maintains a list of certificates that have been revoked before the expiration date (certificate revocation lists), makes these certificates and revocation lists available, and provides an interface so administrators can manage certificates.
  - The **Registration Authority (RA)** evaluates the credentials and relevant evidence that a person requesting a certificate is who they claim to be. The RA approves the request for
issuance of a certificate by a CA. CA and RA functions are provided by Tivoli SecureWay Public Key Infrastructure and by Lotus Domino.

- A **digital certificate** binds an entity's identification to its public key and is issued by the Certification Authority. Digital certificates, based on the X.509v3 standard, enable Internet applications and other users to verify the identity of an entity.

- **PKIX**, the X.509 standard, defines the contents of public key certificates, but certificates produced by one vendor product may not interoperate with other vendor's because X.509 does not define the formats of the certificate entries and other necessary provisions. The Framework provides support for the Public Key Infrastructure for X.509 (PKIX), a set of proposed IETF standards that is intended to resolve these interoperability issues. PKIX support is included in the Tivoli SecureWay Public Key Infrastructure.

- A **digital signature** is a block of data created by applying a cryptographic signing algorithm to some data using the signer's private key. Digital signatures may be used to authenticate the source of the message and to assure message recipients that no one has tampered with a message since the time it was sent by the signer.

- **Kerberos** is an open standard designed to provide strong authentication by using secret-key cryptography. Kerberos Version 5 is supported by the Framework to provide authentication and delegation for back-end systems including IBM and other vendor platforms in the heterogeneous enterprise network. Used primarily for secure interoperation of existing systems, Kerberos is complementary to the role played by PKI infrastructure for user authentication.

- **Single Sign On** enables the use of existing systems with minimal disruption to existing infrastructure and applications. The Framework includes single sign on technology developed by IBM that enables users to access Web resources and other back-end systems using existing Web user names. This support makes it much easier to integrate with existing applications without modifying the application's existing user database. This function is provided by the IBM Web Login Service implemented in Tivoli SecureWay Policy Director for Web-based resources and Tivoli SecureWay Global Sign-On for host-based resources and databases.

- **Directory Services**, based on the Lightweight Directory Access Protocol (LDAP), define and implement a common schema for users and groups. The directory service is the point of integration for user authentication among products within the Framework. This has a positive effect on reducing administrative costs and complexity. A user can be defined once within an enterprise, and information about that user can be accessed in a consistent manner by multiple different applications. By comparison, in today's environment, common objects must be defined and administered on a per-application basis. The directory service is provided by IBM SecureWay Directory and by Lotus Domino Directory.

### Access control

Once a user's identity has been authenticated by the supplied digital certificate or other credentials, his or her access privileges must be determined. An authenticated user does not necessarily have any permissions to access applications within an e-business domain or resources within an application. Permissions are granted by setting up access control lists (ACLs)
on a resource such as a Web page and then evaluating the kind of access requested to determine if the requester has permission. Access is then granted or denied.

Java 2 provides a number of new security features to support its role of access and integration for server-based e-business applications. First, the Java 2 permission model can allow/disallow access to resources based on the "codesource", a combination of the code signature (who signed it) and a codebase URL (where it came from). In a multiplatform distributed IT environment where Java programs can be initiated from and have access to many systems, this may not provide enough information to determine authorization. Packaged as a Java 2 standard extension, the Java Authentication and Authorization Services (JAAS) is designed to authenticate users and assign privileges. When used with the function in Java 2, a Java program can provide code-centric access control (where the Java code came from), as well as user-centric access control (who is executing the code).

e-business applications may scale to dozens or hundreds of Web servers and potentially tens of millions of end users. The administration of ACLs can be very complex if they must be configured on each Web server system. Authorization to back-end data or subsystems must be handled as well, including systems that have existing authorization mechanisms. Existing enterprise-level authorization products such as IBM's Resource Access Control Facility (RACF) must be accommodated. In addition, authorization to other key e-business resources such as objects and message queues must be incorporated.

The Tivoli Secureway Policy Director provides a centralized authorization service that is the point of integration for administering access controls for Web servers, Web applications servers such as WebSphere, firewalls, EJBs, e-business subsystems such as SAP, and end-user systems that implement IBM's Client Security Solutions. The Policy Director API, which implements The Open Group Authorization API standard, is used to manage access controls for back-end systems and third-party applications.

### Asset protection

Access control protects data when authorization rules can be set in a secure system environment capable of enforcing access control policy. When data must travel outside of a secure system environment, it needs to be protected so that the policies governing its use cannot be violated. Asset protection includes:

- Secure communications, ensuring data privacy, data integrity, and origin authentication
- Secure (often encrypted) storage of data on systems where physical security may not be in effect
- Protection of the keys that in turn are used to protect the assets

- **SSL** - The Secure Sockets Layer (SSL) protocol is part of the Framework's network infrastructure. This protocol uses encryption and authentication techniques to ensure communications between a client and a server remain private and to allow the client to identify the server and vice versa.
• **VPN** - SSL is not the only mechanism available for creating secure communications between systems. The Framework also supports Virtual Private Networks (VPN) through its implementation of IETF IPSec (RFC 2401) and related standards. VPN differs from SSL in that it creates a secure channel between two TCP/IP hosts over which multiple TCP/IP connections can be established. VPN support is provided by the IBM Secureway Boundary Server and the TCP/IP security capabilities found on IBM platforms including S/390, AS/400, and AIX as well as various client systems.

• **S/MIME** - Most e-mail client and server programs using Internet systems such as SMTP send e-mail as clear text. The Framework supports Secure Multipurpose Internet Mail Extensions (S/MIME), a specification for secure electronic messaging, to prevent the interception and or forgery of e-mail. S/MIME is provided by Lotus Notes and Domino.

• **SET** - The Secure Electronic Transaction (SET) protocol, developed jointly by Visa, MasterCard, IBM, and other technology providers, is used to protect the transfer of bankcard payment information over open networks like the Internet. SET is implemented by the IBM Payment Suite

Private keys and shared secrets, once acquired, must be protected. End-to-end security must include consideration of the security of the end user device. Private keys stored on a personal computer disk file may be stolen via access to the file system or outright theft of the device. Security can be enhanced by the use of smart cards such as the IBM SmartCard Security Kit, an integrated hardware and software product including a smart card and smart card reader. Another approach is to use a security chip embedded in end user systems like the IBM PC300PL's and IntelliStation's Client Security Solution. In addition, server-side hardware devices can provide tamper resistant key storage as well as assistance for encrypting and decrypting messages and public/private key operations, etc. that require heavy computational load. IBM provides the 4758 Cryptographic Coprocessor for multiple IBM and non-IBM server platforms and the S/390 CMOS Cryptographic Coprocessor for 390 servers.

**Accountability**

A system needs to log all attempts to access corporate resources to ensure that the system is secure. This logging can also facilitate management decisions by allowing analysis of use patterns. Many of the IBM products included in e-business solutions provide extensive logging and audit capability including IBM SecureWay Boundary Server, Lotus Domino, and IBM Payment Manager. A comprehensive, distributed logging and audit facility for Internet-based applications is a future goal of the Framework and IBM will actively participate in the appropriate standards bodies to get this functionality standardized.

**Administration**

Administration and systems management of the entire enterprise network, systems, applications and data is a traditional IT requirement and beyond the scope of this paper. The administration of e-business security products and the information it manages, on the other hand, is critical to your ability to conduct e-business in a secure fashion. The security services defined in the Framework provide centralized management of common information such as users and groups and an
An integrated service for managing permissions across a wide set of components and products. As a result of this comprehensive integration, the complexity of security administration is greatly reduced. Rather than a product by product, server by server, approach to add and delete users and modify ACLs, administration is done in one place, one time for your application and the systems involved. The security services can also work with, and be managed by enterprise system management architectures such as Tivoli Global Enterprise Manager.

A more detailed description of the administration and management services can be found in the IBM Framework for e-business Systems Management white paper.

Assurance

An e-business must provide assurance that the infrastructure and application resources, including systems, networks, and data, are protected with regard to confidentiality and integrity. This includes protecting the enterprise network and systems from various forms of attack, and also requires that the communications between the consumer or business partner and the application is secure and confidential. A solution architect can choose from this set of mechanisms based on the specific security requirements for the solution.

- **Boundary protection** is the logical and physical separation of the Internet and internal IT systems discussed in the DMZ section. It is often accomplished by using two firewalls, one on each side of the Web server or other bastion hosts inside the DMZ. Firewalls police "who" enters and leaves an enterprise network and "what" gets in and out. A complete firewall solution is provided by the IBM SecureWay Boundary Server.
- **Intrusion detection** - Where the firewall emphasizes network protection, intrusion detection services emphasize detection. With an approach that emphasizes buffer networks such as DMZs or extranets, it is essential that detection services are deployed to complement protection services. Should a DMZ or extranet be compromised, you need to detect that fact early, and take necessary actions to prevent the launching of a further attack into the private network. This technology is available in the Tivoli SecureWay Risk Manager product.
- **Virus detection** - The other intrusion threat comes in the form of viruses. Computer viruses can enter your systems in a variety of ways: via e-mail attachments, from software installs, from files brought by employees from home, etc. They can quickly proliferate from system to system, user to user and cause damage to data, applications and networks. Viruses must be identified quickly, isolated, and damage repaired. The Norton AntiVirus/IBM Solution Suite provides virus detection solutions for desktop, server, and gateway solutions.

Availability

Availability is the ability to access data and resources whenever you need them. A robust system architecture is needed to enable you to adapt to just about any circumstance. Disasters do occur, and you must be able to quickly recover. This may mean distributing critical functions and data throughout different physical locations. Not only should your systems and networks have the technical capability to ensure availability, you must have a well defined and tested plan in place to allow your e-business to continue as "normal".
e-business applications based on the Framework can take advantage of multiple fault tolerance and high availability features and functions built into IBM platforms including support for RAID Storage and high availability cluster support. In addition, there are several mechanisms provided by the software technologies and products that make up the Framework, including:

- **Load balancing** requests among HTTP, FTP or other TCP-based servers, file systems, and other resources provided by the Network Dispatcher feature of the IBM WebSphere Edge Server.
- **Replication** for Web and other files, directory systems, mail, collaboration, and workflow database systems provided by the Andrew File System feature of IBM WebSphere Edge Server, IBM Secureway Directory, and Lotus Domino respectively.
- **Backup and Restore/Recovery** for data systems including files, ERP applications, e-mail, and databases provided by the Tivoli Storage Manager products.
- **Key recovery**, a process and supporting technology for recovering keys that are lost, forgotten, stolen, or otherwise unavailable to persons who legitimately need them. This functionality is provided by the key recovery service provider plugin to the IBM KeyWorks Toolkit.

**Consulting services**

As this paper has shown, as you enter the world of e-business, you can expose critical business information and applications to anyone on the Internet. As you begin to define requirements and build your e-business solution it is important to assess your current security policies, understand your current set of security threats and vulnerabilities and inventory the technical countermeasures you’ve already put in place.

**IBM's Security and Privacy services** can help you assess, plan, design, implement, and run a secure environment for your e-business applications. IBM security consultants work with you to assess your current security strengths and vulnerabilities, to determine what assets need to be protected and how best to protect those assets. They work with you to develop a security architecture that fits your e-business needs and maps to your acceptable business risk. This security architecture will be the backplane for the e-business applications you deploy.

**Scenario**

In this section we will define a simple customer scenario that brings together the elements of a successful secure e-business solution; defining the requirements or risks, the policy and implementation to address them, the resultant solution architecture, and deployment and administration considerations. We will then define an end-to-end flow of the application concentrating on security.

A fictitious brokerage firm, Charles Smith, wishes to allow its customers to access and update their account information and use some of the firm’s financial analysis tools via the Internet. The goal of this project is to reduce the cost of customer service. While there are many design areas
at play in this scenario, we will focus on security and how it impacts the design, deployment and management of the solution.

Even before the business/risk assessment is complete the customer knows that the cost of the proposed solution must be less than the projected savings in customer service. Further, the level of security afforded the customer must be maintained or enhanced - no degradation in security to the existing enterprise network will be tolerated.

Charles Smith has identified several risks and general security requirements, defined policies to address them, and set standards to implement the polices.

- **Risk** - Information flow, including passwords and account data, over the Internet is not secure and may be stolen.
  - **Policy** - Ensure there are secure communications between the end user and Charles Smith.
  - **Standard implementation** - All network traffic between Charles Smith and their customers will be protected using SSLv3 at a minimum.

- **Risk** - Unscrupulous people may attempt to access the Charles Smith system by trying user ID and password combinations to impersonate an existing customer.
  - **Policy** - Ensure that the system can determine that users are who they say they are.
  - **Standard implementation** - Implement strong mutual authentication using PKI. Provide smart cards with certificates and smart card readers to all customers who sign up for the service and encourage their use. Provide X.509v3 certificates on a browser key ring to end users as an alternative.

- **Risk** - Hackers may try to attack and penetrate the Charles Smith network, and infect the system with a computer virus, etc.
  - **Policy** - Protect the enterprise network and, where possible, the customer end user system from intrusion and attack.
  - **Standard implementation** - Provide antivirus software for end users who sign up for the service. Install antivirus and intrusion detection software in the enterprise. Implement a DMZ between the company intranet and the public Internet.

- It follows the logical 3-tier Web application model with a thin HTML-based client.
- It uses Java as the common cross-server platform computing environment.
- It uses EJBs for distributed function, including access to the existing customer account database.

- All information about users and groups is stored in a centralized directory service, deployed in the intranet, to decrease complexity and make the application easier to administer when users are added or deleted.
- A centralized authorization service is used to make it easier to define and manage the permission policy for access to programs, data, and other resources. It is deployed in the intranet.
- A trust relationship among the systems used by the application is used rather than enrolling customer end users in(to) existing backend systems; i.e. end user principal delegation will not be used.
• The end user is required to sign on (log in) to the system once and only once. All system interaction is transparent to the end user. Credential mapping is used, where necessary, to implement single sign on.
• The system is designed to fit into the DMZ model. The application's presentation logic is deployed within the DMZ and the application's business logic is deployed within the intranet.
• Charles Smith will not issue certificates. A 3rd party Certificate Authority that implements Tivoli SecureWay Public Key Infrastructure or comparable software is used for this function.

- Define the set of Web pages and objects that Policy Director will manage
- Enroll end users / groups and server principals
- Define the permission policy for Web pages and objects
- Add the credential mappings required for single sign on support to existing systems

The firewall systems are configured on each side of the DMZ. The outer firewall (router) allows only HTTP / HTTPS protocol flows, and the inner firewall allows only IIOP, LDAP, and Policy Director protocol flows.

Now it's time to put it all together to show that the security architecture, when combined with the application architecture, results in a trusted e-business solution. This simplified end-to-end flow illustrates how the various security services and technologies work together to achieve that goal.
First, assume that the systems have logged on during startup and are in a ready state.

End-to-end flow sequence

1. Alice is a Charles Smith customer. She inserts her Smart Card in the Smart Card Reader attached to her PC and enters her PIN number to enable her system. Alice then dials into her ISP for connection to the Internet and starts her Web browser.
2. Alice clicks on the bookmark she's saved for the Charles Smith home page. The HTTP request flows through the Charles Smith outer firewall / router to the Policy Director proxy.
3. The Policy Director proxy inside the DMZ receives the HTTP request and determines that the Charles Smith home page is not protected, so the Web page is sent to Alice.
4. This home page includes a link to a protected page. By linking to this page, an SSL session is established between the browser and the Policy Director proxy. As part of SSL processing, and to identify Alice to the Policy Director proxy, the browser accesses Alice's certificate and private key from the smart card, which was activated in Step 1. (Note that in addition to certificates, user IDs and passwords and other third-party authentication mechanisms are also supported.)

5. The Policy Director proxy sends Alice's certificate to the Policy Director, to establish Alice's logon. The Policy Director proxy then uses its cached copy of the Policy Director access control list (ACL) to determine whether Alice has the permissions needed to access the protected Web page that lists customer applications.

6. The "Welcome to Your Accounts" Web page is sent to Alice. It contains links to available applications. Alice clicks on the "Account Balance" application link which sends an HTTPS request to Charles Smith.

7. The Policy Director proxy ensures that Alice is authorized to obtain her account balance. Once authorized, Alice's user credentials to WebSphere are obtained and the HTTPS request is forwarded to WebSphere, including those credentials. This credential mapping capability provides single sign-on for Web applications.

8. WebSphere issues an LDAP call to SecureWay Directory running behind the inner firewall to authenticate Alice. The LDAP API flows through the inner firewall. This establishes Alice's logon to WebSphere.

9. WebSphere evaluates if Alice is authorized to execute the servlet method. Permission is granted and the servlet executes. The servlet calls a method on an EJB in the local system. WebSphere evaluates the permission to access the EJB and permission is granted. The EJB calls a method on a remote object via an IIOP call using the identity of the server principal (trust relationship). The IIOP flows through the inner firewall.

10. The WebSphere server running behind the firewall issues a call to Policy Director to authorize access to the method. Permission is granted and the EJB executes. The EJB runs a method that contains a request to access DB2 for that object's persistent data (the account balance database).

11. WebSphere issues a call to Policy Director to map the server principle to existing credentials for DB2 using single sign on capability.

12. The EJB uses the credentials obtained from Policy Director and generates an SQL query. DB2 authenticates the credentials, authorizes access, and runs the query.

13. The results of the query are returned. The data is passed back through the systems to WebSphere running in the DMZ where the data is formatted into a Web page which is sent to Alice over the SSL session.

This flow provides one example of how IBM products and technologies will work together in the near future to build a trusted e-business application. We have also documented our test team's design and implementation of real world e-business applications. They are available on the e-business End to End Solutions Integration Reports Web site. In addition, hints and tips on many of the individual products are available at the Technical Support Technical Information Site.
Summary

The security services in the Framework for e-business provide the complete set of integrated technologies required to deliver secure e-business solutions. By effectively decreasing risk, reducing complexity, and helping to lower the cost of secure computing, IBM removes many of the barriers that prevent companies from fully exploiting e-business. By providing the products, technology, architecture, and design guidelines to address key security requirements -- authorization, asset protection, accountability, administration, assurance, and availability -- IBM can offer companies a holistic approach to creating a trusted environment enabling successful e-business transformation.
About the author

Mike Schlosser

Mike Schlosser is a Senior Software Engineer with IBM. He has a broad range of experience with cross platform software integration issues and is a frequent speaker on software architecture at industry conferences. He can be reached at schloss@us.ibm.com.

© Copyright IBM Corporation 1999
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)