RC22125 (W0107-023) July 26, 2001
Computer Science

IBM Research Report

Engendering Trust in a Collaborative E-commerce Solution

Tian Chao
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Engendering Trust in a Collaborative E-commerce Solution

Abstract

The Internet has brought widespread deployment of electronic commerce (e-commerce) and is rapidly changing the way buyer and seller supply-chains transact business over the Net. As e-Markets evolve to support multiple trading partners by forming an extended value chain (e-ValueChain), it is vital to build trust among the partners. Virtual Enterprise is one example of an e-ValueChain that enables collaborative e-commerce, allowing business in e-Markets to rapidly form dynamic coalitions, pursue market opportunities, and then dissolve. Virtual Enterprise Builder (VEB), discussed in this paper, is a collaborative e-commerce solution that supports the formation of Virtual Enterprises. Business transactions hosted by the VEB solution are often highly confidential, with the potential for legal consequences. To mitigate risks and engender trust, establishing a security framework such as the public-key infrastructure (PKI) is essential.

With its added security, a collaborative e-commerce solution enables business partners to trust one another in business transactions and share appropriate resources effectively. Thus business partners in the Virtual Enterprise can collaborate seamlessly and compete better in the marketplace. VEB builds trust by integrating digital certificates into the business registration process and securing the electronic business transactions by signing them with the digital signatures, which supports the non-repudiation of business transactions.

1. Introduction

With the open and interconnected nature of Internet, all communications via the Internet are subject to threats and attacks and therefore are inherently not secure. Any Internet communication may be impersonated, spoofed, eavesdropped, or otherwise tampered with. While the Internet has brought widespread deployment of electronic commerce, businesses are wary about the unknown risks they may face. Businesses may be hesitant to complete transactions that are high-value or share sensitive information due to security attacks by the hackers. As e-Markets, an emerging e-business paradigm, evolve to support collaborative e-commerce where multiple trading partners form an efficient and profitable extended value chain (e-ValueChain) [1], it is vital to build trust amongst the partners. A solid security and trust model is critical to the success of Virtual Enterprises formation for collaborative commerce.

Virtual Enterprise is one example of an e-ValueChain that enables collaborative e-commerce, allowing business in e-Markets to rapidly form dynamic coalitions, pursue market opportunities, and then dissolve. Virtual Enterprise Builder (VEB) is a collaborative e-commerce solution that supports the formation of Virtual Enterprises. VEB focuses on engineered-to-order parts and is targeted for the semiconductor industry. The solution is built on IBM WebSphere Business Integrator (WBI)*, a platform for assembling business-to-business solutions. Business transactions hosted by the VEB solution are often highly confidential, with the potential for legal consequences. To mitigate risks and engender trust, establishing a security framework such as the public-key infrastructure (PKI) is essential.

With its added security, a collaborative e-commerce solution enables business partners to trust one another in business transactions and share appropriate resources effectively. Thus business partners in the Virtual Enterprise can collaborate seamlessly and compete better in the marketplace. VEB builds trust by integrating digital certificates into the business registration process and securing the electronic business transactions by signing them with the digital signatures, which supports the non-repudiation of business transactions.

PKI is a technology that can satisfy certain critical security and trust requirements and, thus enabling secure electronic commerce on the Internet. PKI addresses four principal security issues in Internet communications: authentication, confidentiality, data integrity and non-repudiation [2]. Authentication ensures the identity of an entity, i.e. individual, company, or software application, etc. Confidentiality protects the privacy of sensitive information while it is transmitted or stored. Data integrity prevents communication transactions from manipulation and tampering. Non-repudiation prevents transactions from being denied or disowned after the fact. With Electronic Signatures in Global and National Commerce (e-Sign) Act taking effect in October 2000 [10], it demonstrated that that governments have recognized the need for enhanced security and passed this legislation so that electronic signatures including digital signatures become an alternative to signatures on paper and hold the same weight. Moreover, the benefit of digital signatures generated through PKI is that they can be proved using the non-repudiation services.

This paper reviews the problems encountered in e-commerce solutions and discusses the motivation for security mechanisms. The paper also identifies some of the key security requirements and explains how PKI services can meet these requirements by registering and authenticating the user and business into the Virtual Enterprise solution and securing business transactions. An integral part of registration is the public key certificate request.

The user or business participates by downloading the certificate, obtained as part of the registration process, and presenting it for authentication into the Virtual Enterprise solution. The user can then generate business transactions as authorized by the Virtual Enterprise solution. These transactions are digitally signed by using the digital certificate, which guarantees authenticity of the signer's identity as well as the data integrity of the transaction. Non-repudiation service is used to gather, maintain and verify the evidence generated by the digital signature; it also retrieves and re-verifies the evidence to resolve any disputes or repudiation as part of the business transaction. This paper introduces certain PKI-based security patterns for e-commerce solutions.

2. Collaborative e-Commerce Security Requirements

In a collaborative e-commerce environment provided by Virtual Enterprise solution, multiple companies that may not have known one another previously team up to form a virtual corporation and share resources within that corporation. Therefore, resolving security issues so that businesses can share sensitive information securely is extremely important.

Many challenges and requirements exist in establishing a secure collaborative e-commerce environment. Such security requirements include the following capabilities:

- Authenticate the identity of users
- Authorize users for resources based on user's identity and roles within the solution,
- Ensure the confidentiality and data integrity of a business transaction and the data are not tampered with during the transmission
- Prevent the transaction data from being accessed by unintended recipients,

- Audit business transactions to resolve repudiation:
  - over the contents, the date and time a transaction was submitted or delivered;
  - over whether a user actually participated in the transaction.

Therefore, the need for a solid security infrastructure such as public-key infrastructure (PKI) arises.

The value of PKI is real, especially for business-to-business transactions such as those hosted by VEB. It is not only because of the money involved but also because of the potential legal consequences. For example, a business transaction such as submission of a quotation can include drawings with intellectual properties, which are confidential and very valuable. Therefore, it is extremely important to guarantee the authenticity of the person who submits the transactions, the integrity of the content submitted, and to provide mechanisms to resolve disputes. PKI services address the authentication, confidentiality, data integrity and non-repudiation issues, thus enabling legitimate and tamper-resistant transactions that can be verified.

3. Overview of the Collaborative e-Commerce Solution with PKI

This section provides an architecture overview of the PKI-based solution for Virtual Enterprise Builder (VEB) - a solution developed to create, operate, and dissolve virtual enterprises for the automation equipment manufacturing industry.

Network Security. The network security is provided by double firewalls, which create three zones: the open Internet, the demilitarized zone (DMZ), and the trusted zone (TZ) as shown in Figure 1. The DMZ lies between the two firewalls and prevents direct access to the trusted zone where machines with classified information reside and need to be protected. All communication between the client web browser and the web proxy is handled via Secure Socket Layer (SSL) sessions, which provide data encryption and confidentiality. All traffic using Hypertext Transfer Protocol Secure (HTTPS) protocol into the VEB portal is filtered by a web proxy and authenticated using Tivoli's Policy Director^{TM}.

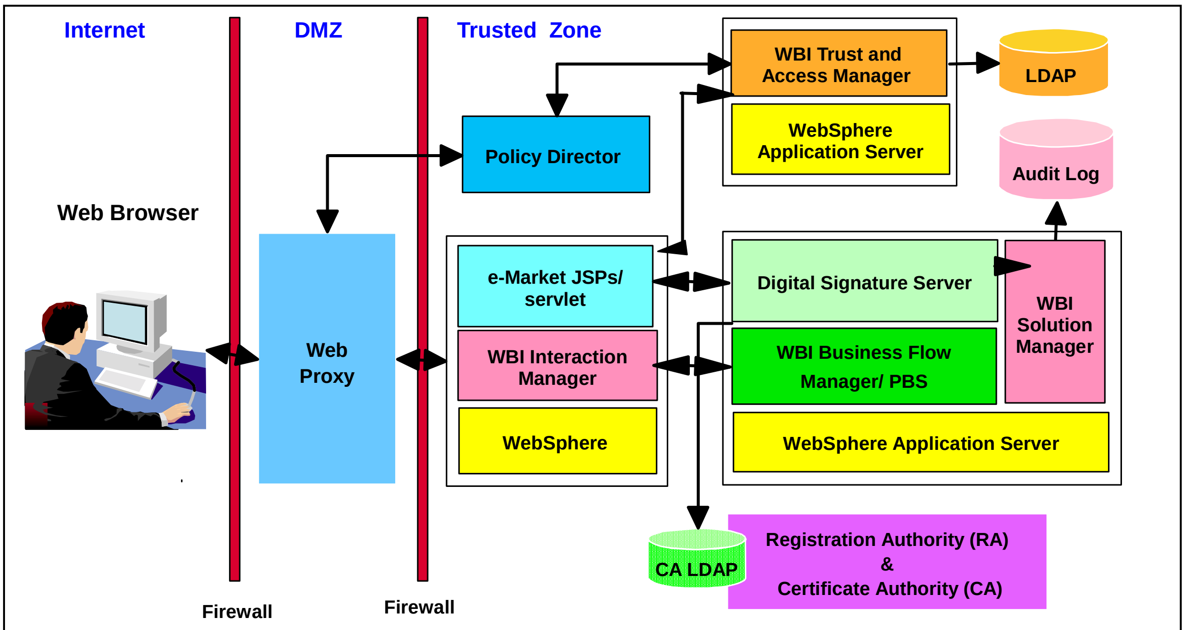


Figure 1. Architecture Overview of the Collaborative e-Commerce solution with PKI

[TM] *Trademark or registered trademark of International Business Machines Corporation and Tivoli.

Public Key Infrastructure. Several PKI-related services are enabled and integrated into VEB to allow users to secure the business transactions with digital signatures. Such services include:

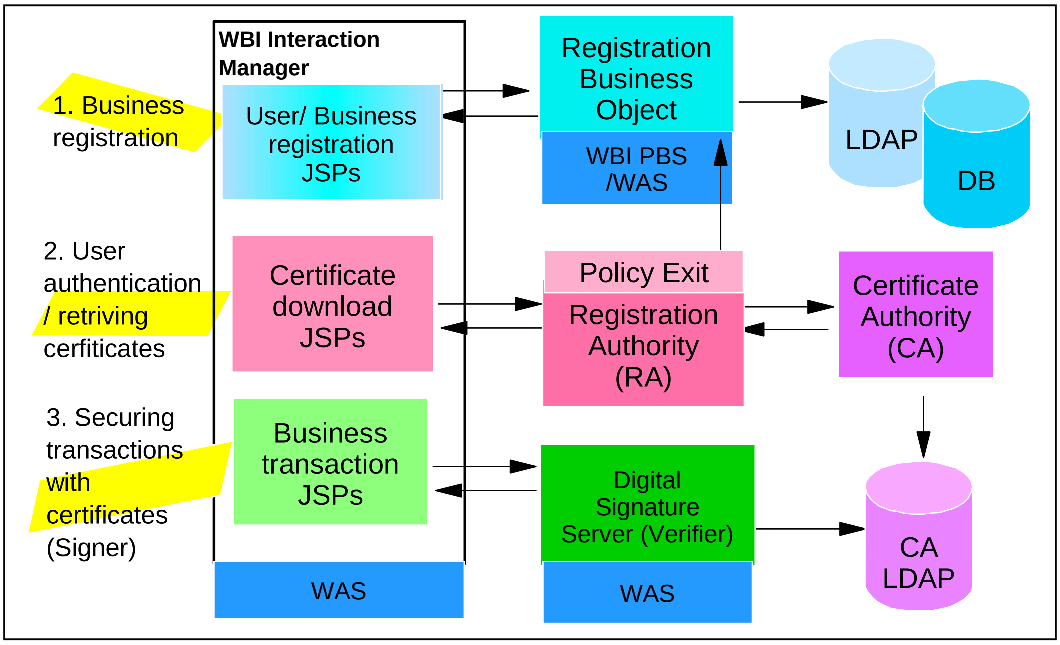
- Registration Authority (RA), which processes certificate requests,
- Certificate Authority (CA), which issues the certificates,
- Digital Signature Server, which verifies the signatures, validates certificates via Certificate Revocation Lists checking, and provides non-repudiation services

IBM WebSphere Business Integrator™ (WBI) Solution Manager, which is not part of the PKI infrastructure, provides logging and auditing services used by the Digital Signature Server.

For a detailed description of these PKI services, please see section “PKI Services Enabled for VEB”.

Transaction Security. In the VEB solution, the security framework is enabled through WBI and IBM WebSphere Application Server™, where the solution is deployed. All client sessions in Web Browsers enter into the WBI system from unsecured Internet through the VEB portal. The flow within the WBI environment depends on the business process involved. For example, in the case of the user registration process, three components from WBI are involved: 1) Interaction Manager, which renders the registration forms in the web browser, 2) Access Manager, which authenticates a user into the solution and authorizes access to solution resources based on the user’s role, and 3) Process Broker Services (PBS), which choreographs the execution of the business objects of the registration process and manages the interfaces with Enterprise Information Systems including IBM MQSeries Workflow*, databases, legacy and independent service vendor applications etc., which are not shown in Figure 1. Once successfully logged in, a user is presented with a role-specific desktop with access to all functions that the role is authorized to perform.

Business processes. Integrating PKI services into the Virtual Enterprise solution is a three-step process, i.e. three processes in the VEB solution need to be augmented to enable PKI services. Figure 2 provides an overview and the subsequent sections give further details.



WBI Interaction Manager
1. Business registration
User/ Business registration JSPs
Registration Business Object
WBI PBS /WAS
LDAP
DB
2. User authentication / retriving cerficitates
Certificate download JSPs
Policy Exit
Registration Authority (RA)
Certificate Authority (CA)
3. Securing transactions with certificates (Signer)
Business transaction JSPs
Digital Signature Server (Verifier)
CA LDAP
WAS
WAS

Figure 2 Certificate-Based Registration Process

The three processes in VEB that are augmented to enable PKI services are as follows:

1) Business Registration – The process of authenticating business entities of users and corporations in collaborative e-commerce starts with the business registration process in that it adds business entities to the e-Market portal. Business entities register via the Interaction Manager, and the registration requests are processed by the business objects hosted on the WBI Business Flow Manager. Registration data are saved in the database and LDAP.

2) User Authentication – VEB integrate the business registration process with the PKI certificate request in a one-step process. Once the user is approved for membership, he or she is also pre-approved for a certificate. The user can then download the digital certificate and later present it for authentication into VEB.

3) Securing business transactions – VEB users secure their business transactions by signing the transactions with digital certificates and the signed evidence is verified by the VEB Digital Signature Server and logged into the audit log. This process supports the non-repudiation. Please see the section of "VEB Non-repudiation Services" for further details.

3.1. Business Registration

Before using the e-Market services, business entities such as users and companies are required to register. VEB business registration is a self-enrollment process that takes place through a Web interface. The registration process provides approval or denial of the registration requests via email; it also assigns privileges, which controls the access to services.

The VEB business registration involves, at the minimum, users, companies, and the e-Market administrator, which approves the registration requests. Companies such as supplier and buyer organizations need to register with the e-Market before users in the companies can register. The contact person of a company registers the company with the e-Market, and each user can self-enroll. Some companies may have a company administrator who registers users with the e-Market.

The company registration process follows the first process as shown in Figure 2:

- The company's contact person registers by completing an enrollment form.
- The e-Market administrator verifies the registration request. If the request is approved, the approval notification is sent to the company's contact person immediately. If the request is denied, the rejection notification is also sent to the contact. The Company registries are updated upon successful registration of a company.

The user registration process follows a similar process, which includes:

- The user registers by completing an enrollment form.
- The e-Market administrator then verifies the user request. If the request is approved, the approval notification is sent to the user immediately. If the request is denied, the user is also notified. The user registries are updated upon successful registration of a user.

3.2. User Authentication – Certificate-based Registration

The VEB business registration process is certificate-based in that the registration is integrated with the certificate request process, and a user only needs to register once with the e-Market portal for both membership and the certificate. Before this process can be initiated, the following requirement must be met:

- Pre-approve the user for a digital certificate as part of the registration approval process

- Develop public-key infrastructure to process, approve, issue, and use the certificates
- Automate the certificate request approval process of the Registration Authority
- Use certificates to sign business transactions such as Request for Quotes and quotations
- Develop a digital signature solution including: the signature verification server and the PKI client

The following additional steps in the certificate-base registration are shown in Figure 2 (process 2):

- As part of the e-mail notification of registration approval, an authorization code and a URL are provided in order for the user to retrieve the pre-approved certificate.
- The user or the company’s contact person accesses the URL and presents the authorization code and the e-mail address. The Registration authority’s auto-approval process is activated to invoke e-Market business objects to verify the data.
- Once the data is verified, the certificate is formally approved and issued by the Certificate Authority; it is then downloaded to the user’s browser. The newly issued certificate will be included in the certificate repository on the next scheduled update by the Certificate Authority.

3.3. *Securing Business Transactions with Digital Certificates*

Once a user has obtained the certificate as part of the registration process, he or she can present it for authentication into the VEB. The user can then generate business transactions as authorized by the VEB. Certain transactions are required to be digitally signed by using the digital certificate, which guarantees authenticity of the signer’s identity as well as the data integrity of the transaction. The process of securing business transactions by signing Web forms using digital certificates and verifying the digital signatures is referred to as form-signing in this paper.

To order to support the form-signing process, two components of the VEB solution need to be augmented and developed for PKI: the Java Server Pages hosted on the e-Market portal, which processes the PKI requests, and the Digital Signature Server, which verifies the digital signatures. These VEB components are further integrated with the PKI services: the client software, i.e. signing applet, which signs business transactions and verifies the Server’s signed receipts, and Registration Authority and Certificate Authority, which process, approve and issue certificates.

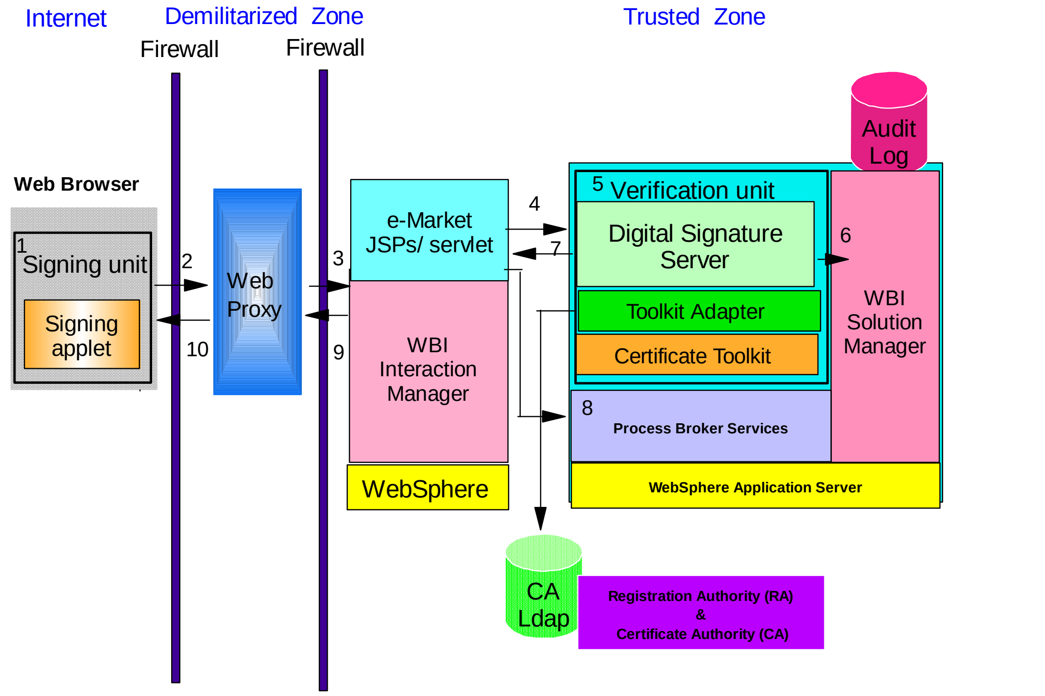


Figure 3 VEB Form-signing Architecture

Signing and Verification of Business Transactions

The process of signing and verifying the business transaction involves a user creating the transaction using a specially designed web form or Java Server Page, which downloads the form-signing applet to the user's Web browser, the signing unit. The form-signing applet is provided by the certificate toolkit. When the user submits the transaction, the form-signing applet prompts the user to select a digital certificate to sign the transaction. Using the selected digital certificate, the form-signing applet creates a digital signature of the form contents and then transmits both the digital signature and the raw data to the WBI Interaction Manager (#1 -#4).

The verification unit (#5) comprises of the Digital Signature Server, the certificate toolkit, and the toolkit adapter. Please see the section that follows for description of the toolkit requirements and the adapter usage. The Digital Signature Server, upon receiving data from the Interaction Manager, verifies the signature, logs the evidence using the WBI Solution Manager (#6), and generates a signed receipt to be sent back to the client. Any tampering of the message will cause the message to fail verification. The raw data of the transaction uncovered by the verification process is passed back to the Interaction Manager (#7) and subsequently to the business objects hosted on Process Broker Services (#8) to process the data. The signed receipt that gets sent back to the client Web browser can be either an acknowledgement consisting of the receipt number, date and time the data were delivered and the data if the signature is verified; otherwise, it is an error message when the signature does not verify or the certificates are either expired or invalid.

Digital Signature Server

The Digital Signature Server is one of the main components in the VEB form-signing architecture, which uses public-key certificates. The Digital Signature Server is a WebSphere-based server application, which provides the following PKI services:

a. Digital signature verification
b. Digital certificate verification and Certificate Revocation Lists checking
c. Non-repudiation service: 1) Generates signed receipt or error response depending on the outcome of the signature verification, 2) Logs digitally signed documents and the signed receipts in the audit log via the WBI Solution Manager

The Digital Signature Server is designed to support plug-and-play of multiple Public-key certificate toolkits via the use of the toolkit adapter [7]. An adapter is created for each certificate toolkit supported by the Digital Signature Server. This adapter alleviates the need for the Digital Signature Server to know the name of certificate toolkit used at runtime. Therefore, supporting a different certificate toolkit requires no change on the part of the Digital Signature Server. Only the configuration parameter needs to be changed to specify a new certificate toolkit to use.

The requirements for the certificate toolkit include a set of high-level server-side Java APIs and a lightweight, downloadable client-side Java solution. The high-level server-side Java APIs are important because they alleviate the need to work with low-level cryptographic functions, which can be both time-consuming and error-prone, taking time away from creating the business logic. The lightweight, downloadable client solution is important because it eliminates the requirement for pre-installation on the client machine. The requirement for Java is platform independence.

Digital Signatures for Message Origin, Integrity and Non-repudiation

A digital signature is a data item that vouches for the origin and integrity of a message [4]. It is one of the services enabled by public-key cryptography, which uses a key pair or two distinct keys, i.e. one public and one private. Although mathematically related, the corresponding private key cannot be computationally derived from the public key. The private key is always kept secret while the public key is not secret and can be freely distributed. The entity that signs the message is referred to as signer or message originator; the entity that verifies that message is referred to as verifier or recipient. Because the signing key is distinct from the verification key, the signer does not need to reveal the signing key for the verifier to verify the authenticity of the message, which is extremely valuable. This property of distinctness provides a way to implement non-repudiation in that the signer is the only person who possesses the signing key; the signer cannot later repudiate the fact that he or she has signed the message [20], thus digital signatures providing strong authentication.

RSA is a public-key algorithm invented in 1977 by Ron Rivest, Adi Shamir, and Len Adleman [11]. Figure 4 illustrates the process of how a digital signature is generated and verified using RSA digital signature scheme with hash function [19]. The signing unit first applies the hash function to the raw data to obtain a message digest (1-3). A hash function or message-digest algorithm is a one-way function that maps values from a variable-length input in possibly very large domain into a fixed-length output called message digest or digest, which is a comparatively small range. The message digest generated is then RSA-encrypted using the private key to produce the signature (4-5). The verification unit, upon receiving both the raw data and the signatures, re-computes the actual digest from the raw data (6-7) and then RSA-decrypts the signature using the public key to produce the expected digest (8-9). The verification unit compares the actual digest with the expected digest and return the verification result to the signing unit (10-11). If the actual digest and the expected digest match, the signature verifies and the recipient is assured that the originator knew the encryption key and that the message contents were not changed during transmission. This is because any tampering of the message will cause the message to fail verification.

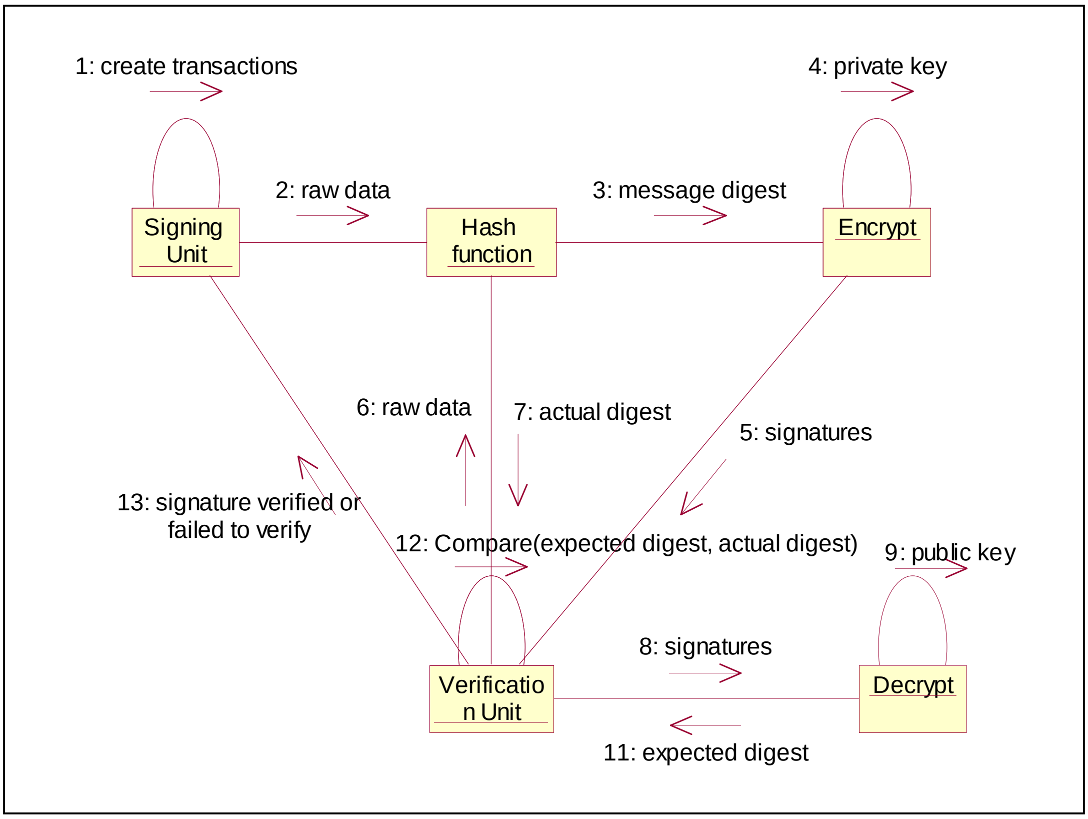


Figure 4 Digital Signature Generation and Verification Process

The reasons why a hash function is used to produce a digest of the entire message instead of signing the entire message are both speed and cost. Signing the entire message can have performance impacts where bandwidth requirements are doubled and the public-key operations are generally slower [20]. Secure Socket Layer can be used to provide confidentiality of the entire communication channel instead.

4. VEB Non-repudiation Services

One other important PKI service that the Digital Signature Server supports is non-repudiation, which is considered one of the most important and complex aspects of PKI. It collects, maintains, validates, retrieves and re-verifies the evidence to resolve disputes about whether or not an event actually took place [8]. However, unless the evidence has been previously preserved, disputes cannot be resolved. Therefore, a non-repudiation service normally is accompanied by other PKI services, thought not implemented by VEB, such as secured time-stamping service, notarization, and data archival for expired certificates and old Certificate Revocation Lists [22].

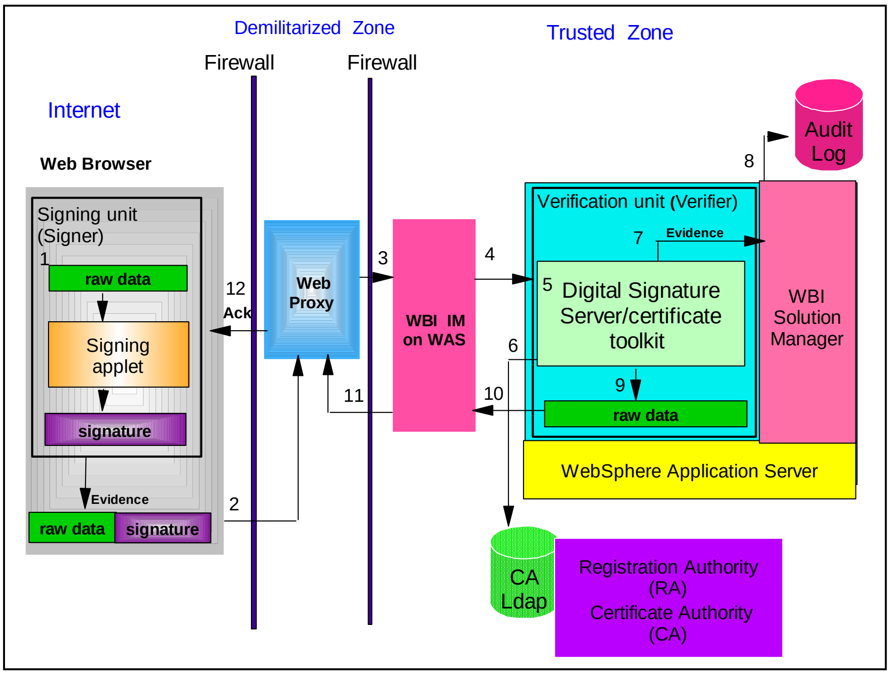


Figure 5 VEB Non-repudiation Service

Non-repudiation of origin and delivery

Non-repudiation services forestall entities involved in a transaction or communication later falsely denying having taken part in the transaction or communication. VEB uses digital signatures to implement non-repudiation services and supports two primary types of non-repudiation services: [6]:

1. *Non-repudiation of origin* prevents the message originator from later falsely denying having originated the message, disputing its contents, or origination time of the message.
2. *Non-repudiation of delivery* prevents the message recipient from later falsely denying having received the message, disputing its contents, or delivery time of the message.

To protect the message recipient, the VCMS non-repudiation of origin gathers evidence to prove: the identity of the originator of a message, content of the message, and the date and time the message was signed or the origination time.

To protect the message originator, the VCMS non-repudiation of delivery gathers evidence to verify: the Identity of the recipient of a message, content of the message, and the date and time the message was delivered.

The sections that follow and Figure 5 describe the VCMS non-repudiation service using the five distinct activities or phases as described by ISO occurring in the following order: Service request, Evidence generation, Evidence transfer, Evidence verification and Evidence retention [5].

Service request – In order to preserve evidence for non-repudiation, entities participating in a transaction or communication have to agree to use non-repudiation services and to generate relevant evidence before the transaction or communication starts. One way to obtain such an agreement may be to specify the use of the non-repudiation services in the e-Market portal policy. For non-repudiation of delivery, the sender initiates the service request; for non-repudiation of origin, the recipient initiates the service request.

Evidence Generation – To achieve non-repudiation, the entity that can potentially be a repudiator of a transaction or communication must take part in generating relevant evidence, which may be accomplished autonomously or through a Trusted Third party. The VEB form-signing architecture has achieved both the non-repudiation of origin and delivery because both the signer, or the client, and the verifier, the Digital Signature Server, have acted as the evidence generator. As shown in Figure 5 unit #1, the signer generates the signatures; and in unit #5, the Digital Signature Server generates the signed receipt.

Evidence Transfer **-** The evidence or signature generated by the client-side PKI software is then transferred via a secured channel to the Digital Signature Server to verify as shown in Figure 5 steps 2-4; the signed receipt generated by the Server is also transferred securely back to the client, steps 9-12. Alternatively, the evidence is transferred directly to a Trusted Third Party and then sent to the verifier to verify.

Evidence verification **-** Digital Signature Server verifies the evidence by 1) checking the Certificate Revocation Lists to ensure the certificates are valid, and 2) verifying the signatures to ensure it is valid and the data content is intact, as shown in Figure 5 steps 5-6.

Evidence retention **-** After having verified the evidence, the Digital Signature Server must log both the evidence from the signer and the signed receipt it generates, as shown in Figure 5 steps 7-8.

Dispute resolution **-** Even though the goal of the non-repudiation is to provide evidence to resolve disputes, but not all disputes can be settled between the parties involved. Therefore, at times, an adjudicator may have to resolve the dispute by evaluating the evidence and determine whether or not the event occurred.

In the event a dispute arises, the e-Market administrator needs to respond to the customer's challenge by retrieving the data from the audit log and have the evidence re-verified. Typically, a user submits the receipt number the server returned in the signed receipt to the administrator who will start the dispute resolution process to retrieve the evidence from the audit log, re-verify to prove that the evidence is not tampered with, and to uncover the raw data for proof after having successfully verified. The raw data uncovered can support the evidence of the following: signing 9time, delivery time, and the content of a particular signed document, i.e. RFQ, quote, or company capabilities. The raw data will be displayed on the administrator's console and also sent to the user via e-mail.

5. Implementation and Alternatives Investigated

This section describes some implementation issues, alternatives investigated and PKI services enabled for VEB.

The way VEB implements the digital signature solution is to develop the verification unit, i.e. Digital Signature Server and the toolkit adapter to integrate with both certificate toolkit and the WBI system and to work with the client solution. Thus, the digital signature solution becomes an integral part of the WBI system. The alternative approach is to install a standalone, commercially available verification server to provide the same functions the verification unit provides. A standalone server would incur high license fee and requires a dedicated environment to operate with, which increases the maintenance cost as well. The benefit of developing the digital signature solution is not only the alleviate integration issues but also the cost issues.

The table that follows provides a summary of the PKI vendors and their PKI services investigated based on the PKI services required by VEB in June 2000 [17], and this is not meant to be a comprehensive comparison of all the PKI features of the vendors [18].

Table 1 PKI Vendors and Services Investigated based on VEB's PKI Services requirements.

PKI Services required by VEB	Baltimore Technologies** [12]	Tivoli SecureWay Trust Authority* [13]	Entrust, Inc.** [14]	Shym Technology ** [15]	E-Lock Technologies [16]**
Registration Authority (RA)	X	X	X		
Certificate Authority	X	X	X		
Certificate Repository		X	X		
RA Policy Exit		X			
Server-side Java APIs	X		X		
Standalone server solution	X		X	X	X
Downloadable Java client	X				

Based on the investigation, Baltimore Technologies FormSecure toolkit was selected for the server-side APIs and lightweight client solution, and Tivoli SecureWay Trust Authority was selected for public-key certificates management. Please see the section that follows for further details.

5.1. PKI Services Enabled for VEB

Several core PKI services are established and integrated with VEB to support certificated based business registration process and form-signing to secure business transactions.

PKI, being a security infrastructure, encompasses a large number of components and services and the following are the ones that are enabled for VEB. The trust model established for VEB includes one Certification Authority, which is the root CA, and one Registration Authority; the trust model can be expanded to multiple CAs with different organizations, which can be crossed-certified. [3].

Managing the public-key certificates
The following PKI services are provided by Tivoli SecureWay Trust Authority*.

- Registration Authority
  - Process the certification requests submitted from the users

  - Support a policy exit that automates the certificate approval process where in the normal case RA desktop would manually approve or rejects the certificate requests
- Certification Authority
  - Provide certification services such as certificate issuance, certificate revocation, and publishing certificates and Certificate Revocation Lists (CRLs)
- Certificate Repository
  - A LDAP directory that stores both certificates and CRLs

Verifying the digital signatures and certificates

- Digital Signature Server
  - The server is developed for VEB to support digital signature verification, CRLs checking and non-repudiation service as detailed in the sections above. It is integrated with Baltimore Technologies FormSecure toolkit.

Enabling business transactions for PKI services

- PKI-enabled Java Server Pages
  - The business transactions documents, such as RFQ and quotations, in the form of Java Server Pages, are PKI-enabled to invoke the Java applet to perform the form-signing and signature verification functions.

The PKI client software

The client software is an integral part of a fully operational PKI because, without it, no PKI services can be made available for use.

- Downloadable Java applet client
  - A Java applet from the FormSecure toolkit that provides the ability to a) sign the data a user entered from a web page and send the signed data to the Digital Signature Server to verify, b) verify the signed receipt from the server and save it to a file, which can be verified again at any time.

Other services of the Public-Key Infrastructure that are not included but can be add through third-party services include: Key Backup and recovery, Automatic Key update, Key history management, Cross-certification, and Time stamping [9].

6. Conclusion

There is an increasing awareness and consensus that doing e-commerce without security is not an option. Businesses may be hesitant to complete transactions that are high-value or share sensitive information for fear of security attacks, ending up losing revenues and opportunities as a result. Engendering trust in businesses that need to collaborate is essential because the security framework enable them to explore new collaboration opportunities and subsequently to increase business revenues. Advanced security provides a distinct competitive advantage.

PKI enables legitimate and tamper-resistant business transactions by addressing security issues of authentication, confidentiality, data integrity and non-repudiation that challenge every e-commerce deployment. It is the authors' hope that the security patterns identified in this paper can serve as a road map for introducing PKI into other e-commerce solutions, and thereby ease some of the growing pains in realizing collaborative e-commerce solutions.

7. Acknowledgments

The author wish to thank Hamid Bacha for helping to resolve several PKI interoperability issues, uncovered while developing the Digital Signature Server, between two PKI vendors; members of his team for assisting the establishment of the Public-Key Infrastructure for Virtual Enterprise Builder (VEB), which provides a platform for this work; Nitin Nayak and the VEB team for their support and work in the registration process. Special thanks go to Kumar Bhaskaran for his support and encouragement and for reviewing this paper. Thanks also go to Jen-Yao Chung for his support.

*Trademark or registered trademark of International Business Machines Corporation and Tivoli.

**Trademark or registered trademark of Baltimore Technologies, Entrust/PKI, Shym Technology, E-Lock Technologies.

8. References and notes

1. Chae An, Kumar Bhaskaran, Nitin Nayak, Sesh Murthy, Frederick Wu, Rama Akkiraju, and Jayant Kalagnanam, “The Drive to e-Markets, E-Commerce and Supply Chains”, IBM e-Markets Whitepaper, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, (May 8, 2000).
2. PKI and the Law, Network Magazine, Jonathan Angel, Vol. 15 No.10, 48-56, (2000)
3. Sanjiev Chattopadhya, Hamid Bacha (Editor), “PKI Conceptual Architecture for VCMS”, IBM Global Services, Version 1.2, (August 4, 2000).
4. Jalal Feghhi, Jalil Feghhi and Peter Williams, Digital Certificates, Addison-Wesley, 45-48, (1999)
5. Warwick Ford, Michael S. Baum, Secure Electronic Commerce, Prentice Hall PTR, 325-330, (1997).). Ford et al uses five distinct phases to describe the Non-repudiation service while the ITU-T Recommendation X.813 (#8) describes it as four distinct phrases: evidence generation; evidence transfer, storage and retrieval; evidence verification; and dispute resolution
6. Jalal Feghhi, Jalil Feghhi, Peter Williams, 17-18.
7. Mark Grand, Patterns in Java Volume 1, A catalog of Reusable Design Patterns Illustrated with UML, John Wiley & Sons, Inc., 89-98, (1998)
8. ITU-T Recommendation X.813 (10/96) - Information technology - Open Systems Interconnection - Security frameworks in open systems: Non-repudiation framework, iii, (1996); http://www.itu.int/itudoc/itu-t/rec/x/x500up/x813.html.
9. Carlisle Adams, Steve Lloyd, Understanding Public-Key Infrastructure Concepts, Standards, and Deployment Considerations, Macmillan Technical Publishing, 33-39, (1999)
10. Electronic Signatures in Global and National Commerce (e-Sign) Act , http://commdocs.house.gov/committees/judiciary/hju62448.000/hju62448_0.htm.
11. RSA public-key algorithm, see http://www.elabhk.net/rsa/rsa.htm.
12. Baltimore Technologies, UniCERT** , http://www.baltimore.com/unicert/index.html, and FormSecure**, http://www.baltimore.com/securityapplications/formsecure/index.html
13. Tivoli SecureWay Trust Authority, see http://www.tivoli.com/products/index/secureway_public_key.
14. Entrust, Inc., see http://www.entrust.com.
15. Shym Technology, see http://www.shym.com.
16. E-Lock Technologies, see http://www.elock.com.
17. Hamid Bacha from IBM Global Services originated the investigation and provided verbal feedback. The author did follow-up investigation and summarized the findings in the current format. Both Shym Technology and E-Lock Technologies provide Web-based solutions.
18. Since June 2000 when we first did our investigation, IBM Denmark has come out with the Crypto Based Transactions (CBT) product, which provides similar functions as Baltimore's FormSecure, including the use of downloadable applets for form signing. Digital Signature Server can support CBT as a certificate toolkit by adding the support for the CBT toolkit adapter

provided that all functions needed to implement the toolkit interface are either present in CBT or can be developed.
19. Warwick Ford, Michael S. Baum, 112-114.
20. Jalal Feghhi, Jalil Feghhi, Peter Williams, 44-46.
21. Kumar Baskeran, “The e-Market Centralized User Management”, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, (November 6, 2000)
22.Carlisle Adams, Steve Lloyd, 57-59, (1999)

Other references:
1. Bruce Schneier, Secrets and Lies, Digital Security in a Networked World, John Wiley & Sons, (2000)
2. Craig Fellenstein, Ron Wood, Exploring E-commerce, Global E-business, and E-Societies, Prentice Hall PTR, (2000)
3. IBM Corporation, IBM WebSphere B2B Integrator System Overview, Version 1.1, June 2000.

Tian Chao *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (electronic mail: tian@us.ibm.com).* Ms. Chao is an Advisory Software Engineer at the Thomas J. Watson Research Center. She received a master’s degree in Computer Science from Virginia Polytechnic Institute and State University and a bachelor’s degree from National Taiwan University. Before joining the Research Division in 1999, Ms. Chao worked at the IBM TPF Systems Development Lab where she was awarded two patents. Her work at the Research Division has focused on the security framework for the collaborative e-commerce solution, Virtual Enterprise Builder. Her current work includes Web Services in a dynamic e-business environment and security issues related to the Web Services and e-commerce solutions.