

Public Key Infrastructure (PKI) System for **BankServ**

Customer Application Case Study



Introduction

Conducting business to business commerce over the internet requires that identity and trust be established between trading partners with no prior relationship. Persistent authentication, in the form of digitally signed contracts, together with certified public keys (digital certificates) provide the foundation for conducting online business.

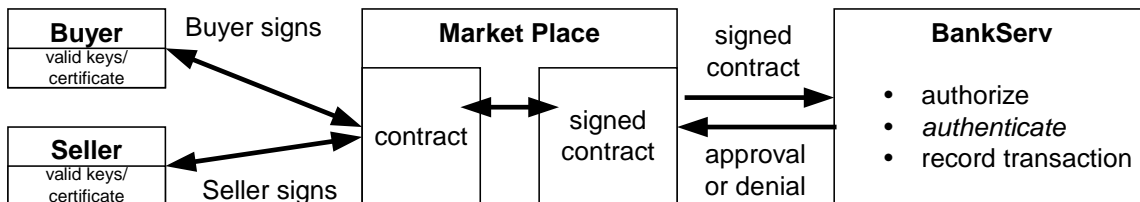
BankServ (www.bankserv.com), a leading provider of payment solutions for online businesses and for financial services companies and retailers, provides a system for the secure brokering of web-based payments. This system enables the participants to digitally sign electronic contracts, which can be authenticated at BankServ and then confidently approved or denied based on the spending levels and other entitlements of the authenticated parties. BankServ looked to Xetex to provide the authentication and digital certificate management components of this system.

Certificate Management and Authentication Requirements

BankServ required a system that could create and manage smart card and browser based public key certificates with all the necessary tools for certificate generation and management. This included traditional Certification Authority (CA) functionality as well as the ability to automate the issuance of the certificates and provide lifecycle management functions such as certificate revocation and renewal. All management functionality would be accessible through a standard web browser via a secure connection.

The system should take as input the digital signatures and contract, verify the signatures and certificate status, and return a list of the user ids of the authenticated signers. The authentication mechanism would need to be available to other Java based server side applications.

The desired transaction flow is shown in the following figure:



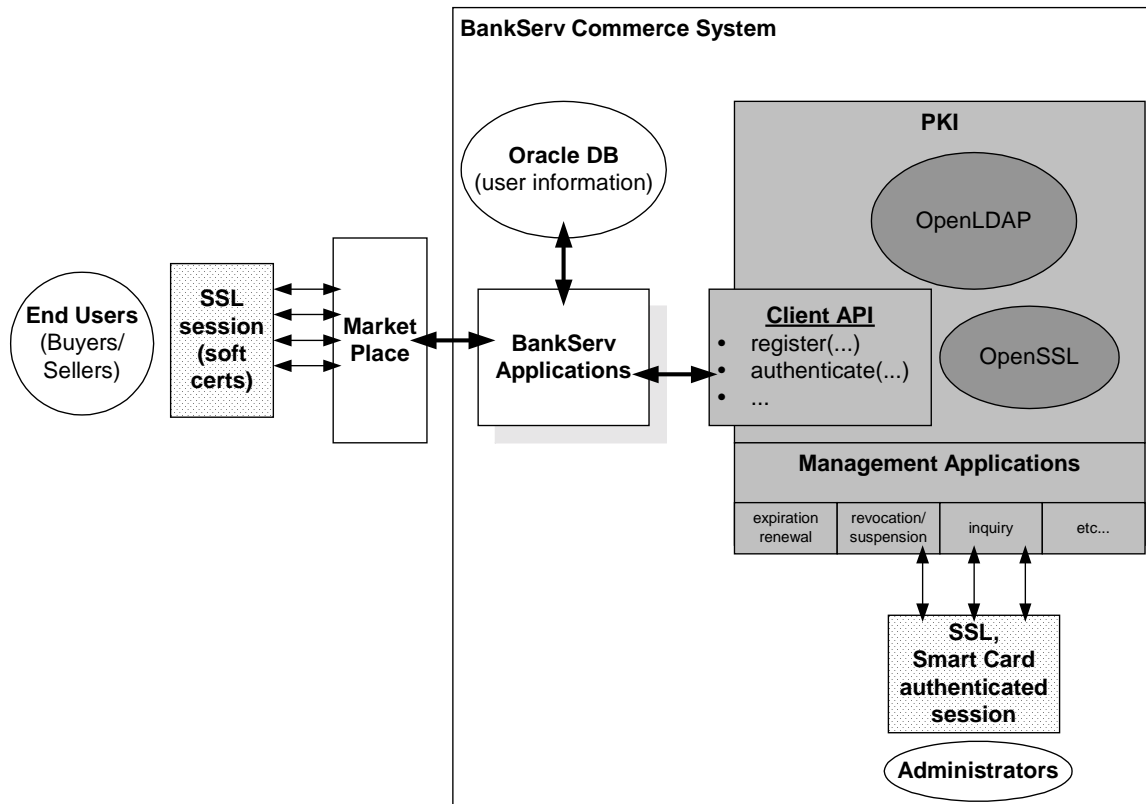
The Solution

The PKI system that was created for BankServ includes a CA, an LDAP accessible certificate repository, a complete suite of web based certificate management applications, and an authentication API. The issuance and management piece applications include registration, browser based key generation/certificate request, approval, certificate download, revocation, suspension, renewal, and CRL generation. The authentication API consists of a pure java library that verifies signatures and performs real time status checks on the signing certificates.

The following points describe the major system components in more detail:

- Xetex enabled the CA functionality by interfacing *OpenSSL* with a hardware security module (HSM) via the PKCS#11 interface. All CA private key data and signing operations are protected by the nCipher nForce HSM.
- To provide a secure web connection to the administrator's browser, the certificate issuance and management functionality is built on a *secure framework* that uses persistent digital signatures to authenticate each client request.
- To produce digital signatures from within the web browser, Xetex developed a crypto module that uses browser-based certificates (“soft certs”) in addition to a smart card based crypto module.
- The signature authentication functionality may be invoked by other server side java servlets and applications. If the cryptographic verification operations or the real-time status checks fail, an appropriate exception is thrown. If the signature verifies and the status validates, then the unique user ids of the signers are returned.

The following diagram shows the high level architecture of the PKI and how it integrates with the rest of the system.



Customer Benefits

Xetex delivered a complete PKI solution using common off-the-shelf components wherever possible. BankServ has the capability to create and issue digital certificates to anyone with a web browser and Internet connection. In addition, users that have been certified as administrators may carry out the certificate management functionality remotely. This system has the following advantages:

- Secure e-commerce is enabled by providing strong authentication capability using digital signatures. The system's authentication mechanism accepts a standard PKCS#7 structure that is typically created by browser based signing operations.
- By using open source components, the system may be extended more easily and the software licensing costs are minimized.
- The system provides an intuitive, user-friendly GUI for managing the certificate lifecycle. The system is web based and works with popular versions of both Netscape and Internet Explorer; the end users do not need to install any additional software or hardware (unless using smart card based certificates).
- Having the ability to use smart card based certificates as well as browser-based certificates provides flexibility in security policy and cost.
- Since the system uses a PKCS#11 enabled CA, it is possible to configure the system with other PKCS#11 compliant HSMs.

"Xetex clearly demonstrated they have the subject matter experts for the development and deployment of PKI and LDAP solutions. I would use them again without hesitation." – **Randy Gutierrez, Chief Information Officer, BankServ.**

"Xetex is very knowledgeable and delivered a quality product within the timelines promised. I would highly recommend Xetex for any PKI or LDAP-related project." – **Julie Conroy, Product Manager, BankServ.**

About Xetex, Inc.

Founded in 1994, Xetex, Inc. (www.xetex.com) is a professional services firm that provides technology solutions to clients that wish to enable or engage in secure electronic commerce. With years of experience designing, implementing, and deploying LDAP directory and public key infrastructure (PKI) solutions, Xetex is able to provide its clients with a full range of professional services including software development, design, integration, project management, strategy, and education.

Xetex, Inc. maintains offices in San Francisco, California (Technology) and Austin, Texas (Corporate). Further information about Xetex and its products & services can be obtained by contacting the company at the following address:

Xetex, Inc.
49 Stevenson Street, Suite 525
San Francisco, CA 94105
Tel: +1 415 512 7050
Fax: +1 415 512 9031