

# Employee Certificate Management System for Major US Bank

## *Customer Application Case Study*



### Introduction

Our customer (a major US bank, headquartered in Charlotte, North Carolina) has recently deployed several web-based applications that associates (employees) use regularly to perform various business processes. The bank wanted to enable associates to access these applications over the Internet as well as the corporate intranet. To do so securely, it needed to deploy a mechanism for strong authentication.

Our customer has elected to use public key technology as the basis for authentication to all web applications as well as for its Virtual Private Networks (VPNs). To do so, the customer is developing a public key infrastructure (PKI) that all applications can use for authentication, and is issuing digital certificates to all of its 150,000 associates. These digital certificates will allow applications to verify the identity of users who authenticate themselves using private key encryption, thereby enabling them to access bank systems securely from anywhere in the world.

Having worked successfully with Xetex on previous PKI projects, our customer retained Xetex to help design, develop, and integrate the certificate issuance and management system for their public key infrastructure.

### Associate Certificate Management Requirements

The customer required a system that could create and manage 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 certificate issuance and management system needed to be capable of integration with the customer's existing corporate directory. The identity of each associate needed to be validated against information in various parts of the directory during the issuance process.

The customer required that the certificates given to their associates be generated by VeriSign, so the system was required to communicate with VeriSign's certificate issuance service on the back end.

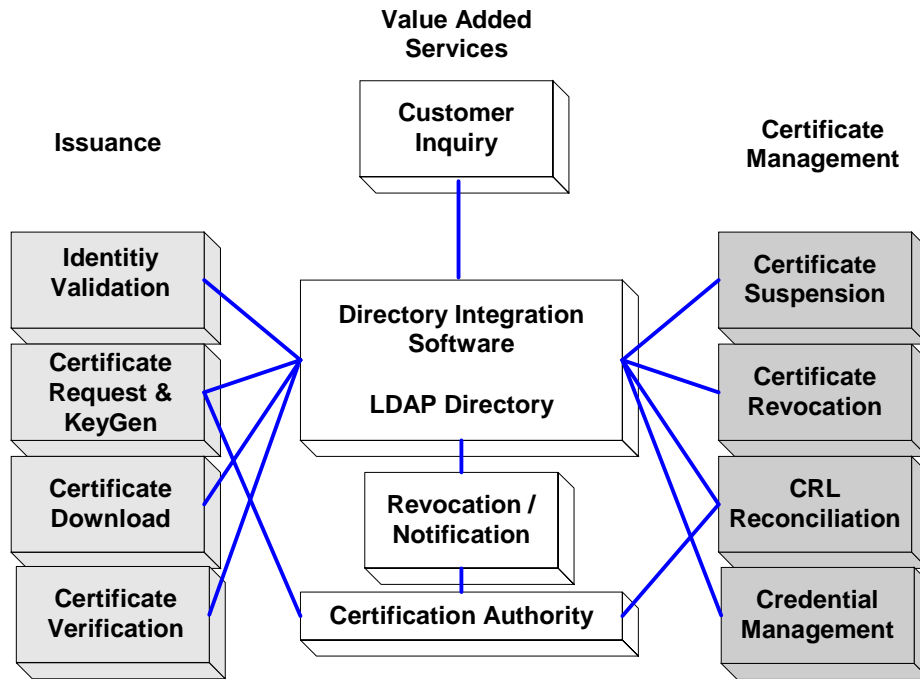
## The Solution

Xetex developed a suite of web-based java applications that perform certificate issuance and management functions. The applications are integrated around a central LDAP directory and constructed in a fashion that automates the entire issuance process. The issuance applications include initial identity validation, browser based key generation/certificate request, certificate download, and certificate status verification. The management applications include revocation, suspension, inquiry, credential management and CRL reconciliation. The system interfaces to VeriSign's Certification Authority and includes a Certificate Request Syntax (CRS) implementation.

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

- Xetex enabled the CA functionality by implementing a Java CRS toolkit capable of requesting and revoking certificates issued a VeriSign CA.
- To provide a secure web connection to the administrator's browser, the certificate issuance and management functionality is built on an application framework that uses persistent digital signatures to authenticate each client request.
- To produce digital signatures from within the web browser, Xetex developed crypto modules that can use certificates stored in both Netscape and Internet Explorer's certificate stores.

The following diagram shows the high level architecture of the PKI:



## Customer Benefits

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

- Applications and VPNs can be made available to associates anywhere in the world using the strong authentication capability of public key technology.
- 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.
- The system interoperates with, and thus leverages the customer's existing corporate directory.
- The system integrates seamlessly with the external CA (VeriSign), while leveraging the customer's existing corporate directory to hold authentication information, rather than the CA's database. This makes it easy for the customer to PKI-enable its applications, and prevents lock-in to a single source of infrastructure products and services.

## Next Steps

Having successfully completed the initial deployment of the customer's Employee Certificate Management System, Xetex has been subsequently retained to add more functionality such as support for billing, audit, and the Online Certificate Status Protocol (OCSP). The customer has also retained Xetex to develop a consumer and commercial customer certificate management system that will be used to provide their customers with a digital identity, made possible by public key technology.

## About Xetex, Inc.

Founded in 1994, Xetex, Inc. 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  
<http://www.xetex.com/>