

# Identrus Infrastructure for First Identrus Certified Level-1 Bank

## *Infrastructure Deployment Case Study*



### Introduction

Commerce on the Internet often requires that identity and trust be established between trading partners with no prior relationship. Financial institutions, the brokers of traditional commerce, can continue to facilitate these transactions on line, by working cooperatively within a common legal framework and using security technology recognized as viable by government legislation.

To establish a global network that allows e-business transactions and traditional bank services to be conducted securely over the Internet, Identrus LLC ([www.identrus.com](http://www.identrus.com)) was incorporated in April 1999 by eight of the world's foremost global financial institutions (ABN/AMRO, Bank of America, Bankers Trust, Barclays, Chase Manhattan, Citigroup, Deutsche Bank and HypoVereinsbank)

The Identrus network of trust uses public key technology to enable trading partners around the world to establish identity and trust. Under the Identrus public key infrastructure (PKI), participating financial institutions certify the public keys of their business customers by issuing them digital certificates. The certificates allow the businesses to authenticate one another during online transactions and to verify digital signatures, which legally bind electronic contracts. Thus, any two businesses with Identrus-certified public keys may engage in secure online transactions, regardless of which Identrus participants issued those certificates.

As a founding member and major technology contributor to Identrus, our client's goal was to establish the viability of its public key infrastructure by becoming the first financial institution to receive Identrus certification. Having worked successfully with Xetex on a previous PKI pilot project, our client retained Xetex to help design, develop, and integrate its Identrus infrastructure.

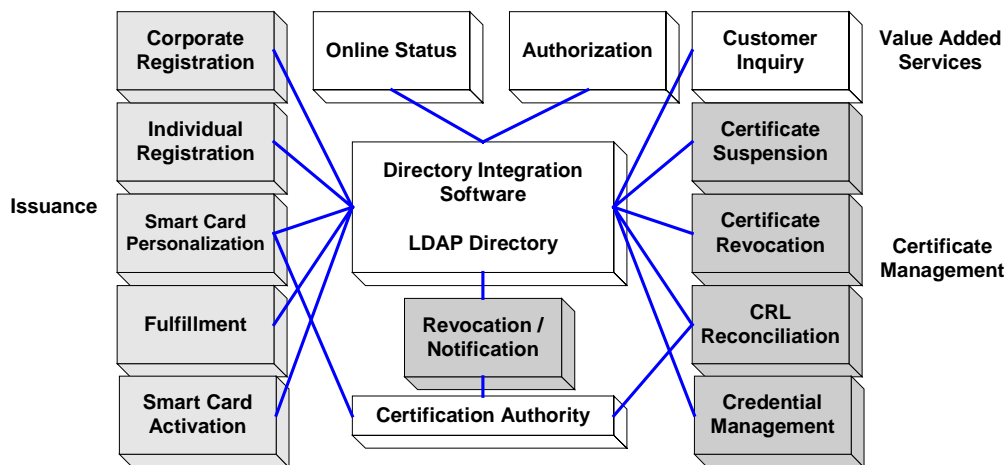
### Identrus Infrastructure Requirements

Our client wanted to create an Identrus infrastructure that would support the automated issuance and management of Identrus public key certificates on smart cards, and provide an online certificate status service that would allow its business customers to determine the status of certificates issued within the Identrus network. Our client wanted to integrate all PKI components around a central repository, which would employ LDAP directory technology.

## The Solution

Our client had selected vendors for their certification authority, directory and smart card personalization products, and leveraged Xetex’s knowledge of directories, PKI, and web-application development to fill in the gaps and bring the infrastructure together in a cohesive fashion. Our client used Xetex to accomplish the following:

- Xetex developed designed and implemented an X500 directory schema, which supports the integration of all PKI components.
- Xetex assisted the directory product vendor in designing, developing, and integrating their directory-based online certificate status protocol (OCSP) responder product. This OCSP responder product can obtain certificate status using the attributes from the directory, without waiting for the publication of a certificate revocation list (CRL).
- To enable certificate management functions to be used remotely by customers, Xetex developed a set of web-based certificate management applications such as issuance status inquiry, certificate suspension, certificate revocation, and CRL reconciliation. Integration with the directory allows these applications to share a consistent view with the OCSP responder and allows the responder to provide online status in real time.
- To enable business customers to register for, obtain, and activate their smart cards remotely and in an automated fashion, Xetex developed an integrated suite of directory-based certificate issuance applications such as customer enrollment, administrative approval, smart card distribution, and smart card activation.
- Xetex developed a Java library for integrating directory applications that was used to develop all of the certificate issuance and management applications described above and to integrate the selected smart card personalization product. The library addresses many of the traditional syntactic and semantic issues related to directory application integration and hides the details of the LDAP schema and Secure Sockets from applications programmers, allowing them to work with application level abstractions.
- Xetex supported the deployment of the infrastructure and supported our client and Identrus throughout the interoperability and pre-production testing.



## Customer Benefits

By providing a well-designed infrastructure that allowed custom developed software to be seamlessly integrated with vendor products, Xetex delivered a complete and automated PKI solution. This infrastructure was instrumental in our client becoming the first Identrus certified bank and gives them several technological advantages moving forward:

- Having an infrastructure integrated around the bank's directory, and not the CA's database, prevents lock-in to a single source of infrastructure products and services.
- Having a directory integration layer that eliminates semantic and syntactic integration bugs, and abstracts the details of directory schema and secure sockets, significantly reduces the cost of maintaining and developing infrastructure applications.
- Having an automated issuance process that enables remote administration by customers reduces operations cost and provides the scalability necessary to support a large customer base.
- Having integrated customer inquiry, revocation, and online status applications eliminates inconsistency and legal exposure during the CRL publication window.

## Next Steps

Having successfully completed the deployment of their PKI to support Identrus, Xetex has subsequently been retained by the same client to build and deploy a PKI to support the issuance and management of digital certificates for their employees and (non-Identrus) customers.

## 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/>