

# Integrated smart card and fingerprint biometric authentication

IIIIII AXA Technology Services: Deployment for Microsoft Windows Platform



FINANCIAL SERVICES & RETAIL

ENTERPRISE > CASE STUDY

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT



**gemalto**  
security to be free

# Integrated Smart Card and Fingerprint Biometric Authentication

## AXA Technology Services: Deployment for Microsoft Windows Platform



### About AXA Technology Services

With over 135,000 employees worldwide and operations in 55 countries, Paris-based AXA Group (91 billion euros in consolidated 2008 revenue) is the 15th largest organization on the 2008 Fortune Global 500 list based on annual revenue. Its wholly owned subsidiary, AXA Technology Services is an independent entity with a team of 3,500 employees who provide IT infrastructure services and support to most AXA Group companies. AXA Technology Services supports approximately 50 "customers" in 21 countries across Europe, North America and the Asia-Pacific region.

Because of the value and confidentiality of information in the financial services business, protecting IT systems and employee identity credentials has always been a priority for AXA Technology Services. Strong authentication systems have been deployed in several locations to address this need. For several years, senior level employees who access sensitive information have used strong authentication to provide an additional layer of security and reduce the risk of unauthorized access and data loss.

### Deployment of smart card devices

Recently, strong authentication devices have been deployed to a much broader user community because more employees are traveling and working remotely while still needing access to IT systems. Smart card-based devices are an optimal solution because of their security, convenience and cost advantages. Since they enable user validation for disparate systems, smart cards can be used as a single identity token for logical access requirements, including logon, secure remote access to web applications and other PKI (Public Key Infrastructure) services.

Users are able to logon to Windows with a certificate stored on their smart card; pre-authorized users may have the ability to authenticate to specific custom applications. In addition, a group PKI system for access to web services, laptop encryption and digital signature is being used by some AXA Technology Services customers. Overall, this improves information security, promotes greater use of electronic documents and enables safe use of Web-based services for more critical applications. The smart cards have additional capacity to support future applications as necessary.

AXA Technology Services is integrating smart card technology with the existing PKI system to define a new global standard for strong authentication. The company has worked with Gemalto and Microsoft® to develop a strong authentication framework based on Microsoft Base CSP (Cryptographic Service Provider)-compliant smart cards (the Gemalto .NET Smart Card) that is fully interoperable with the existing Microsoft environment being used. Globally, this environment includes Windows® XP and Vista® clients, Windows Server® 2003 and subsequent versions, Active Directory® and Microsoft Identity Lifecycle Manager (ILM).

In certain cases where it's justifiable and convenient, some authentication systems are being replaced by the standardized smart card solution. This is done when the solution meets the requirements of the previous system and offers the flexibility to support an array of future applications based on internal customer needs. A resource center and proof-of-concept program have been created to help demonstrate the solution to groups that may be interested in smart card-based authentication.

### Adding fingerprint biometrics

In 2007, an internal customer wanted to replace an existing strong authentication system with a smart card-based solution to coincide with an end-user hardware refresh project. AXA Technology Services initially

proposed its smart card platform and the customer subsequently inquired about extending it to support biometric authentication using fingerprints.

The primary objective was to enhance the user experience by adding support for biometric authentication using smart cards. This would make it easier and more convenient to logon securely and to use PKI certificates for access to more applications while providing same level of security. Login with username and password would still be supported because it was considered to be critical for managing a large, geographically dispersed user community. It would also provide a back-up authentication method for users who did not have possession of their smart card.

Because an off-the-shelf solution was not available, AXA Technology Services approached Gemalto about the possibility of developing a custom solution in a compressed timeframe. Based on a positive assessment of the project's feasibility, Gemalto decided to work with long time partner Precise Biometrics, the market leader in biometric software for smart cards, to develop a robust biometric authentication system for the Gemalto .NET smart card.

### Project scope and requirements

This particular AXA Technology Services' customer provides financial protection, life insurance and investment products to consumers, corporations and other financial services firms. Its products are sold directly by a retail distribution team and through financial intermediaries including brokers, dealers and independent financial planners.

These individuals work from multiple locations and require secure, on-demand access to networks, business applications and data. Secure remote access to an online portal is especially important because employees and external representatives are located throughout the country and often need to use web-based applications during meetings at their customers' locations.

The technology and functional requirements of the project included:

- The smart card and authentication process must be compatible with Windows XP SP2
- Windows logon is enabled by inserting the smart card and authenticating with a PIN or fingerprint scan
- The login process must work even when the PC is off the corporate network
- Removal of the card will lock the PC, re-insertion and authentication with a PIN or fingerprint scan will unlock the session
- The authentication system must provide access to all normal Windows functions
- The Smart Card must integrate with customer's local VPN/remote access solution and the current single sign-on functionality enabled through an intranet portal used by employees and field agents to access business applications
- An alternative Windows login path must be available in case the card is lost, damaged or forgotten
- A process to bind the Smart Card to the user prior to user delivery must be implemented
- There must be a user-friendly, well documented fingerprint registration process
- Cancellation and replacement processes for lost/damaged Cards are needed

### Solution architecture, components and usage

Gemalto and Precise Biometrics worked together to develop a Windows-based smart card authentication system with biometric support that met each of these requirements. Initial deployment was planned to coincide with the hardware refresh project during which the smart cards would be shipped to several thousand users with new laptops having integrated fingerprint scanners.

The Gemalto .NET smart card serves as the primary employee identity credential and incorporates fingerprint Match-on-Card™ technology from Precise Biometrics. Because it is integrated with Microsoft's Windows Smart Card Framework, the biometrics-enabled smart card is fully compatible with the customer's existing Microsoft infrastructure. Integration with Windows XP, Active Directory and Microsoft Identity Lifecycle Manager is seamless

and no middleware was required other than the specific components developed for biometric support.

Identity Lifecycle Manager is used as the certificate and smart card management system. ILM combines meta-directory, certificate management and user provisioning across Windows and enterprise systems in a single packaged offering. Its meta-directory capabilities support a single view of user identities across all enterprise systems and maintain the consistency of this view across all connected systems. The certificate management functionality in ILM significantly simplifies and reduces the cost of deploying and managing digital certificates and smart cards. Both the Gemalto .NET smart card and the biometric solution developed by Precise Biometrics are compatible with ILM so no changes to the card management system were required for deployment.

The solution consists of both on-card and off-card components as shown below. They include four libraries that are installed on the client computer and two applications that reside on the Gemalto .NET smart card itself. Components installed on the client PC enable the user's biometric credentials to seamlessly interact with the Microsoft operating system and applications.

Components of the solution are:

- Biometry-enabled Gemalto .NET smart cards that include a Biomatch Assembly (Precise Biometric's Match-on-Card application) and Mini-driver Bio Assembly

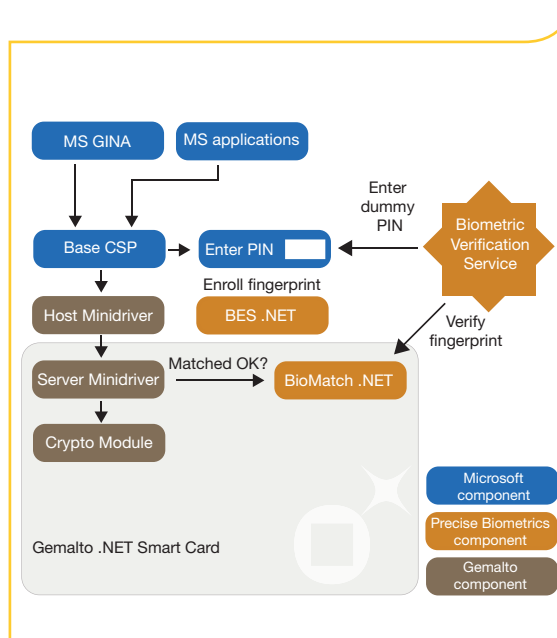
Four libraries are installed on the Windows XP client PC:

- BES – Biometric Enrollment Station Module: a client-side utility that enables users to enroll their fingerprints at any time
- BVS – Biometric Verification Service: a client-side service capturing and managing events from both the fingerprint reader and the Base CSP
- Mini-driver dll for the .NET Smart Card compatible with Microsoft Base CSP v5
- Customized Windows Smart Card logon interface (GINA)

The solution supports three different smart card authentication modes: PIN only, fingerprint only, and PIN or fingerprint. The biometric application stores and verifies users' fingerprint information directly on the smart card for added security. The fingerprint information never leaves the card and is never stored in a database, thus protecting users' digital identities. Privacy issues and security risks associated with other biometric authentication methods are mitigated because the fingerprint credentials are stored and validated on the smart card which is constantly in the user's possession.

The smart card is used to log on to any biometrics-enabled workstation within the customer's domain. The solution includes an enrollment application that lets users enroll their own fingerprints and provides other self-service capabilities, including remote card unblock. Up to 4 fingerprints can be enrolled and stored on the card and then used for biometric authentication.

When employees log on to their desktops or use security-enabled applications such as the secure remote access system, secure email or document signature, they insert their Gemalto .NET smart card into an integrated reader and then authenticate by scanning their fingerprint as a biometric identifier. PIN authentication is always available for workstations that may not have a fingerprint scanner.



Smart card – biometric solution architecture

## Customer deployment

Gemalto .NET cards with biometric support were initially deployed to over 3,000 independent representatives to enable secure remote network access and safe use of Web-based services for business-critical applications. The rollout began in June 2008 and was completed by the end of August. Subsequently, the biometric authentication solution was extended to several thousand corporate employees. This larger population is using the biometric smart card for network logon, digital signature and secure remote access. Smart cards issued to some employees at targeted locations include a contact-less smart card reader interface that can enable physical access to corporate facilities as required.

The impact on the user community was minimized by a close working relationship between the deployment team and branch technology managers located in each branch office. Each site was prepared for deployment by using a structured ten-week readiness schedule.

Several branch technology managers have reported that end users are very satisfied with the speed and ease of the biometric smart card login process. The number of smart card logins to the company's online portal for business applications has continually increased since the deployment began as shown below.

There has only been one reported situation where it was impossible to read and register a fingerprint. The most frequent help desk call is to unblock the card. It can be unblocked online through the Card Management System's web portal or offline with the assistance of a technical support representative over the phone.

## Positive impact on security and convenience

The successful development effort and deployment project helped AXA Technology Services meet its customer's expectations for rapid development and implementation of a smart card-based biometric authentication system. It also enabled AXA Technology Services to extend the corporate smart card framework to include biometrics support without any incremental risk or changes to the existing IT infrastructure.

Adopting the biometric smart card also strengthened the company's overall level of IT security and provided a means for smart card usage to become ingrained in the corporate culture. It has dramatically reduced password sharing and badge swapping. A converged badge for physical and logical access control also provides incremental value by dramatically reducing network attacks and data losses from internal sources.

## Value of Smart Card solutions

Smart cards can be used as a single, portable identity token for a wide range of personalized security services within business and government organizations. They support contact and contact-less communication interfaces and multiple identification, authentication and authorization methods, including single key, one time password (OTP), digital certificates (PKI), and biometrics.

Applications include visual identification, physical access control, computer logon, remote network access, email and data encryption, digital signature, and canteen and vending machine payments. In addition to strengthening security throughout the organization, smart cards provide convenience to users and administrators with significant cost savings through consolidation of security services using a single identity credential.

The biometric authentication solution enhanced the end-user experience by providing added convenience and flexibility for secure network access. Because the fingerprint biometric credentials are stored on the smart card, they are uniquely portable and can be used with any hardware system that has a smart card reader and fingerprint sensor.

For AXA Technology Services, the smart card-based solution extends the range of applications that can be secured with strong authentication. In addition to secure remote access, the company is considering smart card-enabled security for additional Web applications, e-mail signature, encryption and access to printing facilities. Already, there are plans to migrate several campuses to a single converged badge with the AXA Technology Services biometric smart card solution.

