gemalto

# Microsoft Identity Lifecycle Manager & Gemalto .NET Solutions

Jan 23rd, 2007

# Microsoft® Identity Lifecycle Manager 2007

Microsoft® ILM is a comprehensive, integrated, identity and access solution within the Microsoft system architecture. It includes a complete solution for centrally managing a **certificate-based infrastructure and strong authentication credentials, including smart cards.**

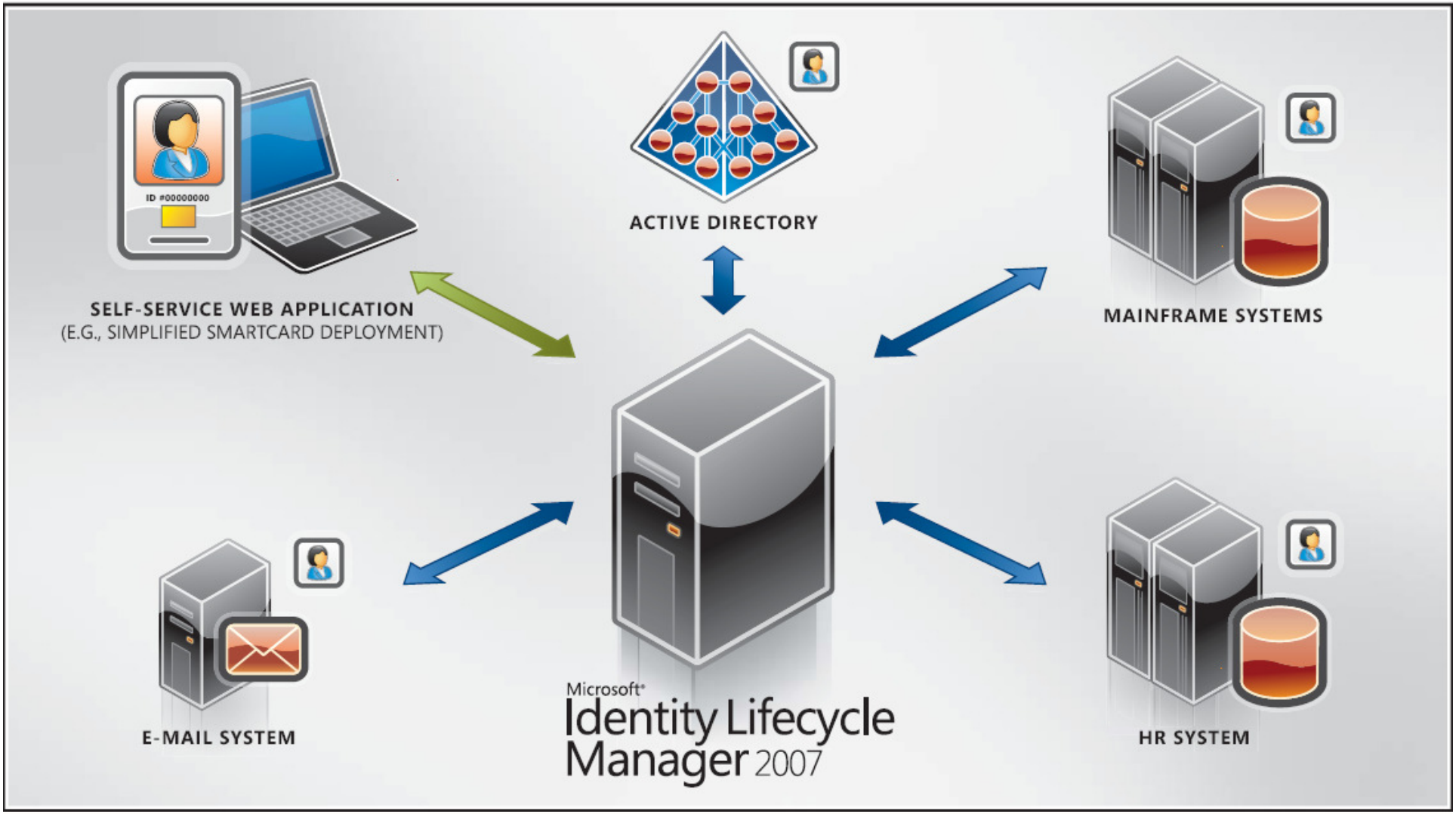
ILM provides a policy and workflow driven solution that helps organizations **manage the lifecycle of digital certificates and smart cards.**

ILM lowers the costs associated with digital certificates and smart cards by enabling organizations to more **efficiently deploy, manage, and maintain a certificate-based infrastructure**.

ILM streamlines the provisioning, deprovisioning, configuration, and auditing of digital certificates and smart cards, while **increasing security through strong, multi-factor authentication technology**.

Microsoft®
# Identity Lifecycle Manager 2007

## Architecture



Microsoft®
Identity Lifecycle Manager 2007

# Certificate Management

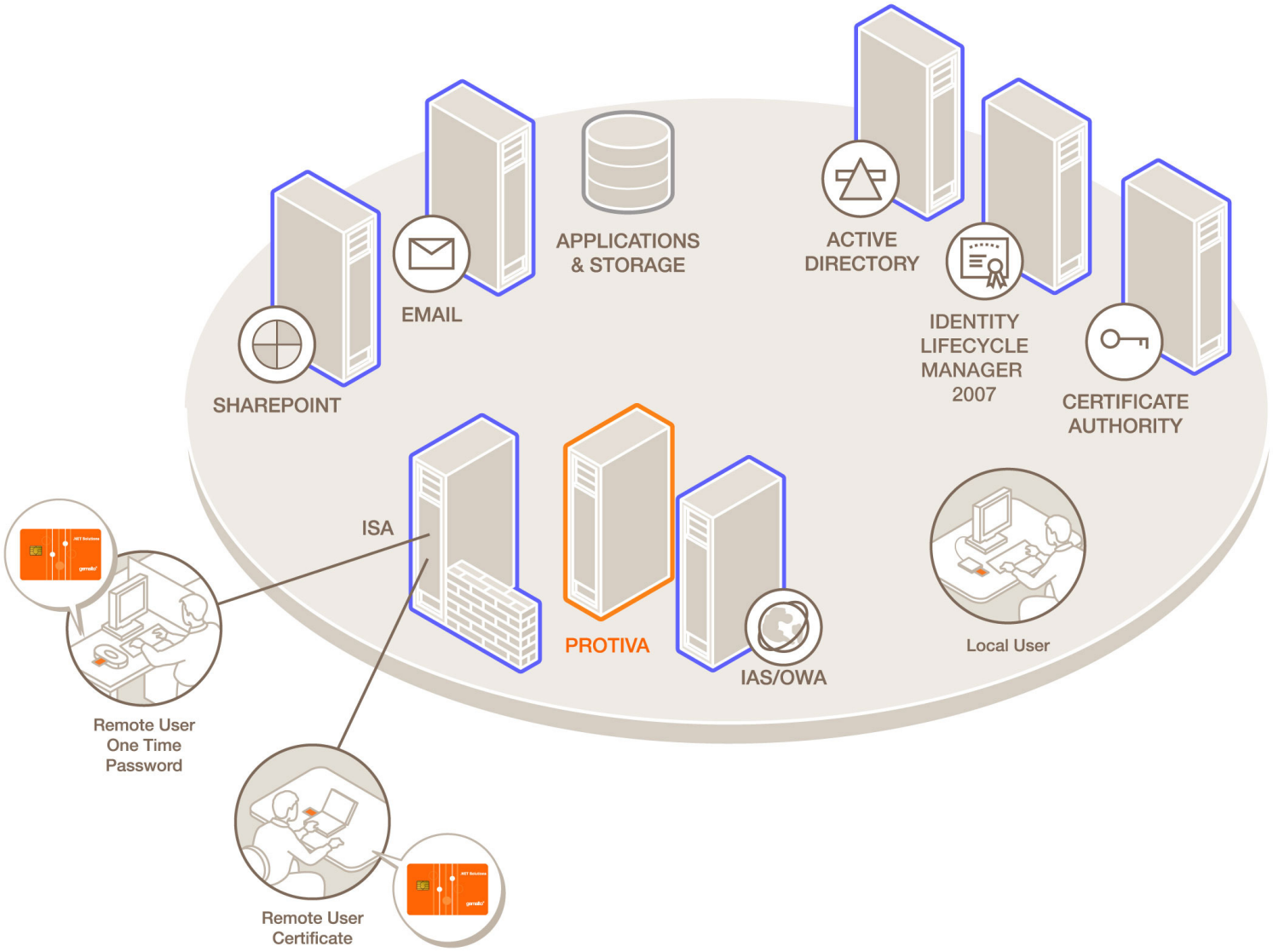
- Single administration point for digital certificates and smart cards
- Configurable policy-based workflows for common tasks
  - Enroll/renew/update
  - Recover/card replacement
  - Revoke
  - Retire/disable smart card
  - Issue temporary/duplicate smart card
  - Personalize smart card
- Detailed auditing and reporting
- Support for both centralized and self-service scenarios
- Integration with existing infrastructure investments
  - Windows Active Directory; Windows Certificate Services

Microsoft®
Identity Lifecycle Manager 2007

# Certificates & Smart Cards

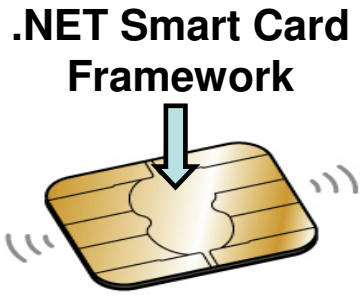
- **ILM features related to Certificate & Smart Card management include:**
  - A complete and integrated management solution for deploying smart cards and digital certificates
  - Delegated request and approval capabilities for distributed environments
  - In-person authentication and self-service management features
  - Closely integrated with Active Directory and Microsoft certification authorities (CAs)
  - Policy support for workflow, registration data collection, and document printing
  - Smart card lifecycle management, including smart card printing
  - Complete Personal Identification Number (PIN) management features for activating and unblocking PINs. This can be managed either in a self-service method or by an administrator.
  - Smart card inventory system that is updated upon smart card activation, simplifying distribution
  - Sophisticated, complete reporting and audit tracking of all smart card lifecycle activities
  - Bulk Smart Card Issuance Tool to facilitate enrollment and smart card issuance for hundreds of users

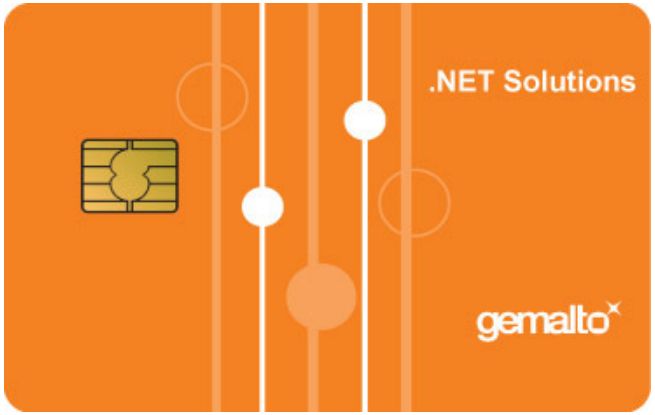
# Gemalto .NET & Microsoft ILM Architecture



# Gemalto .NET Card: Main Benefits

- Provides **strong two-factor authentication** to **secure** a company's **assets and identities** on a network
- Integrates **quickly and seamlessly** within the **Microsoft** world…
- Is **easy to deploy and manage**, resulting in lower implementation cost
- Implements **.NET framework** to enable development of comprehensive **on card / off card security solutions**

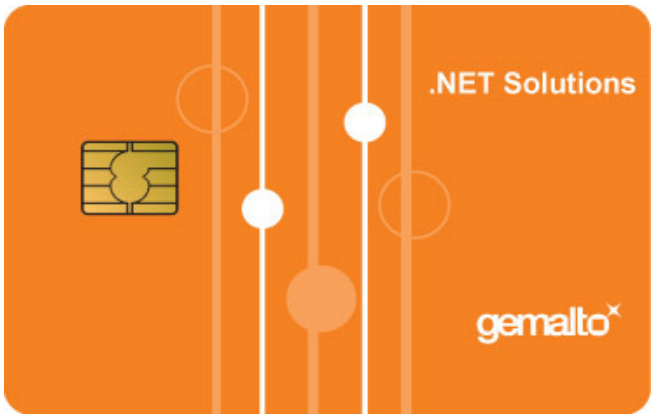


# Gemalto .NET card: Main Characteristics

Microsoft Mini Driver Assembly onboard

.NET Smart Card Framework




PKI Crypto RSA 2048

Protiva OTP Assembly onboard

75KB available for additional assemblies

- Mini Driver assembly compatible with 32 bit and 64 bit Windows platforms
- Available memory for assemblies and certificates can be extended to 85 KBytes by removing the Protiva OTP assembly
- Protiva OTP is Gemalto's OATH One Time Password Key Generator assembly, compatible with Protiva OTP Server Solution. For more information visit www.protiva.gemalto.com

# Technical details I

- **Silicon features**
  - Chip Infineon SLE88CFX4000P (400 KB Flashmask)
  - 32-bit micro-controller in advanced CMOS technology
  - Cryptographic co-processor for faster RSA and 3-DES
  - True random number generator
- **Cryptographic capabilities**
  - RSA signature and verification up to 2048-bit keys
  - DES, 3-DES (CBC, EBC), AES, HMAC, SHA1,SHA2 and MD5
  - Customizable authentication framework and secure channel capabilities
- **Standards**
  - ISO 7816-1-2-3-4 (partial)
  - ECMA 335 / ISO/IEC 23271 – Common Language Interface
- **File system**
  - Secure data storage
  - Role-based access control
  - Enables assembly and data separation
  - Enables Assembly update with data preservation

# Technical Details II

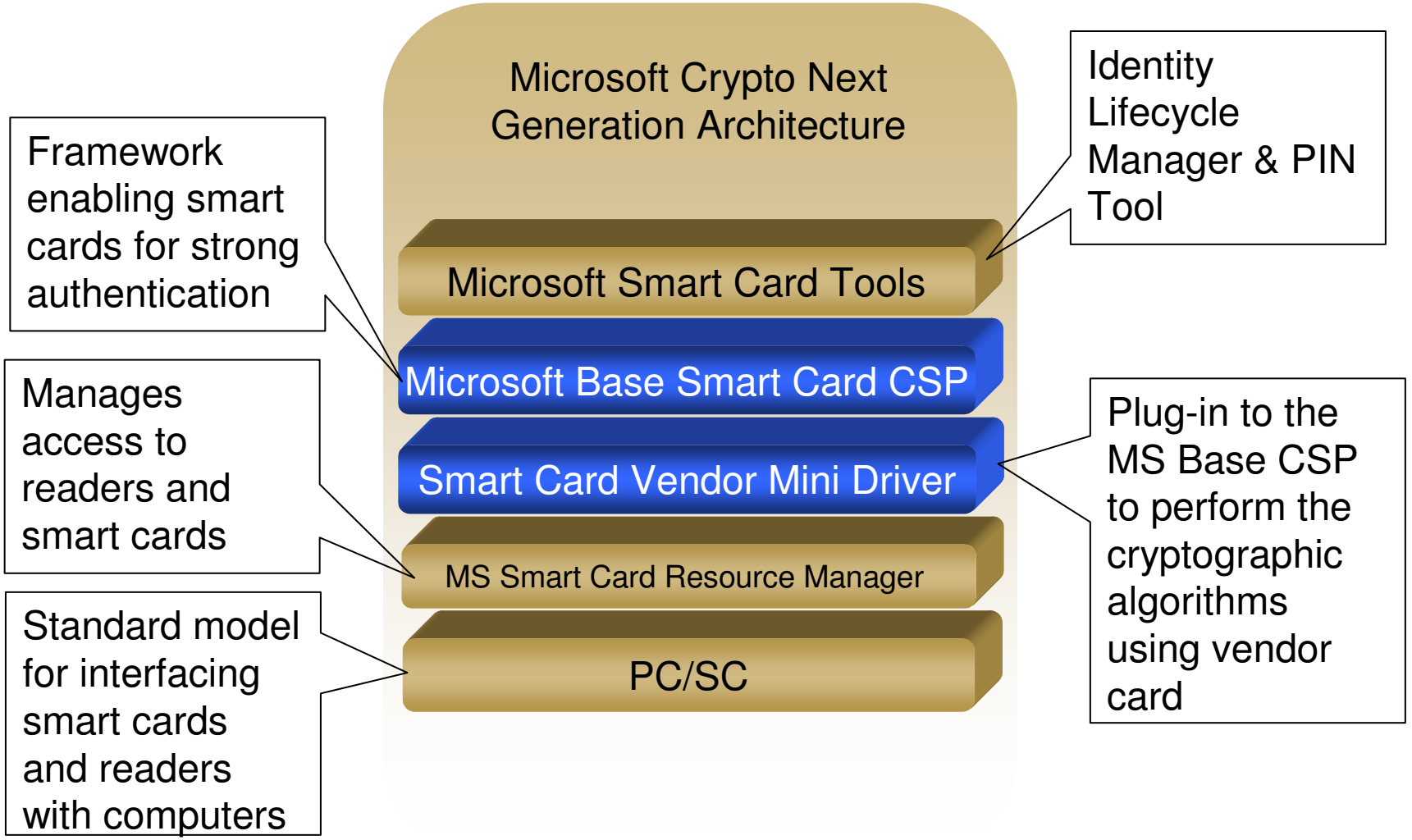
- **Application development**
  - .NET compatible and programming language independent (CLI)
  - 75KB expandable to 90KB memory available for applications
  - Legacy compatible application development
  - On-card XML parser
  - Support for int-64
- **Security**
  - Off-card application verification integrated in tool chain
  - On-card verifier to check type structural integrity and type safety of applications
  - Only strong-name signed assembles can be loaded ensuring integrity and authenticity
- **Communications**
  - Standard I/O transfer speed up to 223 Kbps
  - Negotiable PPS
  - T=0 protocol
  - SConnect
  - .NET Remoting

# Why .NET on a Smart Card?

- Seamlessly **integrates the application developer** language and tools for both on and off-card application development
- "Web Services" enable the smart card to **communicate as a peer** computing device
- The .NET CLR and Remoting provides a **consistent security model** between applications on and off-card
- Makes smart cards available to a wider audience…

  …which will lead to more smart card integrated applications in the future

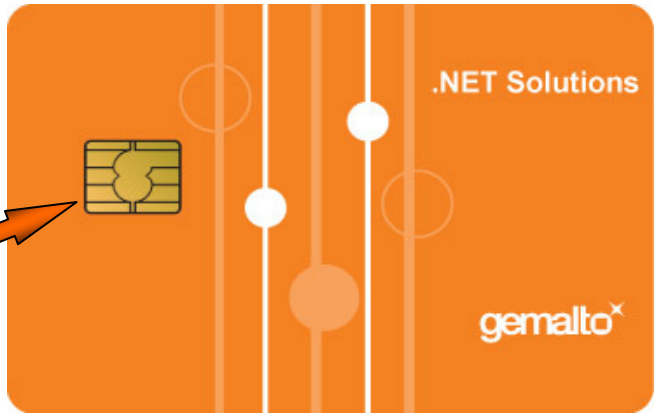
# Microsoft Crypto Architecture



# Gemalto .NET Crypto Architecture

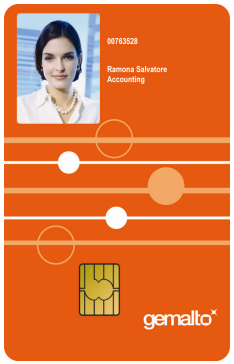

… leveraging Microsoft's new security architecture

Proxy plug-in to the MS Base CSP to forward calls to the Mini Driver on the Gemalto .NET card



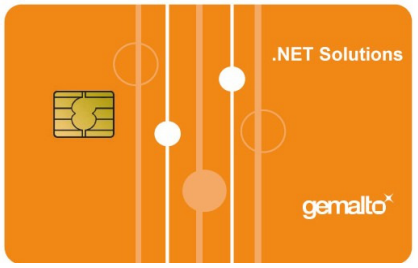
# Gemalto .NET in the Microsoft ecosystem

- .NET card built into Windows Vista
- .NET card built into Microsoft Base CSP Package (available via Windows Update) for Windows 2000, XP & Server 2003
- CMS of reference: Microsoft ILM
- .NET SDK integrated in Microsoft Visual Studio .NET
- Gemalto .NET Card is used by Microsoft's as its own Corporate Badge



# Case Study: Microsoft security solution with Gemalto .NET Smart Cards

Microsoft®




- Complex Situation
  - Despite strong password policies, Microsoft determined that additional forms of authentication were required, especially for remote access to their corporate network.
- Clarifying Solution
  - To counter the threat of unauthorized access to the Microsoft corporate network, Microsoft chose to deploy smart cards because of the cumulative sum of the products' reliability, performance, cost, security features, convenience and portability benefits.
  - The logical access control is provided by a microprocessor contact smart card with specialized security features and large memory for application storage. A contactless feature embedded in the card will provide physical access to buildings and offices.
  - The Gemalto .NET smart card runs a small footprint version of the .NET framework and provides customizable two-factor authentication, in addition to full cryptographic capabilities.
- Better Performance
  - This approach to logical access security, completed worldwide in 2002 for Microsoft's 61,000 employees, has substantially increased the overall security of enterprise network assets and data at Microsoft.

# Case Study: Microsoft security solution with Gemalto .NET Smart Cards

- Corporate-wide deployment
- Issued to 60K+ employees worldwide
- Protects network access and other corporate intellectual property


- Logical and physical access Badge
- Remote access (VPN)
- Web authentication
- Encryption
- Digital signatures
- Password replacement

Microsoft partner Gemalto "has done a super job on this", said Gates. "We will be using their smartcards internally - each employee will use those to get in and out of the buildings as we used to connect to our machines. We're requiring them. We will completely replace passwords."