Gemalto .NET Technology

Smart Card implementation of the .NET Framework

FINANCIAL SERVICES & RETAIL

ENTERPRISE>PRODUCT

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATIONS

gemalto
security to be free

Gemalto .NET smart card technology provides a seamless companion to the Microsoft .NET environment and service-oriented architectures

By extending the Microsoft .NET programming model to the smart card, this Gemalto innovation empowers application developers through the rich features of managed memory, security and language integration

> Secure Execution Runtime and Multiple Applications

Gemalto .NET smart card technology capitalizes on the secure and portable aspects of the Common Language Infrastructure (CLI) enabling application development in C# using the .NET Framework. The CLI implemented in the smart card allows smart card applications to be integrated in .NET solutions. Gemalto .NET smart card technology also supports multiple applications running on the same card simultaneously. Each on-card application is isolated from the others ensuring application safety and integrity.

> Unified communications via Remoting

The use of .NET Remoting mechanisms for communication between smart cards and a host device simplifies the integration of smart card services within .NET infrastructures and devices. Applications communicating with a smart card can be independent of the communications protocol being used, be it the smart card specific ISO 7816-4 protocol or tailored to interconnection buses such as USB. Protocol neutrality also provides a way for smart cards to participate in emerging application architectures such as web services. Investment in legacy host-based applications is preserved by allowing APDU-based communication while simultaneously supporting .NET Remoting technology for on-card applications.

> The Gemalto .NET Smart Card Framework

A subset of the .NET Framework class libraries was carefully selected for on-card application development and host-smart card connectivity. Like the .NET Compact Framework for mobile devices, a reduced footprint, the Gemalto .NET Smart Card Framework was created by retaining classes suitable for smart cards and introducing classes (such as PIN, Transaction, and ContentManager) relevant to on-card application development and card management. Working with a subset of the .NET Framework class libraries provides a programming model consistent with that of the full .NET Framework.

The Gemalto .NET smart card facilitates reusable components focusing on core business services, leveraging Microsoft .NET data exchange standards to eliminate the waste of smart card specific infrastructure development.

> Seamless access to cryptographic services

Secure and reliable cryptographic operations, such as symmetric (DES, AES) and asymmetric (RSA) algorithms are accessible in Gemalto .NET smart card technology via an implementation of the standard Cryptographic Services architecture of the .NET Framework, namely the System.Security.Cryptography namespace. This empowers existing .NET solutions that use .NET cryptographic services to be easily modified to use smart cards, for enhanced security. With an optional application embedded on the Gemalto .NET smart card, secure access to networks, data protection and verification is made possible together with the Microsoft Base Smart Card CSP (Cryptographic Service Provider) for seamless integration that does not require additional software to be deployed.

The Gemalto .NET smart card provides a secure extension to the Microsoft® .NET environment and service oriented architectures By extending the Microsoft .NET programming model to the smart card, this new Gemalto innovation empowers application developers through the rich features of managed memory, security, and language integration

> Application development/integration within Visual Studio® .NET

Applications using Gemalto .NET smart card technology are developed, debugged, tested and loaded using a set of tools integrated within Visual Studio .NET. This functionality is achieved without ever having to leave the IDE (Integrated Development Environment). Enhancements to Visual Studio .NET pave the way for easy integration of smart card applications into other .NET based technologies such as Smart Clients, ASP.NET Web Services, etc.

> Practical and efficient garbage collection

.NET application programming encourages the creation of many short-lived objects that can be reclaimed via garbage collection. However, smart card memories pose a challenge to using classical garbage collection in smart cards. Gemalto .NET smart card technology overcomes this limitation by using garbage collection algorithms designed specially for smart cards, and by providing transparent memory allocation with fast garbage collection, freeing developers to focus on application development.

> Powerful transaction system

Persistent memory allows smart cards to maintain their state across card usage sessions, making the card appear as a computer that is always on. Consequently handling 'tearing' (power loss during card operation) and memory coherence requires smart cards to provide a transaction mechanism that ensures consistent memory updates. Towards this end, Gemalto .NET smart card technology features a transaction system that supports arbitrarily nested transactions with transaction lengths limited only by the available card memory.

> Highly compact yet expressive applications

Microsoft's Portable Executable Common Object File Format (PE/COFF) used by the .NET Framework is transformed into a more compact representation suitable for a resource constrained device such as a smart card. The resulting representation retains the expressivity of the original PE/COFF, implements the ECMA standardized opcodes, and offers a factor of 4X reduction in application size.

The power of .NET in a smart card has resulted in a smart card platform that permits multiple applications in different languages to transparently interact while providing the full range of features one expects from a modern secure application execution environment. This, coupled with the Gemalto .NET powered smart card technology tools integrated within Visual Studio .NET, makes for seamless integration of .NET smart card technology into .NET solutions resulting in an enhanced user experience and increased added value.

> Technical Highlights

- Applications communicating with a smart card are independent of the communications transport being used.
- Development using Visual Studio® .NET enables use of Microsoft's Web Services Enhancements (WSE) allowing easy smart card integration into solutions based on web services.
- Host and smart card applications interact transparently using secure communication channels, allowing multiple card applications to be "active" at the same time without explicit application selection.
- Access to the on-card timer allows new applications such as temporary web-coupons or the use of time based PINs.
- Secure and reliable cryptographic operations including both symmetric (DES, AES) and asymmetric (RSA) algorithms enhance application security.
- Support for on-card garbage collection simplifies card memory allocation and management.

Main features

- Compliant with the ECMA 335 Kernel Profile
- Support for int-64
- ISO 7816-1-2-3-4 (partial),T=0
- PC/SC

File system

- Secure data storage
- Role-based access control
- Enable assembly* and data separation
- Assembly update with data preservation

Application development

- Legacy compatible application development
- Visual Studio.NET add-ins for integrated development
- Smart card application development using .NET Remoting
- On-card XML parser for WS-*/CardSpace integration

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

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 assemblies can be loaded ensuring integrity and authenticity

Communications

- .NET Remoting
- ISO 7816-2: physical contacts (ISO-8)
- ISO 7816-3:
  - standard I/O transfer speed up to 223 Kbps
  - negotiable PPS
- ISO 7816-4:
  - T=0 protocol

Silicon features

- 80KB memory available for assemblies
- 32-bit micro-controller in advanced CMOS technology
- Temperature range of -25°C to +85°C
- Single power supply: 3V or 5V
- EEPROM endurance: 500,000 write/erase cycles
- Data retention: 10 years (ambient temperature)
- Cryptographic co-processor for faster RSA and 3-DES
- True random number generator
- Common Criteria EAL 5+

Pre-personalization capabilities

- Factory provisioning of applications
- XML-based card file properties
- Unique card serial number
- Large choice of key ceremony procedures

*An assembly refers to a binary programming unit that comes in two types, application assemblies (.EXE) and library assemblies (.DLL).

Microsoft®
GOLD CERTIFIED
Partner

www.gemalto.com

gemalto

security to be free