



Gemalto .NET Lösungen

.NET-Lösungen für Web-Dienste, Identitätssicherung, XML

FINANZDIENSTE UND EINZELHANDEL

UNTERNEHMEN > TECHNOLOGIE

INTERNET CONTENT PROVIDER

ÖFFENTLICHER SEKTOR UND TRANSPORT

TELEKOMMUNIKATION



Die Gemalto .NET Smartcard arbeitet nahtlos in der Microsoft® .NET-Umgebung und in serviceorientierten Architekturen

Mit der Erweiterung des Programmiermodells Microsoft .NET auf die Smartcard bietet diese Innovation von Gemalto Anwendungsentwicklern eine reichhaltige Reihe von Funktionen einschließlich Managed Memory, Sicherheit und Sprachunabhängigkeit.

> Sichere Ausführungszeit und mehrfache Anwendungen

Die .NET Smartcard-Technologie von Gemalto macht sich die sicheren und portablen Aspekte der Common Language Infrastructure (CLI) zur Anwendungsentwicklung in C# mittels .NET Framework zunutze. Die in der Smartcard implementierte CLI gestattet die Integration von Smartcard-Anwendungen in .NET-Lösungen. Die .NET Smartcard-Technologie von Gemalto unterstützt auch mehrere gleichzeitig auf der gleichen Karte laufende Anwendungen. Dabei wird jede On-Card-Anwendung von den anderen isoliert, damit die Sicherheit und Integrität aller Anwendungen aufrechterhalten wird.

> Vereinheitlichte Kommunikationen über Remoting

Die Verwendung von .NET Remoting-Mechanismen für die Kommunikation zwischen Smartcards und einem Host-Gerät vereinfacht die Integration von Smartcards innerhalb von .NET-Infrastrukturen und -geräten. Anwendungen mit Smartcard-Kommunikationen können unabhängig vom eingesetzten Kommunikationsprotokoll ablaufen, ob es sich hierbei nun um das Smartcard-spezifische Protokoll ISO 7816-4 oder um speziell angepasste Busanschlussysteme wie USB handelt. Durch die Protokollneutralität wird außerdem ermöglicht, dass Smartcards für neu entstehende Anwendungsarchitekturen wie etwa Web-Dienste herangezogen werden können. Investitionen in ältere Host-basierte Anwendungen bleiben dadurch weiter erhalten, dass APDU-basierte Kommunikationen zugelassen werden, während gleichzeitig die .NET Remoting-Technologie in Ihrer On-Card-Anwendung unterstützt wird.

> Das Gemalto .NET Smart Card Framework

Nach kritischer Überprüfung verschiedener Möglichkeiten wurde eine Untergruppe der Objektklassenbibliotheken des .NET Framework für die Entwicklung von On-Card-Anwendungen



Die .NET Smartcard von Gemalto ermöglicht auch den Einsatz wiederverwendbarer Komponenten mit dem Fokus auf Kerngeschäftstätigkeiten, wobei die .NET Datenaustauschstandards von Microsoft effektiv genutzt werden und sich die Entwicklung einer Smartcard-spezifischen Infrastruktur erübrigt.

und die Konnektivität zwischen Host und Smartcard gewährt. Wie es beim .NET Compact Framework für mobile Geräte der Fall ist, wurde das weniger Aufwand beanspruchende Gemalto .NET Smart Card Framework erstellt, indem für Smartcards geeignete Klassen erhalten und für die Entwicklung von On-Card-Anwendungen und die Kartenverwaltung relevante Klassen (wie etwa PIN, Transaction und ContentManager) eingeführt wurden. Mit dem Einsatz einer Untergruppe von Objektklassenbibliotheken des .NET Framework wird ein Programmiermodell bereitgestellt, das dem vollen .NET Framework entspricht.

> Nahtloser Zugang zu Verschlüsselungsdiensten

Sichere und zuverlässige Verschlüsselungsprozesse, wie etwa symmetrische Algorithmen (DES, AES) und asymmetrische Algorithmen (RSA), sind in der Gemalto .NET Smartcard-Technologie über eine Implementierung der standardmäßigen Cryptographic Services Architektur des .NET Framework verfügbar, und zwar über den Namensraum System.Security.Cryptography. Damit können bestehende .NET-Lösungen, bei denen .NET-Verschlüsselungsdienste eingesetzt werden, problemlos für die Verwendung von Smartcards modifiziert werden. Dies bedeutet für die .NET-Lösungen verbesserte Sicherheit und erweiterte benutzerspezifische Gestaltung. Mit einer optionalen, in der Gemalto .NET Smartcard eingebetteten Anwendung wird der sichere Zugang zu Netzwerken, Datenschutz und -Verifizierung ermöglicht. Bei Nutzung des Microsoft Base Smart Card CSP für eine nahtlose Integration wird kein Einsatz von zusätzlicher Software nötig.

> Applikationsentwicklung/-integration innerhalb Visual Studio® .NET

Anwendungen mit dem Einsatz der .NET Smartcard-Technologie von Gemalto werden mithilfe einer Reihe von Tools der Fehlerkorrektur unterzogen, getestet und geladen, die innerhalb Visual Studio .NET integriert sind. Diese vielfältige

Funktionalität wird erreicht, ohne dass dabei die Entwicklungsumgebung verlassen werden muss. Erweiterungen von Visual Studio .NET bereiten den Weg für die leichte Integration von Smartcard-Anwendungen mit anderen .NET-basierten Technologien wie etwa Smart Clients, ASP.NET Web Services usw.

> **Praktische und effiziente Speicherbereinigung**

Mit der .NET-Anwendungsprogrammierung geht die Erstellung von vielen kurzlebigen Objekten einher, die über die Speicherbereinigung wiedergewonnen werden können. Smartcard-Speicher bilden jedoch eine Herausforderung für den Einsatz der klassischen Speicherbereinigung für Smartcards. Bei der .NET Smartcard-Technologie von Gemalto wird diese Beschränkung mit dem Einsatz von spezifisch für Smartcards konzipierten Speicherbereinigungsverfahren überwunden, und durch die Bereitstellung einer transparenten Speicherzuordnung mit schneller Speicherbereinigung wird es Entwicklern ermöglicht, sich auf die Anwendungsentwicklung zu konzentrieren.

> **Leistungsfähiges Transaktionssystem**

Mit Permanentspeicherung können Smartcards ihren Zustand über verschiedene Sessions aufrechterhalten, wodurch die Karte sich stets wie ein permanent eingeschalteter Computer verhält. Deshalb ist für die Beherrschung des „Abreibens“ (Leistungsverlust während eines Karteneinsatzes) und der Speicherkohärenz erforderlich, dass Smartcards einen Transaktionsmechanismus für die Gewährleistung von konsistenten Speicheraktualisierungen aufweisen. Um dies zu erreichen, ist die .NET Smartcard-Technologie von Gemalto mit einem Transaktionssystem ausgestattet, welches beliebig verschachtelte Transaktionen mit Transaktionslängen gestattet, die nur durch den verfügbaren Kartenpeicher begrenzt sind.

> **Hochgradig kompakte und dennoch ausdrucksstarke Anwendungen**

Das Portable Executable Common Object File Format (PE/COFF) von Microsoft, welches im .NET Framework verwendet wird, wird in eine kompaktere Form umgewandelt, die sich für ein ressourcenbegrenztes Element wie etwa eine Smartcard eignet. In der daraus entstehenden Darstellung bleibt die Ausdrucksstärke des ursprünglichen Formats PE/COFF erhalten, wobei die ECMA-standardisierten Operationscodes implementiert und eine Reduzierung der Anwendungsgröße um den Faktor 4 geboten wird.

Das hohe Leistungsvermögen von .NET in einer Smartcard resultiert in einer Smartcard-Plattform, welche vielfachen Anwendungen in verschiedenen Sprachen und eine transparente Interaktion gestattet, wobei gleichzeitig eine volle Reihe von Funktionen bereitgestellt wird. In Kombination mit den durch die Smartcard-Technologie bereitgestellten Tools von Gemalto .NET, gewährleistet die nahtlose Integration der .NET Smartcard-Technologie in .NET-Lösungen ein verbessertes Kundenerlebnis und eine erhöhte Wertschöpfung.

> **Herausragende technische Vorzüge**

- Anwendungen für die Kommunikation mit Smartcards sind unabhängig von der eingesetzten Übermittlungsweise.
- Entwicklungen, bei denen Visual Studio® .NET eingesetzt wird, ermöglichen die Verwendung von Microsoft Web Services Enhancements (WSE), wodurch Smartcard-Anwendungen leicht in Lösungen integriert werden können, die auf Web-Diensten basieren.
- Host- und Smartcard-Anwendungen wirken transparent mittels sicherer Kommunikationskanäle zusammen, wobei mehrfache Kartenanwendungen gleichzeitig ohne explizite Wahl der Anwendung „aktiv“ sein können.
- Der Zugriff auf den On-Card-Timer ermöglicht neue Anwendungen wie zum Beispiel zeitlich begrenzte Web-Coupons oder die Verwendung von zeitbasierten PINs.
- Sichere und zuverlässige Verschlüsselungsprozesse, wie etwa symmetrische Algorithmen (DES, AES) und asymmetrische Algorithmen (RSA) erhöhen die Anwendungssicherheit.
- Unterstützung für On-Card-Speicherbereinigung vereinfacht die Kartenspeicherzuordnung und dessen Verwaltung.

Hauptfunktionen und -eigenschaften

- Entspricht den Anforderungen des ECMA 335 Kernel Profile
- Unterstützung für int-64
- ISO 7816-1-2-3-4 (teilweise), T=0
- PC/SC

Dateisystem

- Sichere Datenspeicherung
- Rollenbasierte Zugriffssteuerung
- Programmbaustein-* und Datenseparierung
- Programmbausteinsaktualisierung mit Datenerhaltung

Anwendungsentwicklung

- Mit älteren Systemen kompatibel Anwendungsentwicklung

- Visual Studio.NET Zusatzfunktionen für integrierte Entwicklung
- Smartcard-Anwendungsentwicklung mittels .NET Remoting
- On-Card-XML-Parser für WS-*/CardSpace-Integration

Verschlüsselungsfähigkeiten

- RSA-Signatur und -Verifizierung bis zu 2048-Bit-Schlüssel
- DES, 3-DES (CBC, ECB), AES, HMAC, SHA1, SHA2 und MD5
- Anpassbarer Authentifikationsrahmen und sichere Kanalfunktionen

Sicherheit

- Off-Card-Anwendungsverifizierung in Toolkette integriert
- On-Card-Verifizierer zur Überprüfung der typenstrukturellen Integrität und Typensicherheit von Anwendungen
- Nur mit starken Namenssignaturen versehene Programmbausteine können zur Sicherstellung der Integrität und Authentizität geladen werden

Kommunikationen

- .NET Remoting
- ISO 7816-2: physische Kontakte (ISO-8)
- ISO 7816-3:
 - Standard-E/A-Übertragungsgeschwindigkeit bis zu 223 Kbps
 - PPS übertragbar
 - T=0 Protokoll

Silicon-Features

- 90Kb Speicher für Programmbausteine verfügbar
- 32-Bit-Micro-Controller in erweiterter CMOS-Technologie
- Temperaturbereich -25°C bis +85°C
- Einzel-Stromanschluss: 3 V oder 5 V
- EEPROM-Dauerleistung: 500.000 Schreib-/Löschzyklen
- Datenhaltung: 10 Jahre (Umgebungstemperatur)
- Verschlüsselungs-Co-Prozessor für RSA und 3-DES mit höherer Geschwindigkeit
- Echter Zufallszahlengenerator

Vorpersonalisierungsleistungen

- Werksseitige Bereitstellung von Anwendungen
- XML-basierte Kartendatei-Eigenschaften
- Einmalige Kartenseriennummer
- Große Auswahl von Schlüsselzeremonienabläufen

*Ein Programmbaustein bezieht sich auf eine binäre Programmierereinheit, von der es zwei Varianten gibt - (.EXE) und Bibliotheksbausteine (.DLL).

www.gemalto.com

