

Kundenspezifische Sicherheitslösungen für Produkte und embedded Systeme

Die Verschlüsselung von Daten oder Software ist heute ein integraler Bestandteil vieler Systeme und Produkte. Dabei können unterschiedliche Bedrohungsszenarien auftreten.

- Haben Sie Messgeräte oder andere Komponenten, die über ein Datennetz erreichbar sind. Sind Sie sicher, dass dieses Netz vor fremden Angriffen geschützt ist?
- Möchten Sie Ihre Firmware und Hardware vor fremden Modifikationen schützen?
- Möchten Sie neugierige Konkurrenten davon abhalten, Ihr Produkt zu kopieren?
- Möchten Sie kryptographisch abgesicherte Komponenten verwenden und wissen nicht, wie Sie die Schlüsselverteilung managen wollen?
- Möchten Sie für Ihre Komponenten eine Fernwartung erlauben, diese aber trotzdem vor unberechtigtem Eingriff schützen?

Auf diese und weitere Fragen haben unsere Experten Antworten. Ihre individuelle Lösung wird in enger Zusammenarbeit mit Ihnen erarbeitet.

Unsere Security-Spezialisten verfügen über folgendes Know-how:

- Risikoanalysen
- Erstellen von individuellen Sicherheitskonzepten
- Entwickeln von Applikationen für Krypto-Controller
- Entwickeln von sicherheitskritischen Client-Serverapplikationen
- Sicherheitslösungen für embedded Software

Gemeinsam mit Ihnen erstellen unsere Experten eine Risikoanalyse und ein auf Ihre Bedürfnisse angepasstes Sicherheitskonzept. Ausgehend von diesem Konzept werden anschliessend die gewünschten Sicherheitskomponenten in Form von Tools und Applikationen für Smart-Cards und speziellen Krypto-Controller, aber auch in Form von spezifischen Client-Serverapplikationen zur Verfügung gestellt.

Gerne stellen wir Ihnen einige Projekte vor, die unter massgeblicher Mitwirkung von Albis-Security-Spezialisten durchgeführt wurden.

LSVA

Für die Umsetzung der leistungsabhängigen Schwerverkehrsabgabe (LSVA) durch die Oberzolldirektion (OZD) wurden wichtige Sicherheitskomponenten durch Albis realisiert:

- Bereitstellen einer Certificate Authority (CA),
- Bereitstellung von hochverfügbaren, hochsicheren Zertifikaten und Zertifikatsverzeichnissen,
- Online-Zugriff auf sichere Speicher in Smart-Cards und Geräten (On-Board Units) durch spezielle Client-APIs.

In enger Zusammenarbeit mit der OZD wurde das Sicherheitskonzept definitiv festgelegt und die benötigten Crypto-APIs und Client-Serverapplikationen entwickelt.



Qualifizierte Signatur

Das neue Signaturgesetz erlaubt in der Schweiz ein hohes Einsparpotential durch das Verwenden von rechtlich verbindlichen Dokumenten in digitaler Form. Lösungsanbieter für die sogenannte Qualifizierte Signatur müssen dabei auf einen zertifizierten Prozess zur eindeutigen Erfassung der Identität verweisen können. Es muss garantiert sein, dass nur die betreffende Person im Besitz des zugehörigen Schlüsselmaterials ist.



Auch die Schweizerische Post setzt dabei in ihrer USB-Stick-Lösung mit SIM-Karte auf eine Siemens SmartCard mit zertifizierter Applikation. Die entsprechenden Initialisierungstools wurden durch Albis Technologies entwickelt und bereitgestellt.

EasyAccess

EasyAccess bietet Generalabonnement-Komfort für die Kunden von öffentlichen Verkehrsmitteln. Ohne zusätzliche Bedienung erlaubt das innovative, auf einer aktiven Chipkarte basierte Verfahren, eine automatische Abrechnung von Fahrdienstleistungen. Dabei werden die für den Kunden optimalen Rabatte automatisch berücksichtigt.

Im Rahmen eines Pilotprojektes ist in Dresden mit rund 3000 Fahrgästen ein sehr erfolgreicher Praxistest durchgeführt worden.

Basierend auf einer detaillierten Bedrohungsanalyse wurde für dieses Innovationsprojekt ein neues Sicherheitskonzept erarbeitet und in das deutsche Normierungsgremium des Vereins Deutscher Verkehrsunternehmen eingebracht. Damit wurde die Interoperabilität zwischen unterschiedlichen Städte-Regionen sichergestellt.

Eine erste «Light-Version» des erarbeiteten Grundkonzeptes wurde von Albis entwickelt und als Applikation im Security-Access-Modul (SAM) des Lesers und im Krypto-Controller des aktiven Tickets realisiert.

Update von embedded Software

Die Funktionalität und der Umfang von embedded Software haben in den letzten Jahren enorm zugenommen. Viele der embedded Produkte werden für Software-Updates mit dem Internet verbunden. Entsprechend sind die Gefahren gewachsen, denen diese Software ausgesetzt ist:

- Die Hardware wird zweckentfremdet, indem ein Open-Source-Betriebssystem geladen werden kann.
- Sicherheitsfunktionen in der Software werden umgangen oder imitiert.
- Falsche Software-Versionen werden auf die Hardware geladen und belasten den Service.

Albis hat Lösungen realisiert, die vor diesen Gefahren schützen, indem Software-Updates mit Schlüsseln versehen werden. Dieses Verfahren wurde zum Beispiel für Set Top Boxen und einen Digital Music Player implementiert.

Diese Projektbeispiele zeigen die umfangreiche Kompetenz unserer Spezialisten in der Entwicklung von Sicherheitslösungen. Wir würden uns freuen, dieses Know-how auch Ihnen zur Verfügung zu stellen.

Weitere Informationen

Für weitere Informationen kontaktieren Sie:
Telefon +41 58 252 47 77
development@albistechnologies.com

Albis Technologies Ltd
Albisriederstrasse 199
CH-8047 Zürich
Phone +41 58 252 4777
Fax +41 58 252 4778
www.albistechnologies.com