

Mit der zunehmenden Bedeutung des Internets werden auch die Sicherheitsaspekte in offenen Netzen immer wichtiger. Dabei sollen einerseits Daten vor unberechtigter Einsicht geschützt werden, andererseits müssen Kommunikationsteilnehmer eindeutig identifiziert werden.

Eine Public Key Infrastruktur (PKI) ist ein wesentlicher Baustein in einem Sicherheitskonzept. Die PKI dient der Erstellung und Verwaltung von Sicherheitstokens („Smartcards“ und PKCS#11/12), von X.509 Zertifikaten und CRLs (Certificate Revocation List).

Im Rahmen der Entwicklung einer Public Key Infrastruktur waren wir zuständig für die technische Projektleitung sowie für die Systemarchitektur. Zusätzlich haben wir die zur eindeutigen Benutzererkennung benötigten Zertifikate und die zugehörige Auswertlogik realisiert. Dabei wurden Standards für einheitliche Zertifikate wie ITU-X.509 implementiert.

Modellierung nach RUP/UML, realisiert in C++/MFC.

Für einen Kunden im Sicherheitsbereich haben wir eine Applikation zur sicheren Ablage von Dateien auf einem Einzelrechner und im Netzwerk entwickelt. Höchste Priorität wurde dabei auf eine einfache und intuitive Benutzeroberfläche bei gleichzeitig hoher kryptographischer Sicherheit gelegt. Das Produkt integriert sich nahtlos in die Betriebssystemoberfläche. Die Verschlüsselung erfolgt transparent und bleibt damit für den Benutzer unsichtbar. Für Benutzergruppen oder für Einzelbenutzer können sichere Dateiablagen angelegt werden.

Modellierung nach UML, realisiert in C++/MFC.

Unsere Arbeit umfasste Projektleitung, Analyse, Design und Realisierung des Projekts.

