Gennadi Wilgelmi, Entwicklungsleiter, wilgelmi@soft-xpansion.com

soft Xpansion GmbH & Co.KG, www.soft-xpansion.de

SMARTCARDS UND IHRE VERWENDUNG IN DER ZWEI-FAKTOREN-AUTHENTIFIZIERUNG

ALLGEMEINES

Smartcards sind kleine, transportable, in eine Kunststoffkarte eingebettete Computer. Auf der Karte können vertrauliche Informationen gespeichert und wirksam vor unbefugtem Zugriff geschützt werden: die im Mikrochip der Karte gespeicherten Daten sind durch Hacker nur mit relativ hohem Aufwand auszulesen, da kein einfacher Zugriff von außen auf den Kartenspeicher möglich ist, im Gegensatz zum Zugriff z. B. auf die Festplatten eines PCs. Die Größe von Smartcards ist durch den Standard ISO/IEC 7816 (Teile 1 bis 6) normiert. Weit verbreitet sind rechteckige Karten mit folgenden Maßen: 85,6 mm Breite, 53,98 mm Höhe und 0,76 mm Dicke (Scheckkartenformat, Format ID-1).

Der in die Smartcards integrierte Mikrochip enthält

- ✓ **einen Mikroprozessor** - gewöhnlich 8-bit, obwohl auch Modelle mit 32-bit- Prozessoren existieren
- ✓ **Speicher** - die Smartcard besteht speicherseitig aus einem reinen Lesespeicher (ROM), in dem sich das Betriebssystem der Karte befindet, sowie einem NVM-Speicher (Nonvolatile Memory), in den auch geschrieben werden kann. Neben dem ROM-Speicher gibt es noch einen kleinen RAM-Speicher als Arbeitsspeicher u. a. für die Ausführung der Ver- und Entschlüsselung
- ✓ **Eingabe/Ausgabe-Einheit** (I/O-Unit)

Die Smartcard ist aber durch die rein physischen Zugriffsbeschränkungen nicht nur ein geschützter Speicherort für Daten, sondern sie gewährleistet auch den Schutz der mit den Daten durchgeführten Berechnungen, da diese auf der Karte selbst durchgeführt werden (z.B. Ver-/Entschlüsselung oder Berechnung von digitalen Unterschriften). So wird verhindert, dass ein Angreifer die digitale Unterschrift oder entschlüsselte Daten bei deren Versand von der Karte zum Computer bzw. in dessen Speicher abfangen und missbräuchlich verwenden kann.

Um Zugriff auf die auf der Karte geschützten Daten und die damit möglichen Operationen zu erhalten, muss der Besitzer sich als Berechtigter legitimieren. Dies erfolgt durch die Eingabe einer üblicherweise vier- bis achtstelligen PIN. Die Eingabe kann über ein Eingabemodul am Kartenlesegerät oder über die PC-Tastatur erfolgen. Der Vorteil der ersten Alternative liegt darin, dass in diesem Fall die PIN nicht in den Speicher des PCs gelangt, was ihr Abfangen durch nicht berechtigte Personen erschwert.

Die eingegebene PIN wird mit einem Referenzcode verglichen, der in einem besonders geschützten Bereich auf der Karte abgelegt ist. Dabei werden die meisten Karten nach mehr als drei fehlerhaften Eingabeversuchen gesperrt, um die Ermittlung der PIN durch „Probieren“ zu verhindern.

Wenn die Authentifizierung hardwaregestützt erfolgen soll, können neben Smartcard-Lesegeräten auch USB-Tokens verwendet werden, die an die USB-Schnittstelle des Computers angeschlossen werden und somit keine zusätzliche Kartenlese-Hardware erfordern. Sie erfüllen dieselben Funktionen und verfügen mit Blick auf den Schutz der mit ihnen durchgeführten Berechungen über dieselben Charakteristika wie Smartcards, verfügen aber über eine höhere geographische Portabilität und können auch in der Anschaffung preiswerter sein.

PRAKTISCHE ANWENDUNGSBEREICHE VON SMARTCARDS

Smartcards können als ein Element der so genannten Zwei-Faktor-Authentifizierung eingesetzt werden. Anders als bei der einfachen Zugriffskontrolle über Benutzername und Kennwort wird bei der stärkeren Kontrolle durch eine Zwei-Faktor-Authentifizierung (z. B. Smartcards kombiniert mit Geräten zur Erzeugung von Kennwörtern oder mit dem Fingerabdruck des Berechtigten) ein besserer Schutz erreicht. Mögliche Einsatzbereiche sind:

- ✓ Geschützter Zugang zu Windows
- ✓ Authentifizierung im Unternehmensnetzwerk
- ✓ Authentifizierung in unternehmenseigenen Applikationen und Web-Portalen
- ✓ Vertraulichkeit und Integrität der elektronischen Korrespondenz
- ✓ Einführung der digitalen Unterschrift in unternehmensinternen Dokumentenmanagement-Systemen
- ✓ Besonders geschützte Aufbewahrung von vertraulichen Daten
- ✓ Geschützter Zugriff auf unternehmensweite Netzwerkressourcen durch eine VPN-Verbindung
- ✓ Erhöhung der Sicherheit in der drahtlosen Kommunikation (Wi-Fi)

DIE VERWENDUNG VON SMARTCARDS AM BEISPIEL VON KREDITVERGABEPROZESSEN

SITUATION & VORAUSSETZUNGEN

Die kritische Schlüsselstelle in computergestützten Kreditvergabeprozessen ist die Benutzer-Authentifizierung. Vor allem Schnellkredite werden heute häufig über internetbasierte Online-Plattformen verwaltet, für die nur eine klassische Ein-Faktor-Authentifizierung mittels Kennwort vorgesehen ist. Bekanntermaßen droht bei dieser Form der Anmeldung am System Gefahr durch Password-Phishing oder Keylogging. Da zudem bei dieser Form der der Ein-Faktor-Authentifizierung sehr genau darauf geachtet werden muss, dass man ausreichend komplexe, nicht leicht zu ermittelnde Kennwörter verwendet und dass man diese regelmäßig ändert, können mit lediglich einem solchen Faktor geschützte Systeme nur als wenig sicher bezeichnet werden.

Darüber hinaus kann in Standard-WebClient-Lösungen (z.B. WebTop für die Documentum-Plattform) nicht verhindert werden, dass zwei oder mehrere Benutzer dieselben Authentifizierungsparameter verwenden. Aus den genannten Gründen ist in computergestützten Kreditvergabeprozessen die Zwei-Faktor-Authentifizierung unter Verwendung von Hardwareschlüsseln gegenüber der Ein-Faktor-Authentifizierung vorzuziehen.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG IN KREDITVERGABEPROZESSEN AUF BASIS VON THIN-CLIENT-TECHNOLOGIE

Die Authentifizierung in Kreditvergabesystem-Applikationen erfolgt in der Regel nach einem einfachen, standardisierten WebClient-Mechanismus: der Benutzer gibt seinen Namen und das

Kennwort ein, danach werden diese Daten dem Web Server übergeben, der die übergebenen Parameter für den Aufruf der Sitzung mit dem Content Server verwendet. Wie bereits erläutert ist dieses Verfahren nicht sicher genug und relativ aufwändig zu verwalten. Durch Einsatz eines Hardwareschlüssels kann die Sicherheit der Authentifizierung hingegen deutlich erhöht werden:

> jeder Benutzer des Systems erhält bei der Zwei-Faktor-Authentifizierung eine Smartcard, auf der sich ein oder mehrere Zertifikate befinden. Das Zertifikat kann von einer dafür zuständigen Stelle (Zertifizierungsstelle, Certificate Authority oder kurz CA) ausgestellt oder selber erstellt werden. Diese gibt es sowohl für Windows- als auch UNIX (Linux)-Plattformen.

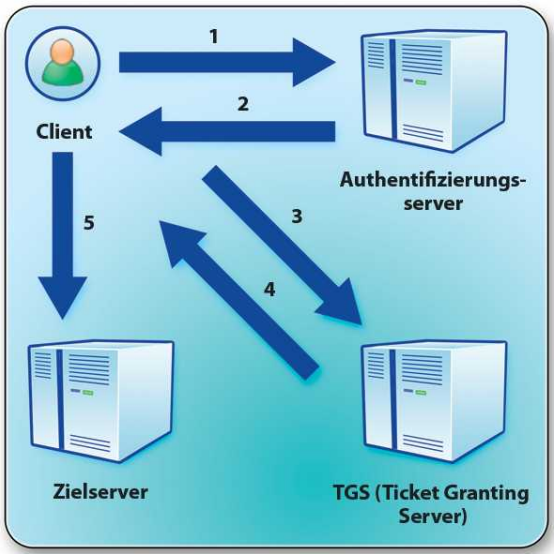
Das einfachste Verfahren zur Implementierung der Zwei-Faktor-Authentifizierung in Systeme, die auf der Thin-Client-Technologie basieren, ist die Verwendung von SSL (Secure Sockets Layer)-Netzwerkprotokollen. Das SSL-Verschlüsselungsprotokoll ist relativ einfach zu verstehen: es werden Algorithmen und Schlüssel auf Client- und Serverseite verwendet, sowie ein verschlüsselter Tunnel für die Übergabe der Daten gemäß anderer Protokolle, z.B. HTTP. Optional bietet SSL die Möglichkeit einer beidseitigen Authentifizierung über Zertifikate. SSL wird von den meisten Application Servern als Authentifizierungsmethode und auch von Web-Browsern unterstützt.

Die schrittweise erfolgende Verbindung zwischen dem Client (in der Regel WebClient) und dem Server (in der Regel WebServer) läuft wie folgt ab:

Dabei wird der private Schlüssel des Clients, der bei der Signierung Verwendung findet, auf der Smartcard abgelegt. Dieser Schlüssel verlässt zu keinem Zeitpunkt die Karte, die Signierung findet auf der Smartcard selbst statt und auch die Verschlüsselung erfolgt durch den Prozessor der Karte. Der Zugriff auf den privaten Schlüssel wird erst nach Eingabe der PIN möglich.

Nach dem Handshake haben sich der Client und der Server gegenseitig authentifiziert.

Eine andere Methode ist die Authentifizierung nach dem Kerberos-Protokoll – siehe das folgende Schema:



Auch dieses Protokoll erlaubt eine gegenseitige Authentifizierung zwischen dem Server und dem Client. Die Option PKINIT dient der Authentifizierung über ein digitales Zertifikat, das im Kartenspeicher abgelegt wird. Im Rahmen des gesicherten Austauschs von Meldungen bei einer Authentifizierung führt der Anwender die Signierung mithilfe seines privaten Schlüssels aus. Der Schlüssel liegt ebenfalls im geschützten Kartenspeicher.

Außerdem kann ein eigenes Authentifizierungsschema als ein "Request/Reply"-Modell realisiert werden:

Die Protokollfamilie, die ein "Request/Reply"-Modell verwendet, enthält einige Protokolle, die die Authentifizierung erlauben, ohne dass Daten über das Netzwerk übertragen werden müssen. Hierzu zählt zum Beispiel das CHAP (Challenge-Handshake Authentification Protocol) – ein weit verbreitetes Protokoll.

Der Verschlüsselungsvorgang wird auf der Anwenderseite auf einer Karte ausgeführt und es ist die Eingabe einer PIN erforderlich. Auch hier sind nach dem Beenden des Vorgangs der Client und der Server gegeneinander authentifiziert.

GLOSSAR

Begriff	Definition
Authentifizierung	Überprüfung der Zugriffs- oder Zugangsberechtigung eines Benutzers durch seine Identifizierung, im einfachsten Fall über einen Benutzernamen und ein Kennwort
Authentifizierungsfaktor	Eine Information oder ein Gerät, die im Rahmen der Authentifizierung erforderlich sind. Das kann ein charakteristisches Merkmal des Benutzers, ein Kennwort oder der Besitz eines Geräts sein, über das der Identitätsnachweis erfolgt (z. B. Smartcard).
Ein-Faktor-Authentifizierung	Die Identität wird hier anhand nur eines Faktors überprüft. Als Musterbeispiel für eine solche Authentifizierung gilt die einfache Kennworteingabe bei Anmeldung an einem geschützten System, aber auch biometrische Verfahren (Überprüfung des Fingerabdrucks oder Irisprüfung) zählen hierzu.
Zwei-Faktor-Authentifizierung	Die Identität wird hier anhand von zwei Faktoren überprüft. Dies kann die Verwendung von Smartcards zusammen mit der Eingabe einer PIN oder mit einem biometrischen Verfahren sein.
Autorisierung	Die Einräumung bestimmter (Zugriffs-) Rechte nach erfolgreicher Authentifizierung
Digitales Zertifikat	Ein digitales Dokument, das die Richtigkeit der Zuordnung eines öffentlichen Schlüssels zu seinem Besitzer bescheinigt, also den Besitzer identifiziert. Das Dokument enthält bestimmte, digital unterzeichnete Informationen über den Besitzer des Schlüssels, über den öffentlichen Schlüssel selbst, seinen Zweck und ein Gültigkeitsdatum.
Smartcard	Eine Kunststoffkarte, die einen elektronischen Speicher, u.a. für Schlüssel und digitale Zertifikate, sowie einen Mikrocomputer enthält.
PIN (Personal Identification Number, Persönliche Identifikationsnummer)	Zeichenfolge, mit der man sich gegenüber einem geschützten System identifiziert und mit dem man Zugang zu dem System erlangt.
Privater Schlüssel	In der Kryptologie ein Schlüssel, der nur seinem berechtigten Besitzer bekannt sein darf und somit das Gegenstück zum → öffentlichen Schlüssel bildet.
Öffentlicher Schlüssel	In der Kryptologie ein Schlüssel, der allgemein bekannt sein darf und somit das Gegenstück zum → privaten Schlüssel bildet.
Händedruck (handshake)	Eine gegenseitige Prüfung der Teilnehmer im Rahmen der elektronischen Kommunikation, z. B. zwischen Server und Client (der Server prüft die Echtheit des Client und umgekehrt).
USB-Token	Alternative zur SmartCard. Wird an die USB-Schnittstelle des Computers angeschlossen und erfordert somit keine zusätzliche Kartenlese-Hardware. Verfügt über eine höhere geographische Portabilität und kann auch in der Anschaffung preiswerter sein.
Verschlüsselung mit öffentlichem Schlüssel	Bei diesem Verschlüsselungsverfahren werden Daten mit einem Paar aus privatem und öffentlichem Schlüssel ver- und entschlüsselt. Daten, die mit dem öffentlichen Schlüssel chiffriert sind, kann man nur mit Hilfe des privaten und mit den Daten verbundenen Schlüssels entschlüsseln. Umgekehrt kann die Authentizität von Daten und Mitteilungen, die mit dem privaten Schlüssel unterschrieben sind, mit Hilfe des öffentlichen Schlüssels verifiziert werden.
Verschlüsselung mit geheimem Schlüssel	Bei diesem Verschlüsselungstyp wird für die Datenver- und entschlüsselung ein und derselbe, von den Beteiligten gemeinsam verwendeter geheimen Schlüssel eingesetzt

Digitale Unterschrift / Signatur	Die digitale Signatur erfüllt bei in elektronischer Form vorliegenden Daten und Dokumenten denselben Zweck wie eine eigenhändige Unterschrift auf Papier. Technisch gesehen handelt es sich um einen Zahlenwert, der aus den signierten Daten/Dokumenten und dem geheimen Schlüssel des Absenders errechnet und mit dem öffentlichen Schlüssel überprüft wird. Die Signatur bestätigt die Identität des Verfassers und die Integrität der Daten/des Dokuments.
Cryptographic Service Provider (CSP)	Ein unabhängiges Modul einer Sicherheitslösung, das eine Bibliothek von kryptografischen Funktionen mit einem standardisierten Interface enthält. Der CSP ist für die Realisierung der Interface-Funktionen verantwortlich. Über ihn wird auch der Zugriff auf alle Schlüsseltypen gesteuert.