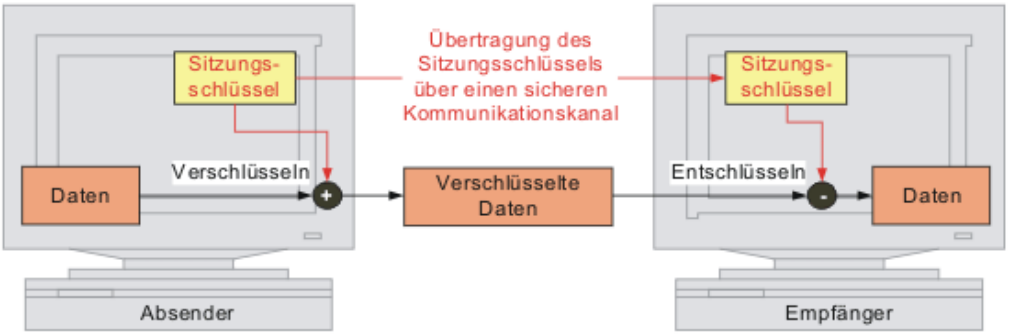
Für die Gewährleistung der Sicherheit in sensiblen Bereichen müssen kryptographische Verfahren (Verschlüsselung zur Verbesserung der Vertraulichkeit oder digitale Signatur zur Sicherstellung der Integrität) eingesetzt werden.
Im Folgenden wird ein kurzer Überblick über die etablierten kryptographischen Verfahren gegeben. Bei der Auswahl ist darauf zu achten, dass nur bekannte und verifizierte Verfahren genutzt werden.

1. Symmetrische Verschlüsselung

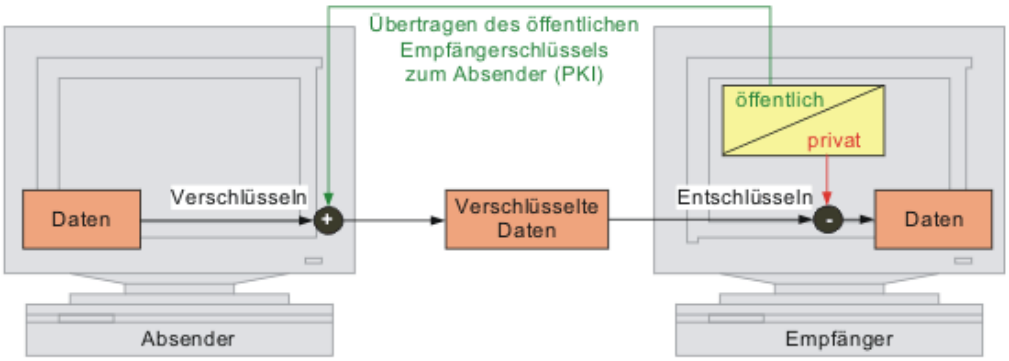
Bei symmetrischen Verfahren müssen alle Partner den gleichen Schlüssel (Sitzungsschlüssel) nutzen. Zum Verschlüsseln werden die Daten mit Hilfe eines umkehrbaren mathematischen Algorithmus mit dem Sitzungsschlüssel verschlüsselt. Aus den verschlüsselten Daten sind die ursprünglichen Daten oder der Sitzungsschlüssel nur mit sehr großem Aufwand ermittelbar.
Beim Empfänger wird der umgekehrte mathematische Algorithmus zum Entschlüsseln genutzt.



Vorteile	• Algorithmen für symmetrische Verschlüsselung sind unkompliziert. Sie erfordern wenig Rechenzeit (schnell, geringe CPU-Last) und eignen sich somit zum Übertragen großer Datenmengen.
Probleme	• Der Schlüssel muss sowohl dem Absender, als auch dem Empfänger der Daten bekannt sein. Deshalb muss er durch einen gesicherten Kommunikationskanal (z.B. persönlich oder per Telefon) übertragen werden. • Die Sicherheit ist vom Algorithmus und von der Schlüssellänge abhängig. • Bei einer Vielzahl von Partnern sind Schlüsselverteilung und vor allem Schlüsselwechsel manuell nicht realisierbar.
Verschlüsselungs-Algorithmen	Stromchiffre: RC4 (gilt als unsicher) Blockchiffre: DES (gilt als unsicher), 3DES, CAST, IDEA, Blowfish, AES/Rijndael (wird empfohlen)

2. Unsymmetrische Verschlüsselung

Um das Problem des Schlüsselaustausches zu umgehen, wurden unsymmetrische Verfahren entwickelt. Bei diesen wird ein zueinander passendes Schlüsselpaar erzeugt und jeweils ein Schlüssel als privat und der andere als öffentlich deklariert.
Die eingesetzten mathematischen Algorithmen stellen sicher, dass Daten, die mit dem öffentlichen Schlüssel verschlüsselt werden, nur noch mit dem Privatschlüssel entschlüsselt werden können.



Vorteile	Es müssen keine geheimen Schlüssel übertragen werden.
Probleme	• Der öffentliche Schlüssel des Empfängers muss zum Absender übertragen werden. • Dafür wird eine Infrastruktur benötigt (Infrastruktur zur Übertragung öffentlicher Schlüssel = Public Key Infrastructure = PKI) • Der öffentliche Schlüssel darf während der Übertragung nicht verfälscht werden. • Der Privatschlüssel sollte möglichst gut gesichert werden. Dafür gibt es die Varianten: - Speicherung im Benutzerprofil - Speicherung im Benutzerprofil und Sicherung mit einem Kennwort - Speicherung auf einem Wechseldatenträger - Speicherung auf einer Smartcard, die per PIN geschützt ist
Verschlüsselungs-Algorithmen bzw. Schlüsselaustausch-verfahren	El-Gamal, RSA Diffie Hellman, ECDH

3. Hashwertverfahren

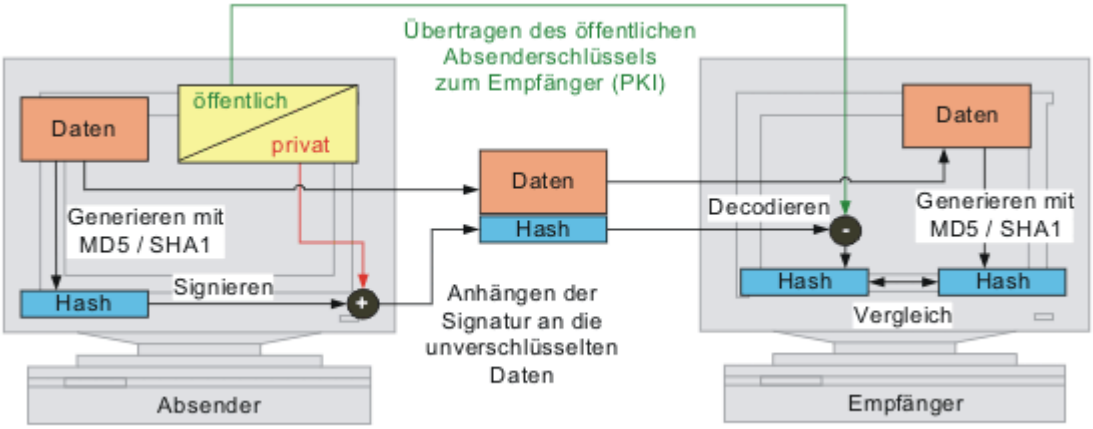
Ein Hashwertverfahren ist ein mathematischer Algorithmus, der aus einem beliebig langen Datenstrom eine Kurzform mit fester Länge berechnet. (engl. to hash = zerhacken). Ein Hashcode wird meist in hexadezimaler Form dargestellt. Dieser Hashwert wird oft auch als Fingerabdruck oder Prüfsumme bezeichnet und muss folgende Eigenschaften besitzen:

- **Einwegfunktion**: Aus dem Hashwert darf nicht der originale Inhalt erzeugt werden können.
- **Kollisionssicherheit:** Aus unterschiedlichen Texten darf nicht der gleiche Hashwert erzeugt werden.
- **Schnelligkeit:** Das Verfahren zur Hashwertberechnung muss schnell sein.

Vorteile	Kennwörter und Prüfsummen können in Form von Hash-Werten einfach übermittelt werden
Anwendung	• Prüfsummen für die digitale Signatur (z.B. für Zertifikate) • Übertragen oder Speichern von Passwörtern (z.B. CHAP, MSCHAP, Passwortspeicher bei Online-Diensten…)
Probleme	Sog. „Regenbogentabellen“ bieten Listen mit Hashwerten für eine Vielzahl von Wörtern an – veraltete Algorithmen vermeiden.
Hash-Algorithmen	SHA1, MD4 und MD5 (veraltet), SHA256, SHA512, GOST, Whirlpool

4. Digitale Signatur

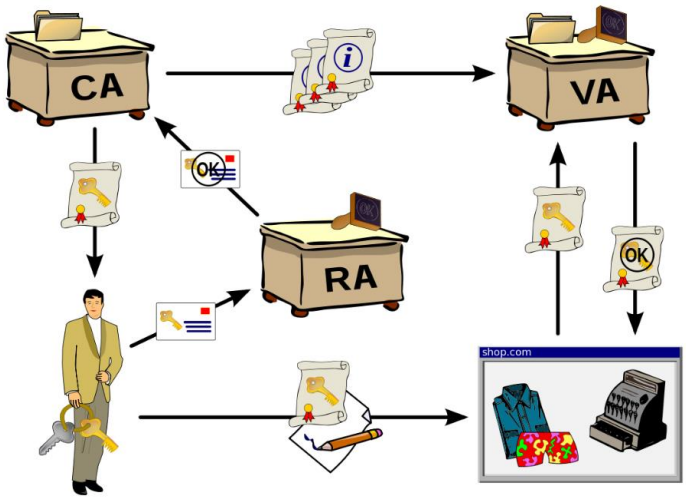
Bei der digitalen Signatur wird das Verfahren der unsymmetrischen Verschlüsselung "umgedreht". Um die Unverfälschbarkeit der Daten zu garantieren, wird ein Hash (Prüfsumme) gebildet. Dieser ändert sich sehr stark, auch wenn an den Daten nur eine kleine Änderung vorgenommen wurde. So soll eine Manipulation an den Daten ausgeschlossen werden.
Der Hash wird mit dem Privatschlüssel des Absenders verschlüsselt und das Ergebnis an die Daten als Signatur angehängt.
Der Empfänger berechnet ebenfalls den Hash. Er vergleicht diesen mit der entschlüsselten Signatur. Bei Übereinstimmung wurde die Nachricht nicht verändert.
Signieren kann nur der Besitzer des Privatschlüssels, also ist die Nachricht unverfälscht und stammt wirklich vom Absender.



Vorteile	▪Die Signatur stellt die einzige Möglichkeit dar, Informationen unverfälscht zu übertragen. Somit muss sie Bestandteil einer PKI sein, da nur so öffentliche Schlüssel sicher übertragen werden können.
Probleme	▪Die Übertragung des öffentlichen Schlüssels muss fälschungssicher erfolgen (z.B. durch Hinterlegung als "vertrauenswürdige Stammzertifizierungsstelle"). ▪Für "fortgeschrittene" und "qualifizierte" Signaturen nach dem Signaturgesetz muss das Zertifikat einer natürlichen Person zugewiesen werden.
Hash-Algorithmen	MD5, SHA1, SHA256

Komponenten einer PKI

Zertifizierungsstelle (Certification Authority, CA):
Die Zertifizierungsstelle signiert mit ihrem Schlüssel die öffentlichen Schlüssel von Benutzern, Diensten oder Computern. Dadurch wird aus dem öffentlichen Schlüssel ein digitales Zertifikat. Je nach Anwendungsfall kann eine fremde (kommerzielle) oder eine eigene CA genutzt werden.



Registrierungsstelle (Registration Authority, RA):
Organisation, bei der Personen, Maschinen oder auch untergeordnete Zertifizierungsstellen Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag, der dann durch die Zertifizierungsstelle signiert wird. Bei einer manuellen Prüfung wird diese durch den Registration Authority Officer durchgeführt.

Zertifikat-Sperrliste (Certificate Revocation List; CRL):
Wenn ein Schlüssel kompromittiert wird, muss das zugehörige Zertifikat gesperrt werden. Die gesperrten Zertifikate werden regelmäßig in der CRL veröffentlicht. Als Veröffentlichungspunkt eignet sich das Active Directory (ldap:), eine Web-Freigabe (http:), eine Dateifreigabe (file:) oder ein FTP-Pfad (ftp:). Im Zertifikat wird der Veröffentlichungspunkt hinterlegt, so dass eine Applikation die Gültigkeit prüfen kann. Diese Gültigkeitsprüfung ist optional und je Applikation konfigurierbar. Im Internet Explorer findet man die Option unter Extras -> Internetoptionen -> Erweitert -> Sicherheit.

Verzeichnisdienst:
Aus dem Directory können die öffentlichen Schlüssel durch die Client- oder Server-Applikation ausgelesen werden. Dies ist besondere bei verschlüsselten E-Mails wichtig, da hier der Absender den öffentlichen Schlüssel des Empfängers benötigt.
Als Directory eignen sich LDAP-Verzeichnisse, wie z.B. das Active Directory (AD). Eine AD-integrierte CA speichert alle ausgestellten Zertifikate als Eigenschaft des jeweiligen AD-Objektes. Diese werden unter "Active Directory Benutzer und Computer" in der erweiterten Ansicht beim Benutzerobjekt gezeigt.

Für welche Applikationen benötige ich eine PKI?

- EFS (Encrypted File System) für Verschlüsselung von Daten auf Festplatten
- HTTPS
- IPSec für VPN-Tunnel
- Wireless LAN mit WPA-EAP (802.1X)
- Port-Authentifizierung bei Switches nach 802.1X
- E-Mail-Signatur
- E-Mail-Verschlüsselung
- Code-Signatur (Authenticode) für Makros, ActiveX-Controls, …