Security-Konzepte für die Medizintelematik

Fraunhofer IBMT Institut Biomedizinische Technik

Juli 2000

Sichere Übertragung vertraulicher Daten ist eine der Grundanforderungen nicht nur im medizinischen Bereich sondern in vielen Bereichen der Wirtschaft und des täglichen Lebens. Seit einigen Jahren sind deshalb Verfahren zur Verschlüsselung und digitalen Signatur elektronischer Dokumente Gegenstand von Forschung, Entwicklung, Politik und Gesetzgebung.

Kryptographie

Bei den kryptographischen Verfahren wird unterschieden zwischen solchen zur Sicherung der Authentizität der Daten, also des Nachweises der Unversehrtheit und der Autorenschaft, sowie Verfahren zum Schutz der Daten vor unberechtigtem Zugriff. Die digitale Signatur garantiert die Echtheit und Unversehrtheit elektronischer Dokumente, während Verschlüsselungsverfahren das Lesen der Daten für Unberechtigte unmöglich machen oder zumindest erheblich erschweren.

Verschlüsselung

Heute üblich sind sogenannte Hybrid-Verschlüsselungsverfahren, bei denen für einen Übertragungsvorgang ein einmaliger („Session"-) Schlüssel erzeugt wird, der zur symmetrischen Verschlüsselung des eigentlichen Dokuments dient. Dieser (zufällige) Schlüssel wird mit einem asymmetrischen Verfahren mit dem öffentlichen Schlüssel des Empfängers codiert und zusammen mit dem Dokument versandt. Der Empfänger kann dann mit seinem privaten Schlüssel zunächst den Session-Schlüssel ermitteln und mit diesem dann das Dokument selbst decodieren.

Digitale Signatur

Für die Sicherung der Unversehrtheit von Dokumenten wird über diese Daten eine Prüfsumme, der Hashwert erzeugt. Dieser Hashwert, der für den Inhalt des Dokumentes eindeutig ist, wird asymmetrisch mit dem persönlichen Schlüssel des Autors verschlüsselt und an das Dokument angefügt. Der verschlüsselte Kontrollwert kann jederzeit mit dem *öffentlichen* Schlüssel des Autors decodiert und mit dem aktuellen Hashwert des Dokuments verglichen werden.

Das Empfänger-Problem

Den heute üblichen Verschlüsselungsverfahren ist gemeinsam, daß sie die Kenntnis des Adressaten voraussetzen, da der zweite, asymmetrische Schritt der Verschlüsselung mit Hilfe von dessen öffentlichem Schlüssel erfolgt. Eine Reihe wichtiger Dokumente im medizinischen Alltag sind aber an keinen festen Adressaten gerichtet. Dazu zählen z.B. Rezept, Überweisung und einiges mehr. daraus ergibt sich das Problem der sogenannten „nicht adressierten Vertraulichkeit", bei dem erst *nach dem Versand* des Dokumentes durch den Patienten festgelegt wird, wer die Berechtigung zum Lesen des Dokumentes hat.

Das Transcoding-Konzept von **PaDok®**

Das Kryptographie-Konzept von **PaDok®** basiert auf einer Variation des Hybrid-Schlüssel-Verfahrens. Dabei wird der eigentliche Session-Schlüssel vor der symmetrischen Codierung „vor-verschlüsselt". Die Information über diese Vorverschlüsselung wird durch den Patienten zum Empfänger überbracht und ist in keiner Weise aus dem elektronisch übertragenen Dokument rekonstruierbar. Der übertragene, modifizierte Session-Schlüssel reicht somit nicht zur Decodierung des eigentlichen Dokuments aus. Diese Session-Schlüssel wird zunächst mit dem öffentlichen Schlüssel eines Kommunikationsservers codiert, der diesen Schlüssel innerhalb eines gesicherten Moduls hält. Im Moment der Anforderung des Dokumentes wird der (modifizierte) Session-Schlüssel mit dem öffentlichen Schlüssel des anfordernden Adressaten transcodiert. Dies geschieht innerhalb des gesicherten Transcoder-Moduls. Der eigentliche, verschlüsselte Datenblock bleibt davon unberührt. Auf der Seite des Empfängers kann dann der (modifizierte) Session-Schlüssel wieder rekonstruiert werden. Unter der Bedingung, daß der vom Patienten überbrachte „Vorgangs"-Schlüssel vorliegt, kann danach die „Vor-Verschlüsselung" des Session-Schlüssels aufgehoben und danach das eigentliche Dokument decodiert werden.

Kompatibilität

Das **PaDok®**-Transcoding-Verfahren setzt auf Standard-Verschlüsselungsverfahren auf. dadurch ist die Kompatibilität zu üblichen PKI (Public Key Infrastructures) gewährleistet. Die einzige Modifikation besteht in einem zusätzlichen Prozessschritt, der zwischen die beiden Komponenten der Hybrid-Verschlüsselung eingefügt wird.

Weitere Informationen:
Fraunhofer-Institut für Biomedizinische Technik
Arbeitsgruppe Medizin-Telematik,
Ressource Krytographie und Algorithmen
Dipl.-Ing. Frank Neurohr
Tel.: +49 (0) 6894 / 980 – 407
email: NeurohrF@ibmt.fhg.de

Fraunhofer Institut für Biomedizinische Technik
Arbeitsgruppe Medizin-Telematik
Leiter: B. Bresser
Telefon 06894 980 206
Telefax 06894 980 117
Mobil 0173 351 3322
e-Mail bertram.bresser@ibmt.fhg.de

Ensheimer Straße 48
D 66386 St. Ingbert

Zentrale:
Telefon 06894 980 0
Telefax 06894 980 400