Die neue ASAS-Version von «Health-Info-Net»

P. Ritzmann

Wiederholt haben wir auf das Problem der Datensicherheit beim elektronischen Datentransfer aufmerksam gemacht. Mittlerweile stehen verschiedene Verschlüsselungsprogramme auch für Private zur Verfügung, die nach dem Austausch von individuellen Schlüsseln eine verschlüsselte Kommunikation zwischen E-Mail-Sender und -Empfänger ermöglichen (siehe infomed-screen März 2001). Einen anderen Ansatz propagiert das schweizerische «Health-Info-Net» (HIN; http://www.hin.ch). Mit dem von HIN vertriebenen «Arpage Security and Access System» (ASAS) kann einerseits der Zugang zu geschlossenen Benutzergruppen auf dem Internet (z.B. HIN-Extranet-Plattform) kontrolliert werden. Andererseits ermöglicht ein sogenanntes «tunnelling» (Verschlüsselung der Internetverbindung) die Übermittlung chiffrierter Daten und das Identifizieren des Absenders.

Ein Nachteil besteht darin, dass damit ein sicherer Datenaustausch nur im geschlossenen Kreis der HIN-Abonnentinnen und -Abonnenten ermöglicht wird. Trotzdem hat ASAS in den letzten Jahren eine grosse Verbreitung unter den praktizierenden Ärztinnen und Ärzten in der Schweiz erfahren. Zwei Gründe tragen hauptsächlich dazu bei: Die FMH übernimmt für ihre Mitglieder die Kosten für das HIN-Basisabonnement (für die übrigen Abonnentlnnen CHF 15.–/Monat), damit wird die Benutzung von ASAS für die FMH-Mitglieder kostenlos. Zweitens wird heute von den Kostenträgern eine elektronische Vernetzung der Hausarztnetze gefordert. ASAS hat sich dabei als Quasi-Standard für die Verschlüsselung der elektronischen Übermittlung von Daten etabliert.

Im Gegensatz zu den älteren Versionen ermöglicht die heute verfügbare ASAS-Version 3.2 (download via http://www.hin.ch/asas) auch das End-zu-End-Verschlüsseln von E-Mails zwischen HIN-Mailboxen. Die verbesserte Sicherheit (die Daten können auch von HIN nicht mehr entschlüsselt werden) veranlasste beispielsweise das Kantonsspital Winterthur, für die zuweisenden Ärztinnen und Ärzte aus der Region die Übermittlung von persönlichen Daten mittels ASAS-verschlüsselten E-Mails freizugeben. Die Benutzung der End-zu-End-Verschlüsselung ist vergleichsweise einfach. Wenn die entsprechende Option aktiviert ist, werden beim Versenden einer Nachricht die öffentlichen Schlüssel der Angeschriebenen direkt vom HIN-Server bezogen.

Störend an der von HIN propagierten Lösung bleibt, dass für die Kommunikation ausserhalb von HIN andere Sicherheitslösungen benötigt werden. Ein weiterer Nachteil ist, dass es trotz einer Ankündigung im letzten Jahr keine ASAS-Version für die Macintosh-Plattform gibt. Mac-Benutzerinnen und -Benutzer müssen ASAS auch weiterhin auf einer Windows-Emulation installieren (z.B. Virtual PC; http://www.connectix.com).

Erschienen in «infomed-screen Nr. 2, Februar 2002, Jahrgang 6