



sic! Benutzerschnittstelle

Skalierbare Sicherheit

Im **Primary-Mode** wird der bekannte Diffie-Hellman Schlüsselaustausch mit einer Schlüssellänge von bis zu 2048 Bit verwendet.

Im **Advanced-Mode** wird das beweisbar sichere Schlüsselaustauschprotokoll PSKE verwendet. Es ist sicher gegen die stärksten aktiven Angriffe. Zum ersten Mal verfügt ein ISDN Verschlüsselungsgerät über ein Schlüsselaustauschverfahren, dessen Sicherheit formal bewiesen wurde. Dem Protokoll liegen das DSS-Signaturverfahren und das ElGamal Verfahren mit bis zu 4096 Bit Schlüssellängen zugrunde. Sichere Schlüsselaustauschverfahren benötigen Zertifikate, in denen die Korrektheit der übermittelten Langzeitschlüssel verifiziert werden kann.

Mit dem neuartigen IKEP-Verfahren zur Schlüsselauthentifizierung wird der übliche Zertifizierungsaufwand erheblich verringert: Der Anwender muss nicht mehr persönlich in einer Zertifizierungsstelle auftreten, sondern kann die Zertifikate über ISDN bequem von zu Hause durchführen - ohne wesentlich auf Sicherheit zu verzichten. Die Langzeitschlüssel werden im System generiert, so dass der geheime Teil niemals das Verschlüsselungsgerät verlässt.

Im **Authenticated Mode** wird zusätzlich eine Benutzer- bzw. Systemidentifizierung durchgeführt. Dies geschieht anhand einer Chipkarte zur Digitalen Signatur oder durch die Verifizierung des Schlüssels anhand eines Fingerprints. Dies kann wahlweise während der Verbindung durch Ablesen des am Telefon-Display angezeigten Fingerprints oder durch einen automatischen Abgleich mit zuvor gespeicherten Fingerprints geschehen.

Ein modernes Schlüsselmanagement realisiert die Konformität zu PGP und X.509v3-Zertifikaten.

