



# sic! User Interface

## Scaleable Security

The **primary mode** is based on the well-known Diffie-Hellman key exchange protocols and supports keys of up to 2048 bits.

The **advanced mode** is based on PSKE, an authenticated key exchange protocol based on DSS and ElGamal with keys of up to 4096 bits. The protocol is probably secure against passive as well as active attackers, a first for an ISDN encryption device!

Secure key exchange protocols require certificates to verify the correctness of established session keys. With **IKEP**, a novel method to authenticate keys, the usual certification effort is considerably reduced: The user doesn't have to appear in person at a registration authority but can register remotely over ISDN with ease and with only a small sacrifice in security. Long-term secrets are generated inside the sic! server and never leave the device.

The **authenticated mode** provides user and system identification. This is achieved using digital signatures and smartcards with certificates or the verification of public keys based on fingerprints. This happens during the connection setup either by reading out the fingerprint displayed on the telephone display or by automatic comparison with previously stored fingerprints.

A modern key management systems integrates conveniently with PGP and X.509v3 certificates.

