



# sic! server

## Problem

The communication infrastructure forms a fragile foundation of our information society. In particular, insufficient security on the information highway causes substantial financial damage to our economy due to industrial espionage. Therefore, it is essential to protect

sensitive information from unauthorized access or manipulation and to prevent severe consequences. Telephone and facsimile services on connection-oriented networks --- still the most widely deployed communication medium --- are particularly exposed to attacks.

## Solution

sic! server, the Secure ISDN Communication server developed by Sirrix AG, provides secure authentication and encryption concurrently on up to 24 B channels. In a user-friendly and easy manner, sic! server secures your communications and protects your assets from eavesdropping and manipulation by both passive and active attackers.

## Innovations

sic! server excels in particular in following aspects.:

- secure key exchange with reduced certification requirements
- novel symmetric cipher mode (OCFB) with considerable efficiency gain
- fulfillment of high security and efficiency needs
- verifiability and high assurance due to public system architecture

## Features

The hardware design permits encryption with minimal latency.

The **scalability** of the system allows the dynamic adaption to varying user needs in terms of key exchange and authentication:

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 provably 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 modern key management integrates nicely with PGP and X509v3..

## Technical Specification

### ISDN

2-12 ISDN basic access lines  
encryption of speech, facsimile and data  
2-24 B-channels  
DSS1-protocol (euro-ISDN)  
data delay < 250  $\mu$ s

### Symmetric Encryption

IDEA/AES with 128bit key  
one-time sessionkey  
self synchronizing mode of operation OCFB (Optimized Cipher Feedback)

### Asymmetric Schemes

Encryption: ElGamal (4096bit key),  
Cramer-Shoup optional

one-time asymmetric sessionkey  
Signature: Digital Signature Standard (DSS)  
key generator included in sic! server

### Key Exchange

Diffie-Hellman (2048bit key)  
Provable Secure Key Exchange Protocol (PSKE), adapted to X.509

### Key Authentication

efficient online certification (IKEP)  
online- and offline verification of public-keys

### User Authentication

fingerprint  
chip card/digital signature (X.509 key certificate)

### Processing Unit

CPU	DualPentium/800MHz
Kernel/OS	Linux
Interfaces	Ethernet 100BaseT 2 to 12 ISDN Ports

### Configurations

Basic	Security Server
Modules	1 to 6 cards with 4 ISDN-Ports each

Sirrix AG security technologies · Postfach 1652 · 66407 Homburg · Telefon: +49(0)681 301 409 90 · Telefax: +49(0)681 301 409 91  
post@sirrix-ag.de · <http://www.sirrix-ag.de>