## Einfache Handhabung mit Plug and Play

Das SECOM wird einfach zwischen ISDN-Anschluß und Endgerät geschaltet. Es verschlüsselt jeden B-Kanal und jede Richtung getrennt. Um eine sichere Verbindung herzustellen, ist ein gleiches Gerät bei der Gegenstelle zu installieren.

## Keine Schalter, keine Knöpfe

Das SECOM erkennt automatisch, ob sich auf der Gegenstelle ein funktionsgleiches Gerät befindet. Für den Benutzer ändert sich nichts. Eine sichere Verbindung wird den beiden Anwendern über eine Leuchtanzeige signalisiert.

## Anwendungsbeispiel

- Verschlüsselung von Telefongesprächen
- Sichere Datenübertragung
- Faxverschlüsselung
- Sichern von Videokonferenzen

## Einsatzmöglichkeiten

- Anschließbar am jeden ISDN $S_0$-Anschluß
- Sichere Kommunikation zwischen Telearbeitern und ihrer Firma
- Sichere Erweiterung von Firmennetzen

## Stromversorgung

- Über Telefonnetz bzw. externes Netzteil
- Geringe Leistungsaufnahme 3 W

## Verschlüsselung

- Getrennte Verschlüsselung der beiden B-Kanäle
- Getrennte Verschlüsselung für Hin- und Rückrichtung
- Hybridverfahren

  Asymmetrisch: RSA mit 1024 Bit Schlüssellänge

  Symmetrisch: Triple-DES mit 168 Bit Schlüssellänge
- Generierung des Sitzungsschlüssels für Triple-DES im Gerät


Institut für Angewandte
Mikroelektronik und Datentechnik
Richard-Wagner-Str. 31
18119 Rostock

# UNIVERSITÄT Rostock

Fachbereich Elektrotechnik und Informationstechnik
Institut für Angewandte Mikroelektronik u. Datentechnik
Richard-Wagner-Str. 31
18119 Rostock


# CeBit 2000 Exponat:
# Eine mobile Einrichtung zum Ver- und Entschlüsseln von ISDN-Datenströmen

**Das SECOM-Projekt**

**Se**cure **Com**munication over ISDN


**Ansprechpartner**

Prof. Dr. Dirk Timmermann
Dipl.-Ing. Mathias Schmalisch
Dipl.-Ing. Hagen Ploog
Tel.: 0381-498-3529
Fax: 0381-498-3601
E-Mail: md@e-technik.uni-rostock.de

**Kooperationspartner**

TAS Telefonbau A. Schwabe GmbH & Co KG
Dieter Fischer
Langmaar 25
41238 Mönchengladbach


**Internetadresse**

http://www-md.e-technik.uni-rostock.de

## Kurzbeschreibung

Mit Hinblick auf die voranschreitende Globalisierung der Wirtschaft und der Einführung von Telearbeitsplätzen nimmt der Informationsaustausch zwischen einzelnen Filialen einer Firma und deren Mitarbeitern ständig zu. Da diese Informationen über öffentliche Netze wie ISDN übertragen werden, steigt auch die Gefahr der Industriespionage. Bei Daten ist es kein Problem, diese mit gängigen Methoden vor der Übertragung zu verschlüsseln und auf der Empfängerseite wieder zu entschlüsseln. Anders sieht es allerdings bei Telefongesprächen, Telefaxen, Videokonferenzen oder ähnlichem aus, denn solche Informationen werden normalerweise unverschlüsselt über das ISDN übertragen und unterliegen gewissen Echtzeitanforderungen.

Um derartige Informationen zu sichern, ist es notwendig, die Nutzdaten des ISDN im laufenden Betrieb zu verschlüsseln. Wegen der Echtzeitbedingungen ist eine Hardwarelösung am besten geeignet. Mit dem SECOM wurde ein solches Gerät für die sichere Kommunikation über das ISDN entwickelt. Es wird zwischen dem eigentlichen Endgerät und dem ISDN-Anschluß eingefügt. Sobald eine Verbindung zu einem zweiten Endgerät hergestellt werden soll, versucht das SECOM auf der Gegenseite ein Partnergerät zu finden. Wenn diese Suche erfolgreich ist, wird ein Schlüsselaustausch durchgeführt und dann die eigentlichen Nutzdaten verschlüsselt übertragen. Falls bei der Suche kein SECOM auf der Gegenseite gefunden wurde, wird eine unverschlüsselte Verbindung aufgebaut. Der Zustand einer Verbindung, ob verschlüsselt oder unverschlüsselt, wird durch eine Leuchtanzeige dargestellt. Dadurch wird dem Nutzer signalisiert, ob eine sichere Verbindung zustande gekommen ist.

## Sicherheit für den Anwender

Das SECOM dient zum Schutz gegen folgende Bedrohungen

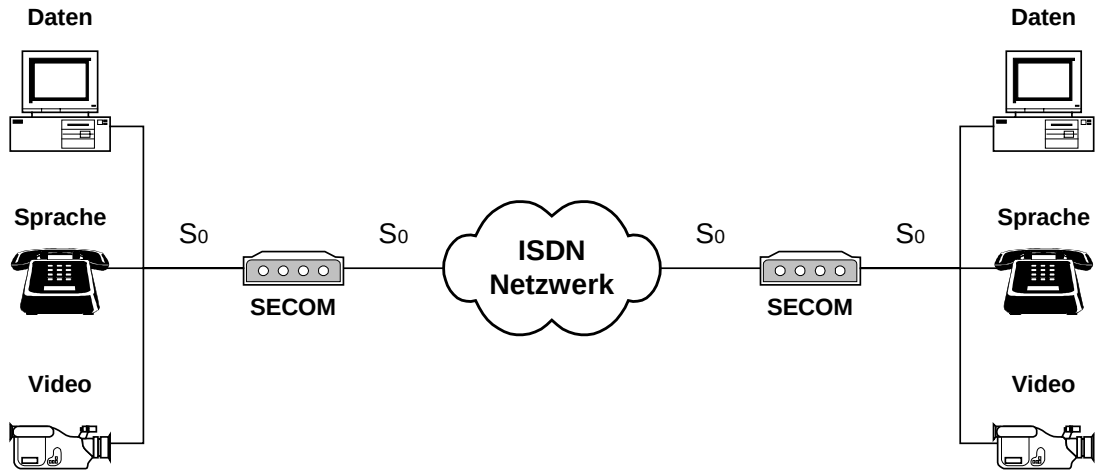
- Unbefugtem Zugriff auf Daten durch Abhören oder Aufzeichnen
- Unbemerktem Löschen von Teilen oder vollständigen Daten auf dem Übertragungskanal während einer Übertragung
- Unbemerkte Modifikation von Daten während einer Übertragung
- Unbefugte Kenntnisnahmen von Informationen durch beabsichtigte oder zufällige Fehlleitung
- Wiedereinspielen von schon übertragenen oder verfälschten Informationen in spätere Verbindungen
- Unbefugter Empfang bzw. Senden von Daten durch Vortäuschen einer falsche Identität
- Unbemerktes Einspeisen von Störkommandos in den Übertragungskanal

## Funktionsprinzip

Das SECOM arbeitet mit einen hybriden Verschlüsselungsverfahren. Dabei wird ein asymmetrischer Algorithmus verwendet, um den Sitzungsschlüssel an das SECOM auf der Gegenseite zu übertragen. Dieser Sitzungsschlüssel wird durch einen Zufallsgenerator im Gerät erzeugt. Das funktionsgleiche Gerät auf der Gegenseite erzeugt ebenfalls einen Sitzungsschlüssel und überträgt ihn. Dadurch wird für die beiden Richtungen jeweils ein anderer Sitzungsschlüssel verwendet, womit sich die Sicherheit erheblich erhöht. Der Sitzungsschlüssel wird für die Verschlüsselung der eigentlichen Nutzdaten auf dem B-Kanal verwendet. Für dieser Verschlüsselung wird ein symmetrischer Algorithmus eingesetzt. Da der Basisanschluß beim ISDN zwei B-Kanäle zur Verfügung stellt, können auch zwei gesicherte Verbindungen hergestellt werden. Dabei wird für jeden B-Kanal ein anderer Sitzungsschlüssel verwendet.

Verschlüsselt werden nur Daten, die über die B-Kanäle übertragen werden. Der D-Kanal wird transparent an das eigentliche Endgerät weitergereicht.

Da das SECOM beide B-Kanäle verschlüsselt und diese unabhängig voneinander sind, können diese für verschlüsselte Verbindungen mit zwei unterschiedlichen Partnern benutzt werden. Es ist auch möglich, beide B-Kanäle für eine Verbindung mit einem Partner einzusetzen, um so die Übertragungsrate zu erhöhen.




*Einsatzprinzip für das SECOM*