ELCRODAT 6-2

Sichere Sprach- und Datenkommunikation im Euro-ISDN

- High-End-Verschlüsselungssystem für Telefon-, Fax-, Daten- und Video-Kommunikation
- Online-Informationsübertragung von OFFEN bis STRENG GEHEIM
- Jeweils ein Modell für Euro-ISDN-Basisanschluss und Euro-ISDN-Primärmultiplexanschluss

ROHDE&SCHWARZ

Höchstmaß an Sicherheit im Euro-ISDN

Die moderne Informationsgesellschaft verlangt zunehmend schnelles Agieren und Reagieren. Der Austausch von höchst sensiblen Informationen über das öffentliche Netz ist deshalb unumgänglich.

Mit den technischen Möglichkeiten aber wächst die Gefahr von Lauschangriffen und Datendiebstahl, die so verursachten Schäden bewegen sich jährlich in Milliardenhöhe.

ELCRODAT 6-2, das High-End-Verschlüsselungssystem der neuesten Generation, überträgt zuverlässig Informationen bis zur VS-Stufe STRENG GEHEIM.

Es ist für alle ISDN-Basisdienste selbst über Satellitenstrecken (Inmarsat M4) einsetzbar, z.B. für

- Sprache
- Daten
- Fax (Gruppe 4)
- Videokonferenzen

Das Höchstmaß an Sicherheit wird mit einem Mindestmaß an Personal- und Verwaltungsaufwand realisiert.

Ein System – zwei Varianten

ELCRODAT 6-2 steht in zwei Varianten zur Verfügung:

- ELCRODAT 6-2 S für den sicheren Euro-ISDN-Basisanschluss (S_0-Bus/Port)
- ELCRODAT 6-2 M für den sicheren Euro-ISDN-Primärmultiplexanschluss (S_{2M}-Port).

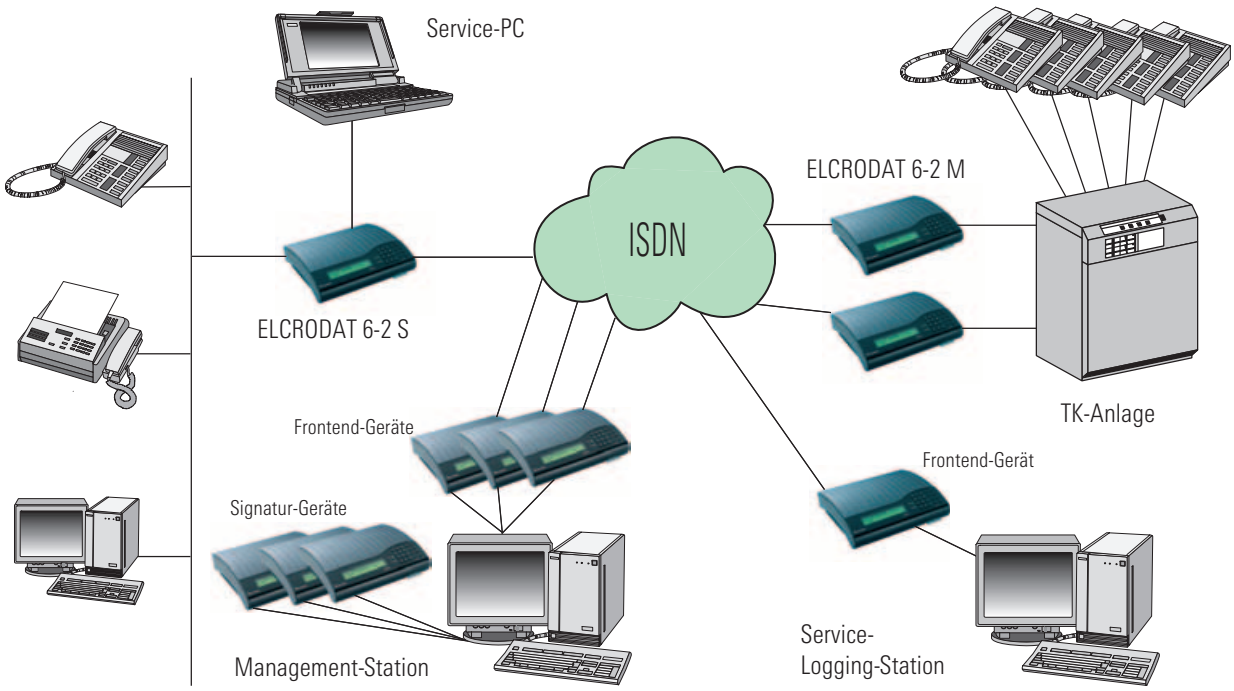
ELCRODAT 6-2 S ist als Ergänzung zu vorhandenen EURO-ISDN-Endgeräten oder Nebenstellenanlagen die ideale Lösung für sichere Sprach- und Datenübertragung von OFFEN bis zur höchsten Geheimhaltungsstufe. Es kann zusammen mit bis zu 8 handelsüblichen ISDN-Endgeräten oder zusammen mit einer Nebenstellenanlage eingesetzt werden. Der Amtszugang erfolgt dabei entweder direkt über den S_0-Basisanschluss oder über eine Nebenstellenanlage.

ELCRODAT 6-2 M ermöglicht die Einzelkanalverschlüsselung von gleichzeitig bis zu 30 Kanälen. Ein typischer Einsatzfall für diese Gerätevariante ist die Portverschlüsselung von 2 Mbit/s vor ISDN-Nebenstellenanlagen. Der Amtszugang erfolgt dabei entweder direkt über den S_{2M}-Anlagenanschluss oder über eine Nebenstellenanlage.

Hochsichere Krypto-Technologien

ELCRODAT 6-2 ist das erste vom BSI in der Bundesrepublik zugelassene Verschlüsselungsgerät, das bei der Übertragung von bis zu STRENG GEHEIM eingestufter Information eine Schlüsselverteilung mit Hilfe eines Public-Key-Verfahrens durchführt. Dabei ermöglicht ein in den Schlüsselgeräten realisierter Rauschgenerator zusammen mit dem Public-Key-Verfahren die gegenseitige Authentisierung und Schlüsseleinigung. Die Sitzungsschlüssel werden für jede Verbindung in den Verschlüsselungsgeräten neu generiert, verlassen diese nicht und werden nach der Sitzung wieder gelöscht. Dadurch wird ein Höchstmaß an Sicherheit erreicht.

Systemübersicht ELCRODAT 6-2 S oder ELCRODAT 6-2 M



Aufbau

Das High-End-Verschlüsselungssystem ELCRODAT 6-2 besteht aus folgenden Komponenten (siehe Systemübersicht auf Seite 2):

- Verschlüsselungsgeräte
- Management-Station zur Zertifikatsverwaltung
- Service-Station zur Fernadministration
- Logging-Station zur Fernüberwachung der Schlüsselgeräte

Management-Station
Die Management-Station erteilt die Berechtigung zur Teilnahme am verschlüsselten Betrieb in einer Benutzergruppe. Sie sendet ein signiertes Zertifikat mit einem sicheren Protokoll über eine ISDN-Verbindung zu dem jeweiligen Schlüsselgerät. Des Weiteren bestimmt sie die Gültigkeitsdauer dieses Zertifikats oder verlängert sie.

Die Management-Station kann entsprechend der Anzahl der zu verwaltenden Verschlüsselungsgeräte und Benutzergruppen ausgebaut werden; sie besteht aus einer Workstation mit Backup-System sowie aus bis zu 3 Frontend-Verschlüsselungs- und 3 Signaturgeräten.

Service-Station
In der Service-Station können die Betriebs- und D-Kanal-Filterparameter zentral eingestellt und mit einem sicheren Protokoll über eine ISDN-Verbindung an die Schlüsselgeräte verteilt werden. Die Service-Station besteht aus einer Workstation mit Backup-System und einem Frontend-Verschlüsselungsgerät.

Filter und Monitor im Signalisierungskanal
Der Signalisierungskanal wird per Monitor überwacht, unerwünschte Protokollelemente werden ausgefiltert. Bestimmte Rufnummern können abgewiesen oder mit Privilegien belegt werden.

Mit dieser Sicherheitsfunktion wird eine Manipulation besonders von Nebenstellenanlagen, aber auch von anderen ISDN-Endgeräten verhindert.

Logging-Station
Das Verschlüsselungsgerät ELCRODAT 6-2 verfügt über einen Logging-Speicher, in den alle unerlaubten Eindring- und Manipulationsversuche, Aktivitäten des D-Kanal-Filters usw. eingetragen werden. Der Speicherinhalt wird mit einem sicheren Protokoll über eine ISDN-Verbindung an die Logging-Station übertragen. An dieser können die Speicherinhalte ausgewertet und archiviert werden. Die Logging-Station besteht aus einer Workstation mit Backup-System und Frontend-Verschlüsselungsgerät.

Service-PC
Alternativ zur Service- und Logging-Station können Konfiguration und Auslesen des Logging-Speichers der Verschlüsselungsgeräte auch lokal am ELCRODAT 6-2 von einem Standard-PC aus durchgeführt werden.

Technische Daten

Modell	ELCRODAT 6-2 S	ELCRODAT 6-2 M
Stromversorgung	230 V AC, ca. 15 VA	230 V AC, ca. 20 VA
Nutzdatenrate (ohne Signalisierung)	max. 128 kbit/s	max. 1920 kbit/s
Unabhängig voneinander verschlüsselbare Kanäle	2	30
ISDN-Schnittstellen zur TE- und NT-Seite	S_0 (4-Draht-Kupfer)	S_{2M} (4-Draht-Kupfer)
D-Kanal-Protokoll	E-DSS 1	
Abstrahlsicherheit	AMSG 720B	
Einsetzbar bis Geheimhaltungsstufe	STRENG GEHEIM	
Abmessungen (B x H x T)	330 mm x 75 mm x 282 mm	

Bestellangaben

ELCRODAT 6-2	3534.3129	3534.3106

Printed in Germany 0901 (Bi bb)

ROHDE & SCHWARZ

ROHDE & SCHWARZ SIT GmbH · Am Studio. 3 · 12489 Berlin
Tel. (030) 65884-223· Fax (030) 65884-184 · E-Mail: info.sit@rohde-schwarz.com ·www.sit.rohde-schwarz.com