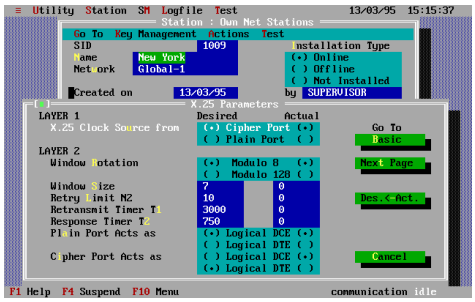
GRETACODER® 545

X.25 Data Encryption



Protects sensitive corporate data on X.25 networks
Provides a virtual, private, highest security intranet
Retains all X.25 benefits in a transparent way

For public and private X.25 networks
For switched and permanent virtual circuits
Network Security Center for larger networks
Highest grade Swiss cryptography

GDS

GRETACODER Data Systems AG

GRETACODER® 545: X.25 Data Encryption

Secure, Corporate-Wide X.25 Service

With X.25, user packets are routed from node to node and channel capacity is shared on a demand basis with other users. This results in generally better channel utilization than with private leased lines, but also increases the vulnerability in regard to security.

The GRETACODER 545 provides top level protection for sensitive corporate data on X.25 networks. By encrypting data end-to-end at up to 64 kbit/s, it allows enterprises to use X.25 services with full confidence. The GRETACODER 545 is intended for use with synchronous X.25 connections. This individual logical channels are automatically encrypted and decrypted with their respective keys. No overhead bytes are added to user packets and all control information is left unencrypted, thus assuring full transparency.

Clear and Encrypted Connections

The GRETACODER 545 can handle a mix of clear and encrypted logical connections simultaneously.

Key Management -- Several Choices

Several options to generate and distribute keys are supported. In the absence of a Network Security Center, the AUTOKEY™ option is probably the most convenient. Based on public key technology, it allows to securely generate new secret Master Keys directly via the X.25 connection. A special authentication procedure protects against potential spoofing attacks.

If preferred, secret keys may also be generated by the built-in true random noise generator and loaded into a Security Module for distribution to the partner station. Or keys may even be manually entered.

Secure Session Keys -- More Protection

Based on the secret master key, a new data encryption key is automatically and securely derived for every new session or after a predefined time. A million such Session Keys, guaranteed to be all different, are associated with each Master Key. Even if Session Keys were changed every five minutes, the supply tied to a single Master Key would last for a full ten years. And a new supply may be generated anytime by simply exchanging a new Master Key.

The rejection of already used Session Keys positively protects against all attacks based on previously recorded messages, e.g. the so called midnight attack, where actual equipment is illegally accessed to decrypt such messages, or replay attacks where previous messages are injected a second time into the communication channel. All of which means more security and less risk.

Swiss Cryptography -- Ultimate Security

The GRETACODER 545 uses a proprietary block cipher of exceptional strength. Key sizes, both for Master Keys and Session Keys, are 128 bit. This key size provides highest, military grade security and renders any known attack infeasible. Each key bit is fully used; there is no redundancy which could reduce the relevant key size. Cryptographic keys are under exclusive control of the user alone.

The DES is available as an option to those who prefer a well established standard.

Define Your User-Groups

If desired, specific stations may be configured as a strictly closed user group or as several such groups. In addition, you are able to precisely define who is authorized to communicate with whom.

Unique Security Module (SM)

All secret elements and set-up parameters are stored in encrypted form in a small, plug-in Security Module (SM). Since the equipment itself contains no secret elements, the critical logistics connected with maintenance, service or exchange are noticeably simplified.

The SM can be electronically locked via a PIN. In addition, a high security mechanical lock safeguards the SM and at the same time protects against unauthorized opening of the all-metal housing.

Start Small -- Expand Later

To centrally manage and supervise larger networks, a Network Security Center (NSC) is available. Since each GRETACODER 545 is already equipped with the necessary software for NSC compatibility, there is no need to upgrade the units when an NSC is added at a later time. The NSC may also be used as an off-line key programming center.

Set-Up and Testing

A display with a menu driven user interface assures easy set-up and configuration on first use; afterwards operation is completely automatic. Diagnostics, such as remote status inquiry, alarm reporting and an integrated self-test, are available for testing and maintenance.

Encryptor Access Control

Access control to specific system functions is handled by defining groups with different privileges (e.g. PIN or token). This guards against unauthorized tampering and unintended set-up changes via button pushing. Several standard classes are offered, but customer specific requirements are easily implemented.

X.25 On-line Network Security Center (NSC)

Application

The Network Security Center (NSC) can centrally control several hundreds or even thousands of GRETACODER 545 encryption units in an X.25 network. This allows systems administrators to perform all critical network security functions from a central point: key management, remote configuration, diagnostics, central surveillance and administration. This monitoring and control of the remote encryptors is performed in an entirely secure way with all commands and service messages being encrypted and authenticated.

All of the NSC's activities, whether automatically done or performed by the system administrator, are recorded in special log files.

The NSC consists of the GRETACODER 549 Secure Network Interface Unit, software for communication and management functions and a dedicated host PC that runs the software and controls the database.

Secure and Automatic Key Distribution

One of the main functions of the NSC is its service as an on-line key distribution center. Key distribution is executed automatically the first time an encryptor calls a particular partner unit for which it does not yet have a key. If the NSC recognizes the contact as authorized, it generates a random Master Key, which is transmitted in encrypted form to the two remote GRETACODER 545 units for storage.

The NSC allows administrators flexible, but precise security management of the network. Only authorized connections are provided with matching keys. This capability allows multiple closed user groups to be designated and managed within individual networks.

NSC Access Control

For operator access to the NSC, up to four different levels can be defined, each with its own individual access means (e.g. identification token or PIN) and its own individual functionality.

Options for Configuration

The configuration data of each encryption unit is stored in both the NSC database and the units's Security Module. Normally, configuration of new encryptors being added to the network is performed via the NSC; a process which does not require technically skilled personnel at the remote sites. The NSC configures a Security Module which is then delivered to and installed in the target encryption unit. For safe transfer to the GRETACODER 545 location, data on the Security Module is encrypted and access to it is PIN protected.

As an alternative, the GRETACODER 545 can be fully configured using its front-panel controls. The AUTOKEY process may then be used to establish a Master Key with the NSC. Once this is done, the NSC has again full remote, on-line control over the remote encryptor via the X.25 network.

Standby NSC

A "Standby NSC" can provide complete redundancy for applications where uptime is extremely critical. This second NSC is on hot standby and preferably placed at another location.

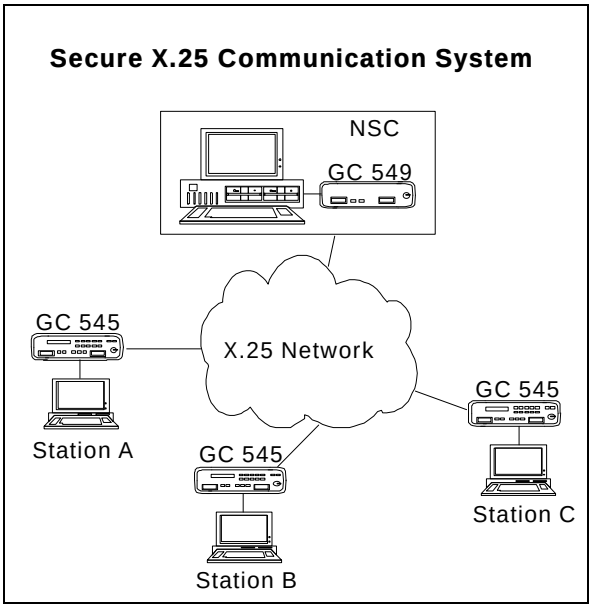
If a GRETACODER 545 cannot reach the Master NSC, it will automatically route the request to the Standby NSC. Database consistency is achieved by periodic secure data transfers, over either the X.25 network or the public switched Telephone network.

Configuration NSC

For networks in which the user wants to separate configuration and maintenance operation from security administration, a "Configuration NSC" (even at another location) may be connected to the network. This NSC is used only for non-security-related management and testing of encryption units. It does not distribute encryption keys.

Central Network Monitoring Functions

The NSC provides an extensive set of control and test features, checking the integrity of all encryption keys, the status of network encryption units and the connections between the units.



Technical Data

GRETACODER		545	549 (NSC)
Data rate	Synchronous, full duplex	≤ 64 kbit/s	≤ 20 kbit/s
Self-synchronizing	After power-down, bit errors & bit slips	fully automatic	fully automatic
Self-test	After power-up, on user command	integrated	integrated
X.25 features	Protocol ITU-T X.25 (1984)	•	•
	Packet size	max. 1024 bytes	max. 1024 bytes
Virtual circuits	PVC (Permanent virtual circuits)	•	•
	SVC (Switched virtual circuits)	•	---
Number of supported LC	(LC = logical channels)	up to 32 standard	up to 32
		up to 128 optional	---
Physical interfaces for	V.24/RS-232-C	•	•
data communication	V.35	•	---
(DTE & DCE)	X.21	•	---
	RS-422/V.11	•	---
Cryptographic algorithm	GDS proprietary	128 bit key	128 bit key
	DES	56 bit key	56 bit key
Key management	AUTOKEY	•	•
(included in GC 545/549)	Keygun / Memory-SM	•	•
	Manual entry (Keypad)	•	•
	Secure session keys	•	•
NSC support		optional	n.a.
Line voltage	User selectable	180 to 280 VAC	180 to 280 VAC
either		90 to 140 VAC	90 to 140 VAC
		45 to 65 Hz	45 to 65 Hz
or		≤ 18 VA	≤ 18 VA
Line frequency		0 to +50 °C	0 to +50 °C
Power consumption		-20 to +70 °C	-20 to +70 °C
Temperature range	Operating	≤ 3.0 kg	2.7 kg
	Storage	220/70/365	220/70/365
Weight	GC 545: depending on interface		
Dimensions	w/h/d (mm), maximum		

Network Security Center (NSC)		PC Requirements
NSC dedicated PC station		Pentium 133 or better recommended
Main memory	Minimum free space	580 kB RAM
Operating system		DOS 6.X
Ports		1 x parallel (printer) 2 x serial (GC 549 and modem) 1 x mouse

---

GRETACODER Data Systems AG (GDS)

Althardstrasse 150, CH-8105 Regensdorf, Switzerland

Phone +41-(0)1-871-1111, Fax +41-(0)1-871-1100, E-mail mailgds@gds.ch, Internet http://www.gds.ch

04/97