Managed WAN Encryption

To ensure your competitors don’t eavesdrop.

With Managed WAN Encryption, you encrypt your connections on Layer 2 (data link layer) securely and reliably. Layer 2 connections are suitable for, among other things, connections between data centres and for encrypting various protocols such as FiberChannel, Ficon and Ethernet. For Layer 3 connections, you need the Managed Firewall/VPN Service.

In order to operate a connection/line securely it is good practice to have encryption. This can, following the OSI model, be implemented either on Layer 2 (data link layer) or on Layer 3 (network layer).

There are many reasons for a connection/encryption based on Layer 2 (e.g. SES or SOS):
> The bandwidth can be optimally utilised.
> You can manage the traffic yourself.
> You can perform key management tasks yourself.
> You profit from dedicated hardware encryption.
> You can easily integrate encryption into an existing Layer 2 network.

There are a variety of encryption solutions depending on which connection product has been selected. Encryption on Layer 2 is further described in this document. Encryption on Layer 3 is known in particular in association with the term VPN (Virtual Private Network). If you have a Layer 3 connection over the Internet, the VPN or Firewall VPN service has been designed specifically for your needs. If you have a Layer 3 connection over MPLS (LAN-i), “SecureCER” is the appropriate encryption option.

Layer 2 encryption can be provided by Swisscom based on two connection technologies. These two products (SOS and SES) are a prerequisite for the encryption service described here. In addition, the Layer 2 encryption service can also be provided on a dark fibre.

Managed WAN Encryption

Encryption over SOS (Swisscom Optical Service):
> Point-to-point encryption
> Different bandwidths are possible
> No limitations as regards L2 protocols (see the SOS service description)
> No QoS (Quality of Service)

Encryption over SES (Swisscom Ethernet Service):
> Point-to-point and point-to-multipoint encryption
> Different bandwidths are possible
> Limitations as regards L2 protocols (see the SES service description)
> QoS (Quality of Service) possible

Recurring services

Health Monitoring and Incident Management	We guarantee that health incidents are processed within the defined service level times. If a security device cannot be reached, Swisscom takes over the troubleshooting and informs you immediately.
Reporting	The dashboard shows you at any time the availability of the link encryption per month.
Key management (optional)	Swisscom renews the master communication key (in the case of "point-to-multipoint" connection also the broadcast communication key) every 12 months.

How you benefit

> You encrypt WAN routes in accordance with regulatory specifications (e.g. FINMA).
> You encrypt various protocols.
> You encrypt high bandwidths without any loss in performance.
> You do not have any additional latency times.

001 11-14

Swisscom (Switzerland) Ltd, Enterprise Customers, P.O. Box, CH-3050 Bern, Tel. 0800 800 900 www.swisscom.ch/enterprise