HITACHI
Inspire the Next

XMC20 SECU1

Quantum-Safe end-to-end encryption for mission-critical real-time communication networks

XMC20 SECU1

The encryption card SECU1 secures data transfer in critical infrastructures. It is used in mission-critical real-time applications for controlling and monitoring networks.

- Offers end-to-end encryption against cyber-attacks in packet-based transport networks (MPLS-TP)
- Includes an integrated QRNG (Quantum Random Number Generator) for the Quantum-Safe user data encryption.
- 4 (8) x SFP+ 1/10 GbE ports per encryption unit
- Causes near zero delay in PTP (Precision Time Protocol IEEE1588) packets
- Tamper-protected to prevent mechanical manipulation

01 XMC20 SECU1 4 port version (left) and 8 port version (right)

Overview
For the encryption card on the XMC20 platform, Hitachi Energy uses a hardware-based QRNG (Quantum Random Number Generator) to generate highly secure keys that really are random. The basis for the trustworthy and protected distribution of keys is provided by a centralized and decentralized generation of keys.

There is no single-point-of-failure and all nodes can securely communicate with one another.

This permanent-encryption method offered by Hitachi Energy prevents the creation of so-called network islands.

SECU1 encrypts the complete network traffic end-to-end natively on layer 2.5 in MPLS-TP transport networks with ultra low latency times of under four micro-seconds. The card is characterized by parallel high-security end-to-end encryption in mission-critical networks and ensuring very high data availability while providing precise timing.

Highly secure encryption
Encryption and authentication is done through the most secure, state-of-the-art, verified and recommended algorithms currently available to guarantee maximum security.
- Master key (session key encryption)
- Session key (user traffic encryption)
- The Atomic master key exchange without interruption.

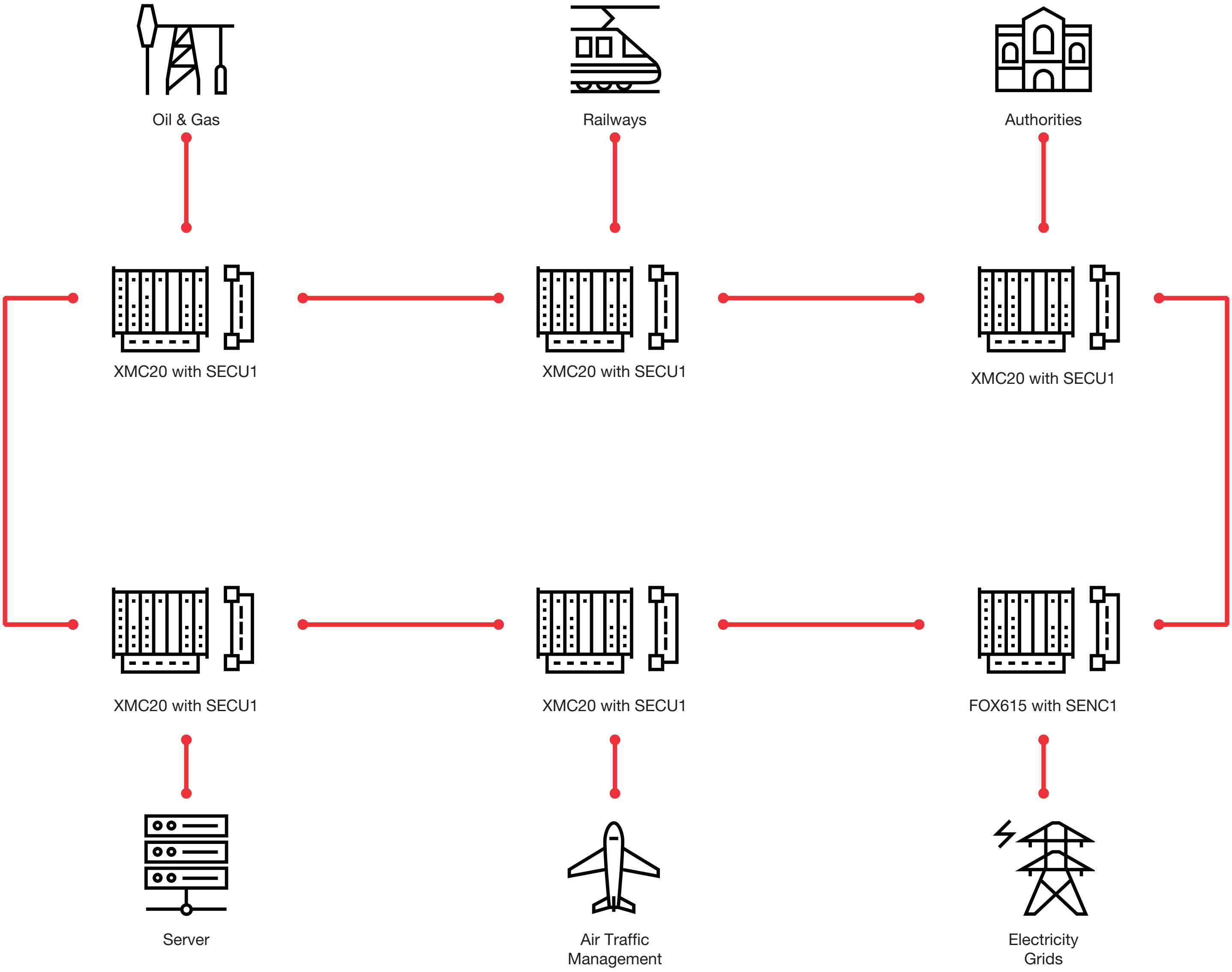
For symmetrical encryption, the AES-GCM (Galois Counter Mode) encryption and authentication algorithm with a key length of 256 bit is applied. The session keys are updated every 60 seconds and offer fully automatic key management based on the “set and forget” principle.

Hitachi Energy

Failsafe operation
Failsafe operation plays a vital role in mission-critical networks. Therefore the card can be operated in a redundant setup.

High compatibility
The SECU1 can easily be integrated into existing networks. No adjustments of network structures nor changes on end devices are required.

Hitachi Energy "Trusted Security"
In the framework of its "Trusted Security" concept, Hitachi Energy researches, develops and produces in Switzerland and in Europe. Hitachi Energy Trusted Securityincludes meeting the highest security requirements, certified employees, a central management of data transfer systems as well as deploying encryption technologies. Hitachi Energy systems fulfill the applicable standards of the industry and comply with the high requirements operators of mission-critical networks have with respect to high availability and low maintenance.



02 Secure communication in mission-critical networks

03 Easy integration into exisiting networks

Technical Data

Hardware	
	4-port (SECU1-4) and 8-port (SECU1-8) hardware version
	FPGA based
	Fanless version available (SECU1F4, SECU1F8)
Interfaces	SECU1-4 - 4x 1/10 GbE optical ports (2x encrypt, 2x decrypt)
	SECU1-8 - 8x 1/10 GbE optical ports (4x encrypt, 4x decrypt)
	1 GbE electrical front port and backplane connection for management
Data throughput	Up to 10 Gbps
Timing	Latency of user traffic <4 µs Delay variation <50 ns (including PTP packets) Jitter and wander Transparent trough-timing. PLL bandwidth 50 Hz
Quantum Random Number Generator (QRNG)	
	Optical component from ID Quantique
	Random numbers for AES-256 encrypted session keys
	Truly random
	Up to 1.5 Mbit/s
Tamper Protection	
	Tamper-protected features to prevent mechanical manipulation
	Fully covered through metal plates
	Tamper action secured by local on-board battery with >20 years life-time (changeable)
Encryption Features	
	MPLS-based Encryption Layer 2.5 (MPLS-TP)
	End-to-End encryption of up to 2048 SECU1-4 (4096 SECU1-8) MPLS-TP tunnels
Management Communication Key	Encryption and authentication of all communication between the DIRAC server and encryption devices (including transmission of the master key) -Post-Quantum Cryptography ready.
Master Key	For session key encryption and automatic tunnel deployment. Encryption and authentication with AES-CTR Key length: 256 bit Key change: manual, non-disruptive.
Session Key	User traffic encryption. Encryption and authentication with AES-GCM (Galois Counter Mode) Key length: 256 bit Key change: automatically min. every 60 seconds, non-disruptive
1588v2 PTP compatible	Encrypts PTP packets with near zero delay variation

Management	
UNEM-UN	Sets up the bidirectional LSP / MPLS tunnels as well as the encryption policy for each tunnel
Dirac Server (Software)	The DIRAC server is a centralized key management system and is responsible for the generation and distribution of the Master Keys used by the SECU1 Crypto Engines.
Command line interface (CLI)	Configuration, supervision, management and activation of the Dirac server and the encryptors

Power supply	
Input voltage nominal (min/max)	–48/–60 V DC (–40.5 V DC … –72 V DC)
Operation environment	
Temperature range and humidity	Acc. to XMC20 environmental specifications

Hitachi Energy
marketing-update@hitachienergy.com

www.hitachienergy.com

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. Hitachi Energy Ltd. does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

4CAE000488