XMC20 SECU1
Unit for highly secure end-to-end encryption in mission-critical communication networks

The encryption card SECU1 secures data transfer in critical infrastructures. It is used in mission-critical applications for controlling and monitoring energy networks, oil and gas pipelines, railways and local authority networks (police, air traffic control, military defense).

- Offers end-to-end encryption against cyber-attacks in packet-based transport networks (MPLS-TP)
- Comes with an integrated physical QRNG random number generator
- Offers a redundant encryption unit per card
- 4 x SFP+/10 GbE ports per encryption unit
- Causes no delay in PTP (Precision Time Protocol IEEE1588) packets
- Tamper-protected to prevent mechanical manipulation
- Can be extended with Quantum Key Distribution (QKD)

Overview
For the SECU1 encryption card on the XMC20 platform, ABB 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 ABB 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. This offers benefits: No loss of bandwidth by overhead and 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 are carried out through the most secure encryption process available at the moment which is also recommended by the BSI (German Federal Office for Information Security) in the TR-02102-2 technical directive. Asymmetrical or symmetrical encryption methods are applied.
- Master key (key encrypting)
- Session key (data encrypting)
For asymmetrical encryption, the algorithm ECDH 512 bit Diffie-Hellman with Elliptic Curve Crypto System (ECC) is applied. The key exchange is executed every 60 minutes – automatically.
Authentication is based on the X.509 certificate.
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.

Failsafe operation
Failsafe operation plays a vital role in mission-critical networks. Therefore, as a card, the SECU1 is designed to be redundant. Two completely independent encryption units, including current and random number generator with quantum physics (QRNG), are located on one single card.

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

ABB “Trusted Security”
In the framework of its “Trusted Security” concept, ABB researches, develops and produces in Germany and in Switzerland. ABB Trusted Security includes meeting the highest security requirements, certified employees, a central management of data transfer systems as well as deploying encryption technologies. ABB 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.
03 Easy integration into existing networks

### Technical Data

#### Hardware
- Fully redundant
- FPGA based
- Fail-safe and space-saving through two independent encryption units per card
- Fanless version available

#### Interfaces
- 4x 10 GbE optical ports (2x encrypt, 2x decrypt) per unit – 8x per card
- 1x 1 GbE electrical port per unit for management – 2x per card

#### Data throughput
- Up to 10 Gbps

#### Ultra low latency
- Low as 4 μs

#### Quantum Random Number Generator (QRNG)
- Optical component from ID Quantique
- Random numbers for AES-256 encrypted session keys
- Truly random
- 1x per unit – 2x per card
- Up to 4 Mbit/s

#### Tamper Protection
- Tamper-protected features to prevent mechanical manipulation
- Fully covered through metal plates
- Powered by two batteries with 10 years lifetime (changeable)
## Encryption Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-based Encryption Layer 2.5 (MPLS-TP)</td>
<td>End-to-End encryption of up to 1024 MPLS-TP tunnels</td>
</tr>
<tr>
<td>Asymmetric cryptosystem (Master Key)</td>
<td>Algorithm: ECDH Elliptic Curve Diffie-Hellman with Elliptic Curve Crypto System (ECC) – BSI Standard TR-02102-2, Key change: 60 minutes automatically</td>
</tr>
<tr>
<td>Authentication:</td>
<td>X.509 certificate</td>
</tr>
<tr>
<td>Symmetric cryptosystem (Session Key)</td>
<td>Algorithm: AES-GCM (Galois Counter Mode), Key length: 256 bit, Key change: 60 seconds</td>
</tr>
<tr>
<td>1588v2 PTP compatible</td>
<td>Encrypts PTP packets with near zero delay variation</td>
</tr>
</tbody>
</table>

## Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNEM</td>
<td>Sets up the bidirectional LSP / MPLS tunnels as well as the encryption policy for each tunnel</td>
</tr>
<tr>
<td>Dirac Server (Software)</td>
<td>Responsible for configuration, supervision and alarming collection of the encryptors inside the network</td>
</tr>
<tr>
<td>Command line interface (CLI)</td>
<td>Configuration, management and activation of the Dirac Server and the encryptors</td>
</tr>
</tbody>
</table>

## Power supply

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input voltage nominal (min/max)</td>
<td>–48/–60 V DC (–40.5 V DC … –72 V DC)</td>
</tr>
</tbody>
</table>

## Operation environment

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature range and humidity</td>
<td>Acc. to XMC20 environmental specifications</td>
</tr>
</tbody>
</table>