




Cybersecurity Package

TTC 2000 Series



- ✓ **Key benefits of the security features**
- ✓ Secure environment for cryptographic operations, storage, and key management
- ✓ Unauthorized code execution prevention during startup sequence
- ✓ Authentication of software binaries before flashing on the ECU
- ✓ Development and post-development confidentiality, integrity of data and functionalities
- ✓ Continuous vulnerability management and fast response on the incident management

As off-highway vehicles continue to evolve, protection against cyber-attacks is becoming more and more important in the new era of safety and trusted machine operations.

By following best practices and guidelines, we ensure that TTC 2000 Security package meets the security requirements recommended by industry standards and regulatory authorities.

It is powered by the advanced capabilities of Infineon 2nd AURIX™ generation of microcontrollers, which include a full EVITA hardware security module that provides comprehensive protection against cyber threats.

Enhanced cryptographic capabilities

The Hardware Security Module (HSM) 32bit ARM Cortex CPU as part of Infineon 2nd AURIX™ of the TTC2000 Series generation provides hardware-accelerated cryptographic capabilities and ensure execution of the cryptographic operations, such as encryption, hashing, message authentication codes, and digital signatures. It also provides true and pseudo random number generation.

Secure boot and download

Secure boot verifies the integrity and authenticity of the customer application software before being executed at start-up. Secure download ensures that

all the software binaries are authenticated before being flashed on the ECU.

Certificate and key management

It ensures that cybersecurity material (e.g. keys and certificates) is securely generated, stored, used and minimizes the risk of unauthorized access or data breaches on the ECU.

Post-development activities

These activities monitor interactions between ECU software components to detect any unexpected behavior or security gaps, vulnerabilities, or potential threats to implement appropriate design countermeasures or adjustments of the security best practices.



Application fields

- Agricultural machines
- Construction / material handling machines
- Municipal vehicles

Functionality overview

Feature	Description	Compliance
HSM	AES*-128 Encryption / Decryption, HW accelerated module using 128-bit key size with ECB, CBC supported modes *Advanced Encryption Standard	FIPS 197 NIST SP800-38A
	Cryptographic hash functions: AES CMAC* and AES HMAC** *Cipher-based Message Authentication Code **Keyed-Hash Message Authentication Code	SP 800-38B NIST 800-107
	Secure Hash Algorithm SHA-256	FIPS 180-4
	True Random Number Generator (TRNG), functionality class PTG.2	AIS-31
	Pseudo Random Number Generator (PRNG), functionality class DRG.2	AIS-20
	RSA* Cryptosystem based on decryption/decryption schemes: - PKCS#1 RSAES-OAEP [RFC-3447] - PKCS#1 RSAES-V1_5 [RFC-2313] *Rivest-Shamir-Adleman	-
	HSM firmware update mechanisms	-
Certificate and key management	Certificates management and update mechanisms	X.509 v3
KDF	Key derivation function (KDF counter mode)	NIST SP 800-108
Secure boot Runtime manipulation detection	Secure boot component is trusted to verify the integrity of the ECU boot sequence. Runtime manipulation detection identifies unauthorized changes to the application and bootloader while they are running.	
Secure download	Software component that ensures the trusted firmware is downloaded and installed securely on the ECU	
Debug port protection	(Only) the API functions are provided to ensure that this interface can be secured against unauthorized access. <i>(The debug port is by default unprotected and physical connector not populated on series devices)</i>	

Maintenance overview

Vulnerability management	Continuous assessment and cybersecurity risks management to identify potential threats, to evaluate the impact, and to implement the risk mitigation strategies. (e.g. relevant for CRA, ISO/SAE 21434, R155, EU 2023/1230 Machinery Regulation) Automated vulnerability scanning of the HSM firmware. (e.g. relevant for CRA, ISO/SAE 21434)
Incident management	Reaction and appropriate measures as defined by company security policies: https://www.tttech.com/responsible-disclosure (e.g. relevant for CRA, R155, ISO/SAE 21434)
Software updates	Depending on the risk severity or impacted parts in case of an incident certain important updates of the HSM or the bootloader may be required for a successful rollout. (e.g. relevant for CRA, ISO/SAE 21434, R156)

Cybersecurity manual	A guideline for proper integration of the security package as component (e.g. relevant for CRA, ISO/SAE 21434, R156)
Cybersecurity Interface agreement	It establishes the followings: (e.g. relevant for CRA, ISO/SAE 21434, R155): <ul style="list-style-type: none"> • identity of responsible individuals • understanding of supplier capabilities • responsibility of both consumer and supplier for the various work products • agreement of the confidentiality level for the various work products



TTControl Italy, Brixen
Phone: +39 0472 26 80-11

TTControl Austria, Vienna
Phone: +43 1 585 34 34-0

© TTControl GmbH. All rights reserved. All trademarks are the property of their respective holders. To the extent possible under applicable law, TTControl hereby disclaims any and all liability for the content and use of this flyer.

products@ttcontrol.com www.ttcontrol.com