YTSEC Secure Microcontroller
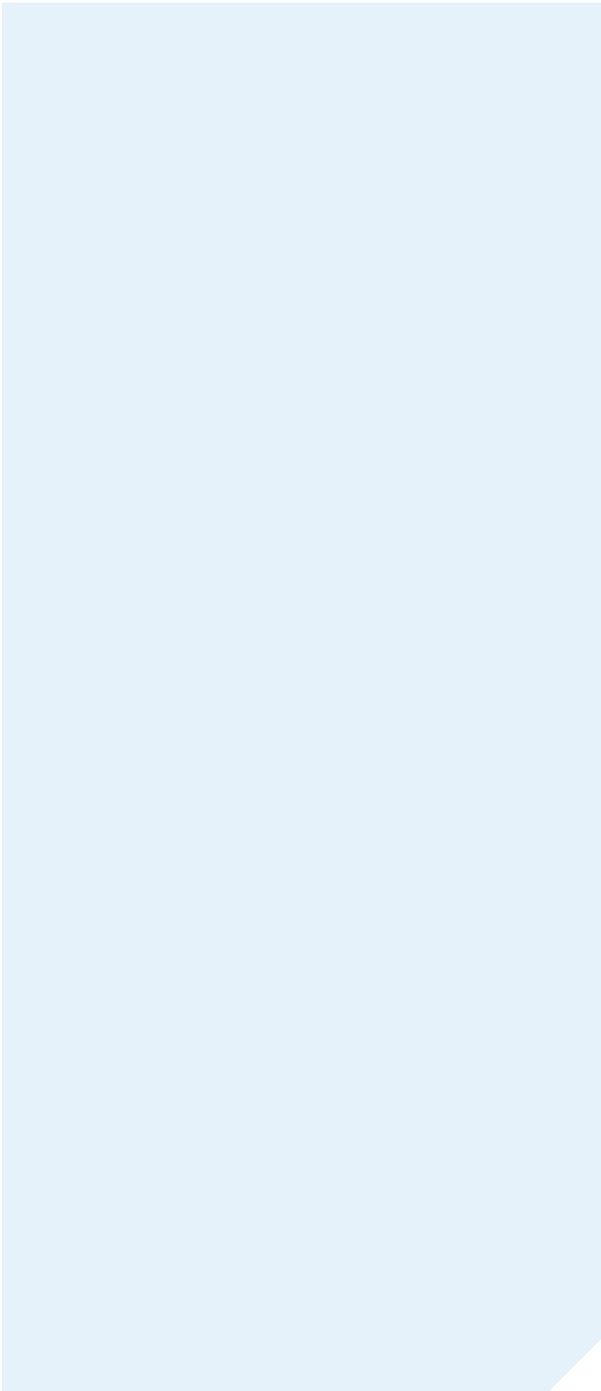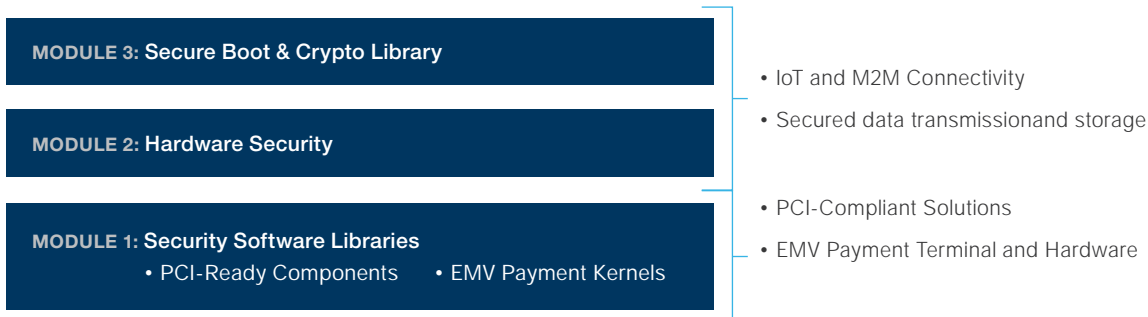
S P à S

In the age of digitization and connectivity, the security of your personal and con dential data is paramount, and in the payment industry, even more so.

YTSEC is a low-cost secure microcontroller featuring key security modules. It implements the security standards de ned by PCI PTS (version 5.x and above) as a **System on Chip** for PIN processing. YTSEC solution can also be used for contact and contactless payments using the Jabil EMV

For additional information visit

Software Security Modules

Implementation of PCI-compliant security standards in the form of software eliminates the need of using a dedicated and expensive secure-microcontroller, thus reducing the hardware and peripheral requirements, and by extension, signi cantly reducing the cost of producing a payment terminal. The state-of-the-art YTSEC ultra-low-power processor reduces the power consumption of the terminal, thus increasing the battery-life and mobility of the payment terminals.

MODULE 3: Secure Boot & Crypto Library

MODULE 2: Hardware Security

MODULE 1: Security Software Libraries
• PCI-Ready Components   • EMV Payment Kernels

• IoT and M2M Connectivity

• Secured data transmissionand storage

• PCI-Compliant Solutions

• EMV Payment Terminal and Hardware

M   1: S   S   a L a

Implementation of PCI-compliant security standards in the form of software eliminates the need of using a dedicated and expensive secure-microcontroller, thus reducing the hardware and peripheral requirements, and by extension, signi cantly reducing the cost of producing a payment terminal. The state-of-the-art YTSEC ultra-low-power processor reduces the power consumption of the terminal, thus increasing the battery-life and mobility of the payment terminals.

• PCI-ready (pre-certified) CE PCI-PTS v5.1

For additional information visit

DATA SHEET

M.   2: Ha   a S   F.   a

Jabil's YTSEC implements security mechanisms based on periodic monitoring of different signals for each of the parameters under observation and erasure of the Master key upon detection of violation signal (secure storage erased if tampered), in addition to updating the security logs.

S   M.

List of key parameters monitored resulting in secure storage being erased if tampered.