NTSecureCloudSolutions

Creating safety.
With passion.

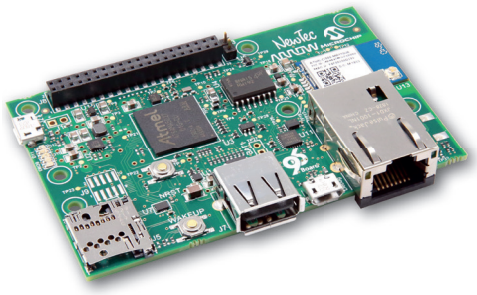
NewTec

NT SECURE GATEWAY

Shield96: development board for prototyping secure applications

The NTSecureGateway Shield96 development board is based on the Microchip® ATSAMA5D27 embedded platform with the high security System-in-Package 32-bit Arm® Cortex®-A5 processor-running up to 500 MHz and is compliant with the 96Boards Consumer IoT Edition Extended specification managed by Linaro.

The combination of the ATSAMA5D27 embedded platform and the ECC608 Secure Element, expands the possibilities of connected computing while providing the ultimate in security. The Shield96 development board supports a wide range of interfaces for prototyping secure applications. With the ECC608 it also provides the possibility for easy cloud / network provisioning. The HelmsDeep 96 embedded platform is designed to provide a fast and secure connection between connected Mezzanine cards and the outer world, via Ethernet or WLAN.



Shield96 embedded platform is designed to provide a fast-track deployment path, with integration services and production-ready, customizable Mezzanine Card to turn a Shield96 based invention into a commercial product.

Typical Applications

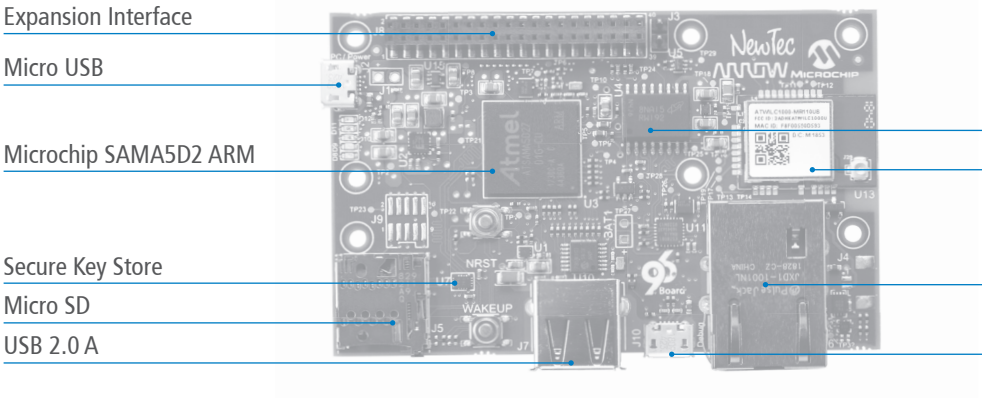
_ Legacy Industrial Applications
_ Facility Management
_ Metering
_ Payments
_ Biometric
_ Smart home devices
_ Building automation

What do we solve?

_ Secure storage / Secure Boot
_ Crypto Engine in TrustZone with SDK in Linux
_ OpenSSL adaptor
_ HW crypto and TRNG
_ Device ID, immutable, bound to the HWRoT (ECC key pair)
_ Managed Key store and Certificate Authority store
_ Factory Provisioning Services
_ Small Footprint due to SIP technology

NewTec GmbH Buchenweg 3 89284 Pfaffenhofen a.d. Roth Tel.: + 49 7302 9611-0 info@newtec.de **www.newtec.de**

System Overview



Key Features

CPU	Microchip SAMA5D2 ARM Cortex-A5 processor-based MPU: - Up to 500 MHz and features the ARM NEON SIMD engine. - A 128KB L2 cache and a floating-point unit. - System in Package with 128MB DDR2 SDRAM.
Flash	64 MB Serial NOR Flash Micron MT25QU01GBBB
Ethernet	10BASE-T/100BASE-TX IEEE 802.3 compliant
Wireless	WLAN 802.11 b/g/n Microchip ATWILC1000-MR110xB With chip antenna
USB	1x USB 2.0 A USB Host 1x Micro USB for Console output 1x Micro USB for power supply and USB Device
Security	Arm TrustZone, Secure Boot, Tamper Protection, Microchip ECC608 Secure Element with pre provisioning for TLS
Expansion Interface	40 Pin Low Speed Expansion Connector according to IoT Edition Extended (1,8V)
OS Support	Yocto Linux
Size	100mm by 85mm meeting 96Boards™ IoT Edition Extended (1,8V) dimensions specifications.

Out of the box the firmware implements a secure boot chain from ROM to the Linux kernel, diversified devices and a secure enclave using TrustZone\TEE all abstracted through an easy to use SDK

For industrial applications the gateway is also available in DIN Rail housing with extended supply voltage range up to 30V and additional features.

Customer Benefit

_ Accelerate time to market
_ Reduction in costs for development and certification
_ Ready-to-use communication interfaces
_ Highly secure

Kit Content

_ Development Board Shield96
_ Demo Support for AWS, MS Azure
_ Root of Trust (HWRot):
ATECC608 Secure Element pre-provisioned with private/public key and certificate chain for authentication of TCP/IP TLS use-cases (PKCS11 available soon)
_ Housing available on request
_ Customization Services for Software/ Hardware and Security concepts
_ Preloaded Sequitur Labs EmSpark Security Suite optional

NewTec GmbH Buchenweg 3 89284 Pfaffenhofen a.d. Roth Tel.: + 49 7302 9611-0 info@newtec.de **www.newtec.de**