SimpleLink™ Wi-Fi® CC3220

Enabling Security for IoT Products

30.7B connected devices by 2020,
75.4B by 2025

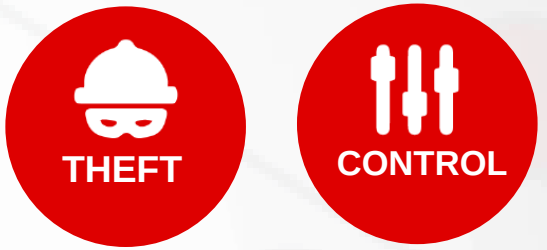
Top IoT concerns…

Sources: IHS Markit and Bain & Company

Security is a top concern

What do you want to protect?

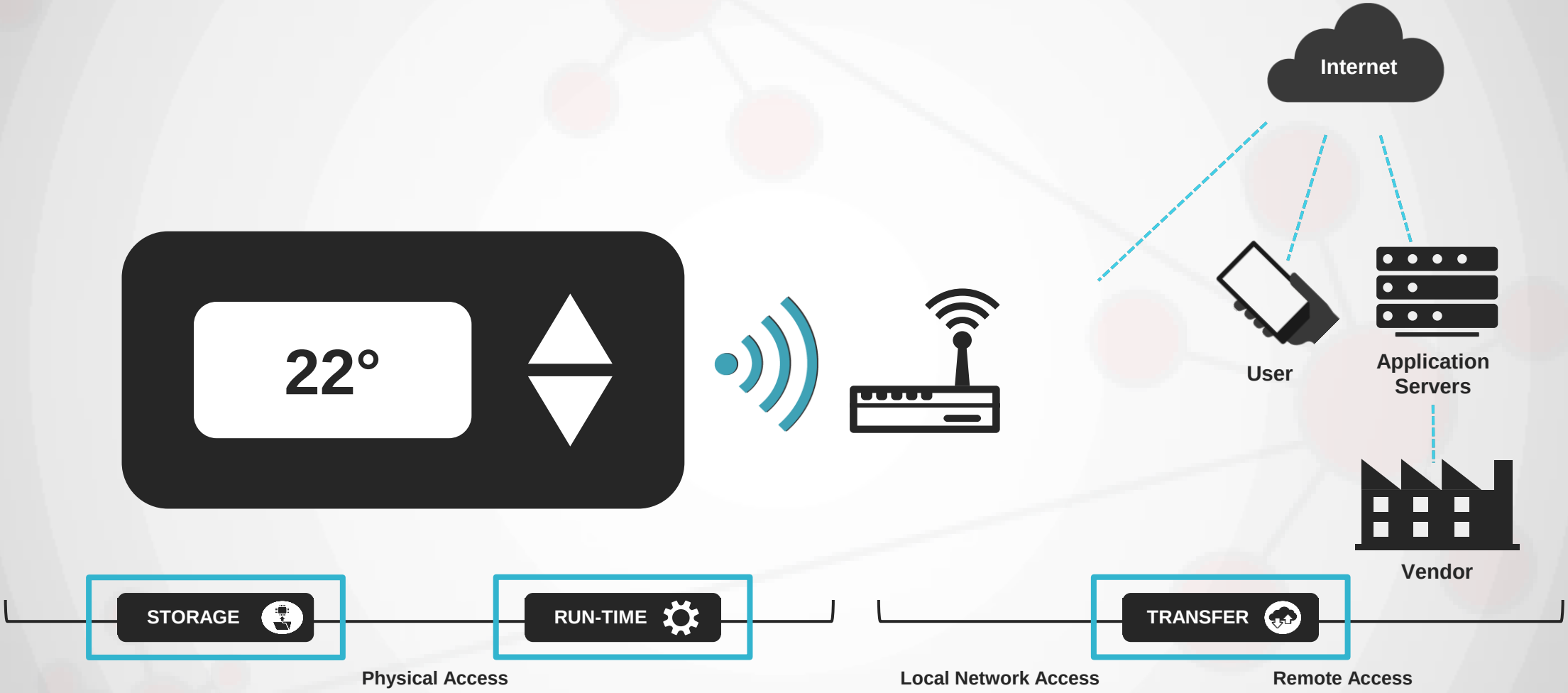
What are you protecting against?



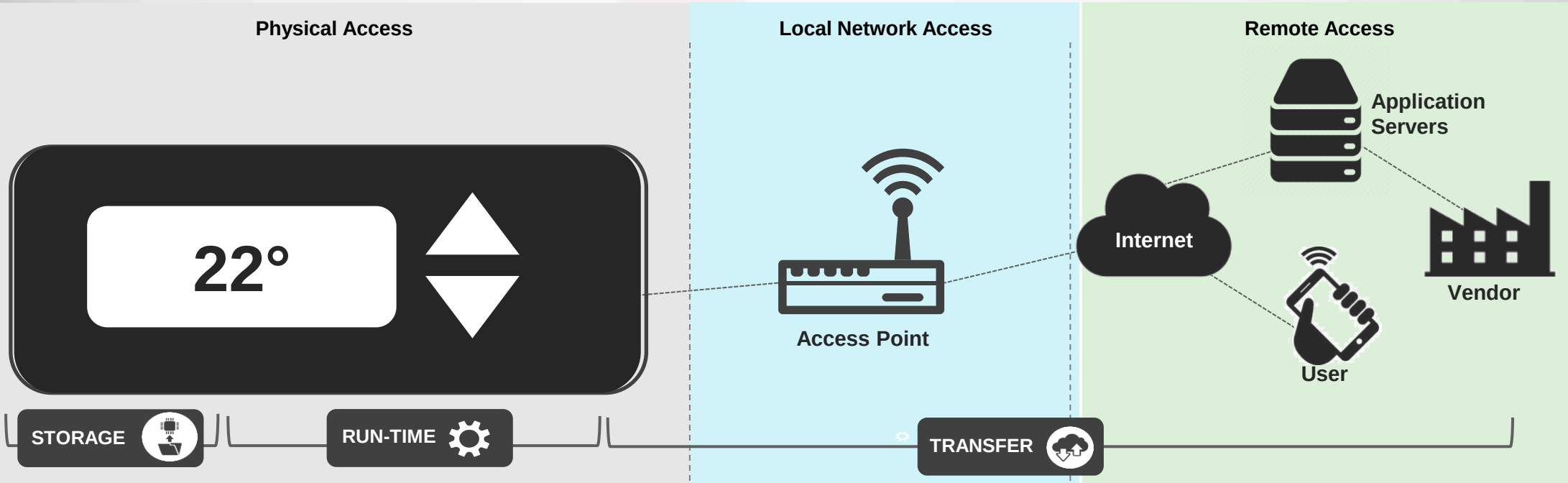
EXPOSURE POINTS

SECURITY ENABLERS

Comprehensive end-to-end security



SimpleLink™ Wi-Fi® – Multi Layer Security Measures



Physical Access Security Features
- Hardware crypto engines
- Trusted root-certificate catalog
- Debug security
- Secure content delivery
- TI root of trust public key
- Secure boot
- Initial secure programming

File System Security Features
- Unique key – cloning protection
- Software tamper detection
- File encryption
- File authentication
- File access control
- Factory image recovery
- File bundle protection

Local Network Security Features
- Hardware crypto engines
- Trusted root-certificate cat
- Secure sockets (TLS/SSL)
- Device Identity
- Secure key storage
- Secure content delivery
- Personal and enterprise Wi-Fi security
- HTTPS service

Remote Access Security Features
- Hardware crypto engines
- Trusted root-certificate catalog
- Secure sockets (TLS/SSL)
- Device Identity
- Secure key storage
- Secure content delivery

Access Distance

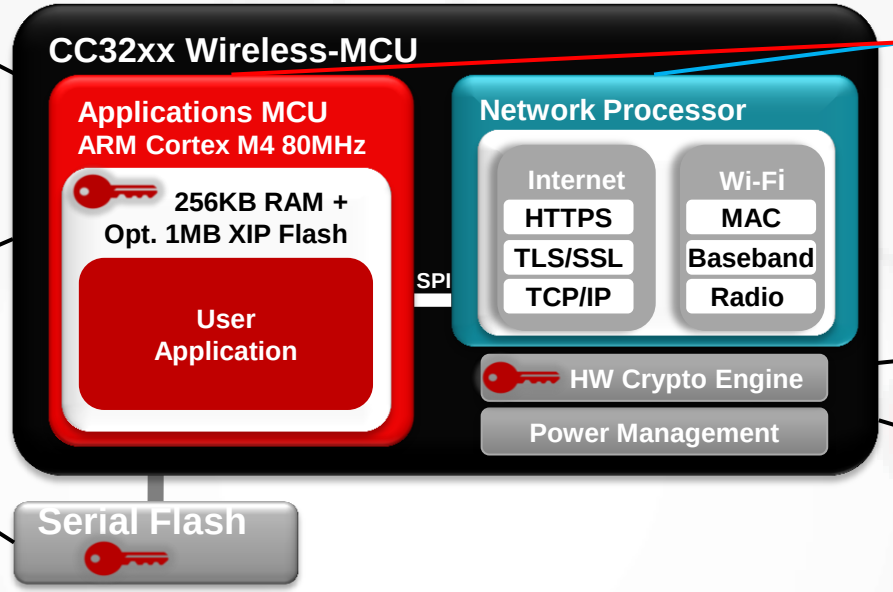
SimpleLink™ Wi-Fi® CC3220
Security Offering

Unique Architecture - Wide Set of Security Features

Single chip enclosed architecture for reduced attack surface

Embedded security features reduce the need for external secure components

Encrypted File System for Customer IP/data and end user's data security



2 Separate execution environments: MCU + NWP for enhanced assets isolation and easy application integration

HW crypto engines offload the MCU and enable fast TLS\SSL secure connection establishment within 200msec

Cryptographic utilities simplify sign & verify operations to validate the authenticity of any new image

Software

- File system security*: Encryption, Access control, Authentication, Bundle protection, Software tamper detection*, Cloning protection
- Initial secure programming*
- Secure Boot

Embedded HW

- Hardware Crypto Engine for advanced fast security, including: AES, DES, SHA/MD5, and CRC.
- Device-Unique Key
- Debug Security*: JTAG and Debug Ports can be Locked

Networking

- Personal and enterprise security: WPA/WPA2 PSK, WPA2 Enterprise
- **16** Sockets**, 6** (SSLv3/TLS1.2)
- Embedded HTTPS Server
- Unique Device Identity
- Trusted Root-Certificate Catalog
- TI Root-of-Trust Public key

*CC3220S and CC3220SF

SimpleLink™ Wi-Fi® – Multi Layer Security Measures

Hardware Crypto Engines

Trusted Root-Certificate Catalog

Debug Security

Secure Sockets (TLS\SSL)

File System Security

Unique Key - Cloning Protection

Device Identity

Software Tamper Detection

Secure Key Storage

File Encryption

Secure Content Delivery

File Authentication

TI Root of Trust Public Key

Personal and Enterprise Wi-Fi Security

File Access Control

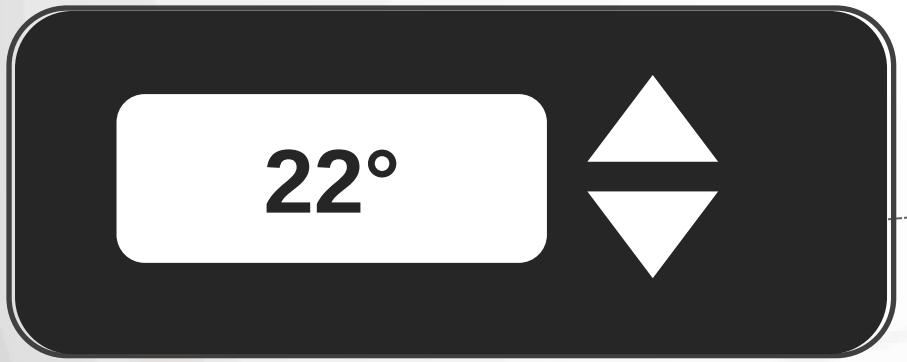
HTTPS Service

Factory Image Recovery

File Bundle Protection

Secure Boot

Initial Secure Programming



Access Point

Internet

Application Servers

Vendor

User

STORAGE

RUN-TIME

TRANSFER

Physical Access

Local Network Access

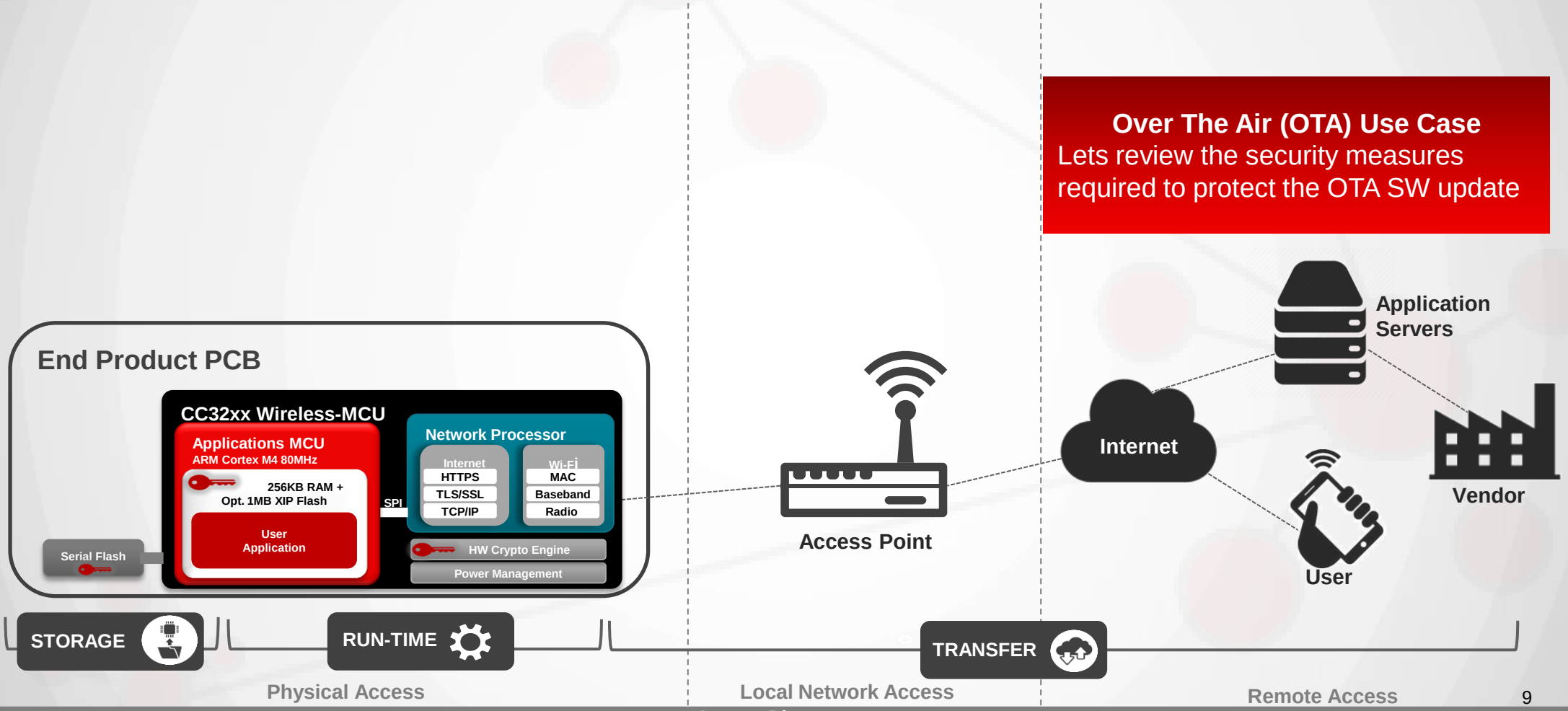
Remote Access

Access Distance

Security Measures to Help Protect

CODE in TRANSFER

Over The Air (OTA) Use Case
Lets review the security measures required to protect the OTA SW update



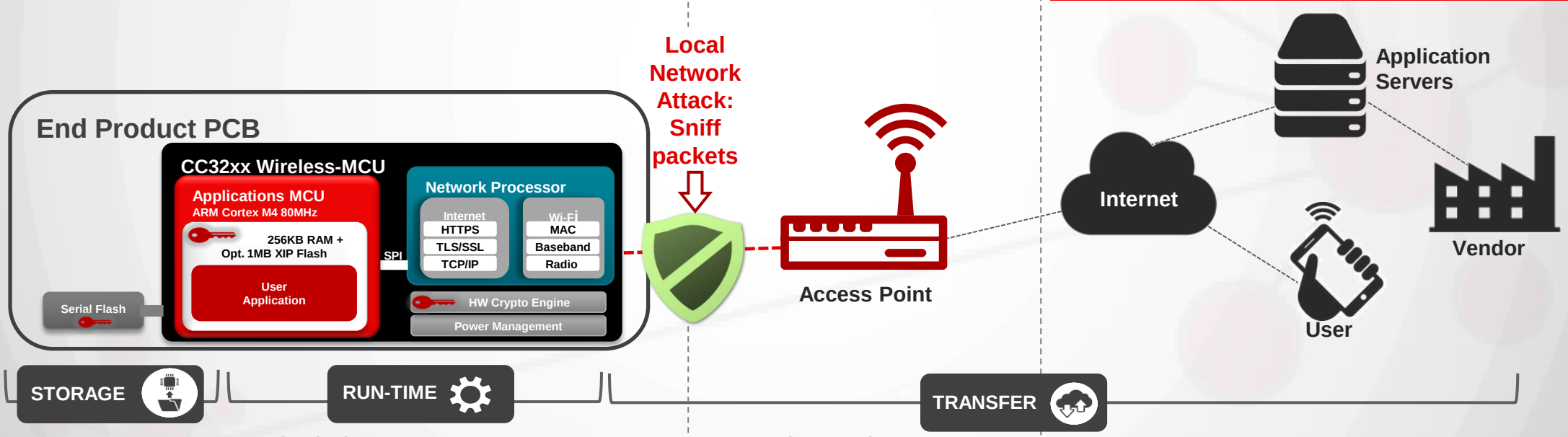
Security Measures to Help Protect CODE in TRANSFER

Hardware Crypto Engines

Local network with WPA/WPA2 encryption by the HW crypto engines, offloading the host

Personal and Enterprise Wi-Fi Security

OTA Use Case – step #1
The SimpleLink device opens a secured Wi-Fi connection to the Access-Point



Texas Instruments

Security Measures to Help Protect CODE in TRANSFER

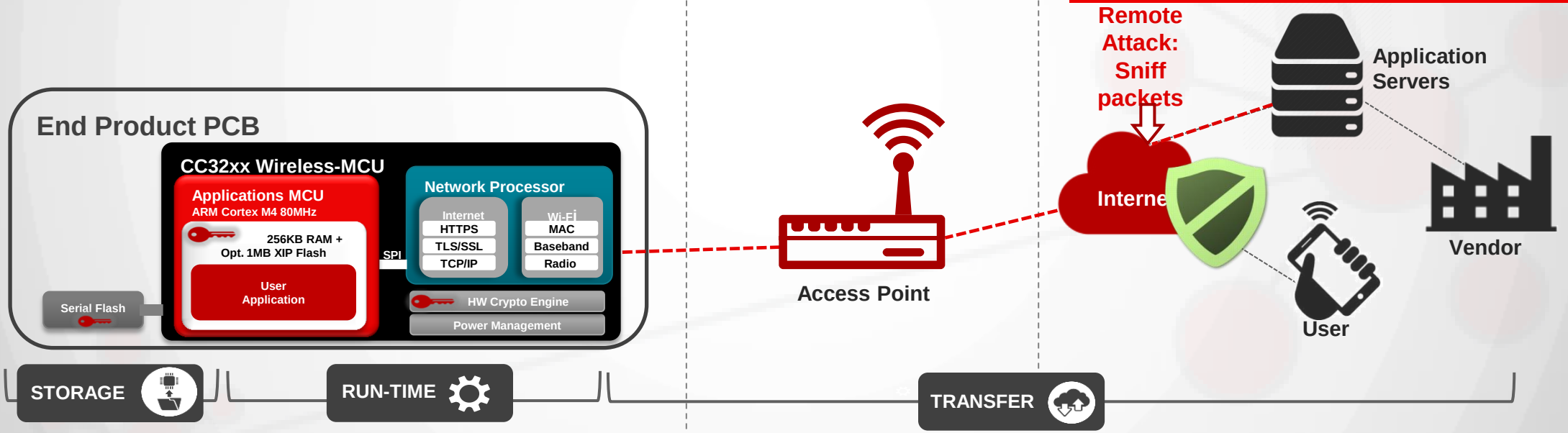
Hardware Crypto Engines

HW encryption engines establish a fast TLS/SSL internet connection within <200mSec

Secure Sockets (TLS\SSL)

TLS/SSL are in the NWP, within the BSD Socket layer

OTA Use Case – step #2
The SimpleLink device opens a secured TLS connection to the application cloud server



Security Measures to Help Protect CODE in TRANSFER

Hardware Crypto Engines

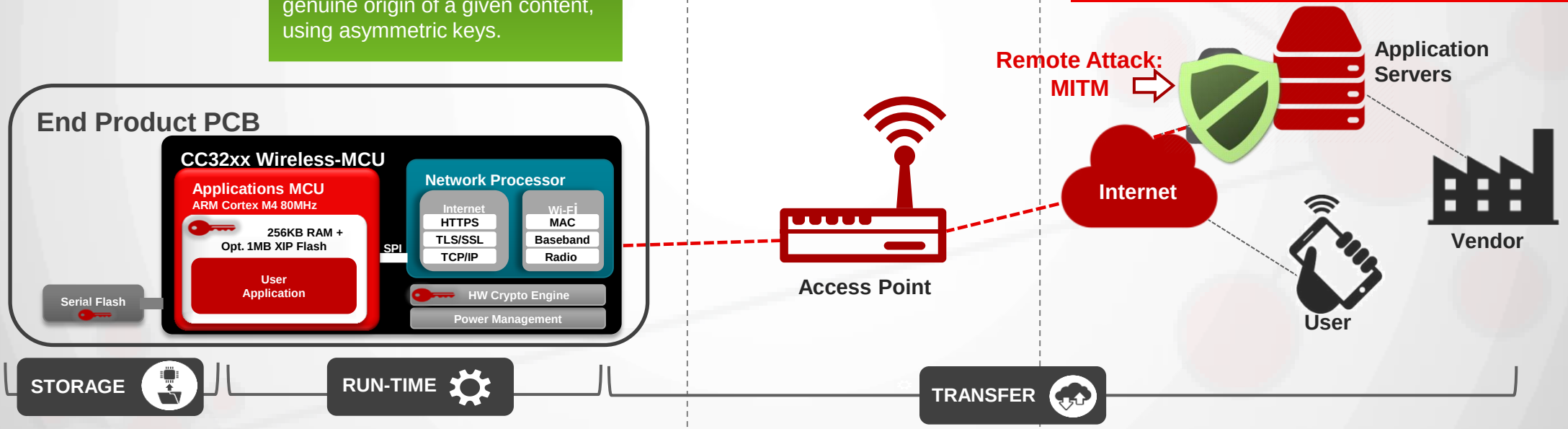
Trusted Root-Certificate Catalog

Built-in secure mechanism to ensure a CA is trusted as root of certificate chain for TLS purpose and file signing.

TI Root of Trust Public Key

HW-based mechanism that allows authenticating TI as the genuine origin of a given content, using asymmetric keys.

OTA Use Case – step #3
During the TLS connection the server is authenticated to the SimpleLink's trusted root certificate catalog



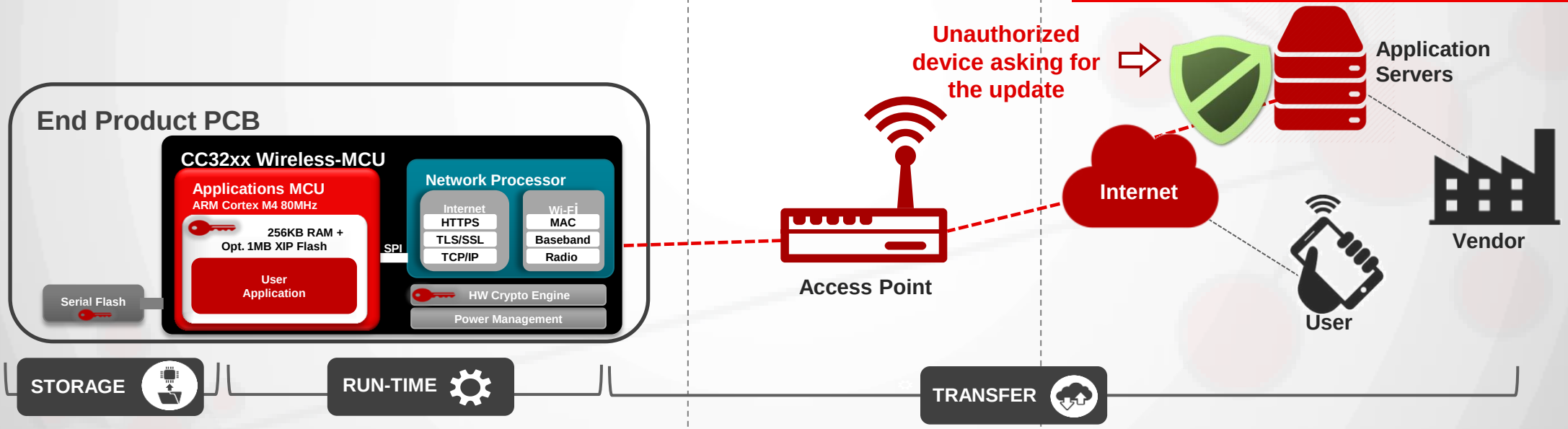
Security Measures to Help Protect CODE in TRANSFER

Hardware Crypto Engines

Device Identity

Unmodifiable unique 128-bit number that TI burns into the device during production

OTA Use Case – step #4
The simplelink device uses its unique device identity in order to be validated and approved to continue with a SW update



Security Measures to Help Protect CODE in TRANSFER

Hardware Crypto Engines

File System Security

Keeps the system's integrity by avoiding intermediate mixture

File Bundle Protection

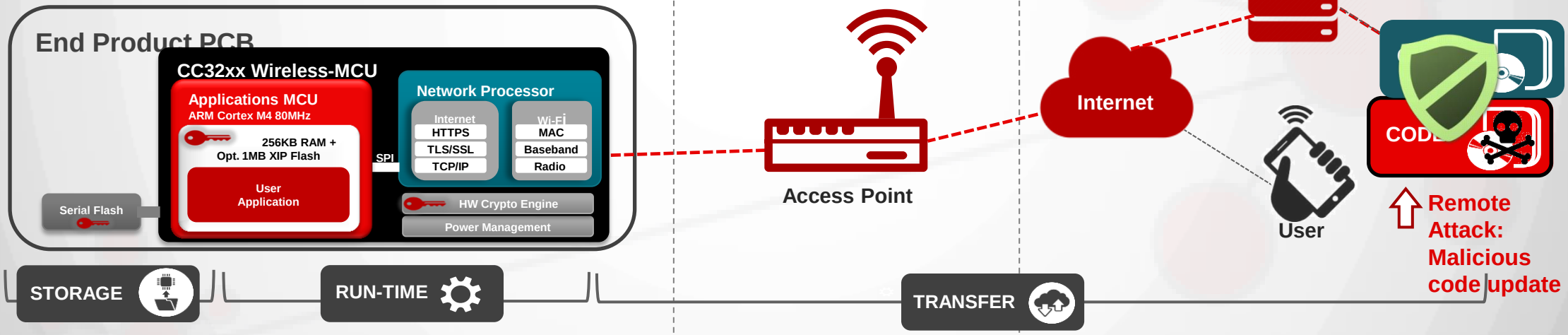
Secure Key Storage

Secure Content Delivery

Provides an end-to-end ability for delivering confidential information to the system independent of the security of the transport layer.

On-chip asymmetric key-pair storage with built-in crypto acceleration and crypto services

OTA Use Case – step #5
Using the secure content delivery the device retrieves the SW image from the application server to the device



Security Measures to Help Protect CODE in STORAGE

Hardware Crypto Engines

File System Security

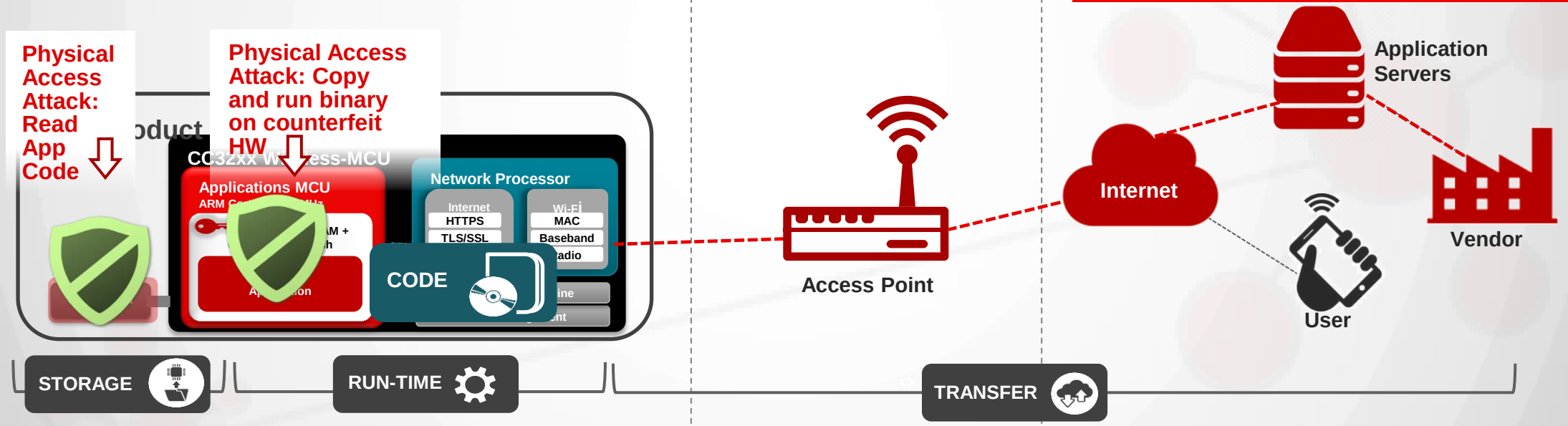
Unique Key - Cloning Protection

The file system is readable only by the device which first booted the image

File Encryption

File system is encrypted so image cannot be read

OTA Use Case – step #6
The updated files access control and authenticity are validated and then stored on the simplelink's secured file system



Security Measures to Help Protect

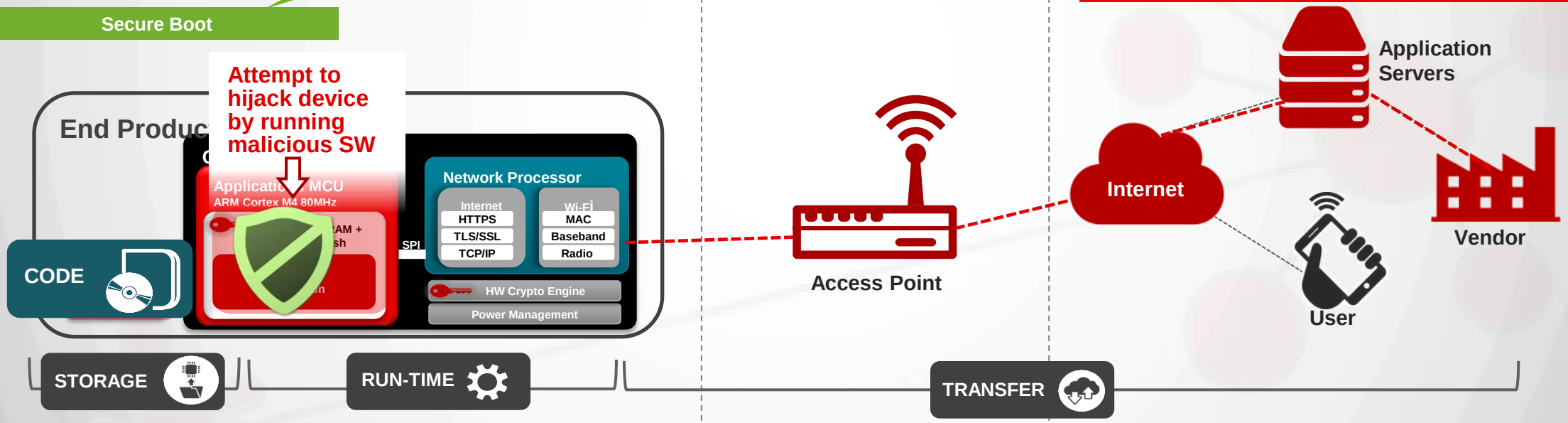
CODE in RUN-TIME

Hardware Crypto Engines

Validate the integrity and authenticity of the run-time binary during boot

Secure Boot

OTA Use Case – step #7
At boot the application code is loaded and run on the MCU



Texas Instruments

Multi Layer Security Measures- All Embedded in the SoC

Hardware Crypto Engines

Trusted Root-Certificate Catalog

Debug Security

Secure Sockets (TLS\SSL)

File System Security

Unique Key - Cloning Protection

Device Identity

Software Tamper Detection

Secure Key Storage

File Encryption

Secure Content Delivery

File Authentication

TI Root of Trust Public Key

Personal and Enterprise Wi-Fi Security

File Access Control

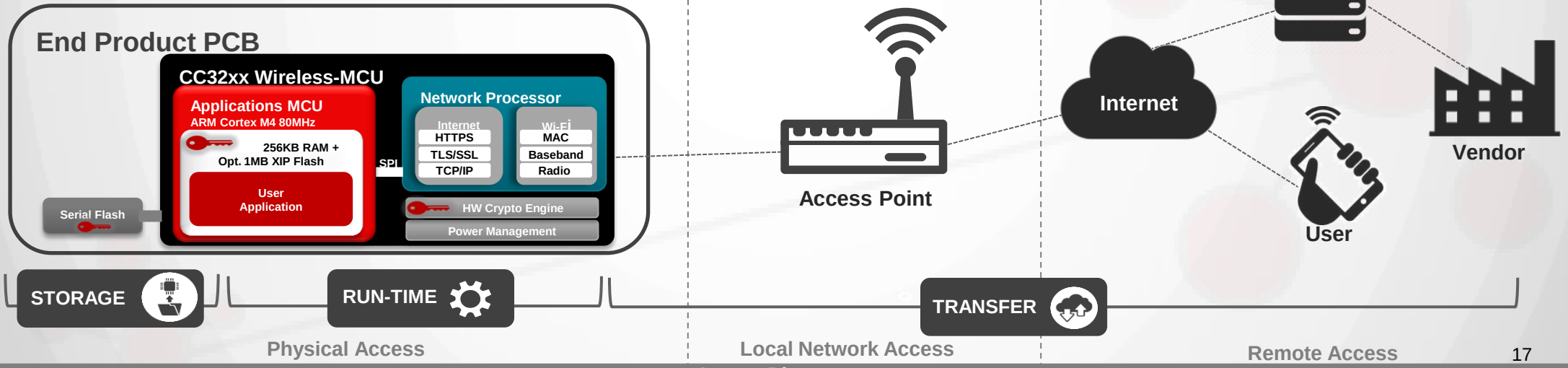
HTTPS Service

Factory Image Recovery

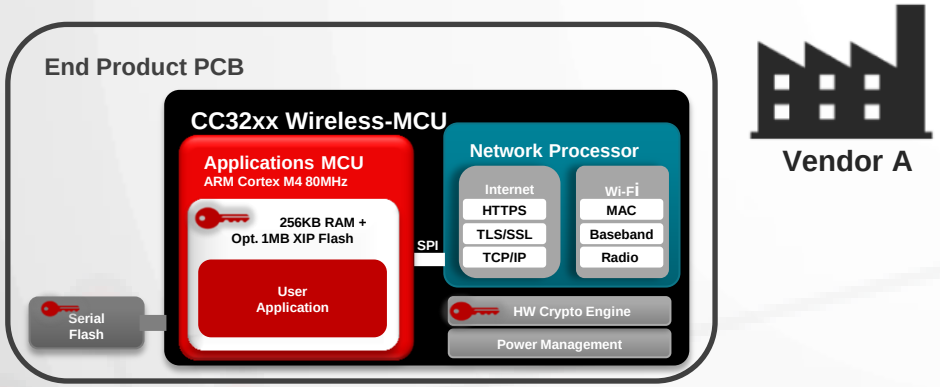
File Bundle Protection

Secure Boot

Initial Secure Programming



File System Security Features – Cloning protection



Vendor A

Cloning Protection

The entire file system content is only readable by the NWP which first booted that image

File System Security Features – Cloning protection

Hardware Crypto Engines

File System Security

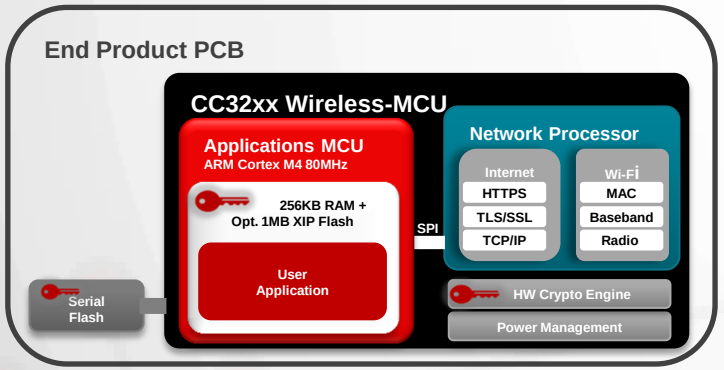
Unique Key - Cloning Protection

File Encryption

The file system, including the user's IP, are encrypted using a unique key per device

Cloning Protection

The entire file system content is only readable by the NWP which first booted that image



Vendor A

File System Security Features – Cloning protection

Hardware Crypto Engines

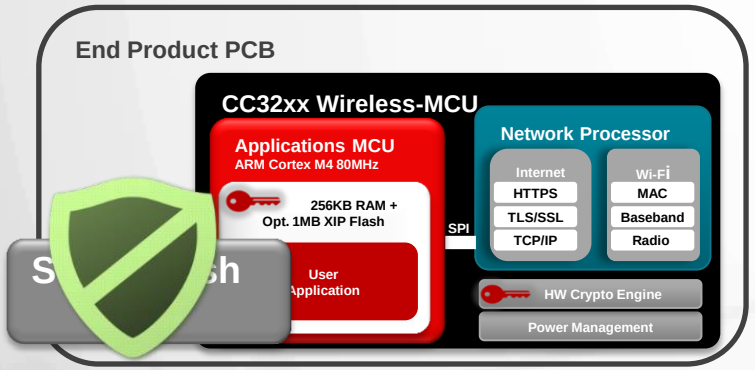
File System Security

Unique Key - Cloning Protection

File Encryption

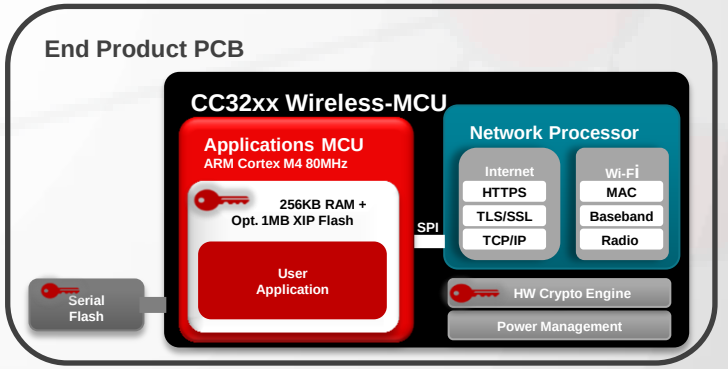
If the content of the serial flash has been copied or the serial flash itself has been connected to a different device from the one it was first initiated with.

Cloning Protection
The file system, including the user's IP, are encrypted using a unique key per device.



Vendor A

Vendor B



File System Security Features – Cloning protection

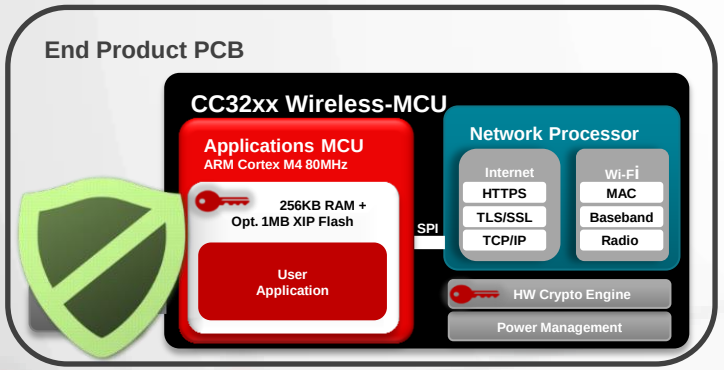
Hardware Crypto Engines

File System Security

- **Unique Key - Cloning Protection**
- **File Encryption**
- **Secure Boot**

During the boot process, the NWP will notice the difference in the file system
➔ **The device will enter a lock state**

Cloning Protection
The file system, including the user's IP, are encrypted using a unique key per device.

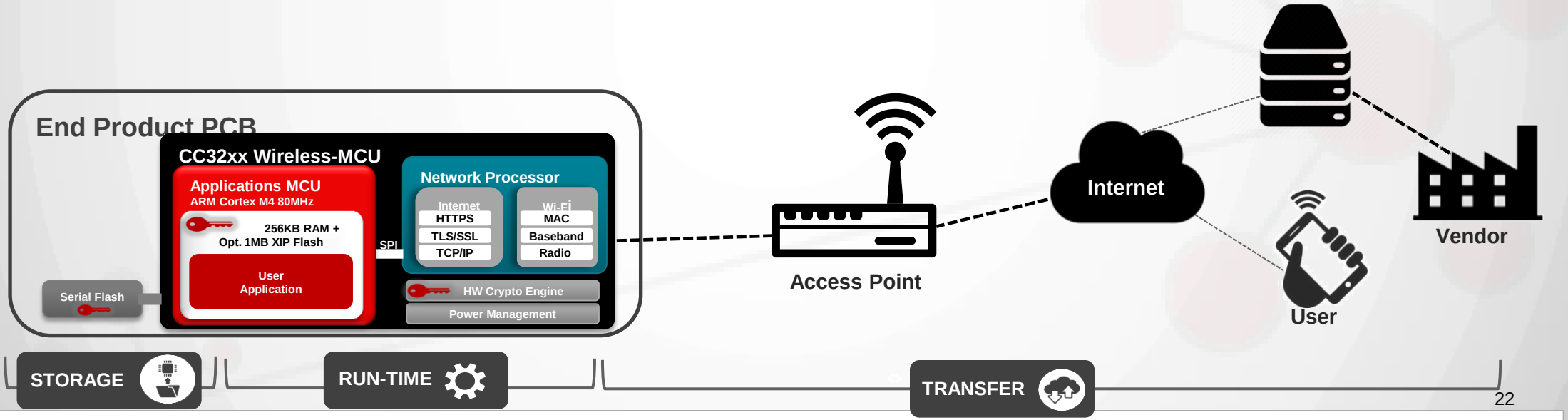


Vendor A

Vendor B

File System Security Features – SW Tamper Detection

Tamper Detection
Tamper detection monitors the use of files and detects attempts to tamper the file system without proper authorization



File System Security Features – SW Tamper Detection

Hardware Crypto Engines

Trusted Root-Certificate Catalog

File System Security

Software Tamper Detection

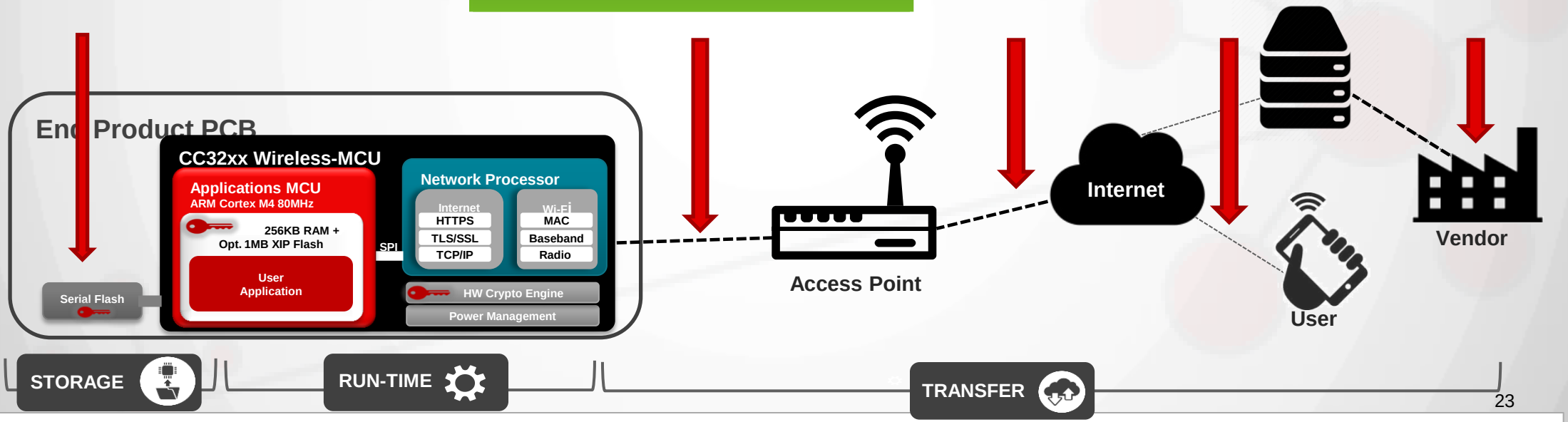
File Authentication

File Access Control

Secure Boot

The secure files can be encrypted, or encrypted and authenticated.
Access to these files requires the correct access token

Tamper Detection
Tamper detection monitors the use of files and detects attempts to tamper the file system without proper authorization



File System Security Features – SW Tamper Detection

Hardware Crypto Engines

Trusted Root-Certificate Catalog

File System Security

Software Tamper Detection

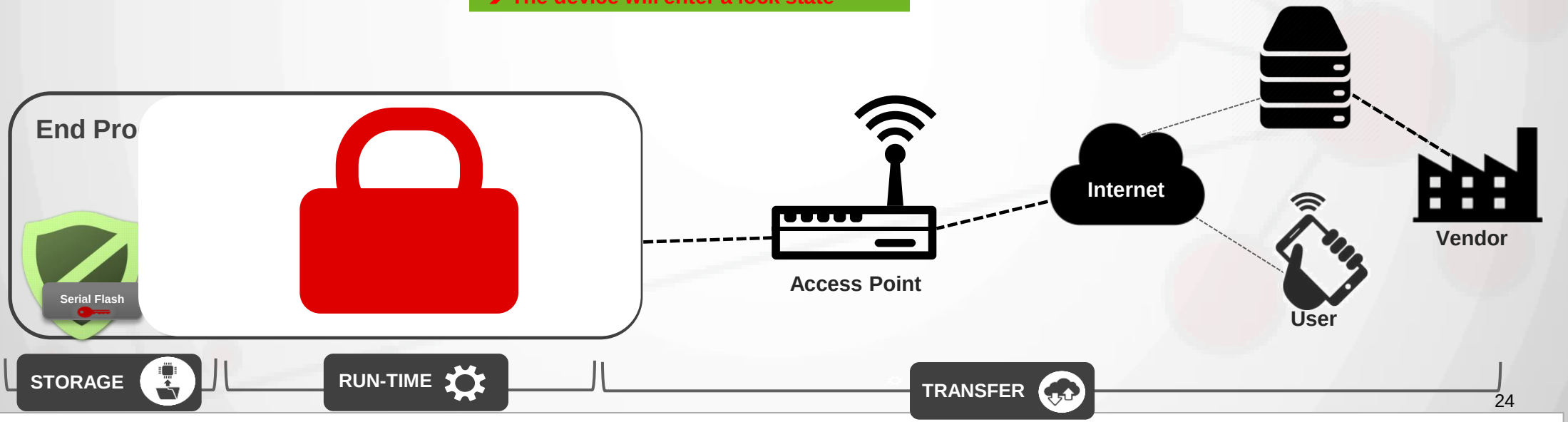
File Authentication

File Access Control

Secure Boot

When detecting data tampering, the data tampering procedure increases the system security-alert counter. When the system reaches the security-alerts threshold
➔ **The device will enter a lock state**

Tamper Detection
Tamper detection monitors the use of files and detects attempts to tamper the file system without proper authorization



Multi Layer Security Measures- All Embedded in the SoC

Hardware Crypto Engines

Trusted Root-Certificate Catalog

Debug Security

Secure Sockets (TLS\SSL)

File System Security

Unique Key - Cloning Protection

Device Identity

Software Tamper Detection

Secure Key Storage

File Encryption

Secure Content Delivery

File Authentication

TI Root of Trust Public Key

Personal and Enterprise Wi-Fi Security

File Access Control

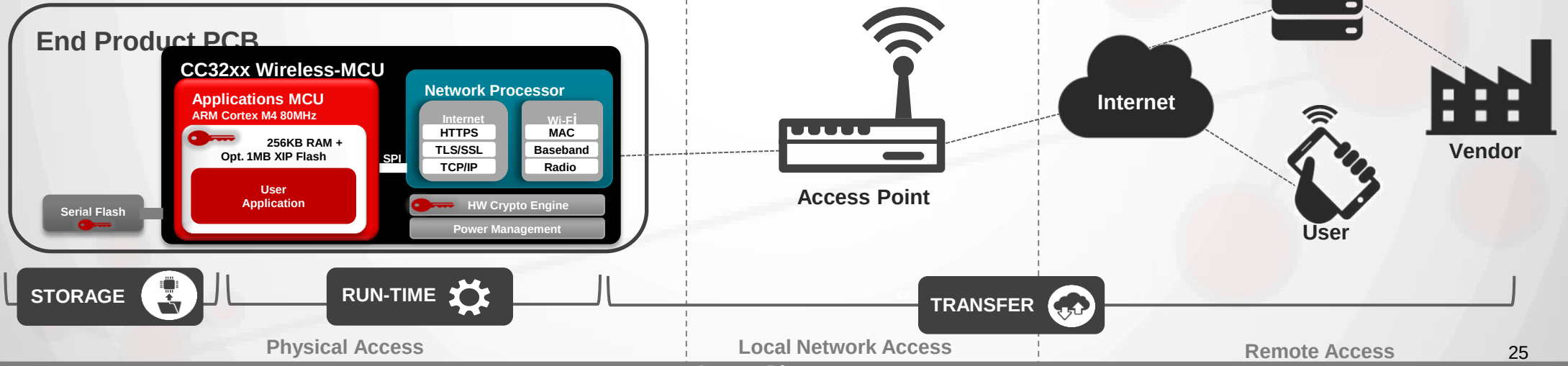
HTTPS Service

Factory Image Recovery

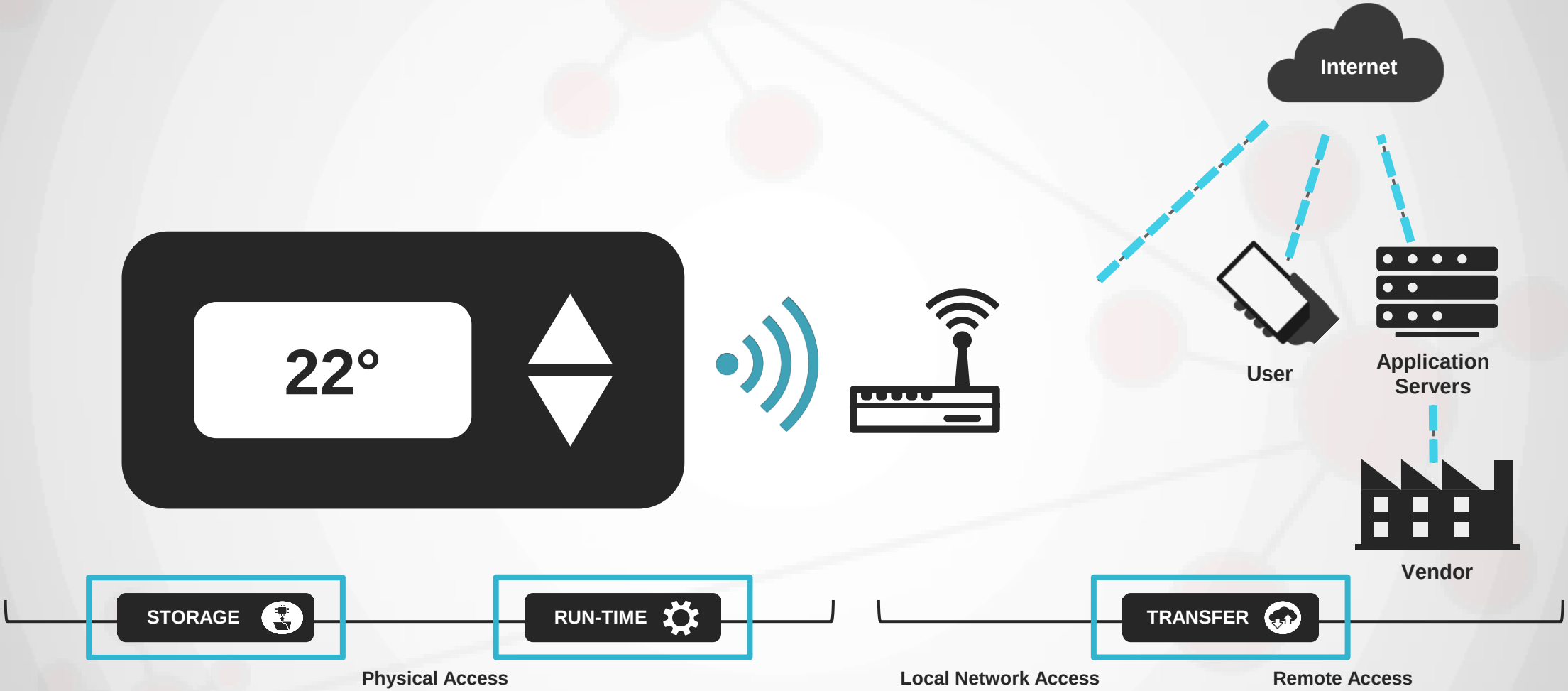
File Bundle Protection

Secure Boot

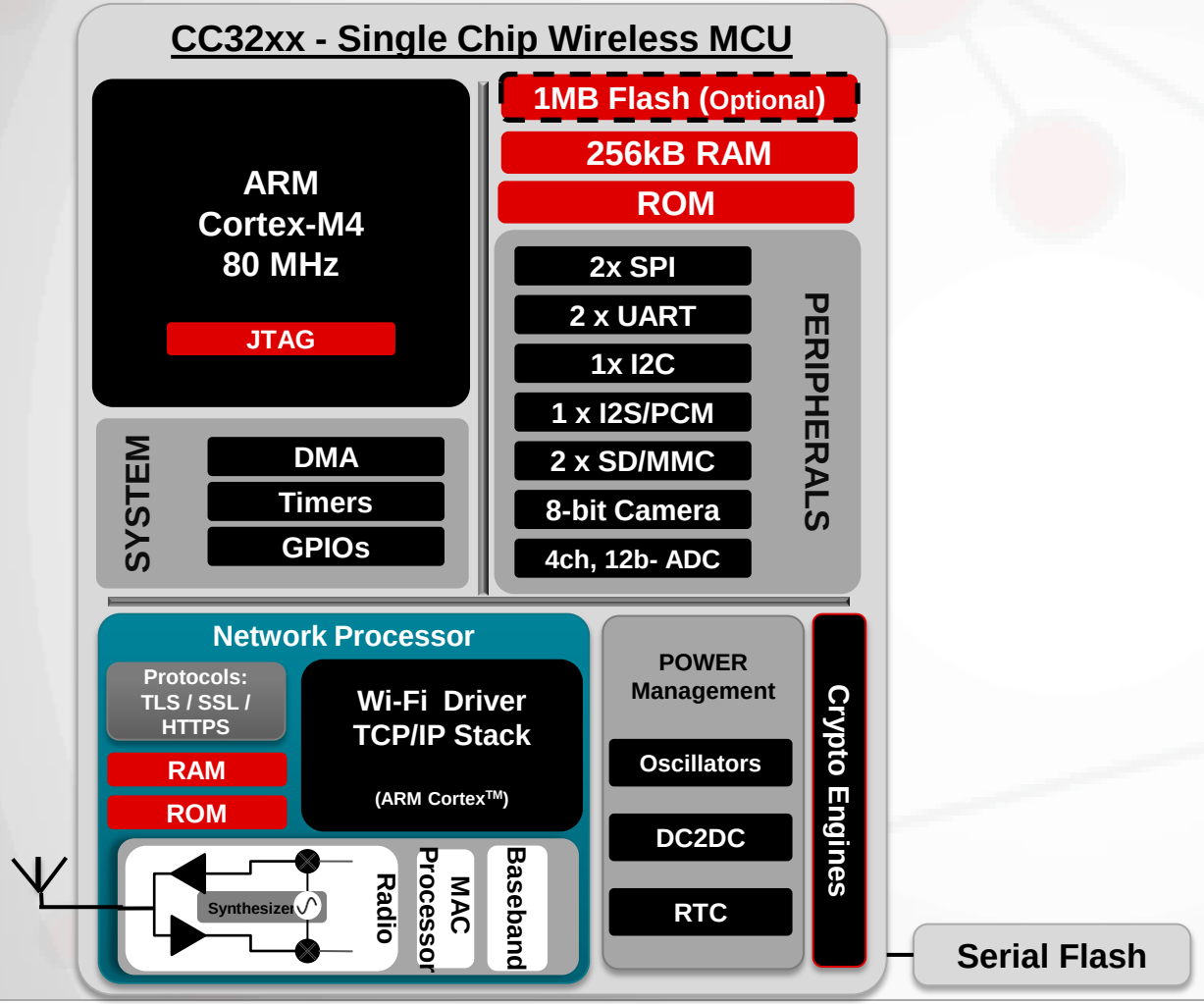
Initial Secure Programming



Comprehensive end-to-end security



SimpleLink™ Wi-Fi® Wireless MCU CC3220 - NWP



Network Processor

The network processor offloads networking and internet tasks from the application MCU

Wi-Fi Core

- 802.11 b/g/n at 2.4GHz
- Modes: STA, AP (4 stations), Wi-Fi Direct®
- Wi-Fi Security: WEP, WPA, WPA2
- Provisioning: AP mode, SmartConfig™, WPS
- Throughput: 16 Mbps UDP, 13Mbps TCP

Built In Power Management

- Integrated DC2DC
  - V_{Bat}: **2.1** V to **3.6** V
  - Pre-regulated:**1.85** V
- Low power modes
  - Shutdown(**1uA**)
  - Hibernate (**4.5uA**),
  - Low power deep sleep (**135uA**)
  - Rx beacon listen (**37mA**)

Internet & Application Protocols

- Embedded webserver (HTTPs)
- Supports IPv4 & IPv6 TCP/IP Stack
- **16** Sockets (**6** TLS v1.2 / SSL 3.0)

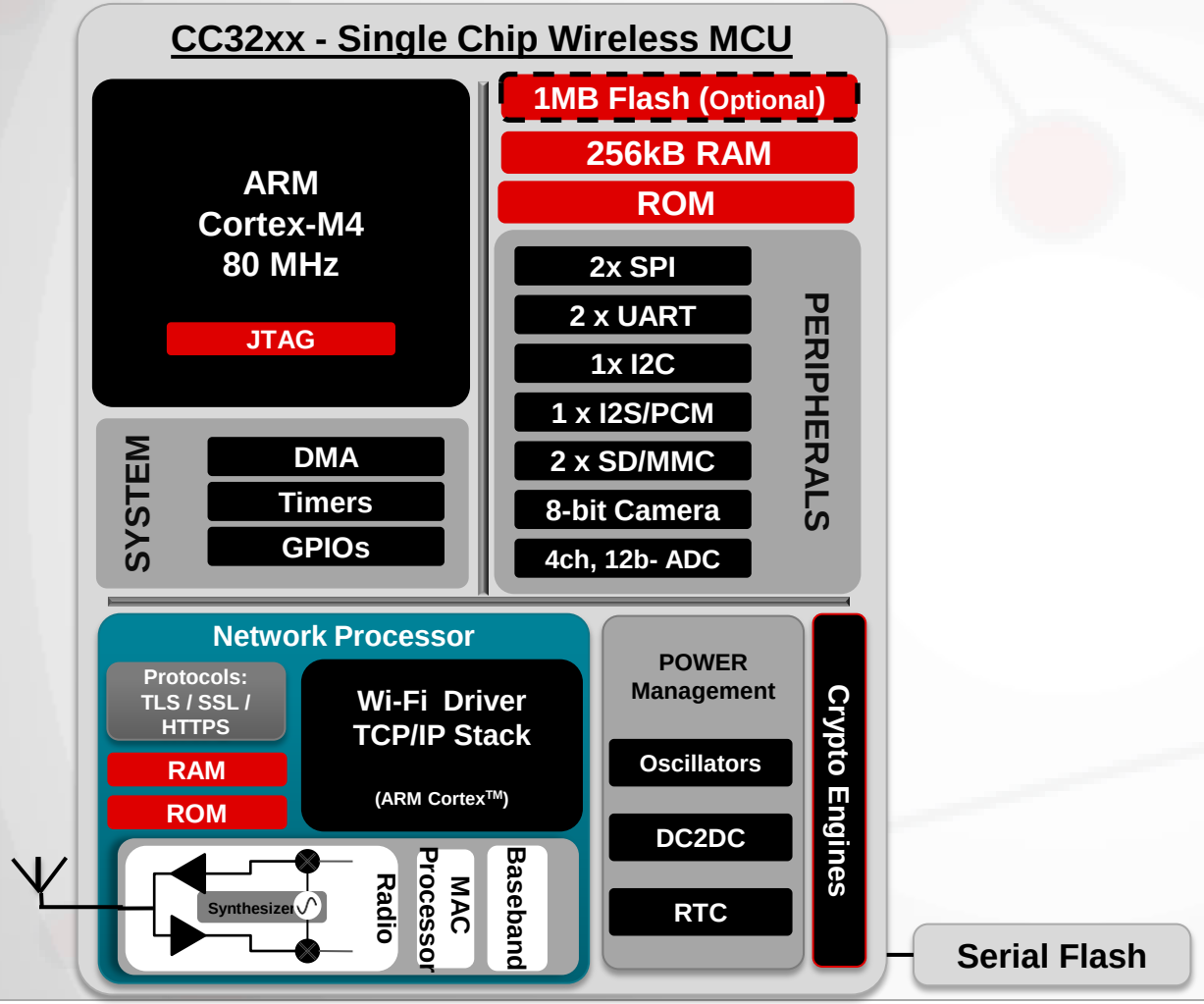
Powerful HW Crypto Engine

- Enables fast secured Wi-Fi and internet connections within 200mSec

Industrial Temp

- Supports -40^{0}C to +85 ^{0}C

SimpleLink™ Wi-Fi® Wireless MCU CC3220 - MCU



Applications MCU

Physically separate MCU and memory, dedicated to the user's applications.

Programmable Applications MCU
- Peripheral drivers and Libraries
- Supports no-OS or TI-RTOS/Free-RTOS

Application-dedicated Memory
- **256KB RAM**
- Additional **1MB XIP Flash** (CC3220SF)

Rich Set of Peripherals & Timers
- 27 I/O pins with flexible muxing options
- 4x General purpose (with PWM support)

Enhanced Features

Rich multi-layer set of **security features,** within a single chip**,** to help protect **IP** and **data**
- TI Root-of-trust and TI Certificate catalog
- File System Security
- Cloning protection
- Initial secure programming
- Secure content delivery

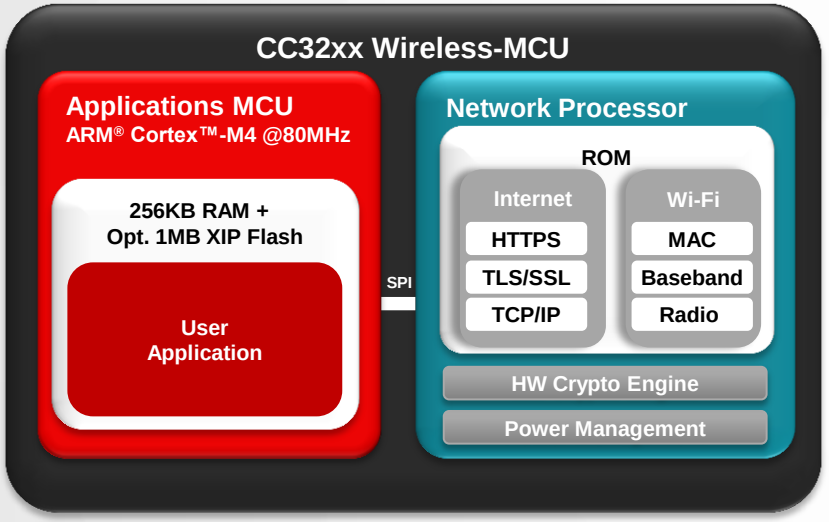
- Enabling Applications with **HomeKit** Technology
- OTA support
- SimpleLink™ **Connected MCU** Platform support

SimpleLink™ Wi-Fi® Wireless MCU CC3220

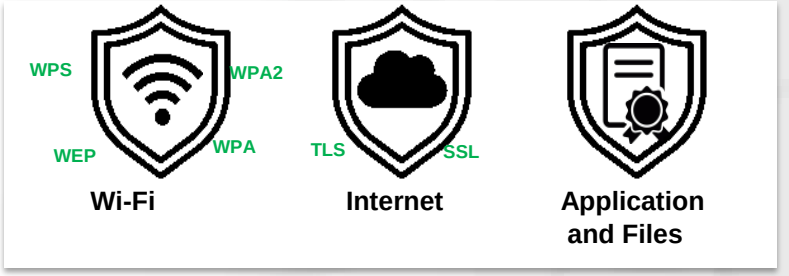
Low Power, Advanced Security, Easy Integration

Lowest Power

Run for Years
on 2xAA Batteries



Multi Layered Security Features



Wi Fi CERTIFIED

Texas Instruments

Learn More

1. Visit www.ti.com/simplelinkwifi

2. Specific Documents
   - CC3220S/SF, Single chip Wireless MCU Solutions: http://www.ti.com/product/cc3220
   - Security App Note: http://www.ti.com/lit/pdf/swra509

3. Tools / EVMs
   - CC3220S-Launchpad: http://www.ti.com/tool/cc3220s-launchxl
   - CC3220SF-Launhchpad: http://www.ti.com/tool/cc3220sf-launchxl

Development Kits

4. TI E2E Support Community
   - www.ti.com/cc3220help

   Ask questions, share knowledge, explore ideas, and help solve problems with fellow engineers

Thank you