Industry Demand

What stakeholders want:

• Secure connectivity for general purpose, low-power, mass-market devices to enable remote management and monitoring
• SMCU-based offerings that can integrate easily with existing IoT services and cloud platforms
• Appropriate hardware and associated software to allow for identification, authentication, integrity & confidentiality
• Secure programming, provisioning, onboarding & lifecycle management
• An emerging market of secure MCUs packaged with software development platforms

What vendors are offering:

• New class of general purpose secure MCUs for the IoT (emerging in 2017)
• Primarily based on Arm Cortex M4 cores (M0 - M7 variations as well, especially for dual core offerings) & Arm V7M architecture
• Newer offerings out this year based on Arm Cortex M23 & M33 and Arm V8M with TrustZone TEE (M35P with tamper resistance built-in)
# Competitive Offerings:

**Vendor Ecosystem**

<table>
<thead>
<tr>
<th>MEDIATEK</th>
<th>ST</th>
<th>REDPINE SIGNALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>life.augmented</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maxim Integrated</th>
<th>Microchip</th>
<th>Cypress</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>nuvoton</th>
<th>NXP</th>
<th>Renesas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note other application-specific MCUs include Infineon Aurix (automotive), Goodix GM6256 (fingerprint), TI Simplelink (Wi-Fi)
# Technology Highlight:

## Hardware

### Security Processor
- Security Subsystem
- Internal Crypto Engines
- Co-processor (dual core)

### Root of Trust
- Secure Boot
- Unique ID (128-bit)
- PUF

### Secure Execution Environment
- Arm Trusted Firmware-M
- Trustonic Kinibi-M
- Microsoft Pluton Security Subsystem (Azure Sphere)
- TrustZone TEE
- Hardware Firewalls

### Cryptography
- Symmetric (AES, DES/3DES)
- Asymmetric (ECC, RSA, DSA)
- Hash Functions (SHA)
- TRNG, PRNG

### Secure Memory
- Secure key / certificate storage
- Flash readout protection
- Memory Protection Unit
- Hardware Firewalls
- Peripheral Protection
- OTP Flash, e-fuse block

### Tamper Resistance
- Time-stamped
- Anti-tamper pins
- Voltage, clock, temp, optical, glitch detection
- CRC, ECC, Parity, Watchdog
- Zeroizable memories

### Certification
- Arm Platform Security Architecture (PSA)
- NIST FIPS 140-2
- NIST Cryptographic Algorithm Validation Program (CAVP)
## Technology Highlight:
### Software and Services

<table>
<thead>
<tr>
<th>SOFTWARE DEVELOPMENT</th>
<th>INTEROPERABILITY WITH 3RD PARTIES</th>
<th>ONBOARDING &amp; PROVISIONING</th>
<th>LIFECYCLE MANAGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proprietary: MCUXpresso, PSoC Creator, X-Cube, NuSMP, Synergy SP</td>
<td>Software, network, communications, key management</td>
<td>Cloud Enrollment (Azure, AWS, Google)</td>
<td>Secure FOTA updates</td>
</tr>
<tr>
<td></td>
<td>WolfSSL</td>
<td>Remote Attestation</td>
<td>Security Analytics</td>
</tr>
<tr>
<td></td>
<td>Segger emCrypt</td>
<td>Certificate-based Authentication</td>
<td>Troubleshooting, Failure Reporting, etc.</td>
</tr>
<tr>
<td></td>
<td>Pluton Key Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amazon FreeRTOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AWS and Google Cloud IoT Core (both use x.509)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arm Pelion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure Sphere Security Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trustonic end-to-end solution support</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data I/O SentiX secure provisioning platform</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SecureThingz Key Provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arm Pelion</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Azure Sphere Security Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure Thingz Secure Deploy Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Arm Trusted Firmware-M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Global Shipments of Secure MCUs

- Shipments start around 2018 (sub 50 million), 2019-2023 CAGR 58%
- 2019-2020 slight pressure on growth from current manufacturing recession & uncertain political climate (i.e. US trade/tariff pressure on China & EU), & newness of technology
- Uptick from 2021 onwards with maturing market demand, movement from early adopters to mass market, additional security features, lowering ASPs (esp. for M4 cores) & increased competition
Target Markets and Applications

**Smart Cities & Buildings**
Commercial Building Automation, Smart Parking, Smart Street Lighting, Environmental Monitoring, Video Surveillance, Enterprise Access Points

**Utilities & Industrial IoT**

**Smart Home**
Home Automation Controllers, Smart Home Devices, Smart Appliances, Smart Home Lighting Units

**Wearables**
Health and Medical, Sports, Fitness, and Wellness Devices, Smartwatches, Smart Glasses

**Other**
POS, ATMs, Kiosks, Vending Machines, Digital Signage, Asset Tracking, Inventory Management, Beacons, Robotics
Shipment Forecast of Secure NCUs by Sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
<th>2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>25.41</td>
<td>32.60</td>
<td>40.42</td>
<td>49.75</td>
<td>61.02</td>
</tr>
<tr>
<td>Utilities and Industrial IoT</td>
<td>22.36</td>
<td>30.99</td>
<td>51.33</td>
<td>74.63</td>
<td>107.17</td>
</tr>
<tr>
<td>Smart Cities and Buildings</td>
<td>13.08</td>
<td>19.29</td>
<td>39.97</td>
<td>74.63</td>
<td>127.72</td>
</tr>
<tr>
<td>Wearable</td>
<td>0.88</td>
<td>1.48</td>
<td>3.70</td>
<td>8.89</td>
<td>15.99</td>
</tr>
<tr>
<td>Smart Home</td>
<td>7.82</td>
<td>24.27</td>
<td>51.82</td>
<td>94.76</td>
<td>121.29</td>
</tr>
</tbody>
</table>

*Note: Millions*
Market Outlook

**Adoption**
Success will depend on cost & usability of hardware & development platforms but especially on the service/cloud connectivity piece.

**Competition**
Emerging cross-over between microcontrollers and application processors will increase competition, pushing dual core offerings, such as NXP iMX, Samsung Exynos i (T200, T100, S111), leveraging Arm Cortex A & M (for dual core).

**Technology**
New Cortex M33 for next generation of Secure MCUs to facilitate TrustZone use, but additional tamper resistance to be served by the Cortex M-35P in the following generation.

**Bottlenecks**
Secure provisioning services are still costly & technically challenging to implement, with the main obstacle around key management for less than 100k devices. Future offerings could focus on providing pre-provisioned secure elements with fixed configuration use cases for cloud authentication at low-cost.
ABI Research’s Digital Security Research Service offers end-to-end market coverage from information and communication technologies to operational control processes.
What Makes Our Research Different?

**Best-in-class Market Data**
We have the most comprehensive secure IC & smart card market data coverage. No other research firm can match the detail of our datasets.

**Close Vendor Relationships**
We maintain close relationships with the top vendors in the secure hardware space, ensuring that we have direct and accurate insight into shipment numbers.

**First to Publish on Emerging IoT & OT Security**
ABI Research was the first to identify and publish on a number of new market opportunities, including M2M security, critical infrastructure security, automotive cybersecurity, medical device security, IoT security, blockchain IoT applications, and secure MCUs.

LEARN MORE