SILICON LABS

The Future of Smart Home Design

It’s not hard to imagine where the smart home industry will be in the next few years. Science-fiction writers have been doing that for over a century. It’s another thing, however, to understand what needs to be done to enable the future smart home.

From a functional standpoint, the future of the smart home lies in improved user comfort, increased safety, and greater energy efficiency. To achieve this, it must become easier to take advantage of smart device capability. This will happen through the evolution of passively obedient devices that need to be manually controlled into actively intelligent ecosystems acting on our behalf. Put another way, the more successful a smart home is, the less people will notice how much it is doing. Eventually, thermostats and even light switches will be considered retro.

Artificial intelligence (AI) and machine learning (ML) are the primary technologies required to give smart devices at-the-edge autonomy. AI and ML will transform historically mundane passive devices into active ecosystem participants that bring value to users through their environmental awareness and decision-making capabilities.

In turn, the use of AI and ML at the edge will increase the need for security. Greater situational awareness drives a heightened need for AI and ML devices to be protected from those with malicious intent through increased security. This means devices that collect and store user data will need to protect the privacy and safety of users by preventing hackers from being able to use smart devices for their own purposes. Security is also required to protect IP from being stolen. Original equipment manufacturers (OEMs) invest a great deal in their AI models and don’t want them stolen and used in counterfeit products.

This article will explore what OEMs need to know about the future of smart home design in order to develop compelling smart devices. Starting with some of the ways that smart devices will improve ease of use, we will describe the role that AI and ML will have in enabling new capabilities and how security will need to be implemented to protect users, devices, and OEMs.

EASE OF USE

Smarter is Easier

Many of today's smart home devices are what could be called passively obedient. Devices do as they are told to do when they are told to do it. Users can schedule tasks, like turning on the coffee pot five minutes before the morning alarm is set to go off. Users can also make rules, such as turning on the air conditioner when the temperature rises to a set threshold.

But schedules and rules are still the system just doing what it has been told to do. Lights can be programmed to turn themselves off at night to save electricity, but a person still determined that this was a good idea. In terms of efficiency, a passively obedient smart house can save only as much energy as a person is able — and willing — to decide and program.

An actively intelligent smart home learns a family's patterns and preferences through observation and inference. Using this data, the smart home can then independently make decisions without human input. A person should be able to oversee — and override — these decisions, but the logic behind them is handled primarily by the home and influenced by learned user preferences. These decisions can consider many factors that users simply do not want to think about or manually program.

The more intelligence in a system, the more ways its performance can be optimized. Consider the following examples of how a smart home can use electricity more efficiently:

PRESENCE

Lights and HVAC are turned on and off based on a person's presence in the house or a room. Presence is determined using in-room sensors. This enables the HVAC system to not only turn on the A/C in the given rooms a person is using, but to also adjust the temperature to that person's preference.

ENVIRONMENT

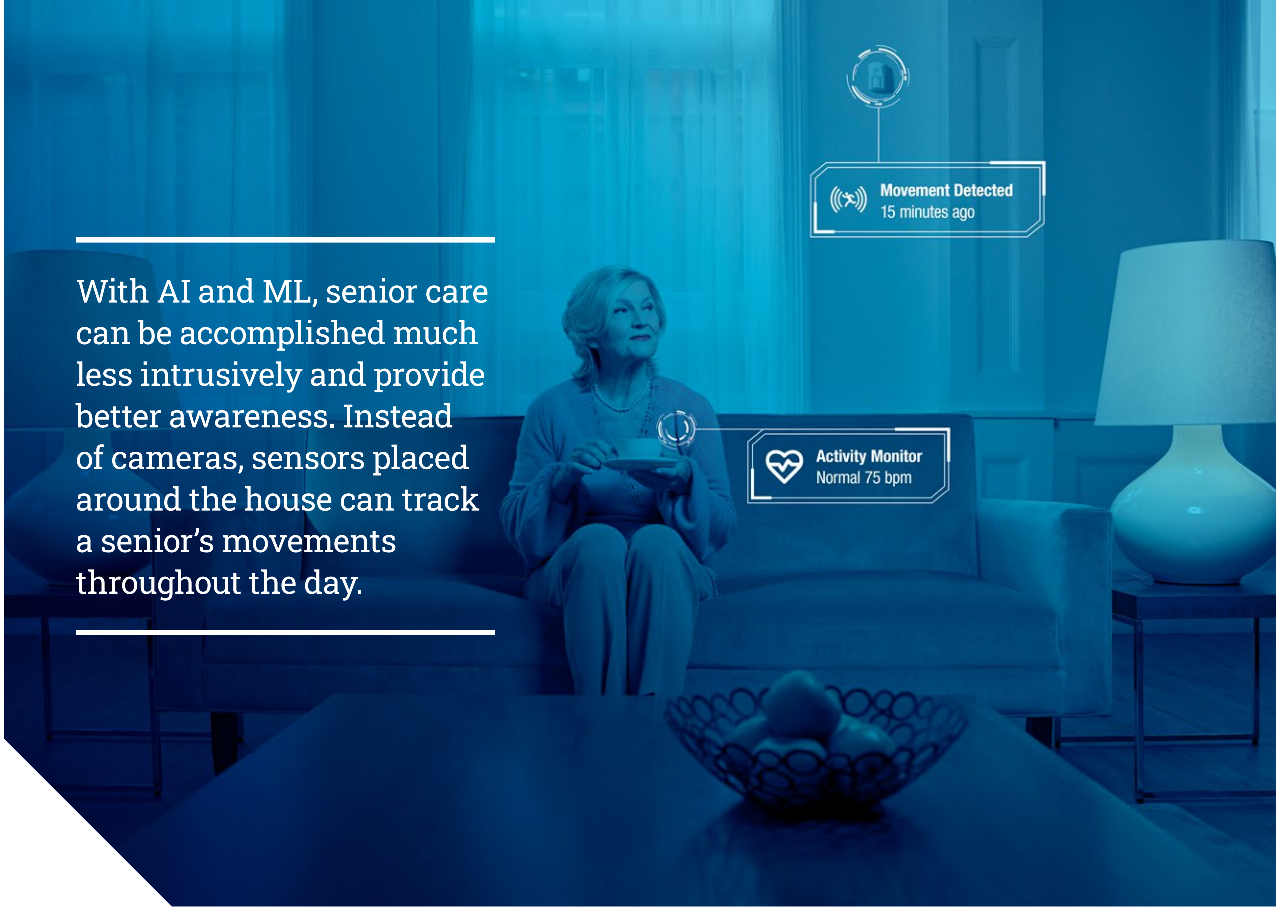
The smart home could track daylight hours and change schedules a few minutes each day to adjust for longer or shorter days. Similarly, a watering system can shut down when it is raining or slowly increase watering periods as spring turns into summer.

PREDICTION

The HVAC system turns on when a person is anticipated to be coming home. For example, a typically traditional thermostat may be limited to the same program for all weekdays. A smart thermostat could learn that the family typically goes out for dinner after work on Friday nights and wait until later to turn on the heat.

An intelligent smart home can be much more flexible than a passively obedient home. Programmed rules must generalize preferences for everyone living in the home, but an intelligent smart home can profile the habits and preferences of each person individually.

When only one person is home, the house can optimize performance based on this person's habits and preferences. When several people are home at the same time, the house could give priority to one person, if that is desired.



With AI and ML, senior care can be accomplished much less intrusively and provide better awareness. Instead of cameras, sensors placed around the house can track a senior's movements throughout the day.

AI AND ML

Improving Energy Efficiency, Safety, and Comfort

One area in which the smart home can demonstrate real value is in senior care and monitoring. Many seniors want to maintain their autonomy, but their adult children want to check in on them regularly to make sure they haven't fallen and gotten hurt or forgotten to take their medication.

Panic buttons were one of the first senior monitoring technologies. However, panic buttons had to be manually pressed so a senior who fell and dropped the button could not trigger the alarm. Panic buttons also had the problem of being easily activated accidentally.

Early senior-monitoring systems distributed video cameras around the house so that a remote caretaker could look in and make sure the senior was all right. However, many seniors resist having cameras in their home because they want their privacy respected.

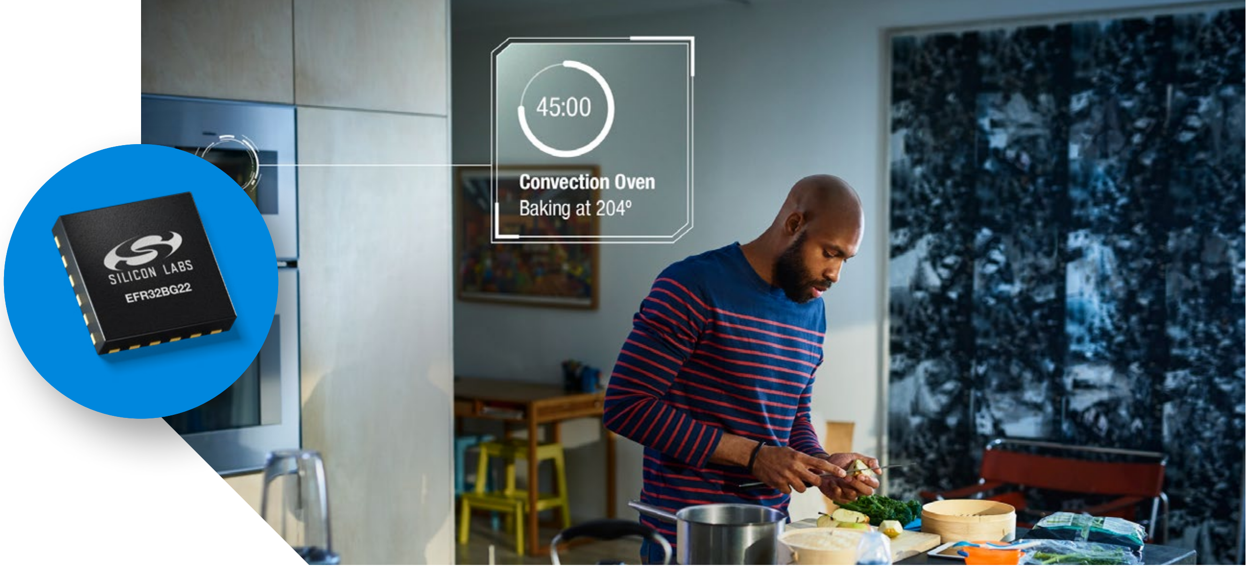
In addition, manually monitoring cameras takes time, especially if when caretakers worry and check that a senior got out of bed, didn't fall in the kitchen making coffee, didn't fall in the bathroom, didn't forget to take medications, didn't fall in the living room, and so on.

With AI and ML, senior care can be accomplished much less intrusively and provide better awareness. Instead of cameras, sensors placed around the house can track a senior's movements throughout the day. By learning daily behaviors, the smart home can monitor the senior's health and safety. The house takes on the caretaker's job in checking that the senior wakes up and makes coffee. It can also track when a nap has started and when it might be expected to end. When an abnormal behavior is detected, the human caretaker can be alerted.

With AI and ML, people won't have to tell smart devices what to do. Automatic blinds will close to block out the sun so the A/C doesn't have to run as long. Appliances like dishwashers and dryers will turn themselves on at night when they are full and need to be run, doing so when electricity demand is low. Smart sprinklers won't just turn themselves off when it's raining; they'll check the weather via the Internet to see if rain is expected tomorrow and whether to hold off from watering. Furthermore, if rain doesn't come as expected, the system can resume normal operation.

Smart lights can offer added capabilities. For example, they know when it's just the dog walking around at midnight, as opposed to a burglar, and so won't turn on the lights or trigger the alarm. Unless it's a teenager trying to sneak out, in which case the home can send parents an alert.

AI and ML will allow people to interact with their homes in new ways as well. For example, smart door locks will allow delivery services to deposit groceries and other packages inside the house so they can't be stolen. Instead of having to give every service person the same key to the house, individual codes can be assigned so the door lock can log who came in and for how long. The keys can also be set to expire and only operate for certain windows in time. Locks can also be paired with other smart devices, such as a camera, to perform facial scans of visitors or to let the new dog walker into the house.



SMARTER DEVICES

Intelligence at the Edge

To enable capabilities like these, intelligence must be brought out to the edge. Initially, the general consensus was that AI and ML would take place in the cloud. To perform more complex functions, however, devices need to collect more detailed information about the home and the people living in it. In addition, the number of co-located devices in the home is increasing. Together, these factors are causing a sharp rise in the amount of data that should be processed at the edge.

Certainly, an increase in data needing to be uploaded to the cloud puts a burden on available bandwidth. However, it is increased latency between data collection and decision-making that is driving intelligence to the edge.

Consider a real-time example: “Turning on a light when a person enters a room”. The sensor must collect enough data to identify the movement and correctly conclude that the person is entering the room, as opposed to leaving it. When the round trip for this data to reach the cloud and undergo analysis to then convert the data into an action takes too long, this impacts the user experience. In this case, the light might not turn on before the person has walked across the room and tripped or simply turned on the lights manually themselves.

AI at the edge will be implemented partially in edge devices and partially in the hubs and gateways through which they connect. Edge devices will need greater local computing and storage resources to support the aspects of AI for which they are responsible.

AI and ML are complicated technologies and have to be developed by a number of vendors, each supplying a critical element of the AI puzzle and adding their own value. An important aspect of component selection for smart devices, then, is how many supporting vendors the silicon manufacturer has brought together. The more comprehensive the options, the more efficient a system can be and the faster an OEM can get to market.

For example, Silicon Labs offers **EFR32 SoCs and modules** to accelerate the design, development, and deployment of smart devices. The EFR platform supports the major standards and protocols used in the smart home. It also offers the compute, storage, and security resources needed to bring intelligence out to the edge. The platform is supported by **Simplicity Studio**, an integrated development environment with the tools and features needed to simplify and optimize IoT development for developers of all skill levels.

SECURITY

Privacy, Prevention, and Protection

With new capabilities come new vulnerabilities.

As devices in the home become more intelligent, they will collect more and more information about individuals in the home. If compromised, this data could be used to track individuals without their knowledge. For example, without privacy measures in place, a thief could simply ask the house when no one will be home.

For many years, user privacy has been something that an OEM could ignore, provide only a token level of protection for, assume the cloud handled, or hope was being managed by the wider home network. Regulation is changing this responsibility. For example, the EU's General Data Protection Regulation (GDPR) exacts stiff financial penalties for violations of user privacy and regulation is expanding with IoT security legislation throughout the world.

California was one of the first U.S. states to pass IoT security legislation. SB-327, also known as the California Consumer Privacy Act (CCPA), requires businesses "to implement and maintain reasonable security procedures and practices … to protect the personal information [of California residents] from unauthorized access, destruction, use, modification, or disclosure." Violations allow customers to bring civil actions and recover damages.

Nearly all U.S. states have introduced bills that resemble California's CCPA. Effective Jan. 1, 2020, it took the CCPA less than three years to progress from its introduction to becoming law. In the U.S. alone, close to 300 bills or resolutions dealing with cybersecurity were introduced or considered close to passing in 2019. This demonstrates the seriousness with which privacy is now being treated from a legal standpoint.

A second aspect of security is prevention. Because smart devices can act on their own, it is important to prevent hackers from hijacking their capability. Attacks could go far beyond a simple bypass of door locks. Nuisance or Ransomware attacks are also a possible concern, hackers could feasibly force the same song to be played at a high volume while flashing the house lights on and off. These attacks could also threaten user safety, such as raising the water heater temperature to scalding levels. Smart devices without security could **and have** been exploited and used as gateways to the entire users network (see Criminals Hacked a Fish Tank to Steal Data From a Casino).

A third aspect of security is IP protection. Developing a robust AI for a particular application requires investment in both time and money so AI development represents a substantial barrier to entry for companies entering the market. With AI at the edge, however, security must be implemented in a smart device or gateway in the home. If devices are not protected sufficiently, an OEM's AI investment could be copied and stolen.

Silicon Labs offers the hardware, software, and tools needed to secure smart systems in terms of user data privacy, prevention of operational disruptions, and IP protection. Table 1 lists some of the security concerns that OEMs need to consider and the technologies available to address them.

Concern	Security Requirement	Technology
Device Identification	The IoT device can be uniquely identified logically and physically.	Secure Attestation
Device Configuration	The IoT device's software and firmware configuration can be changed, and such changes can only be performed by authorized entities.	Secure Upgrade
Software and Firmware Update	The IoT device's software and firmware can be updated by authorized entities using only a secure and configurable mechanism.	
Data Protection	The IoT device can protect the data it stores and transmits from unauthorized access and modification.	Secure Key Management
Logical Access to Interfaces	The IoT device can limit logical access to its local and network interfaces to authorized entities only.	Secure Debug
Software and Firmware Update	The IoT device's software and firmware can be updated by authorized entities using only a secure and configurable mechanism.	Secure Upgrade
Cybersecurity Event Logging	The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.	Anti-Tamper
Software Integrity	Attempts to breach security are logged and developers may select appropriate system counter-measures technologies to protect security.	Secure Boot

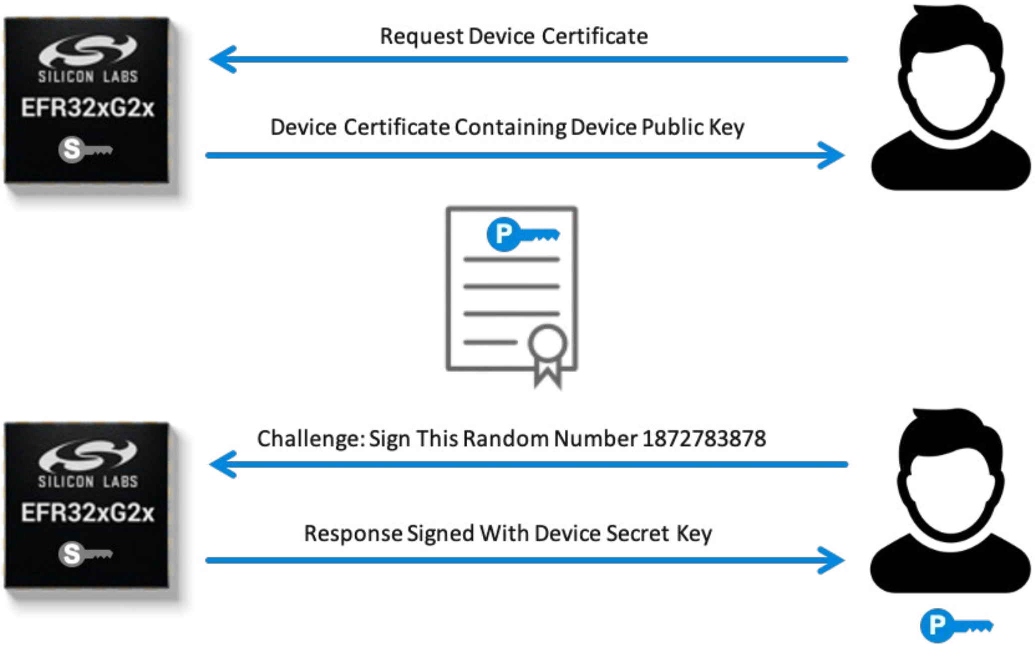
> Security threats evolve, so smart devices must evolve as well. To provide the most comprehensive security possible today, Silicon Labs has developed Secure Vault.

Security threats evolve, so smart devices must evolve as well. To provide the most comprehensive security possible today, Silicon Labs has developed Secure Vault. Secure Vault brings together all of the secure technologies described above — in addition to a true random-number generator, cryptographic engine, and differential power analysis (DPA) countermeasures — into a Secure Subsystem that provides hardware isolation between all security functions and the host processor.

Secure Attestation prevents counterfeit devices from using public device IDs to pretend to be an authentic device. Secure Vault technology is used to generate a unique device ECC-based public/private keypair on-chip. The private key never leaves the device. Using the public key through a certificate, an OEM or external service can challenge the device at any time to confirm that the silicon running the device is authentic.

Figure 1

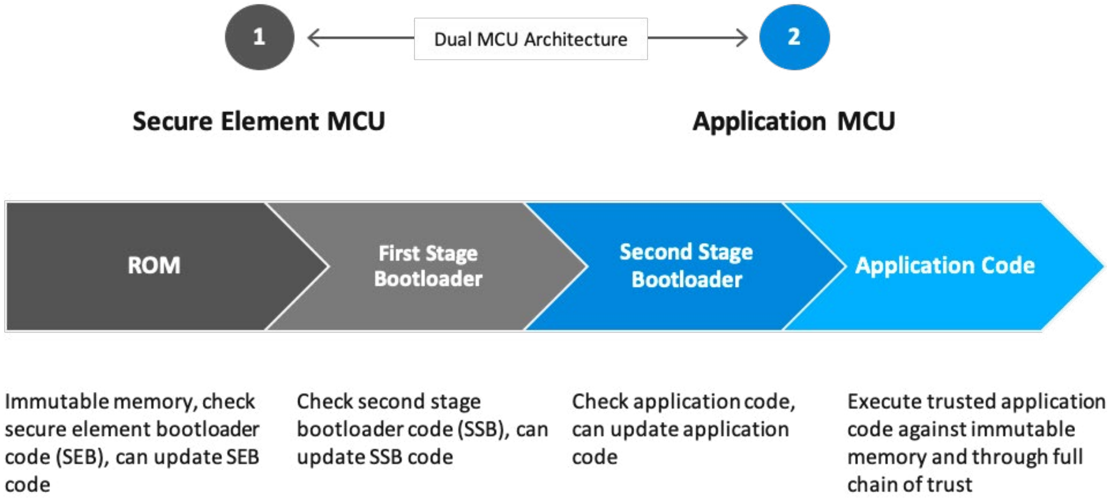
Secure Attestation Prevents Counterfeit Devices from Pretending to be Authentic Devices.


SILICON LABS
EFR32xG2x
S
Request Device Certificate
Device Certificate Containing Device Public Key
P
SILICON LABS
EFR32xG2x
S
Challenge: Sign This Random Number 1872783878
Response Signed With Device Secret Key
P

Secure Boot and Secure Upgrade technology (see Figure 2) prevents hackers from replacing code with hijacked code that appears to operate normally but gives hackers remote control of the device. When Secure boot is combined with root-of-trust and secure loader technology to create a full “chain of trust,” OEMs can ensure that devices will run only trusted application code and that firmware upgrades are authenticated before they are executed.

Figure 2

Secure Boot and Secure Upgrade Technology Prevent Hackers from Hijacking Device Code



Immutable memory, check secure element bootloader code (SEB), can update SEB code

Check second stage bootloader code (SSB), can update SSB code

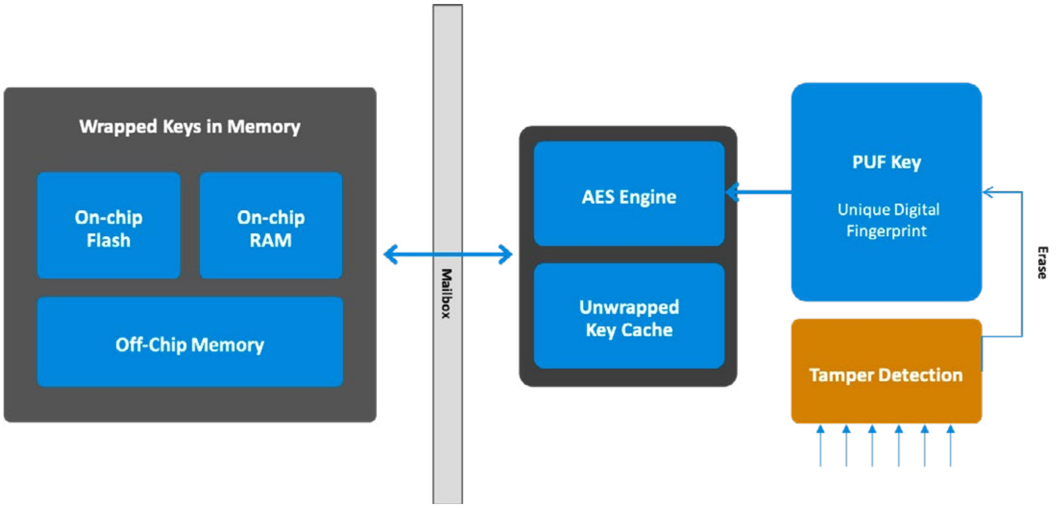
Check application code, can update application code

Execute trusted application code against immutable memory and through full chain of trust

Secure Key Management (see Figure 3) blocks attackers from extracting keys or content from a device. This is achieved by creating a physically unclonable function (PUF) key based on characteristics that are unique to a device. All keys are encrypted in Secure Key Management using the PUF key. In addition, the PUF key is generated at startup and is never stored in flash.

Figure 3

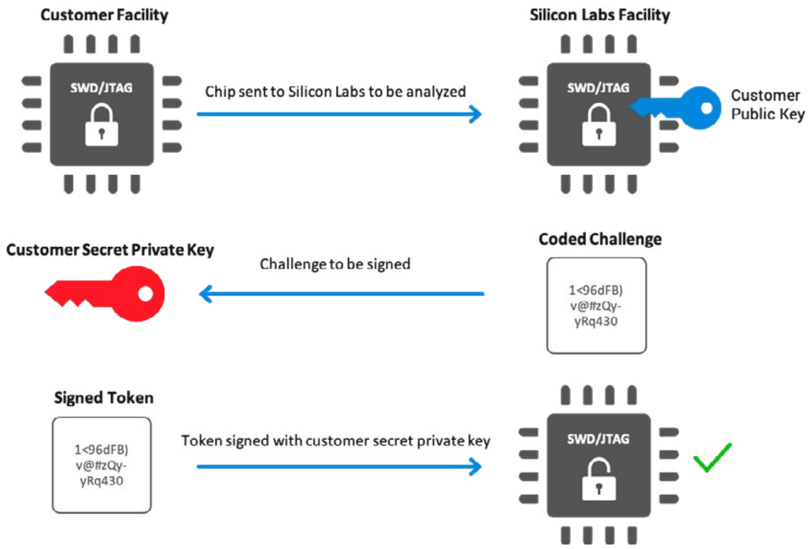
Secure Key Management Blocks Attackers from Extracting Keys or Content from a Device



Secure Debug (see Figure 4) prevents a chip's debug port from being used by hackers to take control of a device. OEMs can still access device failure analysis capabilities by unlocking the port using cryptographic tokens.

Figure 4

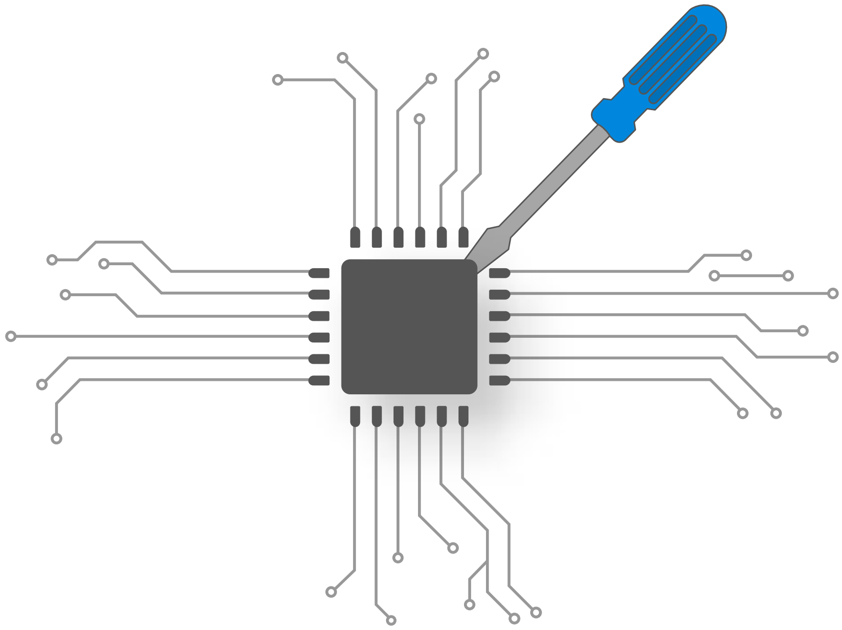
Secure Debug Prevents a Chip's Debug Port from Being Used by Hackers to Take Control of a Device



Anti-Tamper technology (see Figure 5) protects devices from tampering attacks, such as voltage glitching, magnetic interference, and forced temperature adjustment. Upon detection of a tampering attempt, a device can take suitable action, such as immediately deleting all of its keys.

Figure 5

Anti-Tamper Technology Protects Devices from Physical Attacks



Silicon Labs offers a wide portfolio of secure platforms for IoT design. For example, the EFR32 provides important security features in configurations that meet the specific requirements of different applications (see Table 2). Silicon Labs also makes use of leading-edge security technologies, including TrustZone for MCUs based on the Arm Cortex-M architecture.

Table 2

MCUs Like the EFR32 Series Integrates Security Features Important for Smart Devices

Feature	Basic	+Root of Trust	+Secure Element	Secure Vault
True Random Number Generator	✓	✓	✓	✓
Crypto Engine	✓	✓	✓	✓
Secure Boot	✓	✓	✓	✓
Secure Boot with RTSL		✓	✓	✓
ARM® TrustZone®		✓	✓	✓
Secure Debug with Lock/Unlock		✓	✓	✓
DPA Countermeasures			✓	✓
Anti-Tamper				✓
Secure Attestation				✓
Secure Key Management				✓
Secure Key Management				✓
Advanced Crypto				✓

INTEROPERABILITY

Working Together to Win Together

In addition to being more intelligent, smart devices need to be able to interoperate with each other and coordinate their actions. The leading IoT players understand how important interoperability is to the success of the market. This is why standards groups are developing integrated IoT standards and why companies like Amazon and Google are starting to work together to create standardized APIs for the smart home ecosystem. When smart devices can work together, everyone wins.

Developers can learn about new IoT developments at technical conferences such as Works With. Works With is the largest smart home event dedicated to training developers to integrate products with any hub or smart home ecosystem. It brings together the leading ecosystems in one place — Amazon, Google, Comcast, Samsung, and many others. Works With will be virtual in 2020 and in-person in 2021.

We are seeing just the beginning of what will be possible in the smart home. Soon, smart devices won't be limited to areas around the home. For example, Amazon Sidewalk promises to greatly extend the working range of low-bandwidth, low-power, smart lights, sensors, and other devices installed in and around the home. Amazon foresees using sub-GHz technology to increase the connection range of devices to over half a mile. Homeowners will then be able to place smart devices anywhere on their property, even in areas to which their Wi-Fi networks don't extend. Extending the scope of the smart home in this way will open the door to a whole new wave of smart devices and innovations.

Building the Future Smart Home Today

The smart home is evolving quickly. Smart devices need to be easy to use, and the best way to achieve this is for devices to think for themselves through AI and ML technology. The security technologies needed to maintain user privacy, prevent devices from being hijacked, and protect OEM IP are already in place. With a partner like Silicon Labs, you can build the future today. All that remains is to turn imagination into reality.

Learn more about Silicon Labs smart home solutions and join us at the Works With conference.

Take the next step to learn more about designing for the Smart Home by registering for the Works With virtual conference.

Join other engineers, experts and developers for two days of technical training for all levels.

Learn More