Smart Home IoT Devices Require Secure Network Architecture

Jonathan Collins, Research Director, ABI Research

ABIresearch GlobalSign by GMO

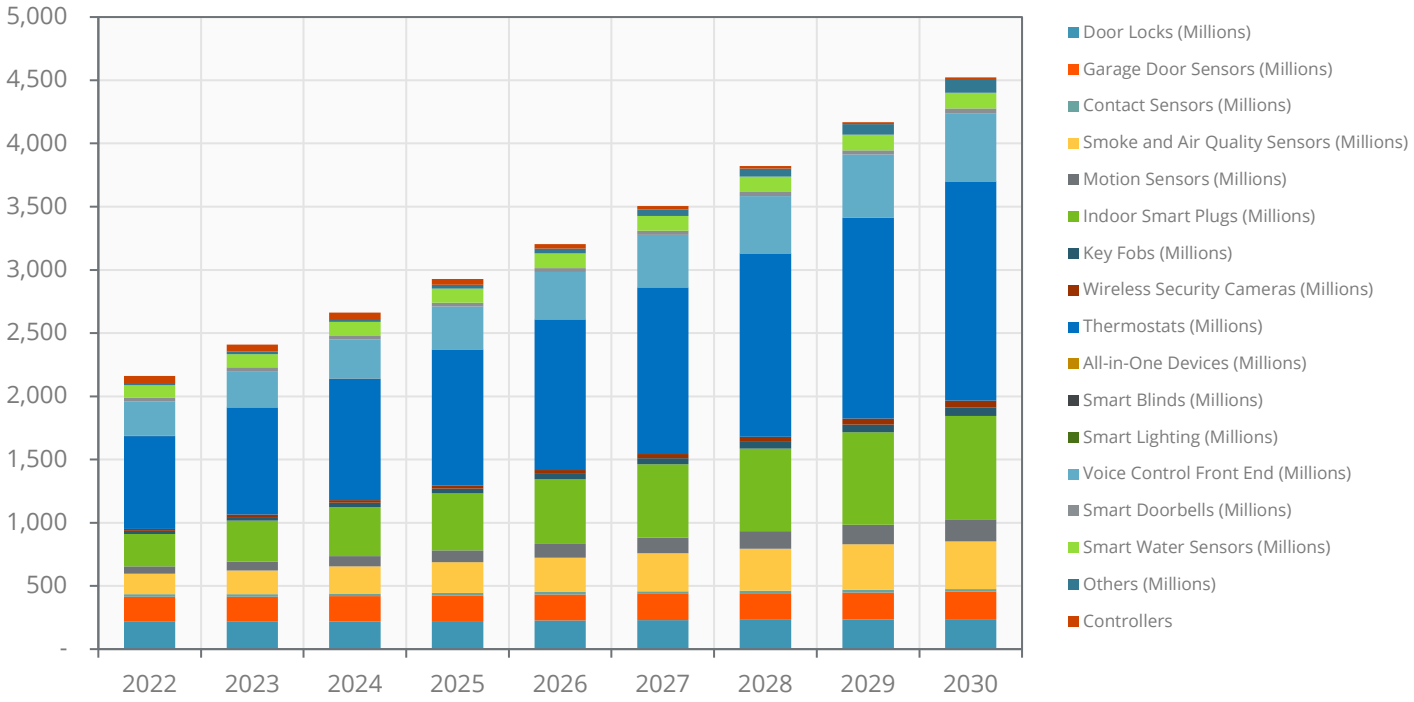
TABLE OF CONTENTS

INTRODUCTION

Homes will change more over the next 20 years than they have during the hundreds of years preceding that. They will expand in capability, function, and activity, reflecting the wider global needs of the planet—from economies to societies and individuals. Smart home capabilities will be the foundation for multiple services and applications as connectivity and intelligence is embedded in devices, appliances, and more, providing application capabilities to manage all home life, in turn improving security, safety, efficiency, and comfort. Over the rest of the decade, smart home hardware shipments will grow at a 9.4% Compound Annual Growth Rate (CAGR) to reach more than 1.7 billion devices by 2030.

Chart 1 Total Smart Home Hardware Shipments, World Markets: 2022 to 2030

(Source: ABI Research)



Extending the reach and appeal of the smart home requires interoperability that can enable multiple applications to leverage and share smart home awareness. This goal received a huge boost with the September 2022 completion of the Matter 1.0 specification, which was developed with the support of the largest home consumer and technology players in the world. Matter defines a universal IPv6-based communication protocol for smart home devices, with the goal of enabling the different types of devices to communicate in an interoperable manner with each other, regardless of the manufacturer.

By 2030, Matter will be integrated into billions of smart home devices. Even the most basic smart home services, such as management subscriptions or video capture storage, will drive more than US$25 billion of revenue by 2030. Applications leveraging smart home data will deliver value to partners, such as advertisers, insurance providers, and mobility providers; more will multiply that value in turn. However, that vision cannot be realized successfully unless consumers are confident that smart home services can be trusted with their most personal data.

The smart home industry is now moving into a new phase where single vendor ecosystems are making way for smart home deployments that support a wide range of vendors within a single system and where even smart home control can be shared between previously siloed ecosystems. This means whole home systems will open up

to multiple players; but they will only be as secure as the weakest point in that system. Matter has recognized the need to specify how devices and applications will be secured, while still leaving vendors with a variety of approaches on how to implement that.

Amazon, which pioneered a new wave of smart home engagement with its Echo smart speakers, regularly describes the future of the ambient home as one where technology is operating in the background in an intuitive, proactive, and personalized fashion. The company states that already 30% of smart home actions are automated by its Alexa platform—ranging from starting robotic cleaning to lowering thermostats or turning on lights when the first person comes home.

As interactions in the home become ambient, this will extend to actions and events beyond the home. Smart homes will become an intermediary for other key activities in life: healthcare, retail, insurance, energy, mobility, and entertainment.

The success of this transition will be increasingly dependent upon gaining consumer trust, and increasingly, smart home device manufacturers, and software and service providers are going to be required by fast developing national policy and recent regulation to implement security in their commercial offerings. The U.S. National Cybersecurity Strategy, published in March 2023, sets out two key strategic objectives that will impact the smart home sector directly:

- To drive the development of secure Internet of Things (IoT) devices through the advance of IoT security labeling products, which will create a market incentive for greater security in smart home devices. This is in alignment with similar efforts in Europe, where the European Union Agency for Cybersecurity (ENISA) is working on developing a cybersecurity labeling scheme.

- To shift liability for insecure software products and services onto software developers and service providers through the development of legislation establishing liability for insecure product development and maintenance. This objective also falls in line with similar legislation already in force in Europe through the Cyber Resiliency Act of 2022, which requires manufacturers to ensure the security of products at the design phase, as well as throughout the product's lifecycle.

The emerging regulatory landscape leaves little room for doubt that security is set to play an increasingly important role for smart home solution providers, and the building of secure network architectures and systems will quickly become the default status quo. Securing those linked activities and services becomes ever more critical as smart home adoption grows.

SMART HOME APPLICATION EVOLUTION

PHYSICAL SECURITY

Mainstream smart home adoption initially rose out of the physical home security market. The latter remains a key application and, importantly, one that continues to support subscription services, especially in the North American market. Smart home physical security systems primarily consist of smart doorbells, smart locks, contact and motion sensors, wireless video cameras, and control panels.

Tellingly, the smart home has become a key feature of any new home security offering, but while the traditional installer market has extended functionality by embracing the smart home, self-install single devices and systems have emerged as competitive alternatives. However, this has not been without controversy and concern, as popular devices, such as wireless video cameras have suffered significant security breaches where highly-sensitive data have been (and continue to be) compromised. More than 400 million wireless security cameras will ship between 2022 and 2030, while other popular devices such as smart doorbells, smart displays equally stream live video demanding consumer privacy and network security. Consumers demand security and trust guarantees from vendors, which can be difficult to obtain from self-install devices, leaving consumers with little recourse in case of a breach. Smart home services provide an alternate platform that can take some responsibility in protecting devices through network security.

ENERGY MANAGEMENT

Smart thermostats spearheaded not just smart home adoption, but also the uptake of demand response, with thermostats becoming key tools for Energy Service Companies (ESCOs) and utilities to enable demand response programs and reduce infrastructure stress during peak demands.By the end of 2022, more than 140 million smart thermostats have been installed worldwide and sales will continue to grow at more the 6% CAGR between 2022 and 2030 creating a significant install base on which to build an array of applications and services. Connectivity is extending into key energy consuming home equipment and appliances such as water heaters and electric vehicle chargers. Increasingly a range of key building services and appliances can be integrated into a whole-home energy management system. Increasingly, management will extend from consumption of energy to local generation and storage. Supporting developments, such as micro-grids and decentralized generation, a smart home system will enable localized capture and trading, as well as detailed fault detection and preventative maintenance.

Ensuring security will be key, particularly from a functional and physical safety perspective. Connectivity will expose energy management devices that can potentially be hacked and manipulated to cause physical damage, and possibly life-threatening scenarios. Locking down access and control to those systems will be a critical requirement to protect those living in the home, as well as their broader neighborhood.

MOBILITY

As the world continues to transition to Electric Vehicles (EVs), the smart home also becomes a center for mobility recharging and management. Interconnectivity and Artificial Intelligence (AI) will support a range of applications and services capable of ensuring that charging takes place at the most efficient time, either with energy pulled from the grid, or through home storage and generation (viewed as the better alternative). Such systems will leverage geofencing and personal schedules to deliver optimum services.

Smart home systems will also draw data from outside the house to determine which modes of transportation should be used, and take into consideration weather and road conditions, preferences, destination, service availability, and other factors. Ride share ordering via smart home platforms has been supported for some time, but extending this to encompass multiple external options and real-time traffic and pricing data will add more value to smart home systems.

The opening up of smart home data, most of which will be personally identifiable information, to external mobility-related applications will require a high level of trust between smart home systems and third parties in order to ensure effective data protection. This means that devices and applications will need to implement adequate security measures that can guarantee the appropriate level of privacy.

HEALTHCARE

The healthcare potential in smart homes remained relatively untapped until the global reaction to the COVID-19 pandemic accelerated the uptake and potential for the connected home. Even so, in 2022, spending on home healthcare equipment and services across, Home Monitoring, Remote Patient monitoring and Social Robotics, reached $100 million. By 2030, that figure will have multiplied more than nine times.

Supporting independent living for the elderly or vulnerable, Ambient Assisted Living (AAL) applications leverage many of the same sensors and connectivity options as those for the smart home. These systems typically extend traditional Personal Emergency Response System (PERS) provisions by providing insight into a resident's movements and habits, as well as detecting any potential deterioration or accidents that may occur.

Managing chronic conditions increasingly leverages connectivity for remote patient monitoring and care for lifesaving applications, such as sleep apnea or diabetes management. Patient behavior and medication adherence can be leveraged to improve care and ensure resources are funded and leveraged appropriately. More and more interactions between healthcare providers and their patients are likely to emerge that will leverage data collected and shared from the home.

As much of the data that will be shared in these settings will be healthcare related, it will likely be subject to regulatory compliance, as is the case in most countries across

the world. Consequently, the data will need to be secured accordingly. Further, there is a growing number of national policies developing around healthcare that seek to strengthen the integration of security into technologies used in the sector. For example, the United Kingdom's proposed Cyber Security Strategy for Health and Social Care will require embedding cybersecurity into the framework of new technologies. In parallel, the United States amended the Federal Food, Drug, and Cosmetic Act (FD&C Act) by adding a new section on Ensuring Cybersecurity of Medical Devices, which requires both secure product development and secure lifecycle management.

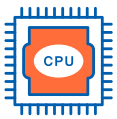
Those providing welfare and healthcare in the smart home will have to ensure the systems they offer comply with emerging policy and regulation so that they are trusted inherently, from the devices and applications through the connectivity and to the back end platforms, in order for them to be able to provide remote consultations, inform on treatments, drive prescriptions, and offer ancillary healthcare services.

HOME APPLIANCES

While Matter has arrived for smart home devices, major home appliances sit outside of Matter's current scope (although robotic vacuums are scheduled for inclusion in the next version). A number of efforts are bringing multi-interoperability with the Home Connectivity Alliance's recently published cloud-to-cloud interoperability standard.

Home appliances can be among the largest energy-consuming devices in the home and the ability to schedule operations to times best suited to a range of criteria assessed by the smart home system will be important to any smart home energy management system. The example of a smart refrigerator able to detect when supplies are running low and reorder accordingly may be long touted, but the infrastructure and embedded intelligence will increasingly make such an application appealing and possible.

Embracing border router support within appliances, a central tenant of the Matter standard, will offer appliance vendors a way to more tightly integrate into smart home platforms, and bring the majority of home appliances under a common application messaging framework. This will allow better development of a homogenous security posture, through built-in firewalls or data encryption features within border routers.



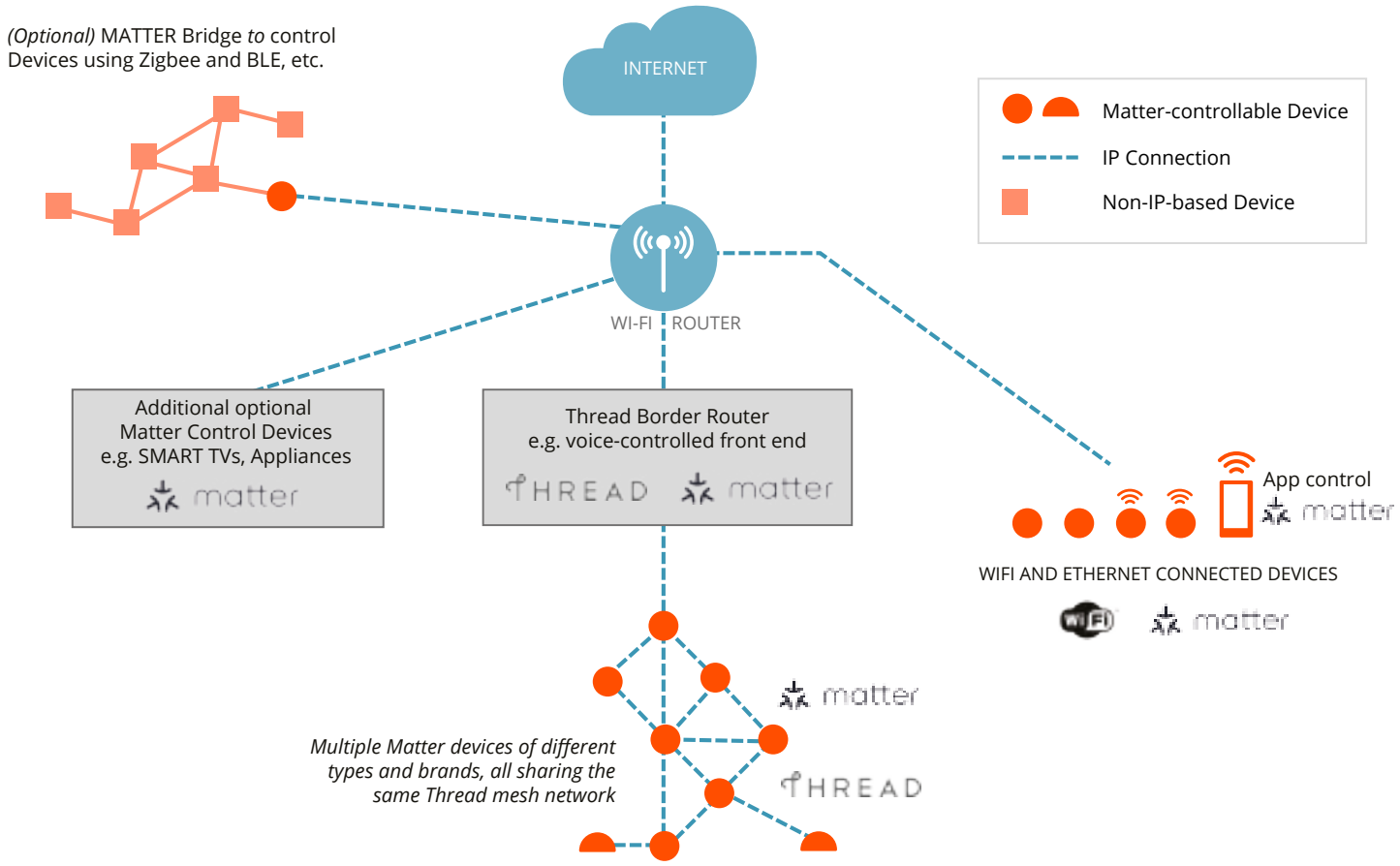
SMART HOME NETWORK ARCHITECTURES

The smart home network architecture will, in time, evolve into one that largely depends upon multifunction gateway devices to connect low-power devices to the home system and the cloud. Gateway functionality has long been a feature of the smart home, but in dedicated gateways, such as the Wink Hub, or in bridges, as leveraged by Philips Hue, among others. Increasingly, this will be seen in multifunction devices, such as voice control front ends or smart TVs.

There is already Thread support for border routers on Apple Home Pod Mini devices. For its part, Amazon has committed to making its Echo devices border router capable. Google, which already has Thread support in its Home voice assistant devices, will most likely do the same. Thread also supports having multiple border routers on the same network that can dynamically take over functions, so there is no single point of failure (see Figure 1).

Figure 1 Matter and Thread in the Smart Home

Sources: Thread Group, ABI Research



With border routing and smart home connectivity capabilities embedded in more devices and from multiple vendors throughout a home, the smart home of the near future will not just see significantly more data and intelligence within the smart home system, it will also require new levels of shared trust and security. Control within the home will extend across multi-vendor hardware, capturing and sharing data throughout the home and across a wide range of third-party applications. When adding more and more functionality to smart home automation, as control becomes ambient in the home, it will not just be consumers, but also vendors, that will have to trust all of those players within a smart home system.

TRUST AND SECURITY AS KEY ENABLERS

SECURITY CHALLENGES FOR THE SMART HOME

Smart homes open up people's private spaces to a host of third parties who can surreptitiously see and act on people's lives through their connected devices. This is both worrying and frightening. Trust and security have become primary concerns in order to ensure that smart home users are protected not only from malicious threat actors and invasive or unscrupulous third parties, but also from misconfigurations and errors that may expose their data by accident.

The priority areas for protection are data and devices. Data, and especially personal data, needs to be protected for obvious privacy reasons. Devices, which are collecting, storing, analyzing, and transmitting that data, need to be protected both from a digital security and physical safety perspective.

Increasingly, regulation mandating both privacy and security of devices is becoming more widespread globally (EU Cyber Resilience Act, General Data Protection Regulation (GDPR), NIS2 Directive, U.S. IoT Cybersecurity Improvement Act, and California IoT Cybersecurity Law), which, in turn, is driving the need to integrate adequate protection mechanisms in the smart home.

Protecting data starts with the secure management of the devices—from their hardware to their software, firmware, and connectivity. The concern is around access control to the devices (and, therefore, to the data). Ensuring lawful and legitimate use is critical in order to minimize the risk of unauthorized actions and modification. Because there are numerous potential threat vectors, key challenges require focusing on ensuring:

- Secure boot
- Root of trust
- Device identity
- Authenticity of firmware/software
- Data integrity
- Communication security

The difficulty in implementing these technologies in a uniform way is due, in large part, to the fragmented nature of the smart home market; there are numerous Original Equipment Manufacturers (OEMs), device types, platform choices, and applications that often have their own specific implementations and protocols. This makes the widespread deployment of security technologies difficult due to the incompatibility of these assets, and the inability to apply security homogenously across the board.

This is changing, however, with the emergence of standards, policy, and regulation driving better integration of relevant security technologies, especially with the Matter standard. Matter, for example, requires the use of device identities for smart home

devices. Identities are the key building block for enabling other security technologies, such as data privacy and secure communications. Matter also includes details on a security layer (secure channel and message layer) to provide a networking service substrate for secure communication. Message encryption allows for data confidentiality, while message signing provides authentication guarantees. The Matter specification designates a core set of cryptographic primitives, algorithms, and protocol building blocks that can be used to these ends.

Standards, such as Matter (but also ETSI EN 303 645, for example), are key to driving interoperability between various smart home technologies and for creating a uniform security foundation that devices can align with to the benefit of manufacturers, software developers, and connectivity providers.

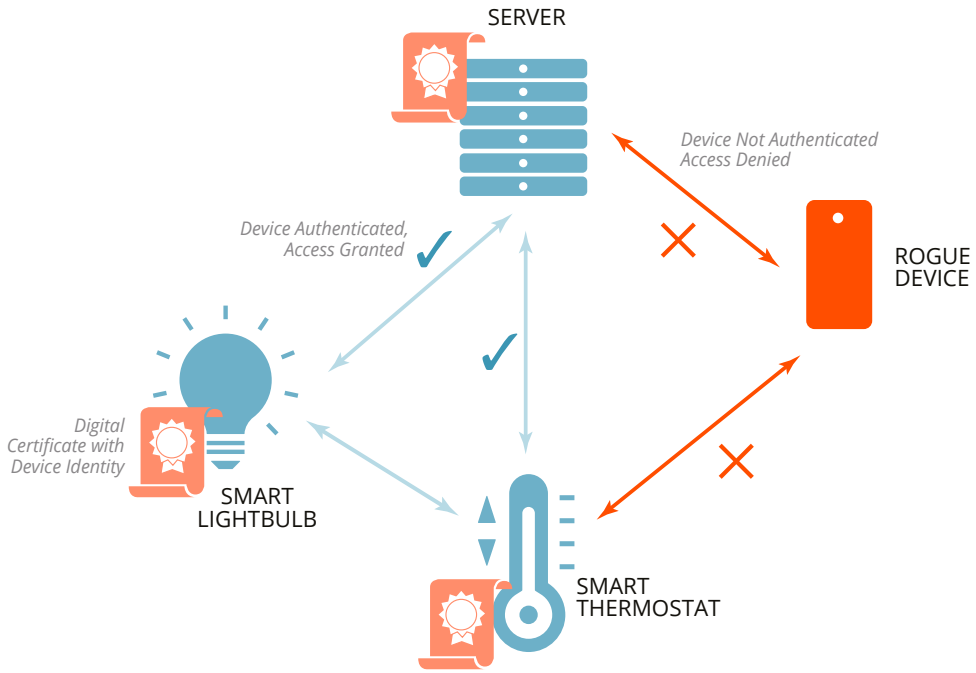
LEVERAGING DIGITAL CERTIFICATES

Providing device identities is a foundational requirement for enabling a whole host of security capabilities. Key to delivering identities is the use of digital certificates and Public Key Infrastructure (PKI). PKI effectively allows for all types of devices to connect from any location to any other device in a secure fashion. Together, digital certificates and PKI can facilitate a wide variety of security applications.

Authentication and Access Control: The identity of a device is encoded within a digital certificate. This provides proof of its authenticity to other devices and to the network, and authorizes it to interact with others in the network. It allows for the setting of access control policies, including setting the appropriate access of legitimate devices.

Diagram 1 Authentication and Access Control

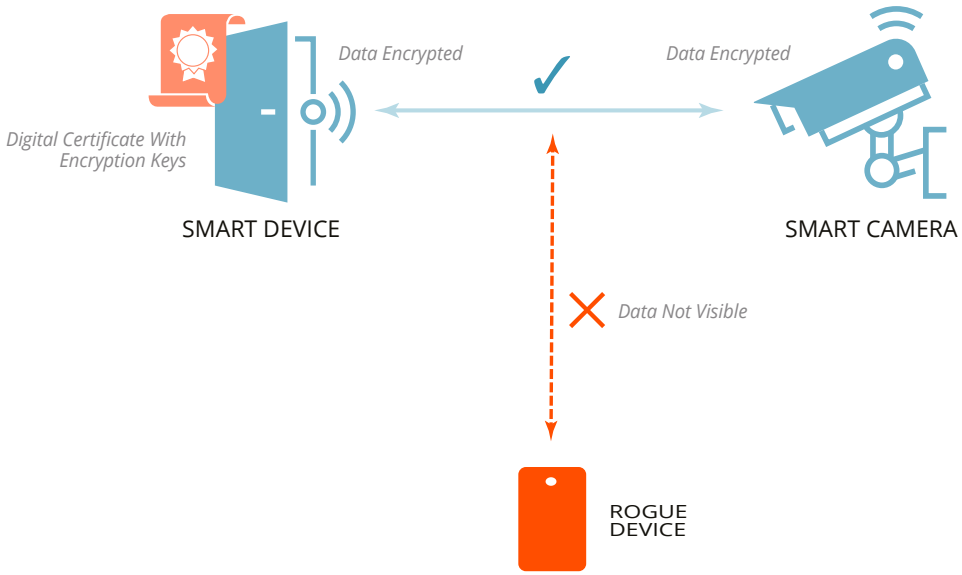
(Source: ABI Research)



Privacy and Confidentiality: Digital certificates include the private keys that are unique to the device and that allow for the encryption of data before transmission into the network and to other devices. This enables secure and private communications, guaranteeing data confidentiality and privacy.

Diagram 2 Privacy and Confidentiality

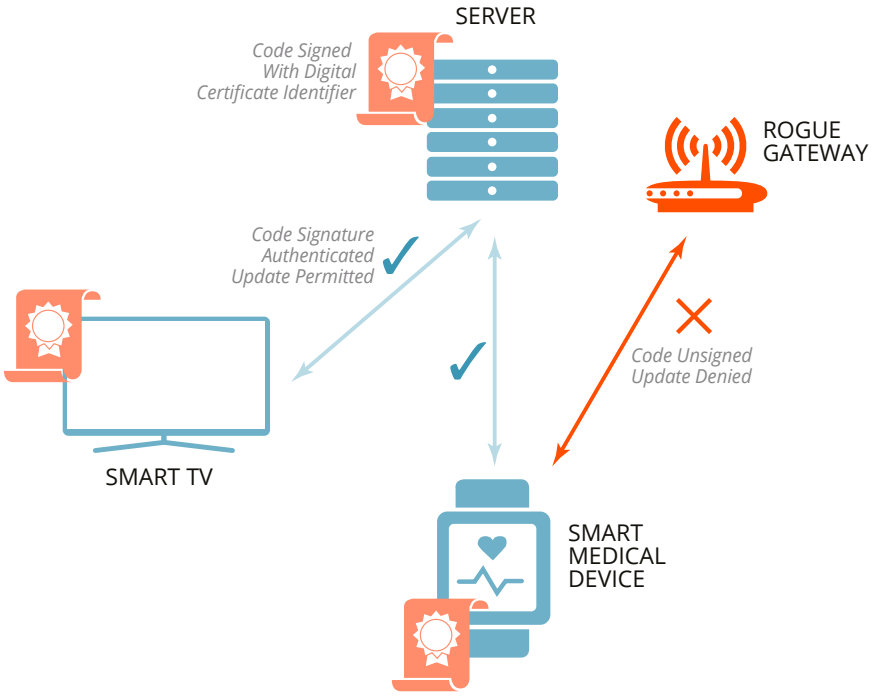
(Source: ABI Research)



Integrity: The use of private and public keys allows for firmware and software updates to be digitally signed and then verified as legitimate, confirming that the updates meant for the device are coming from an authentic source, and ensuring that it has not been otherwise altered by a rogue party.

Diagram 3 Integrity

(Source: ABI Research)



SECURITY, TECHNOLOGY, AND BUSINESS BENEFITS

The security benefits of using digital certificates for smart home devices are clear: threat mitigation and cyber resiliency, privacy guarantees and data protection, and regulatory compliance and customer trust. Importantly, they represent the core technologies for creating and managing a device's digital identity, which is key to enabling myriad business benefits. By providing better control over devices, digital identities can allow for operational efficiencies through visibility and control, which can be further enhanced through automation with the right identity management platforms. For device OEMs, in particular, an identity injected at manufacture can provide a secure root of trust for a device enabling provisioning and onboarding, as well as post-market lifecycle management. Beyond that, however, the technological benefits of digital certificates are just as advantageous. Digital certificates and the use of PKI are well-established technologies, with a mature and experienced market supporting a wide range of available solutions for implementation. As an open standard, PKI offers many flexible options for certificate provisioning and enrollment, as well as deployment and management (e.g., REST API, SCEP, EST, CMP, CMC, and ACME). PKI technologies are expected to adapt well within the smart home ecosystem.

Digital certificates are especially well-suited, as they have a minimal footprint, and there are plenty of lightweight implementations being developed specifically for the IoT. This means that they can be integrated into as many devices as possible, even low-power and resource-constrained ones. Further, the use of PKI and automation can allow for scaling, which will enable the technology to grow relatively easily alongside smart homes as they expand and include ever-more connected devices.

PKI allows for increased visibility of smart home devices and their connectivity to external assets and applications, allowing for fine-grained management of devices and data. From a smart home provider perspective (OEM, connectivity provider, etc.), it is possible to build some interesting platform-based value propositions leveraging digital certificates and their corresponding platforms to enable smart home management around the use cases exposed earlier, such as home security, energy, mobility, and healthcare. In time, as technology advances and behaviors change, it will also allow smart home providers to offer new capabilities, features, and services in a privacy-aware and secure manner that will augment users' quality of home life.

The use of digital certifications and infrastructure, such as PKI, form that core of device identities, allowing for product differentiation, increased visibility, fraud prevention, and attack reduction. Digital identities are a value-add for smart home providers, whether they are OEMs or service providers, allowing them to deliver trusted and reputable smart home brands.

CONCLUSION

The demands of the smart home space are evolving rapidly, with increasing pressure from a trust and security perspective. Smart home providers will need to ensure that their solution offerings, whether these are devices or services, integrate appropriate security technologies. This means deploying digital certificates and associated management platforms, such as PKI, for example. The right security provider will be able to offer:

- Security and safety choice
- Privacy capabilities
- Scalability
- Configurability
- Flexibility
- Automation
- Compliance
- Speed to market

The industry is consolidating around standards and regulations that will alter the way devices are being offered on the smart home market. Standards, such as Matter, are a critical first step, and Matter is likely to be one among many more as governments rightly strengthen security and privacy requirements for smart home providers, and users become more demanding from a trust perspective. Delivering security through device identities provides clear benefits and is set to deliver even greater value to the smart home ecosystem.

Published May 2023
157 Columbus Avenue
New York, NY 10023
Phone: +1 516-624-2500
www.abiresearch.com

About GMO GlobalSign

As one of the world's most deeply rooted Certificate Authorities, GlobalSign is the leading provider of trusted identity and security solutions enabling organizations, large enterprises, cloud-based service providers and IoT innovators worldwide to conduct secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale PKI and identity solutions support the billions of services, devices, people and things comprising the IoT. A subsidiary of Japan-based GMO Cloud KK and GMO Internet Group, GMO GlobalSign has offices in the Americas, Europe and Asia. For more information, visit https://www.globalsign.com.

GlobalSign US Office
Two International Drive, Suite 150
Portsmouth, NH 03801
Phone: 603-570-7060
Email: sales-us@globalsign.com

GlobalSign UK Office
Springfield House,
Sandling Road, Maidstone,
Kent ME14 2LP
Phone: 01622 766766
Email: sales@globalsign.com

GlobalSign EU Office
GlobalSign NV/SA
Diestsevest 14
3000 Leuven
Belgium
Phone: +32 16 89 19 00
Email: sales@globalsign.com

About ABI Research

ABI Research provides actionable research and strategic guidance to technology leaders, innovators, and decision makers around the world. Our research focuses on the transformative technologies that are dramatically reshaping industries, economies, and workforces today. ABI Research's global team of analysts publish groundbreaking studies often years ahead of other technology advisory firms, empowering our clients to stay ahead of their markets and their competitors.