Solution Brief
Intel® Programmable Solutions Group
Smart Building Security

Future-Proof Security for Building Automation Systems

Veridify's DOME™ platform, leveraging Intel's advanced programmable solutions, delivers device-level cybersecurity protection to new and pre-existing building automation systems, with cost-saving zero-touch lifetime credential management.

This solution brief describes how to solve building security challenges with Veridify and Intel's innovative technologies.

If you are responsible for…

- **Business strategy:**
  You will better understand the safety-threat, potential for operational disruption, and the enormous cost of cyberattacks on your building's automation control and its managed 'smart' devices.
- **Technology decisions:**
  You will learn how every device, regardless of size and operating system, can be lifetime managed, with the security necessary to create a safe and trusted environment.

Veridify Security Inc. and Intel® Corporation
Authors

Mark Jervis
Intel® Corporation
Programmable Solutions Group
Marlow, UK
mark.jervis@intel.com

Louis Parks
Veridify Security Inc.
Shelton, CT, USA
lparks@veridify.com

Executive Summary

Today's connected buildings are increasingly susceptible to cyber-attacks that can threaten the safety of occupants, with the potential for financial and reputation damages. This exposure is due to their growing use of poorly secured interconnected systems that can include HVAC, lighting, access control, environmental sensors and elevators. Compounding this situation are the controllers and devices coming from many different vendors, without the compute performance for the trusted security methods used by PCs and smartphones. For hackers, even the simplest of such connected unsecured devices can be an open backdoor, the consequences of which can be disastrous.

Veridify's DOME™ is a security solution designed to protect a building's management system right to its edge on existing network protocols like BACnet. The system provides zero-touch onboarding to reduce the time and errors from manually provisioning, a blockchain pedigree to ensure only authorized controllers can issue commands, and a low-cost 'bump-in-the-wire' tool, leveraging Intel's advanced programmable solutions, to retrofit security to pre-existing systems. DOME enables device-level security, with in-field provisioning, firmware updates, and device ownership management that is simple, cost-effective, and fast. DOME is crypto agile, supporting legacy and quantum-resistant security, safeguarding an owner/manager's investment with the long lifecycle protection needed by a building.

Solution Benefits

1. **Improve security** with tools that address even the smallest devices found at the edge of a network
2. **Reduce deployment cost and time** with easy to implement software tools to secure pre-existing systems and new low resource devices connecting to IoT gateways.
3. **Scale easily** with zero-touch onboarding, lifetime blockchain pedigree, support for in field provisioning and firmware updates, and device-based ownership management that does not require a pervasive cloud connection.

Business Challenge

Digital Transformation

Digital connected technology is transforming buildings. Networking the Operational Technology (OT) of sensors and actuators to the Information Technology (IT) monitoring, control and analytics, allows remote and increasingly automated management to make buildings that are responsive, reliable, efficient and comfortable. New smart building system components installed now must interact with many other devices in the system and be future proof to adapt to changes over long equipment lifetimes. Building owners and managers trying to protect their existing assets are faced with an additional hurdle: How can they justify the price to replace a building's systems that may have years of use left - along with the costs that may come from the disruption to their tenants and rent rolls?

The Cyber-Security Threat

Potential hackers constantly seek out the weakest links to exploit, and the connected IoT in smart buildings offers the potential of multiple points of entry to gain access into building information and critical building operational technology. This could be taking control of the physical systems such as access control, elevators, lighting or power; accessing or controlling data - for example surveillance systems, on onto connected IT. Examples include a bank hacked through its CCTV cameras, a casino hacked through the fish-tank temperature sensor, hotels and hospitals with infrastructure crippled with ransomware, and smart building IoT devices subverted and used in the biggest distributed denial of service (DDoS) attack to date.

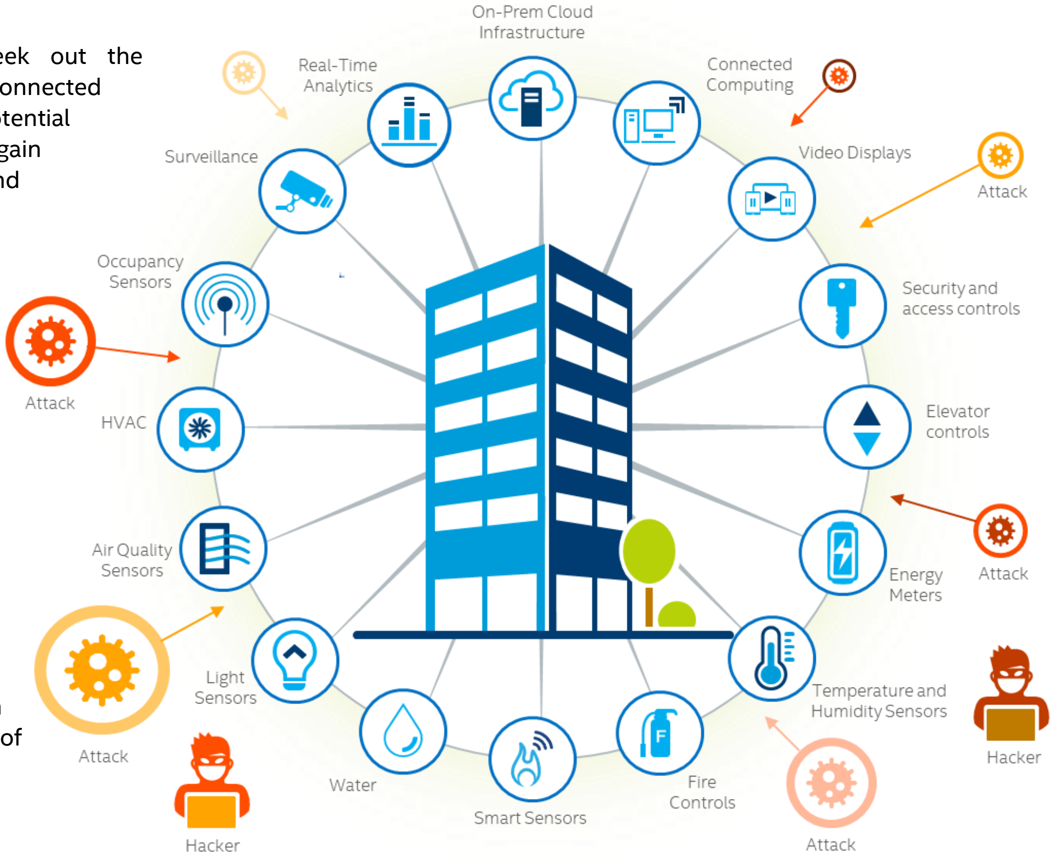
For building owners, the value in adding security lies in avoiding potential future costs and damages related to breaches of security.

Legislation

In the face of these ever-increasing Internet of Things (IoT) security threats, governments around the world are rushing to legislate on enforcing minimum IoT device security standards.

Both U.S. and U.K. governments have recently proposed new regulations. In the U.K the government published their proposal for cyber-security legislation, updated as recently as October 2020; and in the U.S., Congress has proposed legislation (S.734, H.R. 1668) that seeks new security standards for IoT devices sold to government agencies. This comes on top of other legislation and guidance around the world including;

- the California IoT Bill, which requires manufacturers of a connected devices to equip them with reasonable security features;
- the EU baseline requirements for cybersecurity (European Standard (EN) 303 645 v2.1.1);
- the Telecommunications Business Law in Japan which includes conformance to Security Standards of IoT Device;
- the NIST draft report "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline" (Jan 2020); and
- other cybersecurity standards, such as ISO 27001, NIST 800-53, IEC 62443



It is also very likely that the insurance industry will consider future security certifications when calculating insurance premiums for buildings, with lower premiums for buildings that meet certain security levels.

Implications for building security

The move towards legislation and the ever increasing and evolving threat and means building cyber security needs to be updatable and adaptable over its entire lifetime. Cyber-defenses also needs to be in-depth, with multiple layers of protection; from firewalls and data encryption down to individual IoT device security.

There are several practical issues. The process of securely on-boarding the numerous connected IoT components can itself be prohibitively expensive; in some cases, twice the cost of the devices themselves. If retrofitting, it may not even be possible using standard cybersecurity algorithms such as those based on elliptic curves, as many of the endpoint devices may only contain small very small microprocessors. Add on the complexity that many devices will not even have user interfaces

A total security solution also needs to consider that the weakest link to attack may even be before components are installed - in the supply chain. Security needs to cover the lifetime of the devices in the system - from manufacture and supply, through on-boarding and provisioning, right though to retirement.

Solution Value

DOME is a zero-touch onboarding security solution for the Internet of Things (IoT).

DOME delivers in-field ownership management, including secure 'transfer of ownership' between entities based on a block-chain pedigree so you can be assured ownership has been securely passed along to you from the original manufacturer, helping protect against security weak points in the supply chain.

With DOME, a device does not need to connect to the cloud or a network. The device only needs to connect to its owner. The owner only needs to connect to the cloud to enable the ownership transfer function.

What would be time-consuming work of manual security provisioning of devices in-situ by security experts can instead be done automatically and remotely, making it easier, cheaper, faster and less error-prone. And once on-boarded, devices can continue to be security managed remotely.

In many cases, building owners will be looking to add security to existing infrastructure where this still has a long lifetime ahead, but to do so causing minimum disruption. DOME security can also be retrofitted to pre-existing legacy infrastructure; generally, directly integrated onto the existing devices with ultra-small implementation suitable for the smallest microprocessors. Where this is not possible, Veridify's Bump-In-The-Wire gateway platform using Intel FPGAs adds a security gateway over existing wiring while preserving protocol compatibility[1]; given a more cost-efficient solution than rip-and-replace.

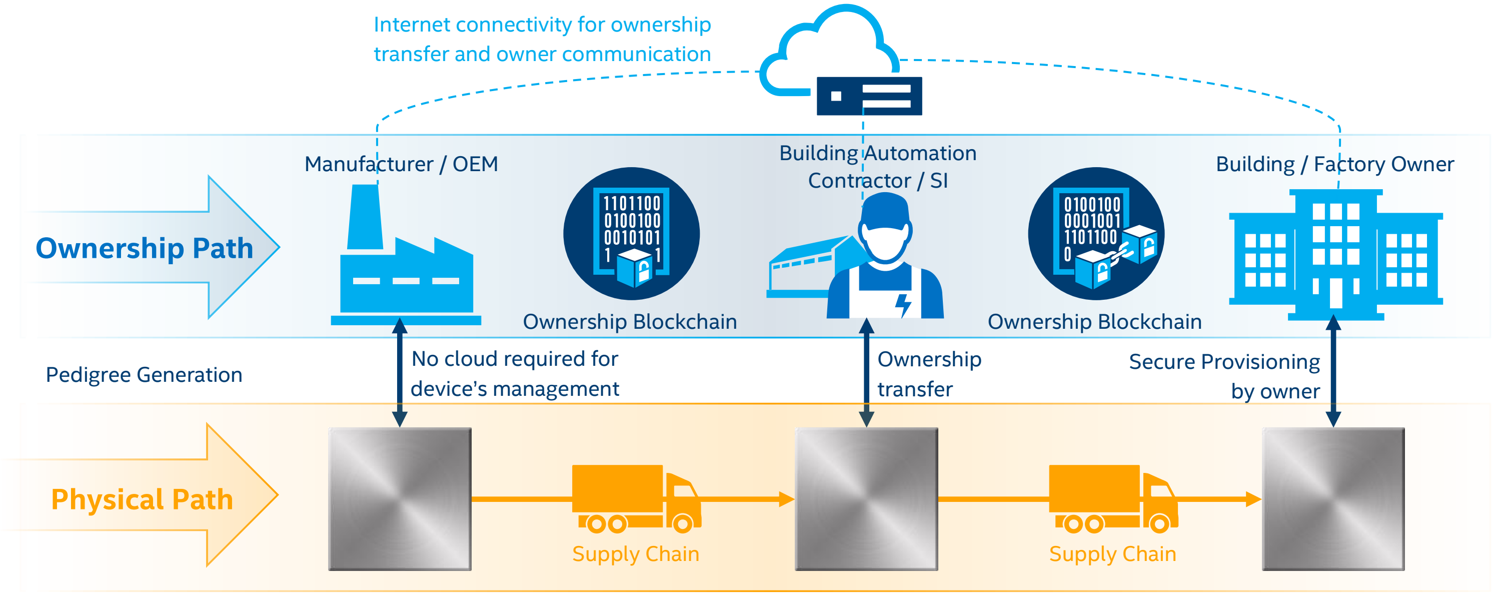


Figure 1: Secure ownership transfer

[1] it may be necessary to add a short wire segment for installations where a bump-in-the-wire security gateway is employed

Solution Flexibility

Securing building infrastructure requires multiple degrees of flexibility.

- **Hardware flexibility** - In any building there will be a wide variety of devices from many vendors to integrate securely. Veridify Security tools are hardware and platform agnostic, with implementations in software or hardware, supporting multi-vendor interoperability. It works with the smallest IoT devices, requiring only 8K of ROM to implement on a deployed processor or microcontroller.
- **Protocol flexibility** - Veridify's security solution is protocol agnostic - working across present, past, and future building automation protocols; including industry protocols such as BACnet, Modbus and KNX and multiple data link protocols such as MS/TP, IP, etc.
- **Crypto agility** Owners can push secure in-field updates devices for both keys and firmware. Managed devices will verify and install the update; keeping security up to date-field. It is also able to utilize one or more security methods, both legacy and future-ready quantum-resistant algorithms, important for infrastructure with long service life.
- **Scalability** Even if the devices are distributed in many buildings, distributed globally, Veridify's on-boarding and chain-of-custody operations easily scale to millions of devices.

Solution Technical Architecture

Device Ownership Management and Enrollment

DOME secures all the connected devices found in an industrial building/campus and establishes a "cyber security perimeter" where all devices and processors inside are trusted and safe.

This starts by providing a lifetime blockchain pedigree for any device used in a building beginning prior to its installation and ending with device's decommissioning and removal from the building. (See *Figure 1*)

Block-Chain Supply Chain

At the start of a DOME implementation, a device is provisioned with the DOME Client software library plus public key credentials that are shared with its original owner (for example – the Manufacturer). This step will allow a device to participate in its ownership management and authentication processes in the field without the need to connect to a cloud or central server. The manufacturer also provides a credential to the device so identification and mutual authentication can be performed with the device anywhere. The DOME Client is implemented in software and requires only 12K bytes of ROM. The credential for each device is signed into a 'block,' giving every device its own pedigree embedded in a blockchain. This framework allows owners to establish proof of ownership without the need for a pervasive cloud or network connection and enables device-level security management.

These root credentials in the DOME Client can also support the secure distribution of secondary crypto keys for user applications and in-field provisioning of user applications and firmware updates. The credentials are signed into the device's blockchain to support each transfer of ownership and follow the physical movement of the devices through the supply chain and each transfer of ownership.

Zero-touch Provisioning

Platform validates device ownership pedigrees before installation. During installation, devices are authenticated, and support in field provisioned by a DOME Interface Appliance (DIA) then handed off to a building's automation or system controller to securely perform their intended day to day function. Devices that do not have DOME security, from supply chain or retro-fitted, can be placed behind Veridify's bump-in-the-wire security. (See *Figure 2*)

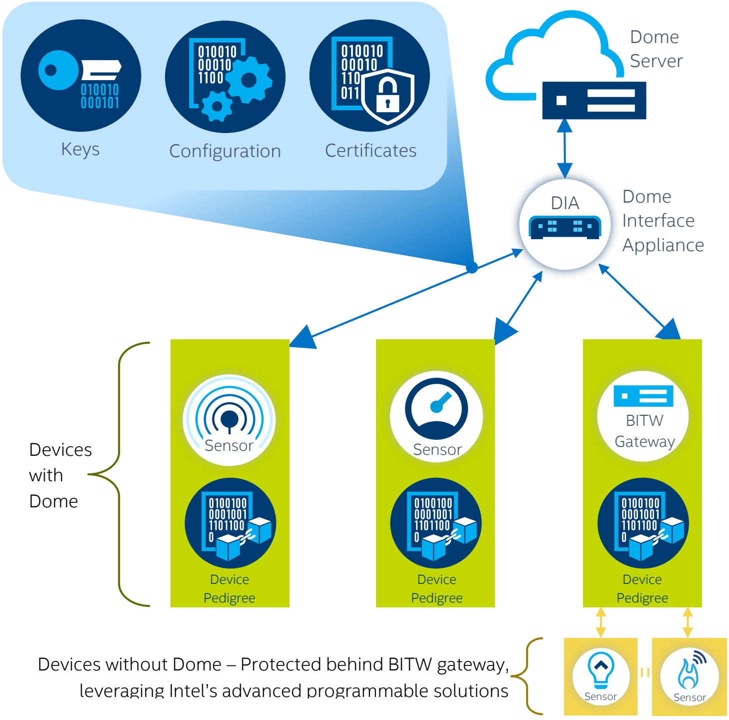


Figure 2: Provisioning

Deployed cyber security perimeter

A DOME Interface Appliance maintains the identification, authentication, and encrypted connectivity to every device it has enrolled within the building's ecosystem as well as the building controllers that interact with those devices. The Interface Appliance monitors device status and can deliver secure firmware update packages and additional provisioning such as building-specific configuration changes. The Interface Appliance also communicates with the building's central management system to report on device inventory, device status, cyber-attack attempts in the form of forged or unauthenticated commands, and users.

Attackers that gain physical access to the building automation network or exploit an entry point into the network by way of an unsecured device will launch attacks on the components that make up the secured building network. Through this they may attempt to conduct malicious activity such as eavesdropping on the network traffic in an attempt to obtain useful data, or capturing, modifying and playing back data in an effort to tamper with sensor readings or issue commands to actuators, etc. In addition, they may attempt to control connected devices to launch DDOS attacks or attempt to access the building owner's IT infrastructure. The attacks could also emanate from a rogue device that was introduced into the network in an unsecured way. With the network secured by DOME, unauthenticated devices and unauthorised accesses can be detected and blocked. (See *Figure 3*)

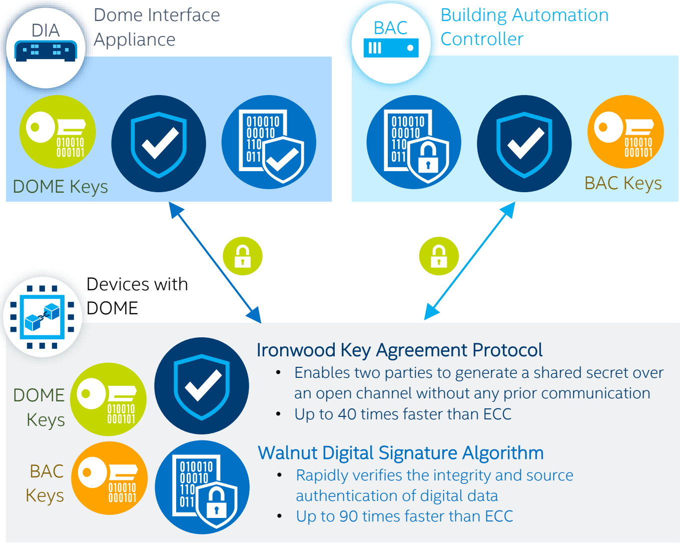

DIA
Dome Interface Appliance
DOME Keys
BAC
Building Automation Controller
BAC Keys
Devices with DOME
DOME Keys
BAC Keys
Ironwood Key Agreement Protocol
• Enables two parties to generate a shared secret over an open channel without any prior communication
• Up to 40 times faster than ECC
Walnut Digital Signature Algorithm
• Rapidly verifies the integrity and source authentication of digital data
• Up to 90 times faster than ECC

Figure 3: Deployed security

Maintained Lifetime Security

Crypto agility is an important consideration when making a long-term commitment to a security platform. Beyond secure remote updates, over the long-life of Building Automation infrastructure, one may need to consider changing the underlying security algorithms too.

This may require the ability to support quantum-resistant algorithms in future, while supporting existing standard methods today, such as ECDH/ECDSA. Veridify support Quantum-Resistant protocols, and 'Next Generation' cryptographic primitives that may emerge in the coming years to ensure the right security method is deployed today and does not become a barrier, or worse, a vulnerability as the cyber landscape evolves.

Conclusion

Together Veridify Security and Intel can help secure a building or a multi-building campus seamlessly and securely. Every device, regardless of size and operating system, can be credentialed, managed, transferred, and retired with the security necessary to create a safe and trusted environment.

From manufacture to retirement, sensor to server, across evolving threats, we can help build a "cyber security perimeter" around your smart building.

Learn More

You may also find the following resources useful:

- Partner Company:
  veridify.com
- Solution Product Company:
  veridify.com/dome, veridify.com/bitw
- Background Whitepaper: The Next Security Frontier – Taking the Mystery out of the Supply Chain
  https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/next-security-frontier-intel-and-goldman-sachs.pdf

Solution Provided By:

Veridify Security intel®

No product or component can be absolutely secure.

Intel technologies may require enabled hardware, software or service activation.

Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

Other names and brands may be claimed as the property of others.