DOME Use Case

Building Automation

Document Rev: DM202007.24

Veridify Security Inc.
100 Beard Sawmill Road, Suite 350
Shelton, CT 06484 USA
+1.203.227.3151
Info@verdify.com

Contents

Glossary

Authenticate The act of proving that a device or entity is really who it claims to be.

BAC Building Automation Controller. In a DOME building automation application, the BAC is a third-party piece of equipment that generally manages and communicates with an installed DOME-enabled device. For example, a fire suppression system may obtain temperature readings from a DOME-enabled temperature sensor.

Blockchain A series of immutable records that collectively represent the ownership pedigree of a DOME device. Each device has its own blockchain associated with it.

Block One record within a blockchain. A block is created for each owner of a DOME device.

DOME Device A product that is DOME enabled. The product is usually a board-level IoT device.

DOME Client The embedded software library that makes a product DOME-enabled.

DOME DIA DOME Interface Appliance. A server appliance that interfaces between a DOME Server and one or more DOME devices and manages the ownership and security functions. Typically, the DIA is only active when a device is initially provisioned, or when it requires a firmware or configuration update.

DOME Mobile An Android or iOS software library that acts as a DOME DIA for low volume or remote deployments.

DOME Server The heart of a DOME ecosystem. Generates the cryptographic keys, digital certificates, and other items provisioned onto DOME devices. It facilitates the ownership transfer of devices and optionally manages the blockchains associated with DOME devices.

HSM Hardware Security Module. A third-party hardware platform that securely generates keys and certificates. In some installations, a portion of a DOME server may manage the generation of digital keys and certificates.

Ironwood KAP Veridify Security’s key agreement protocol that helps DOME devices and the endpoints they communicate with authenticate each other and establish encryption keys to protect the data exchanged between them.

SHA-256 A cryptographic hash function used by DOME to enable a device to determine if the contents of its blockchain have been changed.

WalnutDSA Veridify Security’s digital signature algorithm that is used by various components of DOME to provide message authentication and integrity.

Target audience

This document is written for Veridify Security technology partners and prospective customers and provides a thorough description of how DOME can be used in a market application. In this paper, the use case is Building Automation and is intended to give the reader a better understanding of DOME's functions and benefits.

Introduction to DOME

DOME is Veridify Security's Device Ownership Management and Enrollment solution designed to address the onboarding and management of IoT devices now being deployed in a wide range of markets and industries.

The term 'IoT device' can reference a broad range of products from low-resource sensors and actuators, running on 16-bit or even 8-bit processors, to large industrial machines and automobiles. No matter what the "device" is, securely connecting the device to its owner and maintaining protected communications are critical to establishing a safe and trusted environment. Larger high-value IoT 'things' are typically managed through direct interaction by the owner or manager. However, smaller products, often deployed in the thousands or even millions, demand the same level of security and management but typically cannot be individually addressed in any reliable or productive manner. DOME is designed to address these challenges. It simplifies IoT device enrollment and ownership management, and it provides a secure, scalable framework for the future.

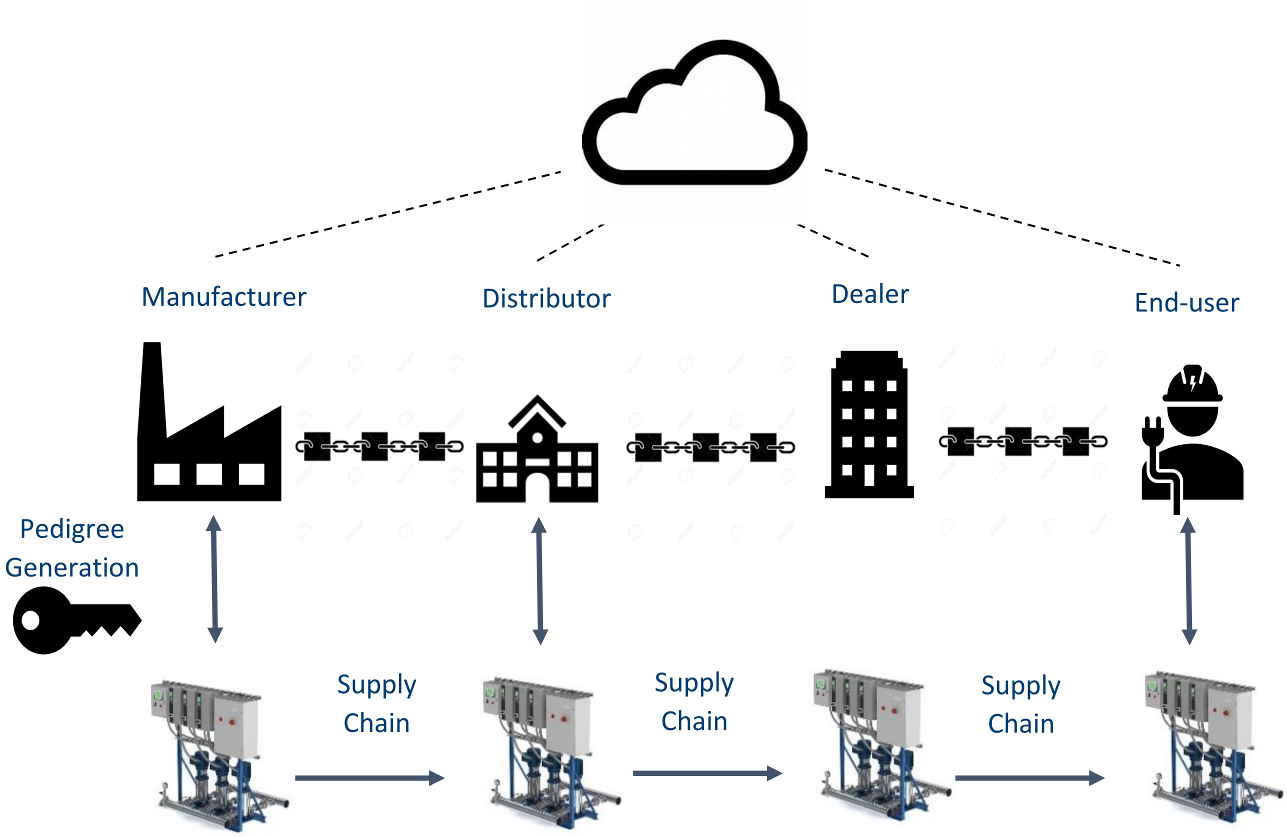

Fig. 1. Device ownership changes throughout its lifecycle.

Fig. 1. shows a general DOME solution. At the start of a DOME implementation, a device is provisioned (left side of diagram) with the DOME Client software library plus public key credentials that are shared with its original owner (in Fig. 1. – 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.

Crypto agility is an important consideration when making a long-term commitment to a security platform. DOME's architecture is designed to recognize that different users will have different priorities when it comes to choosing security primitives and that these priorities could change over time. For example, long-life applications like Building Automation may need to consider quantum-resistance now when selecting a device ownership solution. Still, a shorter market-life solution, such as a consumer product, may not need to address this requirement. DOME supports legacy methods (ECDH/ECDSA), Veridify's quantum-resistant protocols, and 'Next Generation' cryptographic primitives that may emerge in the coming years to ensure the right security method is deployed today. This agility ensures the platform does not become a barrier, or worse, a vulnerability as the cyber landscape evolves. In the proof-of-concept implementation of this use case, this discussion will use Veridify's Ironwood Key Agreement Protocol (KAP) and Walnut Digital Signature Algorithm (DSA) – but the DOME user will make the final choice on primitives. Most important, DOME's crypto agility addresses a broad range of markets and applications today, where trusted ownership, device identity, authentication, and data protection are a must, including industrial IoT, smart grid, automotive, medical devices, and more.

The balance of this paper will describe how DOME can be used to support Building Automation and secure all the connected devices found in an office or industrial building. A building such as an office tower can be viewed as its own ecosystem or, if it is part of a campus or business park, it may be part of a more extensive networked infrastructure. The range of devices in a building or campus that may need to be addressed are shown in Fig. 2. No matter what type of building or campus is under consideration, IT professionals must establish a cybersecurity perimeter inside which all devices and processors are considered trusted and safe.

As noted in Fig. 2, building devices, controllers, and management systems are networked to provide efficient operations, typically using building industry-specific protocols like BACnet, KNX, and Modbus. The list of potential protocols grows when you add the smart home market. DOME and the related applications described in this paper are platform agnostic. That is, the security functions and features described in the following sections are designed to comply with the standard for each building protocol and to not conflict with any specified messaging format. With this in mind, the balance of this paper will not address any particular method but rather discuss the general features and functions of the DOME solution in a commercial building.

The security lifecycle for any device used in a building begins prior to its installation and ends with the device's decommissioning and removal from the building. DOME validates device ownership pedigrees before installation. During installation, devices are authenticated and provisioned by a DOME interface appliance (DIA) and then handed off to a building's automation or system controller to perform their intended day-to-day function securely.

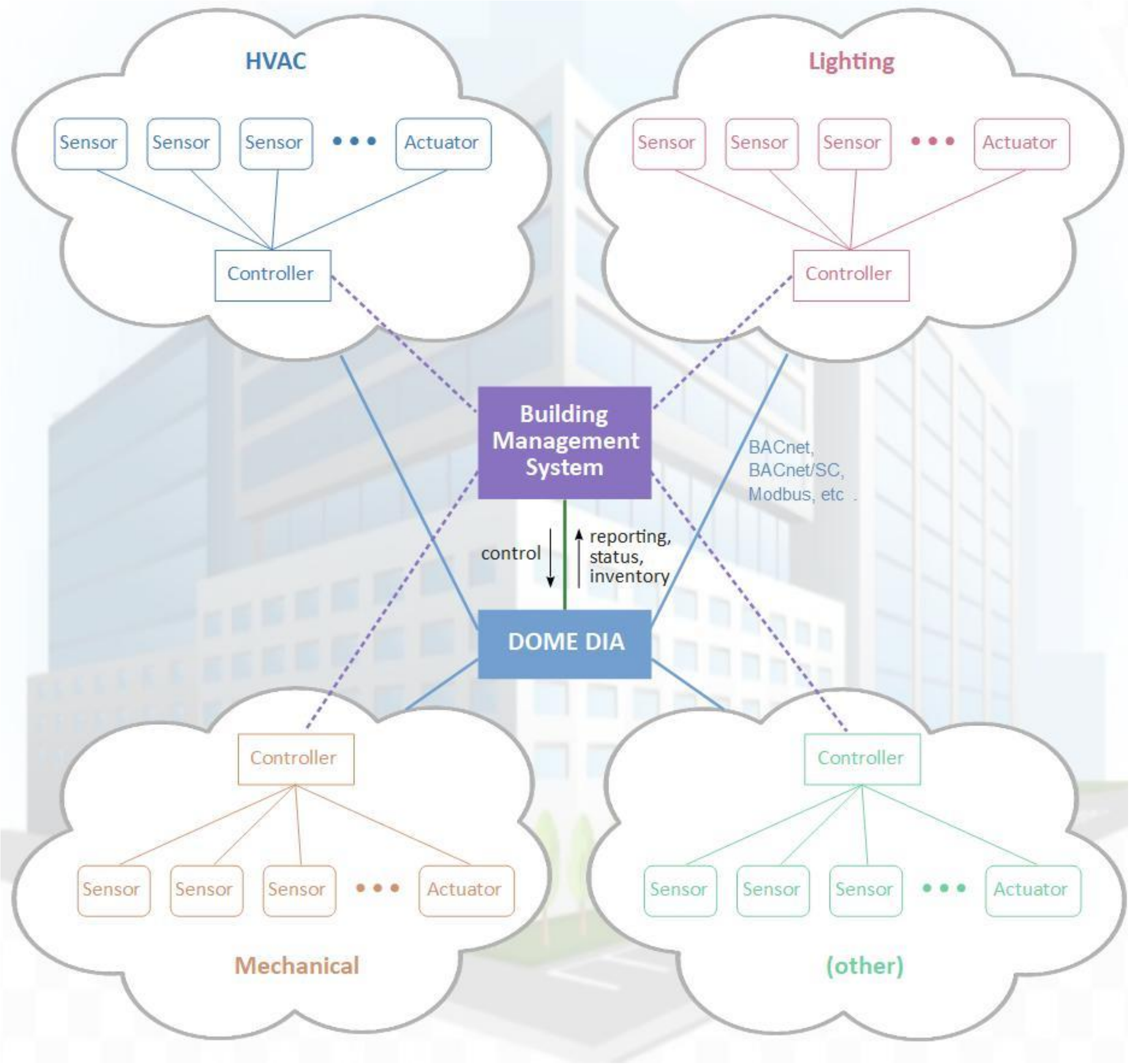

Fig. 2. DOME office building ecosystem

A DOME DIA maintains the identification, authentication, and connectivity to every device it has enrolled within the building's ecosystem as well as the building controllers that interact with those devices. The DIA monitors device status and can deliver secure firmware update packages and additional provisioning, such as building-specific configuration changes. The DIA 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.

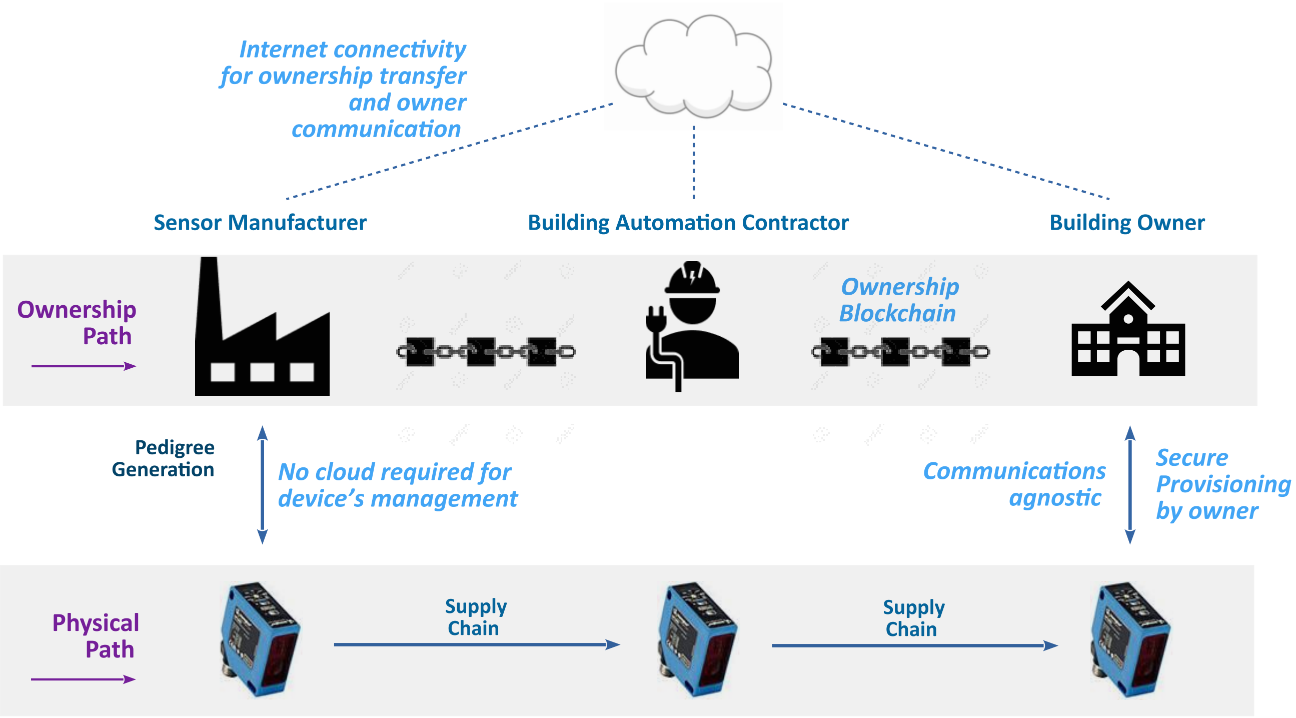
Internet connectivity for ownership transfer and owner communication
Sensor Manufacturer
Building Automation Contractor
Building Owner
Ownership Path
Ownership Blockchain
Pedigree Generation
No cloud required for device's management
Communications agnostic
Secure Provisioning by owner
Physical Path
Supply Chain
Supply Chain

Fig. 3. Overview of Secure Ownership Transfer

Building Automation Use Case

The balance of this document describes a Building Automation (BA) use case for Veridify's DOME solution. An overview schematic of this use case is presented in Fig. 3. DOME can support any number of devices, including smart lighting, elevators, HVAC systems, or fire alarms. In this paper, we will use a building sensor that will be created and credentialed by the Manufacturer and shipped to a Building Automation Contractor who will install and onboard the device within the building's ecosystem.

DOME's physical architecture is presented in Fig. 4. For this paper, DOME deployment has been simplified to aid comprehension. Specifically, this means:

1. In this paper, Veridify Security hosts the DOME servers. In other implementations, a manufacturer, property manager, or building owner has the flexibility to host a DOME server at their location or that of a global partner.
2. The DOME server generates the device's public and private keys and provides all signing on behalf of the device. In some applications, this may be done by a Hardware Security Module (HSM) at the owner's location.
3. Veridify Security stores all blockchains (each DOME-enabled device has a unique blockchain associated with it). Alternately, the ownership blockchain can be passed to each owner and reside within their system.
4. Veridify Security provides a DOME interface appliance (DIA) that interacts with devices at the device manufacturing site and end-user sites.

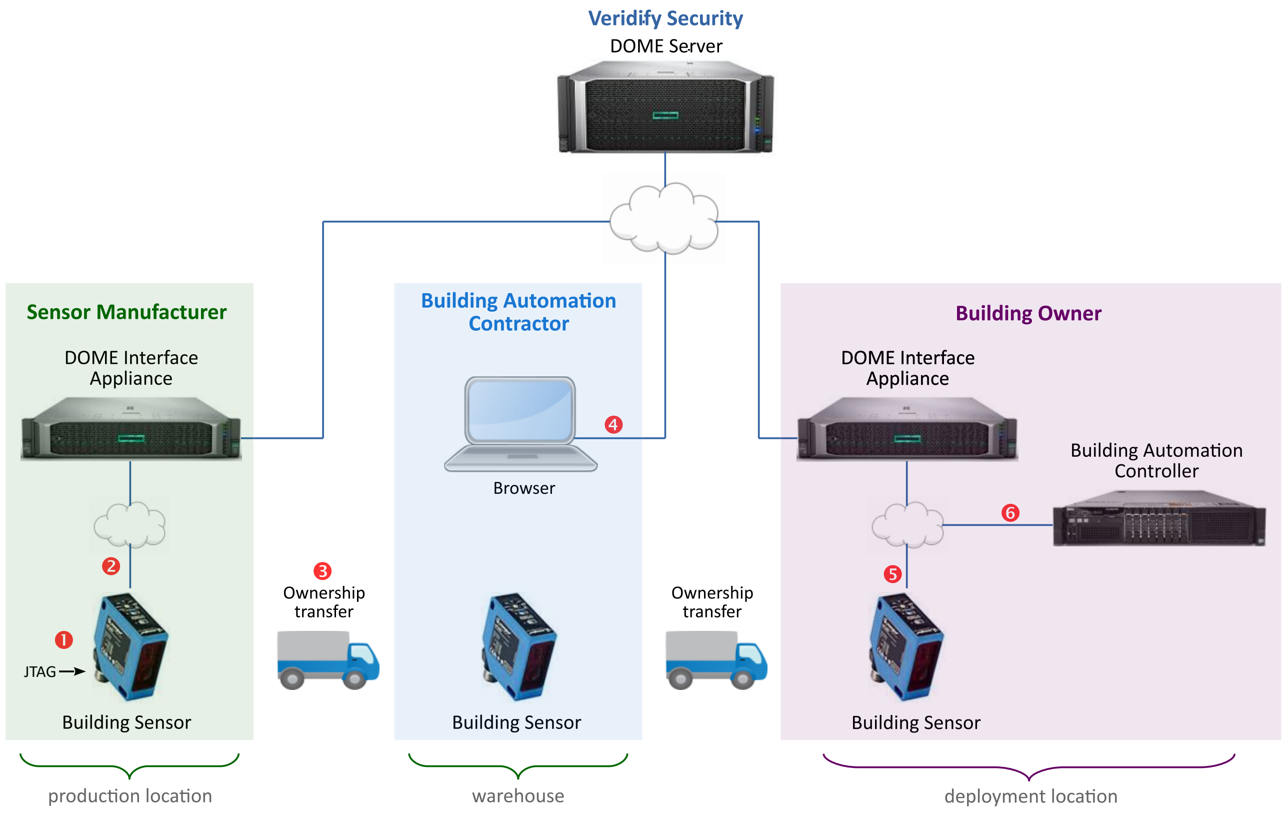

Fig. 4 DOME ecosystem for this use case only

This use case features a sensor manufacturer that sells its sensors to an automation contractor who, in turn, sells them to a building owner. The automation contractor installs the sensors in the building and provides on-going support for the sensors and associated equipment.

The use case components consist of the following –

Sensor device:	An IoT device with low resource processor and Ethernet interface
DOME server:	Hosted by Veridify at Cloud service provider
DOME interface appliance:	Veridify Security model DIA3000 with Trusted Platform Module (TPM)

Overall operation

The operations performed during the sensor's lifecycle are summarized here. A more complete description of each step follows this section.

❶ Provision sensor firmware including sensor application, DOME client library, Key Agreement Protocol (KAP) engine, and DSA signature verification engine. Sensor firmware is a typical build of the software, i.e., nothing is unique from sensor to sensor. Firmware provisioning would generally be done by the Manufacturer using the Manufacturer's preferred process (usually done via JTAG).

❷ Provision sensor ID, sensor DSA public key, sensor KAP private key, and sensor KAP public key signed by Manufacturer. These elements are unique to each sensor. The provisioning is done by way of the DOME Interface Appliance located at the Manufacturer's site. This provisioning may include a Hardware Security Module (HSM) where highly secure implementations are required. For this use case, the provisioning is done via the Ethernet interface. See the "Sensor creation scenario" below.

❸ Ownership transfer is mainly done within the Veridify Security DOME server. This function is where the Manufacturer transfers the sensor's (i.e., sells the sensor) ownership credential to the automation contractor. Then later, the BAC transfers the ownership credential to the Building Owner. This transfer is facilitated by signing the credentials into a block of credentials (a Blockchain) for each sensor.

❹ The automation contractor initiates an ownership transfer of the sensors to the building owner. The contractor performs this transfer using their DOME dashboard account.

❺ Proof of ownership, whereby the Building Owner proves it is the rightful owner of the sensor, and device authenticity where the Building Owner authenticates the sensor (see "Deployment scenario" below).

❻ The Building Automation Controller is the equipment that the sensor connects to for its day-to-day operation. Sensors access the DOME Interface Appliance and/or the Building Automation Controller as necessary per the state and function of the sensor. When the sensor first comes online, it gets provisioned into the BAC's control, and subsequent accesses are between the sensor and BAC using locally defined credentials.

The following sections provide further detail on the operations.

Sensor creation scenario (step 1 and 2)

Before shipping, the sensor needs to be provisioned with unique information. The process begins with the DOME Server creating the sensor's ID, DSA public key, DSA private key, KAP private key, and KAP public key signed by the Manufacturer (collectively called the "initial provisioning items"). This process may be managed by an HSM where required. The server also creates the initial pedigree document for the sensor that contains the initial provisioning items, except for the private keys. The pedigree also includes a timestamp. Lastly, the DOME server creates the first block of the ownership blockchain (Block 0) that consists of the initial pedigree document signed by the sensor itself using its DSA private key. This block is provisioned into the sensor by the DIA together with the initial provisioning items. The security-critical items that are generated during this phase, namely the DSA and KAP private keys, are created within a hardware security module (HSM) located within the server. The DOME server may be hosted by Veridify Security or by the customer.

The sensor's root of trust (RoT) is created when the sensor signs Block 0, and this process is a key differentiator between DOME and other device management solutions. By generating their own RoT, DOME-enabled devices can ascertain ownership (i.e., identify and authenticate who their current owner is) by themselves without the assistance of a cloud service or other entity.

When the sensor is first powered on, after having its firmware provisioned, it goes into an initial provisioning state. Its Ethernet interface comes up with DHCP enabled (DOME also supports wireless connections). A DHCP server on the local area network assigns the sensor an IP address, subnet mask, default gateway, and DNS. The sensor then connects to the Manufacturer's DIA using a local-net hostname and port (the Manufacturer must run either a local DNS server or an mDNS service). This connection initiates a device creation operation whereby the DIA requests Block 0 and initial provisioning items from the Veridify Security DOME server and provisions them onto the sensor. The sensor is programmed to accept these items and write them to Flash memory.

Ownership transfers (step 3 and 4)

When the Manufacturer wishes to transfer the sensor to the automation contractor, the Manufacturer initiates the transfer through the DIA user interface. The Manufacturer enters the sensor ID and automation contractor ID into the DIA, which gets communicated up to the DOME Server; the server looks up all necessary data to transfer the sensor to the automation contractor.

Upon receiving and validating an ownership transfer request, the DOME server creates a SHA-256 hash of the current pedigree block. The server then creates a new block consisting of the hash of the current block, the automation contractor's keys, the automation contractor's ID, and the timestamp. The server then uses the Manufacturer's DSA private key to sign the new block and appends it to the sensor's blockchain and stores it.

Step 4 denotes the transfer of ownership from the automation contractor to the building owner. The contractor facilitates the transfer via their DOME server dashboard account.

Deployment scenario (step 5 and 6)

To move a sensor securely into a building's ecosystem, the DOME interface appliance (DIA) must be provisioned and configured by Veridify Security and then installed at the building owner's site. The Building Automation Controller (BAC) must also be configured with a DSA verification engine, KAP engine, and associated keys. The DIA sits on the network and responds to sensor initial boot-up requests to authenticate; once authenticated, it hands the sensor to the BAC for owner-specific provisioning and day-to-day use. The interactions between the BAC and devices are supported by a secondary set of crypto keys, enabling not only authentication but firmware, application, and key updates to the device's application layer. In general, only a single DIA is required at any given deployment site because typically, the DIA is active only during a sensor's initial provisioning or when a configuration or firmware update is being pushed out to a sensor.

Once installed, the sensor device must be registered. The automation contractor plugs the sensor into the sensor's physical location, and the sensor ID at that location is recorded. This step, associating the sensor ID with its installed location, can be eliminated if the owner's infrastructure is configured to detect which sensor is plugged into which Ethernet port.

The sensor powers up and attempts a network connection to a local-net IP hostname and port on which the DOME interface appliance indicates its presence using the mDNS protocol. If the sensor and DIA are on different networks, the router that passes traffic between the two reflects incoming mDNS requests to both local networks. If the connection is successful, the sensor queries the DIA and is told that it has a new owner. The sensor then initiates a proof of ownership operation whereby the building owner's DIA must prove that it owns the sensor. If the sensor is able to authenticate the DIA, the sensor can optionally be required to authenticate itself to the DIA. The DIA can then install a local credential for use between the sensor and the BAC and inform the sensor how to contact the BAC. From this point forward, the sensor and BAC can interact as they typically would without any DOME input. The local credential enables the sensor and the BAC to authenticate each other mutually, then subsequently encrypts messages passed between each other.

Sensor power-up

When the sensor powers up, it goes through the boot-up procedure specified by the Manufacturer (typically, the standard startup and initialization, possibly with secure boot). After sensor power-up, it determines whether it has already been initially provisioned. It does this via an API call that examines an area of Flash memory reserved for cryptographic keys and other elements. If the sensor determines that it has not been provisioned, it attempts a connection to the DIA, whose default hostname has been hardcoded into memory. Once connected to the DIA, it receives its provisioning (see Fig. 5).

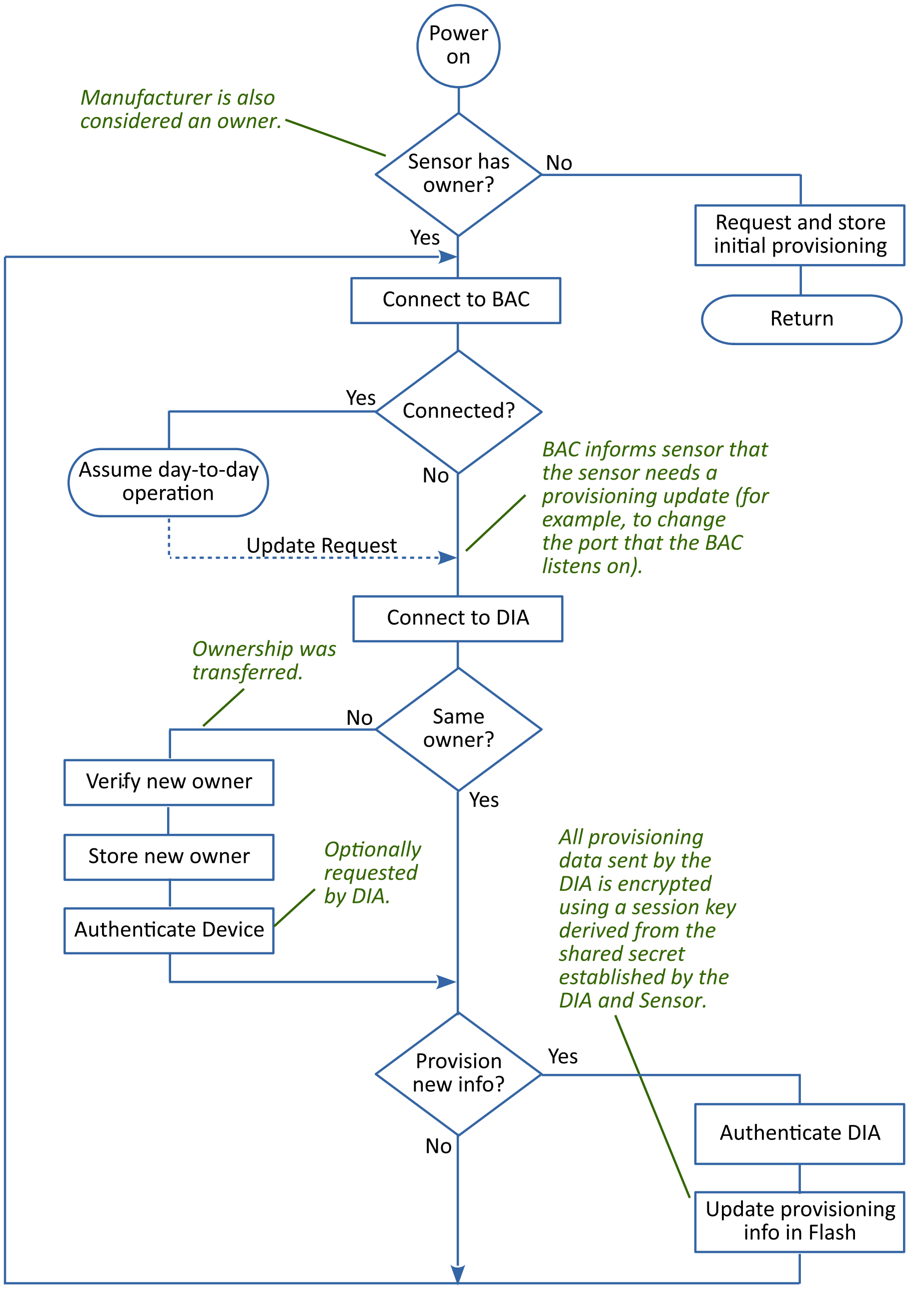
Power on
Manufacturer is also considered an owner.
Sensor has owner?
No
Request and store initial provisioning
Return
Yes
Connect to BAC
Yes
Connected?
Assume day-to-day operation
No
BAC informs sensor that the sensor needs a provisioning update (for example, to change the port that the BAC listens on).
Update Request
Connect to DIA
Ownership was transferred.
No
Same owner?
Verify new owner
Yes
Store new owner
Optionally requested by DIA.
Authenticate Device
All provisioning data sent by the DIA is encrypted using a session key derived from the shared secret established by the DIA and Sensor.
Provision new info?
Yes
Authenticate DIA
No
Update provisioning info in Flash

Fig. 5. Sensor power-on reset

If the sensor determines that it is already provisioned, it attempts a connection to the BAC (based on connectivity information provisioned onto the sensor). If the BAC is reachable, the sensor assumes its day-to-day operation. If the BAC is not reachable, this may signify that the sensor's ownership may have been transferred. The sensor requests its pedigree via the DIA and extracts the "number of owners" information from it. If the number of owners has increased, the sensor initiates a proof-of-ownership operation.

Provisioning by the building owner

The new owner of a DOME device can provision data onto the device, such as the IP address of the equipment the device should connect to for its day-to-day operation. There are two categories of data an owner can provision: 1. device-specific data intended for a particular device; 2. global data that is designed for all devices. The DOME Interface Appliance can handle both categories of provisioning. Most data can be provisioned entirely automatically, but some data, such as the positional location of a particular device, may be automated or require a data entry step by an operator or installer (in this case, to associate the location of a sensor with the sensor's ID). If the owner's IT infrastructure can associate each sensor with its Ethernet switch port, then the owner can associate any given sensor with its physical location. A scan would be run that discovers the device ID for the sensor at each physical location, thereby automating the association of location and sensor. In a production deployment of DOME, an installer would grab any sensor and install it in the building on a particular floor, room number, and place. The system can automatically record the sensor ID for the sensor he or she installed in that location, running a scan to associate all sensors with their locations. If the local system has not automated this process, then the installer can enter the sensor ID manually by scanning a bar code or an embedded NFC chip, and entering the location code. Next, the DIA would import a file in JSON format that contains (in this scenario) a list of device IDs along with their coded location codes ({device_id: "12345", location: "1-3-302-10"}). If necessary, the user can enter this information into the DIA manually. Ultimately, the Building Automation Controller will extract this data from the sensor for its day-to-day operation. The DIA parses the imported JSON data looking for the "device-id" tag to identify the sensor in its inventory with which to associate that record (the DIA receives its sensor inventory when the ownership of sensors is transferred to it).

After the new owner's DIA authenticates the sensor, the DIA would provision the sensor with the following: location code, device secondary KAP private key, device secondary KAP public key signed by the new owner, new owner's DSA public key, BAC hostname, and BAC port. The BAC hostname and port specify how the sensor is to reach the BAC. The secondary keys enable the sensor to authenticate with the BAC mutually. All of the data provisioned by the new owner's DIA is encrypted using a derivative of the shared secret established during the sensor/DIA authentication session.

For this simplified use case, the DIA obtains the sensor's secondary KAP private and public keys from the DOME server. Neither the DOME server nor DIA tie these keys to any particular sensor. Moreover, the DIA never stores the KAP keys. The keys are encrypted when sent by the DOME server to the DIA.

The new owner may need to provision additional data or update existing data (such as a new port number for the BAC). This function is handled by an "Update Request" API call to the DOME client.

DIA user interface

The DIA runs under a secure version of the Linux server. All interaction between the user and the DIA is browser-based. The DIA requires users to log on. The UI enables owners to initiate an ownership transfer of one or more sensors. It displays the sensor inventory and status of any given sensor. The UI is also where the owner enters provisioning information for one or more sensors.

Resulting benefits

As exemplified in this use case report, the main advantages of DOME are:

- Secure zero-touch provisioning of data and configuration settings in the field
- Sensor ability to quickly authenticate its owner with no cloud or third-party
- Every device pedigree captured in a blockchain
- Ability to transfer ownership of a device an unlimited number of times
- Crypto agility – the support of legacy and quantum-resistant methods
- DOME Client deployable as software with support for ultra-low-resource processors

These features enable vast amounts of sensors to be securely and cost-effectively deployed. After the DOME framework is in place, other benefits accrue, as illustrated in Fig. 6. These include:

❶ *Secure channel between the sensor and the building automation controller.*

This enables the sensor to ensure it is talking to an authentic controller, and it allows the controller to ensure it is talking to an authentic sensor. Further, it provides for data integrity and confidentiality for messages passed between the sensor and the automation controller.

❷ *Secure channel between Manufacturer and sensor.*

This facilitates the secure delivery of software updates to the sensor, user registration data to the Manufacturer, etc.

❸ *A pedigree that contains an irrefutable chain of ownership.*

This pedigree enables manufacturers to verify ownership for warranty and other purposes. It also gives manufacturers and owners an electronic trail that records the sequence of custody, control, and transfer of sensor devices.

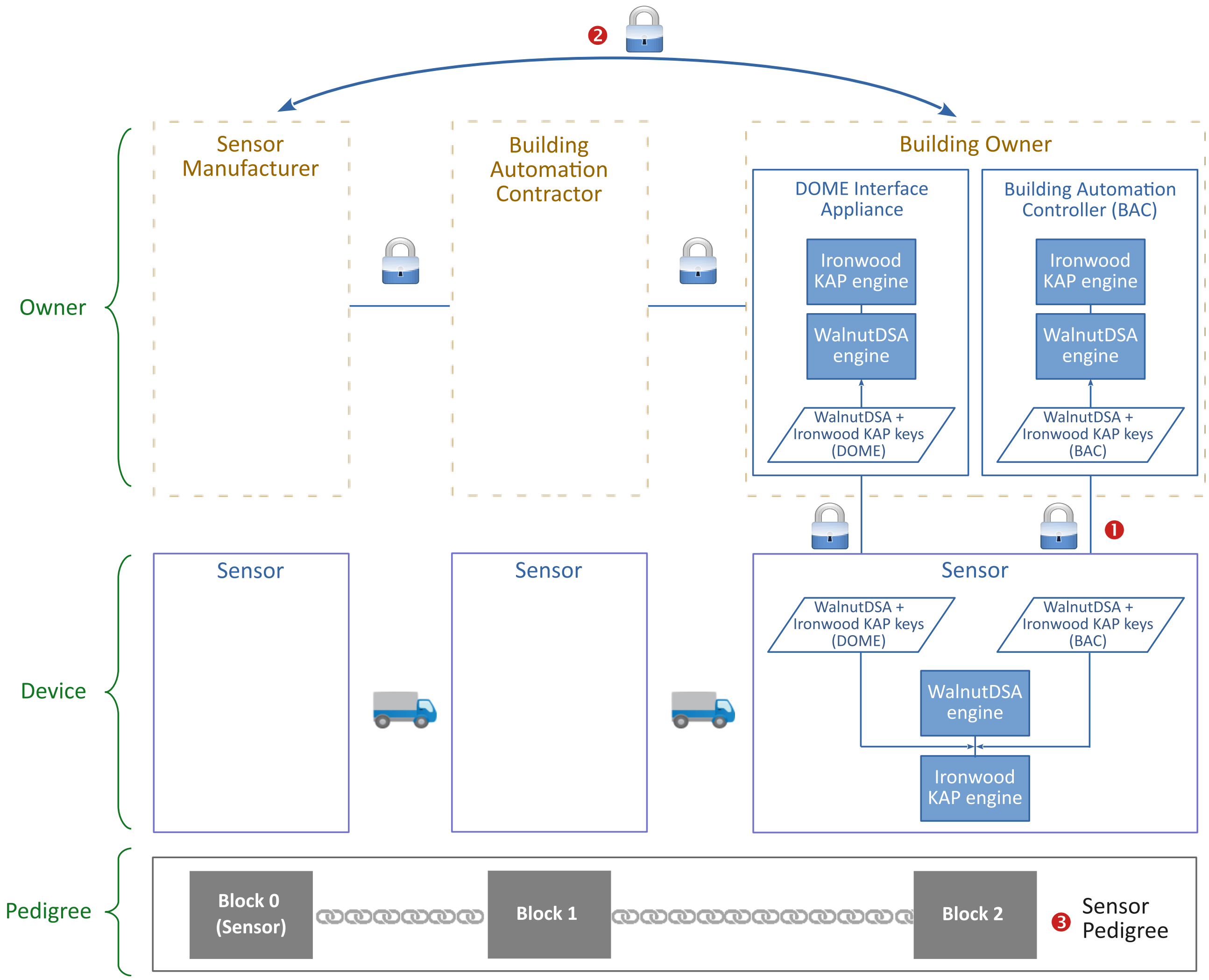

Fig. 6 DOME Framework in place

Summary

DOME is a software-based solution that creates a lifetime ownership model for each device that is then managed in a blockchain. Using DOME's zero-touch onboarding process, every device entering the IoT can create its own credential. With this credential, a new entity can prove its ownership of a device and gain access to critical functions on the device, including keys, passwords, and software updates.

Crypto agility is critical in addressing the security needs of any system in a continually changing digital landscape. DOME uniquely supports legacy methods like Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithms (ECDSA), small, fast, quantum-resistant methods like Ironwood KAP, and WalnutDSA, and 'next generation' primitives that will emerge in the future to protect against the ever-changing cyber environment.

In this white paper, we have used Building Automation to demonstrate how DOME can 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.

In addition to addressing security in Building Automation, DOME is ideally suited for a broad range of markets, including industrial IoT, smart grid, automotive, medical devices, and others where trusted ownership, identification, authentication, and data protection at the edge of the IoT are a must.