White Paper
WP1001.1

DOME™ Platform Features

Introduction

When it comes to large-scale IoT device management and security, a project may find balancing these two considerations to be at odds with each other. Rolling out and onboarding a large-scale IoT device deployment requires a large amount of resources, and project managers facing deadlines may be pushed to cut corners in order to meet their goals. At the same time, security is critical, and any corners cut during implementation may open the device – along with the connected network – to vulnerabilities. Think of a typical project that could be looking to distribute IoT devices throughout the EU into an industrial setting, or perhaps one that has actuators or sensors that need to be placed in hundreds or thousands of locations across North America. Both scenarios are happening every day. So how would you securely add these devices to your network, and then manage them? Equally important, how will this device, possibly living on the edge of the IoT, manage and protect itself to ensure all the incoming communications and commands are authentic? The answer to this question is what led us to develop DOME™, our Device Ownership and Management Enrollment solution – designed to address the smallest processors that power the IoT.

DOME is a zero-touch onboarding and device ownership management solution for globally distributed, low-resource devices at the edge of the IoT. It is a scalable platform that addresses security and provides critical tools for IoT device management. DOME simplifies the delivery of security functions and uses a software-based model to quickly and easily deploy on almost any processor platform - including low-resource 32-bit, 16-bit, and even 8-bit devices. With DOME, every processor is an active participant in authenticating any party connecting to a device, and it leverages a lifetime-pedigree embedded in a blockchain.

At the supply chain birth of a device or processor, DOME creates a device-specific credential that is shared with its first owner, the manufacturer. This process is shown on the lower-left side of Figure 1. This framework allows owners to establish proof of ownership without the need for a persistent cloud or network connection and to securely manage the device throughout its lifecycle in the supply chain. The figure below represents a typical supply chain and illustrates how DOME connects each entity and user in the supply chain to the processor's blockchain pedigree. With DOME in place, owners and devices have mutual authentication that can be used to develop and deliver over-the-air firmware updates and collect data securely.

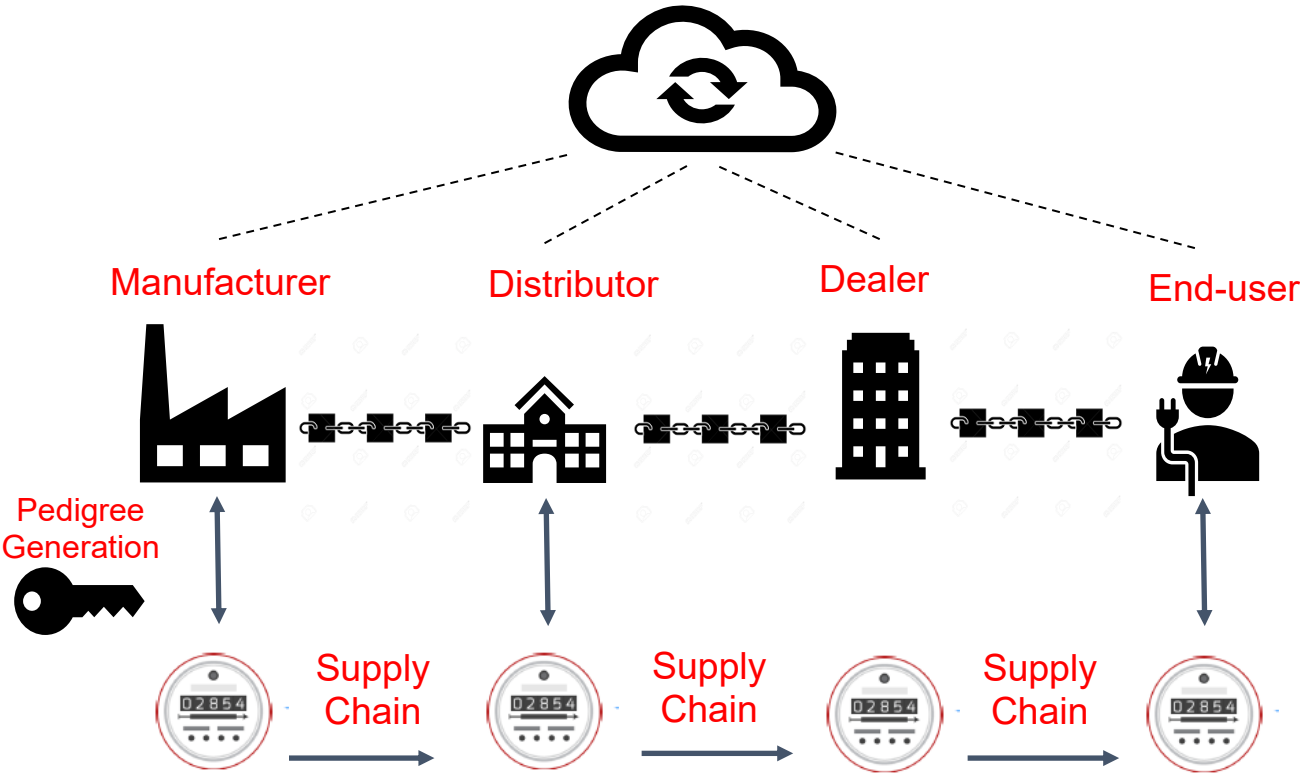

Figure 1: DOME platform

Device owners authenticate their devices and prove their ownership through cryptographic mechanisms and a blockchain-based ownership pedigree that results in mutual authentication between the owner and their device. With this proof of authenticity, the device can show it is not a counterfeit, and as a result, participate in secure communication and management functions. This post-ownership management includes the capability for an owner to supply additional keys and credentials to the device, as well as other personalization parameters.

With a secure DOME platform, users can develop a range of custom applications like improved warranty registration, secure servicing of devices, an improved return authorization, gray-market detection, automated secure firmware update and delivery, and the enablement for custom platform extensions. This paper will give a brief example of how these custom applications can be deployed.

DOME Platform Overview

In addition to the primary benefits of in-field ownership transfer, zero-touch provisioning, proof-of-ownership, and the ability to prevent counterfeit devices, DOME supports the development of communication services between manufacturers and owners as well as additional user-defined features.

With DOME, when an owner initially connects to a device, or later in special update use-cases, it proves its ownership to the device by presenting a blockchain-based ownership pedigree document to that device. The device then verifies the chain because the chain is rooted in the device. Simply put,

the DOME device is the final arbiter of its ownership. This authentication can be mutual and extended beyond the owner-device relationship. For example, an owner can prove ownership and possession to a manufacturer.

A central tenant of DOME is that the manufacturer of a device can generate and maintain a relationship with the end-user (owner) of that device, even if the device has transited several hands in the supply chain before reaching the end-user. This function is an opt-in service for the user.

As illustrated in Figure 2, the manufacturer is the first owner in the chain and holds a unique position in the pedigree document; moreover, the manufacturer can verify the chain back to itself in a similar manner that the device would. In this way, the manufacturer verifies the owner of a device by asking the owner to present the pedigree and then prove possession of their private key, part of the credential structure (in the same way a device would).

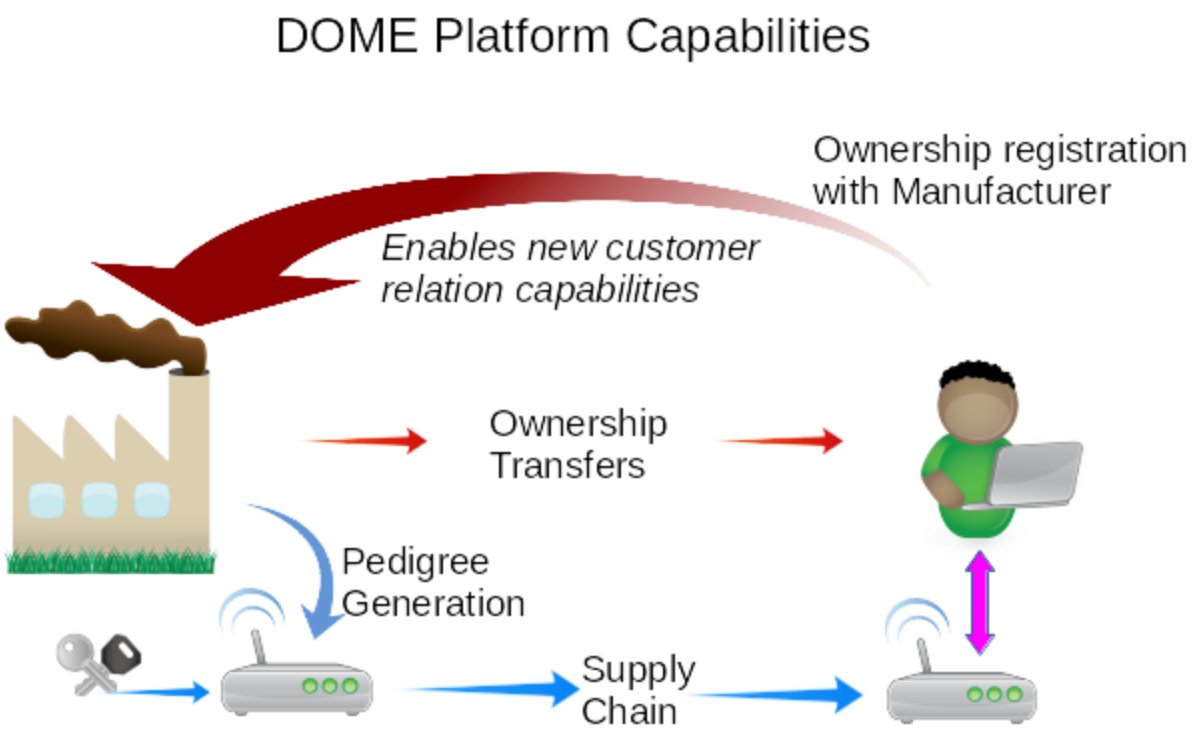

Figure 2: DOME Platform Capabilities

Using DOME, a manufacturer can require a “proof of device possession” to occur, wherein the user proves to the manufacturer that they have the device in their hands, and it is operational. To accomplish this, the manufacturer sends a message to the owner that only the device can read and asks the owner to present the result from the device. This roll-call step can be used to prove that the responder is the current owner of the device. Moreover, these processes also prove to the manufacturer the provenance of the device, because the manufacturer sees and validates the full device blockchain pedigree, which the manufacturer can use later.

With these new relationship capabilities, DOME enables the development of new or improved functionality for customer relationship management and device ownership processes.

Use Case: Warranty Registration, Service, and Returns (Gray-Market Protection)

Today, many industrial products are registered in manual processes, which may involve sending in some documentation. In some cases, an installer may register the product on behalf of the owner. In a growing number of cases, the owner can perform this registration by going to a website and filling in the same information, which includes the owner's information as well as the device model and serial numbers and possibly even a purchase receipt. This typically consists of using a QR code that encodes the device-identifying data, but this often requires manual processing by the owner. This information is usually required by the manufacturer to provide warranty service.

DOME can simplify these steps and speed up the registration process whereby a customer registers the ownership of a product with its manufacturer in an automated manner by simply installing a DOME client. Note that this is distinct from DOME's zero-touch device deployment that enables a device to discover its owner and register itself into the owner's domain.

To register a device with the manufacturer, the owner of the device need only supply their ownership pedigree and then verify their key (the same process they would use to prove ownership to a device when the device is deployed). As the ownership pedigree already contains the device information, the user would not need to enter that separately. Similarly, a receipt would not be necessary, as the pedigree includes date stamps on all transactions showing when ownership transferred. This process can be further automated by DOME, where the registration can occur automatically and simultaneously with device deployment. Imagine the complexity and cost reduction opportunities, especially for high volume applications where there are potentially millions of devices.

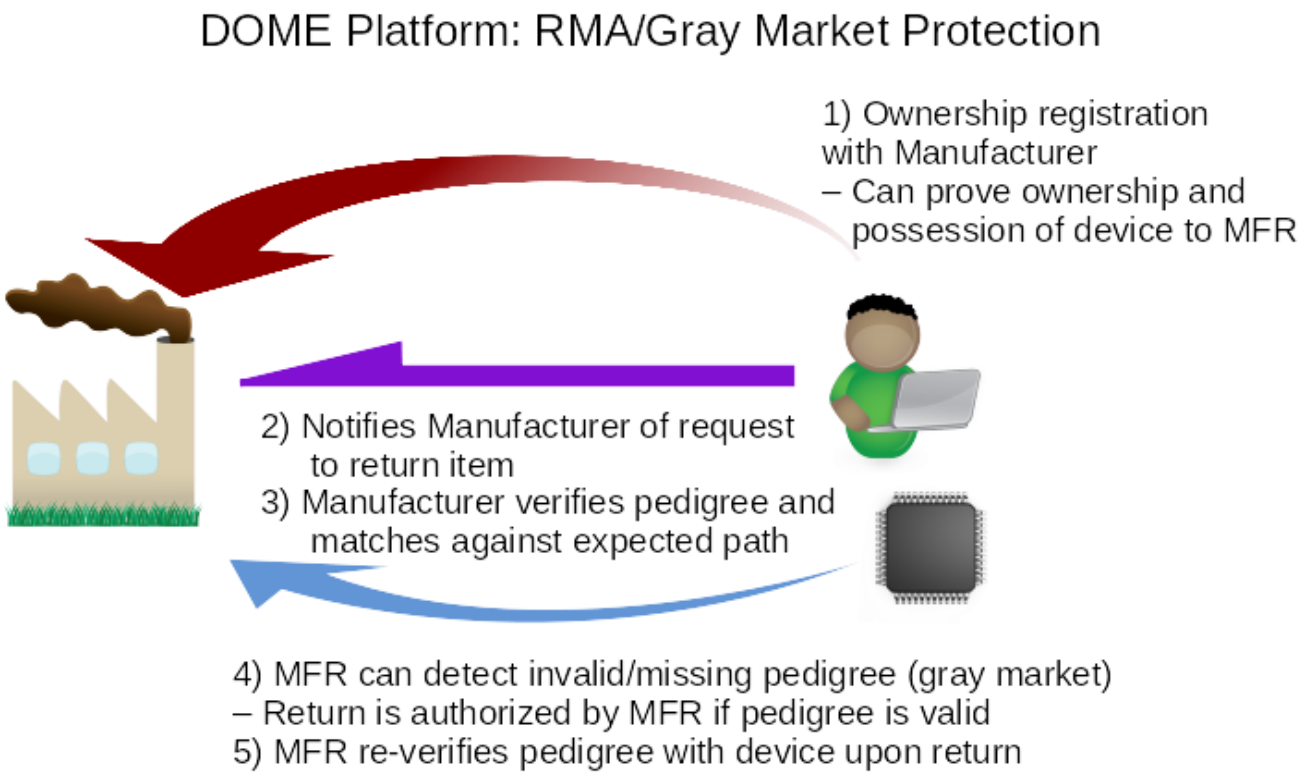

Figure 3: DOME Platform: RMA/Gray Market Protection

DOME users can leverage the authentication of ownership to develop return authorization solutions, to help the manufacturer prevent gray-market arbitrage of a device. As the pedigree refers to a specific device, the manufacturer can verify the provenance of a device when it is returned. Specifically, they can check whether the path claimed is the route the device has taken (which can affect the return policy) by validating the blockchain. A direct-sales customer could not return a part that was acquired (perhaps more inexpensively) through another path because the blockchain would show the alternate sales channel and not the direct path.

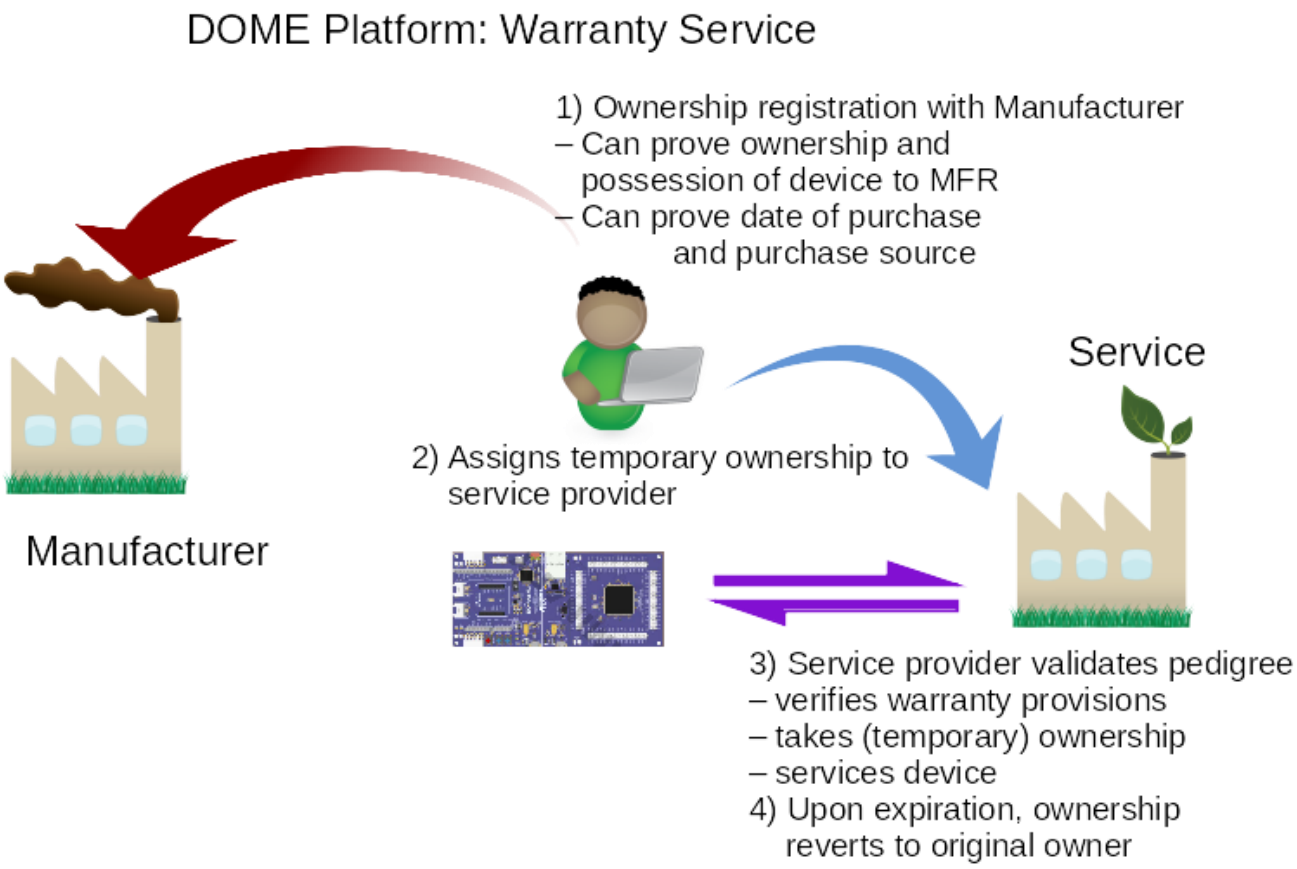

Figure 4: DOME Platform: Warranty Service

Similarly, for warranty service and repairs, the current owner can authorize the manufacturer (or an authorized service center) to have access to the device via DOME's temporary ownership transfer mechanism. In this way, the owner can provide a token to the service center that permits them to "take over" control of the device for a short period. After time expires, the ownership of the device can revert back. Since DOME can tell the manufacturer when the device was sold and when it was deployed, it can help ensure that the warranty service occurs within the authorized warranty period, meets the manufacturer's warranty restrictions, and no longer requires a secondary receipt.

Use Case: Firmware Update

In addition to improved and simplified warranty service, users will also benefit from registering with manufacturer's DOME servers to develop firmware update notifications. Starting with the same

registration process, an owner-created application can automatically inform the manufacturer what devices it owns as a result of the registration. Part of this registration could include a mechanism for the manufacturer to notify the owner (via DOME) of updates, which again can be automated as part of the inter-DOME-server communication. From a user's point of view, the work is correctly delivered as a result of the secure onboarding process. When the manufacturer creates an update, they can sign the update and push it to the owners of the devices. The owners receive the update notification and can audit the changes before pushing them down to their devices. This push "counter-signs" the update, so when the device gets the update, it can verify that it came from the manufacturer (via the original signature). The device can also confirm that the owner signed off on allowing the update (via the countersignature and via the owner's authorized "take the update" command). This process can also support scheduling the update at a convenient time.

Using DOME, users can develop over-the-air (OTA) updates that provide automated delivery. Today, larger devices have automated the update process. Still, for smaller remote IoT devices, users often must search to find whether an update exists, download the update, and then push it out to their devices. DOME enables a user to automate this process, as illustrated below. DOME can also be used to support event-based notifications of updates, rather than waiting for the owner to check a dashboard.

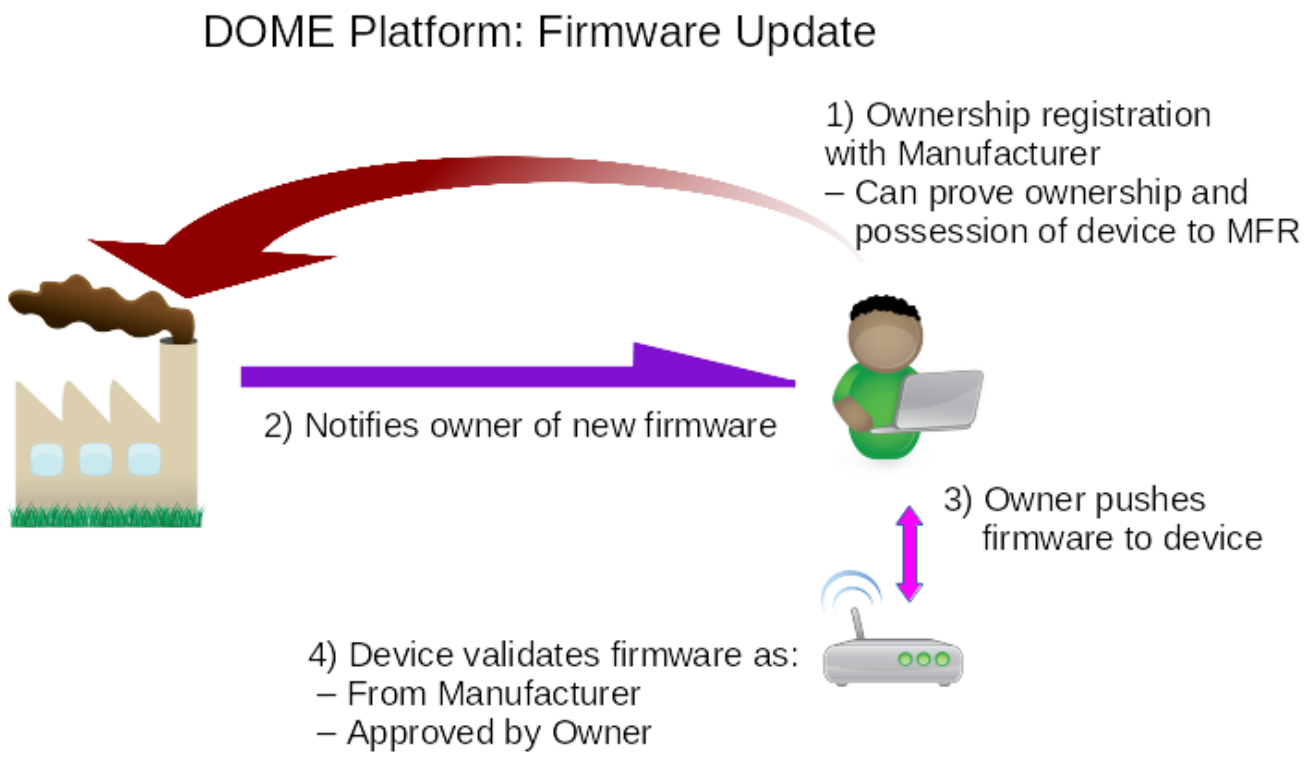

Figure 5: DOME Platform: Firmware Updates

Additional/Future Manufacturer Services (DOME as SaaS)

With the flexibility of the DOME platform, we have shown how manufacturers can create, develop, and deploy additional services to their customers. DOME provides authenticated communication between owner and manufacturer and can give the manufacturer information about what devices are

owned and deployed (registered with the manufacturer). User-developed applications created with DOME include warranty and service registration, gray-market detection, firmware update notification, and delivery services. DOME enables additional services within its communication platform, so users have the freedom to develop custom applications based on the needs and requirements of their marketplace or application.

Conclusion

DOME is an end-to-end framework that allows manufacturers and participating owners to extend their relationship beyond the one-time purchase of an IoT device. It can support the development of additional services such as improved warranty service, gray-market detection, and real-time firmware update notification and delivery. DOME is software-based so manufacturers can develop and quickly deploy future ideas. Finally, manufacturers can leverage the digital relationship with owners and their devices to improve their warranty service and returns policies. Owners can further benefit from developing an automated method to receive and deploy device firmware updates. These initial services should encourage manufacturers to implement DOME and encourage owners to register their devices. Future use-cases are endless.

All of these user-created functions are possible and leverage DOME's zero-touch deployment for low-resource devices requiring small client code size. The result is improved ease of use, with faster and lower-cost implementations running on a quantum-resistant platform that is ISO 26262 compliant.

For More Information

To learn how the DOME platform can benefit your application or to set up a meeting with a Veridify Security expert, contact us at info@veridify.com.