Creating a Secure Chain of Custody for Obsolete Parts

DUST IDENTITY

Executive Summary

Identifying the provenance of a part is the only way you can trust that the part functions as intended and is free of vulnerabilities. Obsolete parts and components lack clear provenance which reduces trust, increases risk, and threatens readiness. The market for obsolete parts requires traceability and a secure chain of custody.

Secure Components implemented DUST Identity's Diamond Unclonable Security Tag (DUST) to see if it could meet the needs of the obsolescence market. The goals were to have individuals with limited training tag parts and components of multiple sizes and types with DUST, attach digital records to those items, and track their movement between geographic locations. DUST exceeded all of Secure Components' objectives.

Company

Secure Components

Industry

Aerospace
Defense
Critical Infrastructure

Outcome

Dust exceeded the requirements for obsolescence provenance.

The Problem

Secure Components is a strategic sourcing company focused on Diminishing Manufacturing Sources and Material Shortages (DMSMS). It maintains AS9120 and AS6081 certification and is on both the Defense Logistics Agency's (DLA) Qualified Suppliers List of Distributors (QSLD) and its Qualified Testing Suppliers List (QTSL). Prior to delivery, Secure Components tests parts and components to ensure they meet customer specifications. Following testing, those parts are tagged to ensure that the delivered part has been validated by Secure Components.

Due to material security requirements, the tagging must occur at a third party. This process is time consuming and delays delivery by a minimum of thirty (30) days. Additionally, the fact that untagged parts travel to a third party is a break in the chain of custody and a security compromise. Finally, there is no method to link individual tested parts to their respective test data, as current tagging methods only provide batch level identity.

> Current technologies such as RFID and UID have proven ineffective as a method to authenticate material after their initial procurement into the DoD's supply chain, let alone commercial contractors and integrators, who generate a large amount of the surplus material, sought after by DoD sustainment activities for legacy weapon systems. DUST Identity reduces the risk of surplus procurement, by providing DoD agencies with a complete chain of custody which would reduce engineering costs and contracting lead times, and increase mission readiness."

Stephan Halper,
Principal, Director of Business Development

The Solution

The Diamond Unclonable Security Tag (DUST) prevents non-genuine parts from entering the supply chain and provides full lifecycle provenance for genuine components. When applied to a surface, the DUST marking creates a unique, physically unclonable "fingerprint" based on the configuration of quantum engineered nano-diamonds. No existing tools can recreate a known pattern precisely, nor can the patterns be removed intact from a given surface.

With DUST, security is embedded in the random nano-diamond configuration, and not only the marking material. Therefore, DUST can be distributed widely and used at any point in the supply chain without fear of compromise (e.g., component manufacturer, distributors, test labs, etc.) This increases mission readiness as parts no longer need to be sent to a secure site to be marked or authenticated. It also allows for a reduction in costs by removing protections (e.g., cleared personnel, 24x7 surveillance, vaults, etc.) that are required to safeguard sensitive material.

DUST allows individual item identification and therefore provides the physical-digital binding to track and secure components throughout the supply chain. It enables association of digital records (e.g., test records) with a specific item and allows global traceability. Alternative technologies cannot provide this capability because, in most cases, they provide only batch level security, are expensive or hard to authenticate, or simply cannot fit on small form factors. DUST is the only technology that meets these requirements as well as providing clear tamper evidence and global scalability.

The Objectives

01 **Mark multiple item sizes and types with DUST.**

02 **Enroll an item with DUST Scanner and associate documents to the physical DUST marking.**

03 **Allow staff, with limited training, to mark, enroll, and authenticate.**

04 **Authenticate enrolled items at another geographic location.**

05 **Download associated documents from the DUST Application.**

The Procedure

Multiple components of varying size were marked with DUST. The DUST material was placed in a MIL-STD epoxy coating and cured with a UV light. The purpose of this element of the effort was to display the ability to apply DUST to a wide range of item types and sizes (Objective 1). A subset of the items that were marked is shown below:

Integrated Circuit

Ancillary Components

Voltage Regulator

Hard Drive

Touch Screen

Transformer

Component Reel

Shipping Labels

Rejected Parts Labels

Following application of the DUST Material, the DUST Scanner was used to enroll the items. The DUST Scanner is a handheld device that can be used locally to rapidly discriminate between genuine and untrusted markings. The time to scan is a fraction of a second ensuring that end users can identify genuine components without creating bottlenecks or requiring that parts be sent to third-party labs.

Once enrolled, the DUST Application was used to associate digital documents to physical items such as images of the item, data sheets, test reports, and part rejection labels (Objective 2).

By associating test reports with physical items, it is possible to ensure the provenance of parts and components and to trust their functionality. The association of part rejection labels with physical items is also important since it prevents rejected parts from making their way back into the supply chain. The DUST Application was also used to chain transaction data to the Hyperledger Fabric blockchain for SAP government and manufacturing customers. DUST Identity is an SAP Partner (Figure 2).

Marking, enrolling, and authenticating was performed by both DUST Identity and Secure Components staff. Secure Components staff was provided with minimal training but was still able to easily mark, enroll, and authenticate items (Objective 3).

Following enrollment, several components were sent from Secure Components facility in Pennsylvania to be authenticated at DUST Identity's offices in Massachusetts (Objective 4). Once received, the items were authenticated, and the digital documents were downloaded from the DUST Application (Objective 5). Using the DUST Application's location-based tracking, it was possible to track the location of the items as they moved between different geographic locations.

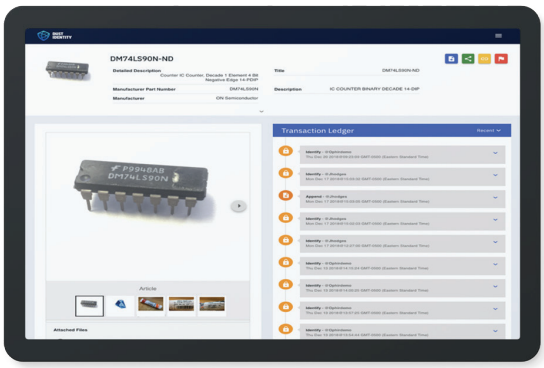

Figure 1
The DUST Application.

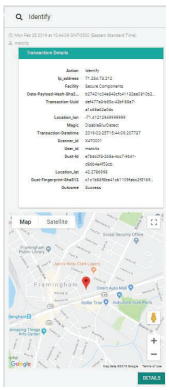

Figure 2
Object transactional details within DUST Application.

The Conclusion

Traceability and provenance are the keys to establishing trust in parts and components. Obsolescence and DMSMS present a difficult use case due to the inability to securely link digital data to physical items.

Secure Components evaluated DUST to determine if it met their requirements for secure and trusted physical-digital binding. The requirements that DUST was forced to meet included flexibility of application, on-site marking and authentication, ease of use, ability to associate multiple document types to a physical item, and global traceability.

DUST provided Secure Components with a scalable and cost-effective solution for validating obsolete parts and tracking provenance.