How to Build Trust & Drive Accountability Across the End-to-End Value Chain

DUST IDENTITY

The Supply Chain Challenge

Due to the global and modular nature of modern supply chains, the authenticity and integrity of a given component threatens the security of the entire system. Any single component represents a potential point of failure or compromise from an adversary. A $5 component has the potential to jeopardize a $50M asset. This is a very real challenge facing government entities and commercial enterprises in today's global marketplace.

Close collaboration is key to combat cyber risks. In 2018, DHS rolled out an ICT Supply Chain Risk Management Task Force – a public-private partnership formed to examine and develop consensus recommendations to identify and manage risk to the global ICT supply. The Department of Defense (DoD) followed suit with the Protecting Critical Technology Task Force to enhance the protection of the Defense Industrial Base.

But concerns go far beyond defense platforms as the commercial market supply chains are also at risk. Leaders on Capitol Hill are deeply concerned that commercial enterprises are not prepared for the nation-state actors that are trying to influence and infiltrate their supply chains. As a buyer of leading technologies, this also puts the U.S. government at risk.

> "I think the question I'd ask every federal employee and contractor to go back and ask your organization is: 'What are we doing to advise and inform your supply chain integrity? What are we doing as an organization to protect our supply chain integrity?'"
>
> **Bill Evanina,**
> Director of the National Counterintelligence and Security Center in the Office of the Director of National Intelligence.

The challenge of supply-chain security for both government/defense and commercial applications is that without fully understanding the chain of custody (i.e., the provenance) of a given component, operations could be compromised. While there have been attempts to verify supply chain integrity, none have been designed to support a global, modular supply chain.

Diamond Unclonable Security Tag

DUST Identity's mission is to solve the inherent problems in supply chain security and to link physical objects to their digital records – securely.

DUST Identity is an asset-centric supply chain security company created to reduce risk and improve trust in complex value chains. Our technology allows tagging of individual objects that propagate into high reliability assets such as data centers, defense platforms and critical infrastructure. The DUST solution allows organizations to associate information with physical objects in a highly secure manner that enforces trust models.

DUST Identity's core technology is based on material engineering of diamond nanoparticles. This allows the extraction of a unique and unclonable identifier from the random configuration of these nano-diamond crystals, or DUST, with a serialization space of over 10^{230} unique IDs. This identifier provides a mechanism for verification of components across the full product lifecycle.

DUST prevents non-genuine components from entering the supply chain and provides full lifecycle visibility for trusted parts.

How the DUST Identity Solution Works

The Material

The DUST nano-diamond material is used to identify components or objects from component or electronic manufacturers and suppliers. The nano-diamond material is a durable and non-toxic carbon-based material. It is an inert material that has no radio frequency, radar, or x-ray signatures, making it suitable for tracking items in areas requiring limited emissions across sectors such as defense and oil & gas. DUST can be incorporated into a variety of host coatings (e.g. acrylic, epoxy) and can be bonded to most surfaces with a minimal footprint as small as the cross-section of a human hair, ensuring it can be used on the world's smallest electronic components.

The Scanner

The DUST handheld scanner hardware enables asset owners and other supply chain stakeholders to validate components at any point in space and time and to immediately detect tampering. It is the "key" to unlock and access the component's associated data within the DUST application.

The Application

The DUST software application stores and matches the digital fingerprint that is extracted by the scanner hardware from the nano-diamond material. The DUST Application can be deployed on-premises, in the cloud, or as part of a distributed architecture. It serves as identity management for physical objects and opens up a number of capabilities and functionalities, including data storage and blockchain and features such as notification services, security modules, and so on.

Features and Benefits

01

Unique and Unclonable Identification

One of the keys to trust and maintaining supply chain component integrity is having a unique identifier. But uniqueness must not be confused with unclonability, which is a critical ingredient for secure identity. Every time the DUST is applied, by the nature of its process, a new identity is created that is both unique and unclonable. This is not derived by some algorithm that must be stored or transmitted somewhere, DUST uses the random physical process to configure its identity. It's like rolling thousands of dice on a surface.

Since security is embedded in the scan of the random nano-diamond configuration, and not an algorithm or secure marking material, the DUST stock material can be distributed widely without extra security costs (e.g., storing material in vaults, application by cleared personnel, etc.).

This facilitates its use at any point in the supply chain (e.g., OCMs, OEMs, integrators, test labs, etc.). Other solutions rely completely on the security of the marking material (e.g., DNA, secure ink, hologram stickers), which presents a huge problem. If those materials are compromised, the entire security architecture could be at risk. For this reason, those marking materials must be controlled and their application performed only by secured parties at secured facilities.

Additionally, with asset tagging systems that rely on some form of cryptography to assure trust into the future, there is a risk that the associated algorithms are not quantum-safe.

DUST Identity offers a differentiated approach that significantly reduces risk and can accelerate mission readiness of a defense platform or uptime of enterprise assets.

The DUST material can exist in nearly any type of polymer, acrylic, epoxy, or urethane. Tagging can be done for multiple types of deployments including high or low temperature and different types of harsh environments.

02 Physical-Digital Binding

In recent years, a lot of focus has been paid by the commercial industry to the potential of blockchain as a means to improve auditability. The challenge with blockchain, however, is that it lacks an anchor in the physical world to define the initial root of trust. DUST Identity enables a physical-digital binding that can anchor a physical object in a digital distributed ledger, auditing system, or blockchain application.

DUST Identity creates a digital binding for physical objects, providing the unique, unclonable identifiers that information can be tethered to, which is a problem with other solutions since they rely completely on the security of the marking material (e.g., DNA, secure ink, hologram stickers). If those materials are compromised, the entire security architecture could be at risk. For this reason, those marking materials must be controlled and their application performed only by secured parties at secured facilities. Additionally, with asset tagging systems that rely on some form of cryptography to assure trust into the future, there is a risk that the associated algorithms aren't quantum-safe.

03 Agile Deployment

The DUST solution was designed to exist within existing workflows and cost structures. The DUST Identity marking material can be distributed globally, enabling agile deployment of tagging for supply chain integrity, without the introduction of excessive friction.

DUST Identity can be implemented when an item comes into existence and is first produced by a manufacturer. It can also be implemented when a given component has been validated and enters a supply chain.

Authentication is done with real-time handheld scanners that an asset owner can use wherever required, without the need to take the part and send it to a third-party lab in order to perform a validation.

04 Secure Information Sharing

DoD and government agency applications are particularly sensitive to information sharing. This sensitivity extends throughout the supply chain with manufacturers only wanting to share information on a need-to-know basis.

DUST Identity only pulls necessary information, and it's only shown or shared when it needs to be consumed, by specific authorized devices, in accordance with policies, and in approved locations. For instance, stakeholders can be notified of verification events, providing an additional level of auditability.

05 Location-Based Tracking

A key attribute of the DUST Identity software is the ability to track locations for a given tag with location-based services. Every time a tag is scanned, the location of the scanner hardware is logged, providing a record of supply chain movement and enabling a visualization of how components move from one location to another.

06

Multi-tier Adaptive Security

The DUST solution offers multiple tiers of security without a change in the underlying nano-diamond material. This is due to its ability to extract additional information, and create a higher and more secure serialization space based on the amount of information extracted from the nano-diamonds. The benefit of offering multiple security levels is this: in order to increase security, the material or marking methodology will not need to change, only the scanner.

Supply chain participants can select a security level based on their deployment scenarios and increase security based on their specific needs. This makes avoiding detection impractical or even impossible and ensures that an organization's physical security protections are always one step ahead of cybersecurity risks.

Implementing Trust

It takes time and resources to establish trust and validate that a given component is suitable for use and consumption. The flipside of establishing trust, though, is quantifying risk, which has become very difficult, and expensive, as the sophistication of adversaries evolves to evade detection. DUST Identity offers the capability to enforce an indelible mark on a validated component, establish trust, and provide full lifecycle provenance. The process of validating trust is highly agile with the use of an easily deployable handheld scanner.

- **The DUST solution is scalable across the supply chain and can be implemented with minimal friction at the point of asset creation or asset validation.**
- **The DUST Identity platform is location and context-aware, such that information is only shared based on strict policy enforcement. The lifecycle of trust is implemented with a full audit chain for all verification events.**

> The key to protecting our digital economy and ensuring the integrity of the global value chain is to build a secure third-party ecosystem. DUST Identity's solution can serve as a 'birth certificate' for hardware and complements value chain security solutions currently on the market."
>
> **Edna Conway,**
> VP & GM Global Security, Risk & Compliance, Azure at Microsoft.

The Future of Supply Chain Security

Components in supply chains, such as the DoD's, can exist for decades, which makes maintaining the ability to verify trust more than a one-time task.

Secrets-based authentication mechanisms are often targeted by adversaries as the ability of maintaining a secret over time diminishes. The operational risk is that if a given tagging solution is compromised, the integrity of the tagged supply chain components is also at risk.

DUST Identity's unique and unclonable tag provides security that can be assured now and into the future.

About Us

DUST Identity is headquartered in Framingham, MA, and is made up of a team of cyber and supply chain leaders, quantum physicists, and nanotechnology experts. The company is an MIT spinoff, has participated in several DARPA programs, and is backed by Kleiner Perkins with participation from Airbus, Lockheed Martin, New Science Ventures, Angular Ventures and Castle Island Ventures. DUST Identity was recently named a BostInno Startup to Watch, a BuiltIn Boston Startup to Watch, and inducted into the prestigious MIT Startup Exchange STEX25.

Ophir Gaathon, PhD

CO-FOUNDER & CEO

Dr. Gaathon is a supply chain security expert with a deep understanding of the complex security challenges associated with global value chains. In his current role as CEO, he is responsible for the company's overall vision and strategy, financial operations, as well as overseeing technology and R&D initiatives. He also serves on the Board of Directors. He has led DUST Identity from inception, through the first DARPA contracts and into commercial success. He received his Ph.D. in Applied Physics from Columbia University, led research projects at MIT and Columbia, and he holds several patents. Dr. Gaathon's prior experience includes working as a postdoctoral research scientist in the MIT Quantum Photonics Lab and as a research affiliate in the MIT Media Lab's Synthetic Neurobiology group.

Jonathan Hodges, PhD

CO-FOUNDER & VP OF ENGINEERING

Dr. Hodges has extensive experience in optical system design, hardware, and software instrumentation interfaces, and microservices system development. He received his Ph.D. in Nuclear Science and Engineering from MIT and held research appointments at Harvard University, Columbia University, and the MITRE Corporation.

The DUST Identity leadership team applies years of research experience at the forefront of quantum physics to the complex challenges of global supply chains.

Investors

KLEINER PERKINS

NEW SCIENCE VENTURES

CASTLE ISLAND VENTURES

Angular Ventures

LOCKHEED MARTIN

AIRBUSVENTURES

Learn More

There's a lot more to DUST Identity than just the promise of helping to improve supply chain security through validation. Email us at **info@dustidentity.com** to request a full demonstration and to discuss your application needs.