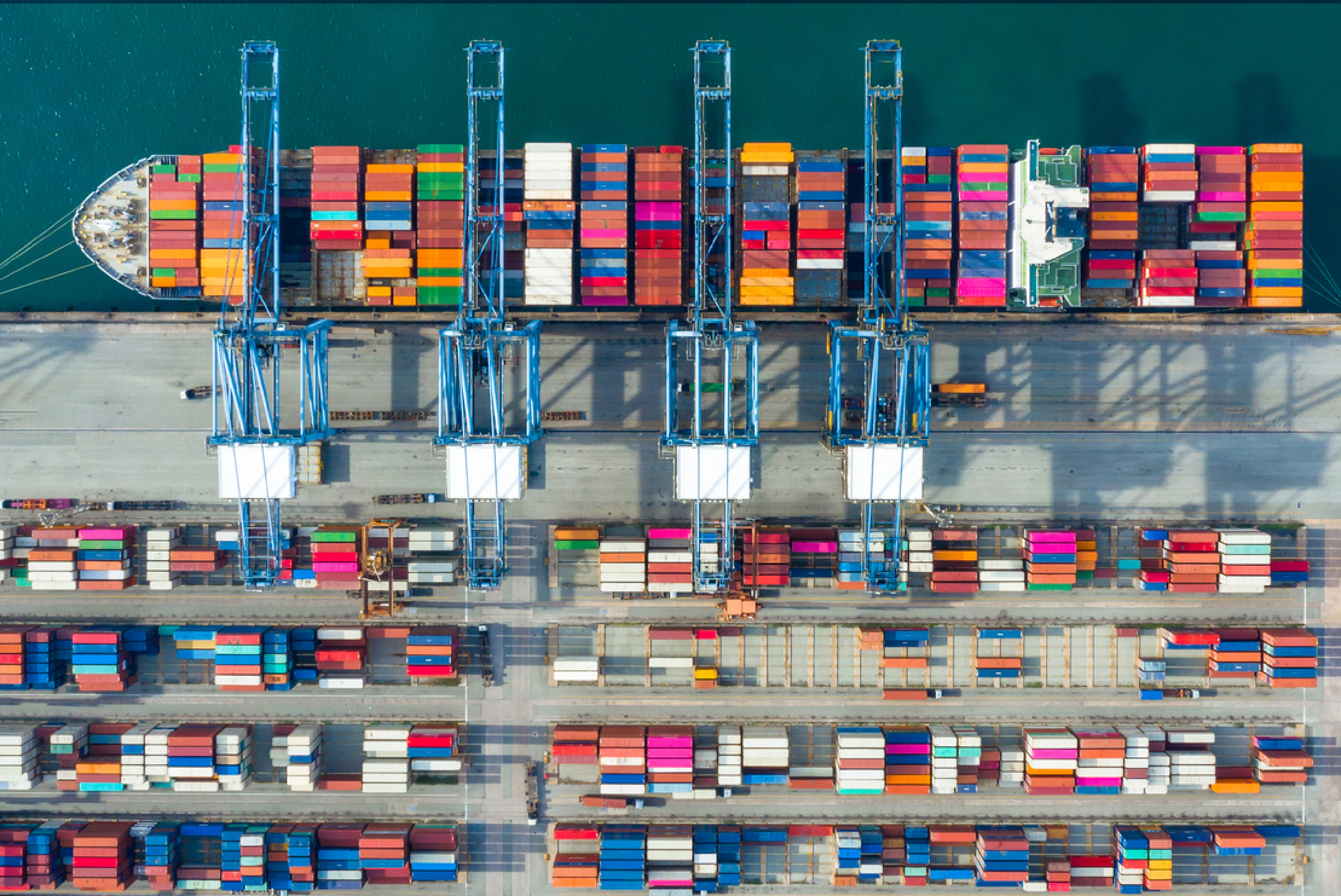
yubico

WHITE PAPER

Protecting the supply chain with highest-assurance security

Go passwordless, ensure product integrity and protect the software supply chain



Contents

The critical need for securing the supply chain

45%

of organizations will experience an attack on their software supply chains by 2025, according to Gartner. This will be a three-fold increase over 2021.[1]

Since March 2020, organizations have faced an unprecedented level of disruption on supply chains, from the global COVID-19 pandemic to the Suez Canal blockage to the freedom convoy blockade. Apart from the obvious drawbacks, these disruptions have also uncovered security gaps in the supply chain—now increasingly the target of cyber attacks. Any risk to the integrity of the products being delivered, or the security and privacy of the data or code being exchanged, could have negative repercussions on business operations and the bottom line far exceeding the immediate costs.

The reality is that organizations are increasingly reliant on a complex and multi-leveled supply chain for the products and services used to support the organization. Today's supply chain includes all the products and services acquired to support an organization, including product parts, hardware, software, and code, as well as the physical and digital interactions between people, applications, and processes. Securing the supply chain is about making explicit trust decisions for each of these products, services, and interactions.

The SolarWinds and Colonial Pipeline security breaches are merely the two most high profile incidents that have helped shed light on supply chain vulnerabilities, but a recent survey found that up to 97% of organizations have had a cybersecurity breach as the result of a weakness in the supply chain.[2] Despite the risk, another survey indicates that 62% of organizations have yet to take any steps to secure their software supply chain.[3]

A supply chain vulnerable to cyberattacks opens up enterprises to significant operational disruptions, financial loss, damage to brand, product integrity, safety issues, and the loss of intellectual property (IP). The top supply chain risks, expanded from a National Institute of Standards and Technology (NIST) brief, include:

- Third-party access (physical and virtual access) to information systems, software code, or IP
- Poor information security practices by suppliers
- Compromised software, hardware or other physical inputs purchased from suppliers
- Software security vulnerabilities in supply chain management or supplier systems
- Counterfeit inputs/hardware or hardware with pre-embedded malware
- Third party data storage or data aggregators[4]

The primary supply chain challenge for businesses is that there are hundreds, if not thousands, of entry points that need to be monitored along the way—this is particularly true as organizations move to the cloud and create more interconnected digital ecosystems with supply chain partners. Within this broader context, your security posture is ultimately only as strong as your weakest supply chain partner.

Once you see the “big picture” of your supply chain, you can set targeted supply chain security goals: assure that every product coming in—software you buy and use, code that someone else has developed, input into manufacturing, or services used—is secure and follows good security practices.

Organizations can begin their journey to reducing risk in the supply chain at all levels, by identifying and mitigating risk in three key areas:

Third-party access

IP and product integrity

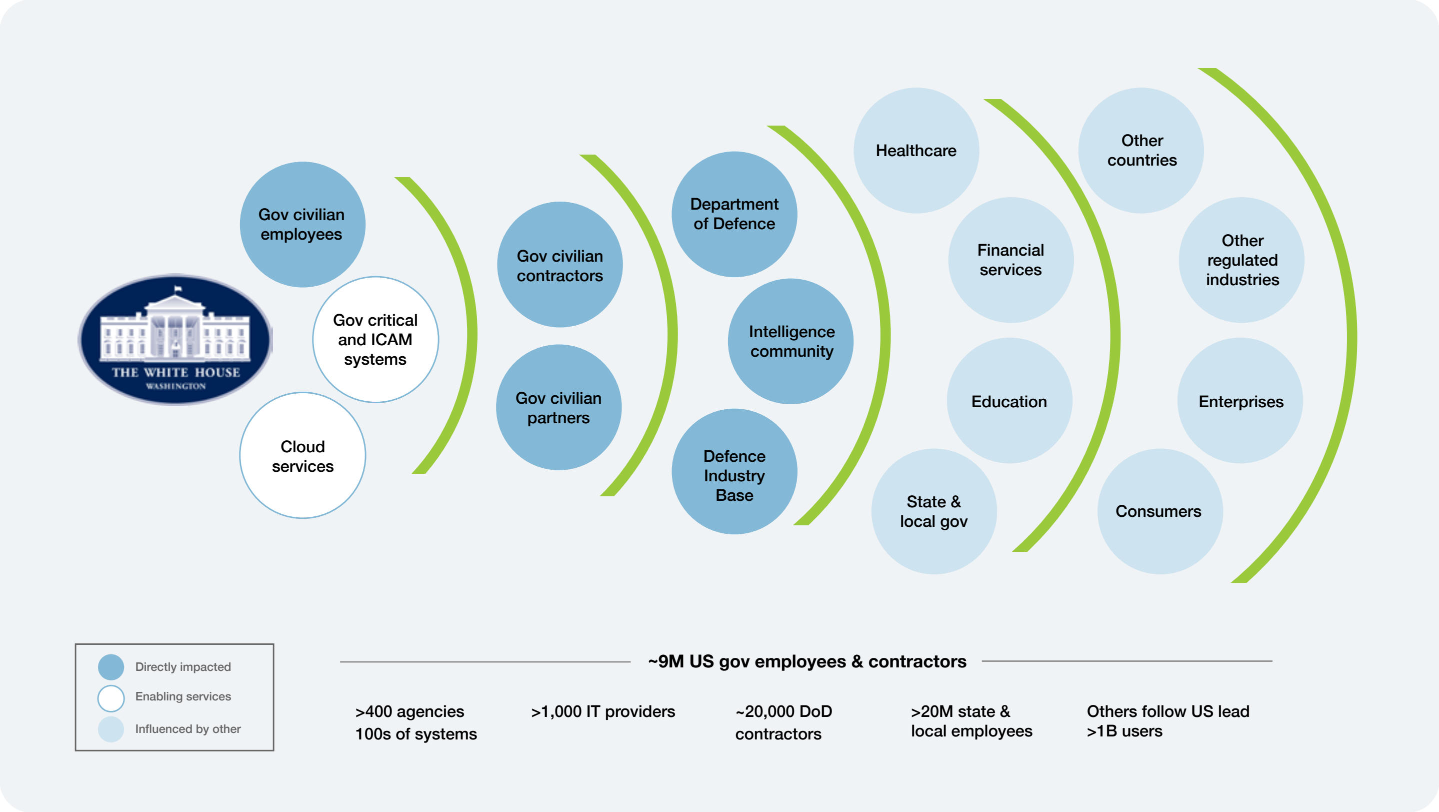
Software supply chain

> Cybersecurity risk in the supply chain also arises as a result of the inadequacy or absence of processes, procedures, and practices used to ensure the security, safety, integrity, quality, reliability, trustworthiness or authenticity of a technology product, service, or source of the products and services.
>
> –National Institute of Standards and Technology (NIST), Cyber Supply Chain Risk Management Practices for Systems and Organizations[5]

The shifting regulatory environment

The Colonial Pipeline and SolarWinds attacks not only highlighted the vulnerabilities of the supply chain, they highlighted the vulnerabilities in the supply chain of critical infrastructure and top federal agencies.

In response to the rising level of threat, in May of 2021, the White House issued Executive Order (EO) 14028, Improving the Nation's Cybersecurity, outlining new expectations & guidelines for Zero Trust and phishing-resistant multi-factor authentication (MFA) for federal agencies—as well as their suppliers and partners.[6]



Further clarifying EO 14028, the Office of Management and Budget (OMB) memo M-22-09 describes a Zero Trust Architecture strategy that urges organizations to trust no one or no thing unless properly verified before being given access to sensitive resources.[7] Zero Trust is designed to minimize uncertainty in enforcing least privilege access to systems and services based on the pillars of **identity, devices, networks, applications and workloads**, and **data**.

The strategy places emphasis on identity and access controls, including the requirement for Federal agencies as well as their supply chain partners to use phishing-resistant multi-factor authentication (MFA) to protect against sophisticated attacks. The only two standards that qualify as phishing-resistant are the Federal Government's Personal Identity Verification (PIV) standard and modern FIDO/WebAuthn.

What qualifies as phishing-resistant MFA?

PIV/Smart Card

FIDO2/WebAuthn

It is true that not all MFA is created equal, nor is all MFA considered phishing-resistant. Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. Commonly used MFA implementations featuring passwords, SMS and other One-Time Passwords (OTP), security questions, and even mobile push notifications are not phishing-resistant, as they are all susceptible to either or both of the aforementioned types of attacks.

CASE STUDY

Colonial Pipeline Attack Leveraged Compromised Credentials

A phishing attack introduced malware that shut down a gas pipeline responsible for 45% of the fuel for the east coast of the United States. After two days, and with uncertainty over the extent of the attack, CEO Joseph Blount agreed to pay a $4.4 million ransom.[8] It took even more time to restore the gas delivery supply chain.

CEO Joseph Blount told the U.S. Senate committee that the attack originated from compromised credentials used to access a legacy virtual private network (VPN) system that lacked multi-factor authentication.[9]

In addition to highlighting the weaknesses in identity and access management, the Colonial Pipeline attack also highlighted the interconnectedness of information technology (IT) and operational technology (OT) systems. Zero Trust begins with identity and access management: eliminating weak forms of legacy authentication (passwords) to shore up the software supply chain, mitigating a potential cascade impact on operations.

This attack has been a catalyst for the recognition of the need to protect critical infrastructure and supply chains. The Transportation Security Administration (TSA) announced two new Security Directives aimed at reducing cybersecurity gaps and implementing specific mitigation measures against attacks and threats for pipeline owners and operators.[10] The new requirements of EO 14028 would also apply to critical infrastructure operators.

Securing supply chain access
with modern, phishing-resistant MFA

NIST recommends organizations employ multi-factor authentication to safeguard remote and third-party access to the network

Organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain. For example, KP Snacks' internal network was breached allowing hackers to gain access to and hold sensitive files which escalated to supply chain disruptions.[11]

The most important thing security professionals can do to secure any environment is to know what they have, where it is, how it's configured, and what it depends upon. In short, it is imperative to have an inventory and a dependency map for your systems and services. While this won't stop an attacker, it is required to understand what you're protecting, who and what can access it, and when something does go wrong, what the "blast radius" is.

One of the top recommendations in the updated NIST 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations, is to update identity and access management controls for individuals, processes, and specific systems/components in the supply chain.[12] NIST recommends organizations employ multi-factor authentication to safeguard remote and third-party access to the network.

Leading the way, Apple recently announced that it would work with its more than 9,000 suppliers to drive mass adoption of multi-factor authentication in its own supply chain.[13] But while considering authentication solutions to improve the security of IT and OT systems in the supply chain, it is important to note again, that not all MFA methods are created equal.

Drawbacks of legacy authentication

Not all forms of MFA are created equal—at protecting against cyber attacks or in terms of the friction created for end users and IT support teams.

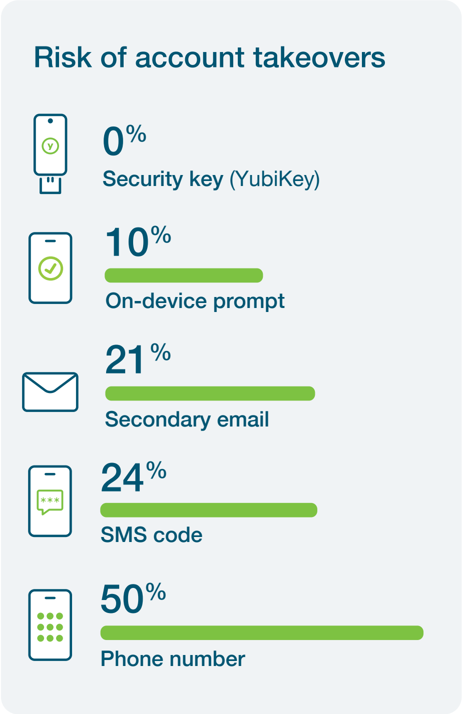
Current authentication and security solutions, including usernames and passwords and mobile-based authenticators, are no longer effective to protect organizations against modern cyber threats. Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based one-time-password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%.[14] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of **if** you will be attacked—it's a matter of **when**.

With legacy MFA such as SMS, OTP, and even push notifications, the second factor is often tied to the mobile device. This is a red flag, because of the aspects listed below:

There can be availability challenges with mobile devices sending codes in a timely manner due to poor connectivity or unreliable services.

There is no real guarantee that the private key ends up on a secure element on the mobile device.

The OTP or private key could be intercepted in some way (such as via SIM swapping)


Risk of account takeovers

Google, How effective is basic account hygiene at preventing account takeovers

Beyond security, legacy mobile authentication creates friction in the user experience, a factor which encourages unsafe behavior such as password sharing, and contributes negatively to support and productivity costs. In fact, organizations spend up to $1 million each year on staffing and infrastructure to handle password resets alone, representing only the first factor in 2FA or MFA authentication.[15]

Due to the high cost and poor security of legacy authentication, global best practice is moving toward passwordless authentication—which as the name suggests, is authentication that does not require the user to provide a password at login at all.

The future is passwordless

Passwordless authentication is any form of authentication that doesn't require the user to provide a password, including smart card and FIDO2/WebAuthn, two methods referenced by name within EO 14028, and generally acknowledged as meeting the ideals of Zero Trust.

Traditional smart cards do offer high security, but generally require high capital expenditure (CapEx) for smart card readers, physical cards, in addition to backend management platforms. Due to this, the industry as a whole is moving toward a passwordless login flow leveraging modern authentication standards such as FIDO2/WebAuthn that work well with the cloud, resulting in lower ongoing costs even as enterprises scale up.

FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.

Modern, phishing-resistant authentication and passwordless with the YubiKey

The YubiKey from Yubico provides modern strong authentication at scale across the supply chain, helping organizations and their suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical IP handoffs.

The YubiKey enables phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware security key protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[16] Finally, the YubiKey offers fast, tap-and-go passwordless login that is 4x faster than login with SMS, and is also platform agnostic, conveniently compatible with devices across the entire spectrum including desktops, laptops, mobile, tablets, notebooks, and shared workstations.

To further improve the user experience and speed of authentication, Yubico also offers the YubiKey Bio Series—FIDO Edition supporting FIDO U2F and FIDO2, which delivers the same hallmark security that all YubiKeys are known for, but with an added biometric-based passwordless experience.

Combined with YubiEnterprise Services (see below), the YubiKey is an inexpensive and easy solution to improve remote and third-party access in the supply chain.

Securing supply chain integrity

One of the risks inherent in supply chain security is the possibility of compromise to the integrity, quality, or reliability of the product, software or service being delivered.

EO 14028 requires federal government agencies, as well as their partners, to vet their software supply chain—to have visibility into all of these components to reduce downstream vulnerabilities. The same visibility should also be supplied to the physical supply chain to ensure the highest integrity of product parts.

Ensuring the integrity of IP and product parts

It is crucial to ensure that all components involved in an end-to-end process are authentic, to avoid unsolicited replication and theft, but also for quality assurance, since a manufacturing assembly line should only consist of genuinely sourced products. As a result, there must always be a solution in place to protect the integrity and intellectual property of all components from production and assembly, to repair and replacement.

The traditional approach to protect intellectual property (IP) and prevent counterfeiting in manufacturing involves the use of digital cryptographic signing keys and encryption. Cryptographic keys would be stored either in software, which is highly vulnerable to a variety of attack vectors including online channels, or a hardware security module (HSM), which is generally accepted as offering greater security by security experts. Unfortunately, conventional rack-mounted and card-based HSM devices are large and expensive, often making them impractical on the assembly floor or for IoT devices, restricting their use exclusively to large data centers.

Ensuring the integrity of the software supply chain

The software supply chain is made up of all the people, systems, and code that go into making, distributing or operating a product, application, or service. Organizations need to manage all the inputs within the supply chain to reduce vulnerabilities, including the developers, third-parties who contribute code, open-source frameworks, libraries or other IT products.

```
package com.ds.ucd.be.becore.solr;

import ...

public final class LocationUtils {

    /**
     * Parses Point from it's String representation.
     * @param locationString - String that represents location, as 2 double values split with coma. Accepts space after/before
     * @return org.springframework.data.solr.core.geo.Point instance
     */
    public static Point parseLocation(String locationString) {
        Preconditions.checkNotNull(locationString,  errorMessage: "Location String should not be null");
        Preconditions.checkArgument(locationString.contains(","),  errorMessage: "Location must be split with coma");
        locationString = locationString.trim();

        if (locationString.contains(" ,")) {
            locationString = locationString.replaceAll( regex: " ,",  replacement: ",");
        }

        if (locationString.contains(", ")) {
            locationString = locationString.replaceAll( regex: ", ",  replacement: ",");
        }

        String[] location = locationString.split( regex: ",");
        Preconditions.checkArgument( expression: location.length >= 2,  errorMessage: "Location should constist at least 2 Double parameters");
        double lat = Double.parseDouble(location[0]);
        double lon = Double.parseDouble(location[1]);

        return new Point(lat, lon);
    }
}
```

Attacks on the software supply chain

In 2020, hackers exploited a breach in the SolarWinds code signing system which allowed them to inject and distribute malicious code disguised as legitimate updates, to more than 18,000 installations of the SolarWinds Orion product across the world.[17] The version of Orion containing the malicious payload came with a valid signature from SolarWinds' software signing keys, but according to SolarWinds, the illicit modification happened in their software build system, and was not visible in their source code.[18]

A similar attack in 2021 exploited an authentication bypass vulnerability discovered within Kaseya VSA Server, and when leveraged against several Managed Service Providers (MSP) and in turn, their customers, it ultimately caused downstream shutdowns of 800 Coop supermarket chain stores in Sweden.[19]

As illustrated by the SolarWinds attack, and in essentially every breach, you'll find credentials, keys, and secrets at the heart of it.

Whether you use code that's been developed by internal teams or from external sources, it is important to always have a method of secure code-signing to make sure the code management process is validated. To manage source code and software products, organizations should:

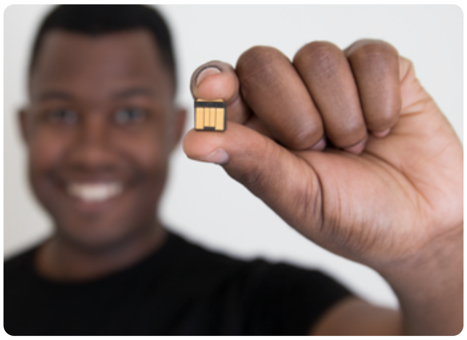
1. **Leverage a source code management (SCM) system** to make sure code is properly maintained, namely, the history of any changes, revisions or modifications (versions) are recorded, and that every person who signs in to the system is authenticated with the appropriate permissions given their role. The SCM must be well managed with clearly defined policies at all times, to establish a chain of custody, and to create a sense of trust surrounding the code.
2. **Include secure code signing** to protect all types of software modules and executables being used, and not just the software being written. This includes but is not limited to software drivers, third party applications, installation files, scripts, and firmware modules in vehicles or industrial systems, which should all be signed with PKI (Public Key Infrastructure) keys and certificates. The goal is to create a mechanism to trust that any code provided is legitimate and has not been produced by a malicious party. When working with outside sources, it is paramount to keep signing keys and certificates secure, to ensure authenticity.
3. **Look for a software "bill of materials" (SBOM)** that identifies each component and where they came from. For example, not all open-source code is created equal and attackers often take advantage of known vulnerabilities. If open-source code is being used, it must be disclosed, to help identify what may need remediation in order to mitigate any potential or discovered security threats. Identifying open-source components will allow you to more quickly address any vulnerabilities that may arise in the future, whether that is code you manage or from purchased software.

President Biden's executive order calls for all forms of code to be protected from unauthorized access and tampering. Phishing-resistant MFA and signing code commits are important security controls to improve supply chain security posture and meet compliance needs. Providing more visibility into what components are being used and how code is securely managed will also improve overall security and increase the level of trust with users.

Safeguarding product integrity, IP and code management with YubiHSM 2

Protecting the signing keys and certificates is crucial in any code signing software system, and HSMs offer a secure way to generate, store and protect both cryptographic keypairs and X.509 certificates on secure, purpose-built hardware. For organizations with increasingly high demands on IT security or those in regulated industries or high-risk environments, the FIPS 140-2 certified HSM is also an option, and recommended or even mandatory for such deployments.

Yubico created the ultra-portable and low-cost YubiHSM 2, the world's smallest HSM that comes in a nano form factor. The YubiHSM 2 enables secure, tamper-resistant key storage and operations, by preventing the copying and distribution of cryptographic keys, and preventing remote theft of keys stored in software. The YubiHSM 2 can be applied to any process where secrets and the authenticity of components needs to be managed, and where tampering needs to be prevented. It can be easily deployed to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices.

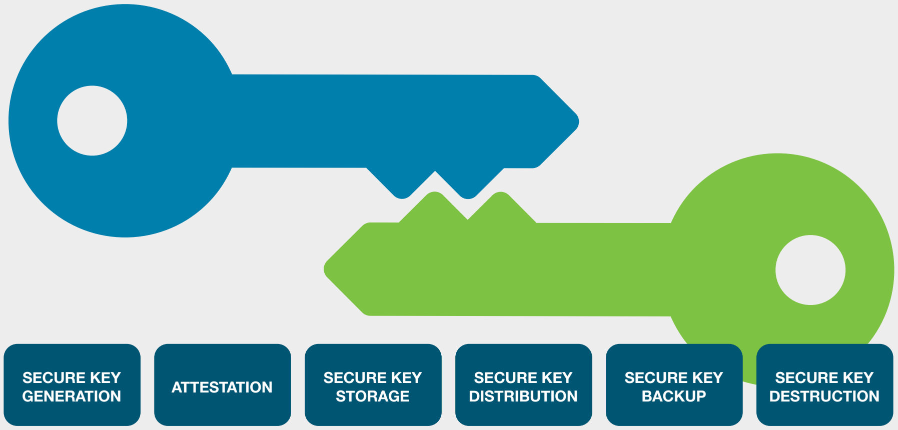


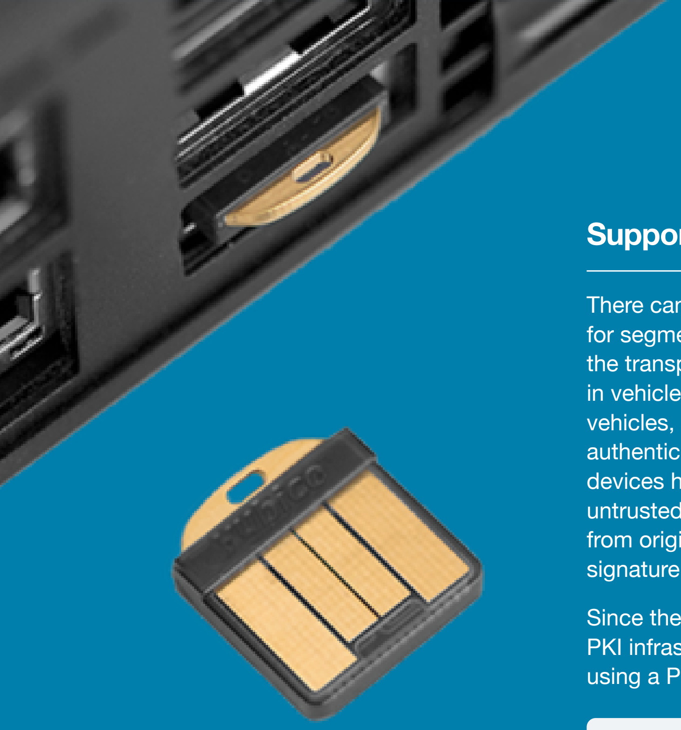
The YubiHSM 2 is currently being used to protect the manufacturing process by some of our largest customers within that vertical, ensuring only certified programming stations can interface with the intended components, or to write digital signatures onto each component to ensure authenticity. In both scenarios, the added security of the YubiHSM 2 helps to maintain a company's reputation and gives them peace of mind that their products will work as expected even after they have left the manufacturing floor.

The YubiHSM 2 is ideally suited to safeguard the signing keys and certificates for both signing code and creating digital signatures, helping support the secrets being shared within the supply chain. For organizations that need to meet the FIPS 140-2 requirements, there is also the option of the FIPS 140-2, Level 3 validated YubiHSM 2 FIPS to ensure the highest levels of data protection in addition to strict levels of compliance.

It's important to note that the cryptographic keys used to sign and/or certify components are never exposed outside of the YubiHSM 2 hardware, ensuring a high level of assurance and security. To illustrate this point with an example, even if a remote attacker is able to compromise a network or specifically the computer connected to the device, there are still no obvious attack vectors as keys cannot be extricated. On the other hand, if the same attacker is able to gain full underlying access to a software equivalent, they might be able to at least run analysis on the memory, connected database or even local files for potential weaknesses or patterns.

Securing the Cryptographic Key Lifecycle



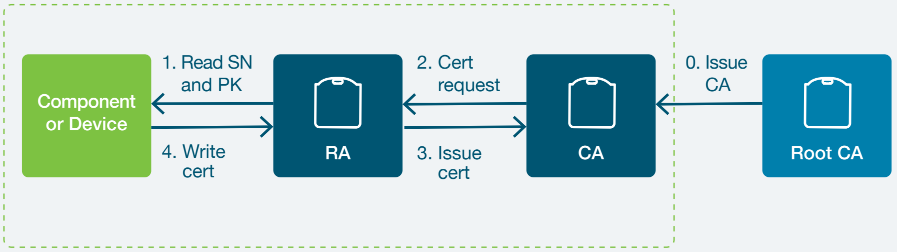


Supporting Public Key Infrastructure (PKI) environments

There can also be industry specific demands on the code signing process, in particular, for segments that are exposed to SolarWinds-type supply chain attacks. For instance, in the transportation sector, there are cases where customized code modules are deployed in vehicles that travel across the world. Security is essential when deploying code in such vehicles, so that the code modules, in many cases, are signed to guarantee their integrity and authenticity, which ultimately serve to prevent tampering or misuse. This means that the HSM devices housing the signing certificates often have to be distributed to remote and potentially untrusted locations, requiring the use of a PKI-based chain to ensure the validity of the data from origin to where the code is ultimately deployed to, and providing a means to provide a signature and verification for each step of the way along the supply chain.

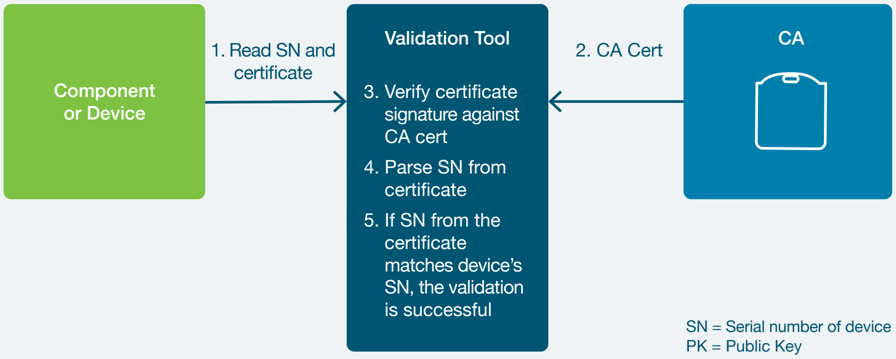
Since the YubiHSM 2 is designed to store cryptographic keys, it is ideally suited to protect PKI infrastructure and its network of cryptographic keys. The issuance process of certificates using a PKI approach, based on the YubiHSM 2 for manufacturing, is illustrated as follows:

Overview of PKI and issuance process of a certificate



In this diagram, the Root Certificate Authority (Root CA) uses a YubiHSM 2 to house its keypair (i.e. both its private and public keys) in addition to its certificate, either on-site or at an off-site data center. On the production line, a Certificate Authority (CA) can be deployed and configured with a certificate that has been signed by the Root CA as a delegate, and with this keypair and certificate, all subsequent credentials may be signed and also protected by a YubiHSM 2. These additional credentials are issued by a Registration Authority (RA) that, in turn, has had its certificate signed by the CA. Ultimately, the component certificates can then be used to check the authenticity of each component, product or device being produced, as shown in the diagram below.

The certificate validation process



3. Verify certificate signature against CA cert
4. Parse SN from certificate
5. If SN from the certificate matches device's SN, the validation is successful

SN = Serial number of device
PK = Public Key

In practical application, this enables manufacturers to verify the authenticity of each component being produced whilst requiring only a single CA delegate to sign each production line. The collection of encrypted serial numbers to the electronic control unit (ECU) can also support testing and can be used for audit tracking.

CASE STUDY

Securing the systems and supply chain at Schneider Electric

Schneider Electric is a leader in the digital transformation of energy management and automation, manufacturing electrical parts and power management systems, including a Supervisory Control and Data Acquisition (SCADA) system used for the remote management of critical infrastructure (e.g. data centers, hospitals, oil and gas).

The YubiKey enabled Schneider Electric to integrate MFA into an isolated system without the reliance on the Internet or less-secure SMS-based authentication, streamlining authentication for shift changes. The YubiKey is also being used in control situations where supervisory override actions are required. Modern MFA through YubiKeys was a part of the process to successfully achieve IEC-62443 SL2 certification.

“Safety and security are paramount at Schneider Electric and are reflected in everything we do,” notes Chad Lloyd, Director of Cybersecurity Architecture for Energy Management at Schneider Electric. “As part of our IEC SL2 certification, we included MFA in our power operation system, well positioning us to meet SL3 requirements in the future. This is now a point of differentiation for Schneider Electric,” said Lloyd.

In addition to the integration of YubiKeys within its SCADA systems used by clients in critical infrastructure, Schneider Electric has taken steps to ensure the quality and integrity of its supply chain by leveraging the YubiHSM hardware security module to integrate with key suppliers in the manufacturing process. The high-security cryptographic hardware security of YubiHSM helps support the rigorous testing and manufacturing processes of all genuine Schneider Electric products.

> “To proactively protect our supply chain, we work closely with key vendors to create dual encryption as both the vendor and Schneider Electric have YubiHSM modules built into the manufacturing process.
>
> –Chad Lloyd, Director of Cybersecurity Architecture for Energy Management, Schneider Electric

Yubico offers simple procurement & distribution

of strong security at scale

Yubico also offers YubiEnterprise Services to help organizations simplify procurement and distribution of YubiKeys for employees at scale across multiple production facilities or across the supply chain.

YubiEnterprise Subscription

YubiEnterprise Delivery

With YubiEnterprise Subscription, organizations with 500 users or more can greatly simplify the acquisition and roll out of phishing-resistant authentication. Organizations can move authentication spend from CAPEX to a predictable OPEX model, and ensure security is always covered as business needs evolve, and experience benefits such as the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to deployment services, priority support and a dedicated Customer Success Manager.

Subscription customers are automatically entitled to access the Console, a web-based interface that helps organizations easily view orders, shipments, inventory status and a wide range of other information that helps with enterprise planning, and are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

Additionally, new YubiEnterprise offerings and additional enterprise capabilities will be designed explicitly for Subscription customers.

YubiHSM 2 provides an accessible solution to strong, phishing-resistant security for a variety of manufacturing and supply chain customers all across the globe

YubiHSM 2 Procurement

YubiHSM 2 is one of the smallest and most affordable HSMs on the market, ideally suited across a wide-range of use cases and all types of organizations and industries, making it simple and quick to purchase, procure, and deploy. With its small footprint, YubiHSM 2 provides an accessible solution to strong, phishing-resistant security for a variety of manufacturing and supply chain customers all across the globe.

Takeaway

The cyber attacks of the recent past have underscored the need to secure the supply chain against disruption. As a result, leading organizations are deploying passwordless authentication and ultra-small HSM to protect against modern cyber threats. These solutions need to be both user-friendly and cost-effective at scale, to make them a realistic option for downstream supply chain partners.

Being proactive and securing your data and products with the right security solution can help you mitigate attacks, minimize attack penetration rates, protect corporate secrets, and provide greater transparency and control over the integrity of inputs into the manufacturing process or software being used.

The YubiKey and YubiHSM 2 are secure, portable, easy-to-use solutions designed to meet organizations where they are, helping to seamlessly support legacy infrastructure as well as modern, cloud-based systems.

Sources

[1] Susan Moore, 7 Top Trends in Cybersecurity for 2022, (April 13, 2022)

[2] BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021, (Accessed February 2, 2021)

[3] CyberArk, The CyberArk 2022 Identity Security Threat Landscape Report, (April 12, 2022)

[4] NIST, Best Practices in Cyber Supply Chain Risk Management, (Accessed April 18, 2022)

[5] NIST, NIST SP 800-161 Rev. 1 (2nd Draft), (Accessed April 18, 2022)

[6] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)

[7] Shalanda D. Young, M-22-09, (January 26, 2022)

[8] Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, (May 19, 2021)

[9] Stephanie Kelly and Jessica Resnick-ault, One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators, (June 8, 2021)

[10] DHS, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021); DHS, Ratification of Security Directive, (September 24, 2021)

[11] Reuters, Hackers Hold Hula Hoops Hostage in cyber-raid on Britain's KP Snacks, (February 3, 2022)

[12] NIST, NIST SP 800-161 Rev. 1 (2nd Draft), (Accessed April 18, 2022)

[13] Jonny Evans, Apple: It's time to bolster supply chain security, (August 26, 2021)

[14] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)l

[15] LastPass, New Forrester Report: The Real Cost of Password Risks, (May 18, 2018)

[16] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[17] SEC, Form 8-K SolarWinds Corporation, (December 14, 2020)

[18] SEC, Form 8-K Solarwinds Corporation, (December 17, 2020)

[19] Charlie Osborne, Updated Kaseya ransomware attack FAQ: What we know now, (July 23, 2021)

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.