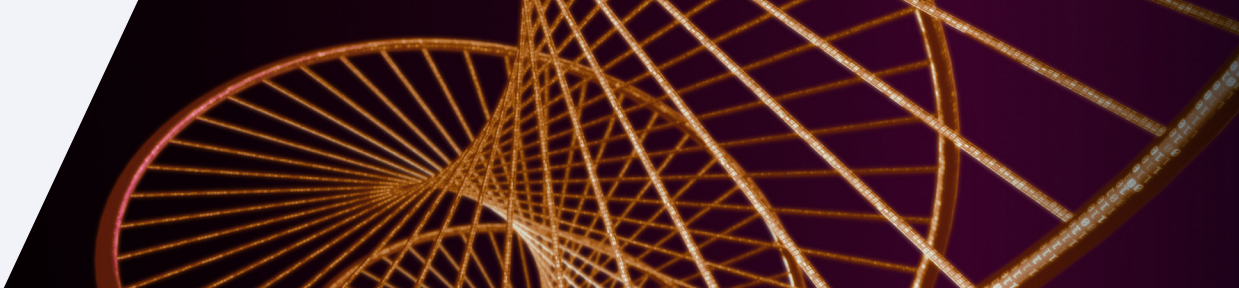
Venafi



SOLUTION BRIEF

Protecting Non-Person Entities in Defense and Intelligence Networks

Machine identity management secures NPE configurations and prevents unauthorized access

Who should read this: Information security teams working for the Department of Defense and intelligence agencies with responsibility for defining proper usage of certificates, PKI and machine-to-machine authentication, as well as the operations teams who maintain critical websites, applications and online services.

Non-person entities (NPEs) are defined as objects that requires a digital identity in cyberspace and are not people. As part of this broad definition, machine-based NPEs on defense and intelligence networks—meaning NPEs such as devices, applications, code and containers—continue to grow exponentially. This growth is exacerbated by ever-expanding infrastructures, with many government environments now blending on-premises, mobile, IoT, virtual and cloud components. With the sheer scale of machine adoption, government information security and operations teams are struggling with NPE security and availability. They face risks ranging from service outages to ineffective network security controls to breaches caused by adversaries. Defense and intelligence agencies, in particular, need to keep machine connections and communications secure in hostile environments while maintaining NPE scalability.

Management Challenges for Machine-Based NPEs

With the growth of NPEs, defense and intelligence agencies are increasingly relying on automated machine-to-machine connections. It is forecast that by 2023 there will be nearly 30 billion connected devices globally.[1] Defense and intelligence agencies need to authenticate the identities of these machine-based NPEs to ensure machine-to-machine communications are secure. Similar to usernames and passwords for people, automated machine-to-machine connections rely on SSL/TLS keys and certificates; SSH keys; and endpoint, user and code signing certificates to authenticate communications—and all of these machine identity types must be managed and secured.

The private sector spends over $10 billion each year on identity and access management.[2] Nearly all of this is spent on protecting usernames and passwords, with little spent towards protecting machine identities. Similarly, defense and intelligence agencies focus on securing Common Access Cards (CACs) with their own certificate management challenges but have historically paid little attention to protecting the NPEs engaged in critical machine-to-machine communications. The security gap around NPE identity and authentication opens the door to the wide range of threats—from outages to breaches—and increases risks to availability, integrity and security. Private-sector industry analysts have created a term for this growing challenge: Machine Identity Management.[3]

Mandates and Directives

In recent years, additional mandates and directives have been established to ensure protection of NPE authentication and access. A few of the more recent mandates include the following:

- **In 2018, the Department of Defense recognized increasing SSL-based threats** and required these actions: Move all DoD sites to HTTPS; use publicly-trusted SSL certificates instead of ones issued by the DoD's own certificate authority; and implement HTTP Strict Transport Security (HSTS) to better secure these systems.[4] (See http://www.documentcloud.org/documents/4620886-Wyden-Letter-DOD-Response.html.)
- **United States Department of Defense X.509 Certificate Policy version 10.6**, published on 20 May 2018 provides explicit guidance on how to secure SSL/TLS certificates used in "workstations, guards, firewalls, routers, in-line network encryptors (INE), and trusted database servers." It defines specific procedures for issuance, renewal and revocation, as well as configuration guidance and requirements for logging, key usage and common actions.[5] (See https://dl.dod.cyber.mil/wp-content/uploads/pki-pke/pdf/unclass-dod_cp_v10-6_20180520.pdf.)
- **Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security Emergency Directive 19-01, Mitigate DNS Infrastructure Tampering, Action Four**, highlights the need to review certificates related to every agency's domains against Certificate Transparency log data and report unauthorized certificates to CISA.[6] (See https://cyber.dhs.gov/ed/19-01/.)
- **National Cybersecurity Center of Excellence (NCCoE) established a project to demonstrate effective Transport Layer Security (TLS) server certificate management**, including a draft of the National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide Special Publication 1800-16, Securing Web Transactions: Transport Layer Security (TLS) Server Certificate Management.[7] (See https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management.)

- **Office of Management and Budget (OMB) Memorandum M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM)**, outlines the need to adopt authentication and access controls, stating, "as technology evolves, the Government must offer flexible solutions to meet changing technology needs and shift the focus from managing the lifecycle of credentials to the lifecycle of identities."[8] (See https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf.)

In addition, some Security Technical Implementation Guides (STIGs), such as the Application Security and Development STIG, have tried to protect the DoD in the face of this explosive growth in sites and services by calling for stringent oversight on the kind of SSL/TLS certificates and certificate authorities that can be used in DoD sites. For example, finding V-70219 states, "The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions,"[9] but references no tool or system to ensure compliance with this requirement. PKI engineers in the DoD need an automated approach to support the thousands of certificates from dozens of certificate authorities in DoD network environments.

Protecting NPE SSH Keys

While these mandates and directives primarily apply to SSL/TLS certificates, SSH keys also serve as machine identities and must be protected to prevent unauthorized privileged access to NPEs. SSH hosts, clients and key pairs are proliferating through government agency networks, and, like SSL/TLS certificate use, SSH use requires continuous monitoring, policy oversight and active control.

NIST provides guidance on securing SSH in the publication, **NISTIR 7966, Security of Interactive and Automated Access Management Using Secure Shell (SSH)**.[10] (See https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf)

With as many as 5,000 websites managed by the Department of Defense alone,[11] and domains supporting numerous websites and services, these mandates have far-reaching impacts. Defense and intelligence agencies are increasing their reliance on encryption and embracing strategies for Encryption Everywhere, IT Modernization and Cloud Migration. But the ever-changing and expanding government mandates that protect these initiatives and require policies for SSL/TLS certificate issuance, installation and management have made the use of traditional manual, government off-the-shelf (GOTS) and siloed certificate management approaches untenable. Defense and intelligence agencies need another solution to protect machine identities.

Gain Visibility, Intelligence and Automation into Machine-Based NPEs

To eliminate these challenges across far-reaching, pervasive government networks, defense and intelligence agencies need visibility, intelligence and automation for their machine identities.

- **Visibility:** Machine identities include SSL/TLS keys and certificates, SSH keys, and mobile, user and code signing certificates. Effective machine identity management for NPEs must start with global visibility into all of these machine identities across the extended agency infrastructure, including those on both internal and external infrastructures, the Internet and virtual, cloud and IoT infrastructures.

  Comprehensive visibility must be based on agencywide discovery of machine identities, providing a complete and accurate inventory. This discovery should include the configuration, location and use of all keys and certificates. Visibility into issuance, installation, policies and risk analytics are needed to make key and certificate lifecycle management intelligent, efficient, secure and easy with dashboards, reports, notifications and escalations delivering this visibility where it's needed.

- **Intelligence:** Real-time visibility into keys and certificates that serve as machine identities is only part of the solution. The DoD and intelligence agencies also need to enforce policies based on security and operational parameters, granular access controls and certificate expiration monitoring.

  When detailed machine identity intelligence is gathered, it enables organizations to apply management and security policies to avoid outages and identify security blind spots. The intelligence should be gathered through continuous monitoring and include use, location, ownership, pending expirations, key lengths, signing algorithms, protocols, ciphers and other attributes. For certificates, agencies should also apply policy-enforced enrollment that allows the use of any policy-approved CA, a self-service portal and standard protocol (e.g., ACME SCEP) or REST API.

  As machine identities, SSH keys have unique policy enforcement requirements. Because SSH keys do not expire, they need to have policy-enforced rotation as well as real-time intelligence on which connections allow root access, which keys are susceptible to port forwarding or pivoting, and which are backed by weak or misconfigured keys. These are just a few examples.

  NPEs are pervasive within all branches of defense and the need to protect NPE digital identities applies to all of them, as well as intelligence agency networks. Machine identity intelligence for NPEs must be integrated throughout network ecosystems. For example, for certificates and keys alike, changes in security posture can be fed into SIEM and analytics solutions, alerting response teams to attacks underway or to unexpected vulnerabilities.

- **Automation:** Intelligence must then be applied to fast and coordinated actions driven by a set of agency policies and controls. With intelligence-driven automation, actions quickly remediate machine identity weaknesses. The result is improved cybersecurity, reduced risk and support for regulatory, legal and operational requirements.

  Every step in the identity lifecycle for machine-based NPEs should be automated. Automation eliminates human error, renews expiring certificates to prevent outages and safeguards agencies against exploits and data loss by automatically discovering machine identity weaknesses and applying defined security policies to remediate them. With automation, agencies can sustain crypto-agility, validate compliance and scale NPEs and encryption safely.

Venafi Secures Machine Identities for Defense and Intelligence Agencies

Venafi has the capabilities to address requirements for even the most secure government agencies and national security systems:

- The Venafi Platform is the only NIAP Common Criteria certified solution that delivers comprehensive orchestration and management of NPE machine identities across the most complex government environments. (See https://www.niap-ccevs.org/MMO/Product/st_vid10800-agd.pdf)
- The Venafi Platform runs on Microsoft Windows Server in FIPS mode and uses Microsoft FIPS-certified libraries for cryptography operations.
- The Venafi Advanced Key Protect option integrates with one or more FIPS 140-2 Level 2 configured hardware security modules (HSMs) to maximize the security of the assets it manages. Advanced Key Protect stores and secures the symmetric keys used for encrypting private keys and other sensitive information in the platform's database.
- The Venafi Platform is the only approved NPE solution for CDM BOUND-E capabilities that meets each category of the DHS required guidelines around collecting and reporting information.
- In addition to these capabilities, the Venafi Platform supports the DoD need for rapidly deployable systems, providing fast protection and management of machine identities that have been newly introduced into war zones and areas of conflict.

Venafi Protects Machine Identities

The Venafi Platform helps defense and intelligence agencies manage and secure the cryptographic keys and digital certificates that make up machine identities. Using the Venafi Platform, agencies can efficiently orchestrate the entire machine identity lifecycle for NPEs, keeping communications between machines secure and private. It also ensures that certificates are up to date, have been issued by authorized sources and have not expired—preventing outages and critical security risks.

The Venafi Platform discovers machine identities of all types, delivers insight and intelligence about these entities, and drives automated actions that securely scale encryption, remove error-prone manual installation and remediate vulnerabilities and weaknesses. The platform also conducts rapid bulk replacement of keys and certificates, in response to sudden security events or changes in the threat landscape that can immediately impact machine-based NPEs.

Through policy-enforced automated installation of the keys and certificates, Venafi enables agencies to build and maintain sustainable and scalable protection plans for machine identities. Built to withstand the rigors of even the most classified networks, the Venafi Platform provides the visibility, intelligence and automation that will help comply with mandates that pertain to protecting machine identities at machine speeds and never-before-experienced scale.

Learn how Venafi solutions can help your agency secure machine-to-machine communications by protecting machine identities across every layer of your IT environment: **venafi.com**

References:

1. Ericsson. Ericsson Mobility Report. November 2017.
2. Grand View Research. Identity and Access Management (IAM) Market Size, Share & Trends Analysis Report by Component, By Deployment (Cloud, Hybrid, On-Premise), By End Use, By Region, and Segment Forecasts, 2019 – 2025. June 2019. Report ID: 978-1-68038-564-9.
3. Ant Allan et al. Hype Cycle for Identity and Access Management Technologies, 2020. Gartner. July 16, 2020. 22.
4. Wyden, Senator Ron. Department of Defense. Letter. May 22, 2018.
5. United States Department of Defense X.509 Certificate Policy version 10.6, published on May 20, 2018.
6. Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security. Emergency Directive 19-01. Mitigate DNS Infrastructure Tampering. January 22, 2019.
7. NIST Special Publication 1800-16. Securing Web Transactions: TLS Server Certificate Management. Draft: July 2019.
8. Office of Management and Budget (OMB). Memorandum M-19-17. Enabling Mission Delivery through Improved Identity, Credential, and Access Management (ICAM). May 21, 2019.
9. United States Department of Defense. Application Security and Development Security Technical Implementation Guide, Version 4, finding V-70219. December 24, 2018.
10. NIST. NISTIR 7966. Security of Interactive and Automated Access Management Using Secure Shell (SSH). October 2015.
11. Garland, Chad. Stars and Stripes. Want to Know How Many Websites the Pentagon Runs? So Does the Pentagon. May 8, 2019.
12. Acumen Security, LLC. Venafi Trust Protection Platform 17.1 Common Criteria Guidance. July 22, 2017.

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**