Trusted Cyber Technologies

THALES
Building a future we can all trust

Meeting U.S. Government requirements for phishing-resistant MFA

White Paper

Contents

Introduction: Toward phishing-resistant multifactor authentication

The acceleration of digital transformation for U.S. industries, including those in critical infrastructure, and the adoption of a hybrid workforce, have exposed essential systems and sensitive data to increased cyber threats and risks. Cybersecurity incidents such as SolarWinds, Microsoft Exchange, and the Colonial Pipeline incident serve as a sobering reminder that U.S. public and private sectors increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals.

There are multiple ways this malicious activity impacts organizations – disruption of essential services, malfunction of critical systems, and increased cost for remediation and restore. The IBM 2021 Cost of Data Breach report indicated that there was a 10% increase in the average total cost of a breach compared to 2020, reaching $4.24 million. 38% of these costs were associated with lost business, including lost revenue due to system downtime, and the increasing cost of acquiring new business due to diminished reputation.

Looking at the vectors used by criminals to launch their malicious activities and either extort data or disrupt business processes, the Verizon 2021 Data Breach Investigations Report indicates that 61% of the breaches involved compromised or stolen credentials. To combat this trend, organizations are investing in strengthening their access controls, moving toward a zero trust cybersecurity model, and leveraging the power of multifactor authentication (MFA).

CISA states that "MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised.[1]"

Understanding the Federal Zero Trust Strategy

In May 2021, President Biden signed Executive Order 14028 on Improving the Nation's Cybersecurity[2]. One of the goals of the Executive Order is to "modernize and implement stronger cybersecurity standards in the Federal Government." According to the Executive Order, the Federal Government and private companies doing business with the Government must move to secure cloud services and a zero trust architecture, mandating the deployment of multifactor authentication and encryption within a specific time period.

In support of the Presidential Executive Order, the Office of Management and Budget released the Federal Zero Trust Strategy – OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"[3].

The strategy is based on the Department of Defense Zero Trust Reference Architecture[4], which states:

[1] CISA Alert (AA22-074A), https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[3] https://zerotrust.cyber.gov/federal-zero-trust-strategy/#overview or download as PDF from https://zerotrust.cyber.gov/downloads/M-22-09%20Federal%20Zero%20Trust%20Strategy.pdf

[4] https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

"The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction."

The Zero Trust Strategy is based on five pillars:

1. "Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while **remaining reliably protected from even targeted, sophisticated phishing attacks.**"
2. "The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources."
3. "Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted."
4. "Enterprise applications are tested internally and externally and can be made available to staff securely over the internet."
5. "Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information."

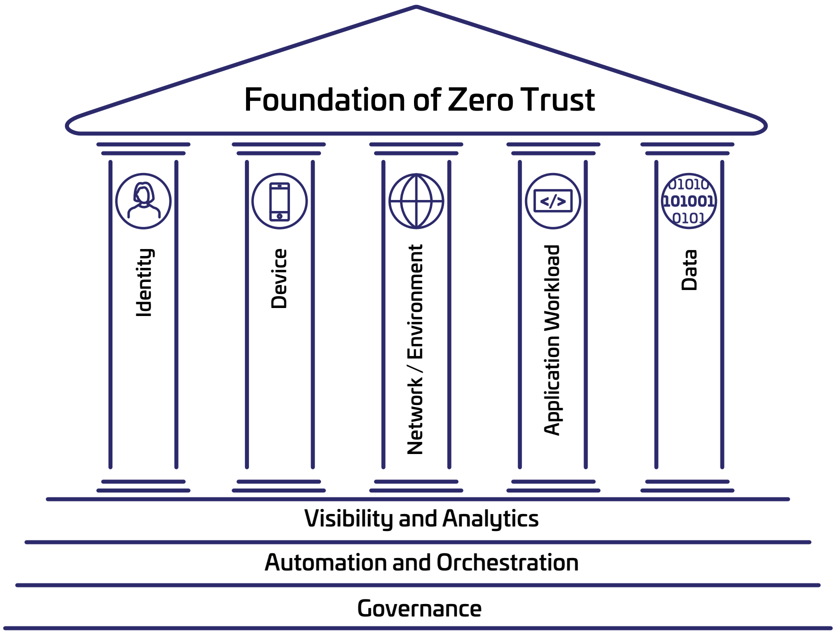

Figure 1: Zero Trust Pillars. Image courtesy of CISA.

The strategy places significant emphasis on stronger enterprise identity and access controls, including multi-factor authentication (MFA). Without secure, enterprise-managed identity systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks. The strategy prioritizes defense against sophisticated phishing and directs agencies to consolidate identity systems so that protections and monitoring can be consistently applied.

While the scope of the Executive Order and the OMB Memorandum M-22-09 is a blueprint for Zero Trust security for the Federal Government, many of the key tenets included in these guidelines will likely be adopted in other sectors as well including the broader public sector, critical infrastructure, critical manufacturing, oil and gas suppliers and other key industries such as pharma, food industries and agriculture.

Requirements for a central, modern, and risk-based authentication system

The Government's vision for a Zero Trust identity-based cybersecurity is summarized in the following abstract:

"Agency staff use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks."

The core IAM functionalities required by federal agencies and other organizations to implement this vision are listed below and shown in Figure 2:

1. Enterprise-wide identity systems
2. Multifactor authentication
3. User authorization

Enterprise-wide identity systems

"Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms," states the strategy, adding that agencies "should ensure that information is accessed by the right users, at the right time, and for the right purposes."

Tightening access controls will require agencies to leverage data from different sources to make intelligent decisions, such as analyzing device and user information to assess the security posture of all activity on agency systems. This metadata about the user will permit agencies to make risk-based decisions at the policy enforcement point.

In addition, the strategy requires that the enterprise identity management system integrates into as many agency applications as possible. Beyond compatibility with common applications, an agency identity management program should facilitate integration among agencies and with externally operated cloud services; the use of modern, open standards often promotes such integration.

Multifactor authentication

Multifactor authentication plays a critical part of the Government's strategy. "Agencies must integrate and enforce MFA across applications involving authenticated access to Federal systems by agency staff, contractors, and partners," states the publication. To achieve this goal, "MFA should be integrated at the application layer."

Although MFA generally protects against common methods of gaining unauthorized account access, not all multi-factor authentication methods can protect against sophisticated phishing attacks. For this reason, the strategy requires the use of phishing-resistant approaches to MFA in most cases:

- For agency staff, contractors, and partners, phishing-resistant MFA is required. Options include PIV (including Derived PIV[5]), FIDO2 and Web Authentication-based authenticators as well as PKI certificate-based smart cards.
- For public users, phishing-resistant MFA must be an option and can be provided in addition to other types of authentication.

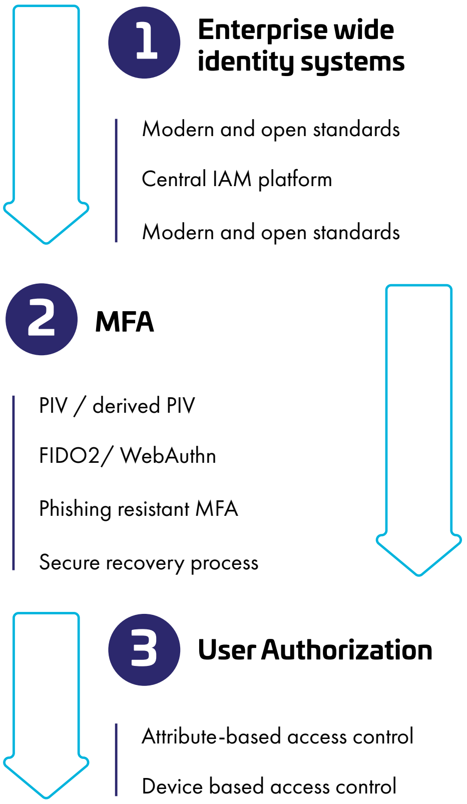
1
Enterprise wide identity systems
Modern and open standards
Central IAM platform
Modern and open standards
2
MFA
PIV / derived PIV
FIDO2/ WebAuthn
Phishing resistant MFA
Secure recovery process
3
User Authorization
Attribute-based access control
Device based access control

Figure 2: Core IAM Functionalities for Implementing Zero Trust Security

User Authorization

In addition to authentication, agencies should ensure their tools can execute certain protocols for authorization.

Currently, the federal systems focus on role-based access control (RBAC), which relies on static pre-defined roles that are assigned to users and determine their permissions within an organization. However, a zero trust architecture should incorporate more granularly and dynamically defined permissions, as attribute-based access control (ABAC) is designed to do.

NIST defines ABAC as "An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions.[6]"

Authorization systems should incorporate at least one device-level signal alongside identity information about the authenticated user when regulating access to enterprise resources.

[5] NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials, https://csrc.nist.gov/publications/detail/sp/800-157/final

[6] https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf

Which OTP methods are being deprecated?

As cited in NIST's MFA Update from February 2022[7], "All MFA processes using shared secrets are vulnerable to phishing attacks."

This includes authentication methods that rely on memorized secrets, look-up secrets, out-of-band authentication (SMS/PSTN) including push notification, and one-time-passwords (OTP). Specifically:

> **" All MFA processes using shared secrets are vulnerable to phishing attacks."**

SMS-based OTP

SMS authentication is considered insecure, as cited by NIST's SP 800-63 publication[8], which specifies that SMS-based authentication is "a restricted" one, meaning that it is less reliable in today's threat environment.

Authentication using Public Switched Telephone Networks

Use of public phone networks is considered insecure due to the risk of device infection or SIM swapping, code interception, authentication spamming and other risks associated with social engineering.

Knowledge-based Authentication

NIST does not recognize knowledge-based authentication (KBA), also known as "security questions", as outlined in SP 800-63.

Push OTP

While NIST considers PUSH OTP to be a better MFA method than SMS/PSTN authentication, it is not considered to be phishing-resistant.

Alternative OTP methods

There is recognition that phishing resistant MFA methods may not be suitable for all contexts and circumstances. Therefore, NIST recommends that in addition to providing phishing resistant MFA when needed, organizations should offer users at least one alternate authenticator that is not restricted and that is appropriate to the level of assurance for the selected app or service.

To this end, PUSH OTP although not phishing-resistant, could be offered as a complementary MFA method for some services, depending on the user, the context and the sensitivity of the data.

In addition, when implementing PUSH OTP, or phone-based authenticator apps, there are ways to harden security by:

- Combining PUSH OTP with conditional and contextual authentication. If a login context is considered to be high risk, the user could be required to provide additional methods of authentication.
- Combining PUSH OTP with device-native biometrics can demonstrate that an individual intended to authenticate with a specific device.
- Ensuring the integrity of the authentication through risk monitoring, end-point security and anomaly detection.

[7] https://csrc.nist.gov/csrc/media/Presentations/2022/multi-factor-authentication-and-sp-800-63-digital/images-media/Federal_Cybersecurity_and_Privacy_Forum_15Feb2022_NIST_Update_Multi-Factor_Authentication_and_SP800-63_Digital_Identity_%20Guidelines.pdf

[8] https://pages.nist.gov/800-63-3/

Achieving Phishing-resistant MFA with Thales IAM Solutions

By end of 2024 all US Federal Agencies must comply both with U.S. Executive Order 14028 and the OMB supporting strategy for Zero Trust cybersecurity. It is likely that the spirit of these recommendations and NIST guidelines for authentication will also trickle down to non-federal agencies as well, and particularly to state agencies, public sector departments, privately owned utilities, manufacturers and enterprises that do business with the US government.

Thales provides an end-to-end access management and authentication platform that meets all the Identity Pillar requirements of the US Zero Trust Strategy.

With the Thales OneWelcome Identity Platform, organizations and agencies get a centralized risk-based access platform which supports a broad range of strong MFA and risk-based authentication to protect all services, apps and environments whether hosted, on-premises or in the cloud.

OneWelcome Identity Platform is an enterprise-wide identity system that supports a broad range of authentication methods, including:

- PIV cards
- FIDO2 devices
- Virtual PKI smart card
- PKI smart cards and USB authenticators
- Two factor Push OTP in combination with biometric, contextual and risk based authentication
- Two factor OTP hardware authenticators
- Contextual / adaptive authentication
- Risk-based authentication

Thales provides a large portfolio of phishing-resistant authentication methods required by EO 1408:

- IDPrimePIV cards
- FIDO devices are compatible with any IDP supporting FIDO2

Thales IAM solutions are ideally suited to meet EO zero trust identity requirements.

OneWelcome Identity Platform Meets Zero Trust Identity Protection requirements

1 Enterprise wide identity systems

Modern and open standards

Central IAM platform

Modern and open standards

2 MFA

PIV / derived PIV

FIDO2/ WebAuthn

Phishing resistant MFA

Secure recovery process

3 User Authorization

Attribute-based access control

Device based access control

OneWelcome acts as a single identity provider for both enterprise IT and OT/ICS domains.

EO 14028 Requirement	Thales Solution	Thales Benefits
Enterprise-wide identity system	**OneWelcome Identity Platform**	
Central IAM solution	Integrated access management and authentication platform	Enables central unified management of authentication and access controls for all users. Offers standalone IDP or integrates seamlessly with existing IDPs.
Modern and open Standards	Supports RADIUS, OIDC, SAML, rest APIs, Agents, Access Gateway	Integrates with standard, non-standard, legacy and cloud services wherever they reside
Risk-based authentication	Risk scoring and policy configuration	Enables policy enforcement and risk scoring for groups, users and groups of applications
Multi-factor Authentication	**Thales Authenticators**	
Phishing-resistant MFA	PIV cards FIDO2 / WebAuthn security keys Certificate-based smart cards and USB tokens	Offering the broadest range of authentication methods and form factors, Thales allows customers to address numerous use cases, including authentication, physical access, digital signature, and encryption. Thales offers combined PKI and FIDO authentication in a single device enabling organizations to transition to FIDO or maintain both methods as needed.
Alternative MFA options	PUSH OTP OTP authenticator apps OTP hardware authenticators Pattern-based authentication	NIST recommends that in addition to providing phishing resistant MFA to meet required assurance levels, organizations should offer users at least one alternate authenticator that is not restricted and that is appropriate to the level of assurance for the selected app or service. Thales provides both phishing resistant and alternative methods of authentication, allowing organizations to deploy the appropriate authentication method to their users. OneWelcome centrally manages multiple authentication methods per user so users can be assigned several authentication methods as needed, without incurring administrative overheads or unnecessary IAM silos.

EO 14028 Requirement	Thales Solution	Thales Benefits
Enterprise-wide identity system	**OneWelcome Identity Platform**	
Passwordless authentication	PIV cards FIDO2 / WebAuthn security keys Certificate-based smart cards and USB tokens PUSH OTP OTP authenticator apps OTP hardware authenticators Pattern-based authentication	All authentication methods can be configured to be passwordless using access policies in OneWelcome
Authorization	**OneWelcome Identity Platform**	
Attribute-based access controls	Broad range of supported attributes.	Allows for optimized security and convenience by combining conditional access policies with ABAC and MFA.
Device-based access controls		Offers device risk monitoring, and device attributes for conditional access and maintaining authentication integrity.

Conclusion

The US Executive Order and EO14028 clearly reflect the growing emphasis on access security and multi-factor authentication as foundational to reducing the threat of data breaches and malicious access to sensitive resources.

The guidelines calling for organizations to achieve zero trust security by deploying a centralized identity platform, phishing resistant as well as alternative authentication mechanisms and attribute based access, point toward solutions such as Thales OneWelcome Identity Platform, which offers integrated access management, and a broad range of multi-factor, adaptive and contextual identity validation methods.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirementsFor more information, visit www.thalestct.com

THALES

Building a future we can all trust

Contact us

Please visit www.thalestct.com/contact-us

> thalestct.com<