DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

APR 14 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Approval of Multi-Factor Authentication Alternatives – Rivest Shamir and Adleman and YubiKey

Reference: (a) DoD Chief Information Officer and Commander, United States Cyber Command Memorandum, "Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication," July 5, 2015

(b) USCYBERCOM TASKORD 15-0102, "Implementation and Reporting of DoD Public Key Infrastructure (PKI) System Administrator and Privileged User Authentication," July 2015

References (a) and (b) directed DoD Components to require privileged users to authenticate to their privileged user accounts with "DoD PKI credentials on smart cards." The references also stated: "If certain information technologies….do not support DoD PKI authentication for privileged users, the use of alternate two factor authentication technologies is authorized." The DoD Chief Information Officer (CIO) formed the Privileged User Working Group (PUWG) to evaluate alternate multi-factor authentication (MFA) technologies to be used in situations where DoD-approved PKI is infeasible.

This memorandum certifies the Rivest Shamir and Adleman (RSA) SecurID authenticator and the Yubico YubiKey Universal Two Factor (U2F) authenticator as DoD-approved alternative MFA under References (a) and (b). RSA and YubiKey are interim capabilities not intended as broad replacements for DoD PKI. They provide greater assurance than user name and passwords, but less assurance than DoD PKI. RSA and YubiKey tokens have been evaluated by the PUWG and the Defense Information Assurance Security Accreditation Working Group, and may be used to authenticate to non-privileged user accounts as well.

The Attachment to this memorandum specifies the circumstances under which RSA and YubiKey may be used, and delineates DoD implementation requirements for the two technologies. Additional implementation instructions and requirements will be provided in forthcoming guidance from the Defense Information Systems Agency.

My point of contact is Mr. Andy Seymour, charles.a.seymour.civ@mail.mil, (571) 372-6990.

Marianne Bailey for

Essye B. Miller
Deputy Chief Information Officer
for Cybersecurity and DoD Senior
Information Security Officer

Attachment:
As stated

Distribution:
Secretaries of the Military Departments
Chairman of the Joint Chief of Staff
Under Secretaries of Defense
Deputy Chief Management Officer
Chiefs of Military Services
Chief of the National Guard Bureau
Commandant of the United States Coast Guard
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Director, Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director, Operational Test and Evaluation
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director, Administration and Management
Director of Net Assessment
Directors of the Defense Agencies
Directors of the DoD Field Activities

ATTACHMENT

Rivest Shamir and Adleman (RSA) and YubiKey Implementation Guidelines

1) DoD System (and application) Owners (SOs), in consultation with their Component/Executive Agent Public Key Infrastructures (PKI) offices and/or the DoD PKI/PK-Enabling (PKE) Offices at the Defense Information Systems Agency (DISA), shall demonstrate to their Authorizing Officials (AOs) that either:

    a. PK-Enabling the system or application in question is technically-infeasible (i.e. the system or application does not support direct authentication with PKI credentials). For implementation guidance on PKI-Enabling, please see the DISA Information Assurance Support Environment PKI page at: http://iase.disa.mil/pki-pke/Pages/index.aspx.

    b. A portion of the system or application's subscribers are unable to obtain DoD-approved PKIs, despite making a good-faith effort to do so.
        i. A "good-faith effort" means the SO or AO determined users in questions did not qualify for any of the DoD-approved PKIs meeting the standard for E-authentication (E-Auth) Level of Assurance (LOA)-4 in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2.
        ii. DoD-approved E-Auth LOA-4 PKIs are paid for by the subscriber's organization, and include: Common Access Cards, Personal Identity Verification (PIV) Authenticators, Alternate Logon Tokens, Personal Identity Verification-Interoperable (PIV-Is), External Certifications Authority (ECA) Medium Token and Medium Hardware Assurance Authenticators, and others.
        iii. More information on DoD-approved PKIs can be found on the DISA Information Assurance Support Environment (IASE) PKI Interoperability webpage (http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx) and the DISA IASE ECA webpage (http://iase.disa.mil/pki/eca/Pages/index.aspx).

2) The system's AO shall approve the use of the RSA or YubiKey Technology for authentication to the system. The system's AO should re-evaluate its authorization of RSA or YubiKey Tokens on an annual basis. The system's AO should also ensure there is a Plan of Action and Milestones for requiring direct PKI authentication when the reasons for not implementing PKI no longer apply.

3) The system's AO shall assess the system for vulnerabilities and residual risk associated with accepting authentication with RSA or YubiKey Technology instead of requiring DoD-approved PKI. This risk assessment should include the: sensitivity of the information on the system (see p. 13-14 of DoD Instruction 8520.03 at http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf), likelihood of a system compromise, impact of a system compromise, the risk mitigations being put in place, and the residual risk after the mitigations are implemented.

4) The system's AO shall ensure users have met the requirements for Identity Assurance Level (IAL) 2 in the draft National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63A

(https://pages.nist.gov/800-63-3/sp800-63a.html) before obtaining an RSA or YubiKey Token. Remote or antecedent identity-proofing should not be used, even if it meets IAL-2.

   a. If possible, the AO shall ensure privileged users have met the requirements for IAL-3.

5) The system's AO shall coordinate with the Component/Executive Agent's PKI Office to ensure RSA or YubiKey implementation meets the requirements for Authenticator Assurance Level 2 in the draft NIST SP 800-63B (https://pages.nist.gov/800-63-3/sp800-63b.html).

6) The system's AO shall ensure the SO has written procedures in place and/or configured their system to disable RSA and YubiKey user accounts if the token or user account is inactive for sixty days or more, and to dis-enroll the RSA or YubiKey Authenticator if it's reported as lost or stolen.