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

CHIEF INFORMATION OFFICER

OCT 05 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Approval of Multi-Factor Authentication Alternatives – Gemalto SafeNet eToken PASS Model 3000

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 [i.e. multi] 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 Gemalto SafeNet eToken PASS Model 3000 as a DoD-approved technology that may be used on the Non-classified Internet Protocol Router Network (NIPRNet) as part of an alternate MFA solution under References (a) and (b). The eToken PASS Model 3000 is a one-time password capability that can be used in combination with another factor (e.g. a PIN) to facilitate user-authentication. While it provides greater assurance than a user name and password, it provides less assurance than DoD-approved PKI, and is not intended as a broad replacement for DoD-approved PKI. The eToken PASS Model 3000 was evaluated by the PUWG, and may be used to authenticate to both privileged and non-privileged user accounts.

The Attachment to this memorandum specifies the circumstances under which the eToken PASS Model 3000 may be used, and delineates DoD implementation requirements for the technology. Additional implementation instructions and requirements may be provided in the future by the DoD CIO and/or the Defense Information Systems Agency.

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

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

Gemalto SafeNet eToken PASS Model 3000 Implementation Guidelines for the NIPRNet

BACKGROUND

The Gemalto SafeNet eToken PASS Model 3000 is a one-time password (OTP) capability that can be used in combination with another factor (e.g. PIN, password, biometric) to facilitate user-authentication to a system or application. Part 1 of these implementation guidelines apply to all DoD System Owners (SOs) and their Authorizing Officials (AOs) that seek to accept user-authentication to their system with the Gemalto SafeNet eToken PASS Model 3000. Part 2 of these guidelines apply to DoD entities, administrators, and/or AOs sponsoring the issuance of the eToken PASS to DoD users.

PART 1: GUIDELINES FOR SYSTEM OWNERS

1) Before accepting the Gemalto SafeNet eToken PASS Model 3000 for authentication to their system, DoD Non-classified Internet Protocol Router Network (NIPRNet) System Owners (SO), in consultation with their Component/Executive Agent Public Key Infrastructures (PKI) offices and/or the DoD PK-Enabling (PKE) Office at the Defense Information Systems Agency (DISA), shall demonstrate to their system Authorizing Officials (AO) 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 PKI-Enabling guidance, please see the DISA Information Assurance Support Environment (IASE) PKI page at: http://iase.disa.mil/pki-pke/Pages/index.aspx. A Common Access Card (CAC) will be required to access some resources in the IASE site.
    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.
        ii. DoD-approved PKIs are paid for by the subscriber's organization, and are listed on the DISA IASE PKI Interoperability webpage (http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx) and ECA webpage (http://iase.disa.mil/pki/eca/Pages/index.aspx).

2) DoD SOs shall ensure, and their system AOs shall certify, that the implementation of the Gemalto SafeNet eToken PASS Model 3000 meets the requirements for Authenticator Assurance Level (AAL) 2 in NIST SP 800-63B (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf).

3) DoD SOs shall ensure, and their system AOs shall certify, that all privileged users utilizing the eToken PASS Model 3000 operate in compliance with Technical Attachment 1 to CYBERCOM TASKORDER 14-0018. The Technical Attachment delineates actions to ensure privileged user accounts remain secure, such as requiring separate, dedicated workstations and credentials for enterprise and domain administrators. The TASKORD and Technical Attachment can be found on CYBERCOM's SIPRNet website. Many of the Technical Attachments actions were taken from or built on Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs).

4) DoD SOs shall ensure, and their AOs shall certify, that there are written procedures in place and/or the system is configured to:
    a. Disable Gemalto SafeNet eToken PASS Model 3000 user accounts if the token or user account is inactive for sixty days or more.
    b. Dis-enroll an eToken PASS if it's reported as lost or stolen.
    c. Block a user's access if the user makes three successive failed attempts to authenticate to the system with the One-Time Password (OTP) code from the eToken PASS and their PIN. The user should not be made aware if it was the PIN or the OTP code that was invalid.
    d. Log and monitor the behavior of eToken PASS users at the server level, with a particular focus on administrative access and attempted command executions.

5) The system's AO shall assess the system for vulnerabilities and residual risk associated with accepting authentication with the Gemalto SafeNet eToken PASS Model 3000, as opposed to requiring authentication with DoD-approved PKI. This risk assessment should include the: sensitivity of the information being accessed (see p. 13-14 of DoD Instruction 8520.03 at http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf)), likelihood and impact of a system compromise, risk mitigations, and residual risk after mitigations are implemented.

6) The system's AO shall re-evaluate its authorization of the eToken PASS Model 3000 on an annual basis. The AO shall also ensure there is a Plan of Action and Milestones (POA&M) for replacing the eToken PASS Model 300 with DoD-approved hardware PKI when PKI implementation becomes technically feasible and/or the system's subscribers are able to obtain DoD-approved PKI.

PART 2: GUIDELINES FOR TOKEN SPONSORS

1) DoD entities sponsoring issuance of the eToken PASS shall ensure recipients meet the requirements for Identity Assurance Level (IAL) 2 in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63A (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf) before being issued the tokens. Remote or antecedent identity-proofing shall not be accepted, even if it meets IAL-2. Privileged users should meet the requirements for IAL-3.

2) DoD entities sponsoring issuance of the eToken PASS shall ensure administrators issuing the tokens verify and record the recipient's identity. If the recipient has a CAC, the issuer shall record information from the CAC, such as the Electronic Data Interchange Personal Identifier (EDIPI). Recipients shall acknowledge their responsibility for, and acceptance of, the eToken PASS by signing or digitally-signing a document to this effect, or by sending a digitally-signed e-mail to the issuer.

3) DoD entities sponsoring issuance of the eToken PASS shall monitor and maintain a list of tokens issued, require recipients to report lost, stolen, or damaged tokens, and revoke tokens as needed.