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

CHIEF INFORMATION OFFICER

OCT 05 2017

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Approval of Identity Federation Service Providers – Centrify Server Suite and Centrify Privileged Service

Reference: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63C

Identity Federation Services (IFS) serve as trusted intermediaries between users seeking to obtain data from a system, application, or device, and the system, application, or device on which the data is stored. IFS capabilities facilitate strong authentication to systems, applications, and devices which are unable to process strong authentication technology directly. Reference (a) focuses on the different ways IFS capabilities can be configured and implemented, and the impact this has on the reliability and trustworthiness of an identity authentication.

This memorandum certifies and approves the Centrify Server Suite (CSS) and Centrify Privileged Service (CPS) as DoD-approved IFS on both the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). CSS and CPS may be used to facilitate user-authentication in combination with DoD-approved Public Key Infrastructure and/or alternative Multi Factor Authentication credentials. Centrify Server Suite facilitates privileged and unprivileged user-authentication via Microsoft Active Directory to workstations and servers utilizing Linux Operating Systems. Centrify Privileged Service is a gateway that facilitates privileged-user authentication to the system or application that the privileged user administers.

The Attachment to this memorandum specifies the circumstances under which CSS and/or CPS may be used, and delineates DoD implementation guidelines for their use. Additional implementation guidelines and instructions 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

Centrify Server Suite (CSS) and Centrify Privileged Service (CPS) Implementation Guidelines for NIPRNet and SIPRNet

BACKGROUND

These implementation guidelines apply to all DoD System Owners (SOs) and their Authorizing Officials (AOs) that seek to implement the Centrify Server Suite (CSS) and/or the Centrify Privileged Service (CPS) on their enterprise or system, and still receive credit for fulfilling the DoD Cybersecurity Scorecard's PKI requirements. CSS facilitates Public Key Infrastructure (PKI) user-authentication via Microsoft Active Directory to workstations and servers utilizing Linux Operating Systems. CPS is a gateway that facilitates privileged-user authentication to the systems or application that the privileged user administers. Both CSS and CPS are considered Identity Federation Services (IFS), which serve as trusted intermediaries between users that seek to obtain data from a system, application, or device, and the system, application, or device that stores the data (i.e. the relying party).

GUIDELINES

1) Before implementing CSS or CPS, DoD System Owners (SOs), shall consult with their Component/Executive Agent PKI office and/or the DoD PK-Enabling (PKE) Office at the Defense Information Systems Agency (DISA), and demonstrate to their Authorizing Official (AOs) that the system or application in question does not support direct authentication with PKI credentials. For implementation guidance on PKI-Enabling, please see the DISA Information Assurance Support Environment (IASE) PKI page at: http://iase.disa.mil/pki-pke/Pages/index.aspx.

2) DoD SOs shall ensure, and their AOs shall certify, that all CSS and CPS users utilize only DoD-approved Multi-Factor Authentication credentials to initially authenticate to CSS or CPS. This requirement only applies to the initial authentication to CSS and CPS, and not to internal CSS/CPS operations or CSS/CPS authentication to relying parties.
    a. Unprivileged users on the NIPRNet shall authenticate with Common Access Cards (CACs) or another form of DoD-approved PKI or MFA. Unprivileged users on the SIPRNet shall authenticate with National Security System (NSS) SIPR PKI tokens.
    b. Privileged users on the NIPRNet shall authenticate to their privileged user accounts with Alternate Logon Tokens (ALTs) or another form of DoD-approved MFA. Privileged users on the SIPRNet shall authenticate to their privileged user accounts with NSS SIPR PKI tokens. Both the NIPRNet and SIPRNet Privileged users are required by DoD policy to use a different PKI token or MFA credential for authentication to their privileged account(s) than the one they use for authentication to their unprivileged accounts.
    c. DoD-approved PKIs on the NIPRNet 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).
    d. DoD-approved alternate MFAs, their implementation guidelines, and the circumstances in which they can be used are described in the DoD CIO memo, "Approval of Multi-Factor Authentication Alternatives – Rivest Shamir and Adelman and YubiKey," April 14, 2017.

3) DoD SOs shall ensure, and their AOs shall certify, that all privileged users administering CSS or CPS, and/or utilizing CSS or CPS to access privileged user accounts, 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 all web-traffic between CSS, CPS and relying parties (including legacy systems) is protected from disclosure with Transportation Layer Security (TLS) or Internet Protocol Security (IPsec). TLS and IPsec shall be implemented on the NIPRNet using algorithms recommended in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131A, and on the SIPRNet using algorithms recommended in Committee on National Security Systems Policy (CNSSP) 15.

5) DoD SOs shall ensure, and their AOs shall certify, that the implementations of CSS and/or CPS meets the requirements for Federated Assurance Level (FAL) 2 in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63C (https://pages.nist.gov/800-63-3/sp800-63c.html).

6) The system's AO shall assess the system for vulnerabilities and residual risk associated with accepting authentication via CSS or CPS, as opposed to direct user-authentication. 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.

7) The system's AO must approve the use of CSS and/or CPS. The AO should re-evaluate its authorization of CSS and CPS on an annual basis.