Implications of Persona User Name (PUN) Guidance on Common Access Card (CAC) Certificates and Email Accounts

Abstract

Forthcoming DoD-wide data guidance requires all email addresses to be updated to follow a new specification which ensures consistency. This change may impact the ability for personnel to digitally sign and encrypt emails as their new email address will not match the current email address on their Common Access Card (CAC) email certificate. Limitations to the DoD Public Key Infrastructure (PKI) preclude a large number of personnel from updating their CACs at the same time outside of their regular re-issuance schedule. Due to this limitation, this white paper provides guidance for DoD email domain administrators to implement configuration changes which ensure continued availability of email sign/encrypt functionality during the transition period.

Problem

New DoD Email Specification

Forthcoming Department of Defense (DoD) Chief Information Officer (CIO) data guidance requires all Sensitive but Unclassified Internet Protocol Router Network (NIPRNet) and Secret Internet Protocol Router Network (SIPRNet) IT System user account usernames to be Persona Usernames (PUNs), as provisioned in the Defense Enrollment Eligibility Reporting System (DEERS) by the Defense Manpower Data Center (DMDC). PUN is an individual's Enterprise Username (EUN) concatenated with their applicable Persona Type Code (PTC) extension.

This new guidance has a similar impact on all DoD NIPRNet and SIPRNet email addresses, where the username portion (the portion to the left of the @ symbol) is made up solely of the PUN. Per the new guidance, NIPRNet and SIPRNet email addresses will be of the form PUN@domain.mil.

While updating all DoD SIPRNet and NIPRNet Simple Mail Transfer Protocol (SMTP) accounts to follow the new specification will be a somewhat challenging task in the short run, the greater concern is how this change may impact user Public Key Infrastructure (PKI) email certificates. The majority of DoD users possess these certificates on their Common Access Card (CAC).

DoD Email Addresses

Within the current DoD environment, a large number of email accounts have been migrated to DoD Enterprise Email (DEE). These accounts follow the PUN specification as defined in the forthcoming data guidance. Additionally, some Combatant Commands, Services, and Agencies (CC/S/As) who are not currently utilizing DEE have already changed their user email addresses to follow the same PUN specification.

While a subset of DoD email accounts have been changed to follow the new PUN specification, many have not yet been updated. These remaining entities will need to be in compliance with this guidance.

S/MIME Security Services

Microsoft Exchange provides the capability that allows users to send and receive digitally signed and/or encrypted e-mail messages via both the Microsoft Outlook desktop application and Outlook Web Access (OWA). These Secure Multi-Purpose Internet Mail Extension (S/MIME) security services require the user to possess a valid PKI email certificate, and present that certificate at the time of service execution.

By default, S/MIME security services are enabled for a given user within the Outlook client when the primary SMTP email address matches the email address found on the PKI email certificate. This is commonly referred to as "name checking". **If these email addresses do not match, S/MIME services will not be available to the user, which negatively impacts the overall security posture of the DoD enterprise, as individuals will no longer be able to send digitally signed and encrypted email.**

CAC Update Limitations

While guiding users to update their email certificate on their CAC at the time they are issued an updated email address seems like a potential solution, technical limitations in the PKI infrastructure eliminate this option. Specifically, the Real-Time Automated Personnel Identification System (RAPIDS), which is the authoritative system used to issue DoD PKI credentials, and DoD Certificate Revocation Lists (CRLs) would encounter unprecedented transaction growth in a very short time period.

Solution

Within Microsoft Outlook, name checking suppression may be enabled to account for the mismatch of SMTP account and CAC email certificate email addresses (see "Microsoft Outlook: Configuring Name Check Suppression" guide available from http://iase.disa.mil/pki-pke under PKE A – Z > Guides). Although the suppression of name checking solves the issue in Microsoft Outlook, it is not supported by OWA. Within OWA, the use of proxy email addresses handles this issue. Use of proxy addresses in OWA is controlled through the UseSecondaryProxiesWhenFindingCertificates registry key in Exchange, which is set to 'true' by default, allowing for the use of proxy addresses. Based on the email client being used, both approaches allow any DoD user with a mismatching SMTP email address and CAC email certificate email address to utilize S/MIME security services.

The following two solutions, which account for DEE and non-DEE email accounts, both take into account PKI infrastructure concerns and allow the DoD to proceed with its forthcoming data guidance. They also enable CC/S/As who maintain Microsoft Exchange-based email systems to achieve immediate compliance with the new guidance via implementing a temporary email system configuration workaround.

Organizations Not Migrating to DEE

1. CC/S/A changes personnel email addresses to follow new specification
2. CC/S/A enables the use of proxy email addresses in Exchange (default setting)
3. CC/S/A enables name checking suppression in Outlook clients[1]
4. CC/S/A lists old email address (same one on user CAC email certificates) as proxy address for each personnel email account[2,3]
5. Personnel update email on CAC email certificate according to their current schedule (when CAC is set to expire)

Organizations Migrating to DEE

1. DEE changes personnel email addresses to follow new specification
2. CC/S/A enables name checking suppression in Outlook clients1
3. DEE enters email address found on user CAC email certificates as proxy address for each personnel email account2,[4]
4. CC/S/A enables name checking suppression in Outlook clients
5. CC/S/A enables auto forwarding for all emails sent to old email address (same one on user CAC certificate) to new DEE address[5]
6. Personnel update email on CAC email certificate according to their current schedule (when CAC is set to expire)

Considerations

Based on the fact that the email address on the CAC email certificate is the official persona email address of DoD personnel, implementation of the identified solution implies that the email address flowing through DoD Enterprise Directory Services (EDS) will be a user's old email address until their CAC email certificate is updated according to its regular reissuance schedule[6]. For example, DoD Enterprise White Pages will show a user’s old email address. The EDS team is currently pursuing potential solutions to this issue.

From a communications perspective, no issue will be encountered since email rerouting and auto forwarding will be enabled. However, individual users may notice incorrect email addresses provided by EDS and attempt to update their CACs, leading to the aforementioned capacity concerns with RAPIDS and CRLs.

[1] Allows Outlook users to utilize S/MIME security services in the case of email address mismatch

[2] Allows OWA users to utilize S/MIME security services in the case of email address mismatch

[3] Ensures emails sent to old CC/S/A email address are rerouted to new CC/S/A email address (aka email hijacking)

[4] Ensures emails sent from email account internal to DEE domain to old CC/S/A email address are rerouted to new DEE email address (aka email hijacking)

[5] Ensures emails sent from email account external to DEE domain to old CC/S/A email address are forwarded to new DEE address (aka auto-forwarding).

[6] This is not an issue for accounts migrated to DEE, as DEE addresses take precedence over CAC email addresses within EDS

From an engineering perspective, EDS feeds into CC/S/A directories will need to be configured so that primary SMTP email addresses are not overwritten until all CC/S/A users have updated their CAC email certificates.

Note, this solution only applies to Microsoft Exchange email domains.