USGCB Smart Card Removal Recommendation

Logical Access Working Group (LAWG) Recommendation

The purpose of this document is to present the findings of the LAWG's evaluation of the "Interactive Logon: Smartcard removal behavior" configuration options against agency needs and to provide a recommendation to the Technology Infrastructure Subcommittee (TIS) of the Federal CIO Council Architecture and Infrastructure Committee (AIC) to modify the configuration baseline.

The LAWG recommends changing the policy setting for "Interactive Logon: Smartcard removal behavior" to "Not Defined." This would effectively remove the behavior upon smart card removal from the baseline and allow an agency to select the behavior that best supports its use cases and requirements.

Background

The United States Government Configuration Baseline (USGCB), formerly known as the Federal Desktop Core Configuration (FDCC), currently has a requirement for federal agencies to configure their computers with the policy setting[1] "Interactive Logon: Smartcard removal behavior," which locks the workstation when a logged-on user removes[2] a smart card (also known as Personal Identity Verification [PIV] Card) from the smart card reader.

Natively within Microsoft Windows, there are three options when the smart card is removed:[3]

- **No Action**. Computer takes no action and there is no change to the system.
- **Lock Workstation.** Computer locks requiring user to re-insert card and provide pin/passcode to unlock.
- **Force Logoff.** Computer forces user to log off the system requiring user to re-insert card and provide pin/passcode to log back on.

Some agencies have use cases that necessitate configuring workstations to take "No Action" when a smart card is removed (e.g., system administrators who must access multiple workstations simultaneously with the same smart card). These cases result in a deviation from the baseline configuration, which requires the agency to develop a Plan of Action and Milestones (POAM) to realign their deviated configurations with the baseline configuration. This process does not accommodate known circumstances where an agency needs to permanently deviate from the baseline configuration, as in the case with smart card removal behavior.

In response to this situation, the Identity, Credential, and Access Management Subcommittee (ICAMSC) Logical Access Working Group (LAWG) under the Federal Chief Information Officers (CIO) Council evaluated the current USGCB requirements to determine if a change to

[1] As defined in USGCB Windows Settings, National Institute for Standards and Technology, May 2012. The USGCB describes Windows policy settings CCE-9067-0 "Smart card removal behavior" related to smart cards.

[2] For information related to insertion behavior (e.g., Windows policy settings CCE-9317-9 "Interactive Logon: Do Not require CTRL+ALT+DELETE") see USGCB Windows Settings, National Institute for Standards and Technology, May 2012.

[3] As defined in USGCB Windows Settings, National Institute for Standards and Technology, May 2012. Smart card removal behavior is set within Microsoft Group Policy. Some PIV Card middleware may have their own settings that should match the agency's policy for the workstation.

the current baseline configuration settings was necessary to better address agency needs and requirements.

Rationale

After conducting an analysis of the agency use cases and the benefits and limitations of the configuration options, the LAWG concluded that a single configuration for workstation behavior upon smart card removal is not viable. Federal agencies operate in diverse user and operating environments, so a “one size fits all” configuration does not appropriately address the specific needs and requirements of each agency. Depending on the operating environment, it could be appropriate for the workstation to “lock upon smart card removal” (the current baseline) or perform “no action” upon smart card removal (currently a deviation) to promote usability and a positive end-user experience.

For example, an agency would likely configure its workstations to “lock upon smart card removal” in the following cases:

- A user typically works on a single device at a time;
- For users who are prone to forget to lock their workstations, the need to display the credential for physical access will prompt the removal of the credential and automatic locking of the workstation;
- Environments where users do not leave their workstations frequently and maintaining smart card presence in the reader can minimize wear and tear on the credential; or
- Environments where users frequently perform advanced security functions (e.g., encryption and digital signature) and it is more convenient to maintain smart card presence in the reader.

Alternately, an agency would likely configure its workstations to perform “no action” upon smart card removal in the following cases, for example:

- A system administrator or other user who must access multiple workstations simultaneously with the same smart card;
- A system administrator must service end user workstations with the member logon session active (the current configuration would require multiple card readers and additional expense to the agency);
- Workstations tied to public display monitors that are activated following a personal logon and must persist a data display session; or
- Environments where a user must visibly display their smart card identification on his/her person at all times, even while at a workstation.

Changing the configuration baseline to “Not Defined” effectively removes the configuration baseline and offers agencies the flexibility to choose the smart card removal behavior that best suits their environment without being subject to a deviation. Since either configuration may be appropriate, having to complete a POAM to address a deviation is not suitable to the situation.

Security Considerations

While the LAWG’s recommendation offers agencies the discretion to choose the configuration that best meets their requirements, it should be noted that there are risks that accompany the implementation of either configuration. It is expected that the National Institute of Standards and Technology (NIST) will provide a risk and security analysis as part of the Federal CIO Council

AIC TIS review of the LAWG recommendation. The following risk matrix provides an overview of some of the security risks that may arise from implementing the configurations outlined in this document.

Risk Topic	Description
Unauthorized Access	• If a user leaves his/her workstation and forgets the PIV Card in the reader, then an unauthorized user may access the workstation. • If a user forgets to manually lock the workstation (where the smart card has already been removed with “no action”), then an unauthorized user may access the workstation.
Exposure to Security Threats	• If the PIV Card is kept in the reader for long working sessions, it may be exposed to potential security threats, such as malware, for a more extended duration.
Lack of PIV Card Possession for Physical Identification and Access.	• If a user leaves his/her workstation and forgets the PIV Card in the reader, he/she will not be in possession of the credential for identification and physical access to move within or re-enter the facility.
Cached PIN	• If a user leaves his/her workstation and forgets the PIV Card in the reader and the PIN is cached, then an unauthorized user may be able to perform security functions with the PIV Card (i.e., encryption, digital signatures).

Figure 1: Security Risk Matrix of the Baseline and Alternate Configurations

Should the LAWG recommendation be accepted, an agency is expected to implement compensating controls to mitigate known security risks associated with the configuration chosen. These compensating controls may include:

- **Automatic workstation timeout.** The workstation should be configured to meet mandatory security controls for automatic workstation timeout after a defined period of inactivity. This can help mitigate risks associated with a user either forgetting his/her smart card in the workstation or forgetting to manually lock the workstation when the smart card has already been removed with “no action.”
- **User training.** Many of the risks associated with smart card removal configuration result from instances where a user either leaves his/her workstation and forgets the smart card in the reader or forgets to manually lock the workstation when leaving. Training users on proper workstation locking behavior can mitigate both of these risks.