TECH BRIEF

BeyondTrust™

VISIBILITY. KNOWLEDGE. ACTION.

# Utilizing CAC and PIV Cards to Enforce Multi-Factor Authentication in Federal Government Agencies

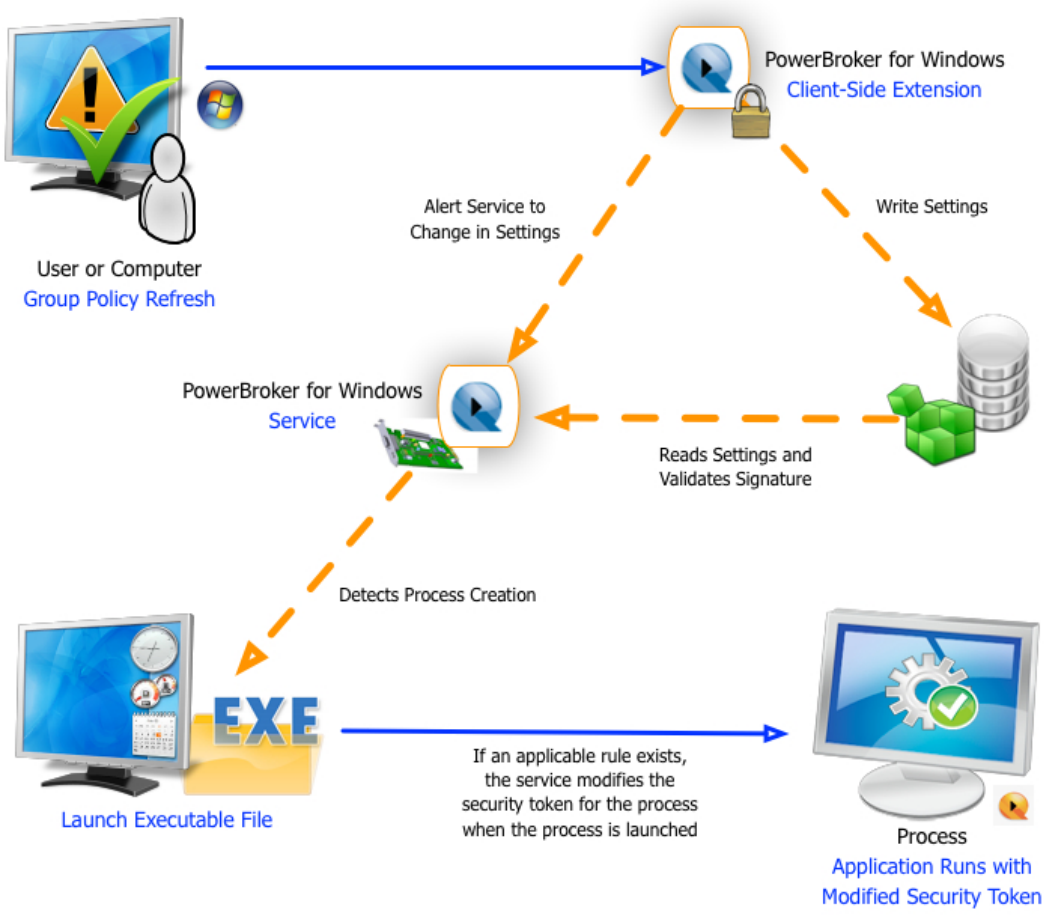
## Table of Contents

# Introduction

The primary purpose of a Smartcard – known as the Common Access Card (CAC), or the Personal Information Verification (PIV) Card - is to provide a multi-factor authentication to a system using embedded integrated circuits, a username, and a corresponding complex password. The combination of a user's possession of the card, knowledge of the username, and current password authenticates a user against a given system. The Smartcard itself must be available and valid, and inserted mechanically into a system such that the integrated circuits are active for the duration of the session. If it is removed, typical policies dictate that the session should be terminated immediately. Thus, the user and smartcard are the basis for authentication during the entire length of the session.

# How to Enforce Least Privilege With CAC and PIV

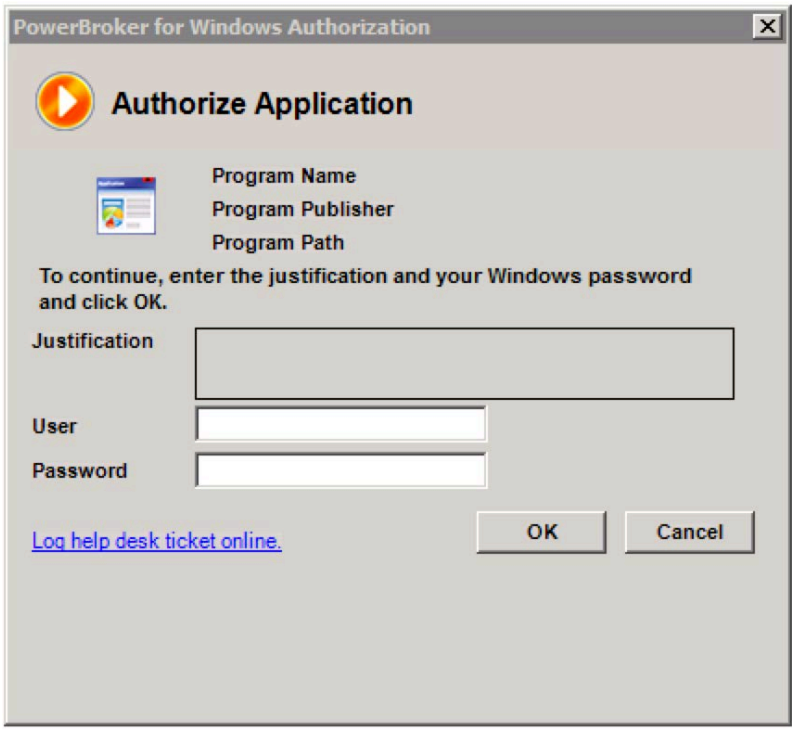
Administering the BeyondTrust PowerBroker for Windows solution for least privilege enforcement does not require integration with CAC or PIV cards; therefore, being CAC or PIV compliant is not relevant. PowerBroker for Windows is designed to intercept a user's launch of an application or operating system feature and modify the security token of the application to meet the privileges required for it to operate as designed. The process requires a user to be authenticated on the asset to launch applications and that only occurs once they login locally, from remote desktop session, or even a virtual desktop environment.




The illustration above documents the process and is only viable after the user has established an interactive session.

In a typical deployment of PowerBroker for Windows, the policies that are active are hosted by Microsoft Group Policy and replicated automatically via Active Directory replication. As an Active Directory User, they are enforced once a user authenticates (whether using a Smartcard or standard NTLM authentication) and the session is available for interactive use. These rules can be applied to applications with various outcomes:

- Automatically change the security of the application to a local administrator
- Customize the security token of the application to meet a specific privileged objective
- Deny the application from launching
- Display a User Message requesting additional information including:
    - A justification for the application launch
    - The current username and password of the authorized user
    - A text only message displaying the current state of policy
    - Hyperlinks including email addresses to launch
    - Customization of the items above to cater the end user experience including graphics, colors, and localization.

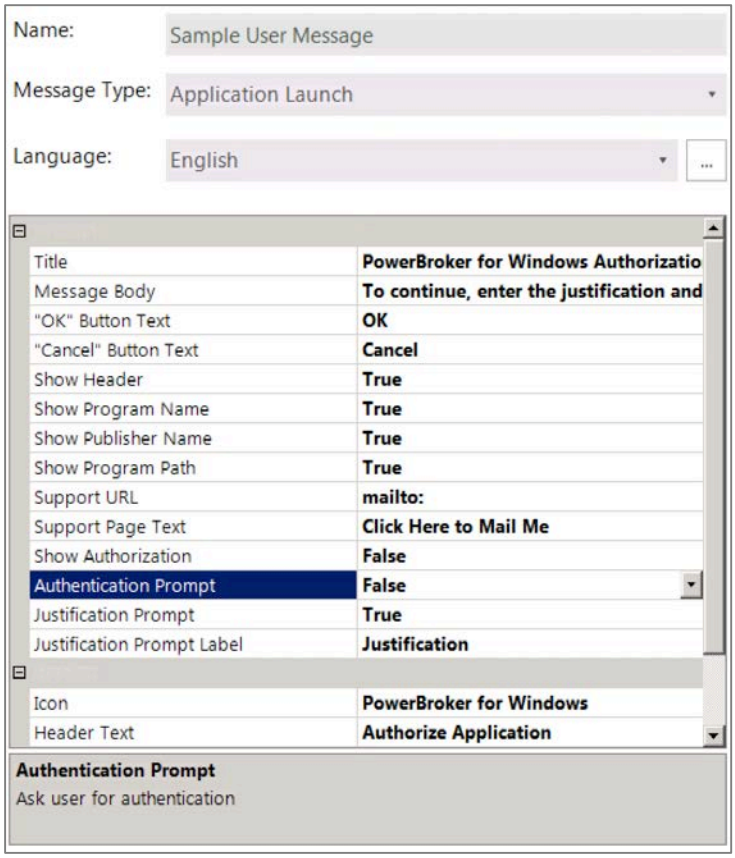


## Patented PowerBroker for Windows

PowerBroker for Windows has a patent on the elevation of an application and secondary justification of why the user requested the application (patent **8566586**)**.** This approach provides a seamless experience for an end user (or administrator, helpdesk, executive, etc.) to raise applications' privileges (not the user) and document why the application was used. User justifications are centrally available in a report from BeyondTrust's Privileged Access Management Platform, BeyondInsight.

This entire process assumes that the Smartcard is mechanically inserted, electronically connected, valid, and that the end user is indeed still the same person at the keyboard. As noted, this is in fact policy for most organizations to never leave your Smartcard in a terminal. Therefore, launching an application with privileges relies on a valid Smartcard user and the policies assigned to them via Active Directory Group Policy Options.

The only time this scenario is not valid is if the User Message is customized to require a Username or Password in addition to a justification or standalone. This use case is designed for environments that only user standard Microsoft Challenge Response NTLM paradigms for usernames and passwords. It is not valid for an environment using Smartcards because the user is authenticated for the length of the session and should not need to re-justify whom they are. It is therefore recommended to customize user messages for Smartcard environments with the parameters shown below:




## The BeyondTrust IT Risk Management Platform for Federal Agencies

As breaches and threats continue to refine their methods for penetrating agencies' security perimeters, it is more critical than ever for IT security administrators to have a complete view of their IT landscape and its potential risks.

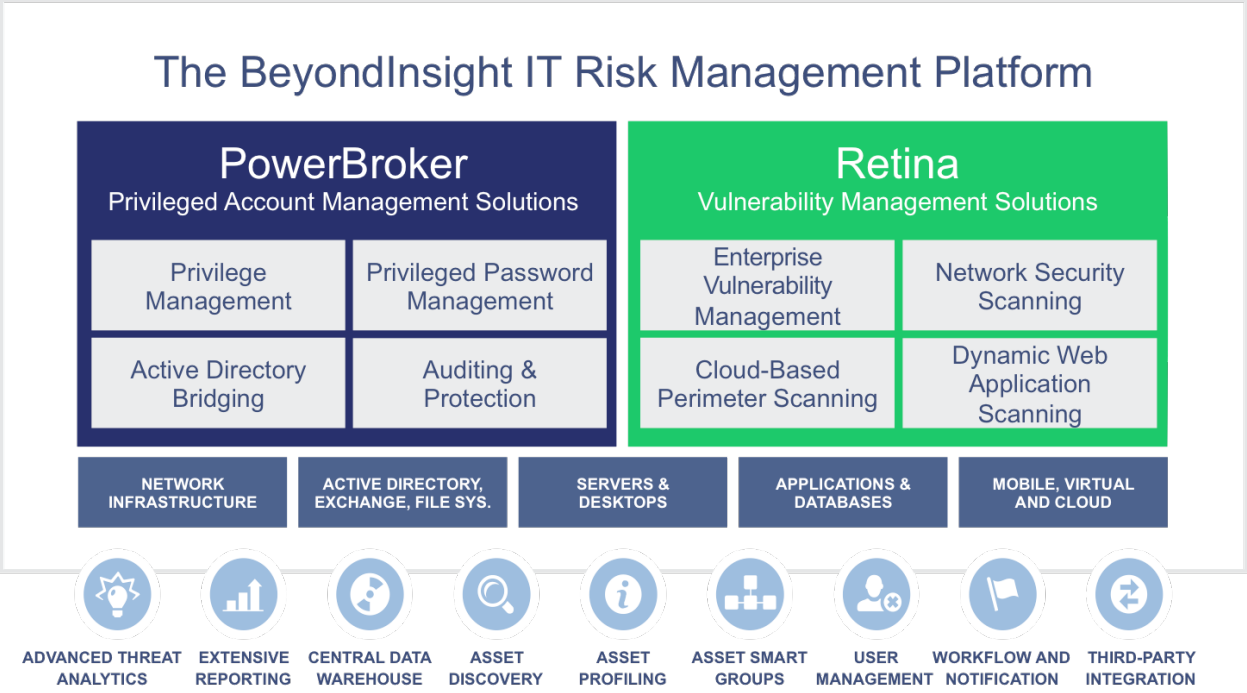
The BeyondTrust IT Risk Management Platform helps agencies fulfill government requirements through its integrated suite of IT security solutions that reduce user-based risk and addresses security exposures. The platform provides IT security leaders with a single view of all assets and user activity. With behavioral analytics to understand anomalies, compliance reporting, and the ability to leverage third-party data, the platform reduces risks while helping to maximize the value of existing security investments. Available in software and hardware appliance formats, the BeyondTrust platform integrates two foundational security methodologies.

**Privileged Access Management**

BeyondTrust Privileged Access Management solutions close the gap between IT security requirements and user enablement. With BeyondTrust, security and IT operations teams gain a comprehensive privileged account management solution, deep analytical insights for better decision-making, and extensibility across the security landscape. As a result, your organization reduces IT security risks, simplifies compliance, and maintains user productivity.

**Vulnerability Management**

BeyondTrust Vulnerability Management solutions provide security professionals with vulnerability assessment and risk analysis in context. With BeyondTrust, IT teams can proactively identify security exposures, analyze business impact, and plan and conduct remediation across network, web, mobile, cloud and virtual infrastructures, and communicate that risk to operations and compliance teams to reduce risk.




For more information on the BeyondInsight IT Risk Management Platform for Government Agencies, checkout the Government section of our website, request a free trial, or contact us.

# About BeyondTrust

BeyondTrust® is a global cyber security company that believes preventing data breaches requires the right visibility to enable control over internal and external risks.

We give you the visibility to confidently reduce risks and the control to take proactive, informed action against data breach threats. And because threats can come from anywhere, we built a platform that unifies the most effective technologies for addressing both internal and external risk: Privileged Access Management and Vulnerability Management. Our solutions grow with your needs, making sure you maintain control no matter where your organization goes.

BeyondTrust's security solutions are trusted by over 4,000 customers worldwide, including over half of the Fortune 100 and over 200 U.S. Federal Agencies. To learn more about BeyondTrust, please visit www.beyondtrust.com.