


How to Embed Security into Fast-Paced Agile and DevOps Environments in the Public Sector

 Click here to explore >



GOLDFINGER
HOLDINGS

Introduction

With uncompromising security and data protection being absolutely necessary in the federal sector, it is critical for government agencies to ensure robust and effective information security in their development environments. Designing a comprehensive approach to identity, credential, and access management in fast-paced Agile and DevOps environments is key to addressing information security priorities and reducing the risk of unauthorized access to federal resources and information systems.

The purpose of this guide is to:

- Explain the need for a modern authentication solution that can integrate authentication in a smart way without compromising operational speed and agility
- Provide best practices for adopting a solution that meets the above requirements
- Discuss ways to further strengthen security using a process improvement approach

DevOps in the Federal Sector

Due to the critical nature of software-driven innovation today, more and more government entities are turning to Agile and DevOps methodologies in order to deliver applications faster, more securely, and with better quality. The pace at which agencies can make critical changes to applications and roll out new functionalities is vital. Modern practices such as Agile and DevOps are inherently more efficient, and help organizations iterate quickly and be more nimble with product enhancements, faster integration, and more sustainable applications. What used to take several months using traditional “waterfall” methodology can now be done much more rapidly – sometimes in a matter of days or even minutes.

As a leading provider of collaboration, development, and issue tracking software as well as enterprise DevOps solutions, Atlassian’s suite of solutions are quite popular in the federal sector. Because development and IT operations are intertwined in a DevOps environment, applications such as Jira, Confluence, Bamboo, and Bitbucket, Jira Service Desk, and Crowd are typically available to all team members. These tools are used on a daily basis as the mechanism for continuous innovation, feedback, and improvements, while eliminating the traditional barriers of siloed teams, tools, and processes.

The Security Challenge

The government sector faces unique challenges to adopting a robust DevOps process, particularly as it relates to security and compliance requirements within agencies. Whether an application is designed for general use or is mission-critical to an entity, DevOps must be secure. Not only should the application be secure, but the entire development environment must be secure too. It is important to design critical security controls, such as access and credential management, in a way that would meet federal security requirements and standards without slowing down operations. The key question is: How can an organization embrace a transparent, collaborative development process that can meet the required speed and frequency of software development and delivery in a modern Agile/DevOps setting, while ensuring uncompromising security and data protection?

CAC/PIV for Improving Security

Every government organization needs to comply with a mandatory standard for secure and reliable two-factor identification to control access to all federally-controlled facilities, networks and information systems. A common access card, or CAC, is used by the Department of Defense, while non-DoD agencies typically use a personal identity verification, or PIV, card. Both cards, in combination with a personal identification number, satisfy the two factor requirement and greatly reduce the risk of unauthorized access to federal resources.

An attacker would need to compromise two factors – not just a single one – to gain access to an agency's systems and/or networks, such as something the user has (a CAC/PIV card) and something the user knows or is (a personal identification number or a biometric characteristic to unlock the card). This allows for a high level of assurance and ensures resistance to identity fraud, tampering, counterfeiting, as well as exploitation.

Continued...

The Security Challenge

The best way to design a comprehensive approach to identity, credential, and access management in a development environment is to therefore enable applications to be smart-card compliant. Applications should be able to utilize CAC/PIV credentials for logical access control and identity management in Agile and DevOps-driven environments in order to reduce vulnerabilities and ensure uncompromising security.

Here are a few reasons why CAC/PIV enabled applications are the best way to resolve key security challenges in government agencies:

1. First, users can leverage the same card that hangs around their necks to be the key to access all applications.
2. Smart cards meet the demand for a secure and robust form of authentication based on client certificates – thus several risks can be mitigated. They execute cryptographic operations where the private key never leaves the card; all crypto operations involving the private key are carried out on the card itself and that makes it difficult to compromise smart-card enabled applications.

“The best way to design a comprehensive approach to identity, credential, and access management in a development environment is to therefore enable applications to be smart-card compliant.”

The Importance of a CAC/PIV Authenticator Solution in Busy DevOps Environments

Enabling applications to be CAC/PIV compliant using custom code can be a difficult, expensive, and time-consuming process. Deploying a CAC/PIV authenticator can fulfill the role of an ideal security control for a wide spectrum of applications in busy DevOps environments, providing secure two-factor authentication without slowing down the login process for users.

A CAC/PIV *authenticator* is a solution that can rapidly enable your agency applications to accept CAC/PIV credentials and verify users before logging them into an application. When a user wants access to an online DevOps environment, for example, they browse to the login page and enter their username and password.

The authenticator solution reads a digital certificate stored on the user's smart card and compares it to information in an authentication database. If the credentials match and the user has permission to use the application, login is granted, quickly and easily, without compromising security.

What to Look for in a CAC/PIV Solution

An Agile/DevOps development environment typically consists of a variety of tools for project management, issue tracking and team collaboration. Because development and IT operations work together closely in a DevOps environment, tools such as Jira, Bitbucket and Jira Service Desk from Atlassian are typically available to all team members. And everyone is subject to the same access to security rules.

Continued...

The Importance of a CAC/PIV Authenticator Solution in Busy DevOps Environments

When evaluating CAC/PIV authentication solutions for a DevOps environment, consider these questions:

Q1

How successfully will the solution help meet your service goals?

Q2

How will it integrate with your organization's existing CAC and PIV authentication infrastructure?

Q3

Does the solution integrate authentication in a smart way? Or does it introduce any additional complexities that can adversely impact the day-to-day workflows of users?

Q4

Does it support government security initiatives and policies?

Q5

And does it provide cost-effective, easy-to-implement ways to enable applications to meet the challenges of smart card compliance?

Continued...

The Importance of a CAC/PIV Authenticator Solution in Busy DevOps Environments

Goldfinger's CAC/PIV Authenticator for Atlassian is one such solution, providing secure and seamless access to Atlassian's Jira, Confluence, Bamboo, and Bitbucket, Jira Service Desk, and Crowd tools – without compromising operational agility and speed. It ensures consistent user authentication by allowing only valid CAC/PIV card holders to access their Atlassian tools, thereby fulfilling critical security requirements and maintaining the highest level of compliance.



CAC/PIV Authenticator

Strengthening Security Using a Process Improvement Approach

Once a solution is in place, it is important to follow industry best practices for managing users and accounts to enhance your overall security and compliance posture. For instance, you should inventory all privileged users and accounts and then remove all unnecessary privileges and access. This includes default accounts that are no longer needed, and accounts for users who no longer need access.

Maintaining only active or necessary accounts helps to prevent impersonation of *privileged users*. A privileged user has more permissions in a system than a general user. An attacker who gains access using a privileged account can do much more harm than using a general user account.

Implement other necessary security controls, such as:

- Policy and procedures related to system access and privileged users,
- Continuous monitoring of access,
- Logging of system events related to privileged account use, and
- Automatic locking of privileged user sessions after a period of inactivity or upon user request

Conclusion

When it comes to security and compliance for government entities, the stakes are high and the cost of failure is even higher. A CAC/PIV authentication solution that allows integration of authentication in a smart way, without burdening users or adversely impacting their day-to-day workflows, is ideal in modern Agile and DevOps settings to stay nimble and productive while maintaining the highest levels of security and working within stringent government mandates.



GOLDFINGER
H O L D I N G S

Goldfinger Holdings is an industry-leading technology company dedicated to helping organizations extend the capabilities of their mission-critical applications to power innovation, deliver value, and drive growth. We offer a comprehensive suite of solutions – ranging from value stream integration, to agile test management, to federal identity and access management – to introduce enhanced levels of visibility, quality, and security into the software development lifecycle.

Goldfinger's CAC/PIV Authenticator ensures consistent user authentication for a broad spectrum of Atlassian tools by allowing only valid CAC/PIV card holders to access their Atlassian systems, thereby fulfilling critical security requirements and maintaining the highest level of compliance. For more information, contact us at sales@goldfingerholdings.com or follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).