HIGHLIGHTS

Strengthened security posture for regulation such as **NIST and CMMC**

Improved user experience with **Axiad ID mobile authentication**

Reduced security incidents by moving to a **true MFA solution**

DEFENSE CONTRACTOR ENHANCES SECURITY AND USABILITY WITH AXIAD SOLUTIONS

REDUCING COST AND COMPLEXITY WITH UNIFIED CREDENTIAL MANAGEMENT

In large organizations like defense contractors, it can be difficult to find the right balance between security and usability. Updating legacy systems across widespread workforces is time-consuming, and often the simpler-to-use products don't come with the same level of protection. For contractors working with the DoD, this is a problem – they need to meet a variety of security standards such as NIST-SP800-171 and CMMC (Cybersecurity Maturity Model Certification) to maintain their business.

One US defense contractor wanted to enhance their credential management so they could easily meet these security standards without creating logistical hassles for their IT teams or employees. After their previous password-based authentication led to a security incident within the organization, they expedited their transition to multi-factor authentication. They needed a secure solution that was simple for employees to use, and a cloud-based management system that could reduce maintenance time for their IT team.

The contractor ultimately selected Axiad Cloud for their credential management and Axiad ID for their mobile authentication. These solutions were the most secure options they considered: Axiad deploys every platform as a virtual private cloud so the organization didn't need to worry about data breaches on a shared cloud infrastructure. They were able to manage their Axiad ID mobile authenticator and their smart cards for privileged users in one centralized portal.

The Axiad solution strengthened the defense contractor's security posture – the VPC and advanced encryption in Axiad ID meant they were prepared to meet NIST compliance and CMMC in the future. The new solutions reduced their dependency on passwords and offered them a true MFA solution, which stored certificates separately from the mobile devices, unlike other providers. The strength of their new solution has helped them prevent multiple security incidents since their deployment.

Beyond the security benefits, their IT team also benefited – the Axiad Cloud platform put an end to the constant maintenance of their legacy credential systems. The automation of the platform meant they could redistribute their team to different projects and increase their productivity. On the end user side, employees no longer were dependent on their help desk. They could manage their own credentials in their self-service portal - whether they're onboarding, have changed devices, or need to update a certificate.

> “Axiad was the obvious choice for us to improve our MFA. We had numerous standards we needed to meet and wanted a trusted partner with expertise in all the credentials we would require. The Axiad solution offered the strongest security with a virtual private cloud and unparalleled encryption.”
>
> - Systems Engineer, Sr. Manager, US defense contractor

THE CHALLENGE

When this large defense contractor was faced with password-based security incidents and upcoming regulations such as NIST-SP800-171 and CMMC, they needed to refresh their authentication. Their legacy credential system required a large team to maintain, and their users were struggling to use their OTP tokens to quickly access their resources. The organization wanted a solution that met their high security requirements without burdening IT or the end user.

THE SOLUTION

After a full analysis of alternatives, they deployed Axiad Cloud to fully manage their multiple credentials in one unified platform. They selected Axiad ID as their mobile authentication solution due to the advanced encryption it offers. Axiad ID and their additional credentials, such as smart cards for privileged users, can be issued, updated, and managed in their employees’ user portal. They were able to transition their legacy on-prem system into a virtual private cloud, which strengthened their standing in audits and regulation since it eliminated the risk of a shared infrastructure.

Axiad’s credential management solution offered benefits to all their users and devices:

- The Axiad Cloud user portal for any lifecycle management or support needs
- Axiad ID for push notification-based authentication on users’ mobile devices
- Smart cards for privileged users, managed in the same unified platform
- Authentication for mobile devices and other machines in the future

THE RESULTS

With the Axiad solution, the contractor strengthened their defenses against credential theft – they have since prevented multiple attempted credential thefts from accessing their resources.

Their multi-factor authentication ensured their success in future audits. The IT team no longer had to spend time maintaining legacy credential systems and end users no longer need to assist employees in issuing/managing credentials thanks to the self-service portal.

- Prevented multiple credential theft attacks with MFA technology
- Re-focused IT team from credential system maintenance to strategic projects
- Enhanced employee usability and login experience with Axiad ID authentication