VANGUARD ez/PIV Card ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Validation

Provides out-of-brand and enhanced PIV card and password generation and validation

Authentication

Requires multifactor authentication to validate employees and external contractors before they gain access to critical resources

Security

Once a PIV card has been revoked, a user is no longer permitted to access mainframe resources

Vanguard ez/PIV Card satisfies FIPS 201, HSPD-12. It allows your users to authenticate to z/OS Security Server through the use of a government PIV or CAC Card.

Key Features:

- ez/PIV Card is an authentication solution that ensures z/ OS Security Server complies with Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standards 201 (FIPS 201).
- Increases system security by requiring multi-factor authentication to validate employees and external contractors before they gain access to an enterprise's most critical resources.
- Provides out-of-band password generation and validation.
- Provides enhanced PIV Card and Password validation.
- Once a PIV Card has been revoked, a user is immediately denied access to z/OS Security Server.

VANGUARD ez/PIV Card ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Background on Homeland Security Directive (HSPD) to Implement PIV Systems for Physical and Logical Access to All Government Employees and Contractors

In 2004, the White House issued Homeland Security Presidential Directive (HSPD) 12 in order to establish more uniform standards for issuing government identity credentials. HSPD-12 applies to all government employees and contractors and governs physical (facility) and logical (systems) access.

Born from this directive was FIPS 201 — a requirement by the National Institute of Standards and Technology (NIST) that specified architecture and technical requirements for a common identification standard for U.S. government employees and contractors.

The standard outlined the Personal Identity Verification (PIV) system that supports a common smartcard-based platform for identity authentication and access to multiple types of physical and logical access environments. Smartcards carry the physical and digital components forming the user's PIV credentials.

85% of Our Most Critical Data is on Our IBM Mainframe. Is There a PIV Solution for z/OS?

Yes, and Vanguard was the first vendor in the INFOSEC industry to enable the applications and services running on IBM mainframes to be accessed utilizing PIV authentication. Vanguard Integrity Professionals specifically developed ez/PIV Card Authenticator software for federal agencies that use IBM z/OS systems and want to comply with HSPD-12 and FIPS 201.

The Solution: Vanguard ez/PIV Card Authenticator

VANGUARD ez/PIV Card Authenticator software authenticates users to a z/OS Security Server and validates identities to a personal identification verification (PIV) authentication server that is either hosted within an agency's secure domain or by a third party outside of the secure domain. VANGUARD ez/PIV Card Authenticator is the only PIV card authentication solution that ensures IBM z/OS systems comply with Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standards 201 (FIPS 201).

VANGUARD ez/PIV Card ™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

How ez/PIV Card Works

A user self-registers their PIV card using the Vanguard ez/PIV Card Authenticator client software's simple point-and-click interface. Then, Vanguard ez/PIV Card Authenticator validates the PIV card and its certificate via a certificate revocation list (CRL) or an online certificate status protocol (OCSP). Once the card is validated, Vanguard ez/PIV Card Authenticator issues the user an 8-character PIV password that they can use for a specified time period. The PIV password is created from a combination of information about the specific user from their PIV card, RACF user ID and password, and a time-based element. The user enters the PIV password to authenticate to all or some applications running on z/OS Security Server that have been specified by an agency or department to require PIV validation.

Increasing Security, Ensuring Compliance

VANGUARD ez/PIV Card Authenticator increases system security by requiring multiple factor authentication to validate employees and external contractors before they gain access to an agency's most critical resources. With VANGUARD ez/PIV Card Authenticator, once a PIV card has been revoked, a user is no longer permitted to access mainframe resources.

Key Differentiators

- Provides out-of-brand password generation and validation
- Provides enhanced PIV Card and password validation.
- Once a PIV Card has been revoked, a user is immediately denied access to z/OS Security Server.
- Allows z/OS Security Server to verify PIV credentials from other agencies.
- Easy point-and-click PIV password creation. Uses OCSP or CRL authorities to check for current certifications.
- Compatible with IBM's new password algorithm.
- Deployable in an enterprise extender environment as a pass-through request.

VANGUARD ez/SignOn™

VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

Why Vanguard to Secure Your Enterprise?

Almost half of the Fortune 1000 companies in the world spanning banking, retail, insurance, as well as numerous government agencies trust Vanguard with their enterprise security.

About Vanguard Security Solutions

Vanguard offers the most advanced and integrated portfolio of enterprise security products and services in the world. The portfolio was the first to offer fully automated baseline configuration scanner for Mainframe DISA STIGs— the Gold Standard for Security.

For More Information

To learn more about Vanguard Security Solutions please call 702.794.0014 or visit www.go2vanguard.com

Corporate Headquarters

6625 S. Eastern Avenue—Suite 100
Las Vegas, NV 89119-3930