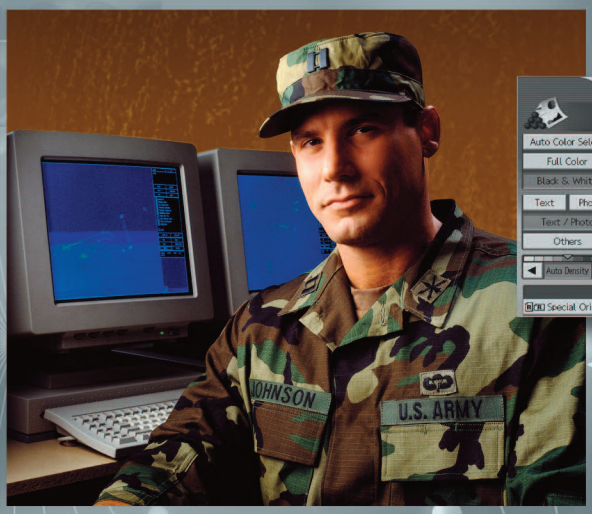
LANIER

Common Access Card

SOLUTION



Common Access Card (CAC)/Personal Identity Verification (PIV) Authentication Solution, Version 3

Smart Card Technology for the United States Government

LANIER

SOLUTION

CAC/PIV Authentication Solution V3

Strong User Authentication for Securing Information Assets

The United States Government has launched a global initiative to deploy standardized Common Access Cards (CAC)/Personal Identity Verification (PIV), smart cards, to millions of active duty military, reserve personnel, civilian employees and contractors. Among its many functions, the pocket-size CAC/PIV allows the card holder to physically access secure areas and permits entry into U.S. Government computer networks. A critical element to this infrastructure is that it requires strong and substantial evidence of the individual's identity.

Information Remains Vulnerable

CAC/PIV technology was developed in response to government directives to secure the computer infrastructure, as well as other vital assets, including connected MFPs (multifunctional products). Without access controls in place, MFP users are free to capture, distribute, store and retrieve digital data via the network. As such, digital imaging systems pose a threat to information security.

LANIER® Addresses Vulnerabilities

Lanier developed the CAC/PIV Authentication Solution as a tool that allows only holders of a valid CAC/PIV to access device functions. Simple yet effective, the Lanier solution permits the authenticated user to perform Copier, Scanner (e.g., Scan-to-Email and Scan-to-Folder), Facsimile and/or Document Server functions.* This strong authentication method helps Government departments, agencies, officers, employees and contractors to implement a common identification standard that enhances security and efficiency, while protecting personal privacy.

How It Works

All Lanier MFP functions* are locked until the user inserts their valid CAC/PIV into the card reader (attached to the device) and enters their Authentication PIN. The user's CAC/PIV credentials, embedded on the card, are automatically compared against a database of authorized users. During the authentication process, the exchange of credentials results in success (identity is confirmed) or failure (identity cannot be confirmed).

Under CAC/PIV Authentication, it is also possible to specify which functions can be performed. Device A may allow users to access all functions, while Device B users can only access Copier functions. Selective authentication controls how data is introduced into a digital workflow; for instance, Scan-to-Email functions can be restricted to only certain areas. This eliminates the anonymous use of Scan-to functions that can lead to potentially damaging information leaks.

*Authentication of Printer functions is handled on the PC level using existing desktop policies regarding CAC/PIV Authentication.

For more information about the Lanier CAC/PIV Authentication Solution V3, contact your Lanier sales representative or visit www.lanier.com.

www.lanier.com

Email with Digital Signature and Encryption

Lanier's CAC/PIV Authentication Solution V3 Scan-to-Email feature offers enhanced security through Secure/Multipurpose Internet Mail Extension (S/MIME), a technology that allows authenticated users to digitally sign and encrypt email. Only recipients with the associated private/public keys can decrypt the message, providing enhanced assurance of document integrity and confidentiality. Combined with local (MFP) and global (LDAP) address book search capabilities, users have a fast, simple and secure way to capture and distribute documents.

FIPS 140-2 Level 1 Certification for scan to email*

Lanier's CAC/PIV Authentication Solution V3 is FIPS 140-2 Level 1 Certified. The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard, issued by NIST (National Institute of Standards and Technology) and used to accredit cryptographic modules that include both hardware and software components.

*Certificate #792

Supported Authentication Methods

Common Access Card Authentication Solution supports the following authentication methods:

- OCSP Server
  - Primary
  - Secondary
  - Proxy
- Active Directory
  - Kerberos Realm (Microsoft Windows® Server 2003 and 2008)
- CRL (Certificate Revocation List)

CAC/PIV-compatible Lanier MFPs

- Java Version 4.x, 5.x, 7.x MFPs

Required MFP Features/Options

- Printer/Scanner Kit
- USB Host Interface
- Java VM SD Card

Lanier-tested CAC/PIV Readers

- SCM Microsystems: SCR331 or SCR3310
- OMNIKEY: CardMan 3121

Required Customer-supplied Items

- CAC/PIV Card
- OCSP Server URL(s)
- OCSP Server Certificate(s)
- Root CA Certificate(s)
- Sub CA Certificate(s)

Note: The OCSP Server URL(s) and Security Certificates can be obtained from the on-site Security Administrator.

1.
Insert a valid CAC/PIV Card into the card reader.

2.
Enter your Authentication PIN.

3.
Identity is confirmed allowing access to secure MFP functions.