IDENTITY MANAGEMENT

Mitigating Risk for Federal Agencies

A Vision Technologies Whitepaper providing an overview of the processes and procedures developed to provide for Identity Management and Information Assurance.

VISION TECHNOLOGIES

Making Vision Reality

Identity Management

MEETING ORGANIZATIONAL NEEDS FOR IDENTITY MANAGEMENT & INFORMATION ASSURANCE

BACKGROUND

The risk of a cyber-attack, malicious or unintended, is one of the most serious economic and security challenges facing the Federal Government today. Mitigating that risk requires comprehensive scalable solutions for managing identities and access to logical and physical assets. To directly address the cyber-security needs of the Federal Government the Homeland Security Presidential Directive 12 (HSPD-12) was developed in 2004 as a strategic initiative to standardize on an identity credential that would increase security, reduce identity fraud, and be compatible with widely deployed technologies. That credential is the Personal Identity Verification (PIV) card.

Federal Agency response to HSPD-12 was immensely successful. The final 2012 implementation statistics report over 97% of targeted PIV card issuance for to civilian and military personnel, and 88% of contractors, met[1]. In 2011 as a continuing resolution to HSPD-12 the Office of Management and Budget (OMB) released Memorandum 11-11 (M-11-11), which calls for expedited 'full use' of PIV credentials. With the majority of the federal work force now in possession of PIV cards Federal Agencies are tasked with individually deploying technology and procedures that follow the published security considerations and guidance for Federal Identity, Credential, and Access Management (FICAM).

IDENTITY MANAGEMENT CHALLENGES

Identity Management (IdM) programs bidding for compliance with M-11-11 face specific challenges in an increasingly mobile and collaborative work environment. Planning for external users, mobile devices, universal availability of data, and remote access to secure private networks are common Agency goals for defining FICAM implementation strategies. Existing legacy infrastructure, insufficient help desk resources, and disparate physical and logical access control systems are the limiting factors to an Agencies M-11-11 compliance success. Updating, or migrating from, legacy infrastructure to PIV enabled systems may lead to service outages if proper planning and management is not applied to projects. Limited help desk resources can becomes strained, costly, or both when implementing new technologies. Disconnected infrastructure can become a configuration nightmare for organizations managing authorization to various resources.

Highlights

- HSPD-12 standardizes identity credentials
- OMB calls for "full use" of PIV credentials
- Leveraging external credentials can produce cost savings
- There are cost effective, interoperable, solutions for external users
- CIV provides a scalable, rapid-to-deploy, scalable solution
- Mobile solutions are also available

PLANNING FOR EXTERNAL USERS – TRUST VS. BUY

Visitors, contractors, and business partners often hold federally issued PIV or commercial PIV-I badges are federally trustworthy identity credentials. Leveraging those existing credentials can show a cost savings to your Agency. However, trusting external credentials can prove challenging for systems that are deployed without a centrally managed Public Key Infrastructure (PKI) trust settings and external infrastructure issues can generate system outages and help desk calls. Trust setting audits and infrastructure monitoring can eliminate those unwanted outages, and reduce call time with your organizations help desk, when dealing with trusting external credentials directly.

Alternatively, for some agencies, trusting externally issued credentials from external entities is not desirable, and existing visitor badging practices are often not in-line with FICAM goals.

If the above is true, there are cost effective, interoperable, solutions for external users such as Commercial Identity Verification (CIV) solutions for Government. CIV provides a scalable, rapid-to-deploy, visitor badging solution with Agency defined policies and practices that are in-line with security requirements. CIV works at the door and on the network the same way a federally issued Contractor PIV badge would, with a drastically lower cost of issuance.

When planning for external users and making the Trust vs. Buy decision Vision Technologies, partnered with Castle PKE, has a proven track record of designing large-scale IdM and Federated IdM solutions that are in-line with Agency FICAM goals.

Information Assurance Challenges

Information Assurance can be broken down into three sub areas, integrity, confidentiality, and availability. Following M-11-11 guidelines in both logical and physical environments proper use of a PIV card will provide (a) integrity via digital signature of data and (b) confidentiality via encryption. Data availability is the true information assurance challenge for Agencies with remote users and mobile device requirements.

Information at your fingertips – Securely & On demand

Mobile file management (MFM) solutions address the availability challenge and provide for secure transfer and storage of sensitive files to an employee's mobile device or remote workstation that can only be accessed through use of a valid PIV card. With mobile devices such as iPad®, iPhone® or Android® devices, a PIV enabled MFM solution allows for the greatest amount of availability while meeting M-11-11 PIV usage requirements.

M-11-11 aligned MFM solutions also further address integrity and confidentiality through integration with Agency IdM systems such as Active Directory to provide Agency Oversight of access rights to data, and will only utilize FIPS-140 approved cryptographic algorithms and Software Development Kits (SDKs).

Vision Technologies, partnered with Castle PKE, can expertly guide MFM deployments that integrate with IdM solutions to provide the highest levels of oversight and information assurance Agencies.

Castle PKE provides software and services that extend the usefulness of Public Key Infrastructure (PKI) for daily use with critical business applications. Castle makes integration convenient, cost effective, and clear for organizations exploring the use of high assurance identity credentials for current (and planned) business applications. Whether you are planning to extend your organizations FIdM or architecting one from scratch Castle Consulting Services can help by setting a strong foundation with you.

