Evidian

Boost PIV compliance with Enterprise Access Management

Trusted partner for your **Digital Journey**

Aventex + Atos

Personal Identity Verification (PIV) program

To remediate security issues, federal agencies adopted the Personal Identity Verification (PIV) program, a new authentication system based on Smart cards and public Key Infrastructure. Deploying this new system was expensive, but nothing compared to the actual cost of enforcing smartcard use across multiple systems, applications and devices.

Password limitations

Passwords are widely accepted security systems. Everyone understands how to use them, they are free, they work from every platform and in every situation. For all the hypes about multi-factor authentication, every application still comes with a password authentication. A Password is safe, in and of itself, as long as the application it guards uses encryption. It would take hackers 19.24 years to try every combination, assuming that those hackers have enough computing power to mount a 100-billion-guesses-a-second effort, in order to break a 10-character password.

It is with the end users, the password holders, that we have a problem. Passwords become vulnerable because end users have too many of them, so they write them down, they try to get away with "easy to remember" passwords and they reuse the same password across as many applications as they can. Also, end users are not as good as they should at keeping those passwords to themselves, they share them, for convenience and expediency. All too often, they get abused by hackers and their passwords get fished.

Adopting strong password policies, which means forcing end users to choose complex passwords and change them regularly, may look good on paper. But the hardest it is for end users to remember passwords, the more they are going to write them down... Password policies are a never-ending whack a mole game.

HSPD 12

Recognizing the risks associated with passwords, the federal government signed Homeland Security Presidential Directive 12 in August 2004. This directive mandates Federal agencies to issue a PIV (Personal Identity Verification Card) to all staff and deploy a Public Key Infrastructure that will process certificate authentications.

PIV cards are smartcards, their chips contain an authentication certificate. The card allows end users to sign in using certificate authentication and 2 factors (what I have, the card and what I know, the PIN code) which is much stronger than a simple password login. PIV cards are a major tool to secure access to government networks and applications.

Once the PIV cards got deployed, the first objective for federal agencies was to protect desktop and network access with smartcard authentication, instead of the default Windows password. Their long-term objective has been to replace all password login with PIV authentication, starting with sensitive applications and privileged accounts. To that effect, Office of Management Bureau memorandum 11-11 ask that all new systems under development be enabled to use PIV credentials, prior to being made operational.

PIV program implementation

But what about the legacy applications? PIV enabling legacy applications represents a huge undertaking. For some of those applications, especially mainframe systems, the smartcard enablement is simply impossible.

Even for the seemingly simple windows login, switching to smartcard login turned out to be more challenging than it looked. Windows desktops must be configured for mandatory smartcard logon. But this Windows setting has two unfortunate side effects:

1) The end-user Windows password is obfuscated in Active Directory, as a result, all the applications that worked with the Windows password are rendered inoperable.
2) There is no easy solution to grant temporary access to workers who misplace or forget their smartcard.

For some federal agencies, those issues have proved insurmountable for others, PIV implementation is almost achieved but for a few lingering passwords. Whatever the situation, Evidian Authentication Manager has a solution to tackle your issues.

Enterprise Single Sign-On

The indispensable companion for smart card deployment

With Evidian Authentication Management (EAM), Evidian Enterprise SSO and Authentication manager software's from Atos, federal agencies can take full advantage of their smartcard infrastructure. EAM helps its customers enforce smartcard logon, using the native Microsoft authentication system. Smartcard logon compliance is fully audited. With EAM, organizations also extend the security that comes with smartcard logon to most of their applications without having to modify those applications. EAM comes with a safe yet easy solution to unlock workers who lose or forget their smartcards. Thanks to EAM, password security is enforced, yet there are no more passwords to remember, type and change and there is no more password reset calls. Beyond security benefits, EAM boosts smartcard adoption, improve workers' productivity and reduce support costs.

Replacing password log in with a PIV card authentication

Evidian Authentication Manager (EAM) automates the login for legacy and web applications. Once the passwords are collected from end users (in the normal course of their work), they are strengthened and randomized. Those passwords can't be guessed, hacked or fished because they are complex and because the users themselves do not know them anymore. Although EAM still technically delivers password authentication to the applications, those passwords are like tokens and they are encrypted at all time with each user's own PIV card certificate. With EAM, users access all their applications seamlessly after one single PIV card authentication. As for the applications, they have never been modified, thanks to EAM, they have been PIV enabled with minimal efforts.

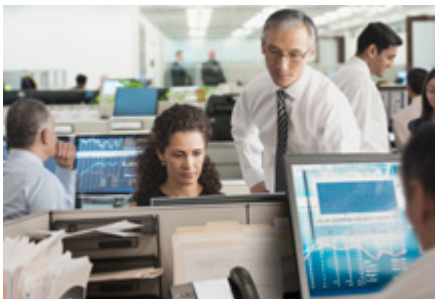
Smartcard Login with EAM

Our solution enforces Smartcard logon without erasing the Windows password. EAM captures and randomizes the Windows password. As a result, the end-user is forced to use the smartcard login. When the end user logs in to an application that request the Windows password, EAM injects the password into the login field and the user seamlessly access the application.

For all the legacy applications (whether or not those applications use the Windows password) the administrator can either let EAM seamlessly do the authentication (SSO authentication) or challenge the user for the PIN code in order to reinforce access security (Re-authentication followed by SSO authentication).

Emergency access when the PIV card is lost or forgotten

We offer an emergency access solution for end-users who misplace or forget their PIV card. The user selects the emergency access option and answer a challenge (Question and answers/ OTP/call to support or a mix of those methods), then EAM issues a temporary password that will last until the PIV card is recovered or reissued. While the user is in emergency access mode, it is up to the administrator to decide which accounts can be accessed and which ones remain locked, as a result, the user can communicate and fulfill most of the daily tasks, but the security standards are not compromised. Our solution issue a report for security administrators which list the users that had to go through emergency access, from this report it is easy to single out users who abuse the emergency access.



Provide reports about PIV enablement

Every single authentication is logged in a central database and the system build reports that outline the percentage of users who utilize the PIV card. Our reporting tool also offers crucial data for accounts management, application deployment and use. It gives management a perfectly clear picture of PIV card enablement and allow you to report progress to the Chief Information Security Officer and the OMB.

Aventex & Evidian partnership

Evidian EAM, the Enterprise Access Management has a long-proven track record helping organizations deploy smart card projects. Evidian EAM is a leader in Enterprise Single Sign On and authentication management. Evidian EAM secures and automates logins for web and legacy applications, it also helps clients replace the default Windows password with 2 factor authentications. Aventex is a New York based consulting firm which resells, and support Evidian EAM in the US and in EMEA. Aventex executives, all former Evidian staffers, have a combined 25 years' experience deploying EAM. Aventex's knowledge of PIV needs for federal agencies combined with Evidian's security expertise and technology creates a strong EAM partnership.
Evidian EAM is an Identity and Access Management product of Atos.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/careers

Let's start a discussion together

For more information: **evidian.com**

CT-200629-RY-J4130-EVIDIAN-BR-BOOSTPIV