Fact Sheet

Cogito Group

Benefits of PIV PACs

What are PIV PACs?

Personal Identity Verification (PIV) tokens are cards that are tied to a specific user through a digital certificate, unlike traditional access tokens which are tied to the user through an external system. Physical Access Control systems (PACs), also known as Electronic Access Control systems (EACs), integrate a wide variety of hardware (card-readers, access cards, door locks, turnstiles, etc) and software (access control servers, identity databases, policy data, control panels, etc), providing organisations with the ability to control people's access to physical facilities.

PIV-based PAC systems are considered to be the most secure available due to their use of certificates and the PKI underpinning them. PKI is the infrastructure needed to create, manage, and distribute digital certificates in a manner which provides ongoing confidence in the security and confidentiality of business solutions leveraging the capability.

Separate Keys for Each Token

PIV tokens each contain a set of four unique keys, ensuring each token is securely unique from all others regardless of batch. Traditional access tokens, on the other hand, will often use the same key across all tokens in a batch, meaning a compromise of any one token exposes all other tokens in the same batch.

The increased security of PIV tokens ensures that if one PIV token is compromised, other PIV tokens are not at risk. This increased level of complexity is one of the many reasons PIV tokens are a key component of the most secure PAC systems in the market.

PIV Tokens as MFA for Logical Access

PIV tokens may be used to provide Multi-Factor Authentication (MFA) for logical access systems. MFA systems enhance their access security by requiring the user to present additional authentication components derived from factors such as something you have, something you know, and something you are. The personal certificate installed on the PIV token provides the 'something you have', whereas a PIN satisfies the 'something you know'.

Benefits of PIV PACs

Fact Sheet

Extends Biometrics

PIV tokens are additionally able to store the biometric data associated with the owner. Biometrics such as fingerprint, iris, and facial recognition data stored on the PIV token allow for biometric matching to be performed and add the third authentication factor of 'something you are' to the MFA process. These authentication challenges are performed within the secure confines of the PIV token to remove the risk of such data being leaked or otherwise intercepted.

Additional Uses for PIV Tokens

PIV tokens extend their practicality by providing a number of additional uses. A token programmed with a PIV application can be used for:

- **PACs Access:** Physical access to an environment, such as passing through doors, gates, turnstiles, etc.
- **LACs Access:** Logical access to an IT system, such as logging in to an application or system.
- Digital Signing: Electronic, encrypted stamps of authentication on emails or electronic documents.
- **Key Management:** Securely storing and controlling important cryptographic keys, allowing encrypted storage on premises or in the cloud.

Replacing Compromised Keys

Two types of traditional access tokens are currently available in the market; proximity tokens, which express a simple number, and basic smart tokens that contain a single asymmetric key and simple identification details.

Proximity tokens express a number that a terminal reads and grants permission to, based upon whether the correct number has been expressed. Devices such as card sniffers can be utilised to capture the number the proximity card is emitting, which can be loaded onto different cards.

Basic smart tokens, which contain a single asymmetric key, express encrypted data to the terminal. This system is more secure than that of the proximity token but is still easy for threat actors to compromise.

A threat actor can capture the data sent from terminal to token and back, which can help in discovering how that data is being encrypted, allowing them to crack the system's cipher. Once this cipher has been cracked, these actors can access all cards within the batch, as they will often use the same master key.

Benefits of PIV PACs

Fact Sheet

PIV PAC systems are difficult to compromise. A compromised PIV token can be identified and replaced without having to impact or update other keys in the batch. 'Jellyfish', Cogito Group's comprehensive cybersecurity platform, can be used to either remotely remove the keys on a missing token, or clear and reissue keys on a retrieved token. This prevents organisations who have suffered a compromise from needing to replace their door readers, systems, software, or entire batches of PIV tokens.

Supports Select Individual Guest Access

PIV PAC systems additionally possess the ability to manage individual user's access across an organisation. As PIV tokens leverage PKI to manage credentials, they can be added to multiple PAC systems with ease. A user's credentials housed on a PIV token can be shared between consenting organisations or government agencies who can individually dictate an individual user's access.

Traditional access tokens do not leverage PKI to manage their credentials, instead utilising symmetric credentials. Symmetric credentials cannot be shared across organisational boundaries, as this would requiring sharing the credentials used by an organisation's entire system, leading to a major compromise.

PIV PACs and Jellyfish

'Jellyfish' by Cogito Group can facilitate and enhance an organisation's use of PIV PAC systems. 'Jellyfish' can:

- Link PAC systems and LAC systems together.
- Register and provision PACs and LACs simultaneously.
- Adjust LACs access rights when PACs change.
- Adjust PACs access rights when LACs change.
- Deprovision LACs when PACs is deprovisioned.
- Deprovision PACs when LACs is deprovisioned.
- Make provisioning more efficient, using sources such as visitor management systems to give the data, name, and photo required secure provisioning.
- Utilise data to determine where people are located in shared buildings, or where an emergency evacuation has occurred.
- Utilise data in shared accommodation to determine where vacant desks may be available.
- Collaborate with other systems such as WIFI access points to create even more organisational benefits.

Benefits of PIV PACs

Fact Sheet

Converging PACs and LACs

Security Benefits

Converged security management can more easily identify and address the vulnerability issues to actively plug those gaps in security.

Operational Benefits

Converged security eliminates the time-consuming need to manage multiple systems, reduces need for auditing, reduces user administration cycle time, and improves risk management productivity.

Financial Benefits

Consolidation of common technologies yields cost savings in productivity as tasks are automated. Convergence also removes the ongoing costs of multiple systems being actively managed and reduces recovery costs from security incidents.

Compliance Benefits

Converged security systems make reporting simpler, by automatically separating report creation, review and analysis.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.