WHITE PAPER

The Convergence of IT Security and Physical Access Control

Using a Single Credential to Secure Access to IT and Physical Resources

Executive Summary

Organizations are increasingly adopting a model in which multiple access control use cases and identities can be supported on a single card or smartphone, thus eliminating the need to remember passwords, or carry multiple cards. This convergence allows smart cards or smartphones manage network and physical access, accessing cloud-based applications, and enables other applications including cashless vending, time and attendance, and secure print management.

There is growing demand for provisioning IT and physical access control system (PACS) credentials to a single card or smartphone, using a single set of processes. Beyond convenience, the convergence of credentials onto a single card or device can greatly improve security and reduce ongoing operational costs. It also centralizes identity and access management, consolidates tasks and enables organizations to quickly and effectively use strong authentication throughout their infrastructure to protect access to all key physical and IT resources.

The new, integrated credential management model moves organizations in four important directions: beyond cards to smartphones; beyond readers to “tap-in” access convenience; beyond Public Key Infrastructure (PKI) technology to simplified solutions for higher security; and beyond legacy PKI to true converged strong authentication access control.

This white paper looks at the drivers, challenges, deployment options and results associated with a converged IT and physical access control solution, and describes the value of a seamless user experience when using cloud-based applications and services, accessing data, and opening doors. It also explains the benefits of unified enrollment processes and workflows spanning multiple identities across multiple IT security applications and the PACS.

Understanding the Drivers for Convergence

Historically, the focus for organizations has been on creating a strong perimeter to secure access to their physical and IT resources. Legacy access control relies on a user presenting an ID badge to gain entry into a building, and once inside, using static passwords to authenticate to IT resources. Given the nature of today’s Advanced Persistent Threats (APTs) and all the internal risks associated with Bring Your Own Device (BYOD) adoption, these methods of securing access are insufficient.

Organizations require the ability to better control access and employ strong authentication throughout their infrastructure as part of their multi-layered security strategy. Unfortunately, choosing an effective strong authentication solution for enterprise data protection has traditionally been difficult. Most available solutions are inadequate in their security capabilities, the costs and complexities they introduce for the organization, or the user experience.

Employees want the convenience of being able to use a single card or mechanism to quickly and easily access the resources they need to conduct business. To accomplish this, organizations must

deploy a solution that can be used to secure access to everything from the door, to data, and to the cloud. They must combine the traditionally separate domains of physical and IT security, and management of users' identities and access into one credential.

The Value of Converged Access Control

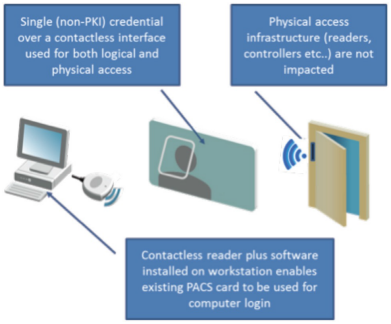
Truly converged access control consists of one security policy, one credential, and one audit log. In some organizations, user management is already fully converged, with a single corporate policy that defines acceptable access and use of resources, a single master user repository, and a single logging tool for simplified reporting and auditing. This approach enables enterprises to:

- Deliver Convenience – replaces one-time password (OTP) tokens and key fobs, negating the need for users to carry multiple devices or re-key OTPs to gain access to all the physical and IT resources they need.
- Improve Security - enables strong authentication throughout the IT infrastructure on key systems and applications (rather than just at the perimeter).
- Reduce Costs – eliminates the need to invest in multiple access solutions, centralizing management and consolidating tasks into a single set of administration and help desk processes around issuance, replacement and revocation.

Exploring Multiple Deployment Options

With a converged access control model, the credential can be delivered in a variety of form factors, such as a smart card (e.g. ID badge) or even a smartphone. Depending on the enterprise's requirements and existing infrastructure, there are several ways to architect the solution. The following are the three most common models:

- **Legacy Contactless**: Enables an existing card-based physical access control system utilizing technologies such as iCLASS Seos®, iCLASS SE®, standard iCLASS®, MIFARE™ and MIFARE DESFire™ to be extended to authenticate to enterprise networks and applications. Software is deployed on the end user's workstation, with a contactless reader connected to or embedded in it. The card can be "read" without needing to be physically inserted into the reader device. This is convenient for users, who can take the same card they have been using with a door reader and tap it to a personal computer or laptop in order to gain access to their computer and to corporate and cloud applications.

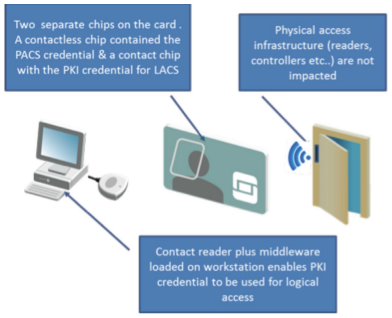


This approach doesn't employ PKI, which binds public keys with user identities through a certificate authority (CA). PKI strong authentication is a key element of logical access, digital document signing and highly secure access control for sensitive areas (i.e. power stations, data storage, nuclear power, water and petrochemical facilities and other critical infrastructure). A digital certificate including the user's public key is placed on a Personal Identification Verification (PIV) card, which leverages smart card and biometric technology (a digitally signed fingerprint template) and also supports multifactor authentication methods. Rather than relying on a shared, secret key for authentication, a pair of public and private keys is used and these keys are linked such that information processed with one key can only be decoded or validated using the other key.

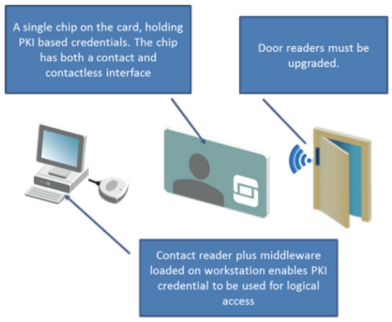
The legacy contactless approach eliminates many of PKI's key management challenges, but it also supports a more limited range of use cases and doesn't deliver the same security strength as PKI-based solutions. The contactless, non-PKI model is being deployed in hospitals, schools and other environments, where multiple users need access to the same workstation in quick succession. It is also being used as a bridging solution where mandates require workstations and applications to be protected by strong authentication.

- **Dual Chip Card:** Embeds a contactless chip for physical access control and a contact chip for logical access control on a single smart card. Credentials, such as PKI certificates and OTP keys, can be managed on the contact chip using a card management system (CMS).

The dual chip card model is popular with medium to large enterprises with sensitive intellectual property (IP) or customer data on their networks, because it delivers strong security. It also enables the enterprise to simplify management of their IT security infrastructure and leverage their existing PACS investments because, in many cases, the CMS can be integrated directly into the PACS management system (often referred to as the PACS head-end).



- **Dual Interface Chip Cards**: Leverages a single PKI-capable chip, with both a contact and contactless interface to support both physical and logical access control. The card can be used to support a contact card reader for logical access use cases, such as logging into a computer or signing an email, and PKI authentication for physical access.



The dual interface card model is applicable primarily in U.S. Federal government organizations. By default, PKI over a contactless interface can be slow for physical access usage. To address this challenge, FIPS 201-2 is expected to allow the use of the Open Protocol for Access Control Identification and Ticketing with privacY (OPACITY) suite of authentication and key agreement protocols that will add roughly four times the performance for critical tasks. It will also deliver secure wireless communications, which enable the use of PIN and biometrics on the contactless interface. This will further strengthen authentication for both physical and logical access control.

Bringing Strong Authentication to the Door

An important benefit of convergence is that it enables enterprises to leverage their existing credential investment to create a fully interoperable, multi-layered security solution across company networks, systems and doors. Strong authentication will increasingly be employed not just for remote access, but also for desktops, key applications, servers, cloud-based systems and facilities. This requires bringing strong authentication to the door.

One of the first places this will occur is in the federal space with users' existing PIV cards. To use a PIV card to enter a building, the PIV card's digital certificates are checked against a Certificate

Revocation List (CRL), which is provided by certificate authorities. PKI authentication is a highly efficient and interoperable method not only for logical access control to protect data, but also for physical access control to protect facilities, the latter referred to as “PKI at the door.”

It is expected that PKI at the door will become more widely adopted as FIPS 201 evolves and there are more products available to support it. There also will be significant opportunities to deploy PKI at the door at lower cost with Commercial Identity Verification (CIV) cards, which are technically similar to PIV cards, but don’t carry the additional requirements associated with being trusted by the federal government. Unlike federal agencies, CIV card users do not have to purchase certificates from a trust anchor or pay annual maintenance fees, but instead generate their own certificates. While the cards will be a little more expensive to accommodate the extra memory for certificate storage, this modest incremental cost will deliver the valuable additional benefits of stronger authentication at the door. Consider the example of a municipal airport, which can use CIV cards alongside sibling PIV cards that are already being carried by federal Transportation Security Administration (TSA) employees. Airport management can create a single access control system that supports both airport employees and federal agencies that are operating there, while ensuring higher security through strong authentication.

Extending strong authentication throughout the physical and logical access control infrastructure will be important to the enterprise. Organizations need a range of authentication methods, along with the flexibility to easily support different users and protect different resources appropriately. With simple-to-use solutions, enterprises can secure access, from managed and unmanaged devices, to an enterprise’s resources. Without having to build or maintain multiple authentication infrastructures, enterprises can use a single solution to secure access to all their resources, from a facility door or copier to a VPN, terminal service or cloud-based application.

What About Mobile?

As we all know, users are increasingly mobile and bringing their own devices (BYOD) into enterprise environments, using smartphones, laptops and tablets to access the resources they need. According to ABI, there will be 7 billion new wireless devices on the network by 2015, which is close to one mobile device per person on the planet.

Organizations are trying to support mobile access, while looking at ways to leverage their users’ mobile devices as platforms for carrying credentials for physical and logical access control. There have already been pilots, such as one with Arizona State University, that has proven the concept of using a smartphone to carry a physical access credential.

Mobile access control requires rethinking how to manage physical access credentials, and make them portable to smartphones so that organizations have the option to use smart cards, mobile devices or both within their PACS. To do this, HID Global has created a new data model for its iCLASS SE® platform called the Secure Identity Object® (SIO®), that can represent many forms of identity information, on any device that has been enabled to work within the secure boundary and central identity-management ecosystem of the company’s Trusted Identity Platform® (TIP). TIP uses a secure communications channel for transferring identity information between validated phones, their SEs, and other secure media and devices. The combination of TIP and SIOs not only improves security, but delivers the flexibility to adapt to future requirements, such as adding new applications to an ID card. It is designed to deliver particularly robust security, and will be especially attractive in a BYOD environment.

With a mobile access control model, any piece of access control data can be supported on a smartphone, including data for access control, cashless payments, biometrics, PC logon and many other applications. The authentication credential will be stored on the mobile device’s SE, and a

cloud-based identity provisioning model will eliminate the risk of credential copying while making it easier to issue temporary credentials, cancel lost or stolen credentials, and monitor and modify security parameters when required. Users will be able to carry a variety of access control credentials, as well as an OTP computer logon token on their smartphone that they simply tap to a personal tablet for authenticating to a network. By combining mobile tokens on a smartphone with cloud application single-sign-on capabilities, it will be possible to blend classic two-factor authentication with streamlined access to multiple cloud applications on a single device that users rarely lose or forget. Plus, the same smartphone can be used for opening doors and many other applications.

There will be challenges to solve since smartphones and other mobile devices being used for physical and logical access control applications will often not belong to the organization.. For example, when a student graduates from a university, he/she doesn't hand their smartphone back, in the same way that employees would hand their cards back when they leave a company. It will be critical to ensure the personal privacy of BYOD users, while protecting the integrity of enterprise data and resources. IT departments won't have the same level of control over personal smartphones used in the workplace, or the potentially untrustworthy personal apps they may carry. IT administrators also are not likely to load a standard image with anti-virus and other protective software onto these smartphones. We will need to find new and innovative ways to address these and other challenges. Notwithstanding the risks, the use of smartphones equipped with SEs, or equivalent protected containers, opens opportunities for powerful new authentication models that leverage the smartphone for securely storing portable credentials, enabling use cases ranging from tap-in strong authentication for remote data access, to entering a building or apartment.

Mobility is driving ongoing convergence, as it forces the physical and IT security teams to work together to come up with a solution. The result can be a solution for easily managing PACS credentials and IT access credentials on smartphones in a cost-effective way, while delivering higher levels of security than cards.

Realizing the Benefits of True Convergence

The ability to combine access control for physical and IT resources on a single device that can be used for multiple applications, improves user convenience while increasing security and reducing deployment and operational costs. It will eliminate the need for separate processes for separately provisioning and enrolling IT and PACS identities. Instead, it will be possible to apply a unified set of workflows to a single set of managed identities for organizational convergence. Organizations will be able to seamlessly secure access to physical buildings and IT resources, such as computers, networks, data and cloud applications. An effective solution will also scale to secure access to other resources, as needed, to support a fully interoperable, multi-layered security strategy that can protect the organization's buildings, networks, systems and applications, now and in the future.

2014-05-13-hid-converged-access-wp-en PLT-01896