Physical & Logical Access Solutions

Platform Approach to Proven Security Convergence
As approaches for physical and logical access increasingly draw on similar technologies, CIOs seek efficient methods to consolidate these two environments to save money and enhance security.

With the evolution of smartcard technology, enterprises can integrate two security environments — physical and logical access — to provide consolidated management, improved ROI and a total security view. Organizations can also deploy a single strong authentication platform to facilitate enrollment, issuance and management, providing further efficiencies.

Access Convergence
An individual maliciously obtaining sensitive information by circumventing an online access point or a thief walking into an enterprise and taking laptops illustrate the same alarming issue — a major lapse in enterprise security. And regardless of the means used to infiltrate an organization, the damage can be significant.

Traditionally, physical and logical access solutions have been the responsibility of two distinct organizations within a company. And each are often managed by two separate administrators and systems.

Multipurpose Credentials
Securing multiple access points — wireless, VPN, desktops and facilities, for example — by relying on separate, often incompatible solutions is expensive, inconvenient for end-users and difficult for administrators to manage. And legacy solutions are typically tied to different suppliers, vendors or contractors.

But advances in smartcard technology have made the convergence of physical access and logical access affordable and simple to deploy.

Platform Approach
Comprehensive physical and logical access is secured by the use of digital certificates, public key infrastructure (PKI) and a proven strong authentication platform.

Entrust is distinct in being able to bring together all of the elements necessary for physical and logical access solutions — on a single software platform — and provide the PKI to issue and manage digital certificates that are deployed to smartcards, mobile devices or USBs and distributed to end-users.

And as a U.S. Federal government-approved provider of PIV and PIV-I credentials, Entrust is an expert in the Personal Identity Verification (PIV) standards that industries and enterprises are adopting to govern their authentication strategies.
Versatile Authentication Platform

By leveraging a software-based platform approach, organizations can consolidate all authentication processes with a single, proven solution — Entrust IdentityGuard.

Whether it’s a smartcard or mobile smart credential for physical/logical access, or a unique grid card for strong authentication to a VPN, Entrust IdentityGuard is one of the most versatile authentication platforms available. It allows organizations to deploy the right authenticator to different user groups based on the amount of associated risk, access requirements, unique user needs and cost.

Entrust’s open API architecture allows for tight integration with today’s leading mobile device management (MDM), identity access management (IAM) and public key infrastructure (PKI) vendors. This enables Entrust IdentityGuard to work with new and existing enterprise implementations, plus adds the ability to integrate in-house or managed service-based digital certificates.

More Information

For more information on Entrust solutions for physical and logical access, contact the Entrust representative in your area at 888.690.2424 or visit entrust.com/physical-logical.

Figure 1: Entrust IdentityGuard leverages smartcards, mobile devices, tokens, digital certificates, biometrics and more to help realize true physical and logical access convergence in any environment.