Entrust®
Securing Digital Identities & Information

EntrustSecurity
@Entrust

Beyond Passwords & Outdated Physical Access Systems

Smart credentials are the best bet for strong physical and logical access security

Get this White Paper

Entrust.com
1-888-690-2424
Entrust@Entrust.com

Entrust®
Securing Digital Identities & Information

Contents

Introduction

In the 1980s, car-theft prevention consisted entirely of locking car doors. A thief with a bent coat hanger could easily bypass a lock and, with rudimentary skills, access the exposed ignition wires, hotwire the starter and drive away.

For modern cars, a bent coat hanger is a waste of time. And, Hollywood depictions to the contrary, modern cars cannot be hotwired.

If your company relies on passwords to prevent unauthorized computer access, or low-tech memory cards (e.g., swipe cards) for facility access, you have security on par with the average 1980s car.

Smart credentials — embedded in plastic smartcards, USB tokens or mobile devices — offer companies advanced and versatile user authentication features.

Smart credentials eliminate the inherent weaknesses and costs of password authentication, and bypass the risk posed by legacy physical card-access systems.

Smart credentials let you provide secure access to computer networks (logical access) and buildings (physical access).The purpose of this white paper is to:

- Discuss the advantages of using smart credentials for multifunction access
- Describe the hardware and software components used in a smart credential environment
- Provide questions to ask when searching for a smart credential solution provider

Advanced smart credentials are crucial for the implementation of physical and logical access systems for enterprises, governments and other security-conscious organizations.

The Trouble with Passwords

Human creativity knows no bounds, especially when it comes to creative malice. There are as many ways to steal passwords as there are ways to protect them.

Password Vulnerability

Password vulnerabilities take on many shapes, from simply peering over a user's shoulder to the more sophisticated options discussed below:

- A Trojan, keylogger or other malware can be passed to the system from a variety of sources, such as email, compromised websites, file-sharing or hacking. With a compromised system, many of these threats then begin collecting usernames and passwords.

- By taking advantage of a breach in building security, a hacker can plug in a low-cost microcontroller hidden in a keyboard or mouse to capture plaintext passwords, hashed passwords and other data.

A relatively newer hacking technique — the use of rainbow tables — occurs offsite, which makes it hard to guard against. It works like this:

- When a computer user sets a password on any system, the password is stored in a hashed format. A hashed format can be thought of as a numerical representation of the plaintext password.

  When a user logs in, the hash of the entered password is compared to the hash of the stored password. If they match, the login is correct.

  It is virtually impossible to "unhash" into the plaintext version. The possible combinations of upper and lowercase letters, numerals and special characters used in a password can number in the billions or trillions. So, it seems safe.

> *A relatively new hacking technique — the use of rainbow tables — is executed offsite, which makes it hard to guard against.*

- Today, any hacker can purchase a multi-terabyte external hard drive on the Internet that's fully loaded with billions of plaintext passwords and their hashed equivalent (i.e., rainbow tables). Alternatively, hackers can download free software to create their own rainbow tables.

- When the hacker gains possession of a hashed password (by means described earlier), it can take minutes to search the rainbow table and find the plaintext equivalent.

- Since the employee has dozens of systems requiring a password outside of the enterprise, they begin to share the passwords across systems. The attacker will go after the weakest link, and reuse that same password for enterprise access.

High Maintenance Costs

Passwords also cause costly maintenance headaches. The best passwords — a long string of upper and lowercase letters, numerals and special characters — are also the easiest for users to forget. Couple that with 30-day password changes, due to the fear of compromise, and the enterprise will realize high password-reset costs.

(For details, see "Business Case.")

The Trouble with Old Physical Access Cards

The majority of physical access systems use 20-year-old technology. They typically have a small numerical value encoded on a chip representing an employee's identity. When placed on or near a card reader, the reader energizes the chip, which then repeatedly broadcasts its specific employee number. The system compares the number to a lookup table. If the number is in the table, access is granted.

Unfortunately, these outdated cards are easily copied. A hacker can place a battery-powered reader in a small suitcase, stroll through a cafeteria or food court, and record every card ID within two to six feet of the case. The IDs can then be copied onto lookalike cards. Vendors have attempted to scramble the number stored on the card, but this does not prevent cloning the card.

It only takes a few minutes to search the Internet to learn how to attack a physical access system. Example search terms include "Indala vulnerabilities" and "Mifare attack." *(See Entrust Blog: "New Attack on Low-Cost Contactless Smartcard" for one example on how to steal access codes.)*

Online videos are often available that provide step-by-step instructions on how to use $50 worth of hardware to crack physical access security systems.

Within the last decade, with the introduction of more powerful chips, vendors started to develop proprietary systems. These systems did not benefit from the worldwide contributions of an open standard. They relied on security through obscurity. Ultimately, these approaches have been successfully attacked.

Even the HID propriety iClass approach, long considered superior security, can be cracked. One online video shows how to clone an iClass card.

Organizations should seek an open physical security standards, such as FIPS-201 (public key infrastructure approach) or Desfire (Symmetric Key Approach), which benefit from worldwide security expert contributions.

***Note**: Mifare, Indala and iClass refer to brand-name chip formats used on access cards.*

The Advantage of Smartcards

Smartcards consist of a powerful CPU and memory. These attributes give them the ability to perform fast cryptographic calculations with sophisticated logic, going well beyond simply broadcasting the contents of its memory. It is replaced by encrypted data exchange between the card and the card reader, along with challenge/response protocols.

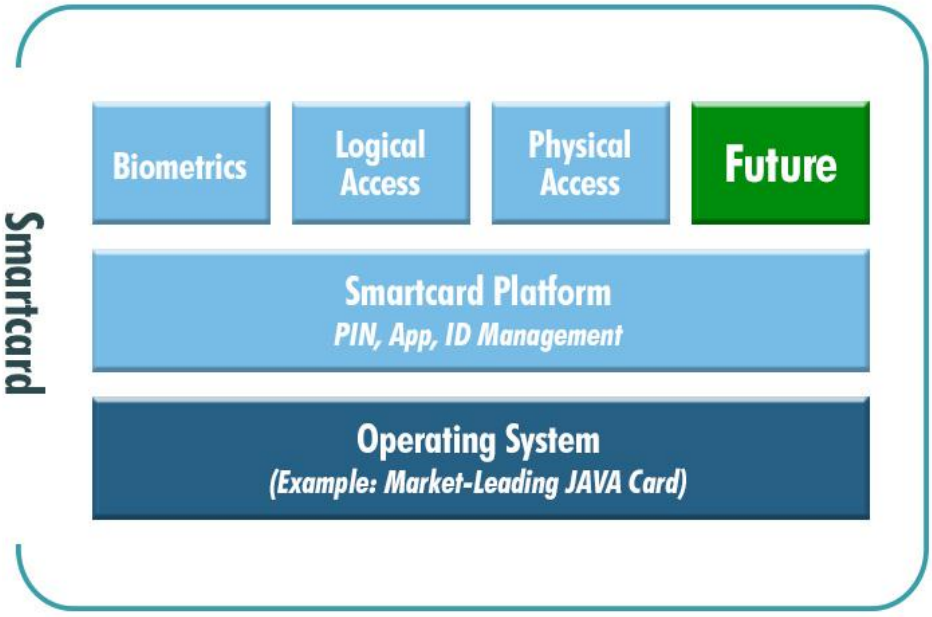

Figure 1: Smartcard architecture has room for features and evolution.

Smartcards eliminate the risks associated with old swipe cards, and provide additional security features, such as replacing passwords for computer access.

Smartcards with embedded smart credentials also include:

- **Tamper-proof data that uniquely identifies an individual.**

  The smartcard holds two types of information representing the owner.

  1. The card holds a public key infrastructure (PKI) private key, which represents the owner. This private key never leaves the chip and is protected by hardware controls. The private key is paired with a public key, which is placed into a digital certificate along with the name of the owner.

     The pubic key and name are cryptographically bound together, and any change can be detected. The certificate is public information and can readily leave the card.

     Whatever the private key does, only the paired public key can verify, and vice-versa. This is the value over a symmetric key approach where everyone has the same key, which greatly increases the risk of being compromised.

  2. The card holds biometric information that represents the owner. The information is digitally signed so any modification will be detected by the reader. This information is used to further identify the owner in the event the card and PIN have been stolen.

     To protect the privacy of the owner, the card will not release private information or perform an authentication function unless authorized by the user entering a numerical or biometric PIN.

- **An app that performs services using that personal data.**

  Services performed can include challenging the card reader to prove it is legitimate, or comparing a fingerprint to the fingerprint stored on the card.

Make sure your card provider has the capability to capture and store biometric data on the smart credential, and allows one or more additional authenticators, such as a grid. The latter can provide additional user-identity assurance when smartcard readers are unavailable.

Replacing Passwords for Logical Access

A smartcard — a micro-chipped plastic card with a photo and optional graphics — performs several tasks. One of its key tasks is serving as a replacement for a password when logging in to a computer, website, VPN or other IT component. How it works:

1. The user places the smartcard into a card reader attached to or embedded in a computer, smartphone or tablet.

2. The reader asks the card to digitally sign a random challenge to prove it holds the private key associated to the identity in the certificate. A random value is used to fight a replay attack. The card signs the challenge if the owner approved it by entering a PIN.

3. The card returns the signed challenge to the reader. The private key is NOT returned.

4. The reader uses the public key, contained in the certificate, to verify the signature.

5. The reader receives the owner name from the certificate associated with the public key and checks to ensure the certificate has not been revoked due to theft or the person is no longer with the enterprise.

Mobile Smart Credentials

Mobile devices are a popular form factor that could complement or replace the physical smartcard. Such devices can act as a smartcard or smart credential. A mobile device may contain a smart credential to log a user in or out of a computer, similar to a smartcard.

- If the device uses near-field communication (NFC), the user brings it within close proximity.
- If the device uses Bluetooth technology, the range of operation greatly increases, making contact unnecessary.

In either case, the computer performs the same process as described above for a physical smartcard reader.

With a smart credential-enabled mobile device, you can configure a computer to lock the screen or log off the user when the user's device moves outside of the NFC or Bluetooth broadcast range.

USB Tokens

USB tokens also can act like a smartcard for logical and physical access. A USB token has the advantage over cards or mobile devices of not requiring the user's computer to have Bluetooth or NFC capabilities, or a physical card reader attached.

User Authentication

With any form factor, the username does not need to be entered, because it is included in the certificate on the card.

- In normal security environments, the user will be required to enter a PIN, like with a bank-machine card. This way, the user authenticates with something they have (e.g., the smartcard and something they know (e.g., PIN).
- In high-security situations, biometric data can be required. This way, the user authenticates with something they have, something they know and something they are (e.g., a fingerprint).

Defending Against Malware

Malware infecting a desktop is difficult to prevent. If malware is installed to a desktop, there is a risk it can steal a PIN to operate the card remotely. Look for solutions that reduce this risk.

- A smartcard allows for a PIN to be entered where it's unseen by the malware. A secure PIN entry device is a card reader that has its own keyboard for both entering the PIN and sending it to the card to permit an operation. The desktop does not ask the keyboard for a PIN, nor does it send it to a card.

  As such, the malware running on the desktop cannot steal the PIN. This also may be accomplished when the smart credential is running on a smartphone. The smart credential uses the phone's keyboard to capture the PIN so it cannot be stolen by the desktop malware.

- Combine logical access with physical access so the card is not left connected unsupervised in the desktop.

- Use a smart credential on the mobile device so the credential leaves the proximity of the desktop when unattended.

Together, the card, PIN and other authentication information eliminate the likelihood of someone logging in with a stolen smartcard. The physical form factor of a smartcard allows the lost or theft to be known earlier, whereas a compromised password may not be detected as quickly, if at all.

Replacing Old Physical Access Cards

A smartcard increases the security of building access. Old-style swipe cards are not secure because they can be copied.

Multifactor identification (e.g., PIN, picture, private key, fingerprint or biometric data) on smartcards lets you scale security to fit your needs and your environment.

For example, a smartcard alone can get someone in the front door, but access to a lab could require a smartcard with a fingerprint.

Older swipe cards broadcast the contents of its memory to a reader. The attack simply reproduces those contents onto a duplicate card purchased on the Internet. The private key on the smartcard cannot be copied and reproduced; the biometric cannot be modified without detection.

The smartcard may challenge a card reader for its digital ID before exchanging information. If the response is invalid, the smartcard does not release its information; this way, the user data cannot be stolen by a rogue reader.

Key Considerations for Smartcard Solutions

The following points are the key considerations before migrating to an advanced smartcard solutions from a trusted security vendor.

Transition to More Secure Physical Access Systems

Moving from an old system to smart credentials in a single leap may be disruptive, but proper planning and the selection of the appropriate solution will minimize inconvenience. It is important to think through migration to minimize problems.

For physical access, ask card suppliers for a two-chip smartcard. One-chip technology is for older legacy card readers. The other is a modern chip compatible with new card readers. This way, you can phase out old card readers and avoid the logistical challenge of replacing all readers at once.

Anatomy of Dual-Interface Smartcards

Long-Life Plastic Construction
Composite plastic, compliant to FIPS-201 standards, for longer life than PVC. Optional poly-carbonate available for laser-engraving.

Security Graphics
Optional protection against counterfeiting; including holograms, microtext, optically variable ink, etc.

Bar Codes/Magnetic Strip
For basic, low-security data storage.

Dual-Interface, High-Frequency Chip
Simultaneous support of physical and logical access. Latest chip and Java Card 3.0 technology increases speed and resistance to attacks and multi-application use. The latest cryptography increases card life.

Programmable, Low-Frequency Chip
For interoperability with a wide range of legacy physical access systems.

Decoupled Antenna
Latest technology decouples antenna from the chip to increase lifespan of dual-interface cards.

Transition to More Secure, Cost-Effective Logical Access Systems

After decades of passwords and one-time passcodes (OTP), it is virtually impossible to switch to smartcards in an instance. Look for a solution that supports legacy authentication solutions and the issuance of smartcards.

This includes common work-flow for issuance, approvals, management, temporary replacement, revocation, reports for annual compliance audits and migration from one authenticator to the next.

Card Management System

As with any type of security authenticator, organizations require software tools to manage user credentials (e.g., adding smart credentials to plastic cards/badges, USB tokens and mobile devices).

Make sure the card management system supports the latest open standards for card authentication. Open standards will:

- Achieve higher security of worldwide reviews and contribution. A propriety solution is only as good as the individual who created it, relying on obscurity for security.
- Allow the enterprise to switch out components of the solution, such as drivers, readers and cards, for the best vendor solution.

Select a solution that supports the latest industry standards, including FIPS-201 and Desfire, along with older technologies that enable smoother transitions. Open standards allow for interoperability with a wide variety of third-party applications and hardware.

Organizations may also need an administration interface to manage users and their smart credentials. Look for:

- Flexible methods built into the core product for distributing smartcard PINs to employees without administration intervention. An integrated self-service module lets users encode their own credentials and report missing credentials.
- A print module to let administrators print smartcards, personalized with graphics, certificates and biometrics, in a fully automated manner. The card is simply mailed to the owner, and the PIN sent out-of-band — all of which is accomplished automatically.

Keeping a physical access system in sync with the cards issued by the card management system can sometimes prove to be an expensive, error-prone project. Look for a vendor that truly integrates the issuance and management of credentials into physical and logical access controls.

Procedures must be implemented to deal with common scenarios (e.g., people forgetting or losing a smartcard). For example, a guard station in your building can supply a temporary card for physical access while also placing the user's recovered encryption key on the card so they can decrypt emails.

Virtual Smartcards on Mobile Devices

Smart credentials encoded in a mobile device can perform the same functions as a smartcard without the need to carry another device. Plus, there is no need to ship the device to the employee.

For example, an executive halfway around the world has forgotten or lost their card. With this approach, a new smart credential may be downloaded to their mobile device and they are back in business in minutes.

Make sure the vendor provides the tools to encode smart credentials on a mobile device. This should include a module that enables employees to set up and maintain their own smart credentials, thus reducing administrative overhead.

Digital Certificates

Once the decision is made to move to smart credentials, determine if there's a need for digital certificates. These are required for authentication, digital signing and encryption.

Several smartcard applications can create and manage keys and/or certificates. Entrust recommends using the FIPS-201 (PIV) standard. It guarantees privacy of the holder's personal information and biometrics, FIPS-201 interworks with a wide variety of applications and hardware (e.g., operating systems, browses, WYSE terminals, physical access systems, full-disk encryption products, etc.).

To generate digital IDs, organizations need access to a certification authority (CA). Companies or governments may install their own. If they lack the resources to manage an on-premise CA, look for a vendor that also offers a managed/hosted certificate service offering.

Understanding the PIV Standard

The FIPS-201 standard — often called Personal Identity Verification — comes in three types based on the type of certificate issued for the user.

1. The standard PIV system supports a common smartcard-based platform for identity authentication and access to multiple types of physical and logical access environments. FIPS-201 standardizes the digital certificates and biometrics that describe the cardholder, and how the outside world interacts with the data stored on the card.

2. PIV-Interworking (PIV-I) enables organizations to provide credentials for employees who need to perform trusted transactions with the U.S. federal government. When the digital certificates are issued from a CA trusted by the federal government, and issued in a manner following federal identity proofing policies, the cardholder identity is trusted by government systems and users.

3. Commercial Identity Verification (CIV) takes advantage of the FIPS-201 standard, but the certificate issuance does not need to follow U.S. government policies. This approach will be prevalent within U.S. non-government organizations, as well as organizations outside of the U.S. Organizations benefit from proven security and interoperability with third-party equipment, but are free to establish their own identity-proofing policies.

What's PIV?

The Personal Identity Verification (PIV) system is a direct result of FIPS 201, a requirement by the NIST that specifies architecture and technical requirements for a common identification standard for U.S. government employees and contractors.

The PIV system supports a common smartcard-based platform for identity authentication and access to multiple types of physical and logical access environments.

Building Access

To use smart credentials for building access, organizations need to install physical devices designed to read smart credentials. For maximum flexibility, choose a vendor that can integrate with the major building access manufacturers.

Also ensure the vendor does not require unique card stock for each building system utilized within an enterprise or the need to purchase a separate physical access card personalization system. Select a solution that uses a flexible card platform that's personalized during issuance, not during card manufacturing.

Partner with a trusted security vendor that offers the expertise to recommend the make and model of the system to install. Seek a solution that offers cards that will work with legacy physical access system while allowing for seamless migration to the new, more secure system, without disruption. You may then migrate as time and resources permit.

Capable security vendors also maintain labs where they test the interoperability of smartcards with a wide variety of leading physical access vendors to help ensure an error-free deployment.

Security Compliance Advantage

Smartcard PIV technology is key to conforming to security-conscious government departments and agencies worldwide. Some examples include:

- The FBI's Criminal Justice Information Systems (CJIS) Security Policy for second-factor authentication to access the criminal database
- Standards set by the North American Electric Reliability Corporation (NERC)
- The U.S. First Responder Authentication Credential (FRAC) for emergency services adopted by U.S. federal and state organizations
- Online information exchange security requirements facing healthcare professionals through the U.S. Nationwide Health Information Network (NHIN)

For authentication that complies with these and other emerging security standards, select a smartcard vendor that provides Federal Bridge Certification Authority (FBCA) certificates or publicly trusted certificates.

Interpol, like many governments and law enforcement agencies, leverage high-security multipurpose smartcards to properly authenticate and verify identities for authorized access.

Table 2 — PIV Card Types & Requirements

Industry Name	Card Plastic & Graphics Layout	Card's Applet	Process to Issue Card with Certificates	Digital Certificate Source
PIV	FIPS-201	FIPS-201 Compliant	Defined by Federal Common Policy	CA Cross-Certified to Federal Common Policy
PIV-Interworking (PIV-I)	FIPS-201	FIPS-201 Compliant	Defined by Federal Bridge CA	CA Cross-Certified to the Federal Bridge CA
PIV-compatible or Commercial Identity Verification (PIV-C or CIV)	Customer Choice	FIPS-201 Extended Per Customer Choice	Customer Choice	Any Other CA

Business Case

While advanced security is a top priority, the move to physical or virtual smartcards may actually pay for itself in administrative savings.

As an example, the PIN used with a smartcard is easier to remember than a password. A PIN does not need to be replaced every 60 to 90 days like a password because authentication requires two factors: the smartcard (i.e., something the user has) and the PIN (i.e., something the user knows). How often do you change your credit card PIN?

Passwords as authenticators represent a hidden expense that can grow quickly over time.

For example, a major North American car manufacturer annually shuts down for retooling. Upon returning to work, 10 percent of employees forget their passwords. When 10 percent of 100,000 employees need a new password at $70 each — the low end of the cost range — it could amount to as much as $700,000.

The cost of help-desk operators and the downtime of employees waiting for passwords amount to a huge monetary hit each year. When selecting a new solution, calculate the effort spent on changing and resetting passwords.

Additional Smartcard Benefits

- *Reduce the loss of intellectual property due to a logical or physical attack*
- *Reduce the loss of private data due to employees' failure to secure a desktop when leaving the workplace*

Summary

Passwords alone provide a weak defense against computer intrusion. Outdated physical access cards are more of a nuisance than an obstacle to a determined intruder. Smart credentials provide a robust, proven and sophisticated new technology to secure logical and physical access.

Traditionally, physical access provided just authorized admission to buildings, while logical access provided access to computers and networks. With Entrust, you can have one platform that does both.

Software-Based Authentication: Entrust IdentityGuard

Entrust's flagship authentication solution, Entrust IdentityGuard, continues to lead the industry as one of the most robust software authentication platforms, delivering scalability, reliability and the most diverse set of authenticators supported on the market today.

Entrust IdentityGuard serves as organizations' single comprehensive software-based authentication platform, while concurrently bridging them to emerging technologies for strong mobility, cloud and credentialing offerings.

Physical & Logical Access

Entrust IdentityGuard provides a new standard for physical and logical access control for effective enterprise authentication. This integrated platform approach simplifies the issuance and management of smartcards and certificates, leveraging industry standards such as PIV — all from a single trusted vendor.

Mobile Smart Credentials

Entrust IdentityGuard Mobile Smart Credentials transform a mobile device into a virtual smartcard, eliminating the need for physical smartcards or hardware-based one-time passcodes (OTP).

The mobile smart credential is more convenient, easier to use, less expensive to deploy and provides support for a number of authentication and information protection needs within an organization.

Entrust Mobile Smart Credentials may be leveraged to solve a wide array of use-cases:

- Physical access to facilities
- Logical access to computers, networks and applications
- Digital-signing of forms, documents and emails
- Encryption of email and information

Want to Learn More?

*Visit **entrust.com/physical-logical** to discover how a single authentication platform can be deployed to solve organization's physical, logical and mobile access security challenges.*

More Authentication Choices

The software authentication platform enables organizations to layer security — according to access requirements or risk — across diverse users and applications.

Entrust's authentication capabilities include smartcards and USB tokens, soft tokens, grid cards and eGrids, IP-geolocation, questions and answers, mobile smart credentials, out-of-band one-time passcode (delivered via voice, SMS or email), and a range of one-time-passcode tokens.

Easy Integration

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.

Industry Standards & Support

Entrust IdentityGuard supports more than a dozen types of popular and innovation authenticators. Centralized policy allows the controlled co-existence and transition between authenticators from a single management console.

Entrust IdentityGuard also supports the latest industry standards, FIPS-201 and Desfire, along with older technologies to enable a smooth transition. While Entrust does provide the entire solution to save customers the pain of individual product integration, our standards-use allows for components to be swapped out as desired.

Entrust IdentityGuard provides an optional module, ID-SYNC, that will automatically instruct the physical access control system when a card is issued or deleted. The solution will replicate this information to all systems the enterprise is using worldwide.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries.

Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

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.**

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on twitter tweet