A Practical Approach to Authentication in an Evolving Enterprise Environment

Multilayered security via strong authentication, access convergence and identity management
Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional.

ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NONINFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© 2012 Entrust. All rights reserved.
Table of Contents

The Changing Enterprise Authentication Environment .................................................. 4
Beyond the Single Authenticator................................................................. 5
The Mobile Workplace ........................................................................... 5
Password Vulnerability ........................................................................... 7
  Trojans, Keyloggers & Malware ............................................................ 7
  Physical Breach .................................................................................... 7
  Rainbow Tables .................................................................................... 7
Opportunity for Secure Access Convergence... 8
Regulatory Requirements, Remote Workers & Reducing Costs ..................................................... 9
The Facts on Authentication Factors ................. 10
Demystifying the Top Authentication Methods ......................................................... 11
Selection Criteria for Enterprise Authentication .................................................... 15
Entrust Solutions for Enterprise Authentication ..................................................... 17
Extending the Security Investment ............... 19
  Logical Access Control...................................................................... 19
  Physical Access Control................................................................... 19
  Combined Physical & Logical Access Control..................................... 20
  Secure Collaboration......................................................................... 20
Industry Accolades .............................................................................. 22
Entrust & You ...................................................................................... 23
The Changing Enterprise Authentication Environment

Enterprise authentication used to be simple: passwords for everyone, expensive tokens for a small number who work remotely.

While the demand for strong authentication has extended beyond traditional users, technologies also are emerging that present organizations with new opportunities to improve security, while reducing operating costs.

Mobile or remote employees — the traditional user base for stronger authentication — are commonplace at all levels in all industries.

In addition, the growth of mobile devices and smartcard technology is increasingly playing a role in the development of an organization’s security strategy. Mobile devices enable organizations to leverage a very flexible, convenient and low-cost method for authentication.

Organizations also may leverage smartcard technology to consolidate two security environments: physical and logical access. Once the responsibility of two distinct organizations within a company, combining physical and logical access solutions provides these organizations consolidated management, improved ROI and a total security view.

By leveraging a platform approach to authentication, businesses can broaden their security deployment, provide flexibility for employees and partners, while achieving operating efficiencies.

Whether it’s a smartcard for physical and logical access, soft tokens on a mobile device, or a unique grid card for strong authentication to a VPN, organizations can consolidate all authentication processes with a single, proven solution.
Beyond the Single Authenticator

When a limited community of users with the same basic requirements needed additional protection, a single authenticator such as tokens, though traditionally expensive and sometimes hard to manage, was a reasonable solution.

The authentication requirements of users within an organization now may vary depending on a number of factors, including the level of security required, their usability needs and experience, and where and how they are accessing the network.

Organizations are urged to consider the importance of a software authentication platform that offers a range of authentication options that can be matched to different users based on policy and risk assessment. This allows user identities to be verified via an authentication type that is appropriate for the transactions they conduct and any associated risk.

The Mobile Workplace

The growth of mobile devices is changing the landscape for enterprise authentication. A 2012 Forrester report highlighted that “64 percent of enterprises in North America and Europe are focused on bolstering mobility support for employees, partners and customers” — up from 48 percent just two years ago.¹

And a May 2012 survey by Morgan Stanley found that “purchase intentions indicate tablet shipments will increase to 133 million and 216 million in 2012 and 2013” — growth that is more than 57 percent and 112 percent, respectively, than the firm’s initial estimates in 2011.²

It is a trend that Barclays analyst Ben Reitzes has termed “the consumerization of IT” in which the pattern of consumer adoption of mobile platforms (e.g., iPhone, iPad) is driving behavior within the enterprise.³

Consumerization is the catalyst for CIOs and IT decision-makers prioritizing mobile security in the enterprise. In fact, improving or implementing mobile security ranked highest (see results on page 6) in Forrester’s 2012 survey of large enterprises in North America and Europe.


The (tablet) market is even bigger and growing faster than we initially forecast.

— Morgan Stanley
May 2012
As mobile devices are used increasingly to access corporate networks, enterprise authentication strategies must take consider how users can strongly authenticate to the network with these devices.

At the same time, the proliferation of such devices provides IT organizations with a simple platform for authentication, using soft tokens that can be deployed easily to a mobile device.

This approach dramatically reduces obstacles that have traditionally made enterprise-wide deployment of physical one-time-passcode (OTP) tokens impractical.

---

### “What are your firm’s top mobile priorities during the next 12 months?”

<table>
<thead>
<tr>
<th>Priority</th>
<th>High Priority</th>
<th>Critical Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement/improve mobile security</td>
<td>46%</td>
<td>22%</td>
</tr>
<tr>
<td>Implement a comprehensive corporate mobile strategy</td>
<td>42%</td>
<td>14%</td>
</tr>
<tr>
<td>Support more Internet-connected smartphones</td>
<td>44%</td>
<td>11%</td>
</tr>
<tr>
<td>Support connected touchscreen tablets or slates</td>
<td>42%</td>
<td>10%</td>
</tr>
<tr>
<td>Provide more mobile support for out-of-office users</td>
<td>42%</td>
<td>10%</td>
</tr>
<tr>
<td>Implement a mobile device management solution</td>
<td>34%</td>
<td>14%</td>
</tr>
<tr>
<td>Provide more mobile support for employees in the office</td>
<td>37%</td>
<td>8%</td>
</tr>
<tr>
<td>Provide more mobile support for customers</td>
<td>33%</td>
<td>11%</td>
</tr>
<tr>
<td>Provide more support for employee-owned devices</td>
<td>32%</td>
<td>6%</td>
</tr>
<tr>
<td>Provide more mobile support for partners and suppliers</td>
<td>22%</td>
<td>4%</td>
</tr>
<tr>
<td>Use some/more third-party services for mobility management</td>
<td>21%</td>
<td>3%</td>
</tr>
<tr>
<td>Hire IT staff with mobile app and support skills</td>
<td>18%</td>
<td>3%</td>
</tr>
<tr>
<td>Implement a corporate mobile app store</td>
<td>15%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Base: 576 North American and European mobile decision-makers at enterprises (1,000+)

Source: Forrester Research, Inc.
Password Vulnerability

Password vulnerabilities take on many shapes, from simply peering over a user’s shoulder to the more sophisticated techniques. The most popular techniques to illegally obtain passwords include malware, physical breach and rainbow tables.

Trojans, Keyloggers & Malware

These techniques are often passed to the system from a variety of sources, such as email, compromised websites, file-sharing or hacking. After compromising a system, many of these threats begin collecting usernames and passwords.

Physical Breach

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.

Rainbow Tables

A relatively new hacking technique — the use of rainbow tables — increases the threat even further. 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.

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.
Opportunity for Secure Access Convergence

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.

Easy for the end-user and more efficient for organizations, this convergence enables everything from credentialing, secure access to facilities, strong authentication to desktops and network resources, and digital signature capabilities — all via a single smartcard credential.

Comprehensive physical and logical access is secured by the use of digital certificates, public key infrastructure and a proven strong authentication platform. Some organizations often require an end-to-end solution, which can include data capture, design, vetting, personalization, printing and issuance.

The push toward coupling physical and logical access security not only consolidates efforts, it saves money and reduces the burden on end-users.

This approach means there’s only one card to carry, one PIN to remember and only one process for authenticating users who “left their card at home.” End-user acceptance helps reduce cost and unburdens help desks.
A Balancing Act: Regulatory Requirements, Remote Workers & Reducing Costs

The boundaries of the corporate network are being challenged as more employees need access wherever they are. Extranets, intranets, Web mail and now, more than ever, desktops need strong authentication as they are being accessed from beyond the boundaries of the corporate network.

This increasing pressure to make more information available to employees anywhere, at any time, must be balanced with increasing pressure for corporate and regulatory compliance.

From the PCI-DSS (Payment Card Industry Data Security Standard) to SOX (Sarbanes-Oxley Public Company Accounting and Investor Protection Act) and HIPAA (Health Insurance Portability and Accountability Act), most organizations have or are rolling out new practices to achieve regulatory compliance.

Simple passwords, even for users operating exclusively internally, are no longer enough to prevent breaches, protect privacy and achieve compliance. Strong authentication must be deployed to a wider audience — efficiently and cost-effectively.

Looking at enterprise authentication as a whole, the flexibility to secure different users and their connectivity using different and appropriate authentication methods is critical. Using risk assessment and policy to determine when stronger security is required for access to resources with greater value allows authentication to be layered as needed.

A software authentication platform used across VPN remote access, Microsoft desktop and Web implementations can provide a suitable, cost-effective and easier way to manage enterprise authentication — and can evolve as requirements change.
The Facts on Authentication Factors

Authentication factors are independent ways to establish identity and privileges. They play a key role in helping to determine that you are who you say you are. Authentication methods can involve up to three factors:

- **Knowledge**: Something the user knows
  (password, PIN)
- **Possession**: Something the user has
  (ATM card, smartcard, mobile smart credential)
- **Attribute**: Something the user is
  (biometric, fingerprint, retinal scan)

Adding factors of authentication adds security and can help limit vulnerability to identity attacks. Properly designed and implemented strong authentication methods can offer stronger breach prevention with minimal user impact.

Traditionally, organizations have relied on simple usernames and passwords, combined with business processes, to manage risk. Risks have significantly increased as mobile workforces access the corporate network from remote locations and identity attacks have become more common.

Now, breaches occur more often, brands are impacted by fraud incidents and important regulations have been implemented to help protect users and information. These issues have made the necessity of multifactor authentication increasingly apparent.
Demystifying the Top Authentication Methods

As part of an identity-based security approach, the wide variety of authentication options available today can help increase security for specific activities and user communities.

A number have proven themselves to be very effective for enterprise authentication, including:

- Biometrics
- User-Based Public Key Infrastructure
- Smartcards
- Mobile Smart Credentials
  *(digital credentials embedded on smartphones)*
- Soft Tokens
- Physical Tokens
  *(OTP hardware, display cards)*
- Grid Cards

There are also several alternative risk-based methods that play an increasing role in enterprise authentication:

- Machine Authentication
- Knowledge-Based Authentication
- Out-of-Band Authentication
- IP-Geolocation

These authentication methods, which have broad acceptance in the enterprise market, are detailed on the following pages.
<table>
<thead>
<tr>
<th>Authenticator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td>Biometrics measure and analyze human physical characteristics — such as fingerprints, eye retinas and irises — and facial patterns to identify users. Because they can be expensive and difficult to manage, they are typically not very cost-effective for most large-scale enterprise deployments.</td>
</tr>
<tr>
<td>User-Based Public Key Infrastructure (PKI)</td>
<td>Powerful in-house or hosted PKI models allow organizations to establish and maintain a trustworthy environment by providing certificates that secure many off-the-shelf applications using encryption, digital signatures and strong certificate authentication. These solutions enable enterprises to control access to resources, prevent theft of information and comply with regulations.</td>
</tr>
<tr>
<td>Smartcards</td>
<td>Because smartcards provide portable, two-factor protection for digital credentials, they are a versatile option for enterprises considering convergence of physical and logical access security. The same card that is used for controlling access to a building (or locations within a building) can be used for logical access, whether it is network sign-on, remote access, etc.</td>
</tr>
</tbody>
</table>
| Mobile Smart Credentials              | Taking advantage of near-field communication (NFC) and Bluetooth standards, mobile smart credentials embed digital certificates on smartphones to create trusted identity credentials for stronger, more convenient enterprise authentication. This transforms a mobile device into an efficient, cost-effective smartcard.  
Always on hand, these multipurpose credentials securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data. |
<table>
<thead>
<tr>
<th>Authenticator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Soft Tokens</strong></td>
<td>One-time-passcode (OTP) tokens are generated on mobile devices or laptops, enabling organizations to leverage devices for strong authentication that are already widely deployed within an organization. This makes for a convenient, cost-effective way to roll-out strong authentication to a broader base of an organization’s staff. Digital identities, such as those powered by a PKI, also provide benefits of second-factor authentication, without having to deploy a physical OTP. Digital certificates provide an advantage of extensibility to other functions, beyond authentication, such as encryption and digital signatures.</td>
</tr>
<tr>
<td><strong>Physical Tokens</strong></td>
<td>One of the original second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number OTP tokens, USB tokens and even credit card-sized tokens. Physical tokens traditionally have been relatively expensive to deploy, manage and maintain. New platform approaches to authentication have simplified the management complexity and reduced OTP token prices. Tokens can be used very effectively in combination with other authentication methods to provide organizations-wide coverage based on user risk profiles.</td>
</tr>
<tr>
<td><strong>Grid Cards</strong></td>
<td>Security grid cards can provide strong second-factor protection via a card that’s issued to each user. Users are asked to enter characters from the grid at login. Inexpensive to produce and deploy, and easy to use and support, these highly intuitive cards have a very high success rate in the enterprise. Grid cards can be produced and distributed in a number of ways, including a credit card-like format in thin plastic, paper and even virtually for electronic storage.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Risk-Based Authentication</strong></td>
<td>These non-invasive methods use a combination of techniques that are transparent to the user and only ask for additional authentication from the user when the defined criteria are not met. These transparent methods may include:</td>
</tr>
<tr>
<td><strong>Machine Authentication</strong></td>
<td>This non-invasive method of strengthening user authentication stores and validates a “fingerprint” of a registered machine. The fingerprint consists of a variety of elements gathered from the user’s machine such as the operating system, screen resolution, browser type or even IP address. The stored machine fingerprint is compared with information gathered from the machine when a user attempts to log in. This method does not require any user interaction beyond initially registering the machine and can be very cost effective to deploy.</td>
</tr>
<tr>
<td><strong>IP-Geolocation</strong></td>
<td>Authenticated users can register locations where they frequently access the corporate network. During subsequent authentications, the server compares their current location data — including country, region, city, ISP, latitude and longitude — to those previously registered. Organizations only need to “step up” authentication when the values don’t match. Organizations can create blacklists of regions, countries or IPs based on fraud histories. They can even leverage an open fraud intelligence network to receive updated lists of known fraudulent IPs based on independent professional analysis.</td>
</tr>
<tr>
<td><strong>Knowledge-Based Authentication (KBA)</strong></td>
<td>When using risk-based authentication, knowledge-based authentication is employed when the risk criteria are not met. This intuitive method of authentication uses challenge questions and answers to provide strong authentication. This enhances authentication without the need to deploy anything physical to the end-user.</td>
</tr>
</tbody>
</table>
## Selection Criteria for Enterprise Authentication

With such a broad range of authentication methods available, selecting the appropriate solution can be daunting. When comparing authentication options, a solution that provides multifactor authentication methods from a single administration and management platform provides the most flexibility and allows organizations to match the appropriate authentication method with the user risk profile.

Assess key criteria when evaluating a strong authentication solution for the enterprise:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>There are two critical components to total cost of ownership: purchase cost and operating cost. Be sure to thoroughly evaluate both the up-front purchase costs and the costs over the lifetime of the deployment, including device replacement, management and renewal costs. Lower total cost allows the deployment of strong authentication to more users for the same amount of budget dollars, extending the security coverage.</td>
</tr>
<tr>
<td><strong>Usability</strong></td>
<td>Not all users are the same and not all user environments are created equal. When choosing authentication methods, consider the user’s technical capabilities; ease-of-use considerations (e.g., desk vs. car) and environmental conditions (e.g., user likely to get wet, dirty, etc.). No matter what the authentication method or deployment plan, new authentication methods should not fundamentally change the way employees are accustomed to working. Choose a system that can follow existing user-interaction models and minimize the need for additional technology knowledge for employees.</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Invest in a platform with multiple authentication options that allow companies to match the authentication method to the risk profile of the user. Investing in systems that provide only certain authentication methods ignores the inevitable need to make changes and enhancements to authentication over time. Choose a platform that addresses all needs now and can grow and change as requirements evolve.</td>
</tr>
</tbody>
</table>
Assess key criteria when evaluating a strong authentication solution for the enterprise:

<table>
<thead>
<tr>
<th>Integration</th>
<th>Security Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication is one part of an identity-based security model. Choose a platform that is integrated with key enterprise applications, including:</td>
<td></td>
</tr>
</tbody>
</table>

- Leading VPN remote access vendors, such as NetMotion, Cisco, Check Point and Juniper
- Standard Microsoft Windows client
- Web services and leading applications like Microsoft Outlook Web Access or SharePoint

Choose a company that is an established security leader with a trusted reputation and focused dedication to assist in determining the proper balance between security requirements, budget and usability for the company’s unique situation.
Entrust Solutions for Enterprise Authentication

Entrust’s comprehensive suite of identity-based security solutions are designed to help enterprises and other organizations deploy comprehensive identity management and cost-effective strong authentication to secure users with different needs, in different locations, with varying risk profiles.

**Entrust IdentityGuard**

Entrust's software authentication platform enables identity-based security to safeguard access to sensitive information, secure facilities, protected networks and more.

While harnessing the power of existing end-user devices as authenticators for physical, logical and cloud application access provides clear value, Entrust's comprehensive authentication platform also integrates with existing IT systems and business processes for unmatched deployment versatility.

With the flexibility to be co-deployed alongside outgoing legacy systems, Entrust's platform bridges emerging technologies for strong mobility, cloud and smart credentialing offerings.

The solution enables organizations to layer security — according to access requirements or the risk of a given transaction — across diverse users and applications.
Entrust's diverse set of authentication capabilities include user-based public key infrastructure (PKI), smartcards (plastic and mobile), software tokens, hardware tokens, grid cards and eGrids, risk-based authentication (e.g., machine, IP-geolocation, knowledge-based), out-of-band one-time passcode (delivered via voice, SMS or email), out-of-band transaction verification and a range of OTP tokens.

Offering the broadest range of authenticators in the market, Entrust's software authentication platform is often leveraged to solve challenges related to specific use cases.

The Entrust-patented grid card is a credit card-sized authenticator consisting of numbers and characters in a row-column format. Upon login, users are presented with a coordinate challenge and must respond with the information in the corresponding cells from the unique grid card they possess.
Extending the Security Investment

In an economy where budgets and resources are constantly under pressure, organizations cannot afford to buy single-purpose solutions.

Entrust's platform approach to strong authentication allows organizations to leverage their existing investment to increase security and productivity in other areas.

**Logical Access Control**

Entrust solutions authenticate individuals prior to accessing sensitive computer networks, a method commonly known as secure logical access control (LAC).

Entrust supports a broad range of user authentication methods including physical (e.g., a one-time-passcode token or grid card), mobile- and smartcard-based, or online (e.g., passwords plus questions and answers).

This allows organizations to deploy authentication methods that will ensure strong authentication of the user, be convenient and simple for the individual to use, and meet the budgetary requirements of the organization.

**Physical Access Control**

Entrust authentication solutions integrate with physical access control (PAC) systems to ensure only authorized individuals have physical access to buildings, server rooms, etc.

Employming the latest technology, Entrust captures user information, encodes it on the latest standards-based chip technology and ensures user information remains secure and tamper-proof on the device while communicating with the PAC system.

For physical access control to permanent or virtual borders, Entrust PKI capabilities provide tamper-proof credentials for citizens based on International Civil Aviation Organization (ICAO) Basic Access Control (BAC) and Extended Access Control (EAC) international standards.
**Combined Physical & Logical Access Control**

Entrust solutions allow organizations to consolidate physical and logical access control with a uniform user identity that is managed via a single comprehensive software platform.

This provides the user with the convenience of a single authenticator while consolidating management, improving the return on investment and providing a stronger security position.

**Secure Collaboration**

The critical exchange of sensitive intelligence — whether within a single enterprise or across the globe — must be executed securely and in a timely manner to protect the integrity of the information.

Entrust secure collaboration solutions provide the ability to share and communicate information securely between individuals and groups.

Sensitive information related to a particular project may be automatically encrypted and stored in secure folders. Only current authorized participants in the project can unencrypt, read and add to folder contents, even if access to the folder is compromised. Folder and content access is audited for regulatory compliance.

Entrust provides the ability to communicate sensitive information securely between individuals, regardless of whether the organization is using an in-house email system or leveraging a commercial email system (e.g., Gmail). In fact, communicating individuals do not even require an existing relationship.

The information may be encrypted — preventing unauthorized reading of the text — either by the individual at the time of sending or automatically before it leaves the organization. This facilitates the secure, free flow of information that is critical to efficient business practices.
Entrust IdentityGuard provides strong authentication for applications, including:

- Remote access (secure IPSEC and SSL VPN provided from leading vendors, including NetMotion, Cisco, Check Point, Citrix, Juniper and Avaintail)
- Native Microsoft® Windows® desktop application integration
- Leading Web applications like Microsoft® Outlook Web Access
- Smartcard management, including physical and logical access
- Mobile authentication on smartphone platforms (e.g., Google Android, RIM BlackBerry, Apple iOS, Symbian, Windows Mobile)
- Multifactor options for diverse user groups for any environment (e.g., grid cards, physical tokens, mobile devices or smartcards)

Entrust IdentityGuard Helps:

- Issue, vet and manage all digital identities within an organization — and all from a single software authentication platform
- Simplify migration from outgoing legacy systems via advanced co-deployment capabilities
- Streamline administration with central policy management that can help decrease the risk of policy inconsistency
- Integrate with existing IT systems and business processes for unmatched deployment versatility
- Enable compliance to industry regulations such as HIPAA, CJIS and SOX
- Harness the power of existing end-user mobile devices as authenticators for physical, logical and cloud application access
- Prepare for what comes next thanks to a standard-based architecture and open platform committed to adding new and innovative authentication options
Entrust IdentityGuard — Industry Accolades

- Winner of “Best Buy” award for top authentication platform (five-star rating), SC Magazine, January 2011
- Winner of “Best Buy” award for top authentication platform (five-star rating), SC Magazine, January 2010
- Finalist of “Best Security Solution” in the 24th Annual SIIA CODiE Awards, January 2009
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 about Entrust products and services, call 888-690-2424, email entrust@entrust.com or visit entrust.com/authentication.

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