A Practical Approach to Authentication in an Evolving Enterprise Environment

Better security via versatile authentication, convergence and mobile devices

March 2011
Table of Contents

Current State of Enterprise Authentication 1
A Balancing Act: Regulatory Requirements, Remote Workers & Reducing Costs 4
The Facts on Factors of Authentication 5
Demystifying the Top Authentication Methods 6
Selection Criteria for Enterprise Authentication 9
Entrust’s Identity-Based Approach 10
Regulatory Overview 12
Strong Authentication Secures Enterprise Identities 13
Enterprise Authentication — Industry Accolades 14
Entrust & You 15
Current State of Enterprise Authentication

The changing environment for enterprise authentication

Enterprise authentication used to be simple: passwords for everyone, expensive tokens for a small number who work remotely. But today, authentication requirements are changing. While the demand for strong authentication has extended beyond traditional users, technologies are also 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. 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. But that small community of users who need more than password protection has ballooned.

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 can begin leveraging 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 the platform approach, 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. But today 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 versatile 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 2010 Forrester study highlighted that 48 percent of enterprises were planning to invest in mobile applications to their employees.

While 70 percent of enterprises support BlackBerry devices, the iPhone and Android platforms are gradually establishing their mark — 29 percent of organizations now support the former, and 13 percent support the latter.

And a February 2011 survey by Morgan Stanley found that more than 50 percent of large enterprises expect to purchase tablets for employees through 2011 and into 2012.

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.

Around 75% of organizations deploy mobile applications to increase worker productivity, and 65% to increase employee responsiveness. Forty-eight percent are focused on resolving customer and internal issues faster.

Tim Sheedy
Forrester Research
“Insights for CIOs: Make Mobility Standard Business Practice”
September 3, 2010

---

2 Ibid.
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.

**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 anytime, 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 versatile 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.

Ant Allan
Gartner Research
“MarketScope for Enterprise Broad-Portfolio Authentication Vendors”
September 17, 2010

“... few enterprises can meet the needs of all use cases with a single authentication method, because the trade-offs in authentication strength, total cost of ownership, ease of use and so on lead to unnecessary loss of flexibility in some cases and inappropriately high levels of risk in others.”

www.entrust.com
**The Facts on Factors of Authentication**

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, smart card)

**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 username 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:

- Physical tokens (OTP hardware, display cards)
- Security grid cards
- Soft tokens
- Digital certificates
- Smart cards, typically for physical and logical access
- Biometrics

There are also several new methods that are playing 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.
One of the first second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number one-time-passcode (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 reduced the management complexity and significantly reduced the price of OTP tokens to the $5 range. Tokens can be used very effectively in combination with other authentication methods to provide company-wide coverage based on the risk profile of the users.

<table>
<thead>
<tr>
<th>Authenticator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Tokens</td>
<td>One of the first second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number one-time-passcode (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 reduced the management complexity and significantly reduced the price of OTP tokens to the $5 range. Tokens can be used very effectively in combination with other authentication methods to provide company-wide coverage based on the risk profile of the users.</td>
</tr>
<tr>
<td>Grid Cards</td>
<td>Security grid cards can provide strong second-factor protection using a grid card 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>Soft Tokens</td>
<td>OTP tokens can be generated on mobile devices or laptops, enabling organizations to leverage devices for strong authentication that are already widely deployed within the enterprise. This makes for a convenient, cost-effective way to roll-out strong authentication to a broader base of an organization’s employees that is simple for users to adopt. Digital identities, such as those powered by a PKI, can 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>Smart Cards</td>
<td>Because smart cards provide portable, two-factor protection for digital credentials, they are a versatile option for enterprises that are 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 or the like.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<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>Machine Authentication</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>Knowledge-Based Authentication</td>
<td>This intuitive method of authentication uses challenge questions and answers to provide strong authentication. This method enhances authentication without the need to deploy anything physical to the end user.</td>
</tr>
<tr>
<td>Out-of-Band Authentication</td>
<td>Out-of-band user authentication leverages an independent means to communicate with the user beyond the primary communication channel. Using a different medium such as a cell phone, PDA or home phone, an independent authentication challenge can be delivered to the user. Out-of-band user authentication can be a cost-effective, user-friendly option since existing devices that users have can be leveraged, eliminating the need for the deployment of new or additional devices.</td>
</tr>
<tr>
<td>IP-Geolocation</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>
</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 an enterprise versatile authentication solution:

| Cost | 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. |
| Usability | 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. |
| Flexibility | 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 does not consider 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 over time. |
| Integration | Authentication is one part of an identity-based security model. Choose a platform that is integrated with key enterprise applications, including:  
  - Leading IP-SEC and SSL VPN remote access vendors, such as Cisco, Check Point, Nortel and Juniper using the Radius standard to ensure rapid, consistent integration across remote-access products  
  - Standard Microsoft Windows client  
  - Web services and leading applications like Microsoft Outlook Web Access |
Entrust’s Identity-Based Approach

Core to an identity-based security strategy, the Entrust IdentityGuard versatile authentication platform is a common-sense approach to strong authentication, enabling companies to apply the right level of strong authentication tailored to the risk associated with a user, access requirements or transaction type.

Entrust IdentityGuard integrates into existing environments to provide a range of cost-effective authentication options that can be implemented as required without the need to deploy expensive hardware or force significant changes to the user experience.

The range of authentication includes device authentication, security grids, knowledge-based, OTP tokens and display cards, out-of-band or mobile authentication along with mutual authentication to validate the Web site to the user.

And each authenticator is easy to use with minimal impact to the end-user experience. Organizations can choose how they want to authenticate the identities of their users depending on user type, access requirements, risk or the application being used.

Assess key criteria when evaluating an enterprise versatile authentication solution:

<table>
<thead>
<tr>
<th>Security Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selecting the appropriate technology and vendor to provide a versatile authentication platform is always a difficult task. Ensuring that an organization selects the appropriate vendor for an enterprise will require an assessment of the vendor’s solution to determine if it is able to addresses individual authentication requirements now and as requirements change in the future.</td>
</tr>
</tbody>
</table>

Figure 1: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today

www.entrust.com
Entrust IdentityGuard provides strong authentication for applications, including:

- Remote access (secure IPSEC and SSL VPN provided from leading vendors, including Cisco, Check Point, Citrix, Nortel, Juniper and Avaintail)
- Native Microsoft® Windows® desktop application integration
- Leading Web applications like Microsoft® Outlook Web Access
- Smart card management, including physical and logical access
- Mobile authentication on smartphone platforms (e.g. Google Android, RIM BlackBerry, Apple iOS, Symbian, Windows Mobile)

Entrust IdentityGuard helps:

- Manage cost and complexity with a single versatile authentication platform that provides a range of strong authentication methods as part of a layered security approach
- Streamline administration with central policy management that can help decrease the risk of policy inconsistency
- Be ready for what comes next thanks to a standard-based architecture and open platform committed to adding new and innovative authentication options
Regulatory Overview

HIPAA
The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, seeks to protect the privacy and the security of health information. The HIPAA Security Standard covers the safeguards that should be implemented to protect electronic patient information. Organizations must ensure that private health information is protected both at rest and in transit. Multifactor authentication can play an important role in protecting health information by restricting who has access to that information.

PCI
In response to member, merchant and service provider feedback on the need for a single approach to stronger information security for all card brands, credit card companies collaborated in creating common industry security requirements known as the Payment Card Industry (PCI) Data Security Standard. Compliance with the PCI Data Security Standard is a requirement for all merchants or service providers that store, process or transmit cardholder data.

Password-based authentication or single-factor authentication to critical enterprise resources can leave networks and data exposed to unnecessary risk and compromise compliance to PCI requirements. Multifactor authentication provides additional security to help verify that only authorized individuals access this information.

SOX
The Public Company Accounting Reform and Investor Protection Act — known as the Sarbanes-Oxley Act (SOX) — is legislation intended to help reform accounting practices, financial disclosures and corporate governance of public companies. The SOX guidance suggests that organizations need to focus on reviewing the accuracy of financial information and the reliability of systems that generate it. Under the SOX guidelines, companies must demonstrate system and application integrity for tools used to generate financial reports. Verifying and restricting access to financial systems is a critical component of providing strong IT security for financial data.
The European Union’s Data Protection Directive

The EU Data Protection directive (DPD) has two main purposes: to protect personal privacy and to standardize privacy regulations across member nations. Unlike many North American laws, the EU DPD is very specific in its requirements of the transfer of personal information to countries deemed not to have strong enough data protection policies, including the United States.

American organizations must apply for safe harbor and comply with strict requirements that demonstrate they have the policies and practices in place to protect personal data. These requirements include stringent security practices to protect against loss, destruction, unauthorized access or misuse of personal information.

Strong Authentication Secures Enterprise Identities

As the pressure to comply with regulatory requirements combines with the large number of users working outside the boundaries of the corporation, the need for strong authentication for large portions of an employee community has never been greater.

Organizations need stronger forms of authentication that are easy to use and less costly to purchase, deploy and maintain than traditional “one-size-fits-all” options.

Entrust IdentityGuard addresses this need by providing an open versatile authentication platform, enabling organizations to increase security and help prevent the risk of potential breaches and attacks on digital identities.

Core to an identity-based security approach, the solution provides organizations with strong authentication capabilities that can be deployed to a wider audience, with greater control and flexibility in determining how to secure different users and transactions.
Enterprise Authentication — 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

---

Product Rating

<table>
<thead>
<tr>
<th>Feature</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Ease of Use</td>
<td>★★★★★ ★</td>
</tr>
<tr>
<td>Performance</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Documentation</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Support</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Value for Money</td>
<td>★★★★★</td>
</tr>
<tr>
<td>Overall Rating</td>
<td>★★★★★</td>
</tr>
</tbody>
</table>

For: Full offering, well priced.
Against: Did not find any.
Verdict: With all the options supported, this solution delivers true, layered multifactor identity and authentication management. We give this our Best Buy.
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.

Entrust's identity-based solutions empower enterprises, consumers, citizens and websites in more than 4,000 organizations spanning 60 countries. This identity-based approach offers the right balance between affordability, expertise and service.

For strong authentication, fraud detection, digital certificates, SSL and PKI, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.