



Securing What's at Risk:
A Common Sense Approach to Protecting Users Online

July 2008

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, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

1	Introduction	1
2	The Threat to Online Identity.....	1
3	Entrust IdentityGuard — Versatile Authentication Platform	6
4	Flexible, Risk-Based Security	12
5	Easy to Use, Low Cost to Deploy	13
6	Architecture and Integration	15
7	Conclusion.....	16
8	About Entrust	16

1 Introduction

The Internet has created significant opportunities for organizations to move processes online, benefiting both from the delivery of new services as well as the reduction of costs versus traditional transactions. However, with this opportunity also comes inherent risk — especially in the absence of appropriate security to protect the identities of users online.

Even today, organizations are still experiencing a rapid increase in the incidence of online identity attacks. Typical attacks to perpetrate these crimes include phishing, man-in-the-middle and malware, and result in the rapid increase of online user identities being stolen at an alarming rate. As reported in February 2007, financial institutions were the targets of 92.6 percent¹ of all online phishing attacks.

These attacks are a risk to organizations not only because of the financial losses but, more importantly, they undermine user confidence in online services — preventing organizations from fully realizing the savings from online transactions compared to the traditional phone-based or brick-and-mortar channels.

Taking steps to increase protection of user identities is becoming an imperative for any organization that wants to continue leveraging the Internet to extend services to customers. This whitepaper will explore these issues and offer innovative new tools for combating the threat of online identity fraud.

2 The Threat to Online Identity

Organizations are relying on the Internet more heavily today than ever before to reach their customers and partners. For the Internet-savvy customer, it provides a more convenient way of accessing services and performing transactions. For the organization, it can translate into a competitive advantage as well as delivering significant cost savings versus traditional phone-based and brick-and-mortar transaction methods. Further, in a multi-channel environment, online services can help increase customer retention by being an effective way of delivering new products and services.

At the core of performing online transactions is the need for mutually recognized identities. Users need to feel confident that they are transacting with the intended organization. Likewise, the organization needs to have confidence in the identity of the user. Without this mutual trust, online transactions cannot be completed without significant risk of misrepresentation and fraud. In the past, username and password authentication has been deemed sufficient to meet the needs of many online transactions. However, the rapid increase in online identity-related fraud shows that passwords alone can no longer counter the ever-increasing sophistication of online identity attacks.

Rapid Increase in Identity Attacks

Identity-related online attacks such as account hijacking are amongst the world's fastest-growing crimes. In one example, Gartner reported that in the 12 months leading up to August 2006, almost 15 million Americans were victimized by some type of identity-theft-related fraud.² In addition, fraud losses increased to \$49.3 billion in 2006.³

Compromise of a user's online identity can allow an attacker to gain access to a victim's online accounts, including their bank account. Once access to the victim's bank account has been

¹ "Phishing Activity Trends Report," Anti-Phishing Work Group, February 2007

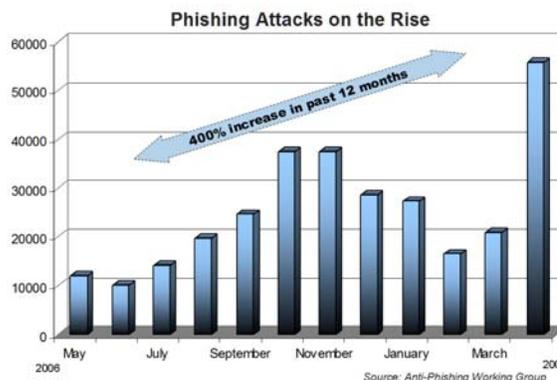
² "The Truth Behind Identity Theft Numbers," Gartner, Avivah Litan, February 2007

³ "2007 Identity Fraud Report," Javelin Strategy & Research

gained, criminals will typically transfer funds from the account, as well as acquire more personal information to perpetrate further crimes. This type of identity fraud is alarming since the perpetrator need not reside in the same region as the victim, nor have access to any physical documentation. From virtually anywhere in the world, thieves need only trick a user into surrendering their password and the rest becomes a simple process of executing online fraud.

Even though stronger authentication policies are becoming commonplace, reliance on simple passwords in the majority of online transactions allows identity fraud to continue to thrive. Two major forms of online identity attacks clearly demonstrate the frailty of password-only authentication schemes. Phishing and man-in-the-middle attacks rely on the use of “spoofed” e-mail messages and other techniques to direct users to fraudulent Web sites where their online credentials (i.e., passwords) are stolen. By fooling victims into divulging their usernames and passwords, attackers can gain access to the victims’ accounts. Malware attacks use different, more invasive techniques to steal the user’s identity, but the end results are the same.

Phishing attacks are accomplished by counterfeiting the trusted brands of well-known banks, online retailers and credit card companies in e-mails to potential victims. These e-mail messages prompt users to go to fraudulent Web sites where the user is tricked into submitting a valid username and password into what appears to be a legitimate log-in page. Attackers are typically able to convince significant numbers of recipients to respond — subsequently giving up identity information that can be used to access personal information at the real bank, retailer or credit company. Attackers are thus “fishing” — or phishing — for online identities.



Malware attacks use several mechanisms to install malicious code on the victim’s computer. Typical methods include e-mail messages or Web sites where the user is tricked into running attached or downloaded code, as well as attacks that exploit known weaknesses in the operating system or browser to install the malware. Once installed, common attacks include recording keystrokes (commonly referred to as a keyboard logger) and mouse movements that lead to the capture of user names and passwords. These are transmitted surreptitiously to the attacker who then uses it for account hijacking. More sophisticated attacks even perform fraudulent transactions during the user’s online session.

Man-in-the-middle attacks occur when a fraudster attempts to intercept communications between two parties, such as a customer and a financial organization, without their knowledge. By doing so, the attacker becomes the “man in the middle.” Both parties are unaware of the attacker’s presence. So, acting as a proxy, the attacker can both review and manipulate the contents of the messages he is relaying between the two parties. This method gives the criminal access to personal information, passwords and usernames without either party suspecting a breach.

All these attacks are made possible due to the inherent weaknesses in password-based, single-factor authentication. Once an online thief observes the user’s name and password, he has all he needs to access the victim’s online account. Unlike traditional forms of identity theft (such as dumpster diving), an online attack can come from anywhere in the world and only needs to reach a small percentage of users to result in the compromise of a significant number of user identities.

Most online organizations provide some — or in the case of retail banks, complete — reimbursement for losses from these types of attacks. This leads to significant cost to these organizations. This alone provides a valid business rationale for addressing the issue immediately. However, this is not the most significant impact or risk from online identity fraud.

Loss of Consumer Confidence is Hindering Adoption

Attacks are increasing and they are impacting consumer confidence and online adoption. In addition, the losses incurred by users have increased by more than 100 percent year over year. As online identity attacks have become more prevalent, a significant number of users have decreased or even discontinued online transactions.

It is inevitable that users will continue to be less willing to take the risk of using online services without better protection of their online identity. This leaves organizations subject to two negative impacts:

- Increasing direct costs of attacks that drive directly to the corporate bottom line
- Limited online service use, impacting both costs and revenue generation

"The average loss in 2005 was \$1,408; in 2006, it climbed to \$3,257. At the same time, the percentage of funds consumers managed to recover dropped from 87% to 61%."

Source: Gartner "The Truth Behind Identity Theft Numbers," Avivah Litan, Feb. 27, 2007

At the same time, there is a significant reward for organizations that address this issue and provide their users with better protection of their online identity, based both on retaining existing customers, as well as having them transact more business in the cost-effective online world.

Increasing Regulatory Pressures

Given the impact to online adoption, pressure from government agencies and industry bodies is increasing. With online service delivery representing a productivity and competitive advantage for all organizations, any significant threat to adoption raises the issue's visibility within legislative and regulatory bodies. With the visibility has come increasing guidance, especially to the banking industry. Global regulations that have been introduced focused on important fraud prevention techniques and best practices include examples like:

- The United States banking community's FFIEC guidance highlights the need for increased online user protection, leveraging authentication and real-time fraud detection.
- The United Kingdom's Faster Payments Initiative (FPI) will speed the processing of financial transactions to clear in seconds versus days, making the need to ensure a valid user is enacting the transaction critical.
- The European Union's Payment Services Directive provides the legal and technical framework for all electronic payments in the EU and transfers responsibility for the prevention of fraud to the payment services providers.

Representing only a subset of what exists today and what is planned for the near future, these regulations provide yet another incentive for organizations to act.

Countering the Threat

There are three key areas to be considered in countering online identity fraud:

- **Detection.** Specifically, monitoring the Internet environment to quickly detect online identity attacks. This typically involves both online monitoring to detect phishing, malware and man-in-the-middle attacks, as well as real-time transaction monitoring on the organization's Web site. Both are important for developing a rapid response to halt an attack and reduce its impact.
- **Response.** Once detection has occurred it is important to quickly act to shut down the fraudulent site being used to phish for user identity information. Likewise, many organizations will want to post notifications on their own Web sites of the attack to provide a warning to all users. Typically this is done in conjunction with the ISP community.
- **Mitigation.** Reducing the impact of an attack when it does occur is one of the most important steps in reducing losses — both financial and in user confidence. In the past, mitigation has also been one of the most challenging in terms of devising an approach that can be successfully implemented.

There are many potential activities and solutions to be considered within a comprehensive response. However, in terms of prioritized action, authoritative sources have consistently recommended that online organizations focus on strengthening mutual authentication. This includes the Federal Financial Institutions Examination Council (FFIEC), who, in 2006, recommend upgrading existing password-based, single-factor customer authentication systems to two-factor authentication, and the Financial Services Technology Consortium who recommend financial institutions investigate and adopt better mutual authentication practices. It is expected that many other regulatory bodies will recommend similar measures over time, extending even beyond the financial services industry.

These recommendations are a result of organizations having to face the reality that attackers can respond very quickly to detection and response techniques that attempt to stop them. However, mutual authentication can help inoculate the user against attacks by increasing the ability to detect fraudulent Web sites and strengthening their online credentials, making them more difficult for an attacker to successfully steal.

Versatile Authentication

Improving online security through the use of versatile authentication solutions can provide a significant defense against the various forms of online identity attacks. However, security must be balanced against the real-life implementation considerations of retail-scale applications that deal with potentially millions of customers. If a particular approach provides improved security but is cumbersome to use or unaffordable to deploy, then it defeats its own purpose. Being difficult to use will lead to users either bypassing the mechanism or electing not to perform the online transaction. Being too expensive will lead to organizations not being able to afford to protect users' online identities.

"A versatile authentication server (VAS) is a common enterprise infrastructure supporting multiple open and proprietary authentication methods. This approach enables an enterprise to use different forms of authentication depending on who is logging in, where the login is taking place and for what purpose. A VAS also gives an enterprise a simple means of migrating to new authentication methods as its needs change and new methods emerge."

Source: Gartner "Token Price Obscures the True Value of Entrust Offering" Ant Allan & Ray Wagner Feb. 2, 2007

This suggests criteria for evaluating effective strong versatile authentication techniques that include the following:

- **Strong Security.** Current password mechanisms are weak in that an attacker need only capture the password to obtain a user's online identity. Authentication solutions must provide mechanisms to determine the authenticity of the Web site being accessed, as well as provide the user's online identity better protection by providing an additional factor for authentication beyond the password.
- **Flexible, Risk-Based.** Stronger authentication solutions now leverage risk assessment to determine the appropriate level of authentication. For example, a user checking their account balance from home has a different risk profile than attempting an interbank transfer from a foreign country. Online organizations must be able to choose from a variety of versatile authentication methods that best align with the risk of a given transaction. This also allows authentication to be only as invasive as required by the risk to improve user acceptance.
- **Easy to Use.** User acceptance is a critical success factor for any security solution. If a particular approach is too cumbersome or confusing, users, especially in the consumer domain, will either turn to expensive alternative channels or disengage completely. Both of these outcomes negate any potential positive impact from improved security.
- **Easy and Low Cost to Deploy.** Many security approaches have been developed to meet the needs of the enterprise and its employees. As such, they do not reflect the financial realities of deploying to a large, diverse customer population. Any feasible solution must be affordable to deploy to millions of users, including fitting easily into existing infrastructures.

Without addressing these considerations, any mutual and strong authentication solution risks not being effective at protecting online identities and restoring customer confidence in online services.

3 Entrust IdentityGuard — Versatile Authentication Platform

To meet the mutual authentication needs of online organizations, Entrust IdentityGuard provides a flexible platform of strong, versatile authentication capabilities. It allows organizations to layer authentication based on their assessment of a transaction's risk profile and individual user preferences. Each authentication method is designed to be easy use and be delivered at a fraction of the cost of traditional time-synchronous hardware tokens.

Layered Authentication

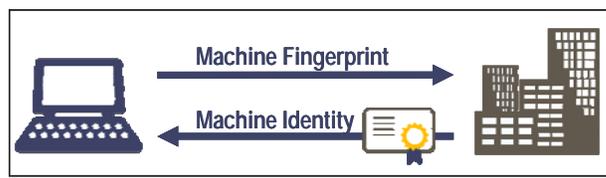
Preventing online identity fraud can be accomplished by employing a separate factor in the authentication process above and beyond the user's password. Often this additional factor is something the user has, in addition to something the user knows (e.g., their password). This prevents the user from unwittingly submitting their complete identity to, for example, a fraudulent Web site. Even if the attacker obtains the user's password, they will not have the physical factor of authentication and, thus, be prevented from accessing the user's account.

With Entrust IdentityGuard, the user continues to employ their current username and password but is also provided with additional factors of authentication. In order to meet a variety of user preferences, as well as respond to different assessments of risk, a comprehensive set of authentication methods are provided. The power of Entrust IdentityGuard is that it allows organizations to layer one or more authentication options required to address risk, with many options not requiring any hardware or software deployment.



Machine Authentication: Machine authentication provides validation of the user's computer in a way that secures against a variety of threats while minimizing user impact. This is an especially attractive method where users typically access their account from a regular set of machines, allowing for authentication to be performed without any noticeable impact to the user experience.

To establish the identity of a user's computer, first a fingerprint of the user's machine is generated and securely stored by Entrust IdentityGuard. This fingerprint is based on a configurable set of machine parameters that can be transparently read from the user's computer. Once this fingerprint is obtained, a machine identity reference is generated and stored on the machine for future authentication. This machine registration process is similarly performed for all computers the user wishes to register.



During subsequent logins, the machine identity can be transparently retrieved and authenticated. In addition, the machine fingerprint is recalculated and compared to that stored for that machine.



Entrust IdentityGuard's machine authentication thus provides protection for users even if they have had their passwords stolen by attackers. Because an attacker would not be using the stolen credentials from the user's machine, the machine authentication would fail and the attacker rendered unable to obtain access.

It is recognized that, from time to time, users may access accounts from computers that they do not typically use. In these cases, Entrust IdentityGuard provides the ability for organizations to still allow the user to proceed and includes the option to use other forms of authentication or limit which transactions the user can perform from that machine.

The machine authentication mechanism is designed to be resistant to attack. First, the machine identity can only be accessed by the legitimate Web site using built-in protection mechanisms in the Web browser. Further, even if a very sophisticated malware application is able to capture the machine identity and try to use it from another machine, the machine fingerprints will likely fail to match. In addition, Entrust IdentityGuard embeds optional sequence information that prevents an attacker from later using the machine identity.

Knowledge-Based Authentication:

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge them to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets," this allows the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process or based on previous transactions or relationships.

For example, during enrolment the user may select and provide answers to easily remembered questions, such as Year of Birth?, Place of Birth?, Favorite Pet?, etc. These questions are relatively easy to remember.

In addition, questions can be drawn from previous user interactions with the organization. These have the advantage of being harder for attackers to harvest through other information sources.

Examples include: *What was the balance on your last statement? How often do you make mortgage payments?*

Entrust IdentityGuard allows organizations to select a number of shared secrets for each user and prompt for all or a subset to increase user authentication strength. By maintaining a larger set, organizations can select a subset that makes it more difficult for an attacker to gather impersonating information based on previous authentications.

With this type of authentication, deployment experience is as important as technology. Entrust has extensive experience in deploying knowledge-based authentication for customers with user

Additional Authentication

To ensure your identity is protected while accessing from this workstation, it is requested you answer the following questions:

Where did you first go to high school?
(drop-down list)

What was the name of your first pet?
(drop-down list)

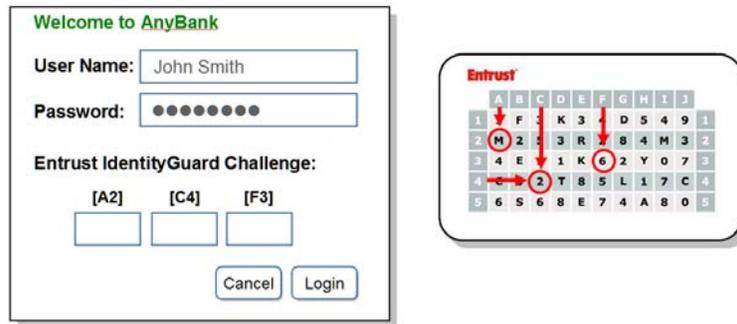
populations of more than one million. Combined with a proven deployment record, Entrust IdentityGuard is an ideal choice for successful deployments.

Grid Authentication: With grid authentication, an additional factor is deployed to the user based on an assortment of characters in a row/column format printed on a card. This innovative authentication method has been recognized by a patent awarded by the U.S. Patent and Trade Office.

The actual format of the card is very flexible. Cell contents could be numeric, alphanumeric, etc., depending on the application requirements. Likewise, the actual number of grid locations is flexible. The key element is that each user has a randomly generated set of grid contents that will be used during authentication — which is now two-factor authentication.

To authenticate, the user would employ their username and password as they do today. But, in addition, the user would receive a coordinate challenge used to demonstrate they are in possession of the appropriate card.

For example, if the user was to be challenged for grid coordinates A2, C4 and F3, the response would be generated as follows:



Similar to a map location or table look up, the user would respond with the contents in the grid cells that correspond to the challenge coordinates. In this example, the user would enter the grid cell contents for locations A2, C4, and F3 — "M," "2," and "6." For each subsequent login, a different random challenge would be generated and the user prompted for the appropriate response.

Using grid authentication, the susceptibility to phishing, man-in-the-middle or malware attacks is substantially reduced. Even if the user is subject to repeated attacks, the large number of potential challenges and responses for any given user significantly reduces the effectiveness of these attacks. Attacks that record several logins will only be exposed to a small portion of the authentication grid. In addition, with the ability to layer other authentication capabilities or transaction monitoring with Entrust TransactionGuard, a zero-touch fraud detection solution, Entrust can enable organizations to effectively combat these ongoing attacks.

To provide for consistent strong security, users could be periodically reissued replacement cards. For example, after a few years of use, a new card would be generated for a given user and distributed. As there is no requirement for specialized hardware distribution, it is cost effective to replace these cards periodically to maintain security.

One-Time-Password List: An alternative to deploying a grid for authentication is the use of a one-time-password (OTP) list. With this approach, end-users are provisioned with a list of

randomly generated passwords that are typically printed on a sheet of paper that is distributed to and carried by the end-user.

Subsequent to the deployment of the OTP list, users are prompted to enter one of the passwords. This can be done during account login, in addition to the user's normal username and password, or when performing a specific transaction as shown in the example below.

To reduce susceptibility to phishing, man-in-the-middle or malware attacks, which OTP to be prompted for is randomly generated and is used only one time, as the name suggests. This renders the OTP useless should it be captured by an attacker. To help the user remember this, they can be counseled to strike used passwords from the list or special "scratch cards" can be employed that reveal the OTP once a covering layer is scratched off.

The fact that sheets must be replenished after all OTPs have been consumed can mean relatively frequent issuance for active users. In addition, organizations must monitor usage in order to replenish passwords before all of the passwords on a current card are used. For these reasons, management of this authentication method can be more intensive than for grid authentication. However, for organizations currently using this method of authentication, this allows current users to continue to use the method to which they are accustomed. In addition, the ability to layer other authentication options over this type of authentication (such as machine authentication) can help to thwart several attacks that have been perpetrated in the past.

Transfer Confirmation

You are attempting to transfer €10,000. Please confirm by entering the following transaction code:

00005: _____

Remember that you will not be asked for this code again. It is recommended you physically strike it from your code sheet as a reminder.

Number	One Time Password
00001	A 3 U D S T 2 3
00002	7 5 G R K Y F Z
00003	H 5 D I 9 7 D C
00004	G H G T 5 R 4 E
.....
00029	O S F 3 W L M O
00030	L B G 6 2 L M Z

Out-of-Band Authentication: One of the challenges of online authentication is that it relies on the same channel of communication as the transaction itself. Out-of-band authentication leverages an independent means to communicate with the user to protect against attacks that have compromised the primary channel.

This is a very effective means of guarding against man-in-the-middle attacks where a legitimate online session may be used to piggy-back fraudulent transactions. Out-of-band authentication is also very convenient as it can leverage channels that already exist and are easy to access for customers. These include voice calls to a telephone, SMS to a mobile phone or e-mail to a computer or mobile device. All allow the user to confirm a particular transaction using a channel already registered with the organization.

Entrust IdentityGuard supports this capability by allowing for the generation of one-time confirmation numbers that can be transmitted along with a transaction summary to the user. This can be done directly via e-mail or SMS, or sent through voice to a registered phone number. Once the confirmation number has been received, it is simply entered by the user and the transaction is approved.



One-Time-Password Tokens: One-time-password (OTP) tokens are a proven and accepted way of strongly authenticating users via a second factor of authentication. Convenient and relatively small, they provide strong security in a portable form factor. They have primarily been deployed in enterprise environments, as tokens have traditionally been cost-prohibitive for large-scale deployments. Most tokens that have been deployed to date also use proprietary algorithms for the generation and validation of one-time passwords, although the inception of OATH has changed the playing field for newer deployments.

Entrust recently changed the industry for OTP tokens by introducing a low-cost, highly reliable token that works as another authenticator on the Entrust IdentityGuard versatile authentication platform. The Entrust IdentityGuard Mini Token is a high-quality, one-time-password device designed to help provide strong, versatile authentication to enterprises, governments and consumers. The token offers easy-to-use, time- and event-synchronous capabilities that can be deployed alone, or in a layered strategy, in combination with other authentication methods as part of the Entrust IdentityGuard versatile authentication platform. The Entrust IdentityGuard Mini Token delivers security and reliability without the traditional high price.



Entrust offers multiple options for token-based authentication, including OATH and 3DES-based tokens, giving deploying organizations a choice on how they want to strongly authenticate users.

Mutual Authentication

With one or a combination of any of the versatile authentication methods provided by Entrust IdentityGuard, organizations can reduce the risk of online fraud in a way that the organization feels best fits the user experience. However, additional protection needs to be provided to help users from inadvertently providing personal information to fraudulent Web sites.

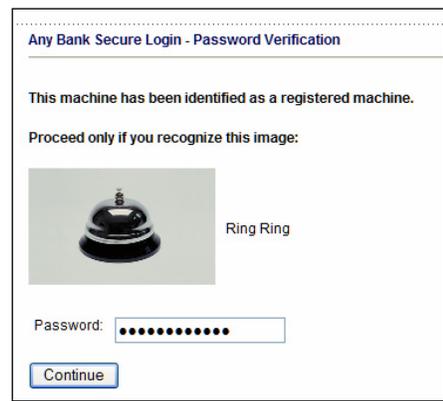
This is especially true given the ever-increasing rates of phishing, including very sophisticated attacks that can direct users to fraudulent sites, even if the user enters the correct URL. This reinforces that organizations must provide easy-to-use tools to authenticate the Web site to users. Mutual authentication methods are designed to do just this by providing information that users can employ to confirm they are on the legitimate Web site. Entrust provides organizations with a range of options for mutually authenticating with their customers, enabling organizations to deploy in ways that they feel best fit into the user experience, including:

- Image Replay
- Message Replay
- Grid Serial Number Replay
- Grid Location Replay
- Extended Validation (EV) SSL Certificates

Each method is designed to replay identifiable information to the user that could only come from the legitimate organization itself, enabling users to quickly and easily confirm the Web site is authentic.

Image and Message Replay

One method of mutual authentication supported by Entrust IdentityGuard is image and message replay. In this case, as part of the registration process, a user selects an image and message that is later shown to them during login. By personalizing the login with the image and message, the user recognizes that only the legitimate site is able to replay



this information before entering sensitive information like their password.

Whether the user picks a picture from an online collection or uploads one of their own, it will be familiar and, thus, easier to recognize when it is not there.

If a phishing site attempts to capture sensitive user information including their password, the user is likely to notice the absence of this personalization information and abandon the Web session.

Grid Serial and Location Replay

Grid authentication not only provides a secure, low-cost and easy way to authenticate users — it also provides built-in mechanisms for mutual authentication.

Given the objective for the authenticating organization to show the user some information that only it and the user could know, the grid provides two options. The first is based on the serial number of the grid itself. As shown in examples earlier, each grid has a unique serial number that is known only to the issuer and the user. As such, during login, this can be displayed to the user before prompting for user authentication.

Before entering their password or grid challenge response, the user simply confirms that the serial number displayed on the Web site matches the one on their grid card. If it does, the user can be confident they are on the legitimate Web site.

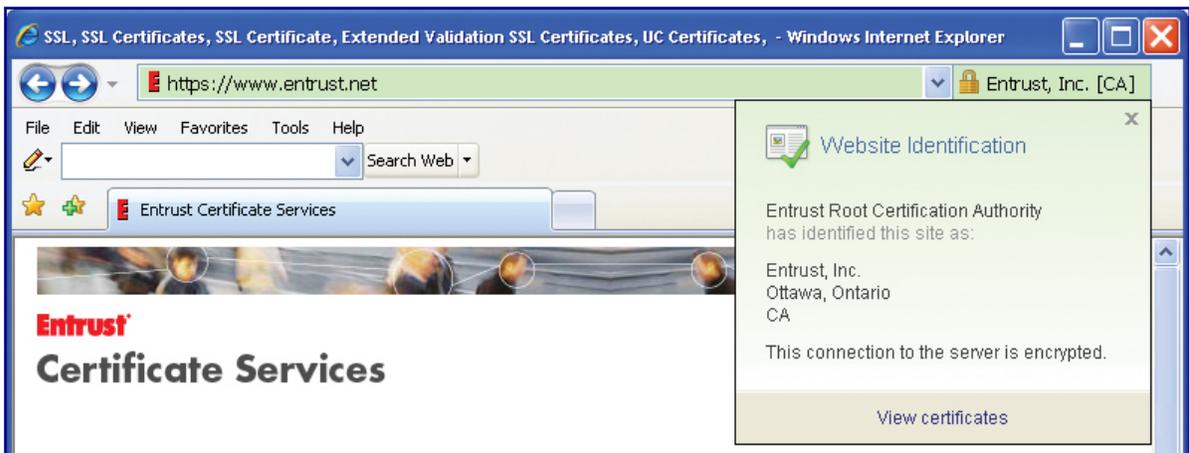
Another method that can be leveraged with the grid card is for the replay of specific grid coordinates. When displayed to the user, this confirms that the site has specific knowledge of the contents of the user's grid and, therefore, must be legitimate.



Additional security measures can be taken to make this information difficult to harvest including obfuscating entries with non-machine-readable characters to help prevent them from being replayed. These two methods can also be used across other delivery channels, including e-mail or electronic literature.

Extended Validation (EV) Certificates

A natural complement to Entrust IdentityGuard and a key component of a layered security strategy, Entrust Extended Validation SSL Certificates — commonly known as “EV” certificates — contain safeguards to help prevent fraud attacks. When consumers use an EV SSL-aware, next-generation browser, the technology will help users make smarter decisions of trust, such as the ability to verify the identity information of the owner of an EV certificate-protected Web site.



Alone or in Combination

These mutual authentication methods can significantly increase the user's defense against online identity attacks and make it difficult to perpetrate fraud against an organization. All these methods are recognized by government agencies and do not require the deployment of any hardware or software to the end user.

4 Flexible, Risk-Based Security

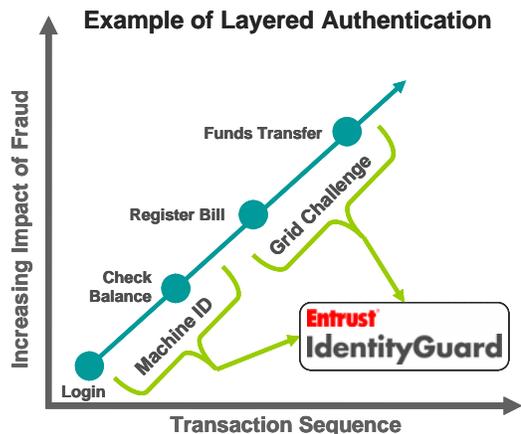
The Entrust IdentityGuard versatile authentication platform allows organizations to add layers of increased authentication to help mitigate risk. Increased confidence in user identity can help to reduce risk, but this must be tempered against the intrusiveness of authentication and the actual impact of potential fraud. For example, the cost and invasiveness of deploying hardware tokens for users to check their account balance would not make sense given the cost of doing so as compared to the impact if an attacker saw the balance.

However, password authentication alone would be insufficient for a user performing a funds transfer to another institution where the impact of fraud would be significantly higher. Accordingly, Entrust IdentityGuard provides a range of versatile authentication methods so organizations can prompt for additional authentication — when their assessment of risk demands it.

Flexibility

Each of the authentication methods supported by Entrust IdentityGuard can be leveraged sequentially or simultaneously for a given user. In fact, it is anticipated that in many cases organizations will deploy multiple methods for a given user to better fit the online experience.

As shown in the example to the right, authenticating the machine identity may be sufficient for users checking their bank account balance. However, those same users could be required to authenticate further while registering a bill payment activity or transferring funds with, for example, a grid authentication challenge. This way the user experience is not impacted for low-risk transactions but additional easy-to-use strong authentication is required when the assessed risk increases.



Risk-Driven

Providing this layered set of strong, versatile authentication capabilities simplifies the risk remediation process by allowing organizations to establish a clear risk-driven authentication policy. First, organizations can quickly establish policy around which transactions are considered higher risk, independent of user context. For example, a bank may decide that all inter-institution transfers greater than \$10,000 require additional authentication above and beyond username and password.

Organizations can also use authentication as an input to and output from their application's fraud detection capability. For example, that a user is authenticating from a registered machine when requesting to register a bill may be a valuable input in assessing the risk of that transaction. However, if the application determines that the bill being registered does not fit the transaction

history and profile of the user, additional authentication can be requested from Entrust IdentityGuard.

This also means that organizations do not need to replace existing or alternative fraud detection capabilities. Entrust IdentityGuard provides the versatile authentication platform that provides input to and processes requests from the application's risk assessment mechanism.

5 Easy to Use, Low Cost to Deploy

By providing a range of low-cost options for more strongly authenticating end-users and is easily integrated with existing infrastructures, Entrust IdentityGuard helps reduce the cost and time to deploy strong authentication. Especially in the face of increased regulatory pressure and waning consumer confidence, there is significant pressure for online organizations to accelerate additional authentication in their applications.

As part of a strong, layered security strategy, Entrust IdentityGuard delivers versatile authentication methods that can dramatically reduce acquisition and maintenance costs compared to conventional single-purpose authentication products. Further, by reducing disruption to current applications, the cost to integrate and deploy the authentication is also decreased. This includes the ability to extend beyond online authentication to phone (IVR) and ATM/kiosk applications.

Low-Cost Authenticators

By providing a range of authenticators that do not require the deployment and management of either hardware or software, procurement cost, as well as that of ongoing maintenance, can be significantly reduced. Conventional single-purpose solutions often focus only on a single, expensive option, and as such can be several times more expensive than many of the methods supported by Entrust IdentityGuard.

Entrust IdentityGuard's range of authentication methods include many that do not require distribution of hardware or software. By leveraging existing devices and knowledge already possessed by the user, and by leveraging cost effective physical form factors, including the \$5 Entrust IdentityGuard Mini Token organizations can anticipate substantially lower authentication costs versus conventional high-priced, single purpose solutions, while still achieving the goal of strong, versatile authentication.

Easy-to-Use Authenticators

Entrust IdentityGuard can fit simply into the user experience to help improve acceptance and reduce support calls. Increased vetting of user identity can help reduce risk, but this must be tempered against the intrusiveness of authentication.

It is reasonable to expect that if this additional security is cumbersome it will result in incomplete or abandoned transactions. Not only does this impact the perceived level of service, it also can result in increased costs as users revert to more expensive channels. Entrust IdentityGuard supports a range of authentication capabilities, many of which do not require the deployment of hardware or software to the end-user. This helps ease the deployment and make the authentication more convenient. Examples of highly deployable and easy-to-use authenticators include:

- **Machine/Device Authentication.** While leveraging the computer being used to conduct the online session, this method of authentication does not require deployment of software or hardware.

- **Knowledge-Based Authentication.** Without the need to deploy any physical authenticator to the user, knowledge-based authentication provides an easy-to-use method of strong authentication, as it draws on information the user knows.
- **Grid Authentication.** Authentication grids themselves can be readily deployed on simple, plastic cards or in conjunction with existing statements or ATM or credit cards. This puts the authentication capability in the hands of users using the same distribution channels that exist today.
- **Out-of-Band Authentication.** Like device authentication, this method leverages hardware that is already in the hands of the end-user.

As a versatile authentication platform, Entrust IdentityGuard allows personalization to improve user acceptance. By providing the flexibility to have users leverage different authentication methods, organizations can provide their users the convenience of personalizing how additional authentication takes place.

For example, if one user would like to receive a one-time-password SMS on their mobile phone versus another whom would prefer a voice call to their home phone, this can be readily accommodated. This can be even more broadly applied with some users leveraging grid authentication while others use knowledge-based authentication to, for example, register new computers for device authentication. In the end, by allowing users some degree of personalization, organizations can make these easy-to-use authenticators even more readily accepted so that security does not impede the transaction flow.

Non-Invasive Integration

Most online organizations have substantial investments in current infrastructure including password and sign-on applications, user repositories and administrative processes. With the pressures to increase security, complex integrations with substantial impact to current systems represent an unacceptably high level of cost and risk.

Entrust IdentityGuard helps reduce those impacts by leveraging current infrastructure, including:

- Preserving current username and password schemes
- Leveraging a current user directory or database for storage of authentication information
- Preserving current fraud detection used for risk assessment or seamlessly integrating with Entrust TransactionGuard for risk-based authentication
- Maintaining current administrative processes with easy to integrate administrative APIs

Alternative approaches to strengthening authentication can also have significant complexities and cost. For example, some approaches tightly integrate fraud detection with authentication, requiring the development of complex access rules that, in many cases, not only duplicate those already in current applications but can also inadvertently block user access, causing help desk calls or abandoned transactions. In some cases, artificial intelligence is used that requires substantial learning time and can result in false positive fraud detections, disrupting the user experience.

Multi-channel Authentication

While online identity attacks and transaction fraud are prevalent, other transaction channels can benefit from a versatile authentication platform. Whereas traditional hardware and software authenticators have challenges, Entrust IdentityGuard has been designed to support other channels including telephone, ATM and in-person transactions.

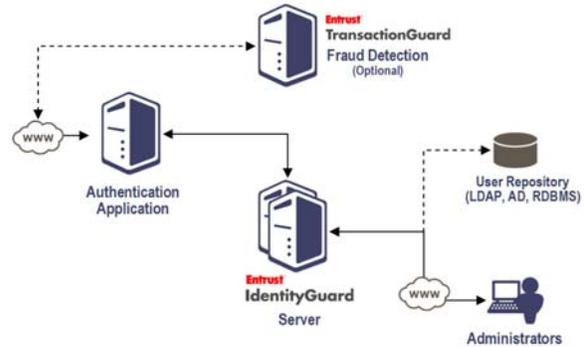
Because the authentication methods can be performed via keypads and do not require complex user interfaces, they can fit easily into alternative channels. For example, grid authentication

could be easily used to support automated call center authentication of users by prompting for a grid location challenge and having the user enter the response via the telephone touch-tone pad.

By providing this extensibility, organizations can leverage their initial Entrust IdentityGuard investment across multiple channels.

6 Architecture and Integration

Entrust IdentityGuard is designed to work in an organization's environment with little impact to existing infrastructure. This includes existing authentication applications as well as user repositories that are found in typical organizations. It also meets the high scalability needs of consumer applications, ensuring the availability and service levels required in that environment.



Low-Impact Integration

Entrust IdentityGuard is designed to compliment an organization's current authentication application. Whether a home-grown password application or a third-party Web access control product, the Entrust IdentityGuard versatile authentication platform provides an interface that adds a second factor of authentication. Virtually all mainstream Web access control products provide an off-the-shelf interface for exactly this purpose.

The authentication interface is provided using either Java or Web Services in order to meet the needs of various potential authentication applications, whether J2EE or .NET. Most transactions center on the authentication application submitting a given user's authentication attempt for verification. Once confirmed, the Entrust IdentityGuard server responds with the result.

Like the interface to the authentication application, Entrust IdentityGuard leverages the current customer's repository to store user data. This repository is leveraged to store and retrieve the authentication information for a given user. When a card is generated for a given user, it is written in encrypted form to the repository. When authenticating a user, it is retrieved from the repository. This interface supports LDAP, Active Directory, JDBC or a customer-defined API. Finally, a remote Web administration interface is provided to access the various user management and authentication functions. Administrative functions are also available via API to make them available to user identity management and provisioning systems.

Robust, Flexible Architecture

Entrust IdentityGuard is designed to address scalability for high-transaction, consumer-oriented applications. As such, it can have several servers deployed at one time in a load-balanced environment, which allows for the ability to increase throughput by adding additional servers. Also, a high-performance cache for user information can help to accelerate transactions.

The Entrust IdentityGuard versatile authentication platform is a server-based software product that can be installed in a typical organization's current infrastructure. It is a J2EE application written in Java and runs on the leading operating systems, including Microsoft® Windows, Sun Solaris, IBM AIX and RedHat Linux. Security operations are performed using Entrust's FIPS 140-2-certified cryptographic software. As a result, authenticating information is generated securely and the risk of a rogue employee successfully tampering with information in the repository is reduced.

Finally, like all Entrust products, software development, quality and security assurance is performed to meet high standards. Further, the Entrust IdentityGuard solution is backed by Entrust's global, 24-7 service and support organization.

7 Conclusion

As online identity fraud continues to grow, organizations need to proactively mitigate transaction risk with stronger forms of authentication that are easy to use and less costly to purchase and deploy than traditional options.

As a flexible, risk-based solution, the Entrust IdentityGuard versatile authentication platform enables organizations to layer a range of strong authentication capabilities across their online presence to increase security and help protect their customers from online identity attacks. It enables organizations to provide strong authentication to a wider audience, with greater control and flexibility in determining how to secure different users and transactions — based on the assessed risk associated with those transactions.

The Entrust IdentityGuard versatile authentication platform is a key component of a strong, layered security strategy. For more information on Entrust IdentityGuard, please visit: <http://www.entrust.com/strong-authentication/identityguard/>.

8 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.