



Entrust IdentityGuard Multifactor Authentication Methods

Entrust IdentityGuard is an award-winning authentication solution that secures many of the world's leading financial institutions, enterprises and global governments. Serving as a versatile authentication platform, it provides a range of strong authentication capabilities for improved confidence for online transactions and identity authentication for access to applications or resources.

A key component of a layered enterprise security model, Entrust IdentityGuard can leverage current fraud detection capabilities from Entrust to help organizations build an authentication strategy based on its unique requirements, not the limitations of an individual authentication method.

The versatile authentication platform allows organizations to match the authentication strength and mechanism to the amount of associated risk, cost considerations and usability requirements.

- Do you want authentication to be transparent to the user?
- Would you like the user to carry a physical device or authenticate online?
- Do you want the Web site to authenticate itself to the user as well?
- How sensitive is the information you are protecting and what is the associated risk?

The flexibility and range of Entrust IdentityGuard authenticators allows organizations to apply strong authentication across the enterprise, instead of just a select group of users. The platform offers a single point of administration, regardless of the authentication option or combination of options deployed, giving organizations the ability to evolve and change authentication methods over time as risks and the operating environment change.

Review the platform's full range of authenticators and discover which may be right for your organization.

Product Benefits

- Proven components of the Entrust IdentityGuard versatile authentication platform
- Comprise widest range of authentication capabilities available on the market today
- Provide advanced protection against man-in-the-middle attacks
- Authenticators deployed as part of non-invasive, risk-based versatile authentication platform proven in mass markets
- Simple, low price that is a fraction of the cost of traditional two-factor options
- Key component of a layered security strategy

Entrust IdentityGuard Multifactor Authentication Methods

Transparent Authentication

Transparent authenticators validate users without requiring day-to-day interaction. Step up to additional authentication only when the transparent authentication fails. Transparent authenticators include:



IP-Geolocation

Authenticated users can register locations where they frequently access the corporate network. During subsequent authentications, the Entrust IdentityGuard server compares current location data — country, region, city, ISP, latitude and longitude — to those previously registered. Organizations can step up authentication only when values don't match.

With IP-geolocation, organizations can create blacklists of regions, countries or IPs based on fraud histories, or leverage the Entrust Open Fraud Intelligence Network (OFIN) to receive updated lists of known fraudulent IPs based on independent professional analysis.



Device Authentication

Authenticated users can register a computer or device that is frequently used to access the corporate network. A sophisticated encrypted profile of the registered computer is created and stored. During subsequent authentication, the Entrust IdentityGuard server creates a new profile and compares it against the stored value. Step-up authentication is required only when the values don't match.

IP-geolocation and machine authentication, deployed in combination, offer an effective and transparent authentication method for users.

Physical Form Factor Authenticators

Physical form factors are tangible devices that users carry and use when authenticating. Entrust offers a number of physical authentication devices to meet diverse corporate user requirements. Physical form factor authenticators include:



One-Time-Passcode Tokens

Entrust offers two versions of the popular one-time-passcode (OTP) token. Starting at just \$5, the Entrust IdentityGuard Mini Token is OATH-compliant and generates a secure eight-digit passcode at the press of a button. The OATH-compliant Pocket Token offers additional features including PIN unlock prior to generating the passcode, in addition to a challenge-response mode.

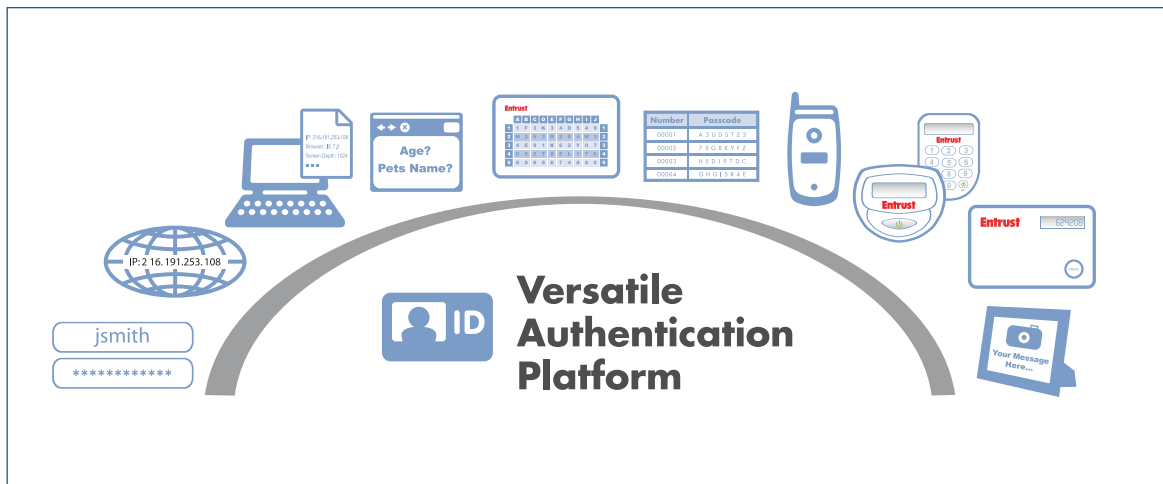


Figure 1: Entrust IdentityGuard's wide range of authentication capabilities



Display Card

The Entrust Display Card provides the same functionality as the popular token in a credit card format. In addition to providing an OATH-compliant, one-time passcode, the Display Card optionally can include a magnetic stripe and a PKI or EMV chip for greater versatility.



Grid Authentication

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.

As a complement, eGrid cards are sent to the user via the Web or .PDF, which easily can be stored on a machine or mobile device for convenient access, eliminating the need to carry a physical form factor.

Number	Passcode
00001	A3UD5T23
00002	75GRKYFZ
00003	HSDJ97DC
00004	GH01584E

One-Time-Passcode List

End-users are provisioned with a list of randomly generated passcodes or transaction numbers (TANs) that are typically printed on a sheet of paper and distributed to end-users. Each passcode is used just once.

Non-Physical Form Factor Authenticators

Non-physical form factor authentication provides methods of verifying user identities without requiring them to carry an additional physical device. Non-physical form factor authenticators include:



Knowledge-Based Authentication

Knowledge-based authentication challenges users to provide information an attacker is unlikely to possess. Questions presented to the user at the time of login are based on information (referred to as authentication secrets) that was supplied by the user at registration or based on previous transactions or relationships. Entrust IdentityGuard allows the administrator to determine the number and type of questions asked.



Out-of-Band Authentication

Out-of-band authentication leverages an independent and pre-existing means to communicate with the user to protect against attacks that have compromised the primary channel. 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.



Strong Username and Password

Entrust IdentityGuard typically provides a strong second factor of authentication to an organization's existing username and password infrastructure. The versatile authentication platform can provide strong username and password login for companies without an existing solution.



Mutual Authentication

Your organization needs to have confidence in a user's identity. Likewise, users must be confident that they are transacting with their organization or intended online site; not a fraudulent organization or spoofed site. Mutual authentication provides methods for your organization to confirm your legitimacy to users. Entrust provides organizations with a range of options for mutually authenticating with their customers, including:



Image and Message Replay

Upon registration, the user selects an image from an extensive image bank supplied with Entrust IdentityGuard. The user also creates a message. During subsequent logins the image and message are presented to the user.



Grid Serial Number Replay

During login, the serial number of the user's unique grid card is presented to the user.

Grid Location Replay

During login, the user is presented with the values of a number of cells from their unique grid card.



Extended Validation (EV) SSL Certificates

Organization can deploy Extended Validation SSL certificates, which confirm the Web site's authenticity by displaying a green address bar — an obvious trust indicator for the end-user.

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.

Entrust & You

The Entrust IdentityGuard versatile authentication platform offers the widest range of authenticators available on the market today. From easy-to-use grid cards, IP-geolocation capabilities to one-time-passcode tokens, the solution provides any organization, financial institution, enterprise and government agency seamless, efficient methods to deploy strong multifactor authentication as part of a comprehensive layered security strategy.

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 2,000 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.

Entrust[®] Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2009 Entrust. All rights reserved.