



Entrust IdentityGuard

Strong Authentication Methods

Entrust IdentityGuard is an award-winning software-based authentication solution that secures many of the world's leading financial institutions, enterprises and governments.

Entrust IdentityGuard serves as an organization's single comprehensive software-based authentication platform, while concurrently bridging them to emerging technologies for strong mobility, cloud and credentialing offerings. It offers improved confidence for online transactions and identity authentication for access to applications or resources.

The platform also leverages Entrust's proven fraud detection capabilities to help financial organizations build a comprehensive authentication strategy based on its unique online requirements, not the limitations of an individual authentication method.

The software authentication platform allows organizations to match the authentication strength and mechanism to the amount of associated risk in the user's role, usability requirements and cost considerations.

- 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 allow organizations to apply strong authentication across the enterprise, instead of just for a select group of users.

The platform offers a single point of administration, regardless of the authentication option or combination of options deployed, and gives 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

- Serves as a single identity management platform for physical, logical and mobile authentication
- Proven authenticators as part of the Entrust IdentityGuard software authentication platform
- Platform offers widest range of authentication capabilities available on the market today
- Deploys authenticators based on user requirements, level of risk and cost
- Advanced protection against man-in-the-browser attacks
- Authenticators proven in mass market deployments
- Cost-effective solution that is a fraction of the cost of traditional two-factor options

TRANSPARENT AUTHENTICATION

Transparent authenticators validate users without requiring day-to-day user involvement.

Digital Certificates

Entrust IdentityGuard can leverage existing X.509 digital certificates issued from Entrust's managed digital certificate service or a third party to authenticate users. Certificates can be stored locally or on secure devices like smartcards and USB tokens. Organizations without an in-house PKI can obtain certificates via the Entrust Managed Services PKI.

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.

One-Time-Passcode Tokens

Entrust offers two versions of the popular one-time-passcode (OTP) token. 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.

Display Card

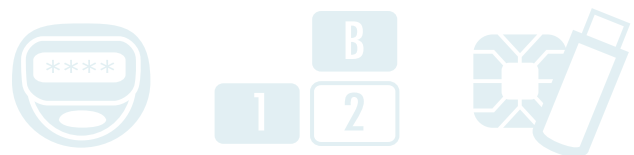
The Entrust Display Card provides the same functionality as the popular token in a credit card format. In addition to providing an OATH-compliant, one-time passcode, the Display Card includes a magnetic stripe and can optionally include a PKI or EMV chip for greater versatility.

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.

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.



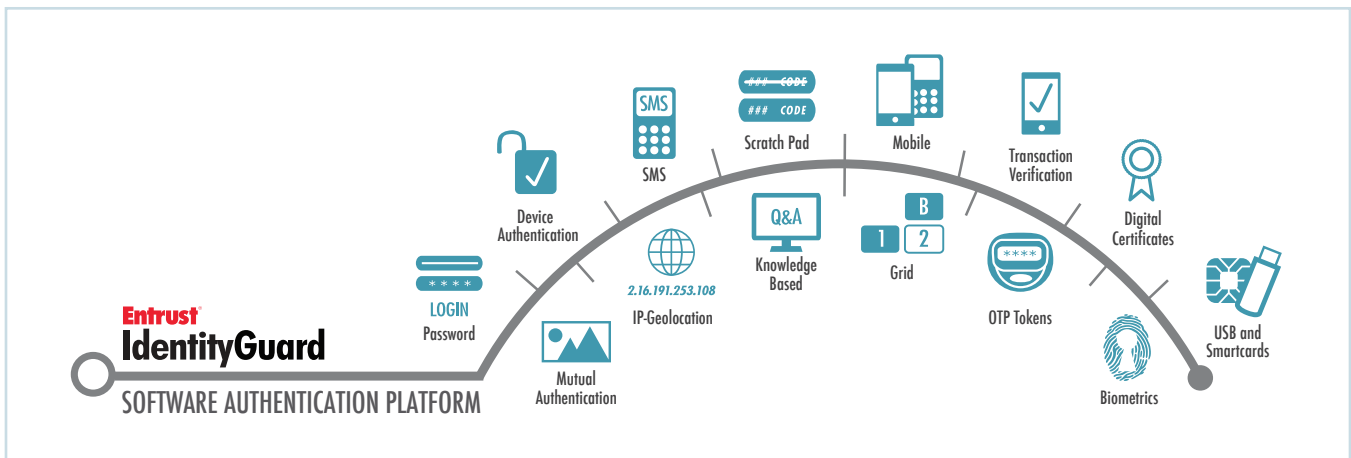


Figure 1: Entrust IdentityGuard provides one of the widest ranges of authentication capabilities on the market today.

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.

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 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 email 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.

Entrust IdentityGuard Mobile

Whether for consumer, government or enterprise environments, Entrust IdentityGuard provides mobile security capabilities via distinct solution areas — mobile authentication, transaction verification, mobile smart credentials, and transparent authentication technology with an advanced software development kit.

Supporting the use of the OATH standard for time-based OTP, as well as out-of-band transaction signatures, Entrust IdentityGuard Mobile is one of the most convenient, easy to use and secure mobile authentication methods available today.

Entrust IdentityGuard Mobile is also one of the only authentication solutions on the market today that addresses the man-in-the-browser (MITB) malware threat — effectively and without user inconvenience.

Mobile Smart Credentials

Eliminate the need for physical smartcards by transforming today's popular mobile devices into mobile credentials for enterprise-grade authentication. Advanced mobile smart credentials can be used with Bluetooth and near-field communication (NFC) technology for greater convenience and secure connectivity.

SECURITY
ON

SMS Soft Tokens

Similar to the platform's out-of-band authentication capabilities, Entrust IdentityGuard also includes SMS soft tokens, which enable the transmission of a configurable number of one-time passcodes (OTP) to a mobile device for use during authentication. Automatically replenished as needed, this dynamic soft-token approach delivers the strength of out-of-band authentication without the concern for constant network availability, delivery timing or software deployment to a mobile device.

eGrid

An alternative to hardware tokens, eGrid cards are sent to users via the Web or as a PDF, which can be easily stored on a machine or mobile device for convenient access and eliminating the need to carry a physical form factor.

Strong Username & Password

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



MUTUAL AUTHENTICATION

Your organization needs to have confidence in the 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.

Image & 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.

Entrust EV Multi-Domain SSL Certificates

Organizations can deploy Extended Validation (EV) SSL certificates, which confirm the website'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 website is authentic.



About Entrust

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 www.entrust.com.

Entrust[®] Securing Digital Identities & Information