Entrust Datacard™

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.

The solution serves as an organization's single comprehensive software -based authentication platform, bridging you to emerging technologies for strong mobility, cloud and credentialing offerings. Improve confidence for online transactions and identity authentication for access to applications or resources.

Flexible Security

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. It's a single point of administration, regardless of the authentication option or combination of options deployed. Evolve and change authentication methods over time as risks and the operating environment change.

▶▶entrust.com/authentication

Security Matches Risk

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.

Understanding Authentication

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 website to authenticate itself to the user as well? How sensitive is the information you are protecting and what is the associated risk? Review the platform's full range of authenticators and discover which may be right for your organization.

Integrates with Fraud Detection

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.

Entrust Datacard Local Partner

ELLIOTT DATA SYSTEMS, INC.

St. Louis, MO
17825 Edison Ave
Chesterfield, MO 63005
(636) 386-8400

Memphis, TN
5045 Covington Way
Memphis, TN 38134
(901) 372-4600

www.elliottdata.com

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
- Offers widest range of authentication capabilities available on the market today
- Deploys authenticators based on user requirements, level of risk and cost
- Enables 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 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 smart cards and USB tokens. Organizations without an in-house PKI can obtain certificates via Entrust's hosted PKI services.

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

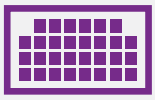
Physical form factors are tangible devices that users carry and use when authenticating. Entrust offers a number of physical authentication devices to meet diverse corporate user requirements.

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.

Physical Form Factor Authenticators (cont'd)

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.

Biometrics

Entrust leverages biometric fingerprint data to provide an effective balance between authentication strength and user convenience for Microsoft® Windows® logon. To protect user privacy, fingerprint data is stored in a database or on an Entrust smartcard as an encrypted mathematical representation — sometimes known as a hash — and compared to the actual fingerprint provided at the time of authentication. This stored information cannot be reverse-engineered, ensuring the protection of personally identifiable information (PII).

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.

Non-Physical Form Factor Authenticators (cont'd)

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

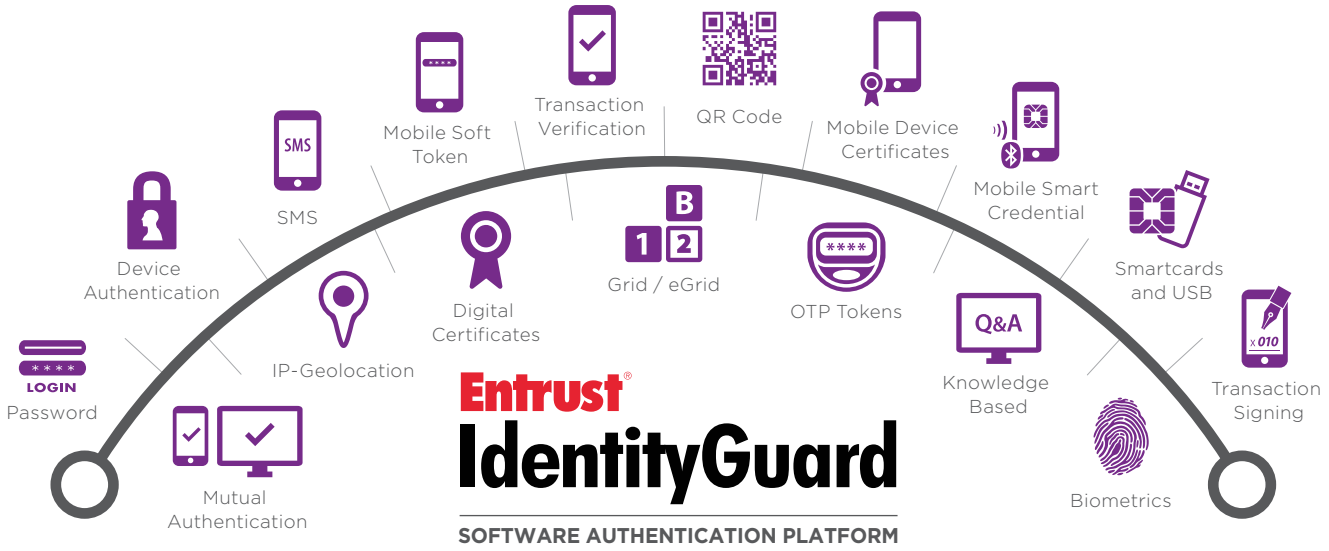
Eliminate the need for physical smartcards by transforming today's popular mobile devices into mobile credentials for enterprise-grade authentication. Advanced mobile smart credentials can be used with Bluetooth and near-field communication (NFC) technology for greater convenience and secure connectivity.

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.

Software Authentication Platform



Powered by Entrust IdentityGuard. The widest range of authenticators on the market today — all from a single platform.

Non-Physical Form Factor Authenticators (cont'd)

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

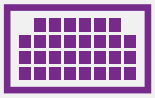
Entrust IdentityGuard typically provides a strong second factor of authentication to an organization's existing username and password infrastructure. The versatile authentication platform can provide strong username and password login for companies without an existing solution.

Mutual Authentication

Your organization needs to have confidence in 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 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.

About Entrust DataCard
Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway,
Suite 1250
Dallas, TX 75240 USA

Entrust Datacard™

23637/9-15