Entrust®

Entrust IdentityGuard Grid Authentication

Easy-to-Use, Cost-Effective Strong Authentication

A component of the Entrust IdentityGuard authentication platform, grid authentication provides organizations a simple, yet effective, strong authentication tool for increased security and logical access control.

Grid authentication increases security by providing an additional (or second) factor in the authentication process. In addition to something you know (e.g., password), it provides something you have: the grid card.

Strong Authentication Made Easy

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.

▶ **entrust.com/authentication**

Importance of Strong Authentication

Many authentication methods and policies from even five years ago are already showing signs of age. 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.

Patented Security

Assigned to Entrust in 2005 by the Eastman Chemical Company, U.S. Patent 5,712,627 (the “’627 Patent”) was issued on January 27, 1998, by the United States Patent and Trademark Office. It covers all methods for determining whether a person seeking access to a secured system is authorized to do so via some form of grid authentication.

▶ **entrust.com/gridcard**

Powered by Entrust IdentityGuard

The Entrust IdentityGuard software authentication platform serves as the foundation for proven grid authentication. The award-winning solution secures many of the world’s leading financial institutions, enterprises and governments. Improve confidence for online transactions and identity authentication for access to applications, devices, resources and more.

+1-888-690-2424

entrust@entrust.com
entrust.com/gridcard

@Entrust
+entrust
/EntrustVideo
/EntrustSecurity

DOWNLOAD
THIS DATA SHEET

Product Benefits

- Simple, easy-to-use authenticator for any industry, region or user population
- Proven authenticator as part of the Entrust IdentityGuard software authentication platform
- Features patented security technology
- Proven in mass-market deployments
- Cost-effective solution that is a fraction of the cost of traditional two-factor options

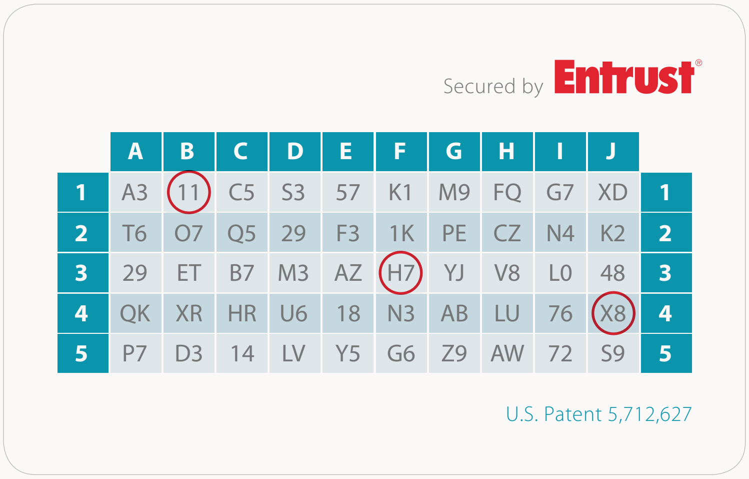
How Does Grid Authentication Work?

A user is presented an authentication challenge when they log in to a restricted network, application, cloud service or site.

In this scenario, the challenge presents the user with coordinates such as **B1, F3** and **J4**.

The user refers to their unique grid card to provide the information from the requested cells: **11, H7, X8**.

Each grid card is unique and carries a serial number, so every user can be uniquely identified and authenticated. Each time a user is asked to authenticate they are presented with a different challenge requiring them to validate via a different set of grid coordinates. The coordinate request changes for each authentication challenge.



Secured by Entrust

	A	B	C	D	E	F	G	H	I	J	
1	A3	11	C5	S3	57	K1	M9	FQ	G7	XD	1
2	T6	O7	Q5	29	F3	1K	PE	CZ	N4	K2	2
3	29	ET	B7	M3	AZ	H7	YJ	V8	L0	48	3
4	QK	XR	HR	U6	18	N3	AB	LU	76	X8	4
5	P7	D3	14	LV	Y5	G6	Z9	AW	72	S9	5

U.S. Patent 5,712,627

Challenge Generation Algorithms

After enabling grid authentication, Entrust IdentityGuard allows you to choose between two challenge-generation algorithms.

Random Challenge

This algorithm (default) picks cells randomly when creating a challenge. The process for creating a challenge does not depend on previous challenges.

Least-Used Cells Challenge

This algorithm uses one or more least-used cells (set in policy) in every challenge. By generating challenges using the least-used cells from a user's grid, it becomes more difficult for an attacker who has previously viewed some successful authentications to correctly respond to the challenge.

Configuring Grid Card Design

Grid card policies define the attributes of individual grid cards. Organizations may specify:

- The number of rows and columns visible on a grid card. This sets the grid size and total number of cells.
- The number of cells displayed in each challenge; also known as the challenge size.
- The number and type of characters in a cell. They can be numbers, letters or a combination of both.

Entropy & Grid Authentication

Grid authentication card security is determined by a number of factors. Card size is arguably the most important variable. Increasing the grid size (i.e., number of cells) and format (i.e., contents of the cell) exponentially increases the number of challenge responses available.

Entropy is defined as the uncertainty involved in predicting the value of a random variable. In this case, it refers to the ability to predict the information contained on a grid card — both coordinates and characters.

A larger grid card and additional cell contents increase the uncertainty of predicting the coordinates and characters on the card. In other words, more variables mean less chance of "cracking" the grid.

Entrust IdentityGuard allows you to change the policy and define the entropy of a card and its strength. Grid cards also may be set to expire with greater frequency — requiring the issuance of new cards — to increase security.

Understanding Grid Complexity

Default grid is 5 rows by 10 columns

Challenge is 3

Default alphabet is 28 characters

In this example, the chance to guess a random challenge of **3** on the default grid is **1** in **21,952** (1/28 * 1/28 *1/28 = 1/21952).

Typical Use Cases

USE CASE

Mobile Emergency Workers

Grid authentication is effective for field workers who are in emergency situations and it is not convenient or possible to carry other types of authenticators (e.g., OTPs, out-of-band notification).

Despite the challenges of their roles, they still have a need for strong authentication and find grid authentication is both secure and efficient.

USE CASE

Military Personnel

Grid authentication is especially useful for military personnel who may not be able to use electronic forms of authentication (e.g., mobile smart credentials) due to the possibility of transmissions being intercepted.

In this scenario, grid cards provide strong, second-factor authentication for access to highly sensitive information without the possibility of interception by attackers.

Card Lifetime & Replacement

In order to minimize the time an attacker has to gather user data, organizations should renew cards on a regular basis. In typical situations, annual renewal is appropriate. However, in higher-risk scenarios cards may be renewed quarterly. Organizations can set their policy according to their own risk assessment.

Definable Card Options

The following grid authentication options, which are configurable by the administrator, are available with Entrust IdentityGuard:

- **Card Lifetime** — The card will no longer be valid after a defined number of uses. (e.g., Once 50 percent of the grid has been used, the card is no longer valid.)
- **Card Expiry Date** — The card will expire on a set date.

Quick Deactivation, Replacement

In the event a user loses their grid card, or has it stolen, the card can be deactivated with immediate effect by the administrator. For greater convenience, the user may even deactivate the card via the Entrust IdentityGuard Self Service Module.

A trusted provider of identity-based security solutions, Entrust secures 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**.

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

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

Entrust®