Entrust Grid Card Authentication

Easy-to-use, low-cost multi-factor authentication (MFA)

Market Challenge

With the increase in cyberattacks due to compromised credentials from weak passwords or password re-use, organizations need to implement an additional layer of security with multi-factor authentication (MFA) to provide secure access to resources for employees. Common forms of MFA usually incorporate the use of a user's mobile device to provide a second factor as that is something that is always in the user's possession and is secured by their unique biometrics (face ID, touch ID, etc.).

But there are situations, such as frontline and field employees accessing critical systems, where a user may not have access to a mobile device to use as part of the MFA operation.

Solution

Grid cards are an easy-to-use and cost-effective way to provide MFA for users that cannot use mobile devices to log in to required systems and applications. The grid card is a paper-based card that can be printed from a PDF file and contains a grid of rows and columns that consist of numbers and characters. As part of the MFA process, users are presented with a coordinate challenge and must respond with the information in the corresponding cells from the unique card that they possess.

BENEFITS

- Cost-effective solution
- Proven in mass-market deployments
- Low support overhead
- Increased security

KEY FEATURES

- Easy-to-configure design
- Unique to every user
- Define challenge characteristics
- Works as second factor for existing IDPs

Learn more about our MFA solutions at entrust.com

Entrust Grid Card Authentication

HIGHLIGHTS

Importance of MFA

Simple password-based authentication, even for users operating exclusively internally, are no longer enough to prevent breaches, protect privacy, and achieve compliance. Weak passwords and re-use due to password fatigue has led to compromised credentials being one of the largest threat vectors in recent attacks. Stronger authentication through MFA must be deployed to a wider audience — efficiently and cost-effectively.

Challenge generation

The grid card challenge presented uses a random challenge algorthm. This algorithm (default) picks cells randomly when creating a challenge. The process for creating a challenge does not depend on previous challenges.

Configuring grid card design

Grid card policies define the attributes of individual grid cards.

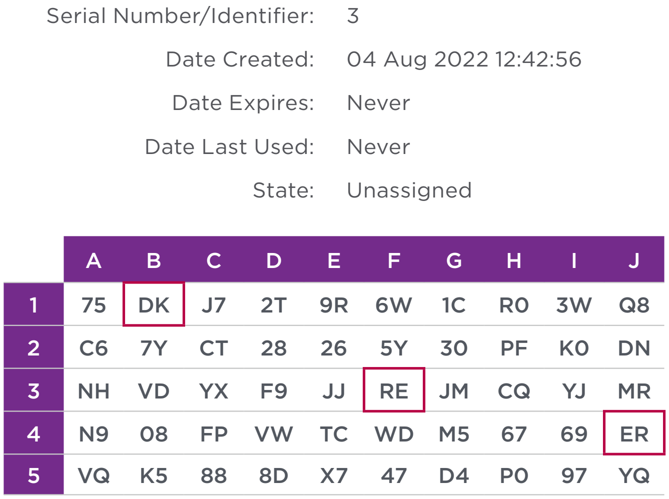
Organizations may specify:

- 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.
- Whether the challenge is retained until it is answered correctly.
- Whether the characters are case-sensitive.
- The challenge lifetime in seconds. A value of 0 indicates the challenge is retained until answered correctly.
- The grid card lifetime in seconds. A value of 0 indicates the grid card never expires.
- Whether to include the grid expiry in the challenge.

HOW IT WORKS

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.



Serial Number/Identifier:	3
Date Created:	04 Aug 2022 12:42:56
Date Expires:	Never
Date Last Used:	Never
State:	Unassigned

	A	B	C	D	E	F	G	H	I	J
1	75	DK	J7	2T	9R	6W	1C	R0	3W	Q8
2	C6	7Y	CT	28	26	5Y	30	PF	K0	DN
3	NH	VD	YX	F9	JJ	RE	JM	CQ	YJ	MR
4	N9	08	FP	VW	TC	WD	M5	67	69	ER
5	VQ	K5	88	8D	X7	47	D4	P0	97	YQ

The user refers to their unique grid card to provide the information from the requested cells: DK, RE, ER.

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.

Learn more about our MFA solutions at entrust.com

Entrust Grid Card Authentication

Works with existing IDPs

Organizations that have a need to provide grid-card-based MFA can use Entrust's Identity platform as part of a second or multi-factor authentication with an existing identity provider (IDP).

Grid authentication and entropy

Security of the grid card authentication is determined by a number of factors. Card size is arguably the most important variable. Increasing the grid size and format 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.

You can configure the policy to define the number of cells, number of characters in each cell, and types of characters allowed. Grid cards may also be set to expire with greater frequency – requiring the issuance of new cards – in order to increase security.

Typical use cases

Call centers

Typical call center operations are usually outsourced to third parties in a different country. However, call center employees need to access critical systems with PII and other sensitive information and cannot use mobile or other electronic devices when working a shift.

Employees can use grid cards as a means to log in to these internal systems as part of MFA to increase security. These grid cards are easily replaceable as they can be printed from a PDF file and eliminate the cost overhead of supporting physical tokens such as FIDO-based keys.

Frontline and field employees

Organizations that have employees who work as field or frontline operations where part-time and shift work is the norm will find using grid cards as part of MFA will greatly reduce the overhead in maintaining and providing support to mobile and physical authenticators.

Grid card authentication is also effective for field employees in emergency situations where it is not convenient or possible to carry other types of authenticators.

Military and law enforcement

Grid card authentication is also useful for military and law enforcement 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 or limitations in carrying devices in certain high-risk situations.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223