

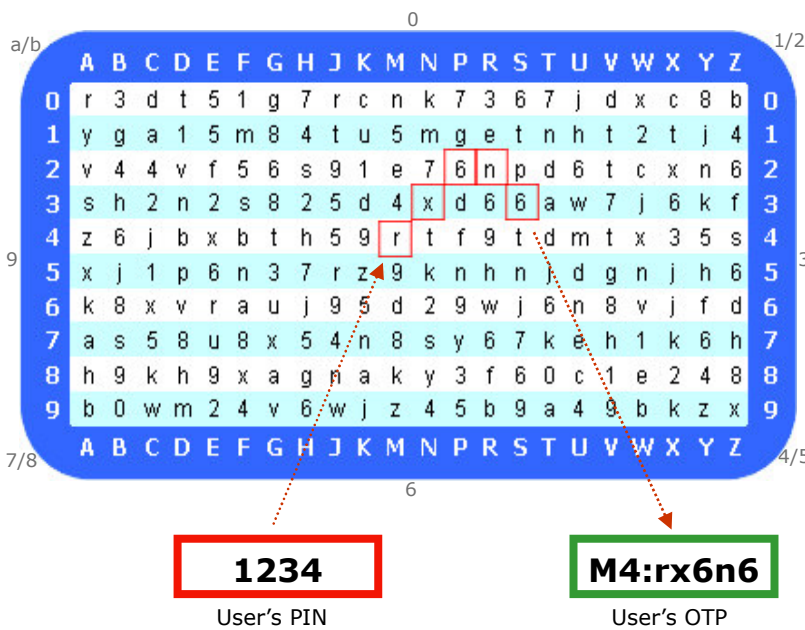
Secure Grid Cards



GridID™

PIN-Protected, Grid-Based One-Time Password

Deepnet GridID is a simple, effective, two-factor and two-way OTP authentication method based on security grids. A security grid contains a matrix of numbers and letters in easily marked columns and rows. These security grids are typically printed on credit card-sized cards that can be easily carried in user's wallets, or they can be printed on the back of employee access badges, credit cards or ATM cards. Security grids can also be delivered to the users in confidential letters, emails or SMS messages.



Two-Factor Authentication

To perform strong user authentication with a security grid, in addition to existing usernames and passwords (something you know), users are required to provide a one-time password generated from their security grid cards (something you have).

PIN Protected

Users can protect their security grid cards with a PIN or password. At each logon, users generate a one-time password by randomly selecting a start point in the grid and navigate in the grid on a secret path that is only known to the users. The secret navigation path is encoded and easily memorized as a PIN or password. This unique, patent-pending technology protects users' credentials even when their security grid cards have been lost or stolen.

Two-Way Authentication

In an application that requires mutual authentication, Deepnet GridID can be configured to provide two-way authentication. Users receive two security grids, a User Grid and a Host Grid. The User Grid is used to generate OTP that authenticates the user to the host, and the Host Grid is used by the user to verify the host's OTP.

Unified Authentication Platform

Deepnet GridID is one of several authentication methods managed by the Deepnet Unified Authentication Platform that enables business organisations to deploy a mixture of security tokens to all types of users, in all types of applications.

