

Secure Your VPN

FireID significantly lowers the risk of office VPNs being compromised, allowing administrators to securely authenticate users and, conversely, exclude or easily disconnect users from VPNs.

Conventional authentication solutions make use of key fobs or hardware tokens to generate one-time-passwords - the cost and maintenance of these tokens, plus the distribution and management thereof, creates a logistical nightmare. Because FireID conveniently generates OTPs on mobile phones, the need for employees to carry any other secure access hardware is eliminated.

REDUCE LOGISTICS AND ADMINISTRATIVE OVERHEADS.

Integration with existing systems

FireID is able to integrate smoothly and seamlessly to almost any infrastructure. This is made possible by FireID's ability to create a real time link to any set of multiple data sources containing user information, such as SQL databases. So, user administration can continue as usual using any existing management systems and tools currently in place, with FireID acting as a backend providing strong authentication.

FireID Deployment

The FireID token application can be deployed remotely and at no cost, via a self-signup process driven by the end-user. This makes it easy to deploy and manage, while integrating simply to your web infrastructure.

Why FireID?

FireID is the first authentication system of its kind. It can be easily downloaded onto almost any mobile phone in just a few minutes, offering superior security along with unparalleled convenience.

FireID is also more accessible and applicable for a wider variety of scenarios and requirements than many other solutions to date. Now you are able instantly generate your own one-time-passwords wherever personal authentication is required.

The Universal Personal Authenticator

OVERVIEW



FireID turns your mobile phone into a self-contained OTP generator.

www.fireid.com

info@fireid.com
0860 FIRE SA (3473 72)

2nd Floor
Block C, Octo Place
Electron Road
Technopark
Stellenbosch 7600
Western Cape
South Africa

www.fireid.com



- 1** Random One-Time-Password generated by FireID application on mobile (no sms or internet activity).
- 2** User types in generated OTP.
- 3** User's authorisation request passes through existing network infrastructure and FireID software authenticates OTP.
- 4** User's request approved and user is logged in.

The Universal Personal Authenticator

The efficiency and convenience afforded by tools such as Internet banking, online shopping and office VPNs make them indispensable in a fast paced, highly competitive world. However, it's an unfortunate fact that modern day conveniences bring modern security threats that require a cutting edge solution.

Introducing FireID, a security system that provides strong personal authentication wherever and whenever it is required, keeping you ahead of Internet fraud and identity theft in the most convenient way possible.

What does FireID do?

Not only does FireID offer superior security, it does so without the need to remember passwords, carry hardware tokens around with you, or even wait for one-time-passwords to be sent via SMS where they are at risk of being intercepted.

No more:

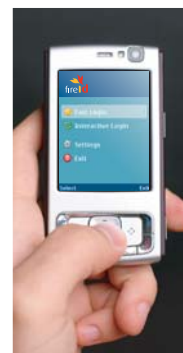
- Remembering passwords
- Hardware tokens
- SMS's

FireID generates secure one-time-passwords instantaneously and completely offline using something that you always have with you: A Mobile Phone.

A FireID enabled phone is able to generate one-time-passwords for limitless different applications, such as online banking, Internet shopping and accessing an office VPN or extranet.

FireID turns your mobile phone into a self-contained OTP generator.

The process is very simple: a random one-time-password is generated by the FireID application on your mobile phone. You then type in the one-time-password for the application you wish to access. The FireID software authenticates the one-time-password. Finally, your request is approved and you are free to log in. As soon as you log in, the password expires and cannot be used again.



How does FireID work?

FireID consists of two core components: the FireID token application and the FireID server. One of the standout features of FireID is that it requires no specialised hardware.

NO SPECIALISED HARDWARE REQUIRED.

The token application is installed on your mobile phone. It performs the task of generating a new random one-time-password on demand each time you need to login to a FireID protected resource.

The server performs the role of authenticating the random one-time-password generated by the token application on your phone. It is able to integrate directly to an existing infrastructure to access the user base, deploy tokens to users, and authorise FireID user authentication requests.

Who is FireID for?

FireID is designed for anyone from private users who want to perform Internet transactions as securely as possible, all the way up to large corporations that depend on access to their VPNs, servers and websites being strictly controlled.

Secure your transactions

FireID means that Internet banking and online shopping are now as safe as they are convenient. FireID is able to deliver unprecedented peace of mind by significantly reducing the risks involved with online transactions and accessing online resources.

The current use of static passwords is not the optimum solution:

- Simple or repeated passwords are easy to crack
- Users write down or store passwords near to their computer
- Key-loggers can capture a user's key strokes
- "Tempest" methods can capture a user's key strokes remotely from 20m away

FireID offers a secure solution for convenient, strong authentication for accessing web services or applications such as Internet banking, e-commerce sites, commercial portals or document repositories.