

Integration with existing systems

FireID is able to integrate smoothly and seamlessly with 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.

Therefore, 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.

The backend server is installed within the company's network infrastructure, or alternatively, hosted by FireID, thereby providing the OTP authentication service, the token deployment system and a web-based management interface.

Fine-grained permissions

Administrators can assign fine-grained permissions to a number of operators using the FireID interface at varying levels, from helpdesk operators able to perform simple user tasks, to super administrators with full control. FireID supports user groups to facilitate user management tasks.

Cost efficiency

FireID offers several cost savings over existing solutions:

- Lower fixed annual cost per user
- No server cost
- No maintenance charges
- Low cost of ownership i.e. distribution and management of hardware costs
- Low integration costs
- No SMS cost for end user

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

www.fireid.com

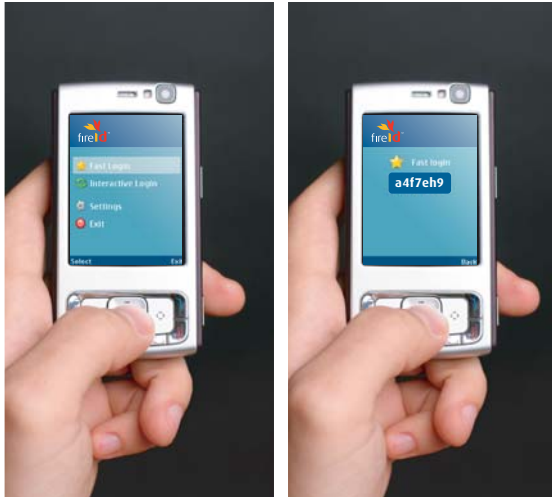
info@fireid.com
+27 21 880 2647

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

Secure
VPN
Online Transactions
Online Banking



www.fireid.com



FireID Features

- Secure one-time-passwords generated on users' mobile phones
- No cellular network connectivity required
- Ease of deployment to almost any mobile phone
- Incorporates your company branding
- Integrates with existing infrastructure using SOAP and RADIUS
- Simple for users to download onto their mobile phones
- Multiple application vectors, e.g. Online Banking, VPN, etc.
- Highly secure and compliant with OATH and FIPS
- Works with existing OATH-compliant authentication servers

Why FireID?

The drawback of static passwords is clearly understood and the increasing regulations around information security have forced a new focus onto alternate solutions for secure identification.

The overhead in providing and managing the distribution of hardware fobs has propelled the need for a soft token solution into the forefront of authentication solutions.

ONLINE BANKING

Securing online banking is essential to financial institutions. Securely authenticating users and, conversely, excluding or easily disconnecting users from accessing their bank accounts via the Internet has never been a higher priority for banks.

FireID allows administrators to securely authenticate users and conversely, exclude or easily disconnect users from accessing bank accounts via the Internet. FireID uses SOAP to authenticate users wanting to access their online banking profiles without the need for hardware tokens or key fobs. Once they are logged in, organisations can require further authentication for specific transactions by requiring their users to perform authentication steps.

ONLINE TRANSACTIONS

Organisations are dealing with ever-increasing volumes of online transactions, particularly with the surge in popularity of cloud computing. While using cloud computing provides a cost effective solution for organisations, a common complaint is that they lack adequate security measures to satisfy stringent corporate requirements.

Organisations can use FireID to authenticate users wanting to access information via the Internet without the need for hardware tokens or key fobs. Once they are logged in, users can be issued with authentication steps for further security. Thus by using FireID, organisations can ensure the authentication of users wanting to access their corporate resources hosted on cloud computing.

VPNS

VPNs carry sensitive information over an insecure network and remote access VPNs often allow full access to the organisation's internal network. Despite security measures, malicious attacks can still reveal information about valid usernames, allowing potential compromise of VPN access.

FireID uses RADIUS to integrate with existing VPN infrastructure to provide organisations with a means to authenticate users accessing their VPNs without requiring them to carry hardware tokens or key fobs.

How does FireID work?

Unlike conventional authentication solutions which make use of expensive and inconvenient key fobs or hardware tokens to generate one-time-passwords, FireID only requires a user's mobile phone.

The process is very simple:

A random one-time-password is generated by the FireID application on the user's mobile phone.

The user then types in the one-time-password for the application he or she wishes to access. The FireID software authenticates the one-time-password. Finally, the request is approved and the user is free to log in. As soon as the user logs in, the password expires and cannot be used again.

How authentication works

FireID consists of two core components: the FireID token application and the FireID Authentication Server. The token application is installed on the user's mobile phone. It performs the task of generating a new random one-time password on demand each time the user needs to login to a FireID protected resource.

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