

# OATH Integration



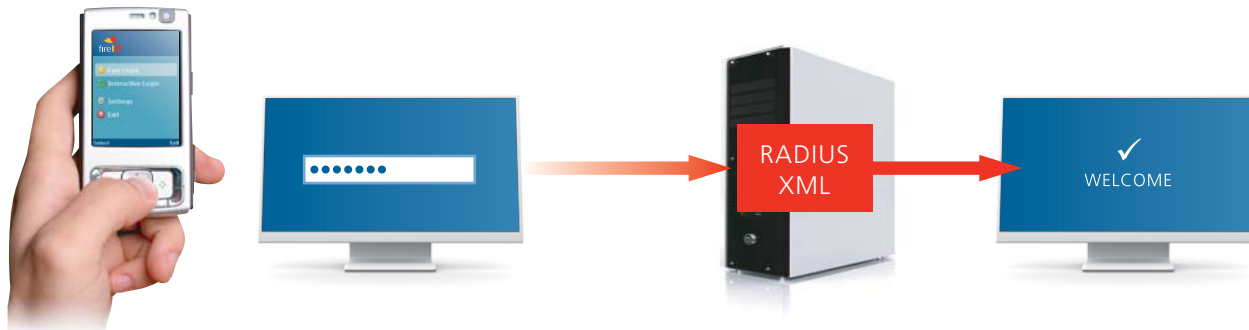
[www.fireid.com](http://www.fireid.com)

[info@fireid.com](mailto:info@fireid.com)  
0860 FIRE SA (3473 72)

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

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

[www.fireid.com](http://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 authentication server authenticates OTP.
- 4** User's request approved and user is logged in.

## OATH integration (VAS Versatile Authentication Servers)

- Secure one-time-passwords generated on users' mobile phones
- No cellular network connectivity required
- Ease of deployment to almost any mobile phone in phone specific format
- Incorporates your company branding
- Integrates with existing infrastructure using SOAP and RADIUS
- Simple to download
- Multiple application vectors, e.g. online banking, online transactions and VPNs
- Highly secure and compliant with OATH and FIPS.
- Will work with existing OATH-compliant authentication servers

## Why FireID?

The FireID token application generates OATH-compliant one-time-passwords (OTP) on users' mobile phones, and can be used with any existing OATH-compliant strong authentication server, such as ActivIdentity's 4TRESS Authentication Server.

This allows customers to deploy a cost-effective and efficient two-factor authentication mechanism to their users, unlike hardware fobs or SMS-based OTPs which present a logistical problem for organisations.

## What is FireID?

FireID is a groundbreaking universal personal authentication system that allows users convenient, out-of-band, secure access to almost any software that requires personal authentication, without the need to remember passwords and by using something they always have with them: their mobile phone.

FireID provides users with three fundamental benefits that set it apart from existing security systems:

1. **One application providing multiple vectors**, e.g. my Bank; my VPN; my Facebook; etc. so users never have to risk writing passwords down or using the same password over and over again.
2. **Elegant deployment to most mobile phones** in phone specific format.
3. **Eliminates the need to carry any other authentication hardware**, e.g., hardware tokens issued by the banks for OTPs (one-time-passwords).

## How does FireID work?

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 third-party authentication server 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 OTP expires and cannot be used again.

## 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. Hence, 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 can easily integrate with an existing OATH-compliant third-party strong authentication server such as ActivIdentity's 4TRESS Authentication Server. The FireID token application will be generated using your existing authentication seed in use by your existing authentication server.

## Cost efficiency

FireID offers several cost savings over existing solutions:

- 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.