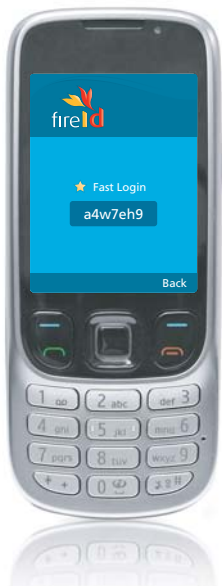


Technical Overview



1
FireID turns the user's mobile phone into a self-contained One-Time Password (OTP) generator. A random OTP is generated by the FireID application on the user's mobile. There is no SMS or Internet activity.



2
User types in the generated OTP. An authorisation request passes through the existing network infrastructure and FireID software authenticates the OTP. The request is approved and the user is logged in.

Introduction

FireID's Universal Personal Authenticator turns any mobile phone into self-contained, out-of-band, one-time password generator. This award-winning two-factor authentication system consists of three components: the Mobile Application, the Authentication Server, and the Provisioning System.

The FireID Mobile Application

is the end-user's interface to the FireID solution. It is easily deployed and installed to any mobile phone, with native versions/builds for specific handsets or platforms where appropriate. The deployment process automatically detects the mobile phone make, model and platform, and delivers an appropriate version of the application.

The FireID application is capable of storing one or many different OTP "tokens", which are used to securely generate one-time-passwords, without requiring any GPRS/EDGE/3G or SMS activity. These tokens can also do Transaction Verification or secure Mobile Web logins.

Transaction Verification — Secures payments and transactions thus preventing man-in-the-browser attacks. The FireID Transaction Verification application generates a unique code for each transaction. This code is based on the full transaction details (amount and account), and can be verified by the server for authenticity. If an attacker attempts to change any details, the code will become invalid, and the server will detect the tampering

Mobile Web — Token can be used to login securely to any website using a mobile phone's built-in web browser. This functionality embeds a FireID-generated OTP into a URL, effectively creating a one-time-URL for logging users into a secure website using mobile phones.

The FireID Authentication Server

is responsible for authenticating users' OTP's as generated by FireID on their mobile phones. The authentication server is able to identify if the password supplied by the user is correct or not using an incremental algorithmic process. It can be easily integrated into the backend of the system such as VPN devices, and web applications via RADIUS or SOAP.

The FireID Provisioning Server

is used to deliver the Mobile Application to the end-users' mobile phones. This innovative method of delivering an application to mobile phones is a 24/7/365 hosted service provided by FireID or can be installed within your secure corporate network.

Integration

The FireID server-based solution is hosted internally by our clients using their own infrastructure. FireID integrates seamlessly with your client database(s) using Active Directory, LDAP, and ODBC, while authentication integration is done via RADIUS or SOAP. FireID also provides a SOAP API for richer integration to other applications.

Technical Details

Algorithms and Standards

STANDARD NAME	TYPE/FUNCTION	OFFICIAL SOURCE
OATH	Open authentication specification for a standard method for generating OTPs	www.openauthentication.org
SHA-256	Hashing algorithm	US FIPS 180-3
AES Rijndael 256	Symmetric encryption	US FIPS 197
HMAC	Message Authentication Code	US FIPS 198-1

System Requirements

Hardware environment

A dedicated computer:

- 1 GHz processor
- Supports 32- and 64-bit CPU's
- Minimum 1Gb RAM
- Minimum 6Gb disk space
- Network adapter with Internet connection
- CD or DVD ROM drive

Virtualized Environment

- VMware Server t
- Microsoft Hyper-V
- Xen

Mobile Platforms Supported

