

TwoSecure™

control who accesses your
networks and online applications



FRONDE
anywhere



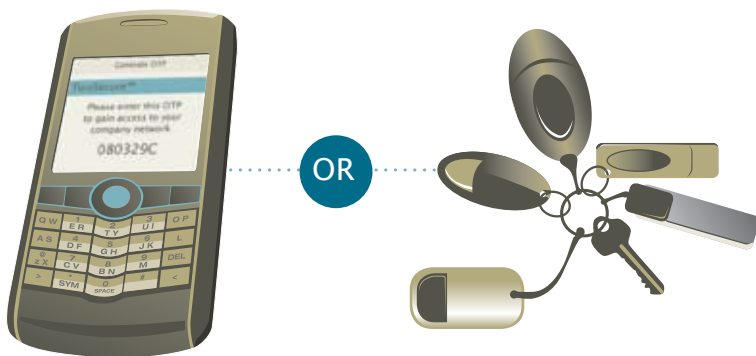
TwoSecure™

An easy to use two factor authentication solution that generates one time passwords (OTPs) via an application on the mobile phone.

TwoSecure™ enables strong authentication using the mobile phone. With no costly hardware tokens to supply, TwoSecure™ is easy to support and distribute for a large number of customers or staff. The mobile phone replaces the need for hardware token generators, making it more cost effective for you, more convenient for your users and more sustainable for our environment.

Whether accessing a company network or completing an online transaction, TwoSecure™ provides an additional level of authentication. The tiered security model, allows you to select the appropriate level of security for your needs. Options include a Standard OTP, a Challenge Response OTP and a Transaction Signed OTP.

The TwoSecure™ application works on most mobile phones. It is easy to download and activate and uses only a small amount of space on the mobile phone. With TwoSecure™ there's no need to carry additional security devices, or remember any extra passwords. Secure, convenient and easy to use.



“By migrating existing hardware two-factor authentication token users to a mobile software or service authentication solution, organisations can cut costs by between 30 and 60 percent.”

Alan Goode, Managing Director, Goode Intelligence
- author of “The Mobile Phone As An Authentication Device” - 2010-2014”.

TwoSecure™ scenarios

TwoSecure™ is currently being used all over the world as an authentication solution for staff, customers or both. TwoSecure™ can be deployed as a standalone product, as part of a wider mobile service offering on the Anywhere Platform, or managed by an organisation on a Software-as-a-Service (SaaS) basis.

Staff

- For enterprise staff accessing email and business applications while travelling, or working from home.
- For businesses seeking to secure staff access to Google Apps and other cloud services.
- For any company that needs to allow (or suspend) real time access for external contractors or suppliers.
- For government agencies, to secure remote access to all agency and inter-agency back office and business systems.
- For bank staff to authenticate themselves when logging in to highly secure bank systems.

Customers

- For bank customers to authenticate themselves when logging on to Internet Banking, or for additional security when making high value transactions.
- For payment providers to add security to online transactions.
- For telcos to offer authentication services for corporate and SME business customers on a SaaS basis.
- For government agencies to allow secure public access to government sites.
- For ISP customers to secure internet or wifi access, using an OTP in place of a WEP/WPA password.

The security behind TwoSecure™

TwoSecure™ delivers enhanced security by ensuring the user has both their username and password (something they know) plus, their mobile phone (something they have). If either of these two requirements is not met, authentication of the user fails.

To use the service for the first time, the TwoSecure™ application must be successfully activated on the user's phone. Each user profile is tied to a specific application (one phone, one user profile) so each application is unique.

TwoSecure™ uses a time based algorithm based on a highly secure digest and two unique security codes that are generated during registration. This ensures that each OTP generated is unique to the credentials of that user.

Security features

- Every TwoSecure™ application is unique to the user.
- OTPs cannot be used twice.
- Optional addition of a PIN / passcode.
- Optional use of transaction signing or challenge response for high value transactions.
- No customer, company or PIN data is stored on the phone.
- No sensitive information is passed over the network unencrypted.
- Users can be suspended or "locked out" at the server side.
- Supports SAML authentication.
- OATH compliant.

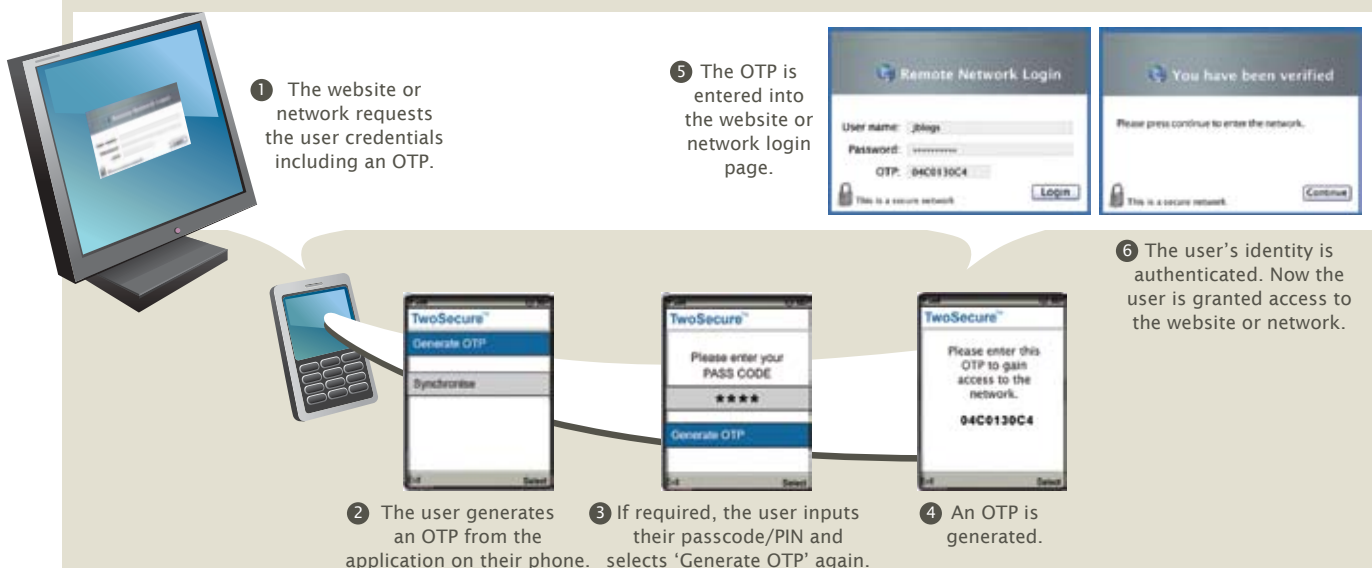
Securing cloud or SaaS services

TwoSecure™ can be deployed into an individual organisation, or deployed into a cloud computing environment and offered to multiple organisations on a Software-as-a-Service (SaaS) model. Each organisation has a fully partitioned view of their own users, administrators and TwoSecure™ services. A SaaS deployment model is proving popular with organisations such as telecommunications providers that want to extend the range of the SaaS offerings they provide for their corporate and SME customers.

TwoSecure™ includes a SAML single sign on (SSO) interface that integrates with Google Apps.

Generating an OTP to login to a web site or remote network

In order to complete the authentication process a user must not only know their username and password, they must also be in possession of the mobile phone registered against their profile.



Implementing & configuring TwoSecure™

Implementing TwoSecure™ is quick and cost-effective because it integrates easily with existing systems and security measures.

- TwoSecure™ includes web service interfaces for integrating user management and OTP services. This allows for easy integration with registration channels such as IVR or Internet as well as websites for authentication.
- The TwoSecure™ Radius interface for OTP validation provides integration with network appliances such as firewalls, proxies and domain controllers.
- TwoSecure™ can be deployed directly into your organisation, or it can be accessed as a SaaS service.
- TwoSecure™ has been benchmarked and tested using IBM hardware. The solution has been independently assessed against US FFIEC guidelines for two factor authentication compliance.
- An optional SMS version of TwoSecure™ is also included with the platform, where the OTP is pushed to the mobile phone via text message.
- TwoSecure™ can be operated by SaaS providers as a cloud service for many organisations.
- TwoSecure™ can be run on a shared installation with other products on the Anywhere Platform.

TwoSecure™ also offers a high degree of configurability managed via the user friendly administration console. Customise TwoSecure™ to align with your brand identity and support deployment in multiple regions. You can change:

- Branding, colours, logos
- Wording and labels
- Language and character sets
- Security levels
- OTP length
- OTP validity period
- OTP numeric or hexadecimal format
- OTP seeds for transaction signing
- Google SSO login page.



About Fronde Anywhere

innovation : mobility : security : payments

Fronde Anywhere provides mobile payment and security solutions to banks, payment providers and mobile operators. The Anywhere platform is the only product that delivers secure mobile channel, payment and security services from a single system.

The Anywhere platform ensures unparalleled security for all mobile services by linking a specific user's identity to their mobile device. Fronde Anywhere's patent pending identity verification technology also underpins, TwoSecure™ the award winning two factor authentication product module. This unique combination of services from one platform sets Fronde Anywhere apart from its competitors in both the mobile services industry and the identity management space.

The Fronde Anywhere team has been developing and delivering pioneering mobile solutions since 2001. Fronde Anywhere serves clients in Europe, North America, New Zealand and South East Asia from its offices in London and New Zealand.

All specifications are subject to change at Fronde Anywhere's discretion.

For more details about TwoSecure™ or to request a demo contact sales@cirrus-ms.co.uk

Distributed by: CRRUS Management Solution Ltd
Milton Innovation Centre, 99 Milton Park,
Abingdon, Oxfordshire, OX14 4RY. Tel: +44(0)1235 854048
Email: info@cirrus-ms.co.uk Web: www.cirrus-ms.com

TwoSecure™

control who accesses your
networks and online applications



FRONDE
anywhere