

The security logic behind TwoSecure™

Two factor authentication (or dual factor authentication) is any authentication protocol that requires two independent ways to establish identity and privileges. This contrasts with traditional password authentication, which requires only one authentication factor, (such as knowledge of a password) in order to gain access to a system.

Common implementations of two factor authentication use 'something you know' (a password) as one of the two factors, and use 'something you have' (a physical device) as the other factor.

TwoSecure™ delivers enhanced security by ensuring the staff member has the following:

- + User name and password for the system (something they know)
- + Their mobile phone (something they have)

If either of these two requirements is not met, authentication of the user fails.

The **TwoSecure™** mobile application uses a time based algorithm based on a highly secure digest and a unique security code generated during registration. This ensures that each OTP generated is unique to the credentials of the staff member who has registered the mobile phone from which the OTP was generated.

To use the service, the **TwoSecure™** application must be successfully activated, either by entering a user name and password or a specific code supplied when the user was added to the authentication service.

If a staff member finds they have generated an invalid OTP, the synchronise functionality on the **TwoSecure™** mobile OTP generator allows them to resynchronise the **TwoSecure™** application on their phone with the **TwoSecure™** server. For example, a staff member may need to use the synchronise functionality if they have moved to a different time zone and adjusted the time on their mobile phone.

If a fraudulent user obtains the OTP generator software and someone else's user name and password they will still be unable to pass the **TwoSecure™** check. This is because the security code embedded in their software will not match the one created for the genuine user. This means that the tokens generated by the fraudulent user will never match those created by the organisation - i.e. access will always be denied.



FRONDE

anywhere

Fronde Anywhere offers mobile banking, payment and two factor authentication solutions for retail banks and the wider financial services industry. Its portfolio of user-friendly solutions enables customers to make payments and bank transactions via their mobile device from any location.

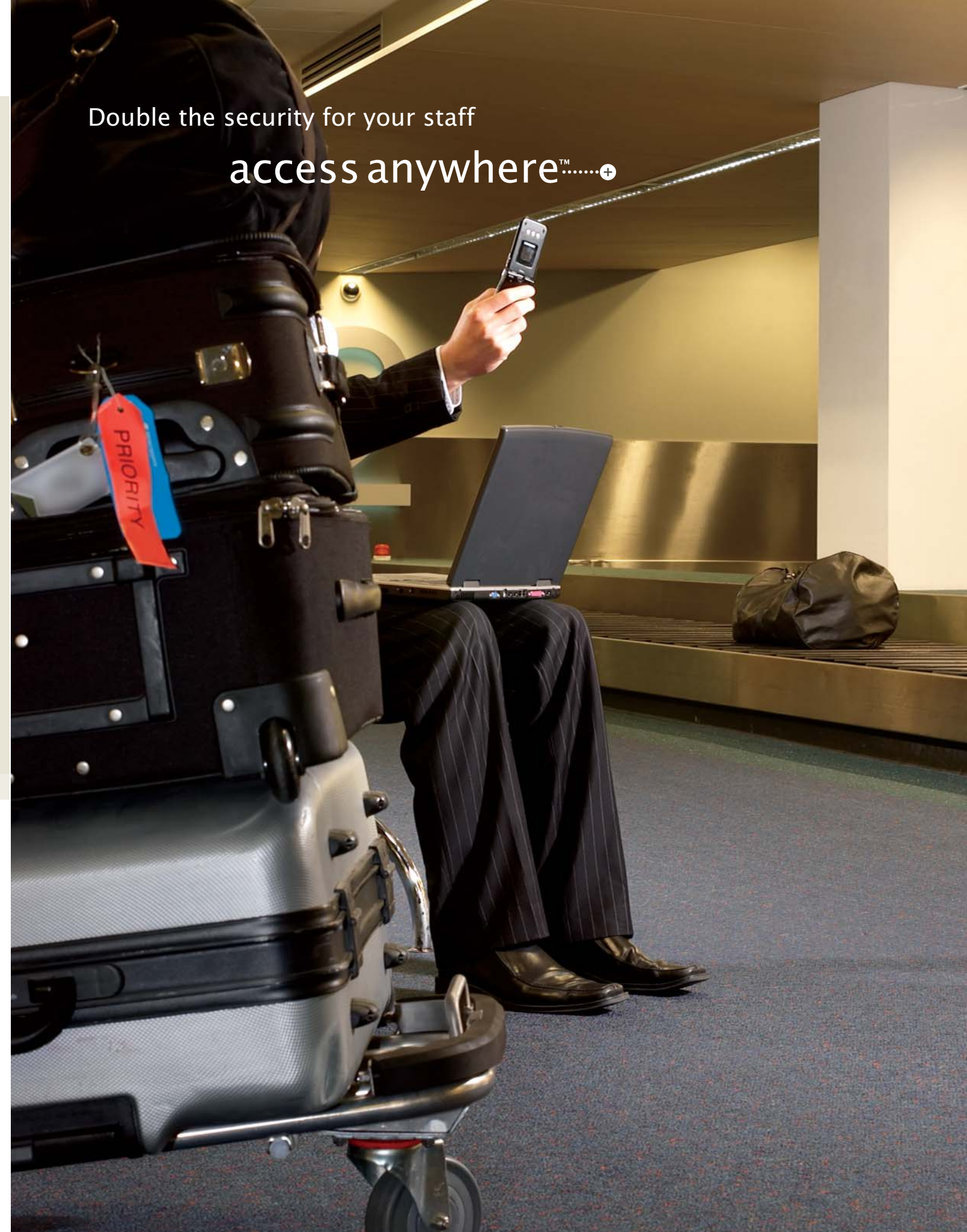
Fronde Anywhere's mobile technology, provides enhanced security for authenticated access to online banking or remote networks.

The company has built its reputation on the proven delivery and implementation of first to market mobile products and solutions that deliver real business benefits to its clients.

Fronde Anywhere is part of the Fronde Systems Group, which serves clients in Europe, North America, Australasia and South East Asia from its offices in London, New York, Singapore and New Zealand.

All specifications are subject to change at Fronde Anywhere's sole discretion.
Contact sales@frondeanywhere.com or view our website www.frondeanywhere.com for more information on **TwoSecure™**.

Double the security for your staff
access anywhere™.....+



EN-TS-3-0607

TwoSecure™

FRONDE
anywhere

TwoSecure™

Double the security for your staff access anywhere™

TwoSecure™ gives your staff a second level of authentication when they remotely access your network and business systems.

Remote working offers huge benefits in terms of productivity and flexibility for your staff – but it carries with it the risks inherent in the online environment: the potential for your company's security to be compromised and malicious damage done to data or systems.

Fronde Anywhere **TwoSecure™** is a solution that will give you and your staff the confidence to work remotely – from home or while travelling – safe in the knowledge that only genuine trusted parties are accessing your valuable core systems.

TwoSecure™ combines static and transient credentials to make it extremely difficult for a third party to assume a staff member's identity.

When **TwoSecure™** has been added to your network's security, a staff member must not only know their user name and password, they must also be in possession of the mobile phone that has been associated with their user account, in order to access your company's systems. The **TwoSecure™** One Time Password (OTP) generator is deployed to the staff member's phone and used to generate a unique time-limited OTP.

Benefits for you

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

With **TwoSecure™** you can:

- + Reduce distribution costs by eliminating the requirement to provide or replace hardware tokens
- + Integrate with existing authentication servers
- + Optionally add additional layers of security, such as pass code protection of the OTP
- + Provide an additional layer of security with minimal costs
- + Remotely suspend or disable individual users
- + Brand the mobile OTP with your company logos, colours, and font styles
- + Configure the length of time the OTP is valid
- + Configure the length of the OTP
- + Have increased confidence that all remote access is by genuine staff members.

Benefits for your staff

Your staff appreciate the importance of security, but they also value flexibility in their working environment. They want the freedom to work from home or in transit – without having to scale complex barriers to access the systems and services they need. **TwoSecure™** employs familiar devices and processes to make remote working smooth as well as secure.

Your staff can have:

- + No additional devices to carry
- + No extra passwords to remember
- + An easy to use application
- + The confidence that no third party can impersonate them
- + No ongoing mobile data charges to worry about – **TwoSecure™** works offline
- + Secure access in any country to the systems and services they need to do their job effectively.

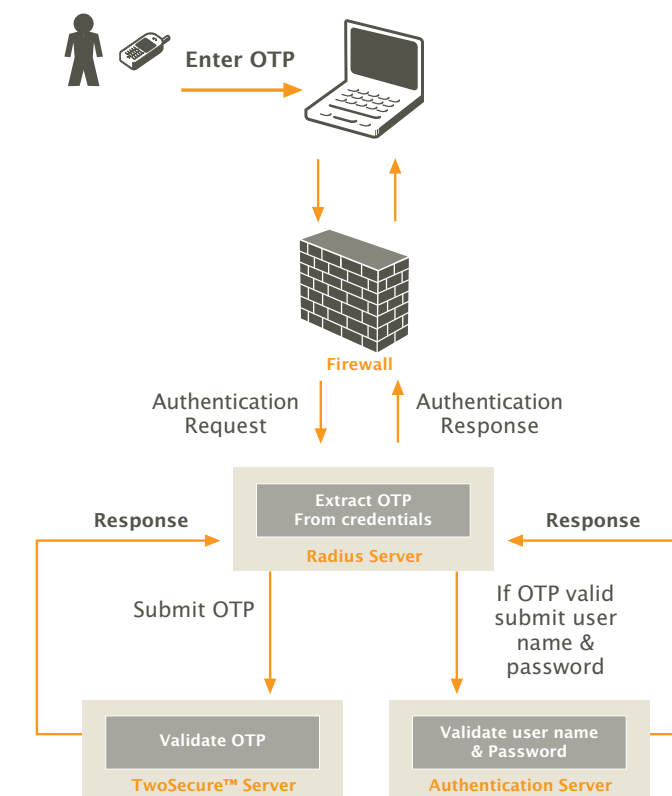
How it works

TwoSecure™ deploys a small application to your users' mobile phones, the application is then accessed when required to generate OTPs. The OTP in combination with user name/password credentials boosts security for remote access to your network.

Here's how it works:

- 1 A staff member needing to work remotely is added to the **TwoSecure™** server and downloads the **TwoSecure™** mobile application to their phone.
- 2 The **TwoSecure™** mobile application is deployed to their phone.
- 3 The staff member activates the **TwoSecure™** OTP generator by entering their staff credentials (or a unique activation code provided in step 1).
- 4 When the staff member wishes to access the network they use the **TwoSecure™** application to generate an OTP.
- 5 The staff member enters the OTP as well as their user name and password into the network log in interface. No connection to the **TwoSecure™** server is required at this time.
- 6 The user credentials are submitted by the firewall to the **TwoSecure™** server. The OTP is extracted and validated.
- 7 The user name and password are then authenticated using the enterprise's existing network authentication.
- 8 Once authenticated the staff member is provided access to the corporate network.

If the OTP is identified as valid by the **TwoSecure™** server, the staff member will be granted access. If the OTP is invalid, the staff member will be notified.



Implementing TwoSecure™

The **TwoSecure™** server exposes a standard Radius interface to the firewall that is providing the remote network access. Radius is a well used standard for network authentication thus is supported by many existing firewalls.

The server can also provide authentication of the user name and password or can be integrated with an existing authentication system such as Microsoft Active Directory or Novell Directory.