nccgroup

Signify Software Tokens

Managed Security Services

The Signify Software Tokens deliver market leading RSA two-factor authentication by turning an Apple iPhone, iPad or iPod Touch, BlackBerry, Android or Windows Mobile device into a strong authentication token. Our service makes it easy to securely identify users 24/7 by confirming they have their smartphone or mobile device with them. As a fully hosted service we ensure that the service works securely and reliably. Signify Software Tokens are ideal for users who need secure remote access from any computer, but don't want to carry a token in addition to their other mobile devices.

What are Signify Software Tokens?

Signify Software Tokens allow a user's Apple iPhone, iPad or iPod Touch, BlackBerry or Windows Mobile device to be used as a strong authentication token. The Signify service delivers RSA software tokens which work just like RSA's market leading SecurID keyfob tokens. Delivered by the Signify hosted service you get RSA security and reliability with the convenience of using your own smartphone or mobile device.

When a user wishes to access their corporate data remotely using their remote access gateway, they simply enter their secret PIN into their mobile device's token application. This then generates a one time passcode which the user then enters into the password field on their remote access gateway. By demonstrating that they have these two 'factors' (a secret PIN and their smartphone or mobile device) the user is securely identified. Signify Software Tokens provide an alternative user experience to hardware tokens because they enable users to use their preferred mobile device to authenticate themselves.

A complete managed service

The successful deployment of two-factor authentication takes more than just technology; you also need to implement a framework of policies, procedures, logistics and user support. These are automated through key features of our service:

- Authentication Infrastructure: Security and reliability is designed in and implemented across multiple data centres, to deliver and validate one time passcodes every time with a track record of 99.999% service availability.
- The Identity Management Centre (IMC): Manage all aspects of your service through our easy to use web portal. This portal gives you more control and visibility of the service than if you ran the servers yourself.
- End User Web Helpdesk: Our 24/7 self-service web helpdesk lets your users resolve their common problems such as forgotten PINs. This reduces your costs and improves the end user experience.

Benefits

Reliable

- Works without mobile phone network coverage
- Distributed and resilient infrastructure
- SLA backed service

Secure

- Market leading RSA software token
- Infrastructure designed and managed with security in mind
- Secure web portal administration

Flexible

- Mix our token and tokenless services
- Utilises your user's existing smartphone device
- Variety of contract lengths

Quick and Easy

- Compatible with all leading VPNs, firewalls and web servers
- No training required
- Efficient software token provisioning process
- No physical token to deploy

- Software Token Provisioning Process: The software token and seed record is simply pushed to a user's Apple iPhone, iPad or iPod Touch, BlackBerry or Windows Mobile device upon request, ensuring that provisioning is quick and easy for the user. We achieve this by streamlining the set up procedure for each user, to ensure they can start working first time, every time, without adding load to your already busy IT team.
- You may not want a software token for all your users. The range of Signify services make it easy for you to give each user the most appropriate form of authentication to match their working pattern and security privileges. You can mix and match the Signify Software Tokens with our RSA SecurID from Signify and Signify Passcode On Demand services.

How it works

- A user working remotely needs access to information, a system or a network.
- They make a connection to the remote access device or web application they wish to use. They are asked to enter their details.
- The user runs the software token app they have on their smartphone. They enter their secret PIN into the app, which then generates a one time passcode.
- They enter their username and the one time passcode generated by the software token on their smartphone.
- These credentials are submitted to Signify for validation.
- If successfully authenticated the user is granted access.

What is included in the service?

Authentication Device

- Uses the existing smartphone or mobile device each user already carries.
- Software token is installed as an additional application.

Authentication Service

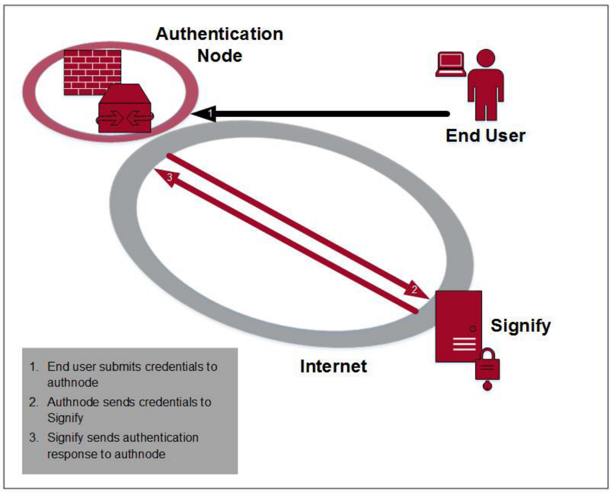
- Annual service fee per user.
- Unlimited authentications per user.

Organisation Base Pack

- IMC web portal for administration.
- Telephone/email support for administrators from our dedicated support team.
- End user web helpdesk for automated resolution of end user issues.

Optional Features

- Discounts for multi-year contracts.
- Software token life to suit how long you keep your smartphones or mobile device.


Authentication Node
End User
1
3
2
Signify
Internet
1. End user submits credentials to authnode
2. Authnode sends credentials to Signify
3. Signify sends authentication response to authnode

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group, please contact:

+44 (0) 1223 472572 signifysales@nccgroup.trust www.nccgroup.trust