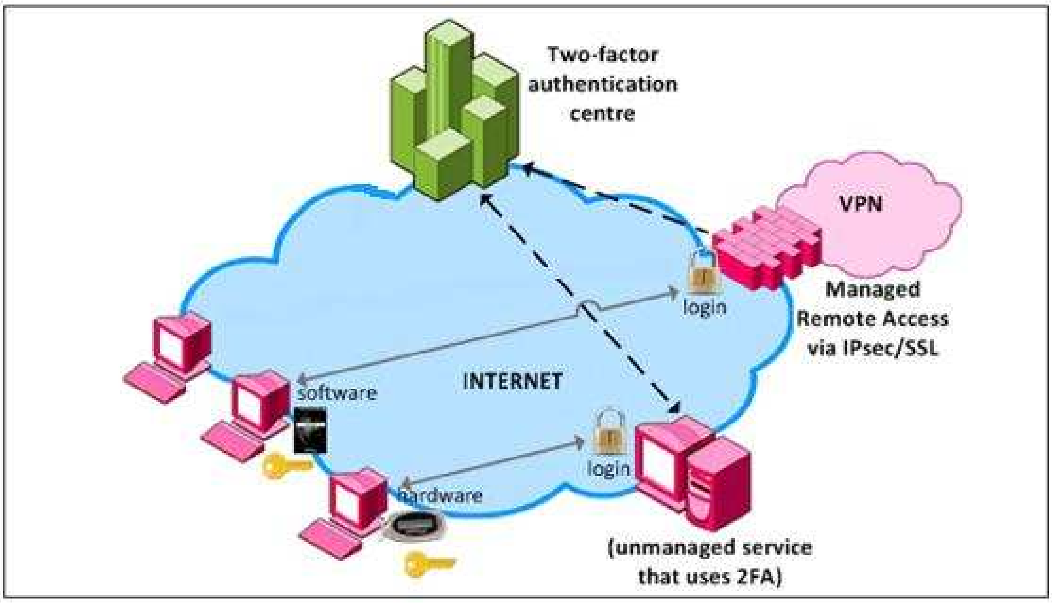
Managed Secure Remote User Authentication

interoute
from the ground to the cloud


Two-factor authentication centre
VPN
Managed Remote Access via IPsec/SSL
login
software
INTERNET
login
hardware
(unmanaged service that uses 2FA)

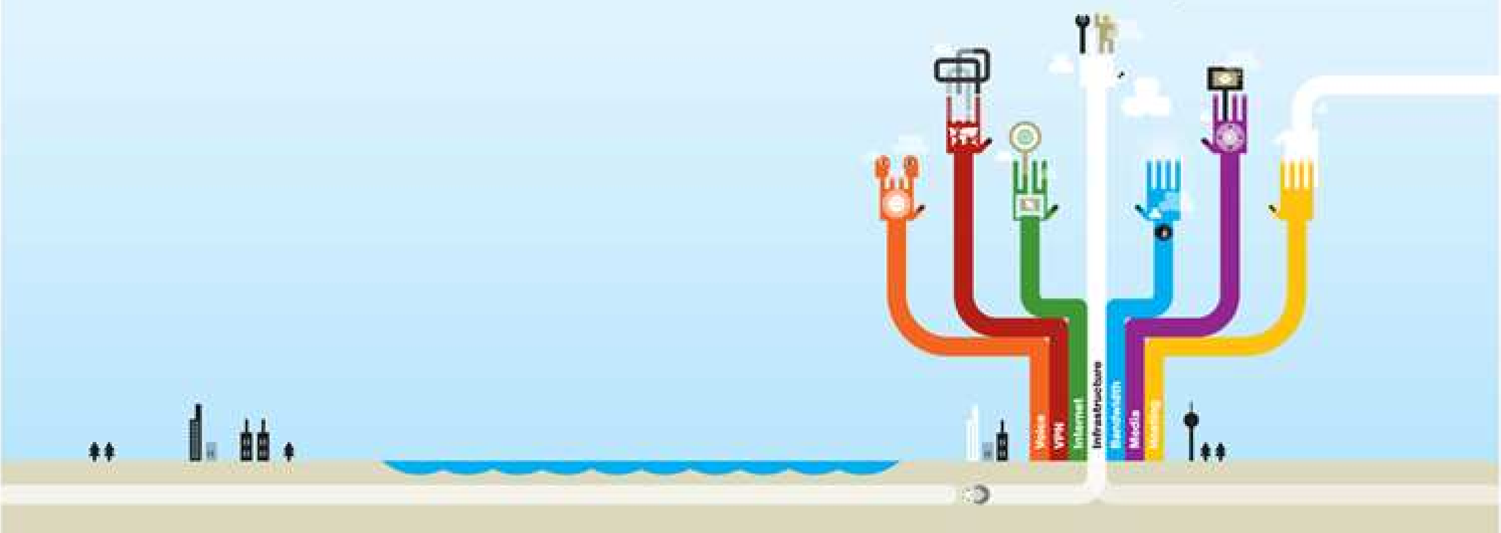
Overview

The Managed Secure Remote User Authentication service replaces static passwords with personalised, one-time passwords via a "token" which can be used to grant access to the Interoute-supplied Roaming Access service and extended to cover your own (or third party) cloud, applications or network.

The two factors involved here are 'something you know' and 'something you have'. A common example of this combination is a bank card: the personal identification number (PIN) is a secret know by the user, and the card itself is the physical item (token).

The password an end user utilises to make use of this service is composed of a PIN and a piece of information provided by a hardware or software token.

This multiple factor authentication reduces the incidence of online identity theft, because a password is no longer enough to give a thief access to your VPN or applications.



Technical Service Details

Interoute, using carefully selected third parties, supplies and supports Two-Factor Authentication (also known as 2FA) as either as a complement for Roaming Access via IPsec or SSL as well as a standalone service for your own specific needs (for example, access to a web server, a cloud service, etc.)

Once implemented, the customer (via a nominated administrator) assumes control of the management and provisioning of its token inventory using the 3rd party's web portal.

The web portal allows the customer and their end users to perform basic operations with their tokens, such as token re-synchronisation and PIN change.

When ordered as a standalone service, the customer is responsible of configuring their equipment to send authentication requests directly to the 2FA supplier's infrastructure. Interoute can provide configuration documentation from the supplier as well as give support customers who require it.

Interoute 2FA service is supported by hardware or software tokens:

Hardware tokens (fob)

A hardware token is similar to a key-fob, which shows the current one-time password. The token is synchronised with the authentication server and the password cycles regularly.

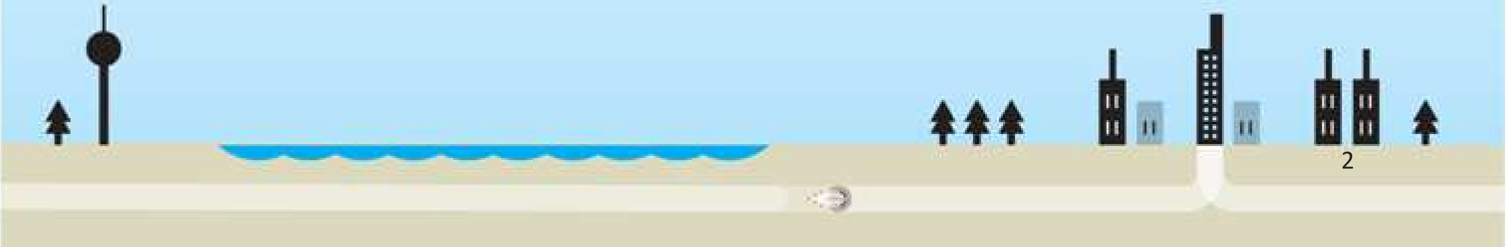
Hardware tokens are tamper-resistant, tamper-evident and machine independent, allowing a user to logon from any location or machine.

Software-based token

A cryptography piece of software is installed on your computer or smart phone, which generates a one-time password anytime you have to present your login credentials.

Software tokens can be massively deployed without hardware distribution. See the table under Customer Requirements for available platforms.

Note: Interoute provides limited support for software-related troubleshooting (see Limitations).



Customer Requirements

Once the tokens are shipped to a designated customer location – for hardware tokens – or made available to the customer via the 3rd party portal for software tokens – it is the customer's responsibility to enrol the end users.

The software tokens can be used on the following platforms:

Platform	Operating System
Windows PC (32/64 bit)	XP, Vista, 7, 2003 Server, 2008 Server
iPhone, iPad	iOS 4.1 or later
BlackBerry	OS 4.5 or later

Table 1: Platform and operating system availability for software tokens

Supported Service Changes

- For any existing service, you can order additional tokens (regardless of type)

Reporting

Token usage log and any authentication events are available via the 3rd party web portal.

Limitations

Support scope for software tokens is limited to dealing with outages affecting the 2FA provider service; any problems resulting from non-network customer configuration or faults in computer and network operating systems (e.g. Windows, Blackberry, Apple iOS, etc.) or any third party software are not within scope.

Billing

The following Billing plan is available for Interoute's Managed Secure Remote User Authentication Service:

- An initial non-recurring charge for service setup and – if applicable – token purchase.
- A monthly flat rate charge based on the number of tokens

Product Codes

Service	Code
Two-Factor Authentication	SVC-TOKEN

Related services

The Managed Secure Remote User Authentication Service improves security of Roaming Access Service to VPN

How to order

Order through an Interoute Account Manager or via the HUB, Interoute's online portal.

More information

For product enquiries, please consult the Security Services Product Manager.