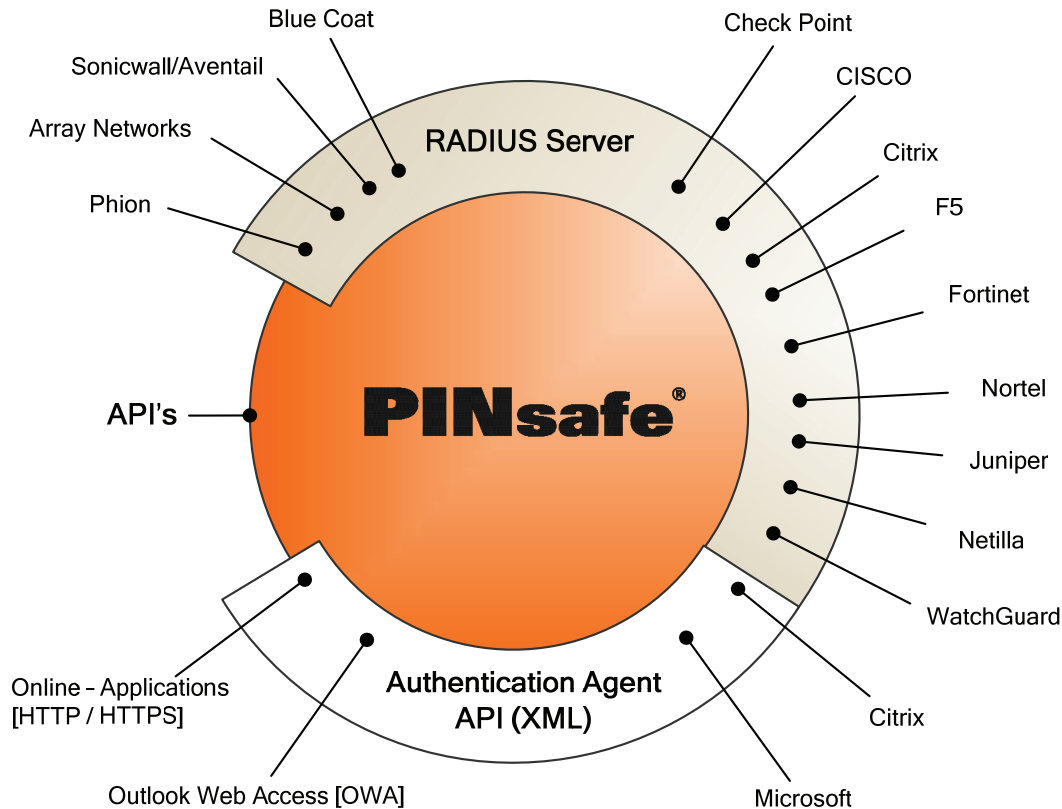


Strong Multi-Factor-Authentication — Integration

PINsafe offers an integrated Radius server technology with an easy-to-use interface for the integration of established VPN and remote access solutions:

- **Array Networks**
- **Bluecoat**
- **Checkpoint**
- **Cisco**
- **Cisco ASA**
- **Citrix Access Gateway Advanced**
- **Citrix Access Gateway Enterprise**
- **F5**
- **Fortinet**



- **Juniper**
- **Microsoft IAG**
- **Nortel**
- **Netilla**
- **Sonicwall/Aventail**
- **Phion**
- **WatchGuard**
- **Imprivata SSO**

XML - Interface:

- **Microsoft IIS**
- **Microsoft ISA Sever**
- **Microsoft Outlook Web Access**
- **Citrix Web Interface**
- **Microsoft IAG**

There is also an *Application Programming Interface (API)* and an *Authentication Agent API via XML* for easy integration with other systems.



Strong Multi-Factor-Authentication — PINsafe

What is PINsafe?

PINsafe is a patented authentication solution which guarantees users a secure access to networks and computers without additional hardware (e.g. token). Using secure network connections (VPN), websites, corporate applications and/or mobile devices PINsafe assures a secure authentication procedure.

Why PINsafe?

PINsafe is applied to ensure only full authenticated users. Based on a unique combination of registered PIN-numbers and randomly generated security codes, sent to the users in an optimal way, PINsafe is one of the most secure, simple to use, reliable and economic authentication solutions in the market.

PINsafe - Total Cost of Ownership (TCO)

Beside the enormous security advantage there are a lot of additional positive facts regarding PINsafe:

- One time installation and never ending **LifeTime License**.
- No Client Software Installation
- No need to renew token or software every three years.
- No external or internal administration costs.
- PINsafe users can be managed very simple with existing user repositories (e.g. Active Directory form Microsoft) - this means quick roll out of the license and easy management.
- The internal administration costs e.g. for shipment, replacement and personalization of token can be reduced to a minimum - because PINsafe needs no token.

PINsafe - mode of operation

The patented One Time Code extraction can be used in combination:

A) via SMS (or App, if user is offline)

-> **Mobile Phone as a Token**

B) via Security Code at the Login Screen

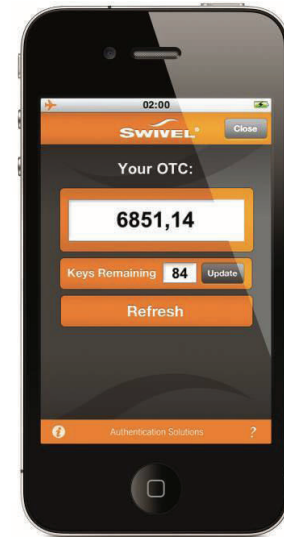
-> **No use of Token**

C) via PositivelD

-> **PC/Laptop as a Token**

This technology uses additionally the PC/Laptop ID (e.g. ID of the processor, Mac-ID).

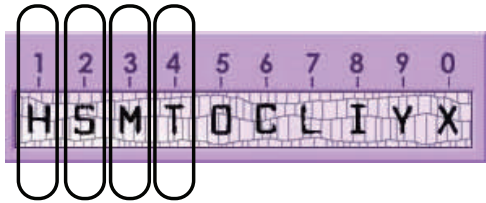
The original PIN number will never be entered directly for authentication!



Patented One Time Code (OTC) Extraction

Example 1

PIN: 1 2 3 4



OTC: H S M T

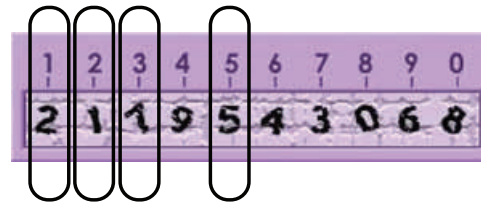
One of the **unique features** of PINsafe: The user only requires the randomly generated security code and a PIN-number of her/his choice from memory for authentication.

The One Time Code (OTC) extraction process is very simple to use: the PIN number defines, which positions and sequences of the security code have to be entered as OTC.

Example 1 above shows the combination of the PIN number 1 2 3 4 (from memory of the user) and the security code - resulting to an OTC of „H S M T“.

Example 2

PIN: 2 3 5 1



OTC: 1 7 5 2

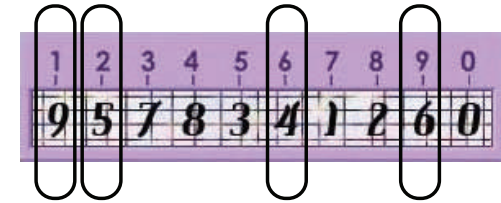
The PIN number can be varied from 4 to 10 positions. The security code can be letters, numbers or letter-number combinations.

The big advantage: The OTC generated from the user varies for each authentication process. Also the PIN number will never be entered directly for authentication.

The authentication process requires two elements: the security code, which be sent to the user in different ways AND the PIN number from the memory of the user. The user never enters directly her/his PIN number for authentication. Thus e.g. key-logging or attacks are useless.

Example 3

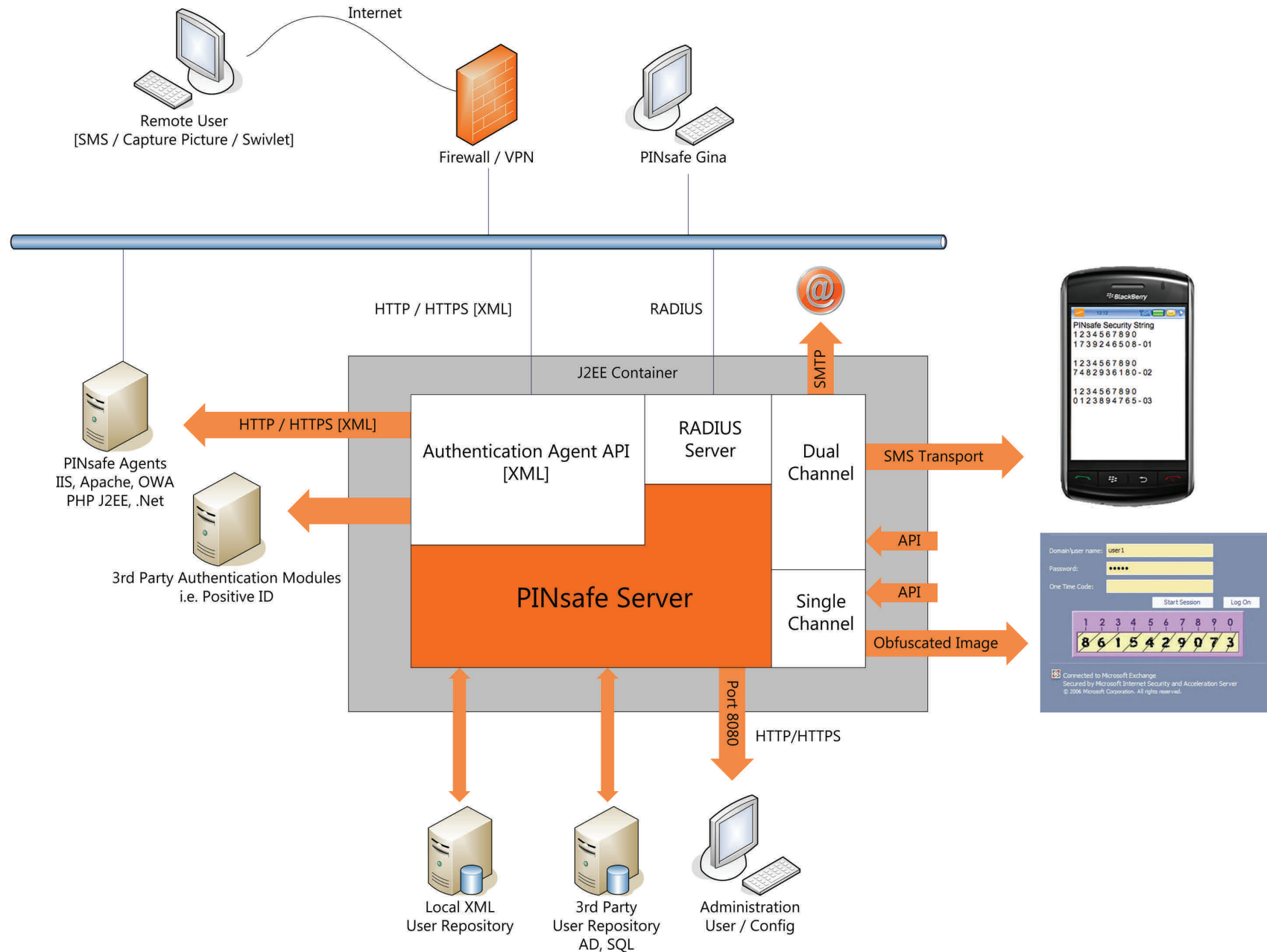
PIN: 1 2 6 9



OTC: 9 5 4 6

The transition of the security codes can be binded on a special channel - e.g. Mobile Phone or PC. Thus a real 2 Factor Authentication can easy be realized.

The main advantage of this model is the easy implementation in different environments. With this unique model you can decide, how strong the chosen authentication scheme must be for different user groups. You can determine for example to present the security code as obfuscated, non-machine readable CAPTCHA image at the VPN Login screen or sent via SMS to the mobile phone of the user.



simplicity

security

freedom

About the company

Established in 2000 and headquartered in Wetherby, U.K., Swivel Secure is specialized in network security solutions. **PINsafe**, Swivel Secure's multi factor authentication, based on patented technologies and thus providing proved security to organizations of all shapes and sizes.

Swivel Secure is a full member of the worldwide Marr T&T Group of companies headquartered in London, U.K. In 2009 the Marr Group realized a business volume more than one billion US\$ based on 8 different product groups. Part of the technology division at the Marr group beside Swivel Secure includes the affiliated companies like Wavecrest, Mobix or ROK, offering solutions in the Telecommunications- and IP-Networking area.

Over the international sales network Swivel Secure supports customers from industry, finance, retail, legal, as well as state and health authorities in over 30 countries.

Swivel Secure provide establishments in the U.K, Spain, France, Portugal, USA and Germany.

Swivel Secure

Cologne, Germany

+49 221-510 7951

www.swivelsecure.com

ce@swivelsecure.com

IT 2 Trust

Brøndby, Danmark

+45 7022 3810

www.it2trust.com

info@it2trust.com