

SA Server with SMS – OTP

||||| One-time passwords go even further



FINANCIAL SERVICES & RETAIL

ENTERPRISE > PRODUCT

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

SMS – OTP Authentication

IIIIII Extending the Gemalto family of OTP devices

With the release of Strong Authentication (SA) Server 3.0, Gemalto has extended the breadth of devices that can be used for one-time password (OTP) authentication. In addition to a family of compatible smart cards and USB tokens, SA Server 3 can securely send a one-time password to any GSM mobile phone using Short Messaging Service (SMS).

This solution provides a safe and convenient authentication method for end users. It enables them to securely access the network wherever they are and not be burdened with carrying an additional authentication device. SA Server with SMS-OTP also gives IT and security teams the ability to leverage two-factor authentication for all users without having to invest in additional authentication devices. It also provides a back-up method for OTP delivery when the user's primary OTP token has been lost, stolen or broken.

■ Highly adaptable OTP solutions

SA Server 3.0 offers a convenient solution for SMS-based OTP authentication with the following benefits:

Maximum availability – implement two-factor authentication policies for all users with ubiquitous mobile phone platform

Hardware cost savings – provides two-factor authentication without investing in additional end-user devices, making the solution ideal for large organizations

No maintenance or renewal needs
Secure network access – two-factor authentication enabled with event-based one-time passwords that have pre-determined validity timeframe
Scalable and adaptable – support for most MMOs and global deployments with high user volumes



Easy to use – simple user experience with no client software to install and maintain and no impact on customer phone

Flexible – ad hoc account creation and SMS profiles can be easily created or updated in a few minutes

■ User-friendly

One-time password authentication is achieved in a two-step process:

First, the user provides the correct User ID and password and requests an SMS one-time password. The server validates the credentials and sends an OTP with a pre-determined validity time.

Next, when the OTP is received by the user, it is entered for secure two-factor authentication in the same way as an OTP that was generated by a hardware token.

■ Flexible and easy to implement

SMS profiles define the format for the message that is sent to the user with the one-time password. Multiple SMS profiles are supported but only one profile at a time can be active and

send the SMS one-time password. With SA Server 3.0, they are easily created and managed with an intuitive, menu-driven interface. New Mobile Messaging Operators (MMO) can be added and either HTTP or SMSC message protocol can be selected.

The SMS profile management interface is also used to specify OATH policy parameters. The OTP lengths of 6 to 8 characters are supported and the validity time period of the OTP can be specified. Once this time period has elapsed, the OTP is no longer valid, even if it has not been used.

The SMS – OTP feature of SA Server 3.0 works with any Mobile Messaging Operator that offers an SMSC- or HTTP-compatible API. Because the OTP is essential for network access, only MMOs with an appropriate service level agreement and coverage area should be considered.

To assist customers in this regard, Gemalto has partnered with TynTec, a global Mobile Messaging Operator that offers enterprise quality SMS services to companies such as O2, British Airways and Skype. The company has multiple points of deep level (SS7) connectivity into the global mobile network, enabling it to act as an operator-level messaging provider. Using these capabilities, TynTec offers a unique level of reliability and measurability in SMS services. TynTec is able to commit on delivery times of less than 15s and provides coverage in more than 150 countries.

For more information, visit:
<http://www.tyntec.com/en/index.php>

TynTec