

One Time Password for Secure Network Access

||||| Full Portfolio of OTP Solutions for Every Business Use Case



FINANCIAL SERVICES & RETAIL

ENTERPRISE > SOLUTION

GOVERNMENT

TELECOMMUNICATIONS

TRANSPORT



gemalto
security to be free

One Time Password Solution for Secure network Access

Static passwords are dead

Can your child's birthday or pet's name cost your company a significant amount of money? Could your network be compromised by a sticky note? If the only barrier to access your network is a username and password, then these bits of personal information could lead to unauthorized access and a significant impact to your business. A compromised network resulting in lost corporate data can damage customer trust and the financial bottom-line. According to a 2009 study by the Ponemon Institute, data breaches cost U.S. businesses an average of \$6.75 million per incident. Given the dollars that are potentially at risk, it is clear that the days of static passwords are over.

Regardless of the security policy in place, usernames and passwords are simply not strong enough. People tend to choose passwords that are easy to remember. If they aren't easy to remember, they write them down and leave them in places they can be found. And even if identity thieves don't find or guess them, users can often be socially engineered into providing their password. In addition, there are more technical and sophisticated methods for stealing user passwords using malware or spyware. This problem is only further complicated with the introduction of smart phones and the ever-increasing mobility of today's workforce. However, with this increased flexibility comes the potential risk of network breaches, presenting new challenges for IT security professionals who must stay one step ahead of attackers in order to protect all access points into networks.

Password administration is costly. To prevent users choosing obvious and guessable access codes, many organizations implement complex password policies that make unauthorized access more difficult. However, with complex passwords come user lock-outs, which are costly to support. Forrester estimates each help desk call from an end-user costs \$25-\$50 and that businesses spend \$200 per year per person on password management.

Strong authentication is the answer

In order to address this problem, there needs to be additional layers of security introduced to reduce the threat posed by weak authentication methods like



- **Protect all access points on your network**
- **OTP Solutions for every business need**
- **Out of the box and up and running in minutes**
- **Tokens are licensed once – no recurring licensing**
- **Token can be re-issued to another user**
- **SA Server provides migration path to PKI authentication**

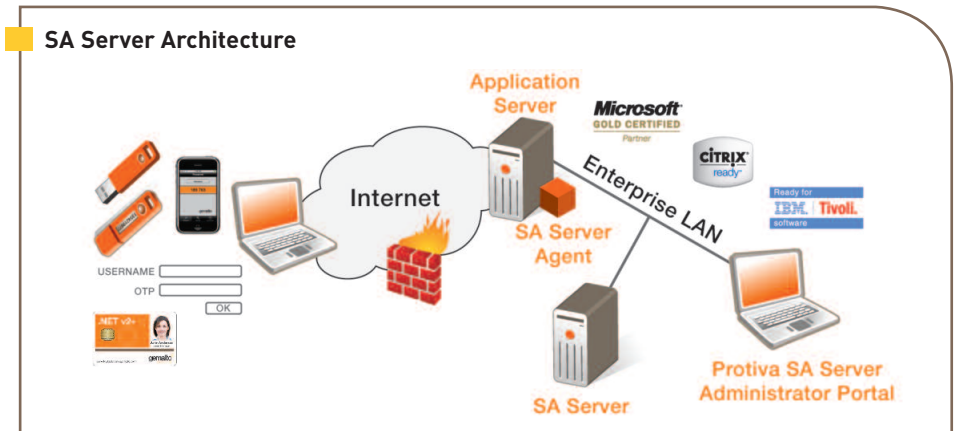
username and password. Strong or multi-factor authentication is the answer to this problem. Strong authentication is defined as authentication that uses different factors to verify a person's identity. The three most commonly recognized factors are something you know, like a password or PIN; something you have, such as a smart card or hardware token; and something you are, like a fingerprint or retinal pattern.

A one-time password (OTP) solution offers two-factor authentication using something you know – such as a pass code – combined with something you have like hardware token to generate an OTP. As their name implies, OTPs are only valid for one login session or one single transaction; they expire once they are used. They avoid many of the shortcomings that are associated with traditional static passwords, the most important of which is that OTPs are not vulnerable to replay attacks. In other words, even if an OTP is stolen, it can only be used one time. OTP solutions are ideal for all companies where a remote workforce needs access to their resources such as network, mail, and webpages, and where they want to access these resources through the Internet or via an intranet.

Protiva OTP: Strong yet simple

Protiva: the umbrella brand for Gemalto strong authentication portfolio is a user-friendly platform that was developed to provide IT administrators a flexible solution to meet all authentication needs. Protiva allows for the creation of risk appropriate policies to ensure strong controls over access to the corporate network and supports solutions ranging from OTP to a full smart card based PKI solution. At the heart of the Protiva solution is the Gemalto Strong Authentication (SA) Server: a flexible authentication platform that is easily adapted to existing network architectures. SA Server runs on Windows and Linux operating systems and is easily integrated into existing network and authentication infrastructure. It offers a range of OTP solutions for every business case.

SA Server Architecture



Protiva OTP: Strong yet simple

The Protiva OTP solution offers a wide range of different network access devices for end-users that are portable, convenient, and user-friendly. They protect against key logging, shoulder surfing, password cracking, and help guard against phishing.

- **Easy OTP** is a user-friendly time-based OTP token that offers unconnected operation. Small enough to hang from a key ring, it generates an OTP at the touch of a button for simple and safe remote access. OTPs are generated with a time stamp and have a limited time window in which they can be used.
- The **OTP Display card** offers the same functionality of the Easy OTP but on a credit card style device.
- **Secure Flash USB Tokens** are personal portable security devices that support OTP as well as PKI functionality and offer secure flash storage and portable applications as well as digital signature.
- The **.NET Key** is the ideal solution for multi-application use of OTP and PKI. With no display, it offers connected operation for automatic entry of OTP.
- **.NET Dual** offers all the advantages of the .NET Key but produces an OTP via a customizable display or offers auto-entry via USB.
- The **.NET Card** solution offers a card form factor that supports OTP for remote access when used in conjunction with a reader, but can also be used to deploy PKI services. The .NET card can also be used as a



corporate badge for physical and logical access.

OTP solutions that harness the strengths of mobile phones

Protiva mobile OTP solutions take advantage of the ubiquitous mobile phone to offer two options for secure OTP generation without the need to carry another physical device.



- **SMS OTP** uses the Strong Authentication Server to send a password to any mobile phone via the Short Message Service (SMS) format. SMS OTP combines two-factor authentication security with the convenience and simplicity of mobile SMS messages. No extra software is needed, there is no impact on the customer's phone and SMS OTP ensures a very simple user experience.
- **Mobile OTP** uses an application installed on a mobile phone that allows users to securely generate an OTP

using their mobile phone as a token. End-users need no additional hardware and can obtain their OTP through a device they always carry with them for a convenient, secure and user-friendly solution that has the added benefit of not needing network access to function. The solution supports a large number of handsets and for enterprises is easy to deploy, and requires no inventory or replacement management.

All Gemalto OTP solutions are managed by the Gemalto SA Server. When an end-user enters an OTP generated by their device, the OTP is sent to the SA Server. The server verifies the OTP and when satisfied with its authenticity, grants the necessary access. Moreover, if an end-user should lose their token or device, when provided with the right answers to a series of secret questions, the SA Server will create a virtual token and generate an OTP that can be used as a one-time access method. It is this flexibility that makes the SA Server unique: it is designed to securely facilitate network access and will not impede it for valid users.

Flexible and Built to Evolve With Your Business Needs

Protiva OTP solutions provide simple, secure strong authentication methods that can be tailor-made to suit every business case. The technology can evolve to meet the needs of your business. Start with the Protiva OTP solution and, as your risks and needs change, migrate to a more comprehensive PKI infrastructure for multi-factor authentication that can provide advanced functionality such as email encryption or document digital signature. The use of open- and industry-standard protocols enables hardware optimization and reduces the total cost of ownership.

With its flexibility, security, and simplicity, Protiva is the industry leading solution to address the limitations of static passwords and offer built-in features to ensure more comprehensive digital security solutions in the future.

Gemalto SA Server Devices



> Business Use Cases

Secure Remote Access to:

- Confidential and Sensitive Information
- Corporate Data (Intellectual Property)
- CRM - Sales Enablement Tools
- Personal Private Information

||||| The world leader in digital security

www.gemalto.com

gemalto
security to be free