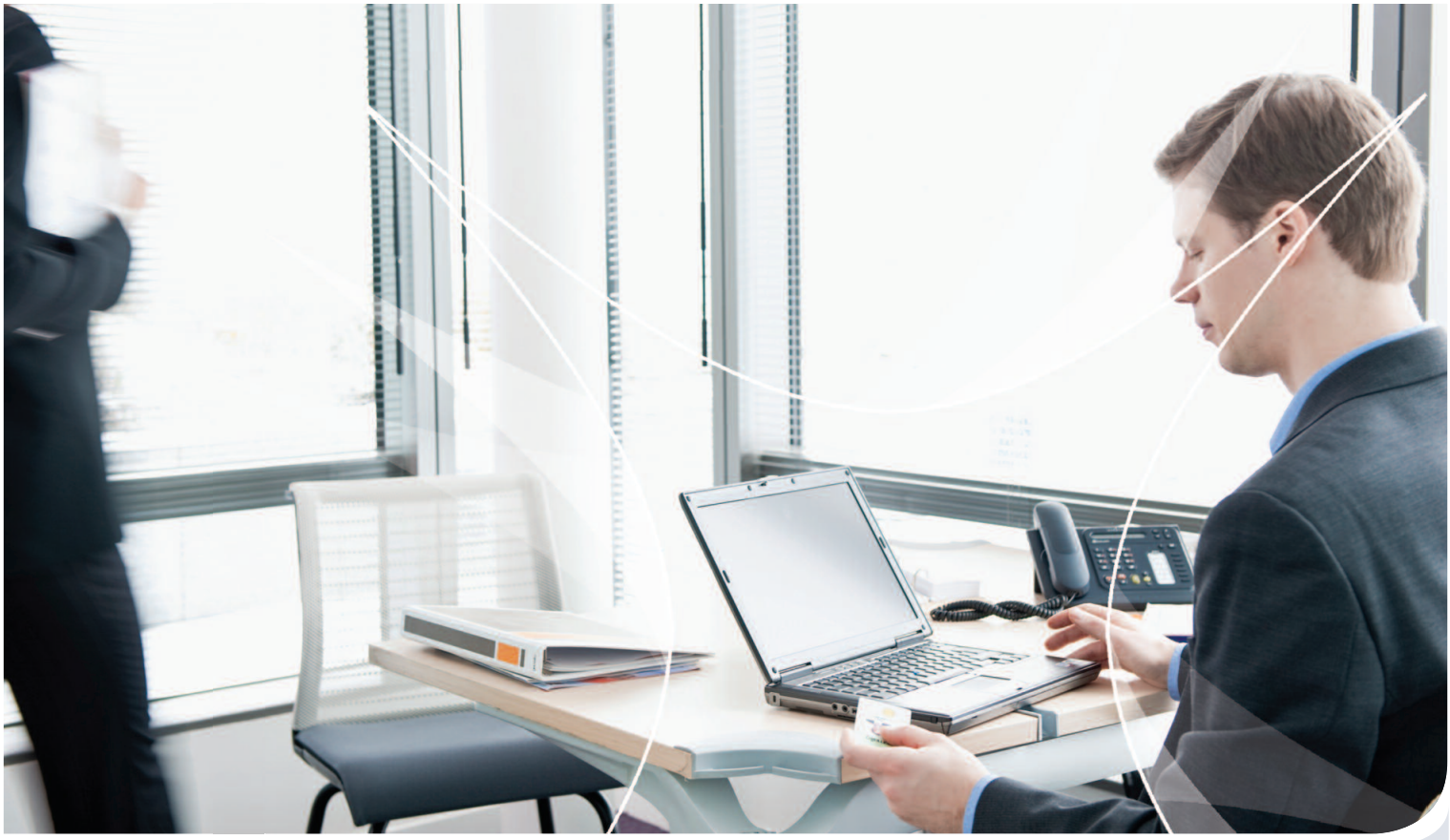
Protiva Strong Authentication

Providing Secure Access Control Technology to Protect Your Business



FINANCIAL SERVICES & RETAIL

ENTERPRISE > SOLUTION

GOVERNMENT

TELECOMMUNICATIONS

TRANSPORT

gemalto
security to be free

Protiva Strong Authentication

Providing Secure Access Control Technology to Protect Your Business

Protecting access to your network

Today's workers are on the move than ever before and the trend towards greater mobility is only increasing. Workers expect to be able to access company resources anytime, from anywhere using multiple devices. But while mobility can increase productivity, it also introduces a significant security risk. With numerous potential entry points into the network, the new challenge for IT security professionals is balancing security with convenience.

Complicating this task is the ever-changing nature of the threat. Evidence of this can be seen in the media on a regular basis, as company networks are compromised and sensitive information stolen. According to a 2009 study by the Ponemon Institute, data breaches cost U.S. businesses an average of $6.75 million per breach.

This clearly shows the need for stronger access control methods to secure all access points into the network. Strong authentication adds layers of identity verification to ensure only authorized users gain network access through a variety of easy-to-use form factors that meet business requirements and ensure user adoption.

The days of the username and password are numbered

Traditionally, we have logged in to workstations and networks using a combination of a user name and password. But such simple technology is no longer sufficient for today's business and regulatory environment.

Most passwords are chosen because they are easy to remember, often being composed of obvious, personal information or well-known words and numbers. In response, many organizations have implemented complex password polices that make it more difficult to gain unauthorized access, but which tend to be costly to manage.

Moreover, users often compromise security policies by writing down their passwords and hiding them in easy-to-find locations. And even if identity thieves don't find them written down, passwords can often be guessed or socially engineered by manipulating people into performing actions through malware or spyware.

The dangers of weak authentication

A business without proper network access controls is putting itself at significant risk. A compromised network resulting in lost corporate data can cause significant damage, both financially and from a customer trust perspective. The financial cost of data breaches reaches far beyond the immediate problem. The Ponemon Institute's average single data breach cost figure of $6.75 million ignores the cost of customer churn due to the incident and the potential for long-term brand damage. Furthermore, not having a full audit trail has ramifications in compliance terms. The importance of ensuring only the right people have access to appropriate confidential data, and that access is reliable and secure, cannot be stressed enough.

Strong or multi-factor authentication meets this critical business need

Strong or multi-factor authentication is defined as authentication that uses two or more different forms of identity verification.

An example of true multi-factor authentication is where a user is required to insert a smart card (something they have) into a reader, and then must enter a PIN or passphrase (something they know) in order to access a secure network. If, in addition, they have to also place their fingertip (something they are) on a biometric fingerprint reader, this would add a third factor of verification. Each level of identity verification adds a further layer of protection.

Protiva: A flexible strong authentication solution

Protiva provides a full portfolio of products to meet the need for secure access to business resources. It is a modular system that allows businesses to choose the security level they need, from a full end-to-end system to .NET-based smart cards that leverage the card management capabilities in Microsoft Server and Windows OS.

Authentication Software

Gemalto's Strong Authentication (SA) Server is scalable and is based on open OATH and EMV CAP standards. The server is designed to work with existing network infrastructure including LDAP and AAA servers. It can be deployed on an existing server and provides authentication services for a full range of devices including OTP (token, card or mobile), Public Key Infrastructure (PKI) -based smart cards and biometrics. The server is equipped with a web based portal for user account management.

OTP Solutions

- Gemalto **time-based OTP** tokens use the current time computed with a secret key to create a password. When the corresponding validation server receives the password, it combines the current time with the secret key and performs the same cryptographic computation as the token. If the two resulting passwords match up, access is granted for one attempt within a 30 second window.
- Protiva's **SMS OTP** solutions use the SA Server to send a password to any mobile phone via SMS. This offers safe and convenient authentication without the hassle or extra cost of having to carry another device.
- The Protiva **Mobile OTP** solution exploits all the convenience of the mobile phone without the need for a network. Users download an application that turns the phone into a token that generates a secure OTP.

Smart Card Solutions

Gemalto's **Protiva smart card-based solutions** leverage PKI to provide certificate-based strong authentication. In addition, PKI certificates stored on the smart card can be used to enable email encryption and digital signature, and when incorporated into a USB storage device, secure data storage.

- Protiva **.NET** smart cards work seamlessly with Microsoft Server and Windows OS to add secure physical and logical access to existing IT infrastructures using two- or three-factor authentication.
- **.NET Bio** adds a further level of security with the addition of fingerprint match-on-card user authentication as an alternative or complement to PIN verification.
- **Secure Flash USB Token** are secure USB tokens that offer simple, highly secure solutions for the mobile office, preventing data loss, securing portable data and digitally signing documents.

Additional PKI Functionality

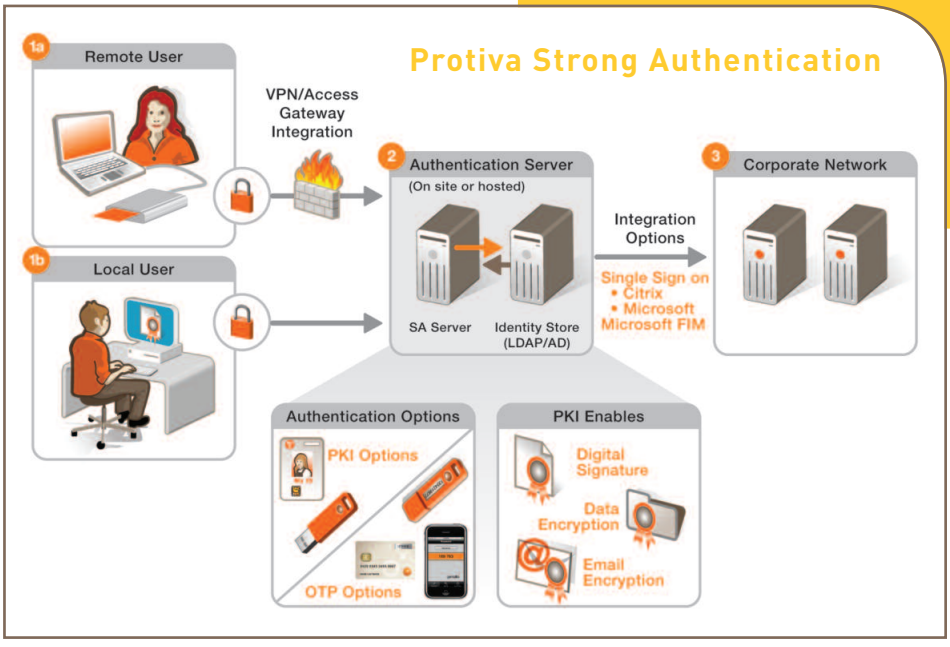
- Using the Internet for business processes is cheaper and faster but these savings can be negated by having to rely on "wet" signatures for validation and approval. **Digital Signatures** created using Protiva smart card devices with PKI can securely authenticate virtual documents saving both time and money.
- Protiva also offers **Email Encryption** using PKI. This is essential for preventing sensitive email content being read by unintended recipients.
- Unsecured USB flash drives can be a major source of data loss but Protiva tokens are perfect for **Secure Data Storage**, ensuring sensitive business information is kept safe, even if the drive is lost or stolen.

Flexible Authentication Built to Evolve with Your Business

Organizations can deploy Protiva for secure user authentication and then evolve to more comprehensive identity protection and network security solutions without having to abandon infrastructure investments or change end-user devices. The Protiva platform can be used for one-time password applications and then expanded to support PKI and the smart card-based security features in Microsoft's Windows and .NET platforms. The use of open standards and industry-standard protocols enables hardware optimization, and also helps reduce the total cost of ownership.

Protiva is unique in meeting the need for enhanced network security and online identity protection with a platform that delivers strong authentication using one-time passwords and the flexibility to implement more advanced user protection services as network security needs expand.

Strong authentication adds layers of identity verification to ensure only authorized users gain network access through a variety of easy-to-use form factors that meet business requirements and ensure user adoption.



The world leader in digital security

www.gemalto.com

gemalto
security to be free