

Protiva Strong Authentication

Brand: Smartjac Industries Inc
Product Code: SMAPSA



Description

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 optimizations, 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.