

# Protiva Strong Authentication Server

IIIIII A Flexible Authentication Platform



ENTERPRISE > PRODUCT

Username and passwords are simply not strong enough to protect data resources from cyber theft. As cyber crime and online threats continue to become more sophisticated, the only way to protect your company's data is to provide additional layers of authentication to ensure you know who accessing your network at all times. Gemalto's Protiva Strong Authentication (SA) Server provides this added protection in an easy to deploy, easy to use authentication platform.

In order to meet the needs of every business, Protiva SA Server supports a broad portfolio of end-user devices for risk appropriate authentication. This portfolio ranges from one time password (OTP) technology to support of a full public key infrastructure (PKI) based smart card deployment. This range of devices provides IT administrators with the flexibility to provide different authentication devices based upon user need managed by a single authentication server. This also provides an easy migration path from OTP to PKI based deployment without having to change the authentications devices or the authentication server. PKI deployment achieved through a



- **Easy to deploy**
- **Leverages existing infrastructure**
- **Flexible and reusable end-users licensing**
- **Scalable portfolio of authentication devices (OTP – PKI)**

plugin to Microsoft's Forefront Identity Manager allowing management from a single interface.

A wizard easily guides the installation of a Protiva SA Server deployment including the installation path, administrative information, and data server and LDAP selections. Once deployed, a web-based interface makes managing end-user hardware and accounts simple.

Protiva SA Server consists of the following components:

- Authentication Modules that perform end-user validation using One-Time Passwords
- A Customer-Care interface for administrators to manage Gemalto end used devices, authentication policies, roles, users, keys, and other functions
- A User Care interface that enables end-users to register and manage their passwords and account information

# Protiva Strong Authentication Server

## IIIIII A Flexible Authentication Platform

### Leverage Your Network Infrastructure Investment

Protiva SA Server works with multiple operating systems and server configurations. SA Server modules support industry standard protocols for seamless integration with existing architectures including RADIUS (Remote Authentication Dial-In Server), AAA (Authentication, Authorization and Accounting) and Web application servers.

To provide the most advanced level of user identity protection, Protiva SA Server integrated a software security module or an external hardware security module (HSM) is linked to an authentication server to store and use cryptographic keys. Using standard frameworks and protocols such as HTTP/HTTPS and RADIUS, authentication modules interact with existing data servers to maintain and update user authentication information. Multiple data server options are supported, including MySQL, Firebird and LDAP directories such as Microsoft Windows Active Directory.

### Provision, Manage and Empower End-Users

Protiva SA Server customer care portal offers three options to provision and manage end-user smart card devices and authentication credentials: batch client provisioning, customer care Interface, and live provisioning. Batch client provisioning enables administrators to create multiple device records at one time and activate multiple users. This is especially useful when setting up a new system since a large number of device records can be enabled in one step.

The web-based customer care portal supports the administrative functions for managing users and their access privileges, smart card devices and system transactions including creating or updating a device record, link a record to a user, and activate the



device. The customer care portal also supports live provisioning, a fast and convenient way to personalize a new Gemalto end-user device or re-use an existing device..

Protiva SA Server also enables end-users to manage routine tasks through a self-service portal. This portal is incorporated into the SA Server web application and can be customized to support end-user access to appropriate SA Server functions.

### Protiva SA Server Integrations

#### OS:

- Windows Server 2003
- Windows Server 2008
- Red Hat Linux

#### Authentication methods:

- SA Server uses the following methods for main authentication:
- OATH HOTP (Event based, Time based)
  - SMS OTP
  - Mobile Time based OTP
  - EMV CAP

#### Web servers:

- Apache Tomcat
- The chosen architecture allows "High Availability" and "Fail-Over" configuration relying on operating systems, databases and monitoring mechanisms.

#### Databases:

SA Server stores OTP related data and User data if needed (DB mode) in:

- Firebird
- MySQL
- MS SQL
- Oracle
- IBM DB2 (Windows or AIX)
- Any other SQL database could be supported through a specific development

#### User Repository:

SA Server can be connected to the following LDAP when Users accounts are managed externally (Mixed mode):

- Microsoft Active Directory,
- Novell eDirectory,
- Sun One,
- Open LDAP,
- Any other LDAP could be supported through a specific development.

#### Authentication Services interface:

Authentication services are integrated using the following interfaces:

- HTTP or HTTPS requests,
- XML requests sent to Web API,
- RADIUS requests through SA Server RADIUS agents for
- Microsoft IAS or NPS (Windows Server 2008),
- Juniper Steel Belted RADIUS,
- FreeRADIUS

### SA Server Architecture

