



Gemalto Strong Authentication Server (SAS)

Protecting your network identities

FINANCIAL SERVICES & RETAIL

ENTERPRISE > PRODUCT

INTERNET CONTENT PROVIDERS

PUBLIC SECTOR & TRANSPORT

TELECOMMUNICATION



gemalto
security to be free

Gemalto SAS: A Flexible Authentication Platform

Gemalto Strong Authentication Server (SAS) protects network users' identities by performing two-factor authentication using Gemalto's proven smart card technology. It is easily adapted to existing network architectures and features customer care and self-service interfaces for managing end-user hardware and accounts. An installation wizard facilitates easy integration and provides an intuitive interface for entering the installation path, administrative information, and data server and LDAP selections.

Gemalto SAS supports a family of end-user devices which can be used when connected to the network or in a standalone mode. This capability enables issuers to provide end-users with the most appropriate form factor for their individual network access requirements while maintaining full compatibility on the backend. The Gemalto SAS 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

> Leverage Your Network Infrastructure Investment

Gemalto SAS works with multiple operating systems and server configurations so existing infrastructure can be used for enhanced network

security and user identity protection. Its Server Authentication Modules fully support industry standard protocols for seamless integration with existing architectures that incorporate RADIUS (Remote Authentication Dial-In Server), AAA (Authentication, Authorization and Accounting) and Web application servers.

These Server Agents extend existing RADIUS and AAA servers by enabling them to deliver incremental, multi-factor authentication using One-Time Passwords. To provide the most advanced level of user identity protection, Gemalto SAS integrated software security module or an external hardware security module (HSM) is linked to the authentication server to hold cryptographic keys and perform operations with them.

Using standard frameworks and protocols such as HTTP/HTTPS and RADIUS, Authentication Modules operate with existing data servers to maintain and update information needed for user authentication. Multiple data server options are supported, including MySQL, Firebird and LDAP directories such as Microsoft Windows Active Directory 2003.

> Provision, Manage and Empower End-Users

The Gemalto SAS Customer Care Portal offers three options to provision and manage end-user smart card devices and authentication credentials: a Batch Client provisioning tool, a Customer Care Interface, and Live Provisioning. The Batch Client provisioning tool enables administrators to create

multiple device records at one time and activate multiple users. It 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 Gemalto SAS Customer Care Interface supports the administrative functions for managing users and their access privileges, smart card devices and system transactions. It provides the functionality to create or update a Gemalto SAS device record, link the record to the 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 for end users. Using a Gemalto SA Easy device and a Gemalto Live Provisioning Kit (LPK), administrators can place the device within the scan area of the reader and automatically create a device record, save it on the data server, and securely transfer the information to the smart card device.

Gemalto SAS also enables end-users to manage routine tasks through a robust self-service portal. The End-User Portal is incorporated into the Gemalto SAS web application and can be customized to support end-user access to specific Gemalto SAS functions.

Gemalto SAS Features:

- Operating Systems: Windows 2003 Server, (Enterprise Edition is recommended but not mandatory); Windows XP, Red Hat Enterprise Linux 4.0, SUSE 10, AIX 5
- RADIUS Agent Servers: IAS (Microsoft), Steel Belted Radius (Funk Software) Free RADIUS Support for Microsoft Outlook Web Access (OWA) and Citrix Access Gateway (Standard, Advanced and Enterprise Editions), Checkpoint, Cisco, Juniper
- Cryptographic standards: OATH, EMV CAP 2004
- Protocols: HTTP/HTTPS, RADIUS
- DataBase: Firebird, My SQL
- LDAP: MS Active Directory, Novell eDirectory, IBM DB2
- Application Server: Apache Tomcat, IBM WebSphere

Gemalto Strong Authentication Architecture

