![gemalto security to be free]

Strong Authentication for Secure Access to Cloud-based (SaaS) Applications

Easily Secure Access to Cloud Applications by Federating Identities with Gemalto

The Security and Business Implications of the Cloud

The move to the cloud has been both widespread and fast. However, for the enterprise security teams tasked with protecting access to sensitive data and systems, this evolution has been presenting significant challenges:

> **Diffusion of access control boundaries:** As enterprises transition to the cloud, they are essentially shifting their focus from controlling security with physical boundaries, to that of a virtual infrastructure. When security is physically contained, information is protected in the data center using methods such as encryption, strong authentication, access controls and application permissions. But when data and applications move to the cloud, user access—by default—takes place remotely, with weak, static passwords serving as the only security mechanism to protect against unauthorized access. Organizations therefore have to contend with a blurred IT perimeter, necessitating access controls for applications both in the cloud and those within the confines of the data center.

> **Identity proliferation:** The deployment of numerous cloud applications that are not part of an enterprise identity scheme, results in numerous additional credentials that users need to memorize. This translates into heightened security risks, greater overhead for helpdesk personnel and inconvenience for users. Users now have an even greater number of identities and permissions that are not necessarily issued by the organization.

The trends described above have direct security and administrative ramifications on how organizations maintain control and manage user access to applications in the cloud, how they cope with the proliferation of user identities, and how they cope with supporting a comprehensive secure mobility policy.

Benefits

> **Seamlessly extend secure access to the cloud:** Protect resources residing in the cloud from a single authentication platform, offering validated integrations with dozens of leading SaaS apps

> **Increased user convenience:** Federated login allows users to log on to the corporate network, on-prem and cloud applications—all with the same enterprise logon credentials

> **Central management of entire IT ecosystem security:** Define and deploy policies for network, web- and cloud-based apps from a single backend, optimizing visibility and facilitating compliance

> **Deploys without changing existing architecture:** Support for a wide range of authentication methods lets organizations implement strong authentication without sacrificing existing investments, with Gemalto solutions available from the cloud or on-premises

> **Automate provisioning of SaaS user accounts:** Automatic provisioning of access to SaaS applications significantly reduces administration overhead by enabling IT teams to centrally configure access controls to all applications from within Gemalto Authentication Manager

Strong Authentication and Identity Federation to Cloud-based SaaS Applications

To contend with the complexity of these security and management challenges, Gemalto's authentication platforms allow organizations to extend users' on-premises identities to cloud applications. By so doing, organizations are able to centrally manage and control their strong authentication environments, automatically provision users with SaaS application accounts, and provide a complete web federated login experience, sparing users the time and effort required to maintain—and log on with—separate SaaS account credentials.

Gemalto's authentication platforms provide a seamless, consistent strong authentication and federated login experience for users who want to access cloud applications such as Microsoft Office 365, Google Apps and Salesforce. By federating an enterprise user's identity via the Security Assertion Markup Language (SAML), Gemalto authentication platforms leverage an organization's existing authentication infrastructure so that users can use the same logon credentials for both on-premises and cloud-based applications.

Gemalto's Gemalto Authentication Solutions: Your Trusted Authentication Provider

Gemalto's authentication management platforms in essence act as the trusted identity provider, giving authorized users permission to access SaaS applications. The SaaS service, in turn, is configured to allow access only to those users given permission by Gemalto's authentication platform.

This unified approach, combined with support for a broad range of authentication methods and form factors, allows organizations to transition to the cloud without compromising their security perimeter. Moreover, since access control settings, provisioning and federated login are handled from one platform, organizations achieve significant cost efficiencies that are reflected in reduced IT infrastructure costs, lower IT maintenance and better productivity and convenience for end users.

Move to the Cloud without Relinquishing Security Controls

Strong authentication and federated login to SaaS applications is available with SafeNet Authentication Service and SafeNet Authentication Manager.

With either platform, the enterprise security team retains complete control over the configuration, deployment, and administration of the authentication infrastructure, which remains in the enterprise's IT domain.

Organizations can deploy either platform in their network's DMZ, so users can authenticate directly to cloud-based applications and services, rather than having to go through the corporate VPN. As a result, users have a faster, more seamless experience accessing on-premises and cloud-based applications, while enterprises enjoy optimized security.

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industryleading protection of data, digital identities, payments and transactions -from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com
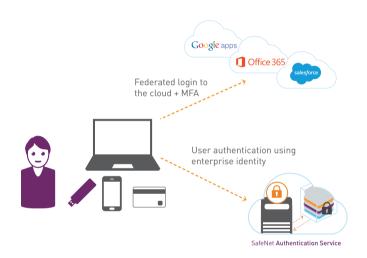
⊕ GEMALTO.COM

Supported Authentication Methods

> One-time passcodes (OTP)
> Out-of-band (OOB) via push notification, SMS and email
> Context-based authentication
> PKI certificate-based authentication
> Pattern-based authentication

Available Form Factors

> Hardware tokens (USB, key fobs and smart cards)
> Bluetooth Smart PKI readers
> Software tokens
> Phone-as-a-token

Gemalto Authentication Platforms

> SafeNet Authentication Service
> SafeNet Authentication Manager

Federated login to the cloud + MFA

User authentication using enterprise identity

SafeNet **Authentication Service**

ISO 27001:2013 CERTIFIED

2014 GARTNER MAGIC QUADRANT for USER AUTHENTICATION
SAFENET THE ONLY COMPANY IN THE LEADERS QUADRANT FOUR YEARS RUNNING

SC MAGAZINE AWARDS 2015 Europe FINALIST Best Multifactor Solution

gemalto
security to be free