IDConfirm

Protecting your network identities

High profile breaches have been at an all time high over the past few years, and at the center of the problem is traditional password-based authentication. Of all the confirmed breaches in 2013, 76% used stolen credentials or exploited weak credentials (Verizon Data Breach Investigation Report, 2014). User names and passwords are just not strong enough to keep criminals at bay. And 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. IDConfirm provides this added protection in an easy-to-deploy, easy-to-use authentication platform.

IDConfirm

Protecting your network identities

The IDConfirm platform includes all components needed to deploy strong authentication in your organization and for a low total cost of ownership. This is realized through packaged plug-and-play solutions that are adaptable to existing networks and AAA servers and built according to open OATH standards.

IDConfim offers the highest level of security for two-factor authentication. You can choose from a wide range of connected or unconnected form factors including smart cards, tokens, and mobile or desktop OTP.

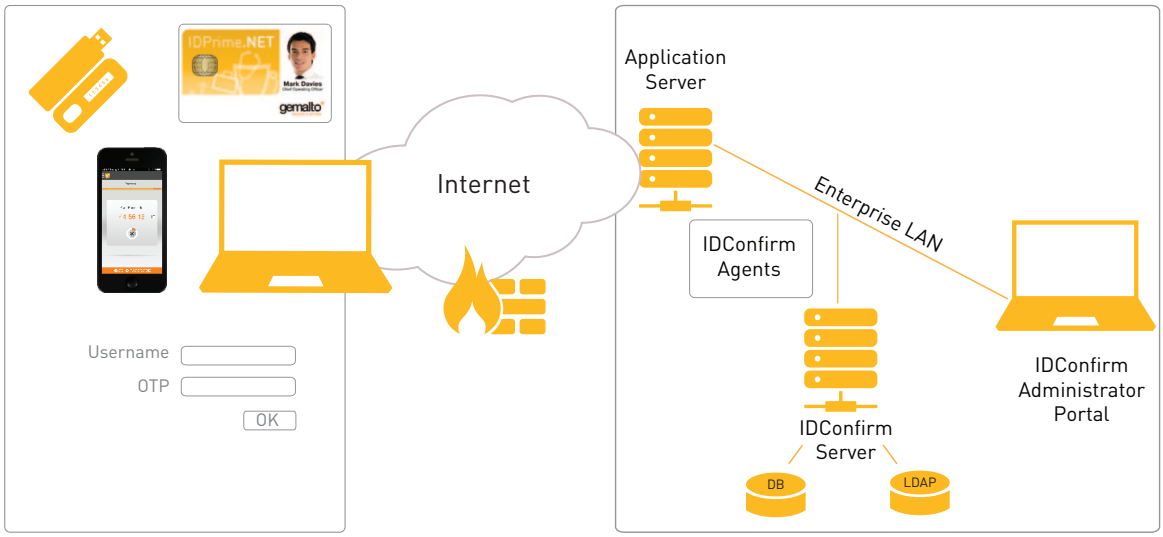
Our software solutions are open, scalable and evolutive and support either an on-premise or cloud deployment model.

Because businesses and users have different security needs, Gemalto offers several solutions from one-time password (OTP) technology to full public key infrastructure (PKI) based smart card deployment. Gemalto solutions provide flexibility and allow IT administrators to provide different authentication devices based upon user need.

With Gemalto solutions, you have a smooth migration path from OTP to PKI based deployment without having to change devices.

- Easy to deploy
- Leverages existing infrastructure
- Scalable portfolio of authentication devices (OTP-PKI)
- New secure, fully configurable, user friendly Mobile OTP

IDConfirm Architecture



Wizard-based installation of administrative information, data server and LDAP selections makes deployment fast and easy. Once up and running, a web-based interface makes managing end-user hardware and accounts simple. IDConfirm consists of the following components:

- Authentication modules that perform end-user validation using one-time passwords
- A Customer-Care interface for administrators to manage end-user 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

IDConfirm works with multiple operating systems and server configurations and 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, IDConfirm's 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 database and directory options are supported.

Provision, manage and empower end-users

IDConfirm's 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, OTP 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. IDConfirm also enables end users to manage routine tasks through a self-service portal. This portal is incorporated into the Web application and can be customized to support end-user access to appropriate IDConfirm functions.

IDCONFIRM INTEGRATIONS

OS

- Windows 2012 and 2012 R2
- Windows Server 2008 R2
- Red Hat Linux

Authentication methods

IDConfirm uses the following methods for main authentication:

- OATH (Event based, Time based)
- SMS OTP
- EMV CAP

Web servers

- Apache Tomcat
- IBM WebSphere

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

Databases

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

- MS SQL
- Oracle
- MySQL
- Firebird
- Any other SQL database could be supported through a specific development

User repository

IDConfirm can be connected to the following LDAP when users' accounts are managed externally (Mixed mode):

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

Authentication services interface

Authentication services are integrated using the following interfaces:

- Web Service REST API
- RADIUS requests through IDConfirm:
  - Microsoft NPS
  - FreeRADIUS
- AD FS MFA Adapter

GEMALTO (Euronext NL0000400653 GTO) is the world leader in digital security with 2012 annual revenues of €2.2 billion and more than 10,000 employees operating out of 83 offices and 13 Research & Development centers, located in 43 countries. We are at the heart of the rapidly evolving digital society. Billions of people worldwide increasingly want the freedom to communicate, travel, shop, bank, entertain and work – anytime, everywhere – in ways that are enjoyable and safe. Our innovations enable our clients to offer trusted and convenient digital services to billions of individuals. Gemalto thrives with the growing number of people using its solutions to interact with the digital and wireless world.

For more information visit www.gemalto.com, www.justaskgemalto.com, blog.gemalto.com, or follow@gemalto on Twitter.

GEMALTO.COM

gemalto
security to be free