Securing the path to your information assets

Data Sheet

Tectia® MobileID

Two-Factor Authentication Made Convenient

Do you want to identify your end users securely and conveniently?
Do you want to do it with a scalable and easily deployable solution?
Do you want to provide better service and increased security for your employees, customers, and partners?

With Tectia MobileID you can:

- Increase security for accessing critical systems with no effort from end users
- Save on operational and maintenance costs with a tokenless solution
- Activate new users, partners, and ad-hoc accounts instantaneously instead of days or weeks

Two-factor authentication provides an additional layer of security by using two different methods to verify the user's identity: What you know (user name and password) and what you have (e.g. a token or software application). Hardware and software solutions can be scalable enough for corporate internal use, but when the organization wants, or more often, is demanded to provide strong authentication also for their partners, suppliers, or end customers, the deployment and management of any hardware devices or software packages becomes a real problem.

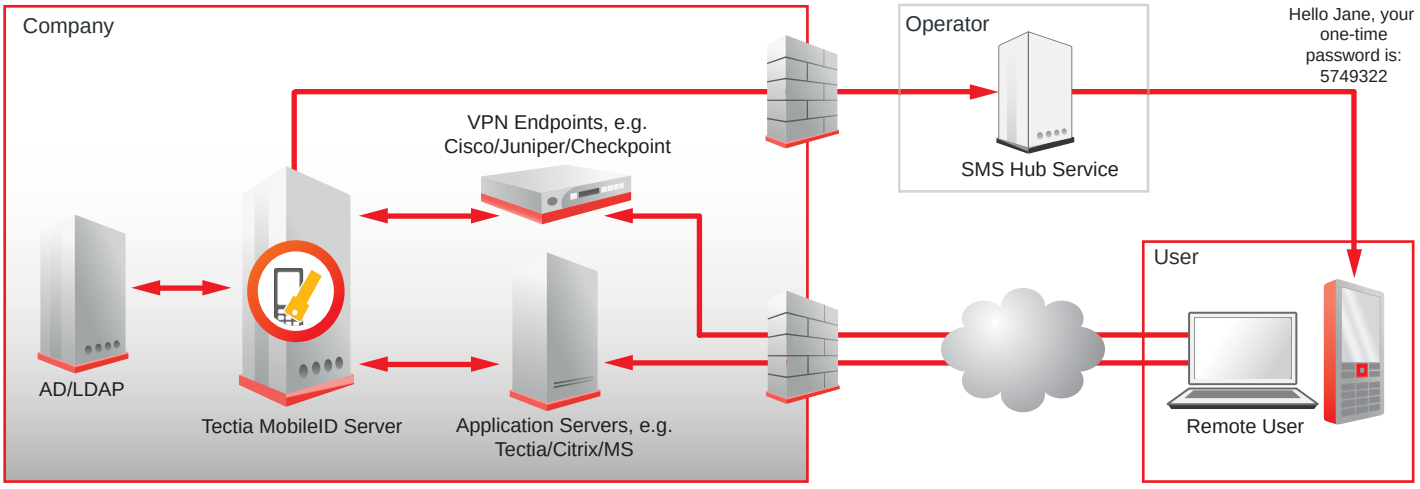
Versatile Authentication Platform

With multiple authentication methods available, Tectia MobileID serves as a versatile authentication platform providing login also through the use of hardware tokens, software tokens, e-mail, or even password lists. The wide range of available methods allows smooth migration and strong authentication beyond the mobile service coverage.

The Most Convenient Two-Factor Authentication Available

Tectia MobileID provides a strong two-factor authentication service through mobile phones. Instead of carrying a separate hardware token or installing a software application, the user simply enters the one-time password provided into his mobile phone as a text message. The one-time password can be pre-sent or delivered at login time using a high-priority SMS operator channel. Tectia MobileID does not require any applications installed on the user's mobile phone making the user experience flawless, easy to understand and use.

Tectia MobileID Server uses the mobile phone numbers stored in internal or external directories of the corporation, and provides multiple interfaces, so it can be integrated smoothly into the existing corporate applications, and the company security processes and systems can be kept intact.



Features

Authentication Options

• Multiple types of One-Time Passwords (OTP):
• On-demand SMS/Email OTP
• Pre-delivered SMS/Email OTP
• Pre-delivered SMS/Email/PDF OTP list (up to 200 passwords)
• Reusable SMS Ticket (time or usage restricted password)
• Failover OTP

• Conventional hardware token with synchronized OTP generator
• Software token with synchronized OTP generator

Customization

• Modular architecture that provides extensive scalability and customization
• Granular control on network conditions and business policies with Rules
• OTP format, length, and life-time are configurable
• All messages customizable and localizable per Domain, Group, or Service

Service Provider Capabilities

• Multi-domain support
• Customer-specific rules for authentication and access
• Customer-specific rules for localization, reporting, billing, and accounting

Server and User Administration

• Web-based GUI for user and server administration
• Integrates with Windows Domain authentication
• Mobile numbers can be retrieved from a directory or from a database
• Support for ad-hoc accounts
• Automatic failover and account locking mechanisms
• Real-time resource monitoring and traps
• SMS and Email alerts

Specifications

Supported Third-Party Products

• F5 FirePass SSL VPN
• F5 BIG-IP Access Policy Manager
• SAP Netweaver
• Juniper VPN/SSL-VPN
• Citrix Access Gateway
• Citrix WEB Interface (5)
• Aventail VPN/SSL-VPN
• CheckPoint VPN/SSL-VPN
• Nortel VPN/SSL-VPN
• MS OWA (2003/2007/2010)
• Tectia Client / Server
• Custom IIS applications
• Custom Apache applications
• Other applications using Unix PAM

Server Requirements

• LDAP/SQL user database
• Connection to SMS-Gateway or SMSC
(Short Message Service Center)

Performance Figures

• 1 GHz, 1 GB RAM machine can handle up to 200 simultaneous logins.

Supported Server Platforms

• All virtual platforms that support Open Virtualization Format (OVF), e.g. VMware ESX, Citrix XenServer, and MS Hyper-V

User Device Requirements

• Any phone capable of receiving SMS messages (for SMS OTP)
• Email-connectivity (for OTP list)