

## *MobiSecure*<sup>®</sup> Strong Authentication

### High Volume Mobile Consumer Authentication:

Diversinet MobiSecure<sup>®</sup> Strong Authentication products offer organizations secure and simple ways to introduce multi-factor authentication and help curb identity theft and online fraud. Online banking, trading, commerce and web applications are the prime targets for transaction fraud, identity theft and identity misrepresentation. Hard tokens are costly, cumbersome and difficult to administer for all customers to use for strong authentication. The exponential growth of malicious attacks is driving the explicit need for Internet-based companies to protect their customers now or lose them forever.

MobiSecure<sup>®</sup> Strong Authentication is a fully automated, OATH-standards based strong authentication server product that will provide the protection your company requires. With MobiSecure<sup>®</sup> Authentication solutions, companies can empower all customers with strong authentication (One Time Password) tokens for online access – effectively, efficiently and economically. The mobile one-time-password is an effective and convenient method for promoting two-factor authentication. It is designed to be easy to deploy and easy to use for high volume internet or wireless based strong authentication of user identity.

### Enhanced Security:

Two-factor authentication adds an additional layer of security for online transactions by requiring a user to enter two pieces of identification: something the user knows (username and password) and something the user has (a device generating One Time Passwords). Without either of these factors, access to the user's information is denied, and impostors are prevented from accessing user information.

### Easy-to-use:

The MobiSecure<sup>®</sup> Strong Authentication application can be downloaded onto most mobile phones, PCs and Internet browsers. It can also be delivered to mobile phones via SMS messaging.

MobiSecure<sup>®</sup> Strong Authentication supports multiple tokens for multiple secure services. Instead of carrying a hardware token keychain for each secure service a customer uses, MobiSecure<sup>®</sup> stores all tokens onto the user's device – all the user needs to do is select the service and the appropriate SoftToken is generated.

### Affordable Deployment:

Hard tokens and other strong authentication solutions are costly to deploy and involve significant support costs. Hard tokens have a relatively short lifespan because they rely on batteries that will require replacement, and are easily misplaced because they are carried separately. MobiSecure<sup>®</sup> SoftTokens run inside users' devices, so there is no need for supplementary hardware and loss is rare since users always carry their mobile devices with them.

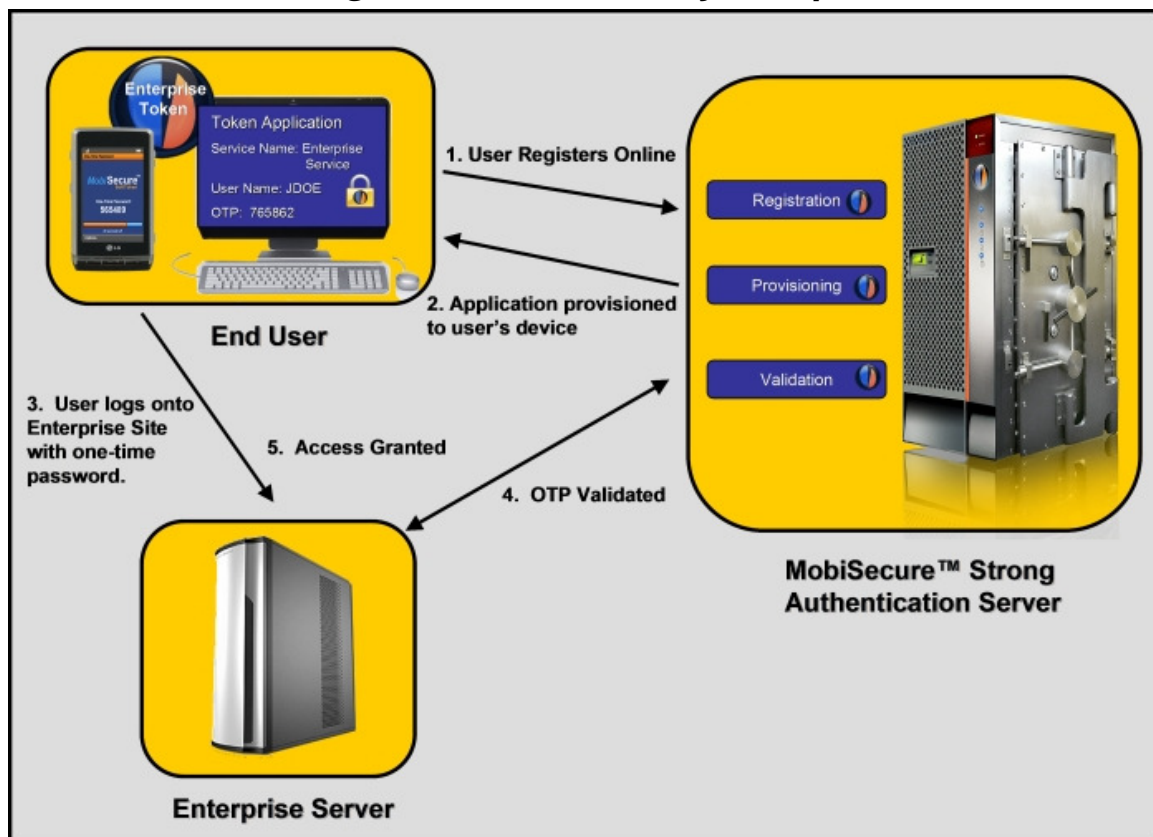


## *MobiSecure*<sup>®</sup> Strong Authentication

### **Key Benefits:**

- **Cost-Effective:** Lower total cost of ownership for token lifecycle management compared to hard tokens
- **Low Cost Usage:** After the initial activation, one-time passwords are generated on the subscriber's device without the need for network connectivity
- **Simple to Install:** Convenient over-the-air device identification and Internet provisioning for mobile devices and personal computers
- **Standards Based:** MobiSecure<sup>®</sup> Strong Authentication uses OATH open standards architecture for universal adoption of strong authentication
- **Extensive Device Support:** Supports all major mobile operating systems (Java phones, Blackberry devices, Windows Mobile, iPhone, Android and BREW)
- **Deployment Flexibility:** Available as a packaged software product for enterprise organizations or as an appliance
- **Customizable:** Fully customizable solution provides white label branding and marketing opportunities

### **MobiSecure**<sup>®</sup> Strong Authentication Key Components



## *MobiSecure<sup>®</sup> Strong Authentication*

### **1) MobiSecure<sup>®</sup> SoftToken**

Client-side token that can be securely delivered to mobile devices or personal computers. It performs functions for generating HOTP-compliant one-time passwords.

Diversinet MobiSecure<sup>®</sup> SoftTokens are supported on a wide range of devices and platforms including:

- Java (J2ME) mobile phones, BlackBerry, Windows Mobile (PocketPC & SmartPhone), iPhone, Android and BREW mobile phones
- Microsoft Windows 2000 and XP and Browser plug-in for a Windows-based version of Internet Explorer 6.0 and above and Mozilla Firefox 3.0 and above
- For customers using older mobile phones or who do not wish to download the application, an SMS-based service can be used to receive mobile SoftTokens

### **MobiSecure<sup>®</sup> SoftTokens have the following features:**

- Lightweight application supporting both Time based and Event based OTP (One Time Password)
- Configurable time steps for Time Based OTP (ie. OTP valid for 30, 60, 90... seconds)
- PIN protection for unauthorized access – subscribers can set Unlock PIN codes for access to the application on their mobile device
- Administrators can configure and manage the PIN policy parameters for Event based One Time Passwords
- Ability to manage SoftTokens (view details, add, delete, change Unlock PIN code)
- Auto-locking feature protects against denial of service attacks and multiple access failures
- Sophisticated Anti-cloning mechanisms implemented

### **2) MobiSecure<sup>®</sup> Strong Authentication Server:**

- **Provisioning:** Provides over-the-air device identification and Internet provisioning for mobile devices and personal computers
- **Validation:** Provides the OATH compliant one-time password validation to grant user authentication, synchronization and access
- **SMSToken:** Provides OATH compliant one-time password generation and delivery to mobile phones using the SMS (Short Message Services) channel.
- **Registration/Administration:** A secure, easy to use administrative web interface for enterprise customer operators to manage subscribers

### **3) MobiSecure<sup>®</sup> Strong Authentication Toolkit**

MobiSecure<sup>®</sup> SoftToken can be embedded into customer client applications using SDK's for mobile platforms and Windows PC. Key features of the MobiSecure<sup>®</sup> Strong Authentication Toolkit are listed below:

- Lightweight library allows for a modular implementation- use only the components you need
- Client API available in C and Java programming languages for software clients
  - Allows organizations to develop their own clients or integrate with existing applications
  - DLL provided for rapid development on Microsoft Windows platform
- Server API
  - SPML interface for integrating enterprise applications
  - SPML Java client libraries for rapid integration
- Free Radius interface to OTP Validation Server

## *MobiSecure*<sup>®</sup> *Strong Authentication*

### **MobiSecure<sup>®</sup> Strong Authentication Server has the following features:**

- Supports both Event and Time Based One Time Passwords
- Supports hosting, distribution and provisioning of several custom mobile applications associated to different client organizations or services
- Capable of hosting multiple client organizations and organizational units
- Auto Device Detection technology that automatically detects the type of device the subscriber is using and will provision the appropriate application to that device over-the-air
- Provisioning confirmation – the one-time-password is tested as a part of the real-time provisioning process
- Can be branded using the enterprise customers specifications upon request
- No sensitive user information is stored in the MobiSecure<sup>®</sup> Strong Authentication environment
- Seamless integration with existing systems based on an HTTP Get Request and Response interface protocol or a RADIUS interface for one-time password validation
- Support for SMS Push and Pull features
- Role-based user access levels – Users can be authenticated via static passwords, HOTP or user certificates
- System configuration, message customization, device management, and subscriber management capabilities
- SPML interface provided for SoftToken management and service ordering

### **4) Security Features**

- Sensitive data is encrypted using a 256 bit AES master key protected in the hardware security module (HSM) or generated in the software and protected in a JAVA keystore per enterprise customer security policies
- Preservation of user anonymity and sensitive data identifiers
- Data in transit between MobiSecure<sup>®</sup> Strong Authentication and external sources is encrypted by a proprietary algorithm and SSL
- Data integrity checks for audit logs
- Unauthorized access data wipe

### **5) Deployment Alternatives**

- The MobiSecure<sup>®</sup> Strong Authentication product can be delivered to enterprise customers in many ways:
  - As a packaged appliance that is delivered to the customer for implementation in their environment. The software comes with SDKs to ensure a seamless integration with legacy systems (Windows & Linux)
  - As an OEM product where selected services can be repackaged for distribution by an enterprise customer. These components can be installed in a single system or distributed environment.
- Service is available in English, French and Spanish