



EzIdentity™ Strong Authentication, Transaction Security, Digital Signing

➤ Multi-factor, Multi-layer Security

Multi-factor, multi-layer strong authentication

EzIdentity™ Authentication platform enables financial institutions, managed service providers, and other organizations to support a wide range of authentication methods, building customer confidence in online transactions, increasing security, and reducing costs. Whether interested in strong 2nd factor authentication or Transaction security or PKI Digital Signatures, the EzIdentity™ Authentication platform provides a highly scalable, centralized authentication server with the capability to manage a wide range of security tokens.

Key features

Wide range of authentication methods

- Hardware and Software One-Time Password strong authentication Tokens.
- Hardware and Software One-Time Password Signature Token transaction security Tokens.
- Certificate Management, PKI-based Digital Signing Tokens.

Comprehensive management tools

- Integration with remote authentication servers, such as LDAP and RADIUS, enables consolidation of multiple physical schemes into a single logical authentication model within a Service Oriented Architecture.
- Full lifecycle management of Software and Hardware token devices.
- All authentication and administration actions are recorded within a centralized, audit logs.
- Web self-service tools including token/ card activation, PIN reset and password maintenance.
- Multiple service channel support (Web, IVR, ATM etc.) using a single authentication method.

Rapid deployment capabilities

- 4TRESS Authentication Server can be deployed in a variety of ways:
- As an appliance
- Software as a Service (SaaS) exposed as a through a standards based public API that can be accessed via SOAP, RMI, standardized XML schemas such as SAML, or HTTP APIs
- Software installation



Benefits

Consistent authentication

Enables a consistent customer verification model to be implemented across various applications and channels.

Ease of management

Supports multiple concurrent authentication methods enabling an organization to implement an appropriate level of security for different user groups and the phased migration of users between authentication models

Scalable resilient architecture

Scales to support large customer bases, e.g. retail banking, and provides the high availability required for customer-facing systems.

Ease of Deployment

Streamlines integration with existing and future applications through industry standard technologies and interfaces. EzIdentity™ also provides a browser-based user interface that requires no client installation.

Return on investment

Consolidate multiple authentication servers across separate business units or subsidiaries into a single solution. In addition, web based self-service function such as card activation and token unlock reduces operational cost of administering strong authentication.



Software



Virtual Appliance



Appliance



SAAS





EzIdentity™ Strong Authentication, Transaction Security, Digital Signing

Operating systems

- RED HAT® Linux 5.3
- Centos®

Hardware

- Dell R-200 Series
- IBM x and p Series® Servers

Application server

- IBM WebSphere® Application Server
- Oracle® Database and Microsoft® SQL Server

Devices

- ActivIdentity Tokens
- VASCO Tokens
- InCard® DisplayCard® and all other OATH compliant hardware devices
- OATH compliant software tokens for mobile phones
- OATH compliant software tokens for laptops, PC, Workstations

Authentication schemes

- One-time passwords (OATH)
- One-time password (OCRA)
- Out-of-band authentication (SMS | IVR | e-mail | USSD)
- PKI PKCS#1 PKCS#7

Administration features

- Token Provisioning
 - Assign
 - Uassign
 - Mark as Active | Inactive | Lost
 - Search
- Device management
 - Synchronise
 - Unlock
 - Import
- Certificate management
 - Generate
 - Revoke
 - Reissue
- User and permission management
 - User and user group management
 - Role management
 - User / role / group permission management

Secure audit

- Audit log queries
- Online audit verification

Event reporting

EzIdentity™ platform is in-built with its own monitoring and reporting module. Real-time alerts are notified via e-mail | SMS.

Standards compliance

- Sun J2EE™
- RMI and SOAP
- PCI DSS v2

Encryption information

- Protects cryptographic keys using HSM
- Triple DES encryption / decryption of secrets
- Database row level signing

External authentication schemes

- Support for 3rd Party token vendors supporting RADIUS authentication interface
- Remote RADIUS servers
- LDAP v3 systems, enabling integration into directories such as:
 - Computer Associates® eTrust Directory
 - IBM Tivoli Directory Server
 - Microsoft® Active Directory
 - Novell® eDirectory
 - Oracle Internet Directory
 - Sun Java™ System Directory

Related data sheets

- EzIdentity™EzToken
- EzIdentity™EzSign
- EzIdentity™EzCert

Related solution briefs

- EzIdentity™ Strong Authentication
- EzIdentity™ Transaction Signing
- EzIdentity™ Digital Signing

Americas +1 (510) 396 3894

Asia Pacific +60 12 644 1115

Email info@ezmcom.com



Copyright © 2009 EZMCOM, Inc.. All rights reserved. EZMCOM® and EzIdentity are trademarks of EZMCOM Inc. All other trademarks, tradenames, service marks, service names, and images mentioned and/or used herein belong to their respective owners.