

# ActivIdentity 4TRESS Authentication Server

➤ Secure customer authentication

## Secure, multi-channel authentication

4TRESS™ Authentication Server 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 one time password tokens or smart cards, static passwords or Q&A, 4TRESS Authentication Server provides a highly scalable, secure, centralized authentication server with the capability to manage a wide range of user credentials.

### Key features

#### Wide range of authentication methods

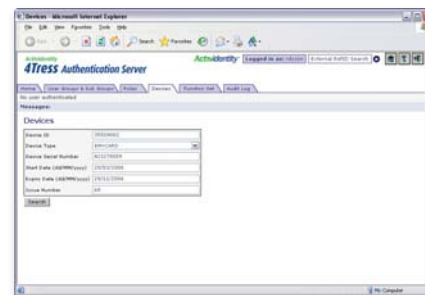
- Token and EMV™ CAP/DPA card based authentication methods.
- Static secrets, in full or partial mode, including passwords, PINs, and secret questions.
- Pluggable framework enables easy extensibility to new authentication schemes such as mobile OTP and voice biometrics.

#### 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 user credentials and physical devices.
- All authentication and administration actions are recorded within a centralized, digitally-signed tamper-evident audit log.
- 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 on a variety of platforms.
- All 4TRESS Authentication Server functions are exposed through a standards based public API that can be accessed via SOAP, RMI, standardized XML schemas such as SAML, or message oriented software such as IBM® WebSphere® MQ.



## Benefits

### Consistent authentication

Enables a consistent customer verification model to be implemented across various service 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.

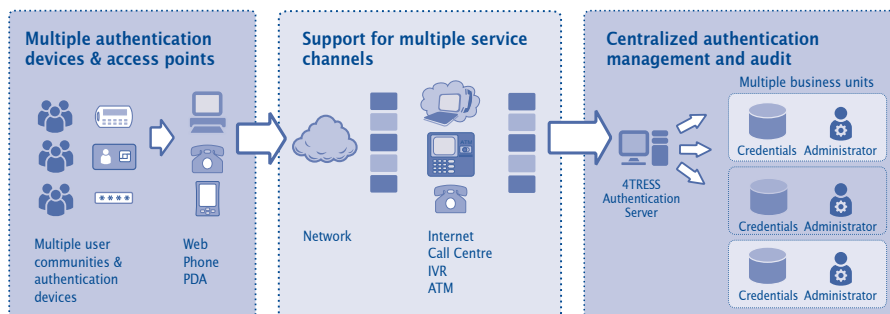
### Ease of deployment

Streamlines integration with existing and future applications through industry standard technologies and interfaces. 4TRESS Authentication Server 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 functions such as card activation and token unlock reduces operational cost of administering strong authentication.

## Complete solution for consumer authentication



4TRESS Authentication Server enables financial institutions, managed service providers, and other organizations to reduce costs and increase security with a scalable and open standards-based platform.

## Operating systems

- IBM® AIX® 5.1
- Sun® Solaris™ 8\*

## Hardware

- Sun SPARC (SunFire 280R, 240)
- IBM pSeries® System p5 Servers
- nCipher® Hardware Security Module (nShield™ and payShield™ for EMV)

## Application server

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

## Devices

- ActivIdentity Solo Reader
- ActivIdentity Tokens
- InCard® DisplayCard® and all other OATH compliant hardware devices
- OATH compliant software tokens for mobile phones
- All EMV™ compliant smart cards

## Authentication schemes

- One-time passwords
  - ActivIdentity one-time password
  - OATH one-time passwords
  - One-time passwords via SMS
- PIN verification
- EMV authentication using ActivIdentity Solo Reader compatible with the following algorithms:
  - MasterCard® CAP
  - VISA® DPA
- Swivel® algorithm
- Static passwords (e.g. username / password logins)
- Question and answer

## Administration features

- Password management
  - Self reset
  - Auto generation
  - Secure PIN mailer
  - Help desk change/reset
  - Set up
- Device management
  - Synchronise
  - Unlock
  - Assign/unassign
  - Import

- Credential management
  - Status (enable/disable)
  - Channel specific usage policies
  - Usage statistics
- User and permission management
  - User and user group management
  - Role management
  - User / role / group permission management

## Secure audit

- Digitally signed tamper-evident log
- Audit log queries
- Online audit verification

## Event reporting

ActivIdentity 4TRESS Authentication Server can report application level events using the following mechanisms:

- Log file entries
- SNMP notifications
- JMX™ messaging

Any enterprise management tool that is compatible with these formats can be used to monitor the ActivIdentity 4TRESS Authentication Server system.

## Standards compliance

- Sun J2EE™
- RMI and SOAP
- MasterCard EMV CAP approved
- VISA DPA compliant
- FIPS140-2 level 3

## Encryption information

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

## External authentication schemes

- Support for 3rd Party token vendors
- ODBC / JDBC data stores
- 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

- 4TRESS Authentication SDK
- ActivIdentity Tokens
- ActivIdentity Solo Reader

## Related solution briefs

- Strong Authentication
- Strong Authentication for Banking
- Device and Credential Management
- Secure Information and Transactions

\*Details available upon request.



To find out more about 4TRESS Authentication Server or for more information about ActivIdentity Financial Services solutions, visit our website

[www.actividentity.com](http://www.actividentity.com)

Americas +1 (510) 574 0100

US Federal +1 (571) 522 1000

Europe +33 (0) 1 42 04 84 00

Asia Pacific +61 (0) 2 6208 4888

Email [info@actividentity.com](mailto:info@actividentity.com)

