

ActivIdentity 4TRESS Authentication Server Appliance for TEMENOS ARC Internet Banking

Versatile authentication appliance for TEMENOS ARC Internet banking




ActivIdentity 4TRESS Authentication Server Benefits

- Trusted and secure electronic channels that motivate customers to move to more flexible and lower-cost service channels
- Strong authentication that addresses user demands for convenience and portability while reducing the cost of fulfillment and management
- Streamlined compliance via a centralized audit trail for customer transactions across channels and products
- The ability to quickly deploy additional layers of security to address new threats

As banks enhance online and mobile channels in response to competition and user demand, they must successfully address risks associated with authenticating their customers and employees. Strengthening security and compliance is an on-going challenge. The ActivIdentity 4TRESS Authentication Server Appliance gives banks using TEMENOS ARC Internet Banking (ARC IB) a unique advantage by accelerating the use of strong authentication. This is accomplished by delivering an appliance pre-configured for TEMENOS T24 (T24) and ARC IB, a Hardware Security Module (HSM), and versatile authentication server all in one cost-effective solution.

The ActivIdentity 4TRESS Authentication Server Appliance provides a complete, versatile authentication solution for banks seeking to easily add authentication from user name and password to a variety of strong authentication mechanisms. The ActivIdentity 4TRESS Authentication Server Appliance adds strategic value by giving banks deploying T24 and ARC IB the flexibility to meet current and future needs for a range of user, device, and service-channel options.

The appliance shortens the deployment time with ARC IB banking software, allowing banks to confidently bring innovative products and services to market across multiple service channels. Securing lower-cost service channels drives economically profitable growth for adopting institutions.



ActivIdentity 4TRESS Authentication Server Appliance Benefits

- Low total cost of ownership (TCO) in a competitively priced all-inclusive package
- Accelerated time to production for banks using TEMENOS T24 and ARC IB
- Streamlined administration leveraging TEMENOS T24 console
- Proven expertise and repeated success with TEMENOS T24 banking environments

ActivIdentity 4TRESS Authentication Server Appliance includes the following features and capabilities for banks using TEMENOS T24 and ARC IB:

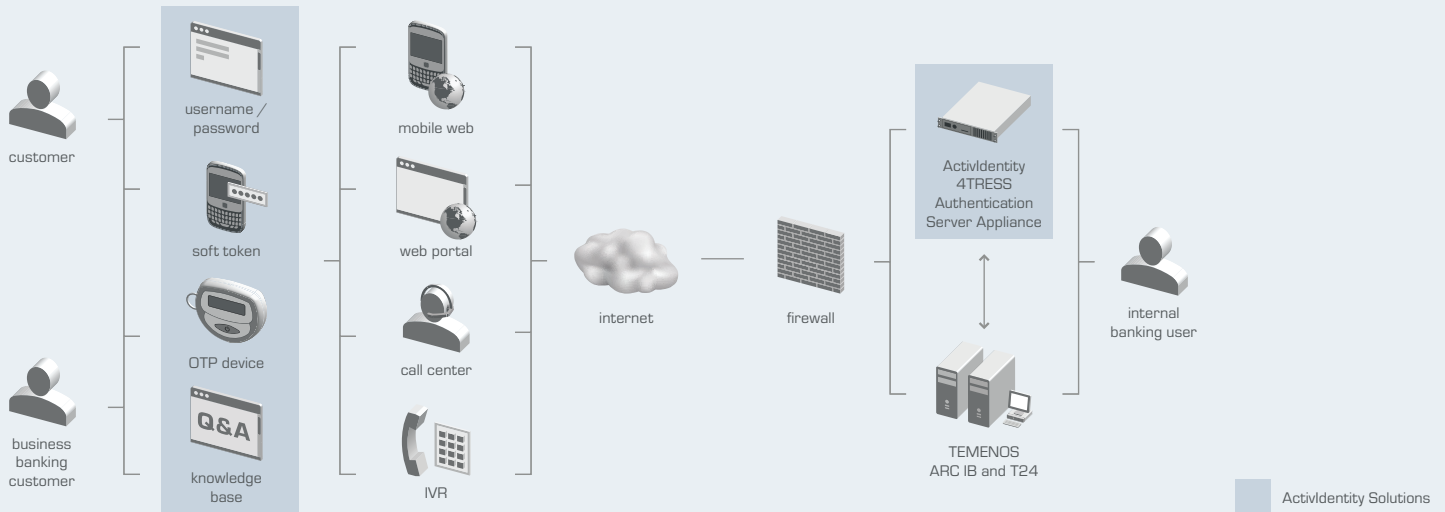
- Pre-configured for easy deployment with T24 and ARC IB
- Automatic creation of user credentials when new users are added via T24 screens
- Management of password lock / unlock and other critical authentication processes directly from T24
- Track authentication events in T24 user views
- Strong authentication and transaction signing for online banking customers
- Hardware security module that is FIPS 140-2 Level 3 certified to meet VISA and MasterCard specifications and provides integrity and confidentiality for keys related to authentication and signing

Versatile Authentication Capabilities

The ActivIdentity 4TRESS Authentication Server Appliance incorporates a versatile authentication server, which is also available as a stand-alone, perpetual software license. This versatile authentication server – ActivIdentity™ 4TRESS Authentication Server – allows banks using ARC IB to use a consistent user verification model across their electronic service channels. The ActivIdentity 4TRESS Authentication Server platform is designed to maximize versatility, accommodate multiple business units, and scale to millions of users.

ActivIdentity 4TRESS Authentication Server includes the following features and capabilities:

- A broad choice of authenticators based on open standards (e.g., Initiative for Open Authentication [OATH] and public key infrastructure [PKI] standards) as well as authentication mechanisms based on proprietary authentication schemes
- Transaction signing and verification support for higher risk interactions
- Centralized authentication, authorization, and audit capabilities to strengthen compliance and streamline reporting
- Device and credential life cycle management



The ActivIdentity 4TRESS Authentication Server supports a broad range of hardware tokens, smart cards, and software tokens.

The ActivIdentity 4TRESS Authentication Server supports a layered approach that enables organizations to tailor the authentication method (e.g., static password, knowledge-based data, OTP, or PKI) and authenticator (e.g., hardware token, software token, or smart card) to specific user groups and risk levels. By providing an open and extensible framework to add new authentication methods and credential types, the ActivIdentity 4TRESS Authentication Server lets organizations respond quickly to new online attacks, evolving business requirements, and changing user needs.

Ease of Deployment

The ActivIdentity 4TRESS Authentication Server Appliance is pre-configured for banks using T24 and ARC IB. In addition, ActivIdentity assists with deployment related to any of the bank’s unique systems environment and ensures a secure key generation process. This allows the appliance to be easily restored or replaced in case of hardware faults or disaster recovery.

At time of deployment, the ActivIdentity Implementation Services team assures proper integration into the bank’s ecosystem. Customers may opt for additional services such as customizations and projects related to ARC IB online banking security including support for PIN mailers and other associated projects.

ActivIdentity 4TRESS Authentication Server Appliance can be deployed in a redundant configuration. In this configuration multiple ActivIdentity 4TRESS Authentication Server Appliances connect to the same external Oracle database. By leveraging a bank’s existing Oracle database investment banks can ensure fault tolerance and high-availability for their mission-critical authentication systems.

Third-Party Interoperability

- TEMENOS
- OATH
- VISA
- MasterCard

Technical Specifications

ActivIdentity 4TRESS Authentication Server		ActivIdentity 4TRESS Authentication Server Appliance for TEMENOS ARC IB	
Built-in Authentication Methods	<ul style="list-style-type: none"> - One-time password: Synchronous (ActivIdentity-patented algorithm) - One-time password: Challenge / response - One-time password: OATH event, time-based, and challenge / response - One-time password: EMV CAP / DPA* - X.509 certificate - Static password - Partial static password - Memorable data (question and answer) 	Appliance	Chassis Form Factor <ul style="list-style-type: none"> - 1U Chassis - 650 W redundant PSU - 8 x 3.5" drive bays - DVD-ROM Processor Type <ul style="list-style-type: none"> - 2.0 GHz CPU Memory <ul style="list-style-type: none"> - 2 x 2 GB RAM Drive <ul style="list-style-type: none"> - 2 x 250 GB Hard Drive Regulatory <ul style="list-style-type: none"> - UL, CUL, CSA, FCC, certification - RoHS compliant
External or Third-Party Authentication Methods	<ul style="list-style-type: none"> - Static password and one-time password (any RADIUS compliant authentication server via proxy) 	Software Operating Environment	Operating System <ul style="list-style-type: none"> - Debian 4.0 R6 Application Server <ul style="list-style-type: none"> - JBOSS 4.2.3 GA Database <ul style="list-style-type: none"> - Oracle 10g Express Edition (local) - Oracle 10g R2 (external high availability configuration)
Authenticators	Hardware Tokens <ul style="list-style-type: none"> - ActivIdentity OTP Token - ActivIdentity KeyChain OTP Token - ActivIdentity Desktop OTP Token - ActivIdentity Pocket OTP Token - ActivIdentity Mini OTP Token - Any OATH compliant event, time or challenge / response-based hardware token - Any EMV CAP / DPA* compliant chip card with reader Software Tokens <ul style="list-style-type: none"> - ActivIdentity PC Soft Token - ActivIdentity Mobile Soft Token - ActivIdentity Web Soft Token DisplayCard Tokens <ul style="list-style-type: none"> - ActivIdentity DisplayCard Token 	Hardware Security Module	Vendor <ul style="list-style-type: none"> - RealSec Crypto Processor <ul style="list-style-type: none"> - ARM7TDMI 50 MHz RISC processor Certifications <ul style="list-style-type: none"> - FIPS 140-2 , level-3 certification - Common Criteria EAL4+ Cryptographic <ul style="list-style-type: none"> - FIPS 186-2 compliant random number generator - Symmetric cipher encryption <ul style="list-style-type: none"> · DES, Triple DES (double and triple length cipher) · SAFER (64 and 128 bits, K and SK modes) - Hash functions <ul style="list-style-type: none"> · MD5, SHA-1, RIPEMD (128 and 160 bits)
Standards Supported	Protocols <ul style="list-style-type: none"> - RMI - SOAP v1.1 - PSKC v1.1 (credential import) Cryptographic <ul style="list-style-type: none"> - OATH event, time and challenge / response-based - EMV CAP / DPA* - 3DES / AES - FIPS 140-2 level 3 (credential storage and data signing) 		
Help Desk and Self Service	<ul style="list-style-type: none"> - Web-based help desk and self service 		
Administration	<ul style="list-style-type: none"> - Device and credential management - User and permission management - Password management 		
Auditing, Accounting and Reporting	<ul style="list-style-type: none"> - Digitally signed tamper-evident log - Audit log queries - Published audit schema - Crystal Reports® 		
APIs and Other Interfaces	4TRESS Authentication Server Public API <ul style="list-style-type: none"> - Authentication - Device and credential administration - Authorization - Session management - Audit - Java RMI and SOAP protocols, libraries for Java, C / C++ and C# included 		

*This functionality is only supported with the software install version.

About ActivIdentity

ActivIdentity Corporation (NASDAQ: ACTI) is a global leader in strong authentication and credential management, providing solutions to confidently establish a person's identity when interacting digitally. For more than two decades the company's experience has been leveraged by security-minded organizations in large-scale deployments such as the U.S. Department of Defense, Nissan, and Saudi Aramco. The company's customers have issued more than 100 million credentials, securing the holder's digital identity.

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
Web www.actividentity.com