

ActivIdentity Solutions for Banking and Finance

Strong Authentication for Banking

For financial institutions seeking to bolster customer adoption of low-cost service channels and ease the management of authentication, ActivIdentity offers a range of leading strong authentication solutions specifically designed for banks. These solutions also help institutions significantly lower the risk of online fraud, comply with industry and government regulations and protect customer data.

Business benefits

Compliance, brand and liability protection

A security or privacy breach can result in high remediation costs and permanent damage to a bank's image. ActivIdentity banking solutions reduce the risks of such events and help banks comply by enabling strong proof of identity, secure transactions and auditing.

Boost image and customer confidence with tangible security

Concerns over security and privacy are key reasons customers abandon low-cost service channels such as online banking. To combat this, banks can provide customers with "tangible evidence" of security using a range of ActivIdentity two-factor authentication devices.

Research confirms that two-factor authentication reduces customers' security concerns and drives online banking adoption. Banks can also extend brand reach by customizing authentication devices with their logo and colors.

Enable online offerings and revenues

Strong two-factor security enables the roll out of additional, higher-value online products and services that may not otherwise be possible with lower security methods. Banks benefit when customers respond to better offerings with increased loyalty and higher-value transactions.

Simplify the customer experience and reduce costs

Institutions can choose to deploy a common method of authentication across all service channels alleviating the burden on customers of remembering complex passwords while lowering associated help desk costs.

For example, banks might leverage their EMV payment card investment and enable customers to use their EMV cards and a single PIN to access ATM machines, pay for groceries at a local shop, and securely access bank accounts and services via phone/IVR or the Internet using a portable EMV card reader.

Highlights

- Tangible two-factor security that enhances customer confidence and increases use of online banking and associated high margin services.
- Broad set of standards-based strong authentication options for consumer and commercial banking and employee authentication.
- Consumer-friendly solutions that address the rise of online attacks and help meet industry regulations for identity, privacy, policy enforcement, audit and authentication.
- Solutions that boost ROI of EMV payment card systems and other banking applications.

ActivIdentity banking expertise

ActivIdentity has over 15 years experience in the banking industry with millions of tokens deployed to hundreds of top banks including the world's largest single consumer banking token deployment. ActivIdentity offers a wide range of authentication options to meet the specific needs of banks.

Authentication management with ActivIdentity 4TRESS™

More than back-end verification of customer authentications, 4TRESS enables highly scalable and secure, open standards-based authentication management capabilities.

Centralized management

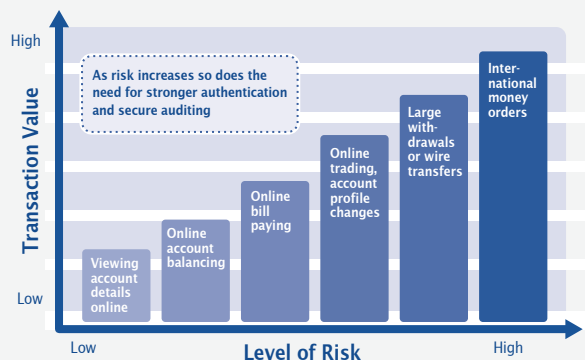
ActivIdentity 4TRESS enables institutions to centrally manage authentication across multiple service channels (web, phone/IVR, ATM, and more) and across unlimited geographically scattered business units. 4TRESS may also be deployed as a managed service to 3rd party institutions. It also enables full lifecycle management of user credentials and physical devices including token/card activation, PIN reset, and password maintenance.

Risk-based authentication

As risk increases, the need for stronger authentication grows. Using 4TRESS, the level of authentication (e.g. static or dynamic passwords) can be adjusted based on customer profile or risk factors such as transaction amount or type.

Secure audit

4TRESS offers unified, digitally signed, tamper-evident auditing capabilities that insure audit log integrity for sensitive data and transactions and facilitate the detection and prevention of fraud and staff collusion.



▶ ActivIdentity Solutions for Banking

Technical benefits

Enhanced security

Enforcement of two-factor authentication through something the user has (the smart card or other security device) and something the user knows (the PIN code). Combined with transaction signing, two-factor authentication guards against phishing and other man-in-the-middle attacks.

Audit logs are hashed, sequenced and digitally signed, making it impossible to eavesdrop or change records without breaking the chain of signatures.

Broad support of authentication methods

ActivIdentity banking solutions support a wide range of authentication methods including: ActivIdentity and all OATH compliant hardware tokens and all EMV™ CAP/DPA compliant smart cards (for one-time passwords and transaction signing) and InCard® DisplayCard®. Also supported are static secrets, in full or partial mode including passwords, PINs and secret questions.

4TRESS™ authentication is easily extensible to support additional authentication methods such as soft tokens on a mobile device and voice biometrics.

Scalable resilient architecture

4TRESS authentication scales to support large customer bases such as with retail banking, and provides high availability required for customer-facing systems.

Rapid deployment capabilities

4TRESS Authentication Server deploys rapidly to a variety of platforms using open interfaces and support for industry standards. All 4TRESS server functions are exposed through a standards-based public API that can be accessed via SOAP and RMI.

Proven technology

4TRESS protects data, with strong hardware based encryption, using widely accepted and verified standards such as 3DES, PKCS#11 and FIPS 140-2 Level 3 validated Hardware Security Modules (HSM). Open standards-based APIs ease integration with other banking applications.

ActivIdentity offers Products

- 4TRESS Authentication Server
- 4TRESS Authentication SDK
- ActivIdentity Tokens
- ActivIdentity Smart Cards
- ActivIdentity Readers
- ActivID™ Card Management System (CMS)
- ActivClient®

Technology solutions

- Strong Authentication
- Enterprise Single Sign On
- Device and Credential Management
- Secure Information and Transactions

Industry solutions

- Smart Employee ID
- Smart Employee ID for PIV
- Strong Authentication for Banking
- Single Sign On for Healthcare

Partner solutions

- Solutions for MasterCard®
- Solutions for Visa®

Smart Employee ID for Banking

Complementary to ActivIdentity Strong Authentication for Banking solutions is the ActivIdentity Smart Employee ID for Banking solution.

The rise in internal attacks at financial institutions globally have highlighted the need for stronger banking employee security solutions. ActivIdentity Smart Employee ID for Banking solution is designed for financial

institutions seeking to deploy a single and secure ID badge allowing employees, contractors, and partners to securely and easily access physical facilities and IT resources. Institutions can look to ActivIdentity to provide market leading solutions for both employee and customer banking authentication needs.

About ActivIdentity

ActivIdentity, Inc. is the trusted provider of identity assurance solutions for business and government worldwide.

ActivIdentity provides the only fully integrated platform that allows organizations to issue, manage and use trusted digital identities for secure access, secure communications, and legally binding digital transactions.

ActivIdentity customers experience multiple business benefits including protection of resources and information, enhanced workforce productivity and regulatory compliance.

Partners and standards groups



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

ActivIdentity®