

# Actividentity Tokens

## ➤ One-Time Password Token Authenticators

### Tokens for a range of user requirements

Strong security starts with ensuring that only the proper people have access to protected network resources and applications. Actividentity offers a range of solutions for strong authentication, backed by a complete line of one-time password (OTP) token authenticators.

Actividentity tokens generate random passwords that can't be reused. Users gain access to resources by possession of the token and knowledge of a secret (a PIN number). The user experience is as simple as using an automatic teller machine, and provides far greater security than a static password.

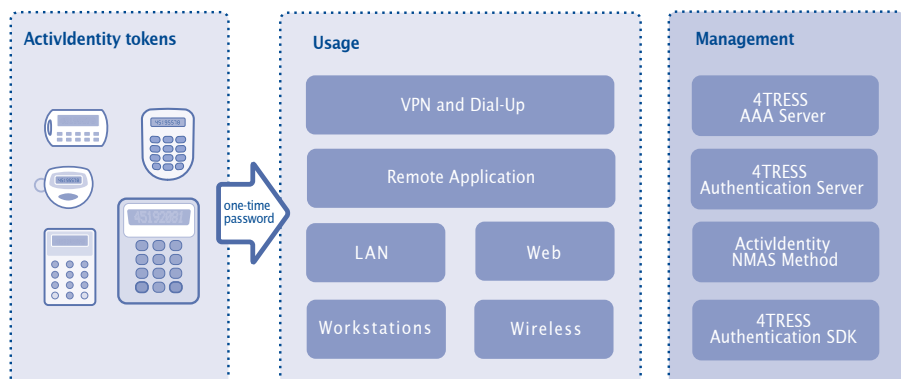
### Key features

#### Strong Authentication

Actividentity Strong Authentication for Remote Access solutions support tokens with VPNs, dial-up networks, web sites, and remote-hosted applications.

- Strong Authentication for Workstation and Network Access solutions support token based authentication with wireless access points and thin clients.
- Strong Authentication for Applications solutions support OTP with standard and custom applications.

### Token usage model



A strong authentication solution for secure application and network resource access

#### Choice of algorithm

- The Actividentity patented 3-variable algorithm is available across the entire token family and provides advanced security for employee authentication and consumers conducting high value transactions.
- Actividentity event-only algorithm provides strong security for everyday consumer authentication.
- Standards-based X9.9 Challenge/Response avoids the problem of out-of-sync tokens for employees.
- OATH algorithm is an OTP open standard, providing compatibility with 3rd party software.

#### Future proof

- Mix and match different tokens in the same deployment. For example, provide Pocket Token to sales representatives, Keychain Token to engineering, and Desktop Token to executives.
- Actividentity algorithms are compatible with the Actividentity OTP smart card applet, providing a smooth path to deploy smart cards in the future.
- Add support for any external data source and extend the data stored on the card with the CMS customizable workflow plug-in interfaces.



### Benefits

#### No expiration date

Actividentity tokens last longer than other tokens on the market. Durability comes from the token design, power conservation, long battery life, and no self-expiration. Stop repurchasing the same token twice - an Actividentity token lasts up to two and a half times longer than a 3 year leased token.

#### Lower operating costs








Re-provisioning an expired token is expensive and inconvenient, and incurs replacement acquisition costs, user down time, and delivering a new unit to the user. Actividentity tokens last longer and can reduce re-provisioning costs.

#### Flexible to meet requirements

With a range of algorithms, form factors, and designs to choose from, customers can choose the right tokens for their diverse user population. Mix and match tokens as needed to get the perfect fit.

#### User satisfaction

Nobody likes security that is hard to use. That's why Actividentity tokens are designed with the user in mind. Consumers appreciate the intuitive one-button design of Mini Token. Employees like being able to set their own easy-to-remember PIN number on tokens with keypads.

|  | Token   | KeyChain Token  | Desktop Token   | Pocket Token   | Mini Token  | Mini Token  | Mini Token  |
|--|---|---|---|--|---|---|---|
|  |                |                |                                |  |  |  |  |
| <b>Version</b>   | V2  | V2  |   |  | AE  | AT  | OE  |
| <b>Key Features</b>  | Range of authentication options plus pin unlock for employee usage                              | Compact and robust design with the same options as the Token v2                                 | Large buttons and display for easier key entry and readability  | Small, durable token for the user on-the-go  | Simple one button design with attractive pricing and long life                      | Support for time+event algorithm for advanced security                              | Support for OATH algorithm for broad open standard compatibility                    |
| <b>Target User</b>   | <ul style="list-style-type: none"> <li>Employee</li> <li>Partner</li> <li>Contractor</li> </ul> | <ul style="list-style-type: none"> <li>Employee</li> <li>Partner</li> <li>Contractor</li> </ul> | <ul style="list-style-type: none"> <li>Employee</li> <li>Office-based User</li> <li>Elderly Consumer</li> </ul> | <ul style="list-style-type: none"> <li>Remote User</li> </ul>                      | <ul style="list-style-type: none"> <li>Consumer</li> </ul>                          | <ul style="list-style-type: none"> <li>Consumer</li> <li>Employee</li> </ul>        | <ul style="list-style-type: none"> <li>Consumer</li> <li>Employee</li> </ul>        |
| <b>Algorithm Support</b>                                   |   |   |   |  |   |   |   |
| ActivIdentity patented Synchronous Time + Event (DES/3DES) | ✓   | ✓   | ✓   | ✓  |   | ✓   |   |
| ActivIdentity Synchronous Event Only (DES/3DES)            | ✓   | ✓   | ✓   | ✓  | ✓   | ✓   |   |
| OATH HOTP  |   |   |   |  |   |   | ✓   |
| Challenge Response X9.9                                    | ✓   | ✓   | ✓   | ✓  |   |   |   |
| Message authentication                                     | ✓   | ✓   | ✓   | ✓  |   |   |   |
| <b>Features and Specifications</b>                         |   |   |   |  |   |   |   |
| PIN Validation on Device                                   | ✓   | ✓   | ✓   | ✓  |   |   |   |
| PIN Validation on Server                                   |   |   |   |  | ✓   | ✓   | ✓   |
| LCD Size (Char)  | 10  | 10  | 10  | 10   | 8   | 8   | 8   |
| Display  | Dot matrix 5x7  | Dot matrix 4x7  | Dot matrix 5x7  | Dot matrix 5x7   | Segments  | Segments  | Segments  |
| Waterproof   |   |   |   |  | 1 meter   | 1 meter   | 1 meter   |
| Battery Life Expectancy                                    | 3 years for main battery; 8 years for backup battery  | 6 years   | 3 years for main battery; 8 years for backup battery  | 6 years  | 8 years   | 6 years   | 8 years   |
| User-replaceable Battery                                   | ✓   |   | ✓   |  |   |   |   |
| <b>Software Support</b>                                    |   |   |   |  |   |   |   |
| 4TRESS AAA Server for Remote Access 6.4.1                  | ✓   | ✓   | ✓   | ✓  | ✓   |   |   |
| 4TRESS AAA Server for Remote Access 6.5                    | ✓   | ✓   | ✓   | ✓  | ✓   | ✓   | ✓   |
| 4TRESS Authentication SDK 2.2                              | ✓   | ✓   | ✓   | ✓  | ✓   | ✓   | ✓   |
| ActivIdentity NMAS Method 3.0                              | ✓   | ✓   | ✓   | ✓  | ✓   |   |   |
| 4TRESS Authentication Server                               | ✓   | ✓   | ✓   | ✓  | ✓   | ✓   | ✓   |
| OATH-based Server  |   |   |   |  |   |   | ✓   |
| <b>Physical Specifications</b>                             |   |   |   |  |   |   |   |
| Size (mm)  | L82xW52xH4.5  | L62xW43xH12   | L140xW108xH35   | L48xW68xH8   | L45xW38xH11   | L45xW38xH11   | L45xW38xH11   |
| Weight   | 25 g  | 25 g  | 225 g   | 28 g   | 25 g  | 25 g  | 25 g  |

To find out more about tokens or other ActivIdentity products, 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)

**ActivIdentity**<sup>®</sup>