HID Global’s 4TRESS Authentication Appliance supports a multitude of authentication methods to protect your data, network and systems. 4TRESS allows enterprises to tailor authentication methods to the needs of specific groups of users, providing each the right balance of security, cost and convenience to meet their business objectives.

4TRESS increases productivity by securely authenticating users remotely via their preferred smartphone, browser or computer through a variety of devices and authentication methods. 4TRESS Authentication Appliance supports the broadest choice of authentication methods, from strong passwords through to certificate-based authentication, including two-factor OATH-standards-based hardware tokens, soft tokens, and SMS Out-of-Band One-Time Password (OTP) options.

4TRESS Authentication Appliance reduces costs with easy installation, worry-free tokens that last up to eight years, and simple integration into the enterprise’s existing network infrastructure.

**Improve productivity**
- Secure access from laptops, browsers and smartphones with two-factor authentication
- Connect employees, contractors and partners as needed for maximum business efficiency
- Simple and affordable enough for telecommuters, day extenders, road warriors and heavy smartphone users
- Standards-based OATH tokens provide the broadest range of features, suppliers and price points to best meet business needs

**AT-A-GLANCE:**

**THE 4TRESS AUTHENTICATION APPLIANCE BENEFITS INCLUDE:**
- Increase productivity: securely connect users from any location through a variety of devices and authentication methods
- Decrease risk: securely connect users via robust two-factor authentication, which inhibits breaches
- Reduce costs: by using a versatile, future-proof authentication platform
- Improve control: by employing an open and fully interoperable OATH-standards-based authentication and by extending the choice of authentication devices
- Extend value: secure smartphone, iPad, laptop & PC access to VNPs, web portals and cloud applications

hidglobal.com
Soft tokens allow more convenient and economical strong authentication of remote workers.

Soft tokens don’t require extra devices or rekeying. They are easy to distribute, cost-effective and can be recycled as employees change.

Short message service (SMS) one-time passwords (OTP) ensure secure connectivity when tokens are not available or preferred.

Easy migration
Appliance simplifies and streamlines deployment.

- Works concurrently with legacy authentication servers for graceful and efficient migration, which maximizes the ROI of old tokens and ensures a low-risk migration.
- Ability to leverage existing user directories eliminates the need for user migration during deployment.
- Able to link to multiple LDAPS with a single front end.

Decrease risk
- Enterprises can generate their own seed files.
- Using PIN + token enhances security and provides the confidence to connect with all forms of digital connections.

Multi-factor authentication limits impact of some forms of malware.

Strong authentication improves regulatory compliance and policy adherence.

Three-factor authentication is provided via time, event counter seed key and PIN usage with algorithm.

Supports the broadest range of OTP algorithms based on OATH open standards, including time-based, event-based and proprietary time+event-based algorithms for maximum security, utility and value.

Tokens auto-synchronize to improve reliability and security and reduce support calls.

Integrates seamlessly with full suite of credential management, middleware, smart card, single sign-on, mobility and physical access control offerings.

Integrates with Active Directory and most standard LDAP to match the scalability and availability of the enterprise’s network.

Versatile authentication reduces costs.

“We wanted the ability to rapidly deploy authentication methods to meet the market need without changing the infrastructure and technology each time and 4TRESS allows us to do this.”

Maud Brunswick, Project manager @ BNP Paribas
Strong Authentication for Cloud Applications: How It Works

1. User navigates to URL of cloud application
2. User is redirected to 4TRESS login portal
3. User authenticates to 4TRESS login portal via strong authentication
4. User is granted access to the cloud application

Broad range of authentication methods

- OTP tokens (Mini Token, Pocket Token, Token One, Desktop Token)
- Display Cards
- 3rd party tokens compliant with the Oath OTP standards (HOTP / TOTP)
- Vasco Digipass tokens
- Mobile, PC, Web tokens
- DeviceID
- Strong passwords (full and partial)
- Security questions & answers (full and partial)
- Certificate-based authentication (PKI)
- Smart cards running the OTP applet
- Out-of-band SMS (password or verification code)
- Out-of-band Email (password or verification code)
- Temporary activation codes
- LDAP passwords
- RADIUS authentication
- Virtual appliance option

- Compliant with the OATH industry standard, eliminating vendor “lock-in”
- Competitively sourced, standards-based OATH tokens ensure right features and best value
- Tokens can last up to eight years, 2x to 3x longer than other solutions, dramatically lowering token replacement and redeployment costs
- Soft tokens deploy more efficiently

Improve Control

- Policy driven, organization-wide authentication solution with fine-grained authentication policies
- Easily integrates with applications to leverage strong authentication
- Digitally signed and sequenced audit logging and policies
- Secure, highly scalable (from 100s to millions), resilient architecture
- FIPS 140-2 HSM option to secure an enterprise’s keys

“Almost 50% of data breaches exploit stolen or weak credentials.”

## SPECIFICATIONS

### 4TRESS Authentication Appliance

#### Built-in Authentication Methods
- One-time password: Synchronous (ActivIdentity patented algorithm)
- One-time password: Challenge / response
- One-time password: OATH HOTP Event, TOTP Time-based, and OCRA challenge / response
- Oath transaction signing (OCRA)
- Smart Card PKI / X.509 certificate
- Emergency full and partial strong Static Password & Security Questions
- Out-Of-Band One-Time Password or Transaction Verification code sent via SMS or Email
- Device ID - Web Browser Registration
- 4TRESS Fraud Detection - Device Profiling & Risk Based authentication

#### External or Third-Party Authentication Methods
- LDAP fallback & passthrough
- RADIUS conditional routing

##### Hardware Tokens
- OTP Token VL
- KeyChain OTP Token
- Desktop OTP Token
- Pocket OTP Token
- Any OATH compliant event, time or challenge / response-based hardware token

##### Software Tokens
- PC Soft Token
- Mobile Soft Token (iPhone, Android, Java, Blackberry)
- Web Soft Token

##### Display Card Tokens
- Display Card Token

##### User Repositories
- Embedded Oracle 11g R2 Standard Edition with integrated fault tolerance
- Microsoft Active Directory
- Oracle / Sun Java Directory
- Novell eDirectory

##### Standards Supported
- SAML v2
- RADIUS Authentication and Authorization
- Web Services (RMI & SOAP v1)
- LDAP v3
- PSKC v1.0 (credential import)

#### Cryptographic
- OATH event, time and challenge / response-based
- 3DES / AES / RSA / ECC / SHA-2
- FIPS 140-2 level 3 HSM (credential storage and data signing)

##### Help Desk and Self Service
- Web-based help desk
- Localizable & U.S. Section 508 compliant

##### Administration
- Device and Credential management
- Authentication Policy management
- User and Permission management

##### Auditing, Accounting and Reporting
- Digitally signed & sequenced tamper-evident audit log
- Audit log queries
- Published audit schema

### 4TRESS Authentication Appliance FT2011

- Processor Type
  - 2.0 GHz CPU

- Appliance
  - Chassis Form Factor
  - 1U Chassis
  - 650 W redundant PSU
  - DVD-ROM

- Memory
  - 8 GB RAM

- Drive
  - 4 x 250 GB Hard Drive
  - Hardware RAID 1 Mirroring

- Regulatory
  - UL, CUL, CSA, FCC, certification
  - RoHS compliant

- Host
  - Recent Intel® 32bit or 64bit; with min. 2.2 Ghz, Dual Core
  - 4GB of RAM (6GB or more recommended)
  - 150GB of free HD space
  - VM Guest
  - At least 2.5GB of RAM (4GB recommended)
  - 2 CPUs/Cores
  - 2 local network connection

- Operating System
  - Oracle Enterprise Linux – Hardened Application Server
  - JBOSS 4.2.3 GA

- Database
  - Oracle 11gR2 Standard Edition
  - Embedded with fault tolerance

- Vendor
  - RealSec Crypto Processor
  - ARM7TDMI 50 MHz RISC processor

- Processors
  - FIPS 140-2, level-3 certification
  - Common Criteria EAL4+

- Cryptographic - Random
  - FIPS 186-2 compliant random number generator
  - AES, DES, Triple DES (double and triple length cipher);
  - SAFER (64 and 128 bits, K and SK modes)
  - Throughput: 320-600 MBs
  - AES, DES, Triple DES (double and triple length cipher);
  - SAFER (64 and 128 bits, K and SK modes)

- Hardware Security Module (optional)
  - RSA 1024, RSA 2048
  - SHA 4096 & ECC ready
  - Throughput: 337-7240 exp/s

- Cryptographic - Hashing
  - Hash functions: MDS, SHA-1, RIPEMD (128 and 160 bits)