

Request a
ZSentry trial

ZSentry™ User Access Control Strong Authentication and Authorization

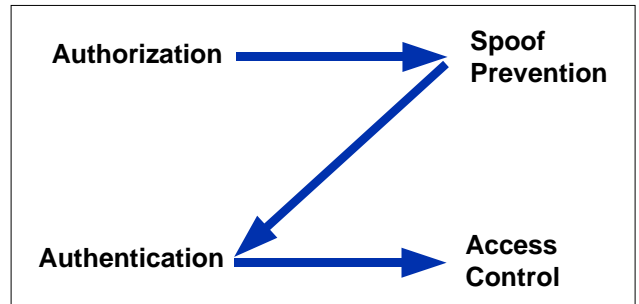
ZSentry is the most **cost-effective** solution for secure and flexible access control. ZSentry provides strong user authentication and authorization that is **easy-to-use** and **easy-to-deploy** for a variety of applications:

- ✓ VPN
- ✓ Web Applications
- ✓ Active Directory and LDAP Services
- ✓ Remote Access
- ✓ RADIUS Authentication
- ✓ File Control
- ✓ Document Signing
- ✓ Wireless Transactions
- ✓ 802.11 Wireless LAN

Key Benefits

- ◆ Includes five credential types for maximum usage and control granularity:
 - DTC, Password, Return Code, User ID, Authorization Information*
- ◆ Immediate credential suspension and revocation
- ◆ Supports non-repudiation and develops trust for both users and managers
- ◆ Operates without databases, shared secrets, PKI
- ◆ Significantly reduces costs and complexity
- ◆ Scalable, flexible, secure
- ◆ Centralized user administration, control delegation and user self-service interface with ZAuthority™ - the NMA ZSentry Administration Authority
- ◆ Supports any client including browsers, PDAs, cell phones and pagers

See the reverse side for a typical ZSentry system diagram and comparison with other systems.



Very Simple User Interface

The *DTC™*, a mnemonic digital transaction certificate (e.g., 4KALEP), and a private *Password* are entered by the user in a familiar "user name and password" login dialogue.

How it Works

The *DTC* is used to calculate a *Return Code* to prevent spoofing, to authenticate the user's private *Password*, and to provide the user's *Authorization Information* and unique *User ID* for back-end access control.

ZSentry is an Integrated Access Control Solution

Access Control	Granting access to objects, based on the trusted identity of users.
Authentication	Corroboration of a credential or claim.
Authorization	Conveyance of rights, power or privilege to see, do or be something.
Control Delegation	Allowing local control of a sub-domain within a domain.
Non-Repudiation	Preventing the effective denial of an act.
Spoof Prevention	Preventing a user from relying on false information that masquerades as legitimate.
Trust	Qualified reliance on information, based on factors independent of that information.



Comparison of User Authentication Systems

User Name and Password
 RSA® SecurID®
 NMA ZSentry™

