

# Strong Authentication

Selim Aissi, PhD, CISSP

Digital ID World Conference 2004

**Session:** Emerging Identity Technologies Next Decade: Role of Smartcards in Strong Authentication

October 26, 2004

# Thoughts

- **Let's agree on one Generic Definition!**

- **Network Security – Private Communication in a Public World.** Charlie Kaufman, Ridia Perlman, and Mike Speciner.
  - *In Strong Authentication, someone can prove knowledge of a secret without revealing it. Strong Authentication is possible with cryptography.*
  - *Strong Authentication is authentication where someone eavesdrops on the authentication exchange does not gain sufficient information to impersonate the principal in a subsequent authentication.*
- **SP 800-63 Electronic Authentication Guideline: Recommendations of the NIST, June 2004**
  - *In Strong Authentication (Level 4), either public key or symmetric key technology may be used.*
  - *Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.*
  - *Strong Authentication is based on proof of possession of a key through a cryptographic protocol.*
  - *The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher.*
- **U.S. Federal government**
  - *Strong authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network.*

- **The 14 Smartcard Values in Strong Authentication**

1. Principle controls the card
2. Walk-away factor
3. Turnkey operation
4. Tamperproof
5. Supports strong cryptographic algorithms
6. Can support Kerchhoff's Principle (Enemy may not be ignorant about the methodology, but rather about "key" information)
7. Can support Zero-Knowledge Proof (Prover convinces Verifier of a statement without revealing any information)
8. Credential aggregation
9. Provisioning/De-provisioning of identities
10. Supports various Policy Enforcement models
11. Can provide Platform authentication
12. Can be leveraged across multiple Applications and Networks
13. Can support anonymity
14. Can support Multiple Trust Levels (between user and service provider)