

Certificate Authorities: Security and Business Considerations

WICS
July 29, 1998



Jim Cowing
Digital Resources Group

jim@drgsf.com
415.508.8959
www.drgsf.com

Agenda

- ❖ **Goals and Overview**
- ❖ **Objectives of a Certificate Authority**
- ❖ **Keys to CA Success**
- ❖ **Authentication**
- ❖ **Other Significant Considerations**
- ❖ **Security Issues**
- ❖ **Technical Infrastructure**
- ❖ **How Do the Existing CA's Compare?**



Goals and Overview

- ❖ Who are Certificate Authorities
- ❖ How do they Authenticate Users
- ❖ Required Attributes of CA's
- ❖ Security Issues for the CA



CA Business Objectives

- ❖ Full Product Line of Certificates
- ❖ Customer Support
- ❖ Timely Delivery
- ❖ Strong Authentication
- ❖ Security everywhere
- ❖ Secure Storage of the Root Private Key
- ❖ Make Money



Customer's View of CA Success:

- ❖ Trust
- ❖ Price
- ❖ Support
- ❖ Reputation (Brand)



Authentication

- ❖ Most Critical Aspect
- ❖ Basis of your Trust Reputation
- ❖ Errors can be Costly
- ❖ Time is of the Essence
- ❖ Cost needs to be Minimized



Authentication Models

- ❖ In Person / Presence
- ❖ Electronic Authentication
 - Dunn & Bradstreet
 - TRW, Equifax and credit bureaus
- ❖ Other validation measures
 - Articles of Incorporation, Bylaws
 - Bank or Employment verification
 - Dial Back validation
- ❖ High Risk Biometrics



VeriSign's Cert Model

- ❖ Class 1: No authentication - email
- ❖ Class 2: Minimum authentication
- ❖ Class 3: Substantial authentication
- ❖ Class 4: High security



Other Required CA Attributes

- ❖ Financial Capability
- ❖ Legal Expertise
- ❖ Technical Competence
- ❖ Support / Operational Infrastructure
- ❖ Security Background
- ❖ Insurance



Financial Capability

- ❖ Substantial Infrastructure Costs
- ❖ Technological Obsolescence
- ❖ Resources
 - Long-term: minimal
 - Short-term: substantial
- ❖ High Level of Required Security
- ❖ Certificate Revenue Model “Shaky”



Legal Expertise

- ❖ CPS required - major undertaking
- ❖ Substantial Liability Risk
 - Subscriber liability
 - Relying party liability
 - RA / CA Liability
- ❖ Risk Assessment key to authentication
- ❖ Localization
- ❖ Compliance with Local Statutes



Technical Competence

- ❖ Certificates are defined by X.509 Intl Std.
- ❖ “Bleeding-Edge” Technology
- ❖ Lack of standards (Netscape, MIE)
- ❖ New Standards are being set everyday
- ❖ Crypto, key management and internet expertise
- ❖ Performance is definitely an issue
- ❖ Business Resumption (Redundancy) key



Operational / Support Infrastructure

- ❖ Secure facilities
- ❖ High availability
- ❖ High performance
- ❖ Scalability
- ❖ Telecom competence
- ❖ Customer Service support intensive



Security Requirements

- ❖ Understanding of Security and Controls
- ❖ Secure Physical Facility with BR site
- ❖ Secure storage of customer data
- ❖ Cryptographic hardware required to store keys
- ❖ Bonded personnel
- ❖ Security policies and procedures
- ❖ Key Management Experience Critical
- ❖ Audit logging of activities



Physical Site Security

- ❖ Secure Facility
- ❖ External Access Control Requirements
- ❖ 7 x 24 x 365 Guards
- ❖ Internal Strong authentication
- ❖ Dual control security devices
- ❖ Biometric access controls to root key generation and storage areas



Cryptographic Solutions

- ❖ Root stored in Hardware (BBN box)
- ❖ PCMCIA cryptographic hardware devices
 - FIPS 140-1 compliance
 - Tamper resistance
- ❖ Consider split key techniques
- ❖ Largest key sizes possible (2048) at the top of the trust chain

Certificate Authority Sites

☞ USA

Entrust www.entrust.com

CertCo www.certco.com

VeriSign www.verisign.com

GTE CyberTrust
www.cybertrust.com

NIST www.nist.gov

IBM World Registry
www.ibm.com/security

Microsoft

www.microsoft.com/security

VeriFone

www.verifone.com

GlobeSet

www.globeset.com

International

SEMPER www.semper.org

Trust Factory www.secude.com

Thawte www.thawte.com

DRG Digital Resources Group



Secure Electronic Commerce Consulting