Overview

- Business-to-Business (B2B) Perspective
- Common PKI Product Shortfalls
- A Certificate Hierarchy for B2B Processes
- MAC Labels Derived from X.509 Certificates
- Label Structured for Business Relationships
- Local Construction & Validation of Label
- Conclusions
**B2B Perspective**

- Public Key Infrastructure (PKI) is basic
  - Overwhelmingly promoted as security answer
- Black Forest Group (BFG) assessment
  - Consortium of global enterprises
  - Represent sectors using half of world’s IT
  - Secure PKI is major enabler for E-business
  - Current products add risks, not solutions
- Proposed BFG PKI Framework
  - Dynamic Distributed Labels are linchpin
  - X.509 certificate extension
  - Demonstrated – 5 Million Novell certificates

**Common PKI Product Shortfalls**

- Distorted Intermediary Liability
  - Inadequate Basis for Damage Recovery
  - Cross Certification
  - Bridge Certification Authority
  - No Clear **Liability Allocation**
- Processing of Certificate Policies
  - Name Constraints
  - OID Policy Constraints
  - Composite Impact of Entire Chain
  - Online Lookup via “Trusted Services”
  - No Support for **Distributed Validation**
A Certificate Hierarchy for B2B Processes

MAC Labels Derived From X.509 Certificates

Key Quality

Reflects the confidentiality and the “unguessability” of the key generation used to generate the subject key of this certificate.

Certificate Quality

Reflects confidence that the certificate contents reflect the intent of the individual who signed this certificate.

Constraints

Reflects constraints imposed upon the identity properties of the subject of the certificate by the certificate issuer.
Label Structured for Business Relationships

Key Quality
Certificate Quality
BFG Security Label

User Label
Enterprise Label
Registry Label

La | Lb | Ca | Cb | Sca-1 | Sca-16 | Scb-1 | Scb-16
---|---|---|---|------|-------|-------|-------
1-255 | 1-255 | 12..96 | 12..64 | Singleton Range | Singleton Range | Singleton Range | Singleton Range

Local Construction & Validation of Label

Certificate Chain
High Integrity Root
Certificate Chain
Greatest Lower Bound Calculation
Dominance Comparison
Certificate Chain Valid for Particular Business Process
Summary

- SAC Needed to Secure B2B Transactions
  - Value Laden Transactions
  - Business with “Almost Strangers”
- Current PKI Solutions Lack Basis for SAC
- Distributed Dynamic Labels Enable SAC
  - Allocation of Liability to Responsible Parties
    - Label Composition Constrains Subordinate Certs
    - Greatest Lower Bound of All Certs in Chain
  - Local Validation of Certificates for Business Use