


B2B Needs For Strong Access Controls

Dr. Roger R. Schell
schellr@alum.mit.edu

Copyright © 2000
Dr. Roger R. Schell



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

Copyright © 2000
Dr. Roger R. Schell



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

Copyright © 2000
Dr. Roger R. Schell

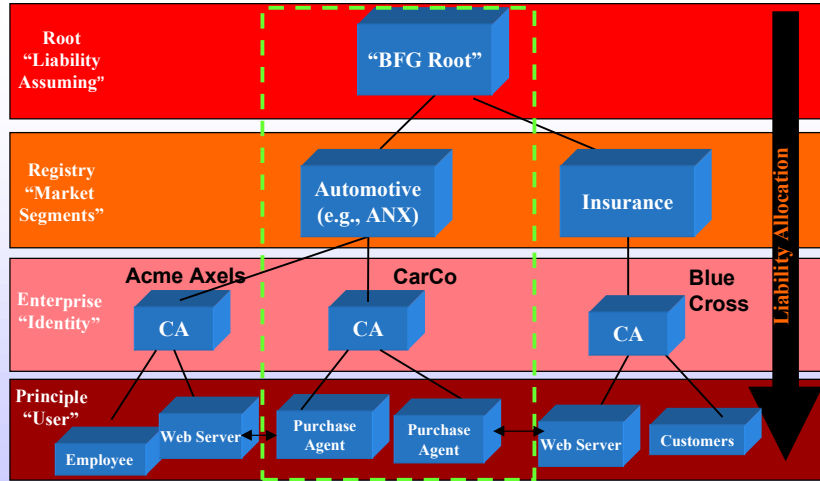


Common PKI Product Shortfalls

- ◆ 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**

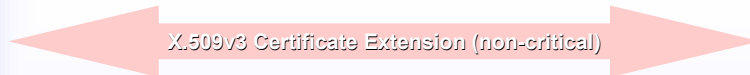
Copyright © 2000
Dr. Roger R. Schell

A Certificate Hierarchy for B2B Processes



Copyright © 2000
Dr. Roger R. Schell

MAC Labels Derived From X.509 Certificates



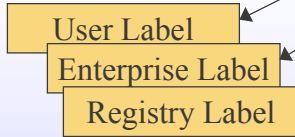
Reflects the **confidentiality** and the **“unguessability”** of the key generation used to generate the subject key of this certificate

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

Reflects **constraints** imposed upon the identity properties of the subject of the certificate by the certificate issuer

Copyright © 2000
Dr. Roger R. Schell

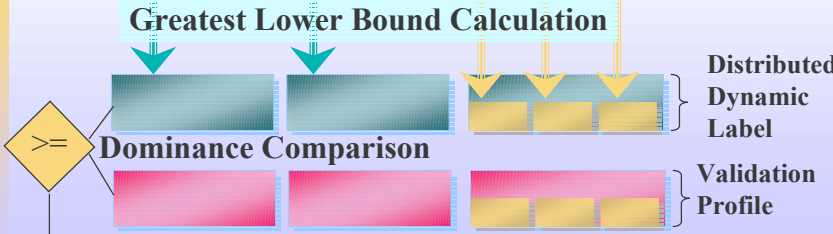
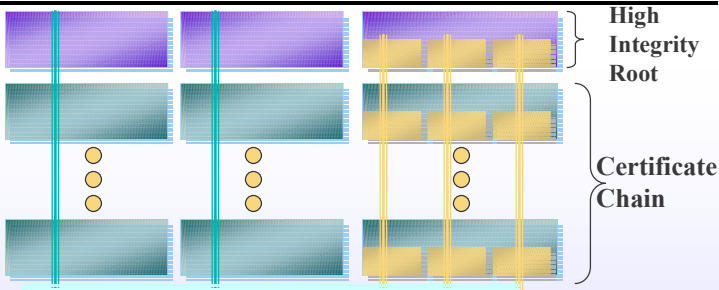
Label Structured for Business Relationships



La	Lb	Ca	Cb	Sca-1	Sca-16	Scb-1	Scb-16
1-255	1-255	1,2..96	1,2...64	Singleton Range	Singleton Range	Singleton Range	Singleton Range

Copyright © 2000
Dr. Roger R. Schell

Local Construction & Validation of Label



→ Certificate Chain Valid for Particular Business Process

Copyright © 2000
Dr. Roger R. Schell



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