

GEMINI
SECURITY SOLUTIONS

Approaches to Certificate Path Discovery

Steve Hanna
Sun Microsystems

Peter Hesse
Gemini Security Solutions

Matt Cooper
Orion Security Solutions

Ken Stillson
Mitretek Systems

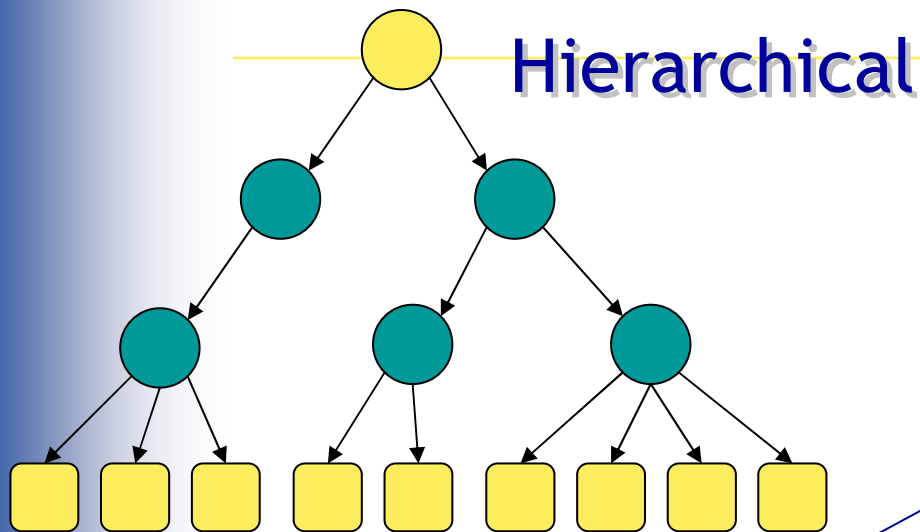
Agenda

- ▼ **PKI Structures**
- ▼ **Overview of Path Discovery**
- ▼ **Path Discovery Implementations**
 - Briefed by each panel member
- ▼ **Questions**
 - Prepared questions
 - Audience questions

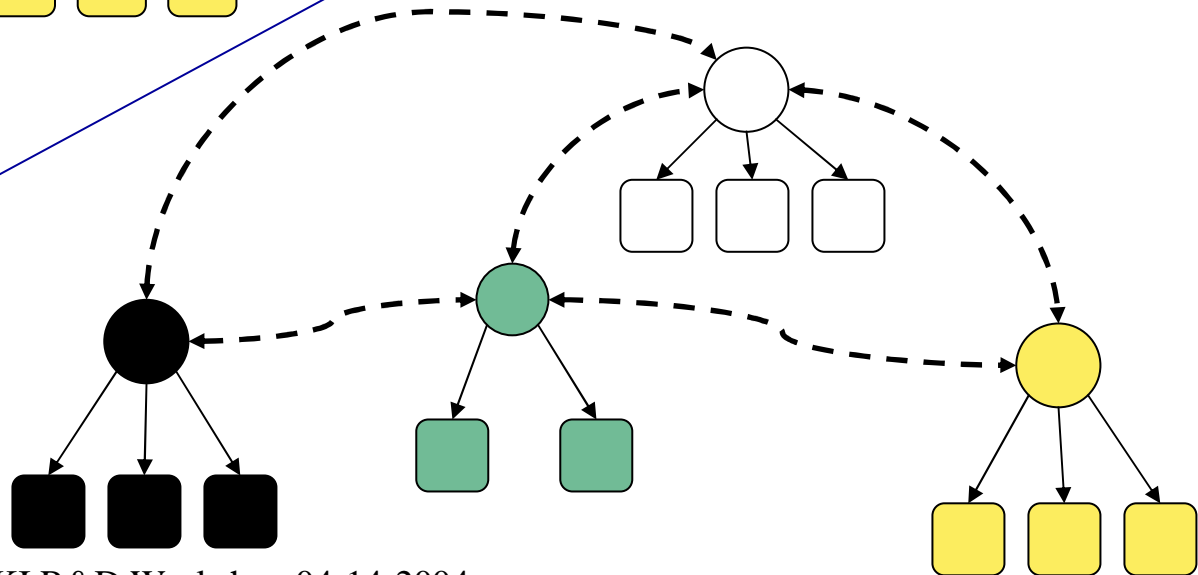
PKI Structures

- ✓ **PKIs can be grouped into conceptual structures**
 - Hierarchical
 - Mesh
 - Bi-lateral Cross-Certified (Hybrid)
 - Bridge
- ✓ **Applications have commonly been developed assuming a particular structure**
 - This limits interoperability

Basic PKI Structures

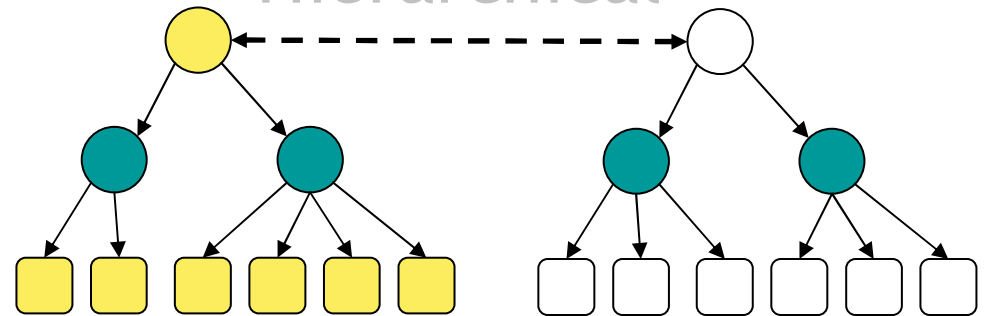


Mesh

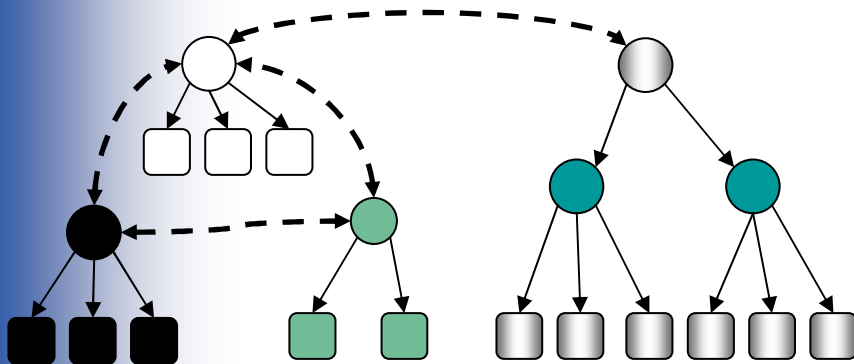


Cross-Certified PKI Structures

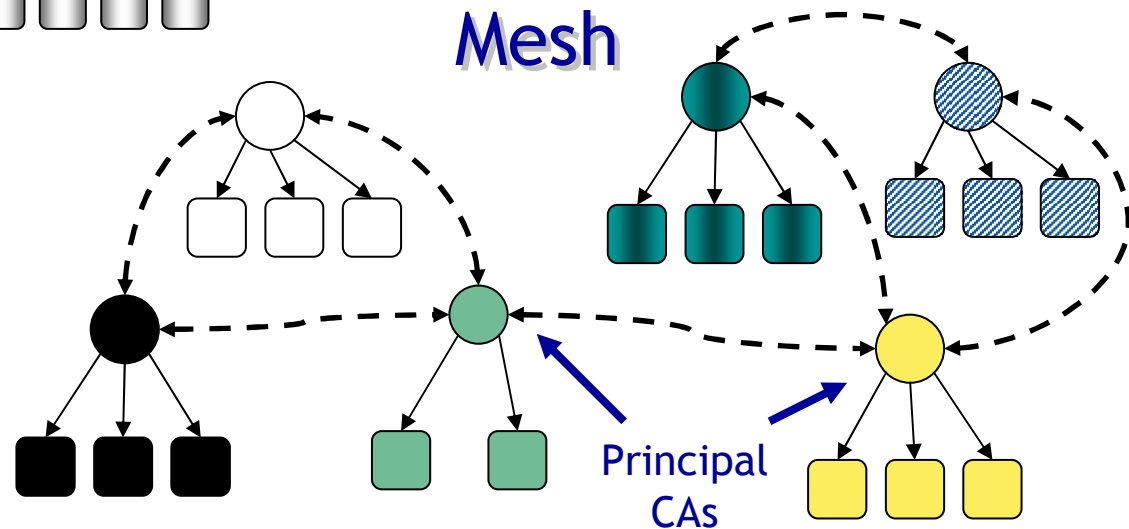
Hierarchical



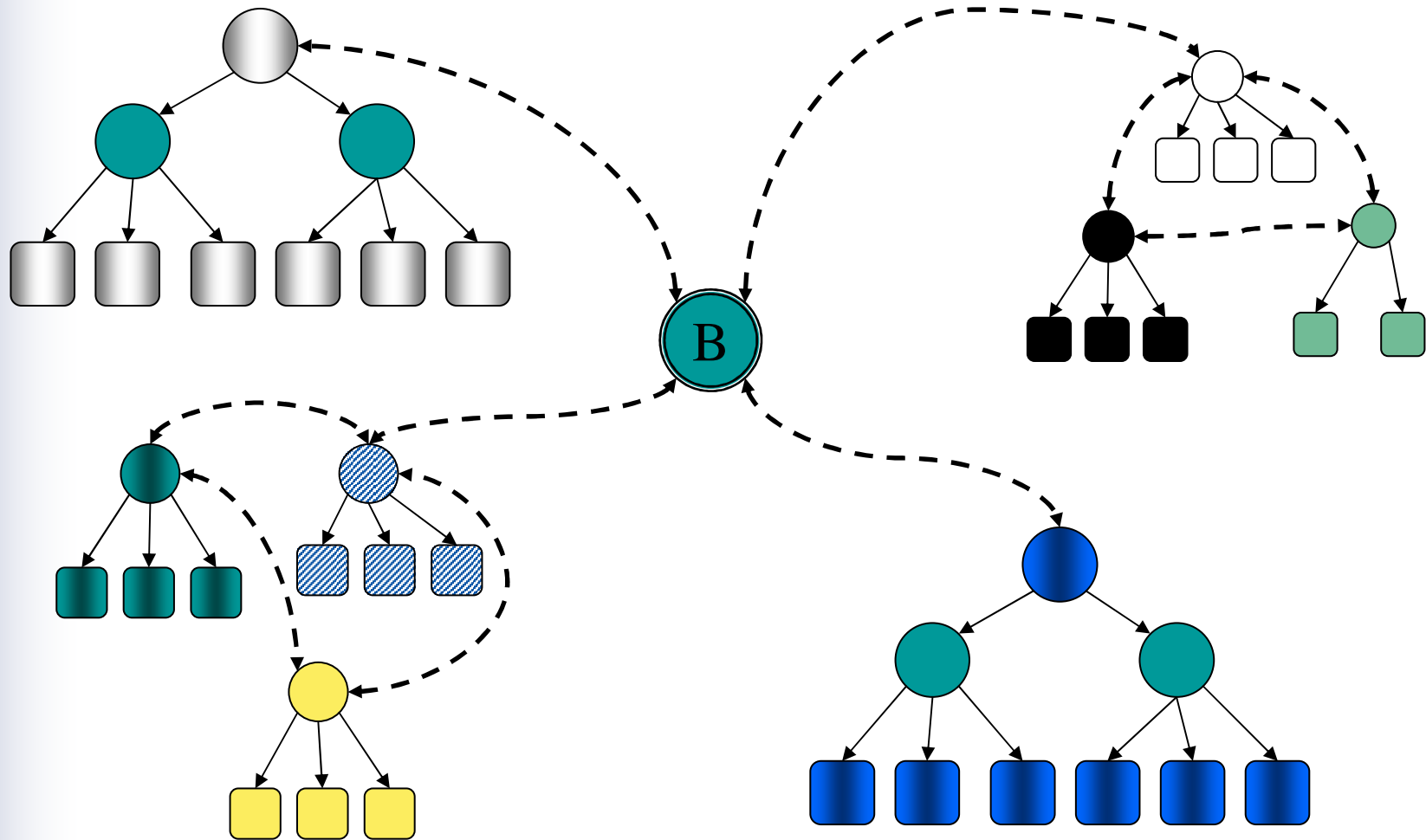
Hybrid



Mesh

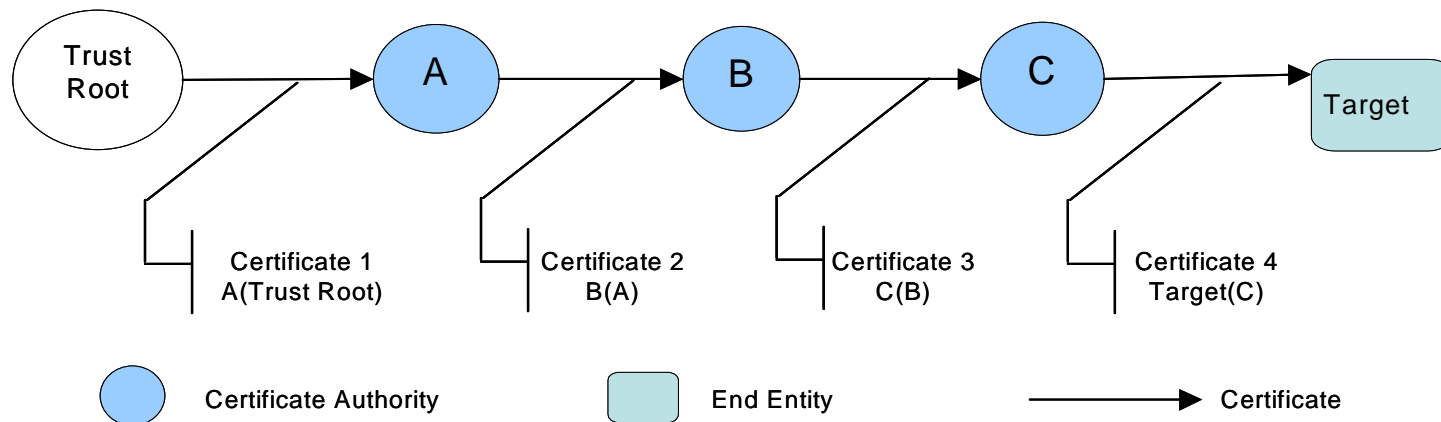


Bridge PKI Structure



Certification Path Building

- A certification path is an ordered list of certificates starting with a certificate issued by the relying party's trust root, and ending with the target certificate that needs to be validated



Certification Path Building (cont.)

- ✔ **Certification path building is not addressed by the standards that define the semantics and structure of a PKI**
 - Internet Draft in the works not as a standard but as an informational draft
- ✔ **The ability to construct or build a valid certification path is of paramount importance for applications that rely on a PKI**
- ✔ **Absent valid certification paths, you are working with PK—not PKI**

Path Building Implementations

- ✔ **Simply put, path-building is nothing more than a tree traversal**
 - certificates do not repeat in a path
- ✔ **Leads us to two basic algorithms:**
 - Start at a root, and work toward the end entity
 - Start at the end entity, and work toward a root
- ✔ **And, two models of implementation:**
 - Client-side
 - Server-side

Path Building Implementations

- ▼ Steve Hanna, Sun Microsystems
- ▼ Matt Cooper, Orion Security
- ▼ Ken Stillson, Mitretek Systems

Questions

- ✓ **First, some prepared questions for our panelists:**
 - What is your implementation's goal when discovering paths? How do you attempt to reach that goal?
 - How does your implementation handle situations involving multiple trust roots?
 - How does your implementation reduce repetition of tasks between path discovery and path validation?

Questions (2)

- What are your recommendations for PKI architects/designers based upon path discovery?
- Give us ideas of your experiences with real/test PKIs (size, complexity, time to get a result, etc)
- Is path discovery best done on the client or server?
- What are the “next steps” in the world of path discovery?

Questions

▼ From the audience...