ValiCert®

Securing e-Transactions™

Bridge Validation Authority

Ambarish Malpani
Chief Architect
ValiCert, Inc.

PKI-TWG March 14th, 2002

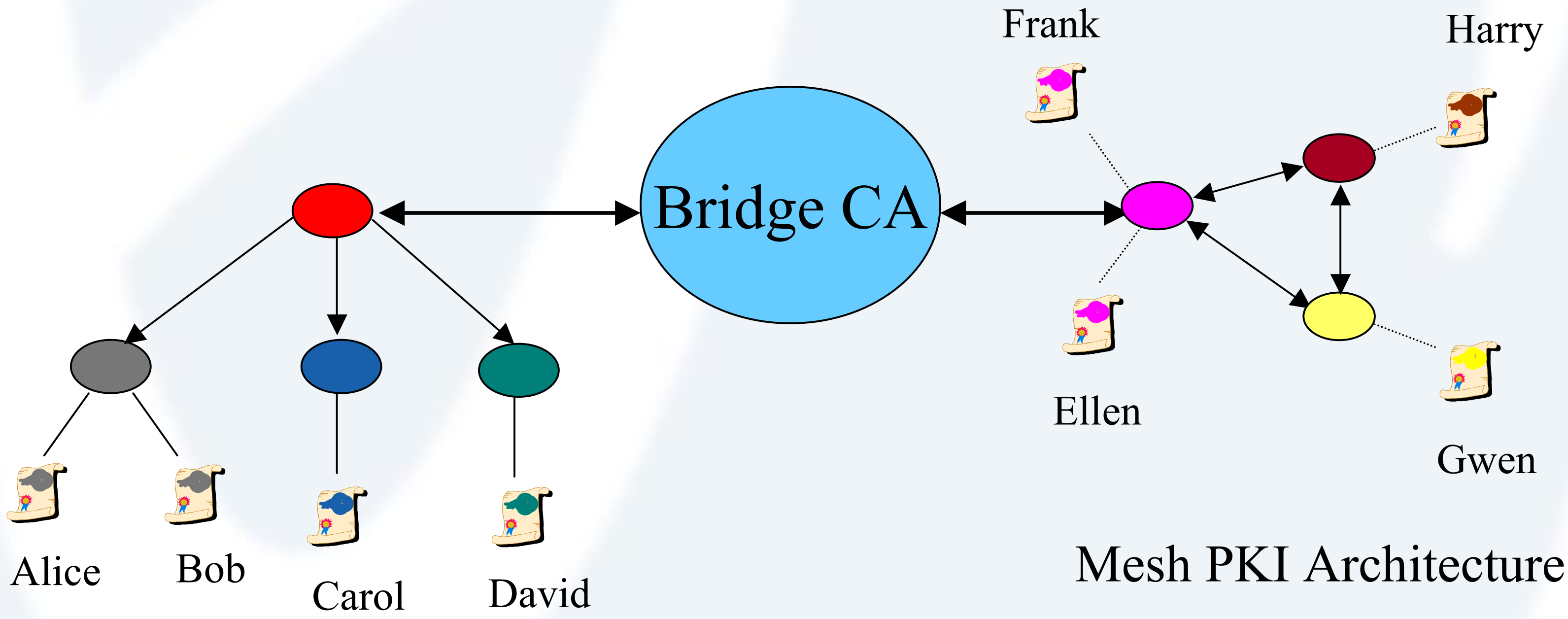
Agenda

- Role of a Bridge CA
- Problems with Bridge CA deployment
- How a Bridge VA Operates
- Properties of a Good Bridge VA
- Deployment models for a Bridge VA
  - Centralized Model
  - Distributed Model
- Benefits of the Bridge VA
- Summary & References

Role of a Bridge CA

- **Bridge multiple** existing **PKIs**
- **Reduce the number of trust relationships required between CAs**
- **Equate different PKI policies**

Bridge CAs Connect Multiple PKIs

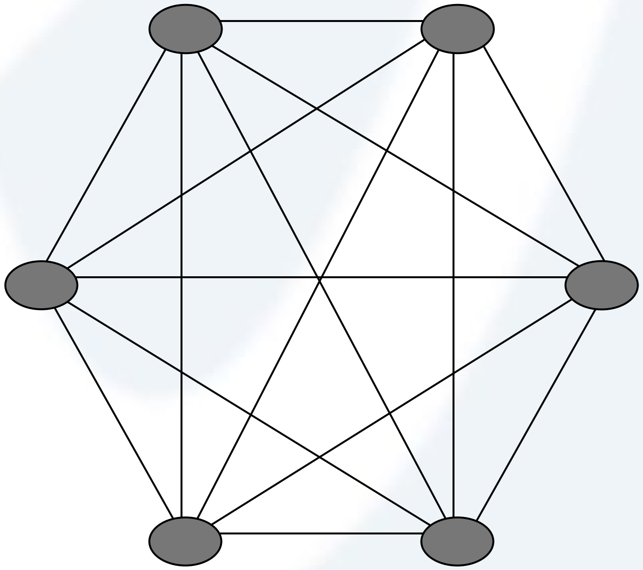


Mesh PKI Architecture

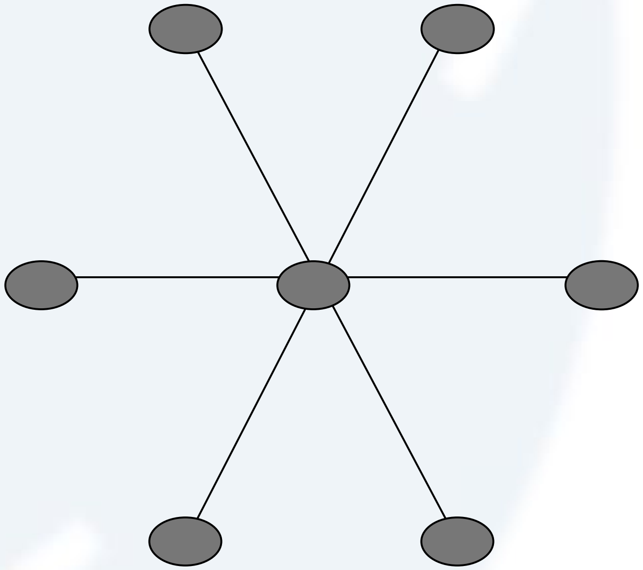
Hierarchical PKI Architecture

Bridge CAs Reduce Trust Complexity

n^2-n relationships
without a bridge CA



n relationships with a
bridge CA

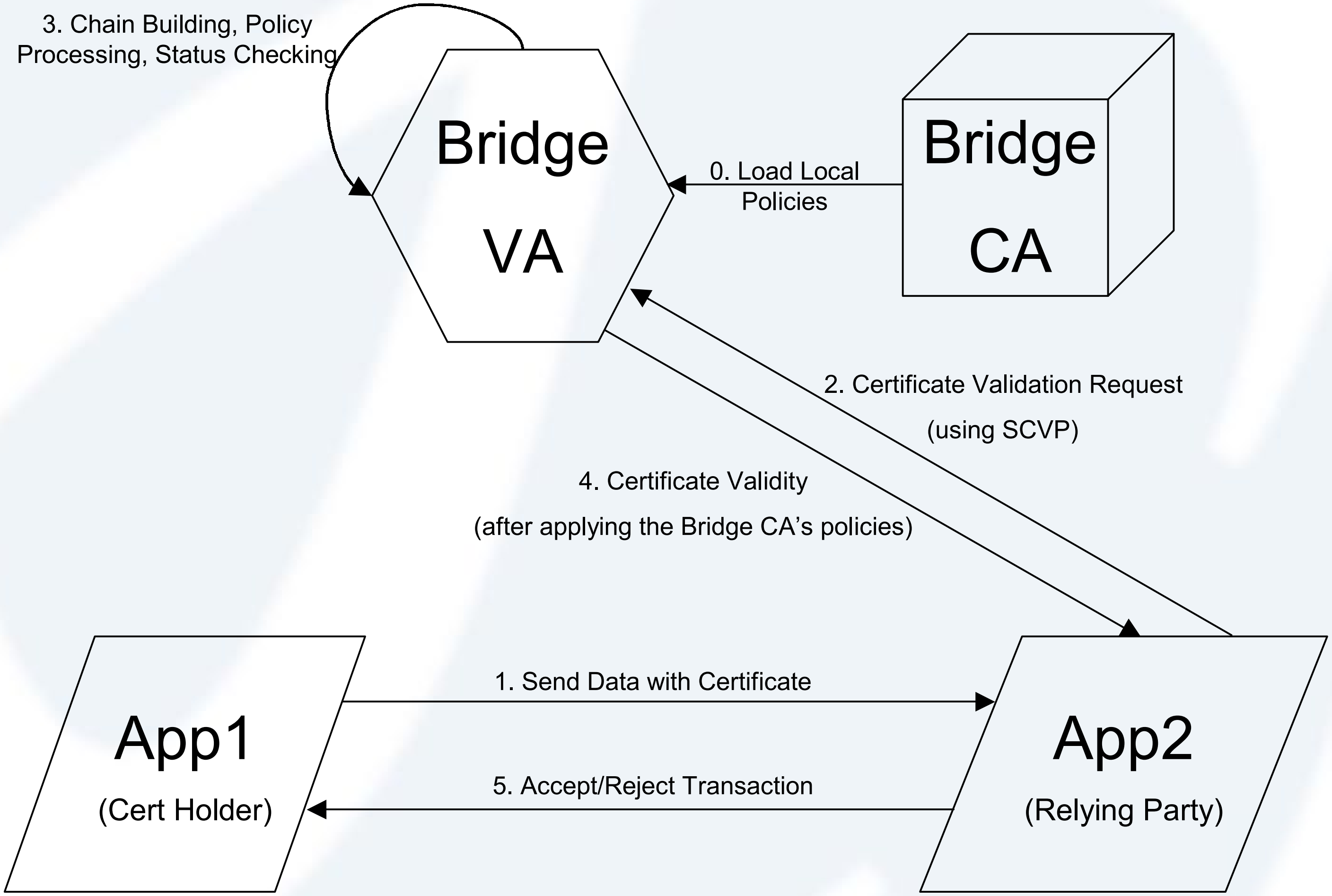


Problems with Bridge CA Deployment

- Complexity required on client applications
- Need to impose rules on CA repositories (or require clients to understand multiple CA repositories)
- Impose rules on access to repositories
- Require clients to support multiple validation mechanisms (CRLs, CRLDPs, OCSP, etc.)

ValiCert
Securing e-Transactions™

How a Bridge VA Operates


3. Chain Building, Policy Processing, Status Checking
Bridge VA
0. Load Local Policies
Bridge CA
2. Certificate Validation Request (using SCVP)
4. Certificate Validity (after applying the Bridge CA's policies)
1. Send Data with Certificate
5. Accept/Reject Transaction
App1 (Cert Holder)
App2 (Relying Party)

ValiCert
Securing e-Transactions™

Properties of a Good Bridge VA

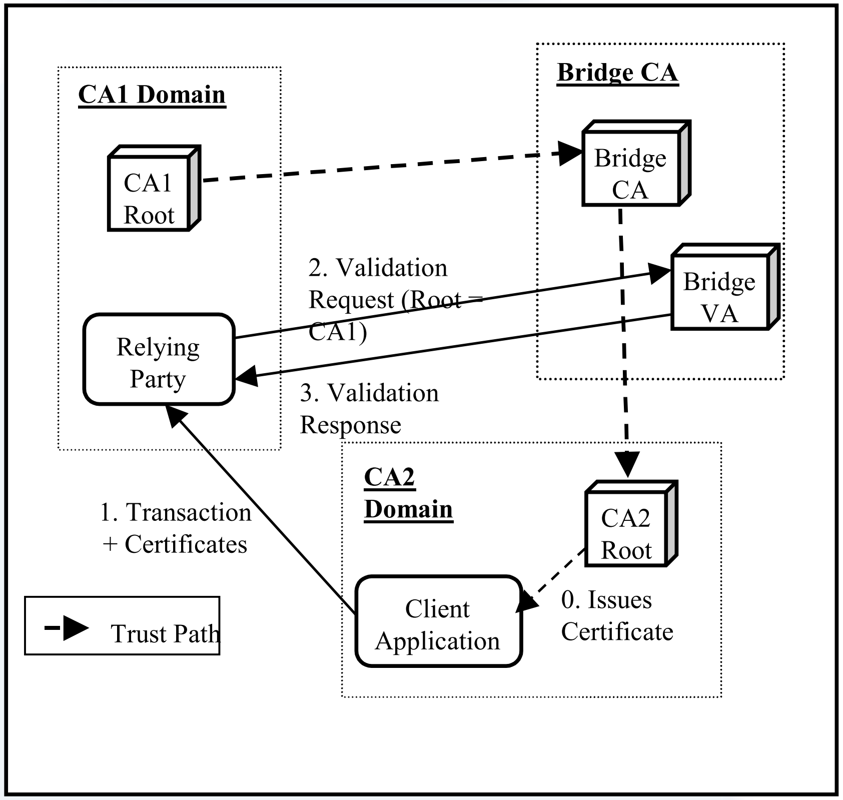
- Ability to deal with multiple CAs and Directories
- Flexible search mechanisms (when looking for certificates)
- Support for multiple Certificate Validation mechanisms
  - OCSP (simple OCSP, Identrus, GTA, etc.)
  - CRLs, CRLDPs
- Ability to enforce Bridge CA policies
- Flexibility in its ability to handle local policies
- **High Performance** with **High Security**

Deployment Models for Bridge VAs

- Single Central Bridge VA
- Distributed Bridge VAs

Centralized Bridge VA

- A single Bridge VA running next to the Bridge CA
- Implements the Bridge CAs policies
- Common service for all relying party applications



CA1 Domain

CA1 Root

Relying Party

Bridge CA

Bridge CA

Bridge VA

2. Validation Request (Root = CA1)

3. Validation Response

1. Transaction + Certificates

CA2 Domain

CA2 Root

Client Application

0. Issues Certificate

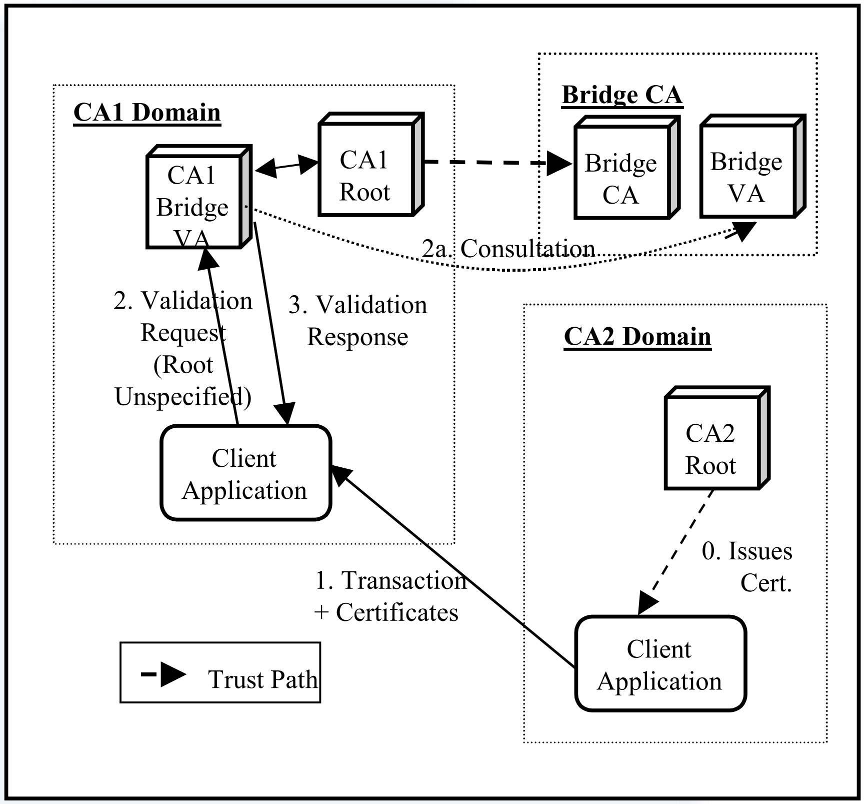
Trust Path

ValiCert®

Securing e-Transactions™

Distributed Bridge VA

- An organization can decide to run its own Bridge VA to override the rules and policies of the Bridge CA (can trust other CAs, not trust some CAs)
- Domains that follow the Bridge CA policies completely, don't need their own Bridge VA



CA1 Domain

CA1 Bridge VA

CA1 Root

Bridge CA

Bridge CA

Bridge VA

2a. Consultation

2. Validation Request (Root Unspecified)

3. Validation Response

Client Application

CA2 Domain

CA2 Root

0. Issues Cert.

1. Transaction + Certificates

Client Application

Trust Path

Benefits of a Bridge VA

- Simplifies Client Implementation
- More control over the correctness of path construction and validation logic
- Easier Interoperability across CAs
- Lowers cost of CA Deployment (can use LDAP directories instead of X.500 directories)
- Performance benefits
- Future-Proofing of Applications

Summary

- Covered the need for a Bridge CA
- Covered the basic ideas behind a Bridge VA
- Covered criteria for selecting a Bridge VA
- Covered 2 deployment models for Bridge Vas
- Covered the benefits of using a Bridge VA
- Questions?

References

- Whitepaper on the Bridge VA
  - http://www.valicert.com/html/products/bridge_VA_wp_form.html
- Details about the SCVP Protocol
  - http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-06.txt
- A Recording of a Webinar on “Universal Certificates: Enabling Interoperable PKI”
  - http://www.valicert.com/events/webseminars.html
- My e-mail address: ambarish@valicert.com

ValiCert® Securing e-Transactions™