TUMBLEWEED COMMUNICATIONS

Certification Path Processing in the Tumbleweed Validation Authority Product Line
Federal Bridge CA Meeting 10/14/2004

Stefan Kotes, Engineering Manager

Agenda

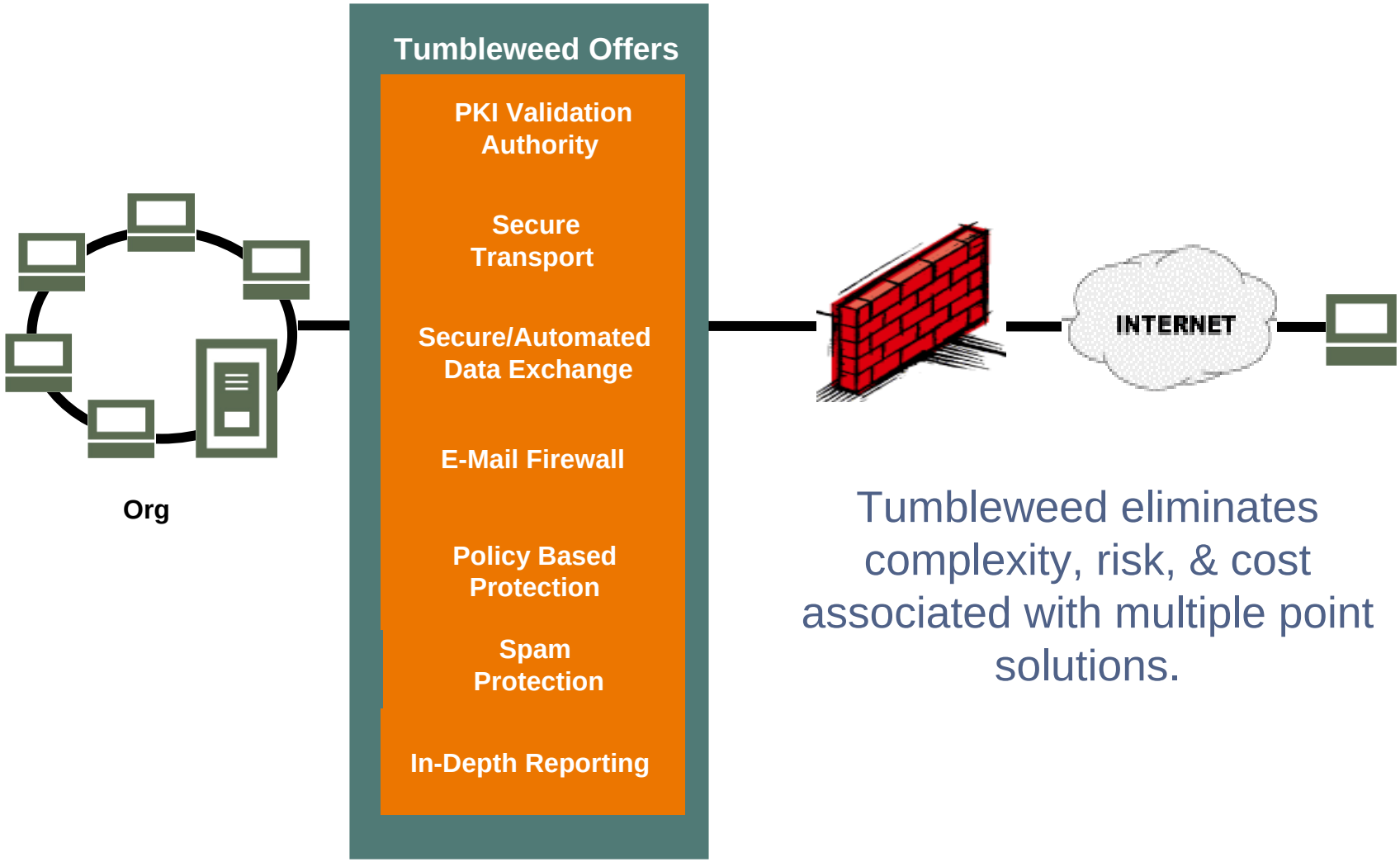
- **Tumbleweed company overview**
- **Certification path processing**
  - » Basics
  - » PKI Structures
- **Path Processing – Tumbleweed Client PKI Applications**
  - » Desktop Validator, Server Validator
- **Path Processing – Tumbleweed Validation Authority**
  - » Overview, VA Distributed Model
  - » Delegated Path Validation, Delegated Path Discovery
- **Case Study – Bridge VA**
  - » Bridge VA Properties, Central & Distributed Model, Bridge VA Benefits
- **Tumbleweed Solutions Recap**
- **Questions ?**

Company Overview

TUMBLEWEED COMMUNICATIONS

- **Founded in 1993**
- **Headquartered in Redwood City, CA**
  - » Currently over 250 employees worldwide
  - » IPO in 1999 (NASDAQ:TMWD)
  - » Tumbleweed and Valicert merged in June 2003
  - » Global Presence
  - » 700+ Commercial and Federal Customers
- **Technology innovators**
  - Identity Management Solution (Valicert Validation Authority)
  - Secure, Automated, Guaranteed Data Transfers (SecureTransport)
  - Secure Messaging & Content Filtering (MMS & SecureRedirect)

Tumbleweed Enterprise Solutions



Tumbleweed eliminates complexity, risk, & cost associated with multiple point solutions.

Certification Path Processing

TUMBLEWEED COMMUNICATIONS

Basics:

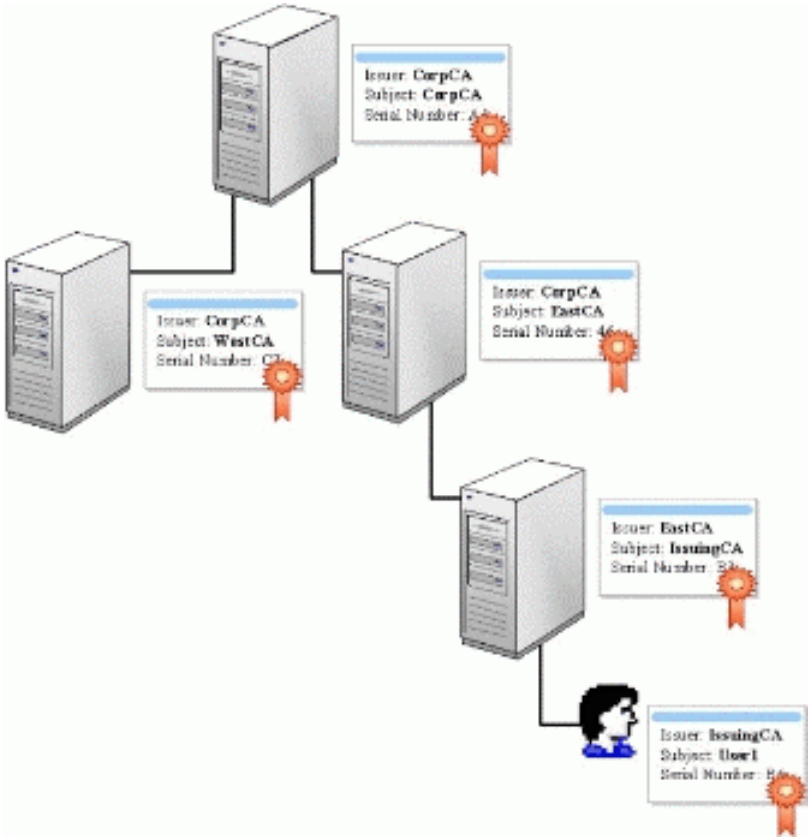
- Digital Certificates – securely binding the identity of a person/device to a public key.
- Core responsibility of an application - verify the authenticity and validity of certificate.
- Certification Path Processing Functions
  - Step 1: Creating chain of trust (establishing a certification path)
  - Step 2: Validating the created certification path

Hierarchical Structure

TUMBLEWEED COMMUNICATIONS

Hierarchical PKI:

- Relying parties trust single “root” CA
- Root CA certifies public keys of intermediate CAs
- Certificates are issued only in one direction (a CA never certifies superior CA)
- Certification path building – simple typically forward build direction is used
- Compromise of trust root may compromise entire system

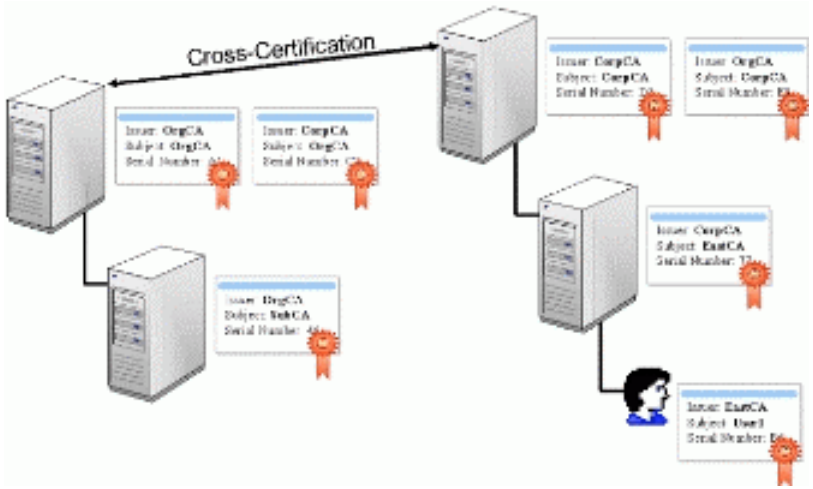


Bi-lateral Cross-Certified Structure

TUMBLEWEED COMMUNICATIONS

Cross-Certification:

- Root CA is issuing a certificate for the other PKI's root CA
- Relying parties of each PKIs can verify and accept certificates issued by other PKI
- Multiple cross-certified PKIs create mesh PKI
- Number of relationships grows exponentially with number of PKIs
- Mesh PKI - creation of unintended certification paths
- Lack of commercial adoption



Cross-Certification with a Bridge CA

TUMBLEWEED COMMUNICATIONS

Role of Bridge CA:

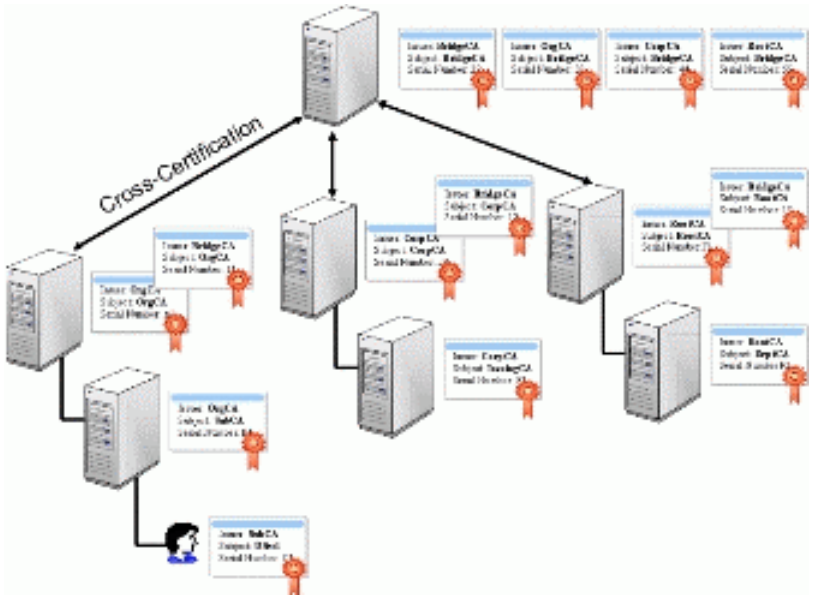
- Bridge multiple existing PKIs
- Reduce number of trust relationships between CAs
- Equate different PKI policies

How it works:

- Bridge CA cross-certifies with “principal” CA in each participating PKI.
- Each participating CA needs to cross-certify with only one other CA
- Number of certified relationships grows linearly

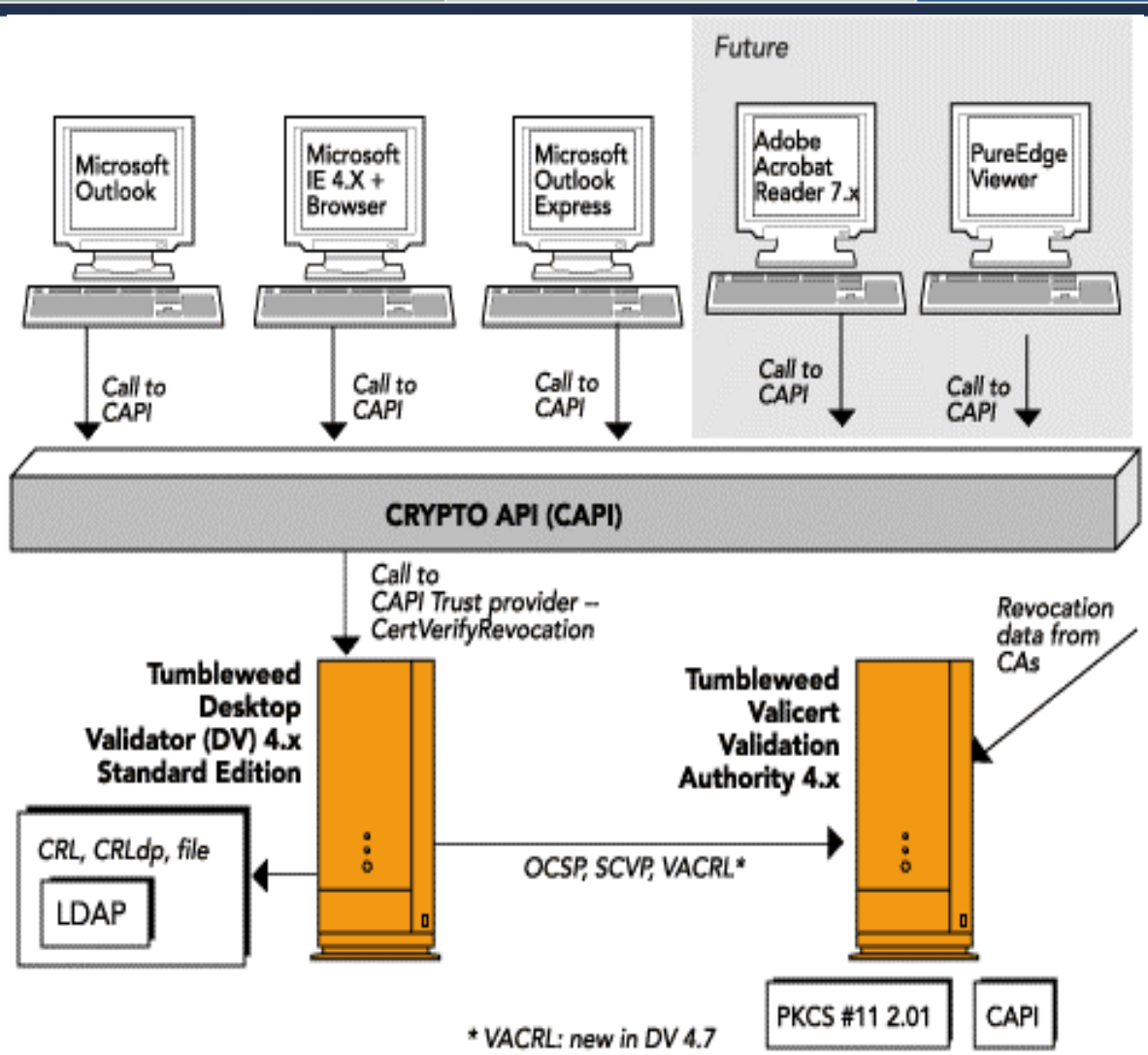
Bridge CA Deployment Issues:

- Complex certification path building
  - traversing multiple PKI directories
  - following AIA extension
  - supporting multiple validation mechanisms (CRLs, CRLdp, OCSP)
  - building paths in forward and reverse directions



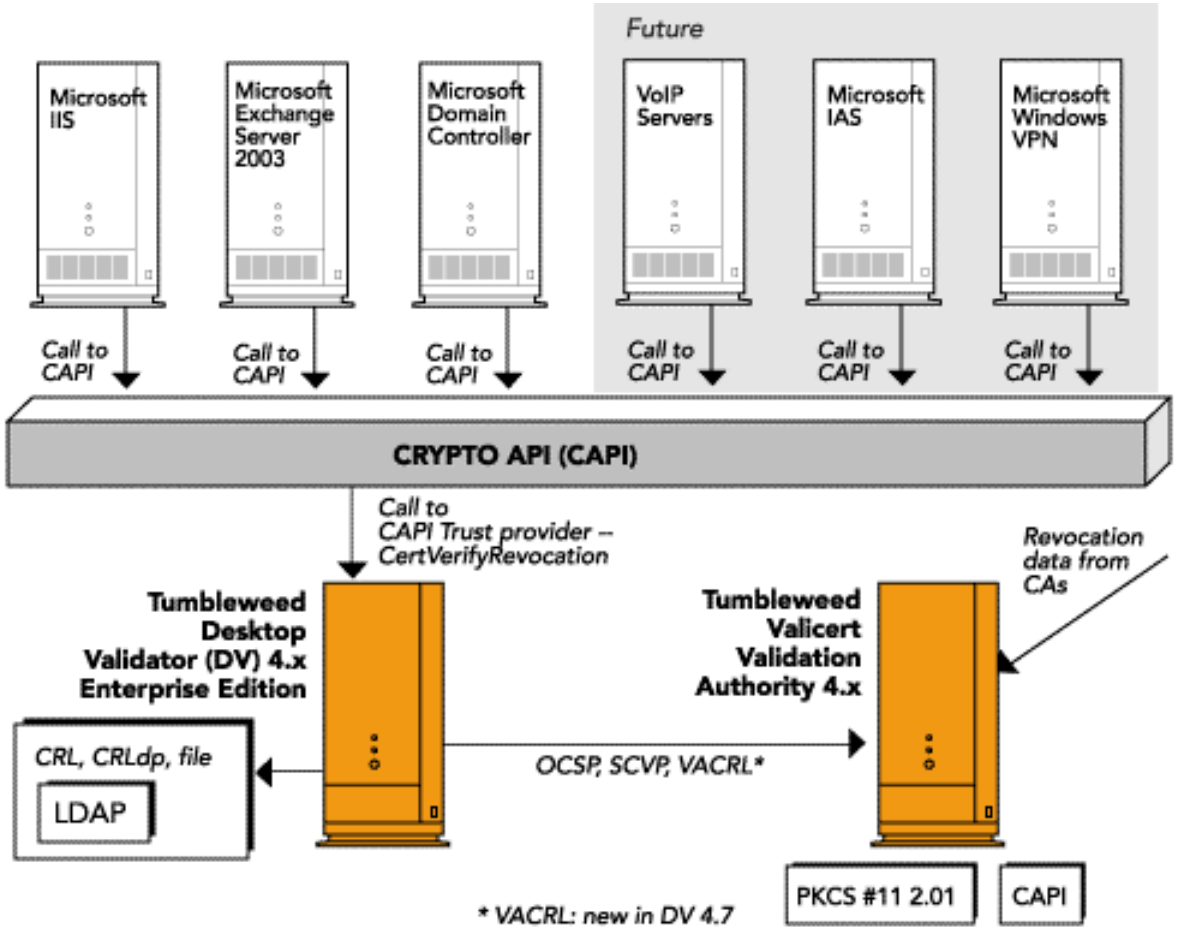
Source: NIST Recommendation for X.509 Path Validation Version 0.5 May 3, 2004 and Internet X.509 Public Key Infrastructure Certification Path Building (DRAFT RFC)

Desktop Validator Architecture



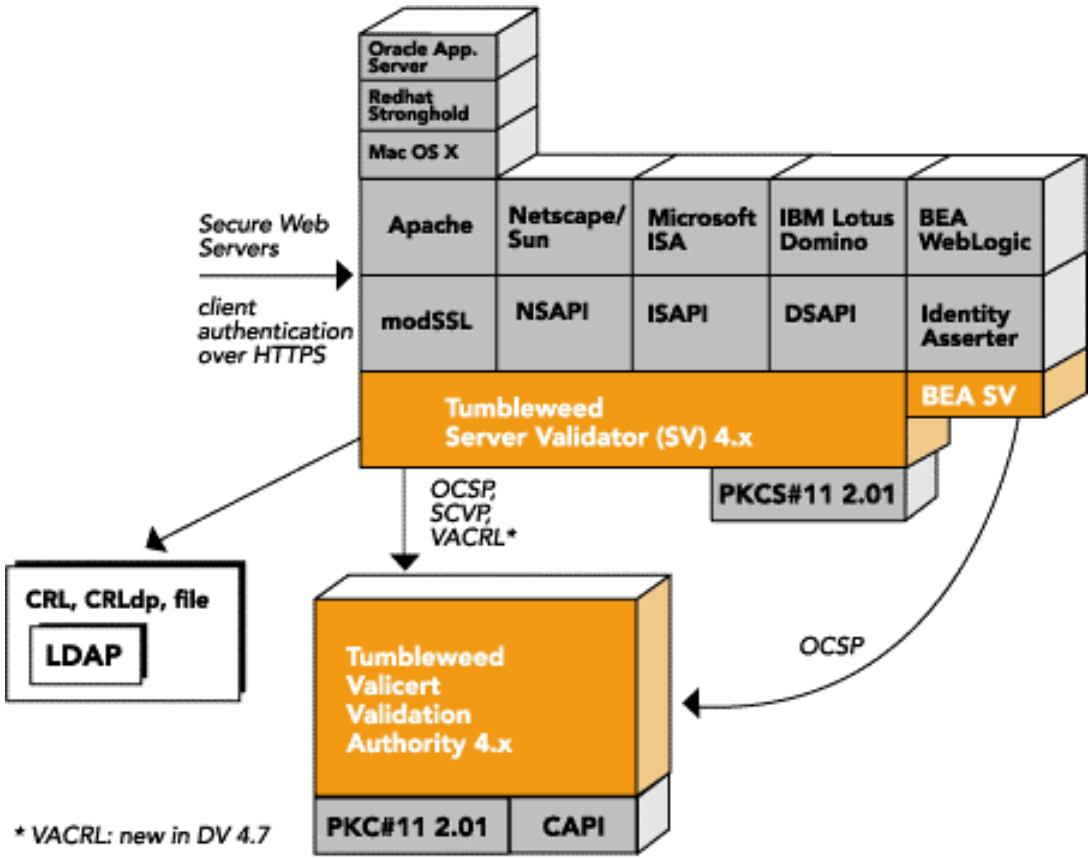
Desktop Validator (Standard) is used to enable certificate status checking for Windows client applications, such as Microsoft IE, Outlook, Outlook Express, Office (for signed word and Excel documents), and other client applications that use CAPI.

Desktop Validator Architecture



Desktop Validator (Enterprise) is used to enable certificate status checking for Windows server applications, such as IIS, Exchange 2003 (for OWA), Domain Controllers (for smart card login), IAS (for wireless authentication), and other evolving secure servers using CAPI (e.g. Voice-over-IP)

Server Validator Architecture



Server Validator (SV) is used to enable certificate status checking for secure web servers. Server Validator is invoked during the SSL/TLS handshake when a client authenticates to a web server using an X509v3 certificate. SV is responsible for ensuring that the certificates in the certificate chain are valid (not revoked)

Server Validator works with a wide range of secure servers, and runs on Windows 2000/2003 and UNIX/Linux

DV/SV Path Processing

TUMBLEWEED COMMUNICATIONS

- Path Building in MS CAPI and Web Servers
  - MS CAPI and Web Servers currently do not allow path building to be delegated to trust providers or web server APIs
  - Default path discovery must succeed before validation plugins are executed
- Path Validation in MS CAPI and Web Servers
  - Not complete
  - Default process differs among different Windows system (NT, 2000, XP, 2003)
  - No certificate policy processing in Windows 2000
- DV/SV Path Validation
  - Follows RFC 3280
  - Provides the same functionality across al supported platforms
  - Can refine and enforce stricter validation rules
  - Based on C/C++ and Java Valicert Validator Toolkit

DV/SV Path Validation Steps

TUMBLEWEED COMMUNICATIONS

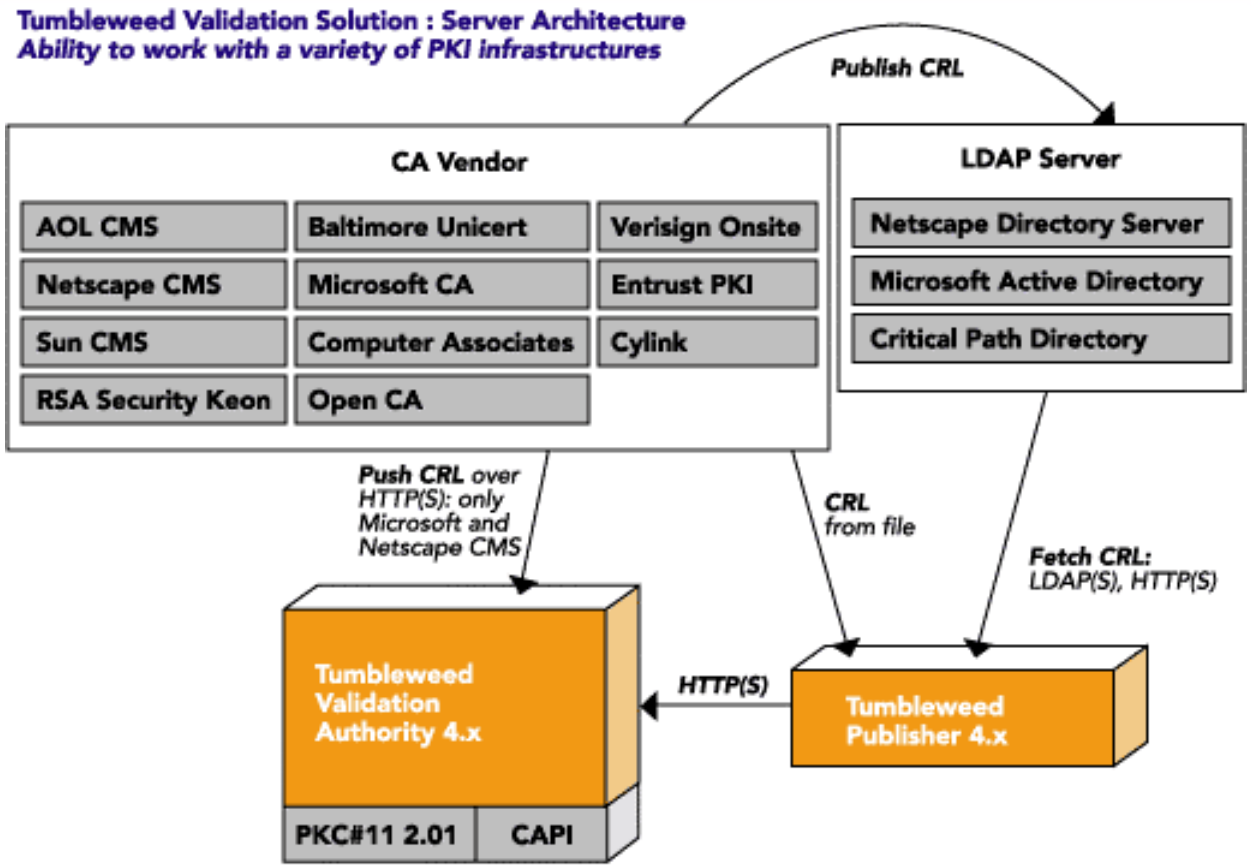
- Completeness of mandatory Certificate Information
- Certificate Time Validity
- Name Chaining (Subject Name, Issuer Name)
- Key Identifier Chaining (Authority Key Identifier, Subject Key Identifier (SKID))
- Certificate Integrity Check (valid signature)
- Critical Extensions Check
- Basic Constraints Validation
  - Is certificate a CA or end-entity
  - Certificate Chain Length (path length = 0 allows only end entity certificates)
- Name Constraints Validation
- Certificate Policy Validation (policy oid assertions)

Path Processing Standards

TUMBLEWEED COMMUNICATIONS

- Desktop Validator and Server Validator have been tested by DoD Joint Interoperability Test Command (JITC) using the NIST test suite.
- http://jitc.fhu.disa.mil/pki/ - For DOD JITC site
- http://www.tumbleweed.com/products/validationauthority/compliance.html -- includes DoD JITC issued certificates of compliance
- Testing of DV/SV in 2003 utilized the 'Conformance Testing of Relying Party Client Certificate Path Processing Logic 1.07 documents, which is the basis for the JITC application testing suite.
- Public Key Interoperability Test Suite (PKITS) Certification Path Validation Version 1.0 9/2/04 will be the basis of our future testing efforts for DV/SV.
- See http://csrc.nist.gov/pki/testing/PKITS.pdf for latest PKITS

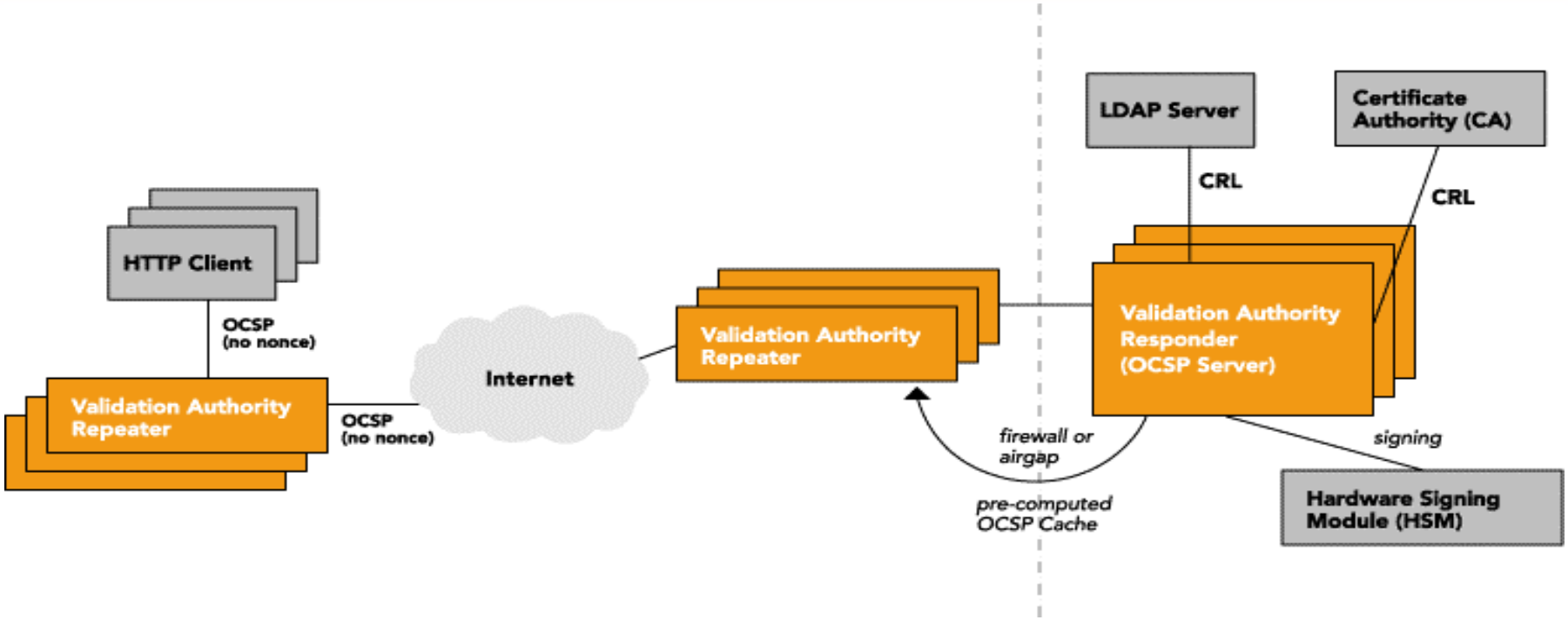
VA Server Architecture



- VA aggregates revocation data (CRLs) from multiple certification authorities (CA).
- VA-to-VA mirroring allows for efficient revocation data transfer between VA's (especially useful for low bandwidth environments)
- VA can integrate with a variety of hardware signing module (HSM) vendors for secure signing of the OCSP response
- VA supports direct, VA delegated, and CA delegated trust models

For VA white papers, see http://www.tumbleweed.com/products/validationauthority.html

VA Repeater Architecture “Distributed”



- HTTP proxy caching is described in RFC 2616 (and the earlier RFC 1945)
- Online Certificate Status Protocol (OCSP) (RFC 2560) is used to check status of a certificate issued by a CA without requiring a client to obtain the CRL issued by that CA. OCSP uses HTTP as its transport protocol.
- By excluding the nonce from OCSP requests, OCSP queries over HTTP are cacheable.
- A Responder can pre-produce signed OCSP responses (section 2.5 of RFC 2560)
- A Repeater can accept pre-produced OCSP responses published by a Responder.
- A Repeater can forward OCSP queries to a Responder on-demand or a repeater can mirror pre-computed OCSP caches periodically from the responder.

TUMBLEWEED COMMUNICATIONS

Path Processing in Validation Authority

- All previous examples show "fat" PKI client application
- What about "thin" clients like phones, PDAs working in constrained execution environments ?
- Solution is the Simple Certificate Validation Protocol (SCVP) which offers server assisted path discovery and validation. Clients have two options:
  - Delegated Path Validation (DPV)
    - DOD's DMS using SCVP
    - CAM (http://cam.mitretek.org/cam/) use of SCVP
  - Delegated Path Discovery (DPD)

Delegated Path Processing

TUMBLEWEED COMMUNICATIONS

Delegated Path Discovery (DPD):

- Getting certificate chain and revocation information (CRLs, OCSP responses) in single request
- Client performs path validation
- Authenticated DPD response is optional

Certificate Sources for Delegated Path Discovery:

- Local certificate stores (files, CAPI stores)
- LDAPv3 Directory
- Authority Information Access extension
- Validation Authority Server

Delegated Path Processing

TUMBLEWEED COMMUNICATIONS

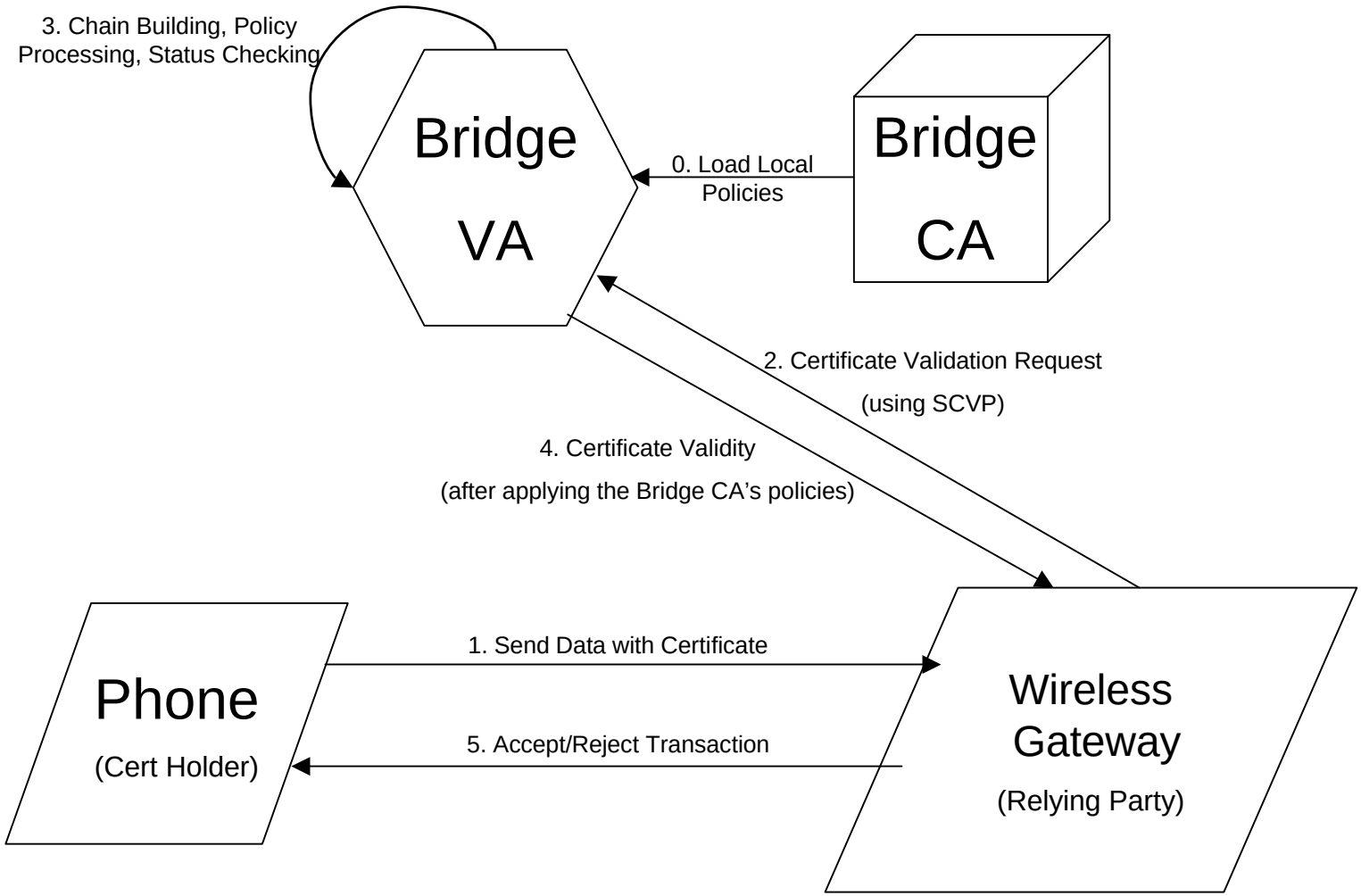
Delegated Path Validation:

- Verifies is requested certificate is valid according to specified validation policy
- DPV response must be authenticated

Revocation Info Sources for Delegated Path Validation:

- CRLs from Certification Authorities
- OCSP responses from Tumbleweed Validation Authority, or other OCSP responder
  - Real-Time or Pre-Computed

Bridge VA


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)
Phone
(Cert Holder)
1. Send Data with Certificate
5. Accept/Reject Transaction
Wireless Gateway
(Relying Party)

Properties of Good Bridge VA

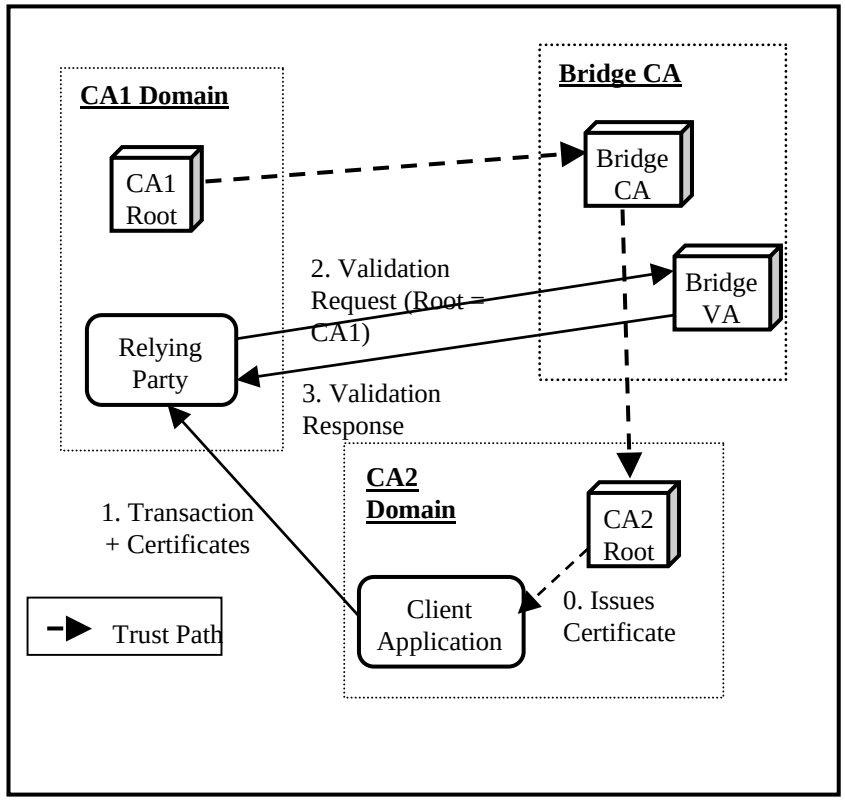
TUMBLEWEED COMMUNICATIONS

Bridge VA Requirements

- Ability to deal with multiple CAs and Directories
- Flexible search mechanisms (when looking for certificates)
- Support for multiple certificate validation mechanisms:
  - OCSP (Real-Time, Pre-Computed, Identrus model, …)
  - CRL, CRLdp
- Ability to enforce Bridge CA Policies
- Flexibility in its ability to handle local policies
- High performance with high security

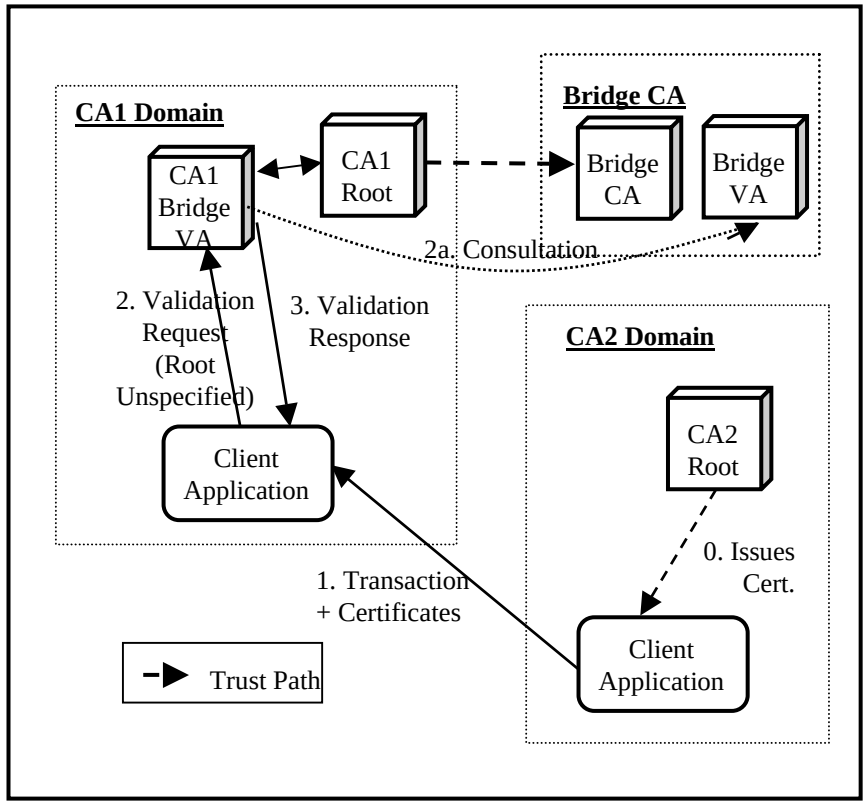
Deployment Model: Central Bridge VA

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



Deployment Model: Distributed Bridge VA

- An organization can decide to run its own Bridge VA to overwrite the rules and policies of the Bridge CA
- Local Bridge VA can trust other CAs, not trust some central ones
- Domains that follow Bridge CA policies completely do not need their own Bridge VA



Benefits of a Bridge VA

TUMBLEWEED COMMUNICATIONS

- Simplifies client application path processing
- Gives more control over path discovery and path validation through centralized policy enforcement
- Easier interoperability across CAs
- Performance benefits for client applications
- Future-proofing of applications

Tumbleweed Validation Solution Recap

TUMBLEWEED COMMUNICATIONS

- Our Validation Authority solution offers a variety of validation protocols (OCSP, SCVP, CRL, CRL DP, CMP, etc.) to choose from, allowing maximum flexibility in customer deployments
- Open standards based (IETF RFC 2560, 3280, NIST FIPS 140-1)
- Desktop Validator and Server Validator available for multiple platforms and applications
- Validator Toolkit available for Win32, Solaris, HP-UX, AIX, MacOS, Linux
- DOD JITC Tested & FIPS 140-1 Certified
- NIAP Common Criteria (EAL3) underway

Resources

- **Contact information:**
  - Stefan Kotes
  - Validation Authority, Client Applications - Engineering Manager
  - 650-216-2082
  - stefan.kotes@tumbleweed.com
- **Product Information and White Papers**
  - http://www.tumbleweed.com/products/validationauthority.html – Main Product web page
  - http://www.tumbleweed.com/products/validationauthority/compliance.html - Security Compliance Information