Certificate Validation across the Federal PKI using Server-based Certificate Validation Protocol

Dr. Sarbari Gupta

sarbari@electrosoft-inc.com

FPKI Certificate Policy Working Group Meeting

February 4, 2016

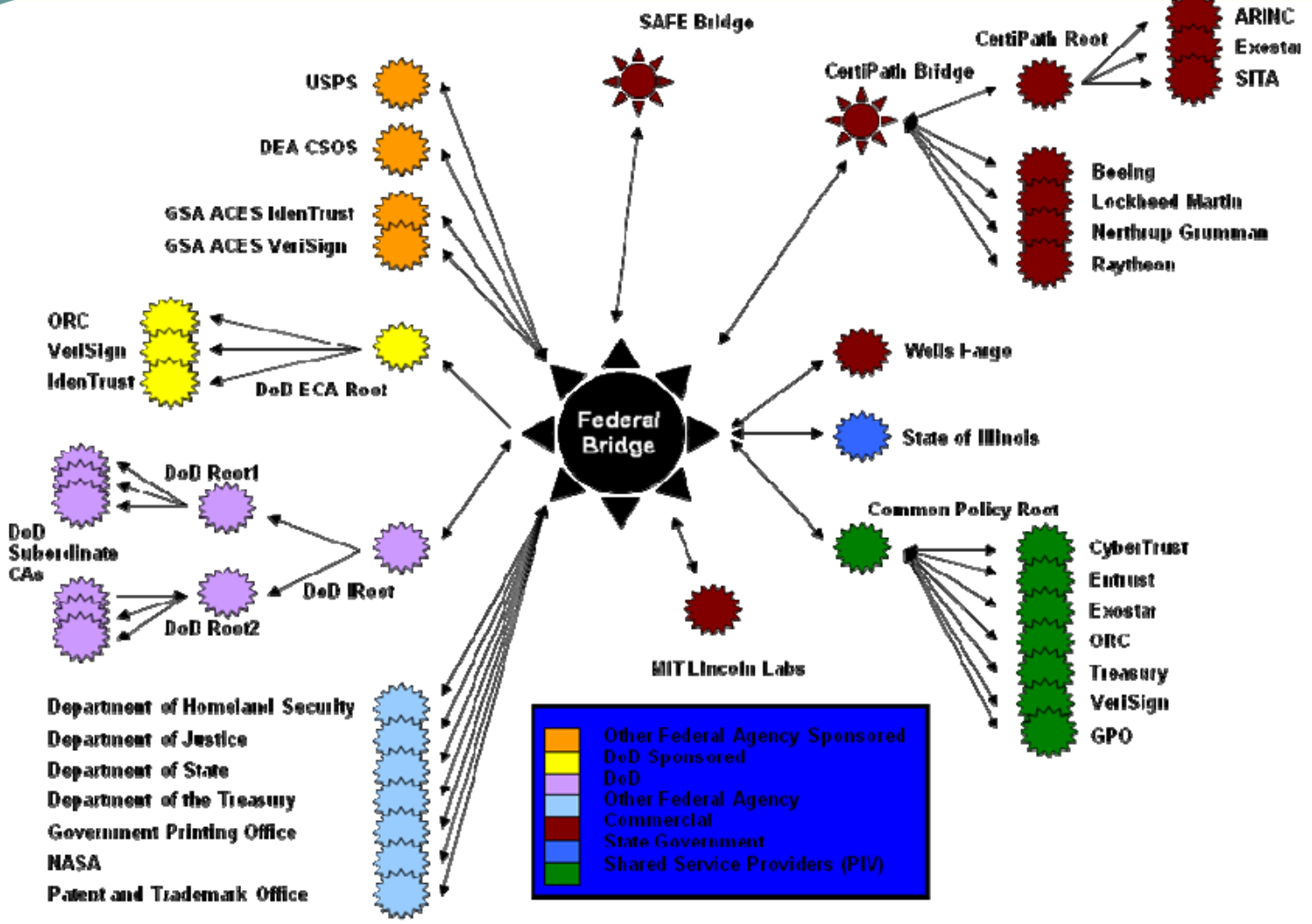
Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Agenda

- Federal PKI Landscape
- SCVP Overview
- Case Study
- PKI Validation Use Cases
- Summary

Federal PKI Landscape



From: dod_pki_interagency_partner_interoperability_test_plan_v_1_0_3_aug_27_2008.pdf

Federal PKI Landscape - Complexity

- **Path construction and validation across the FBCA is difficult**
- **Distributed revocation checking using CRLs and OCSP is very cumbersome**
- **Complex validation and trust requirements (e.g., trust roots, policy checking)**

Challenges in Distributed PKI Validation

- **Impractical to Manage Distributed PKI Validation**
  - ***Configuration of Trust Roots/Intermediate Certificates in RP***
  - ***Complex Validation Policies in RP***
  - ***Heavy network load to download CRLs***
  - ***Complex PKI validation software at every RP***

What is SCVP

- **Server-based Certificate Validation Protocol**
  - ***IETF Standard - RFC 5055***
  - ***Finalized in Dec 2007***

- **Protocol that allows a client to delegate certification path *construction* and *validation* to a server**
  - ***Builds and validates certificate path to Trust Anchor***
    - **Using the AIA extension for path construction**
    - **Applies validation policy parameters**
  - ***Performs revocation checking of all certificates in path***

- **Comprised of client requests and server responses**
  - ***Request***
    - **End-Entity Certificate; [Trust Anchors]; [Policy Parameters]**
    - **MAY be signed**
  - ***Response***
    - **Valid/Not Valid [Error Code]**
    - **MUST be signed**

Advantages of using SCVP

- **Simplifies Relying Party (RP) device/system**
  - ***Complex path validation software not needed***
  - ***Complex client configurations not needed***
- **Centralizes management of:**
  - ***PKI path validation policies***
  - ***PKI trust root(s)***
- **Higher Performance**
  - ***Pre-fetching and caching of Intermediate Certificates***
  - ***Pre-fetching and caching of CRLs, OCSP Responses***
- **Lower load on network bandwidth**
  - ***CRLs not downloaded to every RP***
  - ***Requests and Responses are ~3KB each***
- **Versatile**
  - ***Can be used for both PACS and LACS***

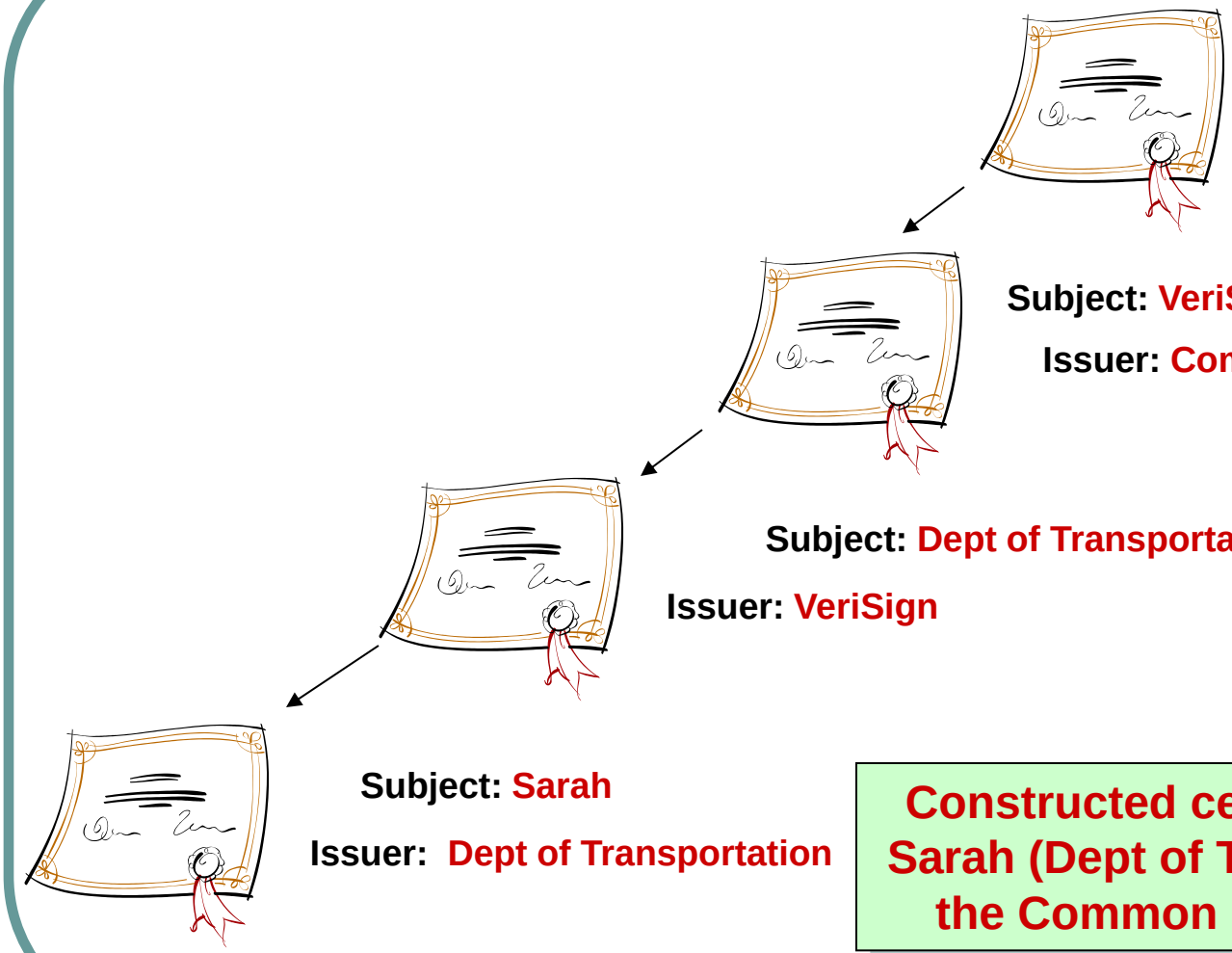
SCVP Case Study

- **GSA Central Certificate Validator (CCV)**
  - *Component of FIPS 201 Evaluation Program*
  - *Operational between 2009 – 2011*
- **Goal**
  - *Implement PKI Validation mechanism compliant with NIST FIPS 201*
  - *Promote evaluation of products that implement PIV Authentication use cases*
  - *Allow agencies to test the validation of PIV certificates*
- **Implementation Details**
  - *Online SCVP Server (Axway VA)*
  - *Standalone SCVP Test Client*
  - *Customized SCVP request and response profiles*
  - *Preset trust anchors and policy settings*

GSA CCV Implementation

- **Scope**
  - ***Validation of PIV Authentication certificates***
- **Default CCV validation policy**
  - ***Trust Anchor* – *Common Policy Root CA***
  - ***Certificate Policy* – *id-fpki-common-authentication***
  - ***initial-explicit-policy* = *true***
  - ***initial-policy-mapping-inhibit* = *false***
- **Has flexibility to override the trust anchors and validation policy parameters**

Certificate path for SSPs



Subject: Common Policy

Issuer: Common Policy

Subject: VeriSign SSP

Issuer: Common Policy CA

Subject: Dept of Transportation

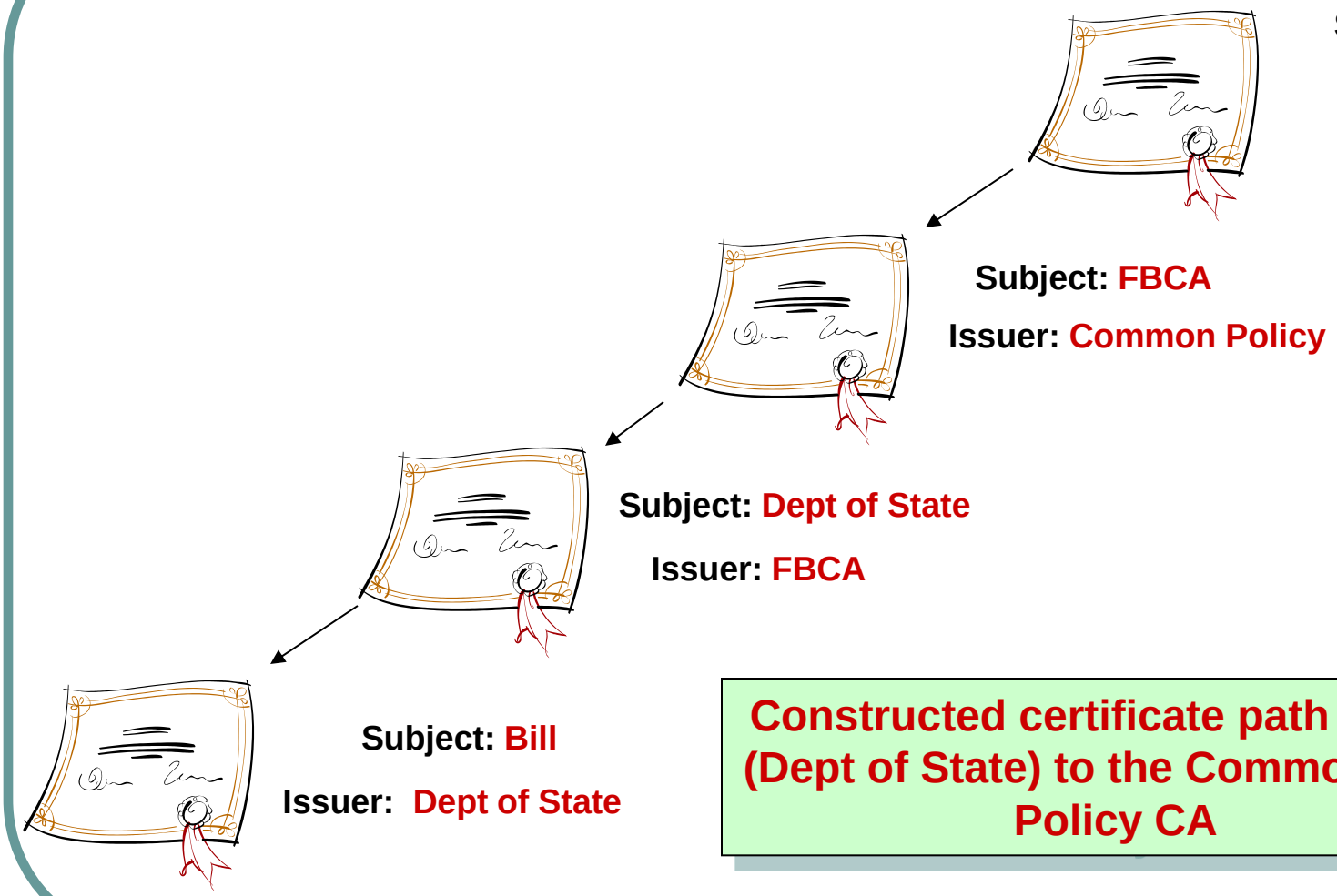
Issuer: VeriSign

Subject: Sarah

Issuer: Dept of Transportation

Constructed certificate path for Sarah (Dept of Transportation) to the Common Policy Root CA

Certificate Path for Legacy PKI



Constructed certificate path for Bill (Dept of State) to the Common Root Policy CA

PKI Validation Use Cases

- **Typical Use Cases**
  - ***Network Logon***
  - ***Secure Email***
  - ***Client Authenticated Secure Web Access (SSL)***
  - ***VPN***
  - ***Single Sign On***
  - ***PKI based Authentication for PACS***

- **There may be Hundreds/Thousands of Relying Parties within a single Federal Organization**

Wrap-Up

- **OMB M-11-11 requires that:**
  - ***"Agency processes must accept and electronically verify PIV credentials issued by other federal agencies"***
- **Cross-Agency PKI Validation is very complex, cumbersome and costly**
  - ***Distributed PKI Validation may also pose a security risk***
- **Agencies are looking for secure, cost-effective mechanisms for validating external PKI credentials**
- **SCVP is a top choice for implementing a Government-wide PKI Validation Shared Service**