



# Technical Approach

*Chris Loudon  
Enspier*



**“Getting to Green with E-Authentication”**

February 3, 2004

**Technical Session**

# *Technical Approach*

## ◆ Lower Assurance Approach

- Overview
- Management
- SAML as an adopted Scheme

## ◆ Higher Assurance Approach

- Overview
- Certificate Validation
- Relationship to Bridge Architecture

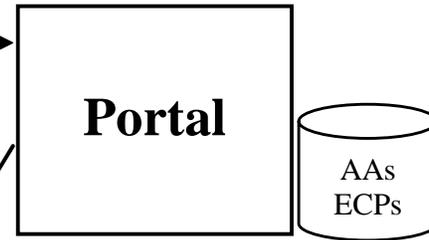
## ◆ Where we are today

- Today
- Near Term

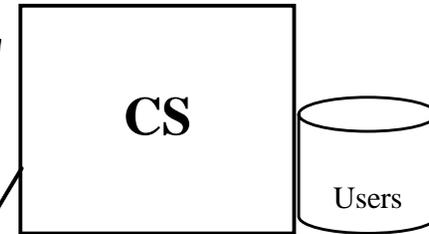
# Base Case



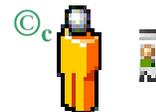
Step #1: User goes to Portal to select the AA and CS



Step #2: The user is redirected to the selected CS with an AA identifier. The portal also cookies the user with their selected CS.

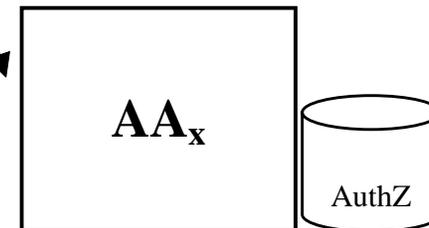


Step #3: The CS authenticates the user and hands them off to the selected AA with their identity information. The CS also cookies the user as Authenticated.

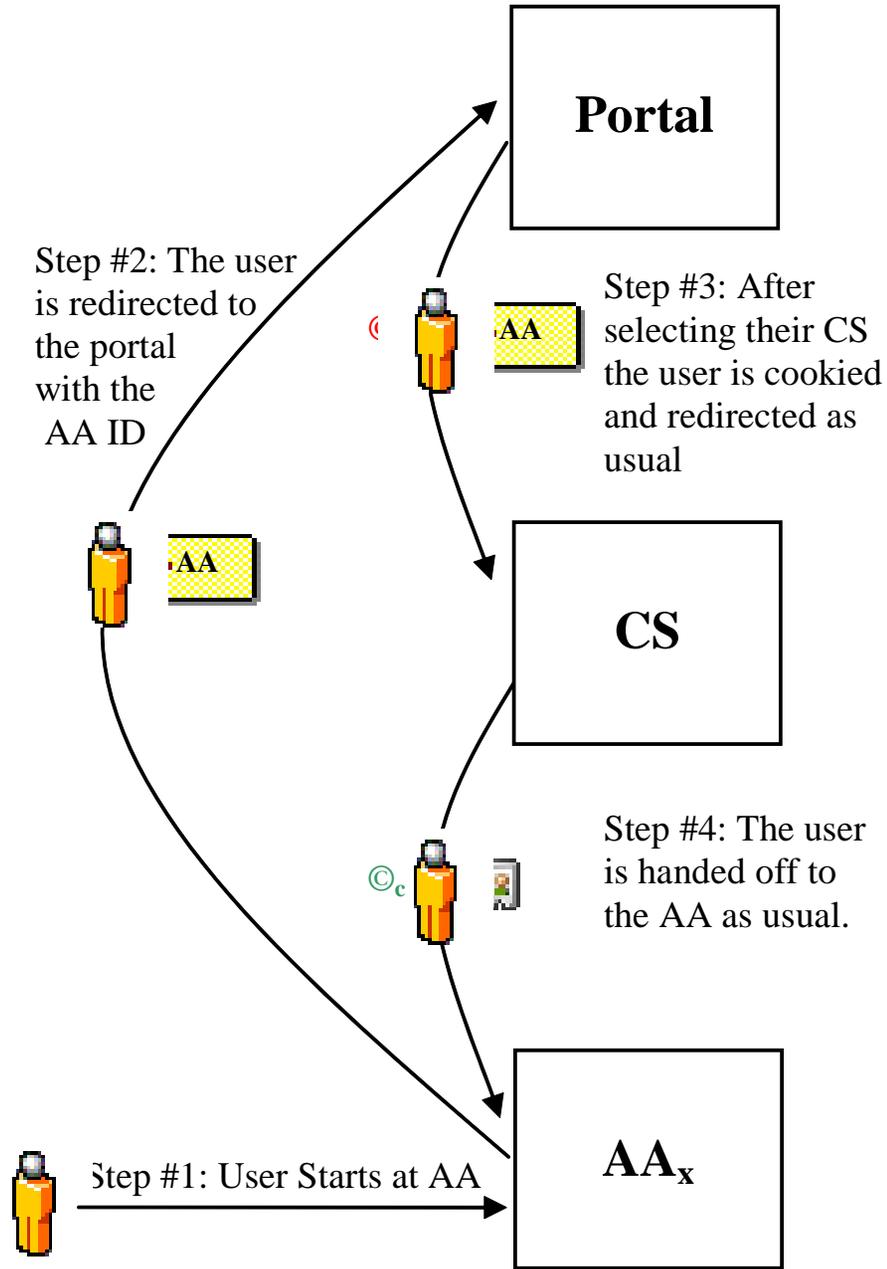


MD SSO Options:

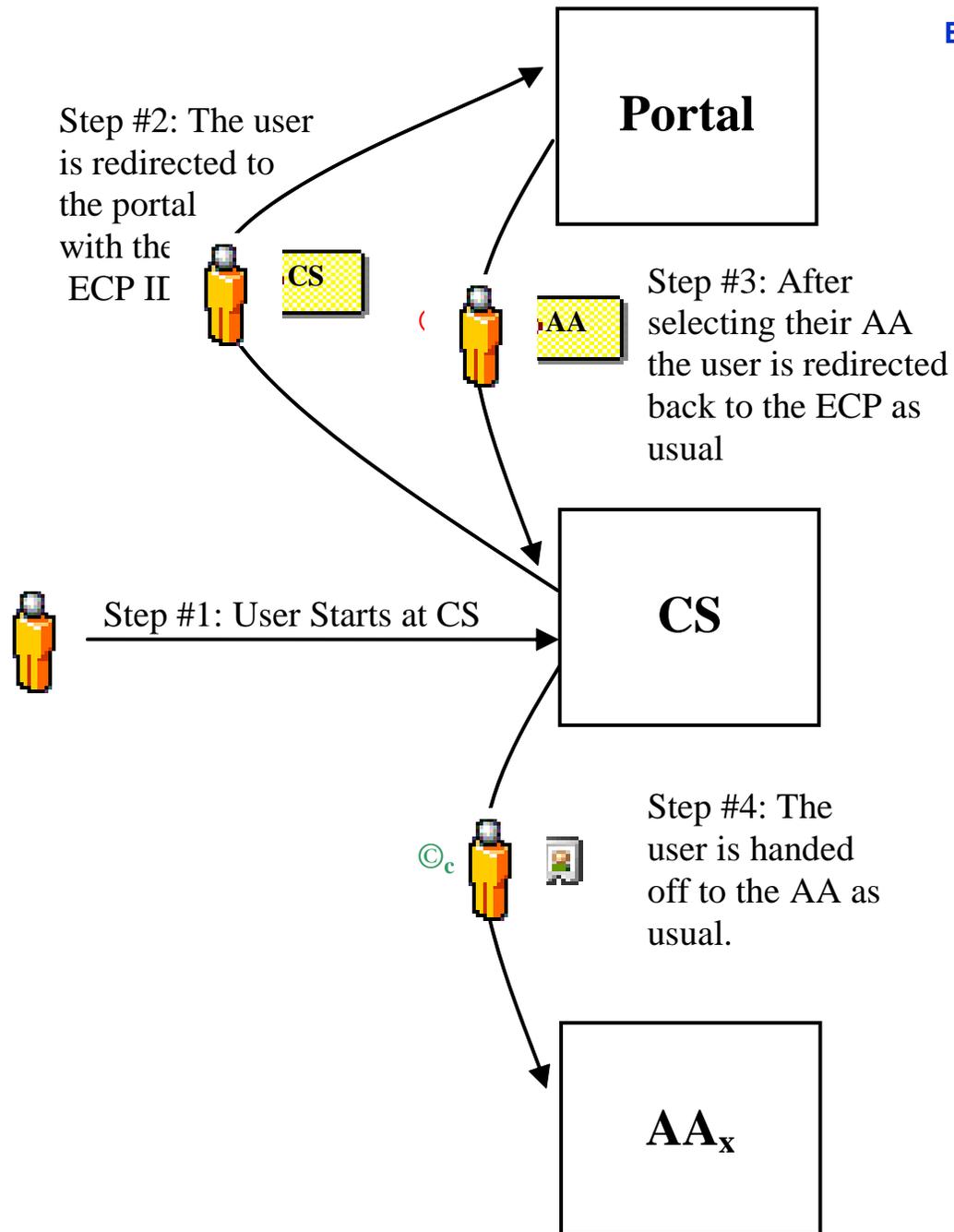
- SAML
- Liberty
- WS-Federation
- Shibboleth
- ?



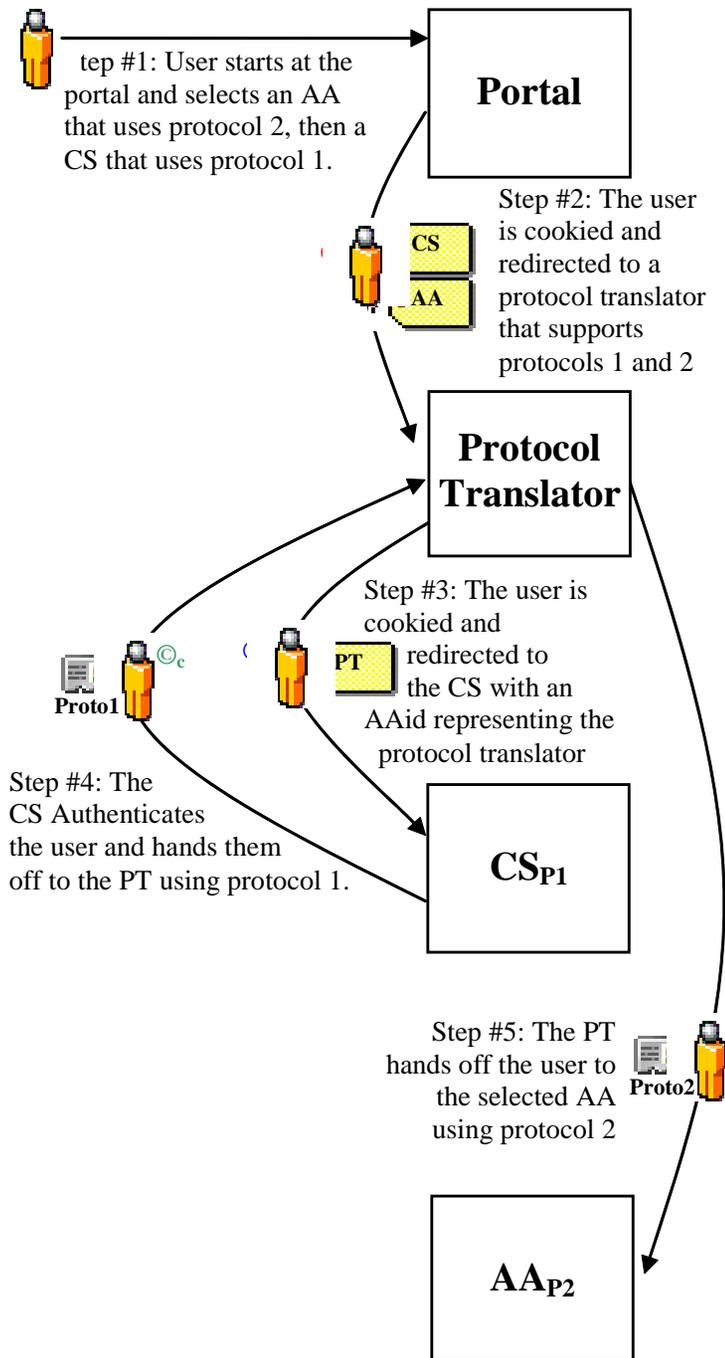
# Starting at the AA



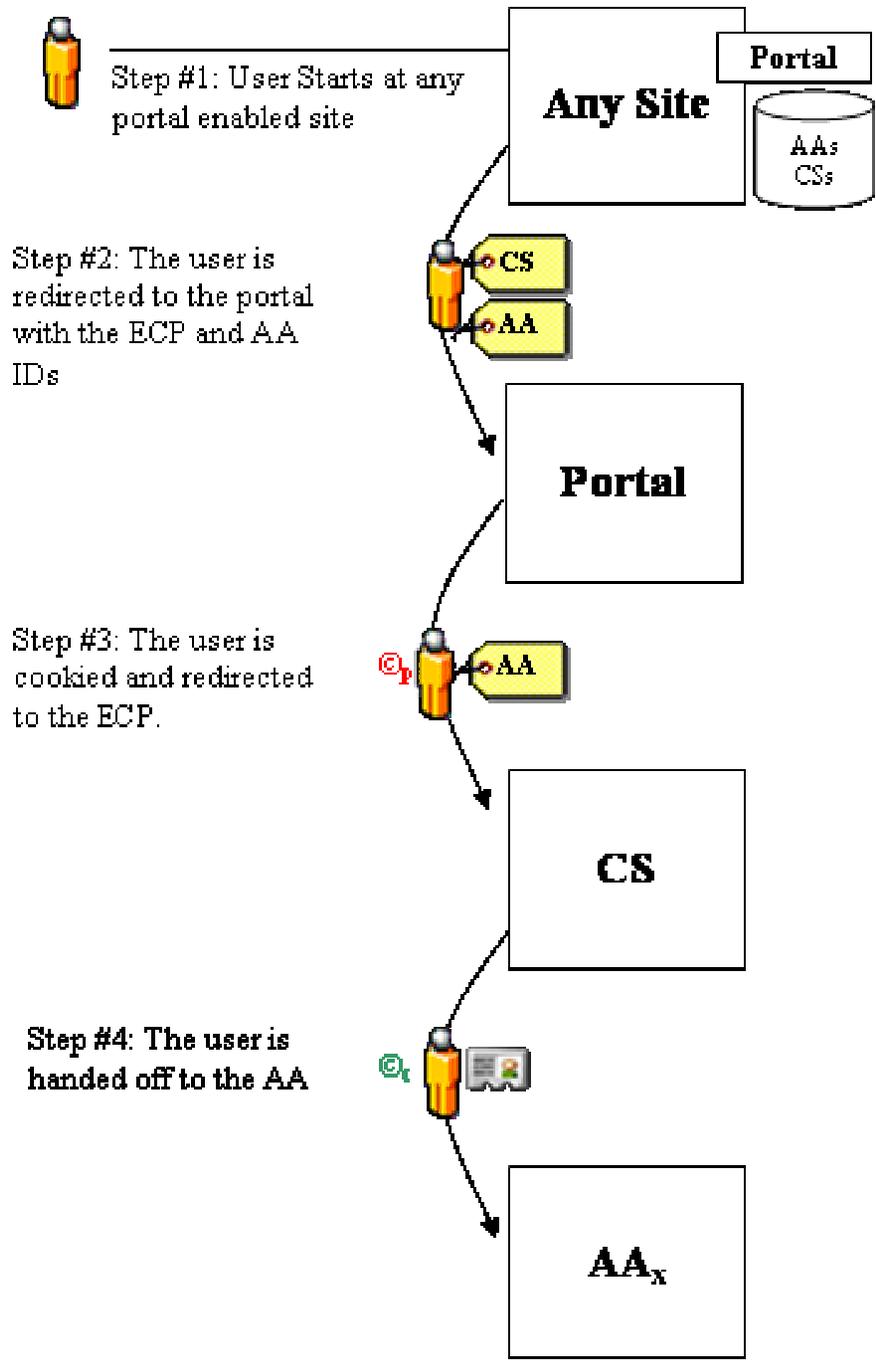
# Starting at the CS



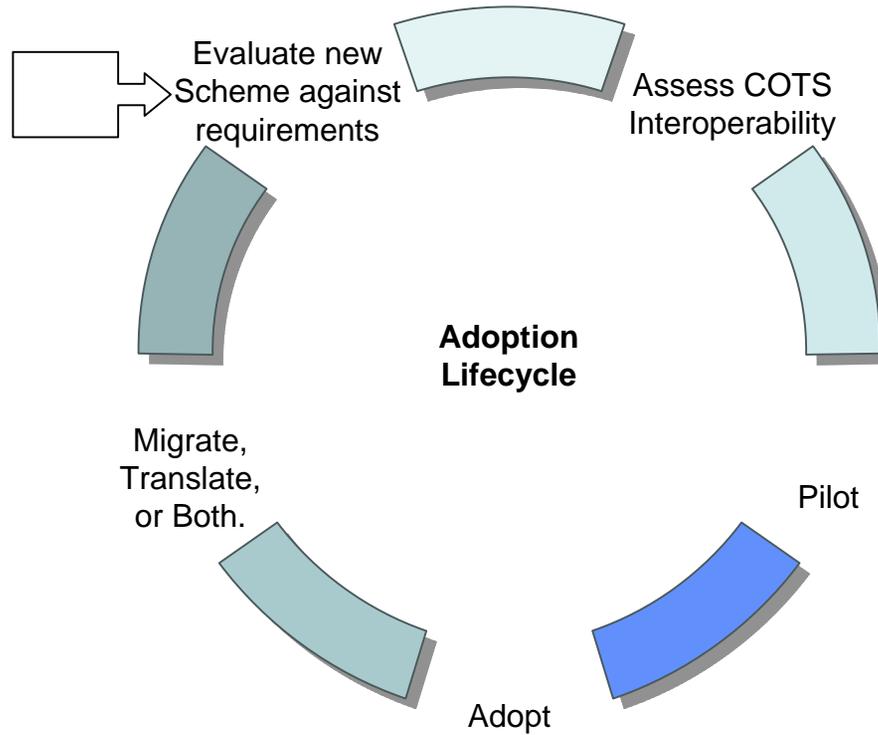
# Protocol Translator



# Specialized Portals



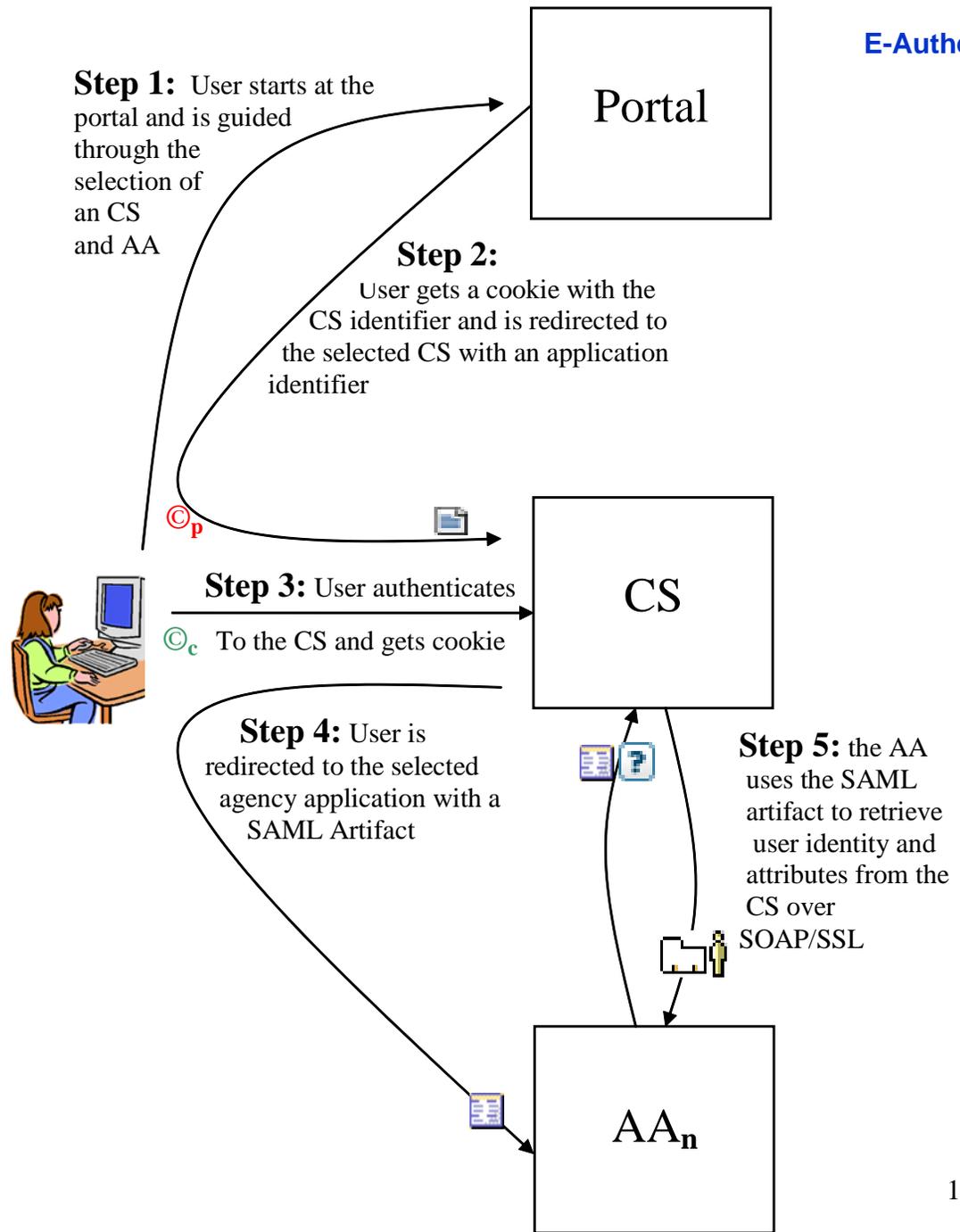
**Figure : Scheme Adoption**



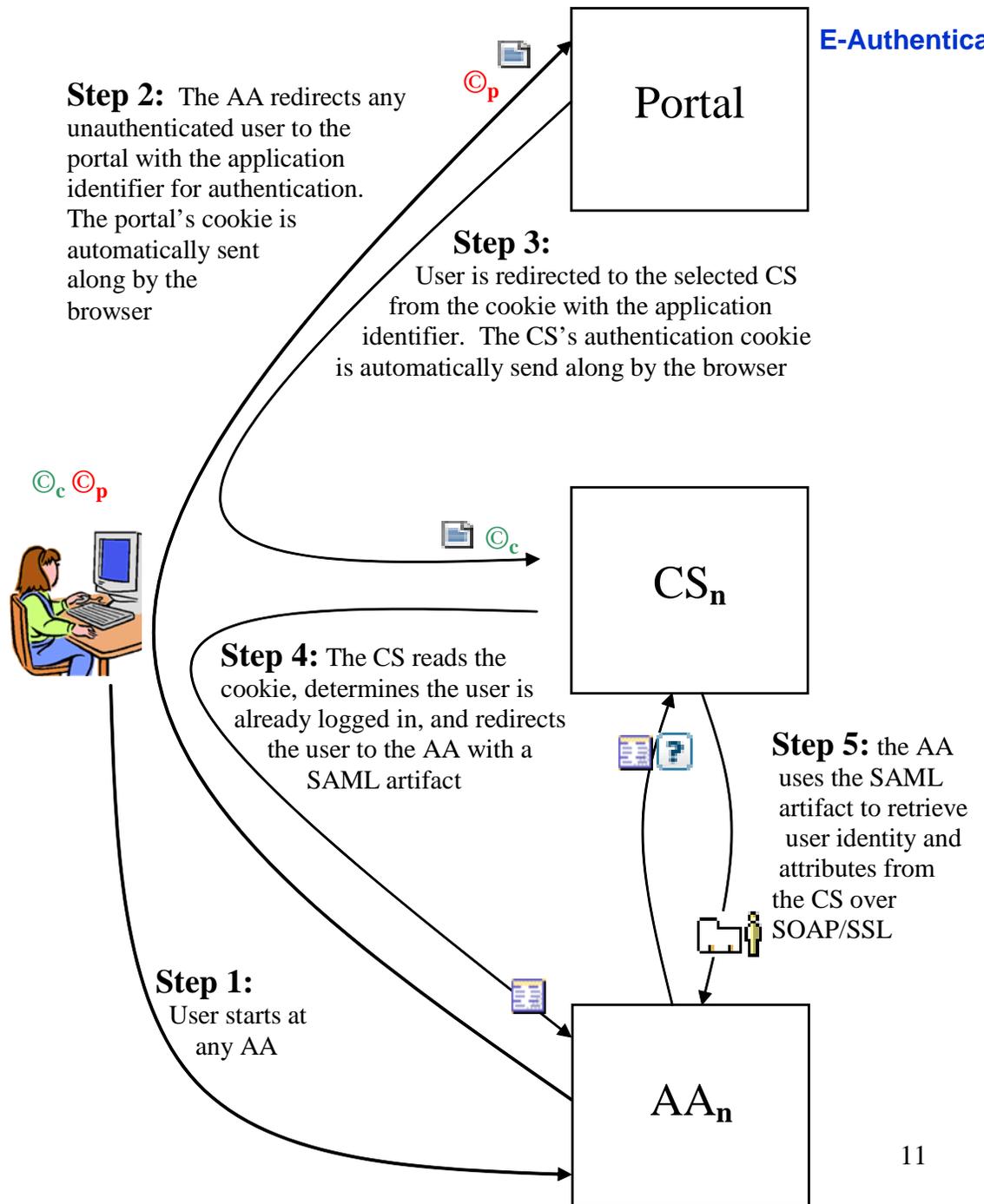
# ***SAML as an Adopted Scheme***

- ◆ SAML 1.0 Artifact Profile
  - Proven interoperability

# Base Case

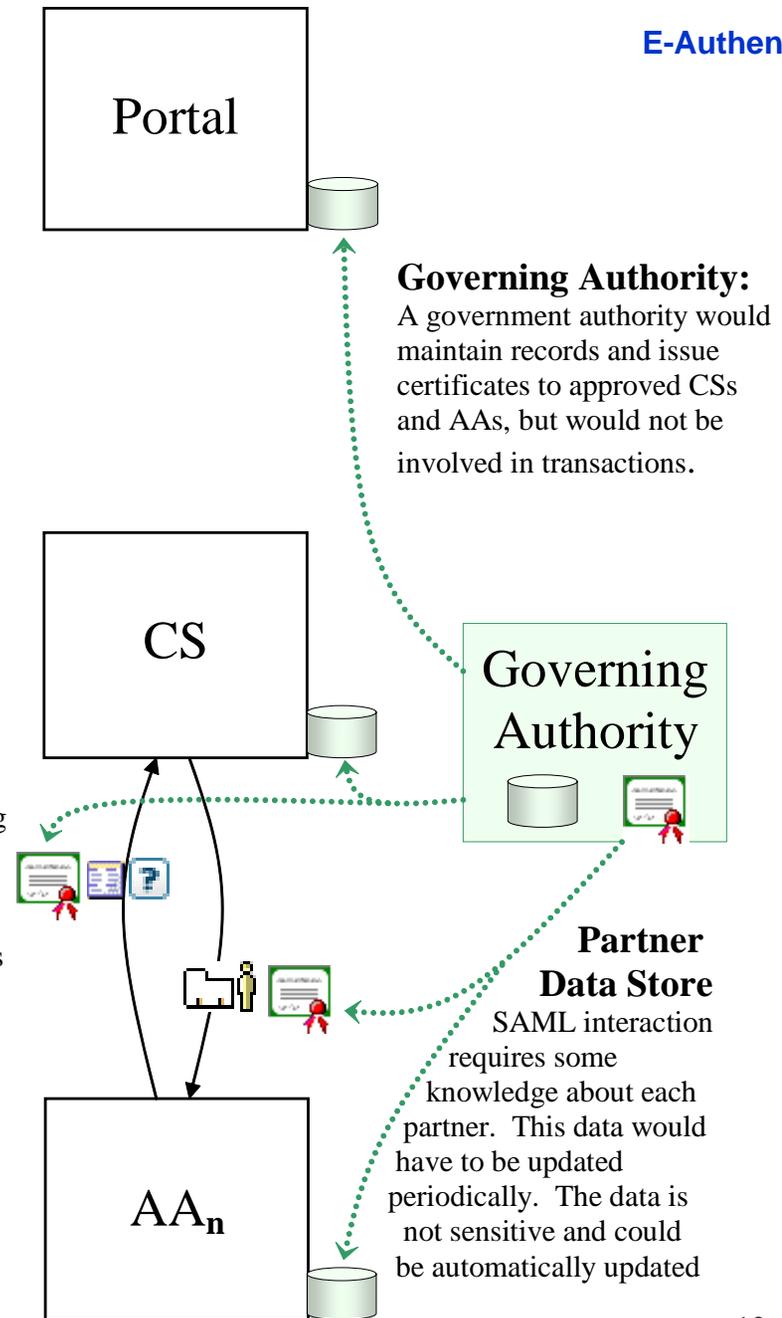


# Single Sign-On



# Governance

**SSL Certificate Authentication:**  
The soap connection can be protected using certificates issued by the governing authority to ensure only approved entities can participate.



**Governing Authority:**  
A government authority would maintain records and issue certificates to approved CSs and AAs, but would not be involved in transactions.

**Governing Authority**

**Partner Data Store**  
SAML interaction requires some knowledge about each partner. This data would have to be updated periodically. The data is not sensitive and could be automatically updated

# ***Lower Assurance Approach***

## ◆ SAML Assertion Contents

- Name
- User ID
- CS ID

## ◆ AA Responsibilities

- Authorization / Entitlements
- Mapping asserted identity to known identity
- May map multiple credentials to a known identity

## ◆ CS Responsibilities

- Identity Management
- Credential Assessment Framework (CAF) requirements

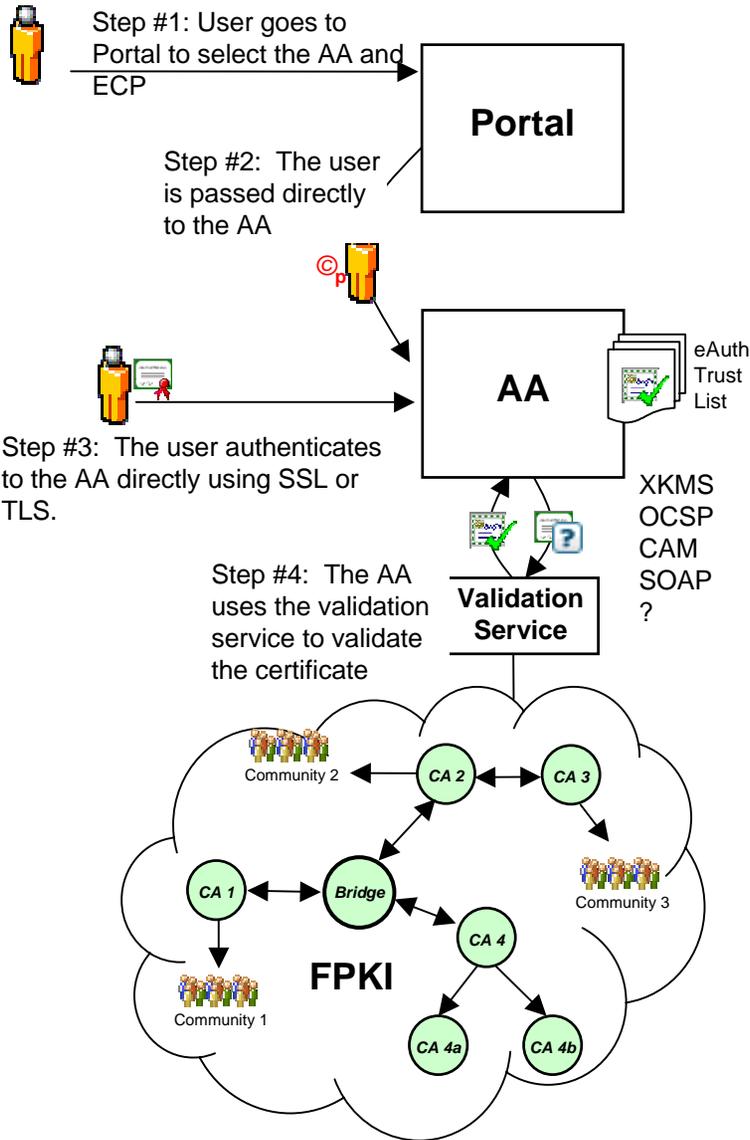
# Higher Assurance Levels

## ◆ Certificate Based Authentication

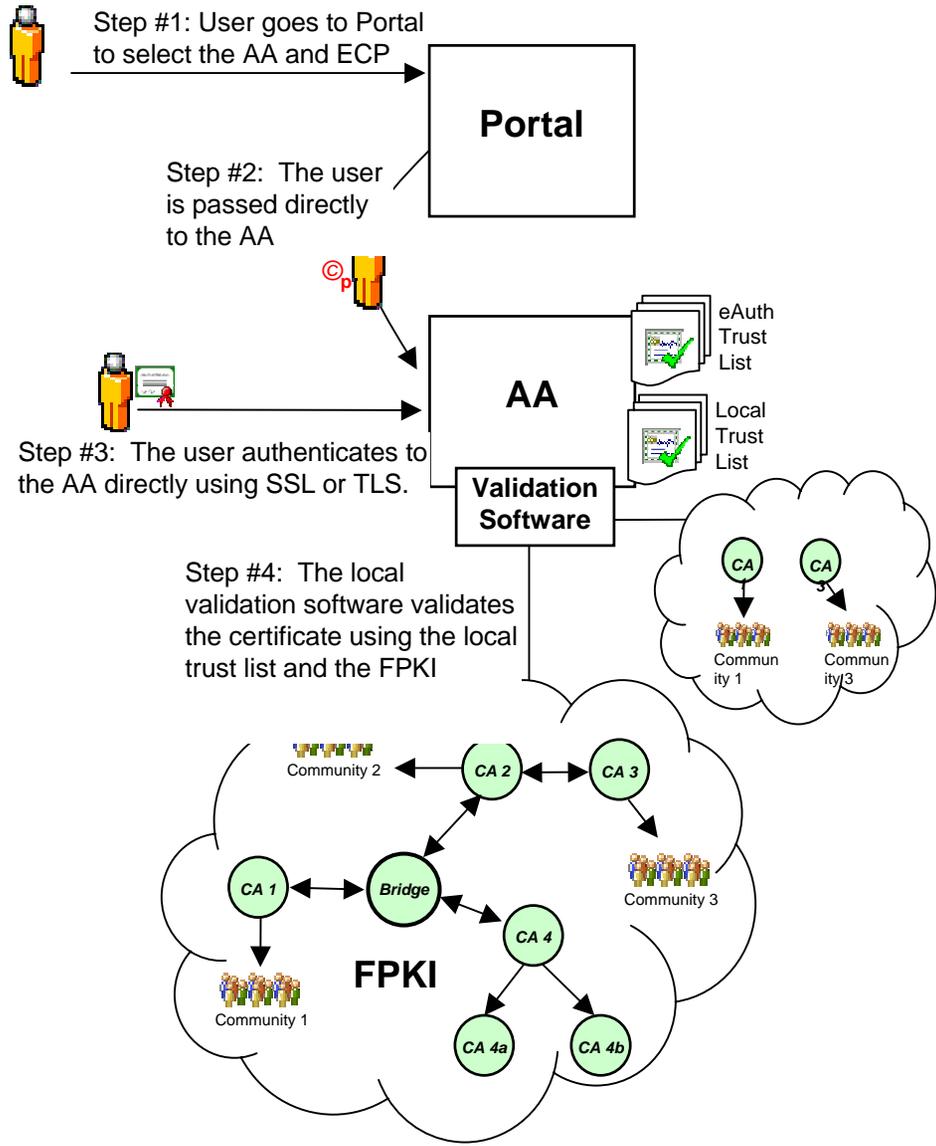
- *“All sensitive data transfers shall be cryptographically authenticated using keys bound to the authentication process” NIST SP800-63*
- Does not require shared secrets
- Certificate Path Discovery and Validation

## ◆ Certificates at lower assurance AAs

**FPKI**



FPKI



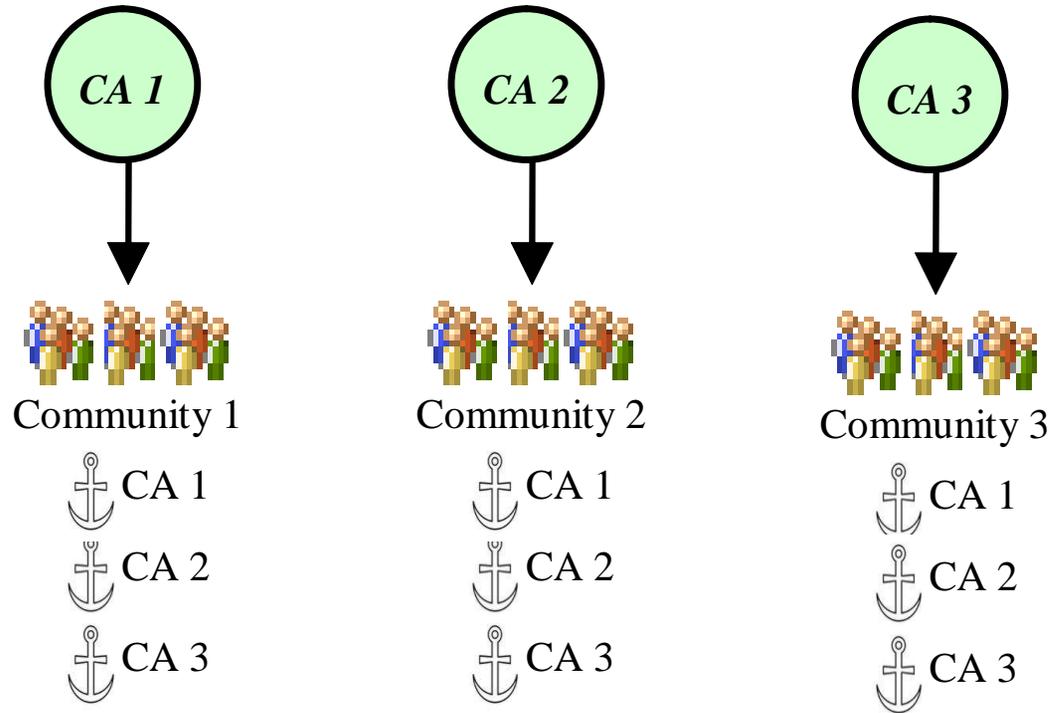
## *Higher Assurance Approach*

- ◆ Certificate Validation is not enough
  - ***Certificate Path*** Discovery and Validation

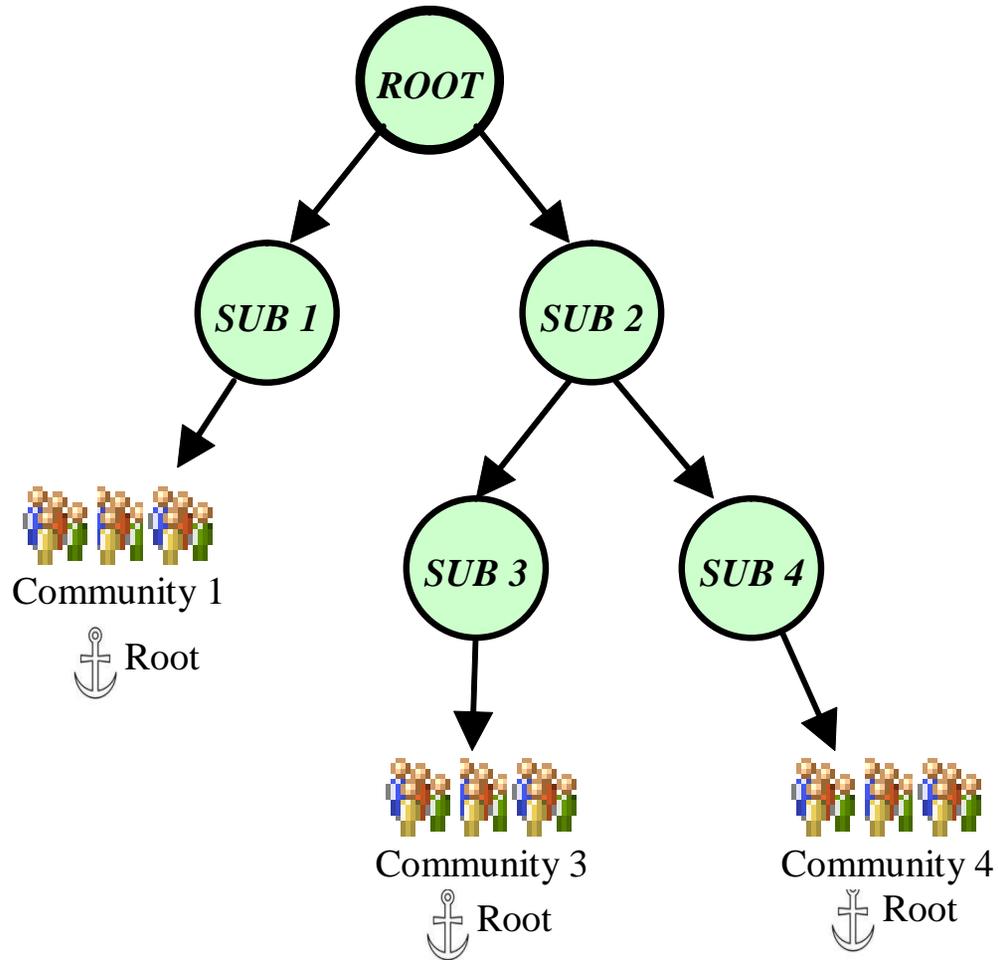
# One Minute PKI

- ◆ Public & Private Key Pair
  - Mathematically bound numbers
  - Encrypt with one, Decrypt with the other
- ◆ Digital Signatures
  - Hashes encrypted with a private key
  - Validate source and integrity
- ◆ Certificate Authorities (CAs) and Certificates
  - Certificates bind a public key to an identity
  - CAs issue certificates based on their policies
  - Certificates are digitally signed by CAs
- ◆ Trust Anchors
  - A CAs self-signed certificate

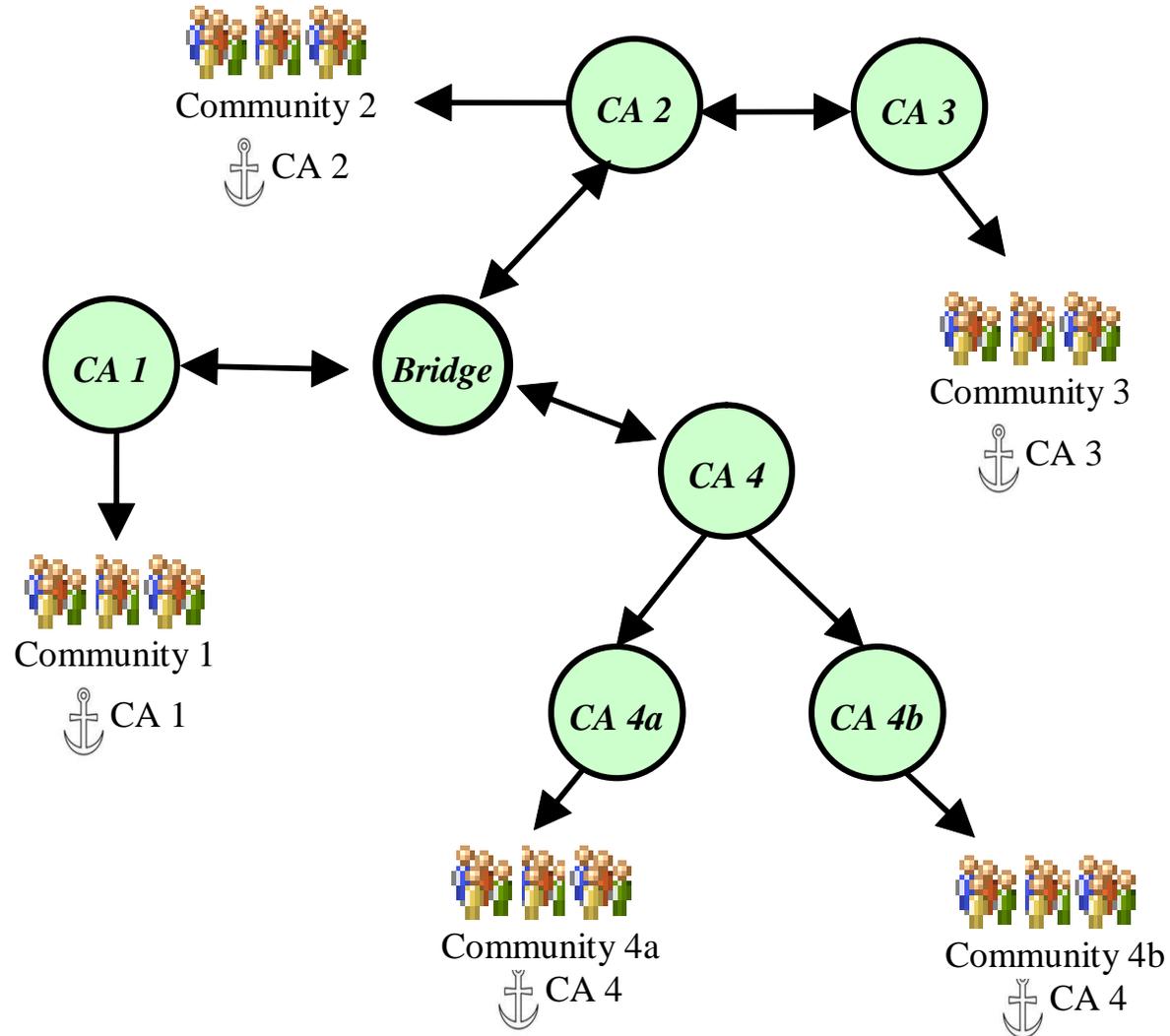
# Typical PKI



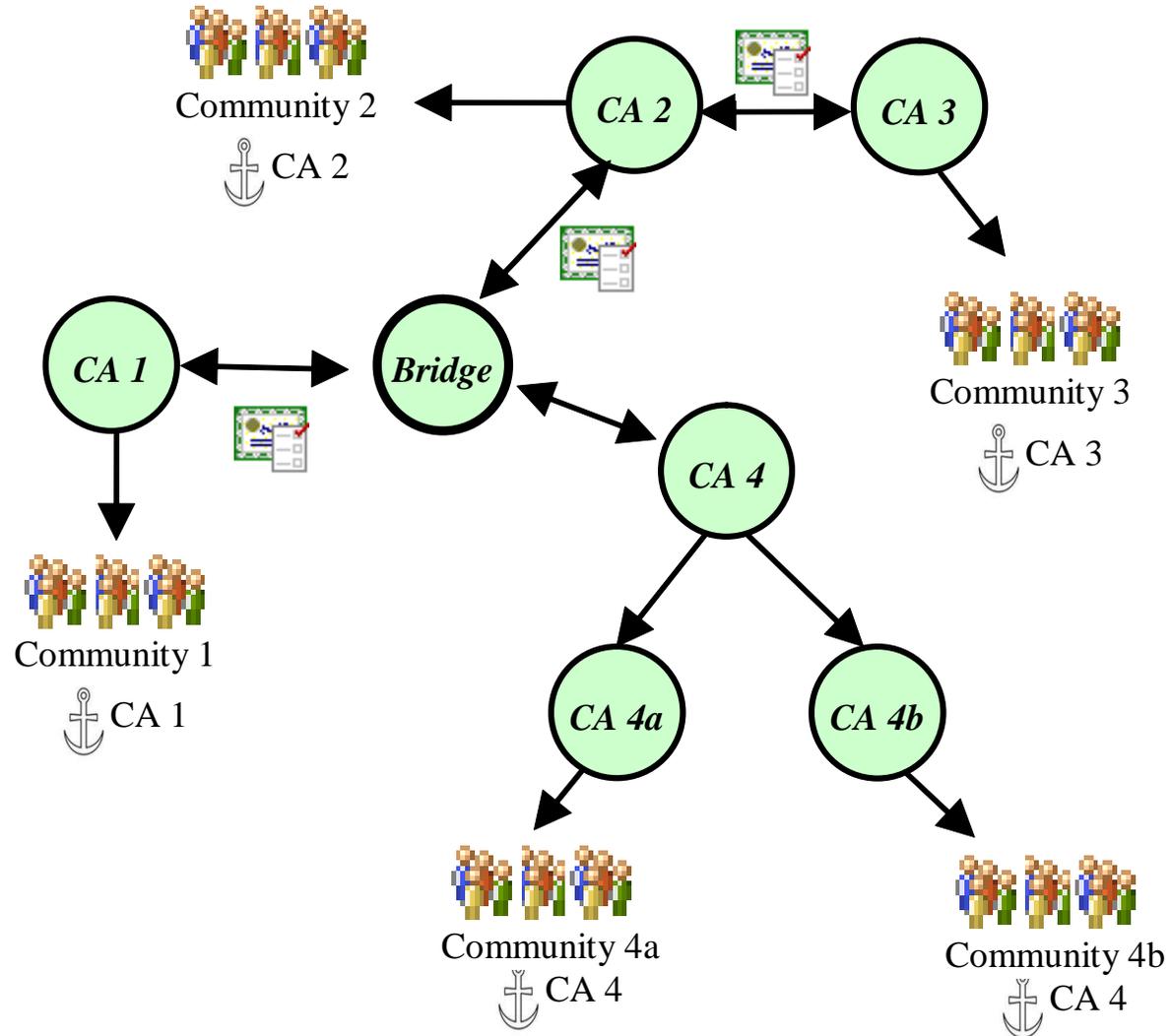
# Hierarchical PKI

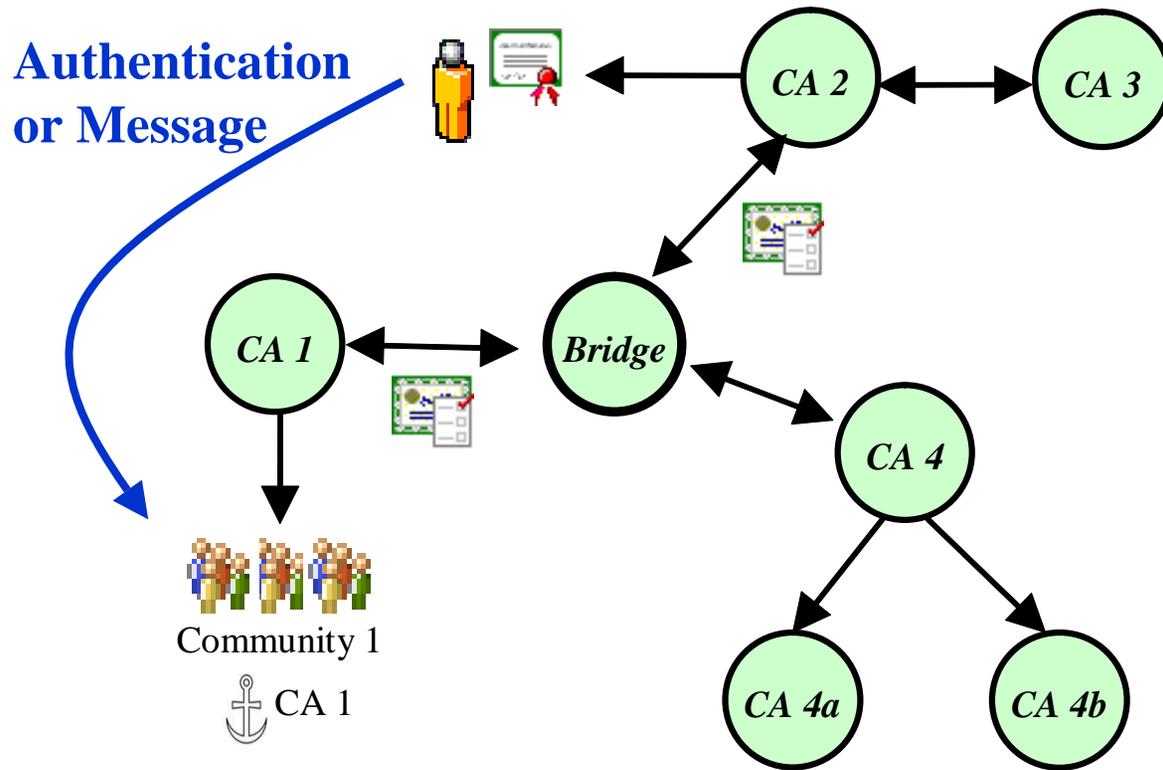


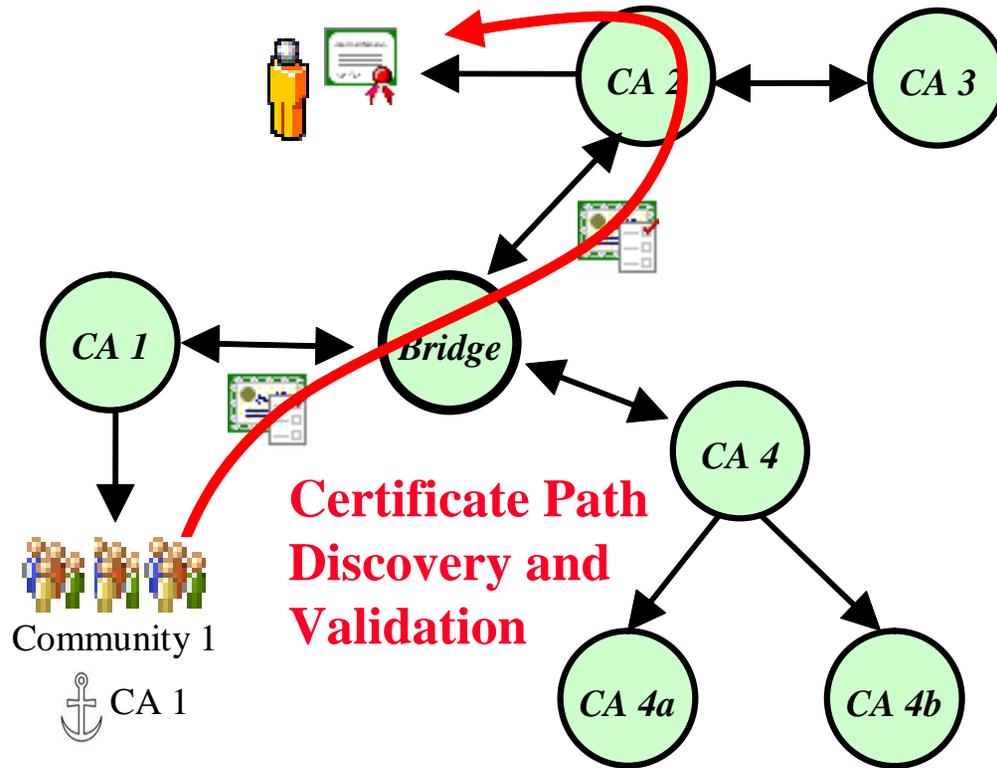
# Mesh PKI



# Mesh PKI



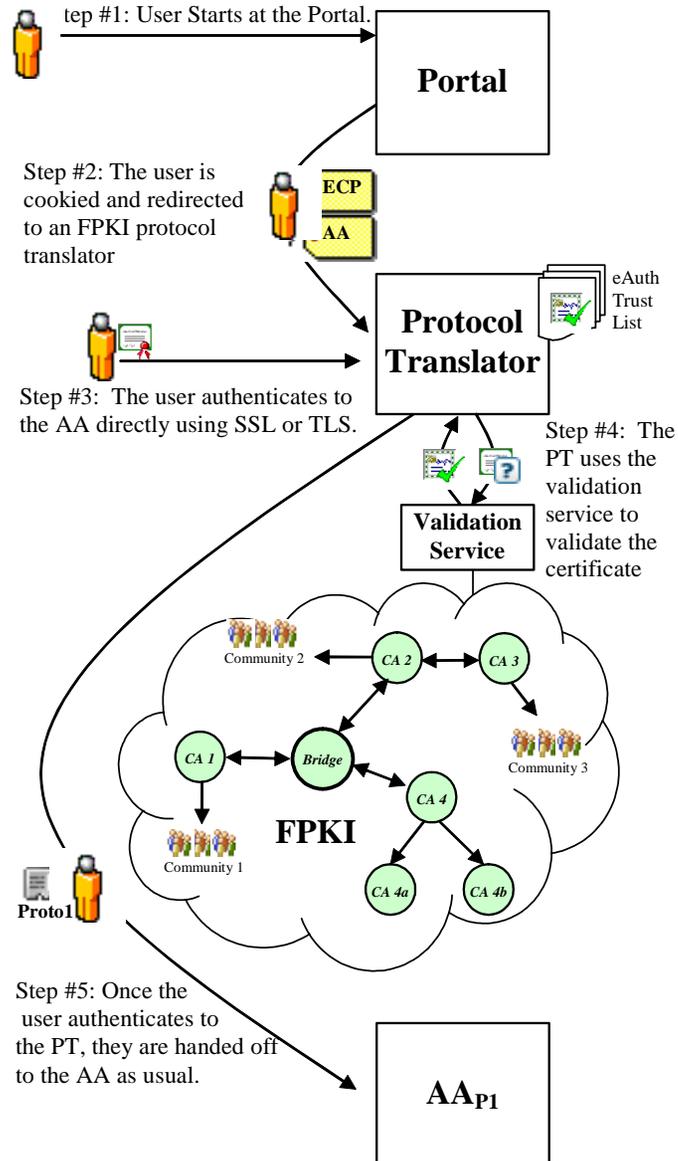




## *Higher Assurance Approach*

- ◆ Certificate Usability at lower assurance AAs
  - Avoid multiple interfaces at AAs
  - Avoid PKI complexities at lower assurance AAs

**PKI credentials for low assurance AAs**



# *High Assurance Approach*

- ◆ Relation to Federal PKI Architecture

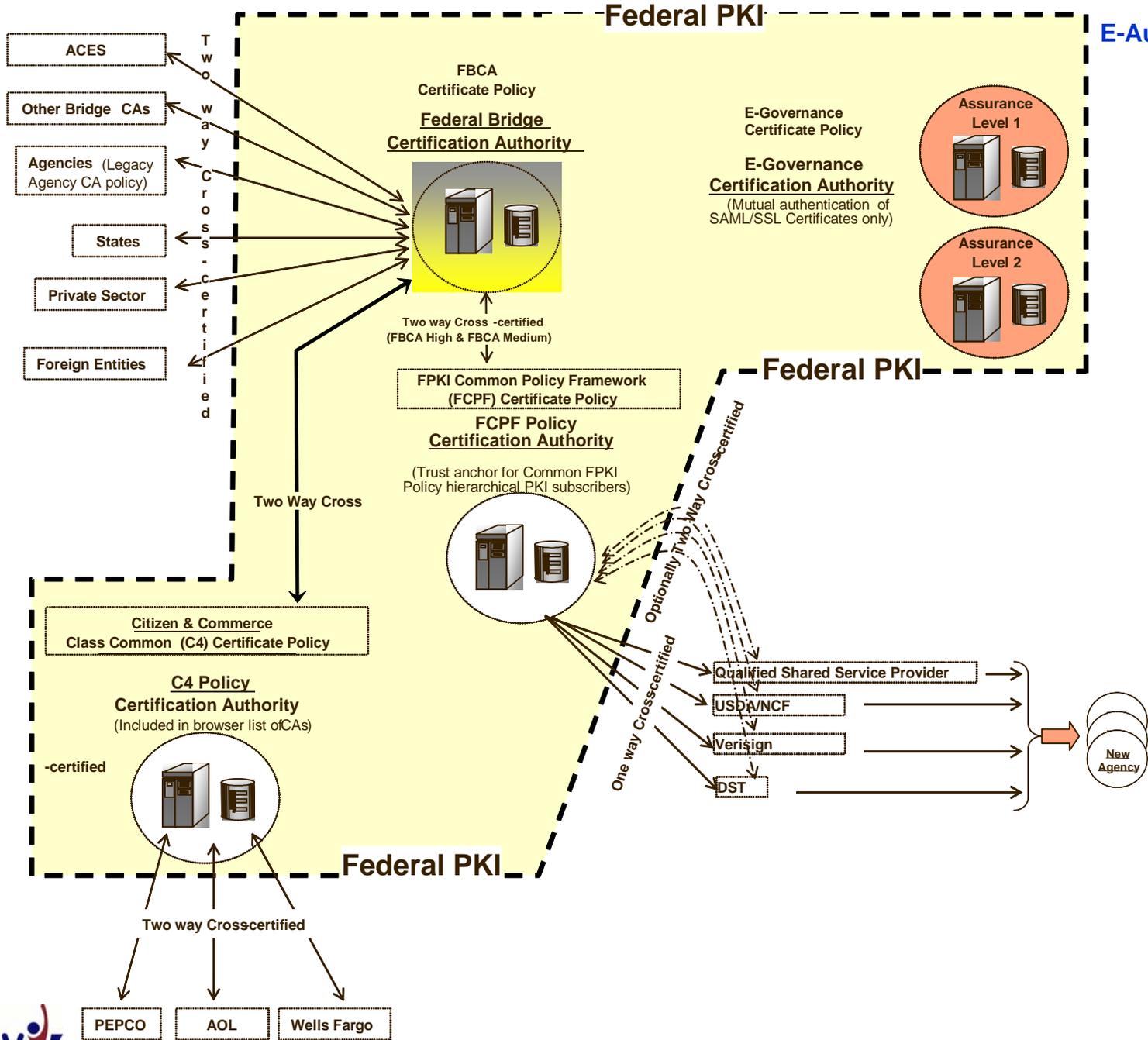
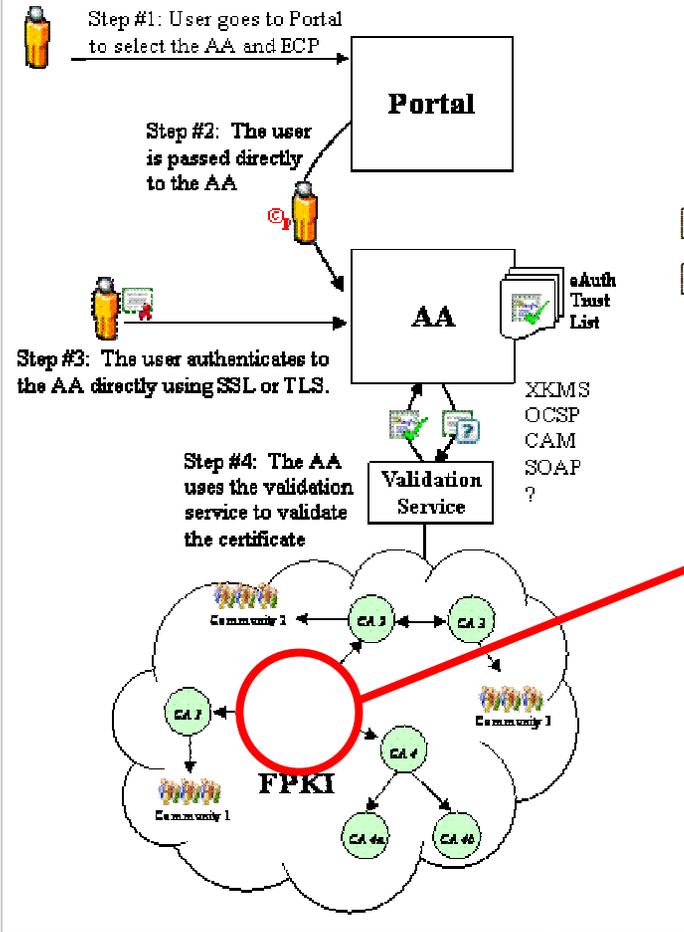
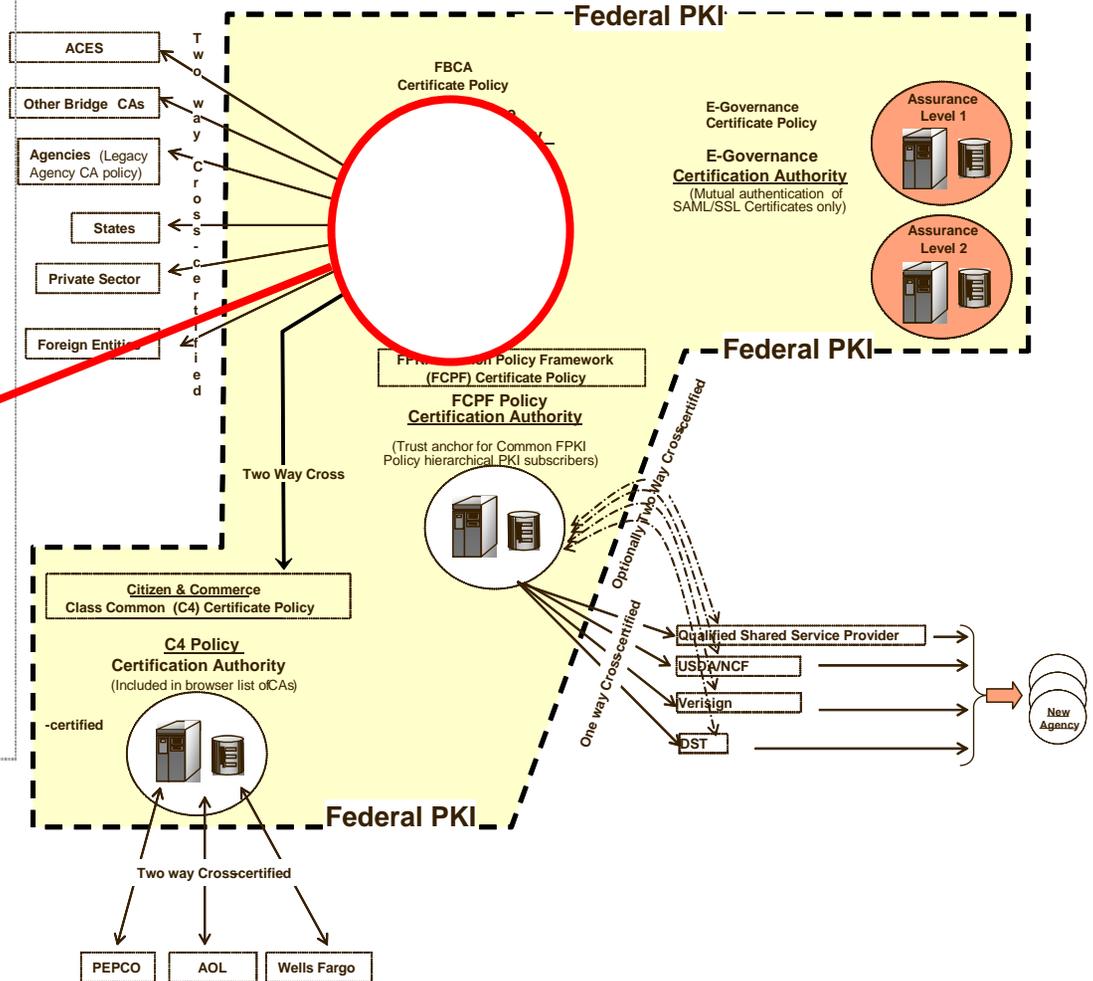


Figure 1: FPKI



*FPKI FBCA and eAuthentication*



# FPKI E-Governance CA and eAuthentication Trusted AAs and Trusted CSs

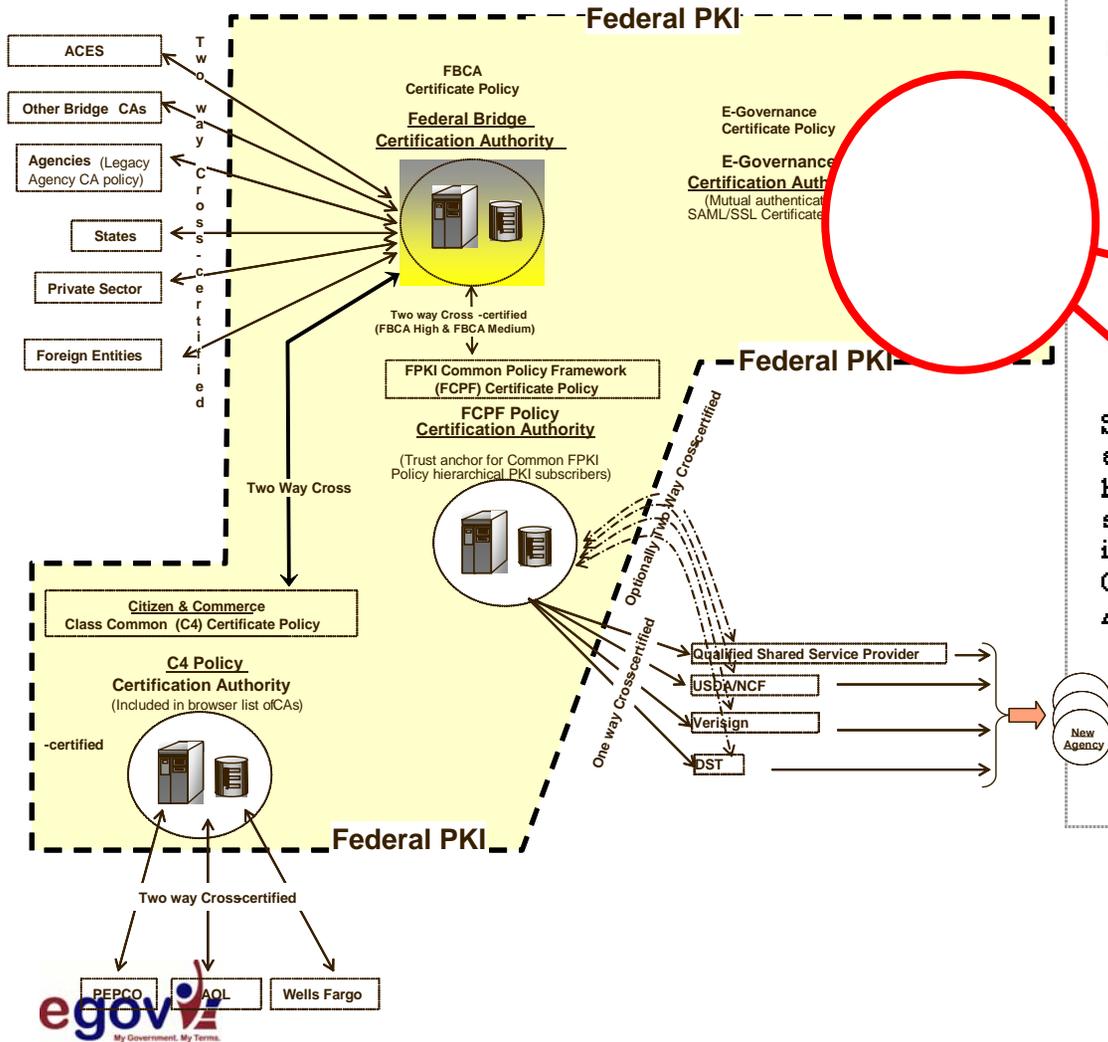
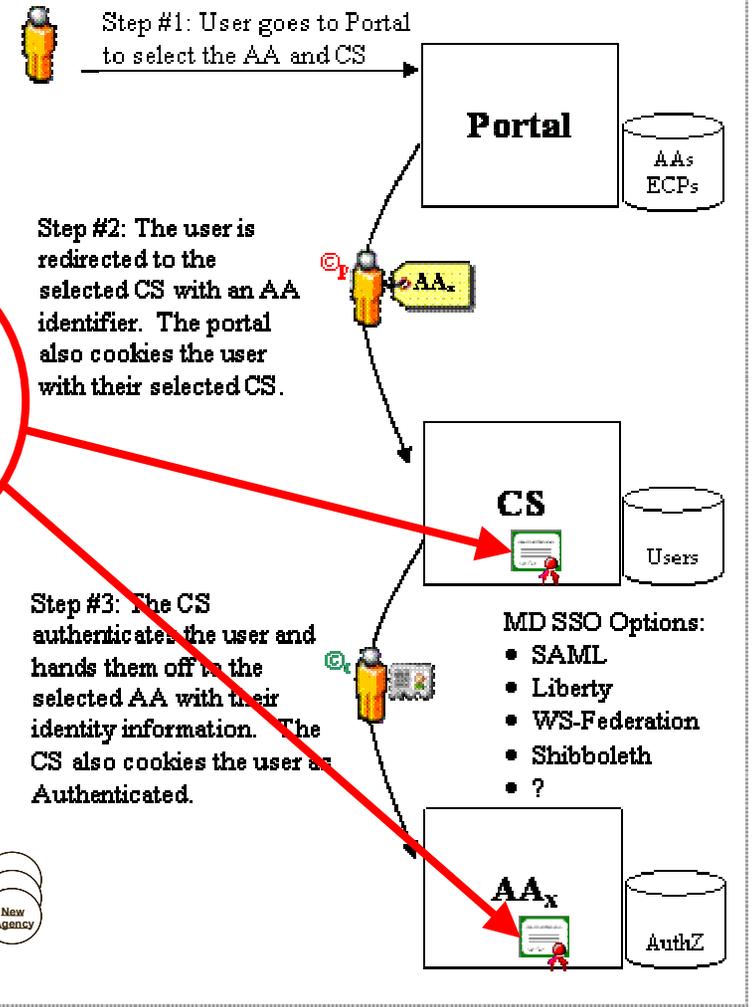
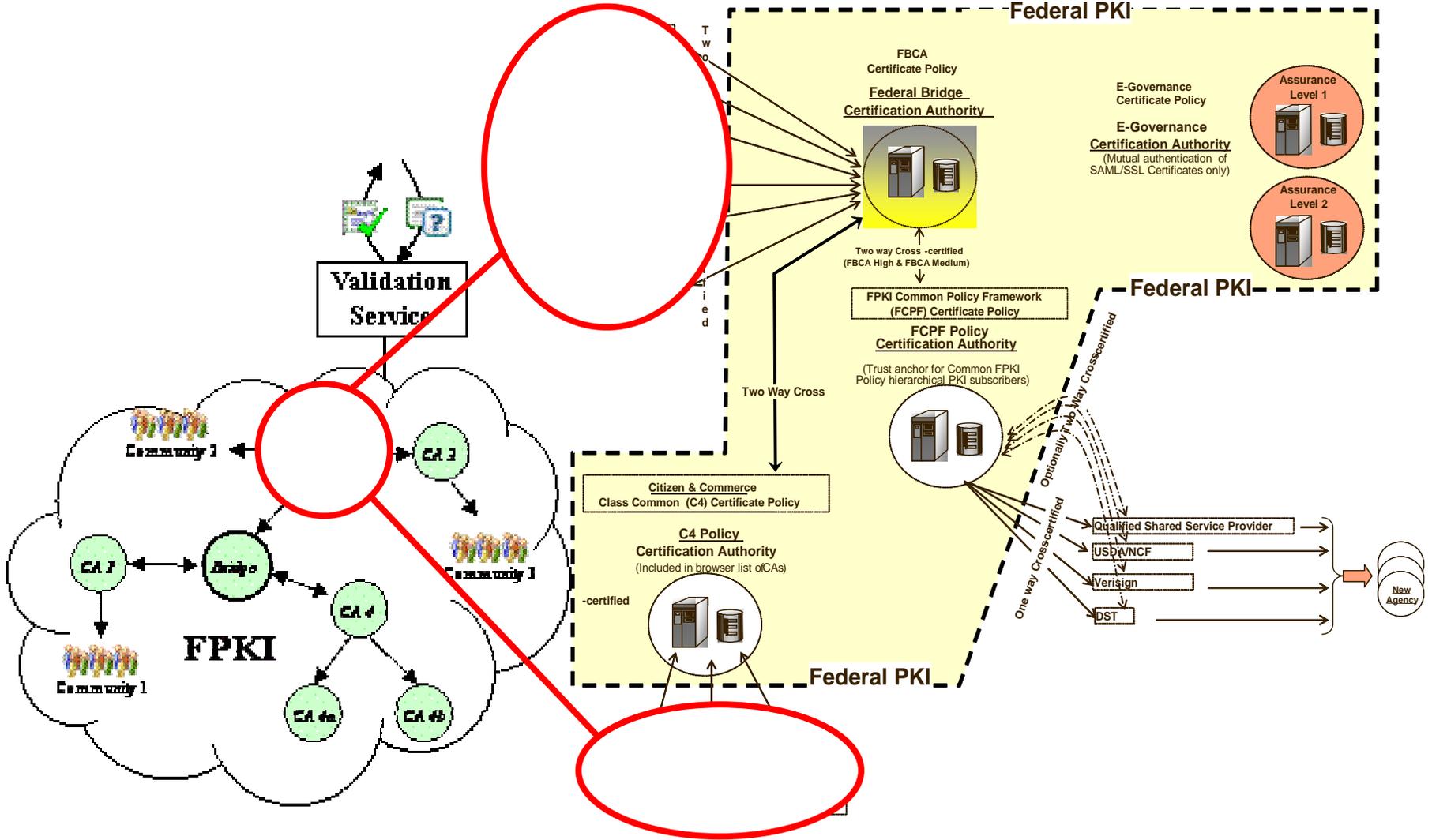
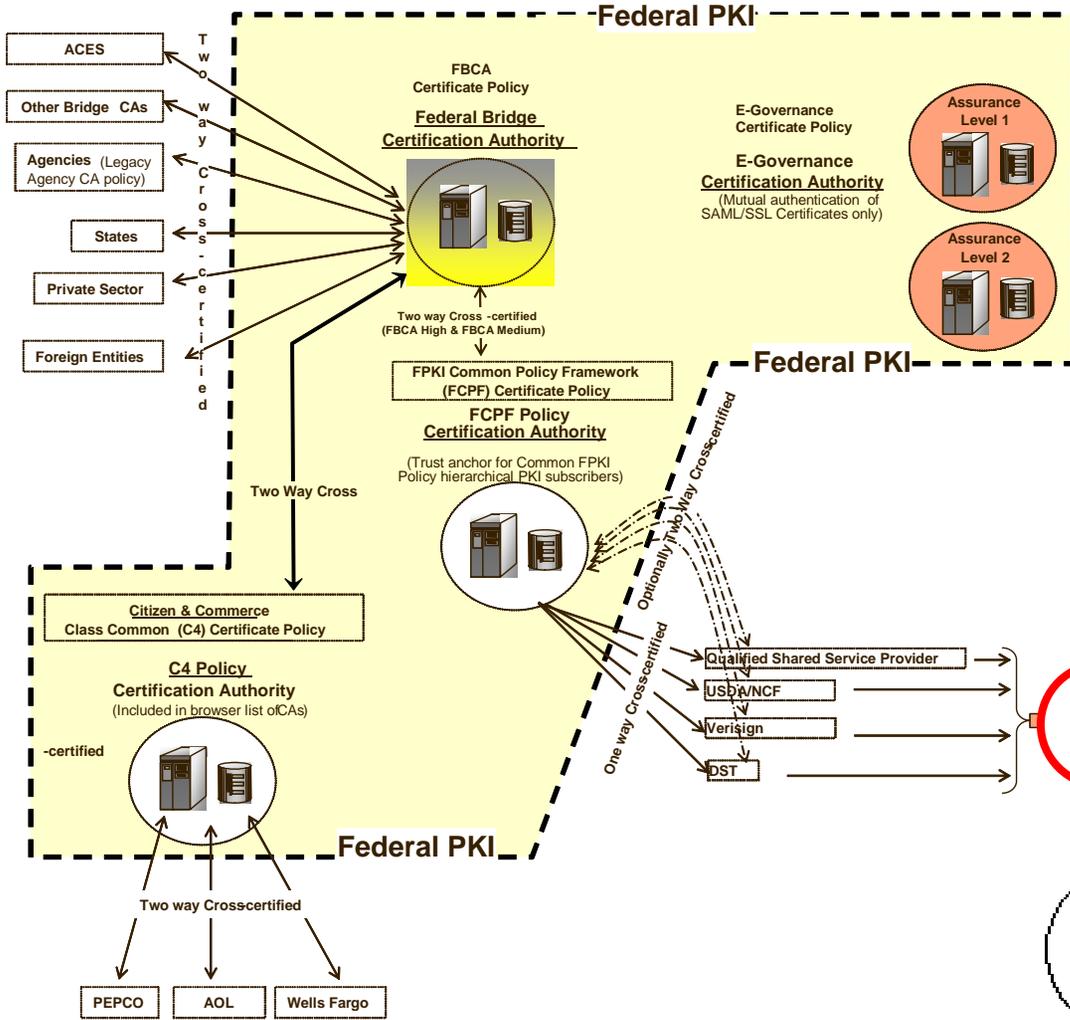


Figure 1: Base Case

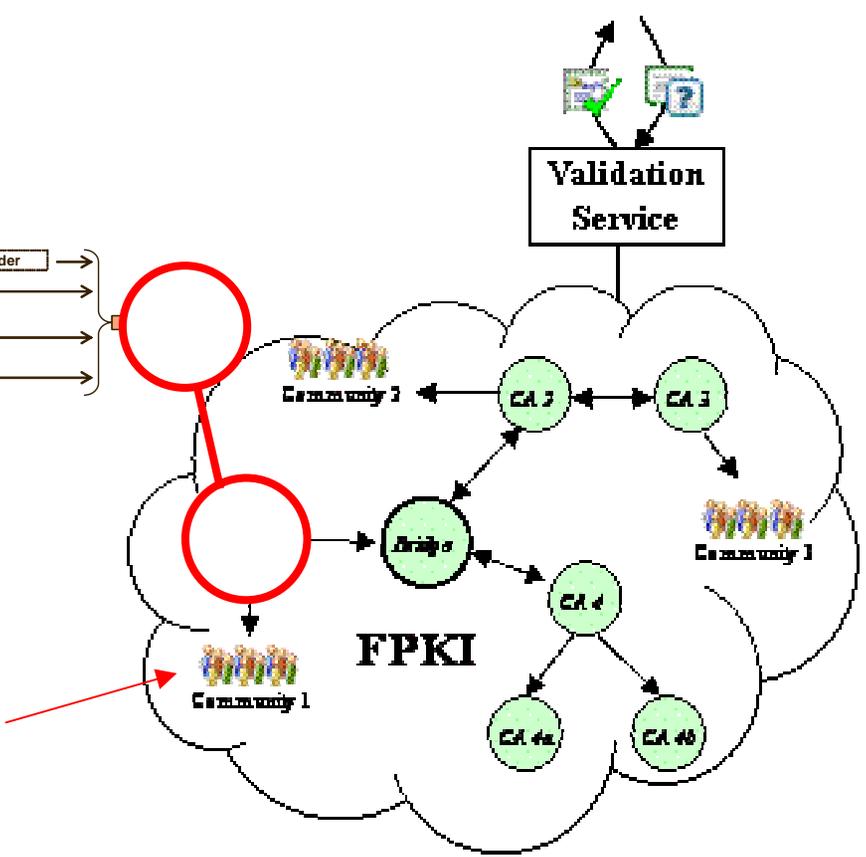




FPKI CAs and eAuthentication



**FPKI Common Policy and eAuthentication**



Federal Employees

## *Where we are today*

- ◆ Proof of Concept
  - SAML 1.0 Artifact Profile
- ◆ Interoperability Lab
- ◆ Architecture Working Group
- ◆ Pilots

# References

## ◆ eAuthentication Documents

- <http://www.cio.gov/eauthentication>

## ◆ NIST Documents

- <http://csrc.nist.gov/pki/testing/x509paths.html>
- <http://csrc.nist.gov/publications/drafts.html>

## *Coming Soon*

- ◆ FOC
- ◆ Forms
- ◆ Web Services
- ◆ Composite Apps
- ◆ New Schemes