# *A Preview of the E-Authentication FOC Architecture*

egov
My Government. My Terms.

# *Agenda*

- Architecture Working Group
- Baseline Architecture
- Changes Coming in the FOC

# ➢ *Architecture Working Group (AWG)*

- Kick Off 10/31/03
- 27 members
  - GSA, NIST, USDA, USPTO, Treasury, HHS, OPM, EPA
  - Enspier, BAH, Accenture, Mitretek, IBM
- Four Sub-Group “Tiger Teams”
  - PKI, Composite Apps, SAML, Use Case
- Decided to use the baseline architecture as a starting point on 11/19
  - Agreed it would not constrain the FOC Architecture

# ➢ *Architecture Working Group (AWG)*

- New Scope Considered:
  - Email
  - Forms
  - Personal Identifiable Information and attribute sharing
  - service discovery
  - single sign-off
  - non-browser thin clients (e.g., personal digital assistant, cell phone)
  - cell phone proxies
  - billing and charge-back protocols
  - group/role identification
  - trust agent and power of attorney scenarios
  - Composite Applications

# ➢ *Architecture Working Group (AWG)*

- Status
  - Release Candidate 1 (RC1) completed 5/17/04
  - RC2 completed 5/26/04
  - RC3 expected to be final, expected this week

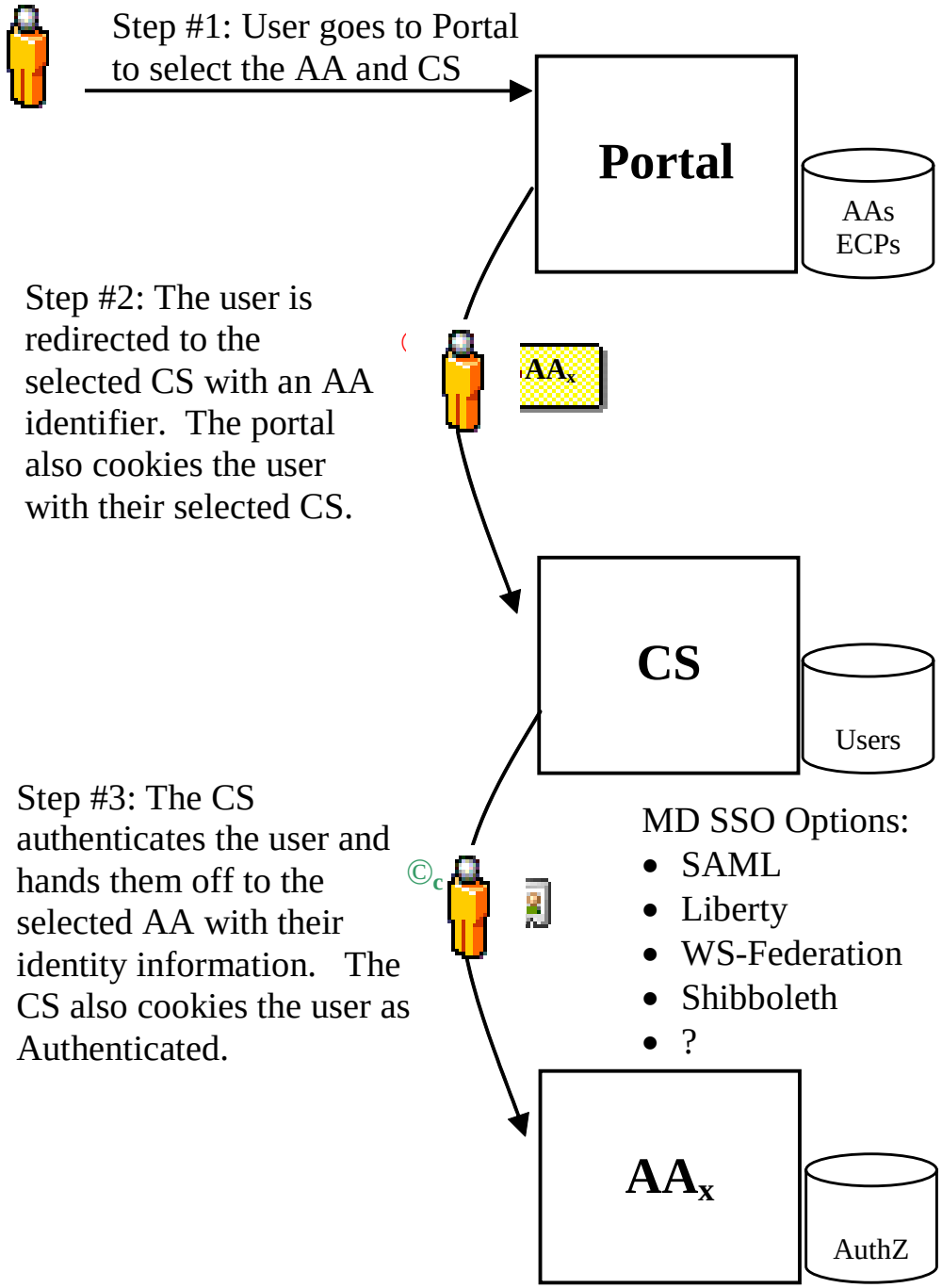
# ➢ *Architecture Working Group (AWG)*

- Result
  - The FOC is a primarily a refinement of the baseline approach, not a new architecture

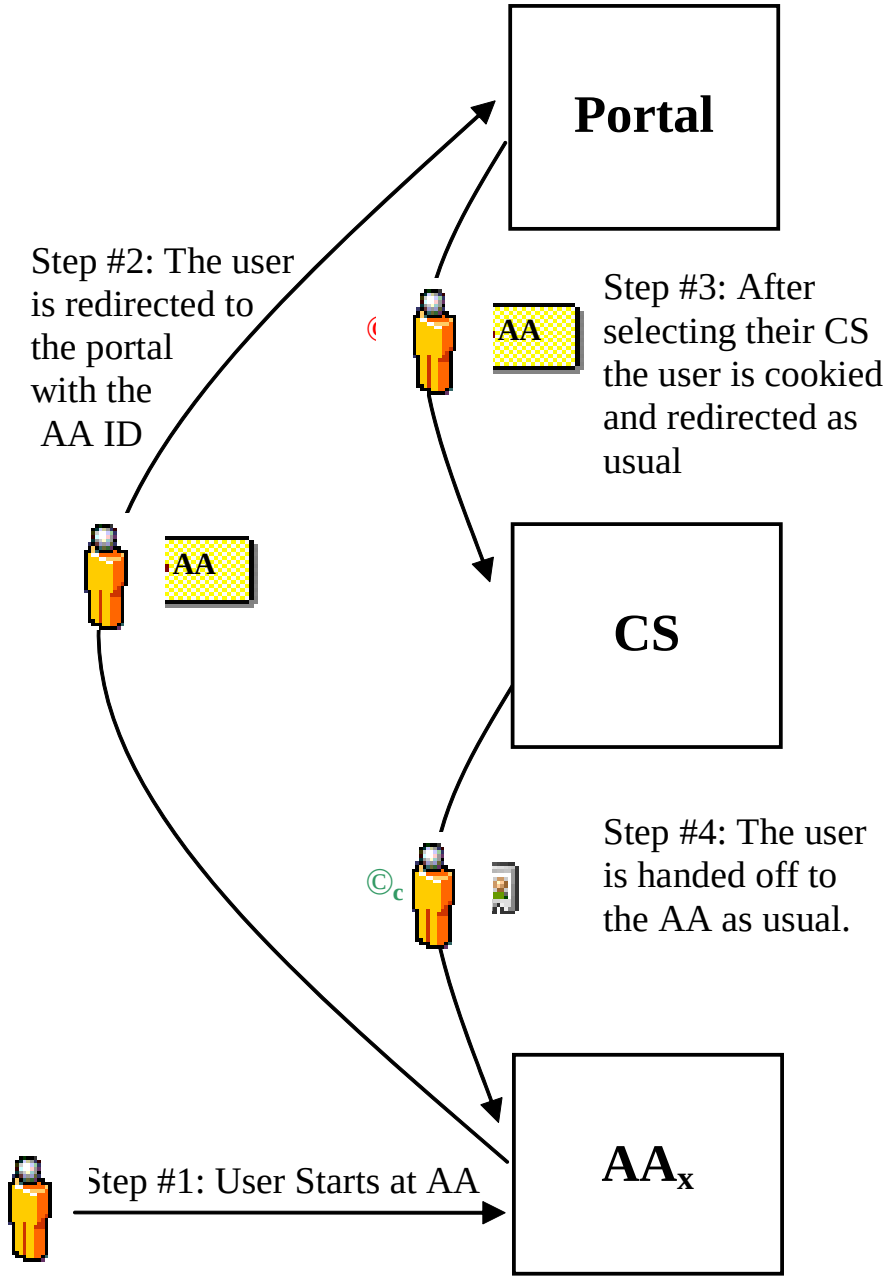
# *Agenda*

- ✓ Architecture Working Group
- ➢ Baseline Architecture
  - ➢ Assertion Based (1,2)
  - • Certificate Based (3,4)
- • Changes Coming in the FOC

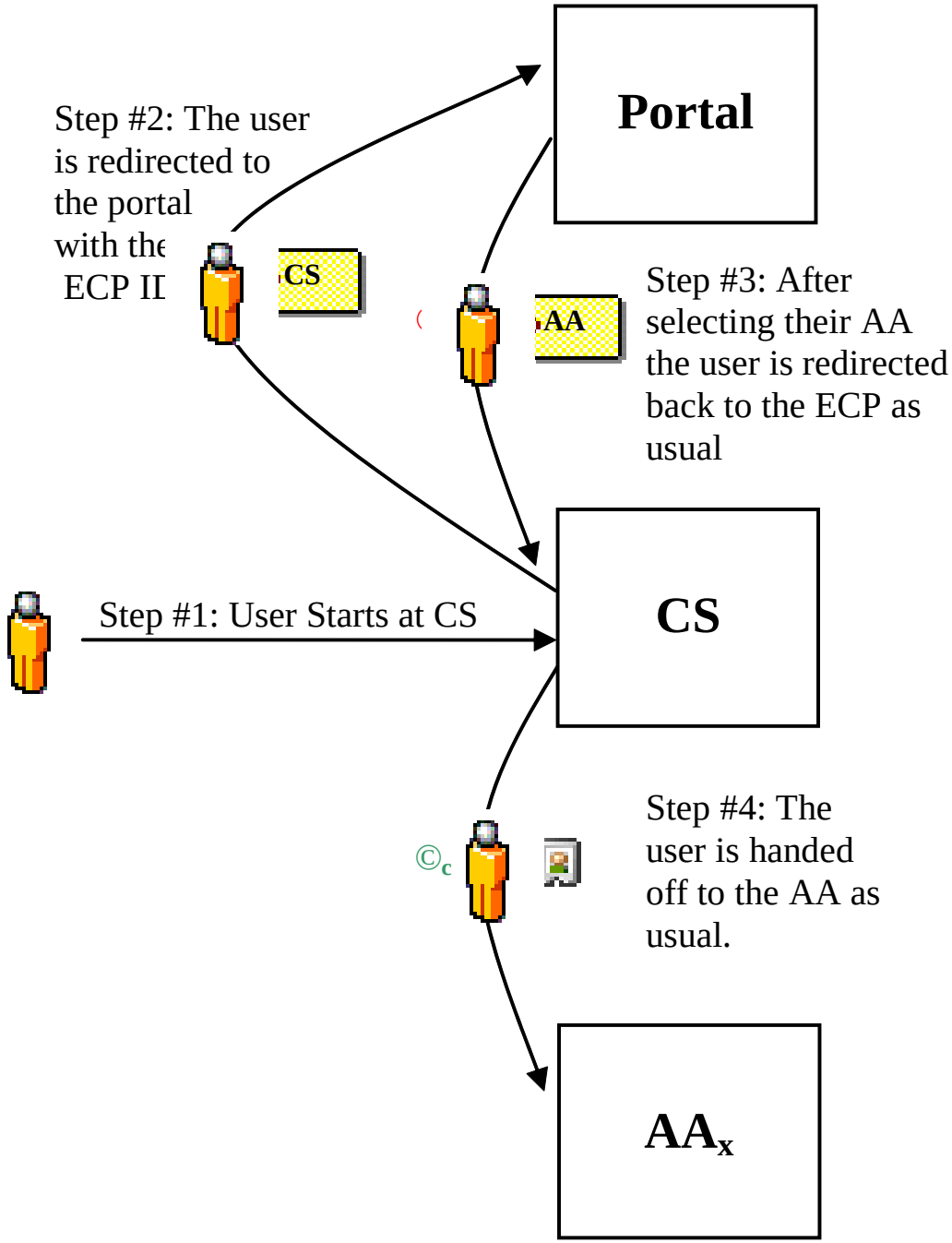
# Base Case


Step #1: User goes to Portal to select the AA and CS
Portal
AAs
ECPs
Step #2: The user is redirected to the selected CS with an AA identifier. The portal also cookies the user with their selected CS.
AAx
CS
Users
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
• ?
AAx
AuthZ

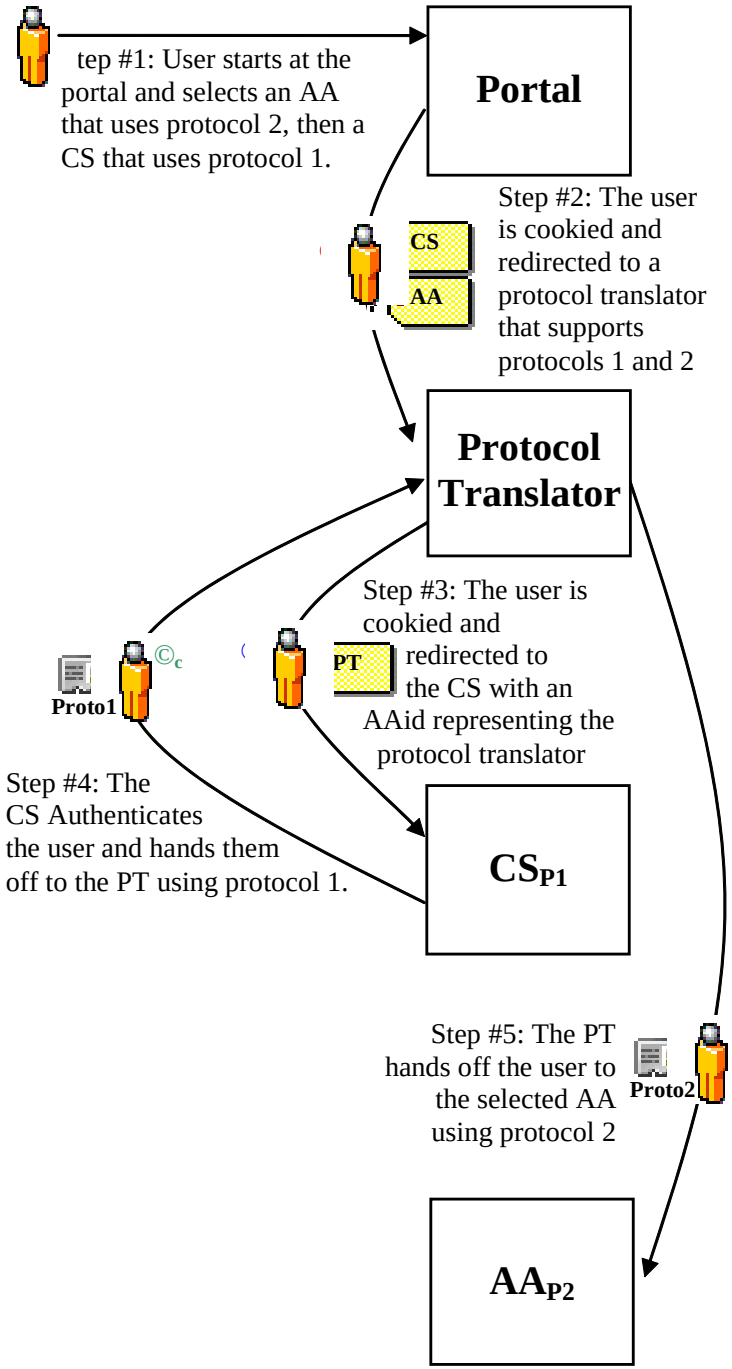
# Starting at the AA

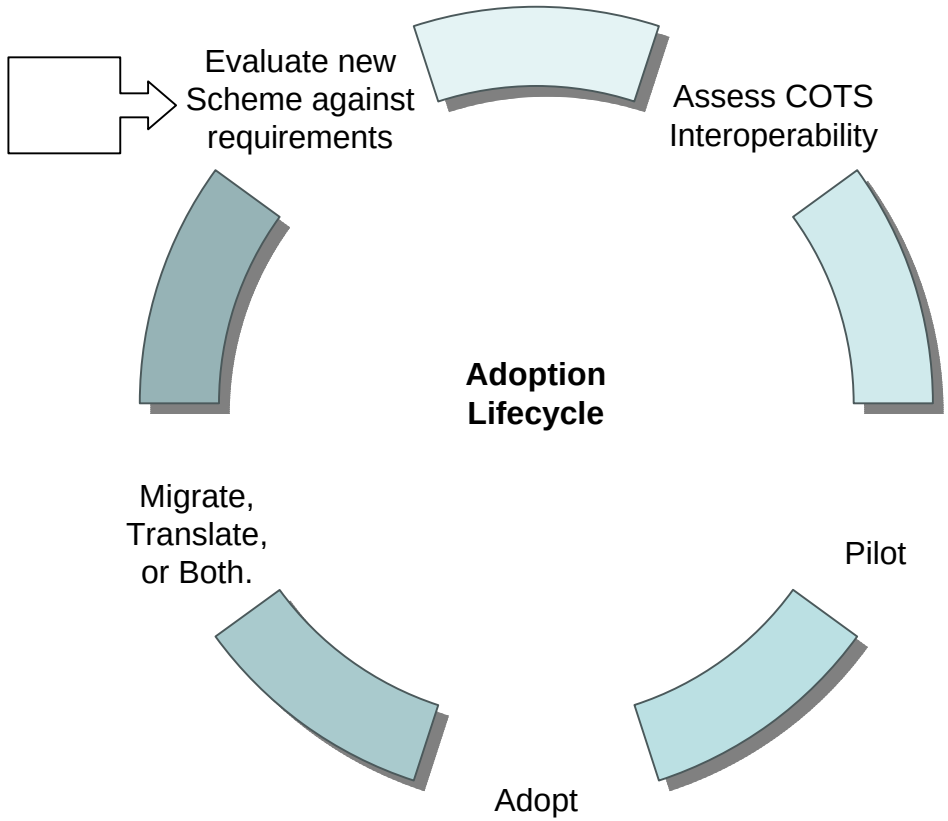


# Starting at the CS



# Scheme Translator

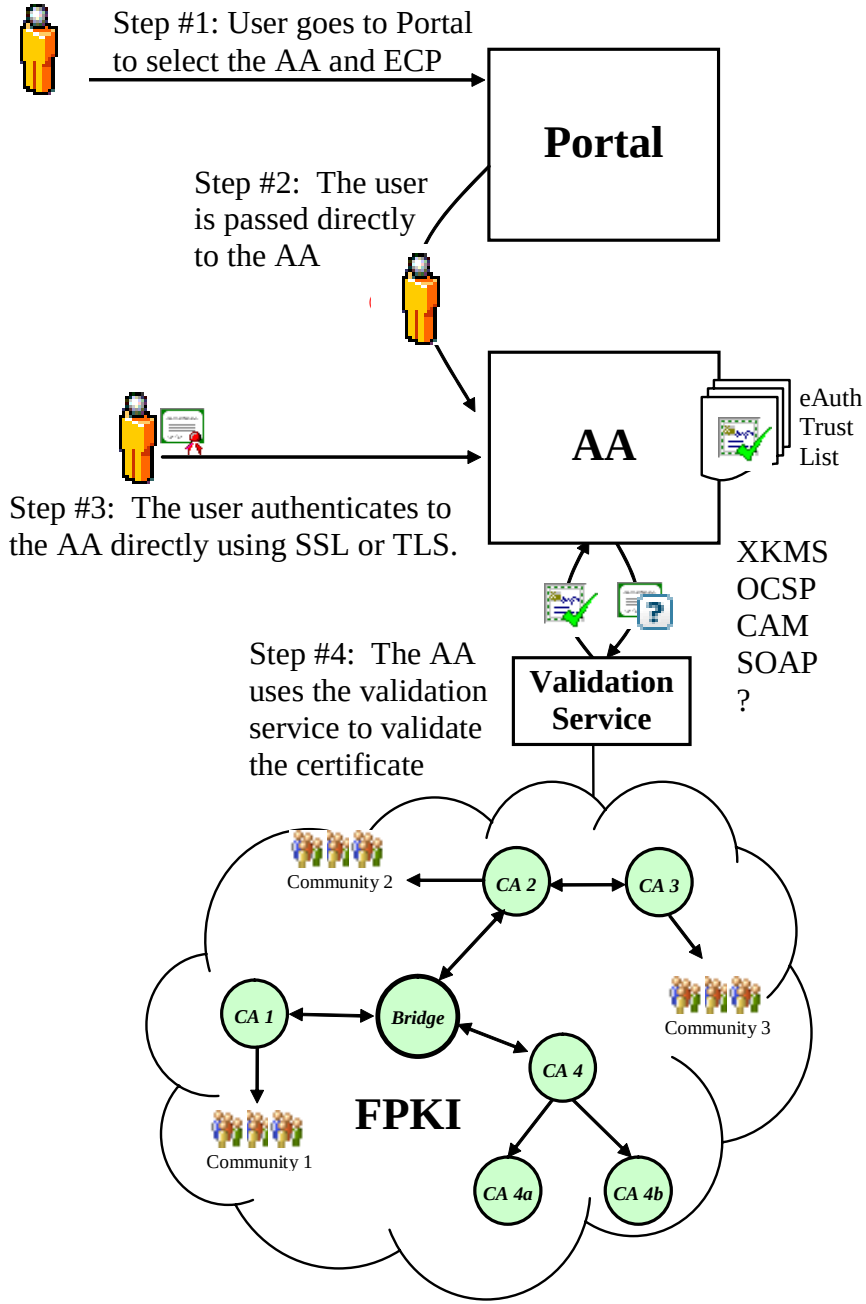



Evaluate new
Scheme against
requirements
Assess COTS
Interoperability
Adoption
Lifecycle
Migrate,
Translate,
or Both.
Pilot
Adopt

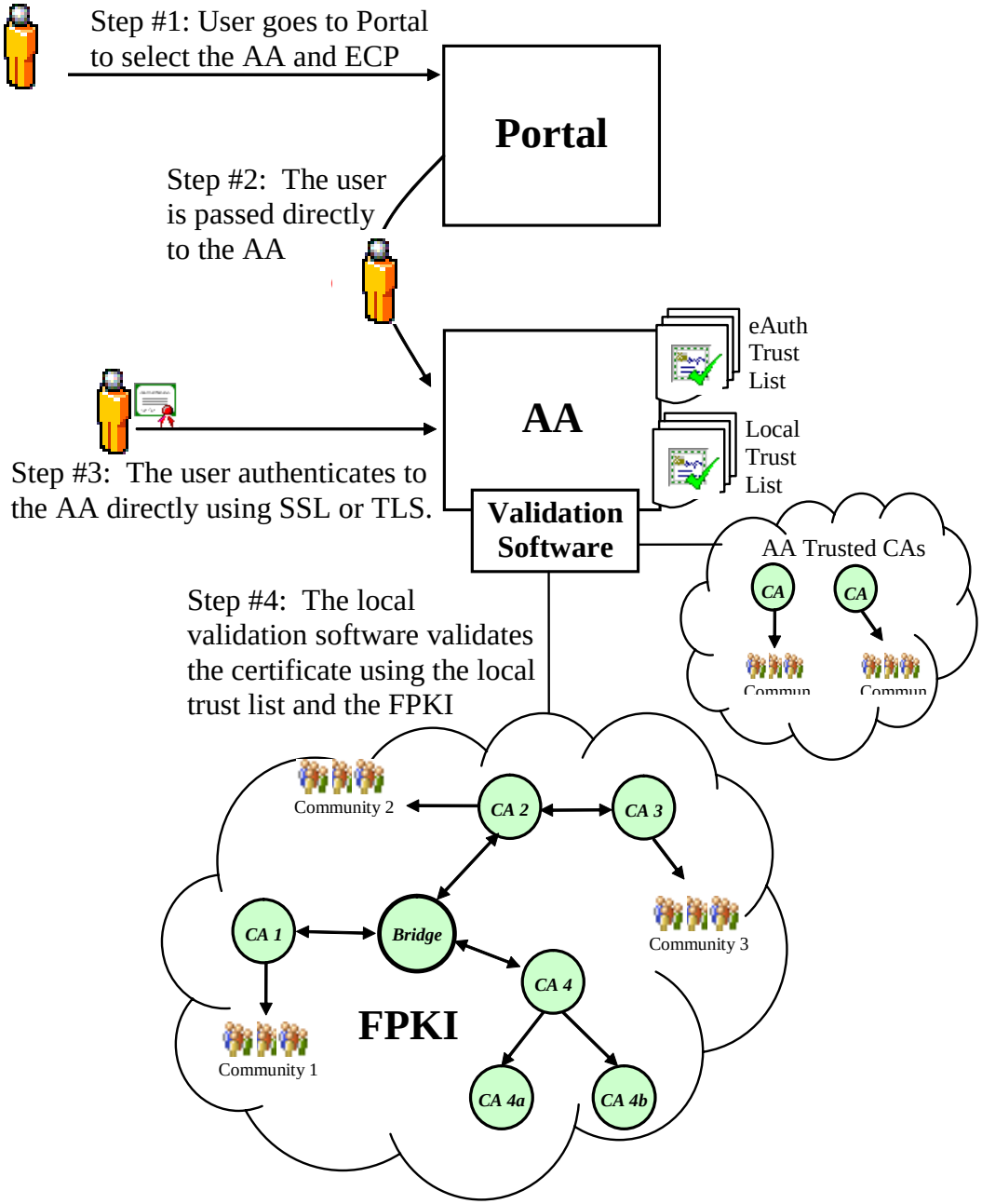
# *Agenda*

- ✓ Architecture Working Group
- ➢ Baseline Architecture
  - ✓ Assertion Based (1,2)
  - ➢ Certificate Based (3,4)
- • Changes coming in the FOC

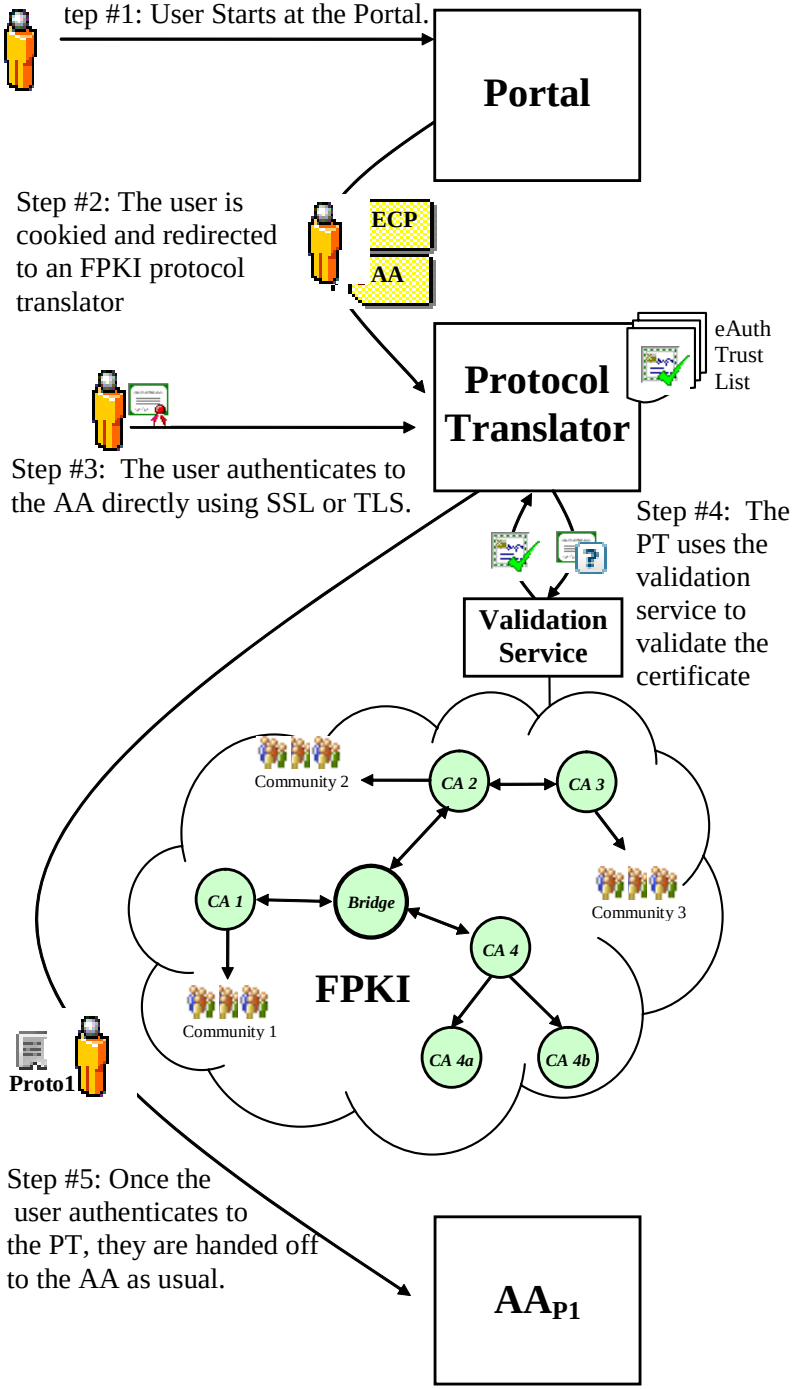
# Validation Service



# Local Validation



# Certificates At Lower Assurance Applications



# *Agenda*

- ✓ Architecture Working Group
- ✓ Baseline Architecture
- ➢ Changes coming in the FOC
  - ➢ Summary
  - • FEA Alignment
  - • Refinements
  - • Email
  - • Forms

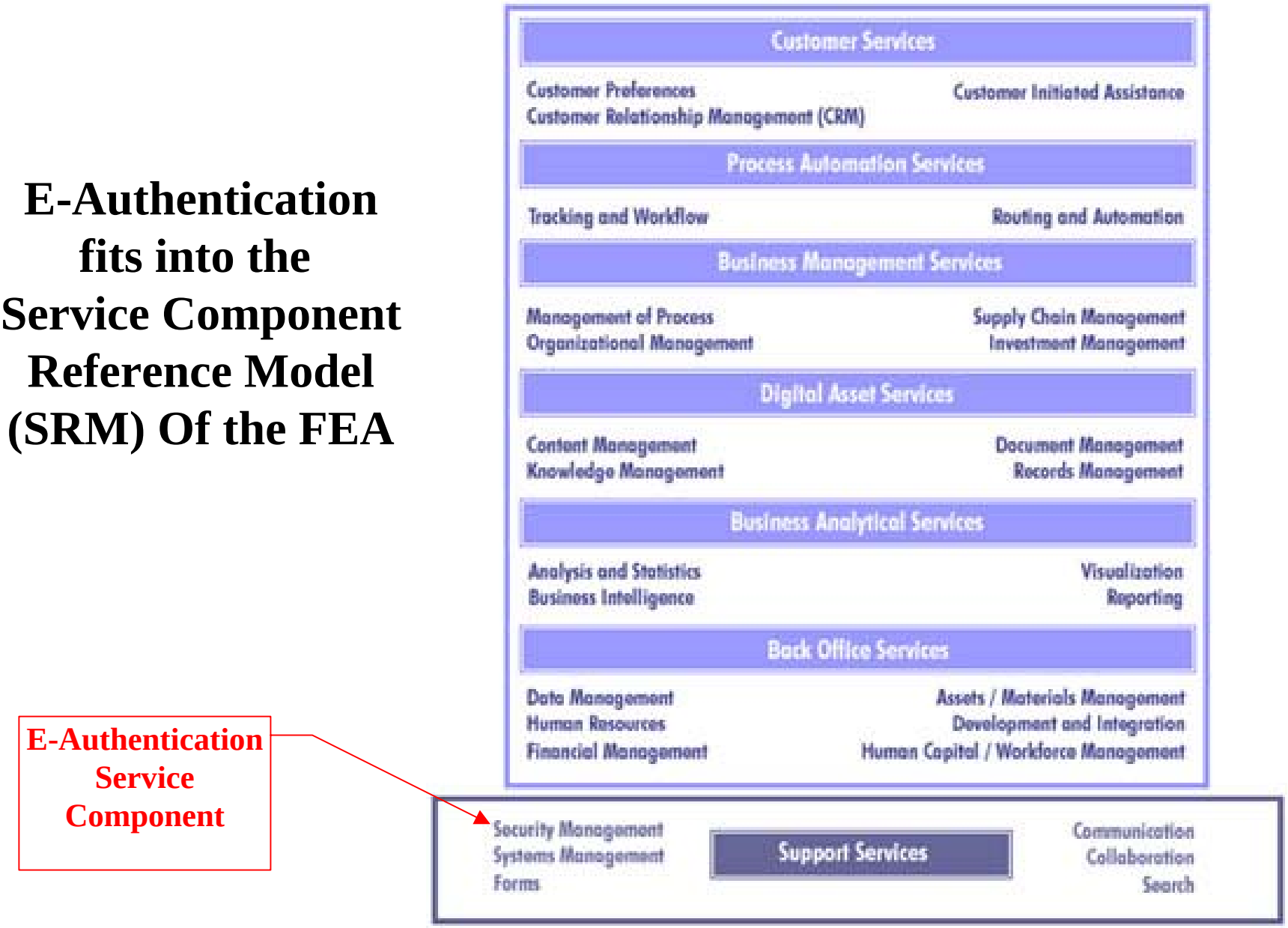
# ➢*Summary of FOC Changes*

- New Name: E-Authentication Service Component
- Clarified relationship to the FEA
- A Refinement of the Baseline Approach
  - Not a new architecture
- New Appendix on Email
- New Appendix on Forms

# *Agenda*

- ✓ Architecture Working Group
- ✓ Interim Architecture
- ➢ Changes coming in the FOC
  - ✓ Summary
  - ➢ FEA Alignment
  - • Refinements
  - • Email
  - • Forms

# E-Authentication fits into the Service Component Reference Model (SRM) Of the FEA

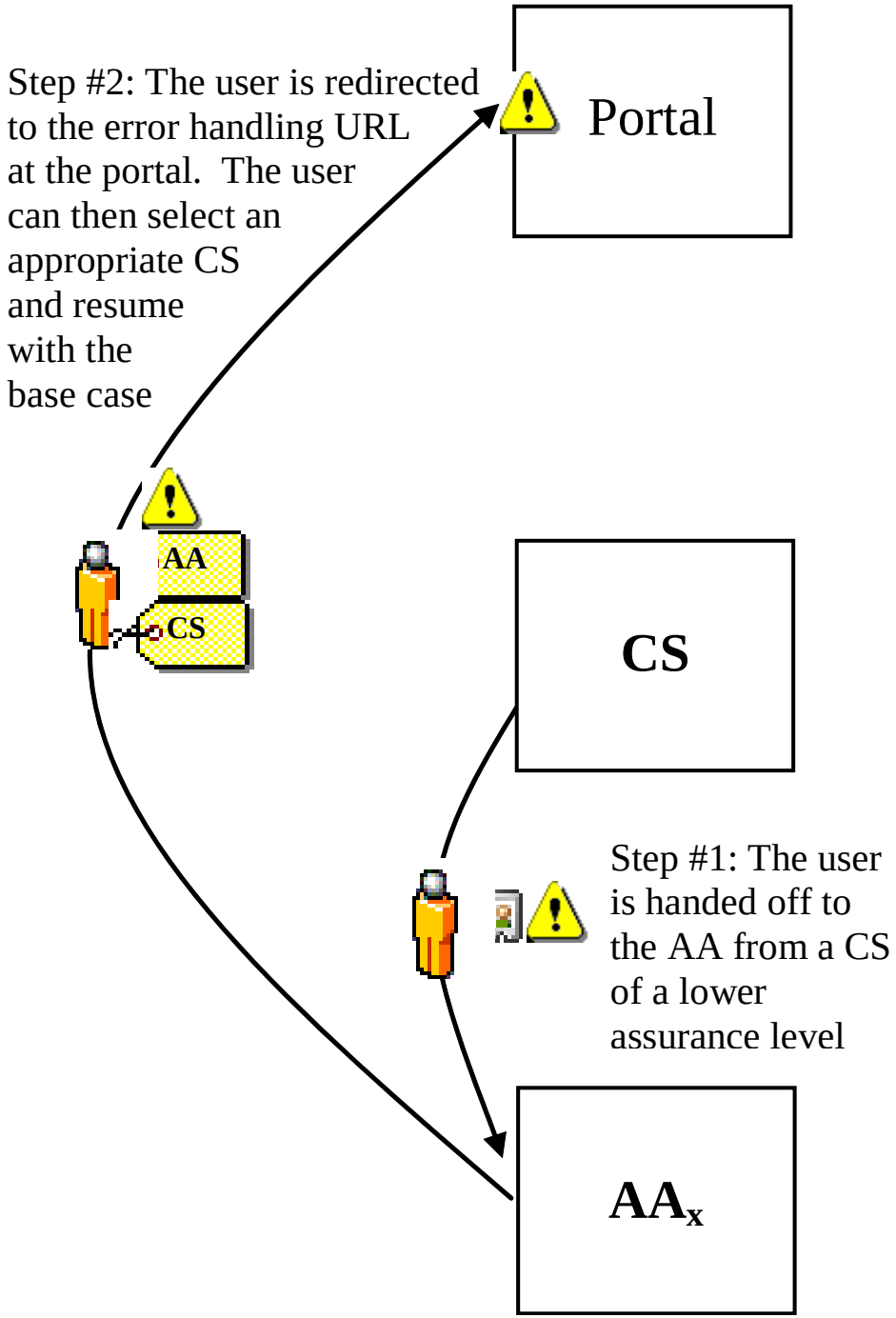



See http://www.feapmo.gov/

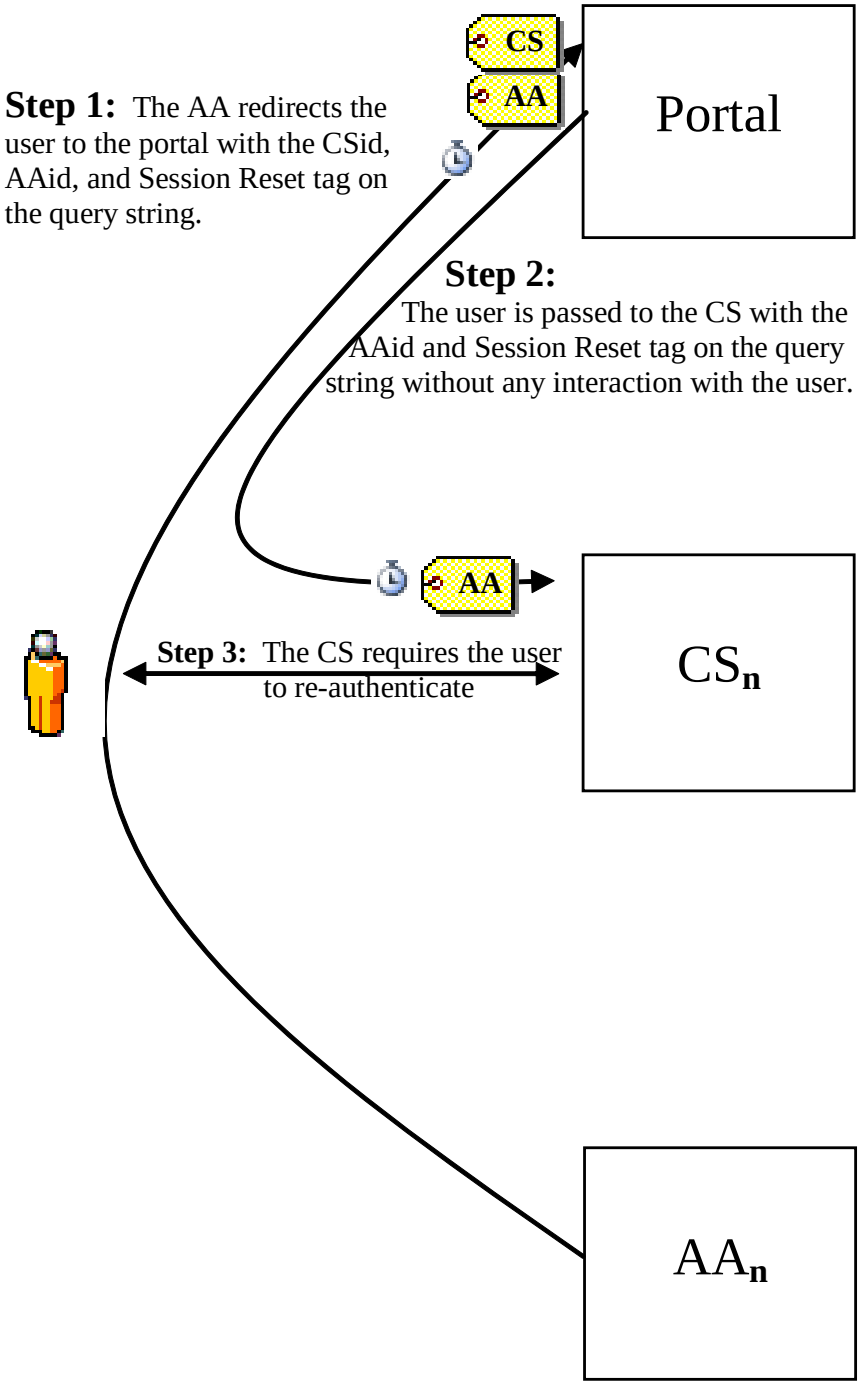
# *Agenda*

- ✓ Architecture Working Group
- ✓ Interim Architecture
- ➢ Changes coming in the FOC
  - ✓ Summary
  - ✓ FEA Alignment
  - ➢ Refinements
    - Email
    - Forms

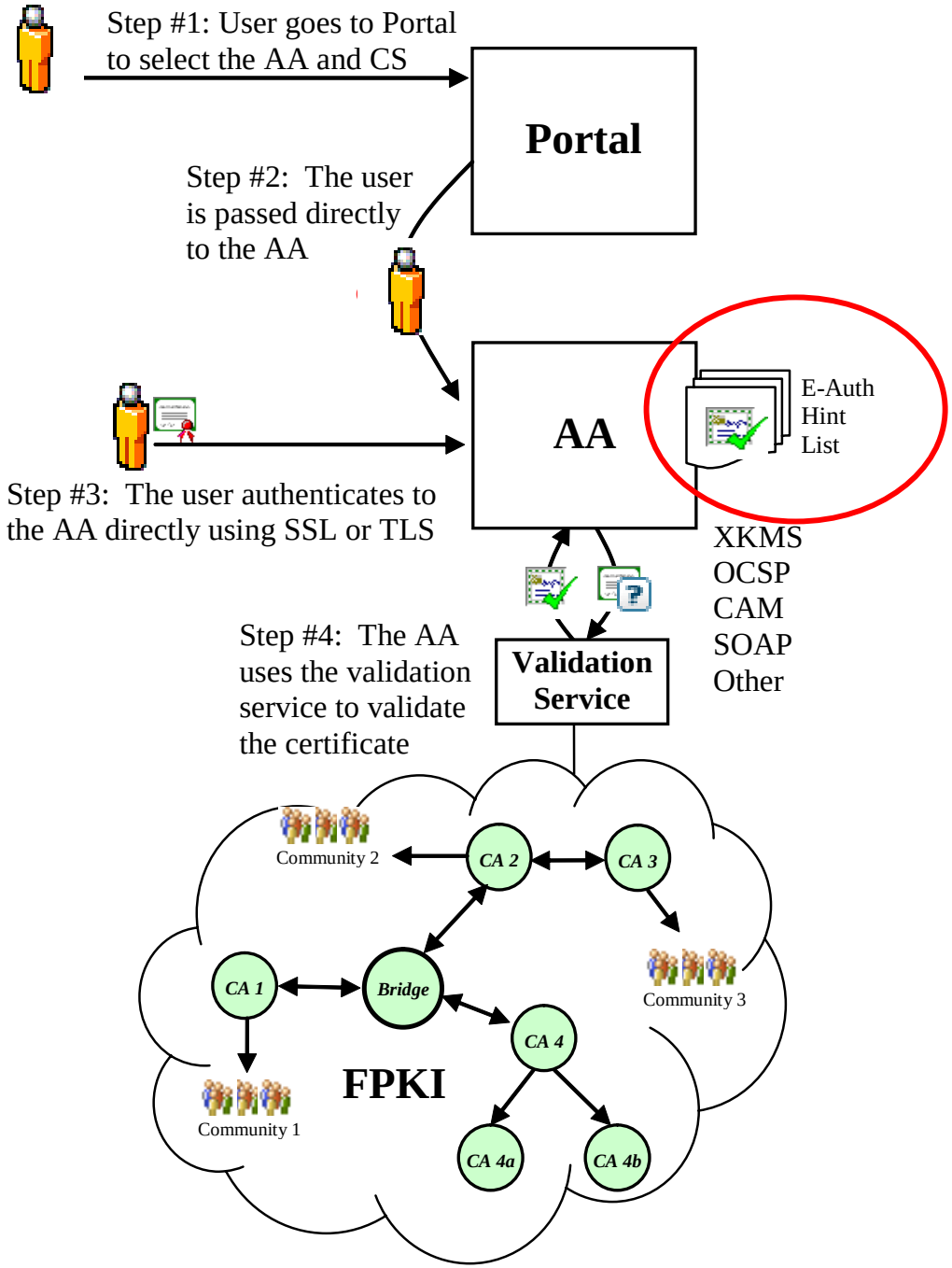
# Exception Fail-Safe



# Session Reset Support



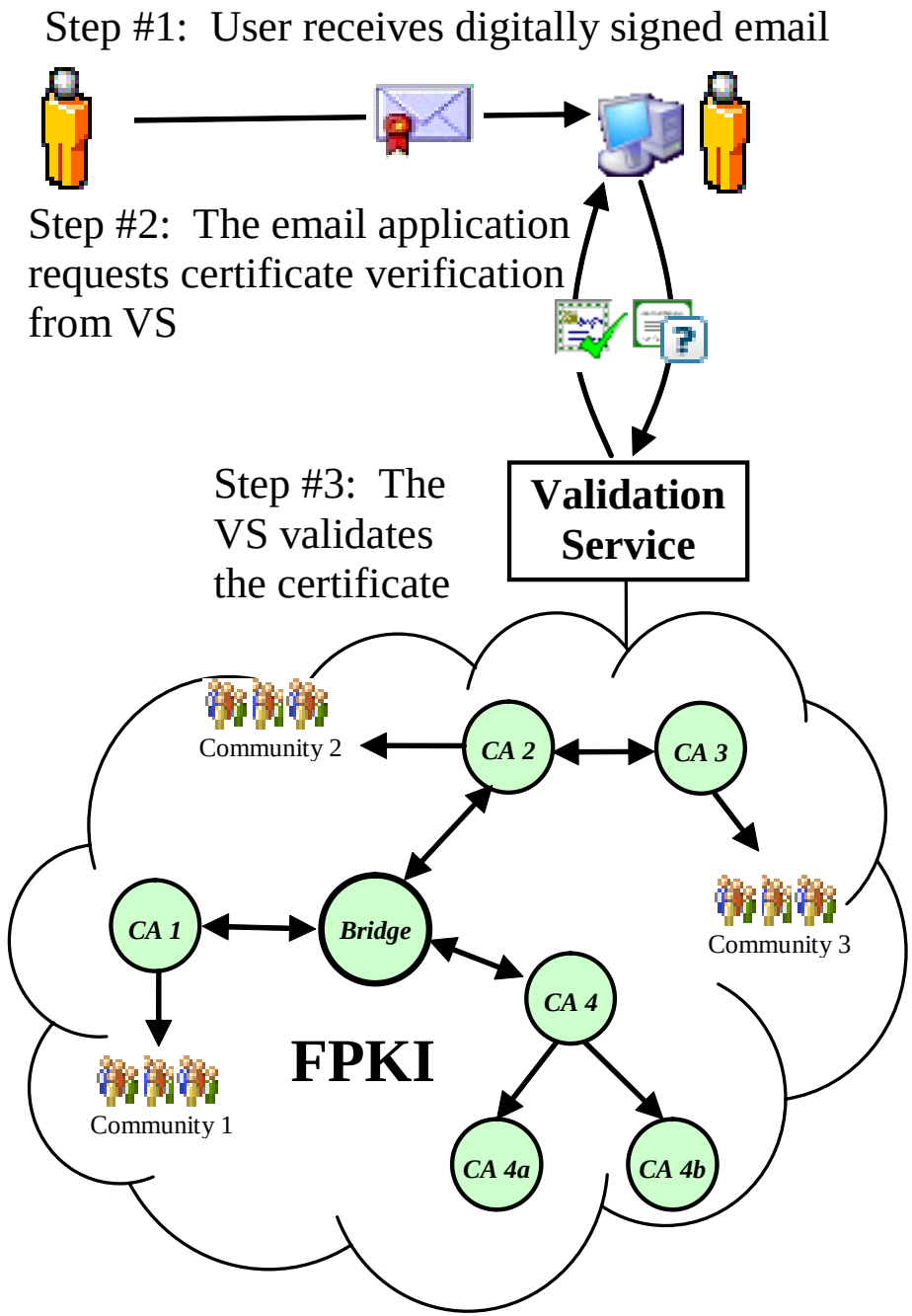
# "Hint List" metaphor



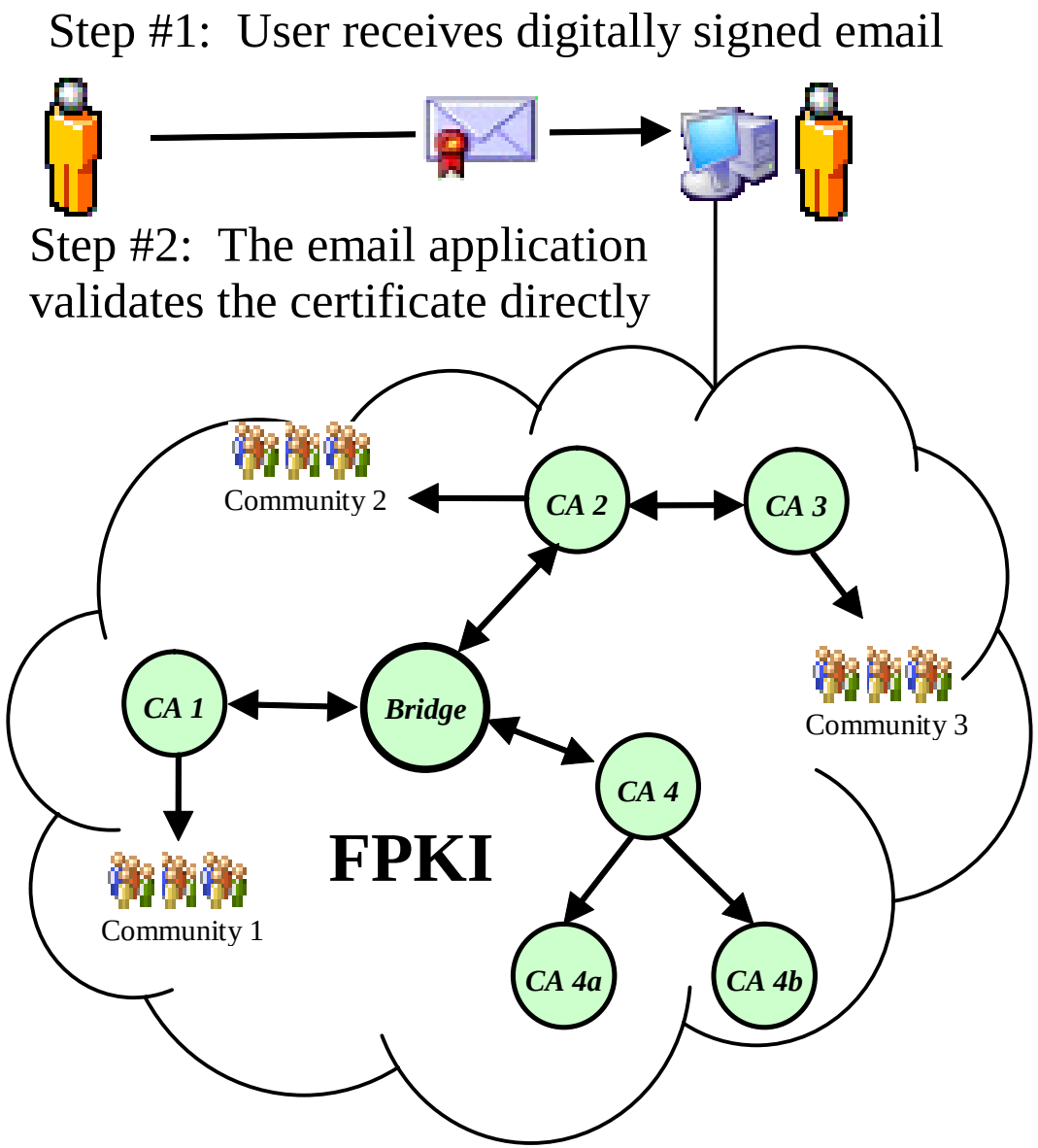
# *Agenda*

- ✓ Architecture Working Group
- ✓ Interim Architecture
- ➢ Changes coming in the FOC
  - ✓ Summary
  - ✓ FEA Alignment
  - ✓ Refinements
  - ➢ Email
  - • Forms

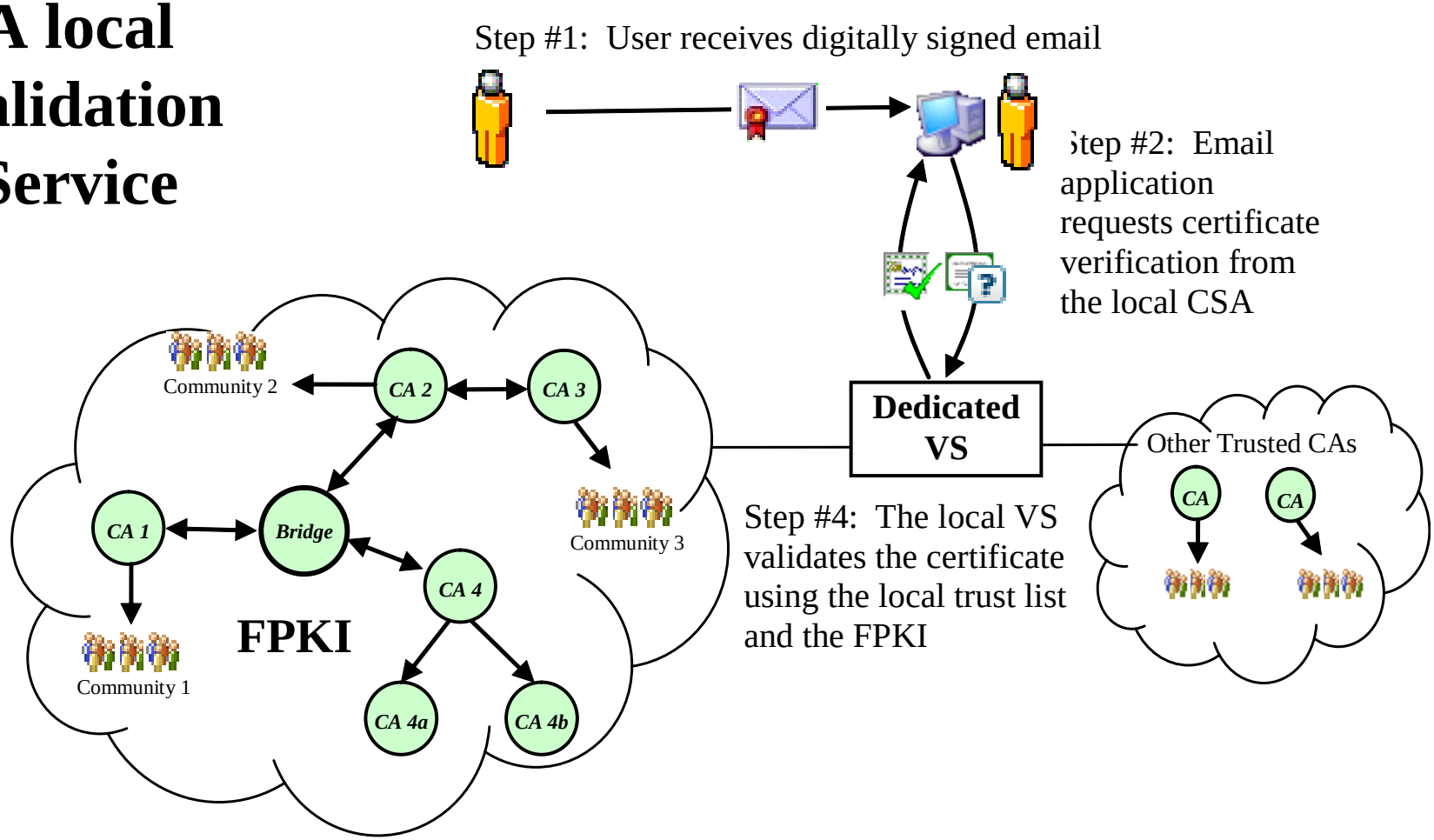
# Email with Validation Service



# Email with Desktop Validation



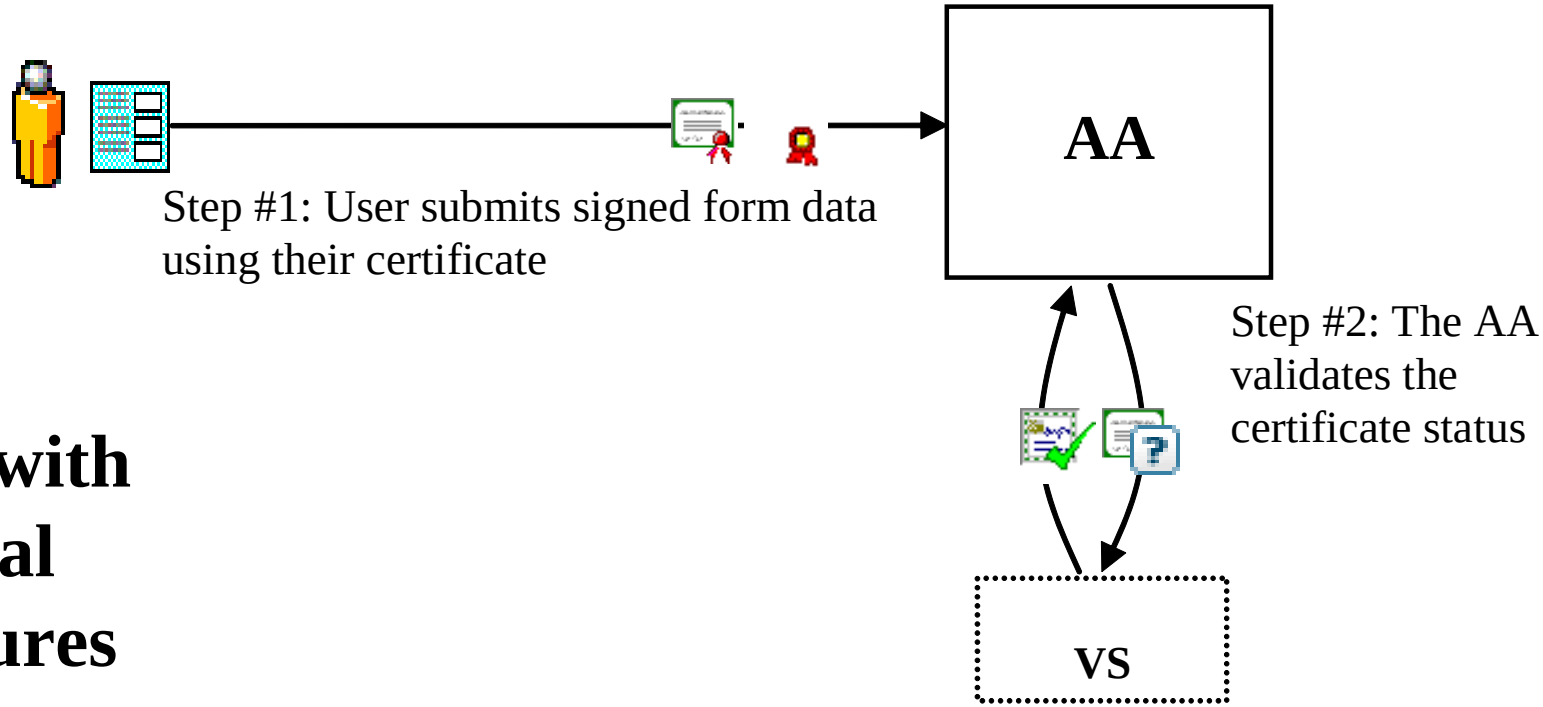
# Email with A local Validation Service



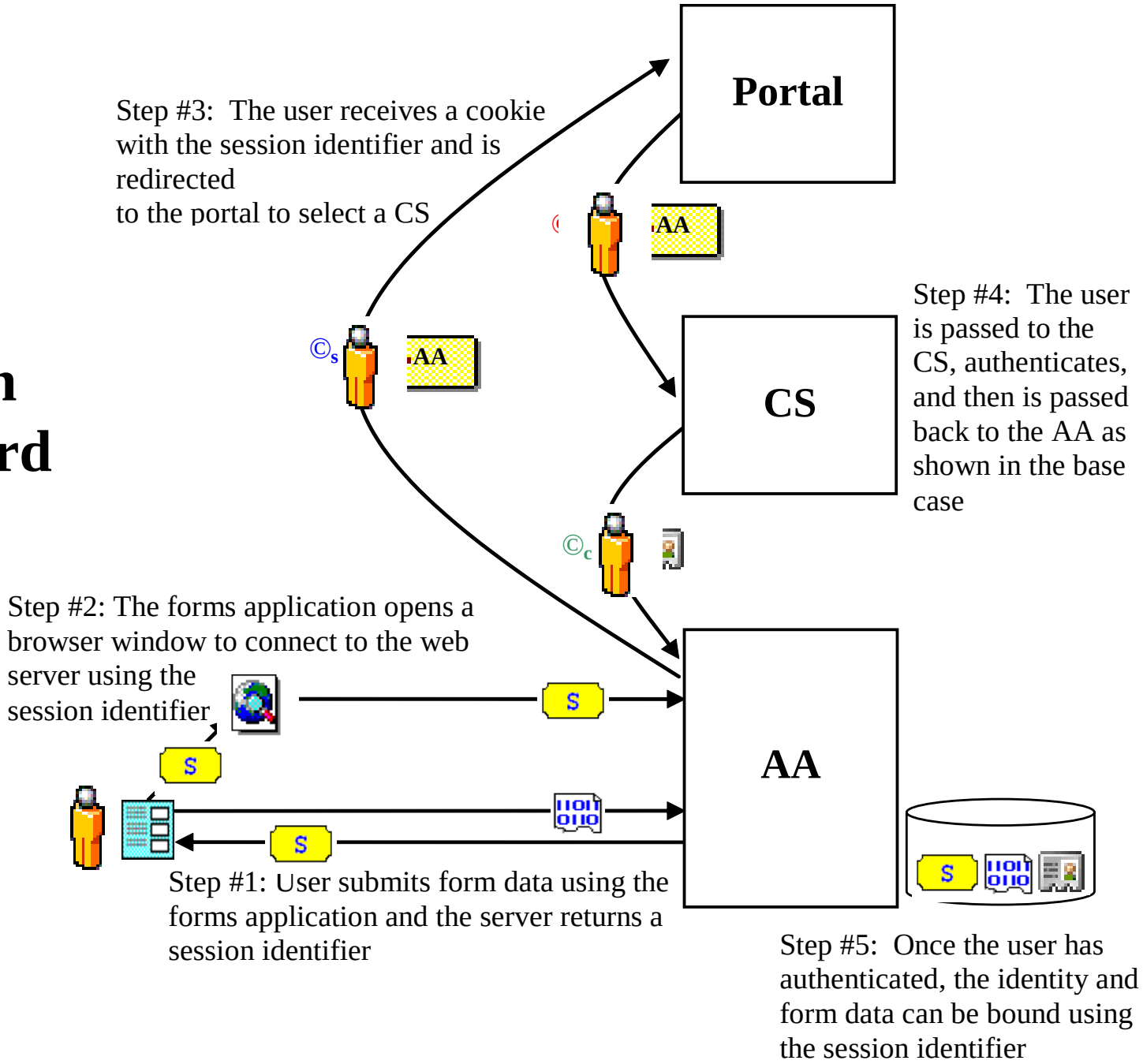
# *Agenda*

- ✓ Architecture Working Group
- ✓ Interim Architecture
- ✓ Changes coming in the FOC
  - ✓ Summary
  - ✓ FEA Alignment
  - ✓ Refinements
  - ✓ Email
  - ➢ Forms

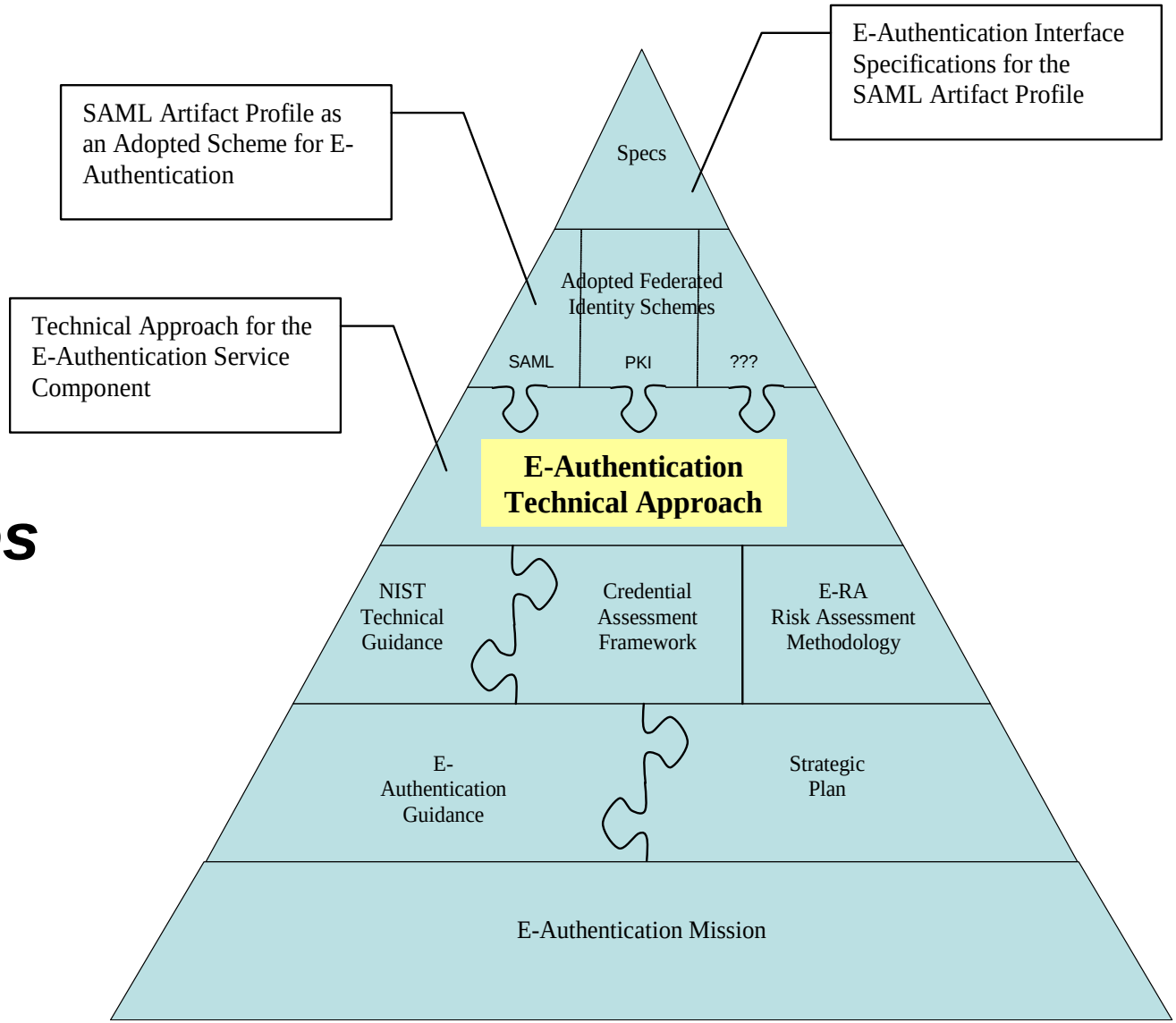
# Forms with Digital Signatures



# Forms with PIN/Password



## ➢ *Resources*




http://www.cio.gov/eauthentication/

- ***Questions***