



Federal CIO Council  
Information Security and Identity Management Committee

# Identity, Credential, and Access Management

BAE v2 and Attribute Governance  
WIS3 Panel  
12/5/11

Chris Loudon  
Protiviti Government Services  
[chris.louden@pgs.protiviti.com](mailto:chris.louden@pgs.protiviti.com)



# Identity, Credential, and Access Management

## Agenda

- Concepts
- BAE v2
  - Background
  - Drivers
  - Document Suite
  - Summary
- Attribute Governance



## Identity, Credential, and Access Management

### Concepts

- Semantics (Meaning)
- Syntax (Formatting)
- Protocols (Delivery)
- Governance



## ICAM SC Backend Attribute Exchange (BAE)

### ➤ BAE addresses

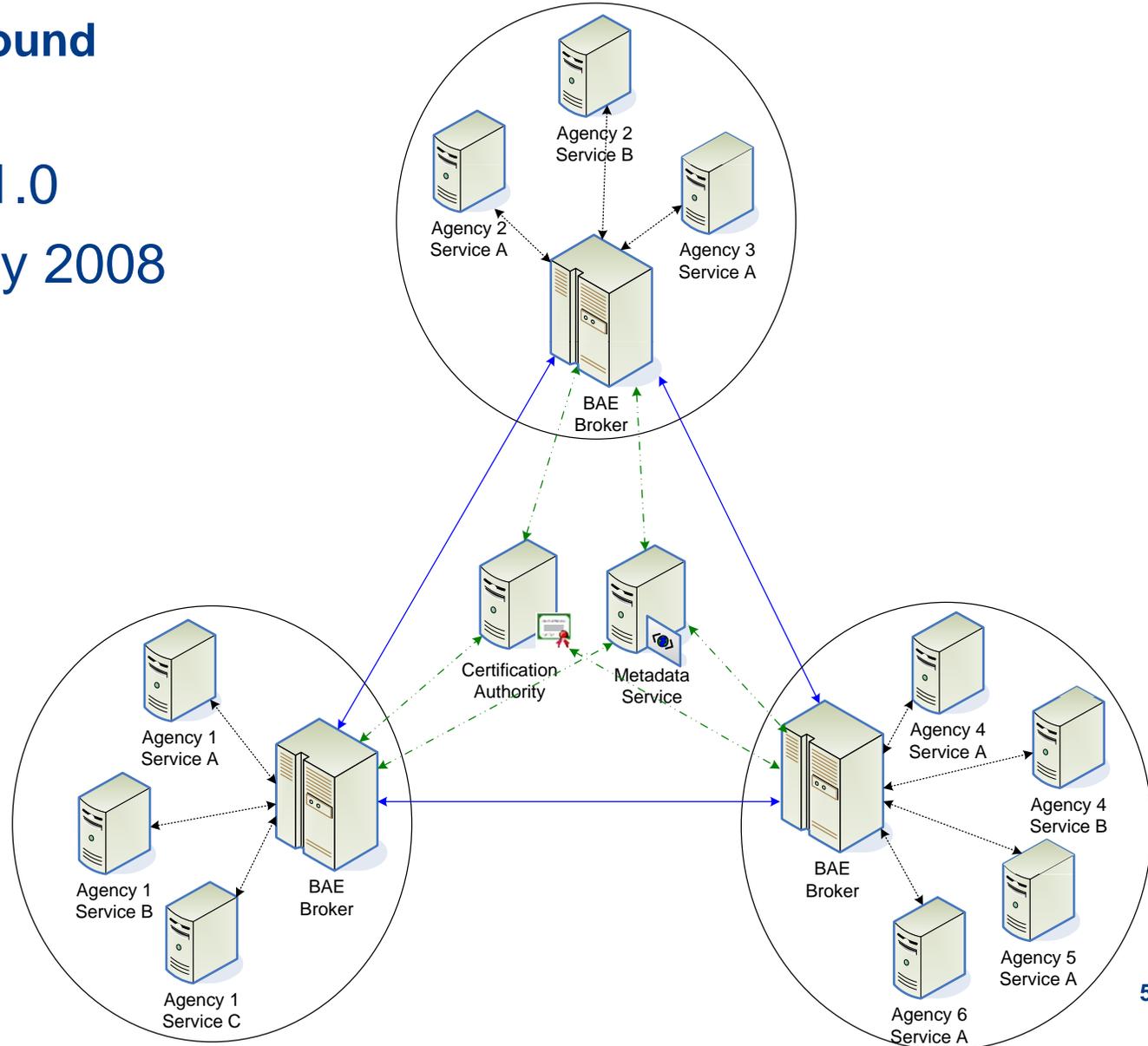
- Protocols for “back channel” delivery
- (Protocols for “front channel” delivery in ICAM SAML Profile)
- Guidance on semantics, syntax, and governance, but currently left to individual Communities of Interest (COI)



# Identity, Credential, and Access Management

## BAE v2 Background

BAE Version 1.0  
completed May 2008





## Identity, Credential, and Access Management

### **BAE v2 Background**

- DHS Pilot completed
- PIV-I Policy completed



## Identity, Credential, and Access Management

### BAE v2 Drivers

- Incorporate lessons learned from the DHS Pilot
  - technical details from real world use
  - lessons from COTS products
- Account for emergence of PIV-I
  - shift from FASCN identifier to a more flexible model
- Update attribute naming and semantics
  - align with work done in other groups
- Address Governance Details
  - How to find trusted Brokers...
  - Knowing whether to trust a Broker...



## Identity, Credential, and Access Management

### BAE v2 Document Suite

- **Overview** – architecture, choreography, use cases, etc.
  - Completed and posted to [IDManagement.gov](http://IDManagement.gov)
- **SAML Profile** – BAE for one specified individual
  - Completed and posted to [IDManagement.gov](http://IDManagement.gov)
- **SPML Profile** – BAE for a batch of specified individuals
  - Being worked through the DHS S&T lab. Will incorporate as applicable.
- **Metadata Profile** – Broker information
  - Completed and posted to [IDManagement.gov](http://IDManagement.gov)
- **Governance** – Rules, Trust, Management
  - Completed and posted to [IDManagement.gov](http://IDManagement.gov)



## Identity, Credential, and Access Management

### BAE v2 Summary

- Overview and Architecture did not change significantly
- The DHS Pilot substantially matured the technical specifications
  - did not fully exercise SPML used for data synchronization
- Governance requires new work
- Basic set of agreed-upon attributes is needed for BAE to be usable between entities



# Identity, Credential, and Access Management

## Agenda

- ✓ BAE v2
- Attribute Governance



## Identity, Credential, and Access Management

### **Attribute Governance – Access Control Attribute Governance WG**

- **New ICAM SC working group to be established: ACAG WG**
  - Focused on Governance, coordination of semantics, syntax, protocol work
- **ACAG WG coordinate a common language and understanding of access control attributes across the federal government (alignment with NIEM)**
- **Membership to be coordinated through ICAM SC Members**



# Identity, Credential, and Access Management

**Questions?**