Backend Attribute Exchange (BAE) v2.0 Overview

Final Version 1.0.0

January 23, 2012

Acknowledgments

The authors of this document, the Identity, Credential and Access Management (ICAM) Architecture Working Group (AWG), would like to acknowledge the work done by DHS Science & Technology Directorate and DOD DMDC West.

Table of Contents

Tables

Figures

1 Introduction

1.1 Background

A Relying Party (RP) may require information about an Attribute Subject directly from an authoritative source rather than from the Attribute Subject's Authentication Credential (e.g., PIV Card, PIV-I Card).[1] Reasons for this include, but are not limited to (1) the information is not available from the Authentication Credential, and (2) information available from the Authentication Credential needs to be verified. Uses include, but are not limited to Authentication Credential tamper detection, attribute-based access control (ABAC) decisions, provisioning in advance of access to meetings at other agency locations, and dealing with an employee or contractor medical emergency. By obtaining Attribute Subject information directly from an authoritative source rather than from the Authentication Credential, the RP gains benefits such as:

1. Enhanced detection of Authentication Credential tampering;
2. Enhanced access control and management; and
3. Enhanced response capabilities (e.g., first responder).

Accordingly, the federal government requires a standard mechanism for RPs to obtain Attribute Subject information directly from the authoritative source (Attribute Authority). The authoritative source is the Issuing Agency, which is the agency that issued the Authentication Credential to the Attribute Subject[2].

Backend Attribute Exchange (BAE) describes a process by which an RP obtains attribute information (Backend Attributes) about a claimant through a direct connection to an attribute source (attribute provider) – in contrast to a front-channel attribute delivery where the claimant is directly involved in the process, typically as part of the authentication event[3]. BAE can be used in physical access control and logical access control situations. Access to Backend Attributes is either in real-time when immediately needed (e.g., guard suspects Authentication Credential tampering at physical access

[1] The focus of BAE is authenticated Subjects, not their Authentication Credentials per se. The BAE document suite discusses several ways to identify an Attribute Subject, but does not preclude other ways.
[2] Note that the attribute contract may not be completely fulfilled by the issuing agency, but rather could be aggregated by the issuing agency from various other sources that own some or all the attributes. For example, certification of training as an attribute may be maintained by the training certification organization.
[3] BAE was previously known as "Backend Authentication".

time), or in advance of need (e.g., provisioning access to a scheduled meeting, loading a handheld device prior to field use). For a discussion of the larger identity management ecosystem in which BAE exists, see [FICAM Roadmap].

1.2 BAE Overview

BAE is a standards-based architecture and interface specification to securely obtain attributes of subjects (e.g., PIV Cardholders, federation members), from authoritative sources, to make access control decisions and/or to do provisioning. The BAE is designed to support any community-defined attribute contract; as such, an agency could use this approach to exchange a wide variety of identity attributes in support of improved identity life cycle management.[4] [BAEv2 SAML] and [BAEv2 SPML] are the normative specifications for BAE.

Specifically, BAE is the exchange of Attribute Subject information in a secure and trusted environment between an Attribute Authority (AA) and an RP. BAE is designed to work with Authentication Credentials that contain a unique Identifier such as the PIV Card that contains a Federal Agency Smart Credential Number (FASC-N), and the PIV-I Card that contains a Universally Unique Identifier (UUID)[5]. There are two BAE models and corresponding interface specifications that can be implemented:

1. **Single Subject, Real-time Query Model** – Security Assertion Markup Language (SAML) based exchange of Backend Attributes for one Attribute Subject per request/response pair.
2. **Multiple Subject, Occasionally-connected Query Model** – Service Provisioning Markup Language (SPML) based exchange of Backend Attributes for multiple Attribute Subjects per request/response pair.

A federal agency may use one or both BAE models, as circumstances dictate. The basic principles and objectives are the same for each BAE model. The RP obtains all requested Backend Attributes from the AA via BAE Brokers, even those Backend Attributes that may already be stored on-card. The AA is the Authentication Credential Issuer and authoritative source for its Credential-holder information. The RP initiates a Backend Attribute request. An Authentication Credential may or may not be present when the request is made, depending upon the use case. Backend Attributes include

[4] [FICAM Roadmap].
[5] Any federation operator can define their own subject Identifiers.

but are not limited to Attribute Subject photograph, Attribute Subject fingerprints, Attribute Subject emergency contact information, Attribute Subject security clearance level, and Attribute Subject emergency responder capabilities. The RP uses returned Backend Attributes as necessary, including but not limited to:

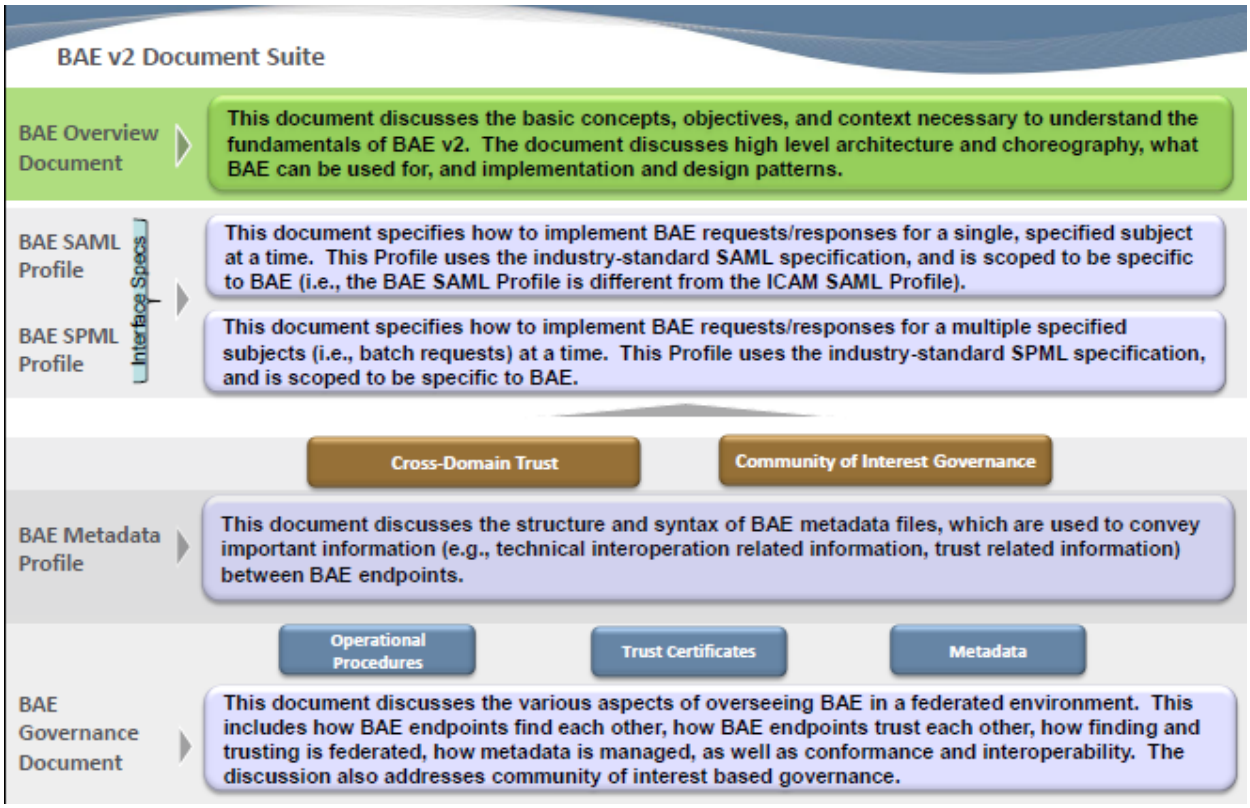
1. Attribute-based Access Control (ABAC);
2. Authentication Credential tamper detection;
3. Provisioning (e.g., in advance of access to meetings at other agency locations);
4. Enhancing response capabilities (e.g., first responders); and
5. Dealing with an employee or contractor medical emergency.

1.3 Objective and Audience

Version 2 of the BAE specification has been developed as a suite of five stand-alone documents to modularize the specification. This will enable more straightforward modification of segments of the specification as technologies and standards at large as well as related federal specifications evolve. The document suite's primary objective is to provide comprehensive guidance on how to implement and use BAE in a secure, federated, trusted manner. Some documents (in part or in whole) in the suite are normative (e.g., interface specifications), while others are informational or guidance (e.g., governance).

Figure 1-1 summarizes the documents in the BAE suite, and shows them in relation to one another. A Data Attribute Catalog is also being developed, but is out of scope here. As the Catalog is relevant to BAE, the Catalog should be reviewed.

Figure 1-1 BAE v2 Document Suite



1.4 Scope

This document suite defines the end-to-end architectural model and interface specification for inter-agency exchange of Backend Attributes. The exchange is ultimately between RP and AA systems. Scope is limited to explaining the two BAE models and defining each model's interface specification.

BAE interface specifications are limited to defining technical interoperation between agency communications conduits called BAE Brokers (see Section 4.1.4.1).

This document suite addresses BAE governance, trust, and privacy matters in [BAEv2 Governance]. BAE security details are discussed in [BAEv2 SAML] and [BAEv2 SPML].

This document suite does not supersede or contradict any existing National Institute of Standards and Technology (NIST) publication, and should be used in conjunction with existing policies and procedures – particularly [NIST 800-47] and its guidelines for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.

1.5 Authority

The Identity, Credential, and Access Management Sub Committee (ICAMSC) Architecture Working Group (AWG) developed this document suite on behalf of the Office of Governmentwide Policy (OGP) and the HSPD-12 Executive Steering Committee in furtherance of their charter to implement HSPD-12 from a “national” perspective.

2 BAE Business Goals and Assumptions

2.1 BAE Business Goals

BAE addresses the following high-level business requirements:

- **Scope of Functionality:** BAE provides federal agencies with a mechanism to access the Backend Attributes from other agencies to facilitate access control decisions and help manage emergency situations, among other uses.
- **Privacy Protection**: Privacy and confidentiality of Backend Attributes are protected.
- **Policy Compliant**: BAE complies with applicable policy framework requirements (e.g., [NIST SP 800-95], [HSPD-12]).
- **Service Transaction Context**: BAE supports conditions where the Attribute Subject is present and not present.
- **Support for Smaller Agencies**: BAE supports use by smaller agencies. Smaller agencies are provided the opportunity to leverage existing BAE architectural components whether provided and run by other agencies or by shared services.
- **Quality of Service:** BAE is reliable, highly available, secure and auditable**.**
- **Types of Service:** BAE provides different kinds of service to support single and batch requests.
- **Open Data Model:** BAE allows the defined set of Backend Attributes to be modified over time, to support agencies needs. Agencies are able to request Backend Attribute table modifications on a per-BAE-release basis.
- **Balanced Approach**: To facilitate government-wide BAE adoption, a proper balance is achieved between convenience (i.e., ease of implementation, use, and maintenance) on the one hand, and security and privacy on the other.
- **Cost-effective**: BAE is financially viable to implement and maintain.
- **Standards-based**: BAE relies on existing industry standards while remaining aware of emerging standards.
- **Distributed, Brokered Trust Relationships**: BAE is based on distributed trust domains with relationships managed by the ICAMSC.
- **Flexibility**: BAE supports various communities of interest beyond federation partnerships between federal organizations. In addition to permitting interaction with non-federal credentials (PIV-I Cards issued by state and local governments and private sector organizations), federation partners are empowered to modify governance and trust models as appropriate for the partnership.

2.2 BAE Business Assumptions

BAE makes the following high-level business assumptions:

- **Governance**: Governance for BAE will be provided to control who is allowed to participate in BAE, and to administer accreditation, provisioning, and configuration of any necessary trust relationships between participants.
- **Use of Information Received**: Agencies can use Backend Attributes in any way consistent with federal privacy and security guidelines in general, and their agency's privacy and security requirements and guidelines in particular.
- **Authentication Credential Validation**: If an Authentication Credential is present, the RP will validate Authentication Credential certificates when conducting a BAE transaction.
- **Identification of Attribute Subject**: Identification of the Attribute Subject and the authoritative source for their Backend Attributes will be based on the Authentication Credential identifier (e.g., PIV Card FASC-N and the organization code contained within the FASC-N).
- **Attribute Authorities**: For initial deployment, AAs are Authentication Credential Issuers.
    - AAs have the information necessary to support all mandatory Backend Attributes.
    - Future BAE versions will likely support other types of AAs.

3 Attribute Exchange Design Patterns

A Relying Party (RP) may require identity and authorization information (attributes) directly from authoritative sources (backend systems) for purposes including, but not limited to access decisions, provisioning, and dealing with an employee or contractor medical emergency. Accordingly, the federal government requires a standard mechanism for RPs to obtain attributes directly from the authoritative source. This exchange of Attributes between backend systems is known as “Backend Attribute Exchange” (BAE) and is conducted between servers called **BAE Brokers**.

As noted in Section 2.1, the BAE Architecture itself must support the following two business requirements:

1. “BAE MUST provide federal agencies with a mechanism to access the Attributes from other agencies to facilitate access control decisions and help manage emergency situations, among other uses.”
2. “BAE MUST support use by smaller agencies. Smaller agencies SHOULD be provided the opportunity to leverage existing BAE architectural components (like BAE Brokers) whether provided and run by other agencies or by shared services."

Within the context of the BAE architecture, the profiles therefore support two distinct patterns of attribute exchange to satisfy the above two business requirements.

- Direct Attribute Exchange via the implementation of an **Organizational Query Pattern**, in which two agencies with BAE Brokers have the ability to exchange attributes. In this case, the **Ultimate Requester** and the **Ultimate Responder** are the same as each Agency’s respective BAE Brokers.
- Brokered Attribute Exchange via the implementation of a **Single Point of Query Pattern**, in which a smaller agency is leveraging the BAE Broker Infrastructure established by a larger agency for participating in the BAE environment. In this case, the **Ultimate Requester** could be the smaller agency, which is utilizing the BAE Broker of a larger agency on the Requester side, and the **Ultimate Responder** could be a smaller agency utilizing the BAE Broker on the Responder side.

The scope of this document is limited to profiling the message exchange between the BAE Brokers and the associated metadata in both of the above cases, but a guiding intent behind this profile is to assure that the profiled message exchange contains enough information to satisfy both of the above attribute exchange scenarios.

3.1 Describing an Attribute Service using Design Patterns

To set the context for further discussion it is important to define the parts of what make up an “Attribute Service”.

From a technical perspective, an Attribute Service is typically composed of three components:

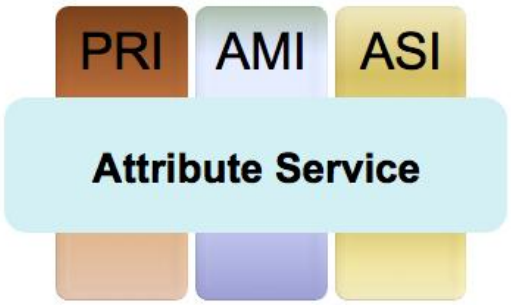
- Interface(s)
- Business Logic for directing and returning inquires
- Connectivity to Authoritative Attribute Sources

Interface(s) define how one interacts with the Attribute Service. Business Logic defines how the Attribute Service handles routing, metadata lookup etc. while Connectivity to Attribute Sources allow the Service to leverage trusted attributes sources.

Within the context of the BAE Architecture, it is important to further define the interfaces that are supported by a BAE Broker as some of those interface descriptions are governed by Federal ICAM requirements while others are left up to individual agencies as to its implementations.

An Attribute Service has three primary interfaces:

Figure 3-1 Attribute Service Primary Interfaces

PRI – A Protected Resource Interface AMI – Attribute Management Interface ASI – Attribute Service Interface	

A **Protected Resource Interface (PRI)** is the mechanism by which an Application or Relying Party, within Organization, queries for the attributes of a Subject. This interface is under the control of the organization and is typically driven by the capabilities of the Relying Party Application. Examples of such interfaces include a SAML Attribute Query, LDAP(S) Query as well as more generic SOAP or REST based interfaces.

An **Attribute Management Interface (AMI)** is currently defined to be the mechanism by which the Attribute Service connects to Authoritative Attribute Sources. In the future, this interface may also provide Attribute Management functionality. Examples of such an interface include LDAP(S), SQL, and SPML.

An **Attribute Service Interface (ASI)** is the Federation and/or Community facing Interface of the Attribute Service which is used by an external Organization to query for the Attributes of a Subject. As such, this is a managed interface that is standardized to ensure interoperability. An interface that is compliant to the SAML 2.0 Profile of BAE is an example of an ASI.

3.2 Organizational Query Design Pattern

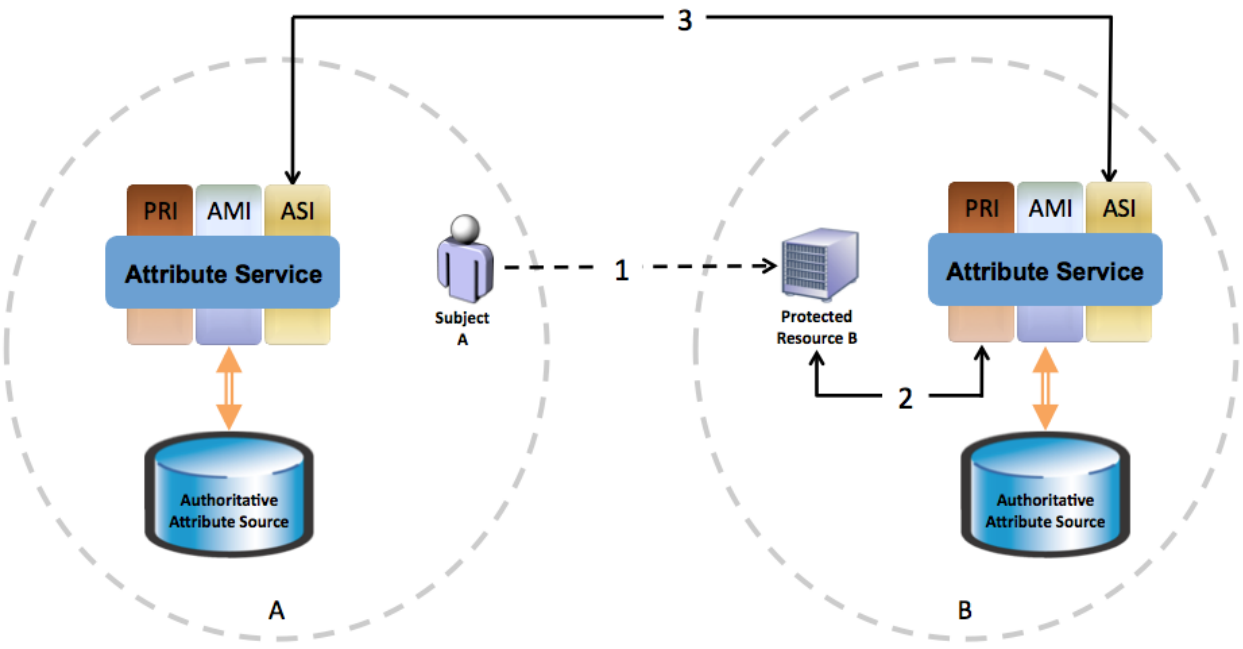
Context

- Subjects in an Organization require access to Protected Resources outside of the Organization.
- The Protected Resource has access to information (via validation of a credential or a trusted directory source) that allows it to obtain the Subject's **Locally Unique Identifier (LUID)** and the **Locale Identifier (LI)** of the Subject's Organization.
- The Organization is the authoritative source of attributes for its Subjects.

Forces

- Organization wants direct control over authoritative sources of attributes.
- Organization has the resources and capability to stand up a BAE Compliant Attribute Service.
- Organization wants direct control over the Federation facing interface (ASI) of the Attribute Service.
- Organization wants direct control over the Attribute Exposure of its membership.

Figure 3-2 Organizational Query Design Pattern Flow



1. Subject A attempts to gain access to Protected Resource B.
2. Protected Resource B, after obtaining the LUID of the Subject as well as the LI of Organization A, requests the attributes of Subject A by calling the Protected Resource Interface of Organization B's Attribute Service.
3. Attribute Service B translates the incoming request and routes it to Organization A via the managed Attribute Service Interface (ASI) to obtain the attributes of Subject A.

3.3 Single Point of Query Design Pattern

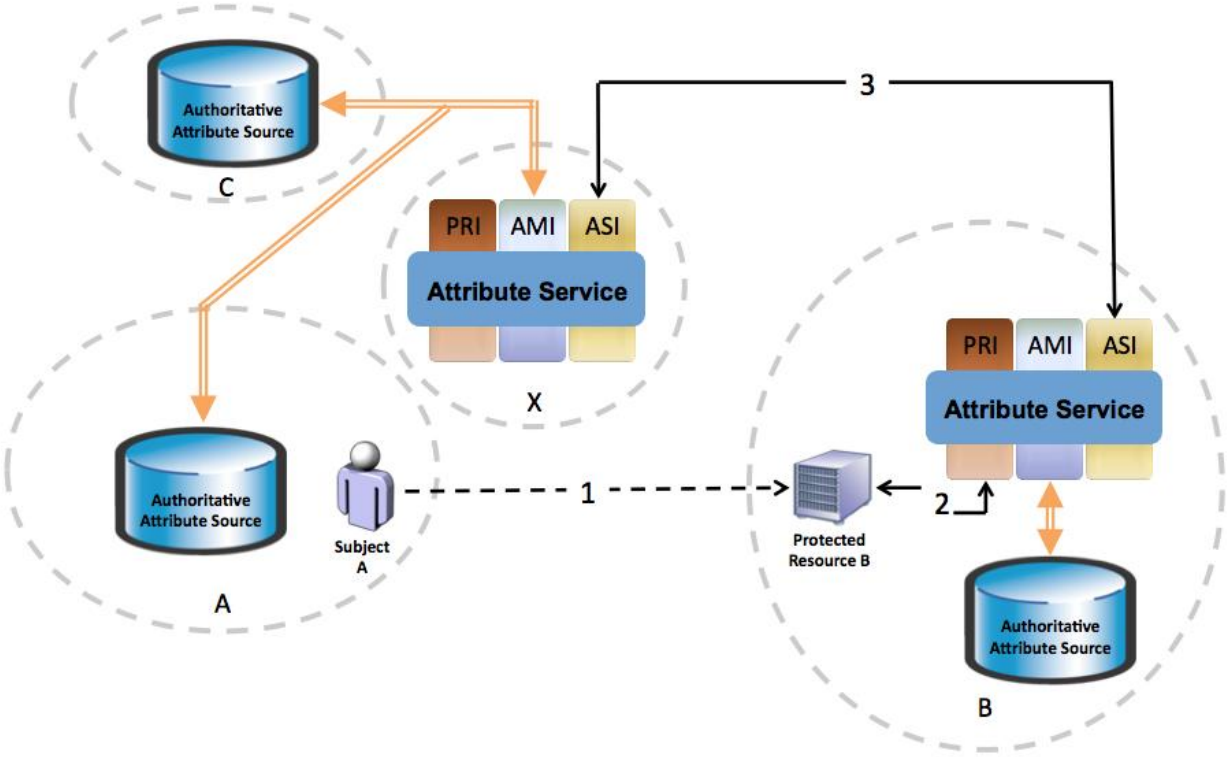
Context

- Subjects in an Organization require access to Protected Resources outside of the Organization.
- The Protected Resource has access to information (via validation of a credential or a trusted directory source) that allows it to obtain the Subject's **Locally Unique Identifier (LUID)** and the **Locale Identifier (LI)** of the Subject's Organization.
- The Organization is the authoritative source of attributes for its Subjects.

Forces

- Organization wants direct control over authoritative sources of attributes.
- Organization does not have the resources and capability to stand up a BAE Compliant Attribute Service.
- Organization does not need direct control over the Federation facing interface (ASI) of the Attribute Service.
- Organization is comfortable with negotiating the Attribute Exposure of its membership.

Figure 3-3 Single Point of Query Design Pattern Flow



1. Subject A attempts to gain access to Protected Resource B.
2. Protected Resource B, after obtaining the LUID of the Subject as well as the LI of Organization A, requests the attributes of Subject A by calling the Protected Resource Interface of Organization B's Attribute Service.
3. Attribute Service B translates the incoming request and routes it to Organization A via the managed Attribute Service Interface (ASI) to an Attribute Service managed by Organization X that has a business relationship with Organization A.

   Organization X's Attribute Service broker's the attribute request on behalf of Organization A and returns Subject A's attributes to Attribute Service B.

4 Attribute Exchange Pattern Implementations for BAE

The Federal ICAM Backend Attribute Exchange Implements the following design patterns:

- The **BAE Direct Attribute Exchange Model** is an implementation of the "Organizational Query Design Pattern" (see Section 3.2).
- The **BAE Brokered Attribute Exchange Mode**l is an implementation of the "Single Point of Query Design Pattern" (see Section 3.3).

In addition, the following also holds true regarding the BAE:

- The "External BAE Service" in the BAE Architecture is an implementation of the Attribute Service Interface (ASI) described in the patterns. The technical profiles regarding the implementation of this interface are described in Sections 4.1.4.1 and 4.1.4.1.1.
- The "Internal BAE Service" in the BAE Architecture is an implementation of the Protected Resource Interface (PRI). This interface implementation is left up to the discretion of agency implementations.

Figure 4-1 illustrates the BAE Direct Exchange Model. Figure 4-2 illustrates the BAE Brokered Attribute Exchange Model. The Figures are not meant to be the only way to implement a BAE Direct and Brokered exchange models. Detailed discussion and process flows for the models can be found in [BAEv2 SAML] and [BAEv2 SPML].

Figure 4-1 BAE Direct Attribute Exchange

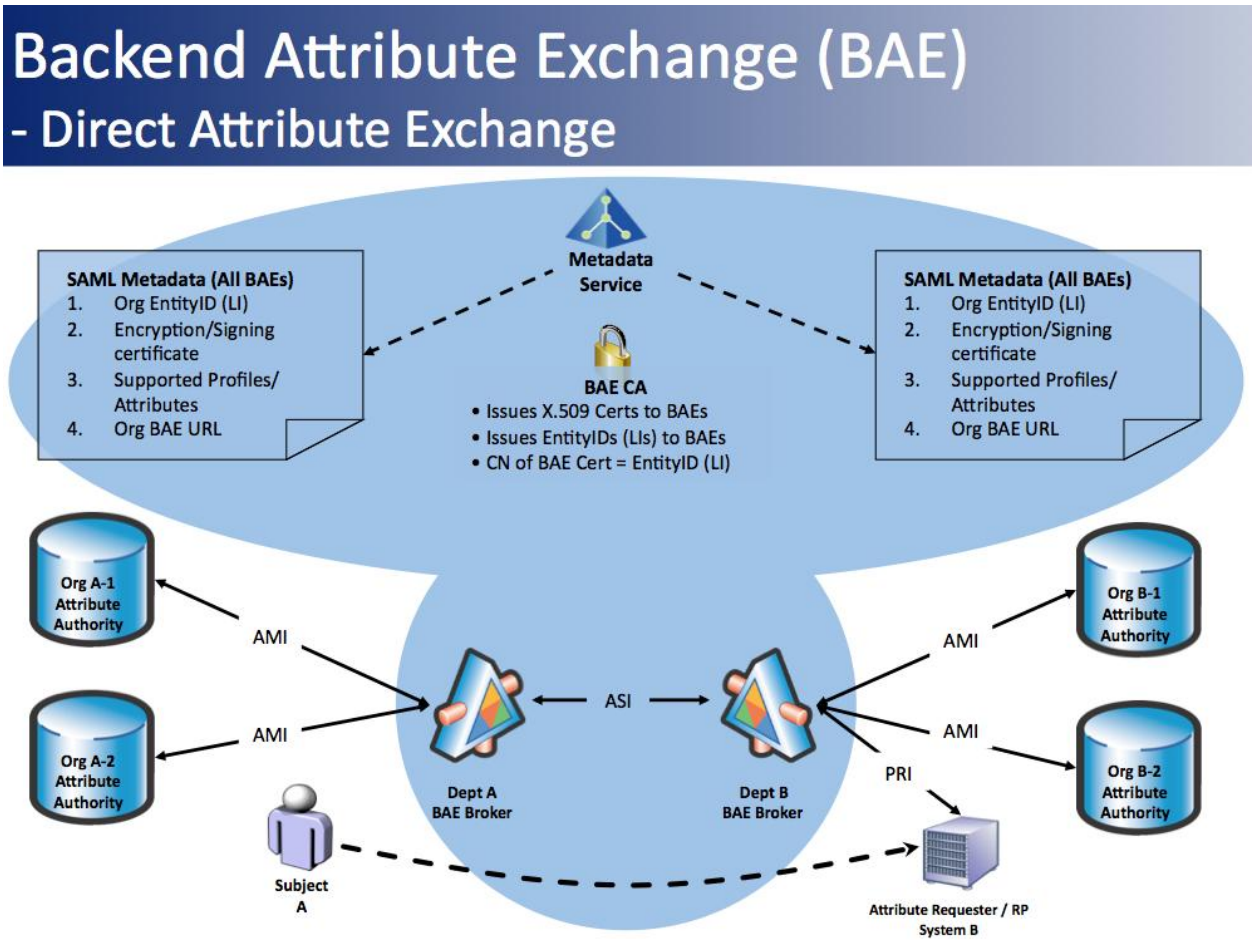
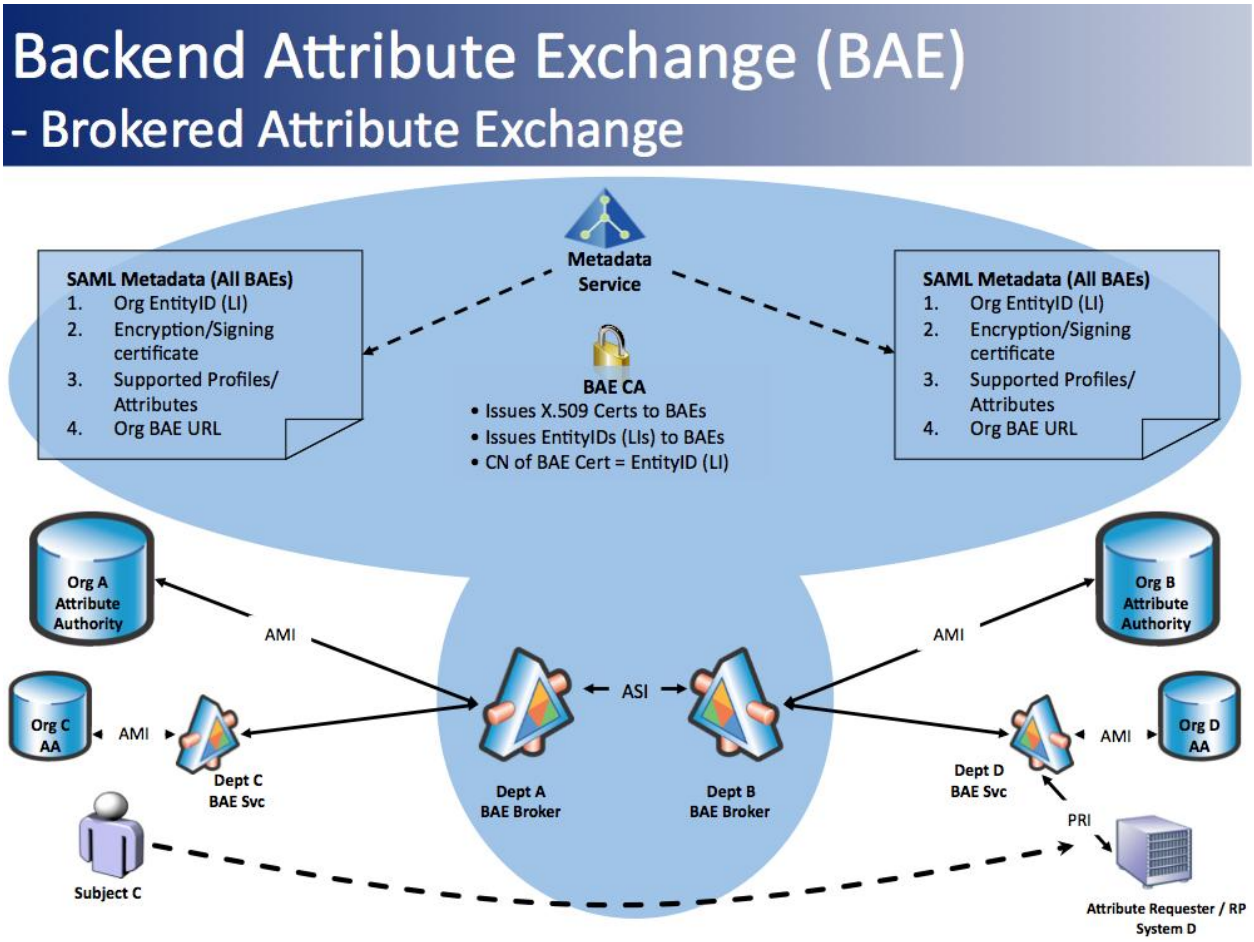


Figure 4-2 BAE Brokered Attribute Exchange



4.1 BAE Architecture and Choreography

The BAE architecture is a technical framework into which approved components integrate and technically interoperate via well-defined interface specifications. The noteworthy design choices include:

1. Separation of profiling the identifiers from the protocol, so that additional identifiers can be "snapped-in" as needed;
2. Agnostic to the attribute contract, so that any set of attributes defined by the Federation operator can be used;
3. Ability to use the BAE technical profiles within a community of interest without dependencies on Federal Identity, Credential and Access Management (FICAM) governance (i.e., communities of interest have their own governance); and
4. Optional support of user consent for attribute release to comply with FICAM privacy principles.

4.1.1 Architecture Assumptions and Considerations

The BAE architecture assumes the following:

1. BAE deployment will be a phased approach.
2. Initially, there will be a few BAE participants (e.g., 15 or fewer). Participation will increase over time. While a small number of participants, BAE may use non-automated approaches to reduce effort or cost, and to expedite roll out.
3. Placing BAE Brokers behind a gateway to segregate the BAE Broker, which is privy to personal information, from the Internet is an important consideration but out of scope for this document suite.
4. For each Attribute Subject, a single AA has primary knowledge of the Attribute Subject, and knows all other AAs (across organizations) that contain information about the Attribute Subject. For initial deployment, the response side of BAE processing collects all requested Backend Attributes, regardless of where located.
5. For initial deployment, BAE requests and responses pertain to Backend Attributes only. In the future, other types of requests and responses may be added.

4.1.2 Design Goals

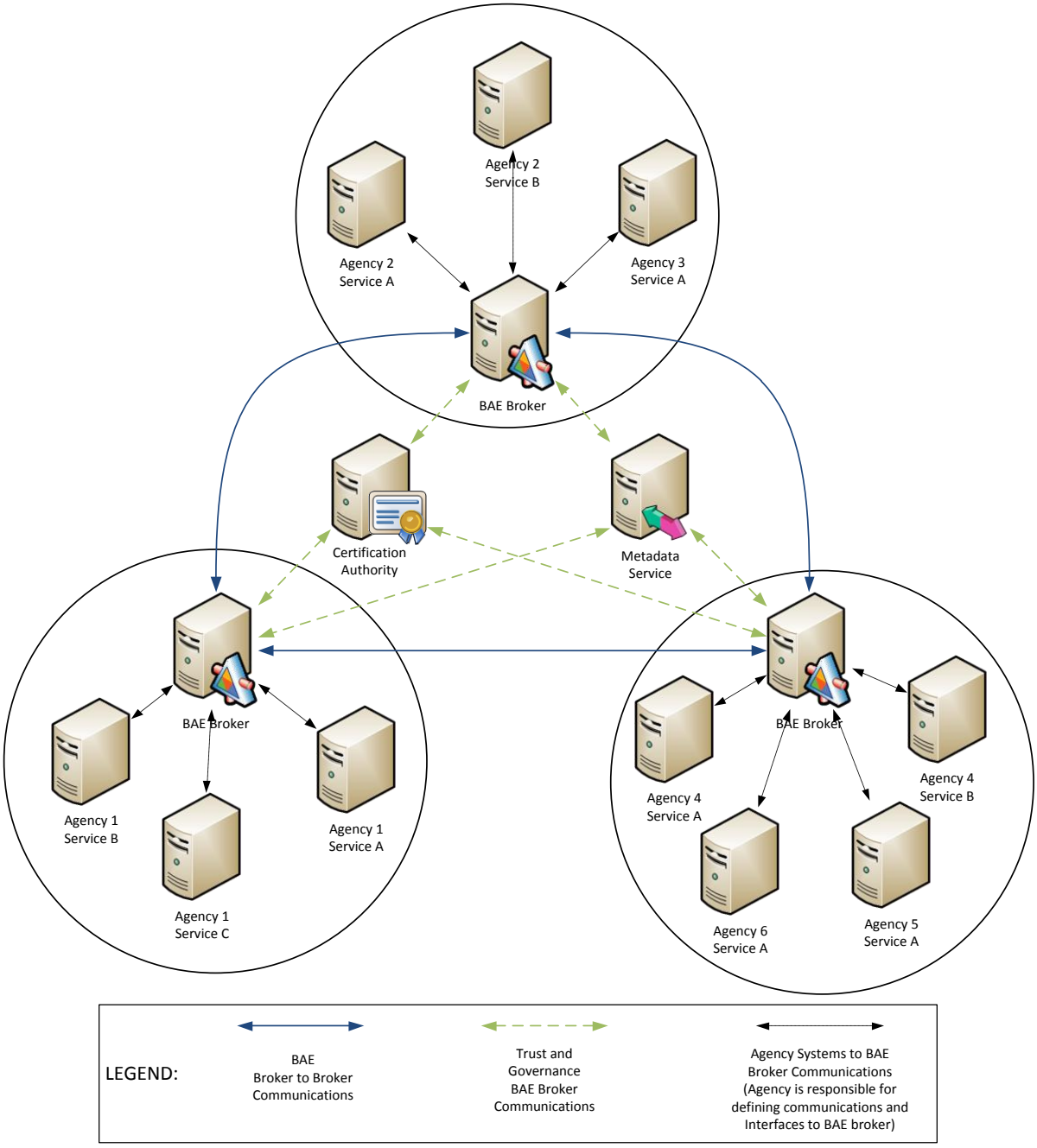
The BAE technical vision derives from the following design goals:

1. **Commercial-off-the-Shelf (COTS)**: The architecture SHOULD employ COTS products wherever possible;
2. **Durable**: The architectural framework SHOULD be designed to allow for the evolution of technology, providing for easy migration as the industry evolves;
3. **Flexible**: The architectural framework SHOULD not rely on any single standard, vendor, product, or integrator;
4. **Scalable**: The solution MUST be scalable both technologically and administratively;
5. **Reliable:** The architecture MUST be very dependable, applying best practices and establishing a high level of credibility and confidence;
6. **Ease of use:** The end user experience SHOULD be as simple as possible by optimizing usability, availability, and response times;
7. **Ease of adoption:** Agency adoption MUST be optimized by mitigating technical barriers to entry;
8. **Extensible**: The architecture SHOULD readily support additional use cases and exchange of additional Backend Attributes;
9. **Seamless**: BAE participants and components SHOULD be minimally affected by future BAE architecture or BAE interface specification changes;
10. **Discovery:** Where applicable, determination of the BAE Responder to send a request must be obtainable from information within the Authentication Credential.

4.1.3 Conceptual BAE Architecture

Error! Reference source not found. depicts the conceptual BAE architecture, which upports both BAE models. Inter-agency communication and data exchange are accomplished via BAE Brokers. All communication is via request/response message pairs. A BAE Broker can be implemented at different organizational levels (e.g., Agency level, Department level).

Figure 4-3 Conceptual BAE Architecture



Error! Reference source not found. illustrates the conceptual BAE process flow, hich Table 4-1 describes. Prior to live operations, BAE Brokers are configured with Public Key Infrastructure (PKI) certificates and metadata to support trusted technical interoperability. Initially, metadata exchange will likely be manual and out-of-band.

Figure 4-4 Conceptual BAE Request/Response Process Flow

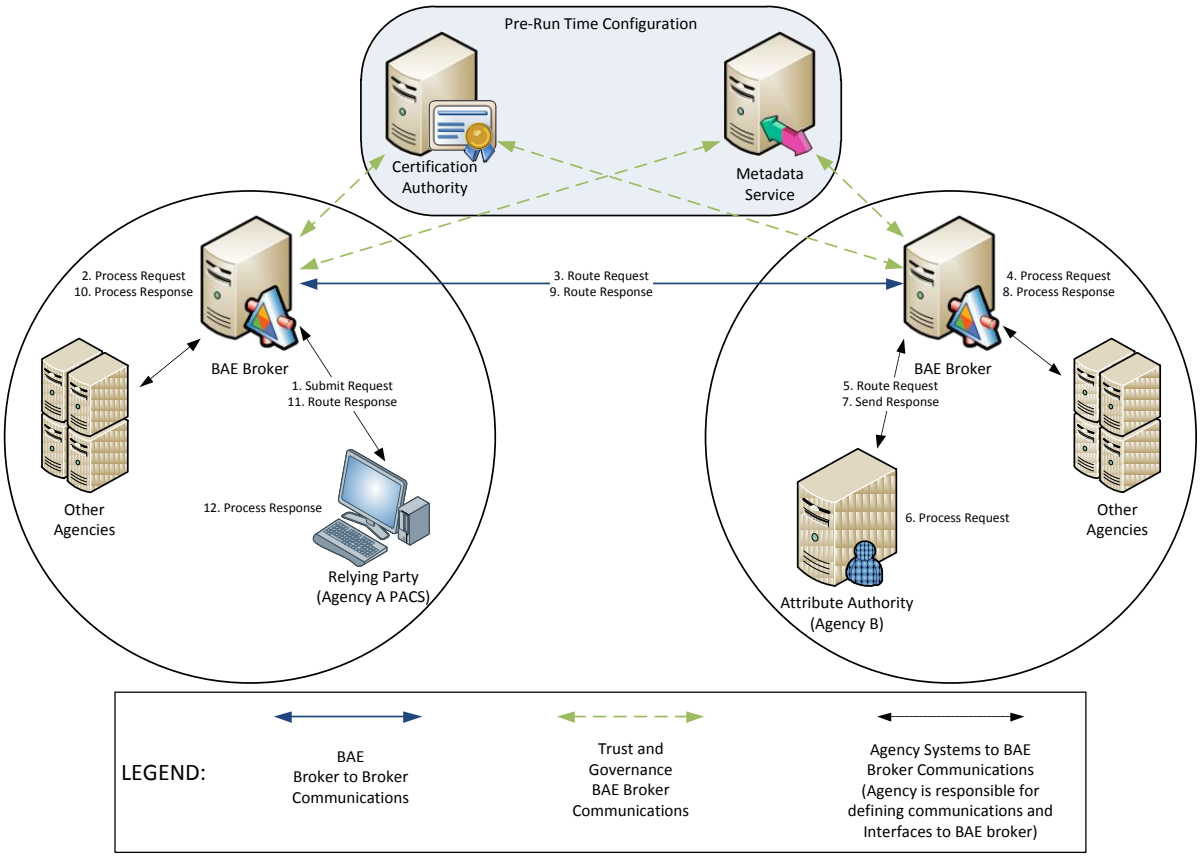


Table 4-1 Conceptual BAE Request/Response Process Flow

Step	Description
1	The RP submits a request to its BAE Broker. This interface is defined within each agency and is out of scope for this document suite.
2	The RP's BAE Broker processes the request as necessary.
3	The RP's BAE Broker then routes the request to the appropriate AA's BAE Broker. This interface is defined by each BAE model.
4	The AA's BAE Broker processes the request as necessary.
5	The AA's BAE Broker then routes the request to the appropriate AA. This interface is defined within each agency and is out of scope for this document suite.
6	The AA processes the request as necessary, packaging a response as appropriate.
7	The AA sends a response to its BAE Broker. This interface is defined within each agency and is out of scope for this document suite.
8	The AA's BAE Broker processes the response as necessary.
9	The AA's BAE Broker then routes the response back to the requesting RP's BAE Broker. This interface is defined by each BAE model.
10	The RP's BAE Broker processes the response as necessary.
11	The RP's BAE Broker then routes the response to the RP. This interface is defined within each agency and is out of scope for this document suite.
12	The RP processes the response as necessary.

4.1.4 Components

BAE includes (a) BAE Brokers that must demonstrate compliance with applicable BAE interface specifications before deployment, and (b) agency systems that communicate with each other via BAE Brokers. Components comprising the BAE architecture may or may not reside on the same physical machine. The specific implementation of components is determined by each participating organization.

4.1.4.1 BAE Broker

The BAE Broker is the communications conduit between RPs and AAs. The BAE Broker includes (1) an Internal BAE Service, and (2) an External BAE Service. External BAE Services exchange Backend Attributes between trusted BAE partners.

When making a request (e.g., requesting Backend Attributes), the BAE Broker is a BAE Requester. When returning a response (e.g., returning Backend Attribute values), the BAE Broker is a BAE Responder.

The External BAE Service processes transactions as necessary, including but not limited to the following:

- Message signing and signature verification;
- Message encryption and decryption; and
- Message routing.

BAE Brokers are configured with BAE metadata as necessary to facilitate trusted, secure technical interoperation and transaction processing.

4.1.4.1.1 External BAE Service

The External BAE Service is an inter-agency communications mechanism. External BAE Services communicate directly with each other to securely exchange BAE messages. Communication is in a request-response manner.

In the Single Subject, Real-time Query Model, the request message is the RP's list of desired Backend Attributes, and the response message is the Backend Attribute values returned by the AA.

In the Multiple Subject, Occasionally-connected Model, there are two sets of request/response messages. In the first message set, the request message is the criteria for selecting Attribute Subjects, and the response is a list of Identifiers that match the criteria (e.g., PIV Card FASC-Ns, PIV-I Card UUIDs). In the second message set, the request is the list of Identifiers and desired Backend Attributes, and the response message is Backend Attribute values for each Attribute Subject returned by the AA.

External BAE Service interface specifications are defined in [BAEv2 SAML] and [BAEv2 SPML].

4.1.4.1.2 Internal BAE Service

The BAE Internal Service is an intra-agency communications mechanism between an agency system (e.g., RP, AA) and BAE External Service. Agency systems interface only with Internal BAE Services. The Internal BAE service does the following:

- On the BAE Requester side, the BAE Internal Service forwards RP requests to the External BAE Service, and forwards results from the BAE External Service to the RP.
- On the BAE Responder side, the BAE Internal Service receives requests from the External BAE Service, selects the appropriate AA, forwards the request to that AA, receives results back from the AA, and forwards the results back to the External BAE Service.

The BAE Internal Service interface is out of scope for this document suite. The participating organization is responsible for implementing the Internal BAE Service and its interface.

4.1.4.2 Certification Authorities and BAE Metadata Service

To manage trust and connectivity in the BAE network, digital certificates will be used to ensure integrity while authenticating BAE Brokers. In addition, every BAE Broker requires certain information about other BAE Brokers with which it will communicate. Certification Authorities and a BAE Metadata Service will be part of the BAE architecture. The manner in which they will be implemented depends on the trust and governance model (see [BAEv2 Governance]) established for each federation agreement. Additionally, the E-Governance Trust Services (EGTS) will provide these services for BAE federation partners in instances where the partners do not have the onus to provide their own.

4.1.4.3 Relying Party (RP)

The RP is the entity that requires Backend Attributes from the applicable authoritative source to satisfy any supported BAE use case. RPs exist within an individual agency infrastructure and are out of scope for this document suite. Examples of RPs include, but are not limited to the following:

- Physical Access Control System (PACS);
- Logical Access Control System (LACS); and
- Security Guard via a web interface.

4.1.4.4 Attribute Authority (AA)

For the initial BAE release, the AA is the agency that issued the Authentication Credential to the Attribute Subject. The AA is the authoritative source of Backend Attributes for that Attribute Subject. The applicable AA system responds to Backend Attribute requests by providing the requested information to BAE Brokers as appropriate. Message transactions between AAs and BAE Brokers are internal to each organization and are out of scope for this document suite. Future BAE releases may support additional authoritative sources.

Appendix A: Document References

The following is a list of documents that will be of interest to BAE participants. The documents provide additional insights, guidance, and requirements. Some documents may be relevant for one task only. Other documents may be relevant in many places.

This document suite uses the NIST convention for citing documents. The shorthand format [*Doc Reference*] indicates a document fully cited in this section. For example, [FIPS 201] refers back to this section's citation for the *FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST, March 2006* document. This convention reduces verbiage throughout the document.

[BAE Use Cases] Use Cases for Defining Backend Attribute Exchange
http://www.idmanagement.gov/awg/

[BAEv1] Backend Attribute Exchange Architecture and Interface Specification
http://www.idmanagement.gov/awg/

[BAEv2 Governance] Backend Attribute Exchange Version 2, Governance Volume
http://www.idmanagement.gov/awg/

[BAEv2 Metadata] Backend Attribute Exchange Version 2, Metadata Profile Volume
http://www.idmanagement.gov/awg/

[BAEv2 Overview] Backend Attribute Exchange Version 2, Overview Volume
http://www.idmanagement.gov/awg/

[BAEv2 SAML] Backend Attribute Exchange Version 2, SAML Profile Volume
http://www.idmanagement.gov/awg/

[BAEv2 SPML] Backend Attribute Exchange Version 2, SPML Profile Volume
http://www.idmanagement.gov/awg/

[FASC-N] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems; Physical Access Interagency Interoperability Working Group
http://www.smart.gov/iab/documents/PACS.pdf

[FIPS 10-4] Federal Information Processing Standards Publication 10-4; Countries, Dependencies, Areas of Special Sovereignty, and Their Principal Administrative Divisions
http://www.itl.nist.gov/fipspubs/fip10-4.htm

[FIPS 201] FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST, March 2006
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[GSA USAccess] GSA HSPD-12 USAccess Program Authoritative User Data Interface Specification
Contact the Managed Service Office

[HSPD-12] Homeland Security Presidential Directive/HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors"; August 27, 2004
http://csrc.ncsl.nist.gov/policies/Presidential-Directive-Hspd-12.html

[FICAM Roadmap] Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

[NIPP] "National Infrastructure Protection Plan" Department of Homeland Security, 2006
http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[NRP] "National Response Plan" Department of Homeland Security, December 2004
http://www.dhs.gov/xlibrary/assets/NRP_FullText.pdf

[NIST 800-47] Security Guide for Interconnecting Information Technology Systems
National Institute of Standards and Technology
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[NIST 800-52] Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[NIST 800-87] Codes for the Identification of Federal and Federally Assisted Organizations
http://csrc.nist.gov/publications/nistpubs/800-87/sp800-87-Final.pdf

[NIST 800-95] Guide to Secure Web Services
National Institute of Standards and Technology
http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[RFC 2119] Key words for use in RFCs to Indicate Requirement Levels
http://www.ietf.org/rfc/rfc2119.txt

[SAML2 Bindings] "Bindings for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-bindings-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[SAML2 Conform] "Conformance Requirements for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-conformance-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf

[SAML2 Context] "Authentication Context for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-authn-context-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

[SAML2 Core] "Assertions and Protocol for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-core-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2 Glossary] "Glossary for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-glossary-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf

[SAML2 Metadata] "Metadata for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-metadata-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[SAML2 Metadata Ext] Metadata Extension for SAML V2.0 and V1.x Query Requesters; OASIS Standard; 1 November 2007
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-ext-query-os.pdf

[SAML2 Profiles] "Profiles for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005. Document Identifier: saml-profiles-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SAML2 Security] "Security and Privacy Considerations for the OASIS Security Markup Language (SAML) V2.0", OASIS Standard, 15 March 2005.
Document Identifier: saml-sec-consider-2.0-os
http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf

[SOAP] Simple Object Access Protocol (SOAP) 1.1; W3C
http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

[SPML2] "OASIS Service Provisioning Markup Language (SPML) Version 2.0", OASIS Standard, 1 April 2006. Document Identifier: pstc-spml2-os.pdf
http://www.oasis-open.org/committees/download.php/17708/pstc-spml-2.0-os.zip

[WS-Security] "Web Services Security: SOAP Message Security 1.1(WS-Security 2004)"; OASIS Standard, 1 February 2006
http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

Appendix B: Web Site References

Topic	Links
JPEG 2000	http://www.jpeg.org/jpeg2000
NIEM	http://www.niem.gov/ http://www.niem.gov/topicIndex.php?topic=documentation
NIST Documents	http://csrc.nist.gov/publications
SAML	http://www.oasis-open.org/home/index.php http://www.oasis-open.org/specs/index.php#samlv2.0 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security http://www.oasis-open.org/committees/security/docs
SOAP	http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
SPML	http://www.oasis-open.org/specs/index.php#spmlv2.0 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=provision
WS-Security	http://www.oasis-open.org/committees/workgroup.php?wg_abbrev=ws-sx http://www.oasis-open.org/committees/workgroup.php?wg_abbrev=wss http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss http://www.ibm.com/developerworks/library/specification/ws-secure/
XML	http://www.w3.org/1999/XMLSchema-instance http://www.w3.org/1999/XMLSchema
XPATH	http://www.w3.org/TR/xpath

Appendix C: Glossary

Term	Definition
Attribute Authority (AA)	Entity providing Backend Attributes to the requesting BAE Relying Party. For this BAE release, the AA is the agency that issued the Credential to the Cardholder. The AA is the authoritative source of Backend Attributes for that Cardholder.
Attribute Subject	Authentication Credential holder for whom an RP requires information (Backend Attributes) directly from the authoritative source (Attribute Authority), which is the agency that issued the Attribute Subject's Authentication Credential.
Authoritative Source	The Authoritative Source for a Backend Attribute is the entity that maintains the attested version of that Backend Attribute. When more than one entity (e.g., another Attribute Authority, a RP) has the same Backend Attribute, the Authoritative Source's value must be considered the correct value, and should take precedent over all other values. Only one Authoritative Source should exist per Backend Attribute.
Backend Attribute Exchange (BAE)	Process by which an RP obtains attribute information (Backend Attributes) about a claimant through a direct connection to an attribute source (attribute provider) – in contrast to a front-channel attribute delivery where the claimant is directly involved in the process, typically as part of the authentication event.
Backend Attributes	Cardholder information stored by an Attribute Authority available to Relying Parties typically to support Cardholder authentication, authorization, or emergency events.
BAE Broker	The Broker is the communications conduit between RPs and Attribute Authorities.
BAE External Service	Handles the exchange of Backend Attributes between trusted BAE partners.
BAE Internal Service	Handles the exchange of Backend Attribute data between local attribute authorities.
BAE Relying Party	Entity requesting Backend Attributes typically to support Cardholder authentication, authorization, or emergency events.
BAE Requester	BAE Broker that sends a request for Backend Attributes.
BAE Responder	BAE Broker that returns Backend Attribute values that were requested by a BAE Requester.
Batch Processing	A data processing operation and where related BAE transactions are grouped together and transmitted for processing in one group.

Term	Definition
Cardholder Unique Identifier (CHUID)	The CHUID is defined to provide the basis for interoperable identification of individuals and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. It contains a series of mandatory and optional tagged objects. Some of these include the Federal Agency Smart Credential Number (FASC-N), the Global Unique ID (GUID), and the Asymmetric Signature.
Claimant	A party whose identity is to be verified using an authentication protocol.
E-Governance Certification Authorities (EGCA)	Established to support government-wide identity management initiatives. In accordance with EGCA Certificate Policy, the EGCA issues various certificates including certificates for signing metadata.
E-Governance Metadata Authority (EGMA)	Government wide repository for SAML Metadata, representing both SAML and non-SAML endpoints (e.g., OpenID, BAE). EGMA collects, consolidates, validates and publishes metadata for identity and attribute providers that conduct authentication and attribute exchange in accordance with the Trust Framework Provider Adoption Process, ICAM adopted schemes, and this BAE document suite. Despite its role in facilitating metadata distribution, EGMA is not directly involved in authentication or attribute transaction processing. Furthermore, EGMA is not a replacement for Federation or Inter-Federation, but rather is a tool for supporting such activities.
E-Governance Trust Services (EGTS)	E-Governance Trust Services (EGTS) facilitate the use of federated identity in a trusted manner throughout the Federal Government, and between the Federal Government and its partners (i.e., citizens, businesses, and other entities). EGTS includes two complimentary services: • E-Governance Certification Authority (EGCA); and • E-Governance Metadata Authority (EGMA). Both the EGCA and EGMA are technical tools that enable governance, convey trust, and facilitate secure communications within ICAM Federations.
Endpoints	Entities at each end of a BAE transaction.
Extensible Markup Language (XML)	Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.
Federal Agency Smart Credential – Number (FASC-N)	The FASC-N is the primary identification string to be used on all government issued credentials.
Federal Identity, Credentialing and Access Management (FICAM)	Government-wide initiative whose goal is a consolidated approach for all government-wide identity, credential and access management activities to ensure alignment, clarity, and interoperability. FICAM provides a common segment architecture and implementation guidance for use by federal agencies as they continue to invest in ICAM programs.

Term	Definition
Federal Public Key Infrastructure Management Authority (FPKIMA)	Provides the best and most cost-effective FPKI Trust Infrastructure services in support of organizations meeting their identity management and data security goals. The FPKIMA's primary focus is to ensure that common identity and access management policies for secure physical and logical access, document sharing, and communications across Federal agencies and between external business partners are realized through the execution and management of digital certificate policies and standards.
Governance	BAE governance ensures trust and reliable technical interoperation between all endpoints involved in a BAE transaction. Given the federated nature of BAE (i.e., inter-organization processing), governance is the responsibility of each participating community of interest. The essential governance functions are: 1. Managing Metadata; and 2. Issuing Certificates.
HyperText Transfer Protocol (HTTP)	Underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. In the Federation, where appropriate, HTTP is used to redirect end users.
Metadata	Message exchange between two BAE entities requires each to have specific knowledge about the other. One example is the URL of each entity a BAE Broker technically interoperates. Without such knowledge, a BAE Broker does not know where to send messages for processing. Metadata describes and conveys such information. Metadata is the primary means of trust within Federal ICAM. Signed metadata is used to bind ICAM members to their digital signature and encryption keys.
Metadata Authority	Entity that oversees and facilitates the overall metadata exchange process, including but not limited to metadata collection, validation, and distribution in a secure, confidential manner. See also E-Governance Trust Services (EGTS) and E-Governance Metadata Authority (EGMA).
Card Issuer	An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.
Relying Party	Entity requesting Backend Attributes typically to support PIV Cardholder authentication, authorization, or emergency events.

Term	Definition
Security Assertion Markup Language (SAML)	The set of specifications describing security assertions that are encoded in XML, profiles for attaching the assertions to various protocols and frameworks, the request/response protocol used to obtain the assertions, and bindings of this protocol to various transfer protocols (for example, SOAP and HTTP). SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications. SAML defines assertion message formats that are referenced in Liberty Alliance, Shibboleth, WS-Security, and other specifications. SAML has become the standard web SSO identity management solution. Several versions have been released to date, including SAML 1.0, SAML 1.1, and SAML 2.0. The Organization for the Advancement of Structured Information Standards (OASIS) oversees SAML.
Service Provisioning Markup Language (SPML)	An XML-based framework, developed by OASIS, for exchanging user, resource and service provisioning information between cooperating organizations. SPML relies on SAML for the exchange of authorization data. Several versions have been released including version 1.0 in 2003 and version 2.0 in 2006.
Shared BAE Broker	A BAE broker used by multiple departments or agencies to participate in Backend Attribute exchanges.
Simple Object Access Protocol (SOAP)	Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP.
Locale Identifier (LI)	The BAE Architecture supports both Direct and Brokered Attribute Exchange Models. In order to retrieve the attributes of subjects who are in remote domains, it is critical that sufficient information be made available to the Requesting BAE Broker to enable it to route the query to a BAE Broker that is authoritative for the attributes of the Subject. The BAE specification uses the term **Locale Identifier (LI)** to define the routing information that is embedded within the unique identifier assigned to a BAE Requester and/or Responder.
Locally Unique Identifier (LUID)	In order to query an attribute service to retrieve the information about a Subject, it is necessary to utilize an identifier that is unique across the domain in which the Subject exists. The BAE specification uses the term **Locally Unique Identifier (LUID)** to define this identifier. The BAE architecture has the ability to support multiple LUID formats.

Appendix D: Acronyms

Acronym	Term
AA	Attribute Authority
ABAC	Attribute Based Access Control
AMI	Attribute Management Interface
ASI	Attribute Service Interface
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
COTS	Commercial Off the Shelf
EGTS	E-Governance Trust Services
FASC-N	Federal Agency Smart Credential Number
FICAM	Federal Identity, Credentialing and Access Management
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FPKIMA	Federal Public Key Infrastructure Management Authority
HSPD	Homeland Security Presidential Directive
ICAMSC	Identity, Credentialing and Access Management Sub Committee
IT	Information Technology
LACS	Logical Access Control System
LDAP	Lightweight Directory Access Protocol
LI	Locale Identifier
LUID	Locally Unique Identifier
NIST	National Institute of Standards and Technology
OGP	Office of Governmentwide Policy
PACS	Physical Access Control System
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
PKI	Public Key Infrastructure
PRI	Protected Resource Interface
REST	Representational State Transfer

Acronym	Term
RP	Relying Party
SAML	Security Assertion Markup Language
SP	Special Publication
SPML	Service Provisioning Markup Language
SQL	Structured Query Language
SSL	Secure Socket Layer
TLS	Transport Layer Security
UUID	Universally Unique Identifier