ICAM

Identity, Credential,
& Access Management

Backend Attribute Exchange (BAE) v2.0 Governance

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

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). 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[1].

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. 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). BAE can be used in

[1] 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.

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 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 Governance Overview

BAE governance is necessary to ensure 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 (COI) as well as ICAM, which is also a COI. Accordingly, each COI is responsible for implementing and operating certain governance functions, which this document describes. The essential governance functions are:

1. **Managing Metadata** – full life cycle management of information needed to ensure robust, reliable, correct technical interoperation between BAE endpoints. Metadata should be shared bi-directionally.
2. **Issuing Certificates** – full life cycle management of certificates issued to BAE Brokers and Metadata Authorities to ensure trust between endpoints, and to facilitate security and privacy of communications between the endpoints. The certificates are used for digital signing and digital encryption.

A COI may establish operational procedures as it sees fit. Therefore, it should be understood by all BAE parties that governance will likely vary between COIs. In addition, a COI may implement additional governance mechanism as necessary. However, a COI must ensure that its governance approach is consistent with overarching BAE governance principles so as not to defeat the essential governance objectives of technical interoperability, trust, security, and privacy.

Federal ICAM is implementing a broader governance capability called E-Governance Trust Services (EGTS). EGTS will 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:

- A redesigned/enhanced 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. The Federal ICAM, through the Federal Public key Infrastructure Management Authority (FPKIMA), will operate EGTS in order to provide governance services to the entire Federal government. EGTS will operate at a level consistent with other components of the Federal Trust Infrastructure.

EGTS will meet the requirements of BAE community governance as specified in this Governance document. In addition, EGTS will meet the requirements of governance specified by ICAM Profile documents (i.e., Open Solutions for Open Government Profiles such as the SAML 2.0 Profile). Specifically, EGTS will:

1. Issue server certificates for SAML using a differentiated Object Identifier (OID). The OID will be determined at a later date; and
2. Publish trusted Metadata.

COIs are encouraged to leverage EGTS governance features and its general approach as much as possible for their own governance responsibilities. Doing so should enhance federation-wide governance consistency and coordination, and therefore federation-wide governance success. See Appendix A for summary of Federal ICAM governance as it relates to BAE.

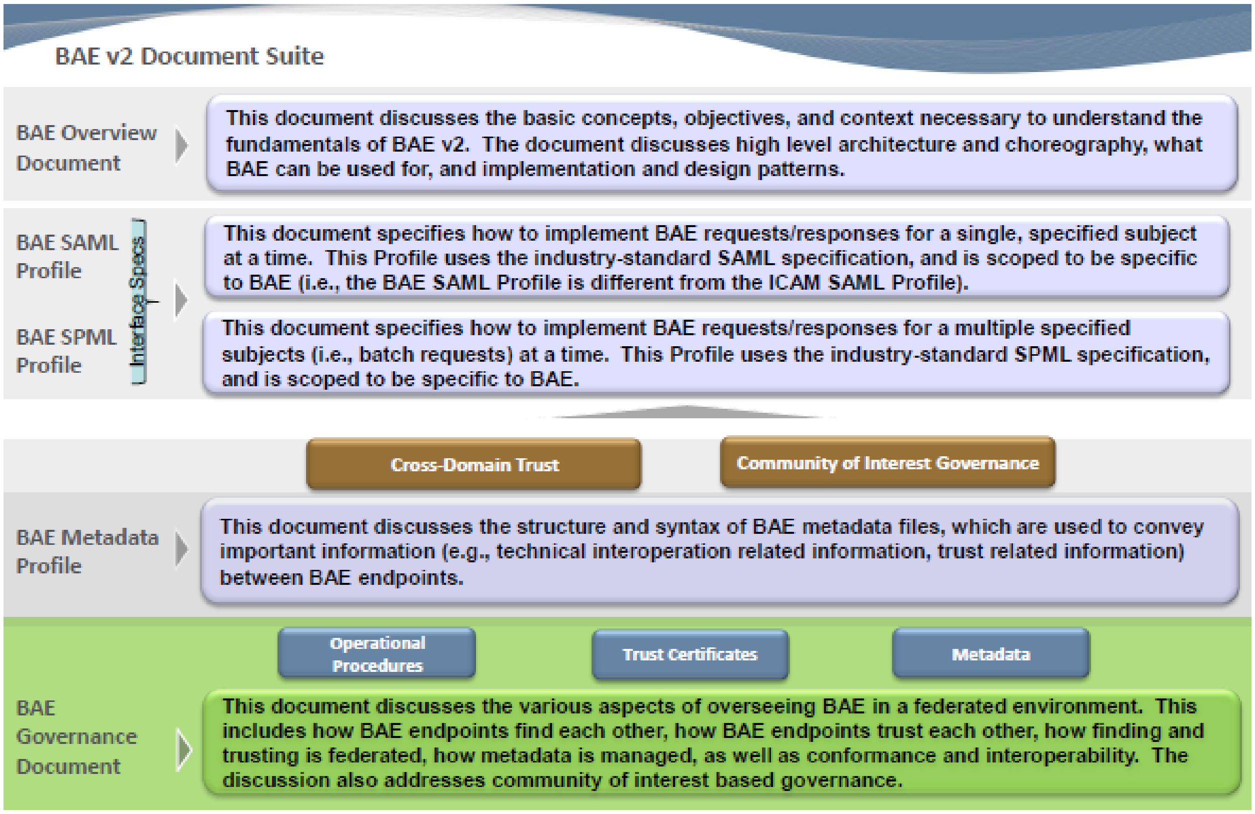
1.3 Objective and Audience

BAE specification version 2 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).

The audience for this document is any IT or Operational Authority that is responsible for a COI's BAE support. The objective of this document is to provide the high-level principles that must be considered when operationally implementing BAE governance.

Figure 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 BAE v2 Document Suite



BAE v2 Document Suite

BAE Overview Document

This document discusses the basic concepts, objectives, and context necessary to understand the fundamentals of BAE v2. The document discusses high level architecture and choreography, what BAE can be used for, and implementation and design patterns.

BAE SAML Profile

This document specifies how to implement BAE requests/responses for a single, specified subject at a time. This Profile uses the industry-standard SAML specification, and is scoped to be specific to BAE (i.e., the BAE SAML Profile is different from the ICAM SAML Profile).

BAE SPML Profile

This document specifies how to implement BAE requests/responses for a multiple specified subjects (i.e., batch requests) at a time. This Profile uses the industry-standard SPML specification, and is scoped to be specific to BAE.

BAE Metadata Profile

This document discusses the structure and syntax of BAE metadata files, which are used to convey important information (e.g., technical interoperation related information, trust related information) between BAE endpoints.

BAE Governance Document

This document discusses the various aspects of overseeing BAE in a federated environment. This includes how BAE endpoints find each other, how BAE endpoints trust each other, how finding and trusting is federated, how metadata is managed, as well as conformance and interoperability. The discussion also addresses community of interest based governance.

1.4 Scope

The scope of this document is limited to describing the Federal ICAM's BAE governance approach. Discussion of the governance approaches and operations of other COIs is out of scope.

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 How to Find Each Other - Metadata

Message exchange between BAE Brokers requires each to have specific knowledge about the other prior to trusted technical interoperation. Without such knowledge, it would be unclear (or unknown) where to send messages, and how to interact with one another in a robust, reliable, consistent manner. Metadata describes and conveys such information. The new EGMA will publish BAE Broker metadata to appropriate participants. In general:

1. Metadata is a means of trust within BAE. Therefore, it must be updated and consumed frequently[2].
2. Signed metadata is used to bind a BAE provider to its digital signature and encryption keys.
3. Prior to run time, trust of a BAE provider's signing and encryption certificates is determined when metadata is configured into the BAE system.
4. At run time, BAE systems must validate that the certificate used to sign the message matches the message sender's certificate in metadata.
5. Metadata does not contain confidential information.[3]

EGMA maintains and distributes metadata for all participants that provide BAE services. All participants must produce and submit their own metadata, and consume the metadata of others as appropriate. All metadata files should be digitally signed to ensure trustworthiness and non-repudiation, and to help detect tampering.

Participants should immediately update and re-submit metadata to EGMA when their metadata information changes. In addition, participants must verify their own metadata for correctness and completeness before submitting to EGMA, and metadata received from ICAM prior to consumption. Participants should check for and consume new or revised metadata on a periodic basis as prescribed by ICAM.

Failure to consume and configure metadata completely and correctly can preclude technical interoperation, undermine trust, or result in unexpected consequences or

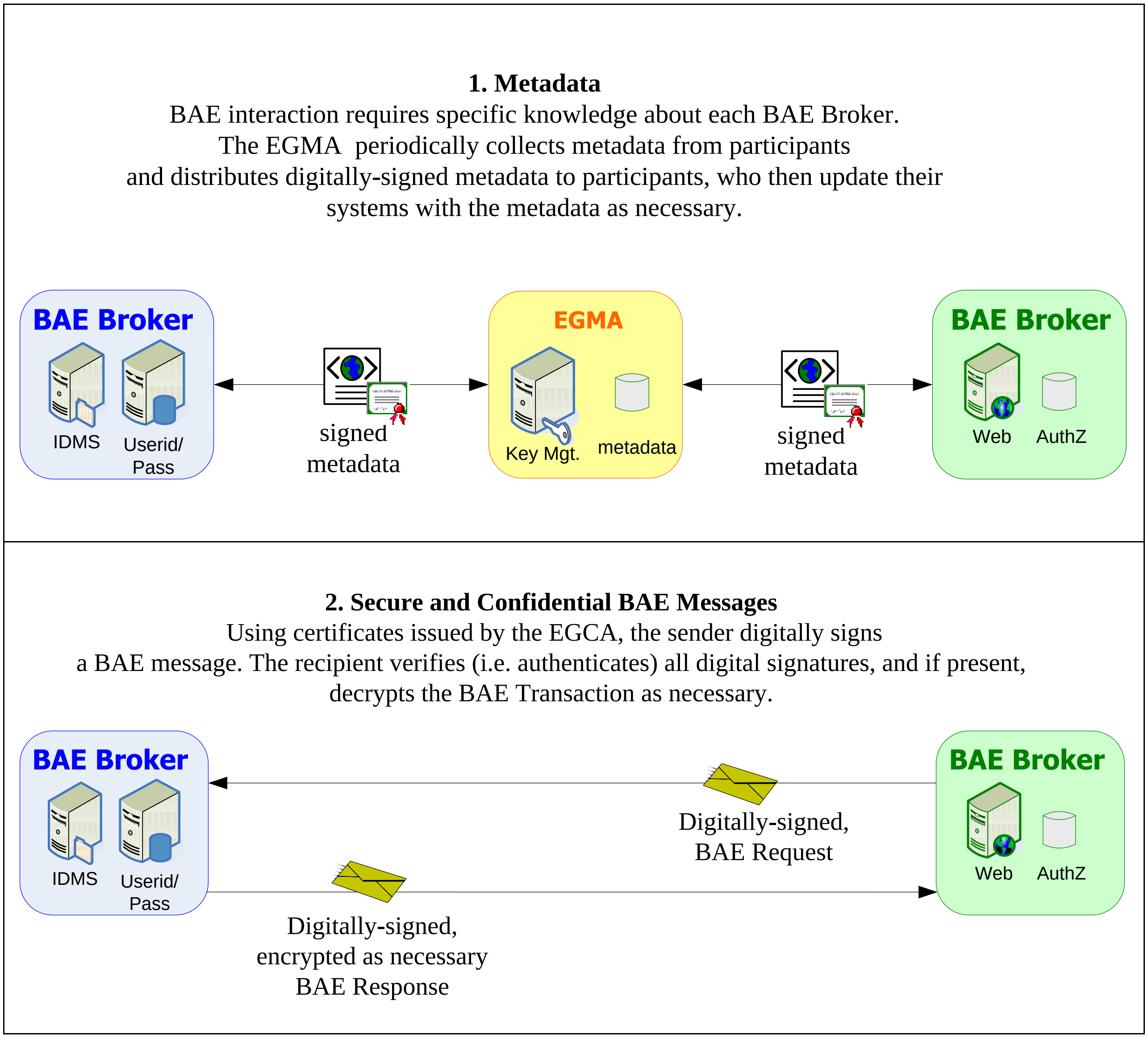
[2] Frequent publication and consumption of metadata serves a similar purpose to that of certificate revocation lists and should be treated with equal importance.

[3] There may be circumstances where confidentiality is an issue. This governance model does not preclude handling those special circumstances (e.g., exchange of metadata only between specific participants).

negative impacts to BAE Brokers, or other BAE systems that might be involved in the BAE transaction chain. Participants should consume only metadata that is trustworthy.

Despite its metadata management role, ICAM (including EGTS) is not involved in BAE transaction processing. Participants use BAE metadata to facilitate direct interaction between BAE Brokers for BAE transaction purposes. The use of signed metadata for the purpose of creating trust between BAE brokers is an essential mechanism for supporting federation in the BAE environment.   Figure 2 illustrates the high-level programmed trust process flow applicable to all SAML 2.0 uses cases.

Figure 2 High-level Programmed Trust Process Flow



1. Metadata

BAE interaction requires specific knowledge about each BAE Broker.
The EGMA periodically collects metadata from participants
and distributes digitally-signed metadata to participants, who then update their
systems with the metadata as necessary.

2. Secure and Confidential BAE Messages

Using certificates issued by the EGCA, the sender digitally signs
a BAE message. The recipient verifies (i.e. authenticates) all digital signatures, and if present,
decrypts the BAE Transaction as necessary.

BAE Broker
IDMS
Userid/ Pass
Digitally-signed, BAE Request
BAE Broker
Web
AuthZ
Digitally-signed, encrypted as necessary BAE Response

Until the BAE environment matures (e.g., a significant number of participants and associated BAE Brokers), metadata management will be a manual process. For example, metadata files will likely be distributed via a secure out-of-band mechanism. Recipients will then implement the metadata into their appropriate BAE systems through mechanisms available to them at the time.

See [BAEv2 Metadata] for additional information.

3 How to Trust Each Other – Certificates

The use of EGCA to issue server certificates for the purpose of creating trust between BAE brokers is another essential mechanism for supporting federation in the BAE environment. The certificates facilitate transaction security, confidentiality, and non-repudiation, as well as tamper detection.

The EGCA will issue server certificates to participants for purposes of signing and encrypting BAE requests and responses. Participants must configure these certificates into their BAE Brokers. The certificates are not end-entity certificates used by humans. They are machine-use only certificates. This approach allows a BAE Broker to verify that a message is from another trusted BAE Broker. In addition, every BAE Broker must perform certificate validation and certificate status checking to verify that the BAE Request/Response certificate is still valid and has not expired or been revoked. Certificate validation and status verification should be done before any BAE message is accepted and processed.

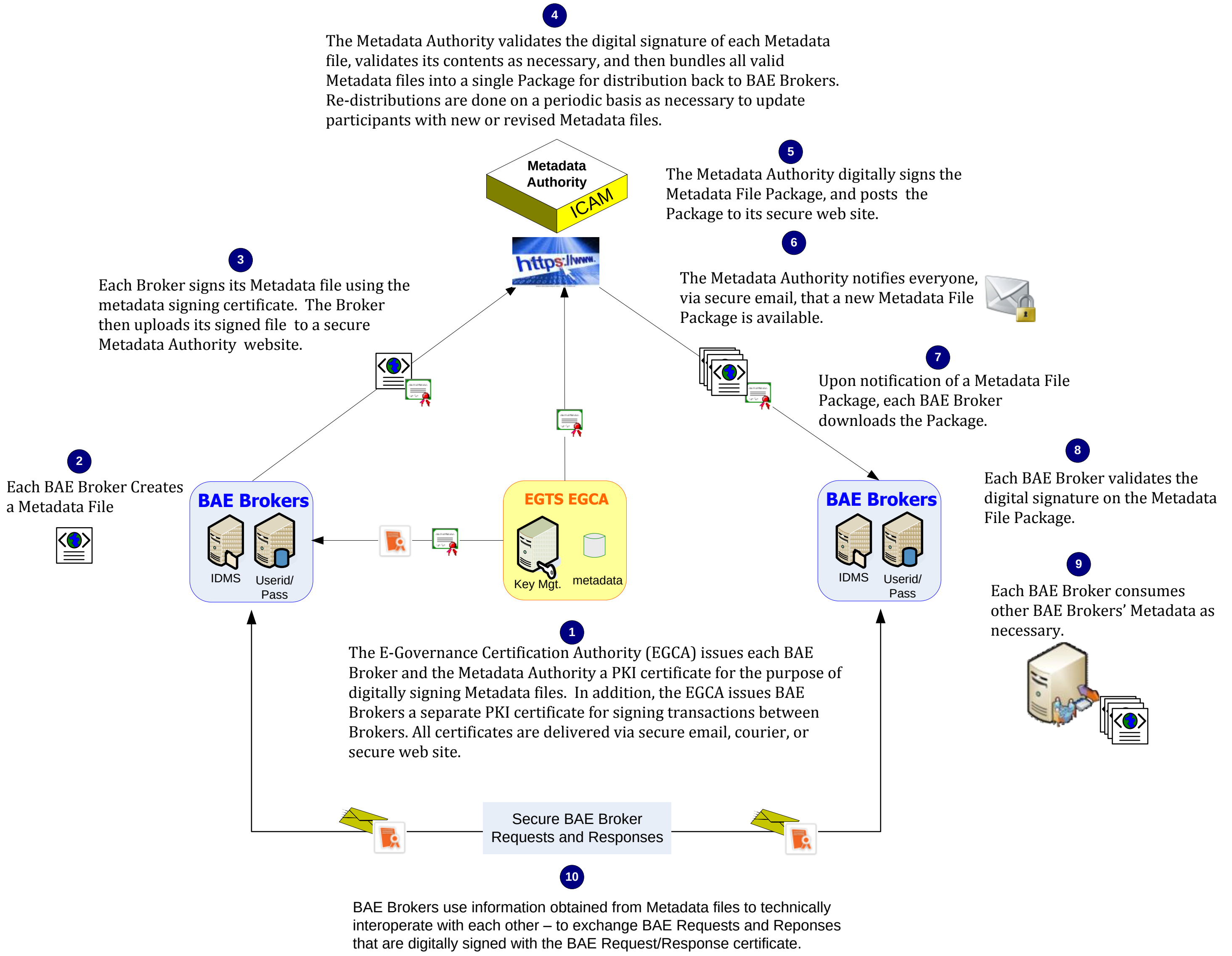
In addition, the EGCA will issue server certificates to participants and the EGMA for purposes of signing Metadata files and Aggregated Metadata File Packages. This is essential to trusting the metadata itself (e.g., the metadata is from a trusted party, the metadata has not been tampered with), which is necessary for proper technical interoperation between BAE Brokers. Trusted metadata is the means for BAE participants to trust other BAE participants whose certificates (and public keys) are included in published metadata. In essence, trusted metadata is a “white list” of trusted participants.

Certificate issuance can be extended. EGCA certificates can also be issued to others such as Trust Framework Providers, and other COIs as circumstances allow. However, this should be carefully considered. Use of signed metadata containing approved certificates may be more preferable, especially for scaling BAE across federations.

The FPKIMA will manage the full life cycle of issued certificates. For example, the FPKIMA will issue revocation data as necessary.

See [BAEv2 SAML] for more information.

Appendix A: Federal ICAM Governance



1 The E-Governance Certification Authority (EGCA) issues each BAE Broker and the Metadata Authority a PKI certificate for the purpose of digitally signing Metadata files. In addition, the EGCA issues BAE Brokers a separate PKI certificate for signing transactions between Brokers. All certificates are delivered via secure email, courier, or secure web site.

2 Each BAE Broker Creates a Metadata File

3 Each Broker signs its Metadata file using the metadata signing certificate. The Broker then uploads its signed file to a secure Metadata Authority website.

4 The Metadata Authority validates the digital signature of each Metadata file, validates its contents as necessary, and then bundles all valid Metadata files into a single Package for distribution back to BAE Brokers. Re-distributions are done on a periodic basis as necessary to update participants with new or revised Metadata files.

5 The Metadata Authority digitally signs the Metadata File Package, and posts the Package to its secure web site.

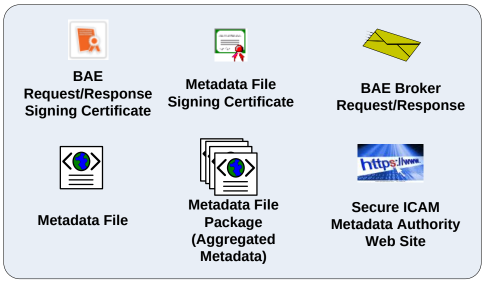
6 The Metadata Authority notifies everyone, via secure email, that a new Metadata File Package is available.

7 Upon notification of a Metadata File Package, each BAE Broker downloads the Package.

8 Each BAE Broker validates the digital signature on the Metadata File Package.

9 Each BAE Broker consumes other BAE Brokers' Metadata as necessary.

10 BAE Brokers use information obtained from Metadata files to technically interoperate with each other – to exchange BAE Requests and Reponses that are digitally signed with the BAE Request/Response certificate.


BAE Request/Response Signing Certificate
Metadata File Signing Certificate
BAE Broker Request/Response
Metadata File
Metadata File Package (Aggregated Metadata)
Secure ICAM Metadata Authority Web Site
https://www.

Legend

Appendix B: 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.

[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/

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

Appendix C: Glossary

Term	Definition
Attribute Authority	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.
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 Relying Party	Entity requesting Backend Attributes typically to support Cardholder authentication, authorization, or emergency events.
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.

Term	Definition
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.
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.
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.
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 participants 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).
Security Assertion Markup Language (SAML)	The set of specifications describing security assertions, 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. SAML addresses web single sign-on, web services authentication, attribute exchange, authorization, non-repudiation, and secure communications.

Appendix D: Acronyms

Acronym	Term
AA	Attribute Authority
ABAC	Attribute Based Access Control
AuthZ	Authorization
AWG	Architecture Working Group
BAE	Backend Attribute Exchange
COI	Community of Interest
EGCA	E-Governance Certification Authorities
EGMA	E-Governance Metadata Authority
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
IDMS	Identity Management System
Mgt	Management
NIST	National Institute of Standards and Technology
OID	Object Identifier
OGP	Office of Governmentwide Policy
PIV	Personal Identity Verification
PIV-I	Personal Identity Verification Interoperable
RP	Relying Party
SAML	Security Assertion Markup Language
SPML	Service Provisioning Markup Language
UUID	Universally Unique Identifier