BUILDING BLOCK

ATTRIBUTE BASED ACCESS CONTROL

V.2

William Fisher
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

April 1, 2015
abac-nccoe@nist.gov

This revision incorporates comments from the public.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NCCoE building blocks address technology gaps that affect multiple industry sectors.

ABSTRACT

Enterprises rely upon strong access control mechanisms to ensure that corporate resources (e.g. applications, networks, systems and data) are not exposed to anyone other than an authorized user. As business requirements change, enterprises need highly flexible access control mechanisms that can adapt. The application of attribute based policy definitions enables enterprises to accommodate a diverse set of business cases. This NCCoE building block will demonstrate a standards-based approach to attribute based access control (ABAC) that offers organizations the flexibility to easily accommodate permissions for different users, environments and conditions; centralized control of permissions; and an efficient way to share resources among partner organizations. This project will result in a freely available NIST Cybersecurity Practice Guide.

KEYWORDS

access control; access management; attribute based access control; attribute provider; authentication; authorization; identity federation; identity management; identity provider; relying party

DISCLAIMER

COMMENTS

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: abac-nccoe@nist.gov

Public comment period: April 2, 2015 to June 2, 2015

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TABLE OF CONTENTS

1. Executive Summary

This document describes the challenges a business might face in implementing attribute based access control (ABAC), an advanced approach for ensuring that access to corporate resources (e.g. applications, networks, systems and data) is limited to authorized users. ABAC offers organizations the flexibility to easily accommodate permissions for different users, environments and conditions; centralized control of permissions; and an efficient way to share resources among partner organizations.

Authentication of a user and authorization of the actions performed by that user are core components of any access control mechanism. Access to an organization's network or assets is traditionally managed according to a person's role. A store accountant, for example, needs access to both financial records and sales software, while a salesperson needs access to sales software alone. If a person changes roles or leaves a company, an administrator must manually change the employee's role to change access rights, and perhaps within several systems. To more efficiently accommodate changes like this, and changes in more complex business cases and IT requirements, organizations need highly flexible access control mechanisms.

This document describes several scenarios where functions are enabled through organizations' successful use of ABAC; identifies the characterstics required in an ABAC system and maps them to relevant standards and best practices; and presents an approach and components for providing those characterstics, along with a high-level technical architecture.

This document has been revised according to one round of public comments, included here; we are seeking further comments to validate our assumptions and approach. The NCCoE is currently engaged with some of its National Cybersecurity Excellence Partners to build an initial reference design in response to this challenge. The center will consider a second build pending public comment and review of this document; We will issue a notice in the Federal Register to invite vendors of applicable technologies to collaborate in the NCCoE labs to build an example solution.

This project will result in a NIST Cybersecurity Practice Guide, a description of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

2. Business Value

ABAC improves the efficiency of access management by eliminating the need for multiple, independent, system-specific access management processes. ABAC replaces these with an enterprise-wide attribute management process and policy management process. The ABAC-managed attributes and policy are used across multiple systems.

Such centralization of access management helps ensure consistent control of access across and between enterprises based on business-related attributes. It allows access to resources to be both granted and revoked in a timely manner, ensuring that access to information is available

when it is needed while protecting information against unintended use. Further, it allows multiple factors, represented as attributes, to be used in controlling access.

ABAC supports business agility by reducing the barriers to sharing resources and services with partner organizations. With ABAC, partner user identities and appropriate access policies for those identities do not need to be provisioned to each information resource or service that needs to be shared. Instead, access is controlled using attributes provided by the partner for partner user identities. This allows an organization to quickly and securely share resources and services with partners who have the ability to accept identity tokens and attributes for access control decisions.

ABAC can reduce the complexity of regulatory compliance. Centralization of access policy management provides a single authoritative source for access rules. This eliminates the need to audit multiple system-specific access policy repositories to ensure compliance.

3. DESCRIPTION

Audience and purpose

The cybersecurity challenge described here requires a technical solution that provides capabilities driven by business needs, as well as security characteristics that are consistent with standards and best practices. This document identifies and articulates the cybersecurity challenges facing organizations interested in implementing ABAC in their environment and provides scope for the NCCoE's effort to address these challenges. The NCCoE is seeking IT security product vendors who may collaborate with the NCCoE on the subsequent efforts to create an ABAC reference design and practice guide. The NCCoE will publish a Federal Register notice inviting IT vendors interested in collaborating on this effort.

Goal

Enterprises face the continual challenge of providing access control mechanisms for subjects requesting access to corporate resources (e.g. applications, networks, systems and data). Authentication is required for a diverse set of subjects, who may be known or unknown to the enterprise, and may present the organization with differing credentials. Once authenticated, enterprises require a strong authorization system that enables fine-grain access decisions based on a range of users, resources, and environmental conditions. These challenges, combined with the growth and distributed nature of enterprise resources, as well as the need to share information among stakeholders that are not managed directly by the enterprise, has spawned the demand for highly flexible access control mechanisms.

This building block will use commercially available technologies to demonstrate an enterprise ABAC implementation that makes run-time authorization decisions and enforces a rich set of access control policies consistently across an enterprise (or enterprises). Information about a subject, the resource being accessed, and the environmental context at the time of attempted access shall form the basis for access control decisions, rather than pre-provisioned privileges within individual systems.

Through the use of an attribute exchange platform, this project will exhibit a federated access control environment, allowing for the secure sharing of IT resources across multiple enterprises. In this manner, enterprises enable unanticipated, yet valid, federated identities to gain access, without the traditional challenge of waiting for identity provisioning or authorization approvals.

Background

Basic read, write and execute permissions along with discretionary access control (DAC) and mandatory access control (MAC) principles, form the basis of today's role based access control (RBAC) models. While RBAC focuses primarily on the use of the role attribute, ABAC allows for access decisions based upon arbitrary attributes.

The NIST Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations,* describes ABAC as "a logical access control model that is distinguishable because it controls access to objects by evaluating rules against the attributes of the entities (subject and object), actions and the environment relevant to a request."

It continues:

> "In its most basic form, ABAC relies upon the evaluation of attributes of the subject, attributes of the object, environment conditions, and a formal relationship or access control rule defining the allowable operations for subject-object attribute and environment condition combinations. All ABAC solutions contain these basic core capabilities that evaluate attributes and environment conditions, and enforce rules or relationships between those attributes and environment conditions." …
>
> "The rules or policies that can be implemented in an ABAC model are limited only to the degree imposed by the computational language. This flexibility enables the greatest breadth of subjects to access the greatest breadth of objects without specifying individual relationships between each subject and each object."[1, 2]

In order to enable ABAC implementations, the standards community has undertaken efforts to develop common terminology and interoperability across access control systems. One such standard is the eXtensible access control markup language (XACML). Built on an eXtensible markup language (XML) foundation, XACML is designed to allow externalized, run-time access control decisions using attribute based policy definitions.

---

[1] Attribute Based Access Control (ABAC) – Overview, Natl. Inst. Stand. Technol. [Web page], http://csrc.nist.gov/projects/abac/, [accessed 9/1/2014].

[2] V.C. Hu, D. Ferraiolo, and R. Kuhn, et al., Guide to Attribute Based Access Control (ABAC) Definition and Considerations, NIST Special Publication 800-162, National Institute of Standards and Technology, Gaithersburg, MD, January 2014, 37 pp. http://dx.doi.org/10.6028/NIST.SP.800-162

As standards such as XACML promote ABAC implementations, enterprises have realized that supporting a wide range of users, which may not be known or managed by the enterprise, requires attributes from external sources. One approach to meeting this requirement utilizes federation profiles.

Federation profiles define the syntax and semantics of the data being federated. These technologies leverage widely accepted, open web communication languages, like the Security Assertion Markup Language (SAML) standard, which utilizes XML, or the OpenID Connect standard built upon JavaScript Object Notation (JSON). Federation profiles allow identity and attribute information to be sent over hypertext transfer protocol (HTTP) in a manner that can be understood and used by the receiving organization (hereafter referred to as the relying party (RP)) to make access control decisions.

Using such profiles, identity information can be federated from a trusted third-party entity that has issued a subject credential known as an identity provider (IdP). Attributes associated with a specific identity may be federated by an IdP, but can also be obtained from a trustworthy or authoritative external source known as an attribute provider (AP). Often, an AP's authority applies only to its domain. A credit bureau, for example, might be authoritative as to the credit worthiness of a subject, but one would look to a health care provider to determine the subject's blood type.

Enterprises looking to participate in federation must have a degree of trust with the organization from which they are receiving identity and attribute information. To facilitate these trust relationships, non-profit organizations such as the Kantara Initiative and the Open Identity Exchange (OIX) have proposed trust framework specifications that provide a complete set of contracts, regulations and commitments that enable parties of a trust relationship to rely on identity and attribute assertions from external entities.

To date, few demonstrations of ABAC utilizing federated identity and attribute information exist.

4. SCENARIOS

While the security mechanisms employed in this building block can address a wide-array of challenges across various enterprises, this building block initially will focus on demonstrating capabilities that enable one the following scenarios:

Example Scenario 1 – Enterprise-to-Enterprise Identity Federation and Access Control

An airline with operations in the western United States, Runabout Air, wishes to expand service from coast to coast. Instead of purchasing additional airliners, Runabout Air has acquired Conway Airlines, which has existing service in the eastern United States. The merger will require the integration of several IT systems including operations, financial and sales.

Runabout will have an immediate need to give Conway employees access to IT systems. An analysis of the Runabout and Conway IT systems has concluded that the quickest way to allow

the two companies to use each other's resources is to establish a trust relationship between the two organizations' identity management systems. To accomplish this, Runabout will implement a federated identity system wherein Runabout resources accept secure authentication tokens from the existing Conway identity and access management (IDAM) system. This will avoid costs associated with password management and replication of user repositories across both enterprises. Additionally, Runabout will use existing business rules to determine access permissions for Conway employees based on attributes from the Conway IDAM system. As a result, Runabout and Conway will enhance their security postures and reduce acquisition costs by implementing a consistent policy across the enterprise.

Example Scenario 2 – Externalized Access Control for the Cloud

After performing a cost/benefit analysis of internal IT resources, a company has determined that moving applications from their own network to cloud-based service providers will reduce the costs of software licensing and technical support labor, and enable cutting-edge capabilities. In particular, core services such as email, customer relationship management and payroll will transition first. The company has also decided to open up its collaboration platform to several partner organizations to facilitate information sharing and innovation within product development. While moving to this new distributed data model, the company does not want the additional overhead of managing multiple employee accounts for each cloud provider, provisioning identities for partner organization personnel accessing internal data resources, or administering separate access control systems for each cloud service.

To support these requirements, the company implements a system that federates identities and externalizes access control. The use of a federation solution allows the company to maintain a single identity for each employee accessing the cloud services while accepting trusted credentials from other organizations. The company can manage access control for corporate data hosted in the cloud through a centralized authorization server that accepts access control policy definitions based on attribute values. External personnel accessing the collaboration platform use their home organization identities and have authorizations dynamically created by the authorization server-based user attributes.

Example Scenario 3 – Distributed Access Control for Public Safety

A hospital faces a crisis requiring the influx of temporary additional personnel (nurses, doctors, administrators, etc.). A doctor who works in a different region deploys to assist the hospital. In order to perform her duties, the doctor needs access to the medical systems and information used by the hospital's medical staff, but only to the data and systems required to perform her duties. Since the hospital and the doctor's home practice are subscribers to a third-party service that allows for the validation of member credentials and sharing of other attributes, the doctor presents her home practice credentials to the hospital. Once authenticated, attributes such as employee status, medical specialization and certifications are authorized for release by the doctor and shared with the hospital through the third-party service. Because the hospital is operating in an "always on" network-connected environment, an account is not created. When the doctor presents her home credentials to any hospital device or service, the service queries the third-party network to authenticate her credentials and authorize access for that session.

5. Security Characteristics

To address these three scenarios, this project will use a collection of commercially available technologies to demonstrate security and functional characteristics of an ABAC implementation. Each characteristic has one or more examples of security capabilities that can meet the intent of that characteristic. Desired technologies are those that contribute to a solution that allows for the greatest level of configurability and flexibility in achieving the characteristics described below.

The list of characteristics and corresponding capabilities below is not exhaustive. Furthermore, capabilities are listed to provide context for the characteristics and are not meant to be prescriptive.

Table 1. Functional characteristics

Functional characteristics	Example capabilities
authentication	• support requirement for multi-factor authentication to achieve degrees of authentication confidence using a combination of factors • support strong authentication between the relying party and attribute providers
attribute based policy enforcement and decisions	• make and enforce access control decisions based on policy defined by attributes
attribute lifecycle management	• attribute provisioning, modification, and de-provisioning
attribute federation	• pass attribute values between relying parties and attribute providers
identity federation	• a relying party can accept an authentication token from an identity provider based on the prior establishment of a trust relationship
identity lifecycle management	• create, read, update, and delete identities in local and federated identity stores
monitoring and reporting	• log all access requests, access decisions, and attributes used and subject identities • provide reports, queries, and analyses
policy lifecycle management	• create, update, audit, and delete attribute-based policies

Table 2. Security characteristics

Security characteristics	Example capabilities
confidentiality	protects: • transmission of identities and attributes traveling between enterprises and across the attribute exchange platform • data for all attribute and policy stores • attribute values used within policy decision logic
integrity	• provides the relying party with assurance that the identity and attributes received are from the intended source and have not been modified • supports strong authentication between the relying party and attribute provider
availability and performance	• assures that systems, access channels, and authentication mechanisms are working properly

auditing	• audits for compromises in the system's confidentiality, integrity and availability
privacy protection	• masks the RP from the IdP in any given transaction • safeguards that prevent the subject behavior from being tracked (i.e. by either the IdP or attribute exchange platform for RPs the subject interacts with) • prevents eavesdroppers from correlating messages or determining that two authentication sessions involved the same subject • supports data minimization and hiding, allowing attributes to be asserted without giving away more than is required; For example, if 'older than 21' is the request, the AP can return a Boolean derived from the subject birthdate, rather than revealing the entire birthdate to the RP

6. Approach

This building block focuses on the demonstration of ABAC technologies and how they can be integrated in an interoperable manner to address challenges across a wide array of business sectors. The initial focus is on the creation and demonstration of a platform that supports the federation of identity and exchange of attributes between attribute providers, identity providers, and relying parties. The capabilities that will be demonstrated include:

- an attribute exchange platform
- subject authentication to IdP, including multifactor authentication
- federation of subject identity to RP
- authorization of RP resources based on attribute assertions from APs and IdPs
- user consent of attribute sharing
- attribute refresh capability

It should be noted that this is an initial approach and that the building block process is intended to be iterative. As technologies and capabilities evolve, the initial technology stack of this building block may be augmented with additional functions

7. Relevant Standards

- NIST Special Publication 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- NIST Special Publication 800-63 rev. 2: Electronic Authentication Guideline
- NIST Policy Machine: Features, Architectures, and Specifications
- OIX: Attribute Exchange Trust Framework Specification
- FICAM Backend Attribute Exchange v2.0
- Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) v2.0 Standard
- Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) v2.0

- Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security Framework
- RFC 6749 - The OAuth 2.0 Authorization Framework
- OpenID Connect Core v1.0
- System for Cross-domain Identity Management (SCIM) v1.1
- User-Managed Access (UMA) Profile of OAuth 2.0
- World Wide Web Consortium Simple Object Access Protocol (SOAP) v1.2

8. Security Control Map

This table maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF), and other NIST activities. This exercise is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

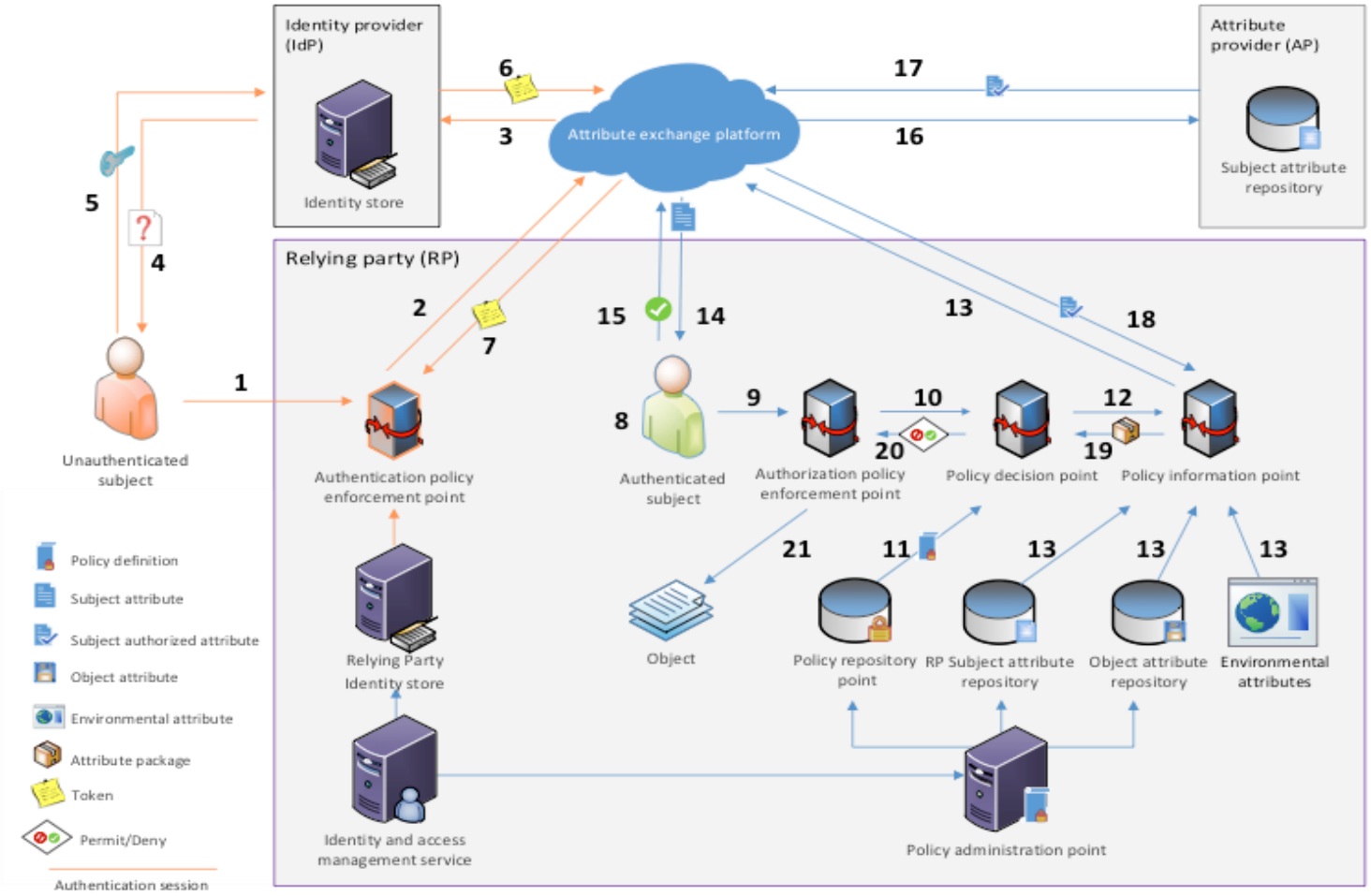
235	Example Characteristic		Cybersecurity Standards and Best Practices						
236	**Security Characteristic**	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS/CSC**	**CSA CCMv3.0.1**
237	identity and credentials	authentication,unique digital ID and type of authentication	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-1, IA Family	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-12	IAM-02, IAM-03, IAM-04, IAM-08
238	physical access	access to facility, rooms	Protect	Access Control	PR.AC-2: Physical access to assets is managed and protected	PE-1 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, PE-16	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	DCS-02, DCS-03, DCS-04, DCS-06, DCS-07, DCS-08, DCS-09
239	remote access	remote access via direct, indirect, and/or external means	Protect	Access Control	PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	A.6.2.2, A.13.1.1, A.13.2.1	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	IAM-07, IAM-08

240	access permissions	authorization	Protect	Access Control	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, 3, 5, 6, 16, CM-5	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	IAM-01, IAM-02, IAM-05, IAM-06, IAM-09, IAM-10
241	encryption and digital signature	protect the confidentiality and integrity of information	Protect	Data Security	PR.DS-1 and PR.DS-2: Data-at-rest and data-in-transit is protected	SC-28, SC-8, CM-5, SC-13, SI-7	A.8.2.3, A.13.1.1, A.13.1.2, A.13.2.3, A.14.1.2, A.14.1.3	CSC 16-16, CSC 17-7	EKM-03, IVS-10, DSI-03
242	provisioning	provisioning and permissions	Protect	Information Protection Processes and Procedure	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS Family, AC-2, AC-6	A.7.1.1, A.7.3.1, A.8.1.4		IAM-02, IAM-09, IAM-11
243	auditing and logging	log account activity	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU family	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CSC 4-2,CSC 12-1, CSC 12-10, CSC 14-2, CSC 14-3,	AAC-01

244	access control	access control mechanisms	Protect	Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC Family CM-7	A.9.1.2	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	IAM-03, IAM-05, IAM-13

Table 1: Security control map

9. HIGH-LEVEL ARCHITECTURE



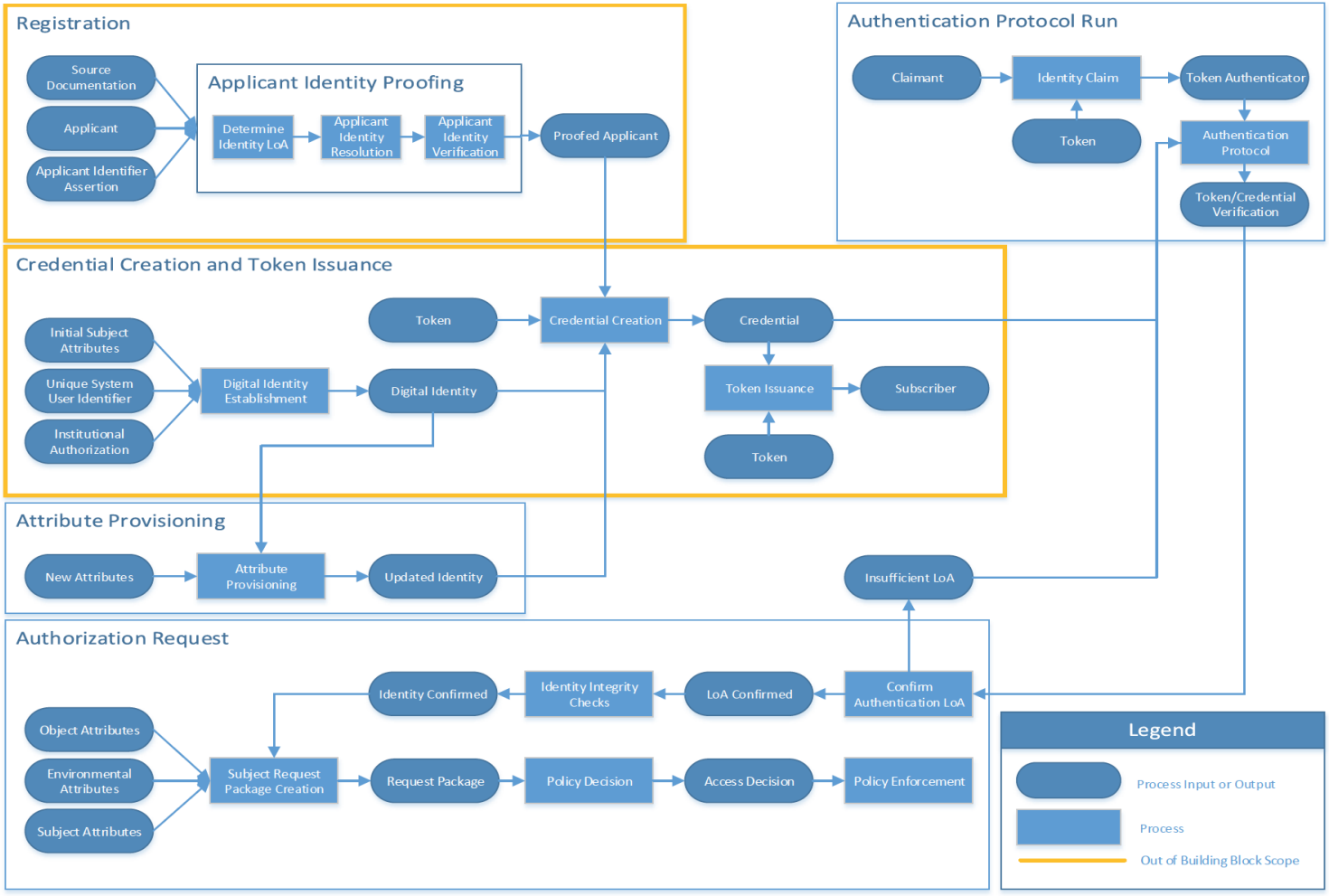
10. Component List

Examples of technologies applicable to this project include but are not limited to:

- identity management software that includes functions like: account provisioning, de-provisioning and directory services
- platform for exchanging attributes
- federation server
- databases for policy database, identity store, subject attribute repository, object and attribute repository
- policy server, to serve as the policy administration point
- access management system, which may include the policy decision point, policy enforcement point and context handler
- authentication server and components supporting two factor authentication
- cryptographic means to protect subject privacy during interactions between RPs, IDPs, APs and the attribute exchange platform

11. IDENTITY WORKFLOW

For the purposes of this building block, the below workflow demonstrates different stages of the identity lifecycle. Note that registration as well as credential creation and token issuance are outside the scope of this effort.



APPENDIX A: GLOSSARY OF TERMS

This building block, where possible, leverages external authoritative sources of terms for identity, credential and access management. The table below outlines terms as they are used within the context of this building block.

Term	Definition	Source
access control	a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes or other systems) according to that policy	RFC 4949
applicant	a party undergoing the processes of registration and identity proofing	NIST SP 800-63-2
assertion	a statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol	NIST SP 800-63-2
assurance	the grounds for confidence that the set of intended security controls in an information system are effective in their application	NIST SP 800-37-1
assurance level	a measure of trust or confidence in an authentication mechanism in terms of four levels: Level 1 - little or no confidence; Level 2 - some confidence; Level 3 - high confidence; Level 4 - very high confidence	OMB M-04-04
attribute	a claim of a named quality or characteristic inherent in or ascribed to someone or something	NIST SP 800-63-2
attribute based access control (ABAC)	a policy-based access control solution that uses attributes assigned to subjects, resources or the environment to enable access to resources and controlled information sharing	Authorization and Attribute Services Committee Glossary
attribute exchange platform	a technological means for federating attributes between enterprises	NCCoE
attribute provisioning	the binding of attributes to a subject (or to a subject's credential) or object	NCCoE
authentication	the process of establishing confidence in the identity of users or information systems	NIST SP 800-63-2
authentication protocol	a defined sequence of messages between a claimant and a verifier that demonstrates	NIST SP 800-63-2

	that the claimant has possession and control of a valid token to establish his/her identity, and optionally, demonstrates to the claimant that he or she is communicating with the intended verifier	
authentication protocol run	an exchange of messages between a claimant and a verifier that results in authentication (or authentication failure) between the two parties	NIST SP 800-63-2
authorization	a process for granting approval to a system entity to access a system resource	RFC 4949
certification authority	a trusted entity that issues and revokes public key certificates	NIST SP 800-63-2
claimant	a party whose identity is to be verified using an authentication protocol	NIST SP 800-63-2
credential	an object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a subscriber	NIST SP 800-63-2
digital certificate	a certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object	RFC 4949
digital signature	an asymmetric key operation where the private key is used to digitally sign an electronic document and the public key is used to verify the signature	NIST SP 800-63-2
federation	a trust relationship between discrete digital identity providers (IDPs) that enables a relying party to accept credentials from an external identity provider in order to make access control decisions; provides path discovery and secure access to the credentials needed for authentication; federated services typically perform security operations at run-time using valid NPE credentials	FICAM
identity	a set of attributes that uniquely describe an entity within a given context	Modified from NIST SP 800-63-2

identity provider (IdP)	a trusted entity that issues or registers subscriber tokens and generates subscriber credentials	Modified from NIST SP 800-63-2
identity proofing	a process that vets and verifies the information (e.g. identity history, credentials, documents) that is used to establish the identity of a system entity	FICAM
identity verification	the process of confirming or denying that a claimed identity is correct	Modified from FIPS 201
password	a secret that a claimant memorizes and uses to authenticate his or her identity	NIST SP 800-63-2
personal identity verification (PIV) card	defined by [FIPS 201] as a physical artifact (e.g., identity card, smart card) issued to federal employees and contractors that contains stored credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable)	NIST SP 800-63-2
possession and control of a token	the ability to activate and use the token in an authentication protocol	NIST SP 800-63-2
provisioning	creating user access accounts and assigning privileges or entitlements within the scope of a defined process or interaction; provide users with access rights to applications and other resources that may be available in an environment; may include the creation, modification, deletion, suspension or restoration of a defined set of privileges	FICAM
public key infrastructure	a set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates	NIST SP 800-63-2
registration	the process through which an applicant applies to become a subscriber of an identity provider and an registration authority proofs the identity of the applicant on behalf of the identity provider	Modified from NIST SP 800-63-2

registration authority (RA)	a trusted entity that establishes and vouches for the identity or attributes of a subscriber to an identity provider	Modified from NIST SP 800-63-2
relying party (RP)	an entity that relies upon the subscriber's token and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information	NIST SP 800-63-2
role based access control (RBAC)	a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.	Authorization and Attribute Services Committee Glossary
subscriber	a party who has received a credential or token from an identity provider	Modified from NIST SP 800-63-2
token	something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity	NIST SP 800-63-2
token authenticator	the output value generated by a token. The ability to generate valid authenticators on demand proves the claimant possess and controls the token	NIST SP 800-63-2
token issuance	process by which possession of a token is passed to an entity	NCCoE
token secret	the secret value, contained within a token which is used to derive token authenticators	NIST SP 800-63-2
verifier	an entity that verifies the claimant's identity by verifying the claimant's possession and control of a token using an authentication protocol	NIST SP 800-63-2

APPENDIX B: PUBLIC COMMENTS

ID	Comment Summary	Response
1	Since you include OAuth and XACML technology in the ABAC building block, and in the interest of enabling full Authorization Server/Resource Server loose coupling and wide-ranging attribute sourcing, information on the User-Managed Access (UMA) specifications may be useful to reference as well: • http://docs.kantarainitiative.org/uma/draft-uma-core.html • http://docs.kantarainitiative.org/uma/draft-oauth-resource-reg.html • http://docs.kantarainitiative.org/uma/draft-uma-claim-profiles.html • http://docs.kantarainitiative.org/uma/draft-uma-trust.html • (all also submitted as IETF I-Ds)	We have added the UMA profile under the relevant standards.
2	I read the document thoroughly and noted that the ABAC system is strongly reliant on the idea that federated identities and authentication is well in place in the industry. It is NOT. Among state and federal agencies and quasi-governmental agencies it often is, but not in the private industry. I think that the ABAC proposal you are making may miss the mark for this reason. I also think that a single sign on approach (technically different than a federated identity system) is more widely implemented and being implemented. Who is your audience? Private enterprise, fellow government types or large hospital systems?	As part of this effort we will be demonstrating an enterprise identity federation implementation. This implementation will be released in detail in the practice guide and can be used as reference for organizations that wish to enable identity federation within the enterprise. We have added a target audience section to the document. We feel this effort applies both to private and public sectors.

3	If you are going to mention both role-based access control AND attribute-based access control, please add a few sentences or references that distinguish them from each other. From a software engineer/system administrator perspective, there really is no difference that warrants separate mention. My suggestion is to remove the mention of RBAC or add a paragraph that outlines such distinctions. To enable a wide array of automated security decisions within and between enterprises, the identity and access control field has moved from individual access control lists, to centralized identity stores (databases), to role based access control, and now attribute based access control (ABAC).	To help better define the terms used within the document, we have added a glossary of terms to the document which included definitions of both RBAC and ABAC.
4	Use terminology consistent with NIST SP 800-162.	We have leveraged a good bit of NIST SP 800-162 to include an excerpt from the document in the background section. It is our goal to remain congruent with 800-162.
5	The document does not explicitly describe how the granularity of access control policies will be enhanced because there is no real discussion of increasing the range of possible attributes other than the mention of 'environment' attribute where additional attributes could be added.	This document mirrors NIST 800-162 in its discussion of environmental attributes as the third attribute type alongside subject and object attributes. This effort will demonstrate access control decisions based on all three types and we will release the implementation documentation as part of our NIST special publication series. We are open to suggestions of other attribute types.

6	Lines 6-8: "…the identity and access control field has moved from individual access control lists, to centralized identity stores (databases), to role based access control, and now attribute based access control (ABAC)" This makes it appear to be a progression or continuum when it really isn't. They are three very different things. Individual ACLs refers to Discretionary Access Control, which gives the owner of an object the ability to control who can see that object. Under DAC, once a user gets access they can write it to another object and give it broader access. Centralized identity stores are not an access control mechanism – but repositories for enterprise or organization management to facilitate e.g., single-sign-on. As such, they can provide Enterprise-level definitions of users or roles, but the underlying mechanisms (DAC or RBAC) is the same. RBAC could be discretionary or non-discretionary: it could be done with role-based ACLs at the object level, or it could be done by overall role-based restrictions on operations that can be performed (which essentially limits which objects can be accessed).	Agreed. The verbiage in the background sections has been modified to better reflect the nuances of various access control methodologies.
7	Lines 14-17: federated identity management environment: not clear how this is different than a centralized ID database and the ability to use arbitrary attributes, not just roles	This verbiage has been removed from the document.
8	Table page 4, data protection: Although the discussion looks at transmission integrity, it does not appear to address attribute integrity in the sense of ensuring stored attributes accurately reflect the real world attribute with confidence. In other words, attacks that give users attributes that they really don't possess is still possible.	This build will not be address attribute assurance as we feel the standards space has not yet developed in this area.

9	Table page 4, identity lifecycle management: One of the more novel aspects of this approach is the environment attribute. You should expand on the discussion of this attribute, noting that it provides the ability to integrate resiliency into the policy, and thus could be used to support dynamic controls in NIST 800-53.	In build #1, we will demonstrate some examples of environmental attributes. We would welcome a larger discussion around which environmental attributes might be most meaningful.
10	Lines 139-154: Is there an assurance issue with implementing the ABAC software on a common OS DAC scheme? In other words, the ABAC approach ultimately must be implemented as hooks that occur before (or as part of) the basic operating system access control checks. This could provide the opportunity for those checks to be bypassed; for any access control scheme to be strong, it needs to be non-bypassable.	There are several implementations possible, some that use a loosely coupled enforcement point that would be external to the OS, others that may involve the enforcement being integrated into the operating system. The final architecture will be dependent on the technology of the companies partnering with the NCCoE in support of this effort.
11	Line 11: Note that a role is a another attribute of a user. So “attribute” based access control is just a generalization of role-based or discretionary access control (depending on whether it is discretionary or not).	Correct, role is simply one of a myriad of attributes that can be used with ABAC.