NIST SPECIAL PUBLICATION 1800-3B

Attribute Based Access Control

Volume B:
Approach, Architecture, and Security Characteristics

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
The MITRE Corporation
McLean, VA

September 2017

SECOND DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-3b, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3b, 48 pages, September 2017, CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

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

Public comment period: September 20, 2017 through October 20, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

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 practice guide details a collaborative effort between the NCCoE and technology providers to demonstrate a standards-based approach to attribute based access control (ABAC).

This guide discusses potential security risks facing organizations, benefits that may result from the implementation of an ABAC system, and the approach the NCCoE took in developing a reference architecture and build. It includes a discussion of major architecture design considerations, an explanation of security characteristic achieved by the reference design, and a mapping of security characteristics to applicable standards and security control families.

For parties interested in adopting all or part of the NCCoE reference architecture, this guide includes a detailed description of the installation, configuration, and integration of all components.

KEYWORDS

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

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Paul Timmel	NIST National Cybersecurity Center of Excellence
Paul Grassi	NIST National Strategy for Trusted Identities in Cyberspace
Mike Garcia	NIST National Strategy for Trusted Identities in Cyberspace
Naomi Lefkovitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriaolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggenstam	NextLabs Inc
John Conduit	NextLabs Inc
Srikanth Karanam	NextLabs Inc
Adam Madlin	Symantec Corporation
Steve Kruse	Symantec Corporation
Steve Schmalz	RSA
Ben Smith	RSA

Name	Organization
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb
Pete Romness	Cisco
Kevin McFadden	Cisco
John Eppish	Cisco
Chris Ceppi	Situational Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Ping Identity	PingFederate Federation Server
NextLabs	Entitlements Management Policy Enforcement Point
Microsoft	Policy Controller Policy decision point
RSA	Control Center Policy Administration Point
Symantec	Active Directory

Technology Partner/Collaborator	Build Involvement
Cisco	SharePoint

Contents

List of Figures

List of Tables

1 Summary

Traditionally, granting or revoking access to information technology (IT) systems or other networked assets requires an administrator to manually enter information into a database—perhaps within several systems. This method is inefficient and does not scale as organizations grow, merge, or reorganize. Further, this approach may not be best for preserving privacy and security: all users of a database have access to all its information, or administrators must limit access by constructing groups with specific permissions.

Attribute based access control (ABAC) is an advanced method for managing access rights for people and systems connecting to networks and assets. Its dynamic capabilities offer greater efficiency, flexibility, scalability, and security than traditional access control methods, without burdening administrators or users.

Despite ABAC's advantages and federal guidance that comprehensively defines ABAC and the considerations for enterprise deployment [1], adoption has been slow. In response, the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example of an advanced access control system. Our ABAC solution can manage access to networked resources more securely and efficiently, and with greater granularity that traditional access management. It enables the appropriate permissions and limitations for the same information system for each user based on individual attributes, and allows for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

Our approach uses commercially available products that can be included alongside your current products in your existing infrastructure.

This example solution is packaged as a "How To" guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. It can save organizations research and proof-of-concept costs for mitigating risk through the use of context for access decisions.

1.1 Challenge

Enterprises face the continual challenge of providing access control mechanisms for subjects requesting access to corporate resources (e.g., applications, networks, systems, and data). The growth and distributed nature of enterprise resources, increasing diversity in users, credentials, and access needs, as well as the need to share information among stakeholders that are not managed directly by the enterprise, has given rise to the demand for an access control system that enables fine-grained access decisions based on a range of users, resources, and environmental conditions.

Consider a patient submitting a health insurance claim. A claims examiner needs to know just billing and diagnostic codes and a few pieces of demographic data in order to permit reimbursement. Interacting with the same system, the patient's doctor needs to verify that the diagnosis and referral information is for the correct patient, but does not need to see payment or address information. The patient needs access to the claim's status, while the patient's employer only needs to see the number of claims submitted by the employee. The insurance company provides a single service, claims processing, but each user of the service has different access needs.

An advanced method of access management would increase security and efficiency by seamlessly limiting some users' views to more granular data. It would enable the appropriate permissions and limitations for the same information system for each user based on individual attributes, and allow for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

1.2 Solution

This document details our approach in developing a standards-based ABAC solution. Through discussions with identity and access management (IdAM) experts and collaborating technology partners, the NCCoE developed a set of security characteristics required to meet the IdAM risks facing today's enterprises. The NCCoE mapped security characteristics to standards and best practices from NIST and other standards organizations, then used products from our technology partners as modules in an end-to-end example solution that mitigates IdAM risks.

1.3 Risks

Access control systems implement a process for defining security policy and regulating access to resources such that only authorized entities are granted access according to that policy. They are fundamental to mitigating the risk of unauthorized access from malicious external users and insider threats, as well as acts of misfeasance. In the absence of a robust access control system, enterprises struggle to control and audit access to their most sensitive data and risk the loss or exposure of critical assets, loss of trust in employees and from customers, and harm to brand reputation.

As technology pervades all business processes, access control systems must support increasing diversity in users, credentials, and access needs, including digital identities from external security domains. This increases the overhead associated with managing access control systems and introduces increased risk of unauthorized access as organizational policies escalate in complexity.

1.4 Benefits

Our example implementation:

- allows products and capabilities to be adopted on a component-by-component basis, or as a whole
- supports organizations with a diverse set of users and access needs, reducing the risks of "privilege creep" (a user obtains access levels beyond those needed), and creating efficiencies in the provisioning of accesses
- reduces the number of identities managed by the enterprise, thereby reducing costs associated with those management activities
- enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policy on subjects and objects, and by using a variety of environmental decisions
- supports business collaboration by allowing the enterprise to accept federated identities and eliminating the need to pre-provision access for identities being federated

- supports the centralization of auditing and access policy management, creating efficiencies of policy management and reducing the complexity of regulatory compliance

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this approach to identity and access management. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-3a: *Executive Summary*
- NIST SP 1800-3b: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-3c: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-3a)*, which describes the:

- challenges enterprises face in implementing and using access control mechanisms
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-3b,* which describes what we did and why. The following sections will be of particular interest:

- Section 4.4, Risk Assessment, provides a description of the risk analysis we performed
- Section 4.4.3, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-3a,* with your leadership team members to help them understand the importance of adopting standards-based access management approaches to protect your organization's digital assets.

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-3c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution that would support the deployment of an ABAC system and the corresponding business processes. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Section 4.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to abac-nccoe@nist.gov.

2.1 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

3 Introduction

Any decision to implement ABAC within an organization must begin with a solid "business case." An important set of inputs to the business case are the strategic and tactical risks to the organization from the standpoint of access control, as outlined in Sections 4.4.1 and 4.4.2. This business case could be an independent initiative or a component of the organization's strategic planning cycle. Individual business units or functional areas typically derive functional or business unit strategies from the overall organization's Strategic Plan. The business drivers for any ABAC project must originate in these Strategic Plans, and the decision to determine if an organization will invest in ABAC by implementing the solution in this practice guide will be based on the organization's decision-making process for initiating new projects.

Some organizations use a systems engineering-based approach to the planning and implementation of their IT projects. Organizations wishing to implement an ABAC system should conduct robust requirements development, taking into consideration the operational needs of each system stakeholder. Standards such as ISO/IEC 15288:2015, Systems and software engineering – System life cycle processes [2], and NIST Special Publication (SP) 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [3], provide guidance in this endeavor. With both these standards, organizations can choose to adopt only those sections of the standard that are relevant to their environment and business context.

In addition to ABAC, basic read, write, and execute permissions, discretionary access control (DAC), mandatory access control, and RBAC are some of the many access control solutions from which organizations can choose. NIST SP 800-160 recommends a thorough analysis of alternative solution classes accounting for security objectives, considerations, concerns, limitations, and constraints. An analysis of alternatives may conclude that for a particular organization's requirements, RBAC or other access control mechanism are most appropriate. In addition, while NCCoE has not implemented such combinations, some authors have implemented and documented hybrid ABAC-RBAC solutions [4], [5].

3.1 Background

NIST SP 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 (a) the subject or user requesting access, (b) the target object for which access or a transaction is being requested, and (c) 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" [6], [1].

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) [7]. Built on an eXtensible Markup Language (XML) foundation, XACML is designed to allow externalized, run-time access control decisions using attribute-based policy definitions.

3.2 ABAC and RBAC Considerations

RBAC simplifies identity management by grouping users with similar access needs by role. Privileges can then be assigned to a role rather than an individual user. This simplification has led to the widespread adoption of RBAC for logical access control. However, many organizations face growing diversity in both types of users and their access needs.

This diversity introduces a number of administrative and policy enforcement challenges. Administrators manage access policy for multiple applications and security domains, each often requiring discrete access control policies. Most systems implement access control in different ways, making it hard to share information across systems and requiring administrators to configure access for like users uniquely in each system, typically by using the roles or groups native to that system.

These roles are sometimes insufficient in the expression of real-world access control policies and cannot handle real-time environmental considerations that may be relevant to access control decisions; examples such as the location of access, time of day, threat level, and client patch level illustrate how enterprises could be afforded a wider range of decisions based on the amount of risk they perceive or are willing to accept. Similarly, RBAC does not readily support attributes relating to authentication context, referring to assurance of a user's login process.

An organization facing the above challenges may meet them using an attribute-based system. Using RBAC, access privileges are assigned to roles. Users are then provisioned those privileges by adding them to a role. This differs from attribute-based systems, which use name:value pairs to establish user, object, and environmental attributes and allow organizations to establish access policy via attribute combinations. These access control policies are then evaluated at access request time for a specific user and resource. Essentially, with RBAC, users arrive at the protected resource with their privileges via an assigned role, while with ABAC, user resource privileges are determined just in time. It is this just-in-time privilege determination that leverages the externalization of policy and enables the incorporation of attributes with dynamic states – such as the environment, resource, user and authentication context.

Attribute policy definitions establish a relationship between subject and object that does not change as attribute values change, thus reducing the opportunity for privilege creep and maintaining separation of duties. ABAC systems have the ability to permit new types of access requests without the need to alter the current set of subject/object relationships. Instead, the enterprise can define a new attribute or attributes (or a combination of currently used attributes) that represents the new level of access needed and then define an attribute-based policy that supports this level of access. Business logic to be translated into attribute-based policies that govern access decisions, allowing for a common and centralized way of expressing policy, and computing and enforcing decisions, over the access requests for diverse systems.

3.3 ABAC Leveraging Identity Federation

As enterprises look to keep up with leading-edge technology solutions, they face the identity management challenge of allowing a diverse set of digital identities to access many different organizational applications and resources. Commonly, this requires recognizing digital identities from external security domains, which are typically trusted strategic business stakeholders. Enterprises have realized that supporting this 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 uses federation profiles.

Identity federation profiles define the methods used to convey a set of user information from the identity provider (IdP), or organization where the user is known, to the target location or relying party (RP) that needs to acquire the information for some use such as access control. These technologies leverage widely accepted, open, web-oriented, standardized communication languages, like the Security Assertion Markup Language (SAML) version 2.0 standard from OASIS [8], which uses XML, or the OpenID Connect (OIDC) standard from the OpenID Foundation [9] built upon JavaScript Object Notation, to carry the assertions about a user. 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 (the RP) to make access control decisions.

In some cases, an RP may need to obtain attributes about a user from a source other than the user's IdP. In such cases, the RP may receive a user's attributes from a trustworthy external source known as an attribute provider (AP). Commonly, identity federation profiles are used to facilitate the federation of attributes from the AP to the RP.

Enterprises wishing to participate in federation must have a degree of trust in the organization from which they are receiving identity and attribute information. To facilitate these trust relationships, nonprofit organizations such as the Kantara Initiative and the Open Identity Exchange have proposed or issued trust framework specifications that provide a set of contracts, regulations, and commitments. These specifications enable parties to a trust relationship to rely on identity and attribute assertions (via federation profiles) from external entities.

Identity federation allows external users to gain access to web-based protected resources without the need for the RP to manage the identity. When identities and access decisions are abstracted into a common set of attributes, access decisions can be externalized and policies can be established across business units or even organizational boundaries. Identity and attribute federation enables access decisions for users from trusted IdPs, even if the users have not previously been provisioned by the RP (sometimes referred to as the "unanticipated user" scenario).

3.4 Security Standards

Table 3-1 lists the security standards and best practices considered during the development of this practice guide.

Table 3-1 Related Security Standards and Best Practices

Related Technology	Relevant Standard	URL
General Cybersecurity	NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
	NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	http://dx.doi.org/10.6028/NIST.SP.800-53r4
	ISO/IEC 27001, Information Security Management	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
	SANS Institute, Critical Security Controls	https://www.sans.org/critical-security-controls/
	ISACA, COBIT 5	http://www.isaca.org/COBIT/Pages/Product-Family.aspx
	Cloud Security Alliance, Cloud Controls Matrix v3.0.1	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
Risk Management	NIST SP 800-30- r1, Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
Requirements Engineering	ISO/IEC 15288:2015, Systems and software engineering – System life cycle processes	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711
	NIST SP 800-160 (Draft), Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems	http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
Access Control (ABAC)	NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations	http://dx.doi.org/10.6028/NIST.SP.800-162

Related Technology	Relevant Standard	URL
Access Control (NGAC)	INCITS 499-2013, Information Technology – Next Generation Access Control – Functional Architecture (NGAC-FA)	http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013
Access Control (RBAC)	American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) 359-2012, Information Technology – Role Based Access Control	http://www.techstreet.com/products/1837530
Language (OIDC)	OpenID Connect Core 1.0	http://openid.net/specs/openid-connect-core-1_0.html
Language (SAML)	OASIS Security Assertion Markup Language (SAML) V2.0	http://saml.xml.org/saml-specifications
Language (WS-Federation)	OASIS Web Services Federation Language (WS-Federation) Version 1.2	http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html
Language (XACML)	eXtensible Access Control Markup Language (XACML) Version 3.0	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
Language (XML)	Extensible Markup Language (XML) 1.1 (Second Edition)	http://www.w3.org/TR/2006/REC-xml11-20060816/
Protocol (HTTP and HTTPS)	RFC 7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	https://tools.ietf.org/html/rfc7230
Protocol (LDAP)	RFC 4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	https://tools.ietf.org/html/rfc4510
Protocol (OAuth)	IETF Request for Comments 6749, The OAuth 2.0 Authorization Framework	http://tools.ietf.org/html/rfc6749

Related Technology	Relevant Standard	URL
Protocol (TLS)	NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://dx.doi.org/10.6028/NIST.SP.800-52r1
	RFC 2246, TLS Protocol 1.0	https://tools.ietf.org/html/rfc2246
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	https://tools.ietf.org/html/rfc4346
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
PKI	PKI Technical Standards	http://www.oasis-pki.org/resources/techstandards/

358

4 Approach

4.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions.

4.2 Scope

This project began with discussions between the NCCoE, IdAM experts across NIST, and IT security vendors partnered with the NCCoE. These discussions enumerated an array of technologies and standards relevant to the ABAC space, but very few implementations of ABAC technology.

In response, the NCCoE drafted a white paper [10] that identified numerous desired solution characteristics. After two rounds of public comments on the document, the NCCoE worked with its NCEPs to design an architecture that would demonstrate an array of ABAC capabilities. This build does not include every characteristic found in the white paper, but does include the relevant set of ABAC capabilities based on the technology available to us through the portfolios of the NCCoE's NCEPs. The scope of this build is the successful execution of the following capabilities:

- identity and attribute federation between trust partners
- user authentication and creation of an authentication context
- fine-grained access control through a policy enforcement point (PEP) closely coupled with the application
- creation of attribute-based policy definitions
- secondary attribute requests
- allowing RP access decisions on external identities without the need for pre-provisioning

4.3 Assumptions

4.3.1 Modularity

This example solution is made of many commercially available parts. You might swap one of the products we used for one that is better suited for your environment. We also assume that you already have some IdAM solutions in place. The use of standard protocols such as SAML, LDAP, and Web Service (WS)-Federation enhances the modularity of the architecture to improve your identity and access/authorization functions without major impact to your existing infrastructure. For organizations that want to limit their ABAC deployment to resources residing on Microsoft SharePoint, this solution can be implemented alongside an RBAC implementation, with the lone configuration requirement of enabling attributes inside Microsoft Active Directory (AD) or other identity stores as appropriate.

4.3.2 Business Policy Language

This build leverages NextLabs technology to decompose natural language business policy into attribute-based digital policies. We implemented example business policies that we feel demonstrate the capabilities of the solution that address business needs. When implementing an ABAC solution, enterprises will need to determine the set of natural language business policies that best meet their access control needs and risk tolerances.

4.3.3 Attribute Semantics and Syntax

An ABAC IdAM infrastructure by its nature is dependent on a predefined set of attribute name:value pairs available for use within its set of rules to determine authorization privileges for users and web service clients. The use of federation, as with this build, expands the domain of agreed-upon attributes to include trusted federation partners. Often a common attribute dictionary is in use for all parties. However, enterprises may look to a third-party service, typically called a trust broker, to facilitate attribute exchange and normalization.

For the purposes of this build, we have chosen an example set of attribute values that we feel is representative of business needs. When implementing an ABAC solution, enterprises will need to determine the set of attribute syntax and semantics that best meets their unique access control needs.

4.3.4 Attribute Provenance

In this build, we utilize Microsoft AD, RSA Adaptive Authentication, and Microsoft SharePoint as sources for attributes. Depending on the types of policy an enterprise wishes to implement in attribute-based logic, there will be diversity in the appropriate sources of attribute information. When planning an ABAC implementation, enterprises should consider their ability to collect the attributes required for access decisions and the level of trust they have with the attribute provider and/or sources of attribute information.

4.3.5 Trust Relationships for Identity Federation

The use of identity federation requires a degree of trust between pairs of sharing partners. When establishing this trust relationship, enterprises need to agree upon the technical specification of the trust relationship as well as the types of metadata to be exchanged. Enterprises should make a decision based on their risk profile when determining the stakeholders with which they wish to establish trust relationships.

This build establishes a trust relationship between two theoretical organizations through the exchange of attribute and identity information between two Ping Federate instances using SAML 2.0. In order to demonstrate federation capabilities, this build assumes complete trust between exchanging parties.

4.3.6 Human Resources Database/Identity Proofing

This build is based on a simulated environment. Rather than re-create a human resources database and the entire identity proofing process in our lab, we assume that your organization has the processes, databases, and other components necessary to establish a valid identity.

4.3.7 Technical Implementation

The guide is written from a technical perspective. Its foremost purpose is to provide details on how to install, configure, and integrate components. We assume that enterprises have the technical resources to implement all or parts of the build, or have access to companies that can perform the implementation on their behalf.

4.3.8 Limited Scalability Testing

We experienced a major constraint in terms of replicating the volume of access requests that might be generated through an enterprise deployment with a sizable user base. We do not identify scalability thresholds in our builds, as those depend on the type and size of the implementation and are particular to the individual enterprise.

4.4 Risk Assessment

NIST SP 800-30, *Risk Management Guide for Information Technology Systems* states, "Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, material available to the public. The risk management framework (RMF) guidance as a whole proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

According to NIST SP 800-30-r1, *Risk Management Guide for Information Technology Systems*, "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."

Through a series of workshops held throughout the country and with industry input, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity* (CSF). The CSF provides industry with a risk-based approach for developing and improving cybersecurity programs. Access control has been identified as a core element of the CSF due to the risks posed by unauthorized access to sensitive data, devices, or IT applications. NIST SP 800-39, *Managing Information Security Risk,* provides guidance on organization-wide risk management. These documents proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

4.4.1 Strategic Risks

Strategic risks are risks applicable to the enterprise or organizational level. The following sections describe strategic risks from unauthorized access.

4.4.1.1 Reputation Risk

Public disclosure (by the attacker or through news reports) of an unauthorized access to sensitive information could jeopardize an organization's reputation. Customers and partners could conclude that the organization failed to put adequate access control restrictions in place. This could result in loss of customers, credibility, and market share.

4.4.1.2 Financial Risk

The organization may incur financial losses directly from the theft of money or indirectly from the additional cost of restoring data, equipment, and services. Intruders may blackmail the organization and extort money by threatening to exploit the security breach or publicize the event. Customers may claim that the organization was responsible for any financial loss they incurred due to lack of access controls.

4.4.1.3 Legal Risk

Security or privacy breaches can expose an organization to lawsuits from employees, investors, customers, or other affected parties.

4.4.1.4 Compliance Risk

Many organizations have to deal with multiple regulations that require the implementation of appropriate safeguards to protect customer and employee data. The lack of an adequate access control mechanism could cause the organization to become noncompliant with applicable regulations.

4.4.1.5 Operational Risk

A user who gains unauthorized access could introduce malicious code, using an initial breach as a launching pad to attack the infrastructure, intentionally overload resources, and disrupt critical ongoing operations. This could prevent legitimate users from access to critical resources in the course of their duties, resulting in a loss of productivity. The intruder could modify or erase critical corporate data, preventing normal operations. The delay from recovering data lost and fixing breaches may occupy operation resources, thus degrading the quality of information services.

4.4.1.6 Intellectual Property Risk

An intruder could rob an organization's intellectual property assets such as ideas, inventions, trade secrets, and creative expressions.

4.4.1.7 Third Party Risks

If the system is a part of a cooperated (or federated) operation, an intrusion due to ineffective access control might cause a delay in operation or even result in a breach to the cooperated (or federated) network. A breach from an originating system could propagate to an RP, where additional breaches could occur.

4.4.2 Tactical Risks

Tactical risks are risks applicable at the information system level. The following tactical risks result from unauthorized access.

4.4.2.1 Insider Threat

Individuals who have a legitimate need to access only a subset of applications and data may extend their reach into domains that should be restricted. Lack of appropriate mechanisms to restrict such access could result in improper use of resources or information.

4.4.2.2 Limited Provisioning

Inappropriate access control mechanisms may be more prone to administrative errors due to cumbersome workflows or procedures. For example, for a large number of users and resources, access control lists are challenging to maintain as individuals are transferred or terminated. In addition, delegation of provisioning may be available only to privileged users (e.g., system administrators), but this functionality maybe necessary to support business needs.

4.4.2.3 Unanticipated Users

Many access control mechanisms are unable to support unanticipated users or are prone to delays in provisioning new users due to their inherent design. This might delay legitimate users from accessing resources they need to perform critical functions within a reasonable timeframe.

4.4.2.4 Dynamic Access

Many access control mechanisms are unable to support dynamic access decisions where risk holders desire to change allowable access requests as environmental conditions change (e.g., Code Red).

4.4.2.5 Information Sharing

Many access control mechanisms can only protect organizational information within the confines of established system security boundaries. Such a capability may be required to facilitate information sharing in a federation to support an organization's mission priorities.

4.4.2.6 Coarse-Grained Operations

Many access control mechanisms can only protect resources where the context of the access applies to fine atomic operations (e.g., Create, Read, Update Delete), whereas more comprehensive operations that might include a sequence of steps to complete a workflow may not be supported.

4.4.2.7 Cost

Some access control mechanisms may cost more than others, depending on the business and operation requirements of the organization. The cost includes design, development, maintenance, and interoperation with legacy or cooperated systems.

524 ### 4.4.3 Security Control Map

525 Table 4-1 lists the major use case security characteristics. For each characteristic, the table provides the matching function, category, and
526 subcategory from the NIST CSF [11], as well as mappings to controls from other relevant cybersecurity standards.

527 **Table 4-1 Use Case Security Characteristics Mapped to Relevant Standards and Controls**

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4 [12]	ISO/IEC 27001 [13]	SANS CSC [14]	ISACA COBIT 5 [15]	CSA CCMv3.0.1 [16]
Identity and Credentials	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	DSS05.04, DSS06.03	IAM-02, IAM-03, IAM-04, IAM-08
Remote Access	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	APO13.01, DSS01.04, DSS05.03	IAM-07, IAM-08
Access Permissions	Protect	Access Control	PR.AC-4: Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	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
Encryption and Digital Signature	Protect	Data Security	PR.DS-1 and PR.DS-2: Data-at-rest and data-in-transit are protected.	SC-28, SC-8	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

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4 [12]	ISO/IEC 27001 [13]	SANS CSC [14]	ISACA COBIT 5 [15]	CSA CCMv3.0.1 [16]
Provisioning	Protect	Information Protection Processes and Procedure	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	PS Family	A.7.1.1, A.7.3.1, A.8.1.4		APO07.01, APO07.02, APO07.03, APO07.04, APO07.05	IAM-02, IAM-09, IAM-11
Auditing and Logging	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,	APO11.04	AAC-01
Access Control	Protect	Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	AC-3, CM-7	A.9.1.2	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	DSS05.02	IAM-03, IAM-05, IAM-13

4.5 Technologies

Table 4-2 lists all of the technologies used in this project and provides a mapping between the generic application term, the specific product used, and the security control(s) that the product provides. Refer to Table 4-1 for an explanation of the CSF Subcategory codes.

531 **Table 4-2 Security Characteristics Mapped to Relevant Build Products**

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
Identity and Credentials	Microsoft SharePoint, Ping Federate IdP, RSA Adaptive Authentication	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
Remote Access	Microsoft SharePoint, NextLabs Policy Controller and Control Center, Ping Federate RP, Ping Federate IdP	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
Access Permissions	Microsoft SharePoint and AD, NextLabs Policy Controller and Control Center	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
Encryption and Digital Signature	Microsoft SharePoint, NextLabs Policy Controller, Ping Federate RP, Ping Federate IdP, RSA Adaptive Authentication	PR.DS-1 and PR.DS-2: Data-at-rest and data-in-transit is protected	SC-28, SC-8	A.8.2.3, A.13.1.1, A.13.1.2, A.13.2.3, A.14.1.2, A.14.1.3
Provisioning	Microsoft AD	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS Family	A.7.1.1, A.7.3.1, A.8.1.4
Auditing and Logging	Microsoft SharePoint, NextLabs Policy Controller, Ping Federate RP, Ping Federate IdP, RSA Adaptive Authentication	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,

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
				A.12.4.4, A.12.7.1
Access Control	NextLabs Policy Controller and Entitlement Manager and Control Center	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, CM-7	A.9.1.2

This build implements the security characteristics through available products, described below, from NCEP organizations. Section 5, Architecture, provides additional insight into the way we used the products.

- The build is centered on a resource server to be protected by the ABAC solution. In this case, Microsoft SharePoint was used. It is a web-based application within the Windows operating environment commonly deployed as a document management system for intranet, extranet, or cloud repository purposes. SharePoint natively uses an RBAC authorization environment, but it also supports the use of attributes within the user transaction request, a capability Microsoft refers to as being “claims aware.” SharePoint also allows for tagging data within its repository, which can be leveraged as object attributes.
- Another important component of the build is identity management software, in this case Microsoft AD. AD is a set of services that reside within the Windows server environment. AD functions as an identity repository based on LDAP technology, but also provides authentication and authorization services. AD also includes the ability to provision and de-provision user identities and create, modify, and delete subject attributes.
- The build needed PEP functionality, and it is provided by NextLabs Entitlement Management, which interfaces and integrates with products such as SharePoint and SAP to provide finer granularity of access decisions than that available using the native access control mechanisms. Entitlement Management is closely coupled with the target application; it traps user access requests and passes access decisions to the policy decision point (PDP).
- Policy life-cycle management and auditing/reporting are facilitated by the NextLabs Control Center, which hosts policy administration point (PAP) functionality, where attribute-based policies are defined and deployed. The NextLabs Policy Controller, as an element of Control Center, hosts the PDP, which uses the policy definitions and subject, object, and environmental attributes to make an access accept-or-deny decision that the PEP enforces. Control Center also includes dashboards, analytics, reports, and monitoring to offer insight into access patterns.
- The build includes a federation server/platform for exchanging identities and attributes. Ping Identity’s PingFederate serves as a federation identity system or trust broker, an identity management component, and supports integrated single sign-on (SSO) within an enterprise IdAM infrastructure. It supports standards-based protocols such as SAML, OAuth, and OpenID Connect. Its trust broker capabilities allow for necessary transformation and interface options between federated partners and internal proprietary target resources. When used within an identity provider, it offers options for integrating with authoritative attribute sources.
- The build has an authentication server that supports multifactor authentication. For this build, RSA Adaptive Authentication (AA) provides this functionality. It is an authentication and environmental analysis system. Its capabilities include a variety of adaptive opportunities, such as Short Message Service (SMS) texting, fingerprint analysis, and knowledge-based authentication. From an environmental perspective, AA collects information such as patch level, operating system, and location, and generates a risk score associated with user authentication. A risk score threshold can then be defined, which, if exceeded, can force a user to step up to an additional authentication mechanism.
- A final necessary component of the build is a certificate authority. In this case, Symantec’s Managed PKI Service product is used for secure issuance of Public Key Infrastructure (PKI)-based certificates. The Symantec certificates enable mutual transport layer security (TLS), digital

signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest within an IT environment.

5 Architecture

5.1 Overview

The following sections detail the ABAC and identity federation architecture that NCCoE staff members and collaborators built. The architecture description details how components from five NCEPs were integrated to achieve the following demonstrable capabilities:

5.1.1 User Authentication and the Creation of an Authentication Context

Our scenario starts with an unauthenticated user attempting to access a target resource for the first time. The user's browser is redirected to his or her home organization (the IdP) for authentication and includes, as required for the target resource, additional (step-up) authentication, and gathering of environmental attributes and authentication context information about the user.

5.1.2 Federation of a User Identity and Attributes

This build demonstrates the federation of subject and environmental attributes between an IdP and an RP. This means that, after the user is authenticated by his or her IdP, the federation protocol that initially redirected the user to the IdP is now used to redirect the user back to the RP carrying the requested identity and attribute information.

5.1.3 Fine-Grained Access Control through a PEP Closely Coupled with the Application

Out of the box, SharePoint access control is more oriented to role-based or group-based DAC. In this build, we enhance the SharePoint access control environment through the deployment of a closely integrated policy enforcement, allowing for a finer degree of granularity based on subject, object, and environmental attributes.

5.1.4 The Creation of Attribute-Based Policy Definitions

This build allows for the translation of business policies into a set of attribute-based policy definitions. These policy definitions establish a relationship between subject, object, and environmental attributes that controls a user's ability to access the RP's resources.

5.1.5 Secondary Attribute Requests

This build provides the ability to make runtime requests for additional attributes from the IdP, should insufficient attributes be presented when making an access decision. When a user accesses a particular resource, or returns to access additional resources, the access control components that we have associated with SharePoint might find that additional subject attributes are needed beyond those that were initially provided. Our build includes components able to search a local cache for the missing attributes and, if not there, issue a new request to the IdP via a SAML attribute request/response for the missing user attributes.

5.1.6 Allow RP Access Decisions on External Identities without the Need for Pre-Provisioning

This build relies upon the trust relationship between the IdP and RP, which enables identity and attribute federation. Once this trust relationship has been established between two organizations, the RP can make runtime access decisions on any individual presenting a credential from the IdP without the need to pre-provision that individual.

5.2 ABAC Architecture Considerations

There are many facets to architecting an ABAC system. As noted in Section 4.3, Assumptions, these include the development of policy, procedure, and/or functional requirements before the selection of technology components. They also include an analysis of business drivers such as those in Section 2.

From a technical perspective, this section outlines a few of the options that an architect will face. Section 5.3, Technology and Architecture of the NCCoE Build, presents the actual architecture chosen for this build.

5.2.1 Industry Standards

When selecting ABAC technologies, it is important to consider the protocols implemented by each technology and whether those protocols are defined by a standards organization. Utilizing standard protocols promotes product interoperability and modularity, and may offer standardized APIs in the event that system requirements drive the need for custom components.

As mentioned earlier, one of the standards for implementing ABAC is XACML. Built on top of XML, XACML offers a core set of rule capabilities for making attribute-based policy definitions and also specific request and response messages for exchange between PEPs and PDPs. Specific details of the XACML 3.0 architecture can be found in the OASIS documentation [7].

Although XACML was developed primarily to fill the need for a standard ABAC protocol, other standard protocols and architectures may be relevant to ABAC use cases. Next Generation Access Control [17], developed by the International Committee for Information Technology Standards, outlines an access control architecture that supports the use of attributes. OAuth 2.0 [18], ratified by the Internet Engineering Task Force (IETF), serves as a rights delegation protocol that grants access to protected resources by defining the allowable user actions for those resources, referred to as “scopes.”

When system requirements include identity federation, protocols such as SAML 2.0 and OpenID Connect can define the syntax and semantics for passing identity and attribute information across organization bounds.

5.2.2 PEP Placement

As it is in the XACML architecture, the PEP is a very important ABAC component, as it enforces the actual access control decision. The location of the PEP may affect the types of access requests the ABAC system can trap and send to the PDP for decisions. It may also contribute to how efficiently the system handles large numbers of access requests. Common options for PEP placement include:

- closely coupling it within a software program

- using an agent to front-end a web browser-based application
- placing it at an enterprise gateway position in order to ABAC-enable a set of applications

The PEP may also be asked to perform additional functions that require a specific PEP placement. Under the XACML standard, the PEP can be configured to handle “out-of-band” instructions known as obligations (mandatory directives) and advice (optional). These instructions trigger secondary actions in addition to the access decision enforcement. An example of an obligation would be where a person is allowed access to a target resource, but the PEP is directed to initiate a royalty payment for its use.

5.2.3 PDP Distribution

The PDP operates a rule-based engine that is called upon to adjudicate access permissions to a selected resource. Typical ABAC installations get involved in deciding whether to locate PDPs centrally where each PDP supports multiple PEPs, to dedicate one PDP to each PEP, or to pursue a hybrid of the two approaches. Different PDP distributions can be associated with various performance and latency characteristics.

5.2.4 Multi-Vendor

ABAC systems have traditionally been classified as proprietary or standards based. Those that are standards based give the option of mixing and matching among system components rather than requiring all components to come from the same vendor. A multi-vendor-implementation solution sometimes needs some advance investigation to ensure that the standardized components will work together as well as promised.

5.2.5 Caching

There are several locations in an ABAC system implementation for an architect to consider the use of memory caching to improve performance. Considerations include caching decisions at the PEP, rules at the PDP, and user attributes at the RP.

5.2.6 Data Tagging

If an organization is migrating from a non-ABAC legacy access control mechanism to ABAC, then the task of going through every record and tagging the data with the applicable attributes must be addressed. If the organization has a considerable corpus of legacy data and resources, this may be both a technical and operational challenge.

5.2.7 Policy Authoring

An important consideration in the selection of an ABAC product is the tools available for creating and modifying policies. Such tools can make understanding policies easier and help with overall policy structure. Organizations could develop a library of sample policies identified by where they might apply within the organization. Some integrated development environments support plug-ins that provide a much more user-friendly syntax for XACML.

5.2.8 Attribute Retrieval

A design consideration in the implementation of ABAC is the mechanism for attribute retrieval by the PDP. To render an access decision, the PDP needs the values of the attributes referenced by the applicable policies. The PDP can obtain these attributes in one of three ways:

1. All the attribute values may be provided in the decision request.
2. If all the attributes are not provided to the PDP and it finds that attributes that are required to make a decision are missing, it may return a decision value of Indeterminate-Missing Attributes and specify what attributes are required. This allows the PEP to fetch the missing values and retry the decision request with them added.
3. Many PDP implementations are able to pause in the middle of an evaluation and fetch missing attribute values before completing the policy evaluation.

If the attributes are being retrieved in a federation scenario, privacy considerations may dictate the choice of the retrieval options in order to ensure a more privacy-enhancing, secure, and efficient implementation.

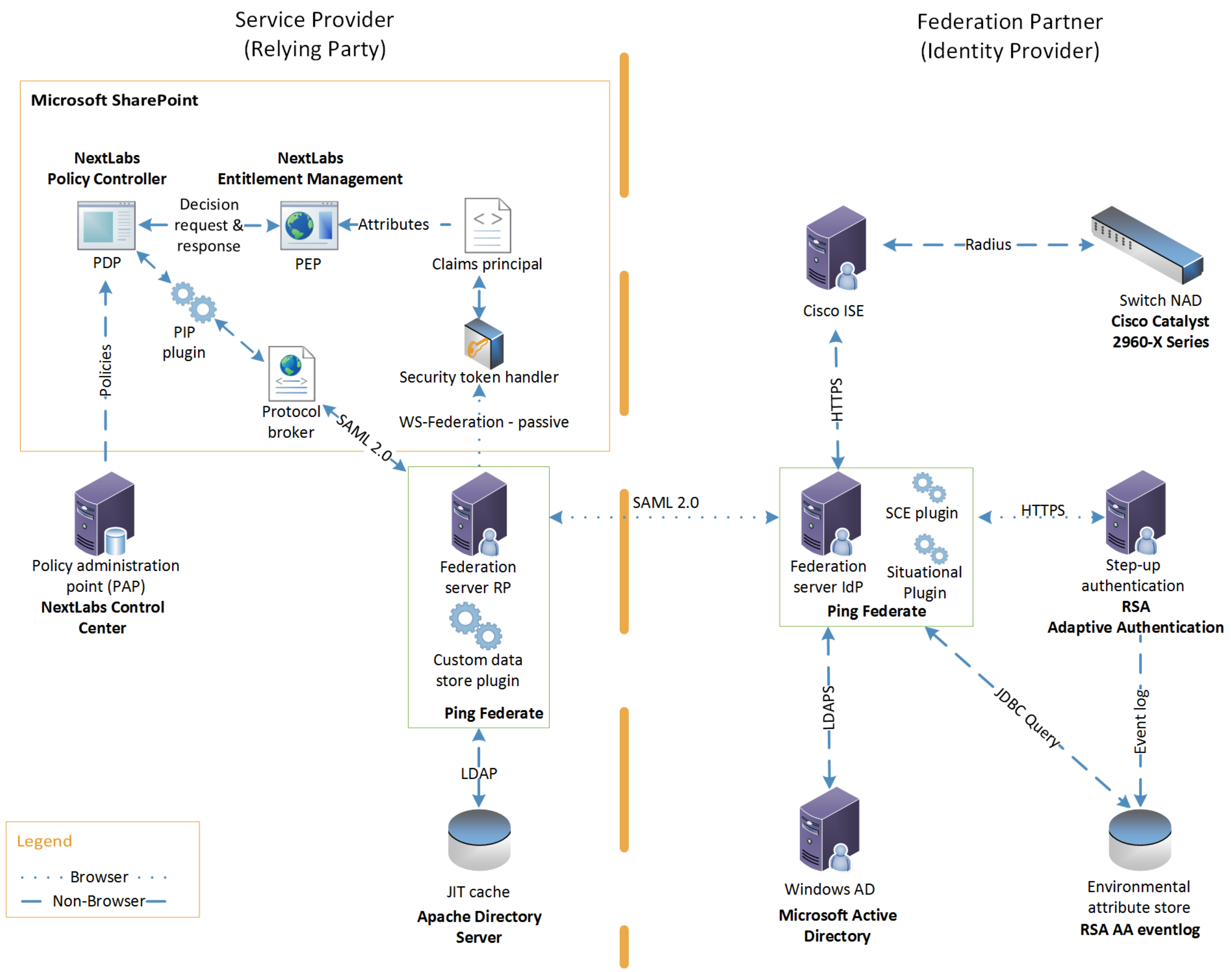
5.3 Technology and Architecture of the NCCoE Build

Section 4.5 provides an overview of the technologies used in this architecture, while Section 5.1 details the functionality found in this build. This section documents how each of the technologies in this build interoperate to achieve the build's functionality. Individuals interested in how these components were installed, configured, or integrated should consult Volume C, How-To Guides, of this publication.

5.3.1 Architecture Diagram and Components

Figure 5-1 illustrates the logical interactions of the components in this build. Interactions are broken down into browser-based or non-browser-based communications. All components in this build are either commercially available through the applicable vendor or can be found publicly with the release of this practice guide.

Figure 5-1 ABAC Build 1 Architecture



The components in Figure 5-1, which were available from NCEP organizations that met the build's functional requirements, provide the following capabilities to this build:

- Microsoft AD acts as a user identity management repository for the IdP. This includes the ability to provision and de-provision user identities; the creation, modification, and deletion of subject attributes; and the provisioning and de-provisioning of subject attributes to specific user identities. In this build, AD is the only source for subject attributes.
- RSA AA gathers environmental information about the user and the user's system or agent at the time of authentication. AA collects information such as patch level, operating system, and location, and it generates a risk score associated with the user authentication. A risk score threshold can then be defined in AA, which, if exceeded, can force a user to step up to one of the additional authentication mechanisms. In this build, information collected by AA to generate a risk score is also passed through PingFederate-IdP to the RP side of the operation to be used as environmental attributes.

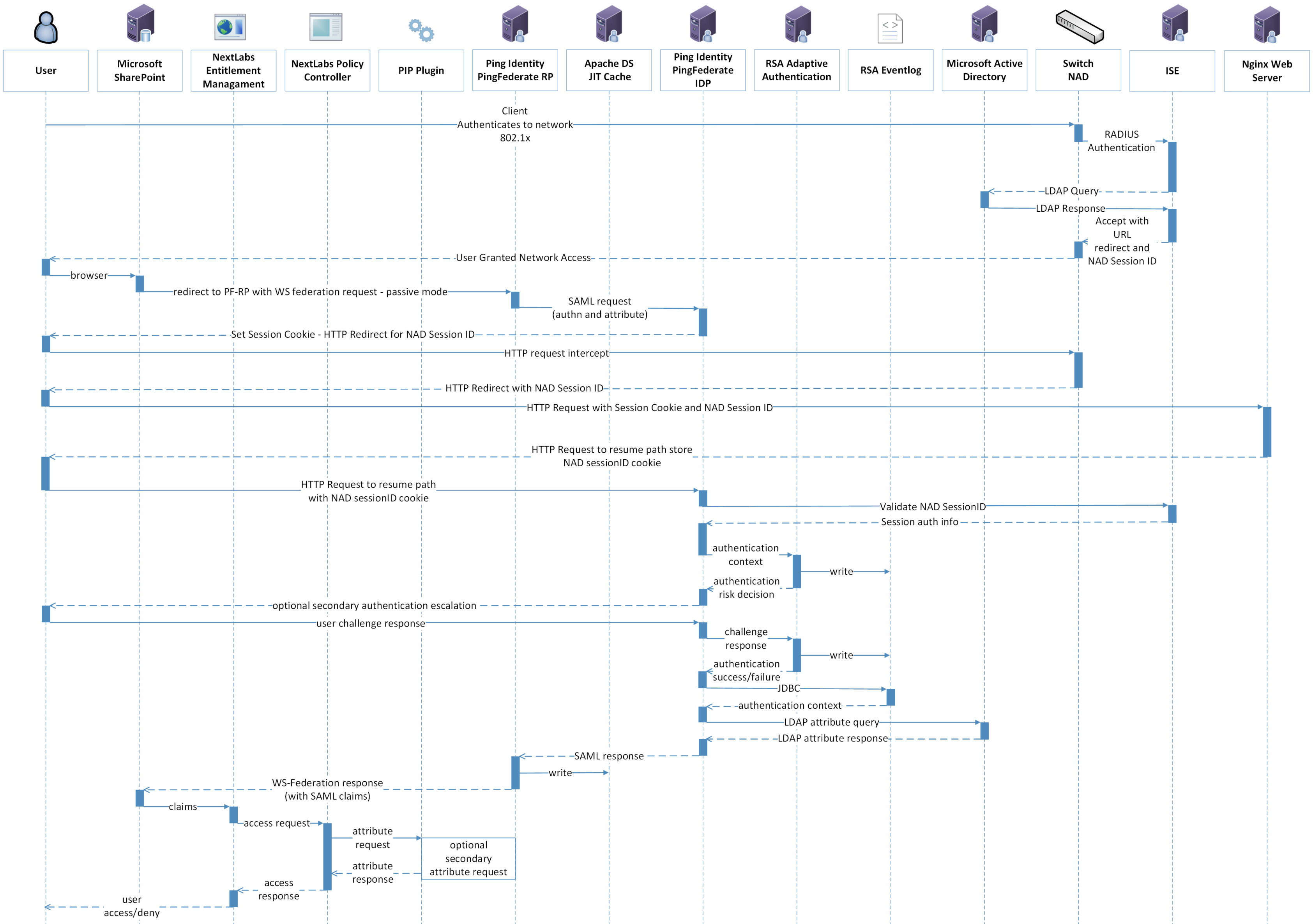
- The RSA AA event log contains the transaction identification (ID) of each user authentication and the associated environmental information collected by RSA AA at the time of authentication.
- Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP. PingFederate-IdP provides initial user authentication and retrieval of user attributes to satisfy SAML requests from the RP. Once the user has been authenticated, PingFederate-IdP queries subject attributes from AD and environmental attributes from the RSA AA event log. PingFederate-IdP packages both subject and environmental attributes in a SAML 2.0 token to be sent to the RP.
- The SCE Plug-in is an RSA component that handles communications between the PingFederate-IdP and the RSA AA. It is responsible for passing the RSA AA transaction ID for the user authentication that PingFederate-IdP uses to query the RSA AA event log.
- Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the necessary assertions. Once authenticated, PingFederate-RP arranges for the browser's Hypertext Transfer Protocol Secure (HTTPS) content to have the proper information in proper format for acceptance at the target resource (SharePoint). PingFederate-RP has the option to utilize the Apache Directory Server as a just-in-time (JIT) cache. Secondary attribute requests can also be made by PingFederate-RP via a SAML query initiated by the PIP lug-in and the Protocol Broker.
- Microsoft SharePoint serves as a typical enterprise repository. In this build, it stores the target resources that users wish to access. SharePoint natively uses an RBAC authorization environment, but it also supports the use of attributes, a capability Microsoft refers to as "claims aware." SharePoint accepts assertions from PingFederate-RP and stores asserted attributes as claims. SharePoint also allows for the tagging of data within its repository, which can then be leveraged as object attributes.
- Microsoft SharePoint Security Token Handler resides inside SharePoint, validating the token sent by PingFederate-RP.
- Microsoft SharePoint Claims Principal is the object inside SharePoint where attribute assertions are stored as claims.
- NextLabs Entitlement Management is closely coupled with SharePoint. It performs the PEP functionality, trapping user access requests. As the PEP, Entitlement Management is responsible for gathering object attributes from SharePoint and subject and environmental attributes from the claims principal at the time of the access request. Entitlement management then passes this information in the form of an access decision request to the NextLabs Policy Controller.
- NextLabs Policy Controller is a component of the NextLabs Control Center that is closely coupled with the SharePoint instance. The Policy Controller is responsible for providing PDP capabilities. The Policy Controller receives attribute-based policies from the Control Center and uses these policies to respond to access requests from Entitlement Management.
- NextLabs Control Center serves as the PAP, where attribute-based policies are created, updated, and deployed using a built-in graphical user interface (GUI). The Control Center also provides auditing, logging, and reporting functions for the SharePoint access requests and decisions.

- Policy Information Point(PIP) Plug-in is a software extension of NextLabs Policy Controller that enables it to acquire unavailable attributes required for policy evaluation at runtime from RP or IdP by communicating with Protocol Broker on an HTTPS channel protected by mutual TLS.
- Protocol Broker is a web application that retrieves attribute values by accepting attributes to be queried from the NextLabs Plug-in and querying the PingFederate-RP by issuing a SAML 2.0 Assertion Query/Request.
- The Custom Data Store is a plug-in built using PING software development kit (SDK) that enables the RP to query the IdP and provides the resulting attribute value back to the Ping Federate RP.
- The Apache Directory Server is an LDAP version 3-compliant directory server developed by the Apache Software Foundation that works as a JIT cache for PingFederate-RP. It stores subject attributes and other relevant information from the SAML 2.0 response that an RP receives from an IdP.
- Symantec Trust Center Account for Enterprise is used for secure issuance of PKI-based certificates throughout this build. The Symantec certificates enable mutual TLS, digital signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest in the RP's JIT cache.
- A Cisco Catalyst 2960-X series switch is used as a network access device (NAD) and provides switching and routing to the network. When a user attempts to access the network, the NAD challenges for credentials and upon successful authentication, a network session ID is created.
- Cisco Identity Services Engine (ISE) is used to provide 802.1X network authentication. In this role, it accepts credentials from the user and verifies this information through radius authentication. The service also collects attributes that are returned to Ping Federate IdP.
- The Situational Plug-In is a Ping Federate plug-in that is used as an adapter to retrieve attributes from Cisco ISE. The plug-in communicates via the HTTP protocol.

5.3.2 UML Diagram

The architecture shown in Figure 5-1 can, in practice, support different types of sequential operations. We have chosen to initially implement, demonstrate, and document two generic types of sequential ABAC operations as being representative of the core operations of the architecture. The ladder diagram in Figure 5-2 contains represents the initial flow of the ABAC architecture, where an unauthenticated user tries to access a resource on SharePoint.

793 **Figure 5-2 UML Sequence Diagram**



794

The sequence starts in the top of Figure 5-2 when a user joins the network and browses to, and attempts to access, a protected resource in SharePoint.

1. The user attempts to join the network and is challenged for login credentials. These credentials are validated by radius authentication to Active Directory. Upon successful authentication to the network, a network session ID is created.
2. SharePoint inspects the user's HTTP content and finds that the user has not been previously logged in (i.e., not authenticated), and therefore redirects the browser to PingFederate-RP via use of the WS-Federation protocol.
3. PingFederate-RP interprets the WS-Federation request as a request for authentication and for attributes, and the user is redirected to PingFederate-IdP carrying a SAML authentication request and SAML attribute request.
4. PingFederate-IdP does an initial (single-factor) authentication of the user, and, if successful, receives the requested subject attributes.
5. PingFederate-IdP then redirects the user's browser to RSA AA to enhance the initial authentication.

   Note: In practice this secondary authentication can be conditionally done based upon the type of protected resource for which access is requested or upon other conditions such as environment. The current installation always calls for the second level of authentication to demonstrate what is known as multi-factor authentication (MFA), and, for this build, achieves it by sending an SMS text message and expecting a particular response. The RSA AA product has additional options that are not being demonstrated at this time.
6. Upon successful completion of the MFA operation, the user is redirected back to PingFederate-IdP. At this time, PingFederate-IdP can query the RSA AA event log for environmental attributes that add context to the authentication.
7. PingFederate-IdP issues a SAML 2.0 token containing the user's identity and attribute information, and redirects the user's browser to PingFederate-RP.
8. PingFederate-RP accepts the SAML 2.0 response and issues a WS-Federation response back to SharePoint with the HTTP carrying the authentication and attribute information.

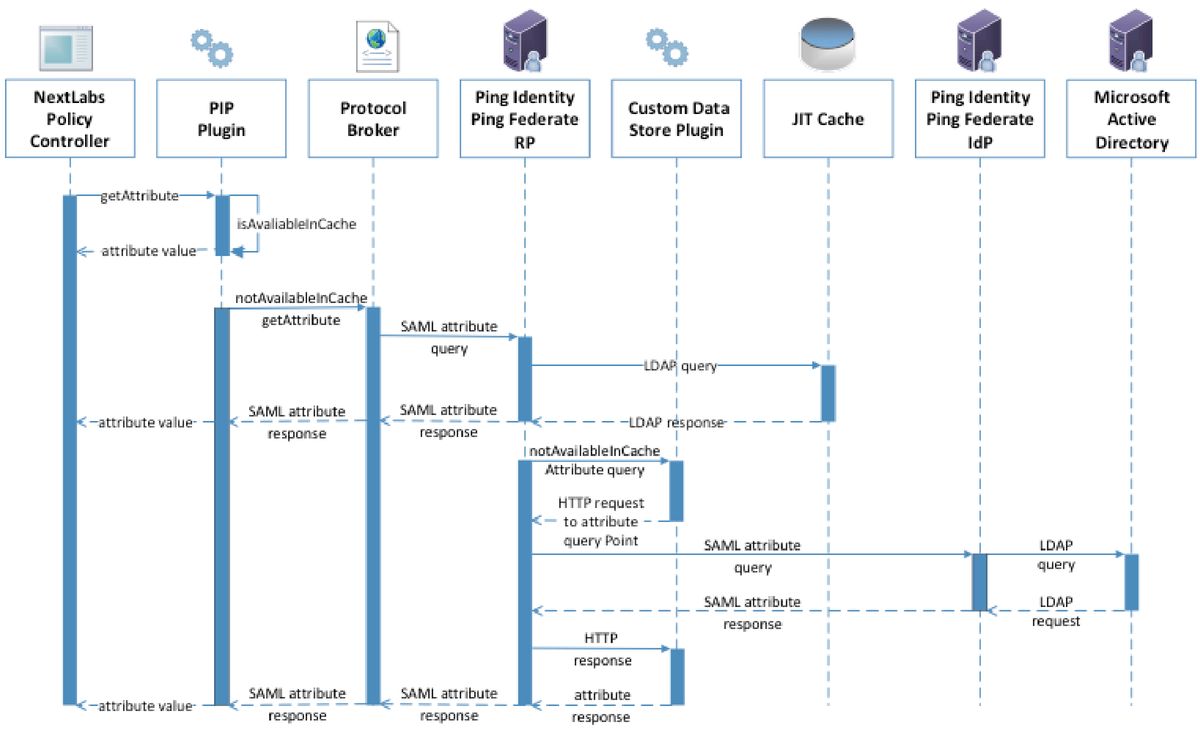
   At this point, the user's browser is issued a "FedAuth" cookie, establishing a session with SharePoint, and resides there until the session is terminated. The rest of this flow occurs as communications internal to the RP or as web service calls back to the IdP, without the user's awareness. Once this session is established, the system is configured to allow the NextLabs components to handle access requests to SharePoint. After the WS-Federation response, the subject and environmental attributes from the IdP are stored in the SharePoint Claims Principal.
9. Access requests by the authenticated user are now trapped by the NextLabs Entitlement Management PEP, which gathers the subject and environmental attributes stored in the Claims Principal and the object attributes stored in SharePoint, and submits the access request to the Policy Controller PDP for adjudication.
10. The Policy Controller uses the attributes provided by the PEP and the policy established by Control Center to determine an access allow or deny. If the PDP is not presented with enough

attributes to make an access decision, it has the option of initiating a secondary attribute query, which is detailed in Figure 5-3 and discussed later.

11. Once an access decision has been made, the Policy Controller responds back to the Entitlement Management PEP, which enforces the decision.

The ladder diagram in Figure 5-3 represents a flow of this ABAC architecture where an authenticated user tries to access a resource on SharePoint but there is a need to initiate a secondary attribute request. If needed, this flow is initiated by the NextLabs Policy Controller in Step 9.

Figure 5-3 Secondary Attribute Request Flow



The basic steps of the Figure 5-3 flow are:

1. When the Policy Controller does not receive the attributes required to make a decision, a secondary attribute request will be initiated by calling the PIP Plug-in.
2. PIP Plug-in is a registered plug-in with the NextLabs Policy Controller. It implements the interface dictated by the NextLabs software. By virtue of this implementation, it receives the subject and name of the attribute that is required for the policy decision.
3. When the subject and attribute name are received, the PIP Plug-in checks its local short-term cache (in this build, configured to hold values for two seconds) to see if the needed attribute for the subject was recently requested.
4. If the attribute is still in cache, the value is returned to the Policy Controller. If the value is not in cache, the PIP Plug-in initiates an HTTPS request to the Protocol Broker.

5. The Protocol Broker receives the attribute name and subject from the HTTPS request and forwards them as a signed SAML 2.0 Attribute Query to PingFederate-RP on a channel protected by mutual TLS.
6. Once PingFederate-RP receives the SAML 2.0 attribute query, it sends an LDAP request to the JIT cache to see if the attribute was previously queried in a secondary request.
7. If the subject does not have the attribute value assigned in the JIT cache, PingFederate-RP will forward the subject and attribute name to the Custom Data Store plug-in. The Custom Data Store plug-in acts as a pointer back to the PingFederate-IdP. To do this, the Custom Data Store dispatches an HTTPS request to the PingFederate-RP with the PingFederate-IdP as the attribute query point.
8. Ping Federate uses an HTTPS query to form a SAML 2.0 attribute query and dispatch it to the Ping Federate at the IdP.
9. The Ping Federate at the IdP accepts the SAML 2.0 request, verifies whether the user has the needed attribute, and replies to the PingFederate-RP with a SAML 2.0 response.
10. PingFederate-RP validates the SAML 2.0 response, retrieves attribute values, and responds to the original Custom Data Store HTTP request with the attribute values.
11. The Custom Data Store then responds to the PingFederate-RP attribute request with an attribute response.
12. The PingFederate-RP constructs a SAML 2.0 response and sends it to the Protocol Broker.
13. The Protocol Broker retrieves the attribute or exception from the SAML 2.0 response and forwards it to the NextLabs plug-in, which passes the attribute or exception back to the Policy Controller.

5.3.3 NCCoE Design Considerations

Section 5.2 outlined the architectural topics and options that entered into our decision making for this first ABAC build and demonstration. In this subsection, we summarize the architectural directions that were chosen for this particular build, and why.

5.3.3.1 Industry Standards

The use of XACML and its importance to ABAC functionality were introduced in Section 5.2.1. Its core parts are the request/response protocol between PEP and PDP, the rule language, and the use of obligation and advice that the PDP can forward to the PEP. Use of a standard like XACML yields potential cost saving for an IdAM infrastructure implementation, as heterogeneous interchangeability of operational components can be implemented more easily.

The use of SAML 2.0 provided advantages from several perspectives. From its documented set of approved federation profiles, the Web Browser SSO Profile (referred to here as “Web SSO”) has a large following in the industry and was chosen for the browser interface because its authentication sequencing stepped between PingFederate-RP, PingFederate-IdP, and the RSA AA system.

SAML 2.0 core was used within the SAML Web SSO exchange, but was also used as a stand-alone for its request/response protocol for backend attribute exchanges of NextLabs’ PIP Plug-in to and from

PingFederate-RP (via the Protocol Broker), and for backend attribute exchanges from PingFederate-IdP to PingFederate-RP.

WS-Federation is a federation protocol that spans important federation functionality, ranging from authentication to metadata, support for pseudonyms, and more. Our use is limited but still key: to carry an authentication request from SharePoint to PingFederate-RP, and then to handle the return response with its identity and user attribute information.

Lightweight Directory Access Protocol Secure (LDAPS), the TLS version of the LDAP standard for interfacing to directory stores, is used in two places in this build. One is PingFederate-RP to its JIT cache based on Apache Directory Server, and the other is PingFederate-IdP to the Microsoft AD LDAP store. Other standards in use include PKI for the structure of the server certificates that are in use, and within TLS operational algorithms. TLS itself is an important standard for promoting communications confidentiality and integrity.

5.3.3.2 PEP Placement

There is a single PEP in this ABAC build for controlling the operations of the SharePoint authorization functionality at a finer level of granularity than is available with the RBAC-oriented access control that comes with SharePoint out of the box. The NextLabs Entitlement Management PEP product was chosen because it meets our requirements, and by its nature it is integrated with and closely coupled with SharePoint. The NextLabs PEP can be considered to be co-located with the SharePoint protected resource.

5.3.3.3 PDP Distribution

With only one PEP in this build, the decisions on PDP quantity and location(s) for placement were simpler than one would find in a typical enterprise installation. The NextLabs Policy Controller PDP is co-located with SharePoint and the PEP.

5.3.3.4 Multi-Vendor

The ABAC implementation represented in this build is a heterogeneous set of IdAM components that have been successfully integrated to achieve the system objectives. To accomplish this, we worked closely with our NCEP collaborator to design an interoperable architecture. Each component performed its functions as required, and Volume C of this guide describes the set of NCCoE experiences and supplemental functionality that was incorporated to achieve the functional objectives.

5.3.3.5 Caching

Caching is a common topic in system integration work as architects work to achieve efficiencies required for their particular functionality. In the current build, two caches have been explicitly implemented by the NCCoE development team:

- NextLabs PIP Plug-in contains a local cache, developed using the EhCache library. This cache stores attributes for two seconds and adds efficiency to the system should multiple requests for the same subject and attribute value pairing occur in quick succession (with two seconds).

- A JIT cache was developed for PingFederate-RP, using Apache Directory Server. It is used to cache user attributes that are retrieved by PingFederate-RP for a finite time (such as up to 24 hours) to avoid future repeated secondary attribute calls to the IdP.

5.4 Security Characteristics

In this section, we re-introduce the security characteristics and security controls that were first introduced in Sections 4.4 and 4.4.1, and relate each to the NCEP's products used in this ABAC build.

- Identity and Credentials and Their Use for Authorized Devices. In NIST SP 800-53, this is tied to AC-1, and in NIST Cybersecurity Framework to PR.AC-1: "Identities and credentials are managed for authorized devices and users." In this build, both user and system identities are managed to ensure linkage with these security controls. Where applicable, systems are given PKI-based credentials for use with TLS via the Symantec Managed PKI Service. User authentication in this first build is multi-factor, with one factor being name and password via PingFederate-IdP and AD, and the second an SMS text message sent to a cellular device conducted by the RSA AA. The RSA AA system offers other options for use as the second factor of authentication through its multi-credential framework.
- Remote Access Being Managed. Several of the NCEP products are involved in ensuring efficient and secure remote access. The two Ping Identity PingFederate installations have federation and authentication features that allow the RP to accept external identities for remote access. SharePoint via WS-Federation trusts external identities sent from PingFederate. NextLabs products enable ABAC functionality for SharePoint access decisions and allow for the auditing and logging of access requests.
- Access Permissions. ABAC systems manage access permissions by defining attribute-based rules that specify what subject attributes are needed to access resources with a given set of object attributes, under a set of environmental conditions. In this build, this functionality is handled by NextLabs products. A NextLabs Control Center allows for creation of attribute-based policies and makes access decisions based on those policies via its Policy Controller.
- Encryption and Digital Signature. Browser-based communications with SharePoint are HTTPS-based, and LDAP is used for all interfacing with AD. All system endpoints are equipped with PKI certificates issued by the Symantec Managed PKI Service, and TLS is used for system-level point-to-point transactions. Examples include full encryption of SAML request/response transactions such as between PingFederate-RP and PingFederate-IdP.
- Provisioning. Identities are provisioned, stored, and de-provisioned inside AD. This process occurs manually through the native Microsoft Windows Server GUI. AD also handles the assigning of subject attributes to specific user identities.

  Object attributes are provisioned via SharePoint. SharePoint sites or individual files can be "tagged" with object attributes by adding columns to the SharePoint site table or document library. The titles of these columns serve as attribute names and the content of the columns serves as the values of attributes for the specific object.
- Auditing and Logging. Each product in this build supports a logging mechanism detailing activities occurring within that component. Access requests can be audited using the NextLabs Reporter, where the user, access decision, and policy enforced can be viewed for each access request.

- Access Control. Fundamentally, this build enhances the native capabilities of SharePoint by adding ABAC functionality. This is achieved through the NextLabs Entitlement Management PEP, which traps access requests, and the Policy Controller PDP, which makes access decisions using attribute-based policies. Organizations implement the concept of least privilege by defining attribute-based policies in the NextLabs Control Center and assigning applicable attributes to subjects and objects using AD and SharePoint. A wider range of access control decisions is enabled through the use of environmental attributes, which can be obtained from RSA AA in this build.

5.5 Features and Benefits

This section details some of an ABAC system's potential benefits through risk reductions, cost savings, or access management efficiencies. As with any reference architecture, the exact benefits derived will depend on the organization's individual implementation requirements and the scenarios to which an organization wishes to apply an ABAC model.

5.5.1 Support Organizations with a Diverse Set of Users and Access Needs

RBAC meets practical limits as roles and their associated access requirements grow in diversity and complexity. This often leads to the overloading of access privileges under a single role, the assignment of multiple roles to a single user, or the escalation of the number of roles the enterprise needs to manage. Moving to an ABAC model allows organizations to specify policy based on a single attribute or a combination of attributes that represents the specific access an individual's needs. This helps eliminate the potential for privilege creep.

5.5.2 Reduce the Number of Identities Managed by the Enterprise

When organizations wish to provide access to users from external security domains, they have the option to provision local identities for these external users. These identities must then be managed by the enterprise. This scenario incurs the costs associated with these management efforts and also presents risk to the enterprise, because these accounts could be orphaned as the users' access privilege requirements change at their home organization. Identity federation can address these issues by allowing organizations to accept digital identities from external security domains, but leave the management of these identities to the users' home organizations.

5.5.3 Enable a Wider Range of Risk Decisions

The ability to define attribute-based policies affords organizations the extensibility to implement a wider range of risk-based decisions in access control policy, compared to an RBAC system. Specifically, the ability to leverage environmental attributes allows for relevant context such as location of access, time of day, threat level, and client patch level to be included in automated decision logic.

5.5.4 Support Business Collaboration

ABAC combined with identity federation helps reduce barriers to sharing resources and services with partner organizations. Under the ABAC model, a partner's user identities and appropriate access policies for those identities do not need to be pre-provisioned by the RP. Instead, access decisions can be made on partner identities using attributes provided by the partner.

5.5.5 Centralize Auditing and Access Policy Management

ABAC can improve the efficiency of access management by eliminating the need for multiple, independent, system-specific access management processes, replacing them with a centralized PDP and PAP. In this way, access decisions across multiple applications could be audited centrally at the PDP, while policies could be created and deployed centrally at the PAP, but enforced locally via an application-specific PEP. The ability to externalize and centrally manage access policies may also simplify compliance processes by reducing the number of places that need to be audited.

Appendix A List of Acronyms

AA	Adaptive Authentication
ABAC	Attribute Based Access Control
AD	Active Directory
AP	Attribute Provider
CSF	Framework for Improving Critical Infrastructure Cybersecurity
DAC	Discretionary Access Control
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IdAM	Identity and Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
ISE	Identity Services Engine
IT	Information Technology
JIT	Just-in-Time
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NAD	Network Access Device
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partner
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RP	Relying Party
SAML	Security Assertion Markup Language
SMS	Short Message Service
SP	Special Publication
SSO	Single Sign-on
TLS	Transport Layer Security

WS	Web Service
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Appendix B References

[1] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication (SP) 800-162, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2014. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf [accessed 09/08/17].

[2] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers, *Systems and software engineering – System life cycle processes*, ISO/IEC/IEEE 15288:2015, 2015. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711 [accessed 09/08/17].

[3] R. Ross, M. McEvilley, and J. C. Oren, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST Special Publication (SP) 800-160 Second Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf [accessed 09/08/17].

[4] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," *IEEE Computer*, vol. 43, no. 6, pp. 79-81, June 2010. http://ieeexplore.ieee.org/document/5481941/ [accessed 09/08/17].

[5] E. Coyne and T.R. Weil, "ABAC and RBAC: Scalable flexible and auditable access management," *IT Professional*, vol. 15, no. 3, pp. 14-16, May-June 2013. https://www.computer.org/csdl/mags/it/2013/03/mit2013030014.html [accessed 09/08/17].

[6] *Attribute Based Access Control (ABAC) Overview*, National Institute of Standards and Technology: Computer Security Resource Center [Web site], http://csrc.nist.gov/projects/abac/ [accessed 09/08/17].

[7] *eXtensible Access Control Markup Language (XACML) Version 3.0*, OASIS Standard, OASIS, January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html [accessed 09/08/17].

[8] *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, OASIS, March 2005. http://saml.xml.org/saml-specifications [accessed 09/08/17].

[9] *OpenID Connect Core 1.0 incorporating errata set 1*, OpenID Foundation [Web site], http://openid.net/specs/openid-connect-core-1_0.html [accessed 09/08/17].

[10] W. Fisher, *Attribute Based Access Control*, Building Block Version 2, National Cybersecurity Center of Excellence. April 1, 2015.

https://nccoe.nist.gov/sites/default/files/library/project-descriptions/abac-project-description-final.pdf [accessed 09/08/17].

[11] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology, February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 09/08/17].

[12] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST, SP 800-53 Revision 4, National Institute of Standards and Technology, April 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[13] *ISO/IEC 27001 Information Security Management*, International Organization for Standardization [Web site], http://www.iso.org/iso/home/standards/management-standards/iso27001.htm [accessed 09/08/17].

[14] *SANS Institute - CIS Critical Security Controls*, SANS Institute [Web site], https://www.sans.org/critical-security-controls/ [accessed 09/08/17].

[15] COBIT 5 Publications Directory, ISACA [Web site], http://www.isaca.org/COBIT/Pages/Product-Family.aspx [accessed 09/08/17].

[16] *Cloud Controls Matrix v3.0.1 (10-6-16 Update)*, Cloud Security Alliance (CSA) [Web site], https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/ [accessed 09/08/17].

[17] *Information Technology – Next Generation Access Control – Functional Architecture (NGAC-FA)*, ANSI INCITS 499-2013, American National Standards Institute, March 2013. http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013 [accessed 09/08/17].

[18] D. Hardt, *The OAuth 2.0 Authorization Framework*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 6749, October 2012. http://tools.ietf.org/html/rfc6749 [accessed 09/08/17].