NIST CYBERSECURITY PRACTICE GUIDE

ATTRIBUTE BASED ACCESS CONTROL

For CIOs, CISOs, and Security Managers

Approach, Architecture, and Security Characteristics

Bill Fisher **Norm Brickman** **Santos Jha**

Sarah Weeks **Ted Kolovos** **Prescott Burden**

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-3b

DRAFT

DRAFT

NIST Special Publication 1800-3b

ATTRIBUTE BASED ACCESS CONTROL

DRAFT

Bill Fisher

National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman

Santos Jha

Sarah Weeks

Ted Kolovos

Prescott Burden

The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief

National Cybersecurity Center of Excellence
Information Technology Laboratory

April 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, 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, materials, or equipment 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,44 pages (April 2016)
CODEN: NSPUE2

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

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

Public comment period: *September 30, 2016* through *December 4, 2016*

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

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

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. The documents in this series 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 that the NCCoE took in developing a reference architecture and build. Included is a discussion of major architecture design considerations, 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 gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

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
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust

Name	Organization
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb

Contents

List of Figures

List of Tables

1 Summary

Traditionally, granting or revoking access to 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 doesn't 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 attribute based access control (ABAC) solution can more securely and efficiently manage access to networked resources, 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 The 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 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 doesn't 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

1.National Institute of Standards and Technology Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

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 The 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 not only from malicious external users and insider threats, but also from 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.

At the strategic level, organizations face risks associated with the acquisition, deployment, and maintenance of access control systems. These risks include the cost of the implementation and maintenance, any compliance or regulatory requirements, as well as a lack of preceding implementations from which to derive lessons learned.

1.4 Benefits

The example solution described in this guide has the following benefits:

- products and capabilities can 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, and there by reducing costs associated with those management activities
- enable a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policy on subjects and objects, but also 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

1.5 Technology Partners

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partner (NCEP). NCEPs are IT and cybersecurity firms that have pledged to support the NCCoE's mission of accelerating the adoption of standards-based, secure technologies. They contribute hardware, software, and expertise. In this project, we worked with:

- Ping Identity
- NextLabs
- Microsoft
- RSA
- Symantec

1.6 Feedback

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. 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. Your comments, suggestions, and success stories will improve subsequent versions of this guide.

- email abac-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/attribute-based-access-control

Or learn more by arranging a demonstration of this example solution by contacting us at abac-nccoe@nist.gov

2 How to Use This Guide

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

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 (this document)
- *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 ABAC, and the limitations of role based access (RBAC) systems

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 4.3, Risk Assessment, provides a detailed description of the risk analysis we performed.
- Section 4.4, Security Characteristics and Controls Mapping, 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.[1] We do not re-create 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

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

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, and join the discussion at https://nccoe.nist.gov/forums/attribute-based-access-control.

3 Introduction

3.1 Background

Basic read, write, and execute permissions, along with discretionary access control (DAC) and mandatory access control (MAC) principles, mark the evolution of access control to the RBAC models that are in common commercial use today. While RBAC focuses primarily on the use of the role attribute, ABAC allows for access decisions based upon arbitrary attributes.

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."[1] [2]

In order to enable ABAC implementations, the standards community has undertaken efforts to develop common terminology and interoperability across access control systems. One such standard is the eXtensible Access Control Markup Language (XACML)[3]. 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 almost ubiquitous adoption of the RBAC model for logical access control. However, in the modern IT environment, enterprises face growing diversity in both types of users and their access needs. This diversity elucidates several limitations of the RBAC model.

This diversity introduces a number of administrative and policy enforcement challenges. Administrators manage access policy for multiple applications and security domains, with each often requiring discrete access control policies. Most systems implement access control in different ways, making it hard to share

1.NIST, "Attribute Based Access Control (ABAC) - Overview". http://csrc.nist.gov/projects/abac/
2.V.C. Hu, D. Ferraiolo, and R. Kuhn, et al., NIST SP 800-162,
Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf
3.OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 3.0", 22 January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

information across systems and requiring administrators to configure the access for like users uniquely in each system, typically by using the roles or groups native to that system.

These roles are often 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.

Attribute-based systems, by the nature of their name:value pairs for each attribute, can support a much finer-grained authorization environment than an RBAC system. ABAC allows 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. These policies include the ability to take environmental considerations into account when making access decisions.

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.

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 access to 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[1], which uses XML, or the OpenID Connect (OIDC) standard from the OpenID Foundation[2] built upon JavaScript Object Notation (JSON), 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.

1.OASIS Standard, "OASIS Security Assertion Markup Language (SAML) V2.0", March 15, 2005. http://saml.xml.org/saml-specifications

2.OpenID Foundation, "OpenID Connect Core 1.0", November 8, 2014. http://openid.net/specs/openid-connect-core-1_0.html

In some cases an RP may need to obtain attributes about a user from a source other than the user's IdP. In this case 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 looking 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, non-profit organizations such as the Kantara Initiative and the Open Identity Exchange (OIX) 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 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
	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

Table 3.1 Related Security Standards and Best Practices (Continued)

Related Technology	Relevant Standard	URL
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
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

Table 3.1 Related Security Standards and Best Practices (Continued)

Related Technology	Relevant Standard	URL
Protocol (TLS)	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
	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/

91

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, identity and access management 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[1] that identified numerous desired solution characteristics. After two rounds of public comments on the document, the NCCoE worked with its NCEP 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[2] based on the technology available to us through the portfolios of the NCCoE's National Cybersecurity Excellence Partners. 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

4.2.1 Assumptions

The ABAC build described here incorporates the assumptions in this section.

4.2.1.1 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 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

1.Fisher, William. *Attribute Based Access Control*, Version 2. NCCoE. April 1, 2015. https://nccoe.nist.gov/sites/default/files/documents/NCCoE_ABAC_Building_Block_v2_final.pdf

2.This project has the overarching goal of demonstrating technical implementations of standards-based ABAC functionality. In enumerating technology relevant to this effort, we worked closely with experts from the identity and access management community. During those discussions, we realized the complementary nature of identity federation when coupled with an ABAC implementation. Identity federation on its own does not constitute an ABAC solution and an ABAC solution does not rely upon identity federation. Future builds under this project name may or may not include examples of identity federation.

to only those 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 or other identity stores as appropriate.

4.2.1.2 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.

4.2.1.3 Attribute Semantics and Syntax

An ABAC IdAM infrastructure by its intrinsic nature is dependent on a pre-defined 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.

4.2.1.4 Attribute Provenance

In this build, we utilize Microsoft Active Directory, 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.

4.2.1.5 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.

4.2.1.6 Human Resources Database/Identity Proofing

This build is based on a simulated environment. Rather than re-create a human resources (HR) 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.

4.2.1.7 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.

4.2.1.8 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.

4.3 Risk Assessment

According to NIST Special Publication (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.” The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of the Risk Management Framework (RMF) material available to the public. The 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.

Using the guidance in NIST's series of SPs concerning the RMF, the NCCoE worked with IdAM SMEs to enumerate areas of access management risk facing today's enterprise. We deemed these the tactical risks:

- not implementing or maintaining least privilege for all users
- access rights accumulation violates the separation of duties
- digital identities of external users become orphaned
- authorization policies cannot account for the context of access request

In addition to tactical risk, enterprises face a series of business risks that are influenced by the acquisition, deployment, and maintenance of IdAM systems. We deemed these the strategic risks:

- cost of implementation
- budget expenditure as they relate to investment in security technologies
- compliance with existing industry standards
- risk of alternative or no action
- lack of successful precedents

We translated this risk information to security characteristics. We mapped these characteristics to NIST’s SP 800-53 Rev.4 controls where applicable, as well as other relevant industry and mainstream security standards.

4.4 Security Characteristics and Controls Mapping

Table 1 lists the major use case security characteristics. For each characteristic, the table provides the matching function, category, and subcategory from the NIST Cybersecurity Framework (CSF)[1], as well as mappings to controls from other relevant cybersecurity standards.

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[a]	ISO/IEC 2700[b]	SANS CSC[c]	ISACA COBIT 5[d]	CSA CCMv3.0.1[e]
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 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	CSC 16-16, CSC 17-7		EKM-03, IVS-10, DSI-03

1.NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0", February 12, 2014. http//www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Table 4.1 Use Case Security Characteristics Mapped to Relevant Standards and Controls (Continued)

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4[a]	ISO/IEC 2700[b]	SANS CSC[c]	ISACA COBIT 5[d]	CSA CCMv3.0.1[e]
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

a. NIST, SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations", April 2013. http://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.800-53r4.pdf

b. ISI/IEC, ISO/IEC 27001, "Information Security Management". http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

c. SANS Institute, "Critical Security Controls".https://www.sans.org/critical-security-controls/

d. ISACA, "COBIT 5". http://www.isaca.org/COBIT/Pages/Product-Family.aspx

e. Cloud Security Alliance (CSA), "Cloud Controls Matrix v3.0.1".https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

4.5 Technologies

Table 4.2 provides a breakout of the contents of table 4.1 organized by the products used within this build. This breakout shows the security controls coverage that each product supports.

Table 4.2 Use Case 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 Active Directory, 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 Active Directory	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

Table 4.2 Use Case Security Characteristics Mapped to Relevant Build Products

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
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, 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, SharePoint is 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 Active Directory (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 the creation, modification, and deletion of subject attributes.
- The build needed PEP functionality. It is provided by NextLabs Entitlement Management, which interfaces and integrates with products like 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 lifecycle 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), which is an authentication and environmental analysis system, provides this functionality. Its capabilities include a variety of adaptive opportunities, such as 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 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[1] 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 Discretionary Access Control (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

1.This project has the overarching goal of demonstrating technical implementations of standards-based ABAC functionality. In enumerating technology relevant to this effort, we worked closely with experts from the identity and access management community. During those discussions, we realized the complementary nature of identity federation when coupled with an ABAC implementation. Identity federation on its own does not constitute an ABAC solution and an ABAC solution does not rely upon identity federation. Future builds under this project name may or may not include examples of identity federation.

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 relying party is afforded the ability to make run-time 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 4.2.1, Assumptions, these include the development of policy, procedure, and/or functional requirements before the selection of technology components. Organizations wishing to implement an ABAC system should conduct robust requirements engineering, 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*[1] and NIST SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*[2] provide guidance in this endeavor.

From a technical perspective, this section outlines a few of the options that an architect will face, and section 5.2.6, Architecture Diagram and Components, 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.[3]

1.http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711
2.NIST, SP 800-160, *Systems Security Engineering (Draft)*, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
3.OASIS Standard, “eXtensible Access Control Markup Language (XACML) Version 3.0”, 22 January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

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[1], developed by the International Committee for Information Technology Standards, outlines an access control architecture that supports the use of attributes. OAuth 2.0[2], 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 since it enforces the actual access control decision. The location of the PEP may affect the types of access requests the ABAC system is able to 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 was 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.

1.INCITS, INCITS 499-2013, *Information Technology - Next Generation Access Control - Functional Architecture (NGAC-FA)*. http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013

2.IETF, Request for Comments (RFC) 6749, *The OAuth 2.0 Authorization Framework*, October 2012. http://tools.ietf.org/html/rfc6749

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

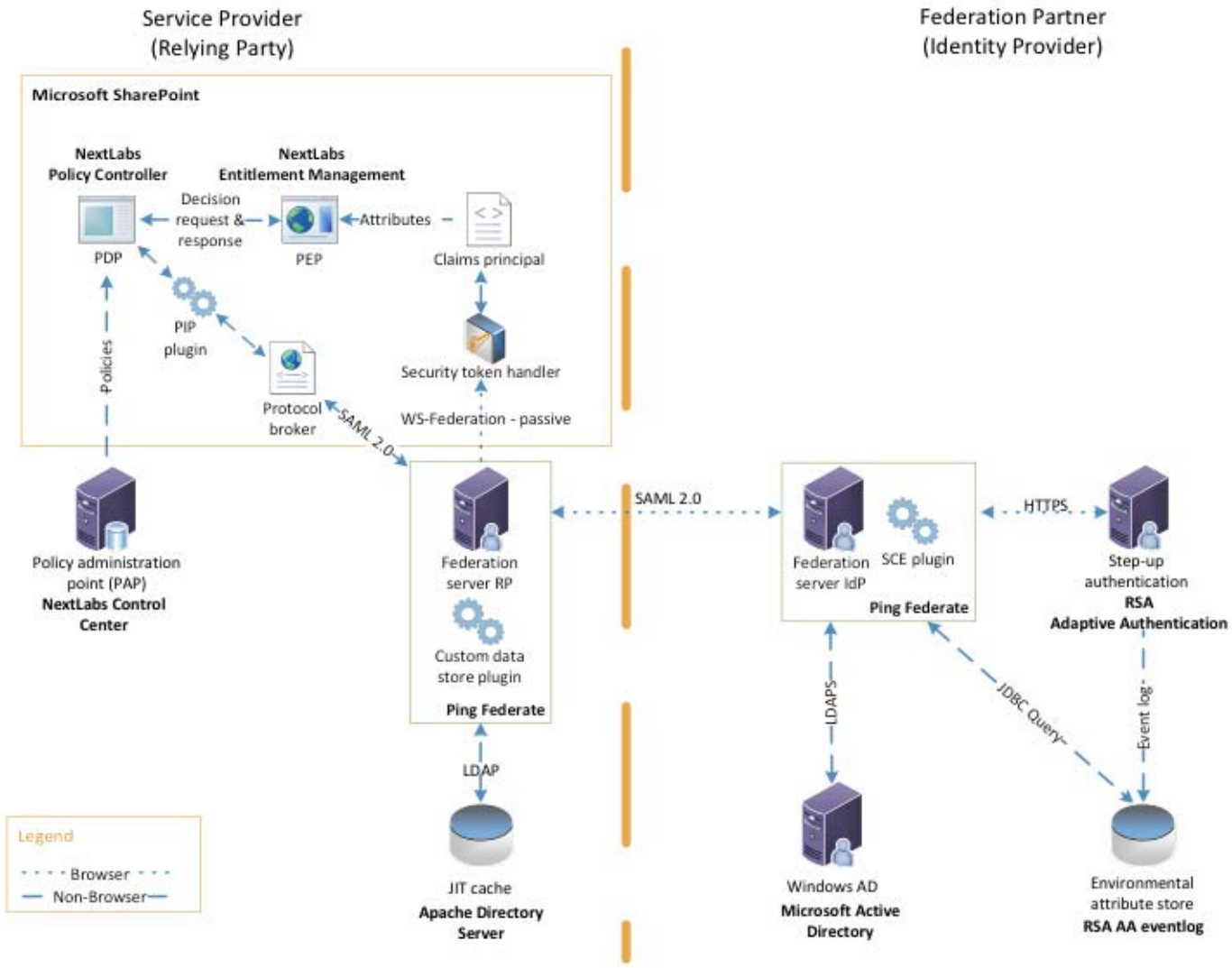
There are several locations in an ABAC system implementation for an architect to consider the use of memory caching to improve performance. Considerations include caching decisions at the PEP, rules at the PDP, and user attributes at the RP.

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.

5.2.6 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.

112 **Figure 5.1 ABAC Build 1 Architecture**



113

The components in figure 5.1, which were available products from NCEP organizations that met the build's functional requirements, provide the following capabilities to this build:

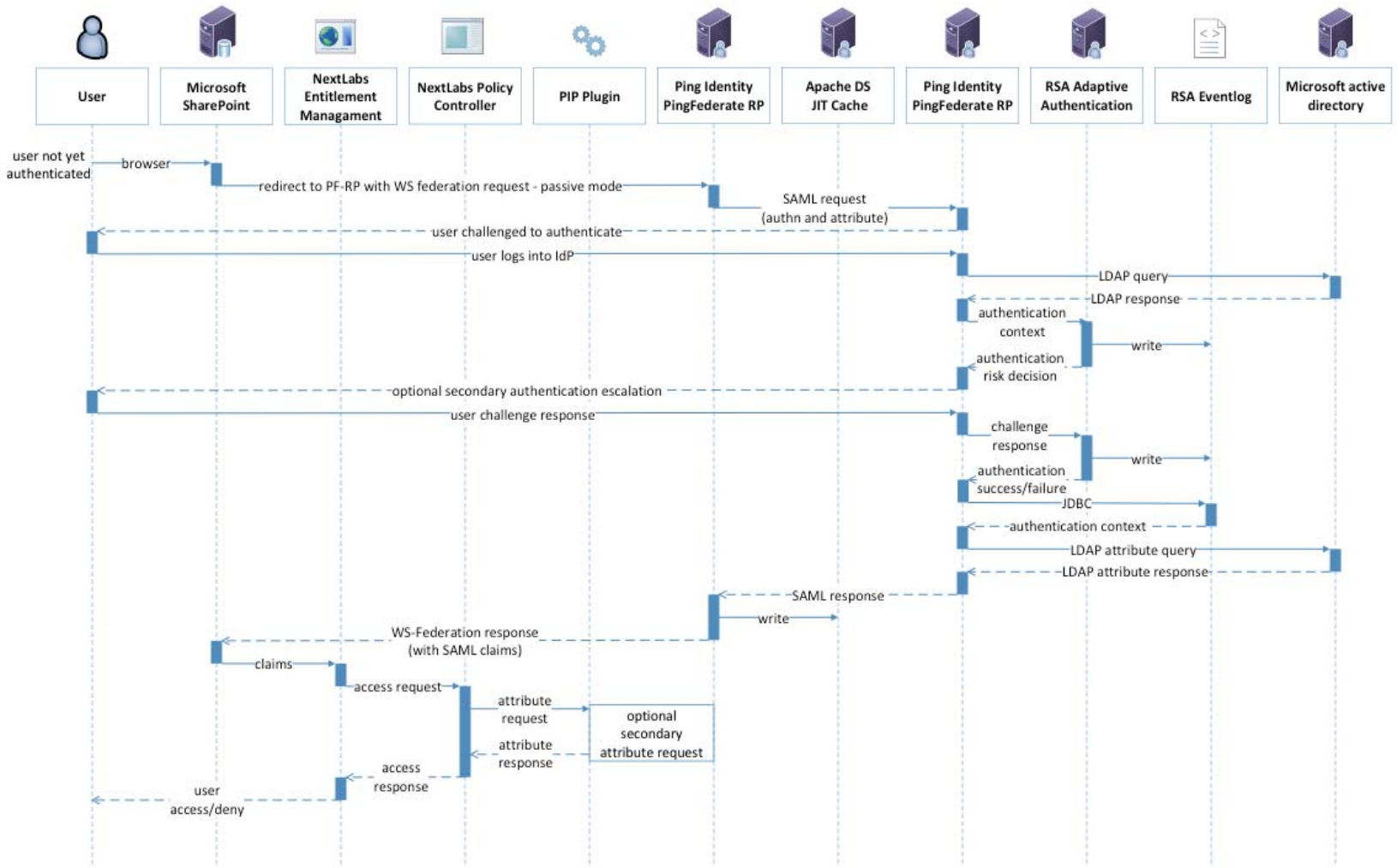
- Microsoft AD acts as a user identity management repository for the IdP. This includes the ability to provision and de-provision user identities; the creation, modification, and deletion of subject attributes; and the provisioning and de-provisioning of subject attributes to specific user identities. 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 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 Plugin 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 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 Plugin and the Protocol Broker.
- Microsoft SharePoint serves as a typical enterprise repository and 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 of SharePoint, validating the token sent by PingFederate-RP.
- Microsoft SharePoint Claims Principal is the object inside of 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.
- PIP Plugin is a software extension of NextLabs Policy Controller that enables it to acquire unavailable attributes required for policy evaluation at run time 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 Plugin and querying the PingFederate-RP by issuing a SAML 2.0 Assertion Query/Request.
- The Custom Data Store is a plugin built using PING 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.

5.2.7 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. Figure 5.2 contains a ladder diagram that represents the initial flow of the ABAC architecture, where an unauthenticated user tries to access a resource on SharePoint.

184 **Figure 5.2 UML Sequence Diagram**



185

186

The sequence starts in the top of figure 5.2 when a user browses to, and attempts to access, a protected resource in SharePoint.

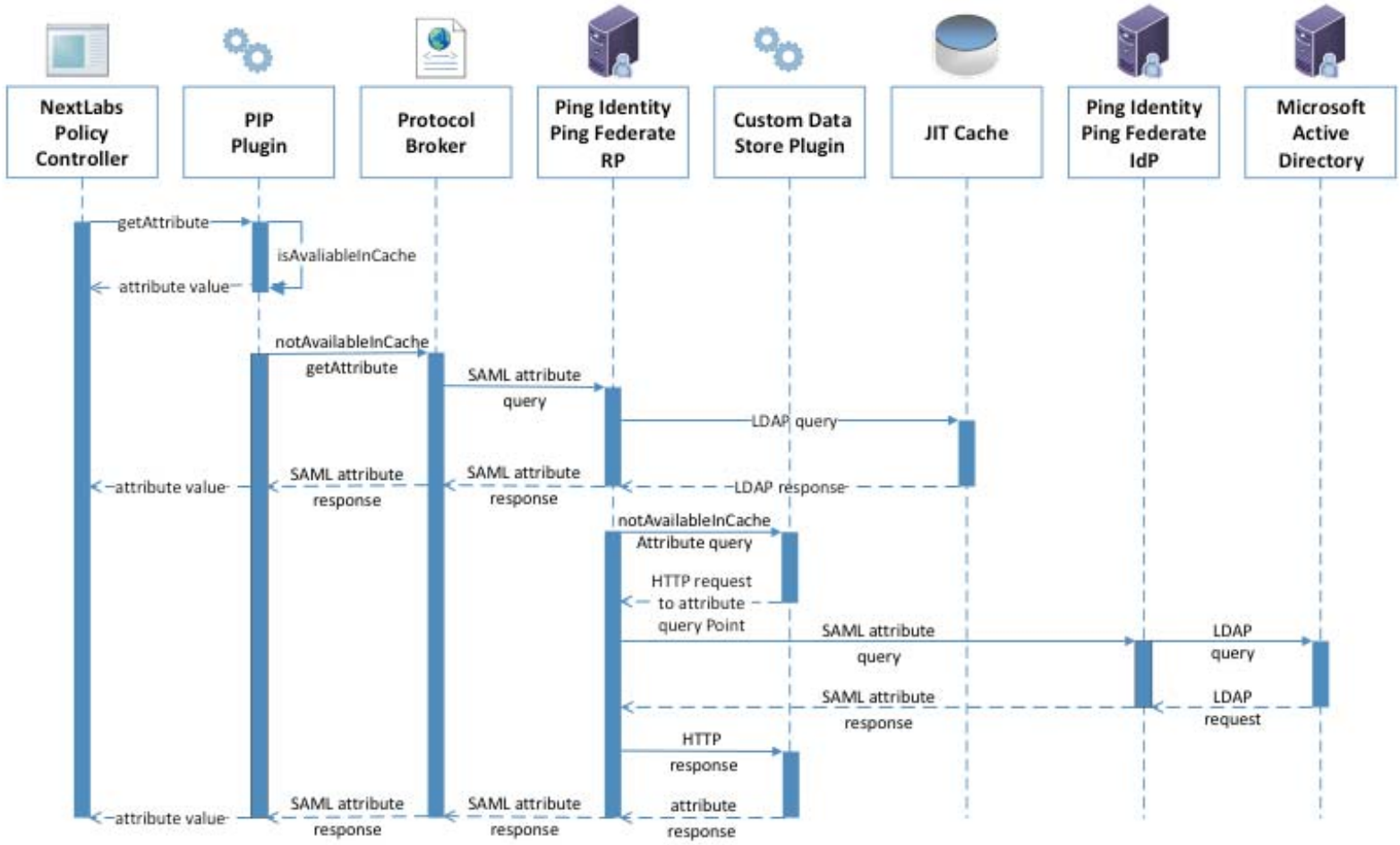
1. SharePoint inspects the user's HTTP content and finds that the user has not been previously logged in (i.e., not authenticated), and therefore re-directs the browser to PingFederate-RP via use of the WS-Federation protocol.
2. The WS-Federation request is interpreted by PingFederate-RP as a request for authentication and for attributes, and the user is redirected to PingFederate-IdP carrying a SAML authentication request and SAML attribute request.
3. PingFederate-IdP does an initial (single factor) authentication of the user, and, if successful, receives the requested subject attributes.
4. 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 via 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.
5. 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.
6. 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.
7. 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, unbeknownst to the user. 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.
8. 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.
9. The Policy Controller uses the attributes provided by the PEP and the policy established by the 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 3 and discussed later.
10. Once an access decision has been made, the Policy Controller responds back to the Entitlement Management PEP, which enforces the decision.

Figure 5.3 contains a ladder diagram that 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.

230 **Figure 5.3 Secondary Attribute Request Flow**



231

The basic steps of the figure 5.3 flow:

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 Plugin.
2. PIP Plugin is a registered plugin 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 Plugin 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 Plugin 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 plugin. The Custom Data Store plugin 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 if the user has the attribute of need, and replies back 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 plugin, which in turn passes the attribute or exception back to the Policy Controller.

5.2.8 NCCoE Design Considerations

Section 5.2, ABAC Architecture Considerations, outlined the architectural topics and options that entered into our decision making for this first ABAC build and demonstration. Now that the chosen ABAC functionality has been described and the flow and sequencing explained, in this sub-section we summarize the architectural directions that were chosen for this particular build, and why.

5.2.8.1 Industry Standards

The use of XACML and its importance to ABAC functionality was introduced in section 5.2.6. 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 gives an IdAM infrastructure

implementation potential cost saving as heterogeneous interchangeability of operational components can be more easily implemented.

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 standalone for its request/response protocol for backend attribute exchanges of NextLabs’ PIP Plugin to and from PingFederate-RP (via the Protocol Broker), and for back-end 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.

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.

5.2.8.2 PEP Placement

There is a single PEP in this ABAC build with the purpose of 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 due to meeting 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.

5.2.8.3 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.

5.2.8.4 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 in order 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.

5.2.8.5 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 Plugin contains a local cache, developed using the EhCache library. This cache stores attributes for 2 seconds and adds efficiency to the system should multiple requests for the same subject and attribute value pairing occur in quick succession (with 2 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.

5.3 Security Characteristics

In this section we re-introduce the security characteristics and security controls that were first introduced in Sections 4.4 and 4.5, and relate each here to the NCEP partner products that are being 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 the 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 MFA with one factor being name and password via PingFederate-IdP and AD, while the second is 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 in use 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 of 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 RBAC 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.

5.4 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 be dependent on the organization's individual implementation requirements and the scenarios to which an organization wishes to apply an ABAC model.

5.4.1 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 needed by an individual. This helps eliminate the potential for privilege creep.

5.4.2 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 organization.

5.4.3 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 decisions in access control policy than otherwise would be available under an RBAC system. Specifically, the ability to leverage environmental attributes allows for the inclusion of relevant context such as location of access, time of day, threat level, and client patch level into automated decision logic.

5.4.4 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.

5.4.5 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.

6 Future Build Considerations

6.1 Potential Additions to This Build

To help us expand this work in future builds, we need feedback from the user community to prioritize additional capabilities and learn from the identity and access management vendor community which commercial products provide those capabilities.

Here are some of the potential technical capabilities that may be added to this build:

- Demonstration of a wider array of authentication methods including but not limited to smart card, biometric and OTP tokens.
- The ability to support RP-initiated step up authentication. After the user has already authenticated, allow the RP to force the user to undergo advanced authentication based on the object they are accessing
- More robust logic relative to the current WS-Federate flow. Potential replacement of or supplement to the existing use of a WS-Federation request to limit the need to have a canned set of attributes with the initial user authentication, and to allow for attributes to be acquired on demand in any subsequent browser-based queries.
- Additional environmental attributes. Any potentially interesting sources for environmental attributes that may be useful for decisions based on risk.
- Implementation of SCIM 2.0 for cross-domain identity and attribute management
- Expand the implementation to include multiple IdP sources. As part of this implementation, at least one home administrative realm discovery approach based on available standards-based methods.
- Pursue an alternate federation approach such as OpenID Connect, an alternative to SAML-based federation that supports the types of browser-based queries in our scenario.
- Expand the set of protected resources beyond the single-product instance of SharePoint.

6.2 Future Builds

In additional to potential updates and add-ons to this first build, there is potential for the development and implementation of new ABAC architectures under this build. To explore these various architectures, the NCCoE would like to engage with any individual or company with commercially or publicly available technology relevant to the ABAC model. The NCCoE recently published a Federal Register notice (https://federalregister.gov/a/2015-20041) inviting parties to submit a letter of interest to express their desire and ability to contribute to this effort. Interested parties will enter into a consortium Cooperative Research and Development Agreement with NISTanticipates publishing federal register notice.

Some topics of interest for future builds include:

- use of other protocols that may be relevant to the ABAC model such as OAuth, OpenID Connect, and User Managed Access
- demonstration additional options for PDP and PEP placement, such as a loose coupling with the application
- potential architectures that use the ABAC model to protect cloud applications to include software as a service (SaaS) applications
- integration of the ABAC model with physical access control systems
- integration of the ABAC model with legacy technology where PEP integration is not feasible

All interested parties are encouraged to engage the NCCoE with additional ideas and system requirements by reaching out to abac-nccoe@nist.gov.

Appendix A Acronyms

AA	Adaptive Authentication
ABAC	Attribute Based Access Control
AC	Access Control
AD	Microsoft Active Directory
CSA	Cloud Security Alliance
CSF	Cybersecurity Framework
DAC	Discretionary Access Control
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IdAM	Identity and Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardiza-tion/International Electrotechnical Commission
JIT	just-in-time
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partner
NGAC	Next Generation Access Control
NIST	National Institute of Standards and Technology
OAuth	Open Standard for Authorization
OIDC	OpenID Connect Core
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RP	Relying Party
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SMS	Short Message Service
SP	Special Publication
SP	Service Provider
SSO	Single Sign-On
TLS	Transport Layer Security
URL	Uniform Resource Locator
WS-Federation	Web Services Federation Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language