National Cybersecurity Center of Excellence Attribute Based Access Control

William Fisher
National Cybersecurity Center of Excellence

Roger Wigenstam
NextLabs

Cyber Innovation Forum
September 9, 2015

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ABOUT THE NCCOE

STRATEGY

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

Focus on technology-driven security challenges

Building blocks address a technology-adoption gap common across multiple sectors by creating reference designs that follow the center's primary tenets (standards-based, modular, repeatable, commercially available, usable, and open and transparent).

Identify building block

Security challenges come from technology companies, systems integrators, industry, academia, NCCoE staff members, other parts of NIST and other government agencies, and the public.

Seek public comment

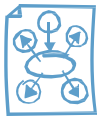
Building block descriptions include a problem statement and goal, security characteristics, approach, architecture, technology component list, and relevant standards and best practices. The NCCoE seeks public comment on the applicability of the challenge and the validity of the proposed approach, then publishes a revised building block description with the public comments and their disposition.

NATIONAL CYBERSECURITY EXCELLENCE PARTNERS

Cybersecurity solutions that are:

based on standards and best practices

usable, repeatable and can be adopted rapidly



modular, end-to-end and commercially available

developed using open and transparent processes

matched to specific business needs and bridge technology gaps

ATTRIBUTE BASED ACCESS CONTROL

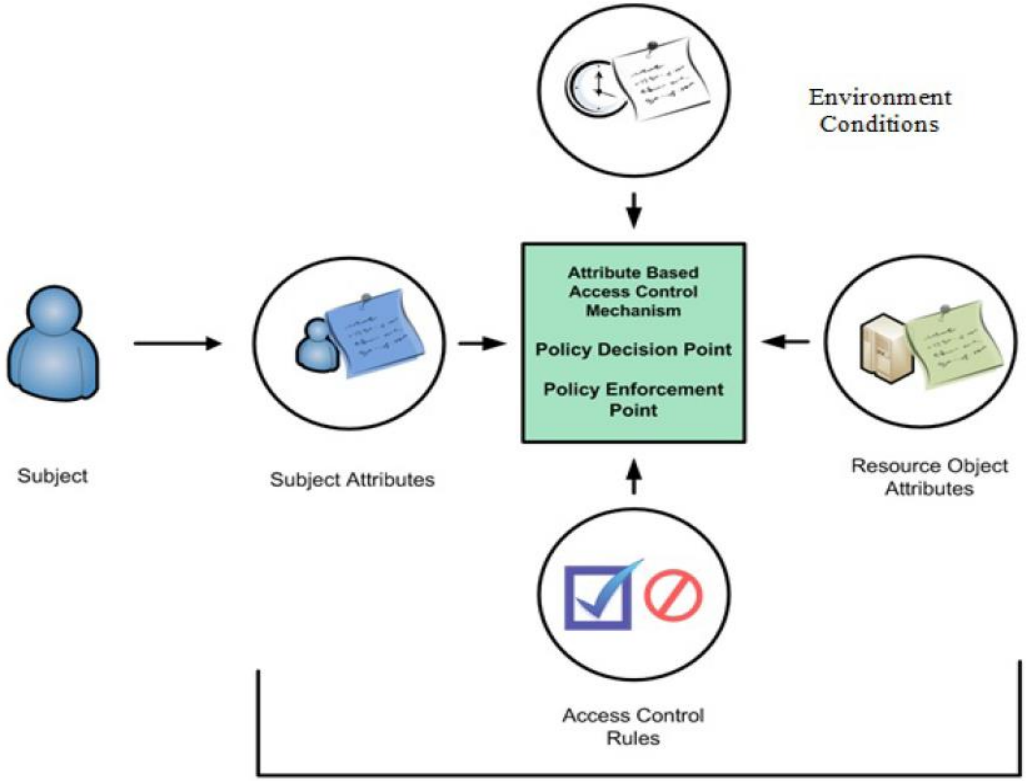
Goals

- Enterprise to enterprise identity federation
- Enable access control decisions for previously unknown users
- Demonstrate security capabilities that support a wide range of enterprise risk postures

Business value

- Simplified identity management
- Shared IT resources across multiple enterprises
- Reduced risk through highly flexible access control

What is ABAC?



"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" – NIST SP800 - 162

How does ABAC differ from RBAC?

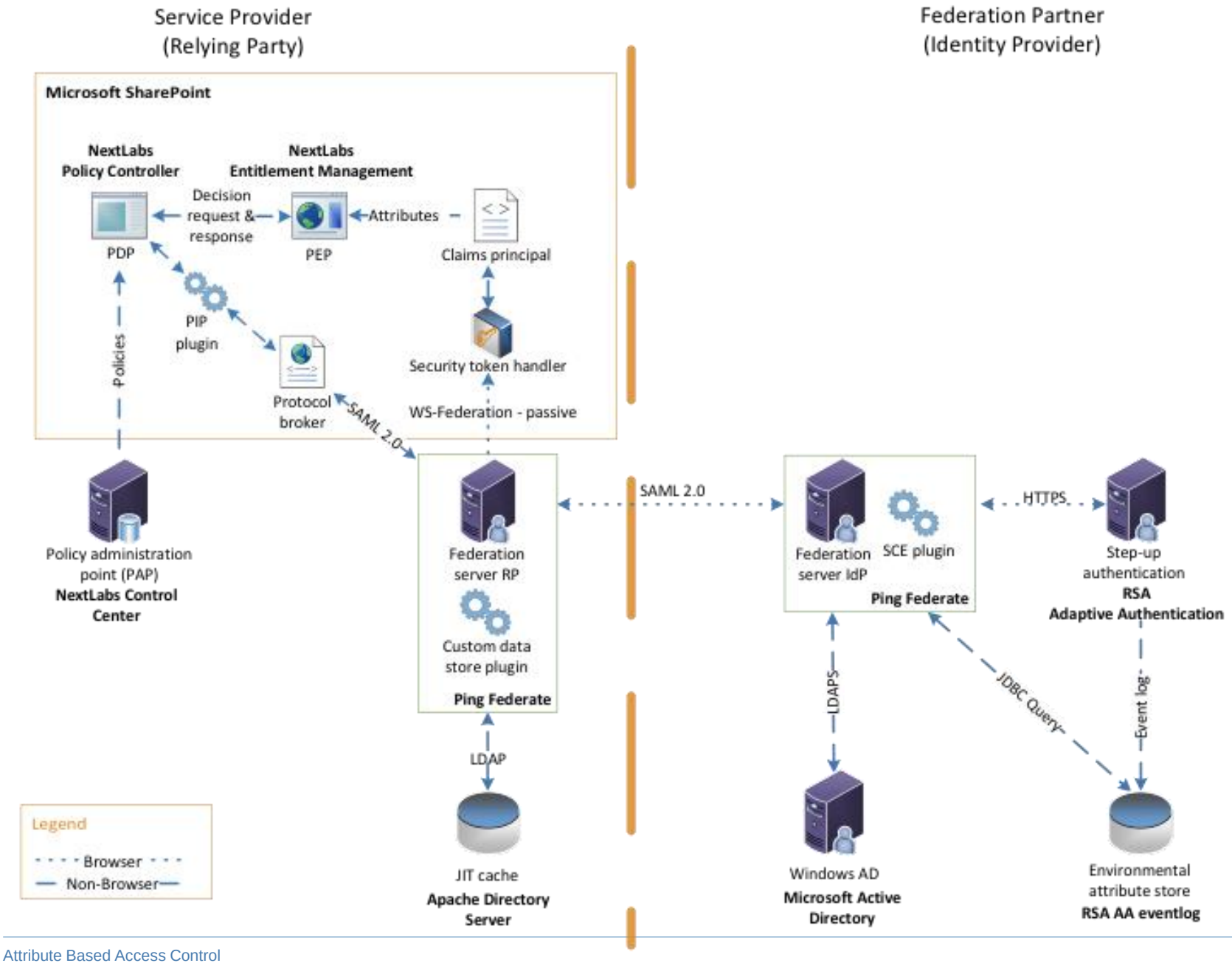
Three primary differences:

- RBAC buckets user into groups based on roles. ABAC does not bucket employees, but rather employee access decisions are made based on a set of attributes assigned to an users digital
- RBAC via roles, creates a one to one relationship between the role and objects that can be accessed by that role. ABAC abstracts the relationship between the role and the objects into policy.
- ABAC allows for the use of environmental attributes, such as time of day, IP address, or threat level to be defined and implemented in access control policy.

Create and demonstrate a standards based service that supports identity and attribute federation and fine-grain access decisions:

- User Authentication and the Creation of an Authentication Context
  - LDAPS, SAML 2.0
- Federation of a User Identity and Attributes
  - SAML 2.0, WS-Federation, TLS
- Fine-Grained Access Control through a PEP Closely Coupled with the Application
  - XACML
- The Creation of Attribute-Based Policy Definitions
  - XACML
- Secondary Attribute Requests
  - HTTP, TLS, SAML 2.0
- Allow RP Access Decisions on External Identities without the Need for Pre-Provisioning

ABAC Architecture



Current Build Partners

Microsoft – Sharepoint: Protected Resource

Symantec – Trust Cert Manager: Certficate Authority

Ping Identity – PingFederate: Federation Server

RSA – Adaptive Authentication: Authentication escalation and environmental attributes

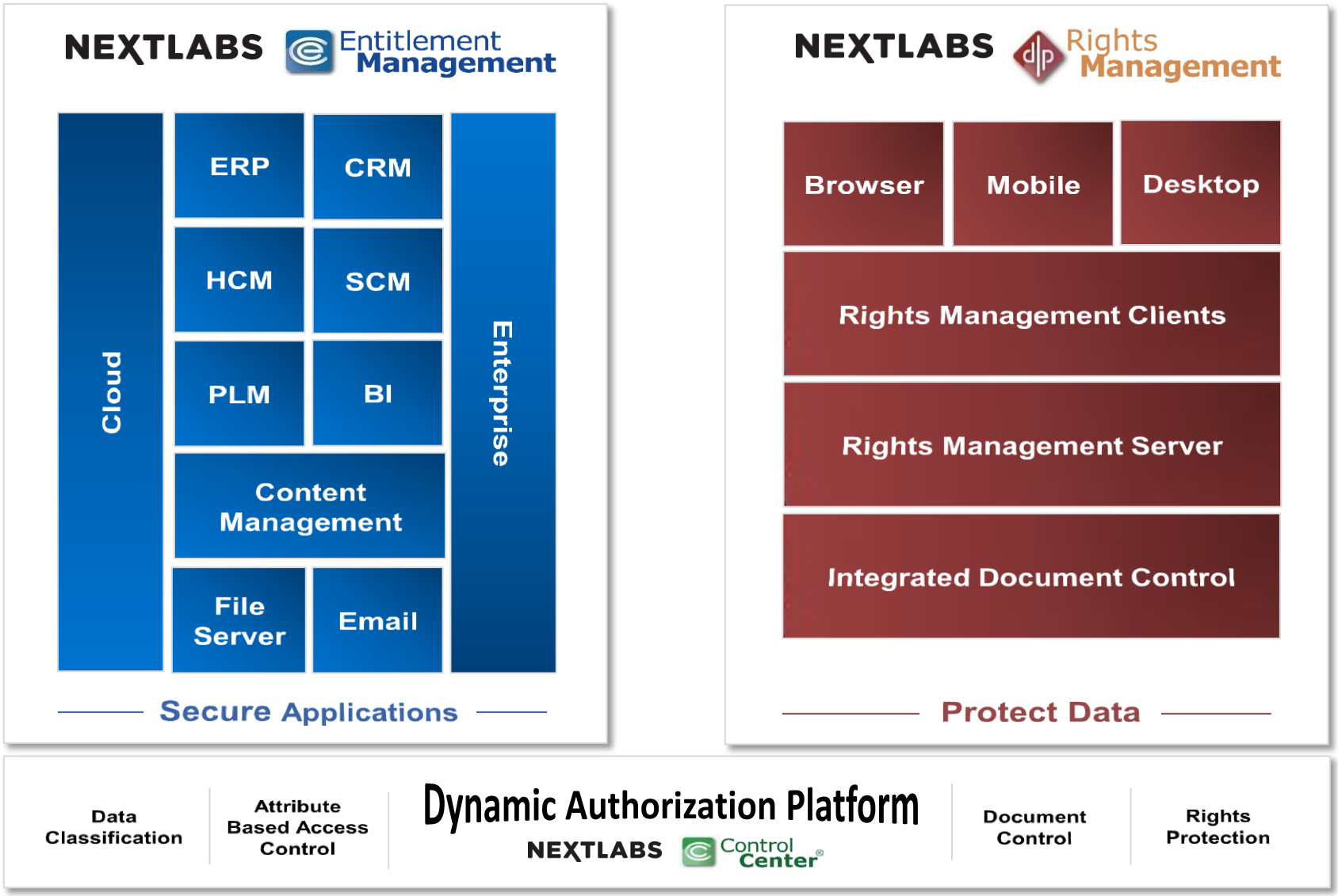
NextLabs – Control Center and Entitlement Manager: XACML PEP and PDP

Note: 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.

Benefits to the Business:

- Supports organizations with a diverse set of users and access needs, offering efficiencies in provisioning access
- Reduces the number of identities managed by the enterprise, thereby reducing costs
- Enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policies for users and networked devices that include factors such as environment and time of day
- Collaboration among organizations by allowing an enterprise to accept identities authorized by other enterprises, eliminating the need to pre-provision access for those identities
- Centralization of auditing and access policy management, creating efficiencies of policy management and reducing the complexity of regulatory compliance

Product Overview:



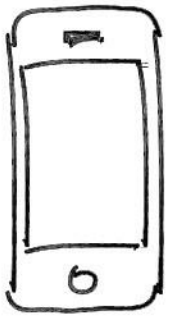
NEXT STEPS

NCCoE:

- ABAC Federal Register Notice
- Release of the SP 1800-3 ABAC practice Guide

Users and other interested parties:

- Provide public comments on SP 1800-3
- Reach out to the NCCoE about applicable ABAC technologies and Standards

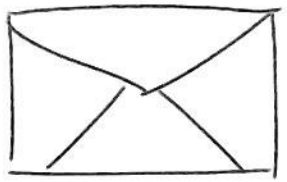


240–314–6800

abac-nccoe@nist.gov

Participate

h/p://nccoe.nist.gov



9600 Gudelsky Drive
Rockville, MD 20850