DATA SHEET

CA Layer 7 Attribute-Based Access Control for Government

At a Glance

The heart of any government information system is its ability to grant access control to those who have a "need to know." CA Layer 7 solutions use federally-recommended Attribute-Based Access Control (ABAC) to address the kinds of security and visibility issues that characterize threats. CA Layer 7 ABAC solutions work with government agencies to support their need to share information more quickly, while introducing a more robust set of access and security controls. With CA Layer 7 ABAC solutions, agencies can implement a "trust but verify" process to counter problems before they occur.

Key Benefits/Results

- **Easily secure users.** Establish or delete user provisioning quickly by assigning appropriate user attributes.
- **Flexible.** Leverage consistently defined attributes to roles or groups while maintaining appropriate levels of security.
- **Share monitoring and access data.** Access the relevant data you need to utilize APIs and services so you can share it with departments or agencies that monitor the network or enterprise.

Key Features

- **Detect data exfiltration.** Define and enforce digital policies to limit the number of times a single user can retrieve a single type or multiple types of data, which could be interpreted as having malicious intent when aggregated.
- **Access control.** Federate enterprise attribute services for attributes shared across departments or agencies to ensure access for users with a "need to know."
- **Data monitoring and visibility.** Track authentication attempts and valid authorizations to analyze distributed data retrieval trends on a per- user basis as a part of federation identity management across departments or agencies throughout the network or enterprise.

Business Challenges

In government, anyone in a position to obtain classified information has been interviewed, reviewed and investigated before they are assigned a security clearance level that allows them access to internal systems and the information they hold. Making attribute data externally available can pose a significant security risk, and locking down classified information across agencies requires more than just the traditional broad clearance bands.

Traditionally, isolated branches of government could grant or deny access to information and sharing systems based on a user's level of clearance, the network being used or course-grained information such as the user's branch of service. But the complex requirements of today's information sharing initiatives can no longer be adequately secured by the Role-Based Access Control (RBAC).

Also, the interconnected agencies, department and systems encounter challenges with variations in attribute data, such an officer's rank being encoded as both "Lieutenant Colonel" and "LtCol," and other inconsistencies that are often found as a result of a process problems, insufficient training or typographical errors.

The traditional use of RBAC on a project-by-project basis lacks the interoperability and flexibility that today's U.S. federal and local governments need to ensure secure access across systems. The emphasis on information sharing between organizations needs a solution with greater reach and broader capacity than past access control solutions.

Solution Overview

CA Layer 7 ABAC solutions give you the ability to assign multiple qualifying attributes to users, resources and environments. Once in place, authorizations can be more closely tracked and monitored, and alerts can be set up to flag unusual behavior.

Not only can CA Layer 7 ABAC solutions provide support for building attribute services based on the leading standards, it can provide policy-based security for authentication, authorization, digital signing and encryption to meet the highest security requirements for information dissemination. CA Layer 7 ABAC solutions allow digital policy to be defined and enforced across distributed information silos, as recommended by the NIST Guide to ABAC Definition and Considerations SP 800-162 and other efforts.

With CA 7 Layer ABAC solutions, government agencies can confidently promote information sharing between organizations as recommended by the Federal Identity, Control and Access Management implementation (FICAM) Roadmap v.2.0.

Critical Differentiators

CA Layer 7 ABAC solutions feature key differentiators for successful, secure ABAC so you can:

Collect and disseminate attributes securely by using Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) which provide the rule sets used to make decisions such as whether or not to authorize the user access to requested resources based on the description of the user's attributes.

Define and enforce WS-Policy and XACML-based rules for information discovery, retrieval and dissemination across a variety of security realms and boundaries, whether internal, enterprise or in the cloud.

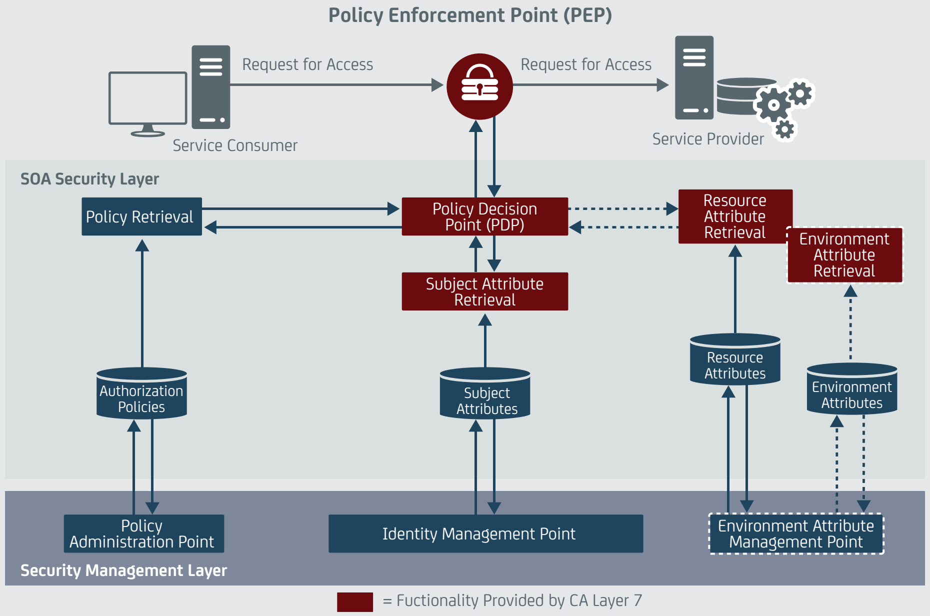
Identify and mediate attribute consistency challenges across shared systems with XML schema (XSD) validation (XSD) and transformation (XSLT) capabilities.

Receive support for SAML Attribute Sharing Profile for X.509, as well as Backend Attribute Exchange (BAE) identified by Homeland Security Presidential Directive 12 (HSPD-12).

WikiLeaks—A Case for Attribute-Based Access Control

WikiLeaks is an international, non-profit organization that publicly publishes private, secret and classified government and corporate information. Based on media reports, the recent leaks of 400,000 classified government documents and 250,000 confidential diplomatic cables were attributed to a single person.

Attribute-Based Access Control–Maximize your organizations attribute services for greater security.


Policy Enforcement Point (PEP)
Request for Access
Request for Access
Service Consumer
Service Provider
SOA Security Layer
Policy Retrieval
Policy Decision Point (PDP)
Resource Attribute Retrieval
Environment Attribute Retrieval
Subject Attribute Retrieval
Authorization Policies
Subject Attributes
Resource Attributes
Environment Attributes
Policy Administration Point
Identity Management Point
Environment Attribute Management Point
Security Management Layer
🟥 = Fuctionality Provided by CA Layer 7

In the government, anyone in a position to obtain classified information has been interviewed, reviewed, and investigated before they are assigned a security clearance level that allows them access to internal systems and the information they hold.

But to lock down classified information, government requires more than just the traditional broad clearance bands. What's required is the ability to assign multiple qualifying attributes to users, resources, and environments. Once in place, authorizations can be more closely tracked and monitored, and alerts set up to flag unusual behavior.

Using CA Layer 7's ABAC solutions, access management will no longer be just a matter of a role-based security clearance.

Government agencies will be able to define and enforce rules for information discovery, retrieval and dissemination across a variety of security realms and boundaries. With the right kind of controls in place, insider-threat security breaches like WikiLeaks can be avoided.

For more information, please visit **ca.com/security**

The CA Technologies Advantage

CA Technologies (NASDAQ: CA) provides IT management solutions that help customers manage and secure complex IT environments to support agile business services. Organizations leverage CA Technologies software and SaaS solutions to accelerate innovation, transform infrastructure and secure data and identities, from the data center to the cloud. CA Technologies is committed to ensuring our customers achieve their desired outcomes and expected business value through the use of our technology. To learn more about our customer success programs, visit **ca.com/customer-success**. For more information about CA Technologies go to **ca.com**.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.