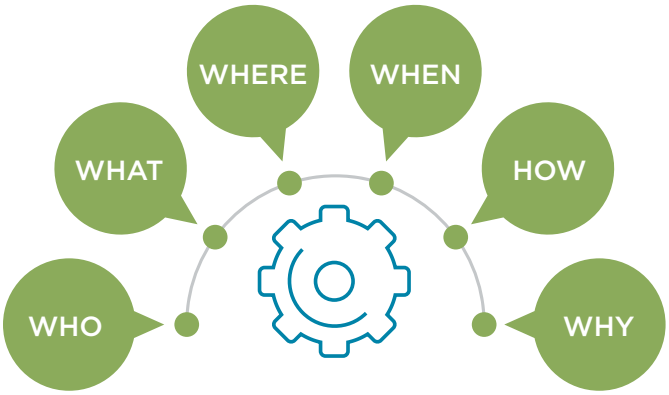
THE KEY TO API SECURITY

FINE-GRAINED AUTHORIZATION FOR THE API-ENABLED ENTERPRISE

BENEFITS IN BRIEF

- Expose data via APIs and microservices securely.
- Enable efficient reuse of sensitive information assets.
- Enforce policy-based authorization aligned with business rules.
- Remove the need to re-code individual applications when corporate policies change.
- Reduce time and cost of developing/maintaining APIs and microservices.
- Extend API Gateway authorization by utilizing OAuth, OIDC and ABAC.

ATTRIBUTES



The Attribute Based Access Control (ABAC) model brings fine-grained, context-aware authorization to APIs. It enforces real-time access controls at the application, API and database layers, in-line with corporate policies.

ENHANCE API SECURITY AND EXPOSE SENSITIVE DATA SECURELY

APIs and microservices have revolutionized the way we exchange data and have become the preferred method for exposing data to external parties. However, APIs that handle sensitive data pose security and data access control challenges, and therefore require advanced security solutions.

An important component in API security is the management and enforcement of authentication and authorization via industry standards OAuth 2.0, OpenID Connect (OIDC) and Attribute Based Access Control (ABAC). API Gateways are very effective at mediating the data flows between these industry standards. If business critical data, personal identifiable information (PII) or any other sensitive data is involved, additional fine-grained authorization capabilities are easily implemented through configuration of the API Gateway.

ATTRIBUTE BASED ACCESS CONTROL- SHARE THE RIGHT DATA UNDER THE RIGHT CONDITIONS

Axiomatics' fine-grained authorization solutions utilize ABAC to ensure only the right users get access to the right information under the right conditions. With the use of attribute-based authorization that is driven by policies, user permissions can be aligned with rules, regulations and corporate policies, thus protecting sensitive information. Attributes from OAuth scopes, OIDC JSON Web Token (JWT) claims and the ABAC system provide the greatest breadth of capability to cover almost any industry use case.

For instance, if insurance customers wish to change their insurance plans online, checks must be made that cannot be managed by the API Gateway. Have all bills been paid or have due dates been exceeded? If the user is a parent, can the plans of a child be accessed? If the user is an HR representative of a corporate client, does the contract allow changes to be made for a given company employee? The ABAC solution will simply evaluate business policies for the correct answer, which can't be done with OAuth or OIDC alone – unless considerable extra

code is added to the API or microservice. It will then return a "permit" or "deny" to the request after all these factors have been considered.

This type of fine-grained access control adds the extra layer of security that is required to support new, API-driven, business opportunities, while meeting compliance regulations.

WHEN IS ATTRIBUTE BASED ACCESS CONTROL (ABAC) THE BEST FIT?

Attribute Based Access Control (ABAC) is used when confidential and sensitive data is at stake. Axiomatics offers solutions that can protect data on the application, API and database layers.

The Axiomatics Policy Server (APS) provides authorization services to API Gateways and applications from a central point. This externalized method of securing data is resource-efficient and scalable, as rules and policies only need writing (or editing) once and can be applied across multiple protected infrastructure components.

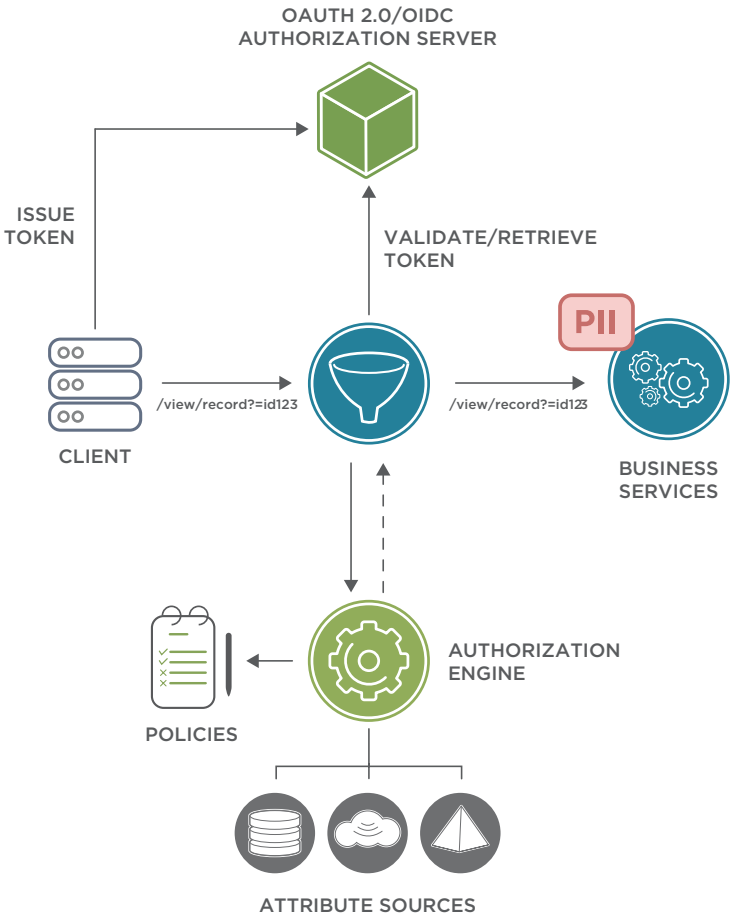
API Gateways are often used to protect web portals exposing different types of web services. The Axiomatics Policy Server then sits at the back-end and acts as the policy decision point. The API Gateway integration ensures that policies are consistently enforced by the API Gateway across all channels and request types.

The integration with the Axiomatics solution means ABAC protection can be leveraged for many different types of resources, such as document management systems, ERP integration points, or message queues for various back-ends.

WHEN OAUTH ALONE IS NOT ENOUGH

OAuth tokens are ideal for delegated consent authorization scenarios and OIDC JWT tokens add a layer of user information useful in single sign-on use cases, but they are not sufficient when fine grained access is required. By using ABAC as a supplement, Axiomatics helps you avoid OAuth being used beyond its intent, resulting in Franken-scopes, scope explosion, and authorization logic creeping into your microservices. The Axiomatics ABAC suite works across the leading API gateways - we've helped customers around the world with varied needs - with one key goal - to securely share data to improve the customer experience. By using industry standards, no custom coding or SDKs are needed to achieve interoperability between Axiomatics and the API Gateways – You only need to configure gateway settings to add enhanced ABAC capabilities to your API security implementation.

A SAMPLE ARCHITECTURE FOR API SECURITY



Find out how you can increase the security of your APIs and protect sensitive and business critical data. Please visit our website or contact us for a demo.

WWW.AXIOMATICS.COM | WEBINFO@AXIOMATICS.COM

525 W Monroe St., Suite 2310
Chicago, IL 60661, USA
+1 (312) 374-3443

42395 Ryan Rd
Suite 112 - PB Box 805
Brambleton, VA 20148
+1 (801) 556-9994
sales@axiomaticsfederal.com

Västmannagatan 4
S-111 24 Stockholm, Sweden
+46 (0)8 51 510 240