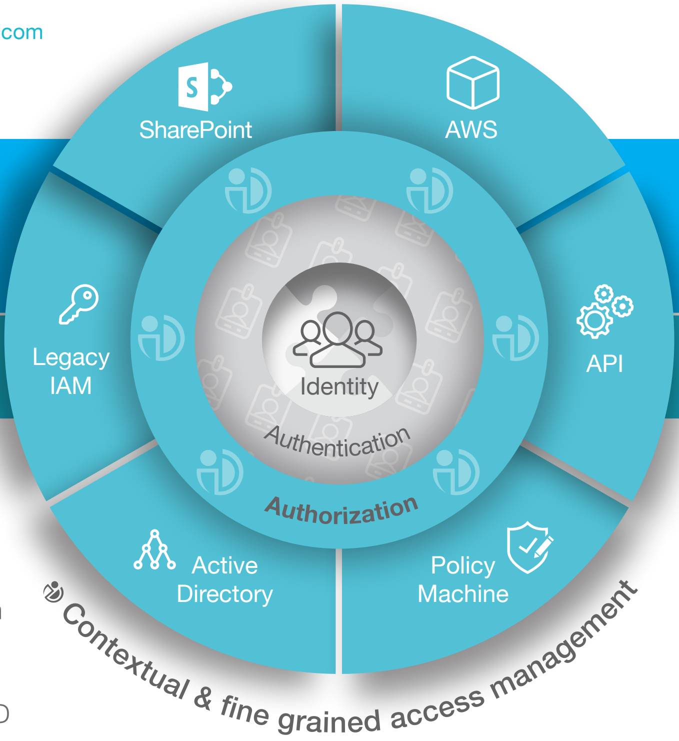
plainID
AUTHORIZATION MADE SIMPLE

info@plainid.com www.plainid.com

# We Authorize!

## Unified Authorization Platform



## PlainID: A focused approach to Authorization

PlainID is the go-to Authorization solution, we secure digital assets with one unified authorization platform that accommodates cloud, mobile and legacy applications. PlainID sorts the Authorization mess using contextual, dynamic based business policy. Companies that use PlainID benefit from a simplified Authorization platform and meet the demands of growth without worry.

### This truly is a fresh approach to prevent time wasting on Identity and Access Management.

## The Challenge

Organizations are trying to deal with the ever-growing complexity of who can access what. This challenge has just reached a whole new level as businesses demand support to back their rapid growth, expand their boundaries to the cloud and mobile.

### Is your legacy IAM up to the increasing challenges?

- How easy is it to adopt new technologies, Cloud & Mobile?
- Does your provisioning solution support high performance requirements?
- How fast can you roll-out new projects?
- Do you support distributed identities and identity attributes?

We Authorize!

### Moving to the cloud is a challenge, Are your Authorizations ready?

- How can existing users access cloud environments?
- How should (or can) existing authorization policy be enforced?
- How can that be done with minimal IT efforts?
- How can a unified view of internal and external managed resources be maintained?
- managed resources be maintained?
- How can we avoid extending the security perimeter of the organization?

### API adoption is increasing rapidly, Are you ready?

- Audit & Compliance readiness – Do you have a visible access policy? How easily can you see who can access your APIs?
- Access control – Do you have a manageable access policy? How many code parts do you maintain, to control that access? How scalable is your access control with the increasing numbers of APIs?
- Cross platform support – your APIs can be scattered, some on premise, some in the cloud. You might even have several API gateways. Can you control and monitor all in one place?
- IAM compatibility – Are your APIs part of you IAM strategy? Can you base access decisions on IAM managed data?

# A Fresh Approach to Authorizations

## Dynamic vs. Static Authorization

Classic Authorization methods rely on repository defined groups or roles that link between users and resources. Those access decisions are preconfigured and can not change in real time.

PlainID lets you influence access decisions in real time based on environmental attributes and events.

For example, you can allow your regional sales team access to accounts data, but restrict it only according to their region and only from their office – and only from 7:00 to 17:00, or even blocked on occasion (such as cyber security breach). The decision of who can access what is not predetermined, it is calculated in real time.

### NIST speaks to the gap in the marketplace and the need for:

- Simplify Access Management
- Reduce Risk due to Unauthorized Access
- Centralize Auditing and Access Policy

## Attribute Based vs. Role Based

Traditional role-based access control (RBAC) connects a predefined role to users. Using this method, the role itself and the connections to users need to be managed. Attribute based access control (ABAC), on the other hand, offers a more flexible method to connect users, based on their attributes to groups, resources and actions. This approach reduces the required Authorization management and enables an easier way to scale up with current and future implementations.

PlainID amplifies Attribute-Based Access Control (ABAC) by providing a flexible policy, that enables attribute based decisions all the way from the user to the group/resource. For example, in just one policy statement you can determine that a user can access his department documents. Which documents, will be determined at time of access, based on a match between the user's department and the document-assigned department.

## Why you need PlainID

✓ **Move forward faster** - Take advantage of PlainID's deployment simplicity. New projects can now be easily deployed and managed to meet growth goals.

✓ **Be ready with new technologies** - PlainID is the first truly technology-agnostic platform for Authorization. It scales up easily on premise and in the cloud and increases the efficiency of new implementations

✓ **Take control of all your assets** – With PlainID's third-generation entitlement platform, AuthZ decisions can be used as a service within the company. You can now set standards, and can use one policy many times over to save resources.

✓ **Enhance your security** - Connect your identities directly to data and resources, based on real time decisions, and with no provisioning.

## Visible Business-Oriented Policy vs. Technical Policy

Today, most applications/platforms have the access policy coded within, usually by someone with a technical background.

PlainID lets you define a business-oriented policy that can be simply managed and used by business owners who have no technical experience. In addition, PlainID provides a much more comprehensible language (through visuals) that enables simple investigation of who has access to what. The application access policy, can then be extracted from the code and mapped accordingly to the visual business policy.

# The Solution: PlainID Unified Authorization Platform

PlainID simplifies AuthZ to one point of decision, one point of control and one point of view.

### • A Business-oriented approach

Our solution is designed for both business owners and administrators to define, understand and use. PlainID “talks” to each in his language enabling better management and control.

### • Universal Authorization support

AuthZ can be consumed using industry leading standards, XACML, OAuth & SAML alongside custom and tailor made protocols. Simple and fast allow/deny per request or a fully detailed access decision.

### • Fine-Grained Authorization

PlainID amplifies Attribute-based Access Control (ABAC) by providing a flexible policy, that enables attribute based decisions all the way from the user to the resource/action, based on a pattern or resource attributes.

### • Distributed identities

Multiple identity types and multiple identity sources. PlainID provides a comprehensive view of the identities you need to authorize. Employees, customers, system accounts - It really is one solution for all.

### • In-depth Analytics and Insights

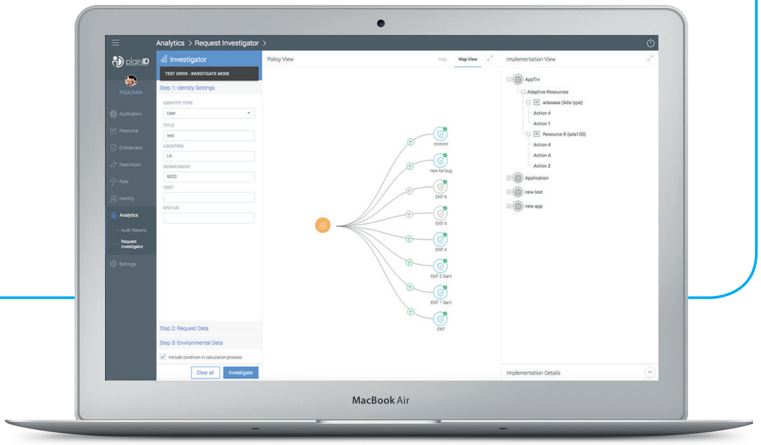
PlainID provides unobstructed visibility with a full audit trail. Compliance, regulation and audit requirements - they’re easy to manage on a simple graph-based UI.

### • Contextual access

Access is determined dynamically and in real time, based on user attributes, environmental attributes (time, location, etc.) as well as event based authorizations. PlainID combines ABAC & RABC to a united policy.

### • Policy lifecycle management

Using PlainID you can build your policy on a graph based editor, have it approved and certified. That, with the policy simulator, provides a tighter control of access to data and resources.



IDENTITY TYPE: User

TITLE: test

LOCATION: LA

DEPARTMENT: 9000

TEST:

STATUS:

☑ Include condition in calculation process

# Your 3 steps to working with an authorization policy:

### Set your building blocks

Discover Users & users’ attributes

Discover security roles

Discover Resources

### Build your policy

Connect identities to data & actions

Set your context considerations

### Provide decisions

Provide real time authorization decisions to your on premise applications, cloud and mobile.

# PlainID: Leading vendors we support

### SailPoint (IdentityIQ)

The integration between PlainID and SailPoint extends the IdentityIQ context into various cloud providers, starting with Amazon Web Services (AWS). Access to AWS resources is now controlled from IdentityIQ, making migration to AWS more efficient and secure while unifying and aggregating AWS access controls into the existing identity governance platform.

SailPoint Identity+ Alliance

### AWS (Amazon Web Services)

PlainID unique integration with AWS, enables the organization to control access to AWS resources, providing full visibility and connection to existing users and managed data.

### ISIM (IBM Security Identity Management)

PlainID offers full integration with ISIM, enabling ISIM customers to enhance ISIM capabilities with business oriented authorization management, attribute based and automatic permission assignments, progressive authorization deployment and adaptive requests work-flow.

PlainID is constantly working towards additional integrations with leading vendors. We'll be happy to share the full details of currently supported integrations, as well as discuss the new ones to expect.

plainID AUTHORIZATION MADE SIMPLE

info@plainid.com www.plainid.com

## It's all about AuthZ

✓ AuthZ should be easily given and easily revoked.

✓ AuthZ should be available anywhere needed (In the Organization, On the Cloud, on the mobile device, etc.)

✓ AuthZ should be spoken in a business language, in addition to the technology one.

✓ AuthZ should be given to any entity, People, Devices, Things (IoT) or services.

We Authorize!