PlainID

Talking business
Delivering security

Simplifying identity management.

Contents

Executive Summary

Security is meant to be a business enabler, assisting an organization to progress and develop. PlainID's focused approach to access rights delivers secure solutions for efficient business management.

The Challenges

- Moving to the cloud – SaaS/PaaS based solutions
- Average growth of 40+ applications a year within the enterprise
- Moving to BYOD and publishing – access from outside the enterprise as well as from inside

Access rights management – a complex, ever-growing challenge for every enterprise

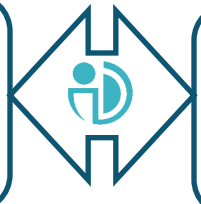
The Solution

PlainID: A focused approach to access rights

Provides business oriented access rights management, easy adaptation to continuing growth, and helps avoid compromises between business needs and security

Enterprise:

Focus on usability
→Business oriented, attribute-based and role-based access rights



Application:

Focus on functionality
→Application capabilities, action and data oriented

Talking business and talking technical – Access rights are discussed in business language as well as in technical language. For example, the employee has access to *Accounting*, which, from a technical aspect, is connected to groupAC in the active directory and to G123AC in the ERP.

Focusing on employees and focusing on customers – PlainID automatically provides the access employees and customers require, according to the enterprise policy, from anywhere – office, mobile, home – to any application.

Unified view – of the employee and the customer access rights; for the enterprise, PlainID, via just one click, presents the access rights and the locations from which they can be accessed.

Easily managed – Access rights are easily assigned or revoked, based on attributes or roles, or manually, via a user friendly interface.

Access rights management requires expert understanding and a focused approach. At PlainID, we are the experts and we offer advanced and focused solutions for access rights management.

The Challenges

Moving to the cloud

For many organizations, moving to the cloud is tempting from a resource perspective, but challenging from a management perspective. Each enterprise decides which applications move to the cloud, and which remain within the enterprise. Moving to the cloud is an incremental implementation, adding to the complexity. As a result, access rights must be managed internally in the enterprise and in the cloud, adapted to ongoing changes. Moreover, access rights management must have the same look and feel for internal and for in-the-cloud management. It must also support phased moving of applications to the cloud while maintaining uniform management language.

Average growth of 40+ apps a year within the enterprise

Enterprises are required to roll out more and more apps to keep pace with business demands. For every app, access rights must again be addressed, and the choice is either a full technical group of admins/tech guys/developers to handle the access rights issue, **or** a decision to compromise in delivery or security.

Either way, dealing with access rights is time-consuming and expensive.

"With "healthcare Y2K" looming and accelerated demand, seven of 10 CIOs are rolling out more enterprise apps during 2013 (46 on average) to keep pace with frontline business needs."
http://www2.delphix.com/cio-outlook-2013

Moving to BYOD and publishing

With the growth of Bring Your Own Device (BYOD), enterprises face a new demand – how to handle access rights that are already managed to some degree within the enterprise, in the mobile environment, and in the publishing platform. Whether BYOD is based on mobile device management (MDM), a publishing platform or native apps, the issue is the same – to provide and manage access rights.

Moving to the cloud to answer business needs, keeping pace with rollouts of new apps, BOYD and publishing necessitate employing a group of tech guys and developers; if not, ease of management and security are compromised. Ideally, the enterprise aims to meet all demands while keeping expenses under control.

The Solution

PlainID answers these challenges with a focused approach to access rights.

PlainID introduces two products solutions: PlainID for IDM simplifies identity management implementation, and PlainID Dynamic access provider (DAP) provides access rights using known standards in the field.

Business Talk

Ask an HR manager and a domain administrator, "What are access rights?" and you will surely hear two different answers. "It's the ability to access the HR module in the ERP," according to the HR manager. Meanwhile, the response of the domain administrator is, "But accessing the HR module in the ERP requires a HRgroup in the active directory (for portal link) and an additional group in the ERP. Since I'm not familiar with all the definitions, we'll need another tech guy to complete this."

Who has the right answer, business or tech?

Both! When talking about access rights, the business owners and users talk about what they know and need, in their language – the business language of access rights.

The tech guys address the actual definitions in the domain, LDAP, Unix, mainframe, ERP, and more.

Clarifying the issue

In general, applications focus on their purpose – for example, HR management or accounting – that's the app's specialty, not access rights. The same is true for provisioning mechanisms – the focus is on provisioning to many platforms and applications, but not usually on access rights. Access rights are a byproduct for applications and most provisioning mechanisms.

What's the solution? PlainID: a focused approach to access rights

PlainID recognizes the needs in both worlds and provides a bridge between them. The business language is required to clearly define user access rights and authorization. The tech language is required for the application, the platform.

PlainID specializes in access rights:

- ✓ Business oriented approach to access rights
- ✓ Multiple environment connections support
- ✓ Many-to-many support for business – tech connections
- ✓ Full presentation from business and tech points of view

Defining authorization with business language relevancy

Focusing on Employees and on Customers

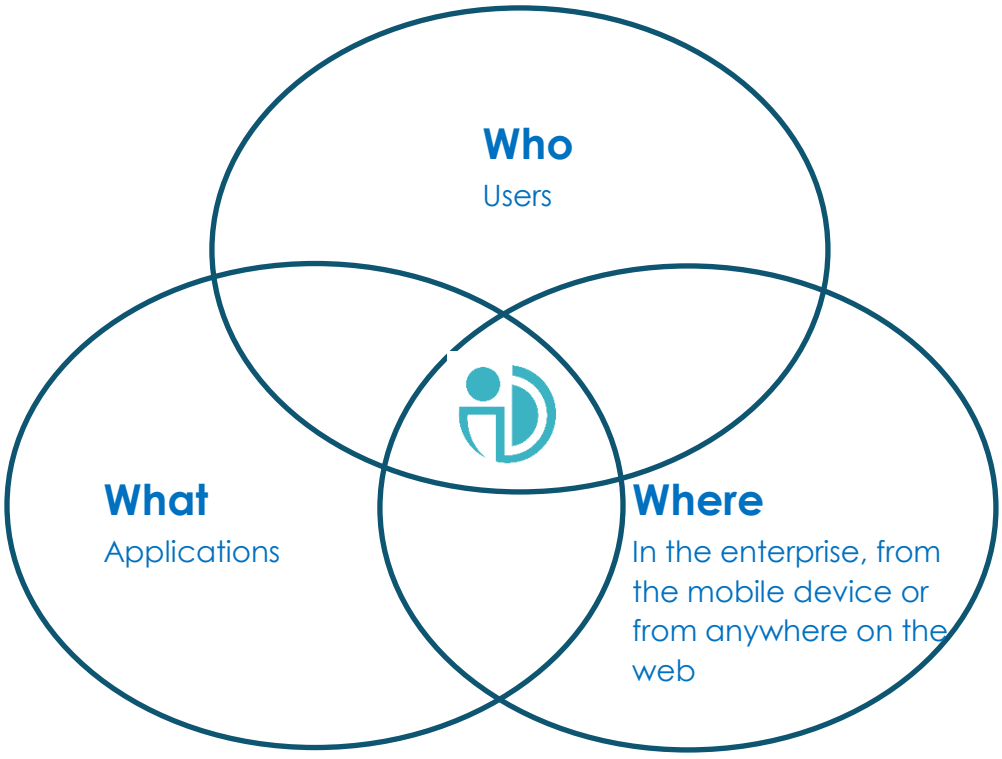
A focused approach to the employee and to the customer answers both business and security requirements.

Define who – attribute or role based, dynamic and flexible rules that determine the "who can access". PlainID enables automatic rule based or manual access rights management.

Define what – Business language and tech language for describing and using the full spectrum of access rights, wherever the application is located, inside the enterprise or in the cloud.

Define from where – From within the enterprise, the mobile device or from anywhere on the web.

According to the enterprise's policy, the **Who** can be connected to the **What** and the **Where.** Dynamic, flexible, and via a user friendly interface.



Unified View

Unified view of the employee and of the customer

The applications, actions, and data that the user can access and from where access is initiated—all in one unified view—and easily accessed by managers, accounting officials, and by any authorized user. All presented in easily understandable access rights business language.

Unified view of access rights

Access rights full spectrum—its business meaning, its technical connections, related owners, dynamic rules and more

In addition, PlainID solutions display all users who have access rights and from where, presenting the actual influence and full impact of any change in definitions.

Second Tier of Cyber Security

After all the locks are in place, a first-class alarm is installed and all surveillance cameras are on full watch … but are your assets fully protected?

No. There should always be a second tier of security.

As cyber security experts, we always assume there could be a breach. We use every option we can – firewalls, antivirus, APT solutions, forensic products, and more – to prevent and detect unauthorized access. The perimeter is secured, but we tend to neglect security inside the enterprise. PlainID provides tighter control over access rights, enhancing the second tier of cyber security protection. With PlainID, users have the authorization they need when they need them, and user authorization are automatically revoked when no longer relevant.

PlainID's unified view also provides valuable knowledge about who can access what and what can be accessed by whom.

PlainID Key Benefits

- ✓ **Business oriented authorization management**
- ✓ **Dynamic, real time authorization**
- ✓ **Self-service for authorization**
- ✓ **Unified view of authorizations**
- ✓ **Built-in integration to leading IAM products**
- ✓ **Scheduled, graded authorization deployment**
- ✓ **User friendly with easy to use interface**

PlainID Dynamic Authorization Provider (DAP)

Access rights anywhere

Adaptive, flexible and available: PlainID AR-Hub enables SaaS based, native apps, IOT based to receive access rights, based on known, leading standards, fast and securely. PlainID AR-Hub eliminates the need to duplicate and maintain more repositories. Access rights that are defined and maintained within the enterprise are easily available outside the enterprise, according to classification definitions.

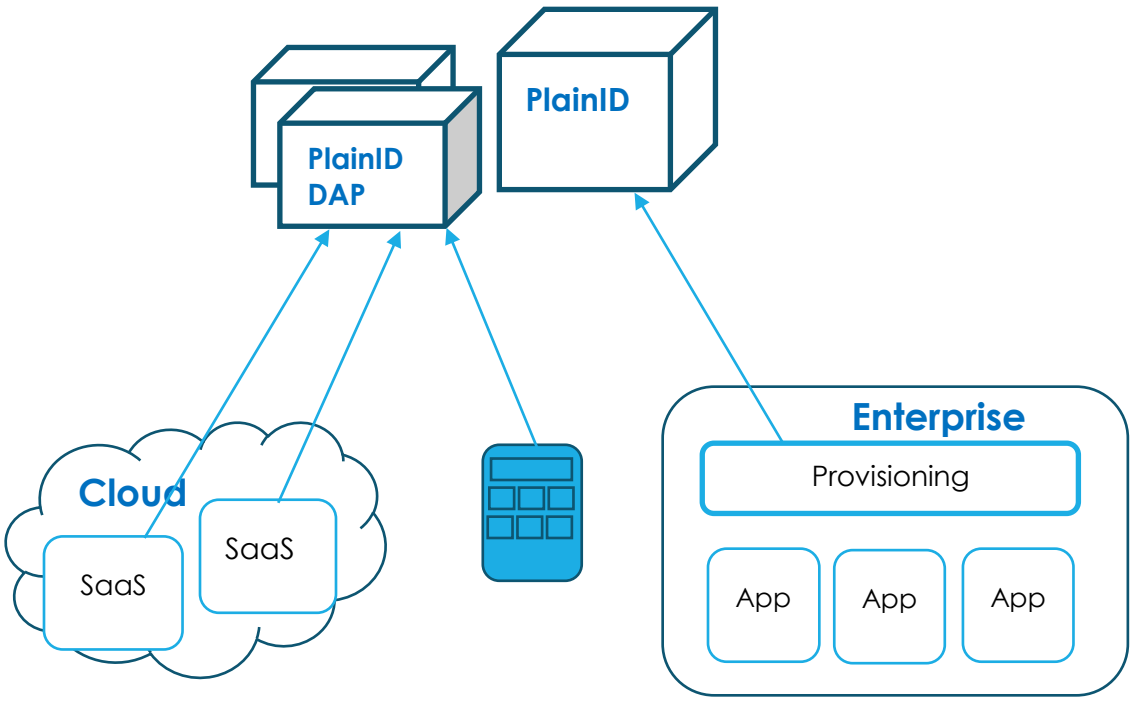
Flexible availability

Real-time filter adds a second layer of flexibility and controls continuous dynamic requirements of each and every enterprise. From where (location and device), to what (app), and any other real-time or predefined attribute, considered in the access token equation.

PlainID Access Token, based on leading standards (OAuth 2.0, SAML, and XACML), and provides the SaaS in the cloud, mobile device, and publishing platform all relevant data needed about user access rights.

PlainID DAP at-a-glance

PlainID AR-Hub, provides access rights anywhere, supporting leading standards. PlainID DAP enables easy and graded adoption to cloud based solutions, native apps and publishing platform, saving the need to replicate repositories and develop adapted solutions.



PlainID for Identity Management

Simplifying Identity Management

Identity management (IDM) has many benefits and enterprises recognize the need. Many businesses already implement IDM, even though IDM is a tedious, expensive, resource-demanding, long-term project.

Can IDM be easier? Simpler?

Yes, it can. PlainID for IDM streamlines identity management.

PlainID for IDM makes IDM easier, quicker, and more efficient. Further, it reduces overall resource consumption during implementation and ongoing operations. PlainID for IDM enables the enterprise to focus on its business authorizations, eliminating handling many, small, highly technical details.

PlainID for IDM at-a-glance

PlainID maximizes IDM product capabilities and minimizes the overall implementation duration. PlainID makes authorization management much more efficient and reduces significantly the overall IDM costs.

Optimizing dynamic authorization

"All HR department employees should have access to HR ERP module and all department managers should have access to employee assessment application."

Can dynamic rules be easily defined?

Yes! With the product's strong and flexible rule engine, it's simple. Just specify **who**, in any way you can (organizational structure, title, employee eye color ☺ or other specs) and define **what** in your business (not technical) language. PlainID gets the job done. Whenever a new user is defined or user attributes are changed, the dynamic authorization are changed accordingly.

Integrated self-service

Authorization can also be requested in an intuitive self-service interface, after the approval process, the user is automatically granted for his request.

Advanced permission deployment

Organizations need the ability to control when a new app is delivered to their users. Providing new authorization to several thousand users, or more, is not always a one-click operation. It often requires early preparations by the technical team and onsite supervision.

Scheduled, graded authorization deployment—is it possible?

Yes. With PlainID for IDM, it's possible. Define **when** and **what**, in your business language, and PlainID will make it happen. Implementing and distributing systems in the enterprise, becomes easier with the ability to schedule permission changes.

Contact Details: Email: info@plainid.com • Visit us at: www.plainid.com