Partner Experience Is the New Customer Experience

Opportunities and challenges of Partner Identity & Access Management: key insights from the expert roundtable hosted by iC Consult and PlainID

In the focus of the discussion:

- What can modern Partner Identity & Access Management achieve?
- What is the difference between CIAM and Partner Identity & Access Management?
- For which industries is Partner Identity & Access Management particularly relevant?
- What are the requirements of the roundtable participants?
- Is authentication taking place – and can multi-factor authentication (MFA) be enforced?
- How important is the user experience?

Whether in wholesale and retail, in finance or in the technology, partner landscapes and ecosystems of companies around the world are becoming increasingly confusing. Unsurprisingly, managing the identities and accesses of external partner companies is also becoming increasingly complex.

Dedicated, professional solutions for Partner Identity & Access Management (Partner IAM) are currently still thin on the ground. But it is already becoming clear that companies' existing IAM and CIAM platforms will sooner or later reach their limits in this demanding and critical environment.

With a view to the opportunities and challenges in the young growth market for Partner IAM, iC Consult and the vendor PlainID hosted renowned enterprise customers for a virtual roundtable in February 2022. Pascal Jacober, Sales Director Europe at PlainID, Måns Håkansson, IAM Solution Architect at PlainID, and Andre Priebe, CTO of iC Consult Group, discussed customers' experiences in implementing customized Partner IAM environments. Together, the roundtable explored concrete requirements and future possibilities of the technology.

Here, we have summarized the most important questions that were raised in the one-hour discussion.

1. What can modern Partner IAM solutions achieve?

The participants agreed: Most companies have made great strides in managing employee and customer identities. Many of the challenges of earlier years – for example, with regard to identity governance & administration, privileged account management, or authentication – have largely been solved now. However, all these solutions focus on the identities of individual users.

In B2B and partner business, on the other hand, it is independent entities and organizations that need to be connected. This brings completely different challenges, for example with regard to the reliable authorization of access across a wide range of roles.

Classic IAM and CIAM solutions, according to roundtable participants, are not designed for this task and, accordingly, usually cannot cope. With its SaaS solution Partner Manager, the specialist provider PlainID offers a dedicated platform for securely connecting external companies with far-reaching access rights – a solution that plays a key role in more and more scenarios.

2. What is the difference between CIAM and Partner IAM?

CIAM usually focuses on the individual customer. Partner IAM, a purely B2B technology, handles the onboarding and authorization of external partner companies.

Because enterprises includes multiple users and user groups, the solutions start one level "higher" than CIAM and focus on authorizing and managing the partner's already-authenticated users according to task and group.

Each partner company is unique, so Partner IAM solutions usually have a high degree of customization – even including dedicated feature sets and interfaces for different user groups.

3. For which industries is Partner IAM particularly relevant?

From the very start, when the participants introduced themselves, it became apparent that Partner IAM is relevant for a wide range of industries. The customers hailed from leading large companies in many different sectors, including wholesale, retail, finance, and telecommunications. What all of them have in common is that they maintain global partner ecosystems and rely on the close integration of these partners.

4. How can consistent and reliable authentication be ensured in such broad ecosystems?

The authentication of participants plays a central role in managing partner identities and partner access. However, the participants pointed out that it is almost impossible to mandate how authentication and verification of identities should take place.

A participant from the retail sector summed it up nicely: As a wholesaler, you have little leverage to prescribe an identity solution to the hundreds of retailers you work with – these retailers buy from a large number of wholesale partners and therefore want to choose which tools to use.

The moderators shared this assessment. This is also why PlainID does not address the topic of authentication itself, but only provides flexible interfaces for connecting leading identity providers such as Okta, Auth0, or SailPoint. This way, PlainID can focus on its core competencies in the area of authorization, and the customer can usually keep using their existing IAM or CIAM solution.

5. Today, many IAM and CIAM solutions offer multi-factor authentication (MFA) as standard. Do Partner IAM solutions like PlainID also support MFA?

The topic of MFA came up again and again during the roundtable – both with regard to the higher level of security that the procedure offers, and with a view to the higher-quality user experience when logging in and when restoring blocked accounts.

However, since authentication is not an integral part of Partner IAM, but is realized via interfaces to external identity providers, pure Partner IAM providers find it difficult to enforce corresponding policies from their side.

6. What do the participants require in terms of Partner IAM?

Several participants emphasized how multi-layered the identities are within their partner ecosystems. It is not uncommon for a user to be maintained as a partner as well as a customer and a supplier. And, even within one user type, multi-layer accounts are not uncommon – for example in the financial sector, where many users have different customer roles (e.g. credit card customer, current account customer, and stock customer). This requires a particularly high degree of flexibility from the IAM partner in terms of managing the access rights and the account lifecycle. Take the case of a user who is maintained as a customer and as an employee, but then changes employers. The customer account must remain accessible – but, of course, with the appropriate access rights.

Roundtable participants also emphasized another key requirement: State-of-the-art Partner IAM must be able to be integrated deeply and flexibly into existing environments – interlocking with the existing IAM environment and connecting multiple identity providers. This can best be ensured by using binding industry standards such as SAML and OpenID – this way, external third-party providers can be easily and reliably integrated into the solution.

A third demand was also voiced several times: When connecting external partners in the B2B environment, it is often necessary to authorize a wide variety of roles, from the employee at the point of sale, to the engineers and developers, to the front-end teams. Since each of these specialist roles need their own toolset, the acceptance of the Partner IAM solution is much higher if an individualized interface and an individualized approach are offered.

7. How important is a high-quality user experience in Partner IAM?

Here, too, the participants agreed: Similar to the handling of customer identities, a high-quality user experience is a central success factor. Or vice-versa: If the experience is perceived as complex, slow, and unintuitive, the business relationship is immediately in danger. After all, everyone works with multiple providers – and can switch at any time.

With a view to maximum user comfort, the participants mentioned that a convenient log-in is particularly important. MFA with the option of biometric authentication is mentioned as state-of-the-art. However, with an explicit restriction: The procedure has not yet reached the level of maturity that would be required for use at the point of sale, for example. After all, authentication in this scenario must function smoothly across all devices and platforms – and that is not yet possible today.

To further optimize the comfort and security of the Partner IAM solution, in the opinion of the discussion participants, identities and accesses need to be increasingly managed with a process- and context-based approach: If the user's location or device are also taken into account when assigning access rights, security and experience can be optimally balanced.

Conclusion: Challenging and rewarding projects

When the roundtable ended after just over an hour, the participants agreed: This fruitful and stimulating discussion had provided valuable insights into the opportunities and challenges of modern Partner IAM services. With a view to the required depth of integration and the critical protection of sensitive data, it is obvious that such projects will be demanding. Companies are well-advised to involve system integrators with many years of IAM experience – early on, in both the selection and the implementation of solutions. This approach sets the course for a successful project from day one, and lays a strong foundation for long-term partner relationships.

About PlainID

PlainID was founded in 2014 by a team of experienced security technologists determined to put an end to the challenges that businesses face when scaling up their IAM capabilities. The solution led to a completely new design that reduces all enterprise authorizations to a single point of view – making Authorization plain and simple for business owners to manage and control.

About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

More information at www.ic-consult.com