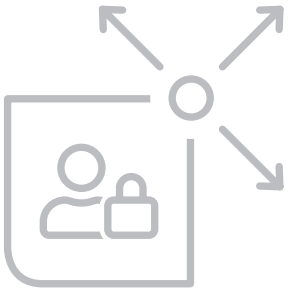
From Zero to Hero: CIAM – Balancing Data Security and Customer Experience



A virtual roundtable with enterprise customers explored the challenges and potential of holistic Identity and Access Management platforms.

Focus of discussion:

- How to differentiate between IAM and CIAM
- The opportunities and challenges of CIAM
- Hub-and-spoke for enterprise environments
- Integration of existing IAM solutions
- Governance and data protection

The digitalization of personal and professional life is advancing rapidly. Around the world, and across nearly all industries, people now work digitally and remotely, shop online, and communicate, consume, and collaborate via the Web. Last year, most companies took the first wave of ad-hoc digitalization in stride – even if the changeover often required an enormous effort behind the scenes. But now the challenge is to transition the systems that were implemented or scaled up under time pressure into stable, secure, and compliant operations – a considerable challenge, especially in terms of secure user registration, authentication, and authorization. What's more, platform operators face a high risk of cyber attacks.

In light of this, iC Consult hosted a virtual IAM Excellence Talk in February 2021, titled "From Zero to Hero: CIAM – Balancing Data Security and Customer Experience", inviting global enterprise customers to an open exchange of opinions and experiences. Also at the table: the Identity Management experts from vendor partner Okta. Solution Engineering Manager Goetz Walecki moderated the discussion, shared best practices from worldwide projects, and gave participants advice for implementing CIAM in distributed environments.

During the hour-long discussion, participants focused on seven key issues and worked with Okta and iC Consult to develop initial solution concepts based on best practices.

How to differentiate between IAM and CIAM

1. We have already implemented Identity Access Management (IAM) for our workforce. Customer Identity and Access Management (CIAM) will be added as a new topic in the course of digitalization. How can the two projects be differentiated?

Participants were unanimous that while IAM and CIAM generally share similar goals – authenticating users in a secure, user-friendly, and governance-compliant manner – they have significant differences in practice. The most important differences:

- **Onboarding** internal employees follows very different process specifications than, say, onboarding customers to an online store.
- In an employee solution, the **user data** is usually located in a dedicated, central directory (most often: Microsoft Active Directory). In a CIAM solution, user data is often located in CRM and sales databases, on the servers of external third parties (Apple ID), or must first be queried online.
- As **authentication tools**, participants today rely on strong multifactor authentication in their workforce IAMs. In the CIAM environment, social authentication solutions are rapidly gaining importance for this purpose.
- The **underlying infrastructure** of IAM and CIAM also differs – while the former are mostly based on HR systems and user databases, classic CIAM solutions, according to participants, are usually portal solutions.

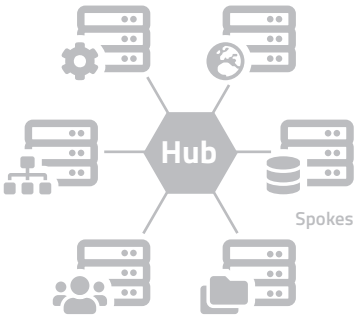
In general, participants handle IAM and CIAM as separate projects with different value drivers and challenges.

The opportunities and challenges of CIAM

2. Participants state that their CIAM is currently in its infancy for them and is perceived as costlier than IAM. Where does this impression come from?

One participant summed it up: Workforce IAM solutions are typically designed for a few tens of thousands of users at most, while CIAM solutions often need to securely authenticate millions of consumers in a compliant manner. In addition, the type of access, the origin of the user data, and the preferred authentication tools vary considerably, and are increasingly difficult for the IT department to control. Add to this the potential risk of governance breaches and the high usability requirements, and it is clear why CIAM projects are often seen as an enormous challenge.

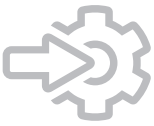
However, other roundtable participants pointed out that CIAM has significantly lower hurdles in several areas: There are generally fewer applications to integrate and fewer roles to manage than with workforce IAM solutions. This means that CIAM is certainly suitable as an entry point into some exciting subject areas – authorization projects, for example.



Hub-and-spoke for enterprise environments

3. In corporate groups with many divisions and international branches, IAM and CIAM projects pose particular challenges. Can such structures be covered with a uniform solution?

Participants who have experience with Okta's hub-and-spoke architecture confirmed: Yes, it works. In this model, the central office (the "hub") specifies which applications are to be included in the authentication solution. The geographically or organizationally remote divisions (the "spokes") then decide autonomously how to make these applications available, and to whom. This approach guarantees a high degree of flexibility in day-to-day operations, according to the participants, and is thus very suitable even for large enterprise environments.



Integration of existing IAM solutions

4. What companies can benefit from tackling CIAM?

Considering the speed at which virtualization is advancing, CIAM is evolving from "nice-to-have" to "must-have". The participants agreed that such a solution will become even more important in the future in terms of governance, security, and data protection. They described the added value of CIAM as particularly high if the solution can be integrated into existing marketing, CRM, and sales databases. However, with a large number of users, this requires comprehensive automation – so the maturity of the implementation must be comparatively high.

5. Is it a good idea to consolidate IAM and CIAM?

The roundtable participants tend to approach IAM and CIAM as separate projects. Currently, most are focused on driving the maturity of their IAM environments and, as a first step, exposing their employees to the benefits of these solutions. Many participants see themselves in the early stages of projects (maturity level 1-2). Several participants explicitly described their CIAM as "still in its infancy". However, the participants all see the potential of the technology, especially with regard to social authentication via third-party providers like Apple ID. The tenor of the discussion was that this could develop into a real growth driver, since many customers already favor single sign-on (SSO) and passwordless models, and perceive them as a noticeable added value.

6. Can legacy solutions be integrated into company-wide IAM or CIAM initiatives?

According to the panel, only very few IAM or CIAM projects today truly start from scratch. Nearly all companies already have experience in this area, and most also have legacy systems in place. Companies who decide to implement an enterprise-wide Identity and Access Management solution usually want to:

- Integrate their legacy systems
- Centralize Identity Management
- Strengthen compliance and governance
- Bring the processes together

Governance and data protection

At this point, particpants with hub-and-spoke experience (see above) emphasized that such tight integration is entirely feasible with Okta. Okta solutions can always be implemented as a sovereign system on the backend, to bring upstream legacy systems together in one platform and coordinate them (unnoticed by the user). In such an environment, companies can also transfer legacy applications to the new backend system as part of a smooth migration.

7. What about governance, specifically data protection, in such a hub-and-spoke environment?

In view of the increasingly strict data protection requirements in the EU and Switzerland, the topic of privacy came up again and again. Moderator Goetz Walecki confirmed the high priority and recommended that user data, usually stored in an existing directory environment, should ideally remain physically and logically in the respective country throughout. This especially applies to the associated passwords. Okta's solution therefore only accesses existing master data, basic user objects, and policy integrations, and leaves all extended attributes and passwords in the original location. As a result, companies can be sure that they are operating firmly within the respective legal framework, even when handling sensitive customer data.

The conclusion of the sixty-minute roundtable was unanimous: IAM and CIAM already offer enterprise customers many opportunities to sustainably optimize their processes and relieve the burden on customers, employees, and IT teams alike. Innovative approaches such as Okta's hub-and-spoke architecture enable those responsible to set the course for the future without compromising on security or compliance. Nevertheless, IAM and CIAM are usually challenging and far-reaching integration projects. Customers are well advised to call in experienced integrators such as iC Consult and the vendors' experts to support the internal team with tailored consulting, implementation, and integration services – and thus help to ensure a successful project.