AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

The customer journey leads to the cloud

IAM as a Service



See also our videos:
airlock.com/fixfertig

Table of contents

1.	**cIAM optimizes and protects the customer journey**	**3**
2.	**Why cIAM requirements are changing**	**4**
3.	**Why cIAM implementation or modernization often fails**	**7**
4.	**Why operation and further development overwhelm companies**	**10**
5.	**Cloud or On-Prem: finding the right operating model**	**11**
5.1	Benefits of Airlock cIAM on-prem	11
5.2	Benefits of Airlock IAM as a Service	11
5.3.	Addressing concerns about SaaS	15
5.4	IAM as a Service from Europe	15
6.	**Rethinking cIAM: Why "as a Service" is gaining importance**	**16**
Appendix I:	**Checklist: What to look for when choosing a cIAM solution**	**17**
Appendix II:	**Who benefits from cIAM**	**19**
Appendix III:	**Glossary and abbreviations**	**22**
Appendix IV:	**Further Information**	**25**

1. cIAM optimizes and protects the customer journey

When customers interact online with a company, organization, or government agency[1], two aspects take center stage: security and user experience.

First and foremost, the user's identity must be clearly established—without identity verification, there is no security, no traceability, no customer relationship, no compliance, and no business. The goal here is to reliably prevent abuse and attacks. This is because the IT world has created new entry points for attackers: from identity theft via phishing or social engineering to attacks on the provider's IT systems, such as through ransomware (forcibly encrypted data), the exploitation of vulnerabilities in applications, or targeted server overload (Distributed Denial of Service, DDoS).

As fundamental as the security of online transactions is from a business perspective, from the user's perspective it is always only a secondary priority: consumers want, above all, to reach their destination quickly and conveniently. They demand easy-to-use, seamless, and personalized online access to services, via both web browsers and mobile apps. Verifying identity must be accomplished with as little effort as possible. Otherwise, users quickly become frustrated and vent their anger to the help desk or on social media (or, in the case of online retail, even switch providers).

That is why Customer Identity and Access Management (cIAM) is an essential component of customer relationships.

This white paper explains why companies need to reevaluate their cIAM today. It describes the most significant changes in the market, highlights typical causes of failed or overwhelming cIAM initiatives, and demonstrates why the choice between on-premises and as-a-service solutions is becoming increasingly important for many organizations.

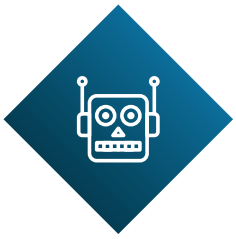


cIAM is the identity verification and security checkpoint at the airport of the customer journey. Companies that can implement these functions in a customer-friendly, reliable, highly secure and with proven compliance, guarantee their customers a smooth, convenient start to their individual journey toward the desired products and services. cIAM accelerates and protects access to the runway of the customer journey.

1 In the following, the term "company" is used, but this also refers to government agencies and other organizations with online customer relationships.

2. Why cIAM requirements are changing

Whether it's initial registration as a new customer or logging in as an existing customer: Authentication always marks the beginning of a user's (business) relationship with a company. This critical first step, mapped within a cIAM system, is therefore crucial for customer satisfaction and, as is often the case, for the success of the interaction in general. This makes it all the more critical that the requirements for authentication—and thus for the cIAM solution—are currently undergoing a drastic, multifaceted transformation. This is because new requirements for cIAM from the user side, new technologies, new security risks, and new regulations are emerging at an ever-increasing pace.



One current development concerns the area of **non-human identities** (NHIs, i.e., digital or machine identities): End users increasingly prefer to delegate tasks to their AI agents—that is, AI bots that can independently initiate actions such as placing orders or making hotel reservations. This raises the question: How should AI agents authenticate themselves to online ordering systems and booking platforms? The cIAM system must therefore be prepared for the integration of NHIs. This is achieved using API keys (API: Application Programming Interface) and tokens (digital credentials). Since identities often originate from numerous identity providers, it is also necessary to securely consolidate the identity credentials via a so-called token exchange to protect systems from misuse.[2]



At the same time, the IT industry has been preparing for some time for the so-called **"Q-Day"**—that is, the day in the perhaps not-so-distant future when quantum computers will be powerful enough to crack today's encryption. This necessitates the use of quantum-resistant encryption algorithms (Post-Quantum Cryptography, or PQC for short). The risk: Attackers could exfiltrate data today in order to decrypt it in a few years with little effort. The key here is to take countermeasures in a timely manner by switching to PQC algorithms.

2 The Airlock white paper "Do You Speak Token?" deals with the principle of token exchange in detail.



An equally dramatic—but more urgent in terms of timing—upheaval is looming for the market with the concept of Self-Sovereign Identity (SSI). SSI is intended to place control over digital identity in the hands of users themselves. Corresponding initiatives are underway in Switzerland with **E-ID** and in the EU under the name **EUDI** (see box). SSI represents a fundamental change in the architecture of identity verification. Companies must be prepared for this. A modern, adaptable cIAM system enables such changes to be implemented and new features or apps to be introduced with a short time-to-market.

What do SSI, EUDI, and E-ID mean for businesses?

Until now, control over digital identities has rested with identity providers (IdPs), including Microsoft, Amazon, and Google. Self-Sovereign Identity (SSI) shifts control over identities from IdPs to the users themselves. This architecture is known as E-ID in Switzerland and EUDI in the European Union. It is based on a decentralized identity model that gives users complete and granular control over their personal data. There is no central authority that aggregates, stores, or controls credentials.

Instead, the user stores all their digital credentials—passport, driver's license, etc.—in their digital wallet, which is installed on their smartphone. With this app, they can, for example, provide proof of age when purchasing alcohol (transmitting only the age information digitally), open bank accounts, sign contracts, or order official documents online. SSI will thus significantly simplify online transactions. The plan is to link this to additional forms of identification in the future: insurance cards, driver's licenses, loyalty cards, etc. SSI is scheduled to launch in 2026.

Therefore, the finance and insurance sectors, retail, healthcare sector, the public sector, and other industries must prepare for SSI support.[3]



Other regulations such as the GDPR, NIS 2, DORA, PSD2/3, etc., also continuously influence the handling of digital identities and thus IAM and cIAM systems. Legislative changes require ongoing adjustments and updates in cIAM operations. For example, the EU is currently discussing, under the heading "Digital Omnibus," how it can harmonize and streamline its digital legislation. Consequently, numerous updated regulations will likely soon affect all companies doing business in the EU—and these changes will certainly not be the last.

3 Everything you need to know on this topic can be found in the Airlock white paper "The (R)Evolution of Digital Identity."



Furthermore, in the field of **authentication,** new hacking attacks are constantly emerging that undermine previously secure methods of strong authentication and require new defense technologies. It is essential to stay up to date and meet the latest security requirements—including the rollout of modern authentication methods—as quickly as possible.[4]



Last but not least, **technological advancements** such as decentralization via the cloud and Kubernetes container technology also play a major role. Many different identity providers with decentralized access to decentralized services make managing identities and access control more complex—and thus more difficult to implement.

Since cIAM is crucial for a secure and seamless customer journey, this complexity can quickly lead to the entire project crashing and burning. That is why an approach is needed that is not only functionally sound but also remains manageable in implementation.



Several factors are driving a flurry of innovation in the cIAM market, including a customer base that—quite rightly—expects an intuitive, elegant user experience similar to that of major cloud platforms. Increasingly AI-driven attacks on user identities, a new generation of encryption technology, and the impending (r)evolution of identity verification architecture via SSI are adding to the challenge. It is therefore more urgent than ever to deploy a cIAM system that not only meets the state of the art: it must also be flexible enough to adapt to new developments at short notice and roll out innovative features quickly.

4 See the Airlock white paper "The Pieces of the Modern Authentication Puzzle."

3. 3. Why cIAM implementation or -modernization often fail

Many companies have recognized the urgency of the situation and are planning to switch to a new, modern cIAM solution. The problem: roughly one in two cIAM projects fails. Why is that?

In cIAM projects, the following eight aspects in particular repeatedly cause turbulence:



The required interaction of numerous systems and identity providers creates a high degree of **complexity,** especially in industries where numerous backend systems need to be integrated. This increases the duration, error-prone nature, and costs of a cIAM project, for example when complex API integrations must be managed.



As a rule, **numerous stakeholders** (see Appendix II) from IT, marketing, compliance, and other departments are involved. A successful cIAM project requires comprehensive coordination and support from all parties involved, especially from senior management (management buy-in). Coordination issues often arise because senior management and line departments speak a different language than the IT and security teams. This makes it difficult to achieve a common direction for the project.



A lack of understanding of user requirements and preferences sometimes results in a cIAM system failing to meet **user-friendliness** expectations. Low usage can then quickly lead to missed revenue opportunities and dissatisfied customers.



Companies often lack in-house expertise. This is because cIAM is highly complex, highly specialized—and never the core business of the client company. Building in-house cIAM expertise is therefore not worthwhile for many companies. Virtually all industries are suffering from an acute **shortage of personnel.** Consequently, it is difficult to find IT professionals with the necessary cIAM expertise—and if they are available at all, only at very high salaries.



As with all IT projects, limited **budgets**—particularly for upfront investments—remain a major hurdle in the cIAM environment, at least until significant financial damage has been caused by identity-related attacks.



Criminals and state-sponsored attack groups are constantly developing new techniques, tools, and methods to compromise and misuse user identities. Companies are often overwhelmed by the need to keep pace with ever-changing attack vectors and **security requirements.** cIAM projects therefore sometimes fail because a company is unable to maintain a robust, long-term security posture for its cIAM environment. Sooner or later, identities and applications are then inadequately protected against misuse, which in turn leads to costly and time-consuming security projects—and in the worst-case scenario, even results in fines for violations of data protection laws and the GDPR.



Due to the aforementioned dynamics in **the regulatory environment,** it is necessary to stay on top of relevant laws, regulations, and initiatives and to map them within the cIAM system. Many companies are overwhelmed by these ongoing updates and the operational costs associated with compliance.



Another common mistake is attempting to expand an existing **enterprise IAM** into a cIAM system. This is doomed to fail for several reasons, including:

1. The range of functions in a cIAM system is considerably broader than what is typical in enterprise IAM. For example, an employer might mandate that all external access must occur from a company laptop using multi-factor authentication (MFA) via a security token. Customer relationships can only tolerate such requirements to a very limited extent. A cIAM solution must therefore be much more flexible. This makes risk-based authentication (which requires additional authentication steps depending on the detected risk level) and adaptive authentication (which selects the appropriate MFA option based on the criticality of the intended action) all the more important. The selection of the most secure possible MFA variant is made in accordance with the industry standard FIDO 2 (Fast Identity Online 2).
2. In enterprises, Active Directory (when used in conjunction with a cloud directory such as Azure AD) typically serves as the central identity provider in conjunction with a cloud directory such as Azure AD) serves as the central identity provider. In customer relationships, however, dependencies are much more complex. For instance, the popular "social login" (signing in via Google or Facebook ID) alone requires support for numerous IdPs.

3. cIAM solutions must integrate seamlessly with backend applications such as CRM systems or industry-specific applications like banking apps.

Companies with small and/or overburdened IT teams and a lack of cIAM expertise will sooner or later run into serious trouble. Since cIAM is smooth, secure customer journey, this can quickly lead to a crash landing of the customer journey that has just begun. That is why an alternative to locally operated cIAM is needed—and certainly to misused enterprise IAM.



4. Why operation and further development overwhelm companies

Even if the project and implementation are successful, the task is not complete. A modern cIAM must not only be implemented but also kept up-to-date, secure, and available at all times. This is precisely where another major challenge lies for many companies.

Project planning must therefore not focus solely on the deployment of a cIAM system. From the very beginning, it must take into account that cIAM requires ongoing updates and that operations must ensure high availability and scalability. Companies must stay on top of this at all times—whether due to new laws and regulations, new identity-based attacks, or new requirements and expectations from end users.

These constant changes sometimes require new features, sometimes updated processes, or technical adjustments during ongoing operations. However, companies whose cIAM no longer meets today's requirements must not put off these updates out of fear of high complexity. Otherwise, they risk compliance violations, security risks, dissatisfied customers, lost revenue, and unexpected project costs.

For companies without a large IT team and their own cIAM specialists, this ongoing operation becomes a particular burden. High availability, scalability, security updates, regulatory adjustments, and the continuous development of the solution create a constant workload. As a result, not only the implementation but also the operation itself becomes a strategic and organizational challenge.

This is precisely why a service-based deployment model is coming into focus. After all, many companies are not just looking for a high-performance cIAM solution, but above all for a way to significantly reduce the effort required for operation, updates, and further development.

5. Cloud or On-Prem: Finding the Right Operating Model

Today, a modern cIAM system must do far more than just provide secure logins. It must meet high standards for user-friendliness, security, compliance, and flexibility—while also being able to adapt continuously to new conditions. This is precisely why many companies are faced not only with the question of the right cIAM solution, but also with that of the appropriate operating model.

Operating a cIAM system is the right first step toward greater customer focus, security, compliance, and flexibility. But this path is usually open only to companies with sufficiently experienced staff. Many companies pursue a cloud strategy but want to position themselves in terms of cIAM in a way that is leaner in terms of organization and personnel, yet equally future-proof. For them, procuring cIAM as a service may be the better alternative.

IAM as a Service is no less exciting for anyone whose existing cIAM solutions do not meet future requirements. In other words: Anyone facing the decision to replace their local cIAM system due to post-quantum computing, SSI, or the need for flexible support of MFA methods and passkeys should also consider the as-a-service option. In doing so, it is important to weigh the pros and cons of the on-premises versus the cloud variant.

5.1 Advantages of Airlock cIAM on-prem

On-premises operation of a dedicated, highly secure cIAM system like Airlock offers a number of advantages, including the following in particular:

- The company's IT team retains **full, sole control** over the systems, security, and compliance.
- Airlock IAM on-prem can be flexibly tailored to meet individual business requirements.
- Nothing stands in the way of **integrating third-party systems**—including legacy applications—via APIs.
- **Data and identities** remain **under the company's control.** On-premise versions are therefore frequently used for highly confidential applications and data, such as core banking.

5.2 Advantages of Airlock IAM as a Service

Many of the benefits of an on-premise deployment also apply to the cloud version: Airlock IAM as a Service likewise offers a high degree of control over security and compliance, but by design, not over the hardware or its operation. Airlock IAM as a Service can also be customized and adapted to the brand's look and feel. Airlock IAM as a Service can also be easily integrated with third-party systems. In addition, the service offers a number of specific advantages:

- **Shorter time-to-value:** Of course, cIAM-as-a-Service projects also require thorough planning and appropriate lead time. However, with Airlock IAM as a Service, there is no need to calculate hardware requirements or procure expensive hardware, nor is there the planning and organizational effort, costs, and pitfalls associated with on-premises IT projects. The customer company thus gains access to a modern and flexibly customizable cIAM system much faster, more cost-effectively, and with fewer complications, as the service is set up, deployed, and operated by the manufacturer.

- **Less effort:** The effort required is reduced not only during setup but also during the ongoing operation of the cIAM system. This is because the operation and maintenance of hardware and software are handled by experts from Airlock, whose core business is knowing the cIAM field and the cIAM system itself inside and out. This allows the company's IT team to focus on other business-critical tasks.

- **Automatic updates and improvements:** A SaaS offering (Software as a Service) operated by the software vendor itself always receives the latest updates, features, and functional enhancements automatically. This saves the user company the effort of testing and implementation while still ensuring it always has the latest software version with the most up-to-date feature set. Since Airlock develops and operates the IAM as a Service solution itself, SaaS user companies always have a certain time advantage over the on-premise version.

- **Compliance:** With Airlock IAM as a Service, users can rest assured that legal requirements such as data protection laws or the GDPR are correctly implemented. This makes it correspondingly easier and less bureaucratic to demonstrate compliance during audits. This is ensured by documented data protection processes and audit reports. Airlock's ISO 27001 certification, in turn, verifies the implementation of an Information Security Management System (ISMS) as required by NIS 2, for example. Through these measures, Airlock IAM as a Service minimizes both the time and costs associated with audits.

- **Staffing needs:** Security and identity management specialists are hard to find in the tight skilled labor market—especially since a user company competes here with well-funded corporations and managed security service providers (MSSPs). By moving cIAM to the cloud, the need for IT, security, and cIAM specialists decreases. This eliminates the time and organizational effort required to recruit specialists and reduces ongoing personnel costs for highly paid experts.

- **Scalability:** As is typical for the cloud, cIAM as a Service scales dynamically with requirements without user companies having to deal with hardware procurement. The company's IT team therefore does not have to concern itself with questions such as how the cIAM system must be initially sized to meet current and, if possible, future requirements. Nor does it have to carry out time-consuming projects to scale the cIAM system in order to keep pace with growing requirements.

- **High availability and disaster recovery:** A cIAM system must be designed for high availability. After all, a system failure means that no online customer interactions are possible during that period—time is literally money here. It also risks dissatisfied customers and damage to the company's reputation. For the same reasons, restarting the cIAM system after an emergency must also occur as quickly as possible. However, high availability requires redundancy and is therefore expensive, while a rapid restart requires automated processes. Airlock IAM as a Service offers high availability and integrated mechanisms for rapid recovery of the environment following a crisis. This covers two core requirements for cIAM systems without any effort on the part of the user company—and minimizes the window of opportunity for revenue losses and reputational damage.

- **Cost advantages:** Airlock IAM as a Service excels in terms of total cost of ownership (TCO). This is because one factor is often overlooked: Annual costs result from the pro-rated sum of implementation, customization, and training costs over the system's lifespan, supplemented by annual costs for software subscriptions, ongoing operations, and support. Personnel and updates often account for 50 to 80 percent of total costs. Airlock IAM as a Service offers advantages not least because, instead of initial investments in hardware and software licenses, only ongoing subscription fees are incurred—operating expenses (Opex) rather than capital expenditures (Capex). Thanks to volume-based MAU (Monthly Active Users) billing, the cost structure always corresponds to actual usage. And with automatic updates, this cost component is completely eliminated for the user company.

- **Operation by professionals:** Every major IT system has its quirks and therefore requires experts who know the system in detail to ensure smooth operation. With on-premise solutions, this entails a high initial and ongoing workload and training requirements for operations staff. But at Airlock, cIAM is our core business. The operation, security, and maintenance of Airlock IAM as a Service are handled by proven specialists from the DevSecOps team who created the system, in line with the motto: *"We build it, we run it."*

- **Partner network:** Depending on the industry, company history, and business focus, implementing cIAM can involve a whole range of specific requirements. That is why it is important for cIAM projects—whether on-premises or in the cloud—to work with a partner who is well-versed in the respective industry and can assist in customizing the cIAM system. Airlock has a proven network of integration partners with broad industry expertise that can also be leveraged for Airlock IAM as a Servic.

Who IAM as a Service is suitable for

IAM as a Service significantly simplifies the implementation of or transition to a modern, flexibly customizable, and future-proof cIAM. This makes it particularly suitable for companies with a cloud strategy and a need for efficient, secure, scalable, and compliant customer engagement, for example in the following cases:

1. With cIAM as a Service, companies can optimize, update, and better protect their onboarding and login processes to future-proof them in light of the highly dynamic cIAM market.
2. When a company migrates business applications to the cloud, the logical next step is to move cIAM to the cloud as well.
3. cIAM as a Service significantly reduces the effort required to address current and upcoming regulatory challenges, such as e-ID or EUDI.
4. In government agencies that must implement eGovernment initiatives, current technical developments and legal requirements can be easily accommodated using cIAM as a Service.
5. Operating cIAM in the cloud frees up resources for overburdened IT teams that would struggle to manage the implementation, updates, and ongoing operation of an on-premises cIAM environment.
6. cIAM as a Service automatically accounts for technical and regulatory cIAM updates, so the IT team doesn't have to stay constantly on top of these critical specialized topics.
7. cIAM as a Service unlocks the full range of features of a mature cIAM solution even for companies that lack the necessary expertise to implement on-prem cIAM projects quickly and effectively.
8. If a company is looking for an alternative to its existing on-prem cIAM solution that is as powerful as it is future-proof and quick to implement, cIAM as a Service allows it to switch cIAM providers quickly and easily.





Traveling to exotic destinations used to be expensive and dangerous. Modern air travel has made what was once an exclusive pleasure accessible to a much larger clientele and made it both easier and safer. In a similar way, Airlock IAM as a Service opens up sophisticated cIAM technologies and state-of-the-art security to a broader base of companies, while removing the complexity of the undertaking. At the same time, Airlock IAM as a Service enables "last-minute" travel should changes to the planned route be necessary. And once again, the path leads through the clouds.

5.3. Addressing concerns about SaaS

Today, countless companies—from multinational corporations to banks, insurance companies, and government agencies—use cloud services such as Microsoft Azure, AWS, or Google Cloud. Nevertheless, concerns about the public cloud persist in many quarters. This is because moving software to the cloud creates a dependency on cloud providers. At the same time, new questions arise regarding data sovereignty and data protection. The advantages of cIAM as a Service must be weighed against these objections—even if these concerns can generally be addressed.

This makes it all the more important to note that when using Airlock IAM as a Service, the option of a short-term migration out of the cloud (declouding) is always available. This is because the on-premises and cloud versions use the same code base. Declouding would therefore be technically possible within a short time if necessary.

5.4 IAM as a Service from Europe

When it comes to the cloud, many companies prioritize working with a reputable provider based in Europe. Airlock is a brand of the leading Swiss IT company Ergon, headquartered in Zurich. Founded in 1984, Ergon combines expertise in technology, security, and business. With Airlock IAM as a Service, data residency in Europe is guaranteed. Equally important: the software is also developed in Switzerland. This avoids dependencies on non-European software providers.



Airlock IAM as a Service brings the benefits familiar from cloud offerings to cIAM. Airlock's DevSecOps team develops, secures, and maintains the environment itself. This guarantees a smooth flight to the cloud with expert operation and timely updates. Thanks to Airlock's proven network of integration and technology partners, the best possible support is always provided on board. Thanks to a unified code base, the option for a quick return flight is available at any time. Important: The flight is within Europe.

6. Rethinking cIAM: Why “as a Service” is gaining importance

cIAM is undergoing a dramatic transformation: Companies are constantly confronted with new customer demands, new types of attacks (such as deepfakes), new technologies (like PQC), and new regulations that are fundamentally changing authentication and authorization. Companies whose customers access products and services online must therefore prepare for these challenges as soon as possible.

Airlock IAM as a Service offers a powerful and rapidly deployable alternative to on-prem cIAM—and certainly to tinkering with an in-house enterprise IAM solution. After all, cIAM projects fail not because the technology is poor, but because implementation is complex. Airlock IAM as a Service eliminates this complexity. It requires no hardware infrastructure, operational overhead, updates, or project risk on the user’s part: Airlock IAM as a Service runs smoothly from day one. Total cost of ownership is lower than that of on-premises operations, and thanks to MAU billing, ongoing costs are always clearly calculable.

Personal data and metadata remain in Switzerland; security and compliance are guaranteed. Ergon Informatik, the provider behind the Airlock brand, is the leading cIAM specialist in the Swiss financial sector and can thus draw on decades of expertise in this critical sector. In short: Airlock IAM as a Service offers a comprehensive, worry-free package from a renowned European provider.



cIAM is the departure point of the customer journey. If things go wrong here, the trip is already ruined before it has even really begun. To ensure that everything runs smoothly, airports outsource the critical tasks related to passenger access: personal identification and property protection to police authorities, and travel security (baggage screening) to specialized firms. In the same way, IAM as a Service enables critical functions to be outsourced to experts. IAM as a Service makes customer authentication as elegant, seamless, and secure as the processes at a Swiss airport—except that the “online security staff” works invisibly in the background. Everything takes place in the look and feel of the corporate brand; travelers simply see the sign: “This way to your gate.” Even as processes, risks, technologies, and regulations are constantly changing, one thing remains true: IAM as a Service boosts customer loyalty.

Appendix I:
Checklist: What to look for when choosing a cIAM solution

1. Basic functionality and integration:

- ☐ Self-registration, social login, and features for bulk import of user data.
- ☐ User dashboards for managing login credentials, devices, user profiles, and consents.
- ☐ Secure account recovery mechanisms (without security questions).
- ☐ Multi-factor and passwordless authentication, with support for various authentication methods such as mobile apps and biometrics.
- ☐ SDK (Software Development Kit) for developing custom authentication
- ☐ features and integrating the cIAM platform into customer applications.
- ☐ Orchestration of onboarding, authentication, and maintenance workflows, including integration with third-party services.
- ☐ Built-in intelligence for detecting compromised credentials.
- ☐ Authentication policies to map security levels to authentication types for step-up authentication.
- ☐ Risk-adaptive authentication with evaluation of runtime parameters, usage behavior, and threat analyses.
- ☐ Support for all major identity federation standards (e.g., SAML, OAuth, OIDC, JWT).
- ☐ Single sign-on (SSO) for all connected customer resources and brands.
- ☐ APIs and connectors for marketing analytics, CRM systems, and other SaaS applications.
- ☐ Identity verification features and/or integration with third-party identity verification providers.
- ☐ Integration with fraud prevention platforms.
- ☐ Integration with customer-side SIEM and ITSM systems (Security Information and Event Management, IT Service Management).
- ☐ Integrated comprehensive security functionality (WAF, WAAP) for usability and security from a single source.

2. System requirements:

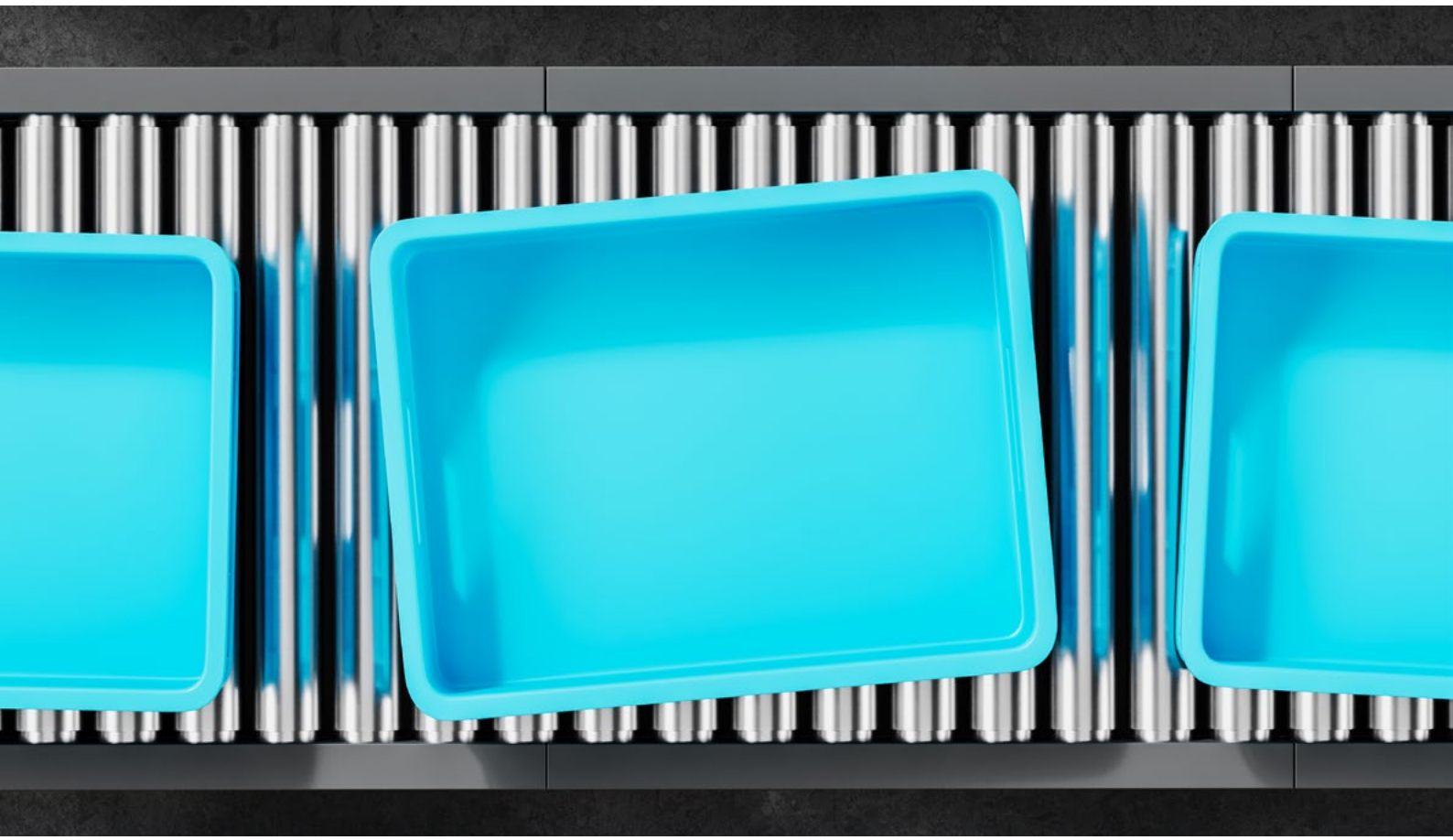
- ☐ Dedicated cIAM system, not a "modified" enterprise IAM.
- ☐ Clear focus on a seamless user experience for elegant customer journeys.
- ☐ Flexible deployment options (SaaS, PaaS/IaaS, hybrid, on-premises).
- ☐ Microservice architecture.
- ☐ High scalability.
- ☐ High availability and resilience.
- ☐ Preparing for the quantum age by integrating hybrid PQC methods.
- ☐ Preparation for SSI architecture (EUDI, E-ID).

3. Operational aspects:

- ☐ Collection and provision of identity analytics.
- ☐ Reports and dashboards for cIAM system metrics.
- ☐ Data localization/residence to comply with data protection regulations.
- ☐ Reports and audit support related to data protection requirements.
- ☐ Option for rapid migration out of the cloud thanks to a unified code base.

4. Vendor selection:

- ☐ Vendors based in Europe to avoid compliance issues and risks.
- ☐ Providers with proven, comprehensive cIAM experience and a European headquarters for support issues and easier compliance verification.
- ☐ Network of integration partners with industry expertise and a local presence.



Appendix II:
Who benefits from cIAM



Business

Customer portals of all kinds benefit from the advantages of an intuitive, secure, and flexibly scalable cIAM system, particularly those with especially high requirements for user experience, integration with third-party systems, scalability, or compliance. This applies in particular to banks, insurance companies, and FinTech firms, the public sector (keyword: eGovernment), the healthcare industry, and, of course, online retail. But cIAM can also bring benefits to large enterprises with numerous locations, both for IAM for a multinational, distributed workforce and for integrating suppliers and sales partners. As a general rule: Cloud strategy + high requirements for managing external access = cIAM is worth it.



Customers

Today's customers are spoiled by the seamless processes they've come to expect from major cloud platforms. They expect a cloud-like customer journey from all other online portals as well: registration and login must be simple, intuitive, fast, reliable, and secure. They also expect multi-channel capability (web, mobile app, and, where applicable, point-of-sale terminals). A bumpy customer onboarding process, in particular, risks damaging a company's reputation (keyword: social media). A user experience (UX) featuring seamless onboarding and convenient login, on the other hand, enables companies to boost conversion rates and increase customer loyalty in the long term.



Support

A seamless user experience not only prevents frustration on the user's part but also reduces costs and staffing requirements for the help desk, service desk, or customer support. This is because modern cIAM solutions replace traditional logins with passwordless authentication using biometrics or passkeys. This eliminates the most common reason for contacting support: forgotten passwords. According to Gartner, 40 percent of all help desk calls are related to expired, changed, or reset passwords. On average, Gartner reports, users forget their passwords 1.8 times per year, resulting in an average cost of 50 euros per incident. Even if costs were merely halved, this would result in savings of 4.5 million euros per year for 100,000 customers. Here, the shift from call centers to digital self-service opens up significant opportunities—especially when the chosen software solution combines high data security with efficient processes.



Security team

Identity-based attacks—such as account takeovers—are among the most common attack methods used by cybercriminals as well as state-sponsored, professional attack groups (Advanced Persistent Threats, APTs). A modern cIAM system must therefore combine cIAM functionality with robust IT security and authentication mechanisms. These mitigate all risks associated with online access: fraud and account takeover, security breaches, exploitation of vulnerabilities in applications, DDoS attacks, and much more. It is also essential to contain AI-enabled threats. This is because AI-generated lookalikes (deepfakes) now pose a threat to video-based customer identification processes in the financial industry, for example. Such AI-enabled attacks can be thwarted through real-time behavioral analysis that focuses not only on biometric patterns but also on the consistency of these patterns.

Compliance officer

Within a company, demonstrating compliance with local data protection laws and industry regulations involves significant effort. If the company operates internationally, additional requirements apply; in the EU, these primarily include the GDPR, and depending on the industry, NIS 2 and others as well. The use of a state-of-the-art cIAM solution significantly simplifies the process of demonstrating compliance with various regulations: ISO 27001 certification proves that Airlock operates a state-of-the-art information security management system; GDPR processes and pre-built reports stored within the cIAM solution, in turn, save time and costs in the event of regulatory audits.



Appendix III:
Glossary and abbreviations

- **Account Takeover:** The hijacking of user accounts, achieved through phishing, → *social engineering,* or the purchase of compromised user databases.
- **API (Application Programming Interface):** An interface for application programming and thus a point of integration for applications.
- **APT (Advanced Persistent Threat):** A professional and often state-sponsored group of attackers.
- **cIAM (Customer Identity and Access Management):** Scalable and secure management of customer and user identities and access. Unlike enterprise IAM, it focuses on external rather than internal users.
- **Declouding:** Migration away from the cloud, either for cost reasons or with the goal of greater data sovereignty. Can be implemented quickly if the on-premises and cloud solutions share the same code base.
- **DevSecOps:** A portmanteau of Development, Security, and Operations. A software development approach that integrates security methods into every phase of the software development lifecycle.
- **DDoS (Distributed Denial of Service):** Targeted overloading of web or application servers through distributed, mass data traffic. Can be mitigated using DDoS mitigation solutions and devices.
- **GDPR (General Data Protection Regulation):** Comprehensive EU data protection regulation.
- **E-ID (electronic identity):** digital proof of identity issued by the Swiss government but managed via a mobile app *(→ Wallet)* under the individual user's granular control. Scheduled for introduction in 2026, it is expected to greatly simplify everything from dealing with government agencies and proving age to placing orders and purchasing tickets.
- **EUDI (European Digital Identity):** The EU counterpart to the Swiss → *E-ID.* Scheduled to launch in late 2026, it will also place control over digital identity and the use of associated data directly in the hands of EU citizens.
- **FIDO 2 (Fast Identity Online 2):** an open standard for strong passwordless multi-factor authentication (MFA). Uses asymmetric encryption, biometrics, → *passkeys,* smart cards, and → *TPM.* The dynamically negotiated selection of the most secure possible MFA method is intended to prevent identity-based attacks.
- **GDPR (General Data Protection Regulation):** English for → *DSGVO.*
- **IAM (Identity and Access Management):** secure management of user identities and access. Originates from the corporate context and focuses there on local and remote access by employees, i.e., internal users (in contrast to → *cIAM,* which is designed with customers and thus a diverse range of external users in mind).
- **IdP (Identity Provider):** A service or system that provides, manages, and authenticates the digital identities of users or devices.
- **IoT (Internet of Things):** The totality of technologies for interconnecting virtual and physical objects (i.e., not just the interconnection of users with applications and data).
- **ITSM (IT Service Management):** The entirety of processes, measures, and methods for supporting business processes through IT systems.

- **AI (Artificial Intelligence):** An umbrella term for IT systems capable of autonomous learning. Although it has existed for decades, it has recently been the subject of intense discussion in the forms of generative AI (AI that generates content, e.g., OpenAI ChatGPT, Google Gemini, or Anthropic Cloud) and agentic AI (AI that initiates actions, e.g., hotel bookings, reconfiguration of network switches).
- **MAU billing (Monthly Active Users):** A method of calculating license costs based on the number of active users in a calendar month.
- **MFA (Multi-Factor Authentication):** A multi-step security verification of user identity during login. Uses multiple factors (i.e., methods or parameters) for identity verification, e.g., username/password and app-generated access PIN, or biometrics and PIN.
- **NHI (Non-Human Identity):** The digital identity of a machine, application, service, or AI bot.
- **NIS 2 (Network and Information Security 2):** EU directive aimed at improving risk management and IT security in 18 critical/highly critical economic sectors.
- **Passkey:** a modern passwordless login method based on cryptographic key pairs, designed to make logins more secure and convenient than with traditional usernames/passwords. Users log in, for example, using biometric data (fingerprint, facial scan) or → *tokens.*
- **PQC (Post-Quantum Cryptography):** Encryption methods that, based on current knowledge, can withstand even future attacks using powerful quantum computers.
- **SDK (Software Development Kit):** A collection of programming tools and software libraries for developing or extending software solutions.
- **SIEM system (Security Information and Event Management):** A solution for the continuous and timely analysis of security alerts in the corporate network.
- **Social engineering:** Deception through the exploitation of human weaknesses (e.g., curiosity) and biases. Occurs both online and in the physical world.
- **Social Login:** Logging in to a service using an existing identity from a social network (Facebook, Google, etc.). Often preferred by consumers because it is convenient.
- **SSI (Self-Sovereign Identity):** A self-determined digital identity, meaning one managed directly by the user themselves rather than by a central authority or government agency. Significantly simplifies many digital processes. Enables the targeted disclosure of specific information (e.g., only the date of birth for age verification) and thus enhances data protection. To be implemented in Switzerland in 2026 via → *E-ID,* and in the EU via → *EUDI.*
- **Token:** physical or digital proof used for authentication or authorization. In physical form, e.g., as a USB stick or USB key.
- **Token Exchange:** A feature for "translating" → *tokens* from various IdPs into task-specific tokens. Resource access can thus be configured both granularly and dynamically and restricted to individual accesses in accordance with the zero-trust principle.
- **TPM (Trusted Platform Module):** A security chip on the motherboard or in the CPU that securely stores cryptographic keys, passwords, and digital certificates.
- **UX (User Experience):** The totality of the user experience when navigating or interacting with a digital environment.

- **WAAP (Web Application and API Protection):** Integrated security platform for protecting web services/applications and → *APIs.*
- **WAF (Web Application Firewall):** A firewall designed to protect web applications from cyberattacks. It is an integral part of a → *WAAP solution.*
- **Wallet:** An app in which a user autonomously manages and controls their digital identities within the framework of an → *SSI architecture.*



Appendix IV:
Further information

Airlock IAM as a Service:
https://www.airlock.com/en/secure-access-hub/components/iam/airlock-iam-as-a-service

Airlock White Paper: The puzzle pieces of modern authentication
https://www.airlock.com/en/puzzle-pieces-of-modern-authentication

Airlock White Paper: The (r)evolution of digital identity
https://www.airlock.com/en/whitepaper-the-revolution-of-digital-identities

Airlock White Paper: How to make cIAM a success?
https://www.airlock.com/en/how-to-make-ciam-a-success

Airlock Whitepaper: Do you speak token?
https://www.airlock.com/en/do-you-speak-token



About Airlock – Security Innovation by Ergon Informatik AG
The Airlock Secure Access Hub combines the key IT security disciplines of filtering and authentication into a finely tuned overall package that sets standards in usability and services. The Secure Access Hub covers all key functions of modern IT security in this area: from an award winning web application firewall (WAF), through a Customer Identity and Access Management (cIAM) trusted by Swiss banks, to API security that meets the latest requirements. Airlock protects more than 20 million active digital identities and 30,000 back ends for over 550 customers worldwide. Further information at airlock.com. Airlock is a security innovation by the Swiss software company Ergon Informatik AG.

Founded in 1984, Ergon Informatik AG is a leader in creating bespoke software solutions and software products. Its success is built on over 400 highly qualified IT specialists who, thanks to outstanding expertise, anticipate new technology trends quickly and ensure decisive competitive advantages with innovative solutions. Ergon primarily delivers large scale B2B projects.

Ergon Informatik AG
Merkurstrasse 43
8032 Zurich
+41 44 268 89 00
info@airlock.com

airlock.com

ergon

Copyright © 2026 Ergon Informatik AG. All Rights Reserved. All technical documentation that is made available by Ergon Informatik AG is the copyrighted work of Ergon Informatik AG and is owned by Ergon Informatik AG. Ergon, the Ergon logo, «smart people – smart software» and Airlock are registered trademarks of Ergon Informatik AG. Microsoft and ActiveDirectory are registered trademarks or trademarks of Microsoft Corporation in the United States and /or other countries. Other products or trademarks mentioned are the property of their respective owners.