kuppingercole ANALYSTS

How to Build the Modern CIAM: For Customers, Consumers, and Citizens

Martin Kuppinger

December 22

In the digital age, the “C identities” of customers, consumers, citizens, and all the other types of external identities, such as tourists, are at the forefront of every digital business and government. A modern CIAM is indispensable for digital organisations.

This whitepaper looks at the trends impacting CIAM, what makes up a modern CIAM, how to make it work across all industries, and the different types of “C identities.”

Contents

Figures

Executive Summary

In the Digital Age, all types of organisations face the challenge of dealing with a growing range of external identities. Digital services are now the face of organisations to all outside parties. Consequently, the digital experience - including a smooth user journey - has become a key factor for success.

This applies to every organisation, from businesses dealing with their direct customers or indirectly with consumers to government organisations where the “customers” are citizens, expatriates, or tourists. Serving these “C-type” identities, the customers, consumers, citizens, etc., is essential to the success of all organisations in the Digital Age.

Digital services must evolve quickly while remaining secure and trustworthy and deliver a modern, consistent user experience, including the user journey for onboarding and authenticating users.

This can be achieved only with a strong CIAM (Customer Identity & Access Management) system as the backend component of digital services for identity and access management. Strong CIAM manages identities at scale with a robust set of APIs (Application Programming Interfaces) that the developers of digital services can use to consume identity services and work with the CIAM system. That way, developers are released from the burden of implementing their identity services and avoid siloed approaches for identities – one silo per digital service.

There are three groups of requirements for a modern CIAM:

1. First, the solutions must support a robust set of standard CIAM capabilities.
2. Second, they must be built for emerging requirements and trends such as passwordless authentication, fraud reduction, and decentralized identities.
3. Thirdly, they must feature a modern architecture supporting a comprehensive set of APIs.

Delivering these solutions requires a well-thought-out target operating model (TOM) and a strong partner with extensive experience in this domain. Ideally, there should be end-to-end support from the assessment of status and requirements to delivering the solution and supporting operations.

Aujas, a global cybersecurity firm and system integrator specializing in IAM (Identity and Access Management) provide such services, building on defined, proven methodologies and the experience gained from delivering thousands of projects to organisations around the globe.

Highlights

- CIAM is a key functionality for delivering the services that organisations require to succeed in the digital age, specifically delivering a positive user experience while onboarding customers and providing them recurring access.

- Modern CIAM goes beyond traditional solutions, which frequently came with a focus on retail and eCommerce. They must deliver to the specific needs in the digital journey of organisations and provide strong support for emerging technologies and capabilities.
- Successful delivery of CIAM projects requires end-to-end support for the project by experienced partners and defined target operating models.
- Aujas provides a proven, end-to-end methodology for implementing complex projects such as CIAM backed by their experience in executing similar large-scale projects.
- Having the right people on board, specifically the business teams, is crucial for the success of CIAM projects. Understanding the business models and business change is mandatory.

The modern CIAM for the Digital Age

> CIAM is the foundation for a modern, positive user experience that supports differentiation in today's fast-changing, competitive commercial landscape.

In the Digital Age, everyone expects organisations to deliver their services digitally. This affects all organisations, including private-sector businesses and government organisations. The digital experience becomes the differentiating factor and is a key element of success.

This is most obvious for customers and consumers. Businesses need to provide a leading-edge digital experience to avoid losing out to the competition. And this is not limited to the retail and finance sectors; tourists today want to book their travel, accommodation, day trips, and everything else online. Citizens expect digital governmental services instead of endlessly queueing at government offices. Investors rate the status of the digital journey as a decisive factor for investments, while students choose universities based on the digital experience and services provided.

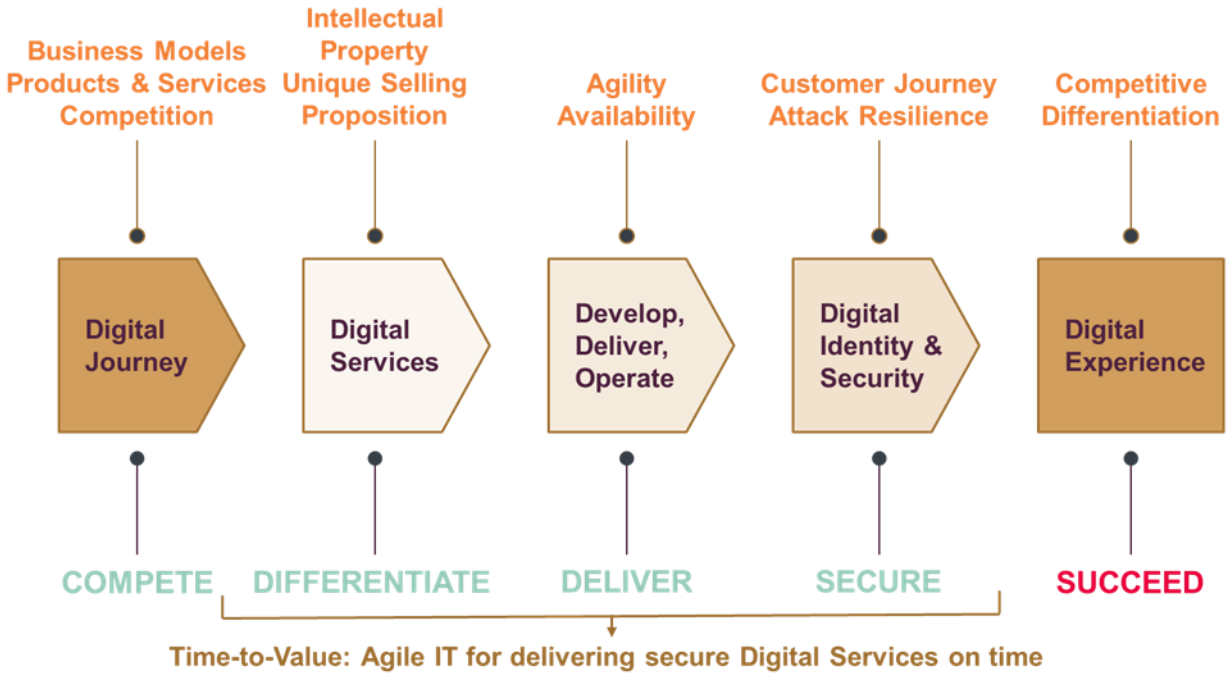

Figure 1: Digital Experience is what makes Digital Services succeed. This requires strong support for the "C" identities, such as customers, consumers, and citizens.

Time-to-Value: In the Digital Age, competition is fast-changing. New digital services can become popular rapidly, putting established players under pressure to innovate their products and services. The rapid change of business models requires every organisation to execute its own digital journey to remain competitive. Notably, this involves continuous evolution, not just a one-time digital transformation.

> CIAM solutions must be able to adapt to the fast-changing business demands in the Digital Age.

Digital services are the foundation for success, but these services must be developed in an agile and timely manner and delivered and operated reliably and securely. Time-to-value is essential to stay ahead of the competition.

Consumer's Identity Security: Just having a digital service, however, is not sufficient. Trust also plays a central role in today's global digital competition. Trust is difficult to earn but can be lost quickly and easily. Digital services, therefore, must not only provide an excellent user experience but they must also be delivered and operated securely to build and maintain trust. Digital identities are at the core of all "C" identities and beyond: For customers and consumers, citizens, tourists, students, expatriates, and all the others consuming digital services. Providing these services is the task of CIAM (Consumer IAM) - the IAM solutions that support onboarding and authentication processes for users on a large scale.

Customer's Data Privacy: Digital Trust is highly reliant on treating customer data appropriately. Complying with regulations such as the EU GDPR (General Data Protection

Regulation) or CCPA (California Customer Privacy Act) is essential. CIAM solutions must support handling customer data and PII (Personally Identifiable Information) according to global and regional regulations.

Customers' Digital Experience: CIAM emerged as a separate category about a decade ago and has undergone much innovation and change in this market segment. Several CIAM start-ups have been acquired, while established IAM vendors have extended their solutions to support CIAM use cases.

Effectively, the CIAM market has also split into two categories:

1. CIAM solutions that focus on onboarding and authentication processes.
2. CDP (Customer Data Platforms) that focus on providing a system of record for customer data.

Both commonly link to customer marketing automation solutions. CIAM, in this context, faces the customer and is essential for:

- Building customer experience with improved personalization.
- Reducing drop-off rates during onboarding.
- Reducing churn rates of existing customers and consumers.

CIAM focuses on onboarding and authentication processes, with Customer Data Platforms and Customer Marketing Automation solutions supplementing CIAM.

Fraud Reduction: Another important element that is integrated into several of the CIAM solutions in the market is Fraud Reduction Intelligence Platforms (FRIPs). These platforms help identify anomalies in user interactions so that systems can react. FRIPs can ask for an additional level of authentication, block transactions, and more. FRIPs are well-established in the payments industry but are now becoming increasingly popular in other industries for preventing online fraud.

Passwordless Experience: The trend to allow passwordless authentication has also impacted CIAM Authentication. Supporting such authentication, based on device possession and binding of the device to a user, and biometric authentication is increasingly becoming the norm for authentication. Passwordless authentication delivers the convenience required for a highly positive digital experience.

Decentralized Identities: A newer trend toward adopting decentralized identities is likely to have an increasing impact on CIAM. Here, the user holds proof of their identities, such as proof of their name and address, derived from an eID card or proof of employment provided by their employer. These proofs can be used to simplify onboarding and authentication processes, further improving the digital experience.

At long last, a growing number of organisations are focusing on a comprehensive strategy for all IAM capabilities by applying the concept of an Identity fabric that caters to all types of

identities and backend services. CIAM is a subset of these capabilities and is increasingly integrated with other IAM services.

Key capabilities of a modern CIAM

> Modern CIAM solutions must support the rapid change in business models and business technologies. They must be able to adapt to new trends and capabilities, including decentralized identities, fraud reduction, and passwordless authentication.

So, what makes up a modern CIAM that can serve all the C-identities and beyond? Essentially, it is about three aspects:

1) A comprehensive set of standard CIAM features, such as support for authenticators and the ability to scale
2) Support for emerging trends such as decentralized identities, passwordless authentication, and Zero Trust models
3) A modern, flexible architecture supporting the customer's preferred TOM

While even traditional CIAM implementations come with comprehensive features, the following two aspects distinguish a modern CIAM from conventional approaches. Emerging trends dictate these six capability areas that stand out:

1) **Central Identity Service:** In the Digital Age, CIAM must serve as the backend for digital services, supporting the identities they need. It must be able to perform a multitude of such digital services without complex adaptation to enable rapid delivery of these services and decrease time-to-value in service delivery.
2) **Focused capabilities & integration:** While CIAM in the past tended to integrate a wide variety of capabilities, including Marketing Automation and CDP (Customer Data Platform) features, the current trend is towards specialization and analytics. This is also because CIAM is an identity-focused backend service that the IAM department commonly owns, while Marketing Automation is owned by the marketing department. The business itself commonly owns CDP with its analytical focus. CIAM solutions should deliver baseline marketing automation and CDP capabilities and provide strong integration into other capability sets.
3) F**raud Intelligence:** FRIPs (Fraud Reduction Intelligence Platforms) have gained substantial momentum in the Digital Age due to a steady and steep increase in cyber-attacks. Thus, such technologies must be part of the overall CIAM solution, either as built-in capabilities or via integration. This helps to detect ATO (Account Take Over) attacks and attacks while onboarding and executing transactions. It is also a supportive technology for Adaptive Authentication and Progressive Profiling.
4) **Support for Decentralized Identities:** Another major trend in the market has been toward Decentralized Identities. These aren't owned and managed by enterprises but by individuals. Modern CIAM must allow for integrating Decentralized Identities and mapping these to the internal customer records.
5) **Support for Passwordless Authentication:** With all the inherent weaknesses of passwords affecting both security and convenience, passwordless authentication has

seen a steep increase in adoption for both workforce and external identities. CIAM solutions ideally support phishing-resistant, passwordless authentication capabilities that build on biometric authentication and device trust.

6) **Built for Zero Trust:** Zero Trust has emerged as the leading security principle. The concepts of "don't trust, always verify," including continual authentication, are therefore also essential to modern CIAM. Many of the trends mentioned above, such as passwordless authentication and FRIP, are essential concepts for supporting a Zero Trust model.

> CIAM must start with a thorough assessment of technical requirements, business requirements, and the evolution of business models.

With the trend of delivering solutions as a service, the requirements for the architecture and implementation of CIAM solutions have also changed fundamentally. There are essential but important principles that must be met:

- **API first**: The design must be API first. APIs (Application Programming Interfaces) take a central role in modern deployments, where customization happens either via no-code configuration or via integration, orchestration, and extension through the APIs. All code-based customization can be done correctly in separate microservices based on a consistent set of APIs; customizations remain unaffected by updates to the CIAM system.
- **Consistent API layer**: A consistent set of APIs defines the API layer that can also be used by the developers of the digital services. Consistency is key to leaving digital services unaffected by the continuous evolution of the underlying CIAM system.
- **Microservices architecture**: Customers should also ask vendors about the architectural details of the CIAM solution. Modern microservices architectures are the foundation for continual improvements and updates.
- **Container-based deployments**: Finally, a flexible deployment model is also essential. Modern CIAM solutions support container-based deployments, which can run in any cloud, even in hybrid and on-premises environments.

There are alternatives for the latter two aspects, such as purely multi-tenant, public cloud solutions, where the Cloud Service Provider fully provides deployment and operations. Customers commonly ask for some flexibility and work with MSPs (Managed Service Providers) to define their Target Operating Model (TOM) of choice. The TOM defines the deployment, the organisation, and the responsibilities for implementing, customizing, and operating the system.

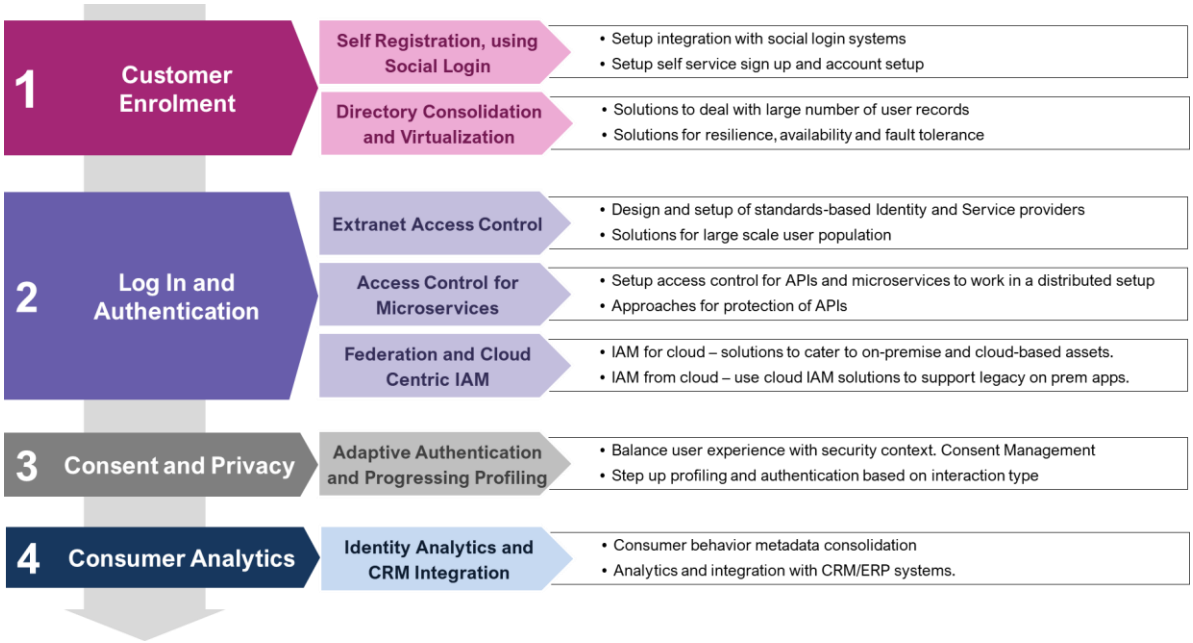

Figure 2: A practical perspective on core capabilities for a modern CIAM from a roll-out perspective (Source: Aujas).

Successful deployments start with a mapping of features and capabilities of modern CIAM to functional areas and taking concrete steps in implementing capabilities. As depicted in Figure 2, such an approach follows the steps from enrolling customers and integrating customer data through to log-in and authentication, consent, and privacy management, and finally, consumer analytics, based on the concrete behavior and working in tandem with integrated Marketing Automation solutions.

Making the modern CIAM a reality: Success Factors

> Many aspects determine the success or failure of CIAM projects. A deep understanding of the business and technical requirements of the business and digital service development teams is essential, as CIAM is more than just a tool deployment.

As with every digital program, the tool is essential. However, deploying the tool is just one success factor amongst many. Other factors such as proper project execution, realistic targets, defined quick wins and big wins, stakeholder management, and more are equally critical. The top five success factors that stand out for a modern CIAM project are:

1) **Strong Alignment with Consumers' Business Needs**: The requirements of today and the foreseeable future requirements must be well-understood. Trends must be factored in. However, the driving factor is the business model. Without a proper understanding of the business model and strong business alignment, CIAM will fail to meet expectations.

2) **Flexibility in Target Operating Model**: As mentioned before, the TOM also plays a critical role. Flexibility in deployment and operations and excellent support for as-a-service models are the keys to success.
3) **Strong Focus on Leading-edge User Experience**: Serving the organisation's Digital Services be it a business or a governmental agency, is key. The success of these depends on User Experience (UX). Modern UIs that work the way the users expect is extremely important– with CIAM remaining as hidden as possible.
4) **Balance Between Security and Convenience in User Journeys**: An essential element within the UX is the user journeys, starting with the onboarding process and recurring authentication. These must be kept very flexible to be able to adapt to constant evolution in this area, such as the trend towards Decentralized Identities, while other approaches, such as Facebook authentication, are losing momentum. Another example is the ever-changing world of authenticators. While fingerprint readers dominated for a while, face recognition has emerged as the current standard. CIAM must deliver the flexibility to adapt to these environmental changes without needing to change the Digital Services built on the CIAM solution.
5) **Extensibility for the Future**: With the continuous evolution we are facing in IT as well as in the Digital Business and Digital Age, successful CIAM implementations must be capable of adapting to that change. This, again, goes back to architecture and APIs, which are the foundations for extensibility.

> The success of CIAM projects is based on having the right people on board across the enterprise – from the IAM team to the business owners of digital services.

Success depends on technology and organisation, but most importantly, on people. Again, this leads to the TOM, which clearly defines the cooperation and collaboration between organisations, the various teams and departments within those organisations, the software vendors, and the implementation and operations partners. Success depends on picking the right partners and collaborators to guide an enterprise through seamlessly identifying the need and requirements to run day-to-day operations.

The Aujas approach to delivering the CIAM for the future

> Aujas Cybersecurity provides end-to-end deployment of CIAM solutions, from assessment to implementation. This experience is derived from executing a large number of projects across industries and regions.

Aujas Cybersecurity is a global service provider for solutions in the cybersecurity and identity market, with CIAM solutions forming a key part of their portfolio. The company has served more than 1,500 customers globally and executed more than 2,000 cybersecurity projects. With 950+ cybersecurity experts and offices around the globe, Aujas can support projects at any scale.

Aujas has an end-to-end approach for projects, from the initial assessment down to the full deployment of solutions and the transition into operations. The comprehensive set of expertise provides an advantage for the customer of working with one trusted partner throughout the project and beyond and supports the operations and continual evolution of the CIAM solution.

> End-to-end approaches in delivering CIAM projects ensure consistent execution and proper management of stakeholders throughout the project.

This approach builds on a delivery methodology consisting of eight stages, following a typical waterfall approach, but targets the CIAM specifics:

- **CIAM Strategy & Roadmap**: Collaborating with the customer to clearly define the strategy, project targets, and roadmap.
- **Getting Ready**: Identifying constraints, targets, deadlines, and restrictions and determining customer requirements in a structured manner.
- **Planning**: Planning the project and finalizing project details.
- **Designing**: Technical design as well as user-journey design for the solution.
- **Build**: Implementing the solution, user onboarding, and conducting knowledge transfers
- **Test**: Testing across multiple stages to ensure that the solution meets the customer's requirements.
- **Go-Live**: Moving to the production stage, ensuring that all involved parties are well-prepared.
- **Enhancement and Sustenance**: Continual evolution of the solution, including audits and benchmarking.

Each stage comprises multiple detailed steps, with defined methodologies and descriptions of the steps within the stages. This, for instance, affects the initial definition of the CIAM target framework from defining constituents to user journeys and, finally, capabilities and configuration.

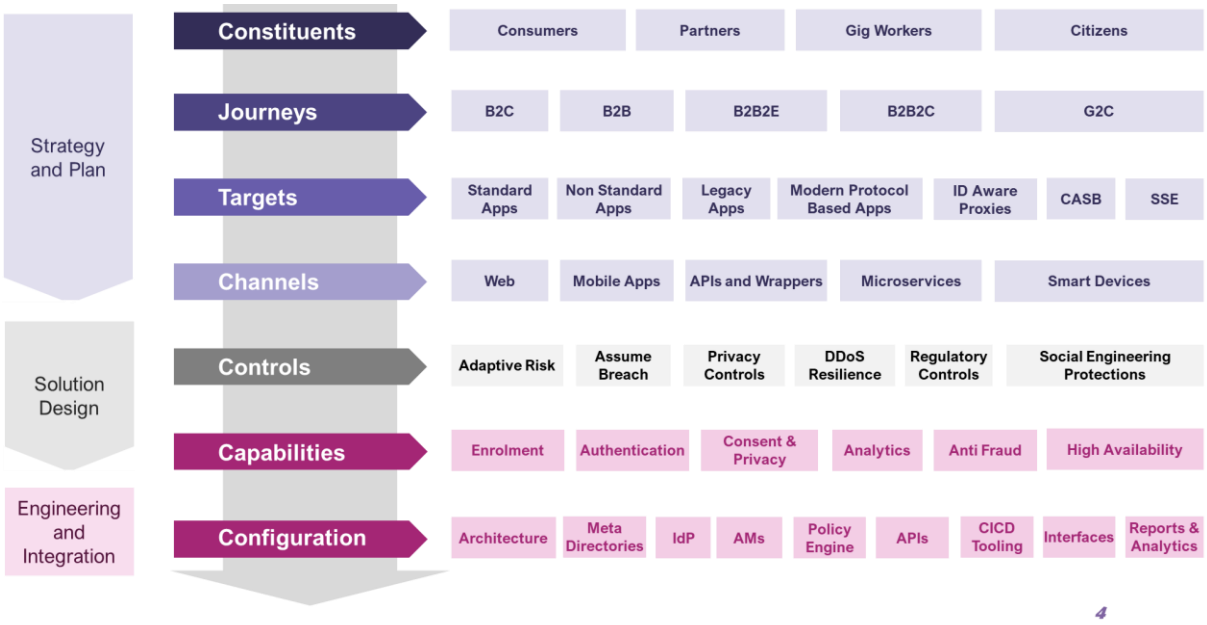

Figure 3: The Aujas methodology supports a 360-degree approach, serving the customer from initial assessment to operations, covering all types of capabilities and application integrations (Source: Aujas).

In this methodology, Aujas focuses on the specifics of CIAM, starting with the broader perspective of which users must be covered. As outlined ahead, CIAM is not only about customers and B2C use cases but can cover a range of other usage patterns such as B2BDE, G2C, and more. For these, the journeys must be defined for both the onboarding pattern and the recurring access. This includes defining the appropriate way of identifying and verifying users.

Also, the channels for interaction with the C users must be defined according to the use case and must remain flexible in an age where interaction is increasingly shifting from traditional web access to apps and other means. The foundation for a successful CIAM deployment is set in the initial strategy and planning phase.

Following this planning phase, the concrete solution must be defined. Journeys must integrate with the existing IT infrastructure, including the backend services. Defining both the use cases, channels, and interactions with the users and the technical architecture that links the users via the CIAM solution to the backend services is covered in defined steps in the Aujas 360-degree methodology for developing a CIAM strategy.

It all culminates in the engineering and integration phase, where solutions are configured and customized to deliver the intended capabilities.

This approach is complemented by defined frameworks covering, on the one hand, the core capabilities for CIAM across multiple stages, from customer enrolment, login, and authentication or consent and privacy to customer analytics, and on the other hand, a comprehensive plan and build a framework for delivering these capabilities.

At a technical level, Aujas works with defined reference architectures and capability maps that define the common elements of CIAM. This supports projects by enforcing standardized,

proven approaches and ensuring that all potential areas of CIAM are discussed with the customer. Customers then can decide on priorities and whether they need certain capabilities in their environments.

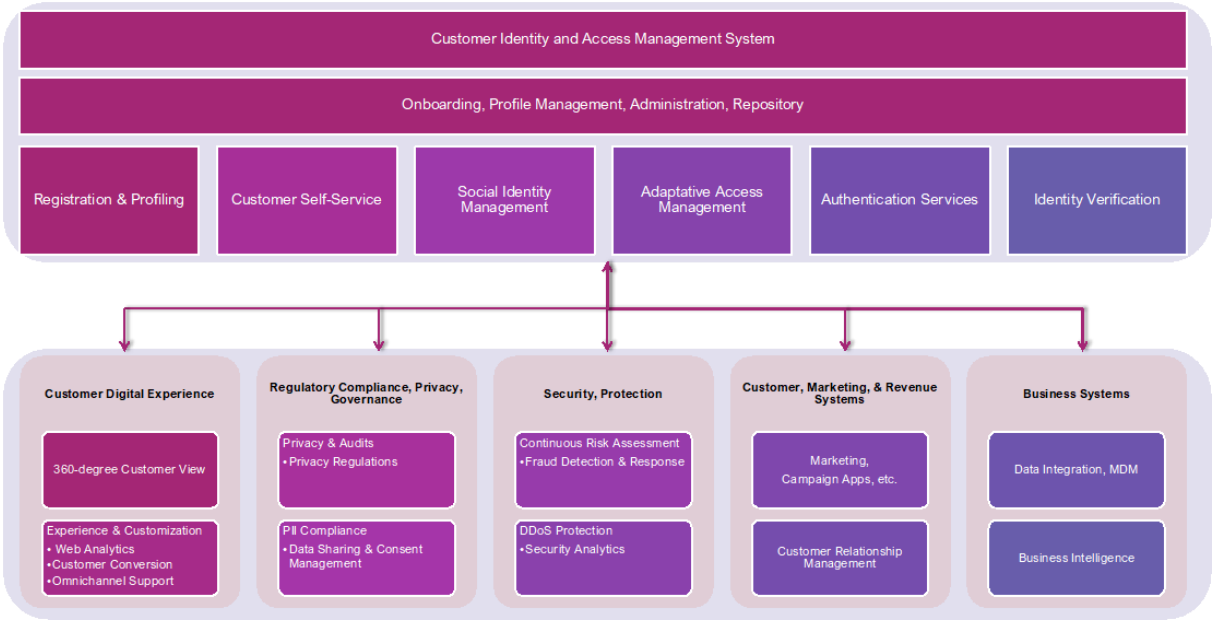

Figure 4: Aujas builds on a standardized view of CIAM foundational elements (Source: Aujas).

These structured approaches, methodologies, and technical blueprints allow Aujas to perform projects efficiently and effectively, limiting project risks by building on standardized approaches and proven methodologies.

The company has extensive experience and specialization in cybersecurity and identity, including a significant number of identity management projects across all types of identities, including workforce, business partners, customers and consumers, tourists, expatriates, citizens, and others. Based on that experience and a wide range of technology partnerships, Aujas can support customers in the successful execution of their CIAM projects in their Digital Journey.

With the shift of CIAM from traditional customers & consumer use cases such as retail and eCommerce towards a wide range of use cases and C-type customers, Aujas also benefits from its experience in other industries and government-driven use cases.

Recommendations

Organisations are challenged by their journey in the Digital Age. In that journey, the digital user experience (UX), the user journey, and trust based on cybersecurity have become critical success factors. CIAM solutions help organisations to serve the needs of their digital business and digital services and the needs of their users, such as customers, consumers, and citizens. Successfully running a CIAM project requires a detailed and systematic approach backed by experience and the right partners.

To succeed in such a project, ensure that the right players are on the field:

- **IAM team**: This is the internal team that owns the CIAM solution. It will work with other teams, such as marketing, in delivering the required integrations.
- **Stakeholders**: The people requesting the project and providing the budget, including the CIO and business owners. With CIAM being at the core of the digital business, this commonly should involve C-level executives.
- **Business units**: The business units that are requesting digital services. Depending on their number, these should either be involved directly or via councils and representatives for gathering the business needs and understanding the current and future business models.
- **Digital Services teams**: The teams creating the digital services and work relying on the CIAM system must be involved and understand the benefits of utilizing a central CIAM solution. They must also be supported in getting the maximum benefit out of it.
- **Technology vendor/provider**: The provider of the CIAM solution, be it as a tool for deployment in the chosen TOM or as a public cloud service.
- **Consulting system integrator**: The partner that serves as consultant and implementation partner, end-to-end, and connecting all the parties for a successful implementation.

CIAM is the link between digital services, the identity and cybersecurity backend, and the business.

Related Research

Leadership Compass CIAM Platforms
Leadership Compass Customer Data Platforms
Leadership Compass Providers of Verified Identity
Leadership Compass Fraud Reduction Intelligence Platforms

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in making decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please get in touch with clients@kuppingercole.com.