AUJAS CYBERSECURITY
An NSEIT Company

aujas.com

Consumer Identity and Access Management

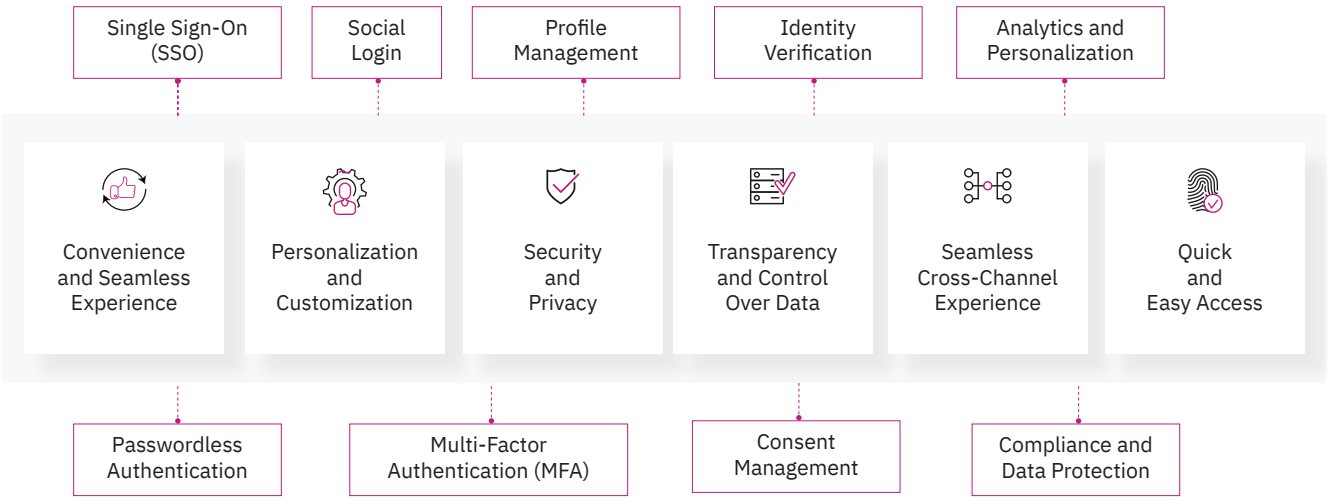
SOLUTION BRIEF

When engaging with brands, customers have two key expectations. First, they desire a seamless, consistent, and effortless user experience across various devices, channels, locations, and applications. Second, they anticipate businesses to offer enhanced online security and privacy safeguards. With a massive volume of consumer data and transactions, businesses face a critical question:

How to effectively collect, store, and manage this data to personalize interactions while upholding the highest privacy standards?

With Aujas Cybersecurity's Consumer Identity & Access Management (CIAM) services you can deliver enhanced security, seamless user experiences, and compliance assurance, while maintaining data integrity and operational efficiency.

What matters to digital consumers?



Why **CIAM ?**

CIAM empowers businesses to gain deeper insights into their customers, safeguard their data, and provide seamless and secure access to services. With CIAM, businesses can create a safe environment for their customers, ultimately driving business growth and revenue.

Core capabilities for consumer IAM

Customer Enrolment	**Self Registration, using Social Login**	• Setup integration with social login systems • Setup self service sign up and account setup • Automated Identity Validations • Progressive Onboarding
	Directory consolidation and virtualization	• Solutions to deal with large number of user records • Solutions for resilience, availability and fault tolerance
Log In and Authentication	**Extranet Access Control**	• Design and setup of standards-based Identity and service providers • Solutions for large scale user population • Adaptive Authentication and progressive Profiling
	Access Control for Microservices	• Setup access control for APIs and microservices to work in a distributed setup • Approaches for protection of APIs
	Federation and Cloud Centric IAM	• IAM for cloud – solutions to cater to on-premise and cloud-based assets • IAM from cloud – use cloud IAM solutions to support legacy on prem apps
Consent and Privacy	**User options regarding data collection and usage**	• Balance user experience with security context, Consent management • Set up profiling and authentication based on interaction type • Self-service consent management
Consumer Analytics	**Identity Analytics and CRM Integration**	• Consumer behavior metadata consolidation • Analytics and integration with CRM/ERP • Navigation Analysis

Social media integration

Integrating social media with CIAM streamlines customer access by allowing users to log in with existing social media accounts. This removes the need for separate credentials, simplifying registration and login. Additionally, it offers verified user information, enhancing identity verification and reducing the risk of fraud.

Biometric authentication

CIAM uses unique biological traits like fingerprints or facial features for secure identity verification offering high security as biometric data is hard to replicate. It strengthens user authentication and enhances convenience by allowing users to access accounts securely without passwords.

FIDO2/Device-based authentication

CIAM enables password less authentication using cryptographic protocols. Users can authenticate with biometric data or security keys stored on their devices, reducing risks like phishing. Device-based authentication uses device security features, ensuring secure access to CIAM platforms.

Our **services**

Key features

- Optimized customer enrollment
- Secure log-in and authentication
- Consent and privacy management
- Consumer behavior analytics integration

Aujas Cybersecurity CIAM services include

In-depth capability planning

- Defined frameworks and capability maps for essential CIAM capabilities
- Employment of standardized technical architectures for efficient execution

Robust approach

- Comprehensive 360-degree methodology from assessment to execution
- Detailed eight-stage methodology for effective CIAM project delivery

User-centric CIAM framework

- Targets varied user groups beyond B2C, including B2B and G2C
- Clearly defined user journey mapping and flexible channel interactions

End-to-End deployment expertise

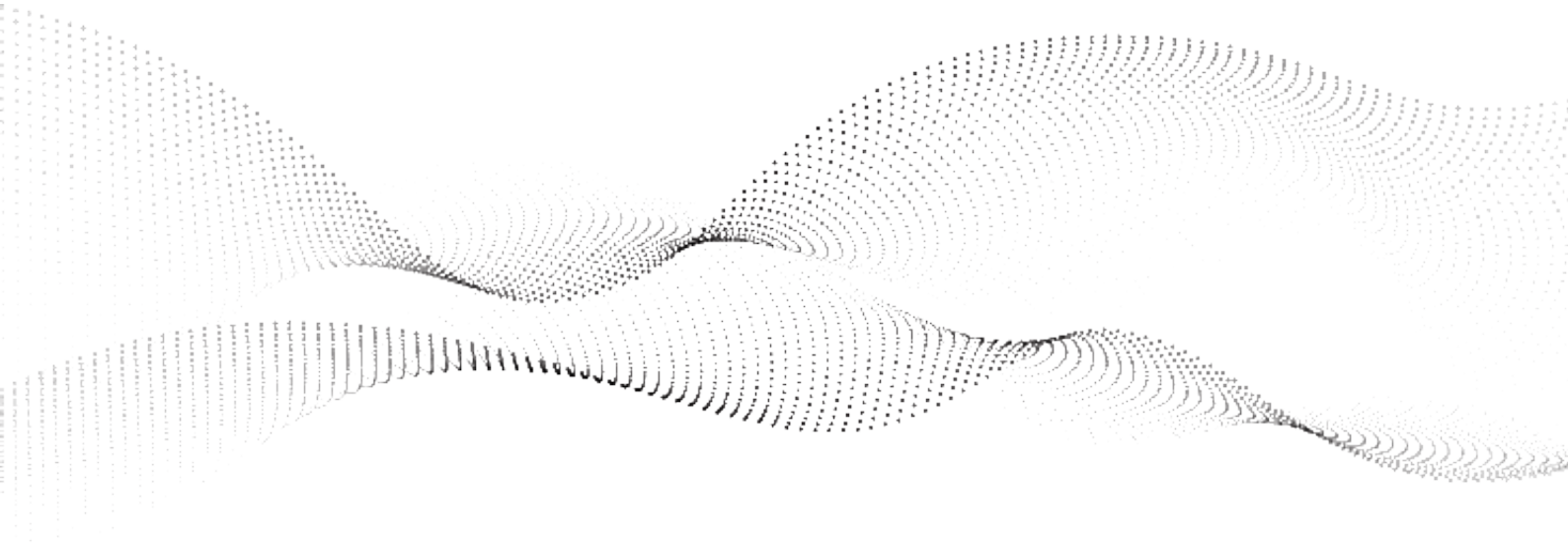
- Comprehensive CIAM assessment and implementation
- Extensive industry-spanning experience in diverse projects

Aujas CIAM - Plan and Build Framework

Stratergy and Plan	**Constituents**	Consumers Partners Citizens
	Journeys	B2C B2B B2B2E B2B2C G2C
	Targets	B2C Standard Apps Non Standard Apps Modern Protocol based apps SSE Legacy Apps ID Aware Proxies
	Channels	Web Mobile Device Interactive Voice Response Kiosk/ATM
Solution Design	**Controls**	Adaptive Risk Privacy Controls Regulatory Controls Assume Breach DDoS Resilience Social Engineering Protections
Engineering and Integration	**Capabilities**	Enrolment Authentication Consent & Privacy Anti Fraud High Availability Analytics
	Configuration	IdP Architecture Meta Directories CICD Tooling APIs AMs Interfaces Policy Engine Reports & Analytics User Journeys

Value we deliver through **our services**

Data breach prevention	• Reduced risk of data breaches through rigorous identity verification and permission-based access control
Compliance	• Swift compliance with international privacy and data protection laws (GDPR, SOX, PCI-DSS, CCPA, etc.) to build customer trust • Customer control over data, profiles, and privacy settings through a central portal
Operational efficiency	• Self-service account management and single sign-on access to multiple services for improved operational efficiency and reduced costs • Empower partners and customers to use digital services independently within defined parameters • Centralized User Repository • Centralized User Policy Management
Improved customer experience	• Enhanced customer experience and loyalty with single sign-on and easy onboarding processes
Insights	• Integration of CIAM with CRM and analytics for a deeper understanding of customer behavior and the provision of personalized experiences across channels • Know your customer (KYC) • Navigation trends and statisitics



Success **stories**

Leading bank in Saudi Arabia

Business challenge

The bank faced challenges in aligning with regulatory frameworks like SAMA Counter Fraud and open banking standards while centrally managing access across diverse applications for external users. Streamlining user login and implementing single sign-on (SSO), along with establishing trust association between old and new portal environments, posed hurdles. Integrating federation services for authentication against a national IAM platform and defining client-user journeys for authorization channels were additional complexities. Developing identity data models and flows for various channels required detailed planning to ensure data security and usability.

Solution

We offered an end-to-end solution tailored to meet the client's unique security needs. We established a foundational user journey covering registration, authentication, password recovery, and account management processes. With plans to manage millions of identities, our deployment supported microservices architecture using OAuth and OpenID Connect, ensuring scalability and interoperability. We centralized the identity repository and authentication services, implemented MFA and SSO across all channels, and provided API protection. Aujas Cybersecurity also enabled limit management for end customers and integrated analytics to monitor user interactions, enhancing the overall user experience while ensuring robust security measures.

Business impact

Aujas Cybersecurity's CIAM solutions offered advanced security through features like multi-factor authentication, biometric authentication, and adaptive authentication, mitigating the risk of unauthorized access and fraud. Our CIAM platforms improved customer experience by providing seamless access to banking services across various channels and devices while offering personalized services through effective data gathering and analysis. Moreover, our services helped the bank comply with regulatory requirements such as SAMA Controls, NCA Controls, GDPR, CCPA, and PSD2 by implementing robust consent management, data encryption, and audit trails. Scalable and flexible, our CIAM platforms provided the client with a competitive advantage in delivering a seamless and secure digital experience to their customers.

Largest hotel and resort chain in North America

Business challenge

The client wanted to boost customer engagement and revenue while ensuring secure sharing and control of consumer identity data with partner applications. They also required user access control at distributed microservices powering their customer-facing portals and mobile apps. Enabling user access and single sign-on (SSO) to applications from multiple platforms posed another challenge, along with managing customer data in compliance with strict privacy regulations like GDPR and CCPA. Additionally, they needed to protect their brand from violations that could lead to lost customer trust and hefty fines, such as unrestricted backdoor access to Marriott services.

Solution

We established a foundational user journey covering registration, authentication, password recovery, and account management processes for the client. This included developing a plan to manage over 50 million identities and replacing the mainframe security model with a modern access management system. Accessibility assessments were conducted to ensure inclusivity and full-scale deployment-supported microservices architecture using OAuth and OpenID Connect. Consistent registration and password recovery interfaces optimized for diverse devices were developed, along with analytics integration to monitor user interactions and enhance the overall user experience. Decentralized access control solutions for microservices, built for scale and interoperability, were also implemented to meet the client's needs effectively.

Business impact

We delivered advanced, easy-to-use security solutions enhancing guest authentication and user experience with a comprehensive 360-degree view of guests. Compliance with local data protection laws was ensured, allowing the organization to keep pace with the evolving regulatory landscape. The implementation of a unified platform enabled seamless integration with APIs for connecting with all native and third-party applications handling customer data. Additionally, the client gained enhanced customer analytics capabilities, receiving deeper insights into customer behavior and experience. Finally, the scalability of the solution enabled the client to meet unexpected demand and reduce the initial entry threshold through features like social login integration.

Large ministry in Saudi Arabia

Business challenge

The client struggled to streamline user login and registration experiences while ensuring security and compliance. They needed to implement single sign-on functionality to simplify access across multiple applications and eliminate the need for users to remember numerous passwords. Additionally, the client required local and federation services to authenticate government employees, citizens, and users against the Saudi NIC IAM system, integrating profiles from both internal and external repositories. Ensuring session termination on the ministry portal E-Services upon logout from the NIC unified portal posed another challenge. Moreover, building a unified user repository and decoupling users from applications while maintaining security were crucial tasks. Extensive support for various.

Solution

We established a centralized CIAM function with defined policies and API management strategies for the client. We defined and documented the CIAM Identity Data Model and crafted a baseline user experience for seamless interaction. Our team developed a detailed migration plan for applications to transition to the new CIAM platform, outlining success criteria, roles, responsibilities, and reporting structures. We facilitated the onboarding and integration of applications with the CIAM solution, implementing robust risk and adaptive access control measures. The successful production rollout ensured the exposure of the Ministry E-Services to government employees and citizens, bolstered by a secure single sign-on (SSO) solution for mobile applications. Additionally, we managed the migration of data from existing repositories, establishing a unified user repository tailored to the ministry's requirements. Our implementation of Web SSO for identified applications and protection of federated services with an access management solution ensured a streamlined and secure user access experience.

Business impact

We enabled the Ministry to meet the Kingdom's digital transformation and service unification goals for government employees, citizens, and expatriates. By ensuring secure access to digital services and compliance with regulatory standards, we effectively mitigated access risks across both internal and cloud-based applications. We set up a federation with the national identity repository, granting access to nearly one million users, and enhancing accessibility and efficiency. Our solutions facilitated a seamless user experience through the transformation of Government E-Services using advanced technologies, including dynamic data synchronization across various platforms. We strengthened security by implementing a reliable solution to prevent password sharing and providing scalable capabilities for the rapid integration of applications with single sign-on functionality.

Cultural smart city in Saudi Arabia

Business challenge

The client wanted to offer a unified customer experience across all services and products. For this, they needed to implement single sign-on capabilities across multiple channels and identity providers. They aimed to consolidate customer activities from various channels into a single, robust view while ensuring the verification of national ID numbers through Abshir or Yaqeen, along with organization registration via commercial registration details. The client wanted to provide a seamless portal for users to access all amenities and enable individual customers to update personal information securely through OTP verification. These requirements demanded an in-depth solution to streamline customer registration and authentication processes while maintaining data accuracy and security across diverse platforms and channels.

Solution

We started by developing a comprehensive plan for migrating applications to the new CIAM platform and defining success criteria. We then focused on developing an API framework aligned with business needs and managed the assessment, assignment, and integration of APIs. Collaborating closely with application owners, we outlined requirements and created detailed designs tailored to individual applications. Our solutions emphasized providing an interactive user experience with personalized and branded designs, along with robust consent management for user data control. We implemented advanced authentication mechanisms and progressive profiling for registration across different channels, ensuring granular access control. Additionally, we developed a user onboarding process for multifactor authentication (MFA) and integrated selected MFA methods. Integration with security tools, threat intelligence sources, and behavioral biometrics solutions was seamlessly executed, enhancing overall security posture. Finally, we enabled and configured identity analytics capabilities to proactively identify operational issues, while managing the migration of existing data to the new platform from previously identified sources.

Business impact

We managed external identities through a robust CIAM platform, offering end-to-end support for understanding and leveraging limitless customer opportunities. We accelerated time-to-market for business units by providing ready-to-use core CIAM functionalities, enabling quick integration of essential features and allowing the client to focus on enhancing specific offerings. With seamless sign-up processes and easy account management capabilities leveraging multiple identity providers, including social media platforms, we facilitated a streamlined user experience. Our solutions also incorporated interactive and personalized designs, reflecting the client's brand identity across all customer-facing portals. Additionally, we ensured agility and flexibility to technological trends by implementing a CIAM platform capable of keeping up with the latest advancements while maintaining scalability for future needs.

Critical government authority in UAE

Business challenge

The client faced challenges in their access management system, including the need to centrally manage access across a diverse range of applications for external users and entities. They sought to streamline the login experience and implement Single Sign-On to eliminate password fatigue. Additionally, they aimed to consolidate identities from various sources, establish trust between old and new access environments, and provide federation services for authentication against national platforms. They needed to decouple users from applications to enhance security while still ensuring seamless integration, implement coarse-grained authorization based on user groups, and establish a policy store for token issuance and validation.

Solution

We offered a wide range of services to the client, tailored to their specific requirements and operational model. This included adapting the solution architecture to accommodate millions of users across various platforms and geographic locations and facilitating a smooth production rollout of client services to citizens and residents. Security measures were enhanced through the implementation of secure authentication methods and advanced access controls, ensuring robust protection against unauthorized access. A unified user repository was created by migrating data from existing repositories, streamlining identity management processes. Additionally, a single point of entry to the portal was established using Web SSO for identified applications, safeguarding federated services with access management solutions.

Business impact

We facilitated the client's digital transformation and service unification objectives for citizens, expatriates, and government entities. By implementing risk-based authentication, the client reduced fraud by evaluating customer behavior and contextual factors in real time. Additionally, secure access to digital services ensured compliance with regulatory requirements while mitigating access risks across internal and cloud-based applications. The seamless user experience was enhanced by leveraging dynamic data synchronization and preventing password sharing. Federation with the national identity repository further expanded access to millions of users, solidifying the client's digital infrastructure.

About **Aujas Cybersecurity**

Aujas Cybersecurity -An NSEIT Company empowers clients with enhanced security resilience by minimizing the potential for attacks, threats, and risks. We specialize in architecture risk analysis, comprehensive threat modeling, rigorous penetration testing, and secure coding guidelines. By partnering with us, you can strengthen your security defenses and maintain a robust security posture.

For more information, visit us at www.aujas.com or write to us at contact@aujas.com.

Cupertino | Dallas | Jersey City | Ottawa | Riyadh | Dubai | Mumbai | New Delhi | Bangalore

Follow us at: