IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

CIAM for Customers with Varying Levels of Experience

Gomathy Kumarakuruparan

Gomathy Kumarakuruparan
Technical Writer
WSO2

Biography

Gomathy Kumarakuruparan has worked for WSO2 (https://wso2.com/) for just over a year and a half as a Technical Writer. Before she joined WSO2, Gomathy worked as a Business Analyst in Programus Lanka Pvt Ltd. She was responsible for requirement gathering, design-documentations, and demos for development teams and stakeholders.

Gomathy has a bachelor's degree in Electronics and Communication Engineering from The National Institute of Technology, Warangal.

Keywords CIAM, Customer experience, API, Passwords, Security, Integration
Paper type Research

Abstract

Customer identity and access management (CIAM) often gets confused with IAM solutions, however, CIAM solutions are still solving identity access related issues, whereas IAM typically deals with authentication and access within an organization. There are many factors to distinguish when using CIAM solutions and in this article the author looks at the key stages in businesses customer evolution with CIAM, depending on levels of experience, and how to begin a successful path with CIAM.

Introduction

Customer identity and access management (CIAM) is no longer a new concept, but some still confuse it with traditional identity and access management (IAM) solutions[1].

Customer identity and access management (CIAM) solutions enable organizations to securely capture and manage customer identity and profile data, and control customer access to applications and services. As such CIAM solutions are still solving identity and access related issues but the difference is that IAM typically deals with authentication and access within an organization – for example, determining what happens in terms of changes to a user account and privileges when employees join, leave, or move roles within a company. In contrast, CIAM is outward-facing. It is also concerned with joining, moving, and leaving, but more

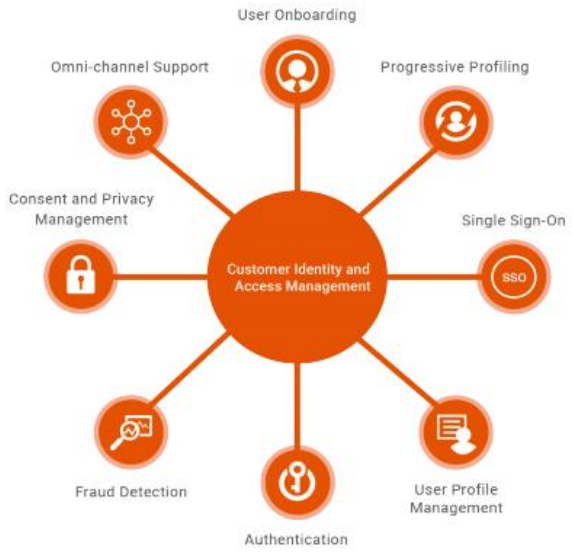
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

usually in the sense of registering for an account, making changes to the account or the relationship (self-service account, consent and preference management), or asking to be removed.

There are many areas to consider when thinking about using a CIAM solution and in this article we look at three key stages in your customer's evolution with CIAM, depending on their level of experience.

Figure 1: Key features of CIAM



Source: WSO2

New CIAM customers

New customers may not be sure what they need from a CIAM solution. Here are six key areas to start them down the right path with CIAM:

1. **Single Sign On** – Logging into hundreds of applications every day is an unnecessary hassle, for example just trying to remember all those credentials is often impossible for customers. Using SSO, the customer is able to experience a smooth sign in since they can access multiple applications using a single log in.

2. **Multi Factor Authentication** – Multi factor authentication (MFA) adds additional evidence to the authentication process and ensures the users who try to access data are the legitimate ones. This is a security enhancement. The most commonly used additional factor in MFA is the one-time password (OTP) usually sent to the customer's registered email or mobile number. Some customers are not very keen on using this since it involves multiple steps.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

3. **Adaptive Authentication** – To remove the tediousness of multi factor authentication, adaptive authentication was introduced. The administrators can decide on how many authentication factors are required, or if MFA is required at all, based on multiple factors like the user's role, risk factor, and IP address.

4. **Social Logins** – SSO made access convenient and secure. However, this experience may need further enhancement. Using social logins, the user can access applications with no registrations required, via social identity providers such as Twitter and Facebook.

5. **Passwordless Authentication** – This is another recent addition to the list of authentication enhancements. Passwords can be risky when exposed to the wrong eyes. It can also be extremely cumbersome to remember and keep an audit of all the passwords people use. With passwordless authentication there is no need to remember a password. Instead, single-factor authentication is all that takes to authenticate the user.

6. **Self-Registration** – Customers do not need a customer care agent to create an account on their behalf. This reduces the waiting time from the customer's end and the overhead from the client's end. The customer care portal should be highly user friendly.

These are all aspects that new CIAM customers should consider at the outset to determine what kind of system they need and where they need to strike the balance between security and a frictionless customer experience.

Intermediate CIAM customers

Customers who have reached an intermediate level have reasonable awareness of CIAM and are looking for ways in which they can attract more customers. To help your customer through this phase you should work with the customer to help them understand what the market trends are and their competitive landscape. More importantly they should know what regulations they are supposed to comply with.

Customer information is worth billions and, if unfairly distributed or carelessly handled, it can lead to harmful breaches which can impact on brand reputation, and cause customer dissatisfaction, not to mention costly fines.

As a solution that handles critical data, any CIAM product is expected to comply with certain regulations that are in place for the sake of customer safety. Data privacy is crucial. An organization cannot collect or handle customer data without their consent. Customers have the right to know what their data is used for at all times, and any CIAM solution should be able to audit this.

If the solution lacks these capabilities, then it is better to pause and get an idea of what others in the sector are doing to satisfy these conditions. Both GDPR and CCPA are two very important regulations that require strict compliance.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Advanced CIAM customers

Once customers trust that their data will be properly safeguarded, it is time to raise the bar and identify the gaps in the market that will make a significant difference. Customers will do their part, identifying and resolving gaps in their respective industries. As a CIAM service provider you will be looking to massively improve your products and services to retain your customers who are working towards exponential growth.

Customer satisfaction is key. This is the stage where you find what you lack, and what you can do to surpass your competitors. Make sure your product supports deployments in on-premises, cloud, and hybrid environments, and the transitions are smooth and speedy. Integration with other products should be a seamless experience.

Most businesses are looking to grow. Therefore, any strategic plan for your product should be made on the assumption that your existing customers will grow significantly and your CIAM solution should be scalable and the performance regularly monitored. Your customers should be able to access all user information with ease. Information in the system should be up-to-date. At the same time access to customer information should be restricted to only those who are authorized, and necessary authentication measures should be taken to confirm the right access.

Congratulations! You've helped your customers with all their CIAM needs. Of course, business doesn't end with just satisfying needs. Now it's time to search for better ways in which you can continue to contribute to the CIAM community. Other aspects to think about are creative ways of managing security audits, centralizing globally available user-based data, automating user reports, securing all the endpoints from brute force attacks and other phishing attempts, and providing easier biometric scanning options as a single-factor, yet a secure, option for signing in. These are just a few examples of what can be done to keep the industry moving forward.

Reference

1 https://wso2.com/identity-and-access-management/