

Overview of Customer Identity and Access Management

By Jharna Roy – ISSA member, Orange County Chapter



This article brings to light the importance of managing a customer user base in today's digital world.

Abstract

This article brings to light the importance of managing a customer user base in today's digital world. The drivers for better managing customer accounts comes from different folds like security, privacy, marketing, regulations, etc. This increases the importance of treating your customers as an entity separate from the traditional workforce. This article does not evaluate any technical products and it is up to the reader to perform appropriate assessments prior to finalizing any technology to meet customer identity needs for his or her company.

In today's digital environment, customers prefer using online portals for the majority of their transactions. This trend has increased post COVID. Customer identity and access management (CIAM) enables the creation of customer identities and managing their access to digital resources in a seamless and secure manner. This user base should be treated outside of your traditional workforce users and their access, as the security and privacy needs for customers are different from those of your internal users.

Why create separate entities for customers and how does it differ from workforce identity?

John Doe likes online shopping and visits your company's site multiple times to view different shopping items. Your company site uses cookies to store user preferences, among other possible related data. Using John's browsing history, marketing emails and brochures are sent to John periodical-

ly. One of the provisions of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR) includes consent management for use of cookies [2] [4]. Additionally, if John creates an account on your site for completing the shopping transaction, you will want to be able to track all his transaction history and securely log him into the site each time—a lot of things to consider that you would not need to worry about for your traditional workforce.

Traditional identity and access management (IAM) systems are focused on enabling enterprise users to access corporate systems. CIAM, a sub-domain of IAM, helps in handling millions of external users across the globe that perform digital transactions. CIAM has its own unique drivers and challenges that require strategies for architecture to scale extensively and to leverage other publicly available identity providers such as social identities.

There are lot of overlapping features between traditional IAM and CIAM when it comes to security such as account provisioning, directory services, password management, etc. [6]. However, the process of managing these pillars of IAM is different for every user base. For instance, customers would prefer to not have to remember passwords for every site visited, whereas internal users do not need to access multiple sites; they only access various applications internal to the organization and you can provide single sign on (SSO) capabilities to those applications. You might want to consider advanced authentication techniques (including risk based) to make logins further secure for the external users, whereas internal user

logins to your applications are being protected using multiple techniques like multi-factor authentication, VPNs, etc. The number of customers in your company will likely exponentially increase, therefore scalability would be something to consider for this user base as opposed to the internal workforce that will not increase to a large extent quickly under normal circumstances.

According to a recent article in 2020 by Forrester, CIAM has started becoming a dedicated solution offering by major IAM vendors [3]. Let us dive deeper into CIAM now and see what drives the need for a CIAM solution and factors that should ideally be considered for this solution.

What are the driving factors for a CIAM solution?

Consider a scenario where you manage your customers without using the CIAM approach. A customer, John Doe, registers on your website and starts shopping. John is prompted to consent to use of cookies and marketing materials and selects decline. Then John logs off. Next time John logs in, he decides to select register again (he has a bad memory and does not remember that he already registered last time on this site) and this time selects to accept cookies and marketing materials. In this instance, how will you track the multiple selections on consent for the same customer without a centralized solution? A similar situation can arise with security of the multiple accounts, wherein, John sets passwords that are not secure, or that he shares with other friends for other websites, introducing various channels for logging into the account.

Typically, a mixture of various business, security, technical, compliance, and marketing factors drive the need for a centralized CIAM solution:

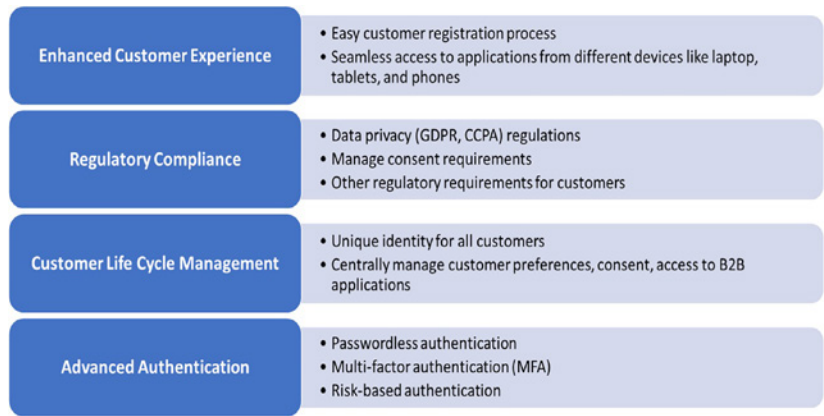


Figure 1 – Areas of focus for CIAM

- Customers would like an easy-to-use solution to register and seamlessly use for purchases across multiple devices
- Multiple regulatory needs across industries (consumer, health care, financial, technology, and others) drive the importance to manage a single identity for a customer
- It becomes imperative to have customers securely log into a company’s portal and access applications without having to remember multiple passwords
- Having a one-stop shop to manage confidential information, marketing preferences, and privacy selections helps in better engaging with customers and managing marketing analytics

Areas of focus

Overall, CIAM can be broken down into four main areas of focus (figure 1). Each is important in its own way and a combination of them would be applicable as a business case for your company’s CIAM program.



Members Join ISSA to:

- Earn CPEs through Conferences and Education
- Network with Industry Leaders
- Advance their Careers
- Attend Chapter Events to Meet Local Colleagues
- Become part of Special Interest Groups (SIGs) that focus on particular topics

Join Today: www.issa.org/join

Regular Membership \$95*
(+ Chapter Dues: \$0-\$35*)

CISO Executive Membership \$995
(Includes Quarterly Forums)

*US Dollars/Year

Customer experience

Why is customer experience important? As we have already seen, many customers now prefer online transactions over traditional in person shopping, more so post COVID.

Continuing our example from above, John Doe likes online shopping but does not like to begin the transaction all over again on his tablet after he has started shopping around on his phone. He also forgets his password pretty frequently. Once John Doe does manage to remember his password and access the same website from his tablet, he is not able to find the registration options on the tablet. John is not very tech

savvy and at one point gives up, logs in to the competitor site, and finds it much easier to create an account and start shopping on that site. He can also hop from his tablet to his new desktop seamlessly and continue the shopping experience.

Think about it, if you have a handful of John Doe-like customers, you could be losing business to your competitors, and this loss will start multiplying in large numbers and revenue could be lost quickly.

End user experience is critical to attract and sustain your customers to manage and grow your business. What does a good customer digital experience consist of?

- **Straightforward user interface:** Have a user interface that is easy to use for various types of customers.
- **Use of already available login IDs:** Provide options for customers to use existing account IDs such as social login accounts.
- **Easy registration process:** Provide options to register across applications used in your company; ideally customers should not have to register for every service or application used.
- **Capability to seamlessly move across devices:** Provide means to continue the transaction and selected options in a shopping cart when a customer switches from one device to another for the same website.



Regulatory compliance

Compliance with various regulations becomes a key factor in driving traditional identity management solutions. Specific regulations in relation to data privacy requirements by country and/or region and/or industry-related regulations are applicable for the customer user base. Let us look at this aspect.

- **Data privacy regulations:** We have heard a lot of noise about GDPR and more recently CCPA. GDPR is applicable to companies having business in Europe [4] and CCPA is for businesses in California [2].

Within each privacy regulation, there are specific requirements for users to consent to use of cookies and receipt of marketing materials used by companies for selling purposes. These specific requirements around both regulations are best handled by using the tactical CIAM concepts and integrating the solution with consent and cookie management tools. The workflows can easily get complex depending on the size of the organization and how deep the consent management decisions need to penetrate your applications in the infrastructure. Its best to consider the holistic picture while designing such a solution.

- **Other industry specific regulations:** Every industry has its own set of regulations. Take, for instance, the cybersecurity requirements for financial services companies laid out by New York state. Multi-factor and risk-based authentication for protection against unauthorized access to non-public information systems is one of the standards laid out [5]. Financial institutions have a huge customer

Using the NIST Cybersecurity Framework to Align your Organization's Risk Management Practices

December 15 @ 1:00 pm - 2:00 pm EST (US)


All organizations are concerned about cybersecurity risk and its impact on their business. This is especially true in the context of digital business strategy and how effectively the organization can manage its risk profile as their business models continue to adapt to meet changing conditions. In this session we will discuss using the NIST Cybersecurity Framework as a vehicle to identify, prioritize, and execute your cybersecurity risk management program, and introduce a road map to help you plan your assessments and actions.

Whether you are a small or medium-sized business or a global enterprise, this approach can help better align cybersecurity into your overall organizational risk management program and provide a vehicle to help you build the adaptive culture you'll need to sustain success.

Moderator: Srinivasan (Mali) Vanamali – Principal, Olympus Infotech

Speakers: Patrick von Schlag – President, Deep Creek Center, Inc.

Generously sponsored by



CLICK HERE TO REGISTER

For more information on these or other webinars:
ISSA.org => [Events](#) => [Web Conferences](#)

base, which means that the company should be compliant for the customer base in addition their own workforce.

As a more recent example, data privacy requirements in the health care sector for COVID-19 contact tracing is still being hashed out and will have implications from the perspective of a customer of the application being used [1].

Similarly, there are compliance needs by other industries, which comes down to how you manage your customer identity and access.

Customer life cycle management

You are already (or at least should be) managing the life cycle of your internal workforce identity and for regulatory applications and have hopefully added a layer of access governance. Similarly, you would want to manage your customer identities before it gets out of control—you certainly do not want to be creating identities and losing track of them (figure 2).

Once a customer has completed registration on your portal, consider that customer to be a single discrete identity in your CIAM solution. Access to applications in your company and single sign on to the applications should be now tied to this identity for the customer. Additionally, marketing preferences, consent management, etc. should be also linked to this identity for the customer.

Let us look at what happens after you have introduced identity creation for each customer. The number of customers will scale as your business expands; therefore, it is best practice to introduce user termination processes to manage the identities better. For instance, John Doe has not logged into his account since the past year. You can de-activate the user in such cases and move to a separate domain in your directory. If Mr. Doe decides to come back and shop a year later, you can set up a few user validation steps to check to see if this is the same user that had been de-activated before, and if the criteria matches, then you can activate the identity again. This will help better manage the storage space. Some examples of checking to see if this is the same John Doe are sending a one-time password to the email address used, asking the user to answer security questions (if you have enabled this option during self-registration) as user verification, etc.

Additionally, it would help to create some checks during the user registration process to see if the same user is trying to register again. You do not want to be creating multiple identities for the same user. Some ways to restrict this would be to check if the email address has been used previously, or checking for a combination of email address, first name, last name, city/location, and phone number to confirm that this is a new user. This also helps better manage consent and marketing preferences by tying them to the same identity for that

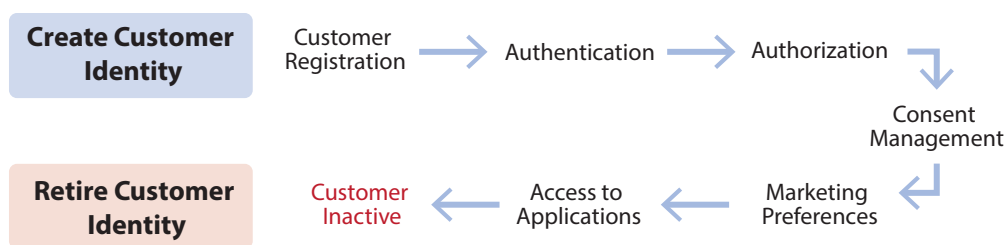


Figure 2 – Customer life cycle management

customer and thereby helps remain compliant with the data privacy regulations.

Advanced authentication

It is not so easy for online portal users to remember their passwords to multiple sites they visit, so for ideal customer experience, you would want to consider using single sign on for all the applications within your organization and passwordless authentication techniques. Many companies therefore are now opting for use of a one-time password (OTP) to log their customers in by sending a one-time code as a text message or email. There are other passwordless authentication techniques that you can assess and pick one that best works for you.

Additionally, with customers sometimes spread globally, you would want to add multiple factors of authentication taking various factors into consideration such as change in geographical location, device used, etc.

Where the executive support meets common ground

C-level executives have objectives that lead to a common CIAM solution. The chief information security officer would ideally like to differentiate between customers and enterprise users and separate the directories and applications used by each user population. Additionally, adding extra measures for customer access helps in mitigating risks to the enterprise environment.

The data privacy officer is motivated to fulfill compliance needs arising from privacy regulations (CCPA, GDPR, etc.). The chief marketing officer would want to determine how marketing data is stored explicitly for each customer and be leveraged to run analytics and sell products.

All these drivers align with the CIO's goals for a company and therefore this lays a common ground for planning and initiating a CIAM program.

Conclusion

It is to everyone's interest to have a strategic and holistic approach to deriving a solution. Most successful programs start with defining a well laid out plan for implementation with achievable goals and milestones. When a company has continued focus on the drivers and initiatives for a CIAM program, rapid progress on the solution can be made.

References

1. Alder, Steve, "Privacy Must Come First with COVID-19 Contact Tracing Technology, Warn Scientists," HIPAA Journal, <https://www.hipaajournal.com/privacy-must-come-first-with-covid-19-contact-tracing-technology-warn-scientists/>.
2. Chau, E. and Hertzberg, Robert, "AB-375 Privacy: Personal Information: Businesses" (CCPA), California Consumer Privacy Act of 2018," California Legislative Information (June 2018) – https://leginfo.ca.gov/faces/bill-TextClient.xhtml?bill_id=201720180AB375.
3. Cser, Andras. "The Forrester Wave: Customer Identity and Access Management, Q4 2020," Forrester, October 8, 2020 – <https://reprints2.forrester.com/#/assets/2/935/RES159083/report>.
4. European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016" (GDPR), Official Journal of the European Union (May 2016) – <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>.
5. New York State Department of Financial Services 23 NY-CRR 500, "Cybersecurity Requirements for Financial Services Companies – <https://www.dfs.ny.gov/system/files/documents/2019/02/dfsrf500txt.pdf>.
6. Ruddy, Rudy. "Key Features for Customer Identity and Access Management," Gartner February 20, 2019 – <https://www.gartner.com/en/documents/3902470/key-features-for-customer-identity-and-access-management>.

About the Author

Jharna Roy, CISSP, is a cyber leader with 15 years of experience solving clients' most complex problems and advising on enterprise-wide strategic cyber initiatives. She is a specialist in identity and access management (IAM) and has led multiple large and complex multi-year IAM programs for companies in various industries including financial, health care, and consumer. Jharna can be reached at roy002@gmail.com.



Thank You, Thom Barrie: 15 Years with the ISSA Journal

Continued from [page 6](#)

learned how to work with others towards a common goal and the camaraderie of working in a large and focused organization. The closest I've had since is being associated with ISSA. Subsequent jobs leading me to the *Journal* have been commercial printer, graphic designer, desktop publisher, high school English teacher [my year of living dangerously], and freelance designer.

What do you consider your most important career decisions that led you to your role as editor?

Saying yes, learning new tasks, wearing new hats. In the early days of the web, a publishing client asked if I could make a website. I was just starting with HTML and JavaScript, but said no. I didn't feel I had the chops yet. A few months later I rectified my error, and my web development career took off. Highlights of that life were developing a website and content management system with PHP and XML for a school district and a website with a seamlessly integrated shopping cart for a brick and mortar custom table and dinnerware business.

I started with the *Journal* when Jim Reavis was executive director. I had been doing some graphics work for an associate of his who asked if I could lay out the *Journal*. I said "absolutely, but it'll have to wait until next issue." And from there the journey began. I started with production, moved on to copy editing, then took on the role of editor with the Editorial Advisory Board (EAB) peer-reviewing the articles. Ultimately, I became the *ISSA Journal*.

Along the way

In what ways has the ISSA Journal impacted readers over the years?

The feedback I have received has always been positive. Most folks say they read and enjoy the *Journal*, though sometimes format proved a stickler. I was thrilled when recently one chapter leader remarked, "The *Journal* has been an important part in my professional life/career and no other publication compares."

Conferences have presented a conducive and captive audience for receiving feedback. I have enjoyed walking around and talking with whomever acquiesces. It's especially gratifying to run into my authors face to face.

What changes in media formats or delivery have you experienced over the years of producing the Journal?

When I started in 2006, we were printing and mailing the *Journal* monthly. In March 2008, we introduced the Bluetoad digital magazine format that we are all familiar with today. It wasn't an either/or at the time; we were still printing and mailing monthly. Then we made the switch to all digital with one proposed printed issue per year that was to be a "best of" for the year. But readers wanted the best of both worlds, so we ended up printing and mailing quarterly, which is what we do today.

By that time, mobile was widely adopted, and we wanted to have the *Journal* become more phone/tablet friendly. Since, Bluetoad was a Flash rendering and not mobile friendly, in May 2013, I started making ePub/Mobi versions, which are basically packaged websites. Benefits are that images are inline, text can be made larger or smaller, and you can take it with you.

The ePub/Mobi version was a hit, at least for two people. Kevin Richards, ISSA president at the time of unveiling, thanked