Expanding the purview of Consumer-facing Identity and Access Management

The advent of General Data Privacy Regulation and its impact worldwide a strict regulatory environment is shaping up. Businesses need a close look at Consumer/customer facing IAM practices

Avancer
Simplified IT Security

Executive Summary

Putting in place the safeguards associated with consumer/customer data are becoming crucial for business to operate. The most recent example is General Data Protection Regulation (GDPR) deadline – it somewhat conveys that the consumers have a say in information demanded by businesses. With technology boom, traditional services delivery model has shifted to digital process. With this, the role of a customer has also undergone transformation from being just a physical entity to consumers interacting with a business remotely to gather insights & use an array of services. This has mandated businesses to manage, govern and secure customers' access to systems and data, while ensuring unflinching digital experience. This experience consists of techniques, processes and tools to manages users' digital omnichannel interactions, and packed with various aspects of identity and access management for consumers, widely known as Customer Identity and Access Management (CIAM). CIAM is a technological solution that provides a mechanism to store customer profile data, authentication services, along with helping to manages identities and securing data across all channels - digital and non-digital. CIAM platforms offered by various vendors include Saas, Paas, on site deployment as well as cloud-based deployment according to the unique requirements of each firm. It acts as a catalyst to connect marketing, business and security teams, and forms an essential part of B2B interactions.

The market value of CIAM is expected to grow to US$ 18.3 billion market by 2019, according to a Markets and Markets Identity and Access Management Report. Data production is estimated to be 44 times greater in 2020 as compared to 2009. In addition, experts estimate a 4,300 percent increase in annual data generation by 2020, according to a CSC report's projection.

Businesses are increasingly seeking insights related to data created on digital platforms with web based consumer engagement. These trends usher a new era of consumer-managed data and driven through a framework of personal identity and data management. All this will be addressed while addressing tools, technologies, responsibilities and requirements that customer insights (CI) will incorporate to build trusted relationships with users. Given the business dynamics in digital arena, the times to come will see CIAM will act as a catalyst to connect marketing, business and security teams, forming an essential part of B2B or B2C interactions.

Thanks,

Rajesh Mittal
CTO, Avancer Corporation

Simplified IT Security

Table of Contents

Section 1 Introduction to Consumer Identity and Access Management (CIAM)..... 4

Understanding Regulations to support adoption of CIAM 5

Section 2 CIAM Lifecycle 8

Customer IAM - a crucial component for digital customer experience 8

Section 3 Solution, Integration and Components 9

Concept of CIAM Integration 9

Component of CIAM 10

#1 Customer analytics to help in business growth 10

#2 Big Data Management that goes beyond 'Brick and Mortar' templates..... 11

#3 Streamlining Processes for Secured User Experience 11

Section 4 How Avancer can add value to your CIAM initiatives 12

Simplified IT Security

Section 1 Introduction to Consumer Identity and Access Management (CIAM)

Consumers' digital interaction with business is a source of insights for businesses, and it is but natural for businesses to capture consumer insights. Consumer-managed data, driven through a framework of personal identity and sensitive information needs to be safeguarded. Identity and Access Management (IAM) has its services focused on employee use cases, while outward-facing consumer centric Identity Management (including identification, authentication and authorization of the customers, their devices and organizations) needs equal attention.

Consumer or Customer Identity and Access Management (CIAM) is a solution to facilitate storing, processing, monitoring and managing customer profile data, authentication services, along with helping to manages identities and securing data across all channels - digital and non-digital. Given the business dynamics in digital arena, CIAM acts as a catalyst to connect marketing, business and security teams, and forms an essential part of B2B interactions.

The regulatory paradigm around consumer driven interactions has run parallelly with expansion of digitization. Paving way for creating systems and processes for CIAM-enabled digital businesses, **Payment Card Industry Data Security Standard (PCI DSS)** recognizes the threats from the industry recognizes a standard for digital data transfer for outward facing transactions. This is just one of the regulations for e-commerce transactions, and the future will see incremental revisions and newer regulations to cover threats in the payment landscape, user data to help businesses use and maintain standard as a business practice.

General Data Privacy Regulation (GDPR) aims to do just that – enforcing businesses to take a step towards protecting consumer information by making use of monitoring technologies and integrating checkpoints. This mandates businesses to manage, govern and secure customers' access to systems and data, while ensuring unflinching digital experience. European Union has enforced the GDPR regulation on all entities that capture user data, and defaulters will be penalized after the deadline of May 25, 2018.

CIAM recognizes that the consumer interaction with services from digital-channels is mostly online. Thus, while developing IAM capabilities, the consumer must be the focal-point along with user experience, security and scalability rather than technology, standards and products. The process facilitated via CIAM connects backend system with consumer community connecting with Enterprise IT System through their individual (or social account) login must be seamless and secure. Such functionality is becoming omnipresent and is essential for marketing, banking, e-commerce, online transactions and so on. This needs a step forward in IAM practices for consumers.

Worldwide, the top performing industry remains IT services where almost two-thirds of organizations (61.3%) achieved full compliance to PCC DSI. It is followed by financial services (59.1%), hospitality (50.0%) and retail (42.9%). Based on full compliance, retail organizations demonstrated the lowest compliance sustainability across all key industries.

Understanding Regulations to support adoption of CIAM

PCI DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. PCI DSS is a set of security standards designed to ensure that all companies that accept process, store or transmit credit card information maintain a secure environment.

55.4% of organizations achieved 100% compliance at interim PCI DSS validation in 2016. This is a 7.0 percentage point increase from 2015 (48.4%), and the fifth consecutive rise— though increases have markedly slowed in the last few years.

Source: Verizon 2017 Payment Security Report

The standard was agreed by major card brands as a common, consistent and secure process for minimum level of protection to safeguard card data and customers. The PCI DSS specifies a list of mandatory requirements of which 6 control objectives are:

- Build and maintain a high-security network
- Protection of cardholder information
- Maintenance of vulnerability management program
- Secure access control measures
- Restricting of physical access to cardholder data
- Regular monitoring & testing of networks and maintaining an information security policy

The requirements introduced in PCI DSS 3.2 are requirements, effective 1 February 2018. PCI DSS 3.2 includes clarifications to existing requirements, new or evolving requirements, and additional guidance. While PCI DSS compliance looks at the biggest payment security challenges facing organizations, the introduction of deadline driven GDPR regulations across borders can impact businesses, and command high penalization costs. E-Commerce Security PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security.

- **Secure network for CC processing**
- **Secure card holder data**
- **Access control measures**

Despite advances in the state of global compliance, hackers continue to pose a great threat. With no slowdown in sight, the effectiveness of the PCI Security standards and PCI DSS, continues to be the most important topic. The purview of information possessed by business houses across consumer-facing businesses has reached a new benchmark with GDPR - Failure to comply will result in fines up to 4% of annual global revenue or Euro 20 million, whichever is greater. In addition to forming swift checks - any rival poaching data that create 'data passports' for consumers to collect personal data from multiple sources needs to be checked and deleted. That's the strategic bit of it – at the technological level – it needs to clear look at processes, regulations and possible technical solution.

Regulatory Environment around CIAM Solutions

Many regulations are in place that requires organizations to harness IAM technology, violations of regulatory compliance often result in harsh penalization. Some of the most important ones with their corresponding solutions are listed below for your ready reference:

Regulation	Industries	Requirements	IAM Solutions
Payment Card Industry Data Security Standard (PCI DSS)	All industries that processes payment card transactions	**Focus – E-Commerce Security** PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security, including secure network, secure card holder data and proper access control measures	**Access Management** – Centralized authentication that ensures single id for each user, Password Management **Identity Management**: Provisioning and role polices to set access control
Sarbanes–Oxley Act of 2002 (SOX)	Finance Banking Insurance	**Focus – Internal controls on financial reporting** – **Section 302**: Companies must safeguard their data responsibly to ensure that financial reports are not based upon faulty, tampered or data that may be highly inaccurate. – **Section 404**: Safeguards listed in 302 are verifiable by independent auditors	**Access Management** – Centralized authentication, Single Sign-On (SSO), **Identity Management** – Role based policies for account provisioning, de-provisioning & approval process **Privilege Identity/Access Management (PAM/PIM)** – Enforce tighter security rules and role based policies for privilege accounts **IAM Auditing –** Capture all user actions and system responses
Gramm-Leach-Bliley Act (GLB)	All financial institutions	**Focus – Information Security** The Gramm-Leach-Bliley Financial Modernization Act enacted in 1999 mandates all financial institutions to safeguard customer data from internal & external threats. Key requirements are to protect and maintain confidentiality information of customers and **protection against any threats to customer information**	**Privilege Identity/Access Management (PAM/PIM)** – Enforce tighter security rules and role based policies for privilege accounts
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare, Lifesciences	**Focus – User Access Rights** Health Insurance Portability and Accountability Act, HIPAA ensures-National standards to protect the privacy of personal health information. Federal privacy protections for individually identifiable health information. That it is easier for people to keep health insurance, protect the confidentiality and security of healthcare information. .	**Access Management** – Federation, Mobile Solutions, SSO, Password Self Service **Identity Management** – Role based policies for account provisioning and de-provisioning

Regulation	Industry(ies)	Requirements	IAM Solutions
Family Educational Rights and Privacy Act of 1974 (FERPA)	Education	**Focus – Access Rights** FERPA is a Federal law that – Governs access to educational records maintained by educational institution and ensures students' rights to privacy – Applies to all elementary, secondary, and postsecondary institutions receiving federal funds	**Access Management**: Identities for teachers, students, parents and other communities to securely login and maintain education records. Federation access for intercampus domains
North-American Electric Reliability Corporation (NERC)	Energy/Utilities sector	**Focus – Access Governance** NERC mandates the core technical requirements for cyber security as outlined in NERC CIP Standards 002-009. It requires accountability through: – Authentication, access control, delegation, separation of duties – Continuous monitoring and reporting of electronic access to critical infrastructure.	**Access Management** – Centralized authentication, Single Sign-On (SSO) **Identity Management**– Role based policies for account provisioning, de-provisioning **Privilege Identity/Access Management (PAM/PIM)** – Enforce tighter security rules and role based policies for privilege accounts **IAM Auditing** **–** Capture all user actions and system responses
General Data Protection Regulation (GDPR)	All Consumer / Customer Data procurement related industries	**Focus – Data Security** GDPR standardizes processing and movement of EU citizens' personal data	**Consumer/Customer IAM capability** **Access Controls** **Audits**

Some of the other compliances that will require IAM technology include FDA 21 CFR Part 11; The Health Information Technology for Economic and Clinical Health Act (HITECH) Act; ISO 27001; Federal Information Security Management Act (FISMA); Freedom of Information Act (FOIA); Federal Information Processing Standards (FIPS 200); National Institute of Standards Technology Special Publication (NIST SP 800-53).

Section 2 CIAM Lifecycle

As the need to secure and provide privacy is of utmost importance while designing a CIAM product, customer ecosystem forms a very important aspect of CIAM. It is a solution that provides authentication services, manages identities and stores customer profile data for businesses worldwide. CIAM is becoming a way of life as far as online transactions–financial or social–are concerned. It is a new direction for the technological boom to continue. IAM capabilities aligned data analytics help in reporting, gathering access information of users and help businesses in making strategic decisions – while keeping checks and balances in place. While consumers expect personalized services, the brands want to make inroads to learn, identify, store and utilize the consumer information to its maximum, for providing impressionable consumer experience and gaining brand loyalty. Thus, shaping the platform's ecosystem is nodal to integrate consumers, services and the market.

Customer IAM - a crucial component for digital customer experience

Companies require customer insights to create newer products and services that help them in increasing and sustaining brand loyalty. **The market value of CIAM is expected to be US$ 18.3 billion market in 2019, according to a Markets and Markets Identity and Access Management Report.** In terms of monitoring consumers, traditionally the marketing team was expected to manage customer data, but with the expansion of a complex IT environment and multiple interaction points.

A broad view of CIAM Lifecycle can be recorded in the following points:

- The lifecycle of CIAM mechanism is to record customer's data.
- Customer's registration (by way of filling forms etc.), authentication (by way of confirming via mail, OTP, etc.) along with their identity management and connection to internal as well as third-party applications
- Initiating business and consumers onboarding to utilize digital properties via social logins or traditional means

Consumers also expect to receive instant insights on their digital investments and customized services. Digital touchpoints are expected to minimize on response time as poorly managed time adds on to customer attrition rates.

Section 3 Solution, Integration and Components

The consumer-centric IAM becomes a key component of a real-time Security Intelligence strategy and must also be seen to strengthen fighting outward facing threat- paradigm. IAM becomes a common denominator for determining appropriate access to resources, regardless of where they reside (cloud, on-premise) or its mode of access.

While it is imperative to understand consumers' requirements, businesses need to integrate various security and privacy requirements, which would further boost the confidence of the consumer in conducting online activity in a platform. With the integration of CIAM, companies can strike an appropriate balance between security and providing a user-friendly platform.

With the integration of CIAM, businesses are able to better utilize their customers' identities and turn that information into action by synchronizing profile data with their email marketing system, CMS, web analytics, targeting, CRM, e-commerce and other marketing tools.

Concept of CIAM Integration

To safeguard the data, adaptive authentication measures should be adopted as being done by almost all online banking services. The adaptive authentication mechanism through its multi-factor channel offers better security and user experience while reducing dependency on passwords for securing both authentication and authorization.

The 3 P's—Profile Management, Preference Management and Privacy Management—as per a Forrester report are very important and are essential to conclude any CIAM solution to be declared successful. Achieving a customer's loyalty towards the brand thus becomes a parameter for customer satisfaction. Privacy Management is one of the 3 P's.

CIAM needs to sensitize consumes' to decide how and when their personal details is used. Multi factor authentication is advocated through CIAM solutions to enhance customer's personal data security. Thus, it is imperative for Security &Risks (S&R) to develop security controls improves customer experience while safeguarding its clients from fraudulent and malicious activities.

Gartner in a synopsis to improve customer experience gave the below pointers for planning a solution and its implementation:

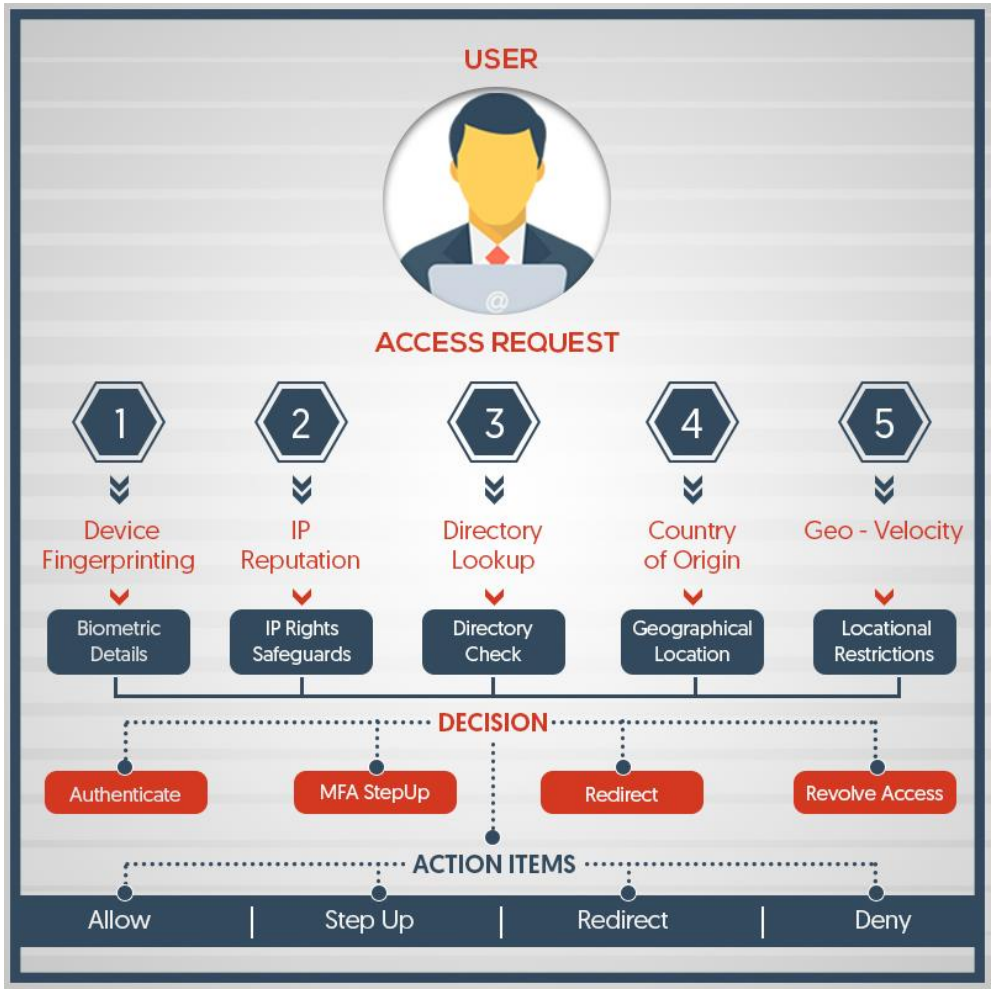
- Act on feedback, and tell staff and customers
- Design the ideal customer experience
- Flexibility
- Design processes from the outside in
- Be open and collaborative
- Personalize products, services, prices, offers and interactions
- Alter attitudes and employee behavior

Component of CIAM

#1 Customer analytics to help in business growth

CIAM solutions help build a bridge between marketing and line-of-business owners. Taking a notch up from enterprise IT borders and limitations, the CIAM solutions reaches to customers or consumers. It delivers consolidated reports and analytics around user demographics, social registration and login data, behavioral data and revenue activity (purchases, purchase amounts, and ad clicks) allowing organizations to gain a 360-degree view of the customer that can drive incremental revenue. CIAM platforms offered by various vendors include SaaS, PaaS, on site deployment as well as cloud-based deployment according to the unique requirements of each firm. Industry experts ask for reimagining IAM in consumer driven formats to accelerate digital business by focusing on following issues, such as:

- Study the impact of cloud, mobility, social media and big data on consumers' digital interactions,



Access Request for CIAM compliant user flow brings greater controls smooth on-boaring while enabling swift user security checks

Avancer
Simplified IT Security

- Analyzing Where and How IAM capabilities for consumer facing platforms can solve business problems and bring insights, and
- Follow best practices of make access processes accountable for transparent business operations

#2 Big Data Management that goes beyond 'Brick and Mortar' templates

Organizations are using big data to get insights related to customers, their behavior on the digital platforms and adapt business processes based on insights gathered. Big Data technologies were invented to store and process data into "Smart" information. A disturbing aspect of these technologies is that it aims for data processing capabilities rather than security and compliance. Big Data technologies need to be managed and secured in the same way as the other components in the IT infrastructure like CIAM. Enterprises want to collect, store and analyze consumer to create additional business opportunities and increase brand loyalty. Many establishments are finding it imperative to provide better digital experiences by gathering beyond templatized 'brick and mortar' information.

Consumers are interacting with online services through various means, including web browser, mobile browser, and mobile app, and have come to expect a consistent experience across all channels. While they bring great insights - security, privacy and managing identities need to be aligned to them.

#3 Streamlining Processes for Secured User Experience

A CIAM solution helps to gain a customer's confidence and loyalty only if the latter is satisfied with the security aspect. It also keeps customers satisfied while simultaneously delivering actionable data to the business in a risk and privacy sensitive manner. Employees and contractors also need to work on customer records — so CIAM connects digital operational excellence and digital customer experience. The entire process of logging in by enabling MFA, SSO or Adaptive Authentication plays a vital role as it takes a group of variables and develops a risk score—using techniques like device registration, finger print, OTP, location, behavioral analysis—based on certain rules outlined by the security team. Each access request from the consumer is thus evaluated and put through a series of checks before they are either granted or denied access.

Section 4 How Avancer can add value to your CIAM initiatives

Typically, IAM solutions can't handle customer IAM requirements as the scope of control goes beyond enterprise IT borders. This includes concerns regarding security, seamless experiences and the ability to support digital services. There is a need to facilitate multiple engagement channels at massive scale. **The basis for CIAM support at Avancer is keeping in perspective the fundamental difference between customers and employees: your customers have a choice. It is crucial to put together the process specific requirements for the right access, streamlined and secured user experience.**

CIAM encompasses a range of different capabilities to help organizations deliver the right balance of strong security and a seamless experience, helping organizations turn their customer identity data into a competitive advantage. The impact and importance of CIAM vary for companies based on their size, customer-base requirements or industry—but the industry research and a deeper analysis brings forth efficiency (in terms of client service and operational services) and significant cost savings — reducing the costs associated with the Support Desk, implementation, authentication processes, application development and maintenance.

The best solution can be provided only after understanding the client's need and priority, which can help in analyzing company's priorities to determine where Identity Management fits as part of a larger Digital Strategy. Consumers are increasingly aware of the data they create as they move about the Web and engage with businesses and with each other. As per a Forrester report, these trends will usher in a new era of consumer-managed data, and that a new framework — personal identity and data management (PIDM) — will drive how, when, and why consumers share their data with organizations. The PIDM playbook addresses the tools, technologies, responsibilities, and requirements that Customer Insights (CI) professionals will need to adopt to build trusted relationships and ensure success in a new era of consumer-managed data.

An array of authentication methods in form of non-password-based such as biometrics, improved predictive customer analytics, and the ability to maintain data compliance with regulations. **In terms of future course of action related to CIAM capabilities, it is imperative to accommodate the requirements of The Internet of Things (IoT).** Given the dynamics of devices and users, creating a system to support magnanimous identities is crucial. Going by the trend, Avancer has brought insights from the business world to CIAM. The integration of CIAM solutions is aimed at safeguarding businesses, to put in place a policy compliant security system and enable a breach-free CIAM mechanism.

About Avancer Corporation

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, it has over a decade's expertise in the field of Identity and Access Governance, IT Security and Big Data Management. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products and services focused in IAM Technology. Our services ranges from full term project life-cycle implementation to tailor made short-haul projects including software procurement, architectural advisement, design and development through deployment, administration and training.

For more on Avancer Corporation, visit https://www.avancercorp.com or email at info@avancercorp.com

CONSULT EXPERTS AT AVANCER FOR MORE

REQUEST EXPERT CONSULTATION ›

Avancer
Simplified IT Security