

White Paper

# CIAM: Trusted Online Relationships

Customer Identity and Access Management for Government Services



**P**ORTAGE  
cybertech

🌐 [portagecybertech.com](https://portagecybertech.com)  
✉ [info@portagecybertech.com](mailto:info@portagecybertech.com)

# CIAM: Trusted Online Relationships

## Customer Identity and Access Management for Government Services

### What is CIAM?

Customer Identity Access Management (CIAM) refers to tools and processes designed to ensure private, secure, and frictionless interactions between customers and digital service providers. CIAM solutions provide traditional identity and access management (IAM) functions – identity management, user authentication, access permissions – that address the challenges of establishing security and privacy for users that exist outside a service provider's direct control and IT boundaries.

### Customer? Client? Citizen?

CIAM solutions do more than support customers in online retail transactions. "Customers" may also refer to clients that receive professional services (e.g., law firms engaged in legal transactions). "Customers" may also refer to citizens interacting with online public services (e.g., online services provided by a municipal, provincial/state, or national government).

### What is the difference between CIAM and traditional IAM?

Both CIAM and IAM solutions help organizations provide "the right person with the right access to the right resources at the right time." Traditional IAM solutions focus on users that are known to the organization and work within the organization's IT environment (i.e., employees). CIAM solutions focus on supporting (potentially) millions of users that are unknown to the organization (at least initially), who often use external digital identities (e.g., social media credentials), and whose devices, locations, etc. vary and change frequently. These users have little patience for technical hindrances and the unauthorized use of personal information.

For these reasons, CIAM solutions go beyond traditional IAM to include enhanced privacy protections, consent management, anti-fraud mechanisms, and dynamic policies to fit the varied circumstances of thousands of users. CIAM emphasizes self-service, profile management, omnichannel support, and digital experiences that are streamlined and personalized.

### Why is this difference important?

Customers want quick, easy, and seamless access to digital services. They want personalized experiences, but not at the loss of privacy and control over personal information. At the same time, service providers need to secure their networks and protect customer data while complying with consumer protection regulations like Canada's Privacy Act and similar provincial legislation, the EU's General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

Traditional IAM is not optimized to provide these capabilities. A good CIAM solution is designed to foster trusted online relationships with customers that are based on a proven identity, openness about data collection and use, and an appropriate balance between security and excellent experiences that reflect user needs and preferences.

# Key CIAM Capabilities: Technical Considerations

Establishing the identity of who we interact with online and building out those interactions into trusted relationships supports the delivery of high-value digital services that exceed customer needs and expectations. CIAM solutions support this goal by providing key capabilities that enable online customer engagement. The following sections identify the key capabilities of CIAM solutions and how CitizenOne™ delivers them.

## Core Capabilities: Identity Management

### Registration and account provisioning

Customers must be able to register themselves with the organization's digital services quickly and easily to avoid frustration and abandoned registrations. Collecting only minimally required personal information expedites the initial registration, reducing time and user aggravation.

#### CitizenOne™ capabilities

- Account registration through a simple process that captures only core information (i.e., username, email address and password).
- Account verification through a simple email verification process.
- Once logged in, users can find and on-board to all government services using a single, intuitive access point.

### Identity proofing

The process by which an organization uses personal information and identity evidence to connect a digital identity to a real person. This is critical to protecting sensitive and high-value transactions (e.g., financial services, legal services, medical services, government grants and benefits).

#### CitizenOne™ capabilities

- Integration of third-party identity providers and verification services.
- Employment of zero-trust architecture best practices, validation of user data against any authoritative source outside CitizenOne™.
- Rules configuration supporting stepped-up ID verification and authentication requirements for enrolling users to services requiring higher levels of identity assurance.

### Progressive disclosure (profiling)

A technique for collecting customer information over time. Rather than overwhelming customers with lengthy forms at registration, progressive profiling allows organizations to incrementally collect information about customers as they interact with its digital services and build online relationships. Detailed information is only collected when relevant to a user's activities, reducing distrust.

#### CitizenOne™ capabilities

- Using the service card construct, which serves as the access point to a given online service, customers are only required to disclose personal information in context of a specific service and the related task they are trying to perform. With this approach, customers are always in control of which personal information they share and when.



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Self-serve profile management</b></p> <p>Customers must be able to modify, add, or delete key personal information without relying on support staff. Ideally, this capability extends to deleting an account and all associated information where applicable.</p> <p>This provides customers control over their data while reducing support and risks associated with bad data.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <p><b>CitizenOne™ capabilities</b></p> <ul style="list-style-type: none"> <li>• Maintain their name, email address, phone number and address in their profile.</li> <li>• Change their password, see what active sessions and devices they're signed in on and consult an activity log of all account activity.</li> <li>• Set their Notification preferences, see a list of all notifications in the UI, and set UI language preferences.</li> <li>• Delete their account – with a pre-configured grace period should they wish to restore it.</li> <li>• CitizenOne™ is fully accessible and mobile responsive, adhering to the latest WCAG conformance criteria.</li> </ul>                                                                                                                                              |
| <p><b>Identity repository consolidation</b></p> <p>Consolidating multiple repositories into one source of identity and profile information is necessary to provide seamless authentication, access, and consistent user experiences across the organization's digital services. The organization is better able to manage customer identities and personal information across business lines.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p><b>CitizenOne™ capabilities</b></p> <ul style="list-style-type: none"> <li>• While it supports the integration of third-party identity providers (IDPs), CitizenOne™ also frequently plays the role of the IDP by providing a single source of truth for user profiles that unlock seamless authentication and access for customers and act as enablers of rich, personalised user experience as customers consume additional digital services.</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| <p><b>Bring your own identity (BYOI)</b></p> <p>BYOI is a type of federated identity where access to one organization's services is granted using identity credentials issued by a trusted third-party. Essentially, customers access services by re-using identity credentials they already own instead of creating new ones. The third-party is typically a social media or IT company (e.g., Facebook, Google, Apple). However, stronger identities (i.e., providing greater assurance that the user is who they claim to be) issued by governments and ID verification businesses are emerging. BYOI enhances customer experience by streamlining registration processes and reducing the number of identities to manage. For small organizations, it reduces the burden of issuing and managing separate identity credentials. BYOI can improve security and privacy by reducing the amount of personal information the service provider collects.</p> | <p><b>CitizenOne™ capabilities</b></p> <ul style="list-style-type: none"> <li>• Interoperability is at the heart of CitizenOne™. Leveraging open standards and an API-first approach to integration, our solution has pre-built integration to over 300 IDPs and SP's leveraging mature, open-source libraries to extend and augment the choice of digital identities available to customers.</li> <li>• The solution supports integration to third-party IDPs and applications via self-service configuration in the administration application.</li> </ul> <div data-bbox="673 1570 1503 1896"> <p><b>BYOI reduces the burden of issuing &amp; managing separate identity credentials. It also improves security and privacy by reducing the amount of personal information the service provider collects.</b></p> </div> |

# Core Capabilities: Authentication & Authorization

| Multi-factor authentication (MFA)                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CitizenOne™ capabilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>A method of confirming user identity by using multiple factors when accessing protected resources. Factors include usernames, passwords, access codes, security questions, and biometrics. MFA increases assurance that users are who they claim to be while making it difficult for attackers to gain access using a single factor (e.g., they know the user's password but do not have a code sent to the user's registered phone number).</p>                                           | <ul style="list-style-type: none"><li>• MFA in CitizenOne™ can be enforced at log-in and, for higher identity assurance use cases, in context during on-boarding to individual service cards.</li><li>• MFA options at log-in include:<ul style="list-style-type: none"><li>• Text, email, authenticator app, and voice (roadmap item).</li></ul></li><li>• MFA options at service on-boarding include sufficient factors to balance the user experience and security requirements including, but not limited to:<ul style="list-style-type: none"><li>• Access codes received via the channels mentioned above, or via email.</li><li>• Identifiers or data from existing identity documents (e.g., driver's license).</li><li>• Biometrics (roadmap item).</li></ul></li></ul> |
| Adaptive authentication                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | CitizenOne™ capabilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>MFA method that changes factors according to the situation. If the system detects unexpected or odd details like the location, type of device, time of day, or transaction type, it prompts users for additional authentication factors. This makes it harder for attackers to gain access with compromised factors and improves fraud detection. It also streamlines the experience for users engaging in low-risk activities, saving additional factors for more sensitive services.</p> | <ul style="list-style-type: none"><li>• The system tracks adaptive authentication data points (e.g., user device OS, browser/agent, and IP address) along with event types and timestamps. Users are notified of any unusual logins to their account and provided with this information.</li><li>• Risk-based authentication – the implementation of logic to score user situations and assign a risk profile. This profile drives an adaptive authentication workflow or experience (roadmap item).</li></ul>                                                                                                                                                                                                                                                                   |



MFA in CitizenOne™ can be enforced at log-in and, for higher identity assurance use cases, in context during on-boarding to individual service cards.

## Authorization (Access) control

A method for determining the resources a user can access and which actions can be performed (i.e., read, modify, delete). For digital services authorization, it is tied to authentication to confirm user identity and grant the appropriate access. Authorization controls ensure personal information remains confidential. It also helps limit the damage attackers may inflict by limiting their ability to access multiple protected resources or move freely from one target to another on the network.

A key capability of CIAM solutions is the ability to allow customers to manage delegates. Delegates are authorized by users to access resources and perform actions on their behalf.

## CitizenOne™ capabilities

- For customer-facing services, CitizenOne™ uses a model of claims and credential-based access control.
- Access policies are established using the solution's rules engine. API end-point configuration supports integration with external data sources needed to verify claims made by the user.
- This process produces a set of verified claims and credentials that are used to prove user identity for both initial and continuous validation, authorizing access to protected resources and services.
- Once users prove their identity by passing an access rule, where they can go next is dictated by the "actions" configured in the UI (i.e., which areas of a protected resource the service provider wants to point them towards). It is intentionally designed to be a highly curated user experience.
- Delegation of authority also allows users to add delegates and grant them permissions to access resources and perform actions on their behalf.
- System administration tasks are governed by roles and permissions in a classic role-based access control (RBAC) model.

## Single sign-on (SSO)

A method for allowing users to access multiple applications without re-authenticating each time (i.e., one username and password accesses multiple applications). Customers often interact with multiple back-end systems or want consolidated information from multiple systems (i.e., a dashboard or portal). SSO reduces the irritation and security issues of managing multiple sign-in credentials to provide this access.

SSO allows larger organizations with multiple brands or service units to provide better, seamless services to a shared customer.

## CitizenOne™ capabilities

- CitizenOne™ supports open, standards-based protocols for authentication and authorization for protected resources i.e., LDAP, OAuth2.0/OIDC, SAML 2.0.
- This support provides the flexibility to integrate third-party IDPs, playing the role of relying party (RP) to such providers but also IDP to downstream RP applications. Assuming third-party providers support the same standards as CitizenOne™, technical effort to integrate for SSO is minimal.
- Low-code model reduces reliance on technical resources and vendors, expediting integration and service delivery timelines.
- The result is an optimized SSO experience, increased satisfaction and digital service consumption, and reduced cyber risk.

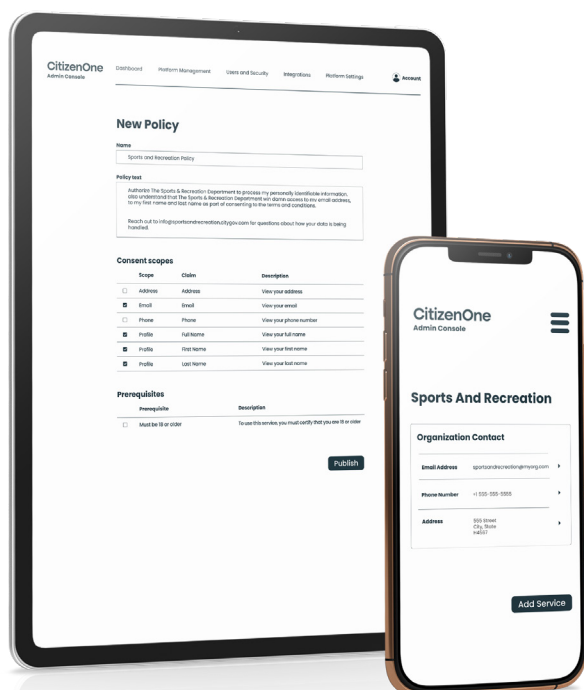


# Core Capabilities: Management

## Consent management

The process of obtaining, recording, and managing user consent for the collection, use, and disclosure of their personal information. This process increasingly includes requirements to allow users to "opt out" of data collection and disclosure practices or withdraw previously given consent.

Consent management is a regulatory requirement in many jurisdictions. However, it is also integral to building trusted relationships online by demonstrating the service provider's commitment to transparency and customer privacy.



## CitizenOne™ capabilities

- In keeping with the principles of [Privacy By Design](#) (PbD), CitizenOne™ provides a user-driven consent model. Users maintain control over which data is shared with government and service providers, for what purpose, and when.
- Data minimization is at the core of the CitizenOne™ data model. It only stores user profile data – generally no more than that required to create an account (i.e., first name, last name, email address, and password).
- The on-boarding process starts with consent for data sharing. Users are presented with the terms and conditions of the service in full transparency. This includes details on why data is collected, references to applicable privacy legislation for review, and an outlet like an email address so they can contact the service provider with questions about data handling.
- During the on-boarding process for a specific service, users consent to sharing attributes from their core profile data and any additional data configured as part of the service's policy.
- Users can opt out of data collection at any time by revoking consent. CitizenOne™ can request downstream applications and service providers to remove data from their systems. Note that these requests are subject to data retention policies and regulations regarding data removal.
- CitizenOne tracks and records all consent events and can generate reports for privacy professionals (e.g., in the case of an audit).
- The combination of these above features ensures compliance with evolving data privacy legislation and service provider obligations to their customers/clients/citizens.

On data protection:

- All data stored in CitizenOne™ is anonymized, so it is not possible to track user activity or extrapolate someone's identity from their credentials.
- All data is encrypted in transit and at rest using industry standard encryption methods and best practices.

### CIAM analytics

The ability to conduct audits and reporting to understand customer behaviour and provide a secure environment. The CIAM solution should be able to fit into enterprise security and compliance programs by providing insights into identity-related events like authentication, MFA/adaptive activity, system access, modifications to personal information, and changes to system configuration.

### CitizenOne™ capabilities

- Built-in analytics that allow a service provider to report on user statistics, including usage levels for a particular service measured against established indicators.
- Leverages integrations to alerting and monitoring tools like NewRelic, Zabbix and Sentry for advanced logging, monitoring, and alerting capabilities. Through its API system, it can build views of data and analytics from these tools in the CitizenOne™ administrator application.
- Integrates with advanced SIEM and threat intelligence tools that service providers may be using.

## Strategic Capabilities

### Omnichannel support

Omnichannel support refers to the ability of the CIAM solution to help ensure customers have a consistent, familiar experience whether they use a website, call center, or service counter.

A good CIAM solution consolidates identity information, preferences, and other basic data used in all customer interactions. It then makes this data available across the organization's service channels while preserving consent, privacy, and security.

### CitizenOne™ capabilities

- As the central source of truth of user profile data, and by leveraging the solution's powerful brokerage model and API system, CitizenOne™ can play a central role in the governance and brokering of trusted data and identity information across the organization's service infrastructure:
  - Support service interactions across digital, in-person and hybrid contexts.
  - Support inter-departmental agreements for data sharing.
  - Move to a more fully decentralized digital identity model

### Modern, API-first architecture

APIs are arguably the building blocks of modern software. Customers, partners, and business units expect data and services to be available across platforms, devices, and networks – expectations that are critical to providing the core functions of a CIAM solution. Modern, API-first technical architectures provide the scalability, performance, and cost benefits needed to integrate a CIAM solution into the organization's broader IT environment.

### CitizenOne™ capabilities

- Designed around a modular architecture, API-first, and standards-based approach to integration. This ensures the service provider can participate in a service eco-system and opens an infinite amount of integration use cases to third-party applications – which supports longer-term goals of interconnected and joined-up services offering enhanced value to users.
- Self-service configuration for end-point management, rules configuration, and service provider integration – reducing reliance on vendors.

A good CIAM solution consolidates identity information, preferences, and other basic data used in all customer interactions.

## Flexible deployment model

Flexible deployment allows the CIAM to be deployed in a manner that meets the service provider's needs, preferences, and regulatory/policy obligations.

To ensure broad support, the CIAM solution should support deployment in both on-premises and cloud-based environments, including multi-cloud, hybrid-cloud.

## CitizenOne™ capabilities

- Deployment options
- On-premises
- Public cloud, private cloud
- Cloud Service Provider (CSP) agnostic:
  - Azure is the current CSP of choice due to current deployments.
  - Digital Ocean is also used.
- Single tenant (which most current deployments use)
- Multi-tenant out of the box:
  - Multiple service providers (e.g., municipal government) can be tenants on the same instance – each with their own URL and branding – creating cost savings and other benefits of a shared infrastructure.

## Open standard support

Open standards provide technical requirements, specifications, or recommendations that anyone can review and implement. For CIAM solutions, standards provide the consistency and uniformity needed for interoperability, compatibility, and security within and between systems and components. They help establish the trust needed to implement BYOI and SSO while avoiding vendor and technology lock-in.

## CitizenOne™ capabilities

- CitizenOne™ supports open, standards-based protocols for authentication and authorization to protected resources i.e., LDAP, OAuth2.0/OIDC, and SAML 2.0.
- Such standards also support the implementation of zero-trust architecture best practices, further bolstering security and bringing it in line with modern cybersecurity architectures and standards.

## Data residency controls

Refers to the jurisdiction in which customer data is stored. To comply with legal requirements and ensure authority over personal information, the CIAM solution must ensure a citizen's personal information is only collected, processed, and stored in their home jurisdiction (usually at country level).

## CitizenOne™ capabilities

- Although we are CSP-agnostic, CitizenOne™ has used Microsoft Azure for our largest deployments to date, ensuring that data remains resident in Canada at the Toronto and Quebec City data centers. We can work with any hosting provider, including the client themselves, to satisfy data residency requirements and infrastructure needs.



# Forward-Looking Capabilities

## Trusted data (Verifiable Credentials) (VCs)

Serving customers and creating trusted relationships with them is a process of using personal information to verify their identities, provide the services they need, and personalize offerings to meet their unique needs. Verification of all this data is often an expensive, time-consuming process dependent on manual and offline procedures. In response, CIAM solutions are adopting new ways of getting the trusted data they need while minimizing security and privacy risks. In many cases, these new ways are enabled by verifiable credential technology.

Verifiable credentials use advanced cryptographic technologies to ensure data contained in a digital credential held by a customer has not been tampered with and that its authenticity can be traced back to an issuing party. This makes it possible to digitally verify customer data, eliminating reliance on self-asserted claims and possibly incorrect data.

## Decentralized customer identities

Customer data often accumulates in fragmented enterprise databases, increasing the risk of non-compliance with privacy regulations and the opportunity for data breaches. Using technology like verifiable credentials mitigates the privacy and security issues this creates by leaving personal information in digital wallets under the customer's control; identity and personal information is decentralized (not stored in or under the control of a single system). The service provider minimizes the amount of personal data collected - requesting trusted data directly from customers only when needed rather than creating large internal databases.

## CitizenOne™ capabilities

- *Credential Engine* is CitizenOne™'s native capability supporting the issuance and verification of Verifiable Credentials.
- Allows for the issuing of verifiable credentials:
  - From any government agency or private organization to any person.
  - For any use case or attribute, limiting data only to what is required.
- Highly interoperable, *Credential Engine* supports all verifiable credential types and specifications that mainstream digital wallet support.

***Credential Engine* is CitizenOne™'s native capability supporting the issuance and verification of Verifiable Credentials.**

## CitizenOne™ capabilities

- To promote their use, service providers can leverage CitizenOne™'s self-serve API end-point management to easily implement workflows for the issuance of verifiable credentials to a user's digital wallet.
- Access management policies can then be further defined at the service or resource level to verify attributes about the user using the credential stored in their wallet before they can gain access to the service.
- Over time, this contributes to an ever-more decentralized model for the storage of trusted data on devices in the user's possession.

**Highly interoperable, *Credential Engine* supports all verifiable credential types and specifications that mainstream digital wallet support.**

# CitizenOne™: Combining CIAM & Service Delivery

CitizenOne™ provides robust CIAM capabilities that enable service providers to securely capture and manage user identity and profile data as well as control user access to applications and services. These capabilities accelerate and extend digital services by:

- Defining user registration, identity proofing, authentication, and authorization processes that are consistent and unified across services and business partners.
- Providing a mechanism for digital identity proofing, to ensure users on the other end of a digital connection are who they say they are.
- Providing users with a single account that can be self-managed and acts as a single source of core user data.
- Separating identity data and service-specific data to ensure the single user account contains only shared or common data.
- Enhancing consent management and privacy controls that provide the ability to opt into the use of a digital service and allows service providers to set discrete policy and consent scopes that a user must accept to access a specific service.
- Replacing fragmented, expensive, and risk-prone IAM solutions across lines of business and partners with a modern, standards-based solution.

Through its CIAM capabilities, CitizenOne™ addresses a major challenge for digital service providers: it's difficult to provide trusted digital access to services in a secure, collaborative, and user-centric manner.

CIAM capabilities alone, regardless of the vendor, will not address a second major challenge for digital service providers: ensuring customers/clients/citizens easily find and interact with the services they need, particularly those they may not know are available, in a crowded online environment.



To address this second challenge, CitizenOne™ marries CIAM capabilities to a [user-focused experience for finding, accessing, and managing relationships with digital services](#).

CitizenOne™ consolidates all your service offerings into one user-friendly dashboard and offers powerful features to simplify your work and ensure you stay compliant with policy and regulation. With one secure login, users can find and subscribe to their services, and service providers can centralize identity, consent, and service access.

In this sense, CitizenOne™ acts as a trusted gatekeeper for all citizen-facing applications within your ecosystem. When users conduct a transaction with a given service, CitizenOne™ ensures the user meets identity proofing, authentication, and access requirements while protecting access to personal information and obtaining user consent when required. As a trusted gatekeeper, CitizenOne™ provides key functions that underlie a superior and trustworthy user experience:

- A single user account to access online services
- Single sign-on and user session management
- User credential management
- A single source of user-managed profiles containing personal information that can be passed to web applications
- Data callbacks that drive service personalization

CitizenOne™ acts as a  
trusted gatekeeper for  
back-end systems.

# Next Steps?

Learn more about  
[Portage CyberTech's solutions.](#)

Book a meeting if you're ready  
to discuss what a strategic  
CIAM implementation could  
look like for your organization.