An Overview of the Digital Identity Lifecycle

By Andrew Cameron and Olaf Grewe

Table of Contents

ABSTRACT **1**

INTRODUCTION TO DIGITAL IDENTITY **2**

KEY TERMS 3

IDENTITY LIFECYCLES **3**

WORKFORCE IDENTITY 3
CUSTOMER IDENTITY 6
DEVICE / SYSTEM IDENTITY 9

CROSS-ORGANIZATIONAL DIGITAL IDENTITY RELATIONSHIPS **10**

CONCLUSION **13**

ACKNOWLEDGEMENTS **13**

Abstract

A digital identity goes through several stages during its existence, from creation, through various modifications in response to different events, to inactivation or deletion. This article walks through the types of digital identities that must be managed, along with the various stages of a digital identity, describing the typical beginning-to-end lifecycle within or across multiple systems. The lifecycles outlined in this document are not meant to be comprehensive but should be applicable over most B2B, B2C, and B2E use cases.

Introduction to Digital Identity

A digital identity, for the purpose of this document, is defined as a unique identifier together with relevant attributes required to enable a digital transaction to generate value. Depending on the complexity of the environment in which a digital identity is used, its lifecycle can be significantly more complicated than a simple create, read, update, and delete (CRUD) lifecycle.[i]

Depending on the type of identity (human such as Workforce or Customer, and non-human types such as System or Device), the lifecycle phases will differ. Enterprise IAM has typically been a well-established set of processes that provide the processes and governance capabilities to ensure only the correct people (accounts) have access to only the required applications (resources). Customer IAM has an entirely different set of requirements that represent value to a business due to the nature of its defining interactions with a customer. Poor or inefficient interactions with customers can have severe negative effects on a business. For these reasons, the different identity types will require separate systems and processes supporting them:

Identity Type	Description
Workforce	A workforce identity is one created to function in an enterprise context, which may include a Business-to-Business (B2B) and/or Business-to-Employee (B2E). Examples of these identity types will be Employees, Suppliers, Contractors, or other human identities that support the corporate workforce.
Customer	A customer identity type will usually function outside the enterprise context, enabling digital business between the owner of the customer identity and the enterprise. Typically, there will be multiple channels (Web, Mobile, IoT Device) of access to manage with a larger set of profile (identity attribute) data necessary to facilitate the interaction.
Device or System	Device identities typically are used to provide identification and representation on a digital network. System identities are used to authenticate services (e.g., applications or server-based processes) to a network.

Key Terms

- Digital Identity - A unique identifier that, together with relevant attributes, is required in the context of a digital transaction to generate value.
- Journey-based Creation – The process that guides a customer through a series of interactions prior to establishing a digital identity. For example, capturing the minimum basic information needed from a customer to enable creation of an identity.
- Attributes - Key/value pairs relevant for the digital identity (username, first name, last name, etc.).
- Inter-organizational (Federation): An organization relies on another organization's digital identity and lifecycle management processes.
- Intra-organizational (Single Sign-On): A central digital identity, such as an account in a directory, is linked by downstream systems as authoritative for authentication.

Identity Lifecycles

For any lifecycle 'create' phase, a digital identity is created as a unique identifier in a system of record. It can be created either as part of a business process (workforce or device identity) or transparently as part of a user journey (customer identity).

Throughout its lifecycle, a digital identity enables digital transactions thru its assigned accounts and entitlements. Although a lifecycle is outlined as a continuum in this document, the reader should expect that:

- The digital identity lifecycle could be distributed across multiple technical solutions in most organizations.
- Some steps in the lifecycle (e.g., authenticate, use) will occur more frequently than others (e.g., merge, delete).

Workforce Identity

The workforce identity lifecycle is addressed through three principal business processes: Joiner, Mover, or Leaver. The **Joiner** processes cover all lifecycle phases that facilitate the creation of assets (identities, accounts, group memberships, etc.) to enable identification and access in an enterprise environment. The **Mover** process allows for changes or updates to identity status while still engaged in the enterprise environment and considers the necessary attestation processes to verify access permissions and entitlements. The **Leaver** process covers the series of steps that must occur when an identity is removed from access to the enterprise environment.

Figure 1 depicts the workforce IAM phases in the lifecycle:

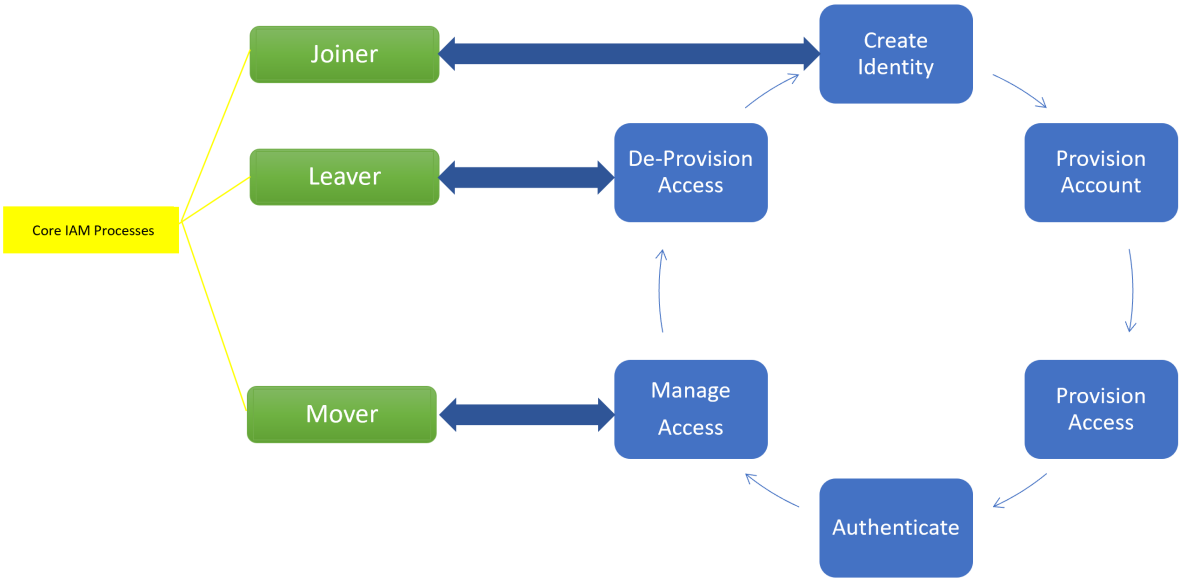


Figure 1 – The Workforce Identity Lifecycle

The following table describes the phases that support the workforce identity lifecycle:

Lifecycle Phase	Description
Create Identity	The creation of a workforce identity as part of a business process (employees, suppliers, etc.) is frequently combined with the collection of proof to establish a minimum set of attributes to be associated with the identifier. The creation of a digital identity may be automated (e.g., synchronized with an HR system event), especially when digital identities are generated at scale for various purposes, such as a merger or acquisition. Enrollment processes for workforce entities frequently involve other human entities (such as a line manager or delegated admin agent) validating the proof provided. In countries without an established national identity system (US, UK, AU, etc.), it can be required to provide multiple documents as proof (driver's license, passport, utility bill, bank card/statement) in lieu of a national identity document.
Provision Account	Create accounts in enterprise systems based on business rules and required access to resources.
Provision Access	Create entitlements to access corporate resources in the required systems. Entitlements are generally represented by attribute values, group memberships, or organizational alignment. Business rules will define access to a resource based on enterprise entitlements.
Authenticate	Require a user account to validate a credential before allowing access to a network or resource.

Manage Access	Validate that the access that has been assigned an account and approving continued access to corporate resources. Access certification is a process that validates all current access and can be used to remove no longer needed access. The attestation process for verifying and access is a critical and often underestimated component of a mature IAM system. Digital identities are frequently subject to updates, primarily of their attributes. Less frequently, the identifier itself may change. An example is a digital identity for which the username is also used as the identifier (e.g., email address). A user may wish to change their username for various purposes, such as a name change due to a life event or a change of preferences. For an in-depth discussion, please refer to Ian Glazer's article, "Identifiers and Usernames."[ii] Frequently update the use cases describing workflow capabilities that address approval, step-up, or notification requirements. These are important controls to address identity take-over risks. Depending on the value of the digital identity for the organization, updates to digital identities may be subject to enrolment-type proofing.
Deprovision Access	Remove access to any or all corporate resources. The need to remove access could occur as a result of a Leaver process or a validation from an Access Certification. When a digital identity is not required anymore, it should be disabled in the system of record. This action implies not only deletion from a central directory but also downstream systems that maintain records associated with this digital identity as well as logging and auditing repositories. Only once the identifier used for this digital identity has been removed from all systems can a digital identity be considered genuinely deleted. A detailed discussion on the importance of account disable or removal given current best practices can be found in Andrew Hindle's article, "Impact of GDPR on Identity and Access Management."[iii]

Customer Identity

Customer IAM has evolved more recently to support the processes that govern consumers' User Experience as they interact with digital business. CIAM solutions have developed to provide companies with added value from the data they collect from customers as a result of the customers' experiences with corporate websites and services. Most customer experiences are described as part of a "User Journey," which represents the interactions (Authentication, Registration, Profile Update) that a customer has when engaging with digital resources such as websites, mobile apps, or IoT interfaces.

The following diagram depicts the phases of the CIAM Lifecycle.

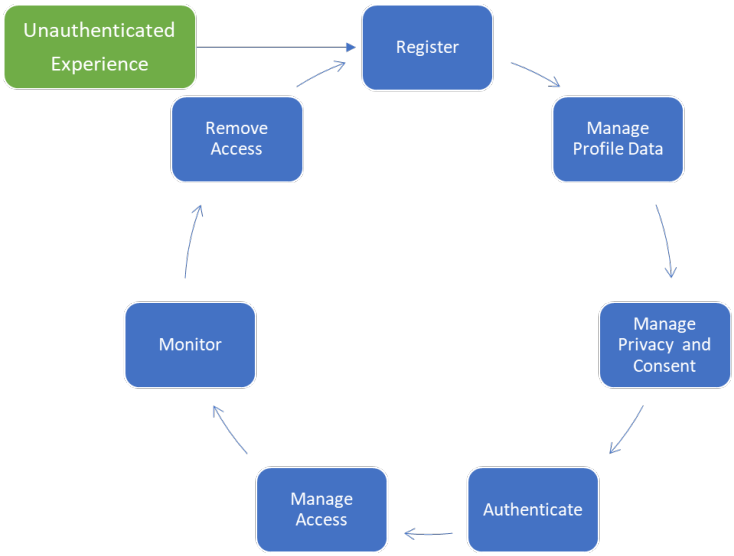


Figure 2 – The Customer Identity Lifecycle

The following table describes the phases that support the customer identity lifecycle:

Lifecycle Phase	Description
Register	The first part of the user journey is the creation of a customer identity through a registration process. This registration typically happens where a digital identity is required to enable an experience. Information is captured from a user as part of a user journey, and the user is allowed to consent to usage of the data provided. Registration interactions are typically a one time interaction with the customer that concludes with a confirmation of the purpose of the flow (i.e. "Your account has been created"). Registration interactions can also be transparent to the user if enabled thru a federated identity such as a social account signin (i.e. "Sign in with your Facebook account to get registered"). Registration does not require mandatory attributes other than the linking steps in the user journey to the identifier. Depending on the nature of the digital transaction, customer identities may require assurance over several attributes. A key consideration here is the attributes used to establish ownership (or recovery) for a digital identity, either via human or non-human means.
Manage Profile Data	Each customer has a profile, and managing the profile data involves a user experience that allows a customer to update their data across corporate resources (e.g., websites or mobile apps). This phase primarily applies to user journey-based digital identities. In order to enable digital services to resume user journeys, it is necessary to enhance the digital identities with attributes that are specific to the way the user accesses the service. Two common techniques are cookies or device fingerprinting. For an illustration of the latter, see the EFFs Panopticlick site.[iv]
Manage Privacy and Consent	The customer lifecycle must include a process that informs and enables the customer to invoke their rights around knowledge and consent of what can happen with their customer information.
Authenticate	As part of the workflow, the customer is required to validate their credential prior to accessing any customer services

Manage Access	The customer lifecycle will require managing access to business services based on customer interactions. The user may also choose to provide additional attributes. The service would typically allow the user to create a username and password to login after their current session has expired. At this stage, a service may be able to combine multiple identifiers created by different devices (mobile, desktop, laptop, etc.). At this stage, the digital identity is considered pseudonymous as there is no assurance over the attributes provided by the user.
Monitor	After the initial phases are complete, the customer lifecycle will move into monitoring, where the process of mining/collecting data about the customer and their experiences support a variety of business and consumer requirements occur. From a security perspective, monitoring data can be used to notify the customer of leaked credentials or other breaches of information. The business can also benefit by leveraging historical usage information of customer activity thru an analytics service.
Remove Access	Removal of customer access is typically done as a result of a customer request or based on some amount of inactivity measure.

Device or System Identity

A device or system identity is an evolving area in that devices are being enabled with increasing levels of technological capability, which increases the need to identify and manage them through a lifecycle. For example, cars have dozens of internal systems that require sophisticated management capabilities over the life of the vehicle identity. On the other end of the scale, some simple monitors can connect to a network and only provide a temperature value or some other basic information. All devices will need specific lifecycle phases to manage them based on their capabilities.

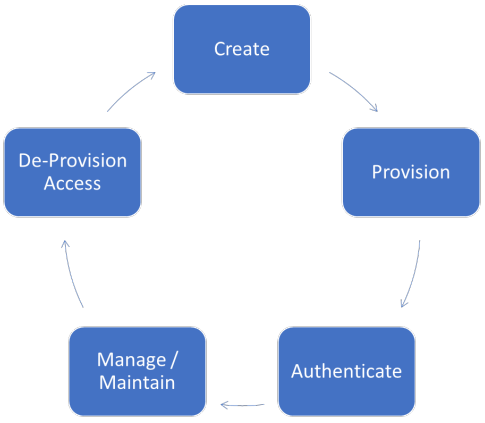


Figure 3 – The Device Identity Lifecycle

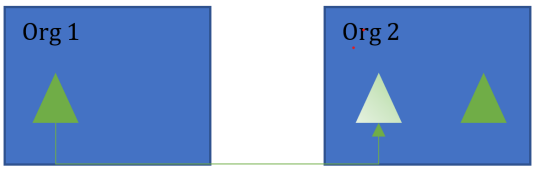
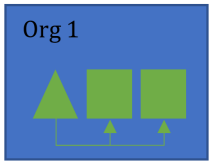
The following table describes the phases in a simple model that support the device identity lifecycle:

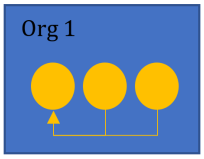
Lifecycle Phase	Description
Create	The first stage in the device or system lifecycle is to kick off the process of creating the identifier that will be assigned to the device or system.
Provision	When the identifier is assigned, the process of enabling the device or system to be recognized, monitored, and managed. Device provisioning is typically done using some sort of certificate or PKI infrastructure to ensure that only known devices can interact with corporate resources.
Authenticate	Device or system authentication typically is done using a PKI infrastructure that ensures that the connected device is known and allowed to interact with the network.
Manage / Maintain	Once the initial phases are complete, the device or system must be monitored to determine if any actions are needed to maintain the device. As an IT security best practice, credentials (passwords) associated with non-human identities should be rotated on a periodic basis to enable protection against brute force password based attacks.
Deprovision Access	When the device or system is no longer in use (which may require different processes than workforce or customer digital identities to determine), remove access of the device or system from the system of record, disabling any access to the corporate network.

Other Digital Identity Relationships

Some digital transactions require an organization to establish relationships between digital identity issuers, also known as identity providers. These relationships may be with external partners (e.g., a B2B relationship) or across various enterprise applications (e.g., a single sign-on environment). In addition, digital identities may be related to other identities within an organization to establish delegation authority or to manage dual-control requirements. In all cases, relationships are typically managed either as attributes of the digital identity (e.g., identifiers for the allowed services) or as separate data points in a central directory (e.g., membership in an LDAP group).

Common types of relationships are:

Inter-organizational (Federation)	 Inter-organizational An organization relies on the digital identity and lifecycle management processes of another organization.
Intra-organizational (Single Sign-On)	 Intra-organizational A central digital identity, such as an account in a directory, is linked by downstream systems as authoritative for the purpose of authentication.
Inter-entity (Delegation)	 Inter-entity Delegation involves assigning a subset of authority from an identity in one organization to an identity that resides in another organization. Authority is granted to across organizational boundaries for the purpose of enabling the executing transactions. Authority can be granted either explicitly or based on business rules at the organizational level.

Intra-entity	 Intra-entity Either user-driven or out of organizational requirements, a relationship is established between multiple digital identities to identify a single human or non-human entity as the owner (see Enhance above).

Conclusion

The complexity of the digital identity lifecycle frequently becomes apparent only after a number of years and as more functionality gets added to systems. Therefore, it is advisable to approach life cycle requirements with a longer-term horizon and ensure user management capabilities are extensible.

Acknowledgements

The author would like to acknowledge Ian Glazer for articulating the progression of an identity from anonymous to pseudonymous and known. Dean Saxe contributed the classification of relationships. Jon Lehtinen and Heather Flanagan contributed encouragement and suffered through early drafts of the article.

---

[i] "Create Read Update Delete" ldapwiki.com, paged last modified 19 March 2020, https://ldapwiki.com/wiki/Create%20Read%20Update%20Delete.

[ii] Glazer, Ian, "Identifiers and Usernames," IDPro Body of Knowledge, 31 March 2020, https://bok.idpro.org/article/id/16/.

[iii] Hindle, Andrew, "Impact of GDPR on Identity and Access Management," IDPro Body of Knowledge, 31 March 2020, https://bok.idpro.org/article/id/24/.

[iv] "Panopticlic 3.0," Electronic Frontier Foundation, viewed 13 April 2020, https://panopticlick.eff.org/.