Proposed Table of Contents for the IDPro Body of Knowledge – Volume 1

(Updated 30 September 2022)

Table of Contents

Introduction

Introduction to Identity – Part 1: Admin-time – *published*

Abstract: This article introduces the concepts of digital identity and identity and access management (IAM). It also discusses the constituents that identity professionals serve, compares and contrasts business-to-employee (B2E) and business-to-consumer (B2C) identity use cases, and considers IAM technologies from the perspective of administrative, or admin-time, technologies.
Bago (Editor), E. & Glazer, I., (2021) "Introduction to Identity - Part 1: Admin-time (v2)", *IDPro Body of Knowledge* 1(5). doi: https://doi.org/10.55621/idpro.27

Introduction to Identity – Part 2: Run-time – *published*

Abstract: Who are you, and what are you allowed to do? In digital systems, these questions are the domain of "Identity and Access Management (IAM)." Access management systems provide the mechanisms for deciding who is who, and evaluate and enforce decisions about who should get access to what. Part 2 of the introduction explores the big picture of access management through a historical perspective. You can expect a little advice, a lot of context, and an experience-based overview of what we do in access management and why our contributions matter.

Dingle, P., (2020) “Introduction to Identity - Part 2: Access Management”, *IDPro Body of Knowledge* 1(2). doi: https://doi.org/10.55621/idpro.45

Background Fundamentals

Proposed Abstract: There are a variety of basic concepts that underly how all computer systems function. Understanding those basics will help an identity practitioner understand how technologies at the network layer impact the architecture of an identity system and how to read technical specifications. Topics in this section include:

- DNS and DNSSEC
- Security Vault
- PKI
- TCP/IP
- HTTPS
- TLS
- Digital Communications Protocols Comparison
- **RFC 2119**: key words in RFCs to indicate the level of requirements

Ethics

Information Security

How to Develop an IAM Threat Model

Abstract: An article that explains the differences in threat models and security postures involved in using different client types, including explanations around common attacks on identity systems (credential stuffing, phishing, password spraying).

Also, in this article or in an additional one, offer information on how to protect against attackers with different capacities and methods of account compromise and cover the importance of researching existing threat models before finalizing an identity system architecture.

Encryption Primer

hashes and cryptographic hashes

symmetric and asymmetric cryptography

keys, key handling, and secret storage

IAM Implications of PKI - *published*

Abstract: Public Key Infrastructure, or "PKI," is a technology that enables authentication via asymmetric cryptography. It is widely deployed for some vital security use cases on the Internet, especially for authentication of servers via Transport Layer Security (TLS).

Despite its wide use for some scenarios, there are significant challenges in deploying PKI for more widespread use among smaller organizations or consumers.

Identity Professionals who need to deploy a PKI or have inherited a deployed PKI from someone else have several important considerations, including lifecycle management of keys and certificates, choosing the appropriate way to encode user identifiers and understanding cross-PKI trust.

Sherwood, R., (2021) "Practical Implications of Public Key Infrastructure for Identity Professionals", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.80

Trust Boundaries and Domains of Administration

Logs, Monitors, and Forensics

Risks, Threats, and Responses

- Common ways to evaluate and register risks
- Threat modeling
- social engineering
- common exploitations
- vulnerabilities and patches

Trust in the IAM Context

Topics to include: technical vs contractual trust.

Privacy

Identification and authentication

Context and Identity

Levels of Assurance

Bias/Diversity in Identity Systems

Topics to cover:

- Implications of bias in biometric recognition, registration questions (gender, name input and change options), social implications of terminology (?), knowledge-based authentication questions
- Awareness of the implications of user tracking and correlation.
- Understanding the implications of data collection. An article that describes the importance and difficulties of normalizing attributes like name and gender in a directory system.

Digital Legacy

Topics to cover: best practices around handling deceased persons' digital ID

Digital Identity

Definition of Digital Identity

Abstract: Despite the difficulty of creating a universal definition of identity, we create a working definition of a more limited concept of digital identity. In this section, we focus on human persons and touch only slightly on non-personal identities such as corporations and devices. Starting with the concept that digital identity is a unique identifier together with relevant attributes required to enable the identifier to be used in the context of a digital transaction, this article elaborates and articulates interesting details, such as the level of certainty about and provenance of attribute values.

Reputation

Digital Identifiers – *published*

Abstract: An identifier is the way an identity management system or other entity refers to a digital identity. The identifier used by the system, however, likely differs from the identifier used directly by the user and will definitely differ from identifiers in another domain. This article reviews the concept of identifiers as they relate primarily to people, both from a user's perspective and a system's perspective, and their impact on the systems that use them.

Glazer, I., (2020) “Identifiers and Usernames”, *IDPro Body of Knowledge* 1(1). doi: https://doi.org/10.55621/idpro.16

Decentralized Identifiers (DIDs) - *published*

Abstract: As digital transformation sweeps across the globe, it has affected everyone – from citizens to employees, from corporations to governments. Digital identity is a foundational enabler for business processes in the digital economy. Decentralized identity is the next evolution of digital identity capabilities and brings with it an opportunity to streamline how people interact with other institutions, physical objects, and with one another. This paper considers the future world of decentralized identity and offers clarity around the benefits of decentralized identity, terminology, sample scenario, and a sample technical implementation, while also addressing some of the limitations of this model. This paper further grounds the reader in the current state of decentralized identity capabilities while outlining the evolution of identity practices from past to present.

Sorokin, L., (2022) “A Peek into the Future of Decentralized Identity (v2)”, IDPro Body of Knowledge 1(7). doi: https://doi.org/10.55621/idpro.51

Digital Identity Lifecycle – *published*

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.

Cameron, A. & Grewe, O., (2022) “An Overview of the Digital Identity Lifecycle (v2)”, *IDPro Body of Knowledge* 1(7). doi: https://doi.org/10.55621/idpro.31

Proofing, Binding or Registration

Abstract: In many contexts, it is important to relate a human to a digital account. Typically it matters in commercial and institutional environments. This activity has been described as proofing or vetting, implying certainty about the mapping. But there is a gradient of need - in some cases, it is very important such as in the fields of medicine or finance, whereas in other cases much less care is needed to achieve the needed level of assurance. This article discusses the drivers and the palette of tactics that can be used to balance the desired level of certainty to the mapping and the desired level of friction to be experienced by the user.

Level of Assurance Model and mapping to risk

Evidence and chain of custody

Creation and delivery of credentials

Self-sovereign credentials (including FIDO style)

Verification/Validation

Credentials

Abstract: When the registration process contains more than a little friction, many systems provide a way to avoid that friction during logins, a process that happens many more times than registration does. In the simplest scenario, this is done by issuing a user ID and a password, in other words, a credential. This section describes the varieties of credentials that are in common use. It also describes methods for establishing credentials (how to convey them safely) and some recovery mechanisms when they are lost or compromised. Because credentials can be stolen, this article touches on the approach that some implementations have taken which look to device identities to reduce risk.

Should include one or more articles describing the use of various credentials and their tradeoffs. These article focuses on credentials, but in some cases the credential and identifier are bundled. Each type described includes benefits and limitations, and common places where you might find the type.

1. passwords, including notions of entropy/strength, hygiene and additional protections such as lock-out, and protection of central password stores using hashes and salts. Some user practices that increase risk, such as re-using passwords.
2. certificates - how it works, FIDO as an implementation
3. biometrics - varieties of methods; philosophy - is it an identifier and/or a credential?
4. passwordless approaches which may use biometrics or certificates, one time use-URLs
5. One Time Password schemes, TOTP, HOTP,
6. Out of band schemes - One time code via eMail, SMS, "push", Discord's session projection scheme, bearer tokens - one time use-URLs

Introduction to Verifiable Credentials

Access Control

Introduction to Access Control – *published*

Abstract: As the name implies Identity and Access Management (IAM) is split into two functions: managing identity information and performing access control. Arguably, if there was no access control requirement there would be no need for identity management; it is therefore the focus for IAM professionals.

At its core access control is ensuring users are authenticated to access protected resources. This is accomplished by managing user entitlements and satisfying the requirements of relying applications so that users can only access the systems and information they are entitled to access. This article looks at the history of access management, the expected current functionality and the trends to be expected.

Koot, A., (2020) "Introduction to Access Control (v3)", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.42

Authentication – *Published*

This article describes the fundamentals of authentication and authorization, two core components of Identity and Access Management. It also delves into federation and Identity Providers, common tools for performing authentication and authorization in an organization.
See Epping, M. & Morowczynski, M., (2021) "Authentication and Authorization", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.78

Dynamic Authentication (risk-based)

Multi-Factor Authentication

Single Sign-on Within a Domain

Centralised Authentication Service

Federated Authentication (between domains)

Device Identity for Corroboration

Fast Identity Online (FIDO)

Session Management

Resources to Protect

Authorization

This article describes the fundamentals of authentication and authorization, two core components of Identity and Access Management. It also delves into federation and Identity Providers, common tools for performing authentication and authorization in an organization.

See Epping, M. & Morowczynski, M., (2021) "Authentication and Authorization", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.78

ACL's

RBAC

ABAC / Dynamic Access Management / Policy Management solutions

Policy-Based Access Control

Abstract: The natural evolution of access controls has caused many organizations to adopt access management paradigms that assign and revoke access based on structured and highly reproducible rules. One such paradigm is known as Policy-Based Access Control (PBAC), which is most differentiated by two key characteristics:

1. Where other access control paradigms often optimize for ease of granting user access to all relevant resources, PBAC optimizes for ease of extending resource access to all applicable users.
2. PBAC facilitates the evaluation of context (time of day, location, etc.) in granting access to a protected resource. Context is used to express who may access a resource and the conditions under which that access is permissible.

Shifting the focus of access controls from the user to the resource allows PBAC systems to be particularly resilient against shifts in organizational structure or regulatory obligations. The inclusion of context (such as an authorized user's location or device) allows for additional security controls to be expressed and extended within resource permissions themselves, ensuring that all facets of access control are contained and auditable within a single structure.

Because PBAC accommodates a very precise expression of who may access a resource and under which circumstances, it lends itself to the automation of access provisioning and deprovisioning in a way that provides ease of management as well as increased security and adaptability.

McKee, M. K., (2021) "Introduction to Policy-Based Access Controls (v2)", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.61

Privileged Access Management

Alignment to Risk Management

Entitlement vs Privilege

Introduction. Distinguish Entitlement and Privilege. What entitlements/privileges are; method to protect confidentiality, integrity and even availability of digital assets, and some physical assets such as doors.

Also, using levels of risk to select permissions

1. Static risks
2. Dynamically determine risk at run time based on context

Additional controls to lower risk of HIGHLY privileged users, such as session recording, credential checkout

Impersonation

Topic - describes the use-cases where one person acting as another make sense and what added controls may be desired.

Delegation

Introduction to the concept of delegation in IAM systems

Techniques to Approach Least Privilege – *Published*

Abstract: This article will describe the lifecycle and techniques that access control practitioners should consider as they grant, validate, and refine permissions as they iterate toward least privilege. The article will compare just-in-time (JIT) approaches with long-standing permissions, balancing productivity with security. The article will explore the risks of using historical data to refine permissions. The reader will learn about refining least privilege in the context of an identity lifecycle and for a specific activity. The article will be agnostic in terms of cloud, hybrid and on-prem, as well as tools.

Carter, M. K., (2022) "Techniques To Approach Least Privilege", *IDPro Body of Knowledge* 1(9). doi: https://doi.org/10.55621/idpro.88

Laws, Regulations, and Standards

Abstract: This chapter provides information about the externally defined environment in which Identity and Access management professionals operate. The laws are documents that define duties and consequences in legal jurisdictions, such as countries. Regulations are more specific and detailed requirements. Standards may also be mandatory; government entities often require compliance with standards produced by certain standards bodies. We also include de facto standards and recommended practices here.

Framework to Understand Legal Environment – *published*

Abstract: Identity systems and its participants are governed by a myriad and complex set of laws, regulations, and contractual requirements, and the obligations they impose are not always clear. This article focuses on the legal environment that governs identity systems. The emphasis is on United States, but references are made to other countries' laws and efforts to coordinate rules underway in the UN Commission on International Trade Law (UNCITRAL) regarding identity management legislation.

Smedinghoff, T. J., (2021) "Laws Governing Identity Systems (v2)", *IDPro Body of Knowledge* 1(5). doi: https://doi.org/10.55621/idpro.8

Approach to Compliance for the Identity Practitioner

Abstract: The overview, above, provides a broad perspective on what the practitioner might encounter. This article provides a companion piece that is less theoretical and more practical and concise. This does not provide legal advice; for that one must consult a legal professional. Instead we chart paths that the reader might take in sample situations to prepare for legal review. The goal is to ensure the identity system, as built and operated, will be in robust compliance with law. This takes the form of three illustrative use-cases where the identity system supports various combinations of jurisdictions, participants and federation:

a) Single jurisdiction, supporting customer access, including out-bound federation for certain aspects of the customer journey;

b) A system that relies entirely on external "identity providers", with operations in several jurisdictions;

c) A multi-jurisdiction employee/contractor-focused system, which wishes to use biometric techniques for authentication.

The general approach is to use the jurisdictions, participants, federations and technologies under consideration in order to locate aspects of the law that must be considered.

Highlights of Selected Laws

Abstract: This section is organized by jurisdiction. It is intended to provide at a minimum a reference to known laws and regulations in jurisdictions likely to be encountered by our membership. At present this includes Europe, United States, and Canada will likely also include Australia in the short term.

Europe

Introduction to GDPR – Published

Abstract: The General Data Protection Regulation (GDPR) applies to any processing (including collection, storage, or sharing) of data relating to identifiable (including by serial numbers, IP addresses, etc.) individuals who are physically in Europe. This scope may well

cover international or online Identity and Access Management (IAM) activities, as well as all IAM activities actually conducted in Europe. All such processing must conform to seven principles: lawfulness, fairness & transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality; accountability. Individuals have rights of information; subject access; rectification, erasure & restriction. Processing must be for one of six legal bases: contract, legal obligation, vital interests, public interests, legitimate interests, or consent. Each basis has its own requirements; some confer additional rights on individuals.

Cormack, A., (2021) "An Introduction to the GDPR (v2)", *IDPro Body of Knowledge* 1(5). doi: https://doi.org/10.55621/idpro.11

IAM Implications of GDPR – Published

Abstract: This article examines the implications of the General Data Protection Regulation ("GDPR", "Regulation") on Identity and Access Management ("IAM") process and system design. It introduces organisational and technical good practices that may help ensure demonstrable compliance with the Regulation as well as improve user experience and customer trust.

Although the focus here is on the GDPR, the approaches described may, by extension, also help in complying with data protection legislation in other geographies including (for example) the California Consumer Privacy Act ("CCPA"), or the Brazilian General Data Protection Law ("LGPD").

Hindle, A., (2020) "Impact of GDPR on Identity and Access Management", *IDPro Body of Knowledge* 1(1). doi: https://doi.org/10.55621/idpro.24

United States

Abstract: This article explains how identity and access management supports the requirements of prominent U.S. laws.

Sarbanes-Oxley Section 404

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH)

Family Educational Rights and Privacy Act of 1974 (FERPA)

Children's Online Privacy Protection Act (COPPA)

Fair and Accurate Credit Transaction Act (FACTA)

Canada

Abstract: This article explains how identity and access management support the requirements of prominent Canadian laws.

Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA)

Regulations

Abstract: This article explains how identity and access management supports the requirements of prominent regulations.

Standards

Abstract: There are many standards. Standards may be mandatory such as when government entities require compliance with standards produced by certain standards bodies. We also include de facto standards and recommended practices here. This is a curated set of standards that have been deemed to be useful to identity professionals. They are organized topically, not by their source. Standards that span more than one topic are possible. In this case cross references may be used.

Architecture - *Published*

Abstract: This is a summary of what is in ISO/IEC 24760-2:2015, one of the core ISO standards on IAM, along with an opinion on its suitability for use by the identity practitioner.

Dobbs, G. B., (2020) "Review - ISO/IEC 24760-2:2015", *IDPro Body of Knowledge* 1(2). doi: https://doi.org/10.55621/idpro.30

Assurance

Abstract: This article surveys the known standards concerning risk and assurance for identity systems.

Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance
[Canada] Government of Canada July 2019 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612

Digital Identity Guidelines
[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
[SP-800-37] NIST Special Publication 800-37r1 June 2014 https://doi.org/10.6028/NIST.SP.800-37r1

Authentication

Abstract: This article surveys the known standards concerning methods of authenticating principals.

Digital Identity Guidelines: Authentication and Lifecycle Management
[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

FIDO2 & WebAuthn

FIDO2 & Client-to-Authenticator Protocol (CTAP)

Introduction to Public Key Technology and the Federal PKI Infrastructure
[SP 800-32] NIST Special Publication 800-32 February 2001. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151247

Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
[IETF RFC 4510] RFC 4510 June 2006 https://tools.ietf.org/html/rfc4510

OpenID Connect Core 1.0 incorporating errata set 1
[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

Personal Identity Verification (PIV) of Federal Employees and Contractors
[FIPS 201-2] NIST FIPS Publication 201-2 September 2013 https://doi.org/10.6028/NIST.FIPS.201-2

Biometric Data Specification for Personal Identity Verification
[SP 800-76-2] NIST Special Publication 800-76-2 July 2013 https://doi.org/10.6028/NIST.SP.800-76-2

Authorization

Abstract: This article surveys the known standards concerning methods of access control. These standards involve protecting resources. This is sometimes called authorization.

The OAuth 2.0 Authorization Framework
[IETF RFC 6749] RFC 6749 October 2012 https://tools.ietf.org/html/rfc6749

User-Managed Access (UMA) Profile of OAuth 2.0
Abstract: The weaknesses of many notice-and-consent paradigms of data privacy are clear. This article notes the social, legal and regulatory drivers and examines some approaches to satisfy them.

[KI UMA] Kantara Initiative UMA Recommendation December 2015 https://docs.kantarainitiative.org/uma/rec-uma-core.html

Federation

Abstract: This article surveys the known standards concerning methods of allowing authentication from one domain to be honored in another.

OpenID Connect Core 1.0 incorporating errata set 1
[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0
[OASIS SAML 2] SAML 2.0 March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Digital Identity Guidelines: Federation and Assertions
[SP 800-63C] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63c

Lifecycle

Abstract: This article surveys the known standards concerning the creation and registration of identities and subsequent changes to the characteristics of those identities and the eventual removal of the same.

Standard on Identity and Credential Assurance
[Canada] Government of Canada July 2019 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612

Digital Identity Guidelines: Enrollment and Identity Proofing Requirements
[SP 800-63A] NIST Special Publication 800-63A December 2017 https://doi.org/10.6028/NIST.SP.800-63a

Digital Identity Guidelines: Authentication and Lifecycle Management
[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

System for Cross-domain Identity Management: Protocol
[IETF RFC 7644] RFC 7644 September 2015 https://tools.ietf.org/html/rfc7644

System for Cross-domain Identity Management: Core Schema
[IETF RFC 7643] RFC 7643 September 2015 https://tools.ietf.org/html/rfc7643

Operations

Abstract: This article surveys the known standards concerning the operation of identity systems.

Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice – Published

Abstract: The document reviewed here is the third and final part of the ISO/IEC 24760 standard, focusing on "Practice", which in the abstract is described as providing *"guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2".* Parts 1 and 2 covers "*Terminology and concepts"* and "*Reference architecture and requirements".* ISO/IEC 24760-3 is in its first edition, dated 2016-08.

Bago, E., (2020) "Review – ISO/IEC 24760-3:2016", *IDPro Body of Knowledge* 1(2). doi: https://doi.org/10.55621/idpro.39

Terminology

Abstract: This article surveys the known standards for the purpose of collating and contrasting terminology defined.

Digital Identity Guidelines

[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

An Ontology of Identity Credentials Part I: Background and Formulation

[SP 800-103] NIST Special Publication 800-103 (Draft) October 2006. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906227

Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts – Published

Abstract: This review offers insight into the first part of the ISO standard for Identity Management, ISO/IEC 24760-1:2019, which covers terminology and concepts.

Scholefield, C., (2020) "Review - ISO/IEC 24760-1:2019", *IDPro Body of Knowledge* 1(1). doi: https://doi.org/10.55621/idpro.18

Emerging Societal Norms

Managing Consent

Workforce IAM / Internal IAM

Key Characteristics of Workforce IAM

IAM Processes

Joiner-Mover-Leaver

HR Ownership

Provisioning (On-boarding and Off-boarding) – *Published*

Abstract: User provisioning is the means by which user accounts are created and maintained in a system (e.g., database, SaaS app, operating system, etc.). When we say that a user-provisioning system maintains a user account, we mean everything from changes to attributes in the user account, changes of entitlements or privileges associated with the user account, locking and unlocking the user account, and even deletion of the user account. User provisioning is primarily an admin-time affair: a user account is created (or changed) based on an administrative action as opposed to a user's action at the time of resource use. This article explores the uses and components of a user-provisioning system and focuses mainly on situations where user accounts are maintained in central repositories, typically enterprise and workforce settings.

Glazer, I. & Robinson, L. & Hamlin, M., (2022) "User Provisioning in the Enterprise", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.84

Role Management

Re-certification

Compliance

Analytics and Intelligence

Handling Business Partners' People

Consumer/Citizen IAM

Key Characteristics of CIAM

CIAM vs Workforce IAM

This introductory article reviews the main key differences between IAM in the consumer world versus IAM in the enterprise. Some of these differences include: focusing on the consumer experience and consumer needs as opposed to the needs of the enterprise and offering a different balance between what a consumer expects in terms of usability and security versus enterprise requirements.

Consumer Journey

Consumers are the focus of the CIAM program. There are several areas that need to be considered that could help you implement a successful CIAM program, including the registration process for consumers, determining and implementing assurance requirements, and the handling of user consent. This section focuses on these areas, offering specific examples and guidance for the IAM practitioner in the consumer-focused industry.

Registration of consumers

This article discusses consumer registration in a product or service. Registration is one of the early experiences in your product. Too much friction in this step would result in consumers going away. In general, it's the idea of asking for as little as possible on first contact (email-only or email+password registration) and then using various profile enrichment strategies later on, e.g., MFA, shipping address, phone number, etc.

Authentication assurance (meeting LoA requirements)

Most activities in CIAM do not require a great level of assurance to be able to do an operation, for example, updating a birthday or a display name. This article explores the concept of levels of assurance (LoA) as it applies to CIAM, including a review of activities that might require a high authentication level of assurance as those are sensitive activities such as the purchase of regulated goods, or access to health-related records. In this case, another authentication process might be rolled out, e.g., prompt another layer of authentication to make sure the consumer is the right people perform the activities.

Data usage consent

The consumer should know how his/her data is being used by the company to give a better experience to the consumer. That’s why it’s important to ask the consumer's consent to make sure they are all aware of their data usage and store the consent to help with a dispute in case it happens. This article references "Managing Consent" by Eve Maler and Graham Williamson, currently in the BoK queue and focuses on additional considerations specific to CIAM.

Social sign-in and sign-up

Social sign-up offers a consumer a way to sign-up to a CIAM system that takes advantage of existing accounts owned by the user. CIAM-focused companies can effectively outsource some of the user support (such as password management) to these social media systems and instead focus on what information is required for personalization. This article explores how social media logins can complement a CIAM infrastructure and offers suggestions on how to offer the maximum benefit to the consumer. This article ties closely to the Data Usage Content article.

Unified consumer view

This article describes the opportunities and challenges involved with supporting a unified view of the consumers of a product or service to a company in order to support targeted marketing, content, or product recommendations. In order to have a unified consumer view, the CIAM system could provide flexible attributes so the application is able to add its own unique fields and help shape the consumer profile. Done appropriately, this service can be of value to both the company and the consumer.

Privacy and Compliance - *Published*

Abstract: This article is the first of several sections of the IDPro Body of Knowledge that address *Privacy and Compliance for Consumers*. This introductory section sets the foundation for subsequent sections on privacy within the IDPro Body of Knowledge, providing an overview of a variety of topics, including definitions of privacy, different approaches to privacy in the consumer sector versus the workforce environment, and more.
Nelson, C., (2020) “Introduction to Privacy and Compliance for Consumers (v2)”, *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.44

Security

Good security must underpin all CIAM initiatives as this is the key to protect consumer data and to maintain their trust in our system. It is important to remember user experience should be considered as well while creating a good security model. The following sections explain some key methods for achieving good security.

Adaptive authentication

It is an authentication action that takes account of other dynamic-runtime environment data or context-based attributes, e.g., device location, time to login, etc., in addition to credentials such as username and password to authenticate users. The authentication is also known as risk-based or contextual authentication.

Multi-Factor Authentication (MFA)

This refers to the use of more than one credential in the authentication of the user. Generally, the use of multiple factors results in a higher LoA for the user's authentication. Two-factor (2FA) is the simplest example of MFA where two different credentials are used. MFA provides a variety of factors to choose from, ranging from asking a security question to capturing and confirming

biometric data to using physical authentication keys, codes or One-Time Passwords (OTPs) over SMS/email or Time-based One-time Password (TOTP) (Google Authenticator).

Non-Human Entity

Introduction – *Published*

Abstract: Non-human accounts are often the "Achilles' heel" of a robust IAM environment. While IAM professionals concern themselves with managing identities, authentication, RBAC, ABAC, governance, and auditing of user accounts, other IT staff are deploying devices and services that are given access to protected resources via hard-wired accounts, exposed services, and APIs.

The management of non-human account control should be consistent with user-based account management, and controls placed on user account access to high-assurance applications should also be applied to non-human accounts.

There is no single solution for dealing with non-human accounts. Some IAM professionals suggest all accounts should be managed via the same processes and same infrastructure to ensure consistent policy deployment. This consistency, they argue, should ensure that non-human accounts are not 'left-out' when IAM deployments occur. Others consider this impractical and recommend that purpose-specific processes be deployed for non-human accounts. But regardless of the mechanism(s) used to manage non-human accounts, ensuring that they are managed is paramount. Otherwise, non-human accounts will continue to be a cybersecurity attack vector favored by hackers for gaining access to corporate facilities.

Williamson, G. & Koot, A. & Lee, G., (2022) "Non-human Account Management (v3)", *IDPro Body of Knowledge* 1(7). doi: https://doi.org/10.55621/idpro.52

IAM Architecture and Solutions

IAM Architecture Overview – *Published*

Abstract: In this section of the BoK, you will explore several conceptual architectures and how they enable IAM solutions across your enterprise. IAM touches all aspects of an organization's IT environment whether it's the HR system, email system, phone system or corporate applications, they all need to interface to the IAM environment. Whether it is by supporting the enforcement of user provisioning rules or validating the access of non-corporate users, IAM will always play a role in making IT operations efficient and secure. An architectural approach will heighten the probability that a consistent and comprehensive IAM solution will be achieved.

Cameron, A. & Williamson, G., (2020) "Introduction to IAM Architecture (v2)", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.38

IAM Reference Architecture – *Published*

Abstract: This article provides a reference model to organize the presentation of technical details associated with various implementations of identity and access management (IAM) architectural concepts. The model is conceptual, as are the set of abstract components which it provides.

To move out of the conceptual realm into specifics additional articles follow, each with a focus on a specific technical use-cases. Each such use-case indicates which of the abstract components comprise a particular implementation

Dobbs, G. B., (2021) "IAM Reference Architecture", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.76

Technical Use Cases

The articles in this section describe a single use-case as implemented in a particular architecture to illustrate a set of components and how they are connected and interact to perform the use-case. These articles are group by the functions defined in the FIRST article (things like authentication, provisioning, authorization...)

The use-case articles follow a common structure:

- Use-case name
- Architecture Type or types (The styles are described in "Introduction to IAM Architecture," IDPro Body of Knowledge" article: Host, Client-Server, N-tier, Hub & Spoke, Remote Access, Cloud Environments.)
- Short description
- Actors, components, and connectors included (with a diagram). The components and connectors refer to the abstract architectural components and their implementations in this use-case.
- Prerequisites
- Exposition on how the components work together and some level of detail. In general this describes the external viewpoint. Internals of the component are minimized.
- Where to find more information on this and adjacent use-cases

Example: of a use-case. This example is chosen to indicate how constrained these articles are intended to be. There could be quite a few variations on Windows login.

Name: Employee logs in to Windows domain - Kerberos Short Description: Interactive domain login using password (Kerberos) Architecture: Client-Server Description: An existing employee logs into the corporate Windows environment with a password. Actors/Components: User (employee), network attached computer running Windows 10, Microsoft Active Directory (IDENTITY REGISTER), Kerberos protocol (AUTHENTICATION)

Function: Authentication

1. Employee logs in to Windows domain - Kerberos
2. Customer logs in from web browser - OpenID Connect
3. Cloud service authenticates via delegation – SAML – *published*
    1. Dobbs, G. B., (2021) "Cloud Service Authenticates Via Delegation - SAML", *IDPro Body of Knowledge* 1(6). doi: https://doi.org/10.55621/idpro.79

Function: Provisioning

1. Directory absorbs changed people information from HR - LDAP
2. Directory synchronizes with downstream resource - SCIM

Function: Attribute Exchange

1. Attributes are provided in assertion - SAML
2. Attributes are requested - OpenID Connect

Function: Authorization

1. File system authorizes access - Windows
2. Application authorizes based on attributes - custom
3. Application delegates to policy service - OAuth
4. Cloud service authorizes based on role assumed from single signon – Cloud

Designing MFA Services - *Published*

Abstract: This article describes how to deploy a thoughtful, consumer-friendly multi-factor authentication (MFA) program that will allow the IAM practitioner to successfully deliver on both the security and usability needs of their authentication systems. The approach is based on a framework of six pillars: determining the viability of different forms of MFA, allowing a multimodal rollout of MFA options, encouraging adoption, supporting MFA across all services and access channels, designing support processes, and creating a trusted environment where MFA can offer additional security to both the consumer and the company.

Kaushik, N., (2020) "Designing MFA for Humans", *IDPro Body of Knowledge* 1(3). doi: https://doi.org/10.55621/idpro.49

Federation Architecture - *Published*

Abstract: This article describes the fundamentals of enterprise identity federations, focusing on SAML and OpenID Connect (a protocol built on OAuth2.0). It will also contain common scenarios where federations are used and high-level terminology. Academic identity federations are out of scope but are mentioned briefly for comparison.

Lunney, P., (2021) "Federation Simplified (v2)", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.62

Operational Considerations

Introduction – *Published*

Abstract: This article will establish recommendations for best practices when managing the identities of your end-users in a customer service environment, considering the risks of both external and malicious insider threats. The following recommendations are built from the authors' experiences and observations, and the recommendations included should be considered a starting point to inspire discussion. More rigorous study is necessary to further refine guidelines for this subject.

Crow, A. & Rowan, J. P., (2021) "Managing Identity in Customer Service Operations", IDPro Body of Knowledge 1(4). doi: https://doi.org/10.55621/idpro.65

Account recovery – *Published*

Abstract: All systems that require authentication of users share a common problem: users are human. Users forget or lose their credentials, lose, reimage, break, or sell hardware with embedded credentials (e.g., a phone or laptop). Account access is lost when users lose access to an email address their account is bound to. In some systems, credentials expire and need to be reissued. The common theme is that users need alternative mechanisms to restore access to the accounts whose credentials are unavailable.

The following article establishes a framework for evaluating Account Recovery mechanisms and establishes recommendations for Account Recovery in consumer, education, enterprise, and government spaces by identifying the benefits and risks of common mechanisms. Given the variety of concerns – privacy, security, and access continuity - in different domains, the reader of this document is expected to apply the guidance herein alongside their domain expertise and judgment to design, develop, and deploy Account Recovery mechanisms for their online systems. Due to the intersection between Account Recovery actions and Customer Service teams, the author strongly recommends that the reader also consult the article "Managing Identity in Customer Service Operations" in the IDPro Body of Knowledge.

Saxe, D. H., (2021) "Account Recovery (v2)", *IDPro Body of Knowledge* 1(8). doi: https://doi.org/10.55621/idpro.64

Call centers

Engagement of user for their own security

Security events and operations

Identity and Access Management Workforce Planning - *Published*

Abstract: This article offers a practical approach to help identity and access management (IAM) practitioners and managers understand how to advise organization leadership on identity and access management workforce planning. While workforce planning is usually a Human Resources (HR) task, the IAM practitioner, their hiring managers, and their HR teams should know the tasks, knowledge, and skills expected across the IAM industry. By capturing the tasks, knowledge, and skills across the various identity and access management service areas, this competency model is tailorable to fit most organizations' needs to include any sector-specific training. Using the U.S. Federal Government's IAM frameworks as a working example, this article seeks to help mature the identity and access management profession and create a more consistent experience across organizations for identity and access management practitioners.

Myers, K., (2022) "Identity and Access Management Workforce Planning", *IDPro Body of Knowledge* 1(9). doi: https://doi.org/10.55621/idpro.85

Project Management

Many Identity and Access Management (IAM) projects proceed without a project manager. In these cases the IT group in charge of identity management are left to deploy the required solution in the absence of any overarching management. While this is sometimes seen as the most expedient way to get a system installed or updated, it is short-sighted and likely to cost the organisation more money in the longer term. An IAM solution touches so many systems within an organisation and is dependent on the current and planned condition of so many applications that to deploy a solution without properly considering the impact, managing the required resources and keeping management advised of progress, will result in a substandard deployment.

Here we look at two ways to manage a project – "Classic", sometimes called Waterfall, and "Agile, a way to manage projects that accommodates changes that inevitably arise during the course of a project.

Reference is made to the Project Management Institute (PMI) Framework. This document in no way seeks to replicate the PMI's methodology or replace the project management training that the PMI provides. The reader is referred to the PMI Body of Knowledge for further information.

Project Management Institute Framework and Project Management Office Issues – *Published*

Abstract: This article serves as an introduction to the practice of project management for an IAM project, describing basic project management terminology and practices. Given the number of systems an IAM project generally impacts, excellent project management is essential for the stakeholders involved.

Williamson, G. & Scholefield, C., (2022) "Introduction to Project Management for IAM Projects (v3)", IDPro Body of Knowledge 1(9). doi: https://doi.org/10.55621/idpro.25

New Implementation Projects