IDPro Body of Knowledge Table of Contents Working DRAFT

December 24, 2019

Contents

1	Intr	roduction	1
	1.1	How to Approach Identity – article in progress	2
	1.2	Constituencies – article in progress	2
		1.2.1 Business to Employee – article in progress	2
		1.2.2 Business to Business – article in progress	2
		1.2.3 Business to Customer – article in progress	2
	1.3	Technologies Involved – article in progress	2
		1.3.1 Admin-time Technologies – article in progress	2
		1.3.2 Privileged Account Management – article in progress	2
		1.3.3 Proofing – article in progress	2
	1.4	Ethics – article in progress	2
	1.5	Information Security	2
	1.6	Trust in the IAM Context	2
	1.7	Privacy	2
	1.8	Identification and authentication	2
		1.8.1 Context and Identity	2
		1.8.2 Levels of Assurance	2
2	Diai	ital Identity	3
_	_		3
			3
	2.2	· ·	3
	2.3	Digital Identity Lifecycle	3
	2.4		3
	2.5		3
		5· 5 5	3
	2.6		3
3	Δες	ess Control	4
_		Authentication	4

CONTENTS ii

		3.1.1		Authentication (risk-based)	4
		3.1.2		ctor Authentication	4
		3.1.3	Single Si	gn-on Within a Domain	4
		3.1.4		sed Authentication Service	4
		3.1.5		ed Authentication (between domains)	4
		3.1.6		dentity for Corroboration	4
		3.1.7		ntity Online (FIDO) and its cousins	4
	2.2	3.1.8		Management	4
	3.2				4
		3.2.1		es to Protect	4
		3.2.2		ation	4
				ACL's	4
				RBAC	4
			3.2.2.3	ABAC / Dynamic Access Management	4
			Pc	olicy Management solutions	4
		3.2.3	Privilege	d Access Management	5
				Alignment to Risk Management	5
			3.2.3.2	System Accounts	5
		_			_
4	Law	s, Reg	ulations,	and Standards	6
4	Law 4.1	_		and Standards Jnderstand Legal Environment – article in progress	6
4		Frame	work to U		
4	4.1	Frame Appro	work to Uach to Co	Jnderstand Legal Environment – article in progress	6
4	4.1 4.2	Frame Appro	ework to leach to Co ghts of Se	Understand Legal Environment – article in progress ompliance for the Identity Practitioner	6 6
4	4.1 4.2	Frame Appro Highli	ework to leach to Co ghts of Se Europe	Understand Legal Environment – article in progress ompliance for the Identity Practitioner	6 6 7
4	4.1 4.2	Frame Appro Highli	ework to U each to Co ghts of Se Europe 4.3.1.1	Understand Legal Environment – article in progress ompliance for the Identity Practitioner	6 6 7 7
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to U ach to Co ghts of Se Europe 4.3.1.1 4.3.1.2	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 6 7 7 7
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Lework to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S	Introduction to GDPR – article in progress In progress	6 6 7 7 7
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Leach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1	Introduction to GDPR – article in progress IAM Implications of GDPR – article in progress	6 7 7 7 7 7 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Upach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2	Introduction to GDPR – article in progress Introductions of GDPR – article in progress IAM Implications of GDPR – article in progress	6 7 7 7 7 7 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Upach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 7 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Use ach to Coghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 8 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Use ach to Coghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3	Inderstand Legal Environment – article in progress	6 7 7 7 7 7 8 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Use ach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 7 8 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Use Ach to Coghts of See Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3 4.3.2.4 4.3.2.5 4.3.2.6	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 7 8 8 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Upach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3 4.3.2.4 4.3.2.5 4.3.2.6 Canada	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 7 8 8 8 8 8
4	4.1 4.2	Frame Appro Highli 4.3.1	ework to Usach to Co ghts of Se Europe 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3 4.3.2.4 4.3.2.5 4.3.2.6 Canada 4.3.3.1	Inderstand Legal Environment – article in progress	6 7 7 7 7 7 8 8 8 8 8
4	4.1 4.2 4.3	Frame Appro Highli 4.3.1 4.3.2	ework to Use ach to Coghts of Securope 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3 4.3.2.5 4.3.2.6 Canada 4.3.3.1	Introduction to GDPR – article in progress Introduction to GDPR – article in progress Introductions of GDPR – article in progress Interest	6 7 7 7 7 7 8 8 8 8 8 8 8
4	4.1 4.2 4.3	Frame Appro Highli 4.3.1 4.3.2	ework to Upach to Coghts of Securope 4.3.1.1 4.3.1.2 United S 4.3.2.1 4.3.2.2 4.3.2.3 4.3.2.6 Canada 4.3.3.1 ations	Inderstand Legal Environment – article in progress ompliance for the Identity Practitioner	6 7 7 7 7 7 7 8 8 8 8 8 8 8 8

CONTENTS

	4.5.1.1	ISO/IEC 24760-2:2015 Information technology Secu-	
		rity techniques A framework for identity management	_
4.5.0		Part 2: Reference architecture and requirements	
4.5.2	Assurar		2
	4.5.2.1	Directive on Identity Management - Appendix A: Standard	_
		on Identity and Credential Assurance	٥
	4.5.2.2	Digital Identity Guidelines	9
	4.5.2.3	Guide for Applying the Risk Management Framework to Fed-	_
4 5 0	A 	eral Information Systems: A Security Life Cycle Approach	٥
4.5.3	Authent		٤
	4.5.3.1	Digital Identity Guidelines: Authentication and Lifecycle Man-	,
	4522	agement	٢
	4.5.3.2	Introduction to Public Key Technology and the Federal PKI Infrastructure	c
	4 E 2 2	Lightweight Directory Access Protocol (LDAP): Technical Spec-	3
	4.5.3.3		10
	4.5.3.4	ification Road Map	10
	4.5.3.5	Personal Identity Verification (PIV) of Federal Employees and	10
	4.5.5.5	Contractors	10
	4.5.3.6	Biometric Data Specification for Personal Identity Verification	10
4.5.4	Authori		10
1.5. 1	4.5.4.1	The OAuth 2.0 Authorization Framework	10
	4.5.4.2	User-Managed Access (UMA) Profile of OAuth 2.0	10
4.5.5	Federat		10
	4.5.5.1	OpenID Connect Core 1.0 incorporating errata set 1	11
	4.5.5.2	Assertions and Protocols for the OASIS Security Assertion	•
		Markup Language (SAML) V2.0	11
	4.5.5.3	Digital Identity Guidelines: Federation and Assertions	11
4.5.6	Lifecycle		11
	4.5.6.1	Standard on Identity and Credential Assurance	11
	4.5.6.2	Digital Identity Guidelines: Enrollment and Identity Proofing	
		Requirements	11
	4.5.6.3	Digital Identity Guidelines: Authentication and Lifecycle Man-	
			11
	4.5.6.4		11
	4.5.6.5	System for Cross-domain Identity Management: Core Schema	12
4.5.7		ons	12
	4.5.7.1	Information technology Security techniques A frame-	
		work for identity management Part 3: Practice	12
4.5.8			12
	4.5.8.1	Digital Identity Guidelines	12

CONTENTS

			An Ontology of Identity Credentials Part I: Background and Formulation	
		4.5.8.3	ment Part 1: Terminology And Concepts	. 12
		4.5.8.4	ISO/IEC 24760-1:2019 IT Security and Privacy A Framework For Identity Management Part 1: Terminology	
			And Concepts	
	4.6		cietal Norms	
5		kforce IAM / I		13
	5.1		S	
		-	Mover-Leaver	
			oning (On-boarding and Off-boarding)	
			lanagement	
	5.2		tification	
			iness Partners' People	
6	Con	sumer/Citizer		14
6	Con 6.1	Consumer Jou	urney (identification to loyal customer)	. 14
6		Consumer Jou 6.1.1 Registr	urney (identification to loyal customer) ration of Consumers 14 . 14
6	6.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther	urney (identification to loyal customer)	. 14 . 14 . 14
6	6.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public	urney (identification to loyal customer)	. 14 . 14 . 14 . 14
6	6.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ	urney (identification to loyal customer)	. 14 . 14 . 14 . 14 . 14
6	6.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health	urney (identification to loyal customer)	. 14 . 14 . 14 . 14 . 14
	6.16.26.3	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care and Sign-on	. 14 . 14 . 14 . 14 . 14 . 14
	6.1 6.2 6.3	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up	urney (identification to loyal customer)	. 14 . 14 . 14 . 14 . 14 . 14
	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices .	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on	. 14 . 14 . 14 . 14 . 14 . 14 . 15
7	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices . 7.2.1 IoT Sec	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on rechnology (OT) ctors	. 14 . 14 . 14 . 14 . 14 . 14 . 15 . 15
	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registre 6.1.2 Author Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices . 7.2.1 IoT Sec 7.2.1.1	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on Ey Technology (OT) Ctors Home Automation	. 144 . 144 . 144 . 144 . 144 . 155 . 155 . 155
	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices . 7.2.1 IoT Sec	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on Ey Technology (OT) Technology (OT) Technology (OT) Technology (Wearables)	. 144 . 144 . 144 . 144 . 145 . 155 . 155 . 155 . 155
	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices . 7.2.1 IoT Sec 7.2.1.1 7.2.1.2	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on ety fechnology (OT) totors Home Automation Personal (wearables) Implants	. 144 . 144 . 144 . 144 . 144 . 15 . 15 . 15 . 15 . 15
	6.16.26.3Nor7.1	Consumer Jou 6.1.1 Registr 6.1.2 Auther Industry Cons 6.2.1 Public 6.2.2 Financ 6.2.3 Health Social Sign-up 1-Human Entit Operational T IoT Devices . 7.2.1 IoT Sec 7.2.1.1 7.2.1.2 7.2.1.3	urney (identification to loyal customer) ration of Consumers ntication Assurance (meeting LoA requirements) siderations Sector vs. Private Sector ial Services care o and Sign-on Ey Technology (OT) Ctors Home Automation Personal (wearables) Implants Plant Automation Vehicle	. 144 . 144 . 144 . 144 . 145 . 155 . 155 . 155 . 155 . 155 . 155

CONTENTS

		7.2.1.7 Agriculture 1 7.2.1.8 Building/Industrial 1 7.2.1.9 Utilities 1 RPA / robotics 1 Security requirements 1	5
8	8.1 8.2 8.3 8.4 8.5 8.6	Architecture and Solutions IAM Architecture Overview – article in progress Architecture Patterns – article in progress 1 Technical Architecture – article in progress 1 Identity Governance – article in progress 1 8.4.1 Elements of IGA Systems – article in progress 1 Key Definitions and Terms – article in progress 1 Business System 1 8.6.1 Business Processes 1 8.6.1.1 Recertification of accounts 1 Recommended Practices 1 8.7.1 Design for security 1	6 6 6 6 6 6 6 6 6
9	9.1 9.2 9.3	rational Considerations1Account recovery	777
	10.1 10.2 10.3 10.4	ect Management 1 Project Management Institute Framework – article in progress 1 Project Management Office Issues – article in progress 1 New Implementation Projects 1 Migration Projects 1	888
11	11.1 11.2 11.3	Knowledge Sharing1Independent Organizations – article in progress1Standards Bodies1Analyst Organizations1Conferences1	9
12	12.1	anced Topics – Parking Lot Digital Legacy - handling deceased persons' digital ID (Advanced Topic) 2 Self-Sovereign Identity	20



Introduction

- **1.1** How to Approach Identity article in progress
- **1.2 Constituencies** article in progress
- **1.2.1** Business to Employee article in progress
- **1.2.2 Business to Business** *article in progress*
- **1.2.3** Business to Customer article in progress
- **1.3 Technologies Involved** article in progress
- **1.3.1** Admin-time Technologies article in progress
- **1.3.2** Privileged Account Management article in progress
- **1.3.3 Proofing** article in progress
- **1.4 Ethics** article in progress
- 1.5 Information Security
- 1.6 Trust in the IAM Context
- 1.7 Privacy
- 1.8 Identification and authentication
- 1.8.1 Context and Identity
- 1.8.2 Levels of Assurance

Digital Identity

- 2.1 Definition
- 2.1.1 Reputation
- **2.2 Identifiers** article in progress
- 2.3 Digital Identity Lifecycle
- 2.4 Mapping to human or device
- 2.5 Proofing, Binding or Registration
- 2.5.1 Verification/Validation
- 2.6 Credentials

Access Control

3.1 Authentication	n
--------------------	---

- 3.1.1 Dynamic Authentication (risk-based)
- 3.1.2 Multi-Factor Authentication
- 3.1.3 Single Sign-on Within a Domain
- 3.1.4 Centralised Authentication Service
- 3.1.5 Federated Authentication (between domains)
- 3.1.6 Device Identity for Corroboration
- 3.1.7 Fast Identity Online (FIDO) and its cousins
- 3.1.8 Session Management

3.2 Authorization

- 3.2.1 Resources to Protect
- 3.2.2 Authorisation
- 3.2.2.1 ACL's
- 3.2.2.2 RBAC
- 3.2.2.3 ABAC / Dynamic Access Management

Policy Management solutions

- 3.2.3 Privileged Access Management
- 3.2.3.1 Alignment to Risk Management
- 3.2.3.2 System Accounts

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.

4.1 Framework to Understand Legal Environment – article in progress

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.

4.2 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.

4.3 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.

4.3.1 Europe

4.3.1.1 Introduction to GDPR – article in progress

Abstract: This article provides a basic understanding of how the *General Data Protection Regulation (GDPR)* applies when processing 'any information relating to an identified or identifiable natural person'.

4.3.1.2 IAM Implications of GDPR – article in progress

Abstract: This article provides information to the IAM practitioner about how to achieve compliance with the European data protection and privacy rules for European and multi-national firms

4.3.2 United States

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

- 4.3.2.1 Sarbanes-Oxley Section 404
- 4.3.2.2 Health Insurance Portability and Accountability Act (HIPAA)
- 4.3.2.3 Health Information Technology for Economic and Clinical Health Act (HITECH)
- 4.3.2.4 Family Educational Rights and Privacy Act of 1974 (FERPA)
- 4.3.2.5 Children's Online Privacy Protection Act (COPPA)
- 4.3.2.6 Fair and Accurate Credit Transaction Act (FACTA)

4.3.3 Canada

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

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

4.4 Regulations

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

4.5 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.

4.5.1 Architecture

Abstract: This article surveys the known standards concerning architecture for identity systems.

4.5.1.1 ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

4.5.2 Assurance

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

4.5.2.1 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

4.5.2.2 *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

4.5.2.3 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

4.5.3 Authentication

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

4.5.3.1 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

4.5.3.2 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_p

4.5.3.3 Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map

[IETF RFC 4510] RFC 4510 June 2006 https://tools.ietf.org/html/rfc4510

4.5.3.4 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.

4.5.3.5 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

4.5.3.6 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

4.5.4 Authorization

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

4.5.4.1 The OAuth 2.0 Authorization Framework

[IETF RFC 6749] RFC 6749 October 2012 https://tools.ietf.org/html/rfc6749

4.5.4.2 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.uma-core.html

4.5.5 Federation

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

4.5.5.1 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.

4.5.5.2 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

4.5.5.3 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

4.5.6 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.

4.5.6.1 Standard on Identity and Credential Assurance

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

4.5.6.2 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

4.5.6.3 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

4.5.6.4 System for Cross-domain Identity Management: Protocol

[IETF RFC 7644] RFC 7644 September 2015 https://tools.ietf.org/html/rfc7644

4.5.6.5 System for Cross-domain Identity Management: Core Schema

[IETF RFC 7643] RFC 7643 September 2015 https://tools.ietf.org/html/rfc7643

4.5.7 Operations

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

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

[ISO 24760-3] ISO/IEC 24760-3:2016 2016 https://webstore.ansi.org/Standards/ISO/ISOIEC2476020

4.5.8 Terminology

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

4.5.8.1 *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

4.5.8.2 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/publicati

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

[ISO 24760-1] ISO/IEC 24760-1:2019 IT 2019 https://webstore.ansi.org/Standards/ISO/ISOIEC247602

4.5.8.4 ISO/IEC 24760-1:2019 IT Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts

4.6 Emerging Societal Norms

4.6.1 Managing Consent – article in progress

Workforce IAM / Internal IAM

- **5.1 IAM Processes**
- 5.1.1 Joiner-Mover-Leaver
- 5.1.2 HR Ownership
- **5.1.3** Provisioning (On-boarding and Off-boarding)
- **5.1.4** Role Management
- 5.1.5 Re-certification
- **5.2** Compliance
- 5.3 Analytics and Intelligence
- 5.4 Handling Business Partners' People

Consumer/Citizen IAM

- **6.1** Consumer Journey (identification to loyal customer)
- **6.1.1 Registration of Consumers**
- **6.1.2** Authentication Assurance (meeting LoA requirements)
- **6.2 Industry Considerations**
- 6.2.1 Public Sector vs. Private Sector
- **6.2.2 Financial Services**
- 6.2.3 Healthcare
- 6.3 Social Sign-up and Sign-on

Non-Human Entity

- 7.1 Operational Technology (OT)
- 7.2 IoT Devices
- 7.2.1 IoT Sectors
- 7.2.1.1 Home Automation
- 7.2.1.2 Personal (wearables)
- **7.2.1.3 Implants**
- 7.2.1.4 Plant Automation
- 7.2.1.5 Vehicle
- 7.2.1.6 Smart Cities
- 7.2.1.7 Agriculture
- 7.2.1.8 Building/Industrial
- **7.2.1.9 Utilities**
- 7.3 RPA / robotics
- 7.4 Security requirements

IAM Architecture and Solutions

- **8.1 IAM Architecture Overview** article in progress
- **8.2 Architecture Patterns** *article in progress*
- **8.3 Technical Architecture** *article in progress*
- **8.4 Identity Governance** article in progress
- **8.4.1 Elements of IGA Systems** *article in progress*
- **8.5 Key Definitions and Terms** *article in progress*
- 8.6 Business System
- 8.6.1 Business Processes
- 8.6.1.1 Recertification of accounts
- 8.7 Recommended Practices
- 8.7.1 Design for security

Operational Considerations

- 9.1 Account recovery
- 9.2 Call centers
- 9.3 Engagement of user for their own security
- 9.4 Security events and operations

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.

- **10.1** Project Management Institute Framework article in progress
- **10.2 Project Management Office Issues** article in progress
- **10.3** New Implementation Projects
- **10.4 Migration Projects**

IAM Knowledge Sharing

- **11.1 Independent Organizations** article in progress
- 11.2 Standards Bodies
- **11.3** Analyst Organizations
- 11.4 Conferences

Advanced Topics – Parking Lot

- 12.1 Digital Legacy handling deceased persons' digital ID (Advanced Topic)
- 12.2 Self-Sovereign Identity
- 12.2.1 Blockchain ID