IDPro Body of Knowledge Table of Contents
Working DRAFT

August 30, 2019

Contents

1 Introduction **1**
1.1 Information security 1
1.1.1 Trust (say more - what is this?) 1
1.2 Privacy 1
1.3 Identification and authentication 1
1.3.1 Context and Identity 1
1.3.2 Levels of Assurance 1
1.4 The Business Case for IAM 1
1.4.1 Workforce IAM 1
1.4.2 Consumer/Citizen IAM 1

2 Digital Identity **2**
2.1 Definition 2
2.1.1 Reputation 2
2.1.2 Laws of Identity (this sounds like jurisdictions and real laws - is that the intent?) 2
2.2 Identifiers 2
2.3 Digital Identity Lifecycle (?) 2
2.4 Mapping to human or device 2
2.5 Proofing, Binding or Registration (?) 2
2.5.1 Verification/Validation 2
2.6 Credentials 2

3 Access Control **3**
3.1 Authentication 3
3.1.1 Dynamic Authentication (risk-based) 3
3.1.2 Multi-Factor Authentication 3
3.1.3 Single Sign-on Within a Domain 3
3.1.4 Centralised Authentication Service 3
3.1.5 Federated Authentication (between domains) 3

3.1.6 Device Identity for Corroboration 3
3.1.7 Fast Identity Online (FIDO) and its cousins 3
3.1.8 Session Management 3
3.2 Authorization 3
3.2.1 Resources to Protect 3
3.2.2 Authorisation 3
3.2.2.1 ACL's 3
3.2.2.2 RBAC 3
3.2.2.3 ABAC / Dynamic Access Management 3
Policy Management solutions 3
3.2.3 Privileged Access Management 4
3.2.3.1 Alignment to Risk Management 4
3.2.3.2 System Accounts 4

4 Laws, Regulations, and Standards 5
4.1 Framework to Understand Legal Environment 6
4.2 Highlights of Selected Laws 6
4.2.1 Europe 6
4.2.1.1 GDPR 6
4.2.2 United States 6
4.2.2.1 Sarbanes-Oxley Section 404 6
4.2.2.2 Health Insurance Portability and Accountability Act (HIPAA) 6
4.2.2.3 Health Information Technology for Economic and Clinical Health Act (HITECH) 6
4.2.2.4 Family Educational Rights and Privacy Act of 1974 (FERPA) 6
4.2.2.5 Children's Online Privacy Protection Act (COPPA) 6
4.2.2.6 Fair and Accurate Credit Transaction Act (FACTA) 6
4.2.3 Canada 6
4.2.3.1 Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA) 6
4.3 Standards 6
4.3.1 Terminology 6
4.3.1.1 ISO/IEC 24760-1:2019 IT Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts 6
4.3.2 Architecture 6
4.3.2.1 ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements . . . 6

4.3.2.2 ISO/IEC 24760-3:2016 Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice . . . 6
4.3.3 Techniques . . . 6
4.3.3.1 LDAP – RFC 4511 . . . 6
4.3.3.2 LDIF – RFC 2849 . . . 6
4.3.3.3 SAML 2.0 . . . 6
4.3.3.4 OAUTH 2.0 – RFC'S 6749, 8252 . . . 6
4.3.3.5 OpenID Connect 1.0 . . . 6
4.3.3.6 User-Managed Access (UMA) Profile of OAuth 2.0 . . . 6

5 Workforce IAM / Internal IAM 7
5.1 IAM Processes . . . 7
5.1.1 Joiner-Mover-Leaver . . . 7
5.1.2 HR Ownership . . . 7
5.1.3 Provisioning (On-boarding and Off-boarding) . . . 7
5.1.4 Role Management . . . 7
5.1.5 Re-certification . . . 7
5.2 Compliance . . . 7
5.3 Analytics and Intelligence . . . 7
5.4 Handling Business Partners' People . . . 7

6 Consumer/Citizen IAM 8
6.1 Consumer Journey (identification to loyal customer) . . . 8
6.1.1 Registration of Consumers . . . 8
6.1.2 Authentication Assurance (meeting LoA requirements) . . . 8
6.2 Industry Considerations . . . 8
6.2.1 Public Sector vs. Private Sector . . . 8
6.2.2 Financial Services . . . 8
6.2.3 Healthcare . . . 8
6.3 Social Sign-up and Sign-on . . . 8

7 Non-Human Entity 9
7.1 Operational Technology (OT) . . . 9
7.2 IoT Devices . . . 9
7.2.1 IoT Sectors . . . 9
7.2.1.1 Home Automation . . . 9
7.2.1.2 Personal (wearables) . . . 9
7.2.1.3 Implants . . . 9
7.2.1.4 Plant Automation . . . 9
7.2.1.5 Vehicle . . . 9

7.2.1.6 Smart Cities 9
7.2.1.7 Agriculture 9
7.2.1.8 Building/Industrial 9
7.2.1.9 Utilities 9
7.3 RPA / robotics 9
7.4 Security requirements 9

8 IAM Architecture and Solutions 10
8.1 Business System 10
8.1.1 Business Processes 10
8.1.1.1 Recertification of accounts 10
8.2 Information/Data Architecture 10
8.3 Application Portfolio 10
8.3.1 APIs 10
8.3.1.1 HTTP 10
8.3.1.2 S/LDAP 10
8.3.1.3 RACF 10
8.3.1.4 XACML 10
8.4 Technical 10
8.4.1 Repositories 10
8.4.1.1 Relational Database 10
Query optimization 10
Replication limitations 10
8.4.1.2 Directories 11
Historical note - X.500 11
SLAPD and its descendants 11
8.4.1.3 NoSQL databases 11
Graph Databases 11
8.4.1.4 Identity Provider (IdP) Trends 11
Distributed Ledger (Blockchain) 11
8.4.2 Identity Provider Services 11
8.4.3 Protocols 11
8.4.3.1 Kerberos 11
8.4.3.2 Lightweight Directory Access Protocol (LDAP) 11
8.4.3.3 SCIM 11
8.4.3.4 SAML 11
SP Initiated vs IDP Initiated 11
Bindings 11
8.4.3.5 OIDC 11
Authentications Flows 11
8.4.3.6 OAuth 12

8.4.3.7 WS-Fed 12
8.4.3.8 FIDO U2F and UAF 12
8.4.4 Enterprise control of “Cloud” 12
8.4.4.1 Public Cloud vs Private Cloud 12
8.4.4.2 Local Connectors and Gateways 12
8.4.4.3 IPSec VPN 12
8.5 Recommended Practices 12
8.5.1 Design for security 12
8.6 Governance and Administration 12
8.6.1 Audit 12
8.6.2 Monitoring 12

9 Operational Considerations 13
9.1 Account recovery 13
9.2 Call centers 13
9.3 Engagement of user for their own security 13
9.4 Security events and operations 13

10 Project Management 14
10.1 Importance of Project Management 14
10.2 Characteristics of a Project Manager 14
10.3 PMI Framework 14
10.3.1 Concept 14
10.3.2 Planning Stage 14
10.3.3 Deployment Stage 14
10.3.4 Methodologies 14
10.4 PMO Issues 14

11 IAM Knowledge Sharing 15
11.1 IDPro 15
11.2 Gartner 15
11.3 KuppingerCole 15
11.4 IIW 15
11.5 Bibliography 15
11.6 15

12 Advanced Topics – Parking Lot 16
12.1 Digital Legacy - handling deceased persons’ digital ID (Advanced Topic) 16
12.2 Self-Sovereign Identity 16
12.2.1 Blockchain ID 16

Chapter 1

Introduction

1.1 Information security

1.1.1 Trust (say more - what is this?)

1.2 Privacy

1.3 Identification and authentication

1.3.1 Context and Identity

1.3.2 Levels of Assurance

1.4 The Business Case for IAM

1.4.1 Workforce IAM

1.4.2 Consumer/Citizen IAM

Chapter 2

Digital Identity

2.1 Definition

2.1.1 Reputation

2.1.2 Laws of Identity (this sounds like jurisdictions and real laws - is that the intent?)

2.2 Identifiers

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

Chapter 3

Access Control

3.1 Authentication

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

Chapter 4

Laws, Regulations, and Standards

4.1 Framework to Understand Legal Environment

4.2 Highlights of Selected Laws

4.2.1 Europe

4.2.1.1 GDPR

4.2.2 United States

4.2.2.1 Sarbanes-Oxley Section 404

4.2.2.2 Health Insurance Portability and Accountability Act (HIPAA)

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

4.2.2.4 Family Educational Rights and Privacy Act of 1974 (FERPA)

4.2.2.5 Children's Online Privacy Protection Act (COPPA)

4.2.2.6 Fair and Accurate Credit Transaction Act (FACTA)

4.2.3 Canada

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

4.3 Standards

4.3.1 Terminology

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

4.3.2 Architecture

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

4.3.2.2 ISO/IEC 24760-3:2016 Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice

Chapter 5

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

Chapter 6

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

Chapter 7

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

Chapter 8

IAM Architecture and Solutions

8.1 Business System

8.1.1 Business Processes

8.1.1.1 Recertification of accounts

8.2 Information/Data Architecture

8.3 Application Portfolio

8.3.1 APIs

8.3.1.1 HTTP

8.3.1.2 S/LDAP

8.3.1.3 RACF

8.3.1.4 XACML

8.4 Technical

8.4.1 Repositories

8.4.1.1 Relational Database

Query optimization

Replication limitations

8.4.1.2 Directories

Historical note - X.500

SLAPD and its descendants

8.4.1.3 NoSQL databases

Graph Databases

8.4.1.4 Identity Provider (IdP) Trends

Distributed Ledger (Blockchain)

8.4.2 Identity Provider Services

8.4.3 Protocols

8.4.3.1 Kerberos

8.4.3.2 Lightweight Directory Access Protocol (LDAP)

8.4.3.3 SCIM

8.4.3.4 SAML

SP Initiated vs IDP Initiated

Bindings

8.4.3.5 OIDC

Authentications Flows

8.4.3.6 OAuth

8.4.3.7 WS-Fed

8.4.3.8 FIDO U2F and UAF

8.4.4 Enterprise control of “Cloud”

8.4.4.1 Public Cloud vs Private Cloud

8.4.4.2 Local Connectors and Gateways

8.4.4.3 IPSec VPN

8.5 Recommended Practices

8.5.1 Design for security

8.6 Governance and Administration

8.6.1 Audit

8.6.2 Monitoring

Chapter 9

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

Chapter 10

Project Management

10.1 Importance of Project Management

10.2 Characteristics of a Project Manager

10.3 PMI Framework

10.3.1 Concept

10.3.2 Planning Stage

10.3.3 Deployment Stage

10.3.4 Methodologies

10.4 PMO Issues

Chapter 11

IAM Knowledge Sharing

11.1 IDPro

11.2 Gartner

11.3 KuppingerCole

11.4 IIW

11.5 Bibliography

11.6

Chapter 12

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