IDPro Body of Knowledge - Demo

Principal Editor: TBD

December 16, 2018

Contents

List of Figures

List of Tables

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

Chapter 4

Regulations And Laws

4.1 Privacy (generic)

4.2 Survey of Jurisdictions

4.2.1 SOX, HiPPA, GDPR, CBPR etc.

4.3 Consent management

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 Handling Business partners' people

5.1.5 Re-certification

5.2 Analytics and Intelligence

Chapter 6

Consumer/Citizen IAM

6.1 Public sector vs. private sector

6.2 Social media

6.3 Consumer journey (identification to loyal customer)

6.3.1 Registration of consumers

6.3.2 Authentication assurance (meeting LoA requiremetns)

6.3.3 Digital legacy - handling deceased persons' digital ID

6.4 Self-Sovereign Identity

6.4.1 Blockchain ID

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 Agricuture

7.2.1.8 Buildiing/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 Provisioning accounts

8.1.1.2 Changes to accounts

8.1.1.3 Termination of accounts

8.1.1.4 Recertification of accounts

8.1.2 Requirements

8.1.2.1 High Availability Requirement

8.1.2.2 High Performance Requirement

8.1.2.3 Auditability

8.1.2.4 Recoverability

8.1.2.5 Access Control Requirement

8.2 Information

8.2.1 Identifiers and Credentials

8.2.2 Protection of secrets

8.2.2.1 Data Encoding

8.2.2.2 Hashing

8.2.2.3 Symetric Encryption

8.2.2.4 Asymetric Encryption

8.2.3 Schemas

8.2.3.1 Attributes

8.2.3.2 Data types

8.2.4 Segmentation

8.2.4.1 Organizational Units

8.3.4.3 Role based

8.3.4.4 Provisioning

Connectors

JIT Federation

8.3.5 DevOps Considerations

8.3.6 Session Management

8.3.6.1 Centralized

Memory or DB backed SSO Cookies/Tokens)

8.3.6.2 Externalized

JWT Tokens

8.3.6.3 None

Anonymous only

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 descendents

Partitioning

Replication Techniques

Recovery Local failures
Disaster Recovery
Failover

Audit and Forensics

Inheritance and structure

LDAPv3 Access Control
Configuration for performance

Active Directory Multi-Trust Relationships
Domain Controllers
Change tracking (Timestamp)

8.4.1.3 NOSQL Databases

8.4.1.4 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 Enterpise 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 New implementations

10.2 Migration scenario's

Chapter 11

IAM Knowledge Sharing

11.1 IDpro

11.2 Gartner

11.3 KuppingerCole

11.4 IIW

11.5 Bibliography