

IDPro Body of Knowledge Table of Contents

Working DRAFT

February 13, 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
4	Regulations And Laws	5
4.1	Privacy (generic)	5
4.2	Survey of Jurisdictions	5
4.2.1	SOX, HIPAA, GDPR, CBPR etc.	5
4.3	Consent management	5
5	Workforce IAM / Internal IAM	6
5.1	IAM processes	6
5.1.1	Joiner-Mover-Leaver	6
5.1.2	HR ownership	6
5.1.3	Provisioning (On-boarding and Off-boarding)	6
5.1.4	Handling Business partners' people	6
5.1.5	Re-certification	6
5.2	Analytics and Intelligence	6
6	Consumer/Citizen IAM	7
6.1	Public sector vs. private sector	7
6.2	Social media	7
6.3	Consumer journey (identification to loyal customer)	7
6.3.1	Registration of consumers	7
6.3.2	Authentication assurance (meeting LoA requirements)	7
6.3.3	Digital legacy - handling deceased persons' digital ID	7
6.4	Self-Sovereign Identity	7
6.4.1	Blockchain ID	7
7	Non-Human Entity	8
7.1	Operational Technology (OT)	8
7.2	IoT devices	8

7.2.1	IoT Sectors	8
7.2.1.1	Home Automation	8
7.2.1.2	Personal (wearables)	8
7.2.1.3	Implants	8
7.2.1.4	Plant automation	8
7.2.1.5	Vehicle	8
7.2.1.6	Smart cities	8
7.2.1.7	Agricuture	8
7.2.1.8	Buildiing/Industrial	8
7.2.1.9	Utilities	8
7.3	RPA / robotics	8
7.4	Security requirements	8
8	IAM Architecture And Solutions	9
8.1	Business System	10
8.1.1	Business Processes	10
8.1.1.1	Provisioning accounts	10
8.1.1.2	Changes to accounts	10
8.1.1.3	Termination of accounts	10
8.1.1.4	Recertification of accounts	10
8.1.2	Requirements	10
8.1.2.1	High Availability Requirement	10
8.1.2.2	High Performance Requirement	10
8.1.2.3	Auditability	10
8.1.2.4	Recoverability	10
8.1.2.5	Access Control Requirement	10
8.2	Information	10
8.2.1	Identifiers and Credentials	10
8.2.2	Protection of secrets	10
8.2.2.1	Data Encoding	10
8.2.2.2	Hashing	10
8.2.2.3	Symetric Encryption	10
8.2.2.4	Asymetric Encryption	10
8.2.3	Schemas	10
8.2.3.1	Attributes	10
8.2.3.2	Data types	10
8.2.4	Segmentation	10
8.2.4.1	Organizational Units	10
8.2.5	Public Key Infrastructure	10
8.3	Applications	10
8.3.1	Consoles	10

8.3.2	Command Line	10
8.3.3	Approval workflow	10
8.3.4	Integration Styles	10
8.3.4.1	Direct "Bind"	10
8.3.4.2	Import users	10
	Local access control	10
8.3.4.3	Role based	11
8.3.4.4	Provisioning	11
	Connectors	11
	JIT Federation	11
8.3.5	DevOps Considerations	11
8.3.6	Session Management	11
8.3.6.1	Centralized	11
	Memory or DB backed SSO Cookies/Tokens)	11
8.3.6.2	Externalized	11
	JWT Tokens	11
8.3.6.3	None	11
	Anonymous only	11
8.4	Technical	11
8.4.1	Repositories	11
8.4.1.1	Relational Database	11
	Query optimization	11
	Replication limitations	11
8.4.1.2	Directories	11
	Historical note - X.500	11
	SLAPD and its descendents	11
	Partitioning	12
	Replication Techniques	12
	Recovery	12
	Audit and Forensics	12
	Inheritance and structure	12
	LDAPv3	12
	Active Directory	12
8.4.1.3	NOSQL Databases	12
8.4.1.4	Distributed Ledger (Blockchain)	12
8.4.2	Identity Provider Services	12
8.4.3	Protocols	12
8.4.3.1	Kerberos	12
8.4.3.2	Lightweight Directory Access Protocol (LDAP)	12
8.4.3.3	SCIM	12
8.4.3.4	SAML	12

SP Initiated vs IDP Initiated	12
Bindings	12
8.4.3.5 OIDC	13
Authentications Flows	13
8.4.3.6 OAuth	13
8.4.3.7 WS-Fed	13
8.4.3.8 FIDO U2F and UAF	13
8.4.4 Enterprise control of “Cloud”	13
8.4.4.1 Public Cloud vs Private Cloud	13
8.4.4.2 Local Connectors and Gateways	13
8.4.4.3 IPSec VPN	13
8.5 Recommended Practices	13
8.5.1 Design for security	13
8.6 Governance and Administration	13
8.6.1 Audit	13
8.6.2 Monitoring	13
9 Operational Considerations	14
9.1 Account recovery	14
9.2 Call centers	14
9.3 Engagement of user for their own security	14
9.4 Security events and operations	14
10 Project Management	15
10.1 New implementations	15
10.2 Migration scenario's	15
11 IAM Knowledge Sharing	16
11.1 IDpro	16
11.2 Gartner	16
11.3 KuppingerCole	16
11.4 IIW	16
11.5 Bibliography	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

Chapter 4

Regulations And Laws

4.1 Privacy (generic)

4.2 Survey of Jurisdictions

4.2.1 SOX, HIPAA, 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 requirements)

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 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 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

8.3.4.3 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 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 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