

IDPro Body of Knowledge Table of Contents  
Working DRAFT

July 31, 2019

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
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
<b>2</b>	<b>Digital Identity</b>	<b>2</b>
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
<b>3</b>	<b>Access Control</b>	<b>3</b>
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
<b>4</b>	<b>Regulations and Laws</b>	<b>5</b>
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
<b>5</b>	<b>Workforce IAM / Internal IAM</b>	<b>6</b>
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	Role Management . . . . .	6
5.1.5	Re-certification . . . . .	6
5.2	Compliance . . . . .	6
5.3	Analytics and Intelligence . . . . .	6
5.4	Handling Business Partners' People . . . . .	6
<b>6</b>	<b>Consumer/Citizen IAM</b>	<b>7</b>
6.1	Consumer Journey (identification to loyal customer) . . . . .	7
6.1.1	Registration of Consumers . . . . .	7
6.1.2	Authentication Assurance (meeting LoA requirements) . . . . .	7
6.2	Industry Considerations . . . . .	7
6.2.1	Public Sector vs. Private Sector . . . . .	7
6.2.2	Financial Services . . . . .	7
6.2.3	Healthcare . . . . .	7
6.3	Social Sign-up and Sign-on . . . . .	7

<b>7 Non-Human Entity</b>	<b>8</b>
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 Agriculture	8
7.2.1.8 Building/Industrial	8
7.2.1.9 Utilities	8
7.3 RPA / robotics	8
7.4 Security requirements	8
<b>8 IAM Architecture and Solutions</b>	<b>9</b>
8.1 Business System	9
8.1.1 Business Processes	9
8.1.1.1 Recertification of accounts	9
8.2 Information/Data Architecture	9
8.3 Application Portfolio	9
8.3.1 APIs	9
8.3.1.1 HTTP	9
8.3.1.2 S/LDAP	9
8.3.1.3 RACF	9
8.3.1.4 XACML	9
8.4 Technical	9
8.4.1 Repositories	9
8.4.1.1 Relational Database	9
Query optimization	9
Replication limitations	9
8.4.1.2 Directories	10
Historical note - X.500	10
SLAPD and its descendants	10
8.4.1.3 NoSQL databases	10
Graph Databases	10
8.4.1.4 Identity Provider (IdP) Trends	10
Distributed Ledger (Blockchain)	10
8.4.2 Identity Provider Services	10
8.4.3 Protocols	10

8.4.3.1	Kerberos . . . . .	10
8.4.3.2	Lightweight Directory Access Protocol (LDAP) . . . . .	10
8.4.3.3	SCIM . . . . .	10
8.4.3.4	SAML . . . . .	10
	SP Initiated vs IDP Initiated . . . . .	10
	Bindings . . . . .	10
8.4.3.5	OIDC . . . . .	10
	Authentications Flows . . . . .	10
8.4.3.6	OAuth . . . . .	11
8.4.3.7	WS-Fed . . . . .	11
8.4.3.8	FIDO U2F and UAF . . . . .	11
8.4.4	Enterprise control of “Cloud” . . . . .	11
	8.4.4.1 Public Cloud vs Private Cloud . . . . .	11
	8.4.4.2 Local Connectors and Gateways . . . . .	11
	8.4.4.3 IPsec VPN . . . . .	11
8.5	Recommended Practices . . . . .	11
8.5.1	Design for security . . . . .	11
8.6	Governance and Administration . . . . .	11
8.6.1	Audit . . . . .	11
8.6.2	Monitoring . . . . .	11
<b>9</b>	<b>Operational Considerations</b>	<b>12</b>
9.1	Account recovery . . . . .	12
9.2	Call centers . . . . .	12
9.3	Engagement of user for their own security . . . . .	12
9.4	Security events and operations . . . . .	12
<b>10</b>	<b>Project Management</b>	<b>13</b>
10.1	New implementations . . . . .	13
10.2	Migration scenario’s . . . . .	13
<b>11</b>	<b>IAM Knowledge Sharing</b>	<b>14</b>
11.1	IDPro . . . . .	14
11.2	Gartner . . . . .	14
11.3	KuppingerCole . . . . .	14
11.4	IIW . . . . .	14
11.5	Bibliography . . . . .	14
11.6	. . . . .	14

<b>12 Advanced Topics – Parking Lot</b>	<b>15</b>
12.1 Digital Legacy - handling deceased persons' digital ID (Advanced Topic)	15
12.2 Self-Sovereign Identity . . . . .	15
12.2.1 Blockchain ID . . . . .	15

# **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**

# **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 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 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**

**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**