# Introduction

## Information security

### Trust (say more - what is this?)

## Privacy

## Identification and authentication

### Context and Identity

### Levels of Assurance

## The Business Case for IAM

### Workforce IAM

### Consumer/Citizen IAM

# Digital Identity

### Definition

#### Reputation

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

### Identifiers

### Digital Identity Lifecycle ?

### Mapping to human or device

### Proofing - we need to avoid this word there are no proofs - can use use binding or registration? Or verification/validation

### Credentials

# Access Control

## Authentication

### Dynamic Authentication (risk-based)

### Multi-Factor Authentication

### Single Sign-on within a domain

### Centralised authentication service

### Federated Authentication (between domains)

### Device identity for corroboration

### Fast Identity Online (FIDO) and its cousins

### Session Management

## Authorization

### Resources to protect

### Authorisation

#### ACL’s

#### RBAC

#### ABAC / dynamic access management

##### Policy Management solutions

### Privileged Access Management

#### Alignment to Risk Management

# Regulations and Laws

### Privacy (generic)

### Survey of Jurisdictions

#### SOX, HiPPA, GDPR, CBPR etc.

### Consent management

# Workforce IAM / Internal IAM

## IAM processes

### Joiner-Mover-Leaver

### HR ownership

### Provisioning (On-boarding and Off-boarding)

### Handling Business partners’ people

### Re-certification

### Analytics and Intelligence

# Consumer/Citizen IAM

## Public sector vs. private sector

## Social media

## Blockchain ID / SSI

## Registration of consumers

## Authentication assurance (meeting LoA requiremetns)

## Consumer journey (identification to loyal customer)

## Digital legacy - handling deceased persons’ digital ID

# Self-Soverign Identity

# Non-Human Entity

## Operational Technology (OT)

## IoT devices

### IoT Sectors

#### Home Automation

#### Personal (wearables)

#### Implants

#### Plant automation

#### Vehicle

#### Smart cities

#### Agricuture

#### Buildiing/Industrial

#### Utilities

## RPA / robotics

## Security requirements

# IAM architecture and solutions

## Business System

### Business Processes

#### Provisioning accounts

#### Changes to accounts

#### Termination of accounts

#### Recertification of accounts

### Requirements

#### High Availability Requirement

#### High Performance Requirement

#### Auditability

#### Recoverability

#### Access Control Requirement

## Information

### Identifiers and Credentials

### Protection of secrets

#### Data Encoding

#### Hashing

#### Symetric Encryption

#### Asymetric Encryption

### Schemas

#### Attributes

#### Data types

### Segmentation

#### Organizational Units

### Public Key Infrastructure

## Applications

### Consoles

### Command Line

### Approval workflow

### Integration Styles

#### Direct “Bind”

#### Import users

##### Local access control

#### Role based

#### Provisioning

##### Connectors

##### JIT Federation

### DevOps Considerations

### Session Management

#### Centralized

##### Memory or DB backed SSO Cookies/Tokens)

#### Externalized

##### JWT Tokens

#### None

##### Anonymous only

## Technical

### Repositories

#### Relational Database

##### Query optimization

##### Replication limitations

#### 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)

#### NOSQL Databases

#### Distributed Ledger (Blockchain)

### Identity Provider Services

### Protocols

#### Kerberos

#### Lightweight Directory Access Protocol (LDAP)

#### SCIM

#### SAML

##### SP Initiated vs IDP Initiated

##### Bindings

#### OIDC

##### Authentications Flows

#### OAuth

#### WS-Fed

#### FIDO U2F and UAF

### Enterpise control of “Cloud”

#### Public Cloud vs Private Cloud

#### Local Connectors and Gateways

#### IPSec VPN

## Recommended Practices

### Design for security

## Governance and Administration

### Audit

### Monitoring

# Operational Considerations

## Account recovery

## Call centers

## Engagement of user for their own security

## Security events and operations

# Project Management

## New implementations

## Migration scenario’s

# IAM Knowledge sharing

## IDpro

## Gartner

## KuppingerCole

## IIW

## Bibliography