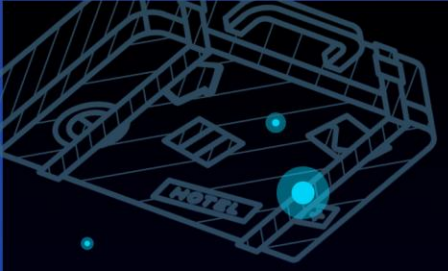
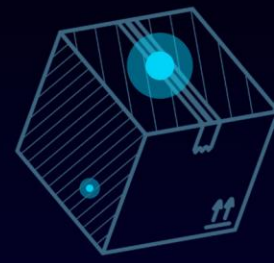
Introduction to Identity







Lance Peterman

Adjunct Professor

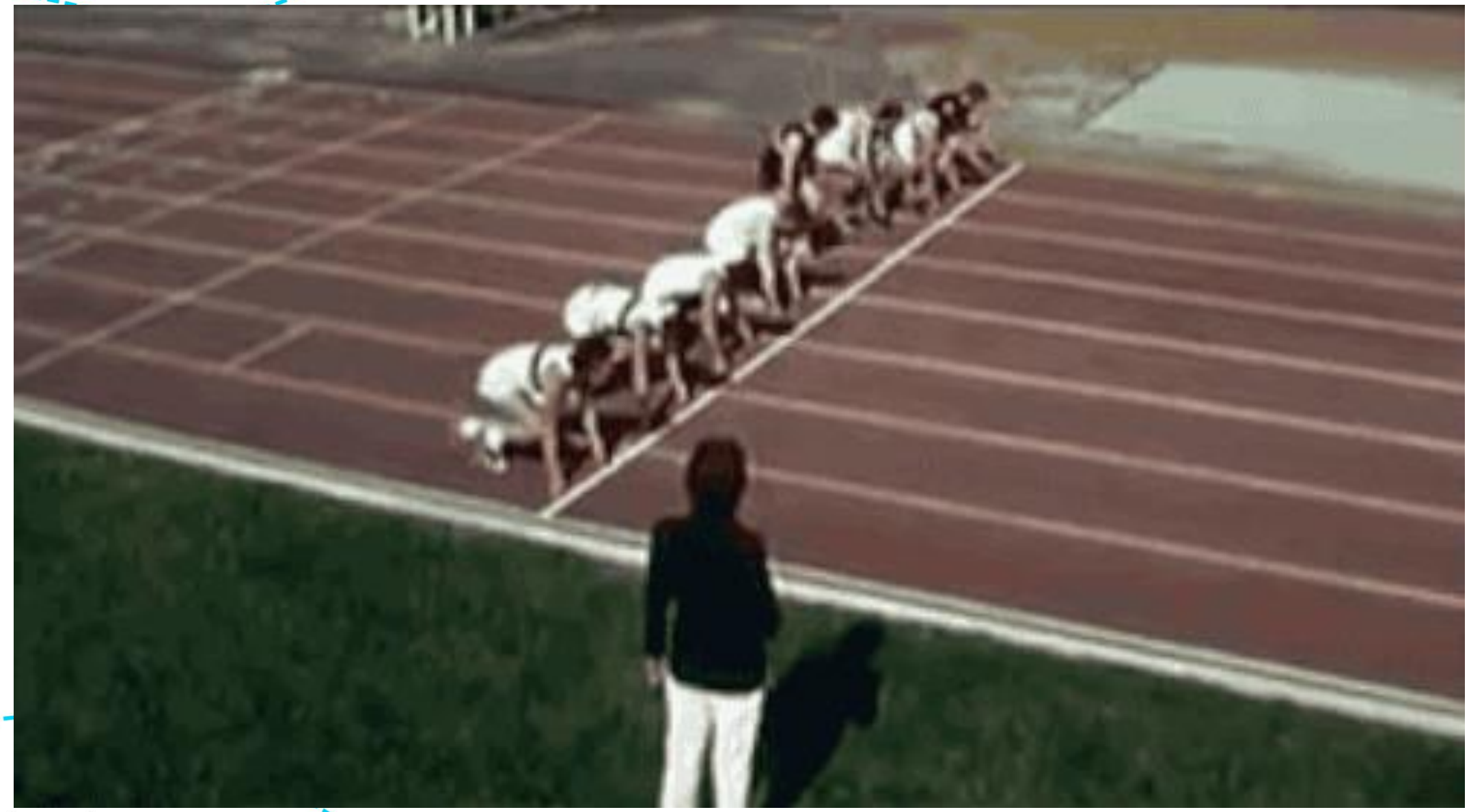
University of North Carolina at Charlotte

Espen Bago

Identity Program Owner

Norwegian Labour and Welfare Administration

Of what kind is the Identity race?



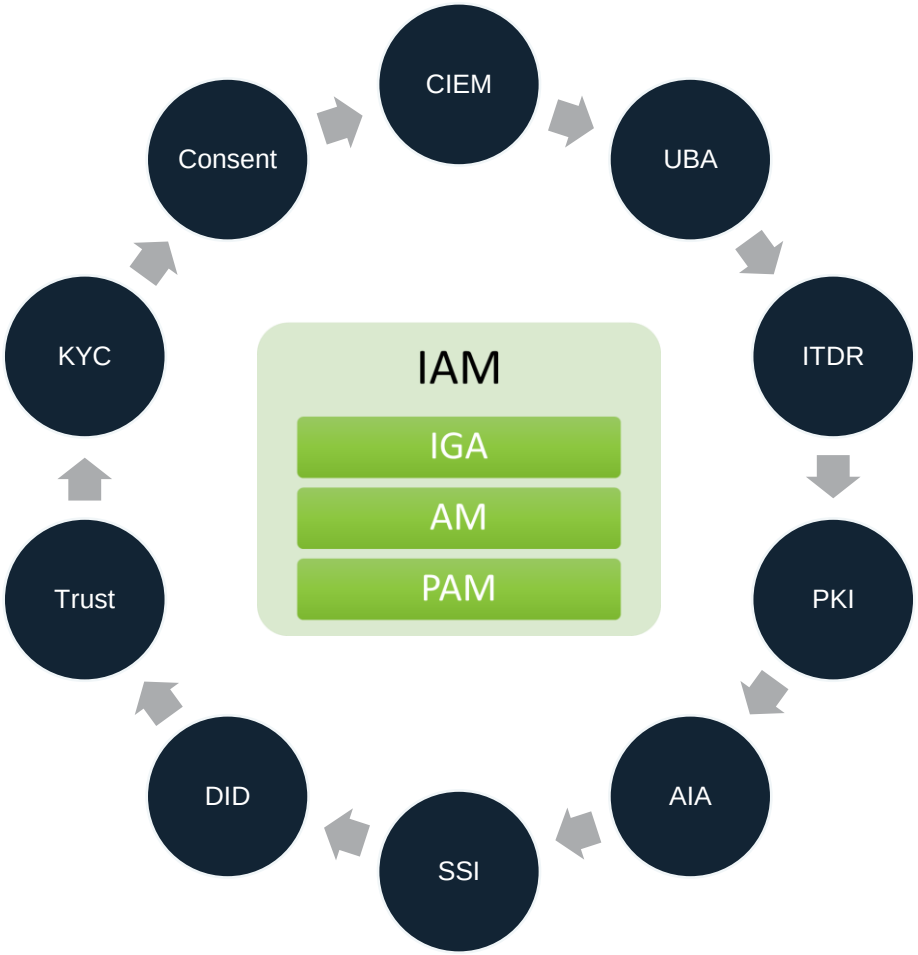
And what is this
- field
- area
- industry
- discipline
- specialty
- ..

of
- Digital Identity
- IAM
- IAG
- IDM/AM/PAM/..
- Access / Identity
- …… control
- …… governance
- …… management
- ..

?

A lot of things, not just

A lot of things, not just



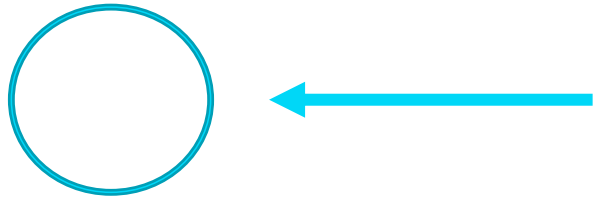
And who is it for?

identity professionals
developers
PMs
auditors
product owners
executives
..

serving

consumers
workers
contractors
citizens
partners
friends
services
devices
..

Enter The Value to be protected



An object

Objects of value worth protecting

Stuff I own

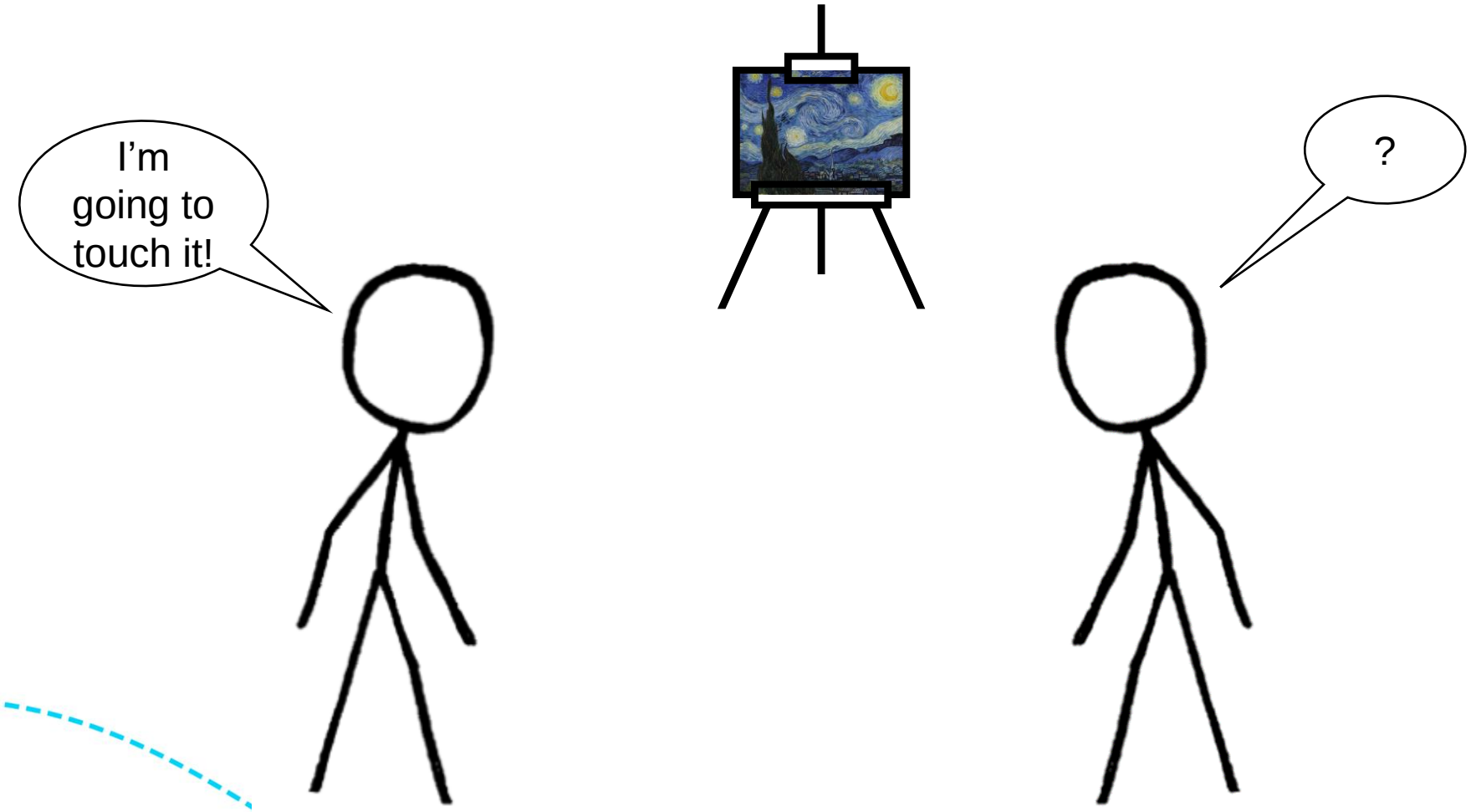
Stuff somebody manages for me

Stuff I manage for somebody

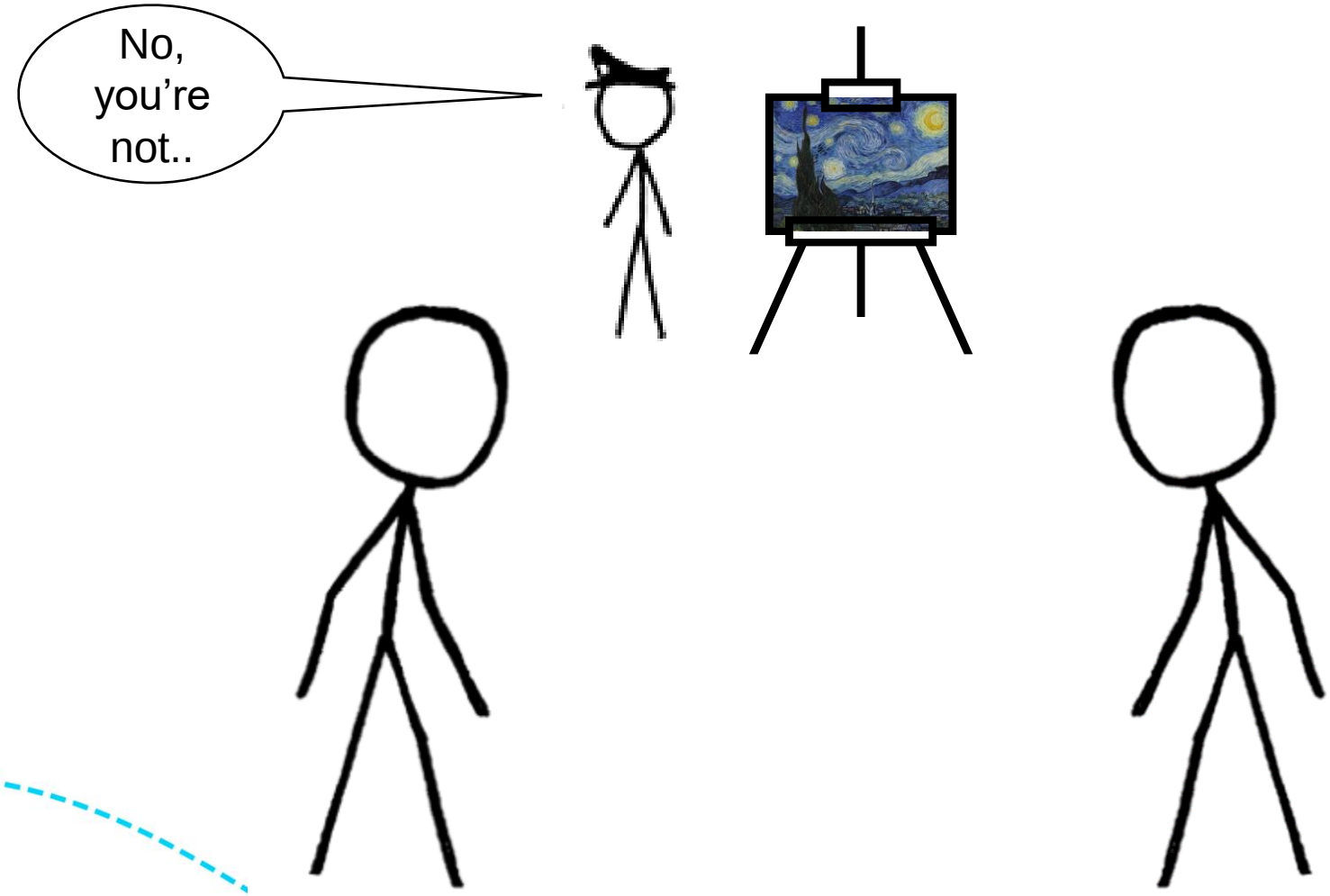
- Information
- Money
- Tools
- Resources
- Anything not limitless
- Anything subject to a (financial) transaction

Objects vs Subjects

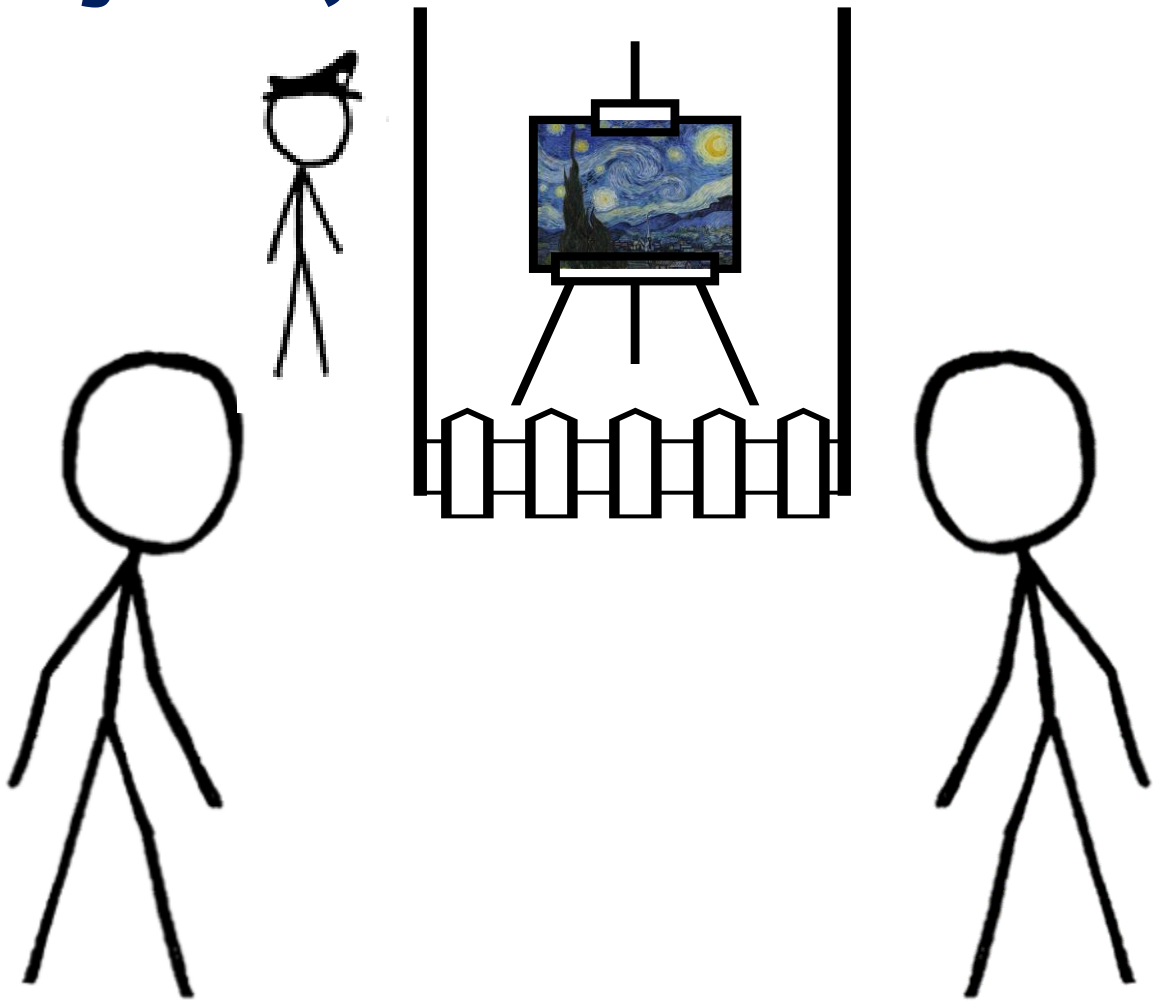
Objects, Subjects and Rules

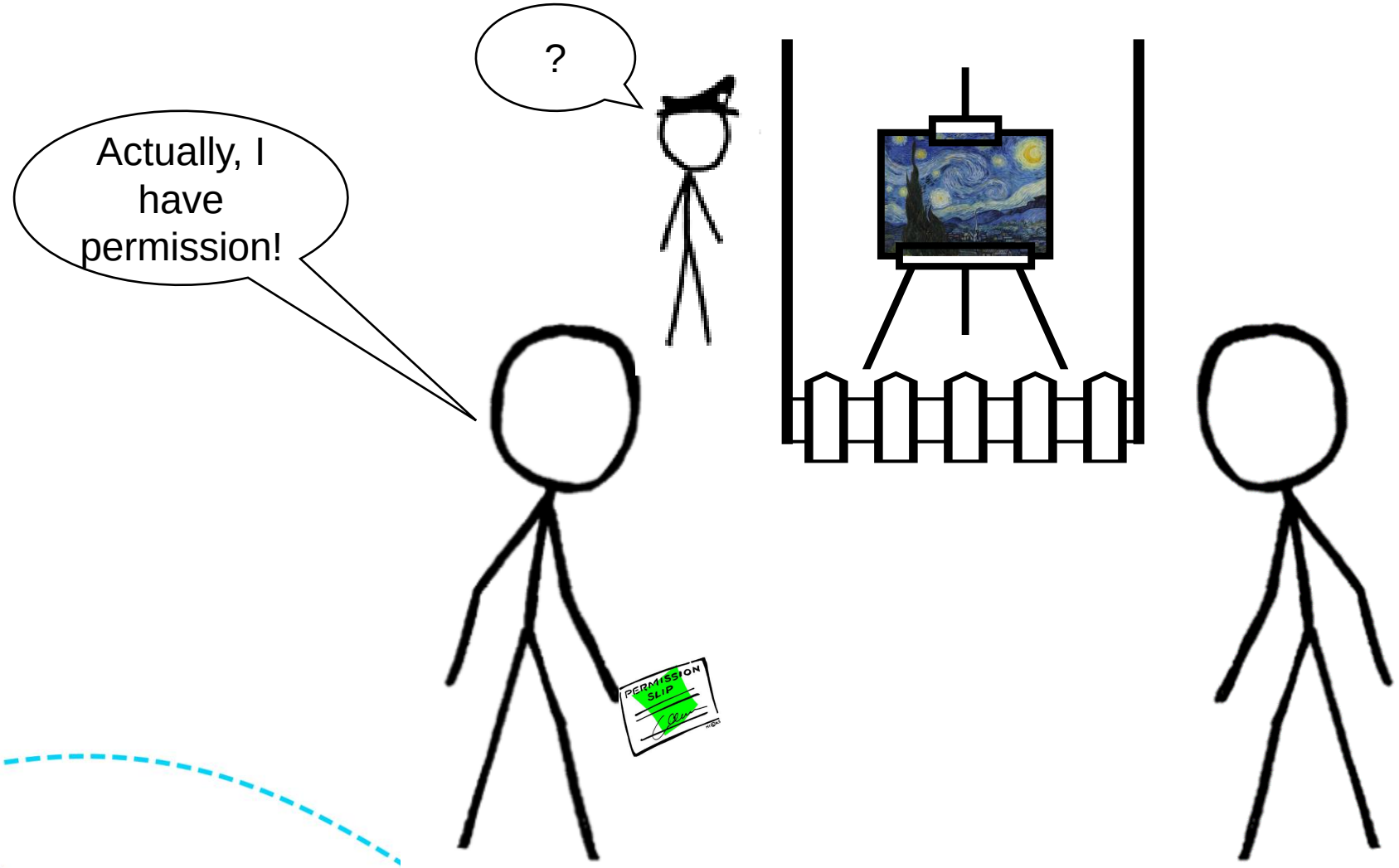


Objects, Subjects and Rules



Objects, Subjects, Rules and Barriers

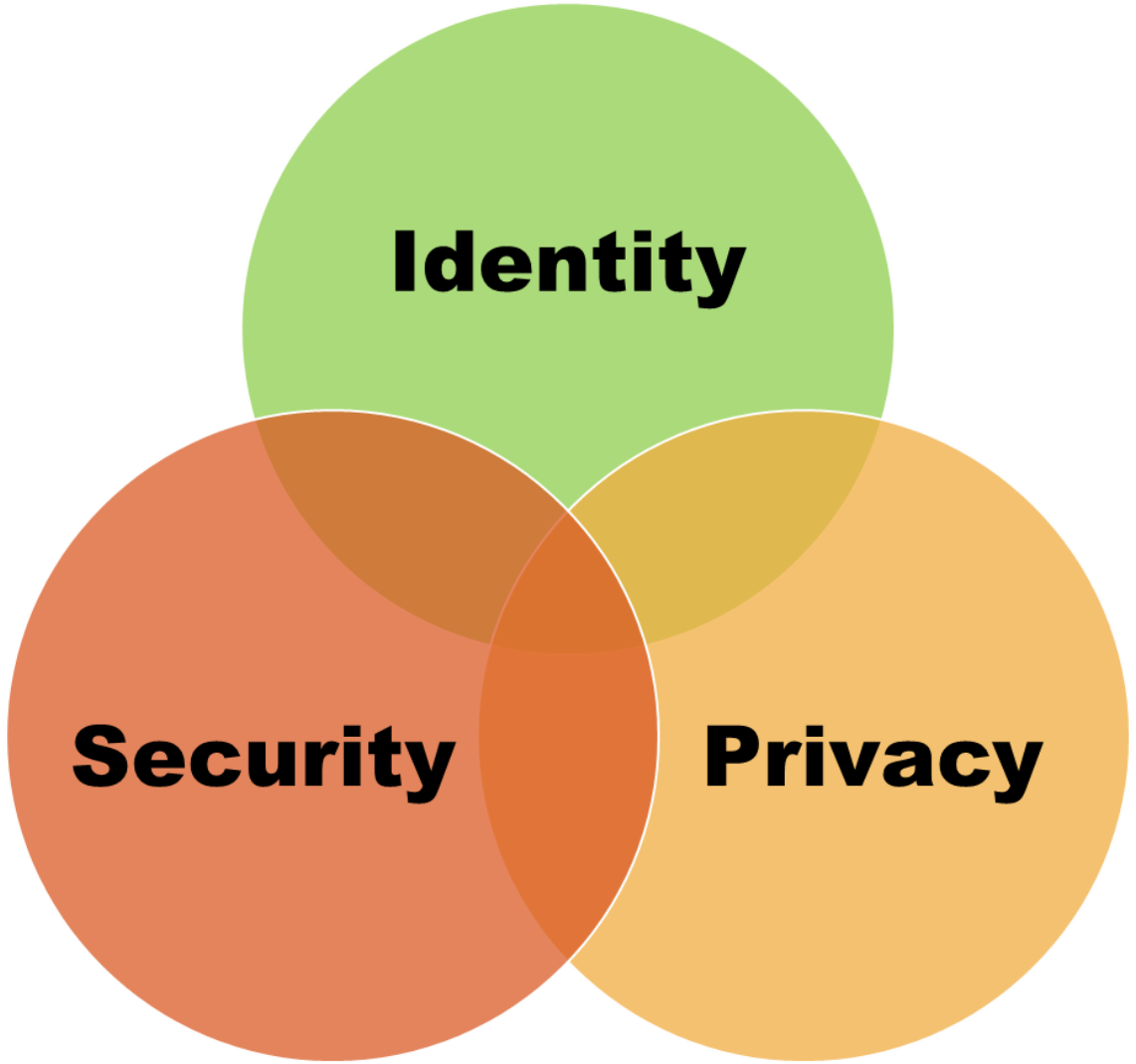


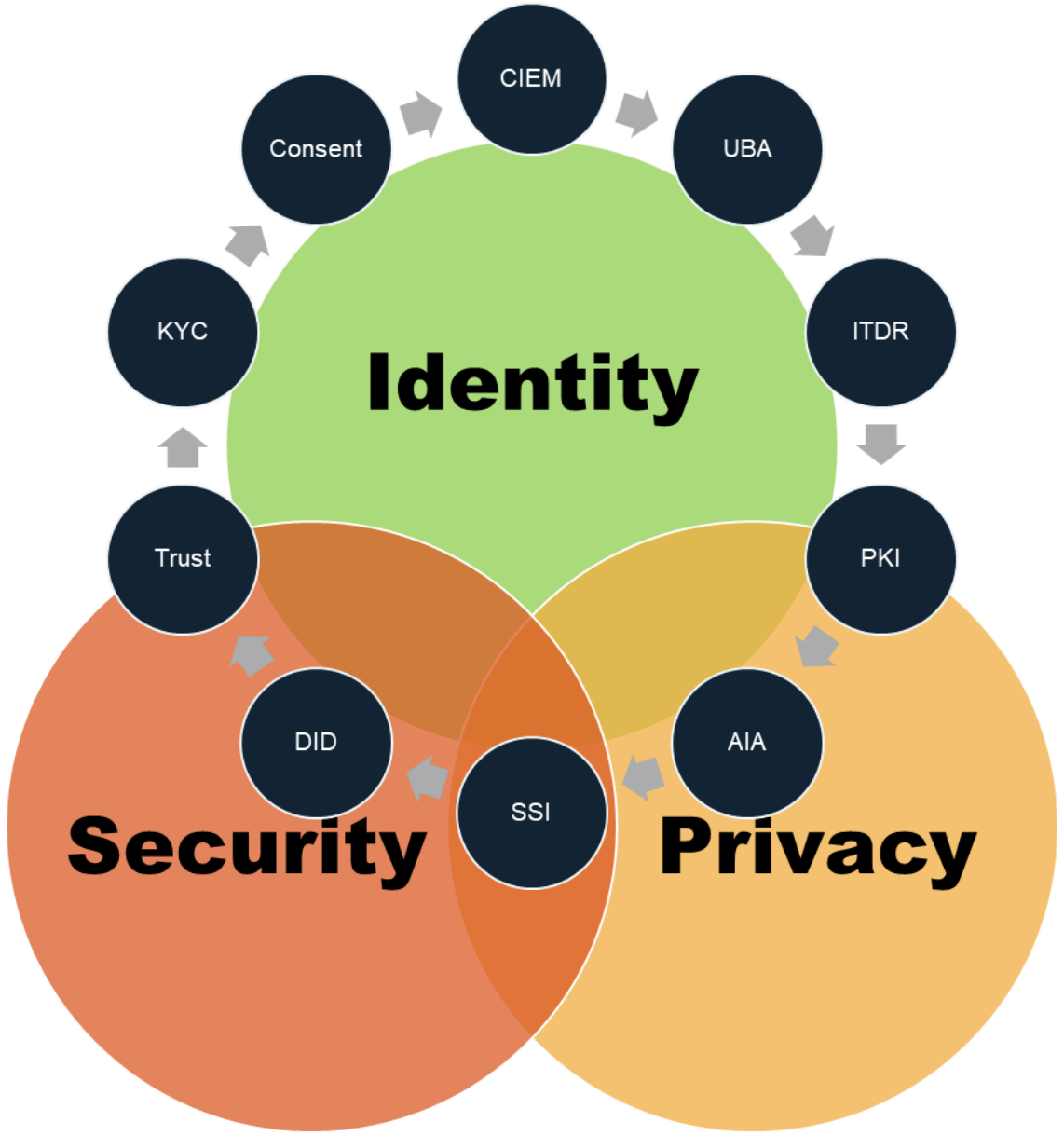

?
Actually, I have permission!
PERMISSION SLIP

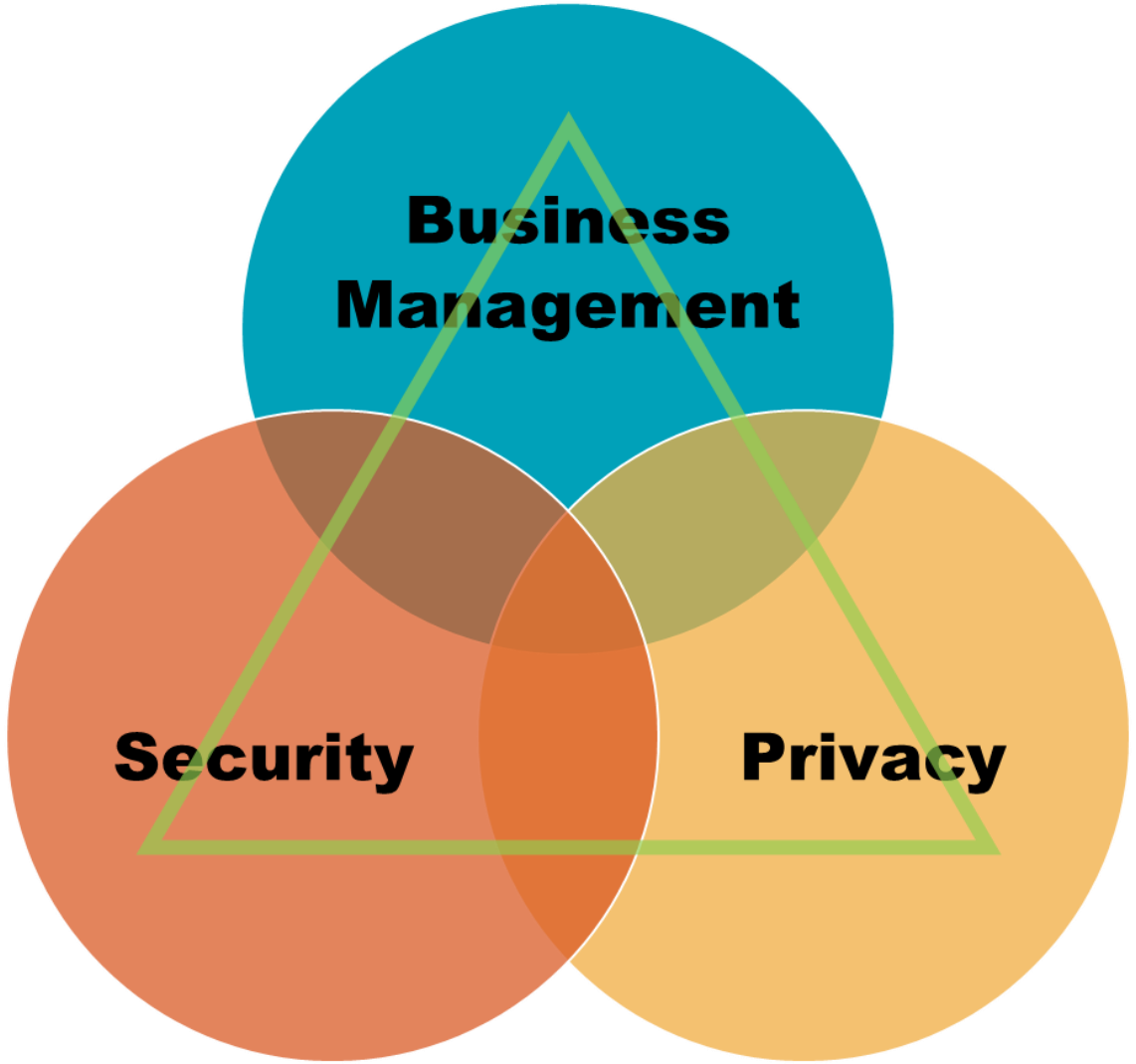
Bearer Token

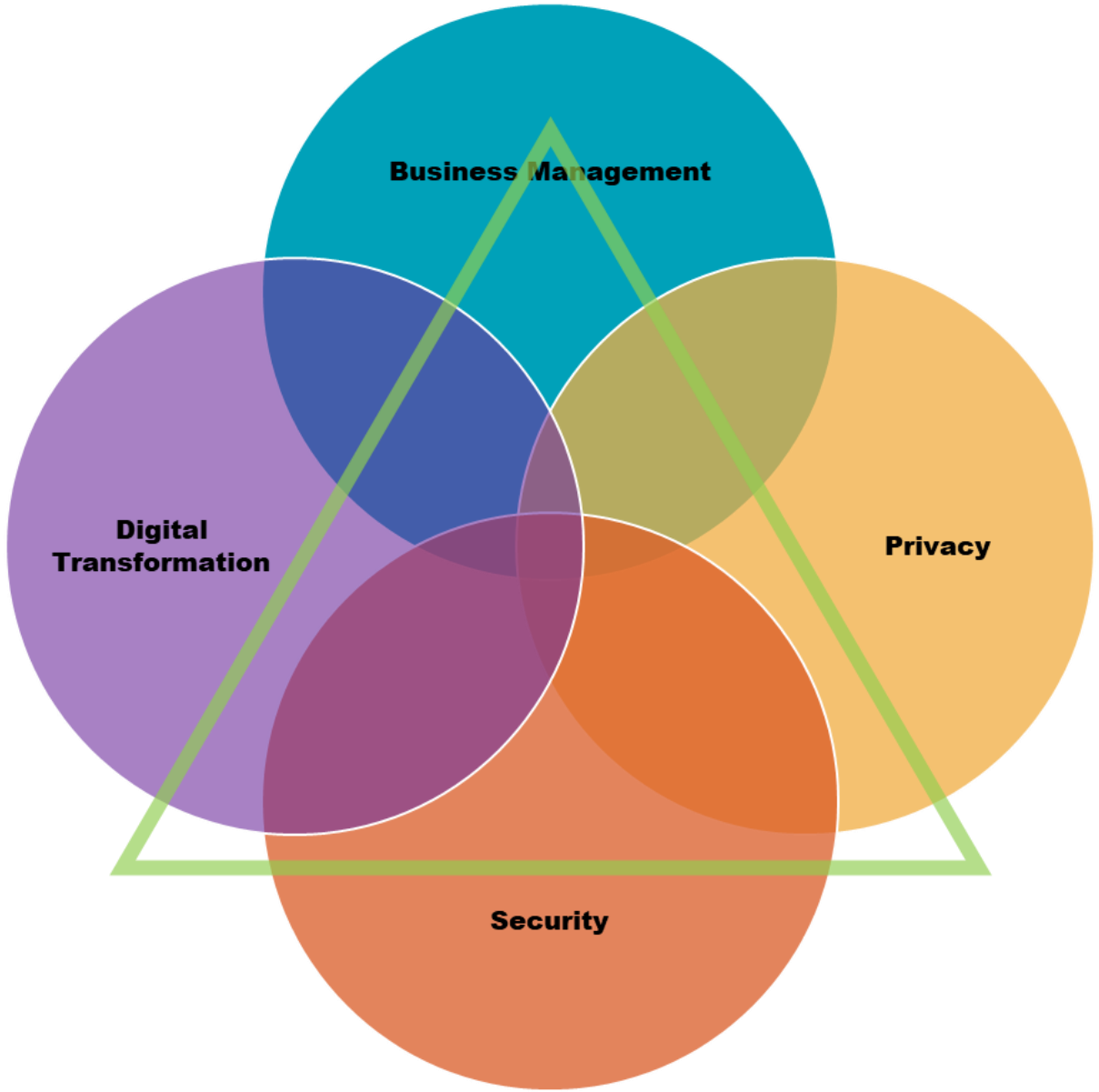
```
{
  "iss": "http://idp.example.com",
  "sub": "248289761001",
  "aud": "http://sp.example.com",
  "jti": "_d71a3a8e9fcc45c9e9d248ef7049",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "nbf": 1311280970,
  "acr": "phrh",
  "amr": "face",
  "uid": "NAV_ident_ebago"
}
```

(Stick figures reprinted with permission from xkcd.com)


Identity
Security
Privacy


CIEM
Consent
UBA
KYC
ITDR
Identity
Trust
PKI
DID
AIA
SSI
Security
Privacy


Business Management
Security
Privacy


Business Management
Digital Transformation
Privacy
Security

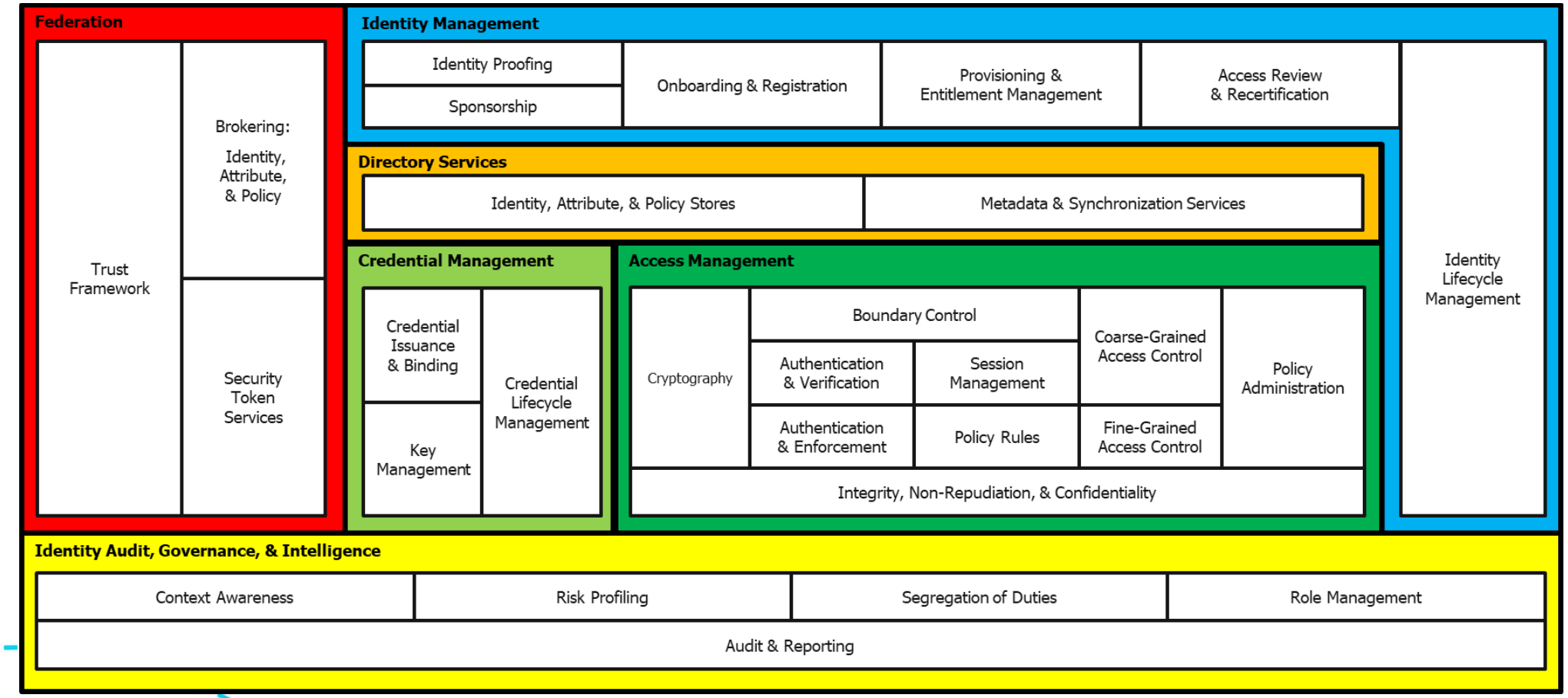
CIA perspective

Confidentiality	Integrity	Availability
• measures designed to prevent sensitive information from unauthorized access attempts. • It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. • More or less stringent measures can then be implemented according the required level of confidentiality (e.g. encryption, access control measures)	• involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. • Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality). • More or less stringent measures can then be implemented according the required level of integrity (e.g. access control, access monitoring, data input controls)	• means information should be consistently and readily accessible for authorized parties. • This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information. • More or less stringent measures can then be implemented according the required level of availability (e.g. fail-over, data recovery capabilities)

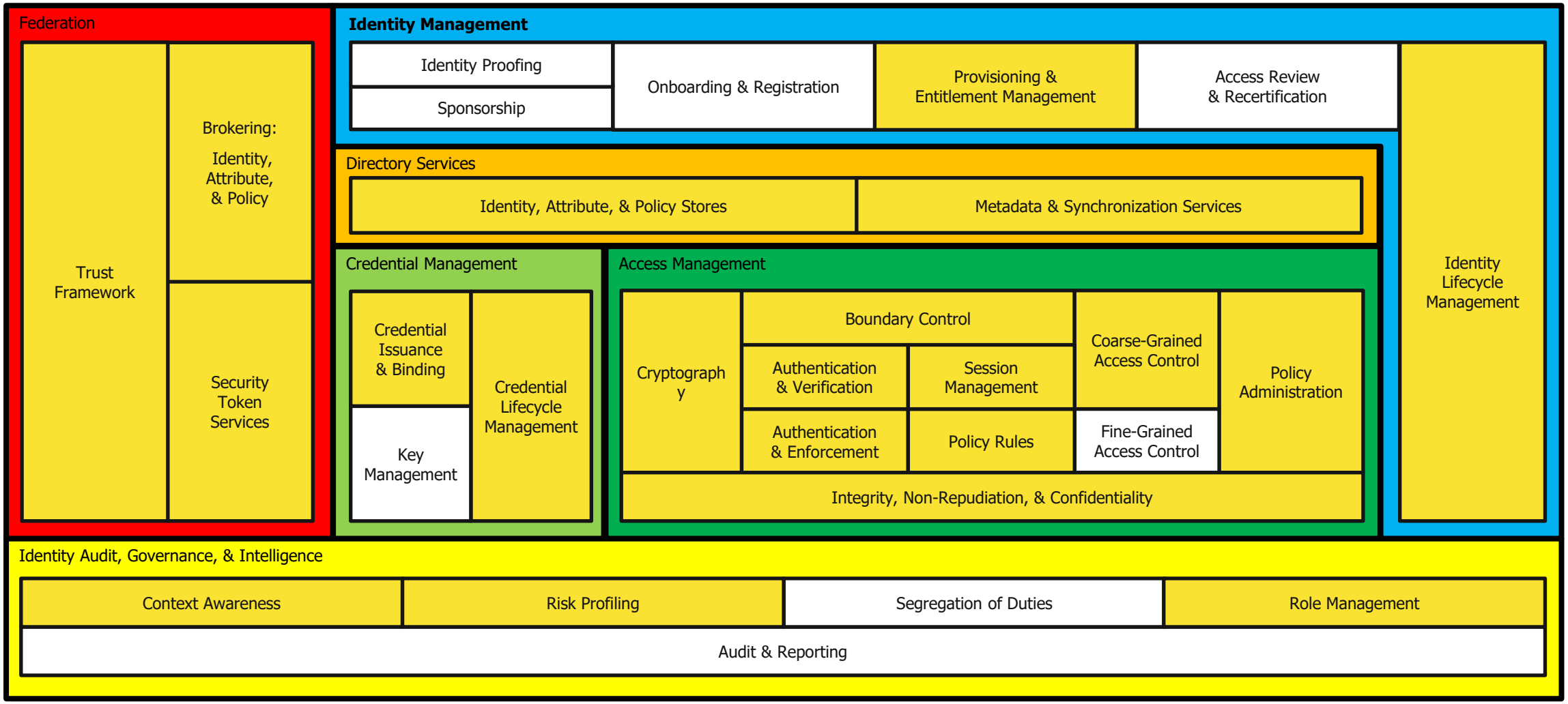
Investor or market perspective

Source: Liminal, 2023

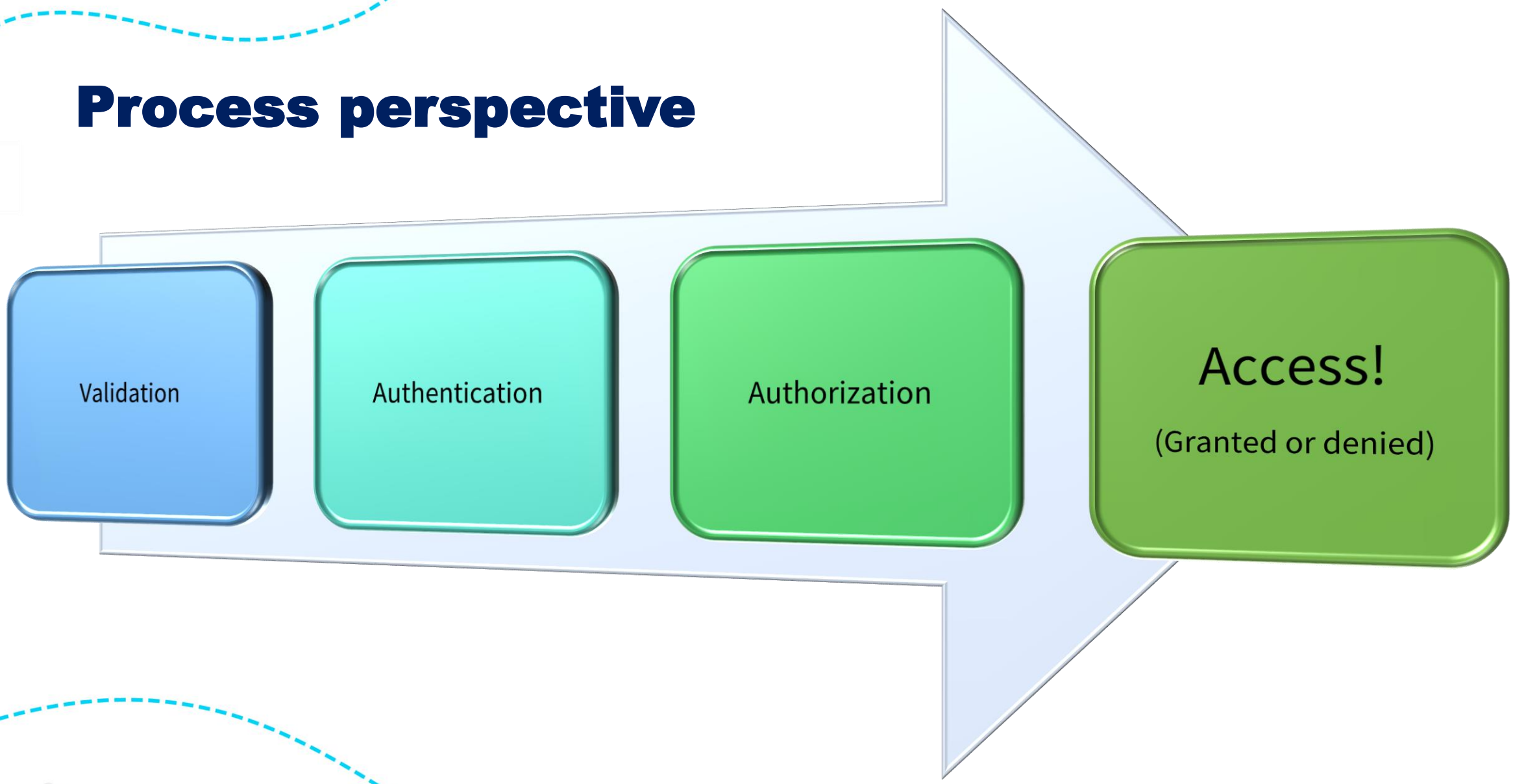
Architecture perspective

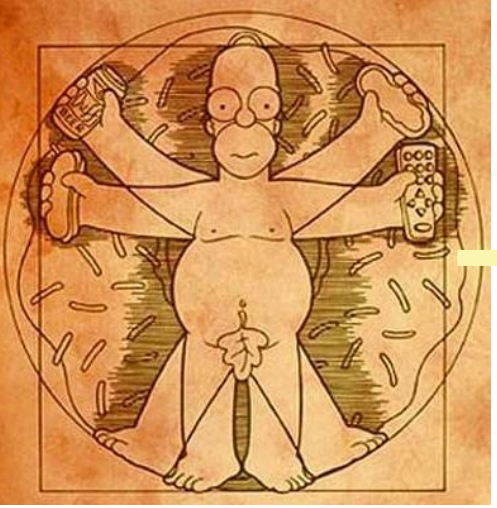


User accesses SaaS app



Process perspective





What if there's a **robot** or some other inhuman thing in between here?

Passwords here (until they aren't..)

ABAC, Access Control ++

For AuthZ we often need to do more lookups for additional data from the swarm

Consent

Delegation «on behalf of»

KYC

Validation

AutheNtication

AuthoriZation

«I have permission»

Manual or automatic fact checking

Results in a swarm of registered data

Make «accounts»

Make «tokens» (for logged in sessions)

Can be used to reference/find attributes to check

But wait, there's more! We also need: Usage data (monitoring, detection, re-checking), stronger mechanisms for high risk accesses, UX++

Let’s structure this

The overall process you’re in uses various functions and mechanisms to achieve **good enough protection**.

Apart from the initial *setup*, the functions are *executing* at different places in the process.

Admin-time vs Run-time

The Process/Timeline requires preparation

- The **Run-time** elements of AuthN and AuthZ require support and preparation.
- The **Admin-time** elements have that job:
  - Cataloguing
  - Classification
  - Governance
  - Lifecycle
- Related:
  - Models for Proofing
  - Models for Authorization
  - Definition and identification of Privileged Access

When are they executed

Admin-time

- In preparation or support for later functions
- Potentially continuous
- Huge potential for automation

Run-time

- At the moment when someone attemps to access the value

Admin-time (aka Config-time, Design-time)

- Cataloguing facts into (Directories, Repositories)
  - “Sources of Truth”
- Classification
  - To prioritize, we need to know the difference between accesses/values
- Governance
  - Every function we set up should be controlled
- Lifecycle
  - Take the necessary actions both at the start, middle and end

Run-time

- Authentication
  - Including Federation
- Authorization

Both?

Some are harder to place

- Proofing, Validation
- Analytics
  - Static typically admin-time
  - Event-based typically run-time
- “PAM” – Handling extra-privileged access
  - E.g. Secrets Management, Just-in-time elevation++
  - PAM is in many ways a mini, mirror universe of Identity and Access

Authentication

Authentication

“Give me your *identifier* and assure me that it represents you”

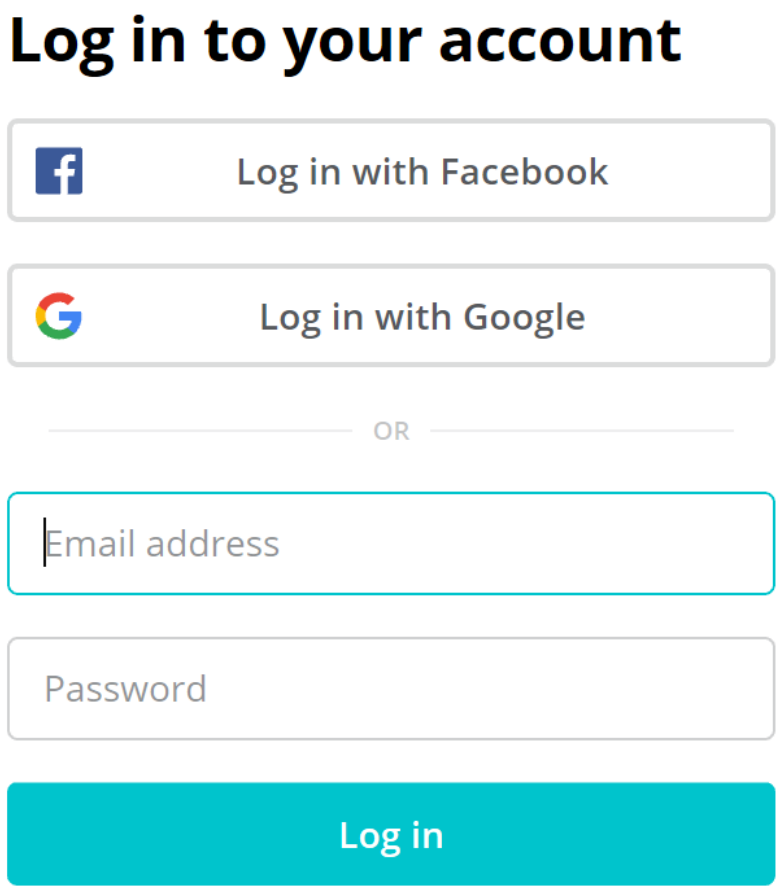
The authentication function takes identifiers as input and aims produce as output:

Confirmation that supposed users are who they say they are.

(Whereas *Authorization* gives those users permission to access a resource, a value.)

Authentication

- Using the established data to bind to something. Why? How?
- Federation
  - Collaborative / Joint Authentication
  - Centralized Authentication – SSO



Identifiers are not factors

Authenticators *are* factors

So email + password is not 2-factor

Authentication: Multi-factor, Adaptive

Active (*challenge*) factors:

- Knowledge – something (only) you know
- Possession – something (only) you have
- Inherence – something (only) you are

Passive (*context*) factors:

- Location, time, behavior, patterns

But what about

- Password managers
- Passkeys

Authorization

Authorization

- OK, you’re authentic and legit – but where can you go?
  - Access all areas
- Principle of least privilege (impossible in practice – why?)
- What data do authorization checks require?
- How do we implement this?
- Authorization decisions
  - If there is a rule (policy) to follow – is it evaluated by a human or by code?
  - Good and bad access policies

Authorization models, standards and frameworks

- Model: abstract approach to implementing authorization e.g. ACL, RBAC, and ABAC.
- Standard: a formally approved set of specifications that define how to address authorization e.g. SAML, XACML, OAuth(!)
- Framework: a technical implementation that handles authorization without being a standard itself e.g. Ruby cancancan, OPA, Oso's Polar, Google's Zanzibar or AWS' Cedar.

David Brossard - https://idpro.org/the-state-of-the-union-of-authorization

Governance

Governance of Identity

- Workforce, Contractors, Partners/Businesses, Customers..
- Sources of Truth
  - Identity Repository, Account Directory, etc
- Entitlement Management
- Access request, approval and re-approval
- Roles
- Policies
- Audit and reporting
- Lifecycles of all of the above

Sources of «Truth»

An authoritative place to go where you can learn about a person

- B2E: HR
- B2B: the partner's HR, a delegated admin, their federation service
- B2C: the individual, their social persona, a government (G2C)
- B2B2C

User Provisioning & Lifecycle Management

- Creates, Maintains, and Removes objects such as user accounts in managed systems
- Automatable by **events** from sources of truth: Join / Move / Leave
- Can assign or remove permissions, entitlements such as group membership, roles, and profiles for authorization purposes

User Provisioning: Continued

- Can have approval processes associated with creation and changes to user accounts
- Relies on connectivity to managed systems
- That doesn't have to be fully automated... could be a manual process driven via a help desk ticket
- Relevant standard: SCIM (System for Cross Domain Identity Management)

Entitlement Management

- Applications have permissions such as "create purchase order"
- Permissions often get aggregated into entitlements for easier management
- Entitlements include groups, technical roles, business roles, profiles, permission sets
- Instead of assigning people individual permissions they are often assigned entitlements

Entitlement Mgt: Continued

- Entitlement Management involves the cataloging of assignable entitlements
- Adding meaningful descriptions
- Adding "owners"
- Mapping entitlements to job responsibilities or types of users
- "Purchasing clerks get these groups"
- "Tier 1 Partners get this profile"
- Often necessarily pre-work before doing segregation of duties analysis and enforcement

Role Management

- Individual entitlements can become hard to manage
- They can get aggregated into roles of 2 flavors:
  - Business roles = job responsibilities
  - Technical roles = collections of lower-level entitlements to enable access
- Roles, especially business roles, can be mapped to HR job codes and positions
- As well as partner classifications
- Entitlements within a role need on-going review
- Assignment rules that map roles to people need on-going review

RBAC – ABAC – PBAC + +

“X” Based Access Control

These are all perspectives on the same thing:

The input for making a Decision about Access (granted or denied)

Access Certification

- On-going review of who can access what
- Ideally a tool to prevent people from keeping access they no longer need
  - But it only works if the certifiers have stamina and the right competency for making those decisions
- Changes to entitlements can trigger reviews
- Changes to job roles can trigger reviews
- Risk events can trigger (scoped) reviews

Identity Analytics and Intelligence

- Find commonalities and outliers among user populations
- Group commonly assigned entitlements together as candidate roles
- Identified over-privileged users and other deviations
- Discovers undocumented high privileged access (HPA) rights assigned to regular, non-privileged, accounts.
- Also a tool for designing better access policies.

Validation / Proofing

- Establishes the data and the resulting data set (digital identity)
- Do we trust the data? Why? How?
- Decentralized Identity
- Self Sovereign Identity
- Verified Credentials
  - mDL
  - CIDPRO

Privileged Access

Privileged Access

- Not a well-defined term
  - PAM: A = ?
- What is more privileged than the rest?
- Why?
  - Your business must decide
  - (It probably means you must decide)
- How good is your CMDB?

Privileged Account Management

- Some user *accounts* are special e.g. sysadmin, root, etc
- Access to accounts like these and account used for service to service integration need management too even though there isn't a single user associated with them
- "Check out" access to root
- Record actions users take while in a privileged state
- Scramble passwords to protect special accounts

Other concepts

Recovery

- Account recovery
- Credential recovery
- Identity recovery
- Biometric recovery

If the cat’s out of the bag.. (Can everything be recovered?)

Assurance

- A central concept in Identity and Access
- How certain are we
  - That a thing is what it is presented as
  - That a thing is the same as the last time we trusted it
  - That someone we trust (Federation) are doing the right thing
- NIST Computer Security Resource Center
  - Special publication: 800-63-4

Attack types (Security purposes)

- Account Takeover
  - Digital means of accessing values are vulnerable
  - And harder to secure than physical?
  - Because they are abstract and complex

ITDR

Identity Threat Detection and Response

- An interesting combination of functionality – is it real?
- Detection is important and Security Operations Centers could be better at understanding Identity event
- Response includes the capability to recover, for example from Identity/Access centric backups
- Compare with SOAR

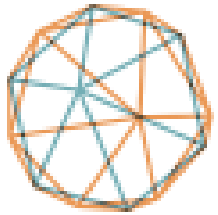
CIEM

Cloud Infrastructure Entitlement Management

- Cloud vs not-Cloud: How does this matter?
  - Is Cloud always more complex?
  - Is on-premise and legacy a «solved problem»?

Educational and other resources

- idpro.org/educational-resources/
- idpro.org/body-of-knowledge/
- idpro.org/cidpro/
- identiverse.com/videos/
- incommon.org/academy/iamonline/
- pages.nist.gov/800-63-4/ (Digital Identity Guidelines)
- idsalliance.org/ (Identity Defined Security Alliance)
- fidoalliance.org/fido2



IDPRO®

a professional association for identity management that exists to globally foster ethics and excellence in the practice and profession of digital identity.


identiverse
#identiverse