

Roundtable Access Governance

13-09-2023

André Koot

André Koot

- Security & IAM Consultant
- Author/trainer IMF-online
- Member BoK Committee IDPro
- Former editor (in chief) PvlB Informatiebeveiliging



Julia Neleman



- Sales Consultant
- 06 - 50844453

Jerrel Abdoel



- Sales Consultant
- 06 - 31649203

SonicBee in short

Our vision:

Bring together and automate the data-driven world



Our drive:

Help organisations to use data to be better equipped to take decisions, enhance the customer experience and lower costs in a secure and compliant way of working



30

IAM business experts & growing fast



Locations:

Amsterdam (NL)
Regensburg (DE)

International (EU) growth ambitions



Founded
2020



By Patrick, André & Anne

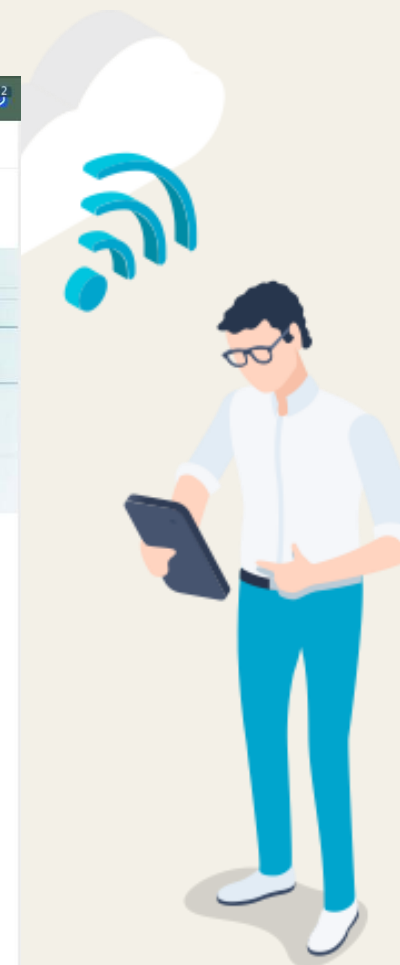
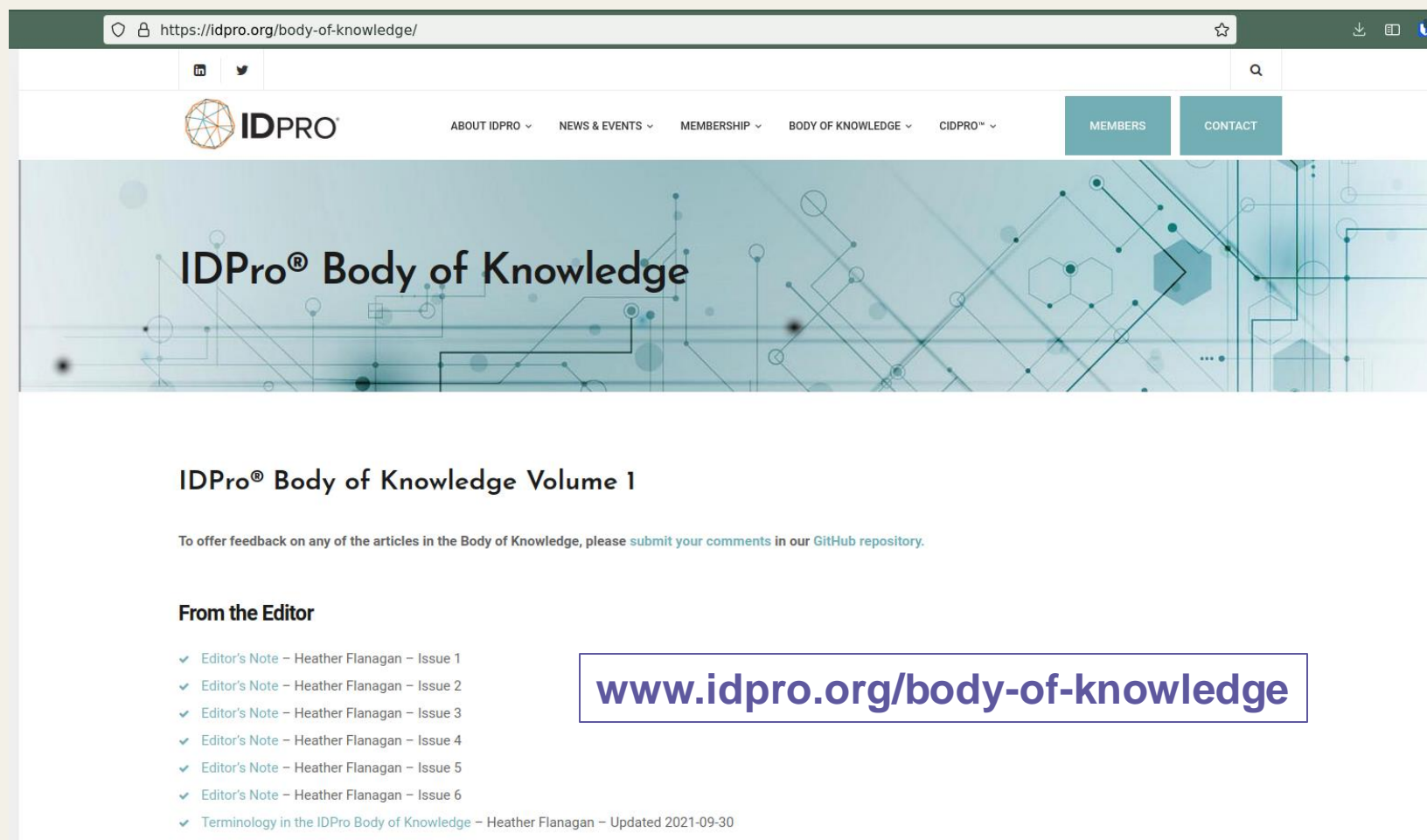
Unique business oriented IAM Advisory Services and portfolio



SaaS developments:



IDPro



Typical audit findings in identity and access audits can include:

1. Inactive or Orphaned User Accounts:

Finding user accounts that are no longer in use or associated with any active employees or contractors. These accounts should be disabled or removed to reduce security risks.

2. Excessive Permissions:

Identifying users with unnecessary or overly permissive access rights to systems, data, or applications. This can pose a security risk, as it increases the potential for misuse or data breaches.

3. Inadequate Access Controls:

Discovering instances where proper access controls and segregation of duties are not in place. This includes situations where individuals have access to both sensitive and conflicting roles or data.

4. Unauthorized Access:

Uncovering instances of unauthorized access to systems or data, potentially indicating security breaches or insider threats.

5. Weak Password Policies:

Identifying weak password policies, such as easily guessable passwords, lack of password complexity requirements, or insufficient password rotation rules.

6. Lack of Multi-Factor Authentication (MFA):

Noting situations where MFA is not implemented for systems or applications that require an extra layer of security for user authentication.

7. Inadequate User Account Monitoring:

Discovering deficiencies in monitoring and auditing user account activity and access logs, which can make it difficult to detect unauthorized or suspicious activities.

Typical audit findings in identity and access audits can include:

1. Unapproved Access Requests:

Finding instances where access requests and approvals are not properly documented or authorized according to company policies and procedures.

2. Incomplete Documentation:

Identifying gaps in documentation related to user access, roles, permissions, and changes, making it challenging to trace access and changes in the system.

3. Lack of Training and Awareness:

Observing situations where employees or users are not adequately trained or informed about security best practices and policies, which can lead to security lapses.

4. Outdated Access Reviews:

Finding that periodic reviews of user access privileges are not conducted or are not up-to-date, potentially leading to inappropriate access over time.

5. Missing Disaster Recovery and Business Continuity Plans:

Noting that plans for managing identity and access during disasters or incidents are inadequate or missing, posing a risk to business operations.

6. Vendor and Third-Party Access:

Discovering weak controls or unmonitored access granted to vendors, third-party contractors, or service providers, which can introduce security vulnerabilities.

7. Compliance Violations:

Identifying instances where the organization fails to comply with regulatory requirements or internal security policies related to identity and access management.

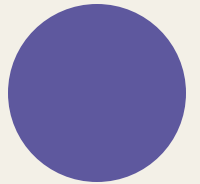
The training program



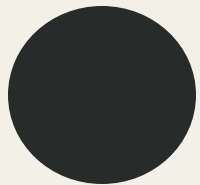
Scope of IAM



IAM is IT...?



Traditional IAM: JML, ACL, RBAC

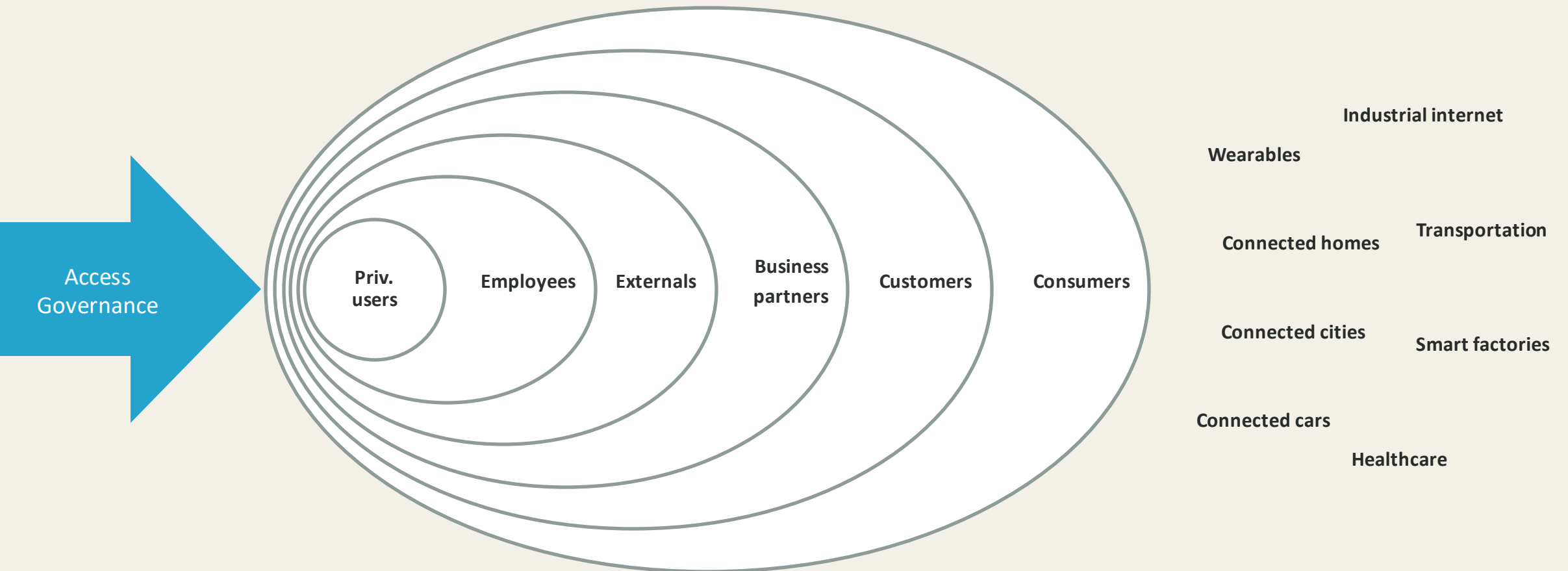


Future of IAM: PBAC and zero trust, impact on audit

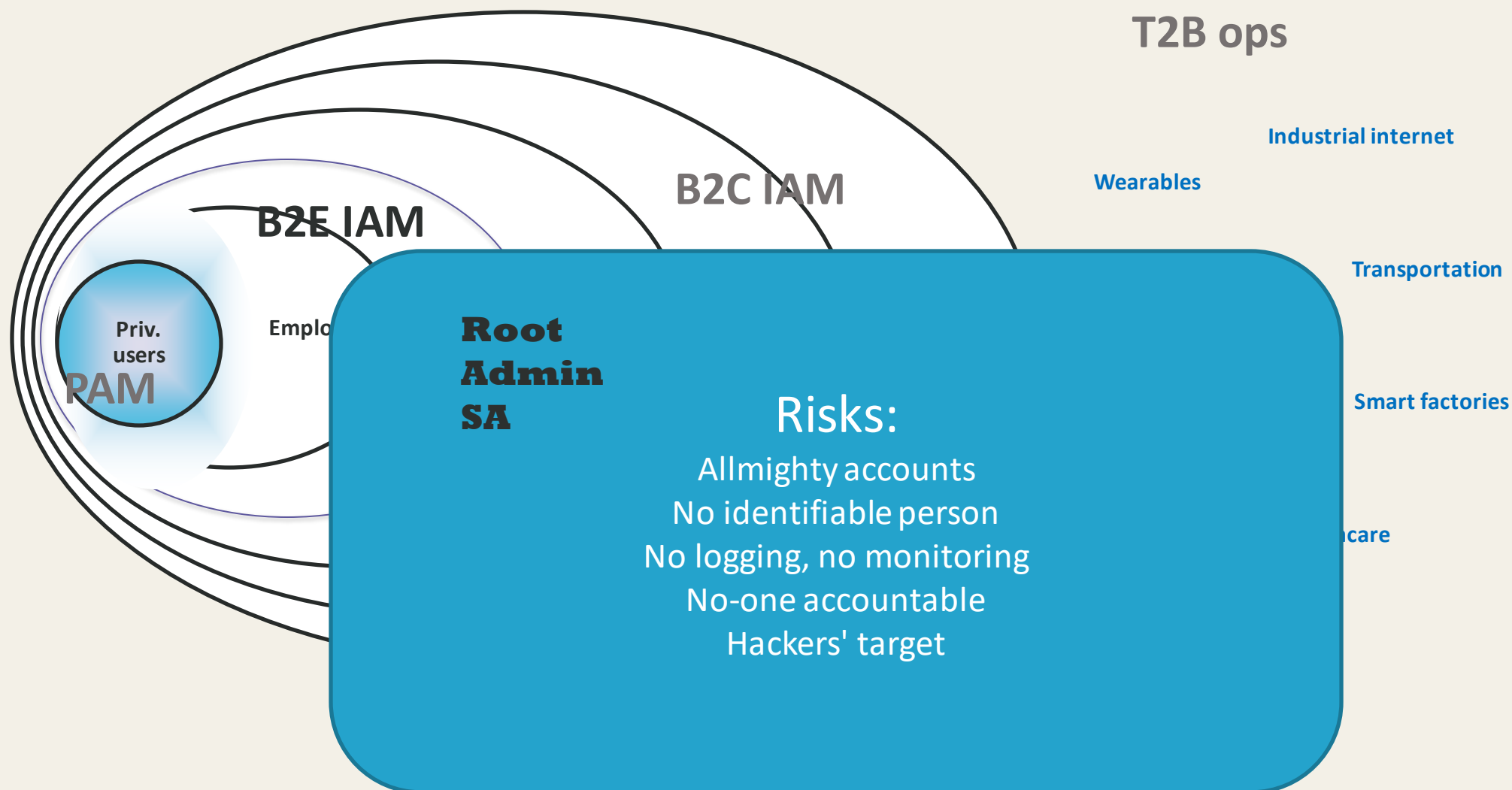


IAM – What is that?

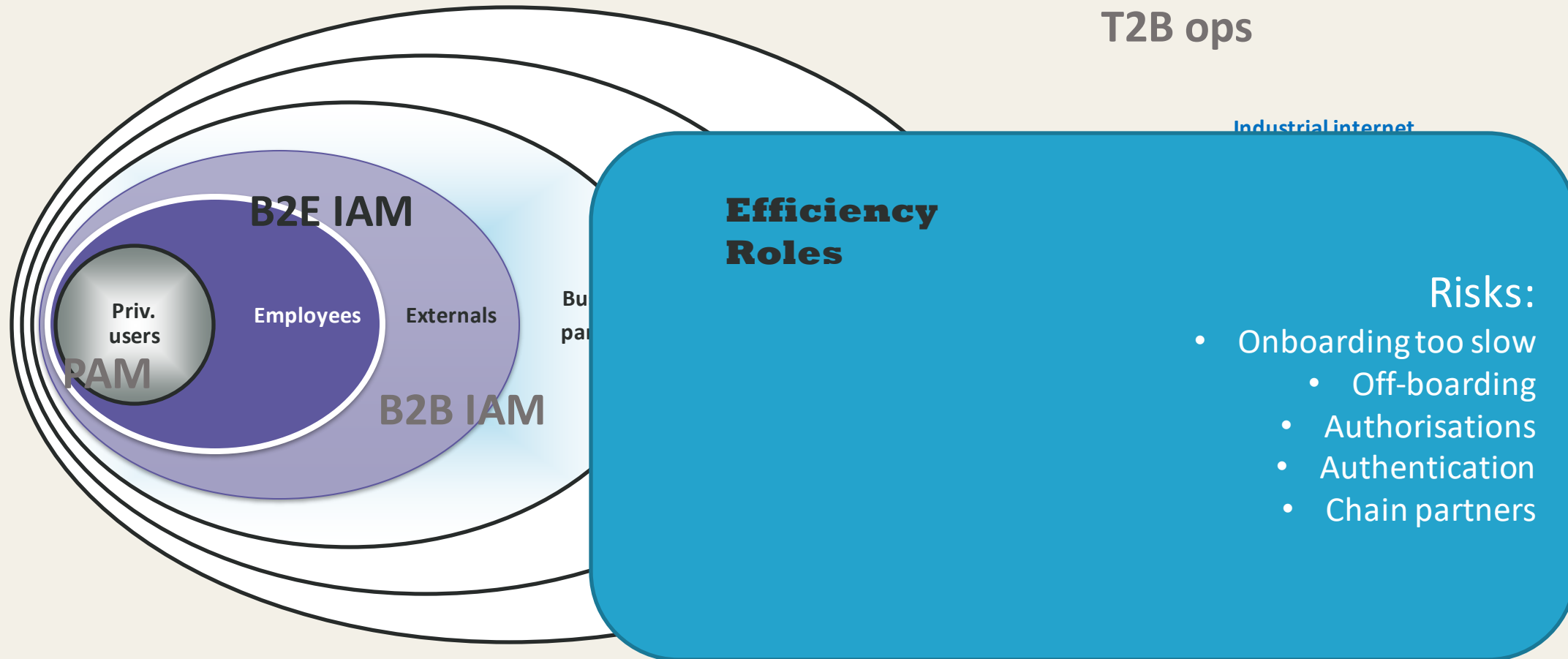
Identity management and access control



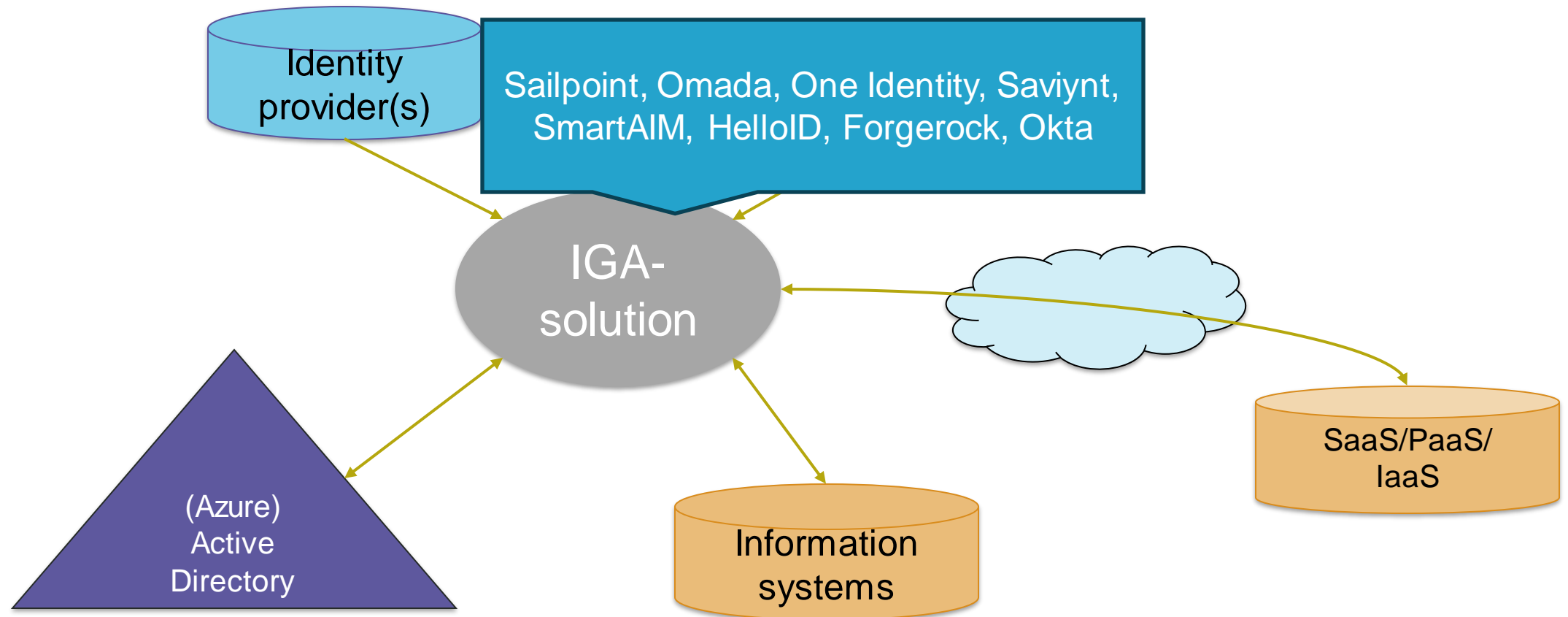
Scope of PAM



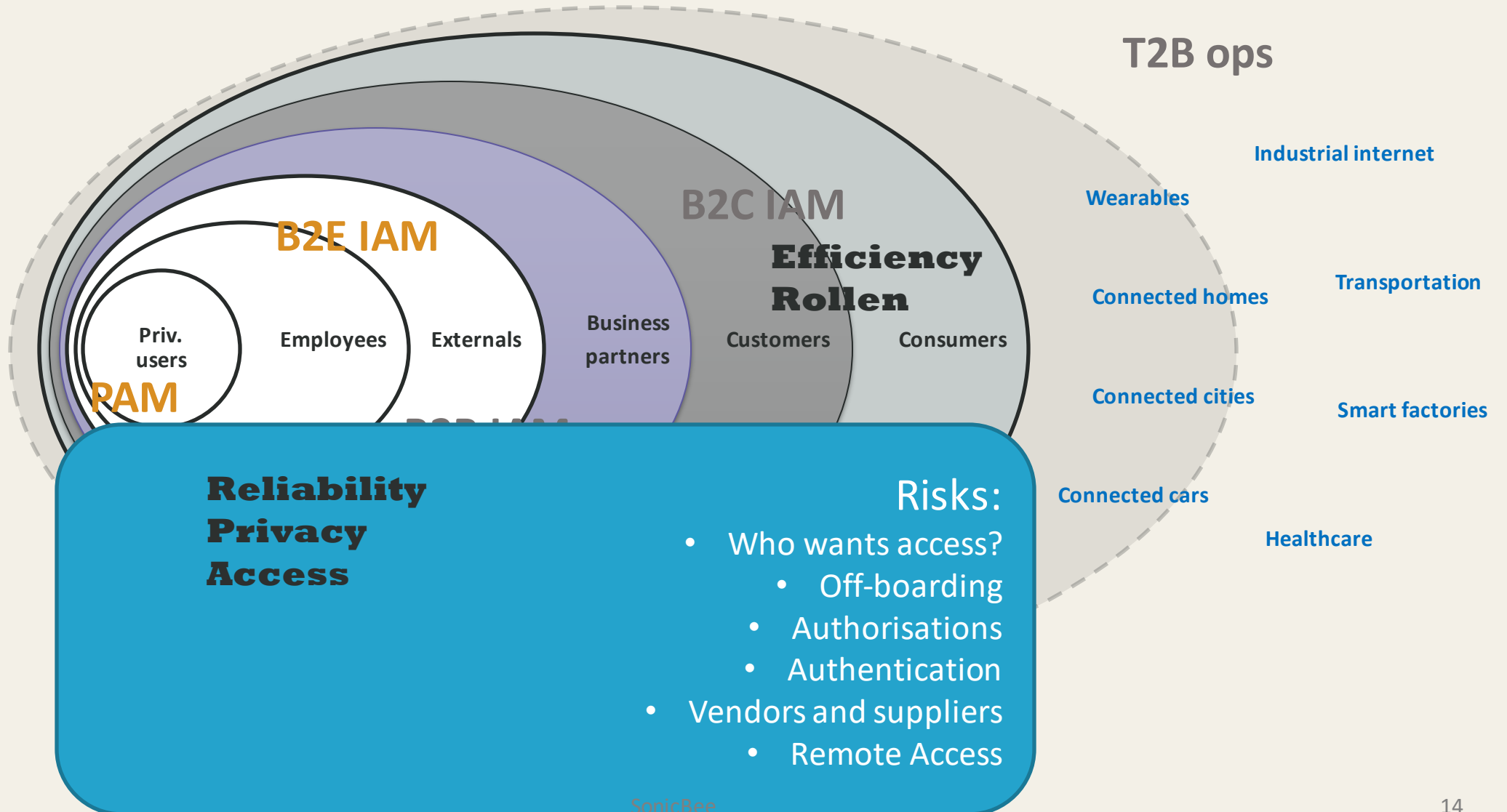
Scope of Internal IAM



Workforce IAM Reference Architecture



Scope of External IAM



Vulnerabilities Internet Trust

Risks:

- Supplier access
 - Updates
 - Access
- Operations
- Back doors
- Remote Access

Consumers

T2B ops

Industrial internet

Wearables

Connected homes

Transportation

Connected cities

Smart factories

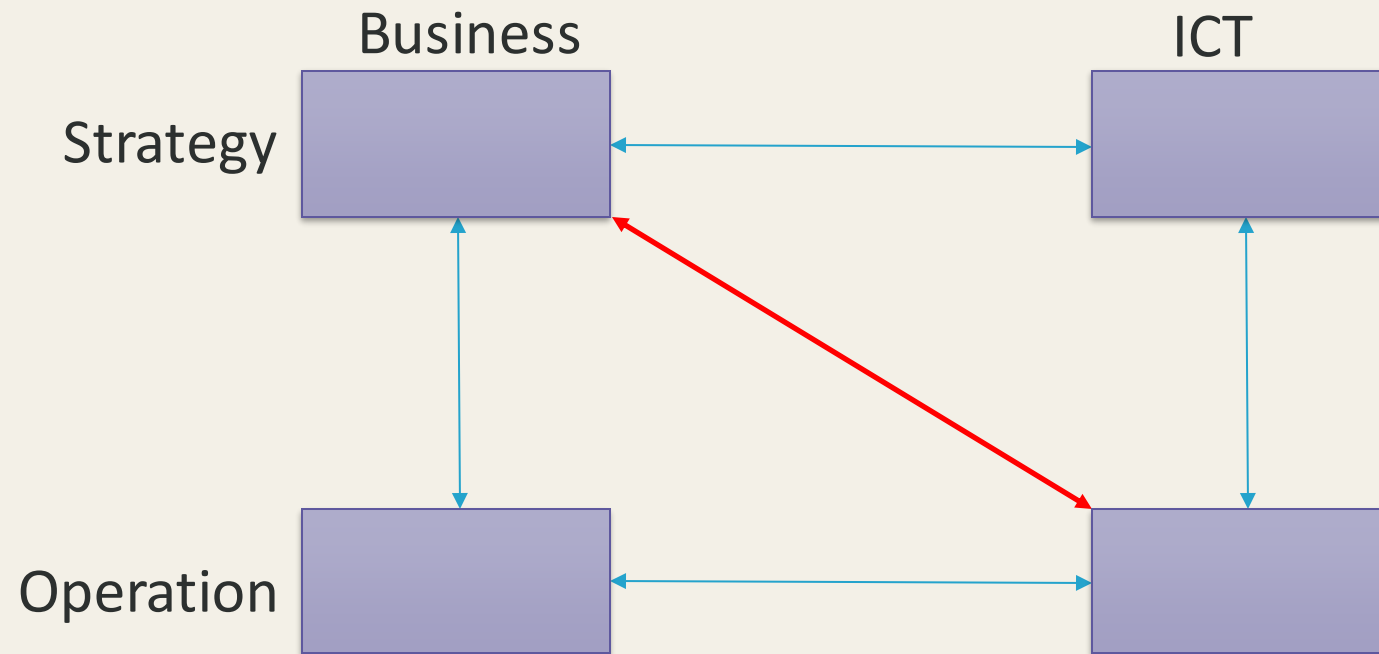
Connected cars

Healthcare

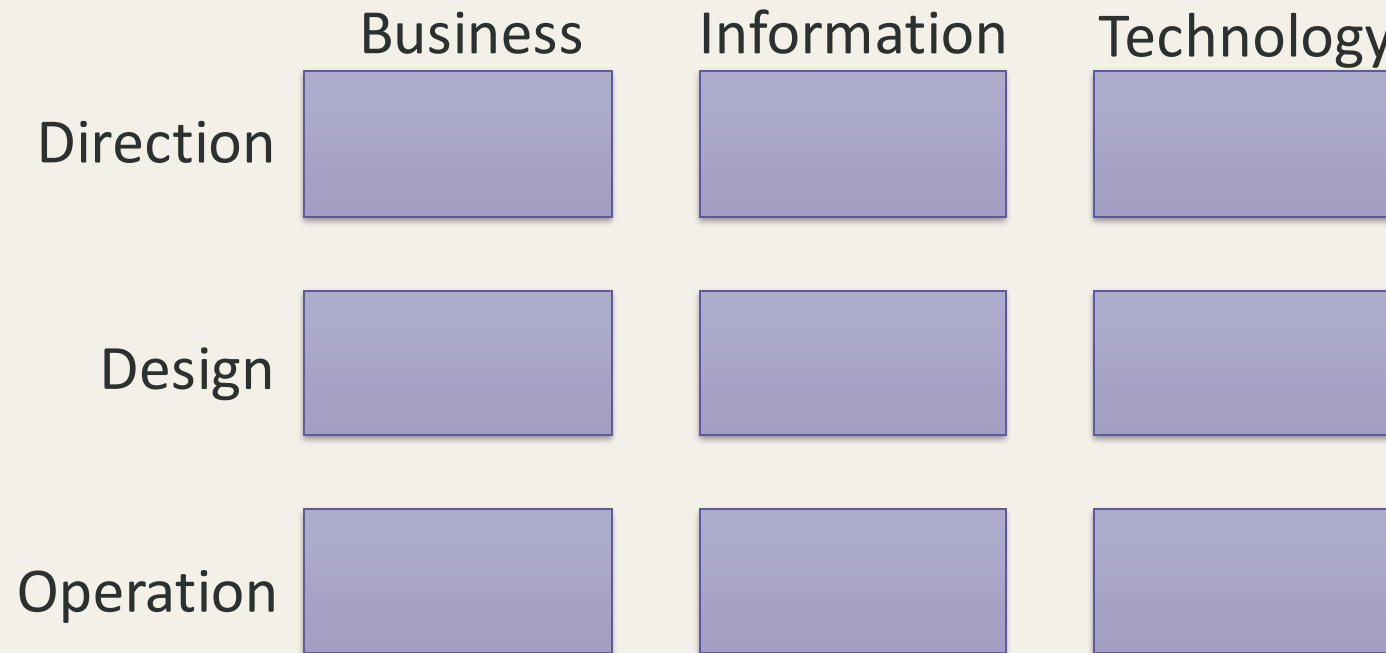


Strategic alignment

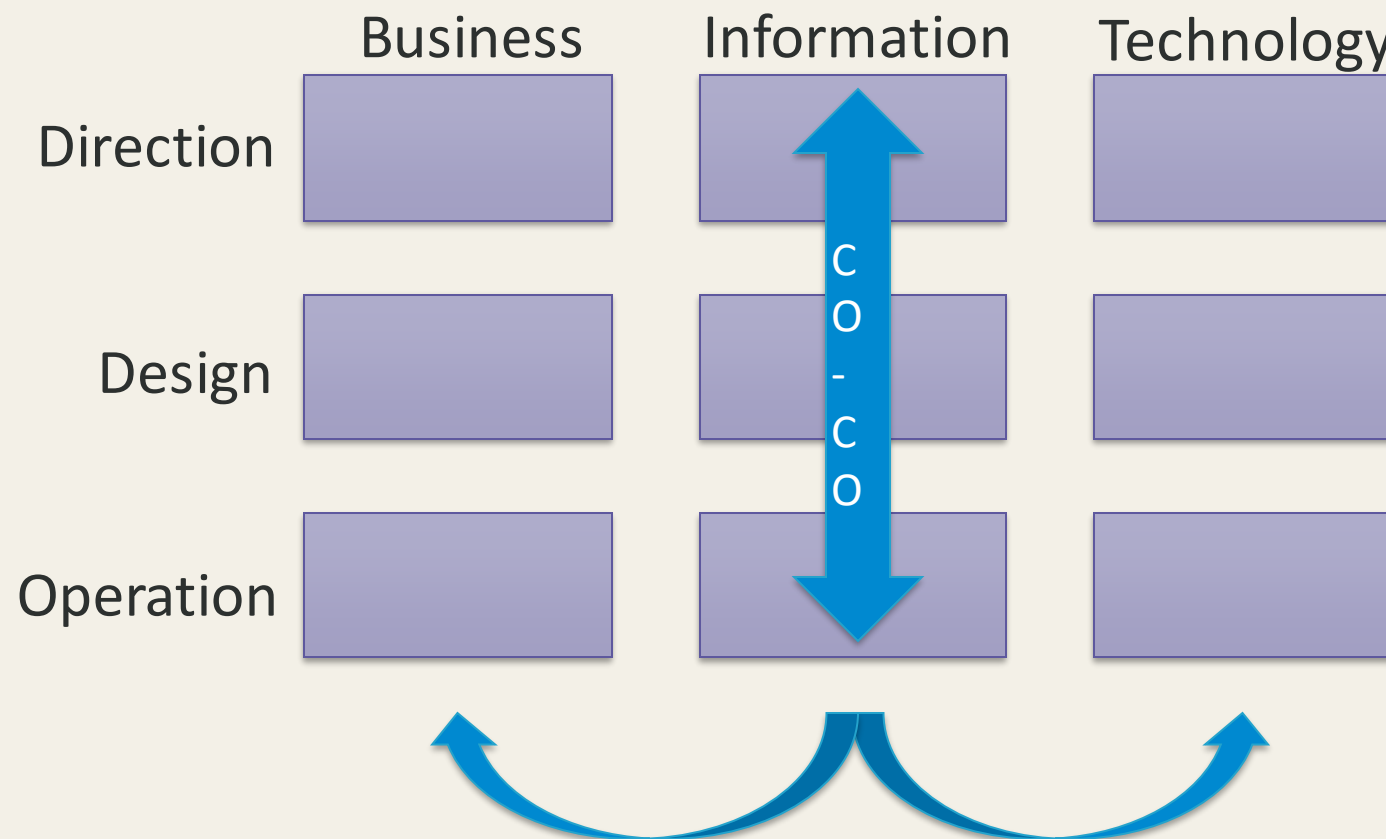
Henderson - Venkatraman



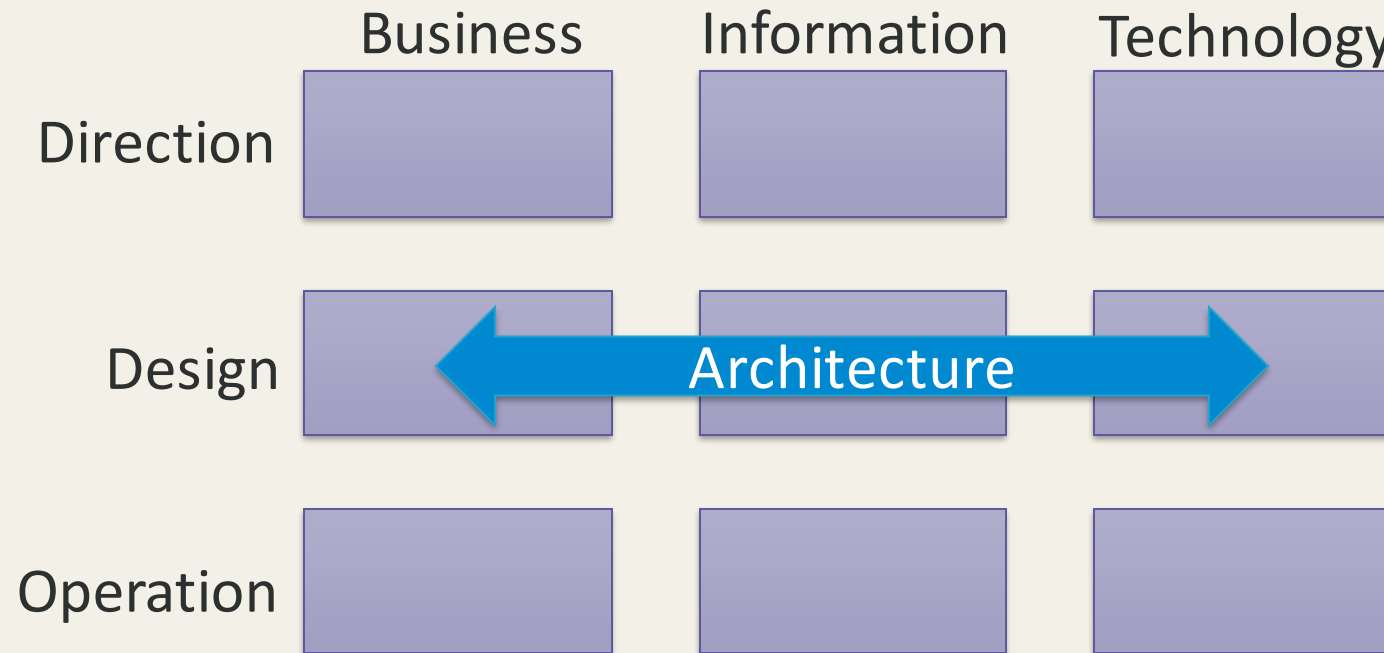
Amsterdam information model



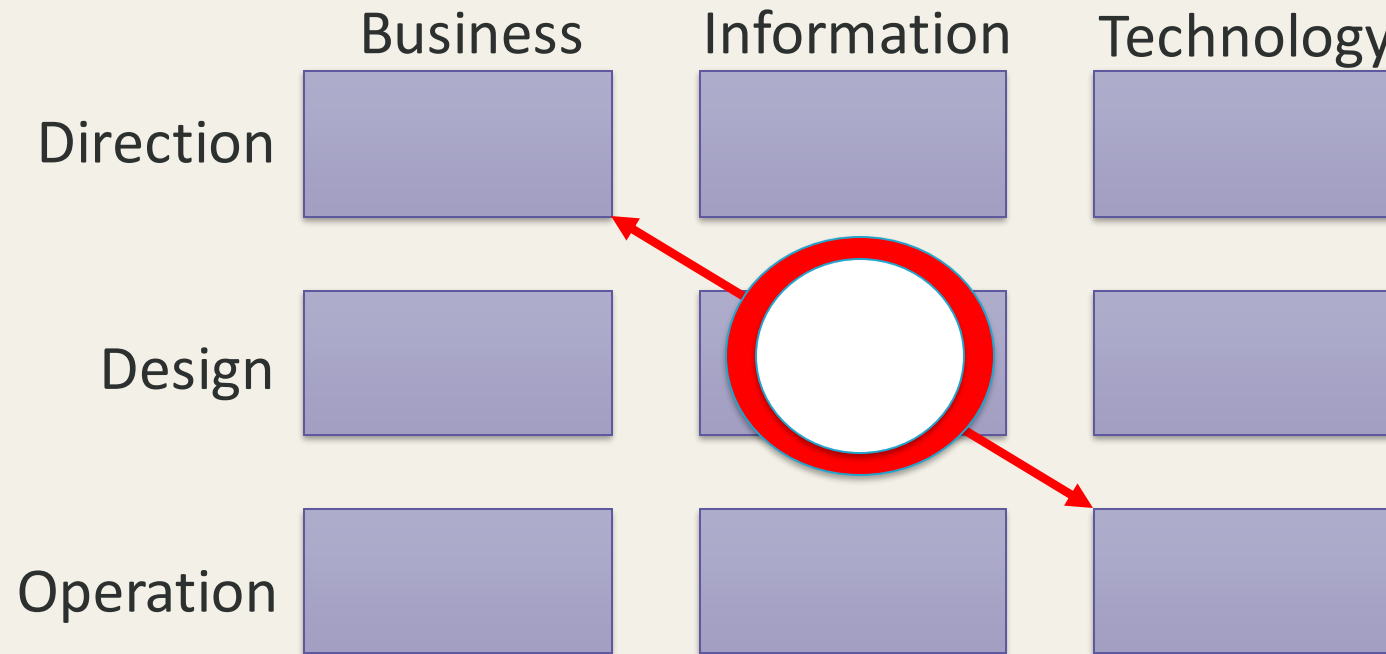
Amsterdam information model



Amsterdam information model



Amsterdam information model



Infosec Pain

- Business versus IT
 - No assurance on “who can do what and why”
 - Is privacy protection at stake?
 - Business doesn't understand what's needed
 - Business doesn't support GRC, whereas they are the problem owner



Infosec Pain

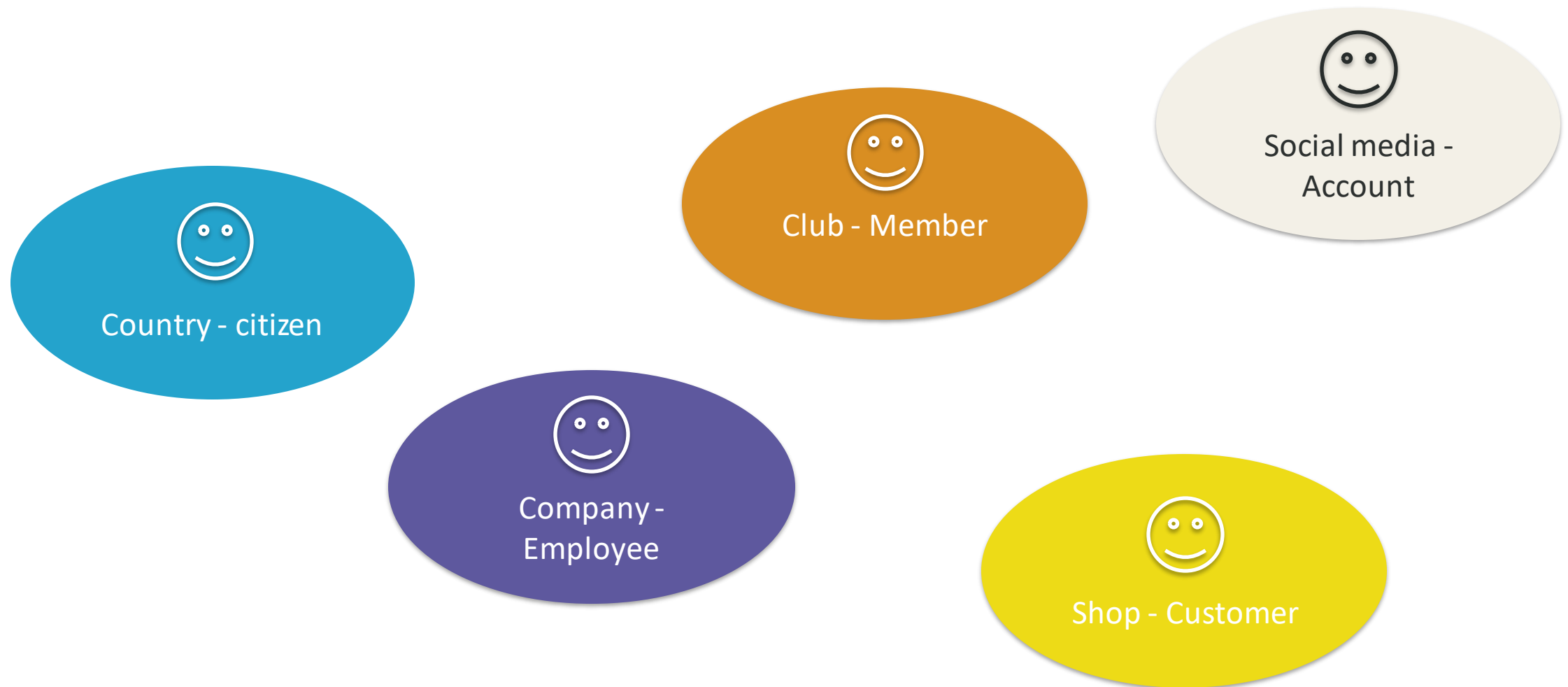
- Auditability
 - (External) auditors need data
 - Too little transparency with regards to access
 - No assurance about “who can do what, why”



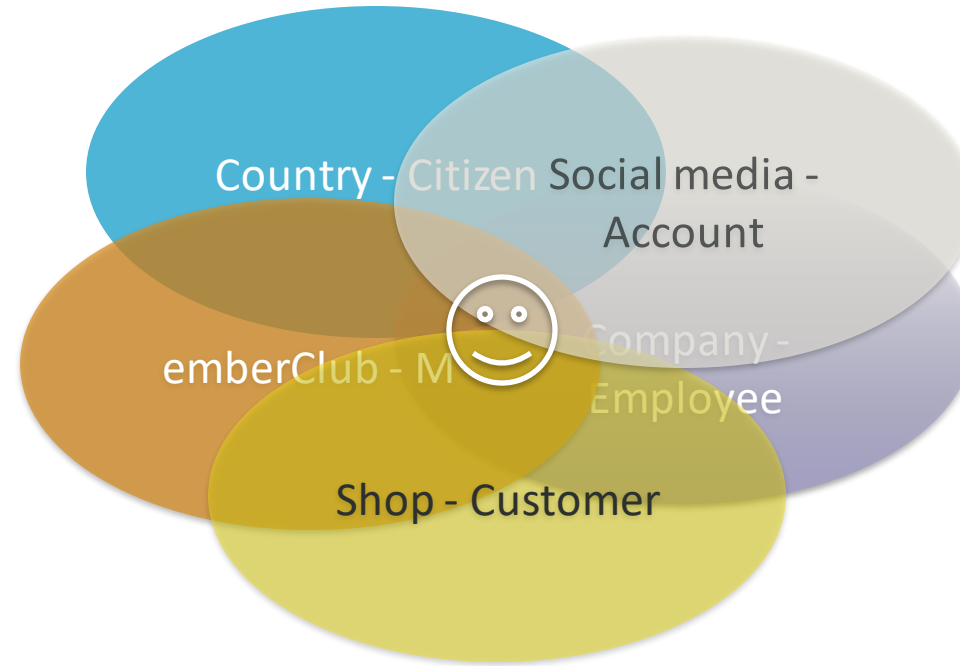


Identity management

Context



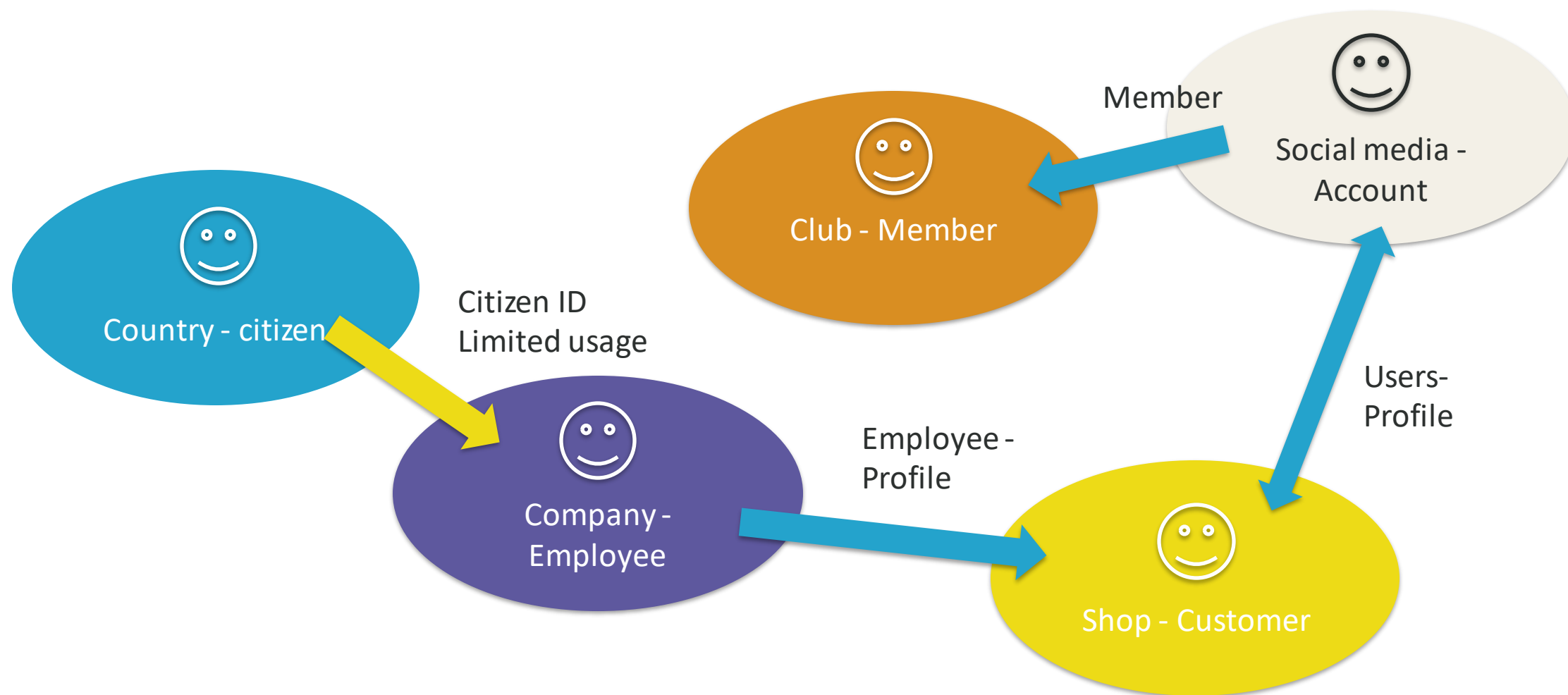
Context





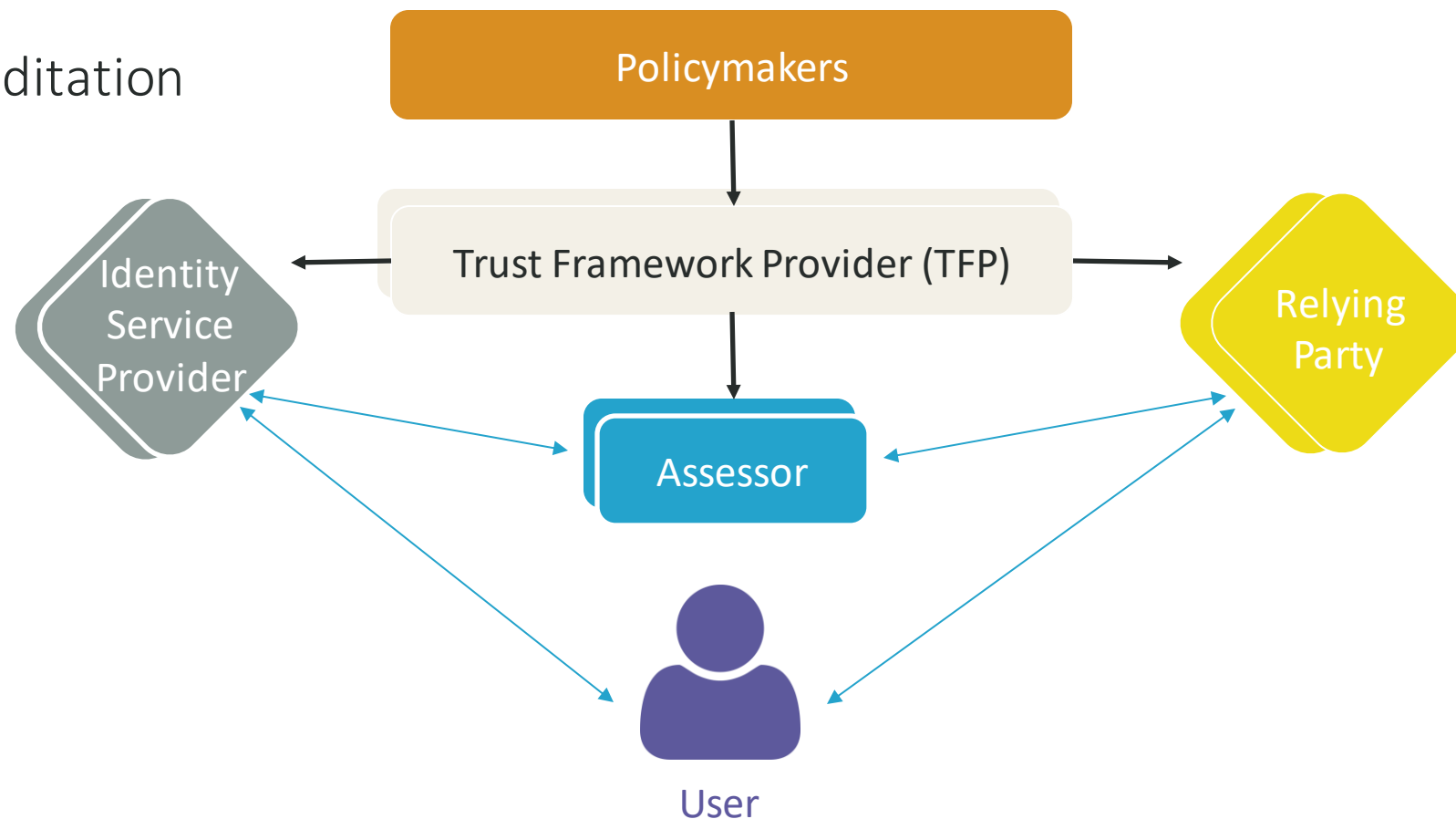
Federation - Trust

Context -> federation



Assurance framework, trust framework

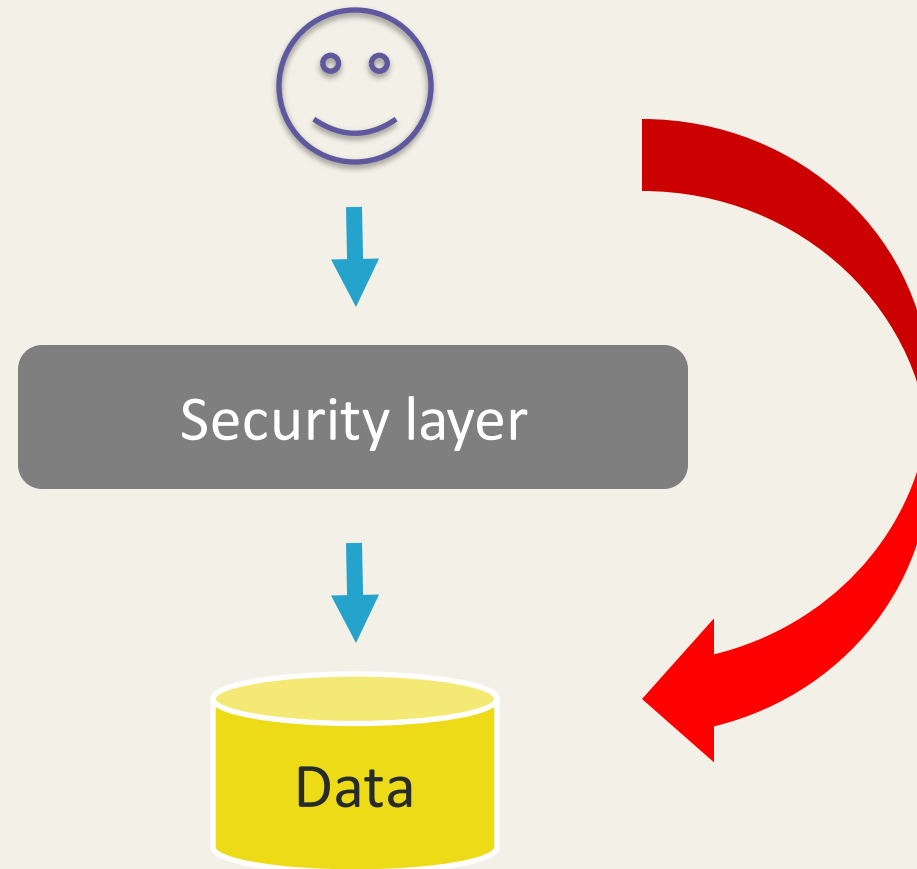
- Certification and accreditation





Access Control

Discretionary Access Control

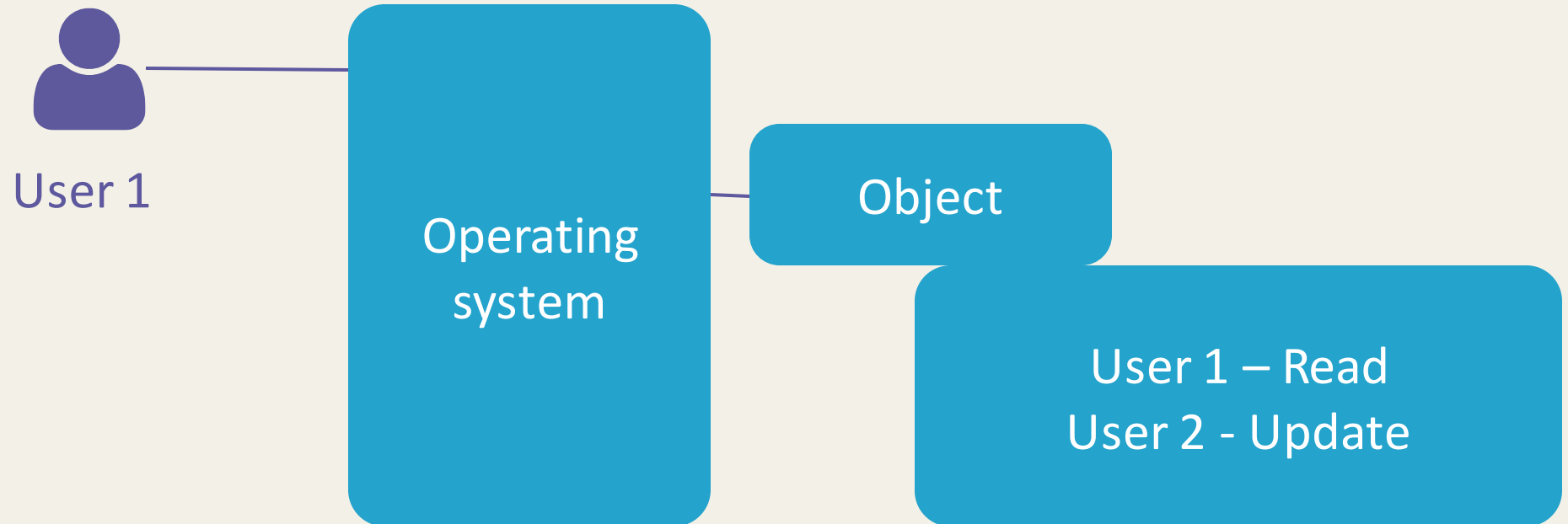


Access Control

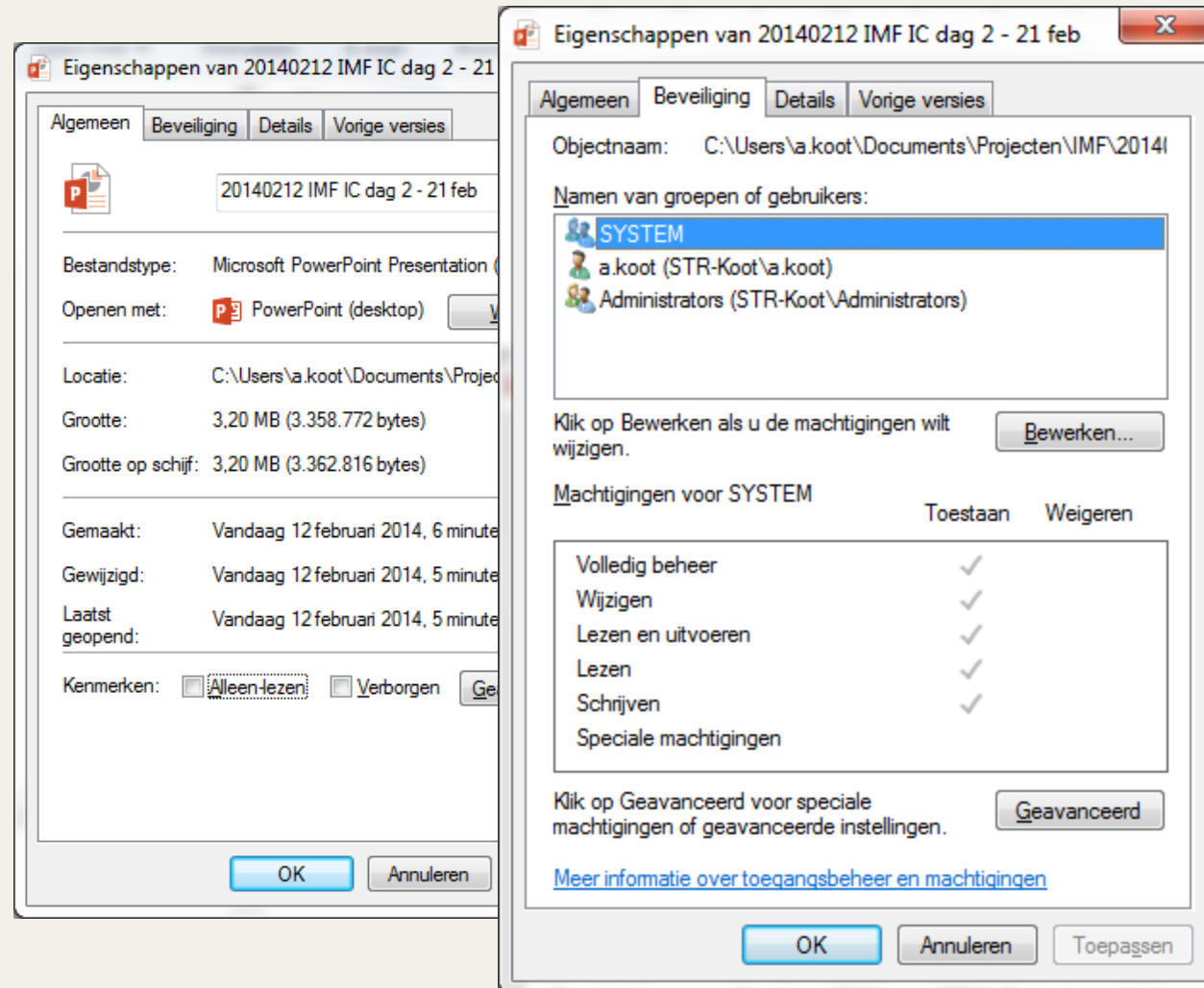
- Traditional: Access Control Lists (ACL)
- Mainstream: Role Based Access Control (RBAC)
- Future: Rule Based Access Control
 - Attribute Based Access Control (ABAC)
 - Or Context Based Access Control (CBAC)
 - Or Policy Based Access Control (PBAC)

Access Control models

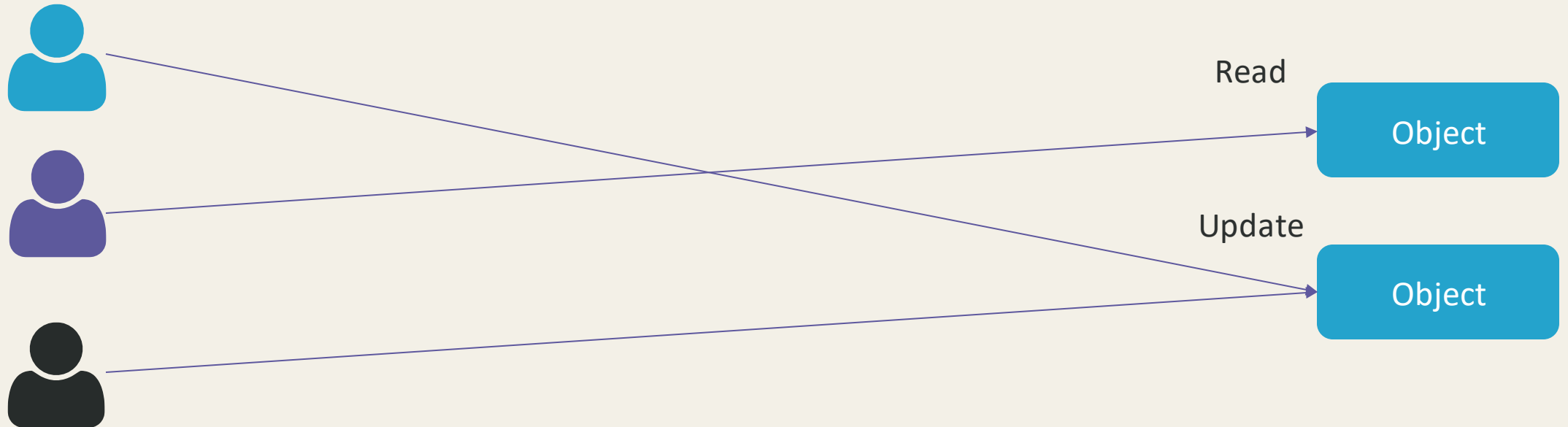
- Access Control Lists



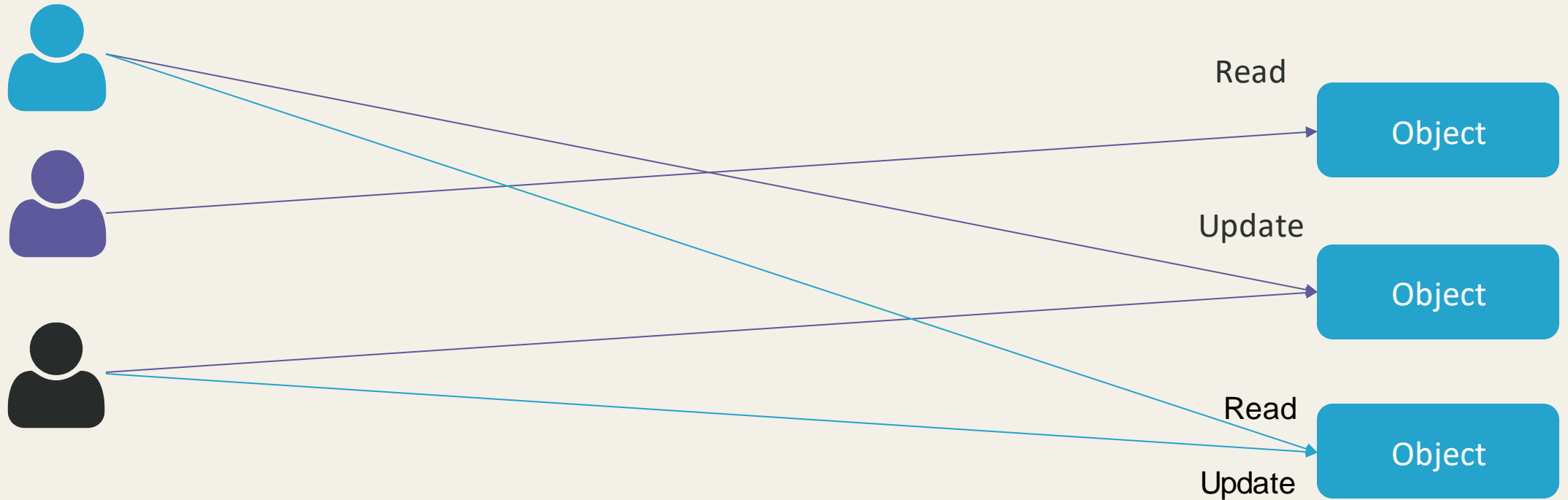
Access Control Lists



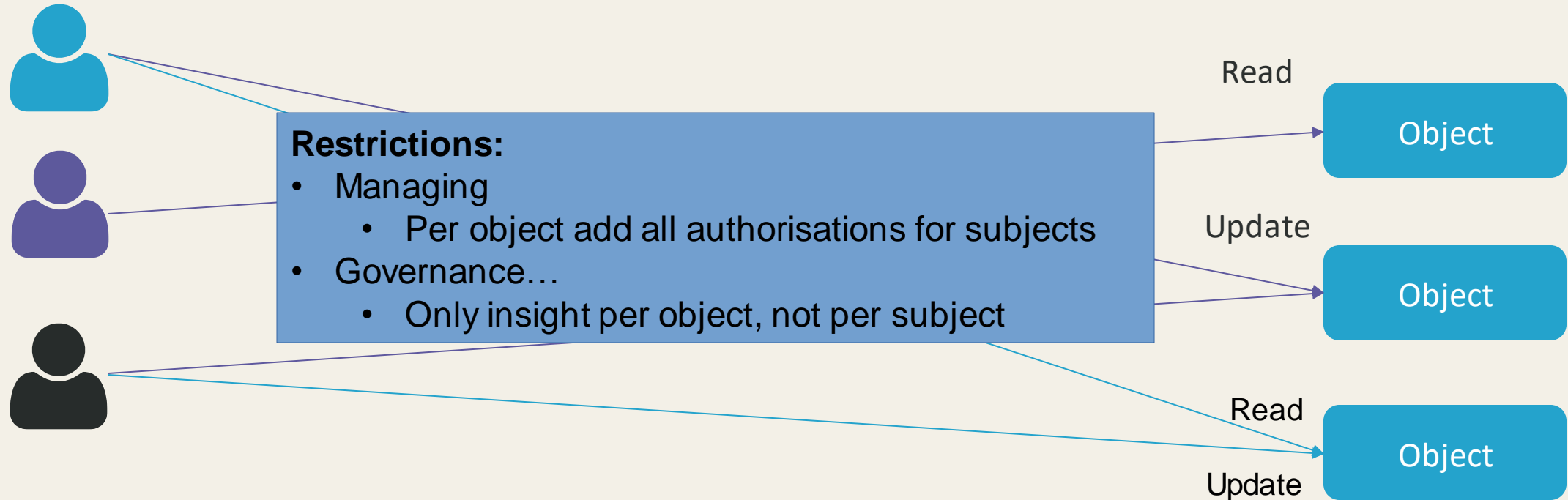
Access Control models



Access Control models



Access Control models

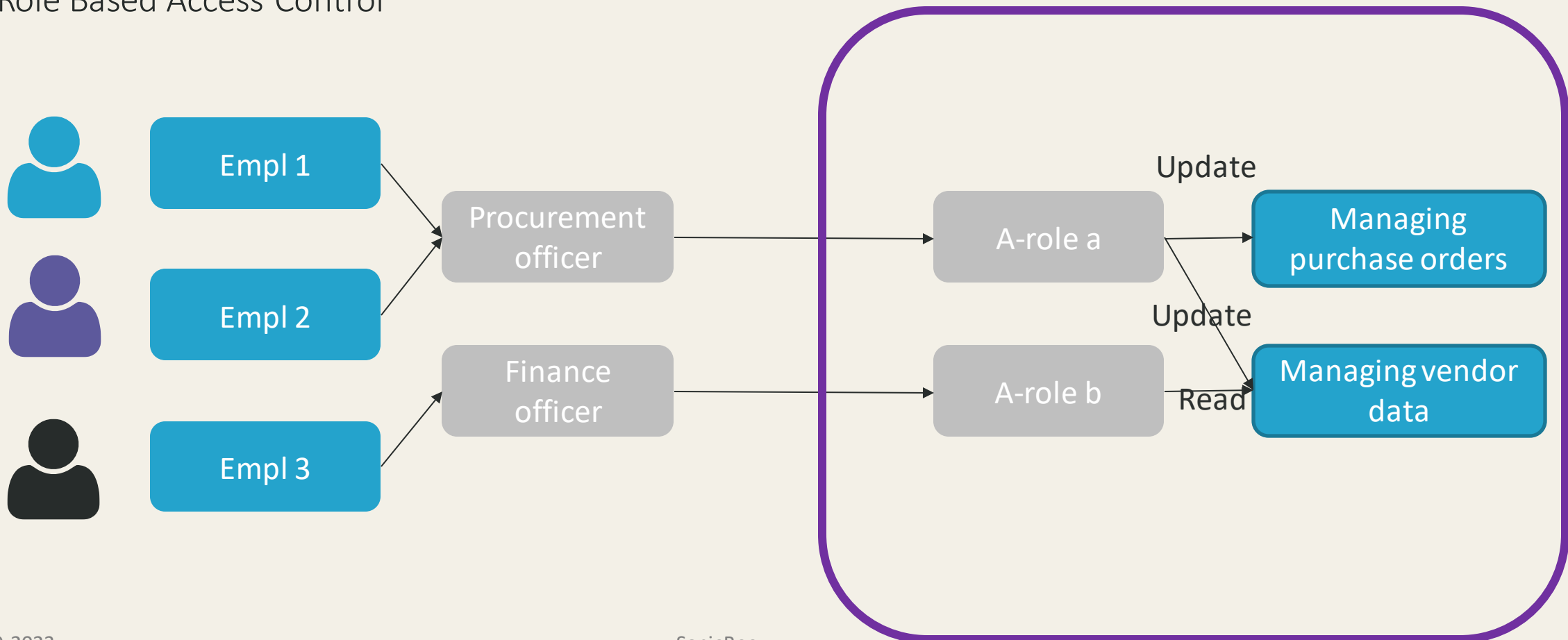




RBAC

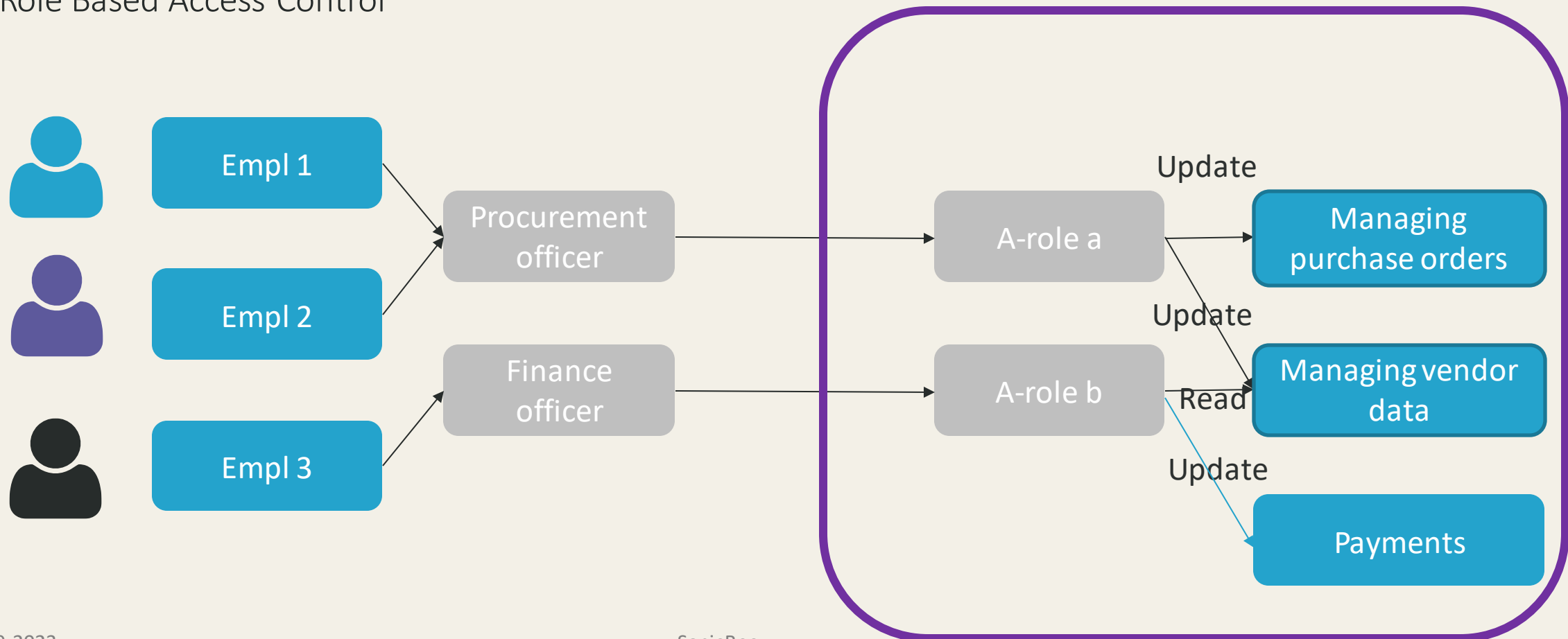
Access Control models

- Role Based Access Control



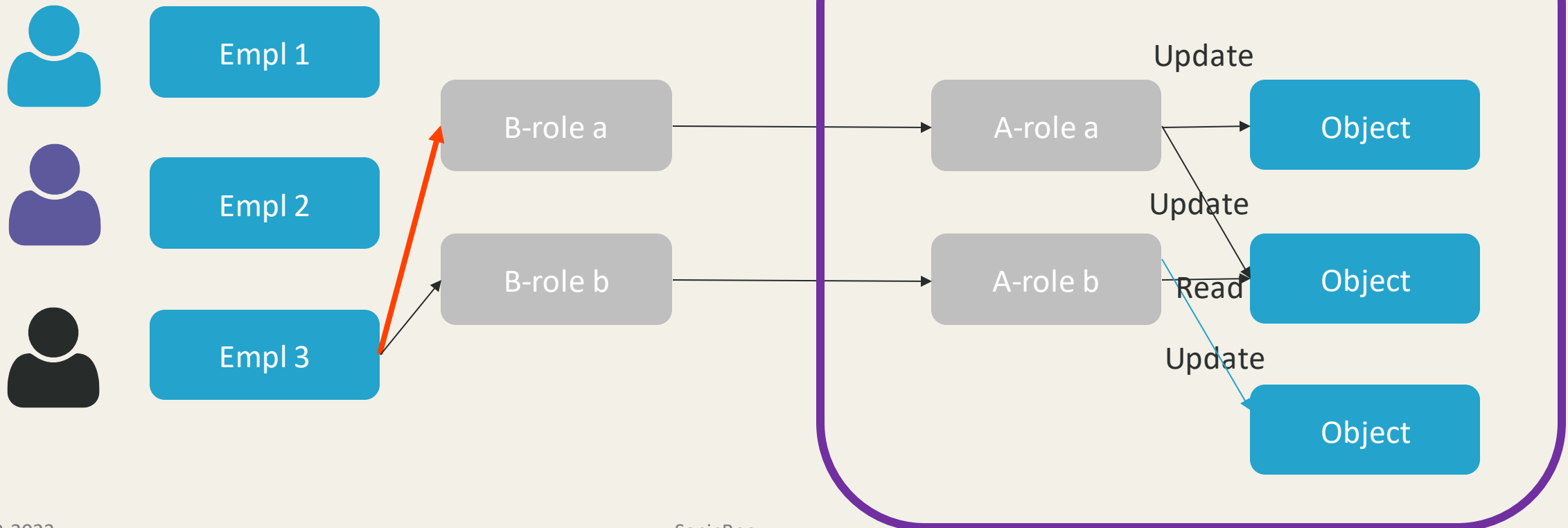
Access Control models

- Role Based Access Control



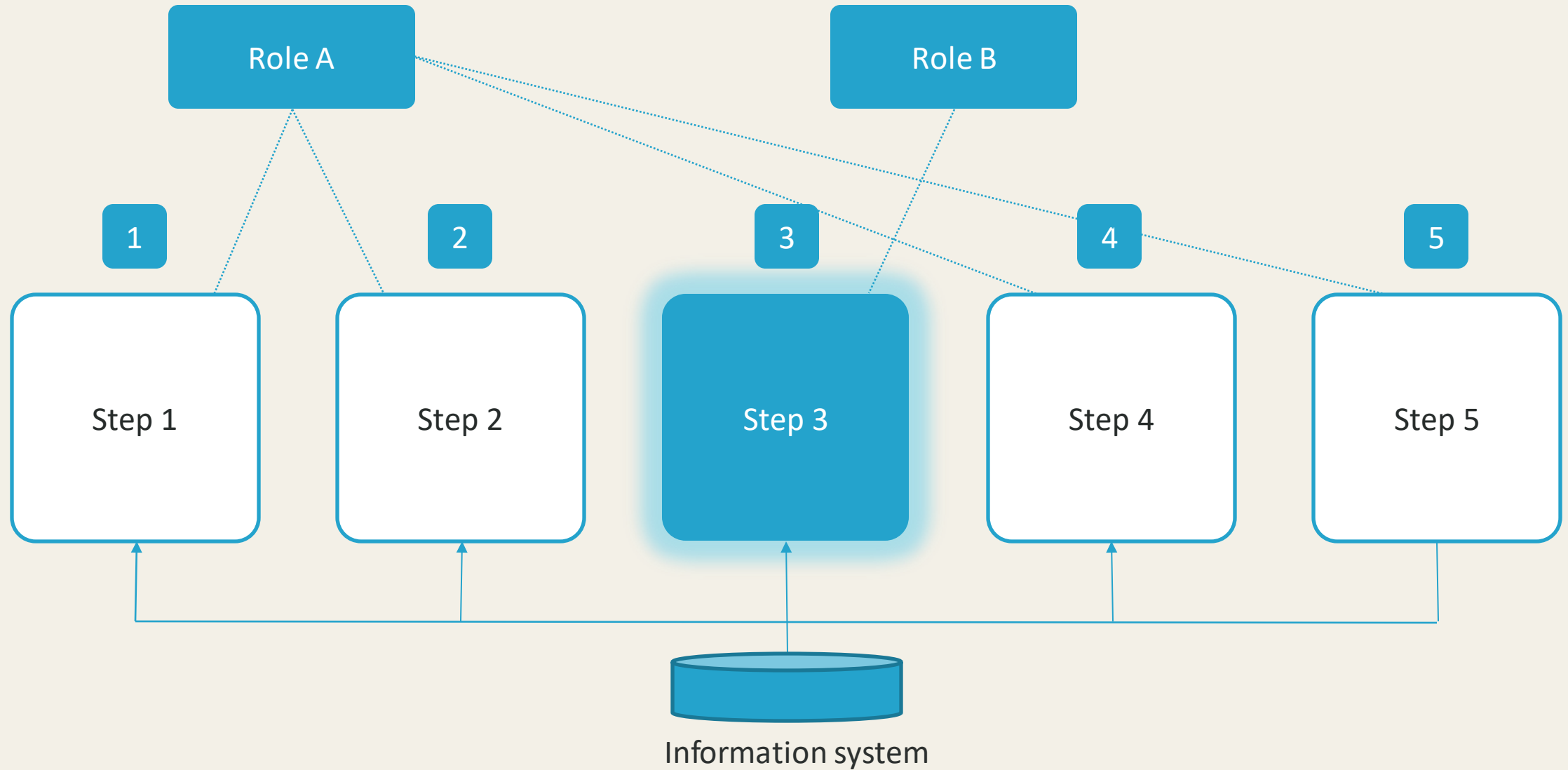
Access Control models

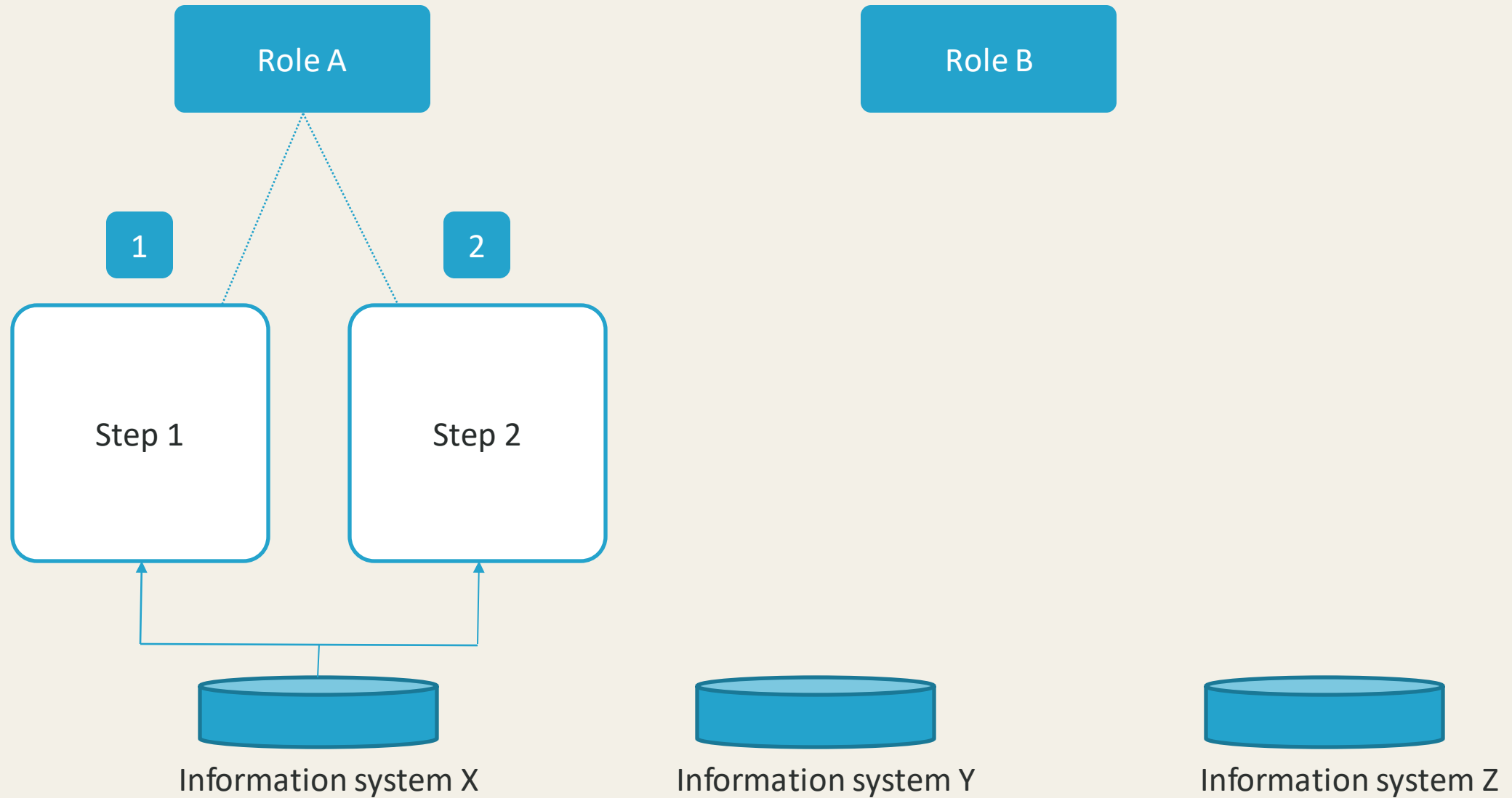
- Role Based Access Control

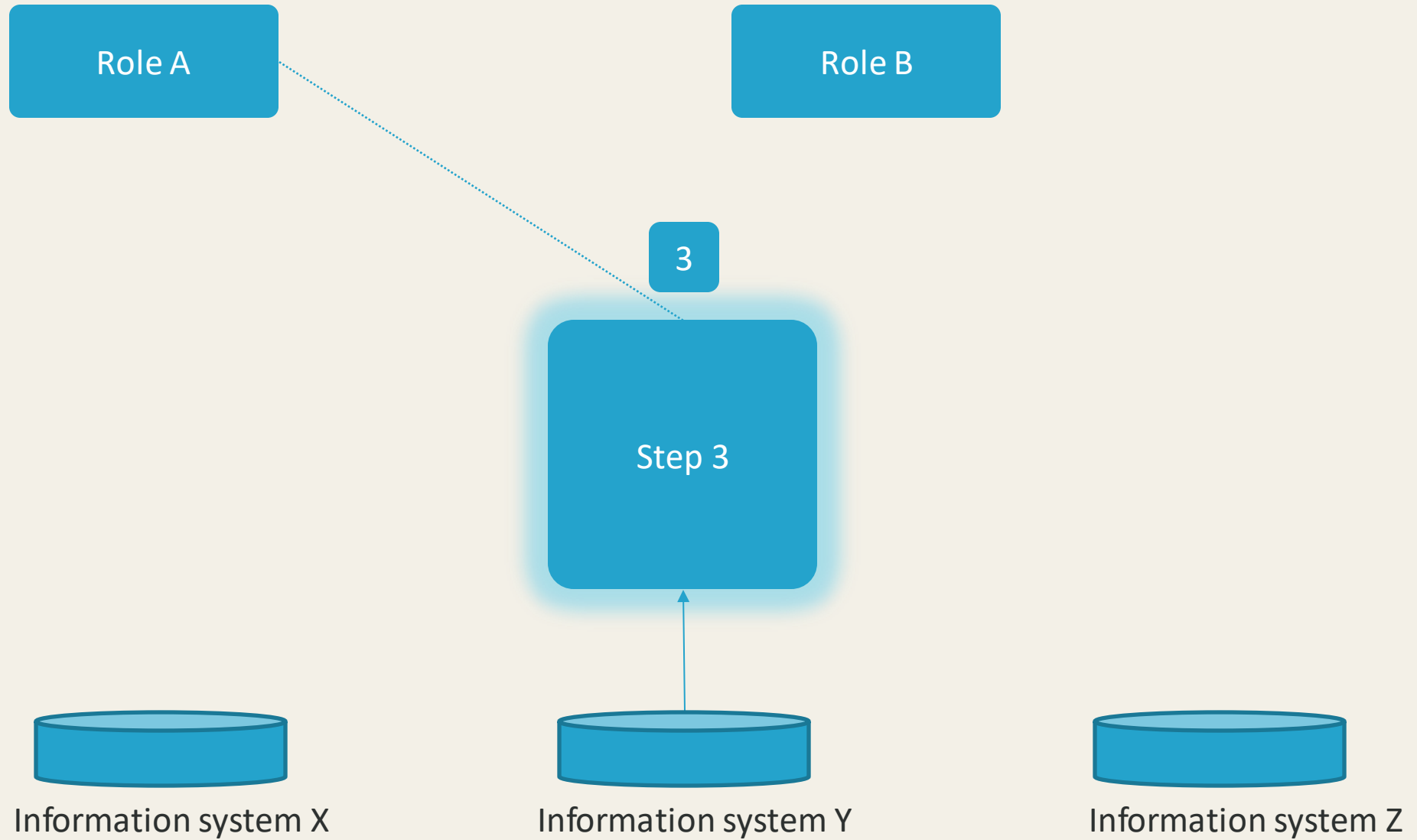


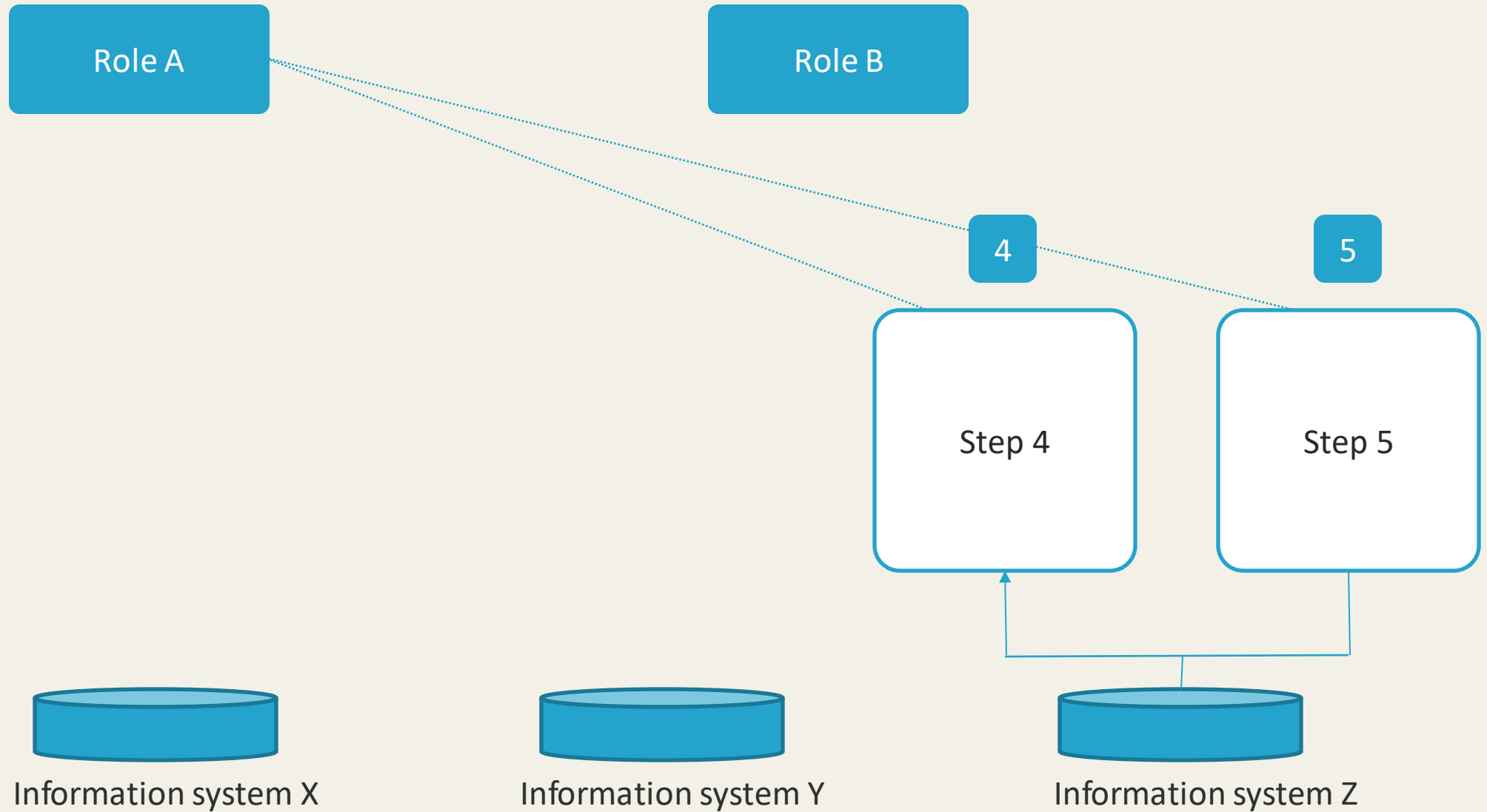


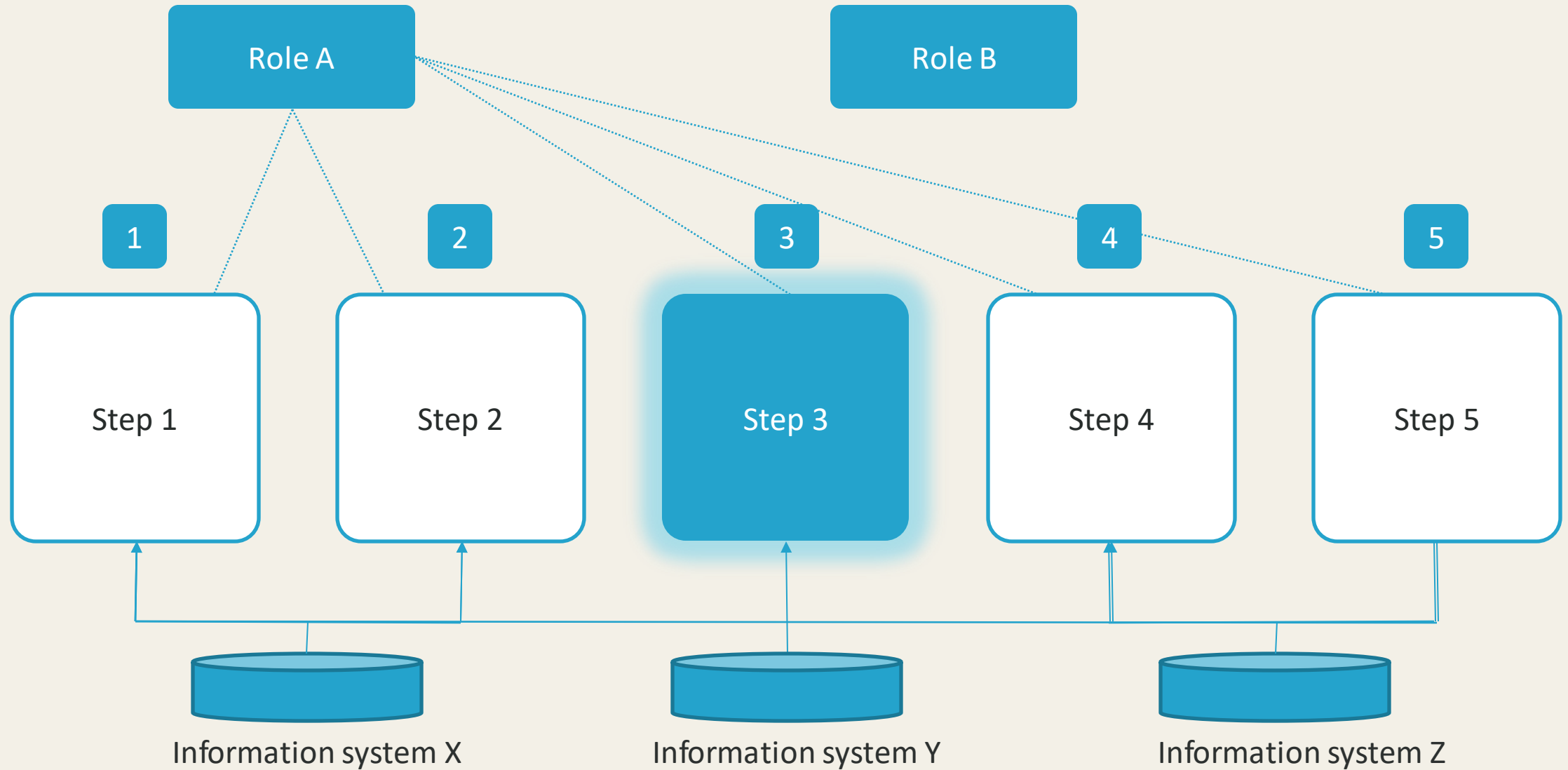
Access Governance



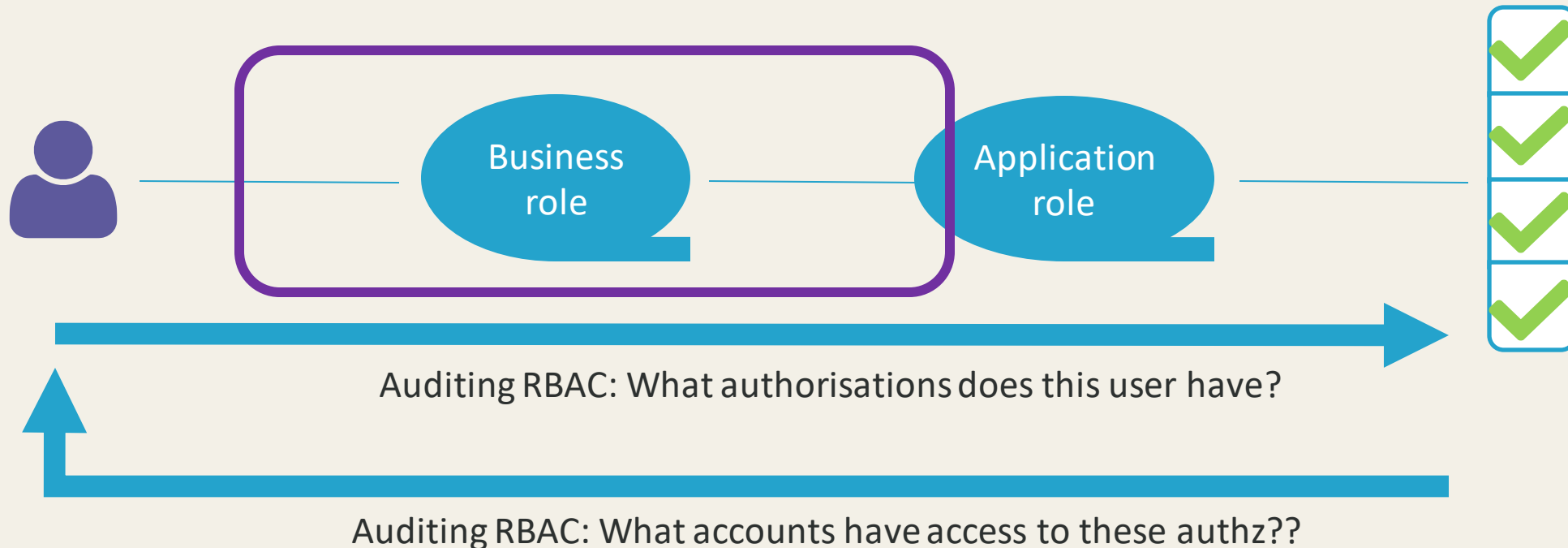








Traditional Access Governance RBAC



Authorisation matrix

- What does it say?
- Soll-matrix
- Ist? Audit?
- Who is the owner?

	Telefoonlijst	Klantenbestand	Salarisadministratie	Schijfsjablonen	Agenda
Directie	L	L	L	-	B
HR	A	L	B	-	B
Manager	B	B	-	L	L
Consultant	L	B	-	L	L
Receptionist	A	L	L	-	A

			Rollen					
			Directie	Financien	Administratie	Planning	Chaufeurs	Receptie
Persoonsgegevens	a	Relaties	x	x	x	x	x	x
	b	Klanten Melding: berging, pechhulp en transport	x	x	x	x	x	x
	c	Klanten Mobiliteitshulp / verhuurcontracten	x	x	x	x	x	
	d	Klanten Bemiddeling autorecyclingbedrijf	x	x	x	x		
	e	Werknemers	x	x				

	Laboratorium	Internist	Diëtist	Fysiotherapie	Apotheek	Patiënt	Oogarts	Podotherapeut	HIS-KIS
NAW	-	•	•	•	••	•	•	•	•
Labuitslagen	••	•	-	-	-	•	-	-	•
Onderzoeken	-	-	-	-	-	•	•	-	•
Medicatie	-	-	-	-	•	•	-	-	-
Co- en multi-morbiditeiten	-	-	-	-	-	•	-	-	-
Risicofactoren	-	-	-	-	-	•	-	-	•
Bevindingen (tekst)	-	-	•	-	-	•	•	-	•
Zorgplan*	-	-	-	-	-	•	-	-	-

•

gestructureerd

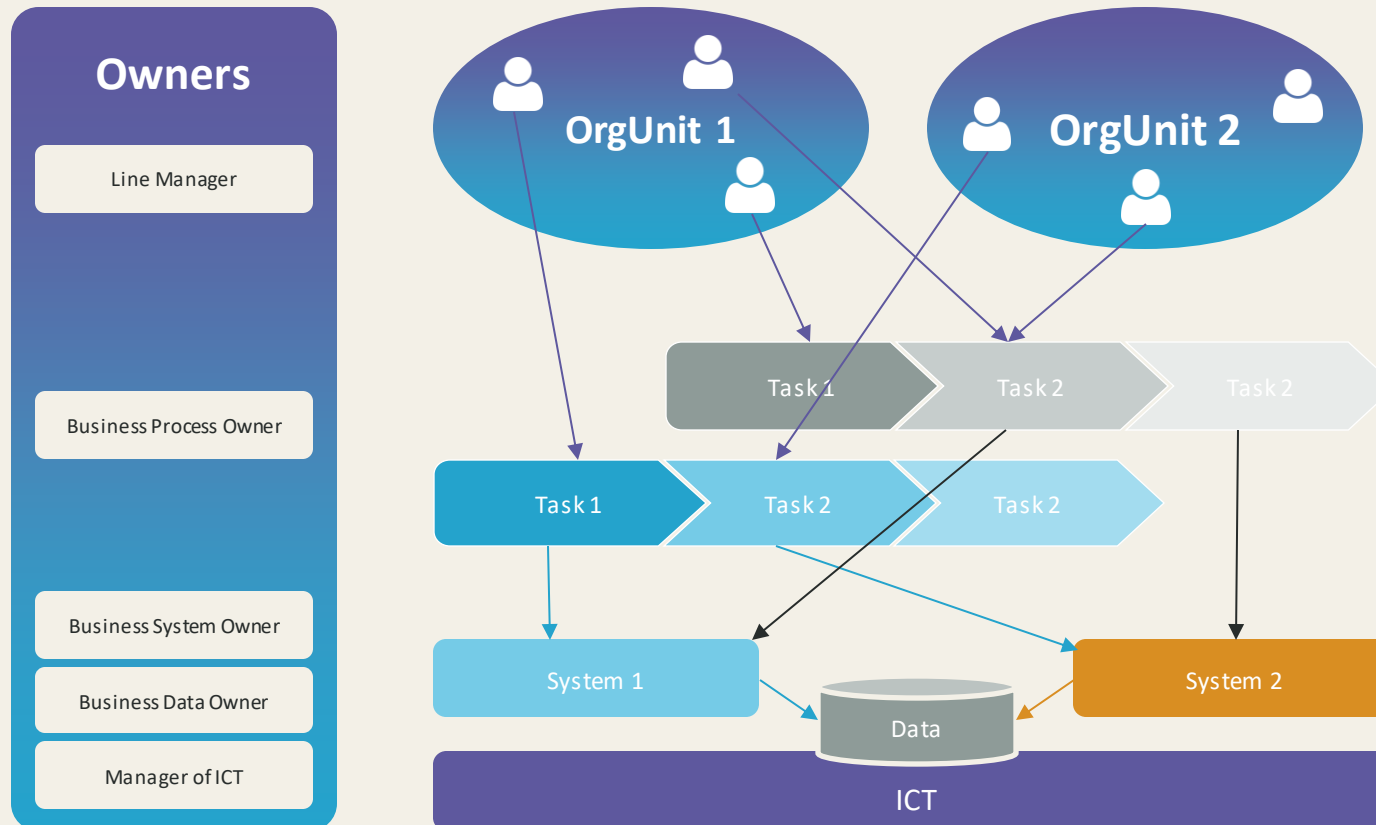
•

ongestructureerd

•

niet digitaal

Access Governance



Security nightmare: RBAC doesn't work across multiple 'domains'...: One needs to know both the Id and the Authz

Governance nightmare: Context...



Business role

Application role



Governance nightmare: SoD...


What authorisations?


What accounts?

Governance nightmare: Rollen are static...


Future


- Processes and process quality will be leading
 - SoD
 - Based on business rules
 - Quality criteria within a proces
 - Based on attributes

 **Acclaim**




André Koot




 Here's where you tell the world a little about yourself and what makes you special. A brief bio can help you stand out from the crowd and give your profile some personality. [Enter your bio now »](#)

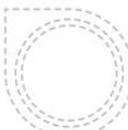
MY BADGES





Certified Information Security Manager® (CISM)
ISACA





Certified Information Systems Auditor® (CISA)
ISACA





[Suggest a badge!](#)
Have an idea for a badge you'd like to see available on Acclaim? We're listening.





André Koot





Share

Certified Information Security Manager® (CISM)

The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs.

ISSUED BY ISACA	ISSUED TO André Koot	ISSUED ON 19 Aug 2006
--------------------	-------------------------	--------------------------

TAGS

Information Risk Compliance

Information Risk Management

Information Security





Information Security Governance

Information Security Incident Management

Information Security Program Development

Information Security Program Management

WHAT IT TAKES TO EARN THIS BADGE

-  Score a passing grade on the CISM exam
-  Submit verified evidence of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice domains
-  Agree to abide by the ISACA Code of Professional Ethics
-  Agree to abide by the CISM Continuing Professional Education Policy



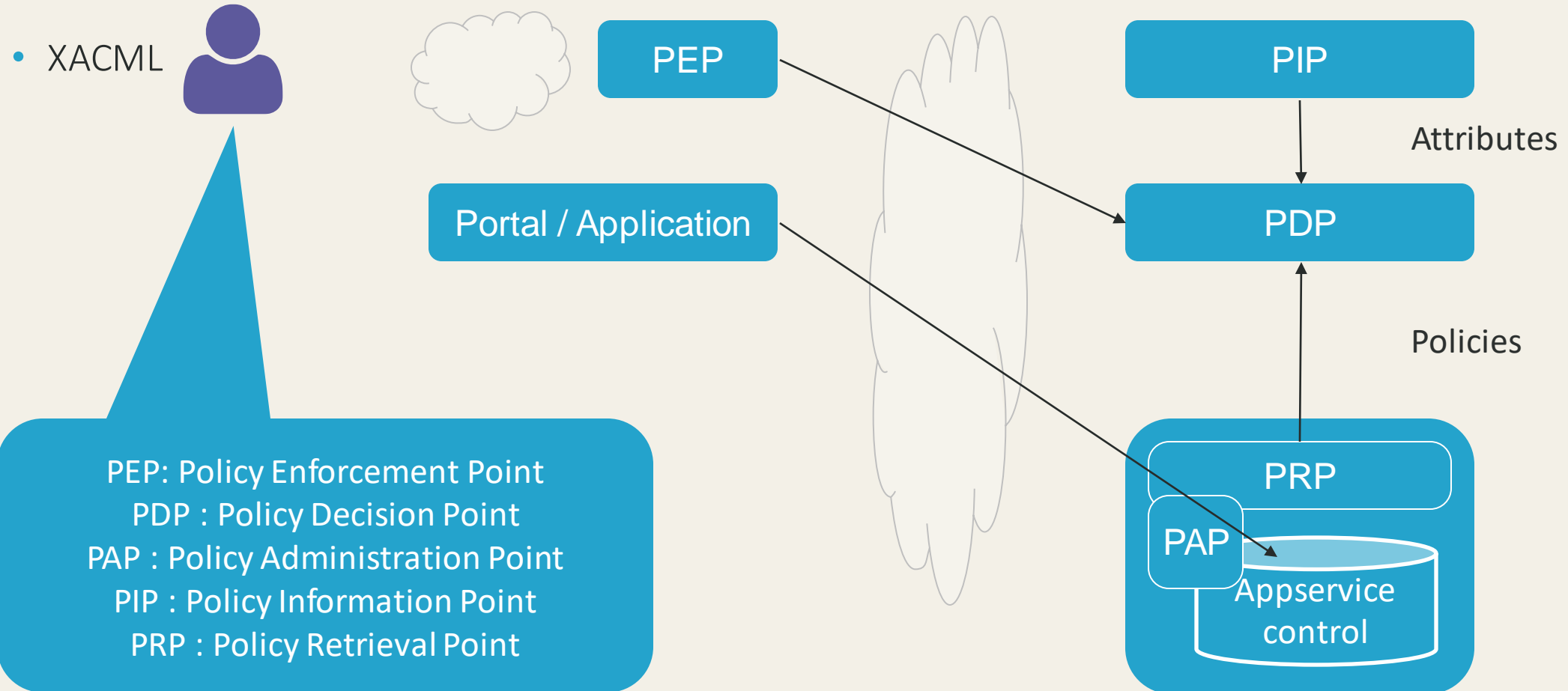
Dynamic Access Control

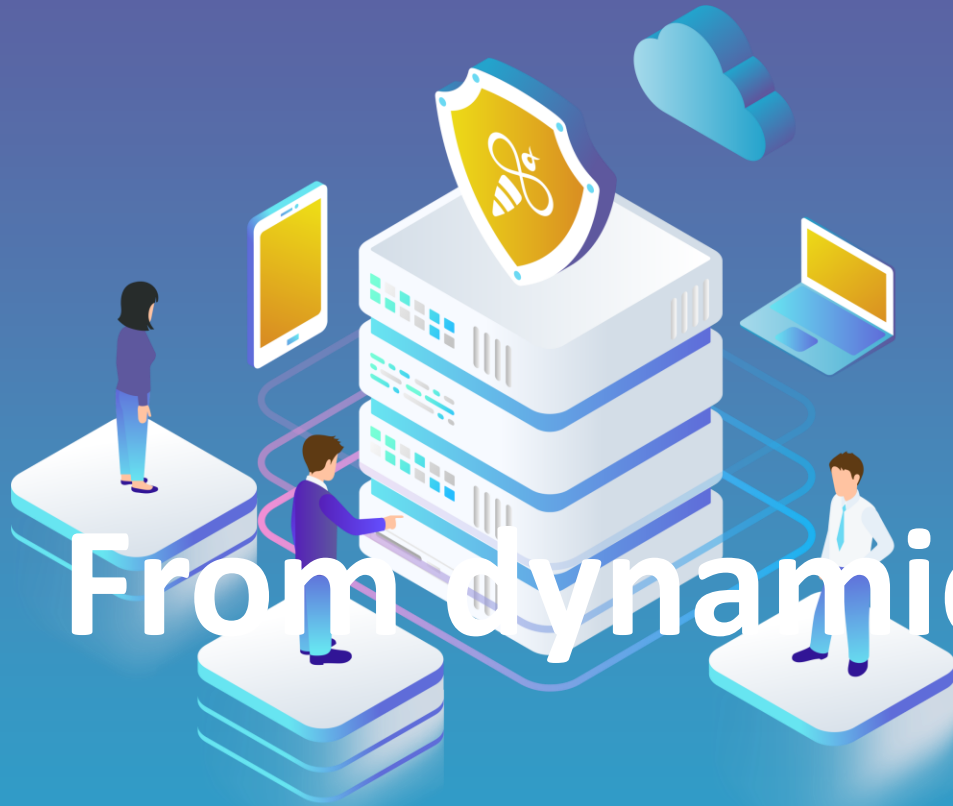
'New': ABAC

- Exit if:
 - Paid amount due
 - Recently...
- Only if...
 - brand is Kia



Access Control models





From dynamic access control to Zero trust

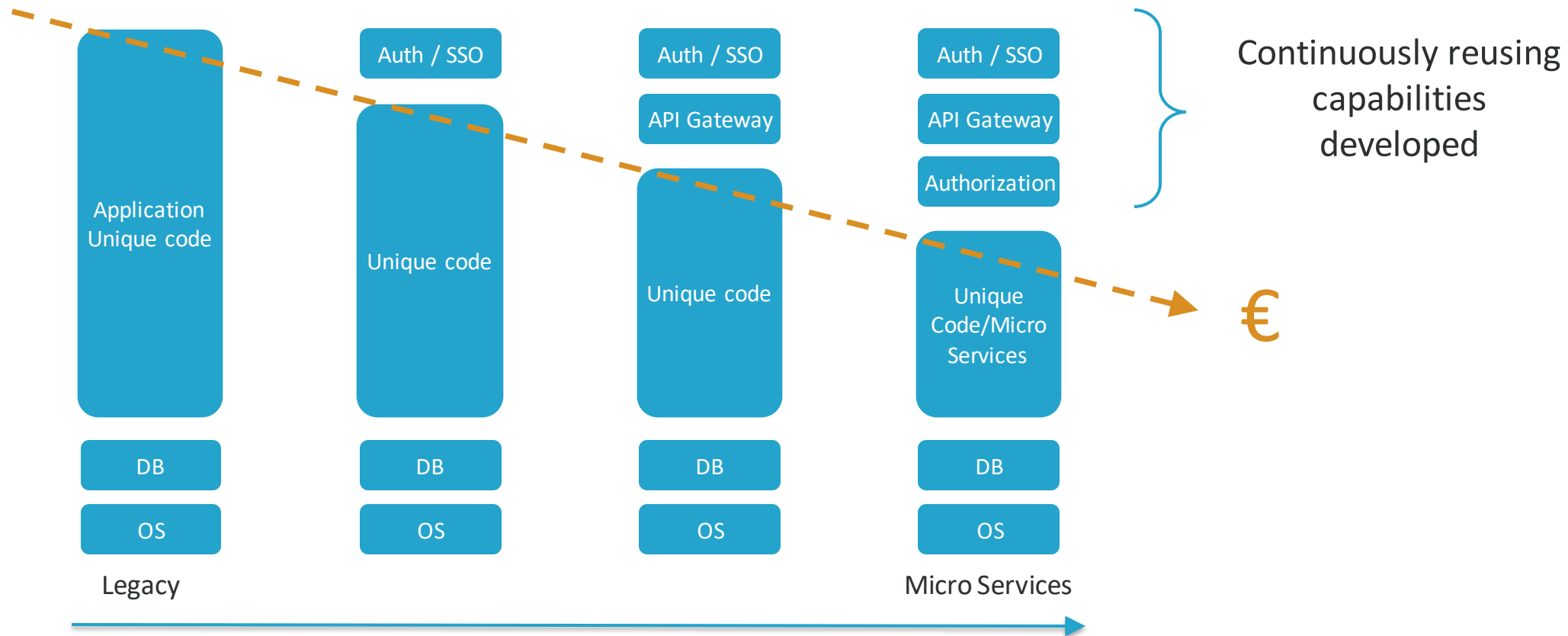
'New': ABAC

- Exit if:
 - Paid amount due
 - Recently...
- Only if:
 - Brand is Kia
- We don't care:
 - Who is the actor...

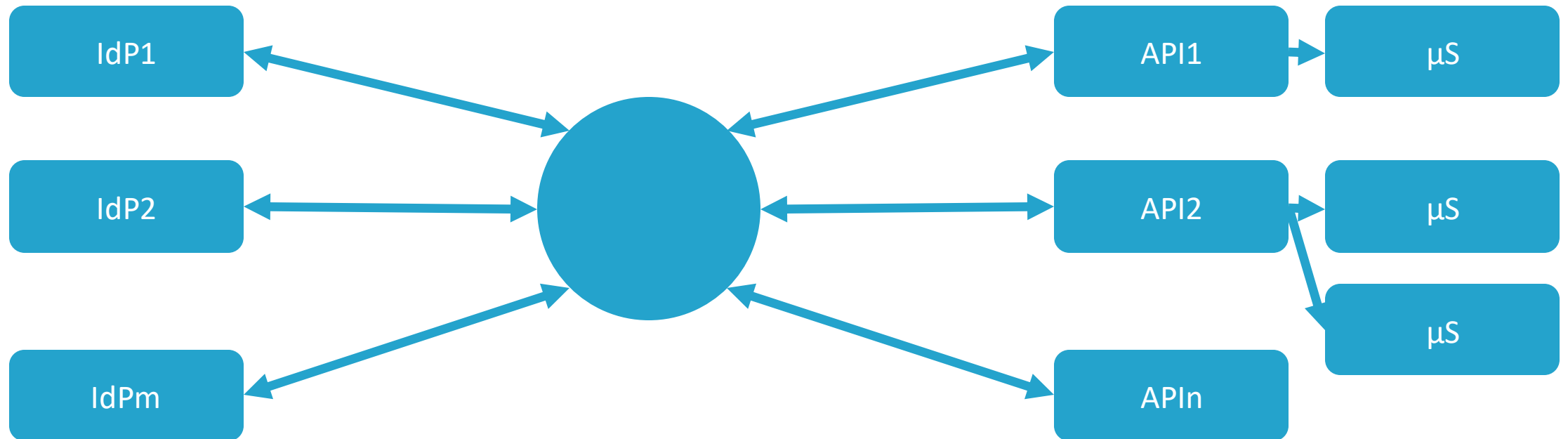


DevOps transition

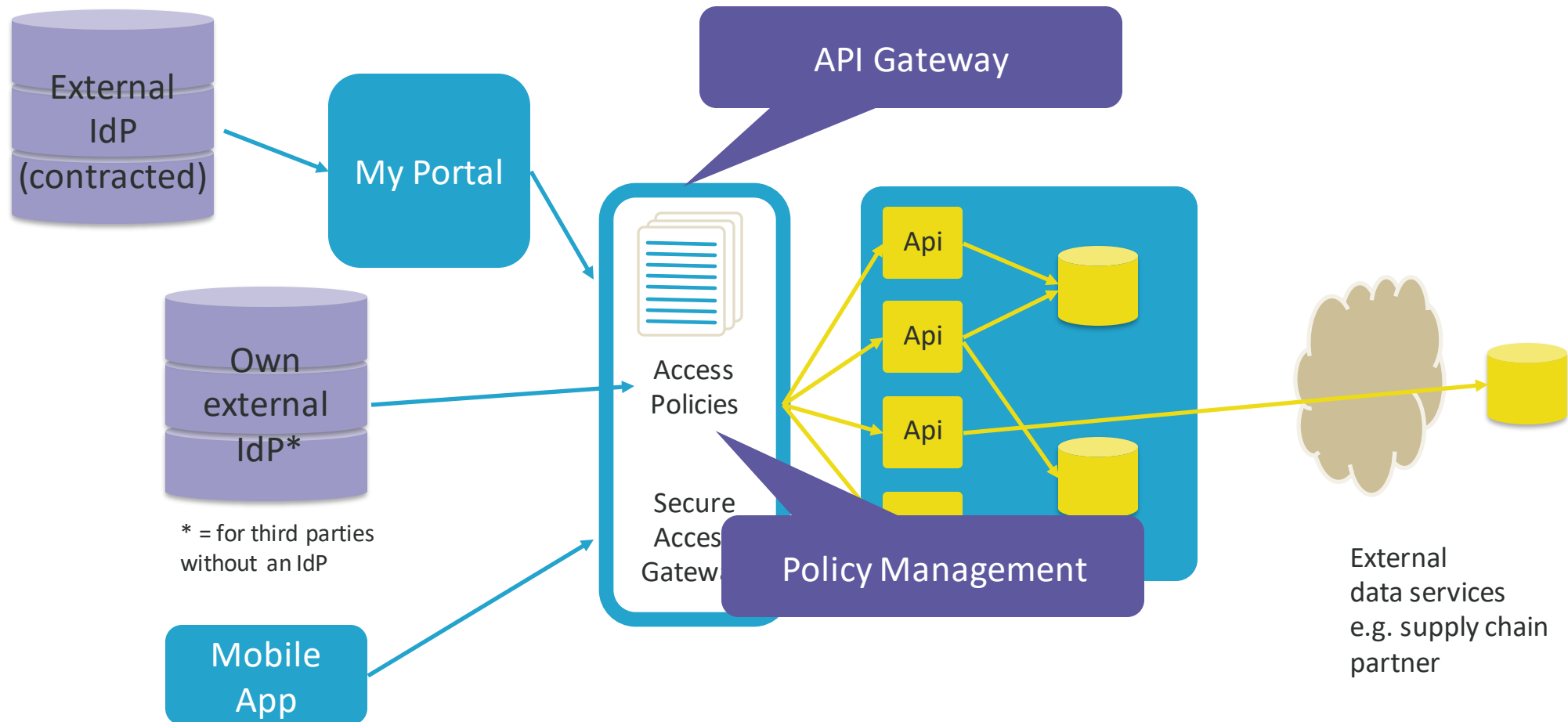
Externalised Services for Application Development



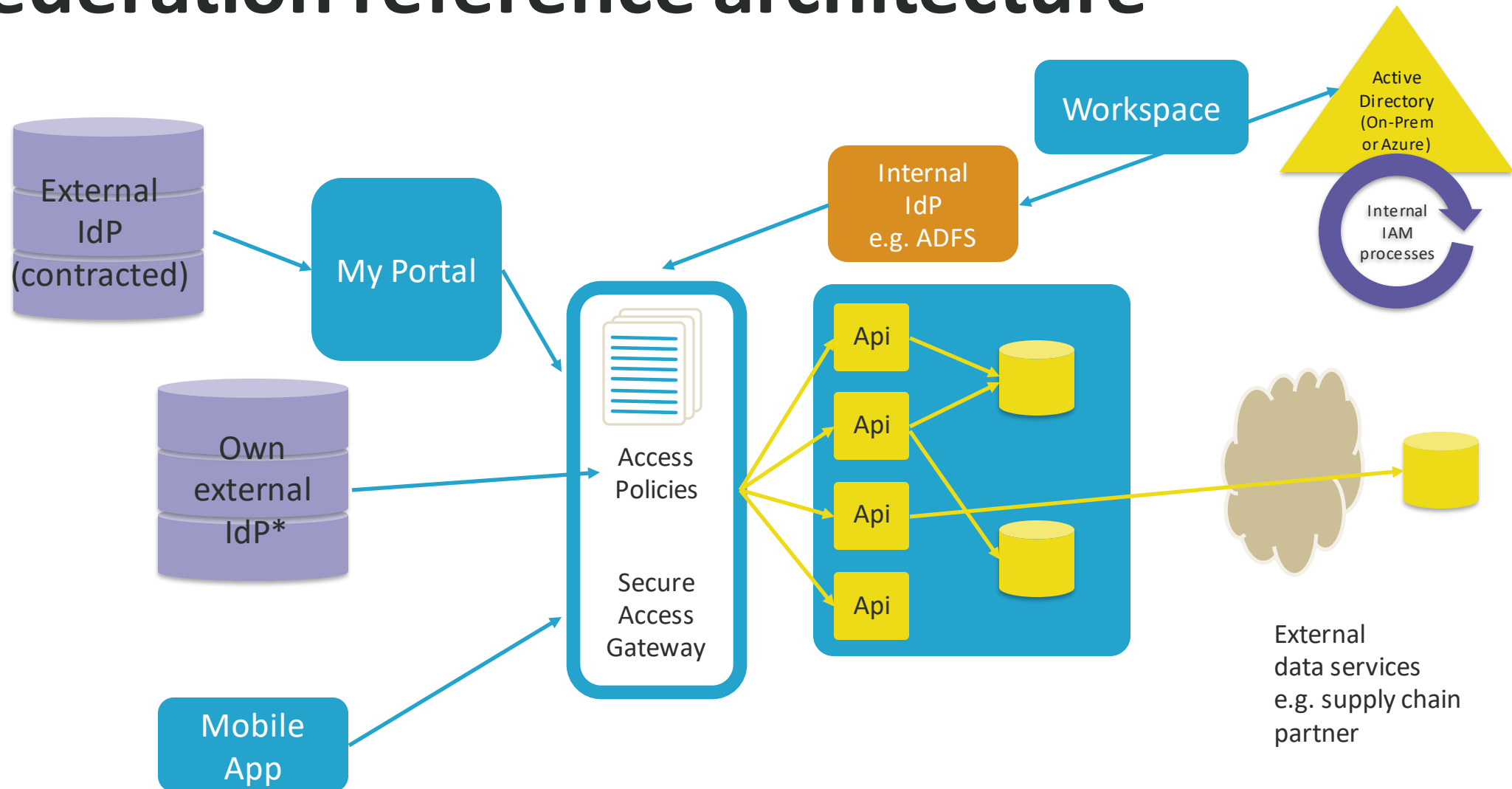
Access Broker



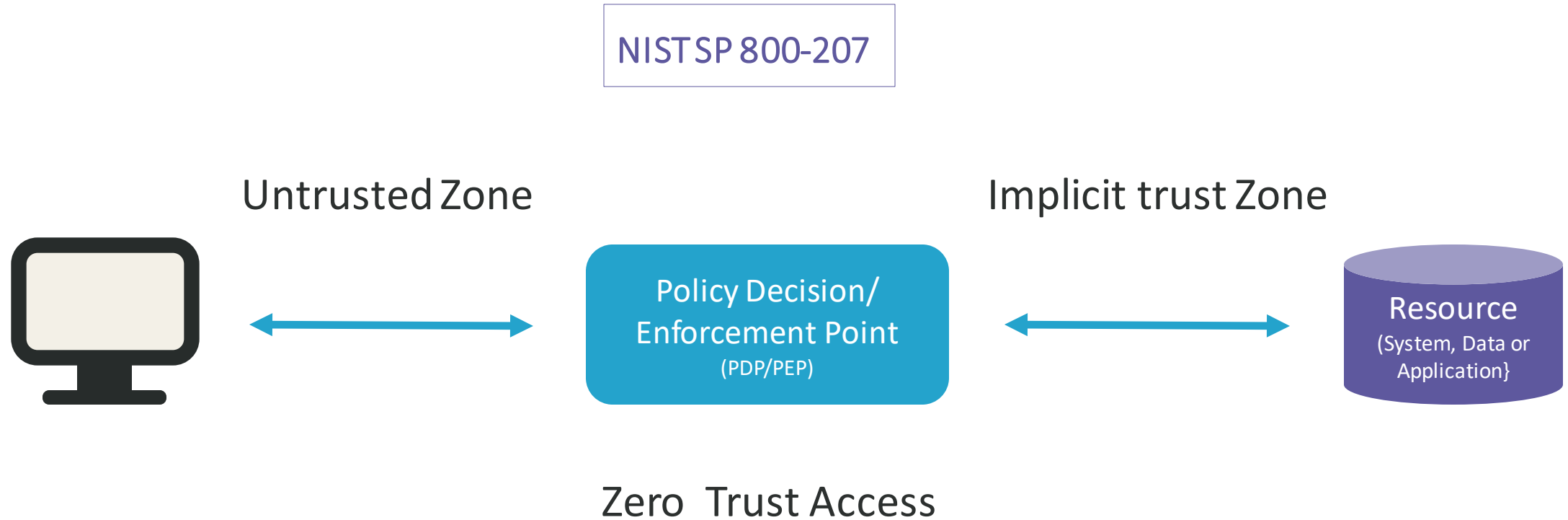
Federation reference architecture



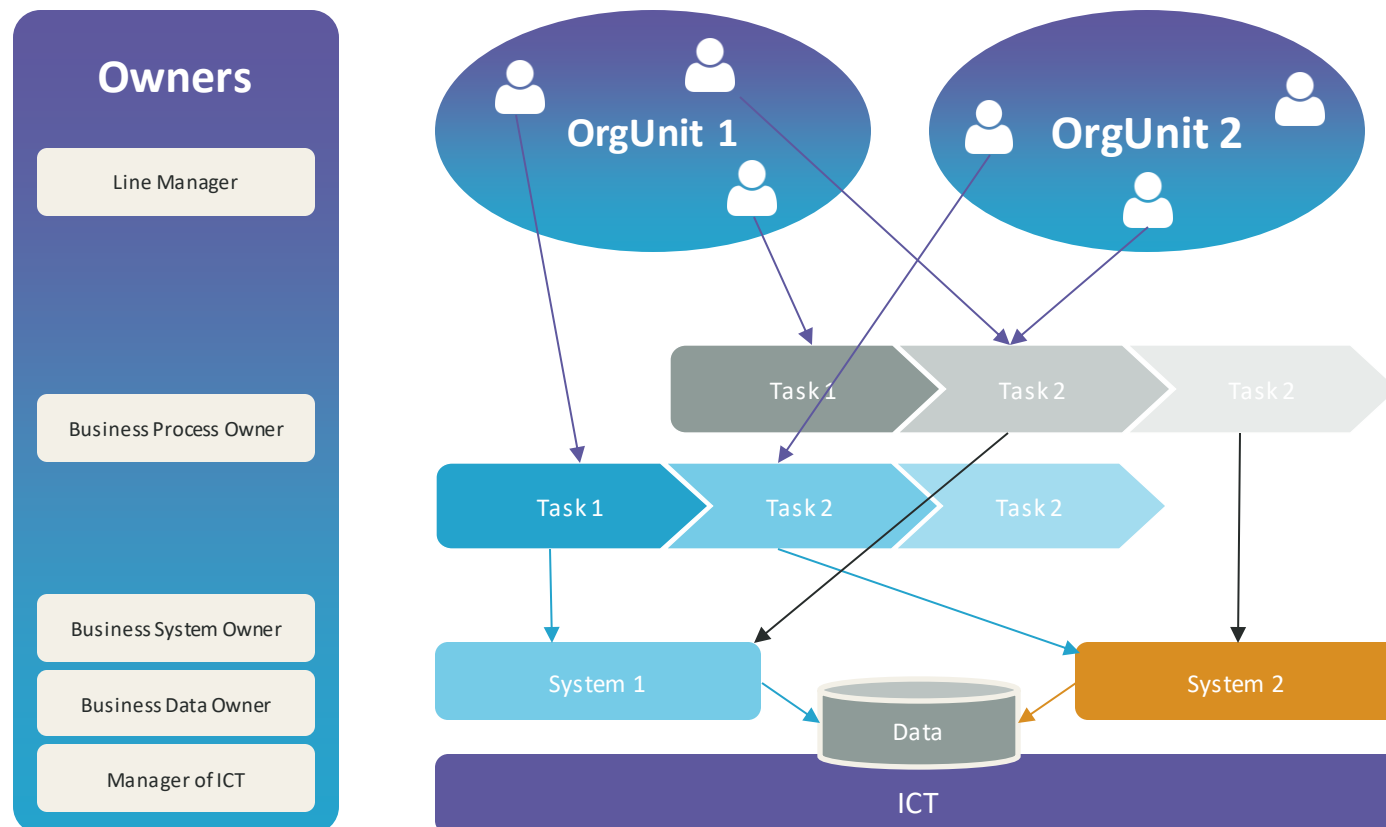
Federation reference architecture



Zero Trust reference architecture



Access Governance



Policy Management where in the organisation:

HR reqs / attribs

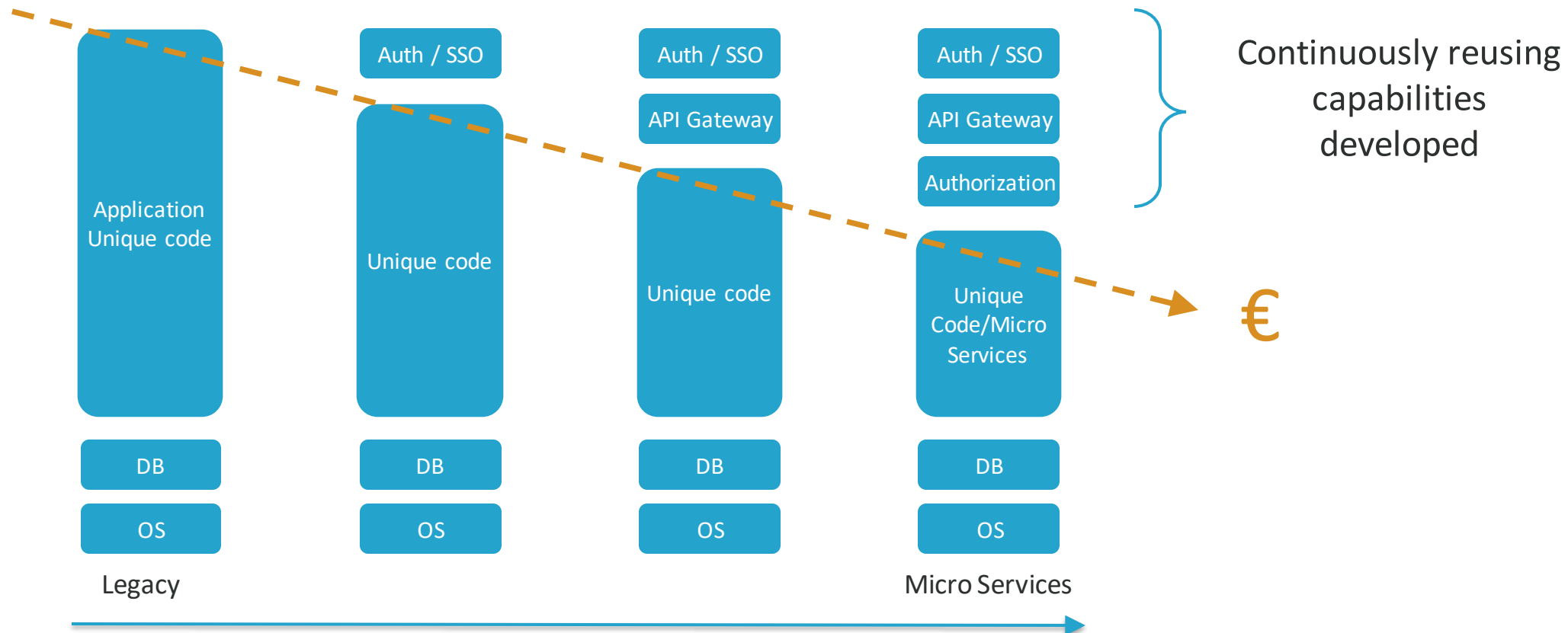
Actor reqs, SoD
Quality reqs

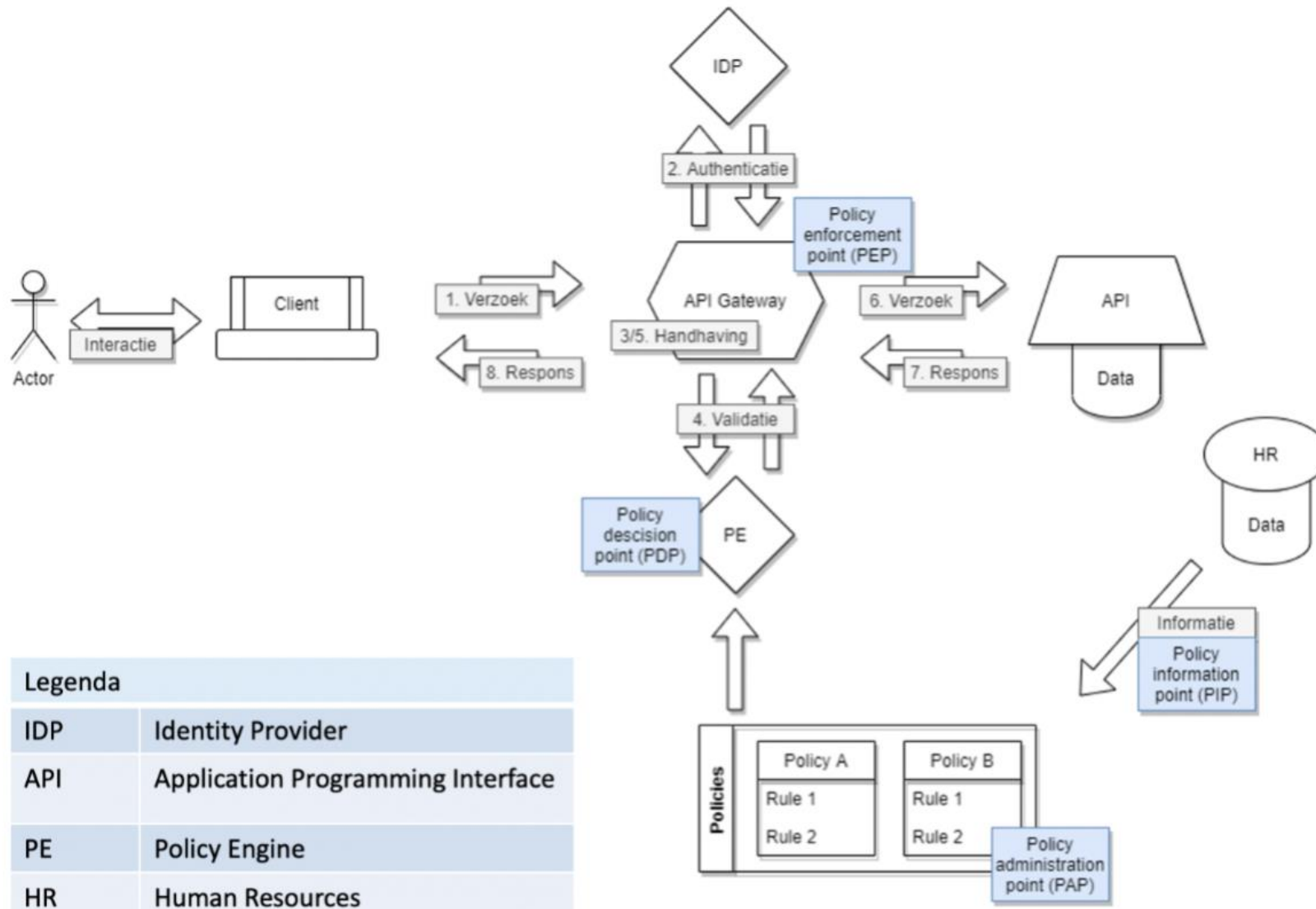
Authz model, licensing

Compliance Access Rules
(privacy etc.)
Physical Access rules

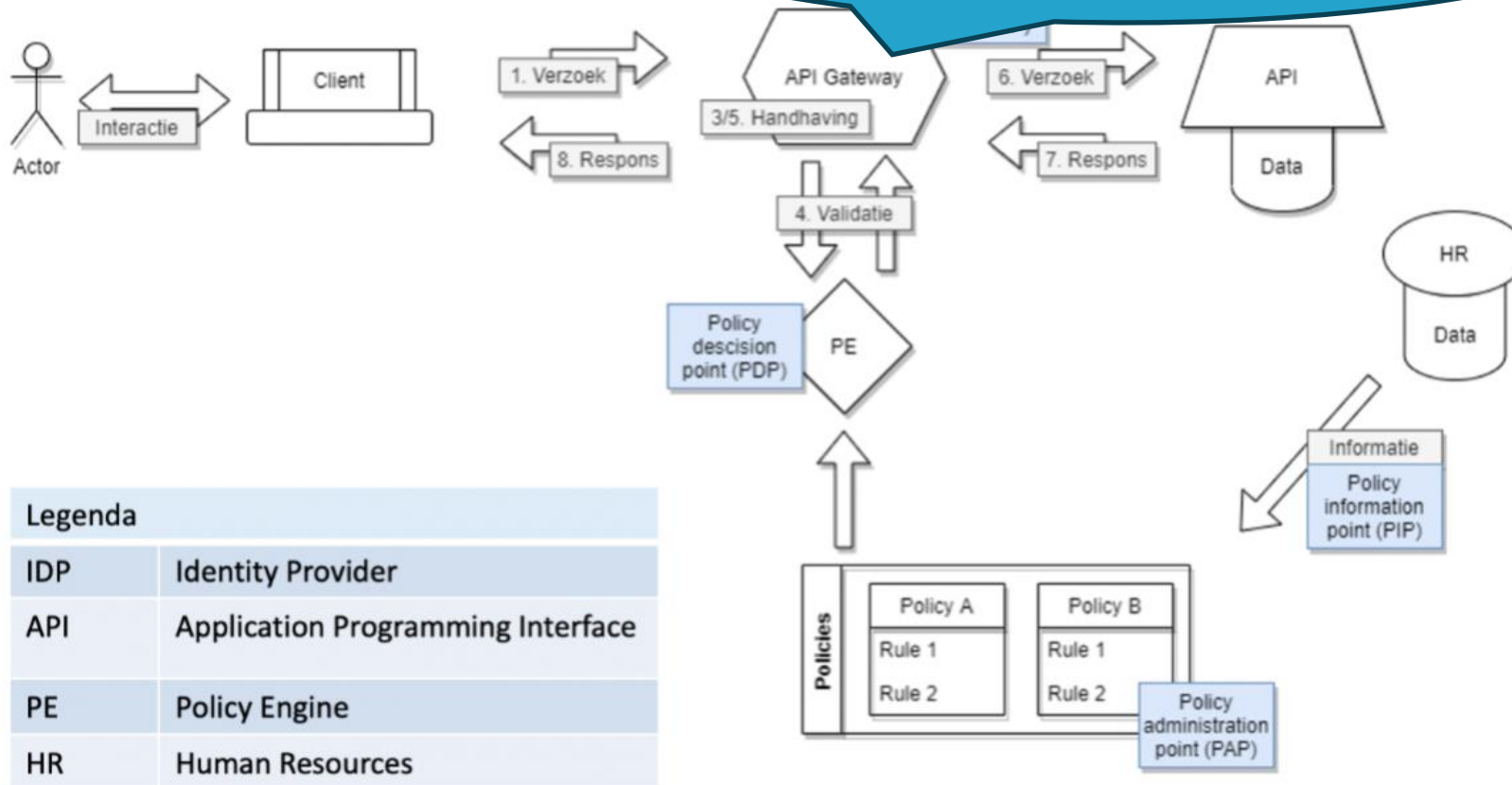
IT architecture transition

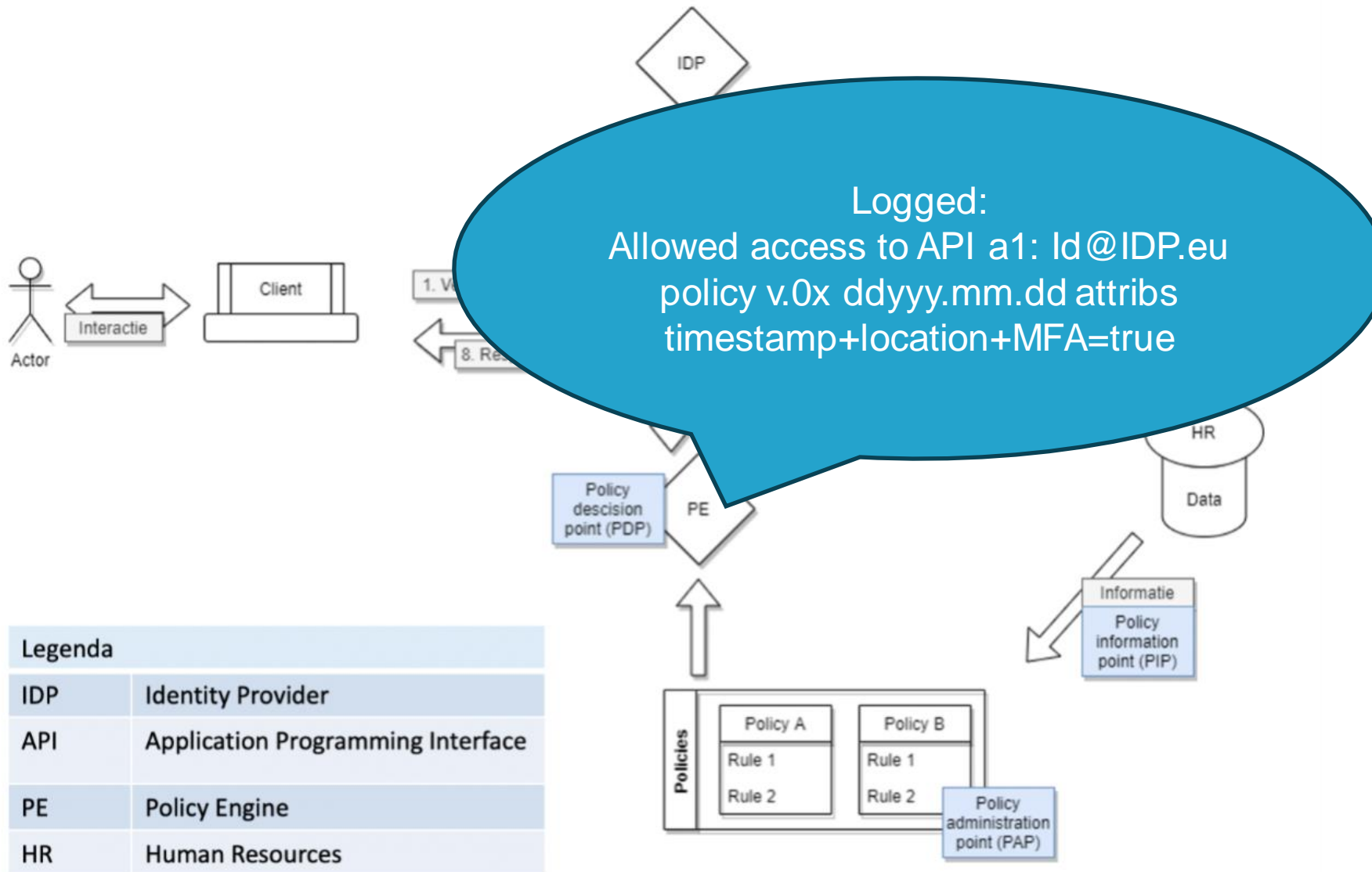
From Platform to Protocol



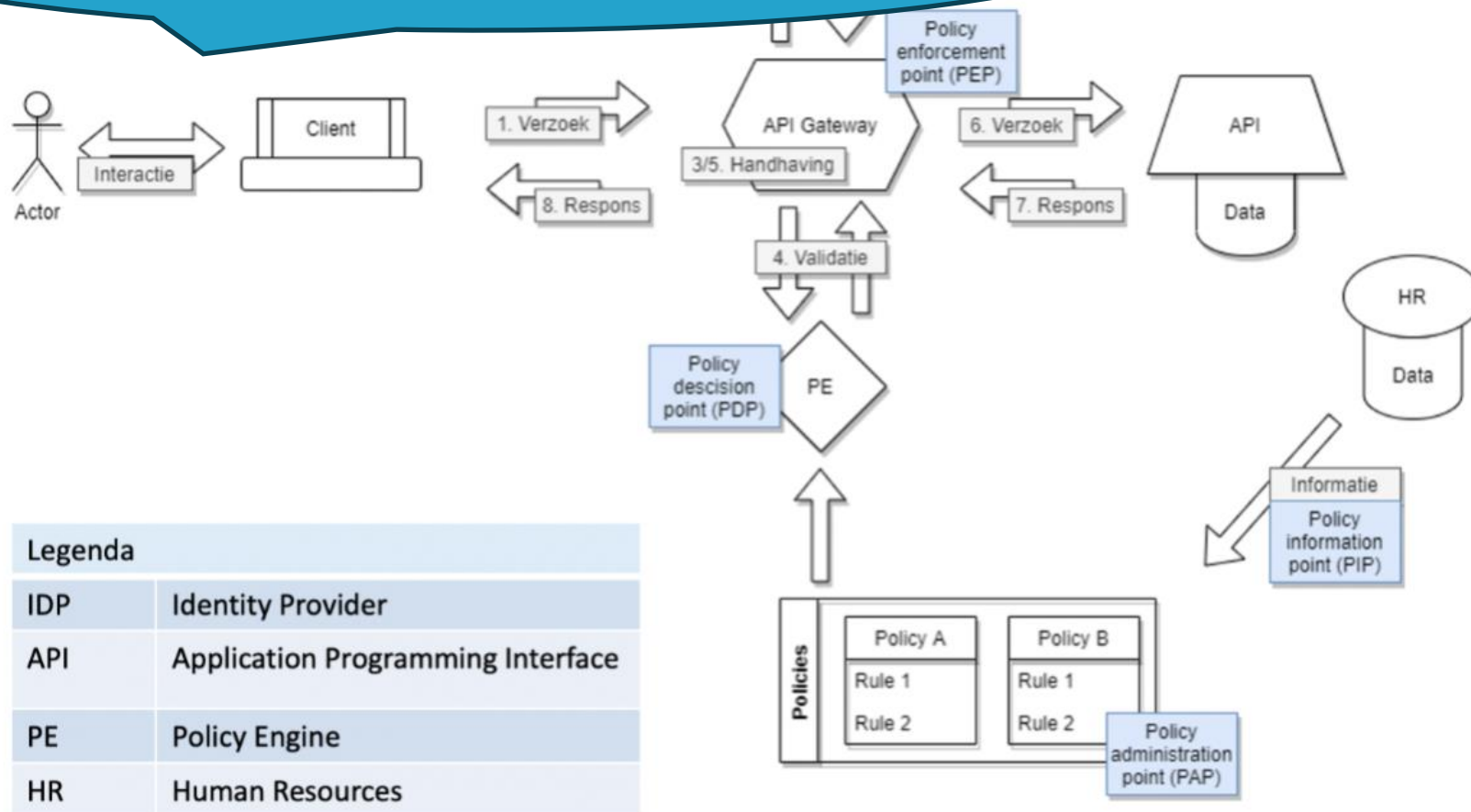


Precondition:
IDP.eu is trusted to access API a1

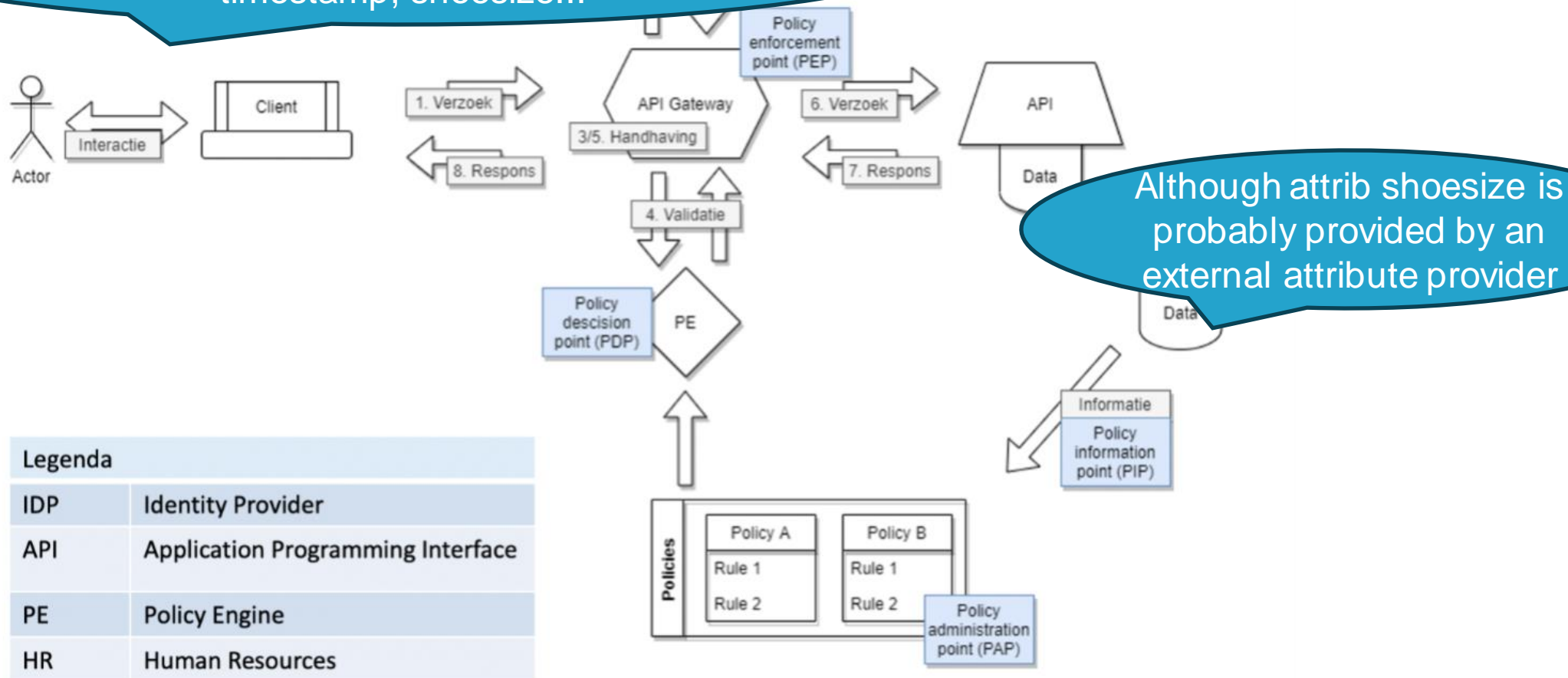




We don't care about the actor with ID@IDP.eu

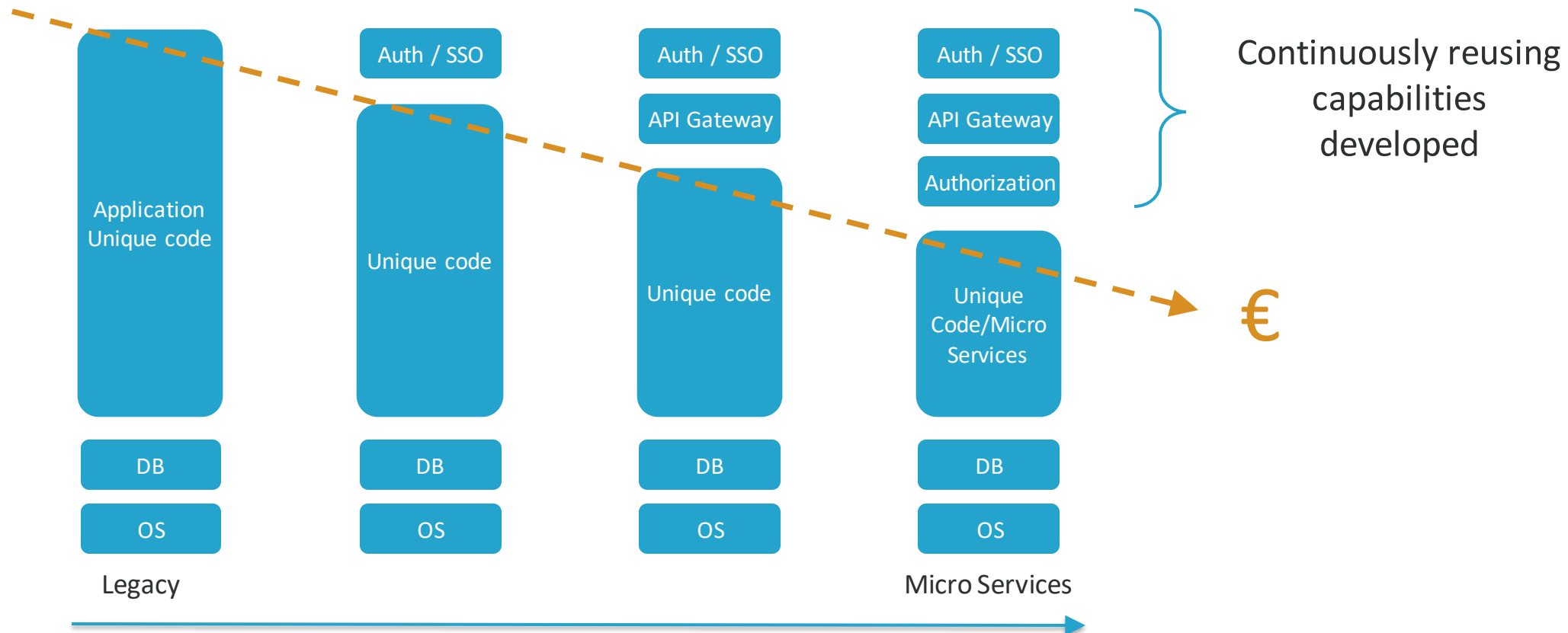


Attributes can be: userid, role (AD group membership), MFA level, location, network, timestamp, shoesize...



Auditing transition

From data and roles to Policy validation



```
1  package test
2  import data.dataset
3
4  default allow = false
5
6  allow {
7      input.token.email == "andre.koot@sonicbee.nl"
8  }
```

JSON ▾

Auth ▾

Query

Headers 3

Docs

1 ▾ {

2 "input":

3 ▾ { "token": {

4 "email": "andre.koot@sonicbee.nl"

5 }

6 }

7 }

8

Beautify JSON

200 OK

121 ms

79 B

Preview ▾

Headers 11

Cookies 1

Timeline

1 ▾ {

2 "decision_id": "13b534d0-77b0-4ec3-8087-de344bc1bbfe",

3 ▾ "result": {

4 "allow": true

5 }

6 }

JSON ▾

Auth ▾

Query

Headers 3

Docs

1 ▾ {

2 "input":

3 ▾ { "token": {

4 "email": "edgar.zitha@sonicbee.nl"

5 }

6 }

7 }

8

Beautify JSON

200 OK

244 ms

80 B

Preview ▾

Headers 11

Cookies 1

Timeline

1 ▾ {

2 "decision_id": "4b2f5d10-324a-4600-9f81-69a9ee5e6156",







3 ▾ "result": {

4 "allow": false

5 }

6 }

Styra Decision logs

>	 Denied	 	12/09/2023, 16:30:58.975 CEST	rules	2ms
>	 Allowed	 	12/09/2023, 16:33:11.311 CEST	rules	< 1ms

Allowed 12/09/2023, 16:33:11.311 CEST rules < 1ms

```
1 {
2   "labels": {
3     "id": "6fcf6c12-4ce9-44a6-a23c-80851fc61246",
4     "system-id": "daa3fdcd615642be92d5bf3428f0a766",
5     "system-type": "custom",
6     "version": "0.51.0"
7   },
8   "decision_id": "13b534d0-77b0-4ec3-8087-de344bc1bbfe",
9   "path": "rules",
10  "input": {
11    "token": {
12      "email": "andre.koot@sonicbee.nl"
13    }
14  },
15  "result": {
16    "allow": true
17  },
18  "requested_by": "172.27.0.1:55962",
19  "timestamp": "2023-09-12T14:33:11.311850416Z",
20  "metrics": {
21    "counter_server_query_cache_hit": 1,
22    "timer_rego_external_resolve_ns": 400,
23    "timer_rego_input_parse_ns": 32695,
24    "timer_rego_query_eval_ns": 309653,
25    "timer_server_handler_ns": 405639
26  },
27  "nd_built_in_cache": {},
28  "agent_id": "6fcf6c12-4ce9-44a6-a23c-80851fc61246",
29  "system_id": "daa3fdcd615642be92d5bf3428f0a766",
30  "system_type": "custom",
31  "policy_type": "rules",
32  "received": "2023-09-12T14:33:23.087361027Z",
33  "allowed": {
34    "value": true
35  },
36  "decision_type": "ALLOWED",
37  "columns": []
38 }
```

Denied 12/09/2023, 16:30:58.975 CEST rules 2ms

```
1 {
2   "labels": {
3     "id": "6fcf6c12-4ce9-44a6-a23c-80851fc61246",
4     "system-id": "daa3fdcd615642be92d5bf3428f0a766",
5     "system-type": "custom",
6     "version": "0.51.0"
7   },
8   "decision_id": "4b2f5d10-324a-4600-9f81-69a9ee5e6156",
9   "path": "rules",
10  "input": {
11    "token": {
12      "email": "edgar.zitha@sonicbee.nl"
13    }
14  },
15  "result": {
16    "allow": false
17  },
18  "requested_by": "172.27.0.1:38560",
19  "timestamp": "2023-09-12T14:30:58.975121793Z",
20  "metrics": {
21    "counter_server_query_cache_hit": 1,
22    "timer_rego_external_resolve_ns": 400,
23    "timer_rego_input_parse_ns": 604496,
24    "timer_rego_query_eval_ns": 441998,
25    "timer_server_handler_ns": 1720590
26  },
27  "nd_built_in_cache": {},
28  "agent_id": "6fcf6c12-4ce9-44a6-a23c-80851fc61246",
29  "system_id": "daa3fdcd615642be92d5bf3428f0a766",
30  "system_type": "custom",
31  "policy_type": "rules",
32  "received": "2023-09-12T14:31:03.096620586Z",
33  "allowed": {
34    "value": false
35  },
36  "decision_type": "DENIED",
37  "columns": []
38 }
```

Typical audit findings in identity and access audits could include:

1.Are the relevant business stakeholders in Access Governance defined:

Access control is a business responsibility, with different stakeholders.

2.Are the relations between identity providers and relying parties formalised:

Services and API's should only be consumed by trusted internal and external parties. If there is no trusted external party, is a trusted IdP available?

3.Are relevant attributes clearly defined in the access policy:

Attributes, claims and verifiable credentials contain information that can be used to validate access requests. Identities and accounts are not relevant anymore (although a role can be treated as an attribute if the back-end system is still an RBAC-application)

4.Have reliable attribute sources been defined:

Attributes can be gathered from multiple sources. Define the one source that is primarily accountable for the attribute operations store.

5.Do access logs contain the relevant data:

We need at least these attributes: id@idp and timestamp.

6.Is version control of policies in place:

An access policy should be treated as a configuration item, it cannot easily change, the policy defined the access control behavior, it's a critical component. With multiple stakeholders relying on the integrity of the dataset.

7. Make sure there is no bypasses accessible:

is zero trust in place, is PKI embedded.



Time for you all...!

André Koot

andre.koot@sonicbee.nl

Tel: +31 6 24512021

#fedi @meneer@mastodon.myfed.space