WAVESTONE

Identity and Access Management

How to secure the access to the information in my IS?

ENSEEIHT 11/12/2020

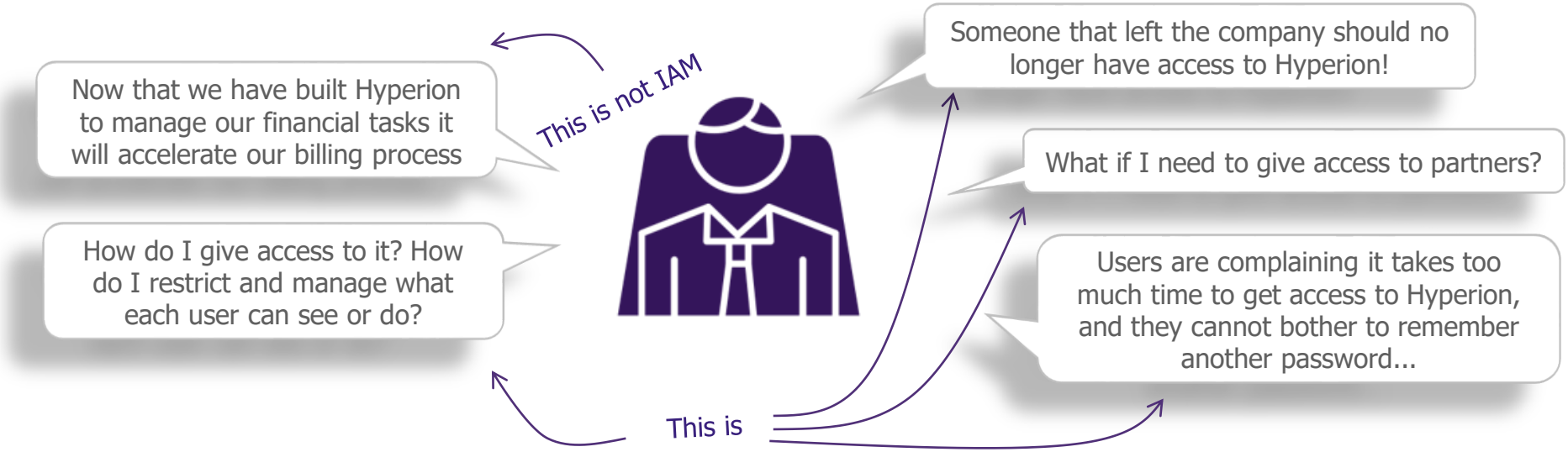
INP TOULOUSE ENSEEIHT

Identity and Access Management

What is IAM ? What does it have to do with the IS ?

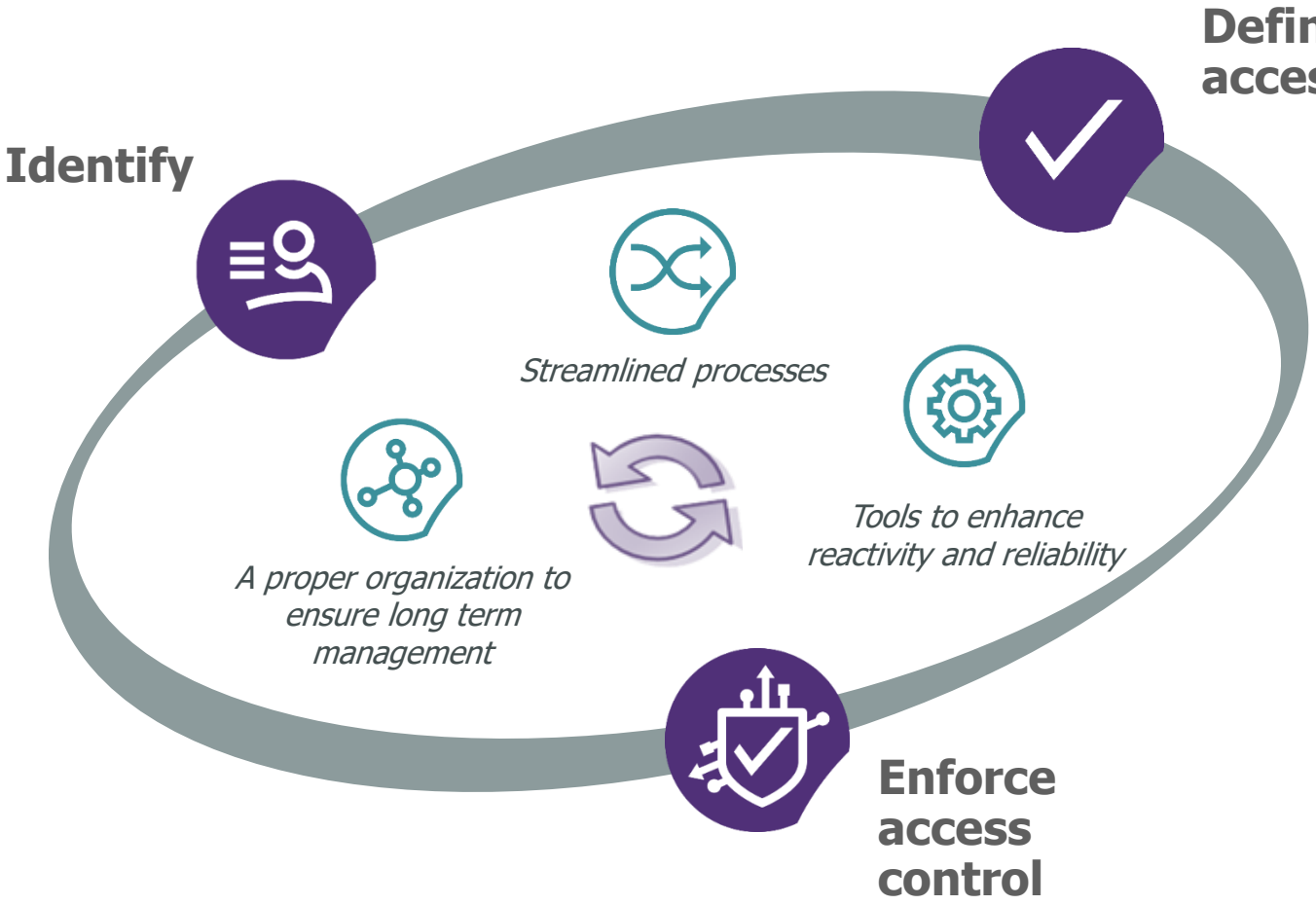
For most companies, the IS is merely a means to an end :
Applications, directories, network : everything in the IS is built towards bettering the product and its distribution (EDF, RTE: electricity providers; L'OREAL: beauty products; DECATHLON: sports appliances and gear; etc.)

➔ IAM is no exception: it aims at providing a set of tools to help build and distribute business



IAM (Identity and Access Management) is the discipline aiming at managing users' access to the IS, while ensuring both ease of use and security

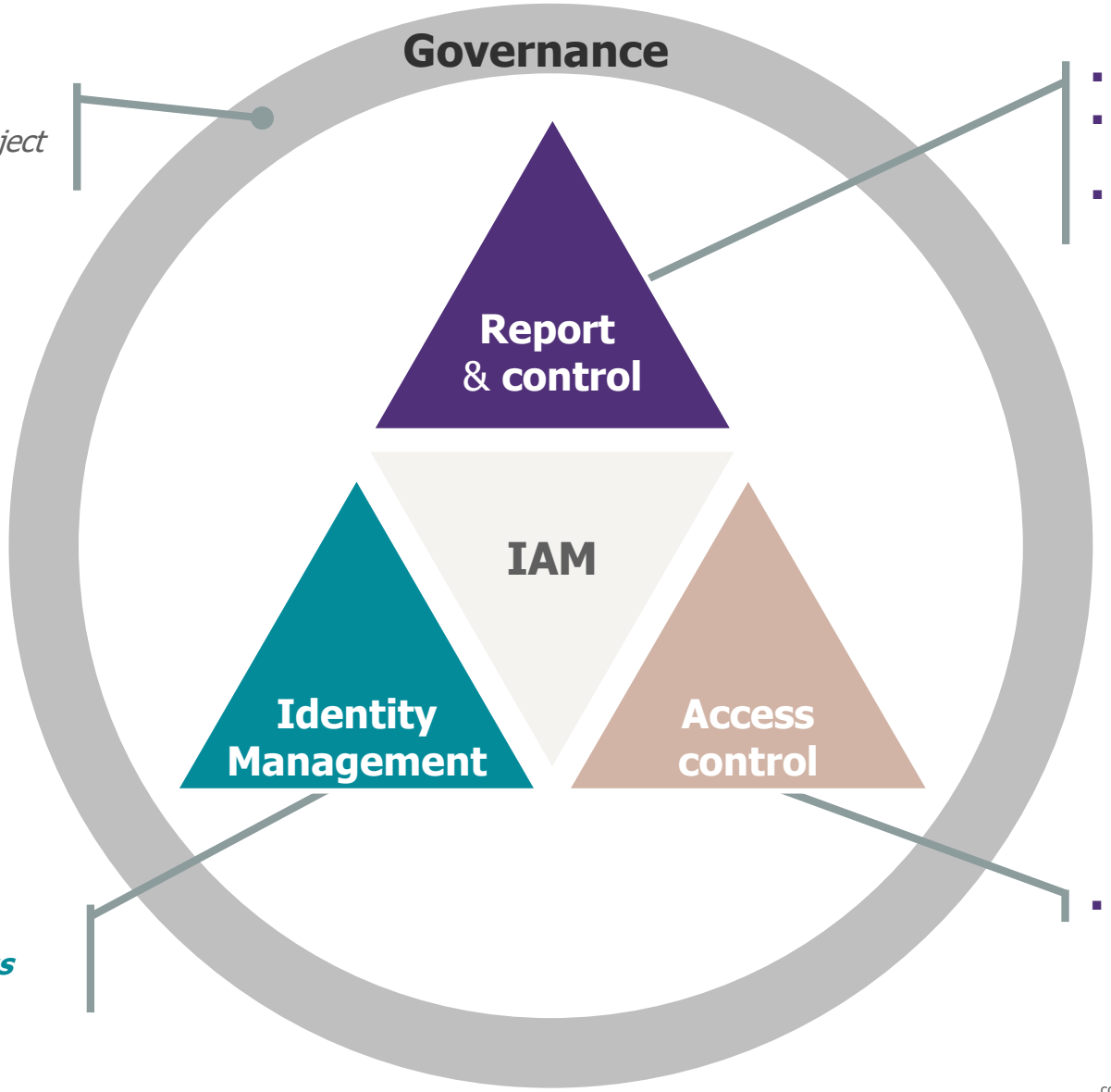
The 3 major stakes of Identity and Access Management



« Give the right access to the right people at the right time »

The 4 facets of IAM

- ***Stakes, goals, means***
  - *Mandatory to any IT project wishing to succeed*



- ***Is my IAM working ?***
- ***Do I respect legislations ?***
- ***What can I do to make it better ?***

- ***Identify***
- ***Define who can access what***

- ***Enforce access control***

Identity Management

How do I exist within the IS ? WHY do I exist within the IS ?

Today we will focus on "user" accounts but there are many other types (generic, bots, service, …)

Let's improve our efficiency with Hyperion!

Foundation wants its employees to have facilitated financial processes to be more efficient in their daily business

Application: it provides services to multiple users
e.g.: list inventory of rooms in an hospital
"I would like to allow users to see the rooms and their availability in Hyperion, but I need a way of differentiating my users. How do I do that?"

To differentiate them, your users need to have accounts in Hyperion

Accounts : accounts allow an application to differentiate users, and personalize their experience.
e.g.: my login/password gives me information of the rooms from the Foundation facility I work at
"I created accounts for my users, can I just stock them in the Hyperion database?"

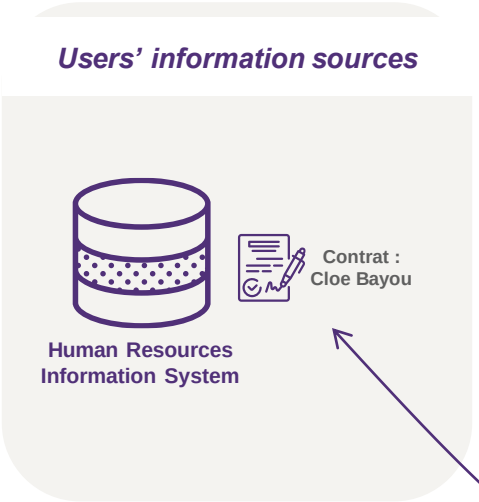
You could use Hyperion's database to store user accounts but it is better to have a directory server

Directory server : data containers, most of the time specialized in storing accounts information (identifiers and multiple attributes). They can be used by multiple applications and allow to use the same login/password.
e.g. : 389DS, Active Directory, OpenLDAP…
"This looks great ! I noticed every application has its own directory so we will create a dedicated one for Hyperion!"

Too many accounts and directories complicate things for the users as well as the IT administration… It would be good to have something to link a user's accounts together…

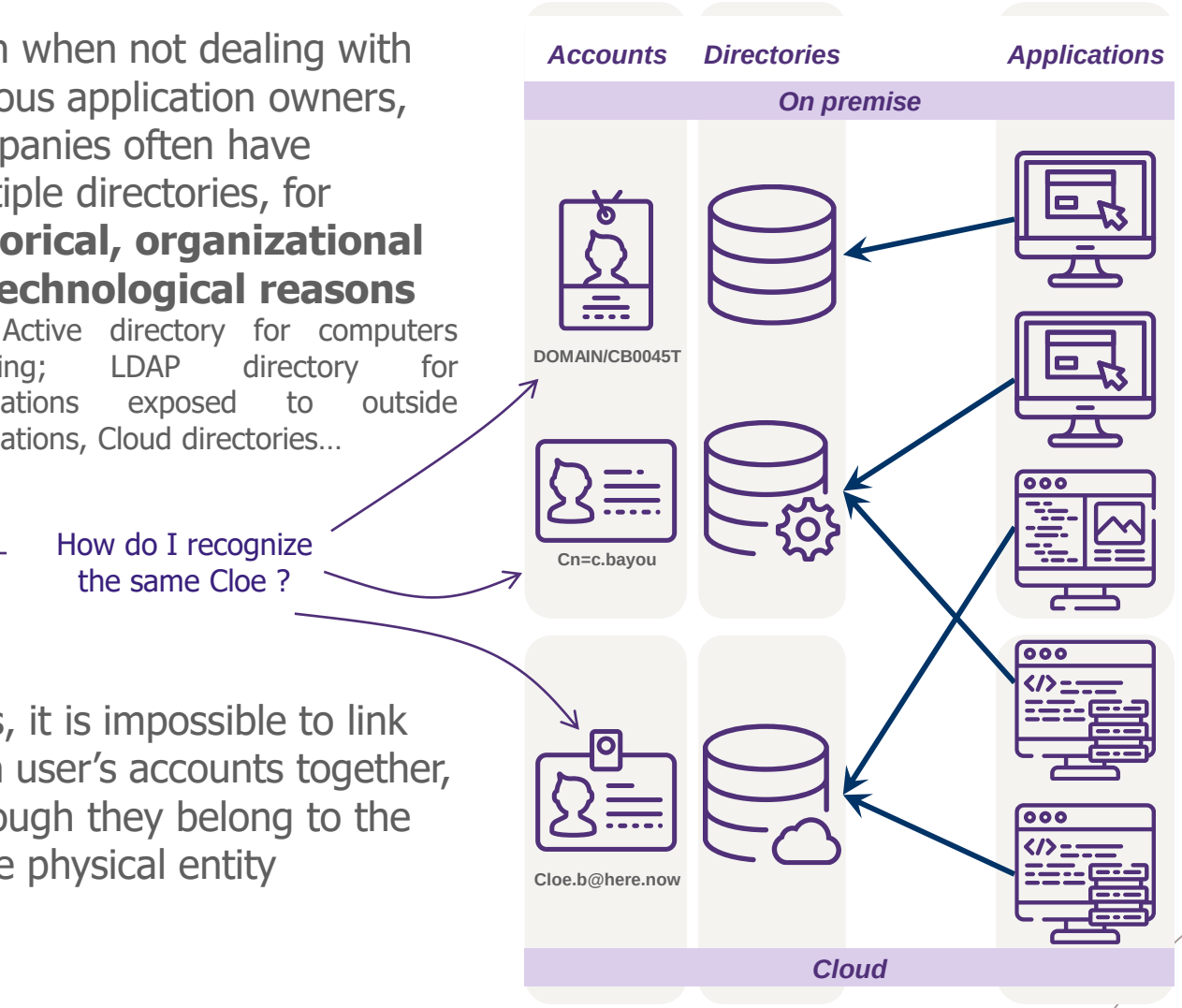
Identity Management

How do I exist within the IS ? WHY do I exist within the IS ?



Even when not dealing with zealous application owners, companies often have multiple directories, for **historical, organizational or technological reasons**

e.g. Active directory for computers handling; LDAP directory for applications exposed to outside applications, Cloud directories…



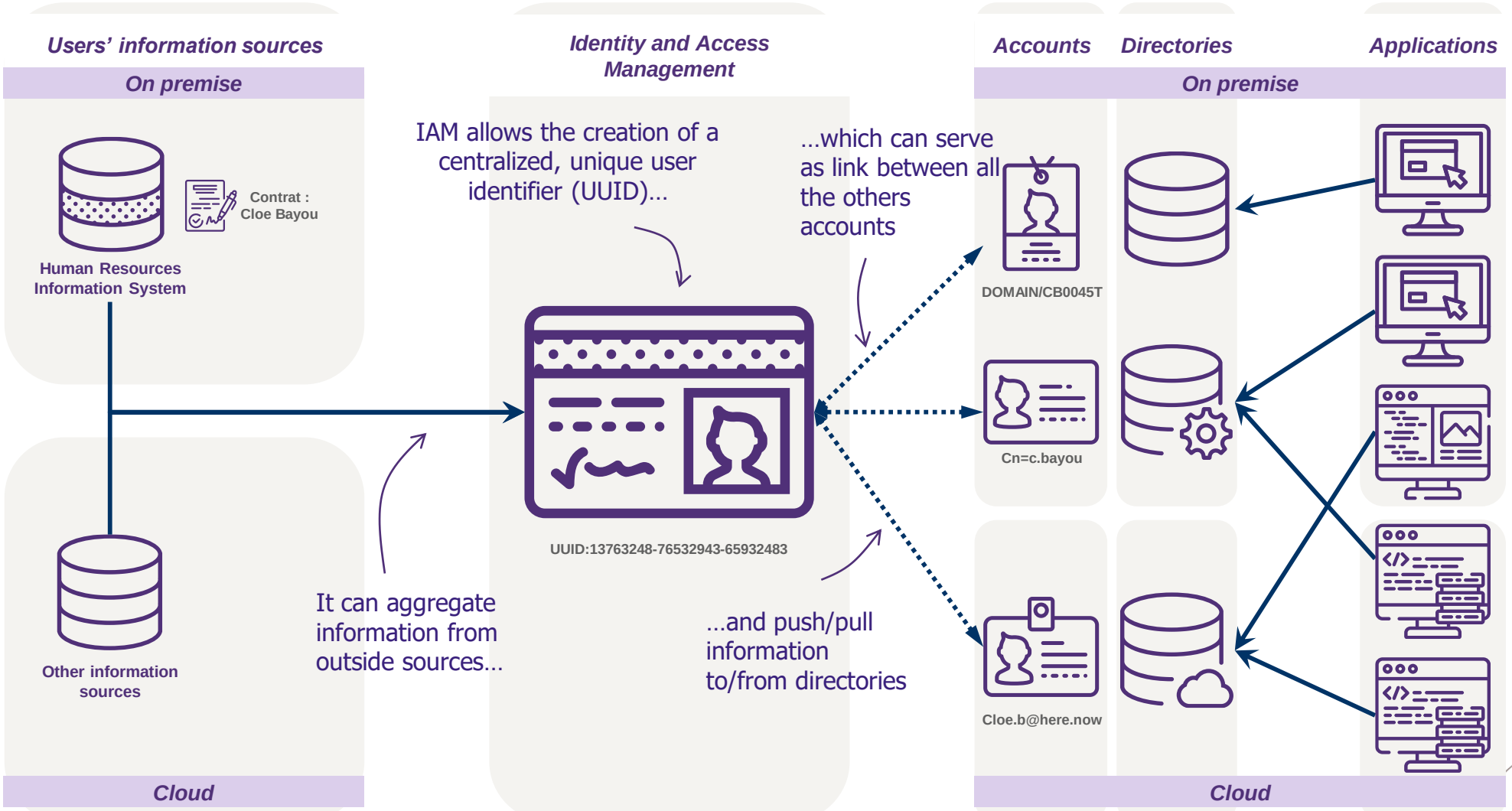
Users' information also exist by design in various parts of the IS, although not necessarily under the form of an account

e.g. : HRIS

As-is, it is impossible to link each user's accounts together, although they belong to the same physical entity

Identity Management

How do I exist within the IS ? WHY do I exist within the IS ?



User rights

What is an access right ?

All users are not equal. You want some of them to have a lot of power on your application…

… and others not too much.

I am a full stack expert and I perform production operations on a daily basis

Can see hidden resources, manage users profiles, modify the application…

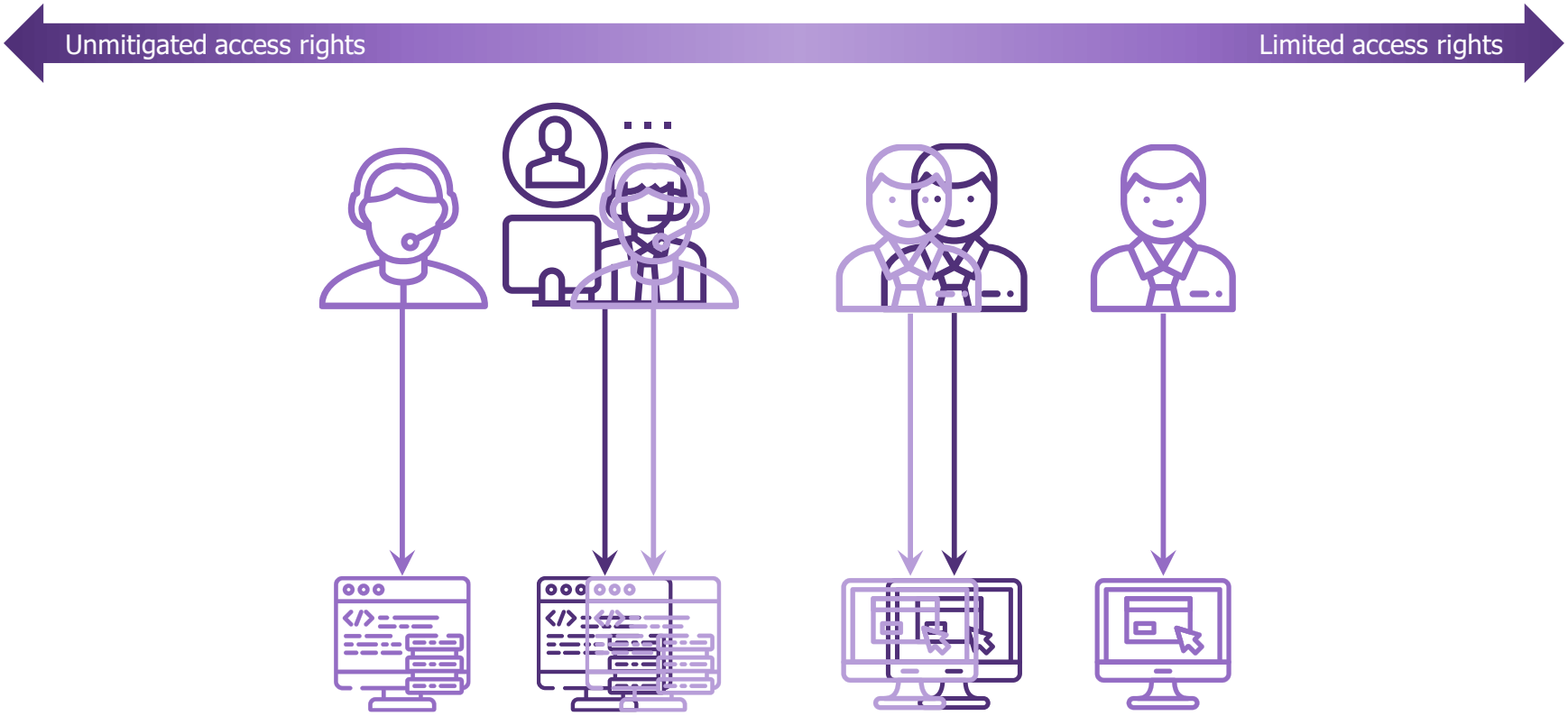
I need to identify available rooms for our arriving patients

Can access specific resources in read-only

Same application, different access rights

User rights

What is an access right ?



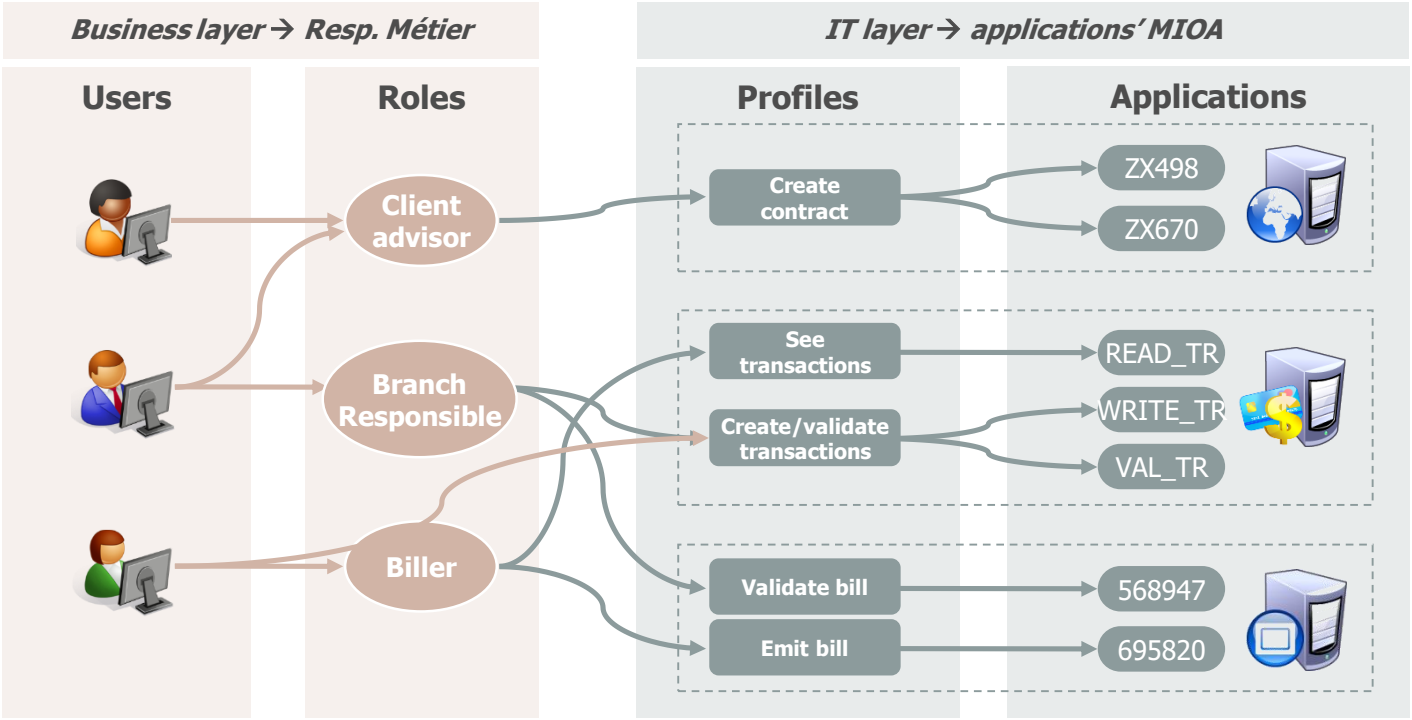
Same application, different access rights

User rights

How are access rights managed ?

Defining a model helps to **better understand access rights**, to better know how to assign them **efficiently and according to business needs**.

Access rights model	The link between People (identities) and access rights



User rights

How are access rights managed ?

Defining a model helps to **better understand access rights**, to better know how to assign them **efficiently and according to business needs**.

Access rights model	The link between People (identities) and access rights

Defining an access models allows for better:

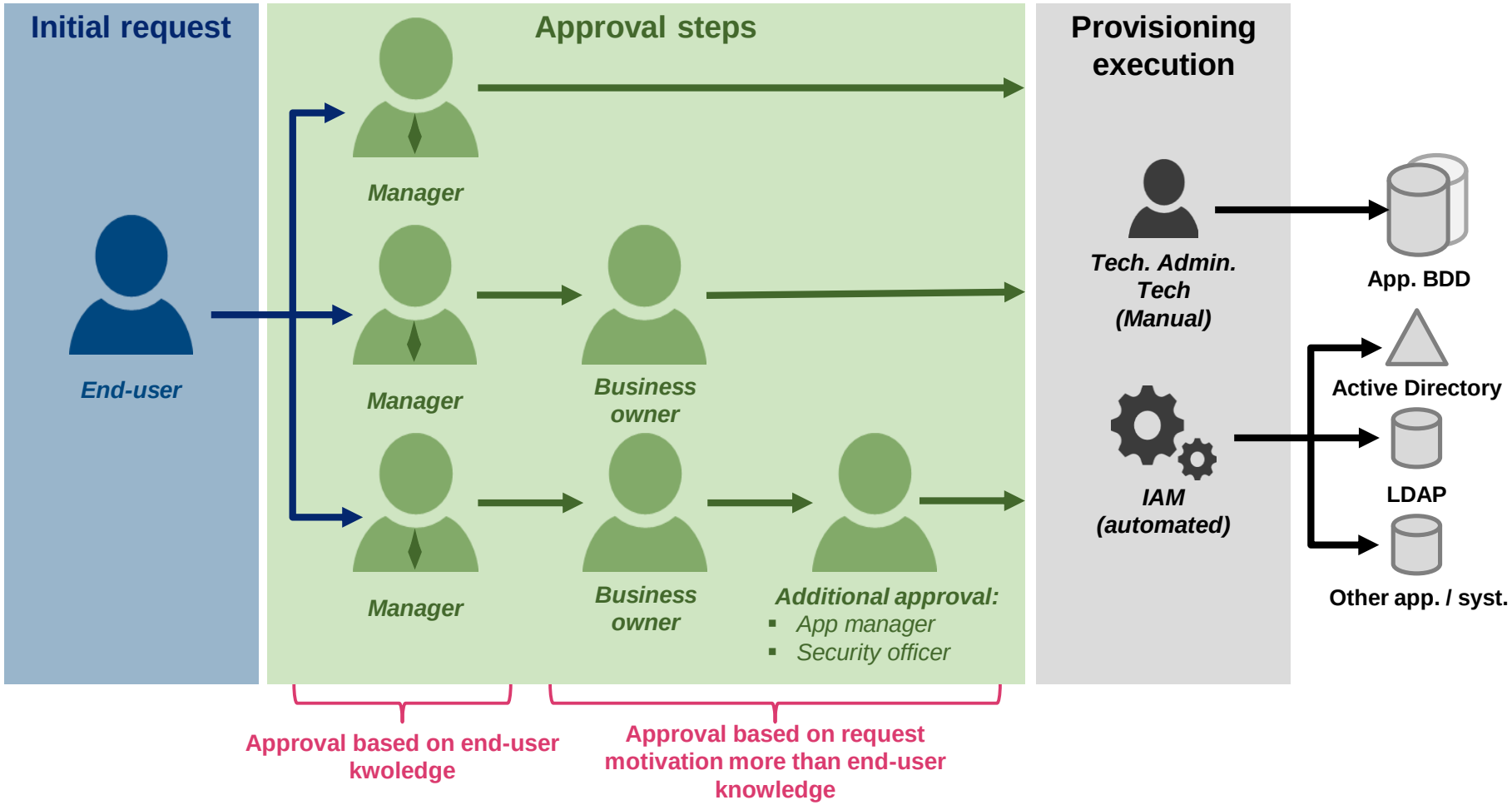
- **Performance** ➔ faster access request process
- **Security** ➔ know what rights are actually assigned and prevent rights copy&paste
- **Compliance** ➔ let managers be responsible and comply with regulation (SoD, SOX…)

But what happens when something
falls out of the loop ?

User rights

How are access rights managed ?

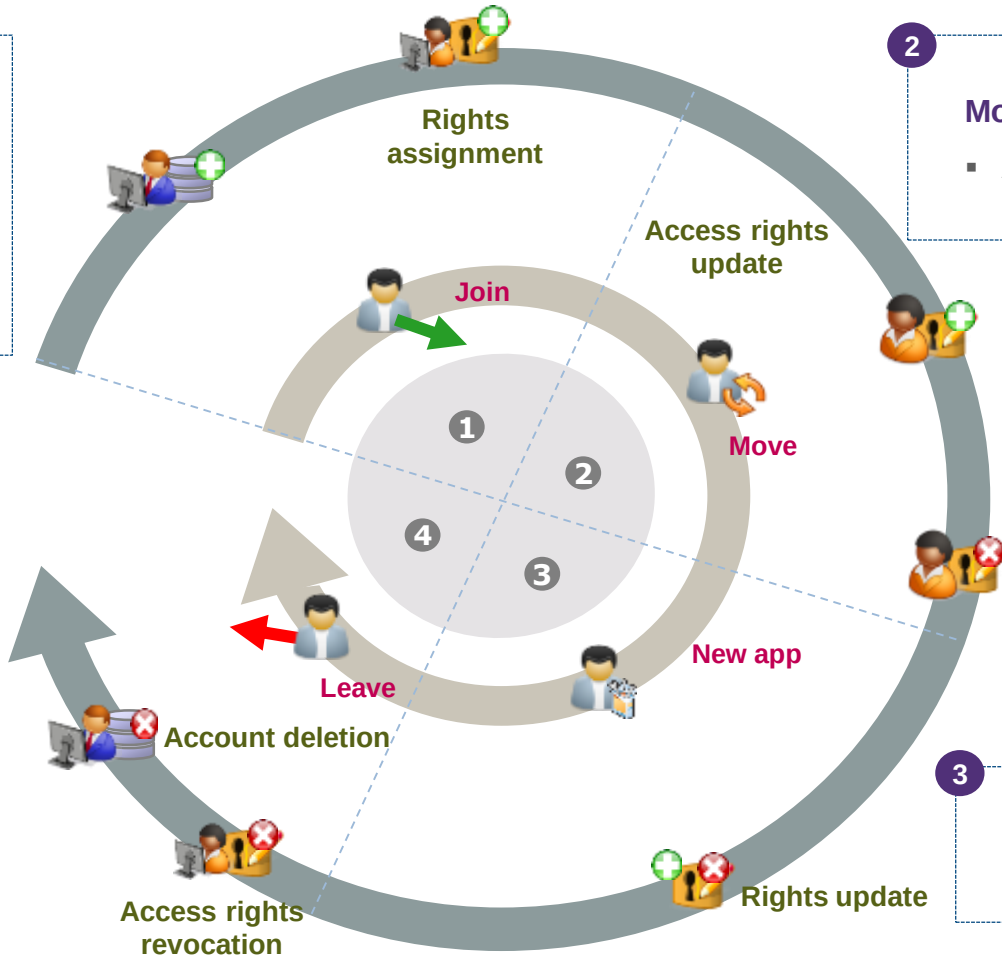
Approval workflows focus



Identity lifecycle and link to access rights

1 Automated identity creation and birth rights

- To be defined through business rules:
  - Everyone gets an AD and email account
  - Everyone in HR gets SAPHR standard access



2 Moves management

- Automated access rights update

New rights assignment linked to new position

Overlap timeframe to define

Removal of rights linked to former position

3 Ad-hoc access rights request *(assignment/removal)*

4 Automated access rights removal

User lifecycle

Access rights lifecycle

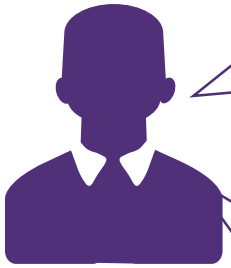
Identity creation

Identity deletion

Rights assignment

Right revokation

First, a few definitions



Identification is the process aiming to disclose the identity of an entity (general case : a user)

Validation is not needed

Authentication is the process aiming to validate the identity of an entity (general case : a user) against a trusted party

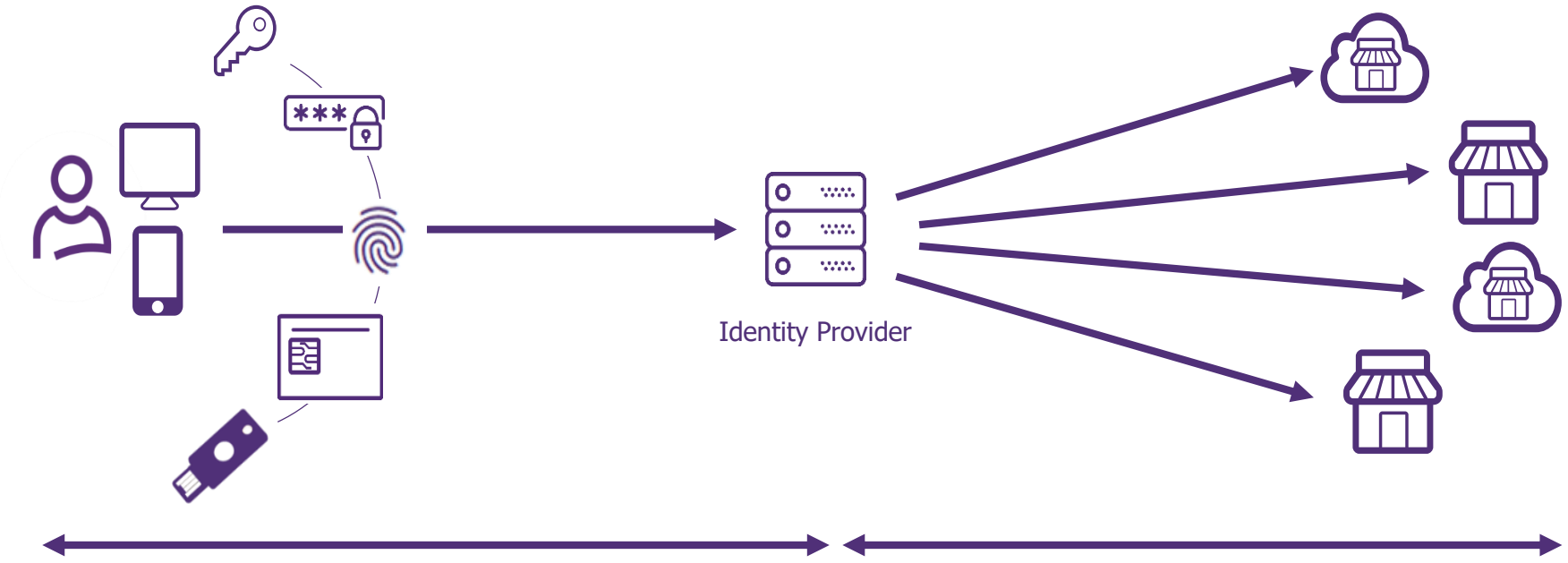
Validation is done using identifiers and credentials provided by the entity

Passwords are still the most deployed type of credentials

Authorization is the process aiming to validate that an **authenticated identity** is **actually authorized** to access a **given resource**

Access control is done relying and access rights previously defined and set

Authentication two phases



"1st mile authentication"

End-user facing

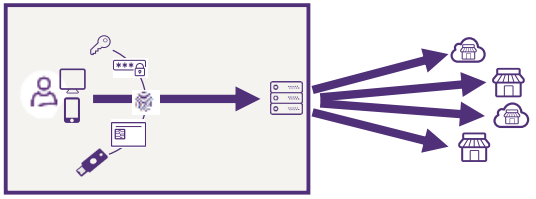
Mot de passe
X.509
OATH
Biométrie
FIDO2

"Last mile authentication"

Application facing

Kerberos
LTPA
HTTP Header / Cookie
SAML
OpenID Connect

Multi-Factor Authentication (MFA)



WHAT ARE THE DIFFERENT AUTHENTICATION FACTORS?

What I know

- Password
- Answer to a secret question
- PIN
- …

What I own

Hardware equipment

- Badge
- Usb token
- Smartphone
- Smartcard
- Hardware token
- …

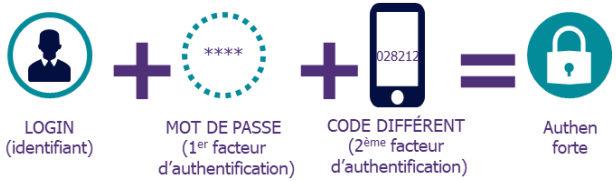
What I am

Physiological Biometrics

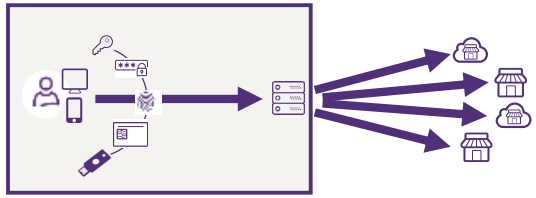
- Fingerprint
- Eye-biometrics (iris & retina)
- Finder/palm vein pattern
- Face shape
- …

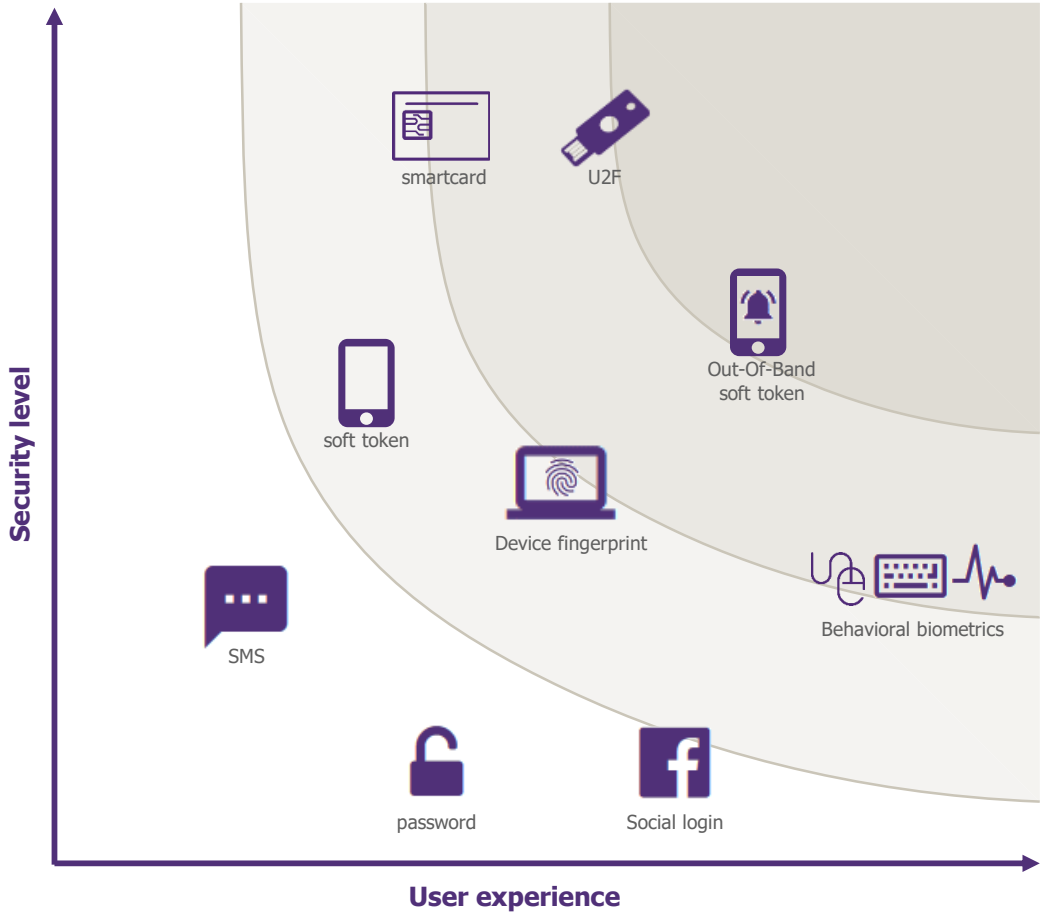
WHAT IS MULTI-FACTOR AUTHENTICATION?

Multi-factor authentication is the combination of two authentication factor in order to strengthen the end-user's authentication. Factors can be of very different forms and should be tied to the target operation whenever possible



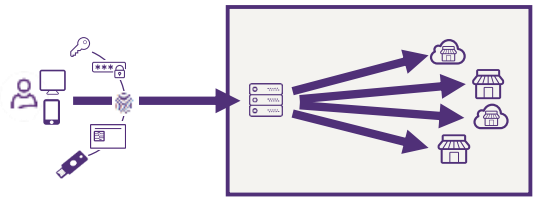
Authentication methods



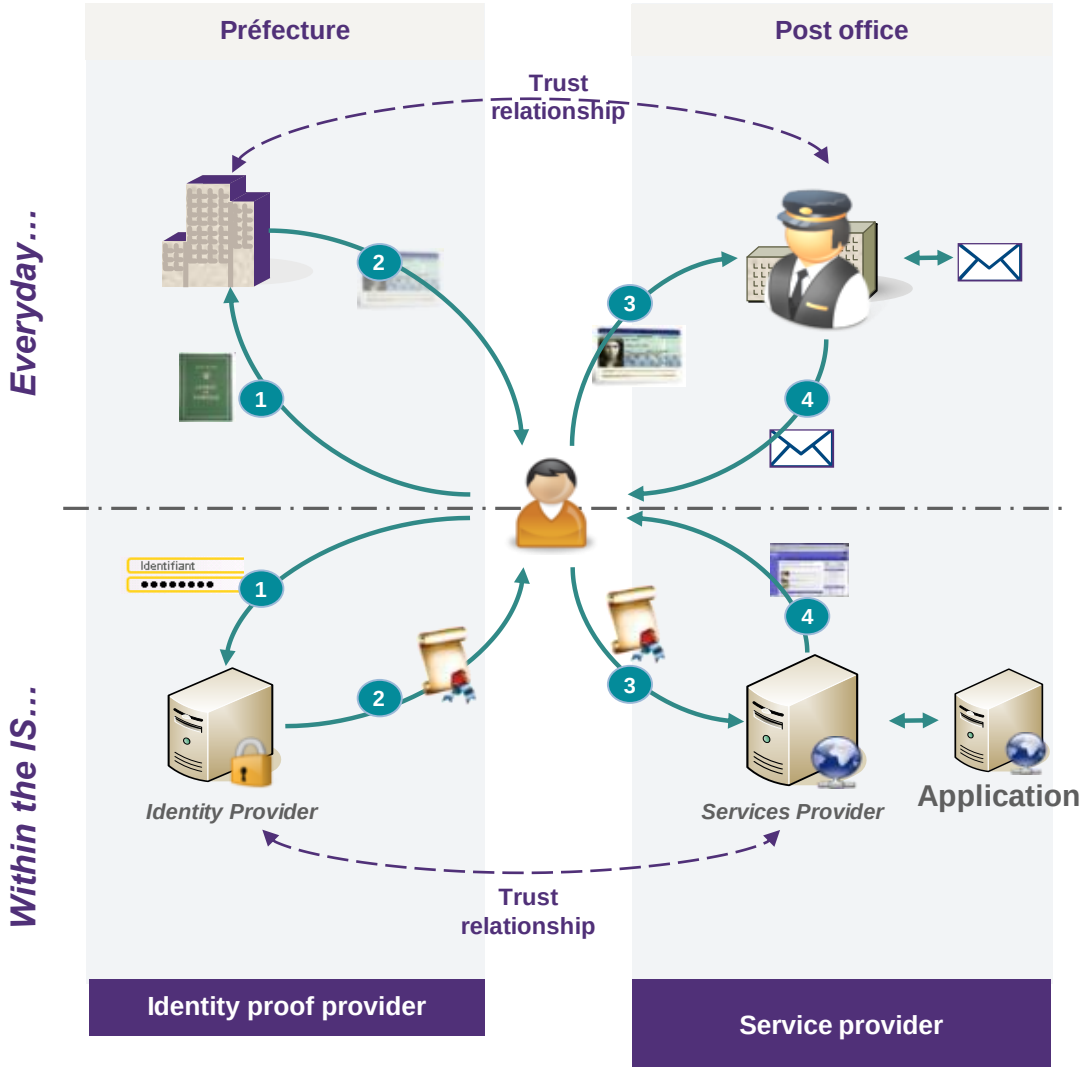


- Security level and ergonomics are not directly linked
- The solutions costs can greatly vary upon
  - The vendor…
  - The target population
- The authentication is not the only moment you can identify an end-user

Identity federation - principles



1. The end-user provides an authentication factor
2. The end-user receives a “federated” identity proof that can be used throughout the federation circle of trust
3. The end-user can request access to a service provider with that authentication proof
4. The Service Provider, who trusts the Identity Provider, checks the proof, authenticates and lets the user access to the application



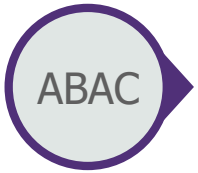
Authorization

Access Control List

- Access rights granted through a list of users and system processes.
- e.g.: "Employees Bob and Alice can open the door"

Role-Based Access Control

- Access rights granted to users through their role only.
- e.g.: "Anybody with the 'Employee' role can open the door"



Attribute-Based Access Control

- Access rights granted through the combination of attributes
- e.g.: "Only employees of the IT department can open the door if they are assigned to an active project"

Operation control… why?

Goal

Implement a **feedback loop** to **follow, analyze and fix** operations done in the IAM solution

Recertify end-users access rights

- *Periodic review of end-users rights*
- *Exception management (SoD, temporary rights)*

Comply to the rules and regulation

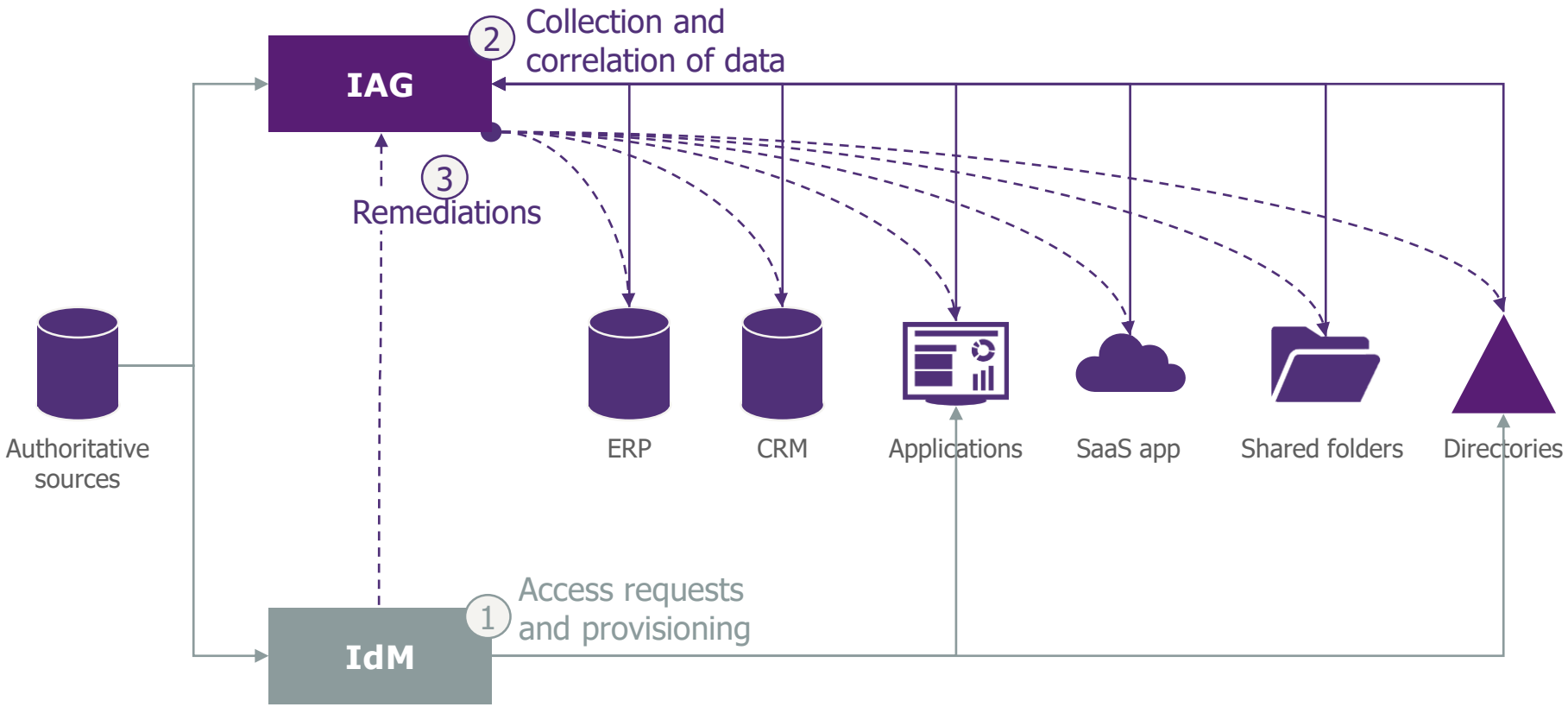
- *Laws and regulations*
- *Best practices and methodology*
- *Enterprise policies*

Control actual use

- *Accounts use*
- *Access rights use (qui a accès à quoi, à quel moment…)*
- *Detect sensitive situations with KPIs (nb of exceptions, nb of roles per user, nb of connection attempts, etc.)*

IDM and IAG are complementary

Combining both IdM and IAG features can help **answering end-users needs as well as ensuring the right control level**



Identity Management (IDM) and Identity & Access Governance (IAG)

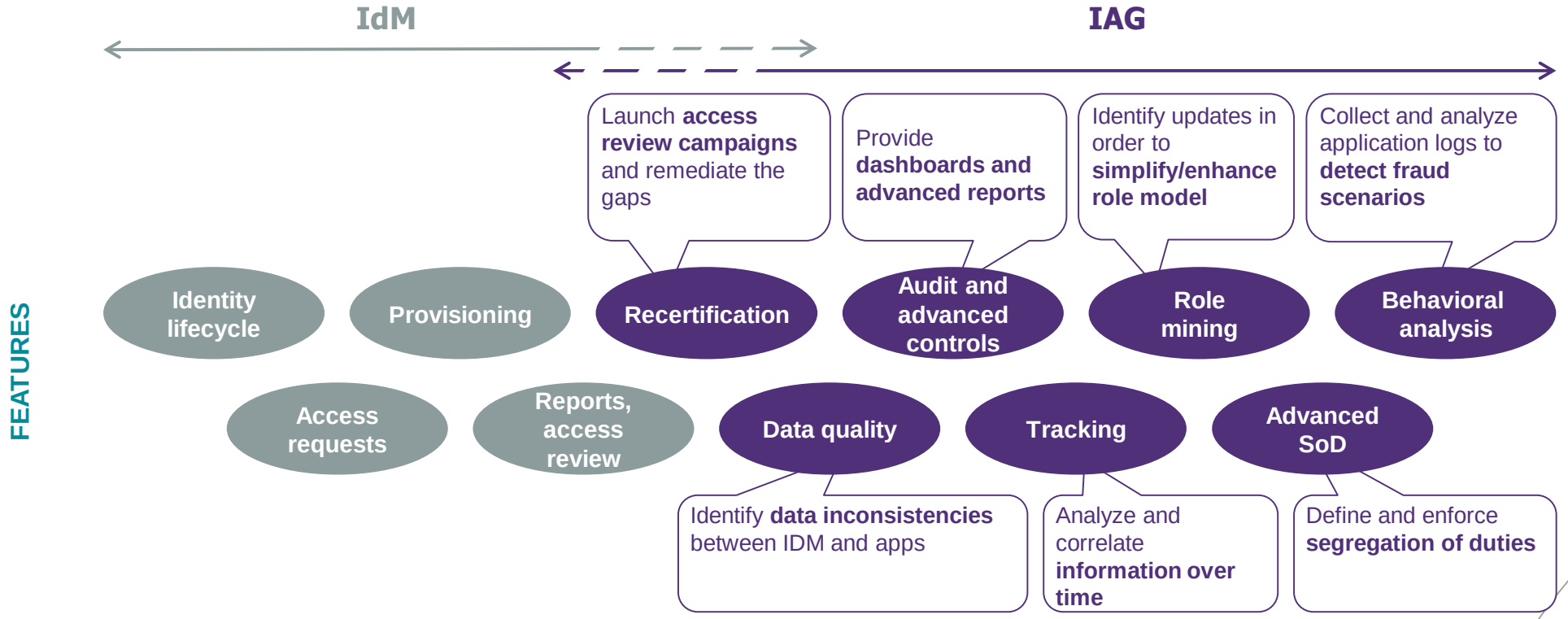
IdM & IAG are different in their approach. Today no solution on the market can correctly cover all functionalities

Identity Management

Focus on **operational management of requests**, with consolidated vision of rights, for a given application landscape

Identity & Access Governance

Focused on the collection, analysis and correlation of data, though a "datalake" and fine-grained accesses, for another given application landscape



What is the future of IAM?

Governance, review & identity federation

SSO and business processes

Automatization

Identity & Access Intelligence

IDaaS

Standards

APIs

Internet of Things

Customer IAM

Agility

Customer IAM

Customer IAM : the big principles

Know Your Customer

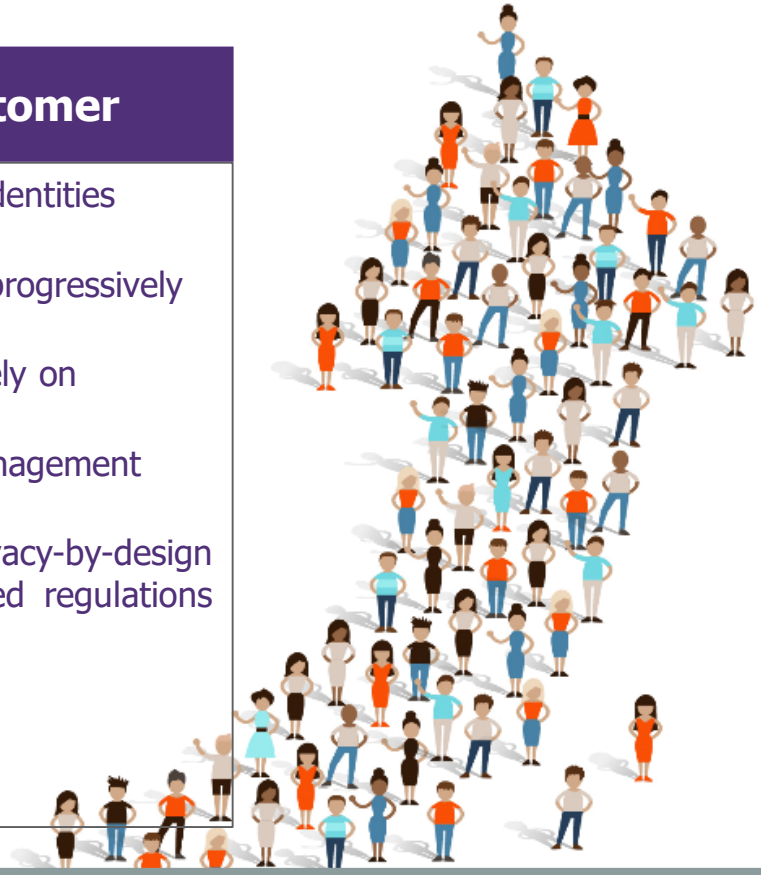
Manage a large number of identities

Collect identity information progressively

No authoritative source to rely on

Mostly self-care account management

A specific attention to a privacy-by-design approach (GDPR and related regulations now enforce this)



Ease the user experience

Do Social login

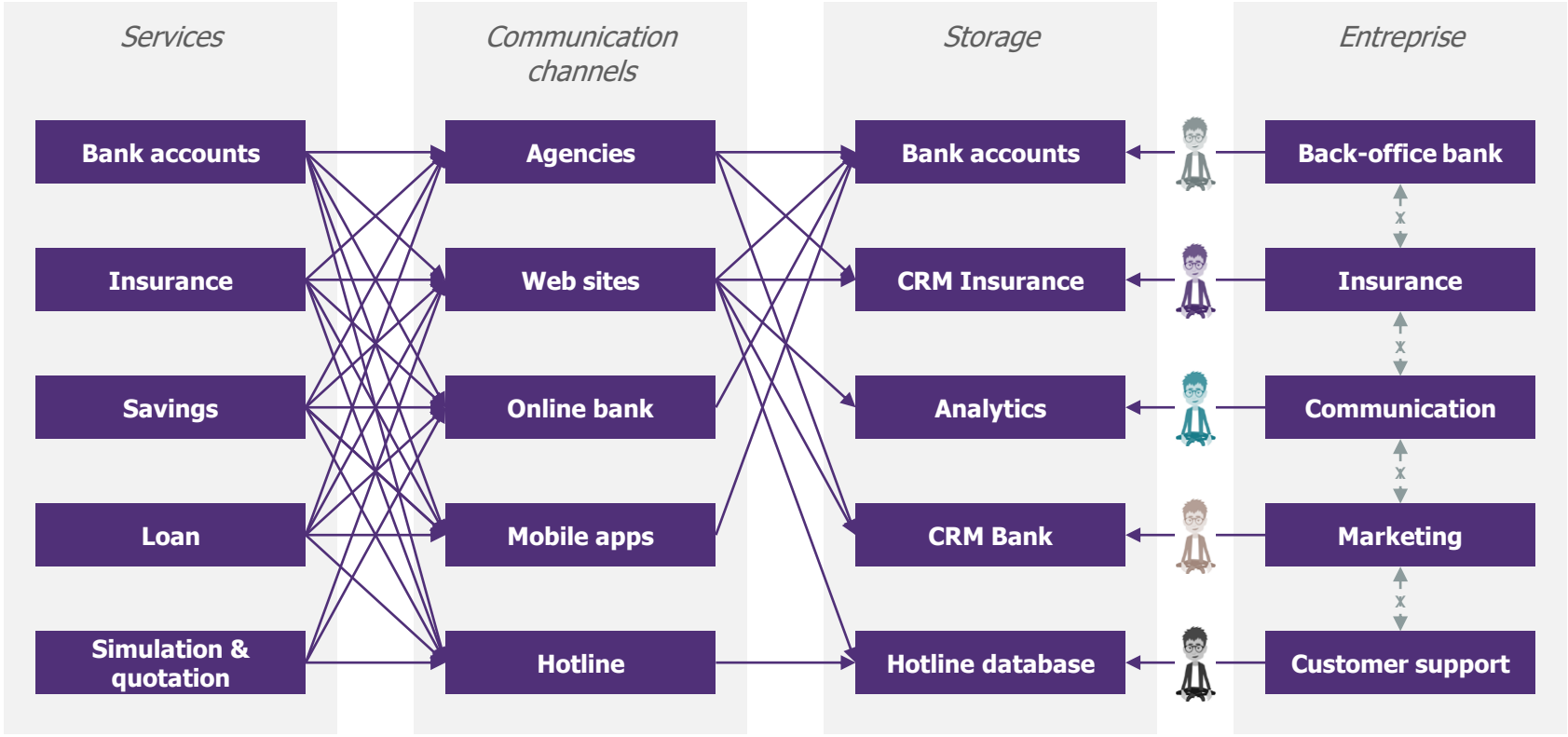
Make authentication an exception event

- Longer sessions, context scoring, behavior analytics
- Only re-authentication upon a sensitive operation (payment, contract change, etc.)
- Use an MFA solution with good ergonomics (Out-Of-band, U2F, etc.)

Towards a decentralized identity, under customer control

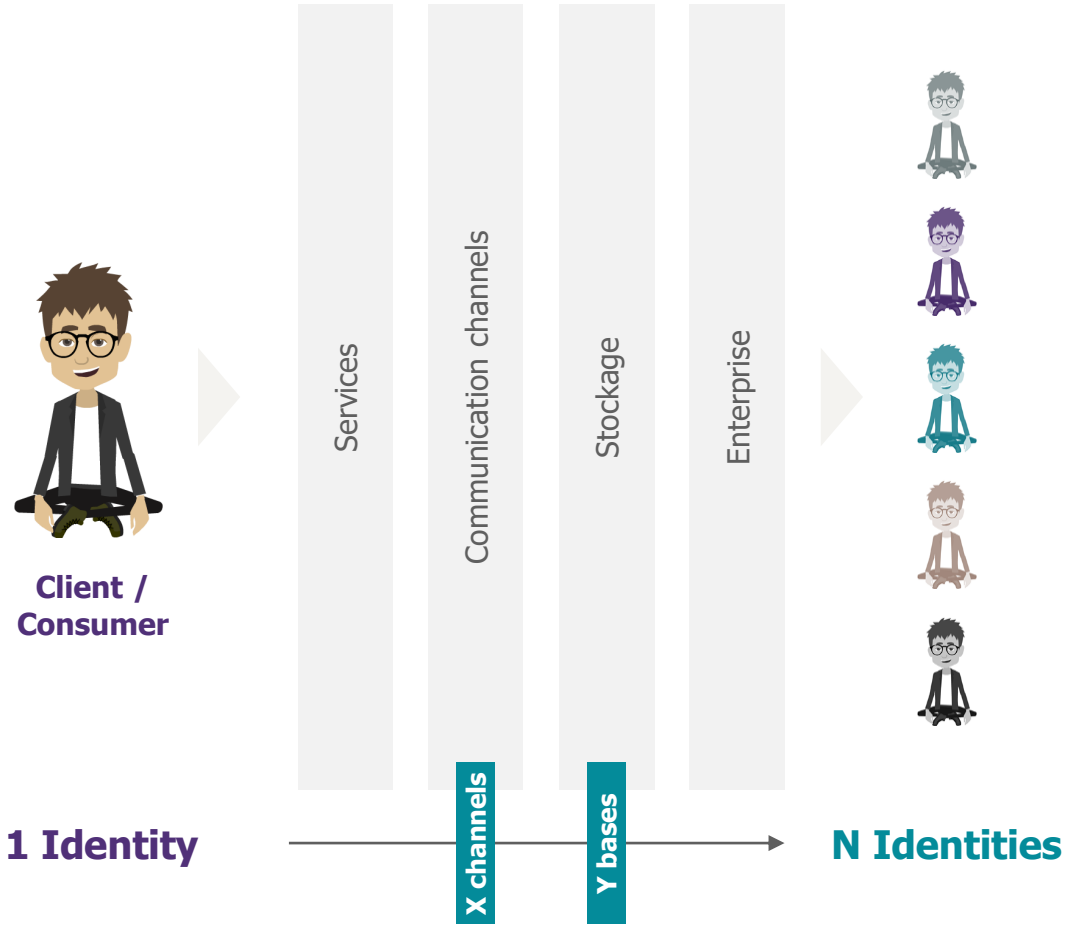
Why do we need to put a 'C' on IAM?

Client / Consumer



but also: IoT, Chatbot, social networks…

Why do we need to put a 'C' on IAM?



Poor user experience(UX)

Heavy registration processes, same information requested several times, wrong advertisements…

➔ **LOW CONVERSION RATE**

Difficulty to retain

Non reliable data, inability to define customer profiles, wrong marketing actions…

➔ **LOSS OF CUSTOMERS**

Data privacy / Regulations

Difficulties to be compliant with regulations (GDPR, PSD2) due to a lack of an aggregated view of the customers data & consents

➔ **LOSS OF TRUST**

The 4 Main Challenges of CIAM

IMPROVE
USER EXPERIENCE

Simple registration, self-service, easy authentication, cross channel experience…

BE COMPLIANT
WITH REGULATIONS

GDPR, DSP2… with the help of a 360° view of the user and by offering to him a simple interface to manage its data

SECURE
NEW DIGITAL SERVICES

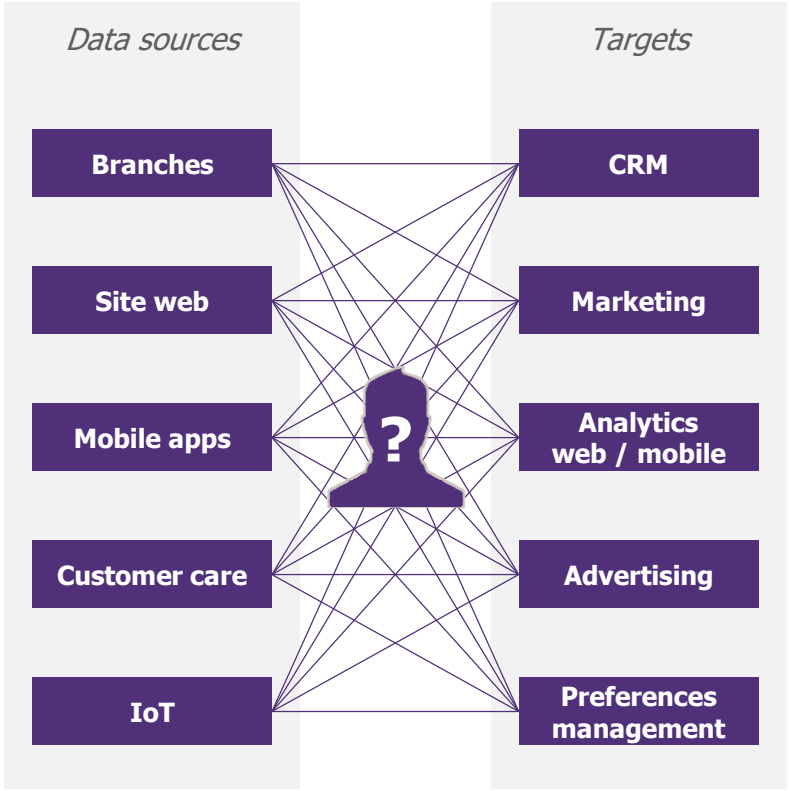
Smartphone, IoT, sensitive operations (enrolment, payment…)

CONVERT
PROSPECTS TO CLIENTS

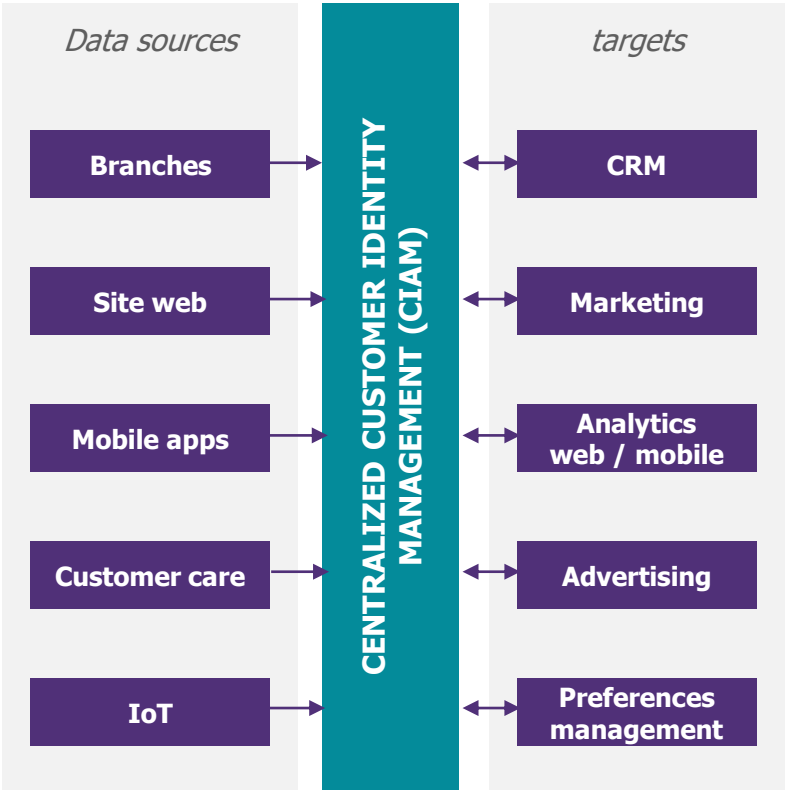
With simple authentication & registration services, relevant communication & services

What about the practice?

From Spiderman



… towards a centralized model



IAM B2C vs IAM B2B

	ENTREPRISE IAM	CUSTOMER IAM
TARGET	**ENTERPRISE** *Employee, contractors, partners…*	**CUSTOMERS**
VOLUME	**THOUSANDS** IDENTITIES	**MILLIONS** IDENTITIES
SCALABILITY	**HIGH** *Security concerns, lower impact on business in case of unavailability*	**CRITICAL** *Issues of image, user experience, direct earning losses*
DATA SOURCE	**HR OR IT** *Static identity management (users are already known from the company)*	**END USER / CRM** *Dynamic identity management based on customer's preferences*
AUTHORIZATION	**VALIDATION** *Role-based, approval workflows…*	**AUTOMATIC** *Attribute-based (services, contracts…)*
CHANNELS	**WEB, ~MOBILE** *Controlled access points*	**WEB, MOBILE, IoT, SOCIAL** *Non controlled access points*
APPROACH	**SECURITY** *Mostly led by IT*	**SECURITY & DIGITAL** *Led by business & IT*

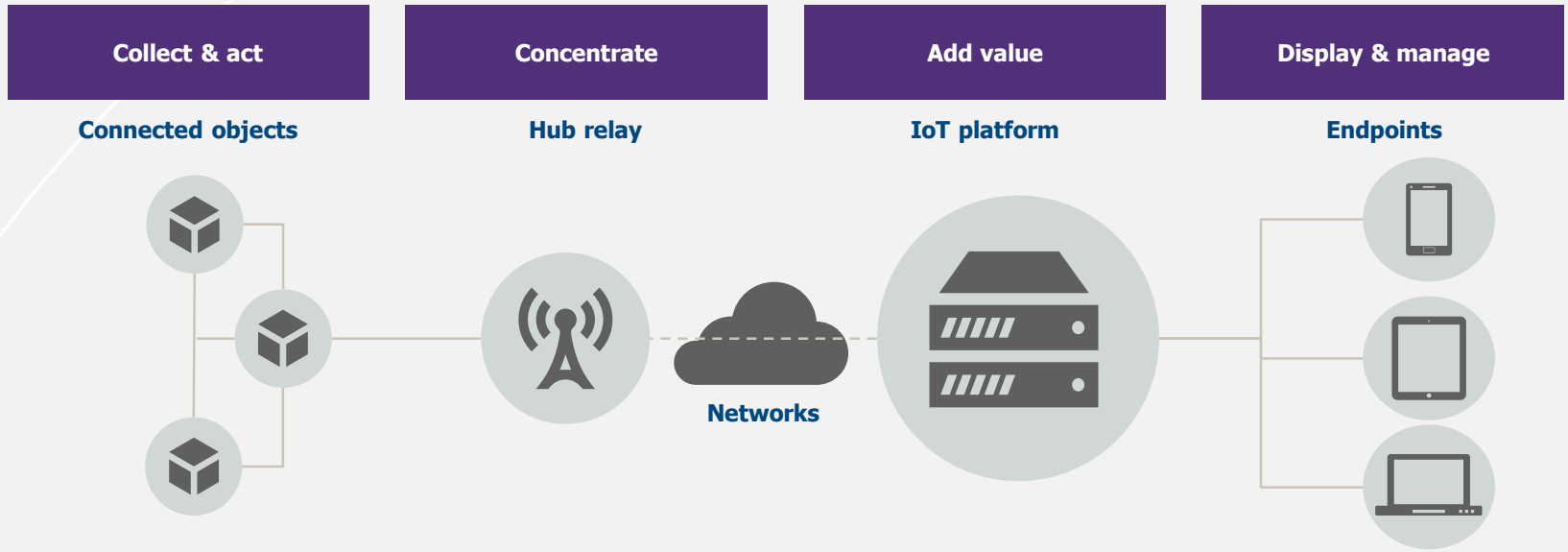
WAVESTONE

Karim BELLOUARAK
Senior Consultant

M +33 (0)7 60 11 43 26
karim.bellouarak@wavestone.com

Internet of Things

Security stakes to address over the entire technological chain



- In « hostile environment »
- Constraints in :
  - Computing power
  - Storage
  - Energy
- Compromise between costs and security

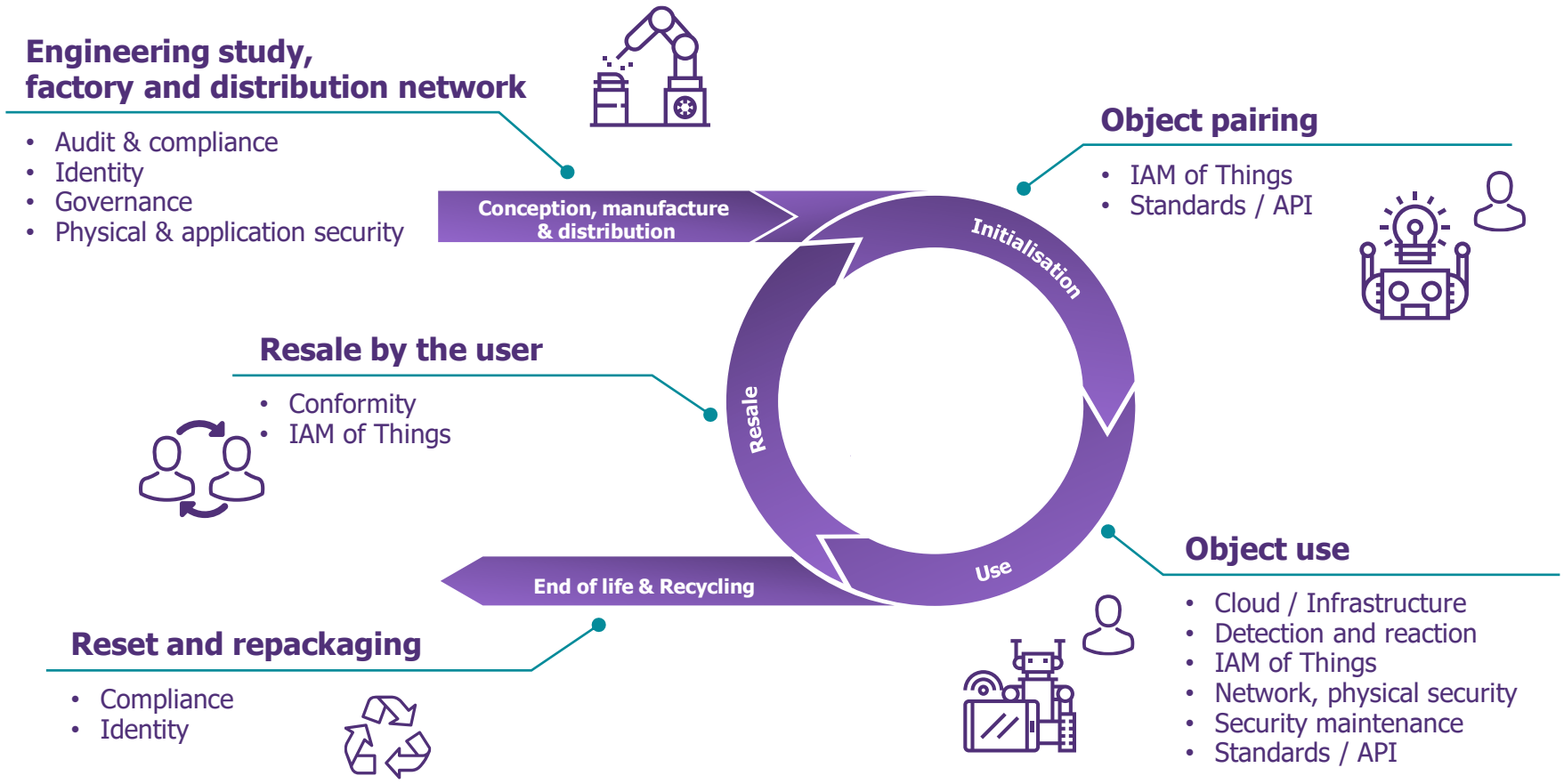
- First trusted component?
- Object protocol gateway <-> platform
- Securing before sending on the network

- Infrastructure access protection
- Legislation compliance on data protection
- Behavioural deviation detection
- Services levels and operational security

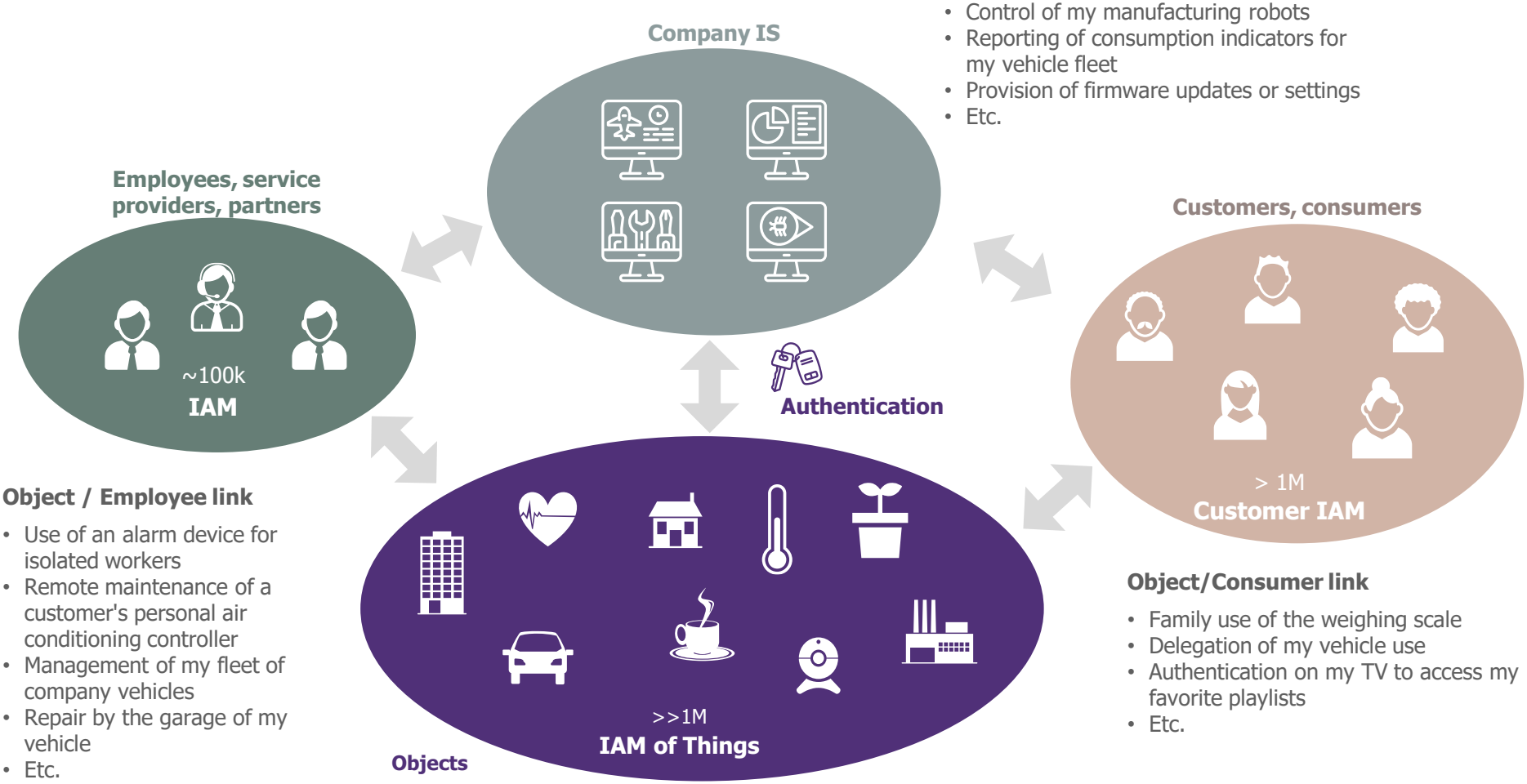
- Data access protection :
  - Authentication
  - Authorisation
- Lifecycle management of the objects

Main security principles to be adapted to many constraints: environment, cost, performance, volume of data… **for specific answers to the context**.

A project approach to be structured according to **the life cycle of the object** to **address all the security topics**



What is the IAM of Things (#IAMoT)?



Object / Company IS link

- Control of my manufacturing robots
- Reporting of consumption indicators for my vehicle fleet
- Provision of firmware updates or settings
- Etc.

Object / Employee link

- Use of an alarm device for isolated workers
- Remote maintenance of a customer's personal air conditioning controller
- Management of my fleet of company vehicles
- Repair by the garage of my vehicle
- Etc.

Object/Consumer link

- Family use of the weighing scale
- Delegation of my vehicle use
- Authentication on my TV to access my favorite playlists
- Etc.

THE RECIPE FOR IAM OF THINGS

#IAMoT

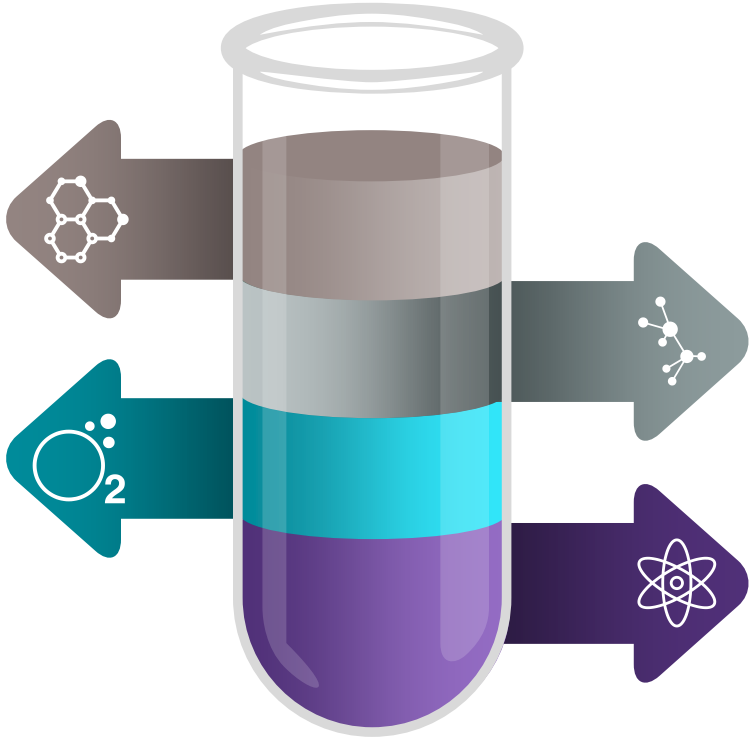
Processes

Pairing, modification or deletion of rights to managed objects, customers, employees, partners, …

CIAM access rights model

Owner, main user, delegate, …

- What interactions with which objects?
- What permissions on data?



IAM access rights model

Fleet manager, maintainer, employee, …

- What interactions with which objects?
- What permissions on data?

Identity of objects and access control

Every object requires accesses to the IS of the company

- Which are my objects?
- How do they authenticate?

Identity as a Service

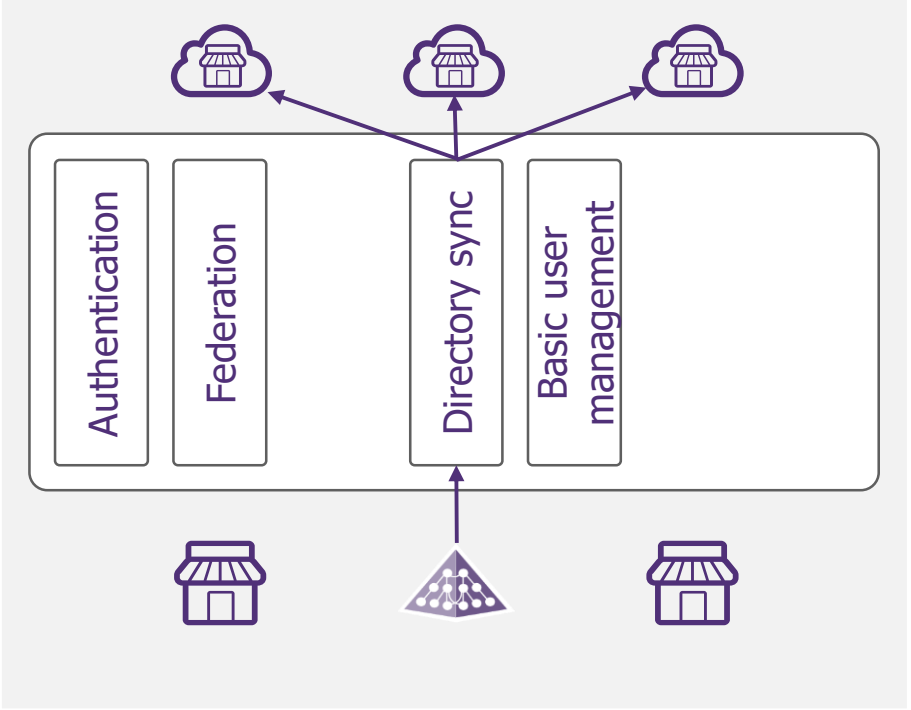
Identity as a Service : the current state

" Lots of marketing; features are still limited "

Cloud applications

Identity as a Service

On-premise applications



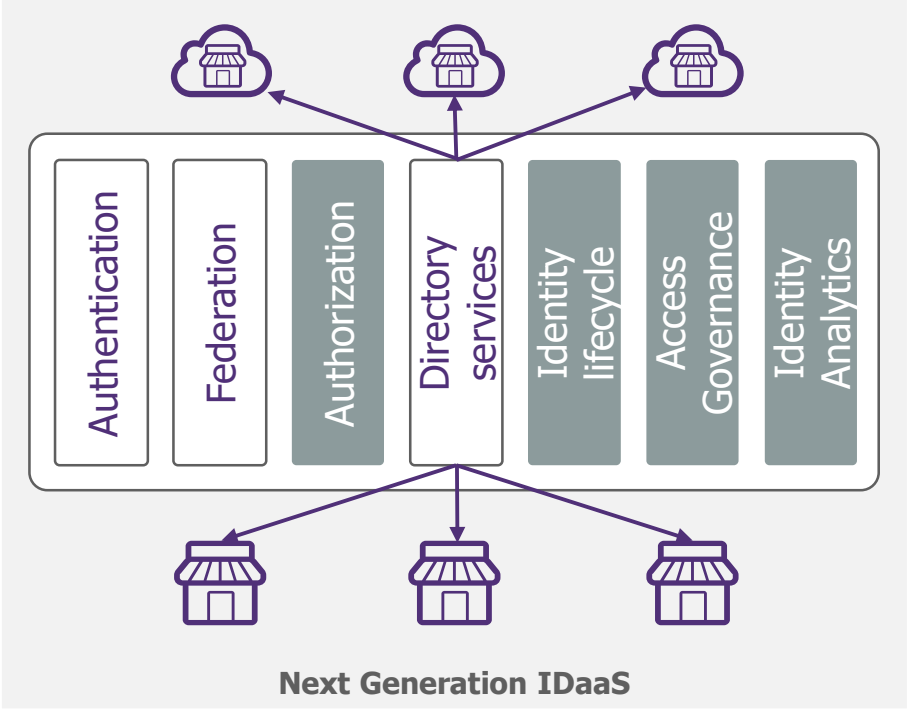
No fine-grained access rights management

Few or no identity management and access rights features

No *on-premises* provisionning

Identity as a Service : Next Generation IDaaS

" A consolidating market; offers will come with richer features "



Next Generation IDaaS

Frequent and transparent update of the solution

New features can be deployed continuously

Makes following best practices and standards more compelling

Tomorrow's IAM : a balance between business and technologies

3 new
business needs
to take into account

IoT

Customer IAM

Agilité

IDaaS

**Identity &
Access Intelligence**

Standards

APIs

4 technologies
to master

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

* Partenaires stratégiques

WAVESTONE