European Commission | Horizon 2020 European Union funding for Research & Innovation

Grant Agreement No 688156

symbIoTe

H2020 symbIoTe project

Security in federated IoT Environment

Mikołaj Dobski, PSNC

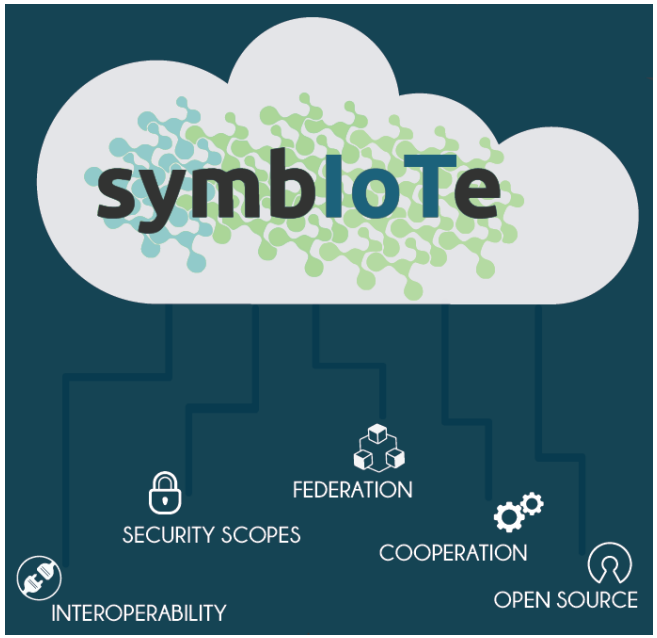
Euro-CASE 2017, Poznań

Agenda

- symbIoTe project overview
  - Interoperability goals & software architecture
  - Security layer(s)
- CDD & symbIoTe's AD
- Data streams mining
  - Constraints
  - Concept drift & its detectors

symbIoTe Overview

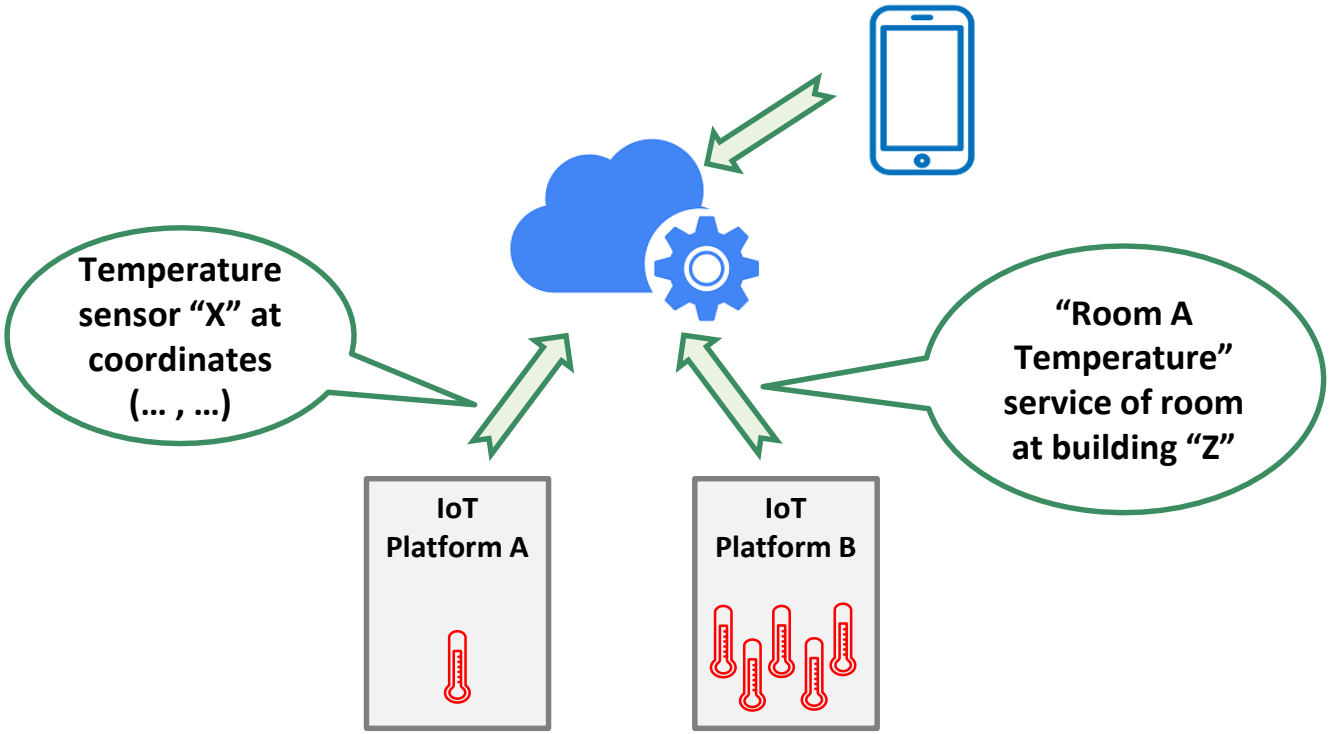
- Architecture: general overview
- Interoperability aspects
- Level 1-4 components
- Auth(n/z) approaches



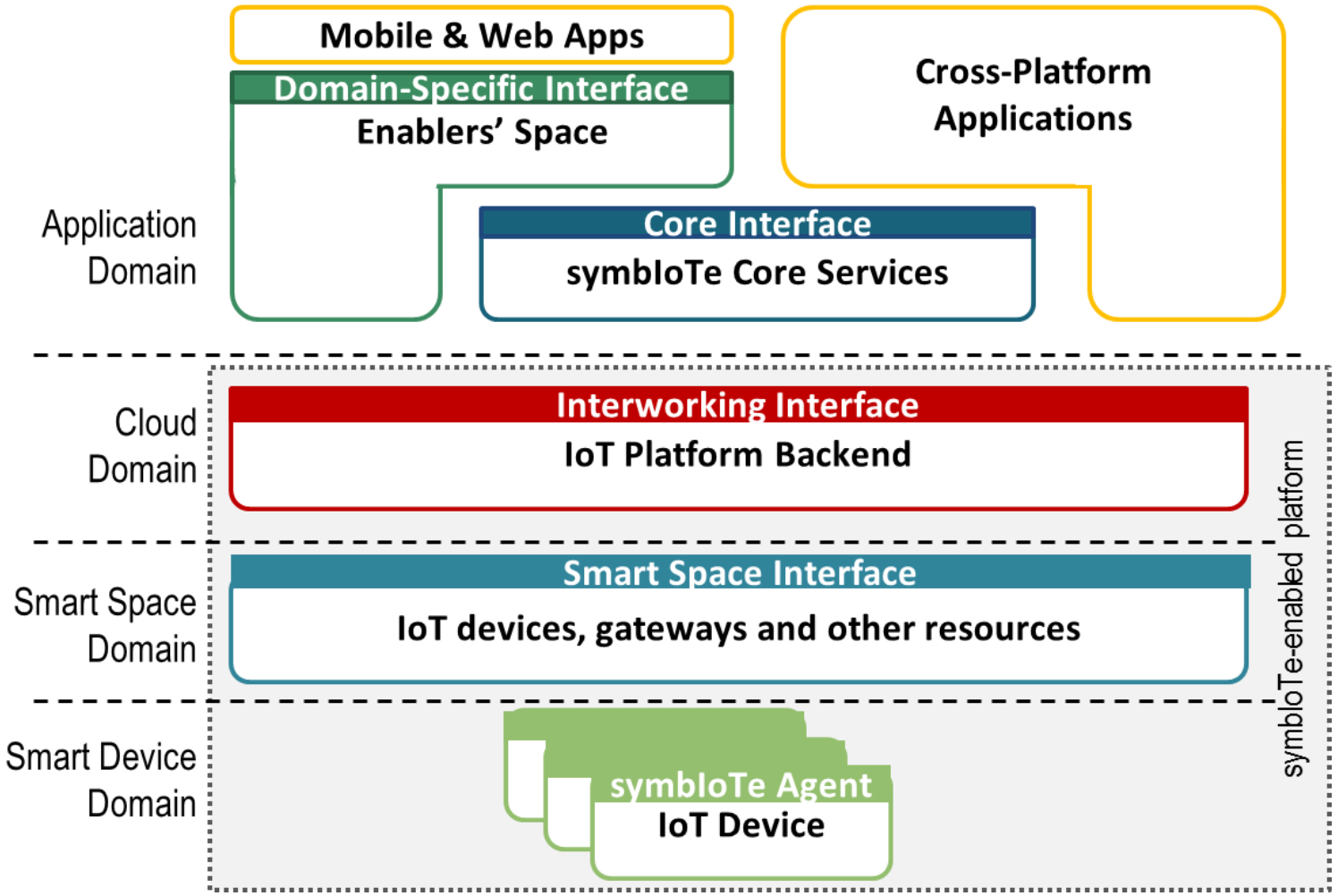
A simple interoperable IoT app

- Universal light switch on your mobile phone
  - … switch on/off the lights wherever you go (at home, in the office, in public spaces…)
  - … but of course, only if you are allowed to do so…

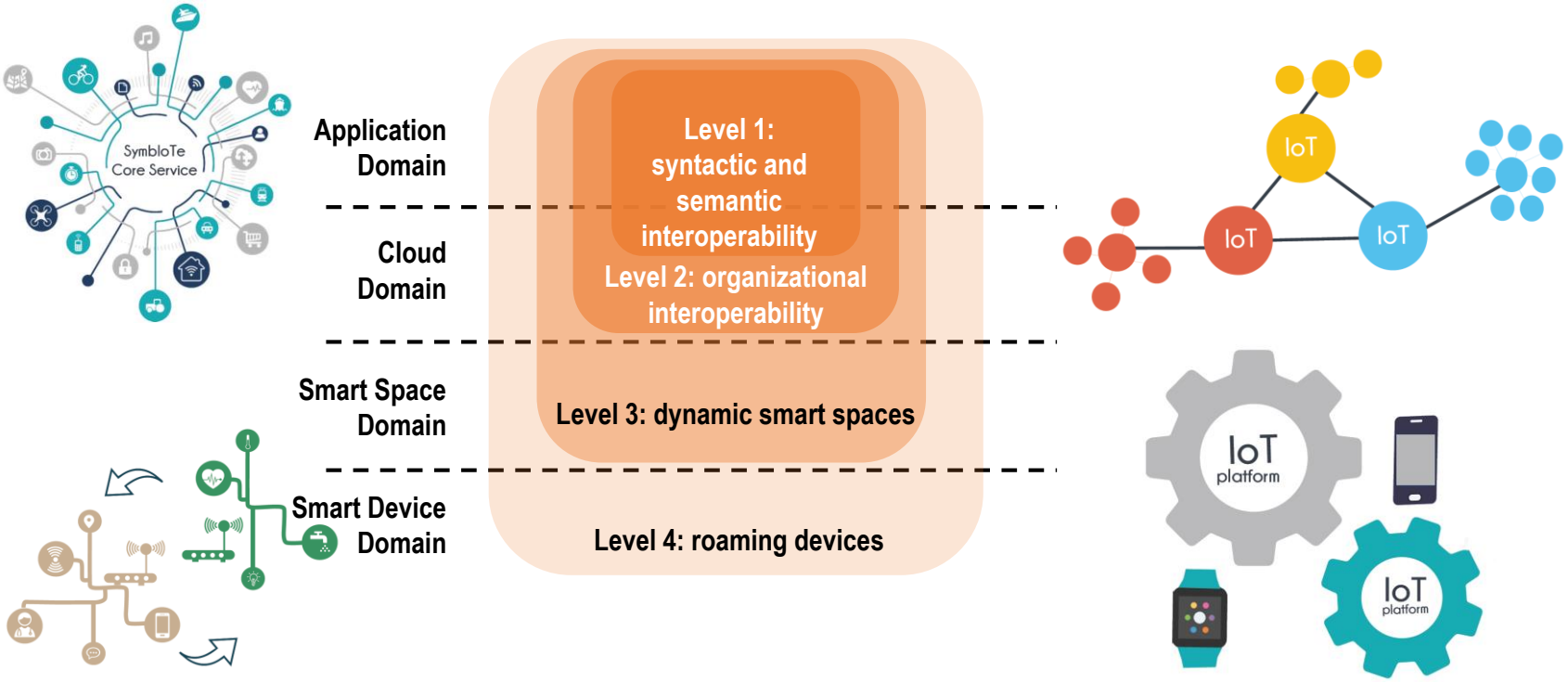
Platforms monetizing their resources



High-level architecture



Interoperability Aspects



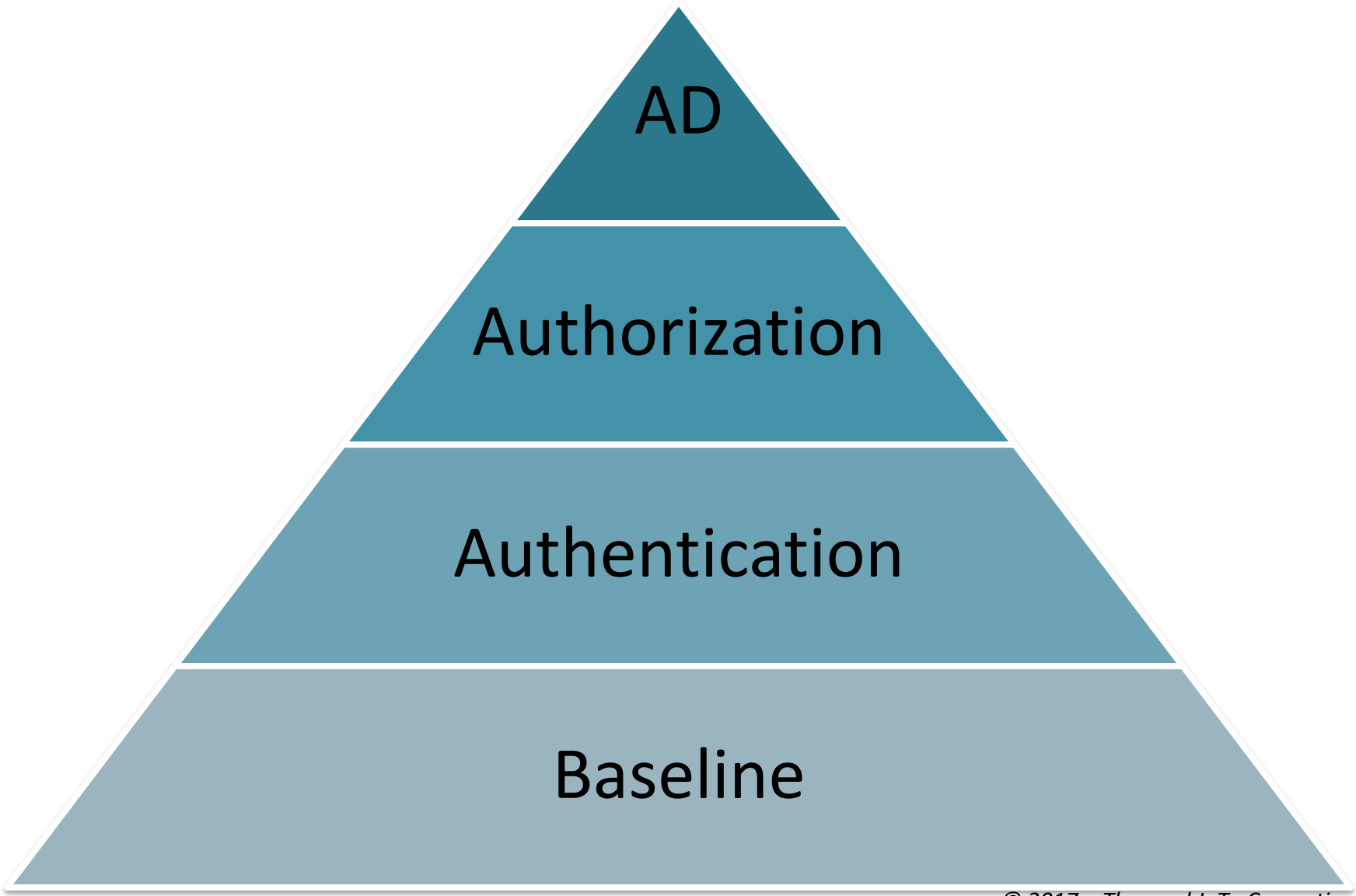
SECURITY IN SYMBIOTE

Challenges and solutions

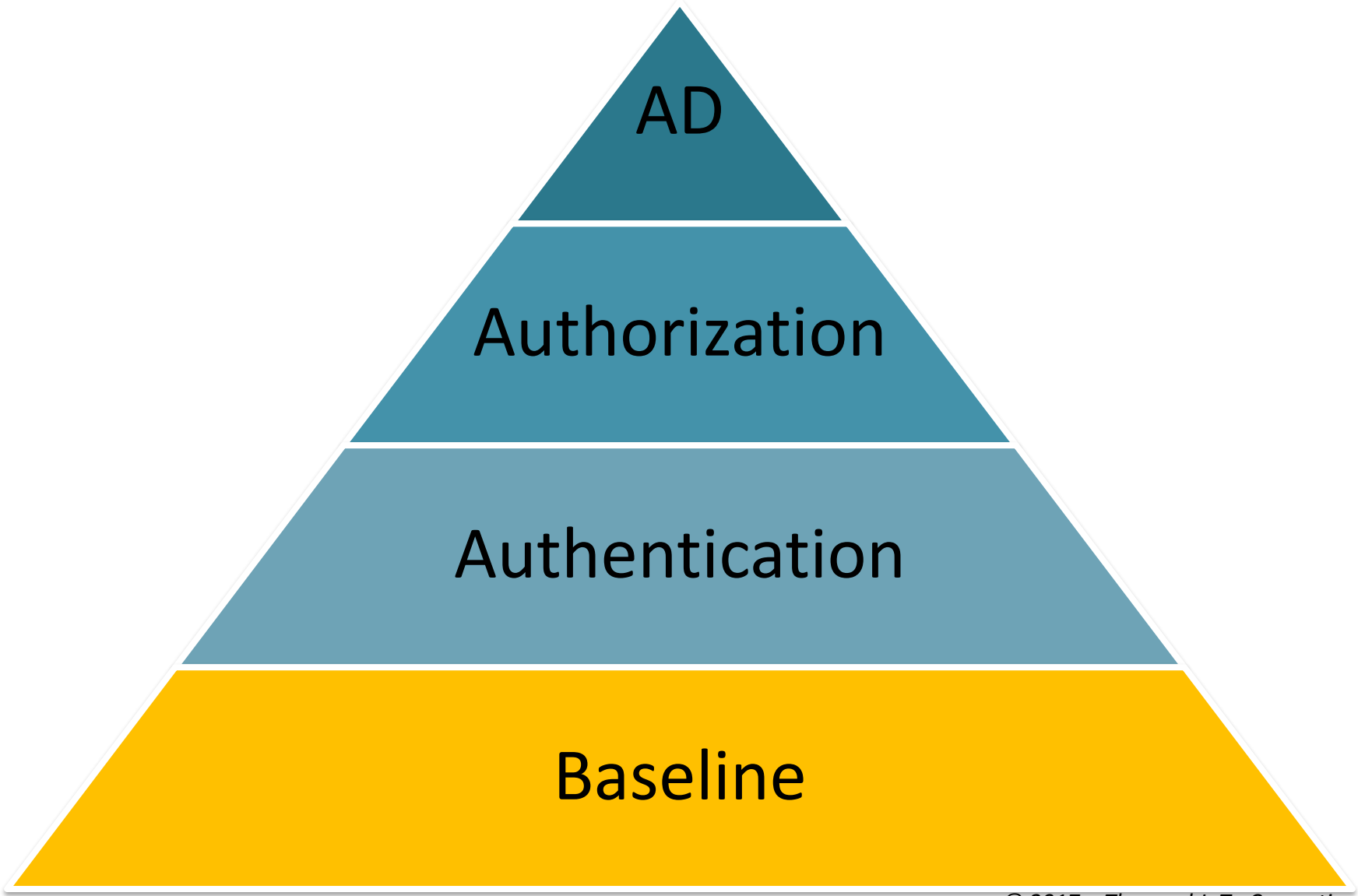
Main goal and approach

- Target goal: **multi-domain access right composition**
- Users registered in one or more platforms are authorized to access resources exposed elsewhere

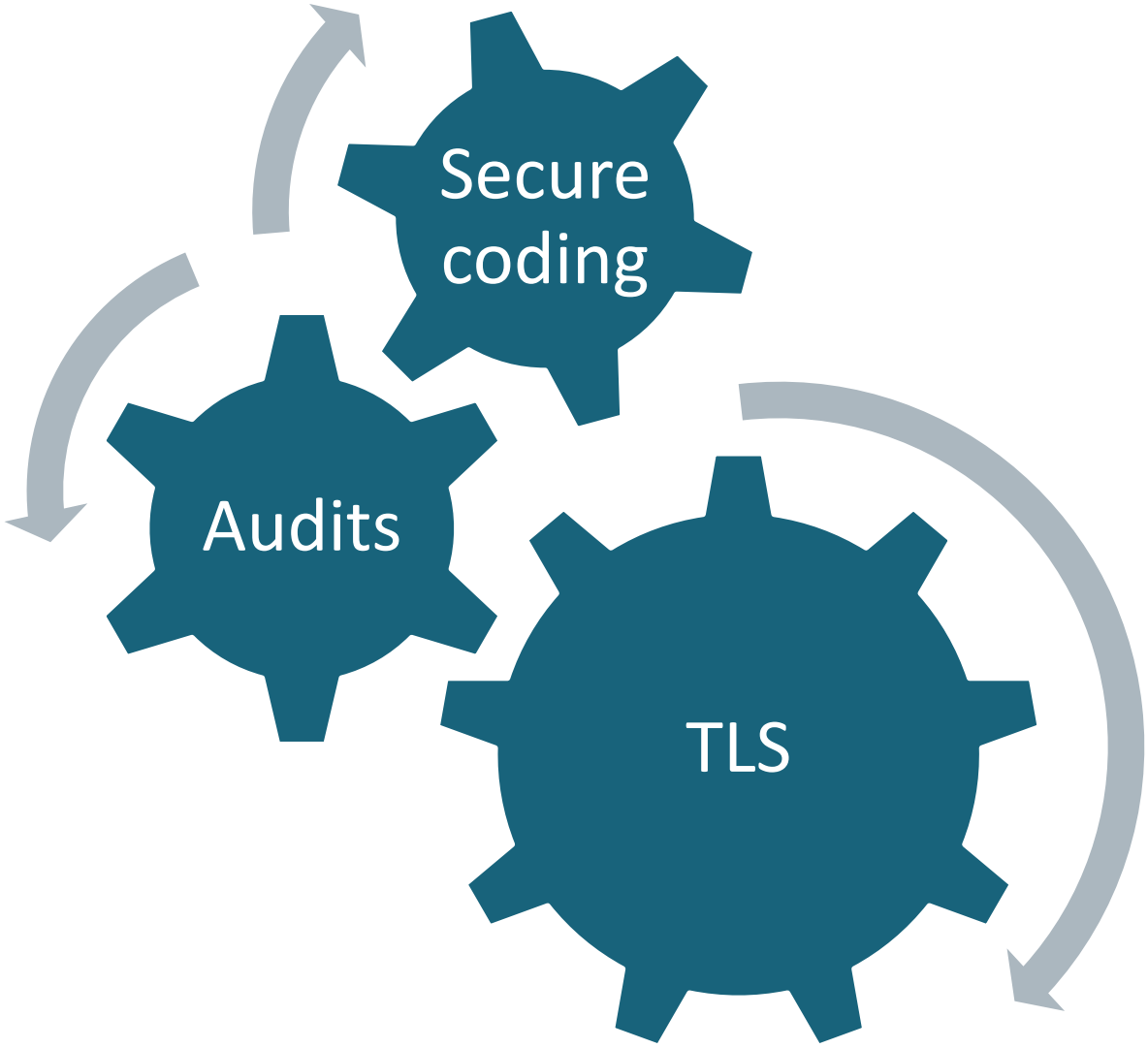
Layers (0)



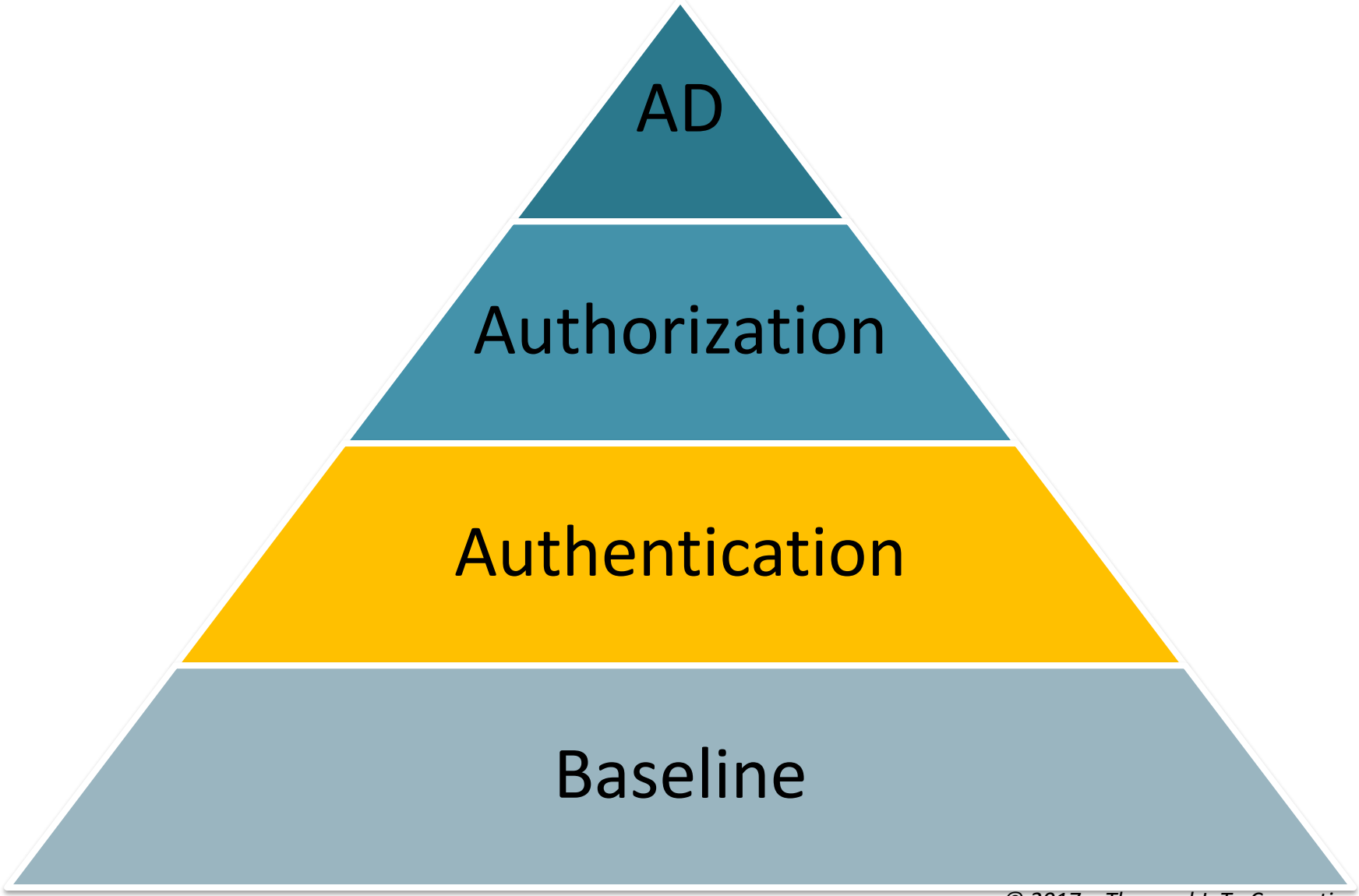
Layers (1)



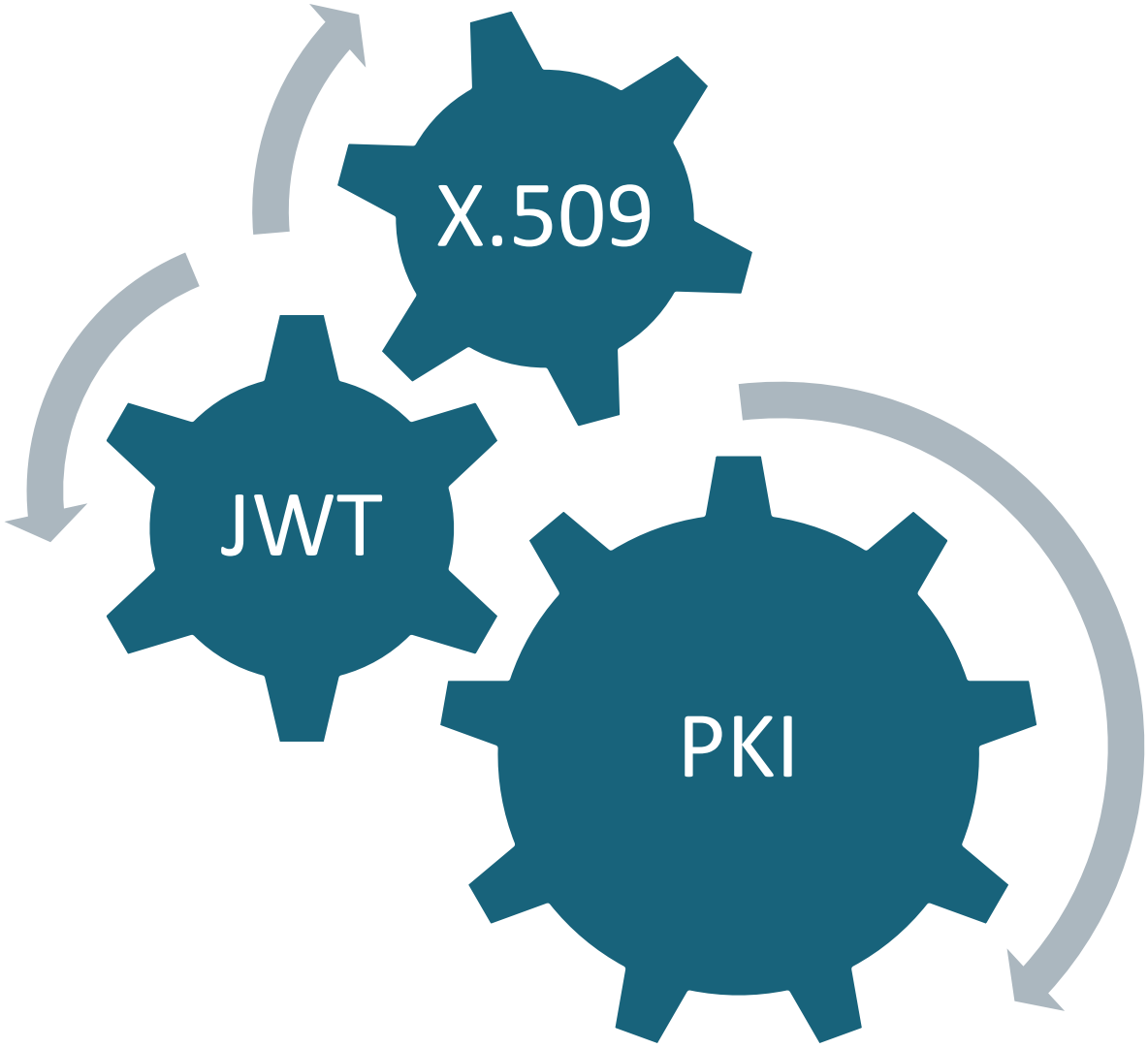
Baseline security



Layers (2)



Authentication layer

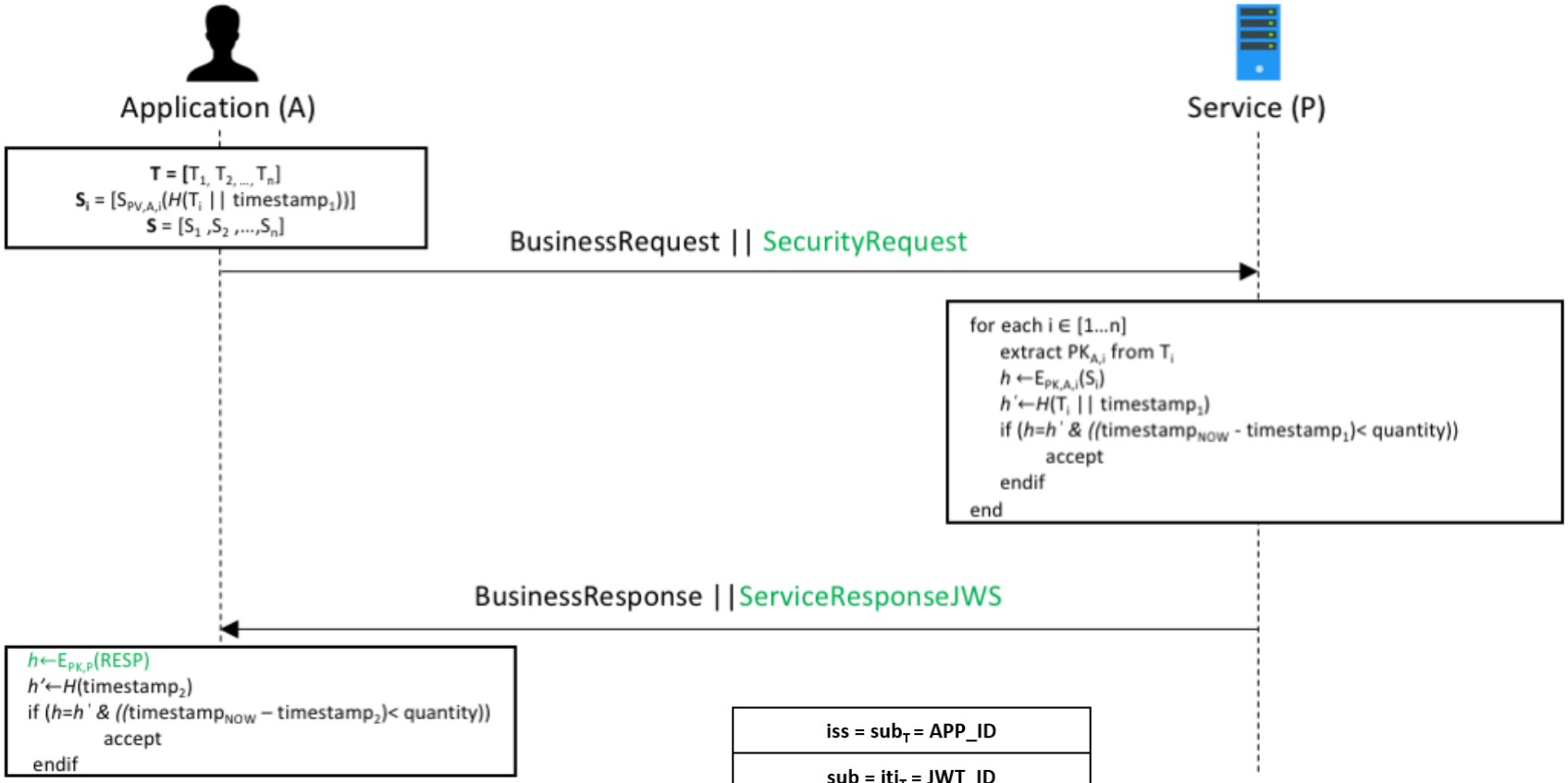


JSON Web Tokens

- Well-known structure used for storing user's attributes
- New claims added by symbIoTe
- Three kinds of tokens
  - Authorization JWS: home, foreign, guest
  - Home Token Acquisition JWS
  - Client Authentication JWS

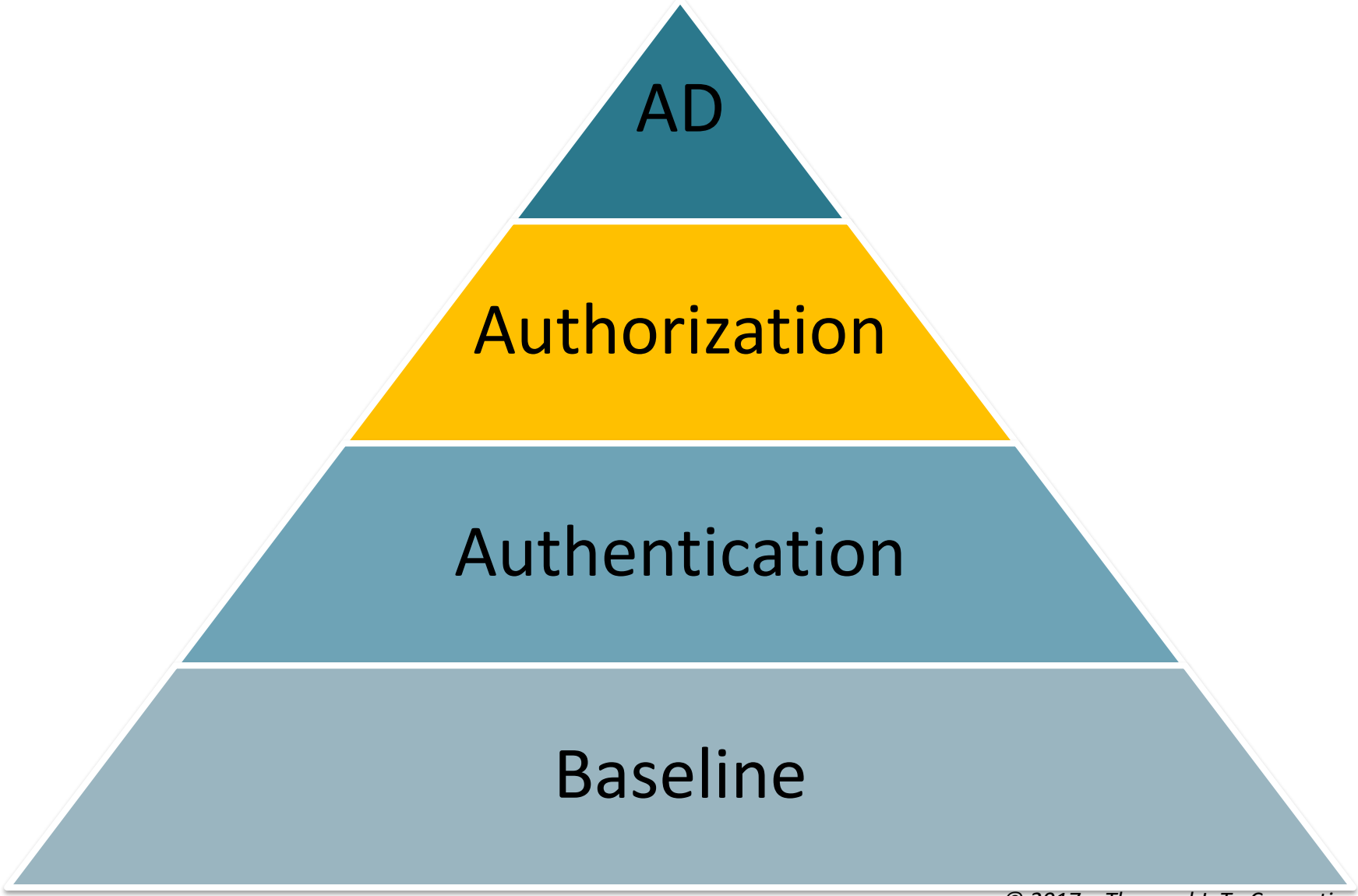
alg = $ECDSA_{256}$
iss = ACTOR_ID
sub = CLIENT_ID
iat = ISSUE_DATE
exp = EXPIRATION_DATE
sign = SIGN-ECDSA256(H(T_U), A_PRIVATE_KEY)

Auth(N) with challenge-response



iss = sub$_T$ = APP_ID
sub = jti$_T$ = JWT_ID
ipk = spk$_T$ = APP_PUBLIC_KEY
hash = hashed(TOKEN+TIMESTAMP)
iat = ISSUE_DATE
exp = EXPIRATION_DATE
sign = SIGN-ECDSA$_{256}$(H(T$_U$), APP_PRIVATE_KEY)

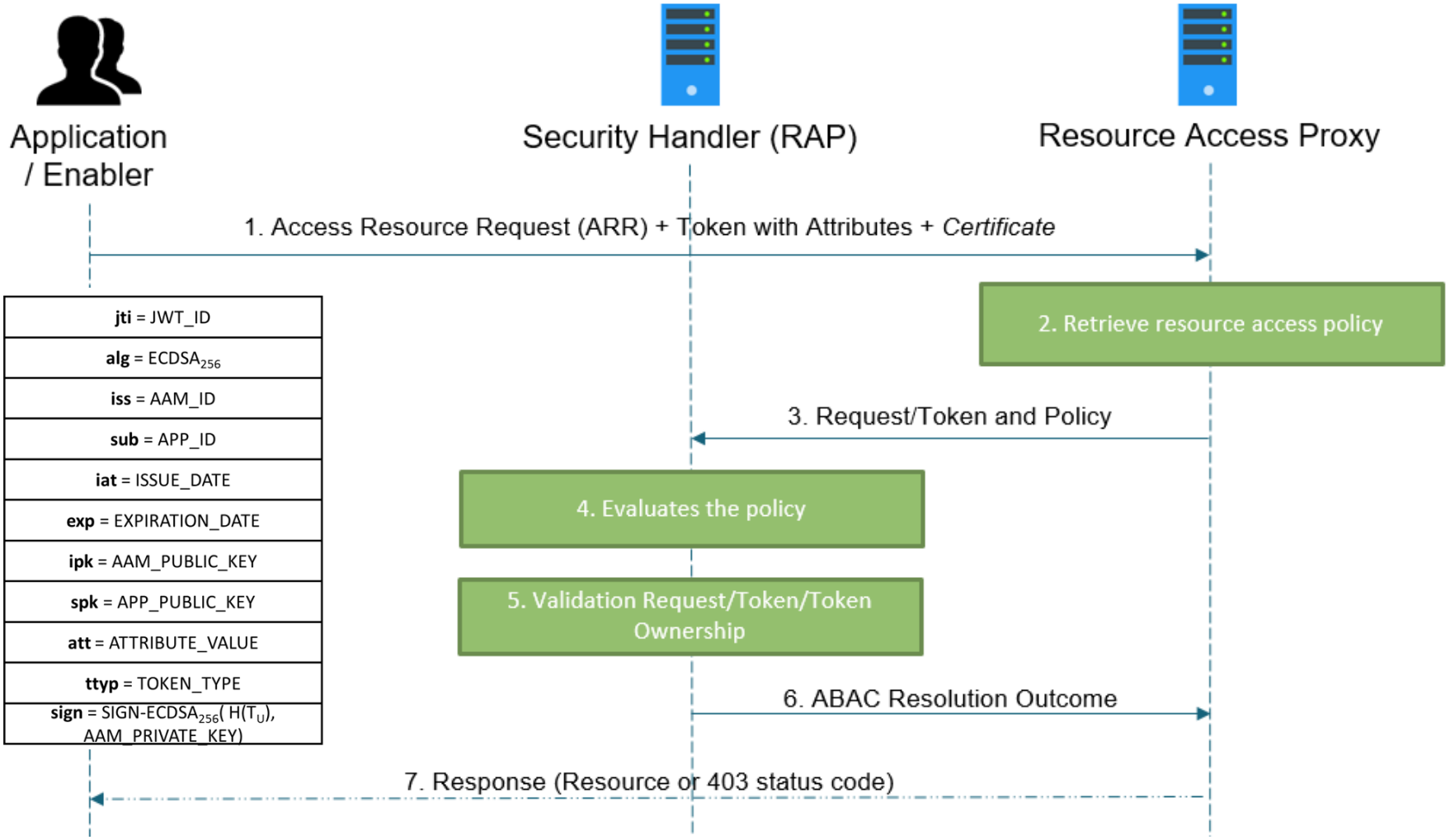
Layers (3)



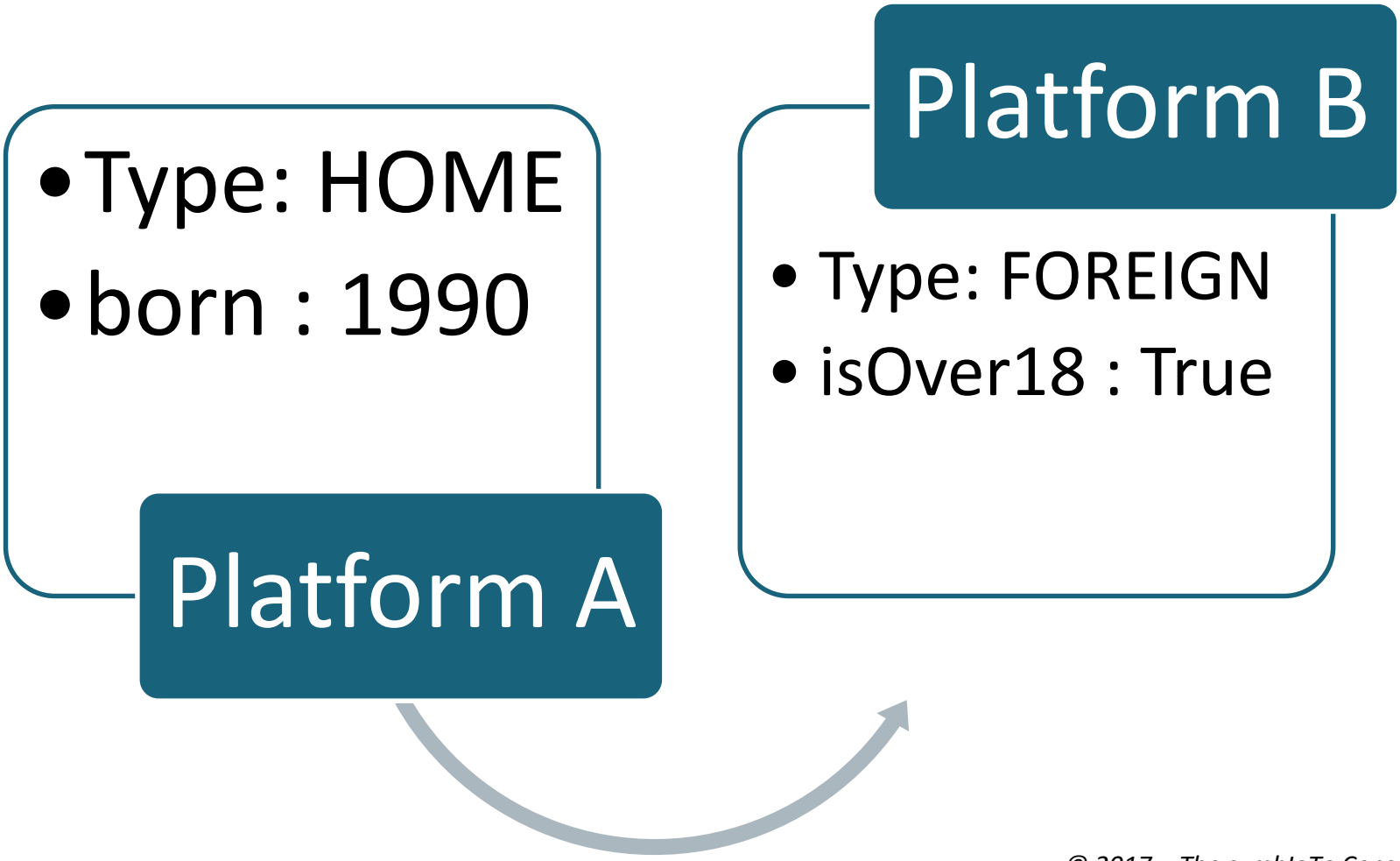
Authorization layer

- Resources protected through the **Attribute-Based Access Control (ABAC)** paradigm
- User's attributes stored in trusted data structures, i.e., **JSON Web Tokens (JWT)**
- **Access Policies** assigned to each resource
- User's attributes processable through a **Mapping Function**

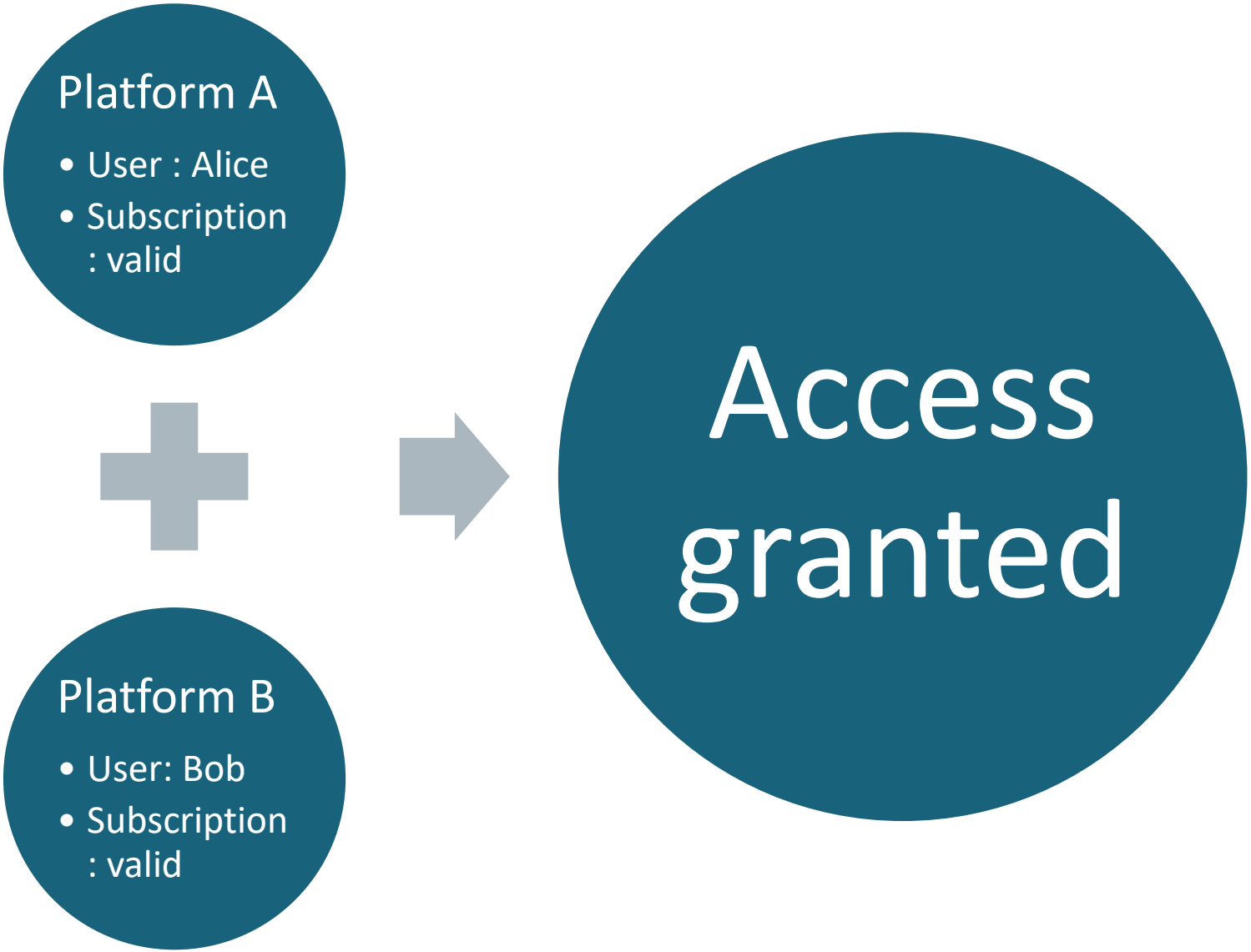
Auth(Z) with ABAC policies



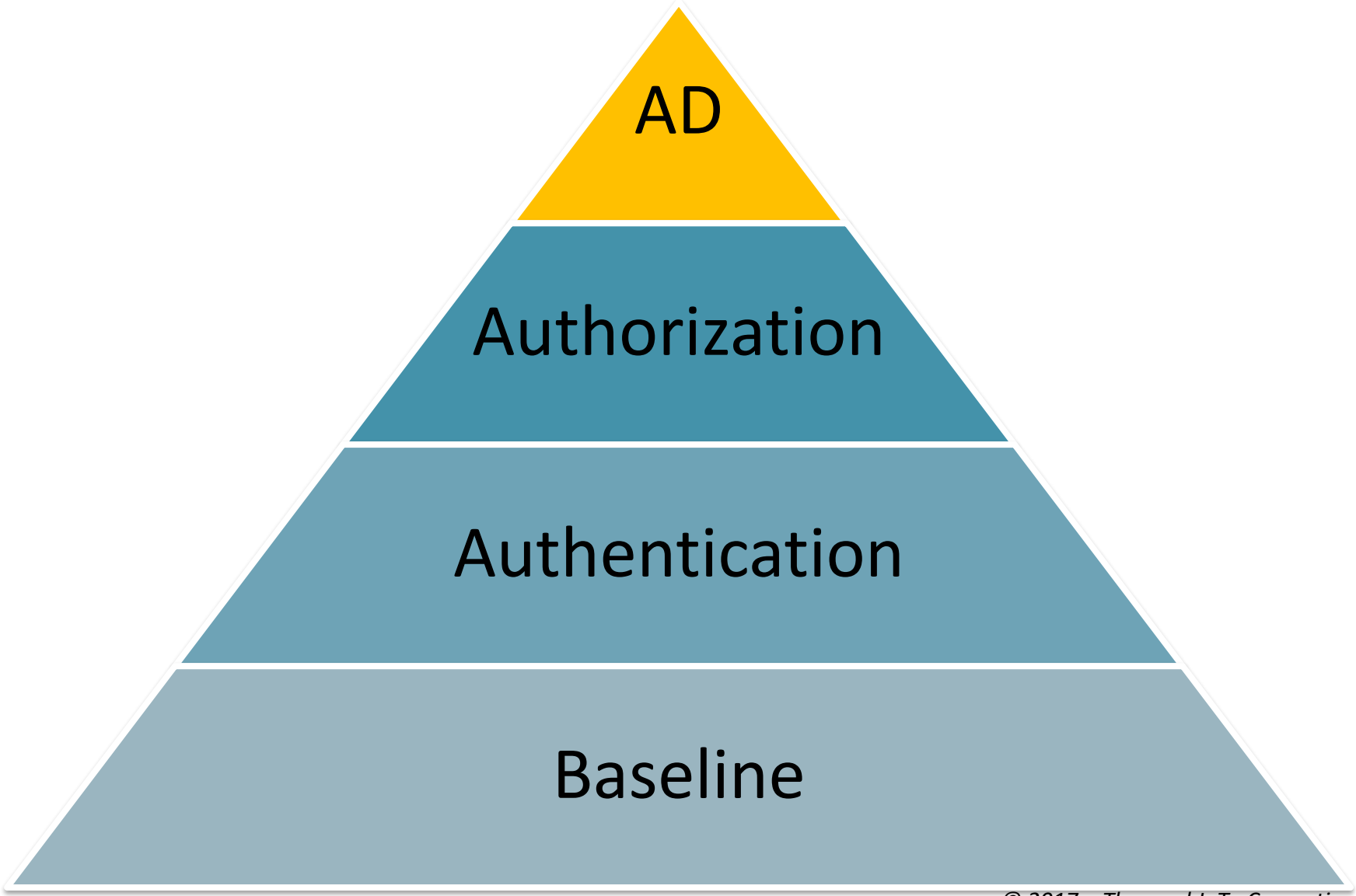
Attributes Mapping



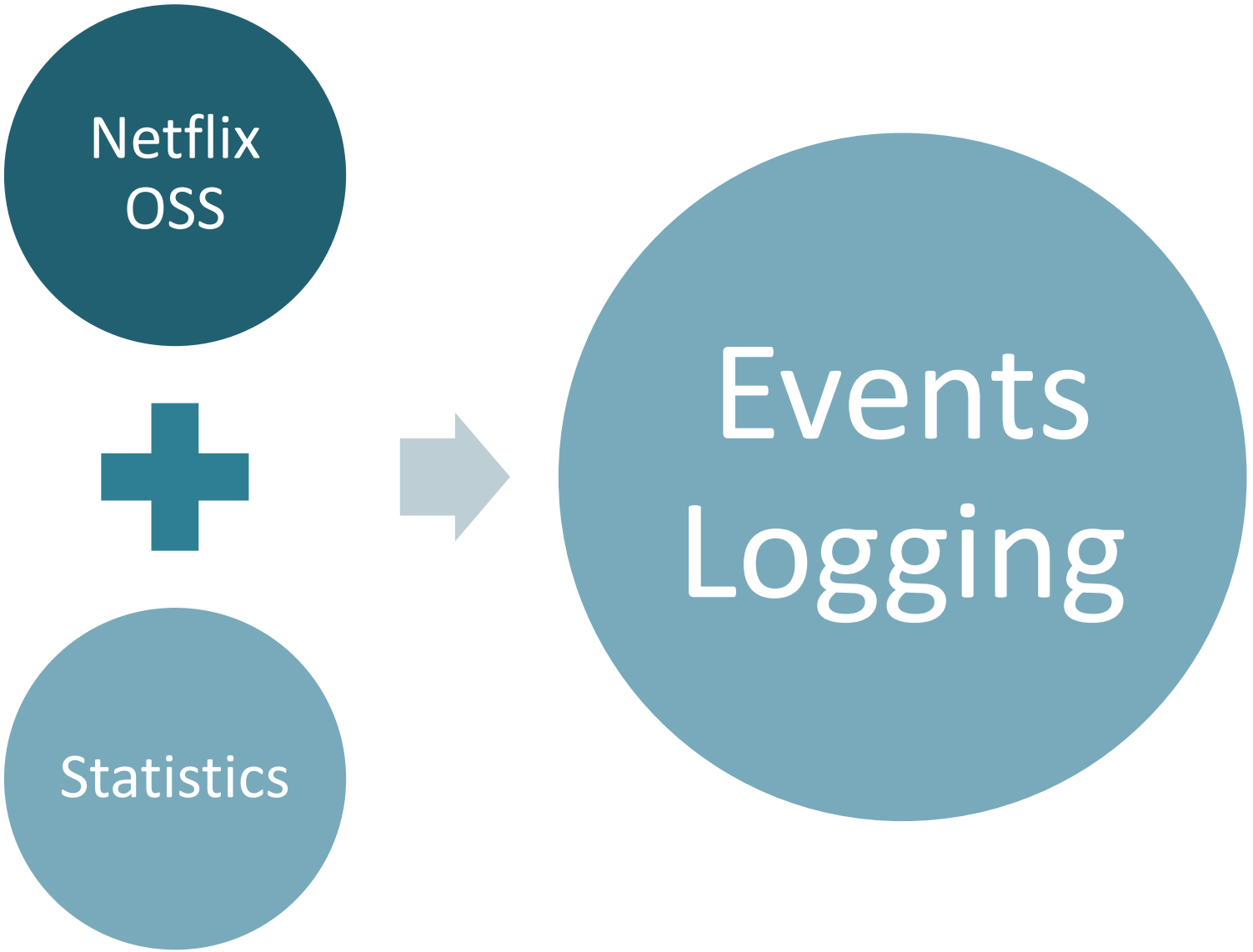
MDARC



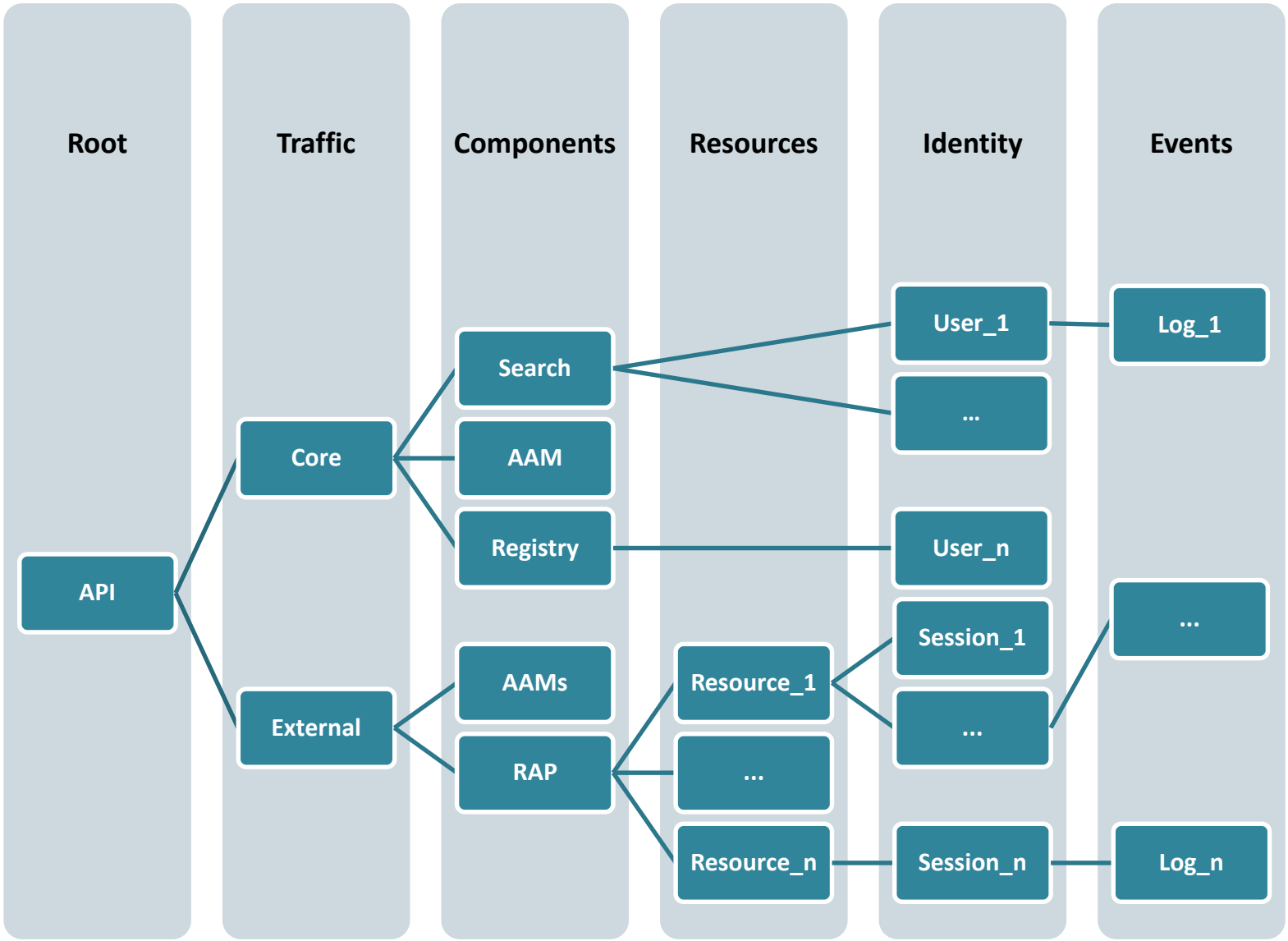
Layers (4)



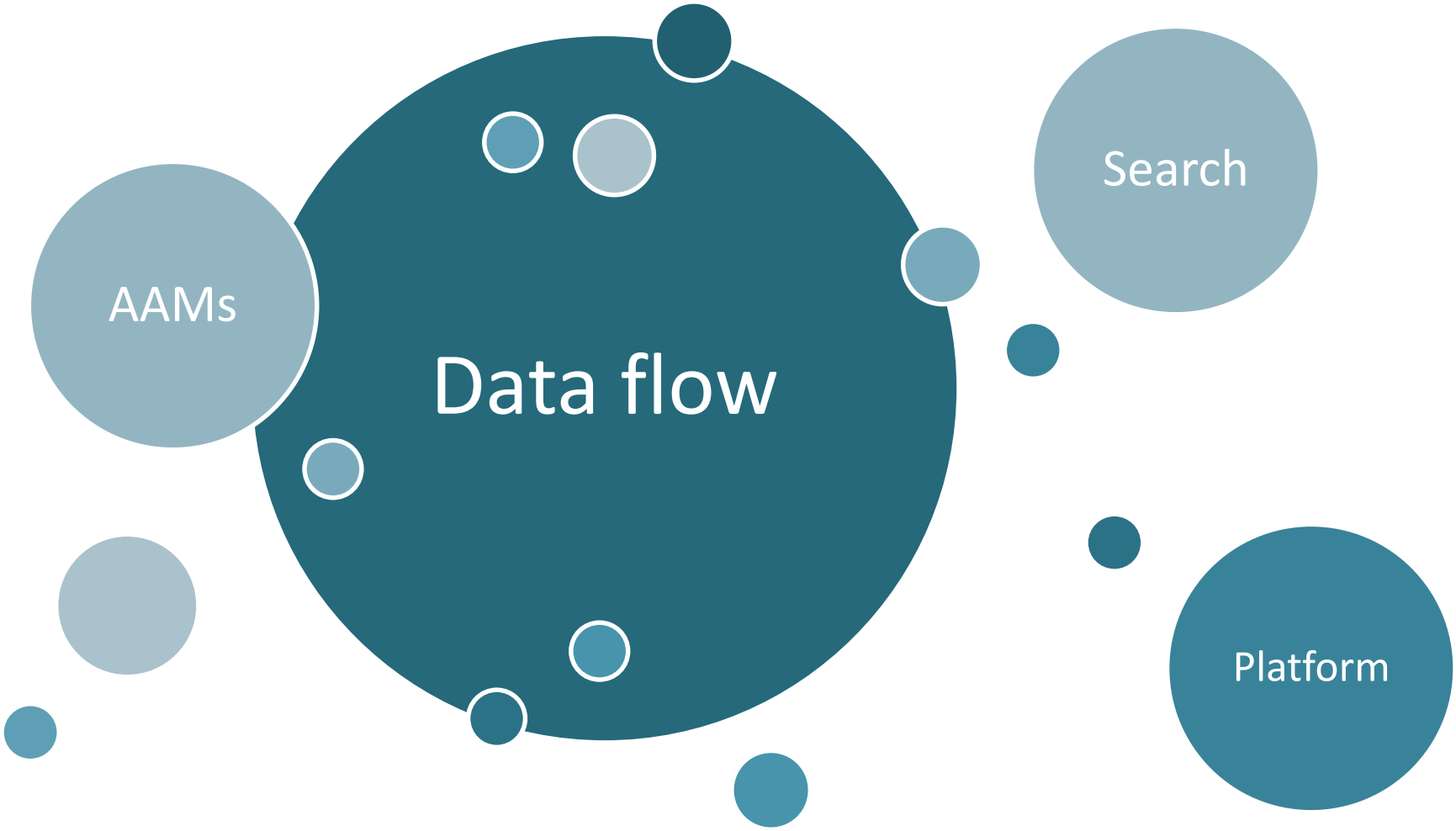
Anomaly Detection layer



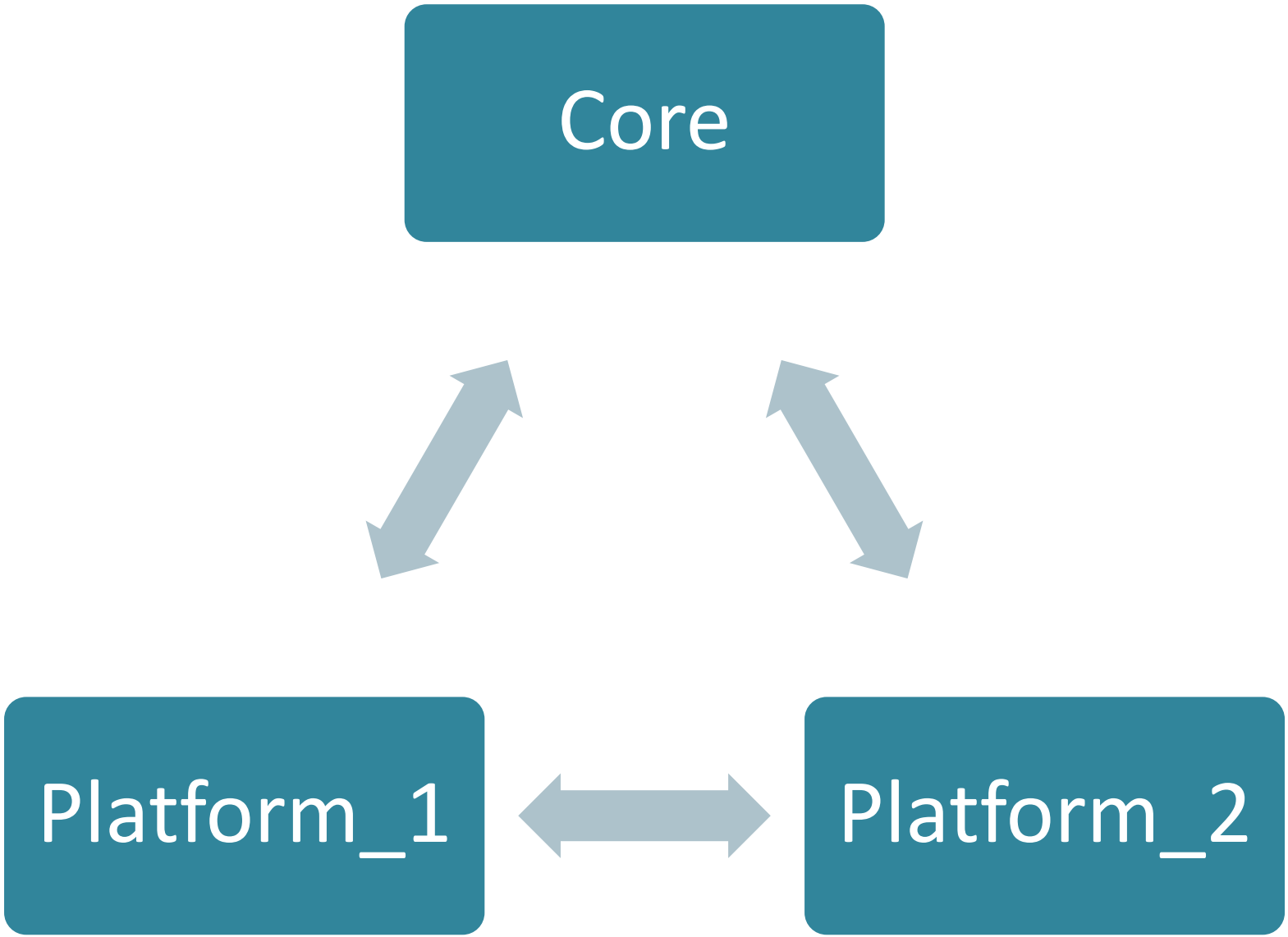
Behavioral patterns Decision Tree



Temporal patterns



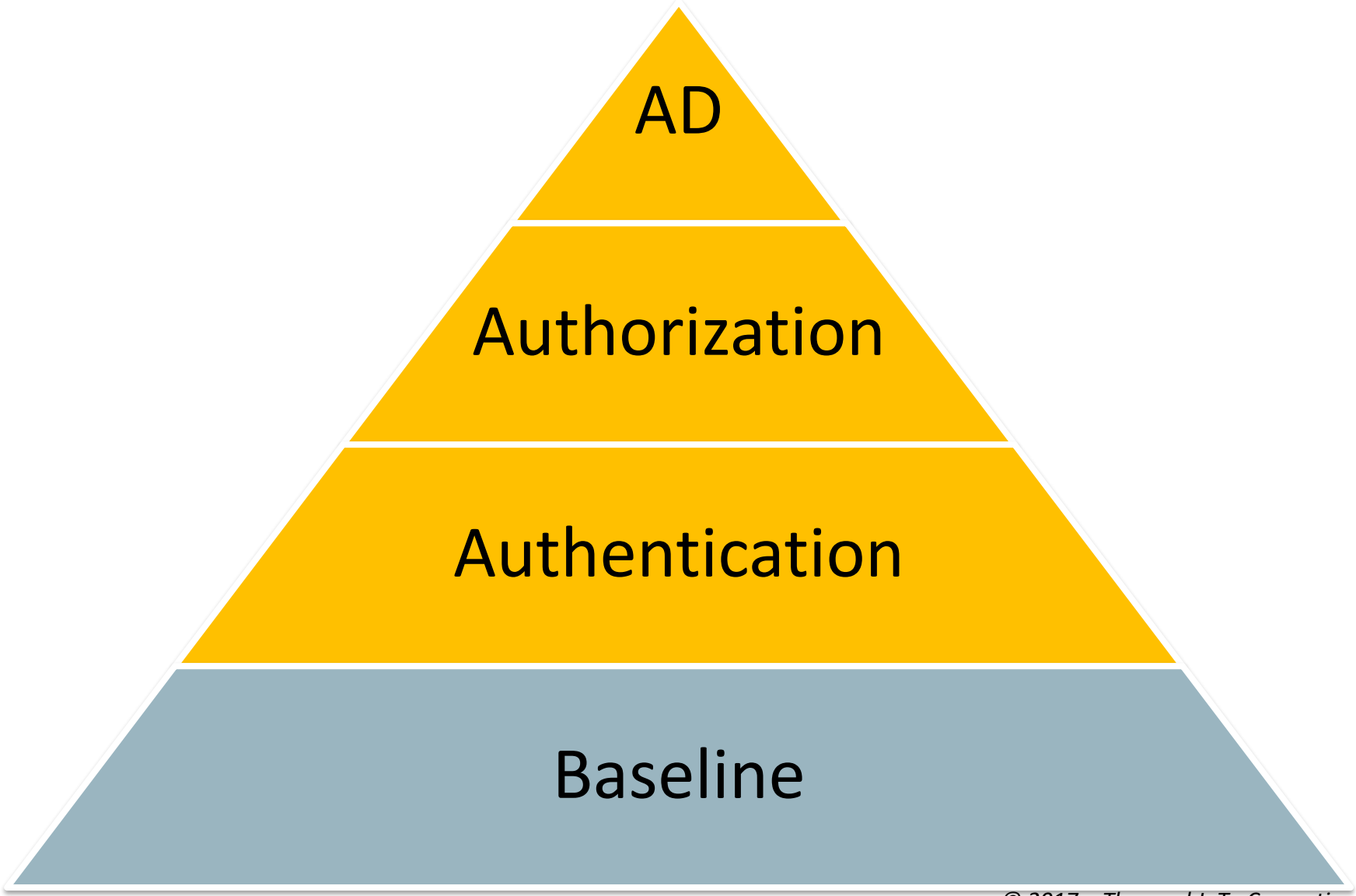
Identified AD threats



Open questions

- Platform usage statistics (GDPR)
- What is an anomaly?
- Quality of AD service
- Decision tree building algorithm
- Anomaly confirmation algorithm

Provided software



Security components

- Authentication & Authorization Managers (PKI CAs)
  - Issuing credentials (X.509 certs and JWTs)
  - Authenticating platforms and users (by credentials validation)
  - Managing credentials translation (Attributes mapping function)
- Security Handlers
  - Reference Cryptography operations implementation
  - Managing a key store with clients' certificates
  - Generating client's Auth(N) payloads
  - Matching ABAC policies against received Auth(Z) payloads
- Anomaly Detection Module
  - Continuously building APIs' temporal and behavioral usage models to detect anomaly spikes

Thank you!

Questions?


www.symbiote-h2020.eu


info@symbiote-h2020.eu


@symbiote_h2020

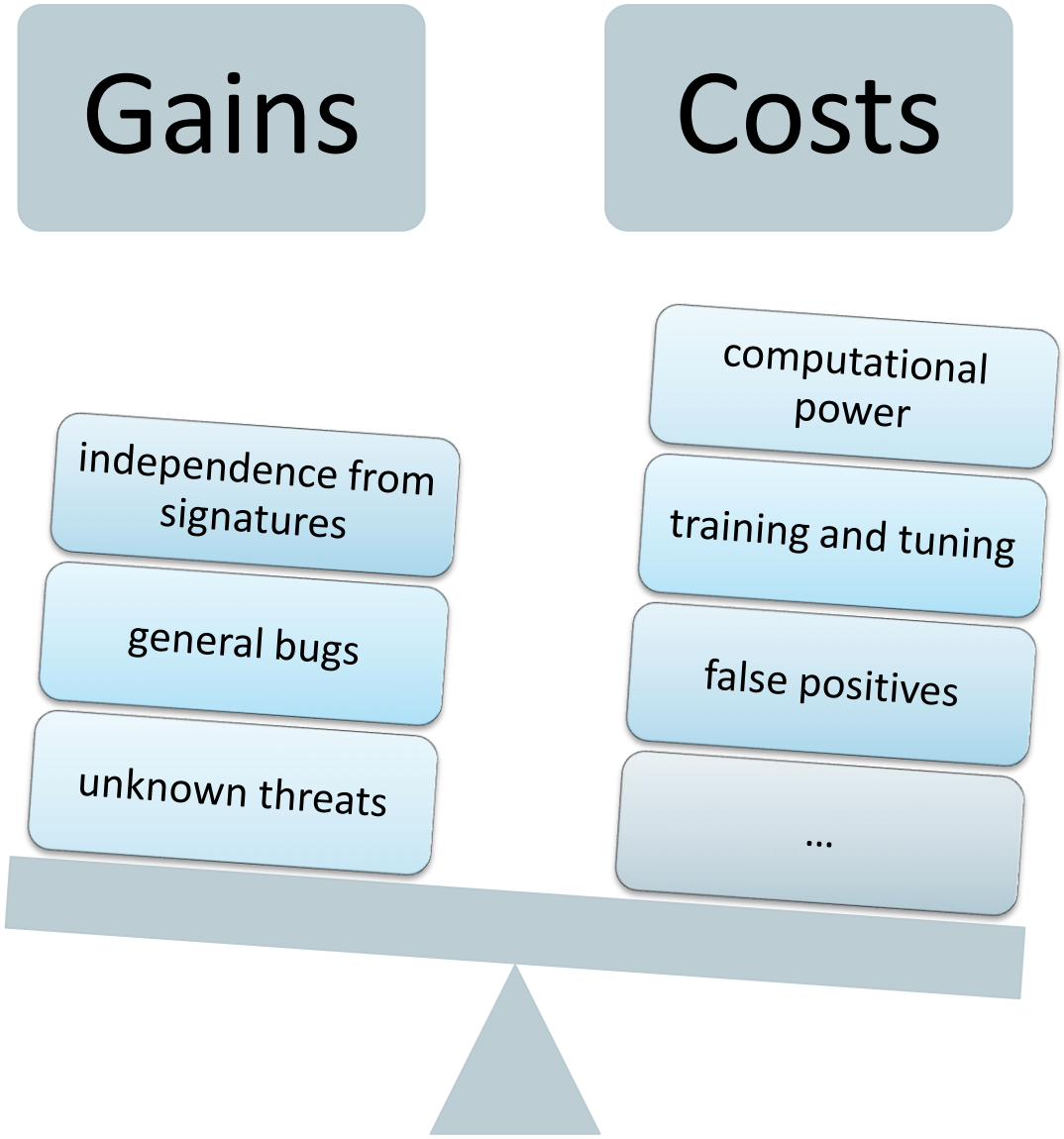

H2020 symbIoTe


github.com/symbiote-h2020

CONCEPT DRIFT & ANOMALY DETECTION

Where humans and rules are not enough…

AD pros and cons

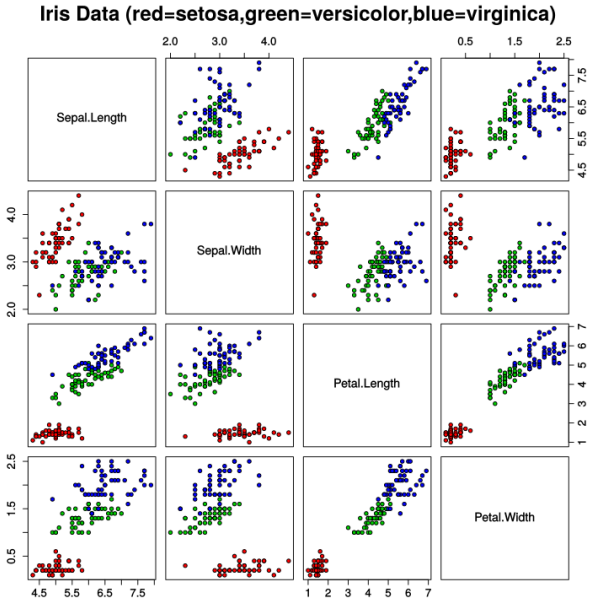


HANDLING DATA AND DATA STREAMS

A bit of theory

Data

- Data Mining



Sir Ronald Aylmer Fisher's *Iris* data set

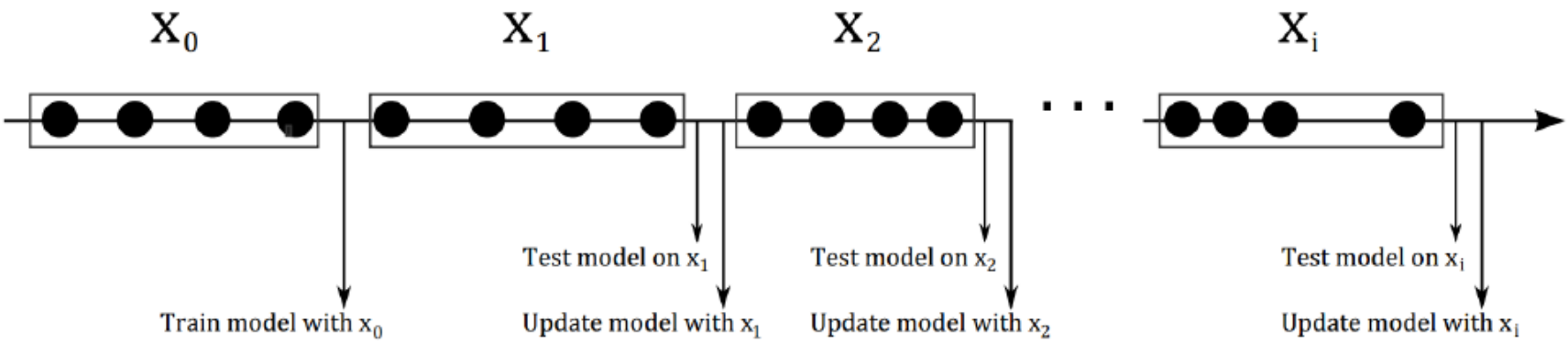
- Data Stream Mining

DSM constraints

	Traditional	Stream
No. of passes	Multiple	Single
Processing Time	Unlimited	Restricted
Memory Usage	Unlimited	Restricted
Type of Result	Accurate	Approximate
Distributed	No	Yes

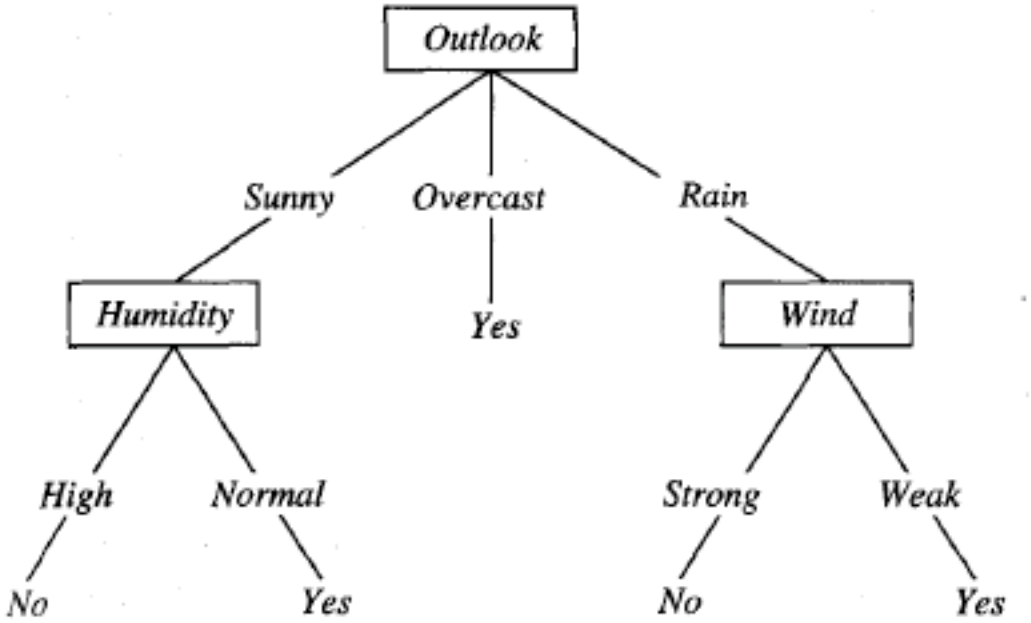
Mohamed Gaber and João Gama, University of Porto,
State-of-the-art in data stream mining. 2007.

Windowing / batches



Dariusz Brzezinski. *Mining data streams with concept drift*. Master's thesis, Poznan University of Technology, Poznan, Poland, 2010.

Inspiration – decision trees

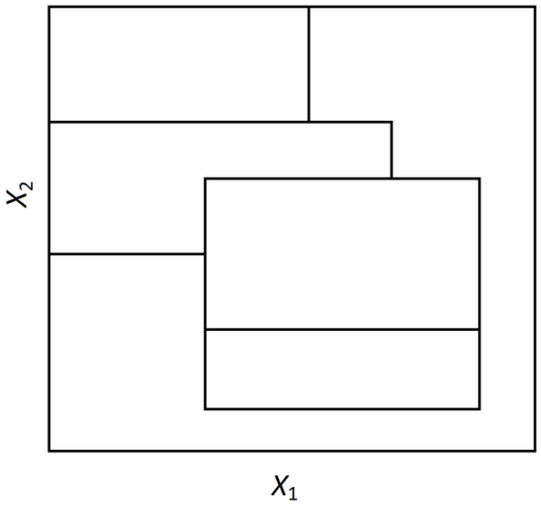


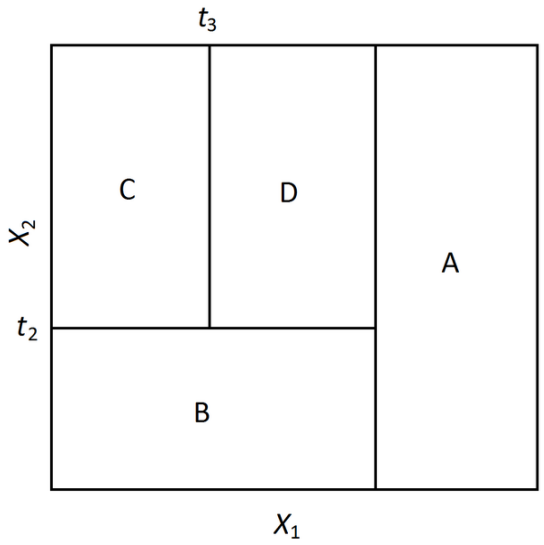
J.R. Quinlan, Centre for Advanced Computing Sciences,
New South Wales Institute of Technology, Australia, *Induction of Decision Trees*, 1986.

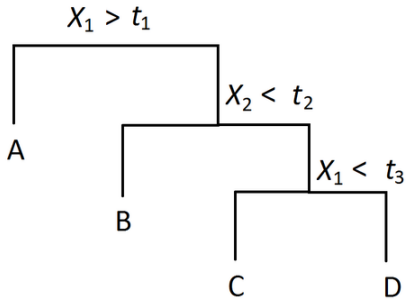
CONCEPT DRIFT

When things start to change…

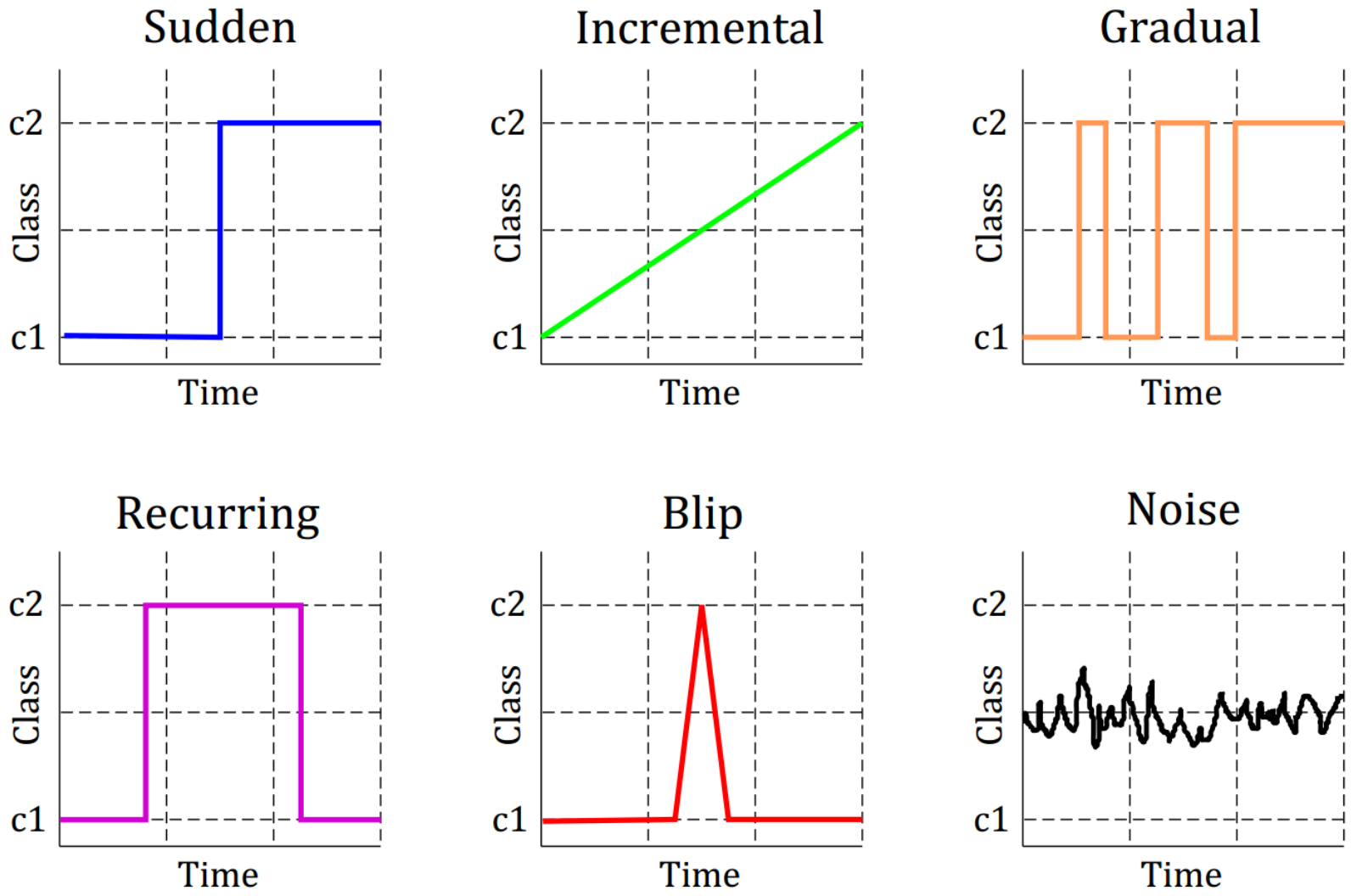
Events' attributes space





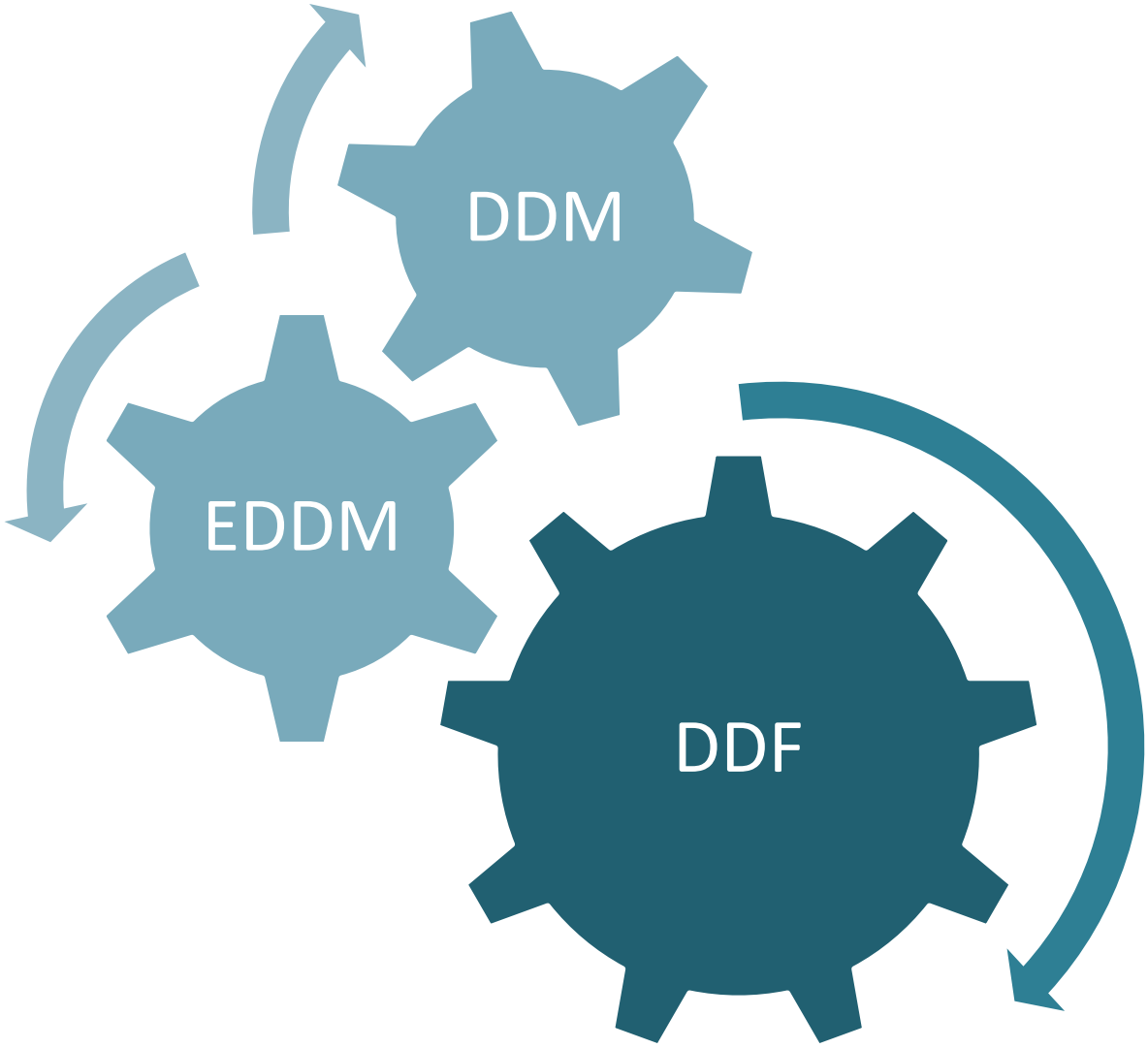


Concept drift types



Dariusz Brzezinski. *Mining data streams with concept drift*. Master's thesis, Poznan University of Technology, Poznan, Poland, 2010.

CD Detector inspiration



Demand driven framework

$$P(l) = \frac{n_l}{N}$$

$$PS = \sum_{l \in dt} \frac{|P_s(l) - P_D(l)|}{2} \times 100\%$$

- 2004, *Active mining of data streams*, Wei Fan et al.
- 2008, *An active learning method for mining time-changing data streams*, Huang
- 2011, *Semi-supervised approach to handle sudden concept drift in enron data,* Kmieciak & Stefanowski
- 2014, *Active learning from partly labeled data streams,* Master's thesis, Dobski