Attribute Based Access Control

Jacoba Sieders - ABNAMRO

OWASP BENELUX DAY

Tilburg, November 24th, 2017

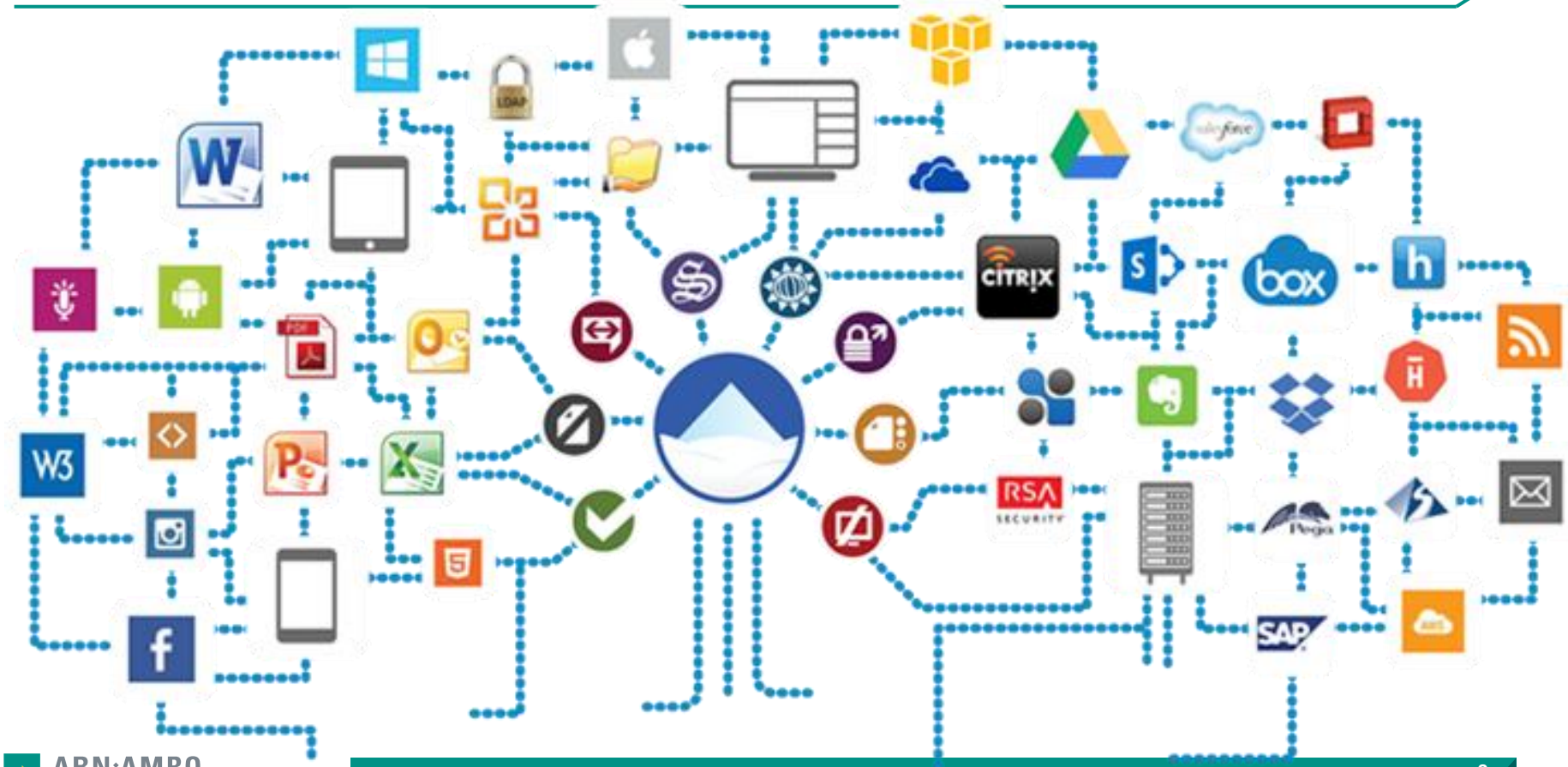
Slide from 2014: predictions on connectivity

Connectivity across
ID federations
Datasets
Applications
Value chains
Companies
Continents
Jurisdictions
Platforms
Devices
Clouds
Things
Services
BaaS = Back-end as a Service

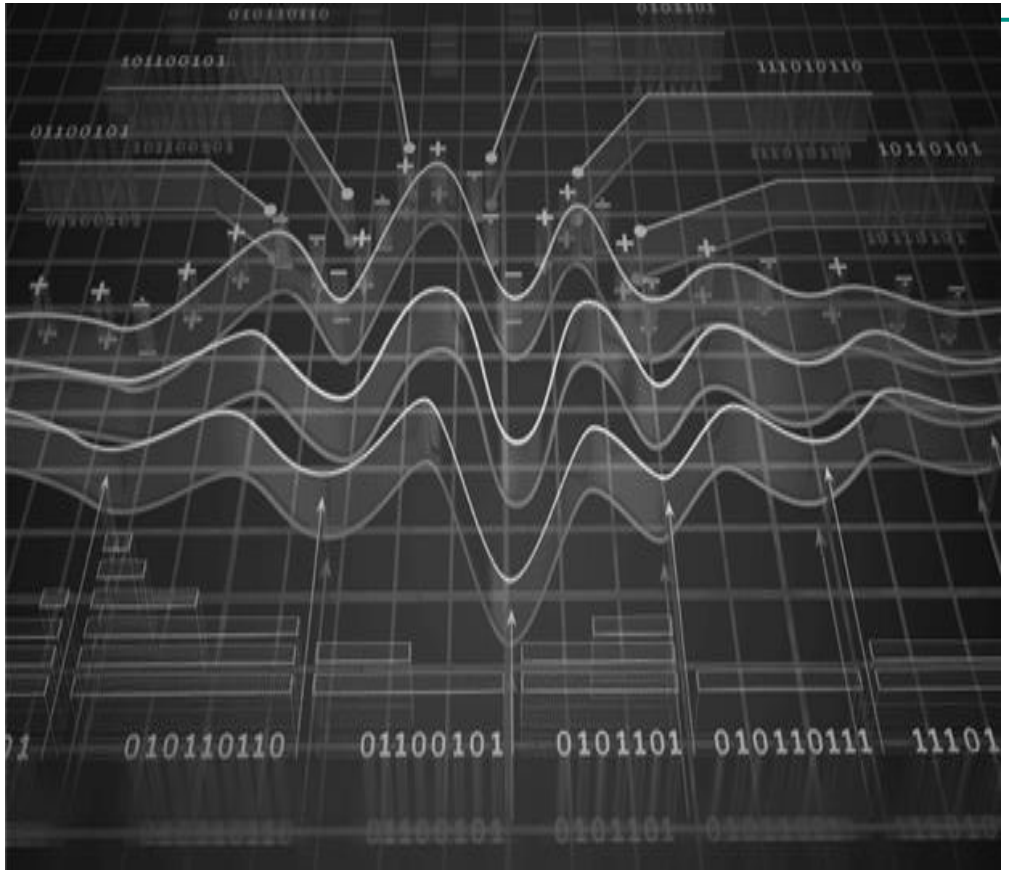
2017: API's

ABN·AMI

API’s and de-perimeterization are daily business



SLIDE FROM 2014: PREDICTIONS ON BIG DATA



- Visual data discovery
- Automated decision-making
- 70% of large organizations purchase external data
- 100% by 2019. (Forbes)
- 180.000 data analysts US 2018

2017:
Artificial intelligence
Predictive analytics
Machine learning
Data driven everything

Purpose of digital data changed: information and operations & decisions

Population of digital users changed

Expert engineers..

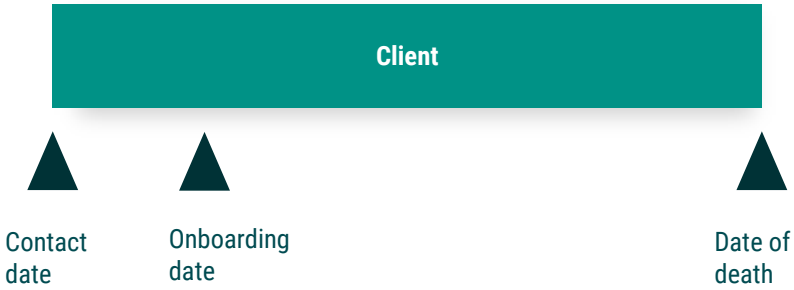
Your grandma
Your toddler
Your malware
Your fridge

Roles of digital users

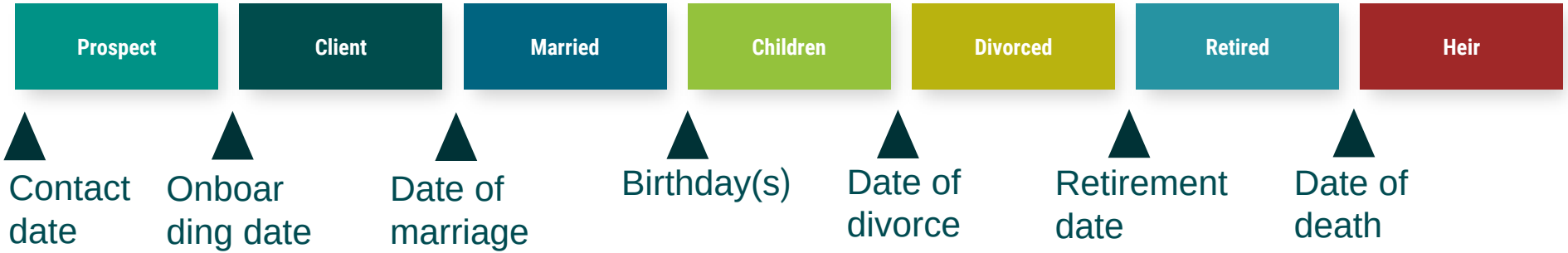
My ID
Customer
Supplier
Partner
Private user
Administrator
Anonymous user
Device
Fraudster, mule
Process
Session
IoT becoming “agent” on behalf of user
Federated ID

Identity Lifecycle: more lifecycle states

from “JoMoLea”



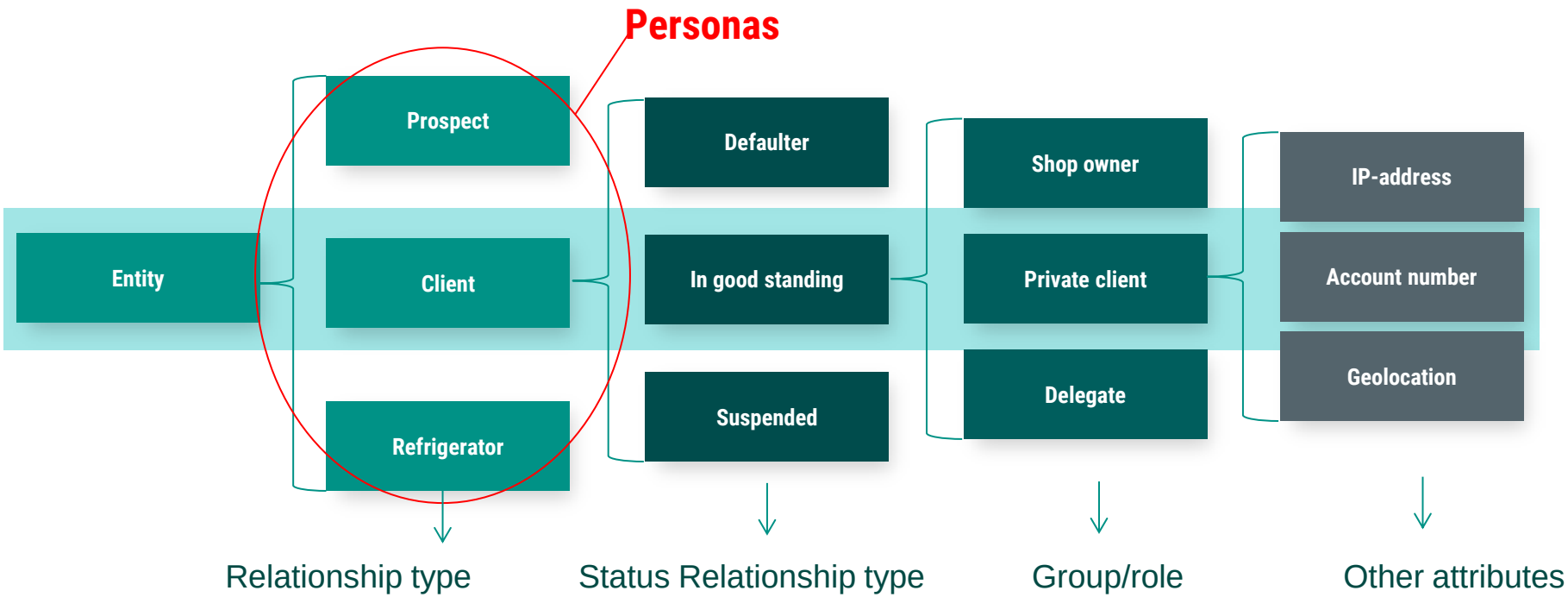
to multiple lifecycle state attributes



ABN·AMRO

Trends in IAM Relationship models; more relationship types

From identities to identity relationships



ABN·AMRO

Identity Analytics

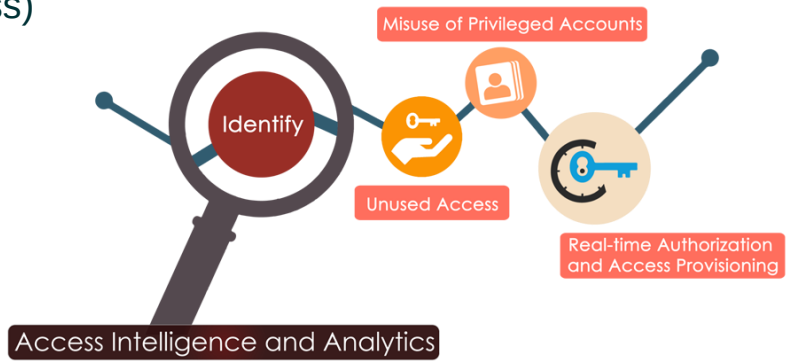
Access requests should no longer be a la carte, **but user context aware** (ala Amazon or bol.com)

Data mining patterns should **reveal similar users** with similar attributes and access, allowing for easy detection of access profiles, and suggested if not automated repair of anomalies.

Identity governance should respond to **user behaviour** (24x7) ,based on IAM data

Need for:

- Data mining/clustering (the ability to detect identical users)
- Weighted search (access request should be filtered based on patterns of the previous requests)
- (semi) Automated repair (removal of anomalous access)



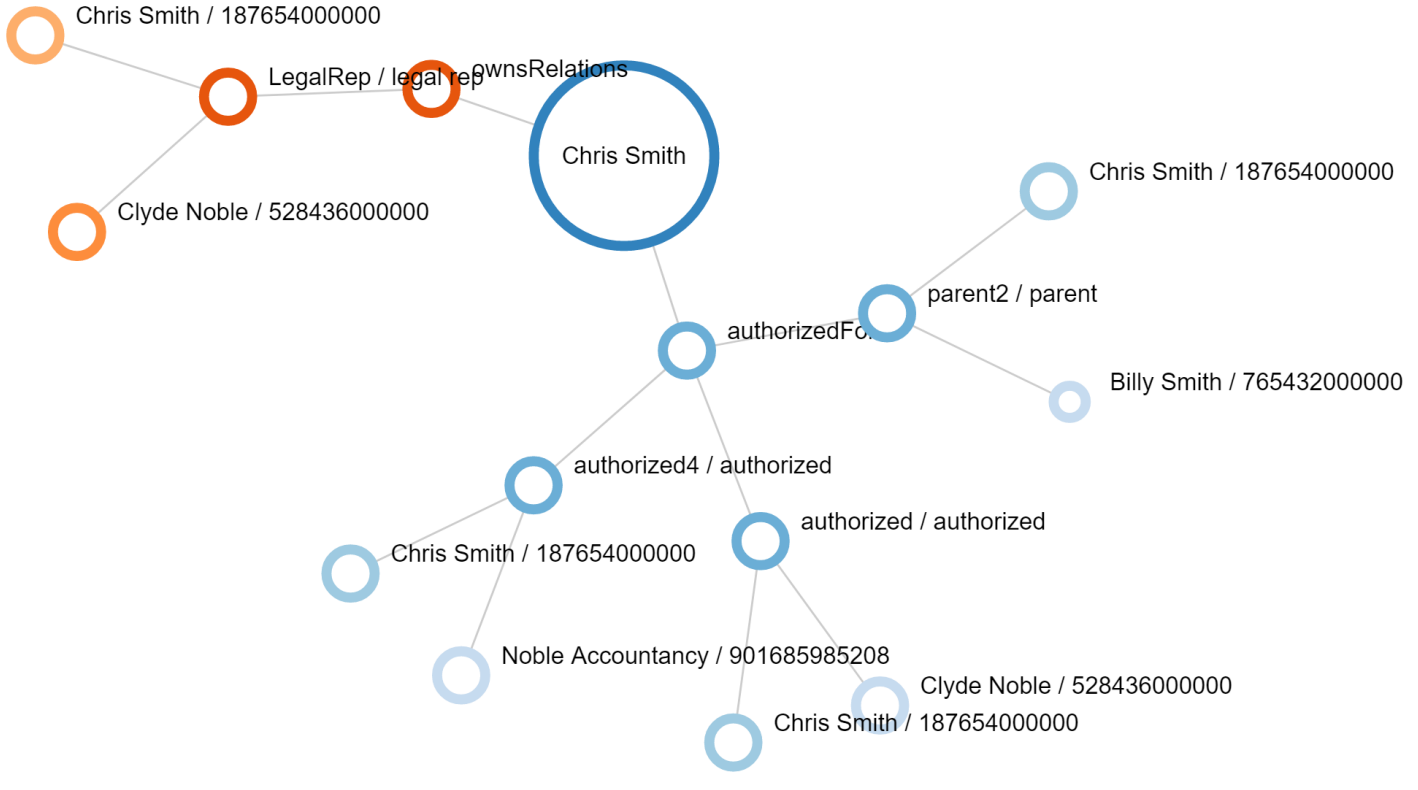
IDENTITY RELATIONSHIPS

Digital Identity Links

Chris Smith

Data Types:

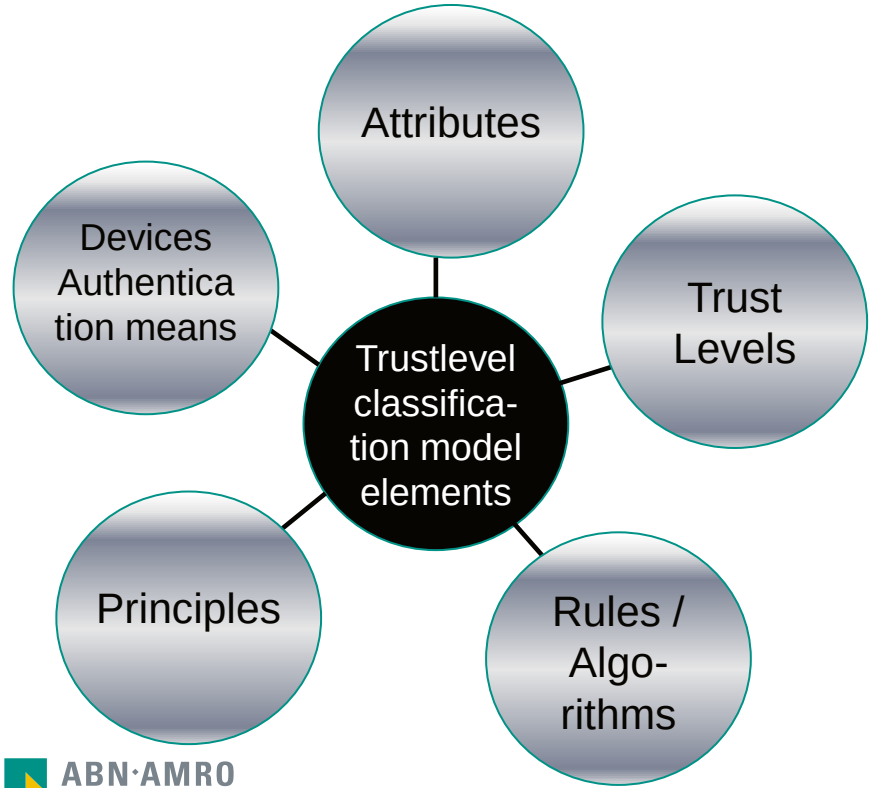
- Digital Identity
- authorizedFor
- authorizedFor-authorized DI
- authorizedFor-object DI
- ownsRelations
- ownsRelations-authorized DI
- ownsRelations-object DI



Conclusion “Seven any” all relevant for access decisions

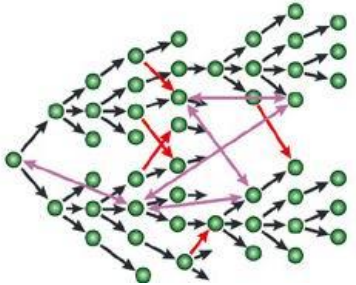
ABAC building blocks

Trust level classification framework



Rulesets and policies

Interaction framework and governance on multiple rulesets with different owners: rules should not clash



- Fine-grained, data-centric
- Context aware, rulebased
- Real time access decisions
- Flex degrees of authentication
- Flex degrees of authorisation
- Trustlevel mapping

ABN·AMRO

Fine-grained context aware access management - building blocks

data classifier

token management system

PDP - Policy Decision Points
PAP - Policy Administration Points
PIP - Policy Information Points
PEP - Policy Enforcement Points

XACML

session integrator

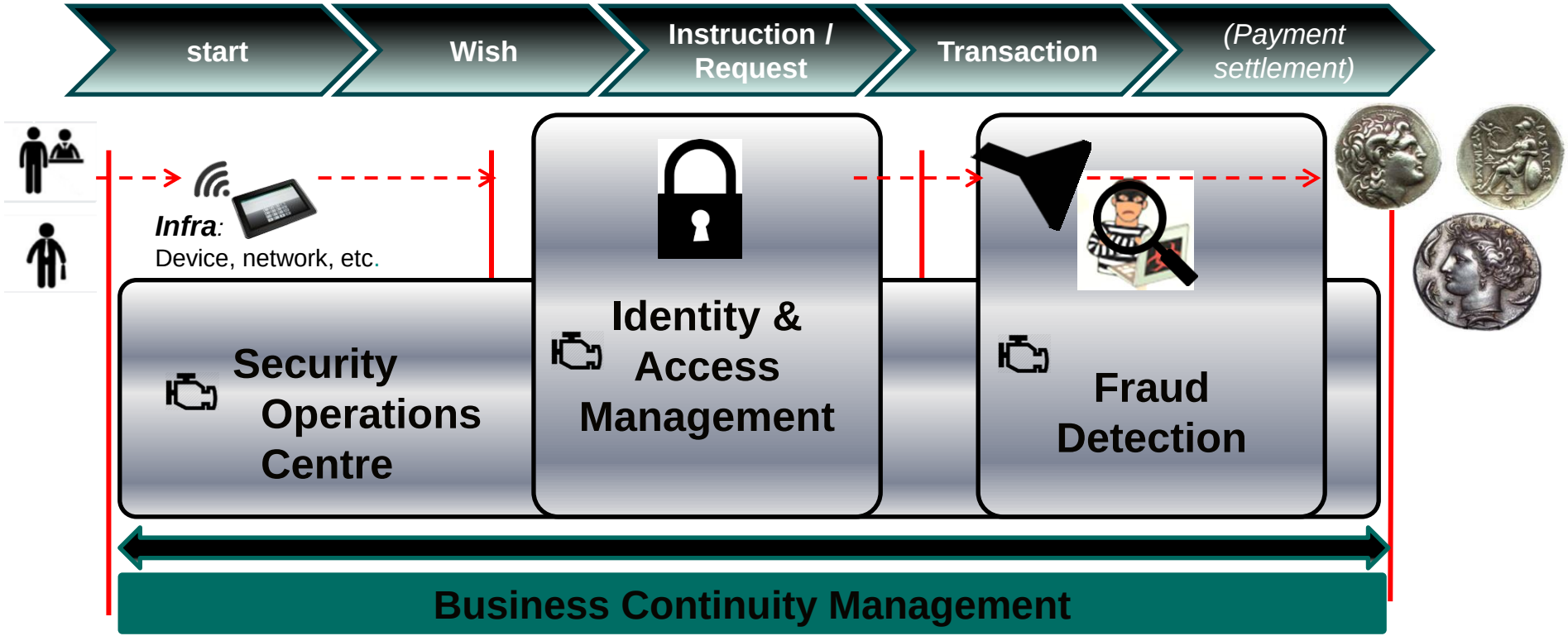
connectors and interfaces

Attributes:
data quality
data management
Meta data

Rules:
ownership in the business
maintenance

Query-based Policy Enforcement Point
Format Preserving Encryption

Traditional preventative/detective/reactive controls + analytics



Full situational awareness through merger of the control landscape

ABAC features

- Context aware
- Rule based
- Fine-grained access decisions
- Step-up authentication (or step **down authorisation**)
- More flexible than Role Based Acces Control (RBAC)
- Less rules hard-coded within applications
- Configuration within IAM tools: short time-to-market of new business rules
- Trustlevel on dataset or transaction
- Trustlevel on transaction request context
- Trustlevel framework enables immediate intervention if compromised
- Implementation: gradually evolve from RBAC to ABAC
- Most feasible: hybrid model serving both
  (a role is also a rule and some access rules always remain fixed)
- Focus on **governance** and **business involvement** is crucial

Summary

“Digitisation”:

Data for information, operations, (automated) decisions
Connectivity
Deperimeterization
Hybrid cloud
Paas, Saas, Iaas, BaaS
API’s
Real time data retrieval
Any device, time, network, user, transaction
Micro services
Automated decision making
Artificial intelligence, machine learning, Predictive analytics

Identity & Access Management:

Increasing importance of digital identity
“Fine grained Identity”
Rule based access decisions
Flexible authentication
Flexible authorisation
Real time
Context aware
Data centric protection

→ For ABAC, focus on:

(Meta)data quality
Governance + ownership
Business risk appetite
Trust level models
Hybrid set-up with RBAC?!

Time for questions!

jacoba.sieders@nl.abnamro.com ABNAMRO Amsterdam +31634150150