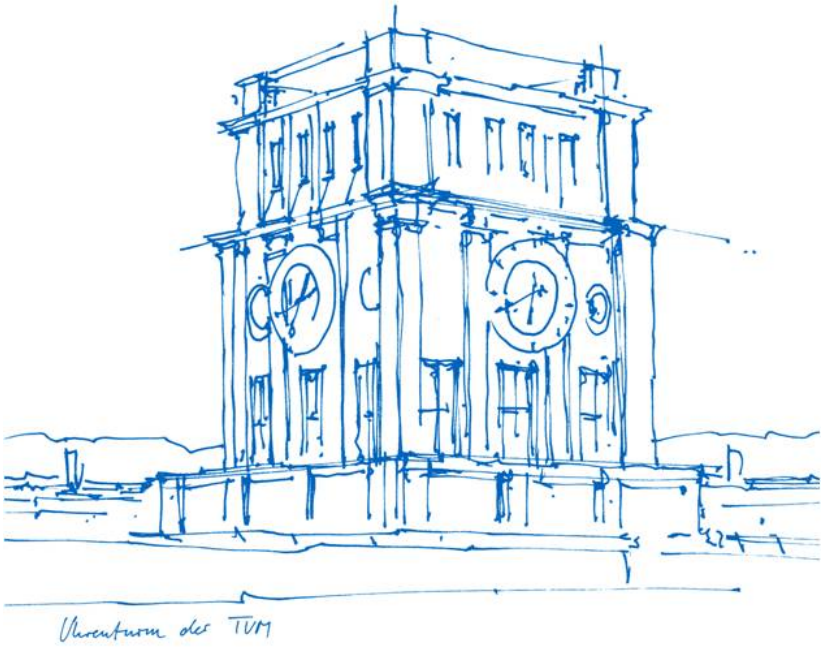
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Secure Multiparty Computation in the Internet of Things

Marcel von Maltitz
vonmaltitz@net.in.tum.de
http://www.net.in.tum.de/members/maltitz



Focus: Smart Building / Smart Homes / Smart Offices

A Siemens building management system in Vienna, which can access some 10,000 sensors, provides extremely energy-efficient lighting, as well as temperature and ventilation optimization.

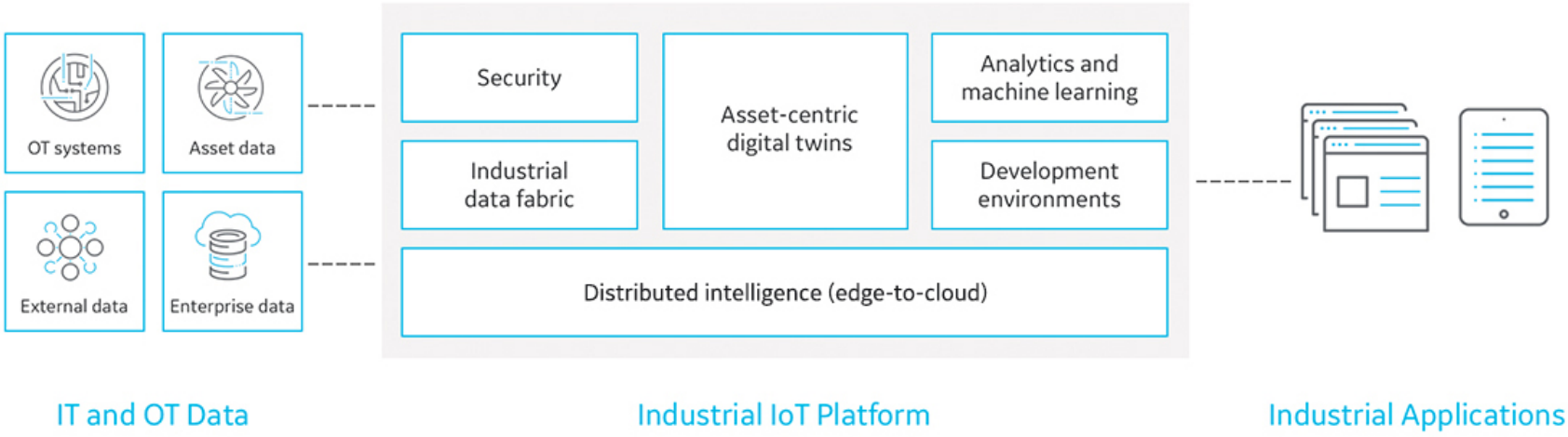
Focus: Smart Building / Smart Homes / Smart Offices

©Siemens

HVAC	Power Consumption	Fire Safety
Lighting	Presence Detection	Guidance Systems
Elevators	Environment Sensing	Energy Management

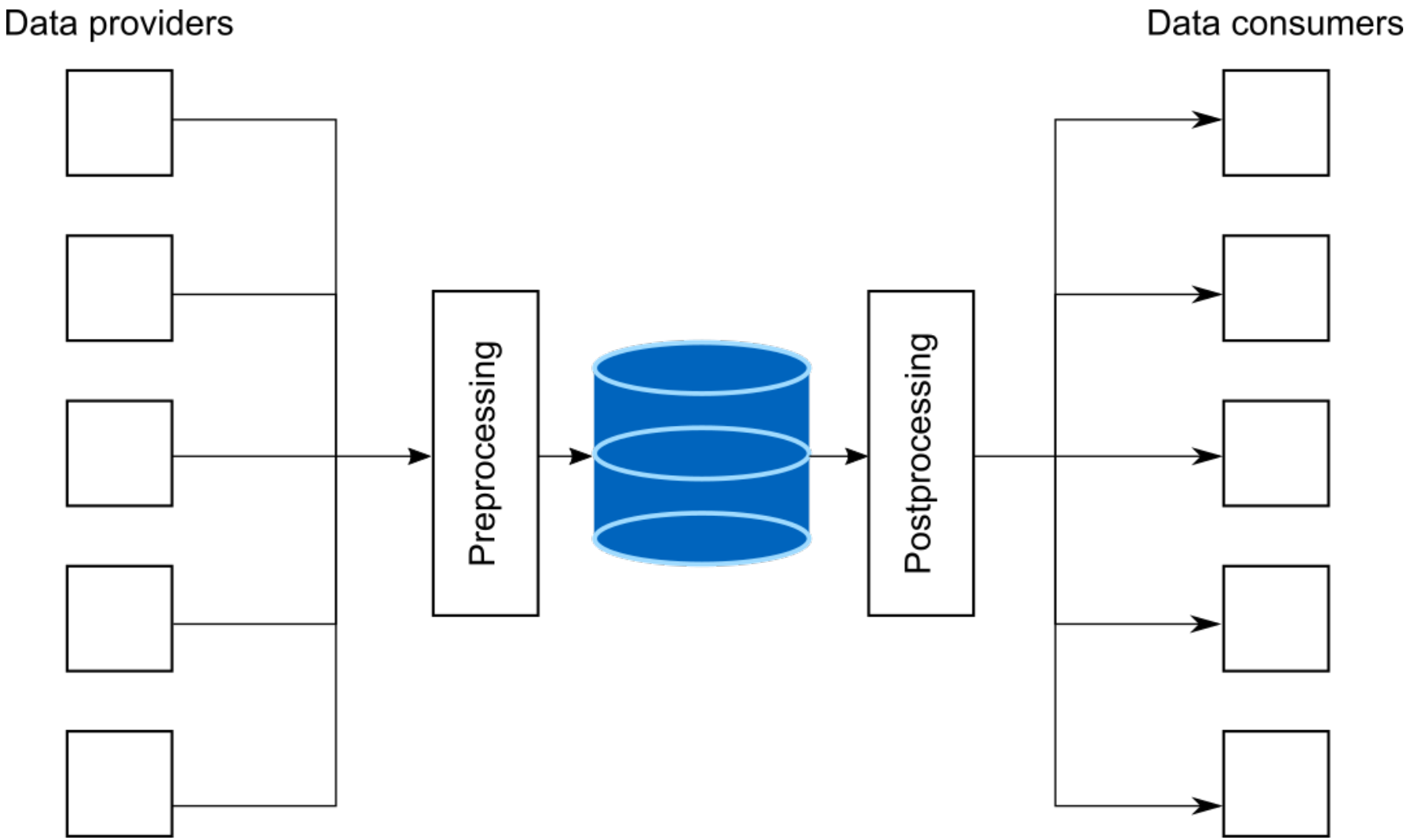
Abstraction

Abstraction



© General Electrics: Predix Platform

Abstraction



Problems

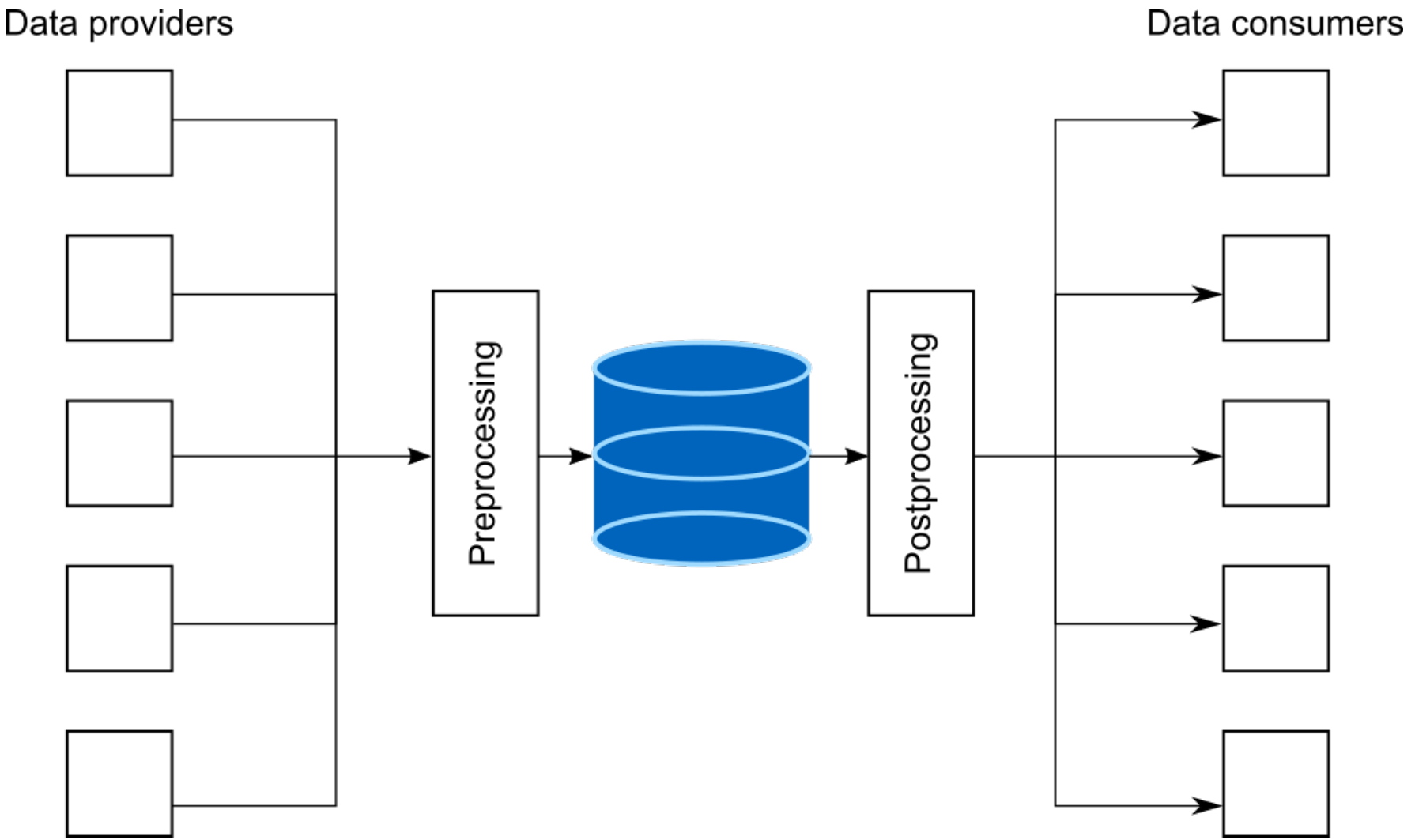
Security

- Collection of raw data
- History of previously collected data
- → Single point of attack, High value target

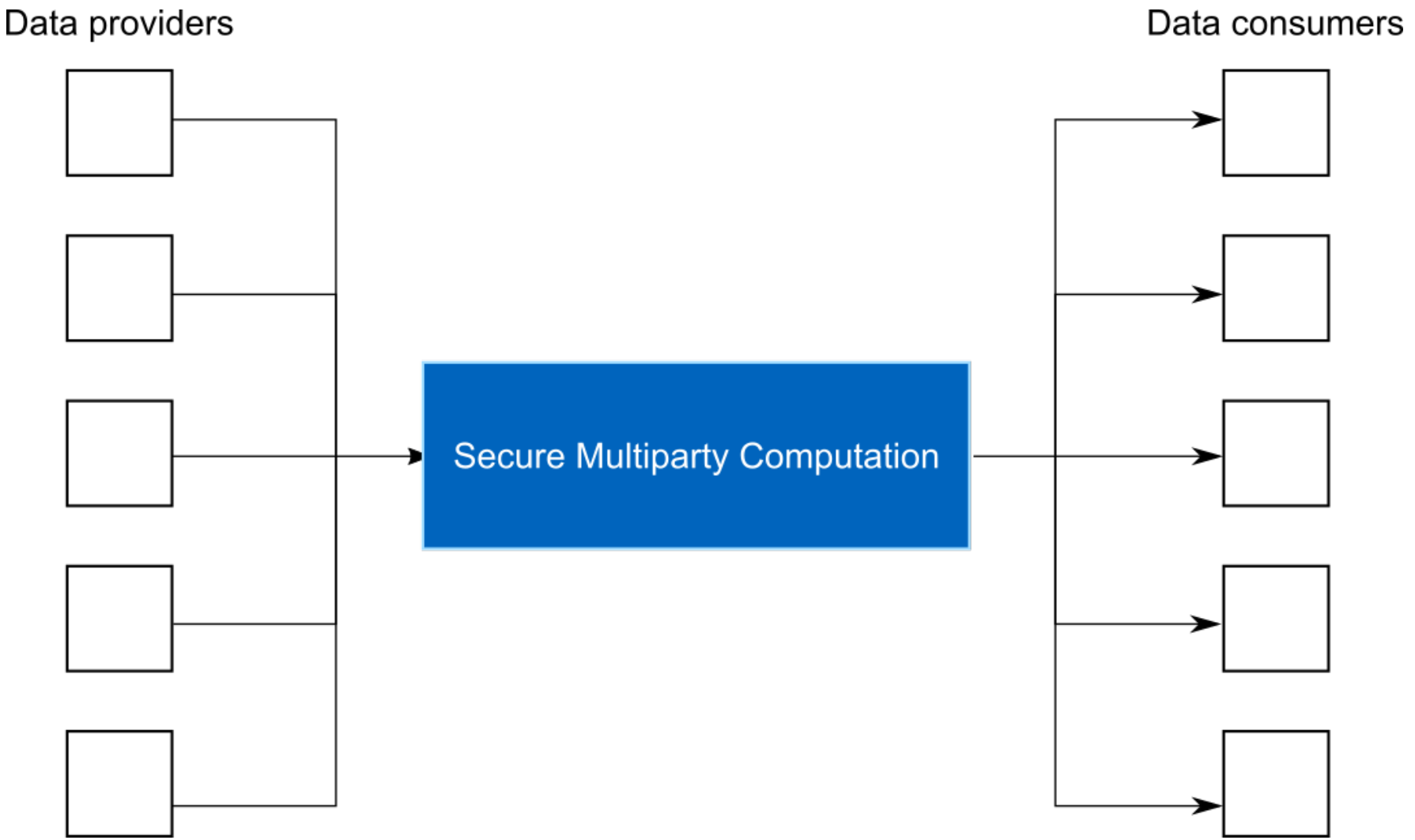
Privacy / Data Protection

- Personally identifiable/relatable information
- Collection and usage intransparent
- Lost of control
- Observation / Tracking / Surveillance
- → Threats to privacy
- → User acceptance?
- → Legal conformity?

Abstraction



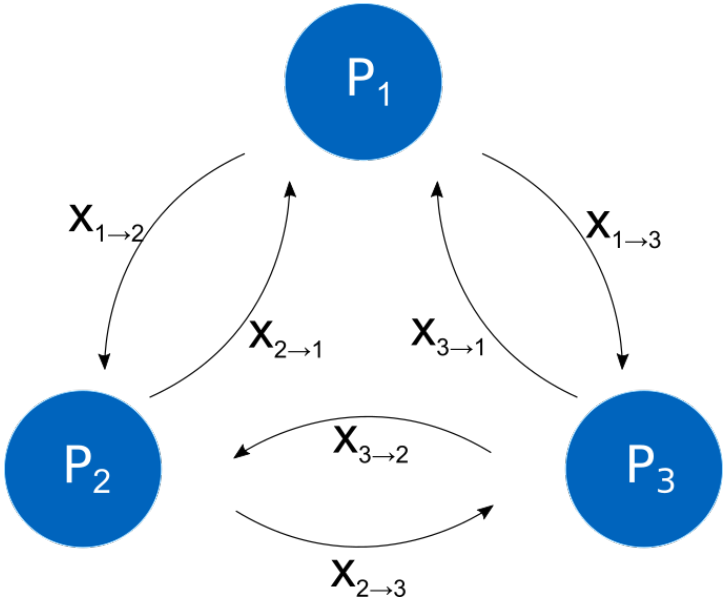
Abstraction



Background: Secure Multiparty Computation

There are n parties P_1, …, P_n. Each party P_i holds a secret value x_i. *Secure Computation* of $y = f(x_1, \ldots, x_n)$ is performed if two conditions are satisfied:

- Correctness: the correct value of *y* is computed
- Privacy: *y* is the *only* new information that is released



Example: Addition

Party	x_i	Share P_1	Share P_2	Share P_3
P_1	10	3	2	5
P_2	5	1	2	2
P_3	7	4	1	2
Result	22	8	5	9

Benefits

Confidentiality

- Raw input data only on collecting device

Unlinkability

- Results give no insights in input data
- Illegitimate combination of information from same device harder

Transparency

- Purpose of computation known due to participation
- Trustworthy accountability by individual parties

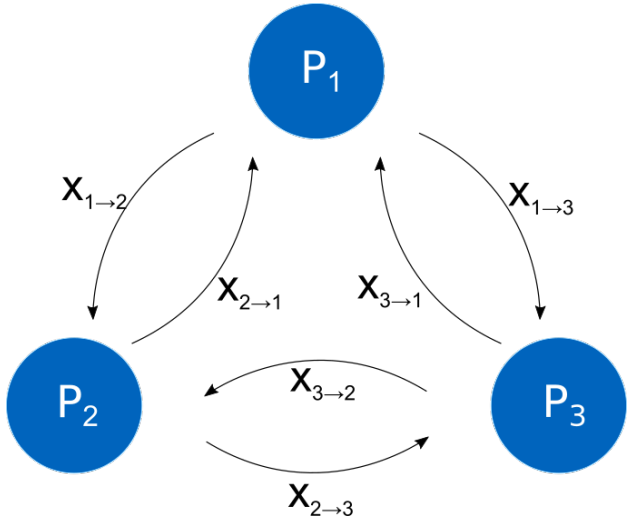
Intervenability

- Parties can refrain from participation → Veto-Mechanism

Challenges

Dynamic Environment

- Parties previously unknown
- Subsets of Parties
- Different input data
- Computations previously unknown



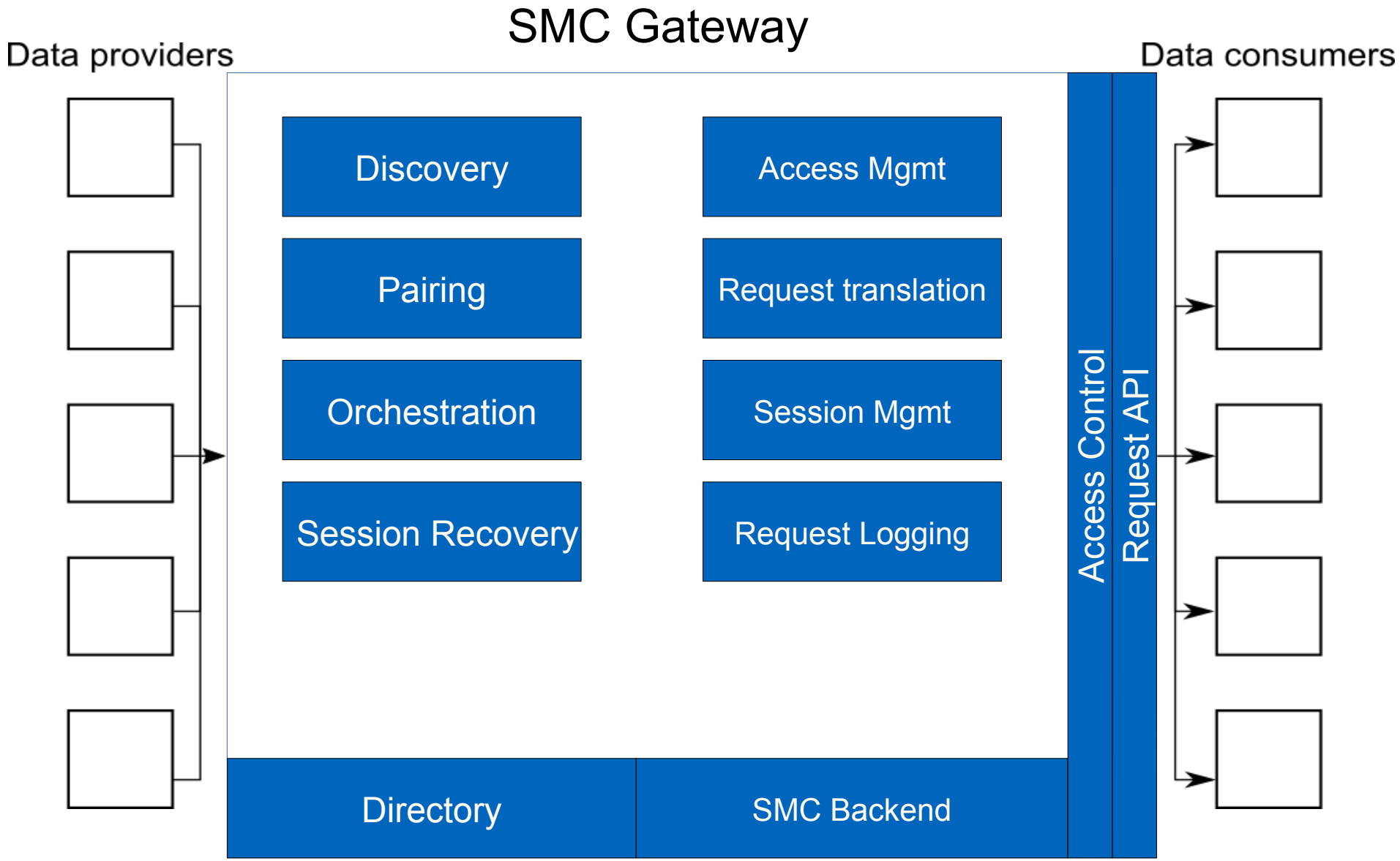
Orchestration of Computations

- Synchronized communication
- No error handling
- Only parties obtain result

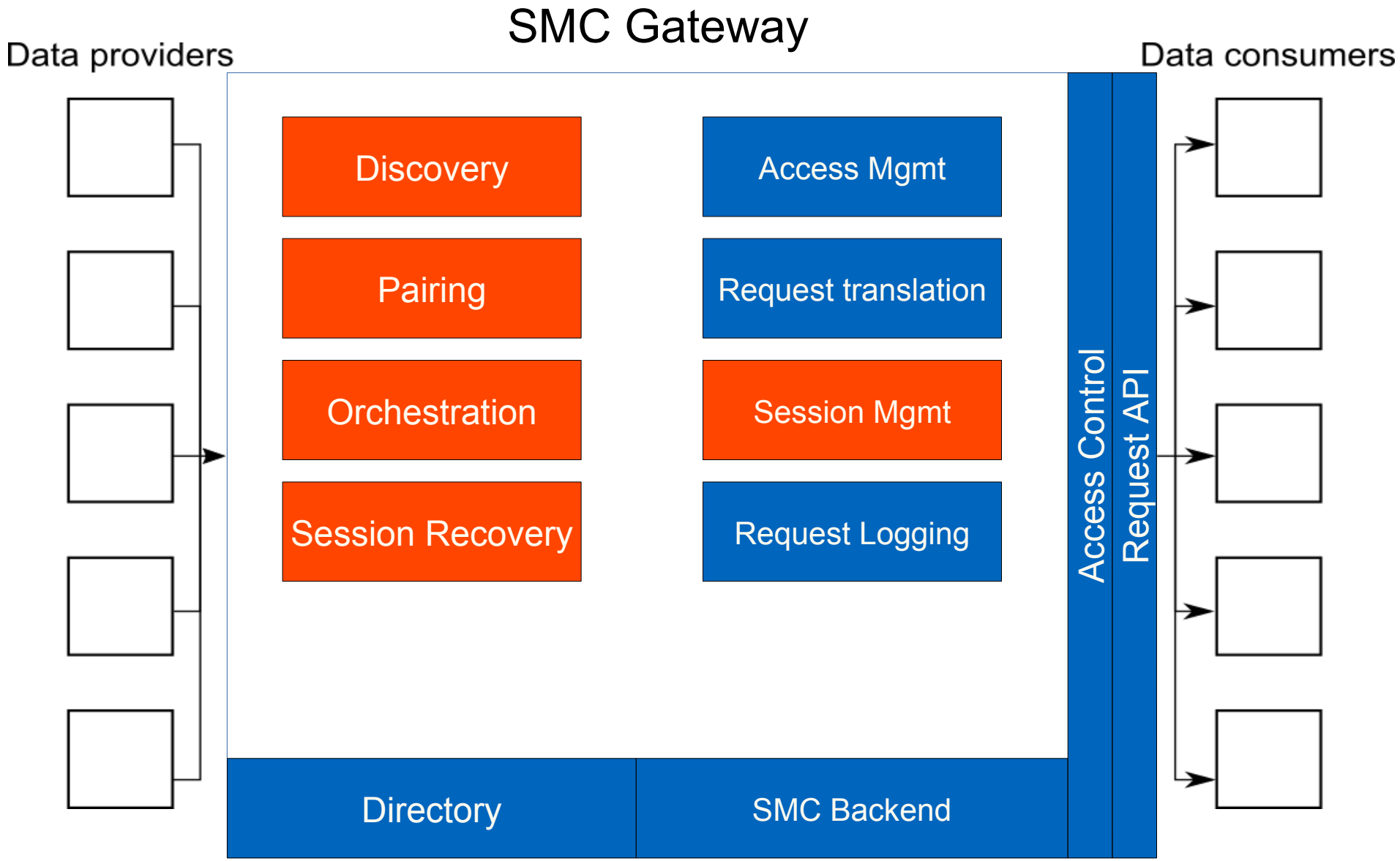
Service character

- Access for data consumers
- Metadata about available information
- Access control

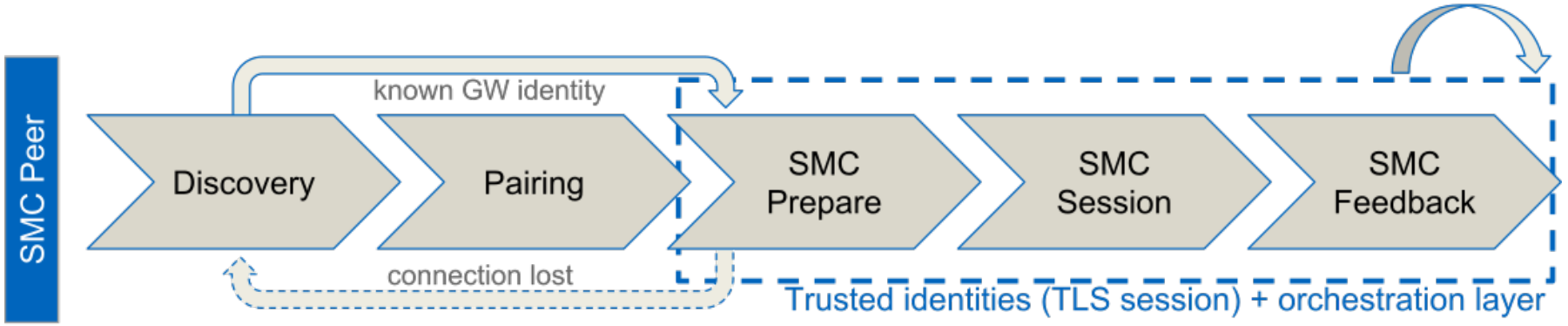
Approach


SMC Gateway
Data providers
Data consumers
Discovery
Pairing
Orchestration
Session Recovery
Access Mgmt
Request translation
Session Mgmt
Request Logging
Access Control
Request API
Directory
SMC Backend

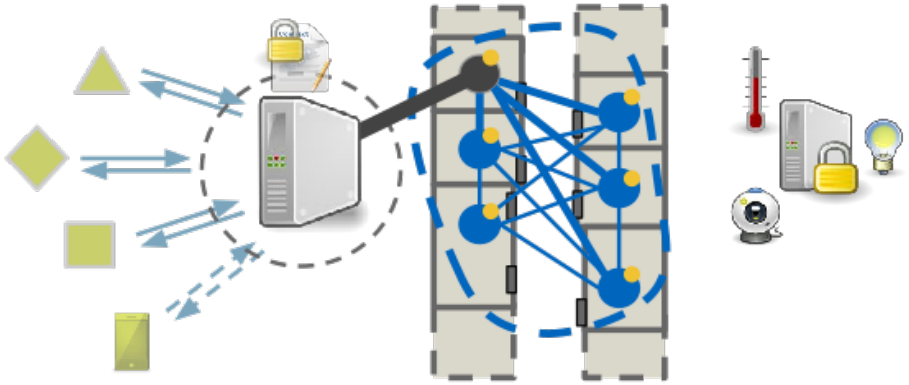
Approach


SMC Gateway
Data providers
Data consumers
Discovery
Pairing
Orchestration
Session Recovery
Access Mgmt
Request translation
Session Mgmt
Request Logging
Access Control
Request API
Directory
SMC Backend

Approach: Self-organizing Parties

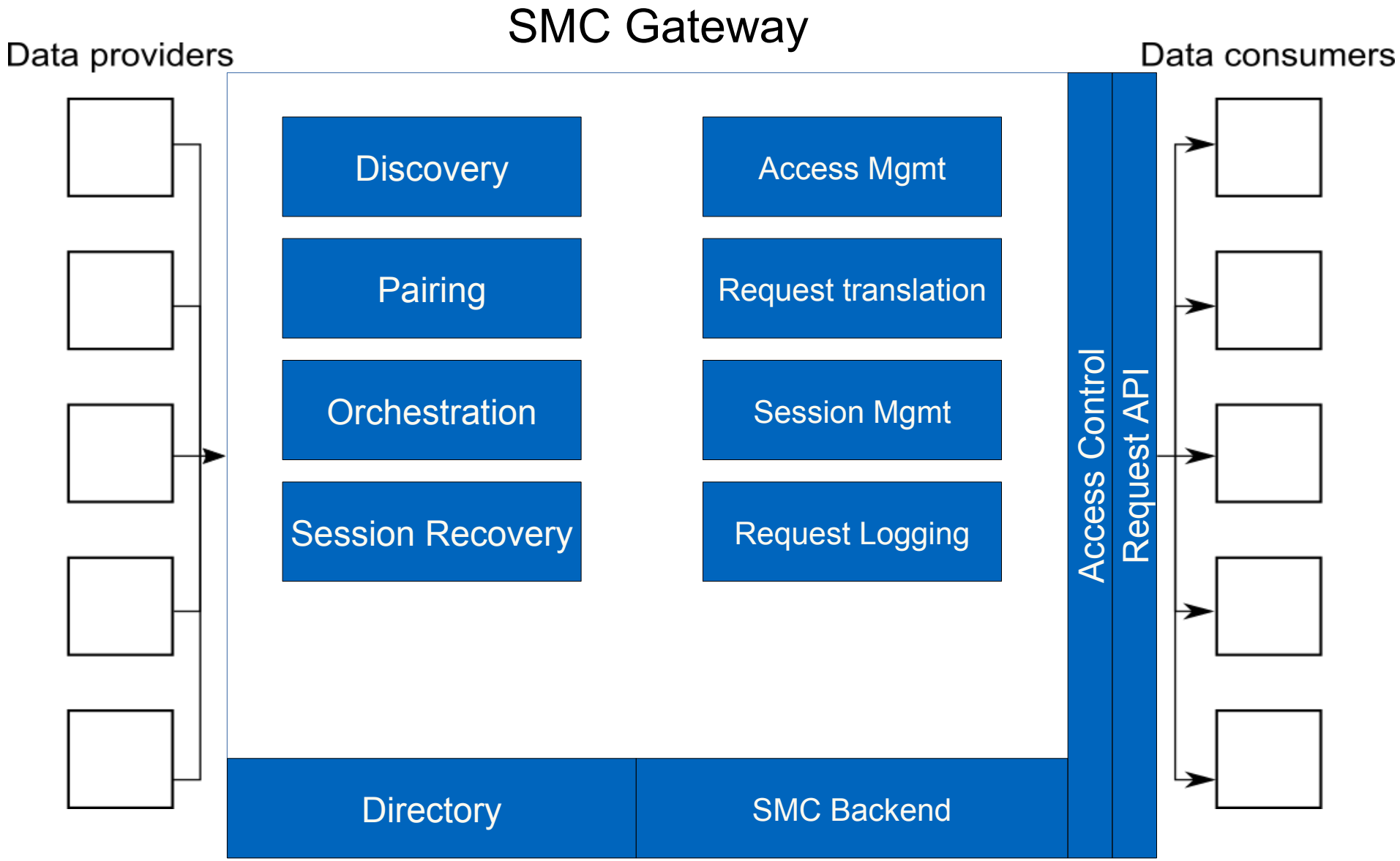


- Bonjour / Zeroconf
- Find GW with matching properties / responsibility
- Match capabilities
- x509 certs commissioning
- Out-of-bound verification
- Request verification
- Preprocessing with selectors
- Synchronized start of SMC
- Check for problems
- (Signed) result sent to GW

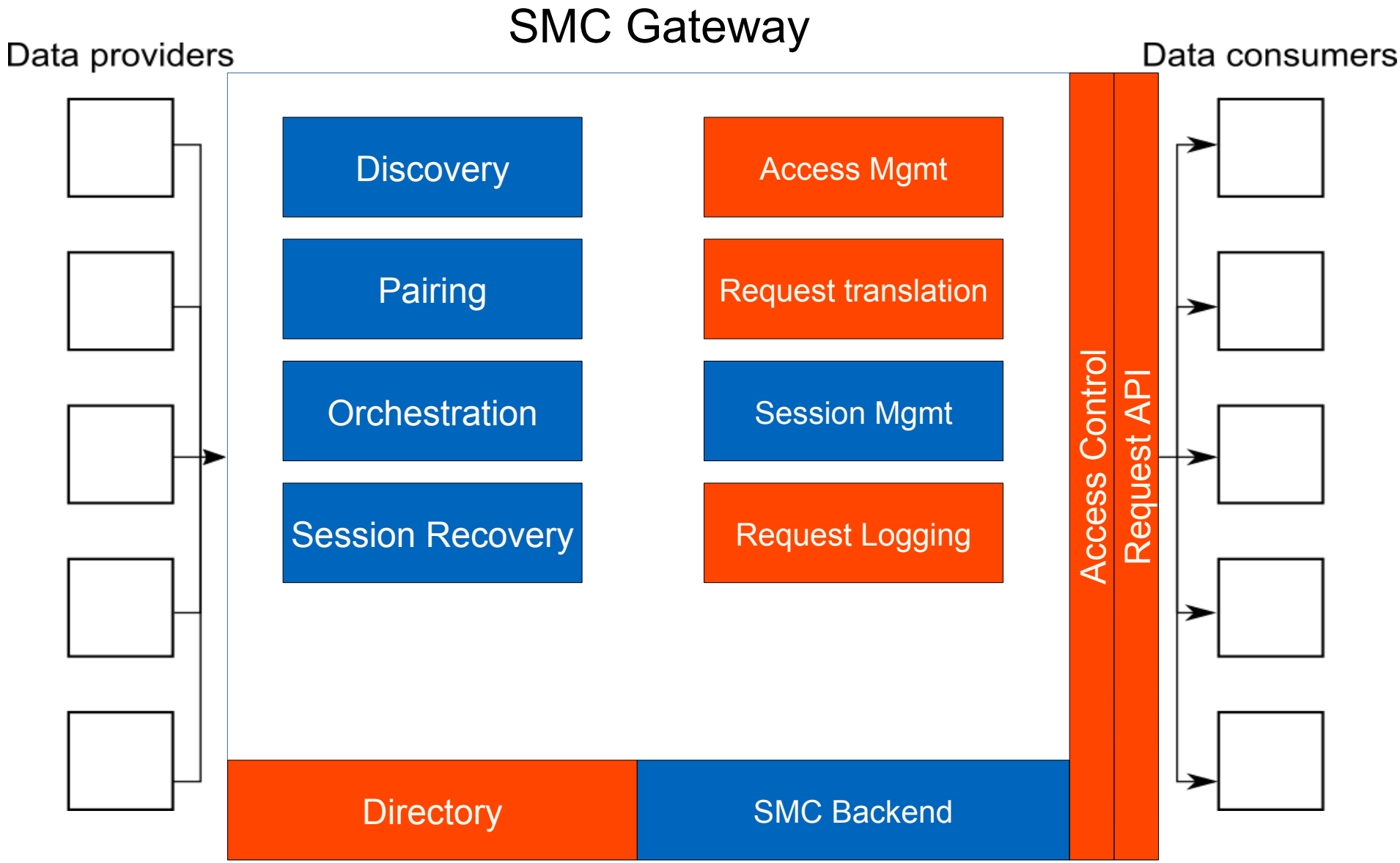


von Maltitz, M., Smarzly, S., Kinkelin, H., & Carle, G. (2018). A Management Framework for Secure Multiparty Computation in Dynamic Environments. To appear in Proceedings of NOMS 2018 -- IEEE/IFIP DOMINOS Workshop. Taipei, Taiwan.

Approach


SMC Gateway
Data providers
Data consumers
Discovery
Pairing
Orchestration
Session Recovery
Access Mgmt
Request translation
Session Mgmt
Request Logging
Access Control
Request API
Directory
SMC Backend

Approach


SMC Gateway
Data providers
Data consumers
Discovery
Pairing
Orchestration
Session Recovery
Access Mgmt
Request translation
Session Mgmt
Request Logging
Access Control
Request API
Directory
SMC Backend

Conclusion

Secure Multiparty Computation in the Internet of Things

- Promising approach
- Solves/mitigates several security and privacy problems in systems handling sensor data
- Challenges emerge from mismatch between SMC premises and properties of dynamic environments
- Convergence possible

Questions?