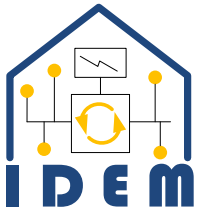


In**d**ividualisierbares **E**nergiecontrollingsystem
mit **M**andantenfähigkeit

The IDEM Project

Energy Management vs. Data Privacy

Cornelia Kappler (deZem)
Holger Kinkelin, **Marcel von Maltitz** (TUM)

21.05.2014

Bundesministerium für Bildung und Forschung
DLR Projektträger
dezem energy controlling
Technische Universität München
IMD

Agenda

- Motivation and Goals of the IDEM Project
  Cornelia Kappler, deZem

- Energy Management vs. Data Privacy
  Holger Kinkelin, Marcel v. Maltitz (TUM)

MOTIVATION AND GOALS

Project Overview

- BMBF-supported project in context of funding program „KMU-innovativ: Ressourcen- und Energieeffizienz“
- Supervised by DLR
- Duration from January 2014 – December 2015
- Partners:
  - deZem (leader)
  - TUM
  - Immobilien Management Duisburg

Motivation

- Energy is wasted because it is not known that it is actually being consumed! (**Intransparency**).
  - Saving potential up to 40% without loss of comfort

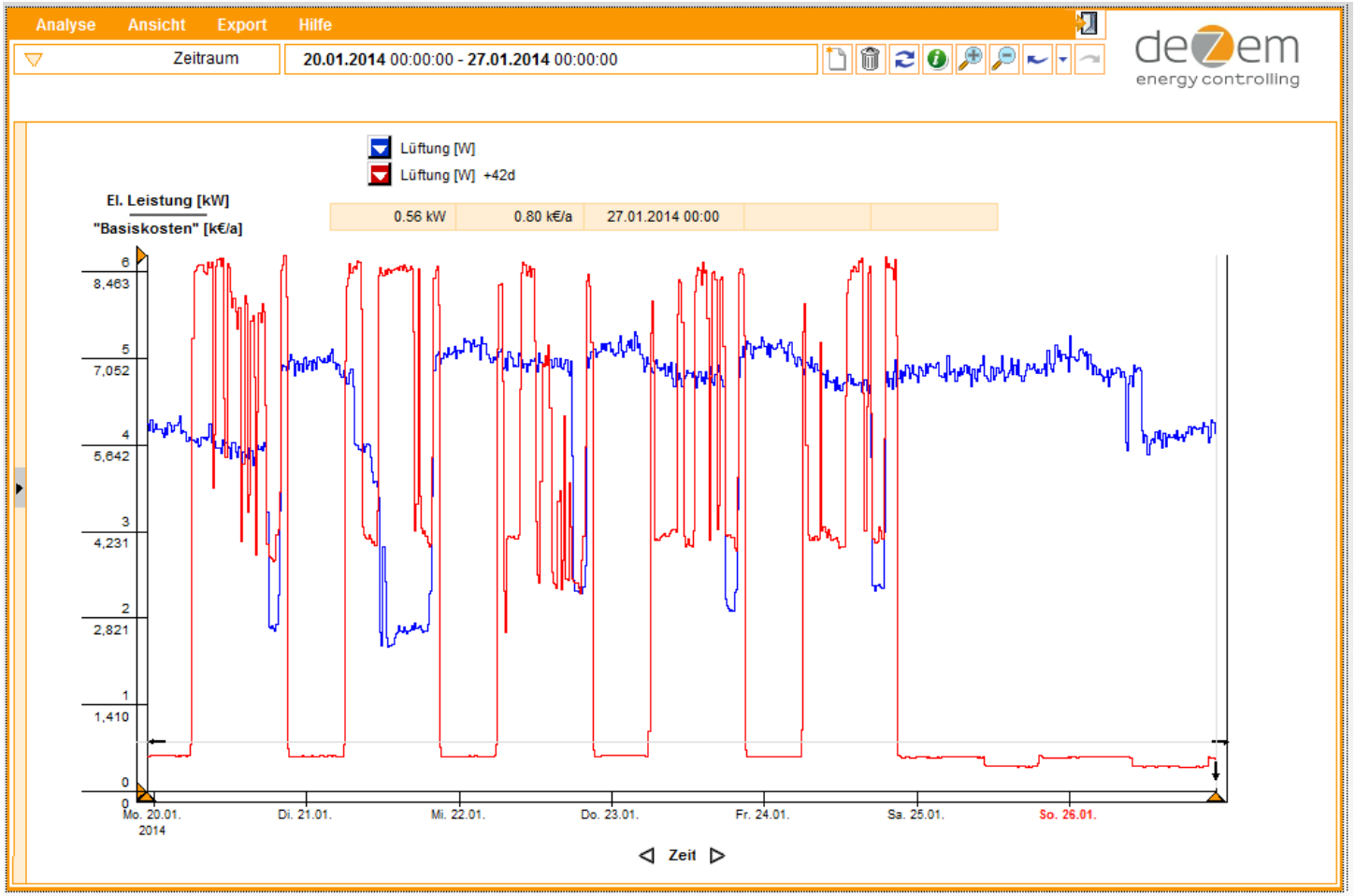
- Energy efficiency can be increased by
  - Measures requiring investment
    - New technology, insulation,...
  - Measures requiring no or low investment
    - Optimization of control settings
    - Educated user behaviour
    - Presence detection
    - ...

IDEM

- Only with monitoring, these potentials are reachable. (**Transparency**)

Motivation

- Example: Ventilation system in an office building „definitly only is active during working hours“...



Motivation

- Example: Ventilation system in an office building „definitly only is active during working hours“...

Zusammenfassung		
	Lüftung:	**Lüftung +42d :**
15' Min [Januar 2014]	(nicht verfügbar)	(nicht verfügbar)
15' Max [Januar 2014]	(nicht verfügbar)	(nicht verfügbar)
abs. Minimum (im Fenster)	1,66 kW [21.01.14 13:45]	273,44 W [09.03.14 19:30]
abs. Maximum (im Fenster)	5,30 kW [23.01.14 04:30]	6,18 kW [03.03.14 21:30]
Max. - Min. (im Fenster)	3,64 kW	5,91 kW
Integral (im Fenster)	747,48 kWh	367,49 kWh
Jahresintegral (extrapoliert)	39,00 MWh	19,17 MWh
Änderung (im Fenster)	-/-	-/-
Jahresänderung (extrapoliert)	-/-	-/-
Durchschnitt (im Fenster)	4,45 kW	2,19 kW
Änderung pro Stunde (im Fenster)	-/-	-/-
Kosten (im Fenster)	143,14 €	70,37 €
extrapolierte Jahreskosten	7,47 k€/a	3,67 k€/a

Savings by improved settings:

Motivation

- Energytransparency ist *necessary*...
- ....but not *sufficient* for reducing energy consumption, because...
  - ...the actual user is not reached
  - ...the user does not feel responsible
  - ...the user doesn‘t know whether saving potentials exist
  - ...the user does not know what to do

- This is especially true in jointly used, „public“ rooms
  - Offices
  - Conference rooms
  - Gyms
  - ...

Motivation

- Energytransparency ist *necessary*..
- ....but not *sufficient* t... ducing e...
  because...
  - ...the actual use...
    - ...
    - ...the...
    - ...
  - This is... ...oms
    - Of...
    - ...ference ...
    - Gyms
    - ...

IDEM:

- **User feedback about energy consumption**
- **Automatic analysis of consumption**
- **Constructive proposals for user action**
- **Intelligent control of devices**

Motivation

- Energytransparency ist *necessary*..
- ....but not *sufficient* ...ducing e...
  because...
  - ...the actual use...
    - ...
    - ...the...
    - ...
  - This is...
    - Of...
    - ...ference ...
    - Gyms
    - ...

IDEM:

- **User feedback about energy consumption**
- **Automatic analysis of consumption**
- **Constructive proposals for user action**
- **Intelligent control of devices**

Test installation and Living Lab at TUM and IMD (gyms in Duisburg)

IDEM Core Ideas

- Idea 1:
  - Sharing rooms and infrastructure is resource efficient
    - Meeting rooms
    - School gyms
    - Printers
  - Energy costs are accounted according to the actual usage.
    - No „Umlage“ (static cost apportitioning)
- Idea 2:
  - IDEM system monitors the environment
  - Gives feedback when needed, e.g.
    - Last user leaves but light is still on -> feedback „please switch off lights“

ENERGY MANAGEMENT VS. DATA PRIVACY

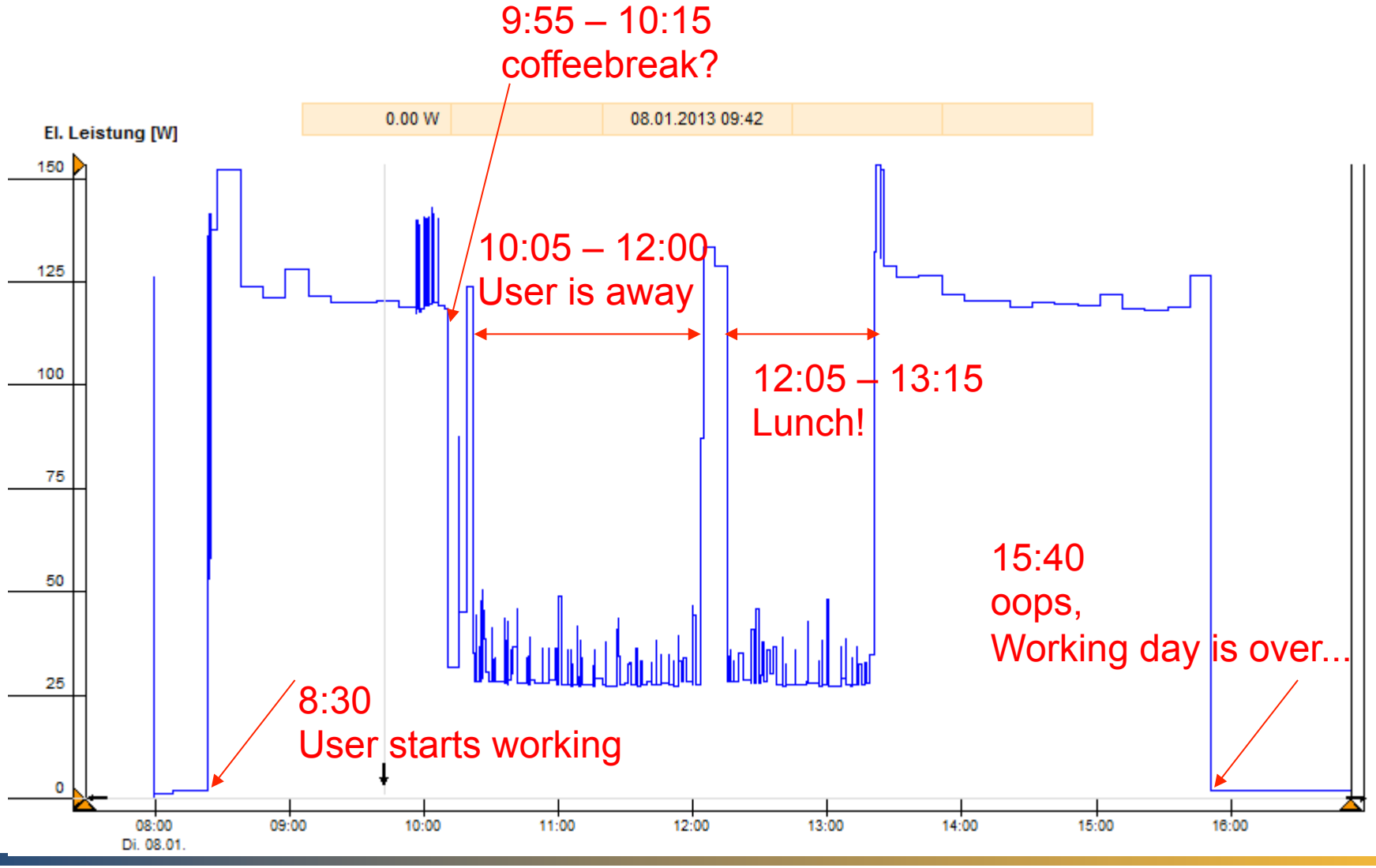
IDEM vs. Privacy

- Let us repeat:
  - IDEM measures, processes and logs vast amounts of energy consumption data.
  - Data is recorded in high temporal and spatial resolution.
    - E.g.: System outputs energy consumption data within one room each second

    ➔We know exactly how much energy is spent at which place

Example of real graph measured by deZem system

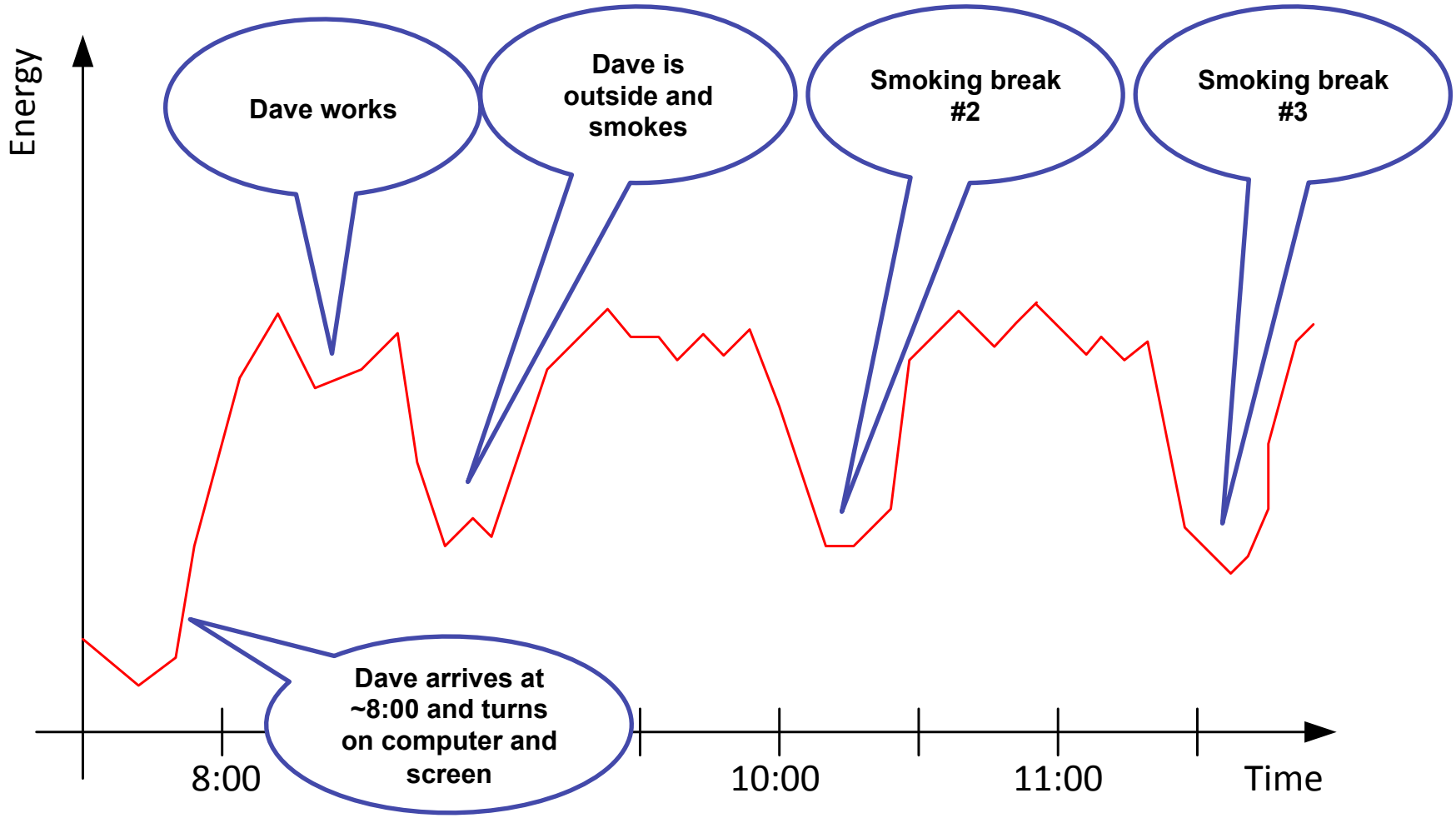
- Usage profile of a PC + Monitor (screen goes off after 10 min.)



Simplified (Worst Case) Example Scenario

- Dave works in his own office.
- The office is monitored by IDEM.
- Dave‘s computer disables the screen when inactive for 3 minutes.
- Dave is a strong smoker.

The Energy Log of Dave's Office



Dave is in Trouble

- From this graph Dave‘s boss learned that
  - Dave arrived late today.
  - Dave interrupts his work every hour to smoke.
  - Dave spends about 7 minutes away from his desk every time.
  - Dave didn‘t work for about 45 minutes this day.
  - The energy monitoring log of the past 3 months show the same behavior.

- Dave is in trouble and receives a written warning.

These events and people are fictional and any resemblance to person living or dead is purely coincidental.

- What do data protection laws mean for a project like IDEM?

Definition of Personal Data

- According to the European Data Protection Directive personal data is defined as

- *“[…] any information relating to an identified or identifiable natural person ('data subject’)”*
- *“An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity “*

Source: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

How to protect Personal Data? (§9 BDSG)

- Public and non-public organizations, which collect personal data […] have to meet the technical and organizational measures that are necessary for the execution of the provisions of this law, especially of those requirements named in the addendum to this law…

- *"Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

§9 BDSG (Addendum)

1) Enforce physical access control to data processing devices (dt.: Zutrittskontrolle).
2) Prevent data access of unauthorized persons (dt.: Zugangskontrolle).
3) Provide fine grained access control (dt.: Zugriffskontrolle).
4) Ensure data confidentiality during transport and processing, and when data is stored.
5) Provide logging mechanisms for data processing.
6) Guarantee that data is processed in the intended way.
7) Guarantee that data can not be destroyed.
8) Guarantee that data sets of different types can not be merged.

(Translated from German; Requirements of European law, OECD, etc. are quite similar)

Implementing the Requirements I

2) Prevent data access of unauthorized persons

3) Provide fine grained access control

- Intention:
  - Prevent 3rd parties from accessing data
- Typically enforced by:
  - Authentication mechanism (e.g. username/password, asymmetric cryptography, …)
  - Subsequent authorization (Access control lists, policies, …)
- State of the Art

Implementing the Requirements II

4) Ensure data confidentiality during transport and processing, and when data is stored.

- Typically implemented using:
  - Symmetric cryptography; works well if key is strong and secret
- Intention:
  - Prevent 3rd parties from eavesdropping information
- State of the Art

Implementing the Requirements III

6) Guarantee that data is processed in the intended way.

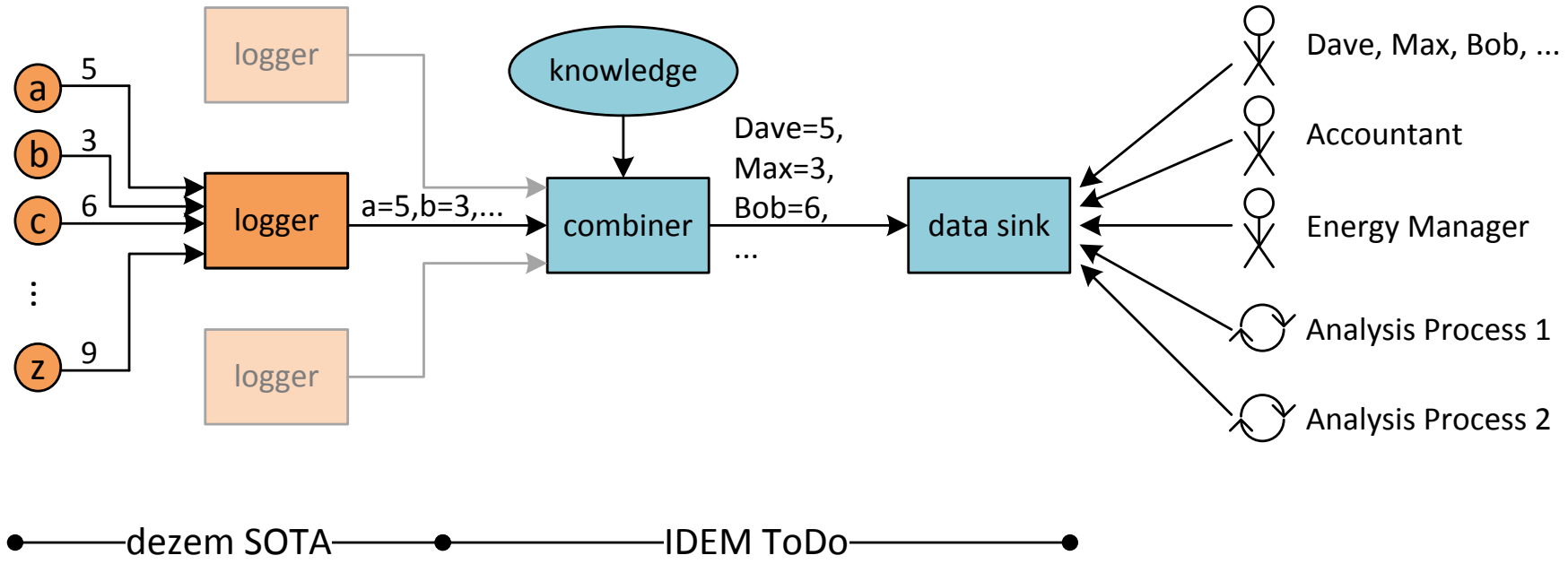
8) Guarantee that data sets of different types can not be merged

- Intention:
  - Different than before!
  - System operator may use data for specific purposes only!

- Can be realized by a system architecture that obeys *privacy by design* rules

➔ Important goal of IDEM

High-Level IDEM Architecture



- Logger sends a stream of measurement values to Combiner
- Combiner enriches data with additional knowledge
  - data becomes richer; it becomes personal data
- Data is stored at a data sink and accessed by different entities

Different Users need different Rights

- Dave, Max, Bob are „ordinary“ users.
  - May access their own data in the highest granularity
  - May not access other user‘s data
- Energy Manager
  - Must see data of all individuals in high granularity
    - otherwise cannot work efficiently
- Accountant
  - May see how much energy was spent in sum in a time slot.
  - May not see personal consumption data
- Rights of processes depend on their purpose
  - Processes might need data in high granularity

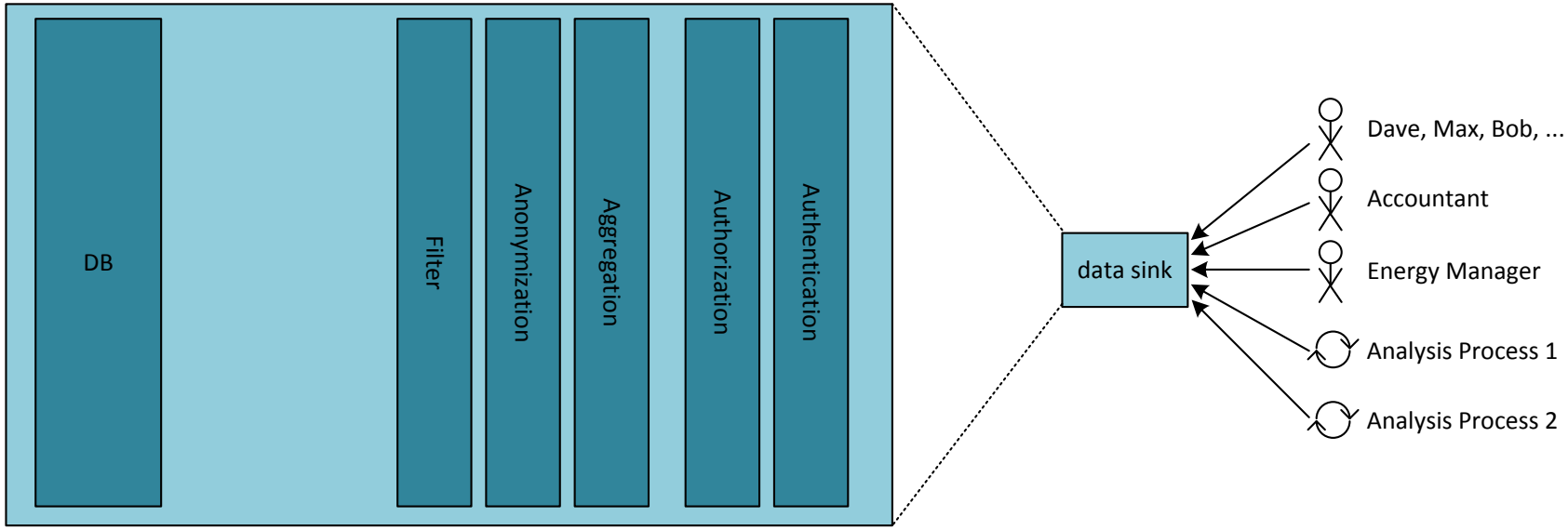
Synthesis

- We can not simply apply some „de-personalization“ function, store the data and are done!
  - E.g. aggregate data of different users

  → good for privacy

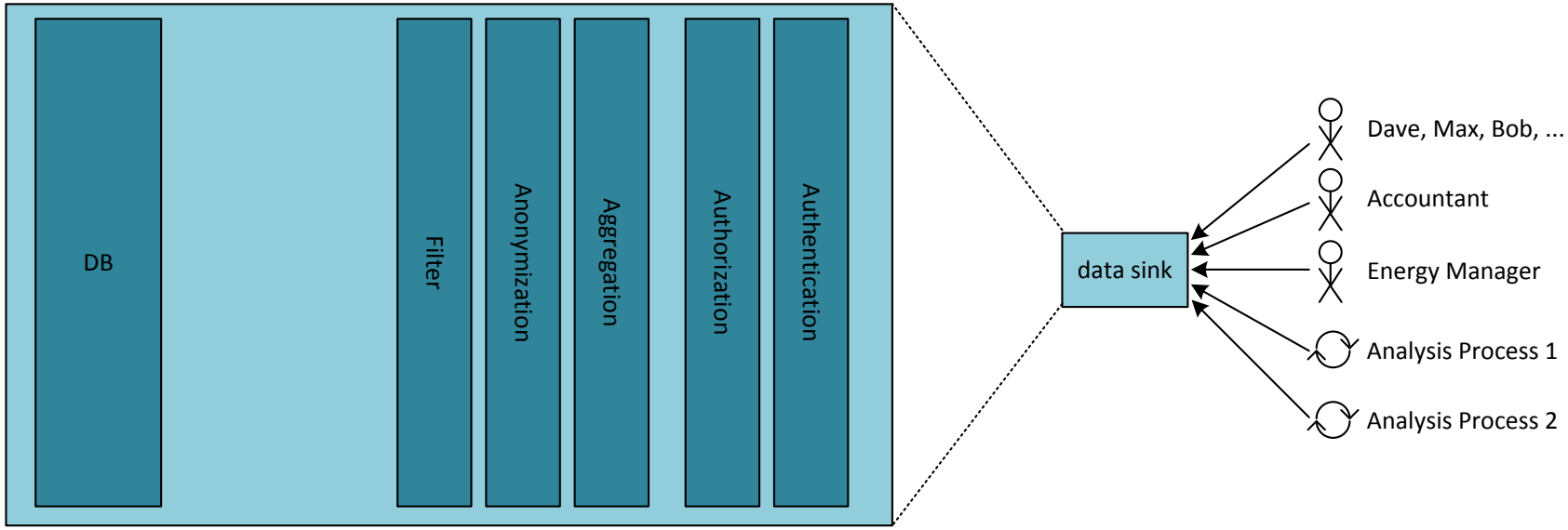
  → bad for data analysis
- We need different “views” on the same data
- Let us discuss some IDEM design options, their pros and cons:
  - Conventional System Design + Central Data Sink
  - Crypto + Independent Data Sinks
  - Attribute Based Crypto + Central Data Sink

Conventional System Design



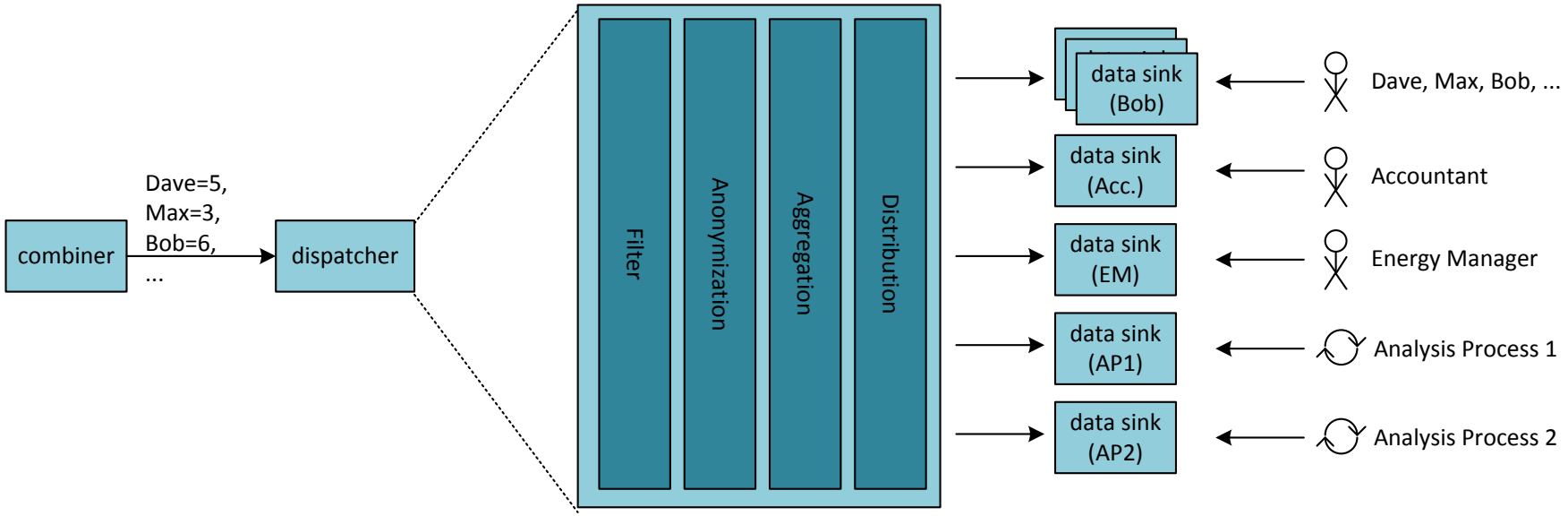
- After user authentication/authorization data can be accessed.
  - Owners of data have direct access
  - For other users data can be „un-personalized“ on-the-fly by different functions such as
    - Aggregation, anonymisation, filtering, …

Properties



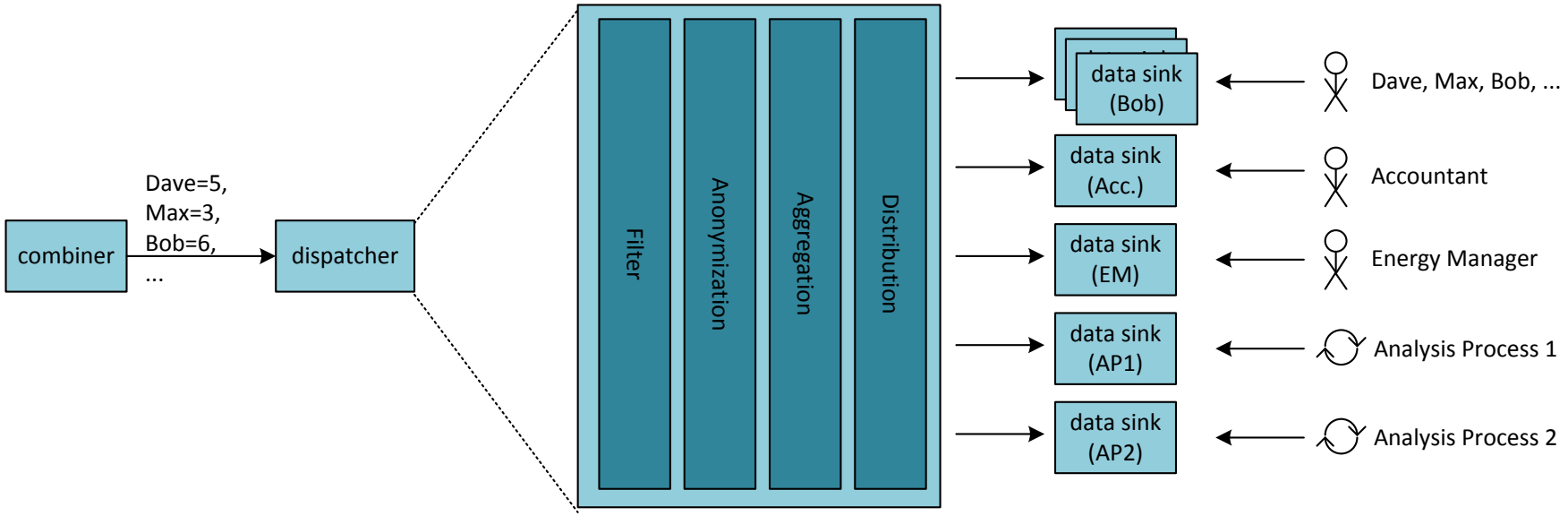
+ Simple
+ No overhead
- Central database holds all information
  - → When data sink is compromised, attacker has access to past and present data
  - → Single point of attack

Design with Independent Data Sinks



- After combination, data is piped through a Dispatcher.
- Dispatcher applies similar de-personalization functions to incoming data as seen before.
- Data is stored at independent data sinks (small devices, VMs, etc.) accessible only by their owners (individual encryption)
  - Data is replicated when necessary

Properties



+ Redundancy protects against loss of data
+ No single point of attack on stored data possible
+ Attacks are made more difficult
- Redundancy costs additional space, bandwidth, processing power
- Overhead for distributed system
- Redundancy causes loss of control over distributed data

Excursion: Attribute Based Encryption

- Problem with conventional cryptographic tools
  - IDEM encrypts data for Dave with Dave‘s public key
  - Dave decrypts data with his private key
  - IDEM encrypts data for Max with Max‘s public key
  - Max decrypts data with his private key
  - ...
- For n IDEM users
  - n trusted public keys are needed
  - Recipients of data need to be known a priori
  - n encryption processes

Solution with Attribute Based Encryption

- IDEM encrypts data with an ABE public key and encodes an Access Policy into the Ciphertext:

```
Policy:Name=Dave|Function=EnergyManager
```

- Some participants own ABE private keys that include specific attributes of the key holder
- Mary‘s private key holds attributes

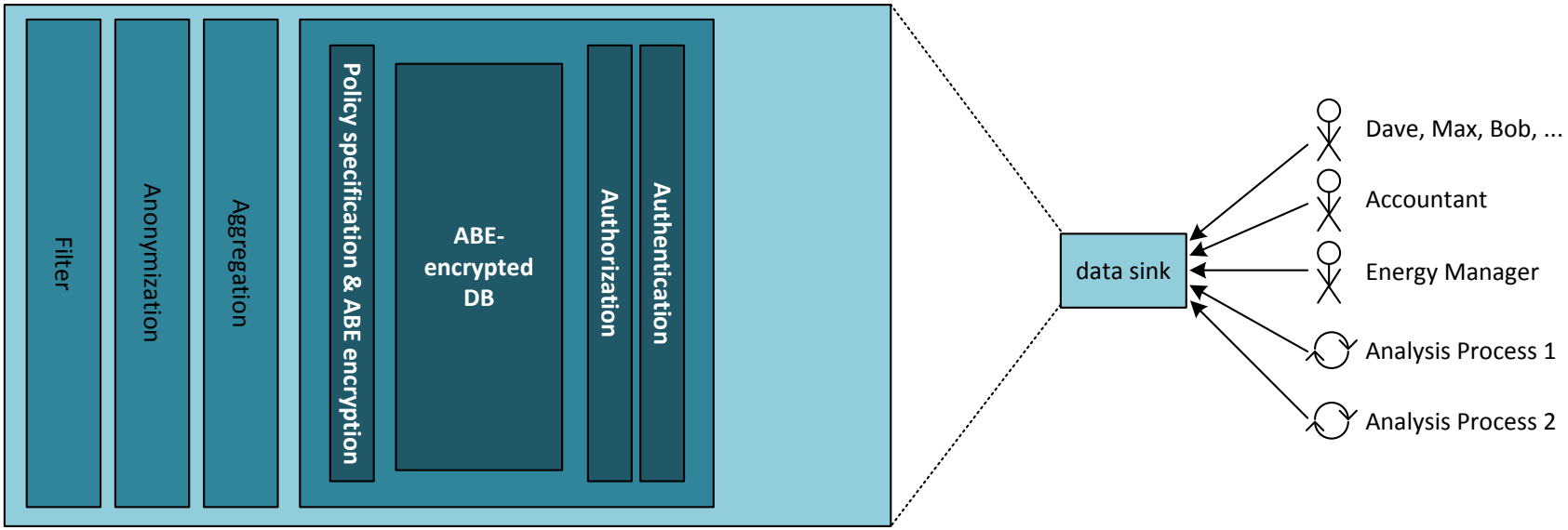
```
Attribute:Name=Mary;Function=EnergyManager
```

- Mary may decrypt above data as she owns the right *function* attribute
- The Accountant’s private key holds attributes

```
Attribute:Name=Alfred;Function=Accountant
```

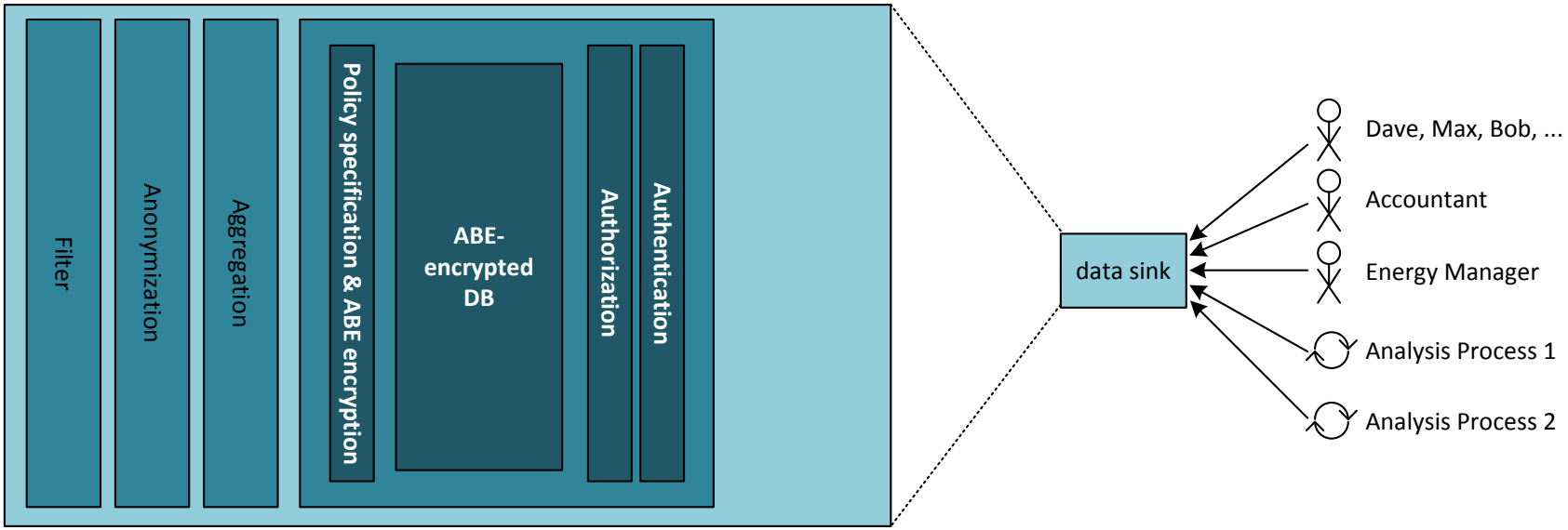
- The Accountant may not decrypt above data as no attribute matches

Application to IDEM



- After combination data is encrypted using ABE with correct access policies
- Data for users such as Accountant, Energy Manager might be de-personalized before encrypted storage

Properties



+ Only legitimate entities can access
  → ABE makes separate access control unnecessary
+ Overhead of managing a distributed system is reduced
+ Avoids unnecessary redundancy
+ When compromised only present data can be eavesdropped

Conclusion

- Privacy regulations and energy monitoring contradict.
- Tradeoff between privacy protection and volume and fine granularity of personal data
- Further goals:
  - Investigate outlined ideas in greater detail → we are at the beginning
  - Find optimal/balanced solution between privacy and functionality

Questions?

Thank you for the audience.

Questions?

http://www.idem-project.de

Use Cases “Adaptive Feedback”

1.	Classify Situation
Description	The System assigns upon request or automatically a predefined Situation to the consumption pattern of a room, based on the Metering Values of potentially all Metering Points installed in the Room.
Result	The Situation of the Room is stored in the System, e.g. as a time-dependent Metadatum.

- Recognize “situation”, e.g.

  user coming / user expected but not present / user leaving...

2.	Analyse Situation
Description	The System analyses whether the current consumption / status of a Metering Point in the Room is adequate for the Situation. This can Use Case can be performed automatically for the present Situation or triggered by a User for the present or past Situations.
Result	The System uses the result as input to further Use Cases. The System may also inform the User whether the current consumption / status is adequate for the Situation.

- Consumption adequate for situation?
  e.g. “user leaving” => lights should be off

3.	Make recommendation
Description	The System uses the result of Use Case "Analyze Situation" to look up and present a recommendation, e.g. "Please close window in Room XY". When several recommendations exist for the Situation, the System considers the rating of each recommendation and may present only the best ones.
Result	The System recommends an action to the User. It may also offer the User to execute the action (see Use Cases for Autonomic Control)

- Lights are still on => recommendation “Please switch off the lights”

Can Users ever Trust a System?

- Important problem:
  - Users of a system must be convinced that the system that processes their data respects their privacy
- Possible solution: Independent privacy expert audits code and design of data processing system
- A certificate might be issued that system is privacy preserving.
- But:
  - How do users know that the certified „trusty“ system is used?
  - Audits are Expensive! How to deal with updates?
- Important problem, but no focus of IDEM