Scalable, trusted, and interoperable platform for secured smart grid

Sealed GRID

Pilot Progress & Results

Prof. Christos Xenakis
University of Piraeus Research Center

IoT Week, June 2022

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 777996.

SealedGRID's **MISSION**:

Develop and implement a **Scalable**, **Trusted**, and **Interoperable** platform for a **Secured Smart Grid**

The project

UNIVERSITY OF PIRAEUS

UNIVERSIDAD DE MÁLAGA

Beia CONSULT INTERNATIONAL

NEUROsoft

FOGUS INNOVATIONS & SERVICES

cnit

European Commission

Horizon 2020
European Union funding
for Research & Innovation

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 777996.

Work Packages Outline

- ✓ – **Requirements, Business Cases and Architecture (WP2)**
  - → Architecture Components
- ✓ – **Key Management and Authentication (WP3)**
  - → WoT (SOMA-MENSA)
  - → BLOCKCHAIN (DHT, Chord)
- ✓ – **Trusted Computing and Privacy Protection (WP4)**
  - → TEE
  - → MASKER
- ✓ – **Authorization and Security Interoperability (WP5)**
  - → Access Control Policy (ACP)
  - → Open ID Connect (OIDC)
  - → Opinion Dynamics (ODYN)
- IN PROGRESS – **Platform Integration and Assessment Experiments (WP6)**
  - → Prototype Architecture
  - → VMs / Scenarios

Architecture Components 1/3

- **SealedGRID Components**
  - **Smart Meters (SM)**

    →**Collect** electricity consumption readings.
  - **Aggregators**

    →**Intermediate nodes** between the **collector** and the **smart meters**

    →**Sum the individual readings** received by the SMs of a neiborhood

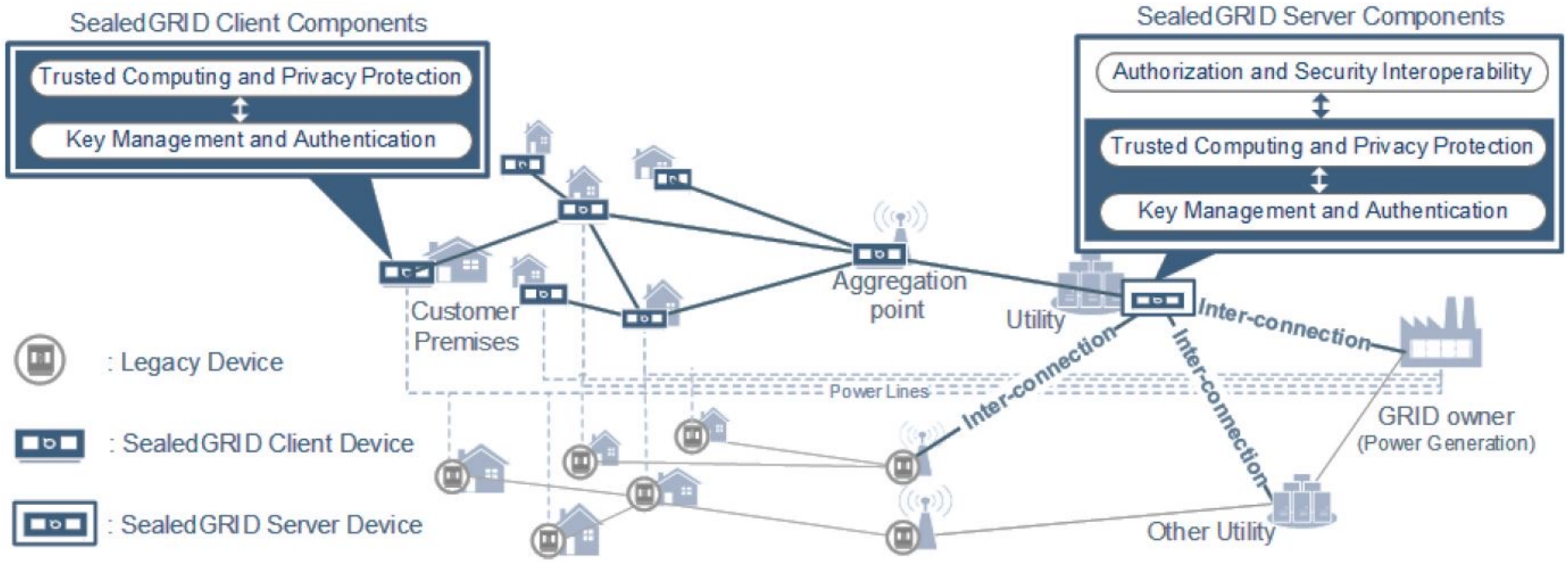
    →**Transmits** the result to the Utility.
  - **Utility**

    →Produces the **energy**

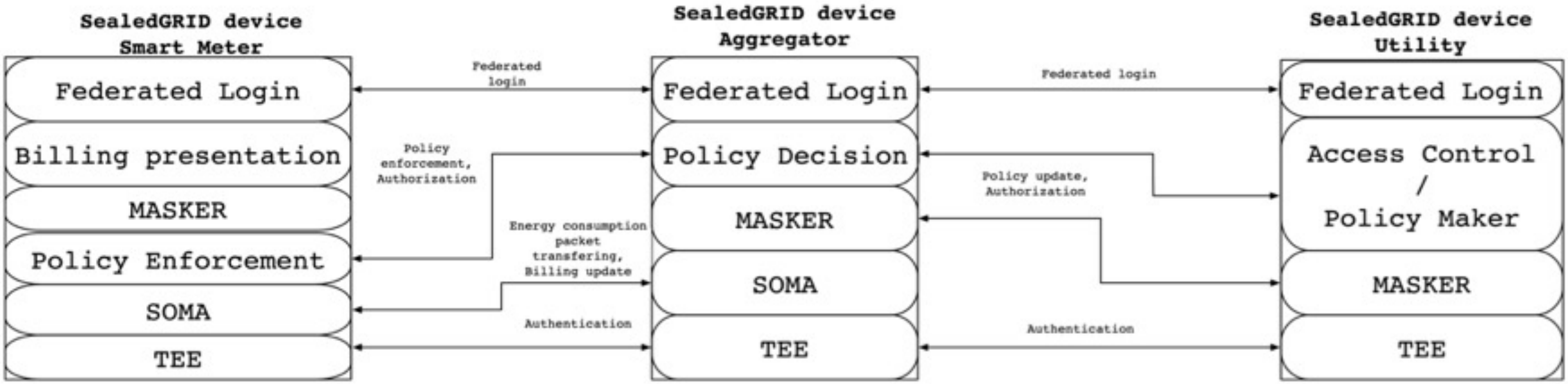
    →Calculates the **final billing**

Architecture Components 2/3

A scalable, highly trusted, and interoperable Smart Grid security platform.



Architecture Components 3/3



Authentication and key management

– **Authentication** and **Key management** in the SG.

→It is based on **digital certificates**

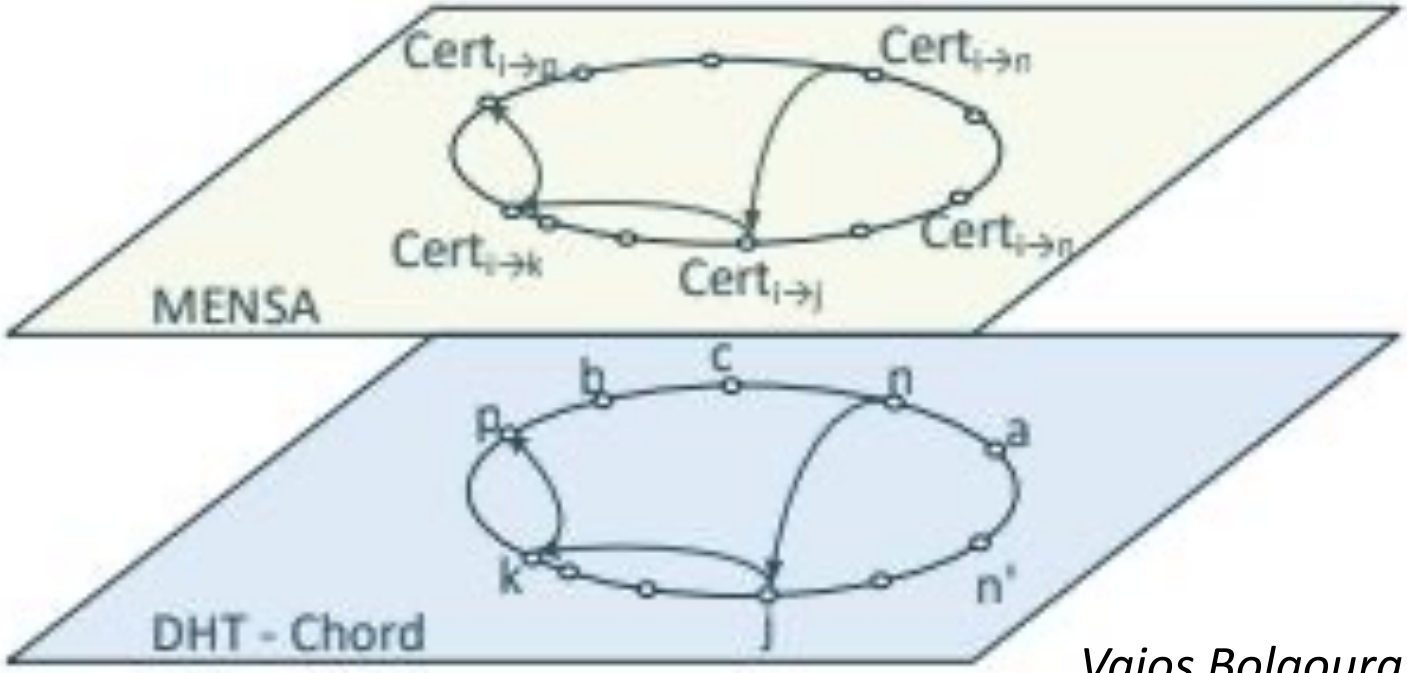
→It supports **decentralized** creation, distribution, exchange and revocation of certificates **(D3.1)**

1. **Web of Trust** (MENSA, DHT, Chord) **(D3.1)**
   - It integrates WoT characteristics for decentralizing the authentication process **(D3.2**
2. **Blockchain technology** **(D3.2)**
   - It is built using the Hyperledger Fabric **(D3.2)**

MENSA: Authentication and key management 2/5

- **First distributed, hybrid authentication and key management system** for microgrids
- **Eliminates** the need for **a TTP**, while ensures **high availability**
- Uses **DHT** for **discovery of trust relationships** among the microgrid nodes
- It is a **decentralized** and **flexible** solution that promotes **scalability** and **resilience**
- It allows **frequent** “Join” and/or “Leave” actions without network efficiency impact
- **No single point of failure** due to decentralized nature

Key Management 3/5



Operations that take place

- **Node join**
- **Normal Operation**
- **Certificate Revocation**
- **Trusted Execution Environment**
- **Node Leave**

Vaios Bolgouras, Christoforos Ntantogian, Emmanouil Panaousis, Christos Xenakis, " Distributed Key Management in Microgrids ," IEEE Transactions on Industrial Informatics, Vol. 16, No. 3, pp: 2125-2133, Mar. 2020.

Evaluation Results

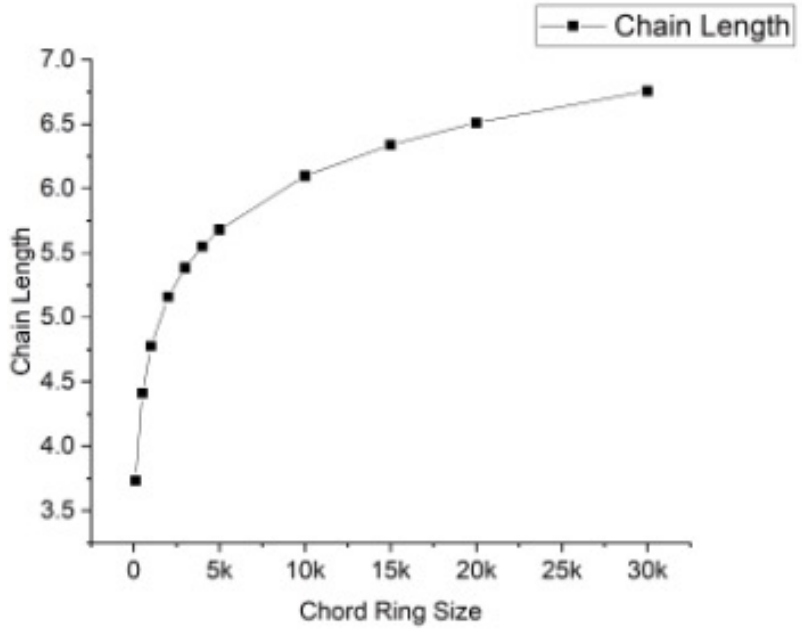
Node **Join time delay**

- For 0 – 5.000 nodes the **delay is 1.55 sec**
- While from 20.000 – 30.000 the **delay is 2.2 sec**

N	fingerTable size
500	8
5,000	12
15,000	13
30,000	14
.	
.	
5,000,000	22

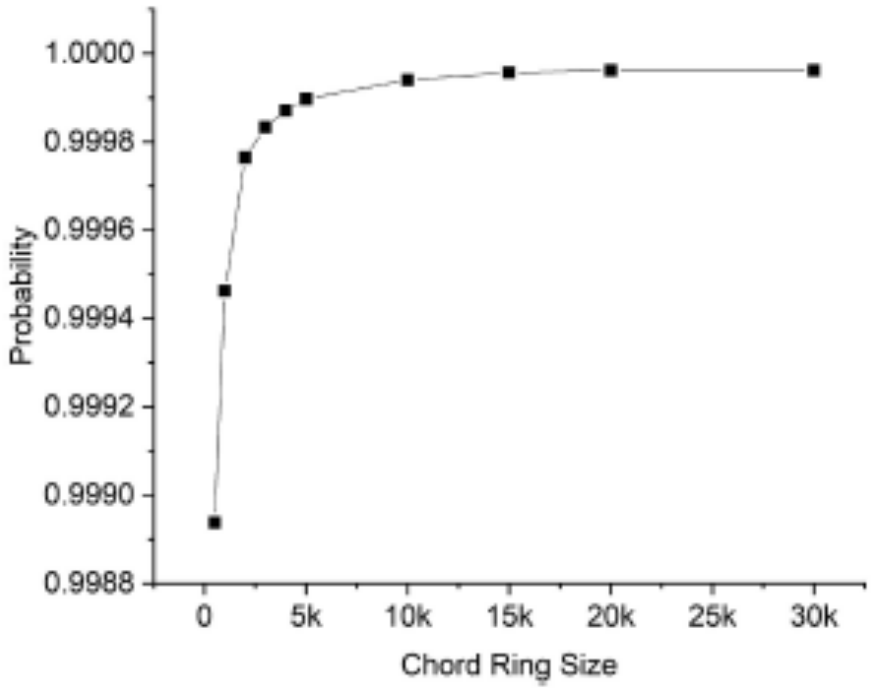
Chain Length

- Ordered list of certificates starting from the node initiating a look-up operation up to the target node
- **Mean length of the chain of trust**
- It includes the initiator & the target node

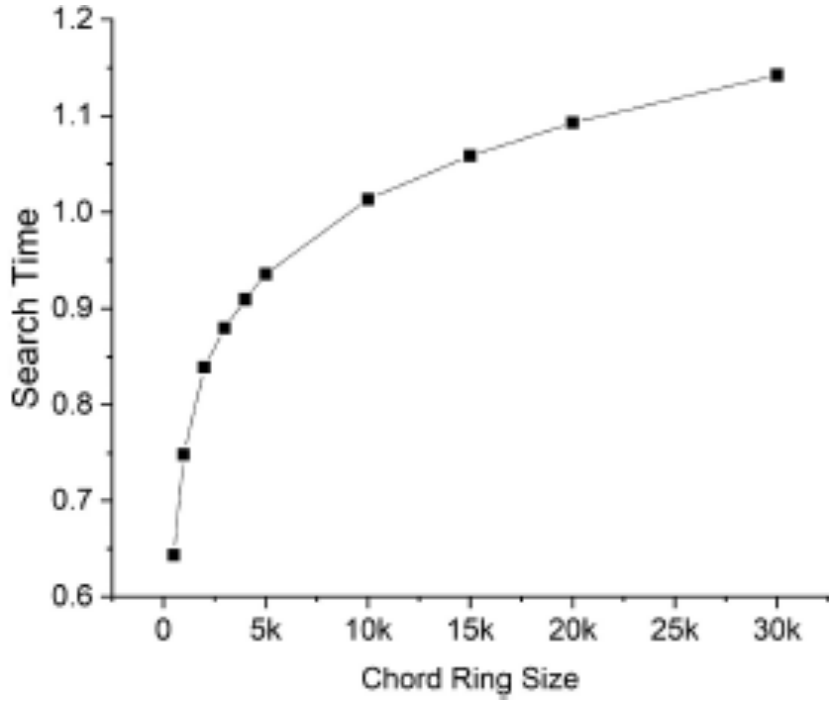


Evaluation Results

The **probability** that **two random nodes** will be able to **establish trust relationship** between them



Average time needed for a random node to establish **trust relationships** with another random node



Trusted computing and privacy protection

– **Trusted computing** and **privacy protection** in the SG

SECURITY BY DESIGN

→A **hardware root-of-trust** mechanism based **Trusted Execution Platform** (TEE) **(D4.1)** ✓

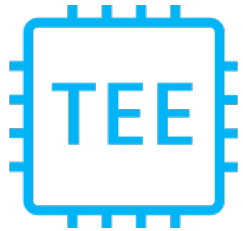
→A **remote attestation mechanism** that allows devices to generate proof that their current state is **trustworthy** **(D4.1)** ✓

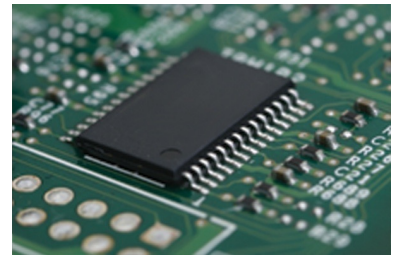
→A privacy protection mechanism for metering results implemented in TEE **(D4.2)**

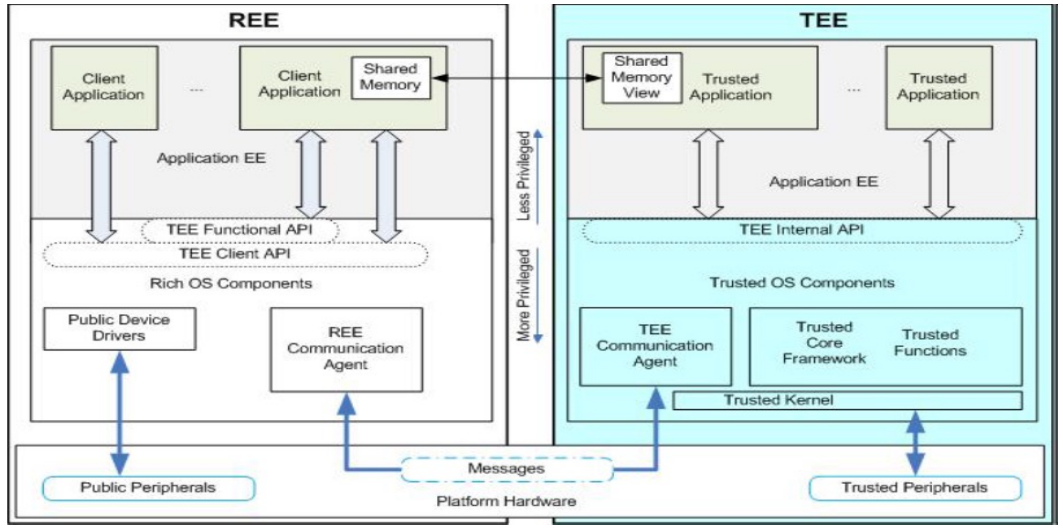
IN PROGRESS

Trusted computing 1/4

- **TEE**
  - Cryptographic Storage.
  - Remote Attestation Mechanism.
  - Generates and securely stores cryptographic keys.
  - Generates random numbers.
  - Executes cryptographic operations.
  - Securely stores certificates.
  - Confidentiality.
  - Integrity.



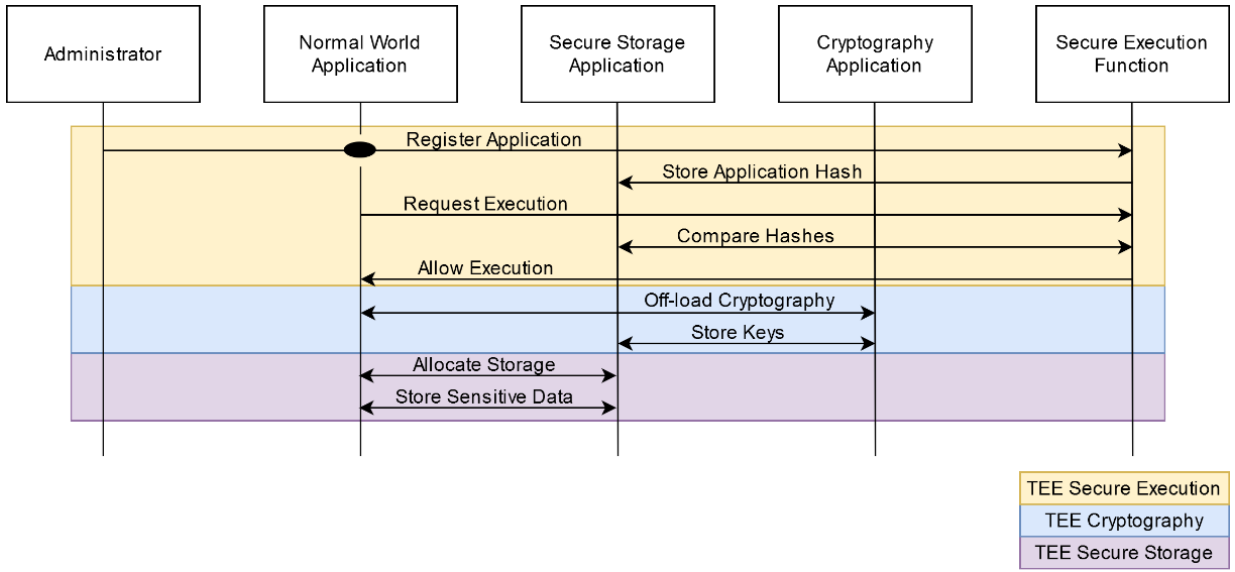




- ✓**OpTEE** is used to implement the **SealedGRID's** sensitive / security-critical functionality.
- ✓The measured speed **is more than enough** to instantly push and pull data from the TEE storage.
- ✓Performance in the order of microseconds

Implementation

- **Cryptography Component**
  - Key Generation
  - Encryption / Decryption
  - Hash
  - Sign / Verify
- **Secure Storage Component**
  - Store Data in the Secure Storage
  - Pull Data



- **Binary Verification Component**

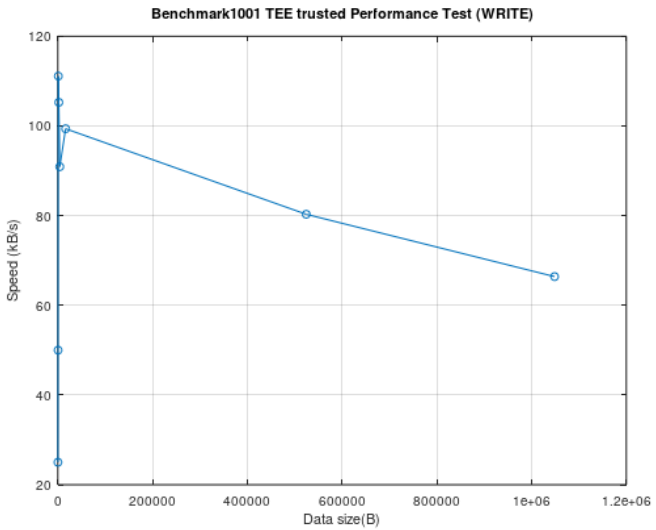
  Enrol Binary

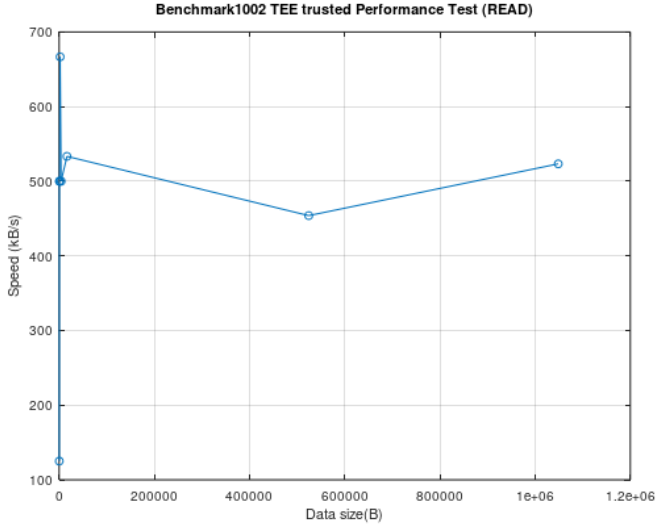
  Verify Binary

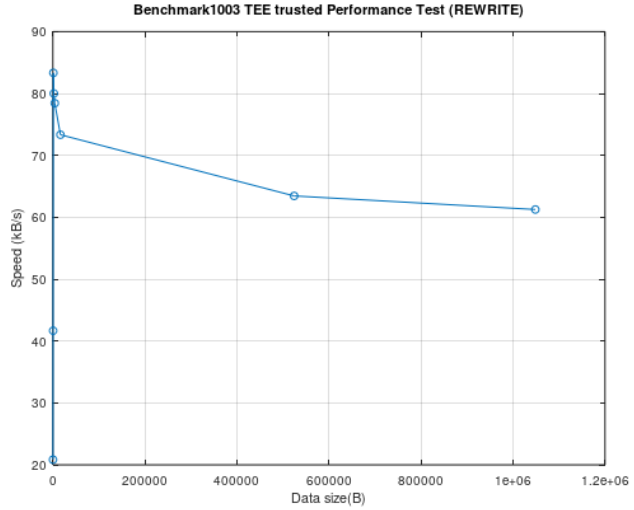
Evaluation- Results

Performance Tests:

- TEE Trusted Storage
  - Write
  - Read
  - Rewrite
- TEE SHA Performance test (SHA1 & SHA256)
- TEE AES Performance test (ECB, CBC)
- Regression Testing





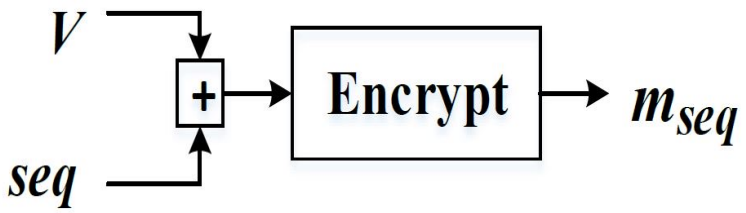


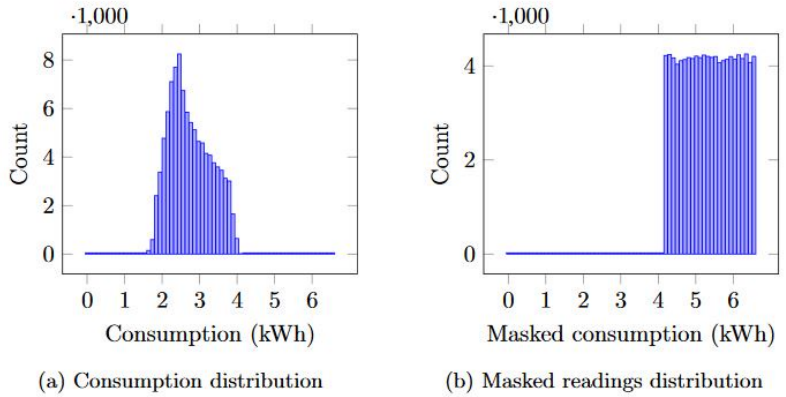
min (us)	max (us)	mean (us)	stddev (us)
586.144	5042.05	729.587	105.52

SHA1 Execution Times - Minimum, Maximum, Mean and Standard Deviation

MASKER: Privacy protection 1/2

- Privacy-preserving aggregation implemented in TEE
- Real-time billing and energy consumption.
- Facilitates Demand Response.
- SMs share **masked values** with the Utility **obfuscating** real consumption readings.
- Aggregators can provide aggregated consumption by several SMs
- Utility **subtracts** the used masks from the total sum, resulting in the real combined consumption.





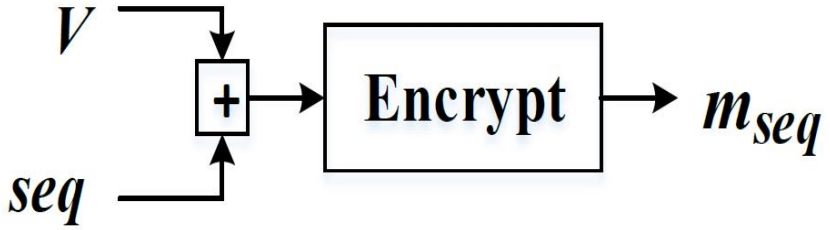
(a) Consumption distribution (b) Masked readings distribution

Privacy protection 2/2

- **MASKER – Evaluation Testing**

  3 Tests

  - 1st Test: A network with 25 nodes in total
    (20 smart meters, 4 Aggregators, and 1 Utility. Therefore, there is 1 aggregator per 4 smart meters)
  - 2nd Test: A network with 55 nodes in total
    (50 smart meters, 4 Aggregators, and 1 Utility. Here, the smart meters are separated into 2 groups of 13 and 2 groups of 12. There is 1 aggregator per group)
  - 3rd Test: A network with 80 nodes in total
    75 smart meters, 4 Aggregators, and 1 Utility. The smart meters are separated into 3 groups of 19 and 1 group of 18 with 1 aggregator per group.



Metric Type	Device		
	Smart Meter	Aggregator	Utility
Top Peak Memory Consumption	2 MB	1 MB	3 MB
Top Average CPU Consumtion	16%	15.40%	15.20%
Worst Case Bandwidth Consumption (Traffic)	Total MAX: 5.85 Mbps		
Maximum Devices in network before system crash	10,240 Devices		

Authorization and security interoperability mechanisms

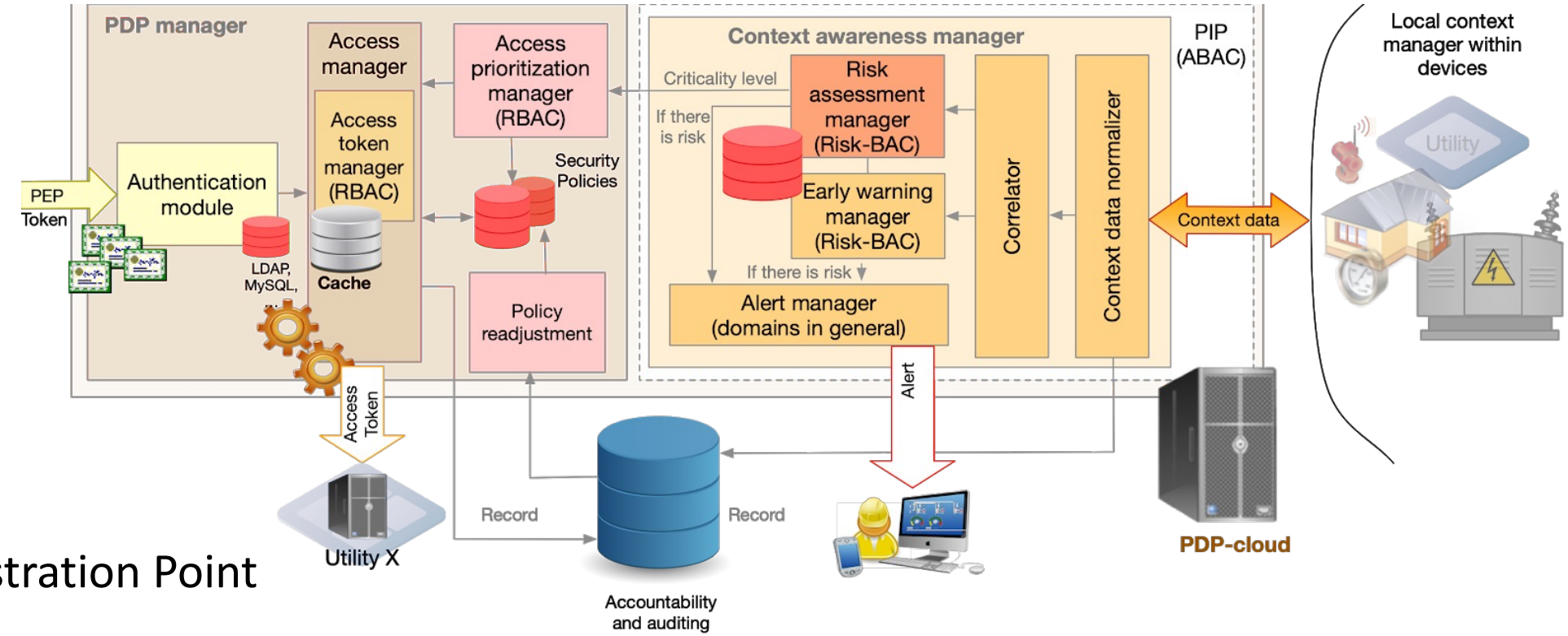
– **Authorization** and **security interoperability** mechanisms.

→**Hybrid access control policies** (ACP) based on RBAC & ABAC **(D5.1)**

→**SSO** for the **inter-connection** and **federation of multiple SG domains** using the **OpenID Connect** (OIDC) **(D5.2)**

→**Context-Aware Mechanism** to **validate access** and **translate the different security policies** to achieve **security interoperability** (ODyn) **(D5.2)**

Access Control Policies 1/2



Policy Points

- ✓PAP : Policy Administration Point
- ✓PDP : Policy Decision Point
- ✓PEP : Policy Enforcement Point
- ✓PIP : Policy Information Point

Access Control Policies 2/2

TESTBED Parameters

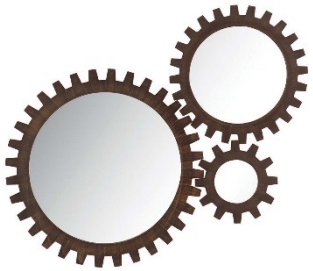
Entity	Setup
Smart Meter	-ARM Device, 4-core CPU at 1-1.2 GHz, 512MB RAM
Aggregator	-ARM Device, 4-core CPU at 1.2-1.4 GHz, 1GB RAM
Utility	-Intel Core i5-6500 CPU at 2 GHz 8 cores, 8GB RAM

Performance Results

# of nodes	Average CPU Utilization (%)			Average Memory Consumption (MB)			API response time (ms)		
	Smart meter	Aggregator	Utility	Smart meter	Aggregator	Utility	Smart meter	Aggregator	Utility
10	6.86	1.39	0.8	154.57	315.69	1455,42	162.85	71	38.62
50	6.68	6.87	3.43	154.71	327.29	1464,28	868.83	357.41	137.96
100	6.58	12.82	6.59	132.28	261.78	1481,81	4041.98	460.3	189.1
500	7.86	19.3	34.3	137.40	304.12	2033,95	6670.35	2529	1545.4

Security interoperability mechanisms 1/3

- **Federated Login**
  - Interoperability
  - Seamless communication among its components.
  - OpenID Connect (OIDC) and OAuth2.0
- **Opinion Dynamics** (ODyn)
  - Context-awareness mechanism
  - Retrieves data of the current state of the system in real-time.
  - Detects and traces APTs during their entire lifecycle



SealedGRID Authorization and security interoperability mechanisms 2/3

ODyn Evaluation Results

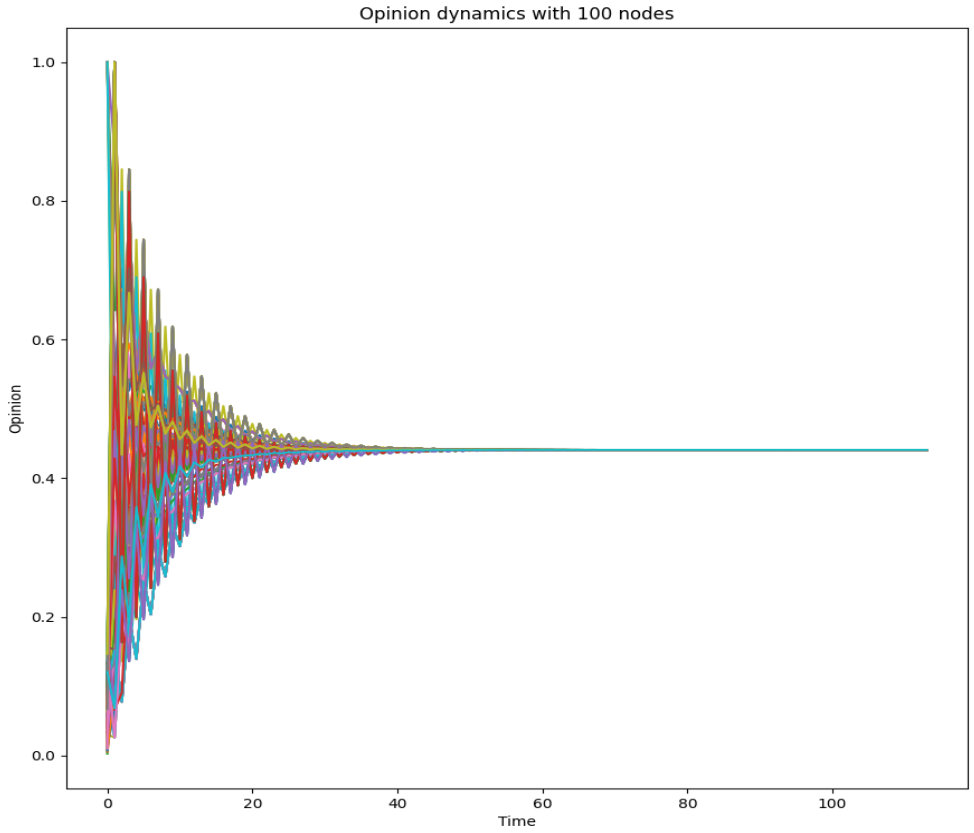
TESTBED Parameters

Entity	Setup
Smart Meter, Aggregator	-ARM Device single-core CPU at 700MHz, 512MB RAM (Download: 9.6 Mbps; Upload: 9 Mbps)
Utility	-Intel Core i5-6500 CPU at 3.2 GHz 4 cores, 8GB RAM (Download: 98 Mbps; Upload: 92 Mbps)

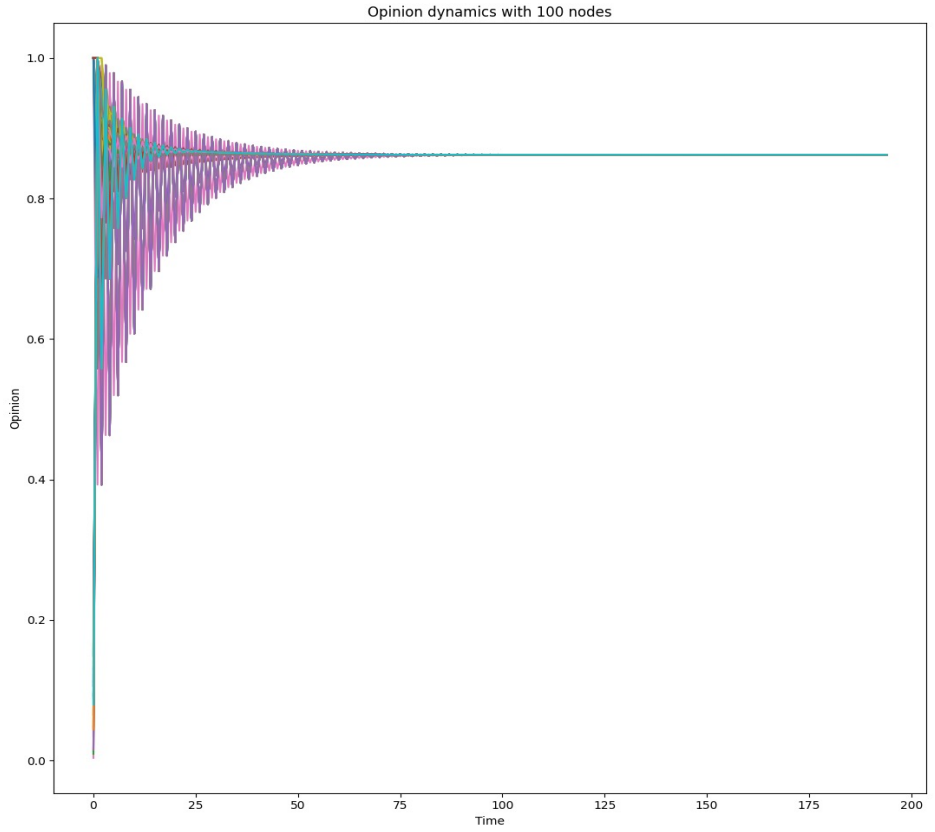
Performance Results

# of nodes	CPU Utilization (%)		Memory Consumption (%)		Network Usage	
	Smart meter, Aggregator	Utility	Smart meter, Aggregator	Utility	Smart meter, Aggregator	Utility
100	1.44	1.47	0.1	0.26	514Kb	51MB
500		18.07		0.9		255MB
1000		25		1.1		500MB

ODyn Evaluation Results



10 out of 100 nodes are infected



55 out of 100 nodes are infected

Platform Integration and Assessment Experiments 1/3

– **Platform Integration** and **Assessment Experiments**.

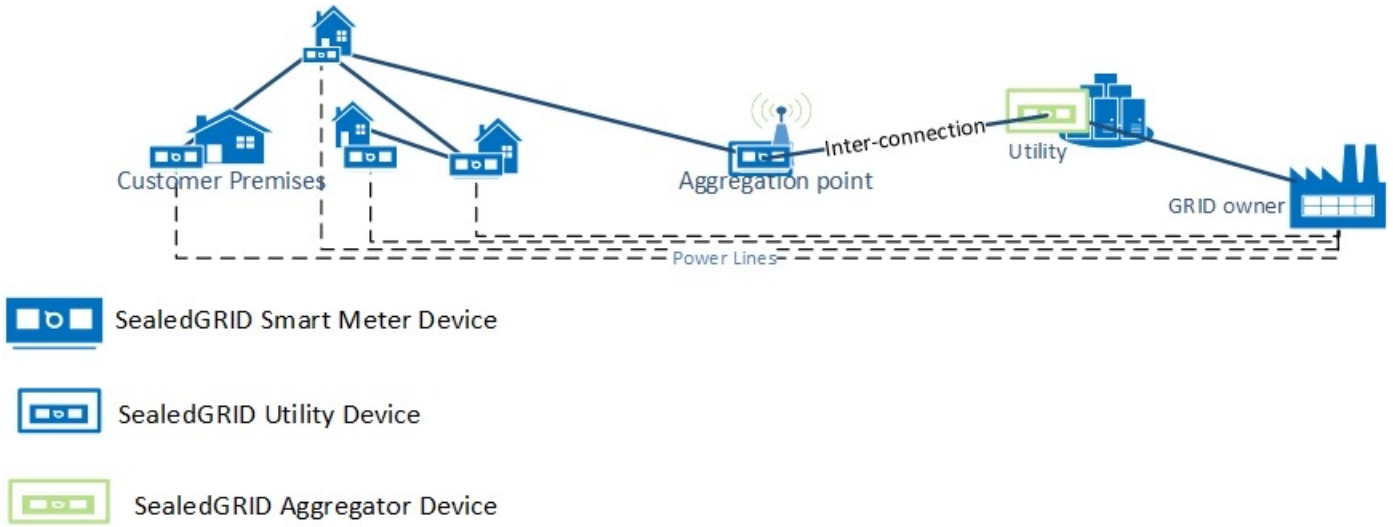
→Initial system design and prototyping **(D6.1)**

- Key Management, Authentication, Trusted computing Integration
- Authorization, Security Interoperability, Privacy Protection

→Final integrated system **(D6.2)**

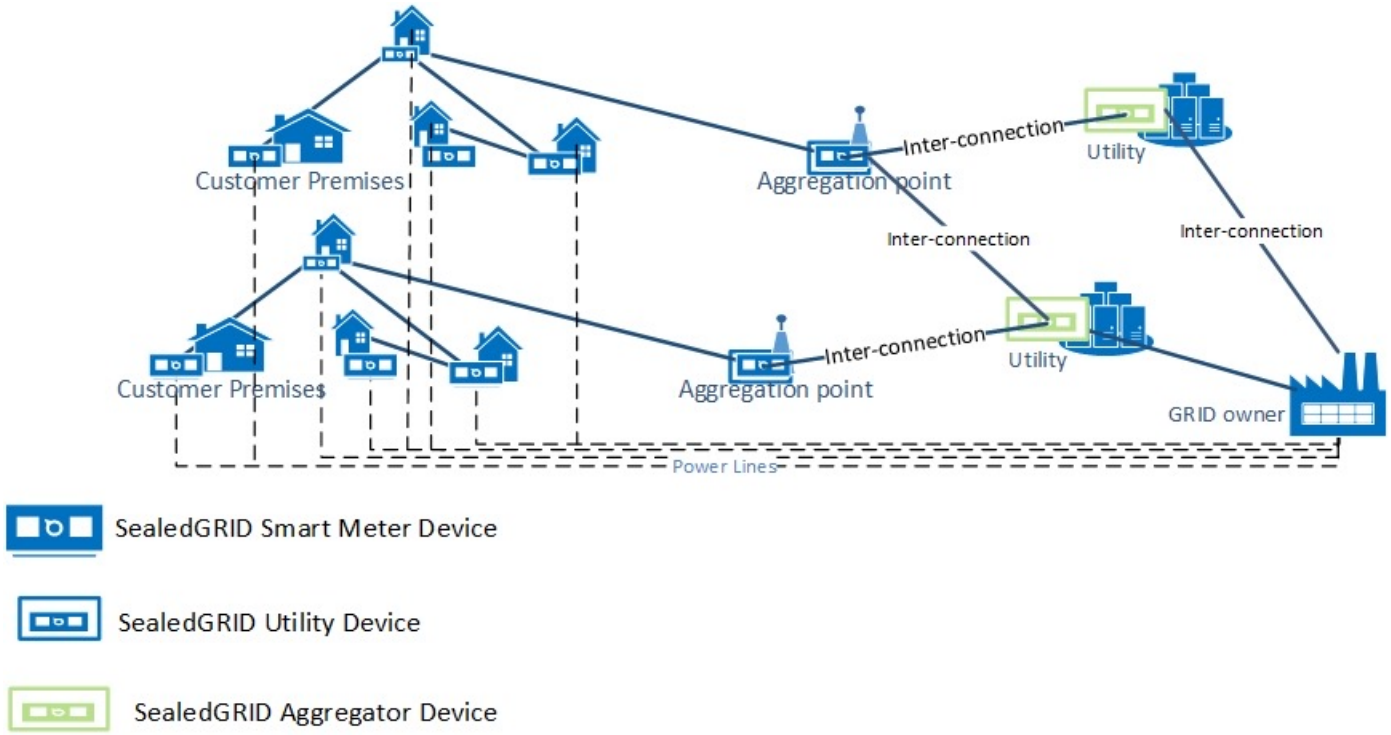
SealedGRID: Business Cases 1/3

- **Use Case A:** The **single-domain SealedGRID scenario**: where all SG devices will be **SealedGRID enabled** and be part of a single administrative domain.
  - 10 Scenarios



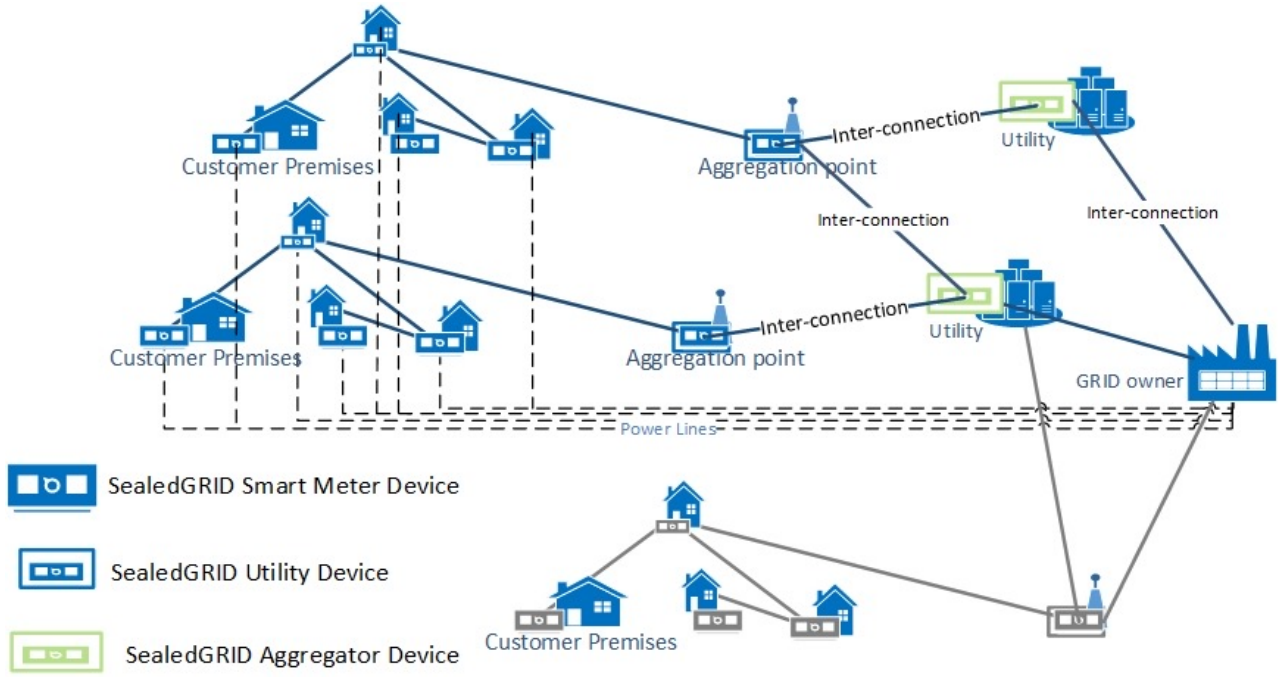
SealedGRID: Business Cases 2/3

- **Use Case B:** The **multi-domain SealedGRID scenario**: where all SG devices will be **SealedGRID enabled** and inter-connections will have to be managed.
  - 8 Scenarios



SealedGRID: Business Cases 3/3

- **Use Case C:** The **mixed scenario**: where only **some of the SG devices will be SealedGRID enabled** and interactions between SealedGRID and legacy devices, as well as inter-connections, will have to be managed.
  - 5 Scenarios



Prof. Christos Xenakis
xenakis@ssl-unipi.gr

SealedGRID

https://www.sgrid.eu/
Facebook: https://www.facebook.com/SealedGRIDH2020/
Twitter: https://twitter.com/sealedgridh2020?lang=en
LinkedIn: https://www.linkedin.com/in/sealedgrid-project-98246b187/
YouTube: https://www.youtube.com/channel/UC7k6Lz_RgV9GDPYyTi8qtTA