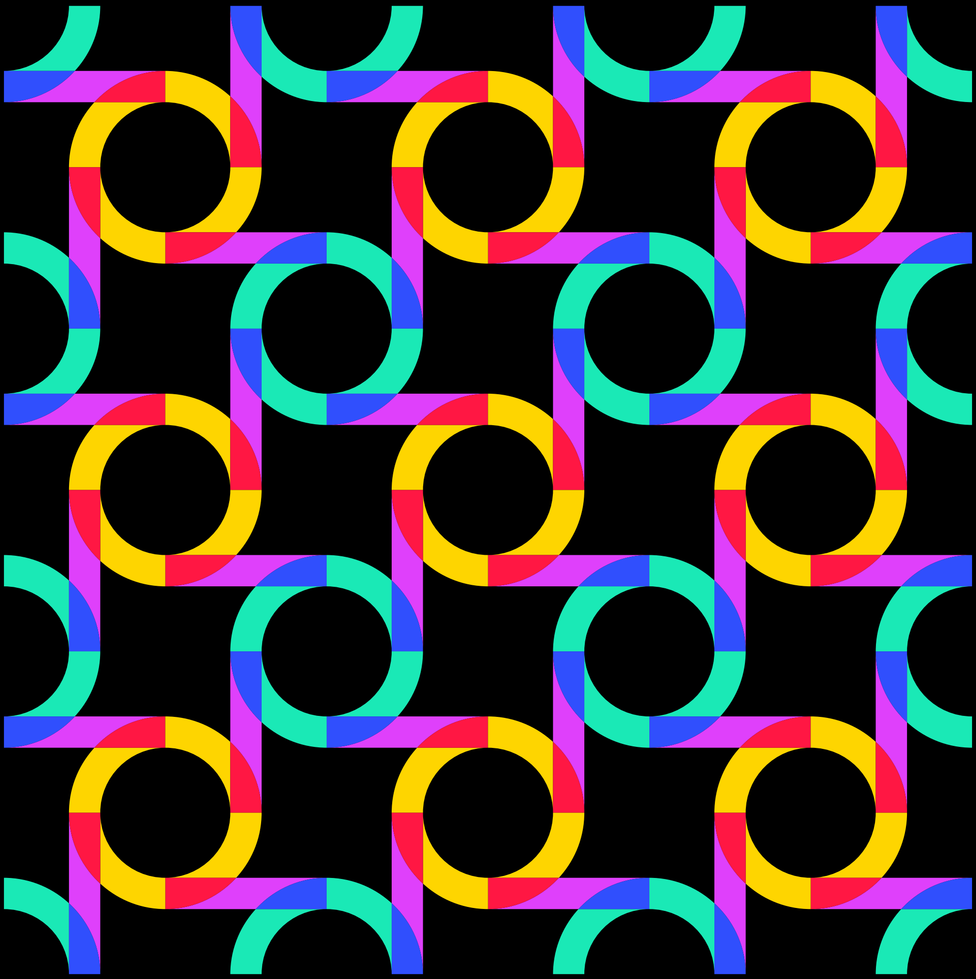
i4Trust



DARE

(Data spAces for smaRt Energy)

Trustworthy and effective sharing of IoT device data

i4Trust – Data Spaces for effective and trusted data sharing

www.i4trust.org

Smart Energy

Data spAces for smaRt Energy (DARE)

Trustworthy and effective sharing of IoT device data

With the contribution of:

ExcID

Gas Options

domx

Chthon

Plegma

National Technical University of Athens

StreamOWL

Challenge & Context

Efficient energy management of buildings is as relevant as ever. The energy crisis and the dramatic increase of the prices of fossil fuels urge for drastic improvement of the energy efficient management and operation of residential and commercial buildings. Traditional “tips” for saving energy do not suffice and there is a need for continuous, real-time energy management tailored to the requirements and habits of each individual consumer. Additionally, faults in energy equipment (e.g., a malfunctioning boiler) or energy leaks cannot be tolerated, and anomalies must be detected as soon as possible. In this respect, traditional, passive methods that rely on end consumers for detecting that “something is going wrong” based, for example, on higher than usual bills, are not sufficient. Similarly, legacy systems that leverage specific data generated by the energy equipment are not anymore adequately effective.

Creating more energy efficient buildings is a challenge that can be addressed by leveraging related data. However, data strictly confined to energy-specific measurements are not enough for addressing this challenge, instead information that concerns the data generator’s “context” should be provided e.g., location of the building, number of people living in the building, inside/outside temperature and humidity, weather conditions, etc. These data can be provided by third parties but also—and more importantly—by IoT devices and sensors located in many “smart buildings”.

Smart buildings employ a variety of IoT devices that generate data, which support various applications, such as energy management, automations that improve comfort, surveillance for security and safety, etc. In most of the cases, installed IoT equipment belong to specific vendor ecosystems and are mainly used for the specific purposes of each application (real-time consumption visualization, remote device management), thus being siloed and restricting their potential for delivering innovative cross-sectoral services.

Nevertheless, these data can be valuable for third party service providers that can collect and analyse them to provide “over the top” services related to the improvement of the energy management and efficiency of buildings. However, the potential of these data is limited by significant security and privacy concerns, as well as by the lack of interoperability across building systems and assets.

On the other hand, end-users would be interested in securely making a subset of their data available to these 3rd parties, in a stratified manner, to benefit from the added value of the provided services. In order to enable this, several barriers must be overcome a) a uniform and standardized way for requesting, and transmitting data should be in place, b) an efficient, usable mechanism for expressing and enforcing fine grained access control policies should be available, c) data access rights should be expressed in a rich and verifiable manner. In addition, proposed solutions should encourage interoperability and prevent vendor “lock-in”.

The Data spAces for smaRt Energy (DARE) project overcomes these challenges by providing a secure and efficient solution by leveraging the FIWARE, iSHARE and Decentralised Security solutions.

Solution

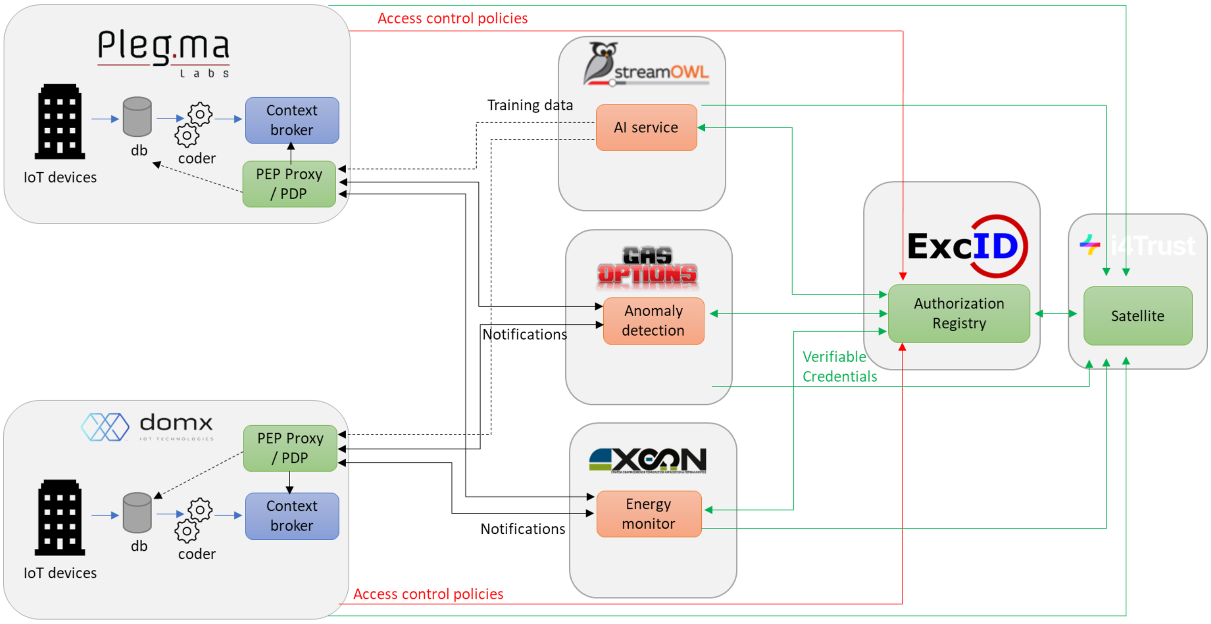
DARE enables innovative cross-sectoral services to be delivered on top of vendor and application specific building IoT equipment. DARE exploits IoT data generated by building IoT equipment, collected and analysed by third party service providers to deliver valuable "over the top" services related to the improvement of the energy management and efficiency of buildings. DARE creates a data space that provides secure access to two types of data: a) generic data, which is used for training related AI models, and b) consumer specific, real time data, which is used for providing tailored services and acute detection of anomalies. DARE consortium has demonstrated two related use cases: energy demand forecasting and energy equipment anomaly detection.

DARE data space includes data collected from smart energy equipment, as well as data related to the consumer context such as the number of persons currently in a building, building location, consumer's schedule, internal temperature and humidity, and many others are generated by smart sensors and IoT devices located inside the buildings.

Additionally, DARE provides an efficient access control system that allows data owners to define fine-grained access policies, as well as to "revoke" access rights at any time. Additionally, it provides mechanisms for transcoding collected data using a well-understood "schema". Finally, it offers a universal API for accessing heterogeneous data sources, enabling create, read, update, delete operations, time-related operations, as well as subscriptions to specific data-driven events.

In order to support its access control mechanisms, DARE leverages W3C's Verifiable Credentials (VCs) to enable decentralised security. VC data model enables an *issuer* to express claims about a *subject,* and VC holders, which is usually the same entity as the VC subject, to prove to a *verifier* that they possess VCs with certain claims. DARE uses VCs to enable data owners to define the *capabilities* of data consumers (e.g., *read, write, subscribe)* over their provided data. Then consumers can use the issued VC to prove that they are entitled to perform a specific operation over a collection of data objects. Furthermore, DARE provides a *Policy Enforcement Point,* implemented as a transparent HTTPS proxy that intercepts the communication between the data consumers and the data sources. By following this approach, DARE can secure any HTTP(S)-accessible data source with little-if any-effort.

How it works



DARE architecture includes the following entities: Data providers, which own IoT devices that produce data, Data consumers, which are third party service providers interested in accessing the generated data, and the Trust provider, which is responsible for storing access control policies and making access control decisions. The communication between Data providers and Data consumers is facilitated by a Context Broker. The following interactions are taking place in DARE architecture.

Data providers through the Trust provider configure the iSHARE Authorization Registries with the appropriate access control policies. Additionally, Data providers store in FIWARE Context Broker their data by leveraging transcoders, which are responsible for encoding the raw data produced by the IoT devices into JSON-LD encoded items.

A Data consumer requests authorization to access stored data from an authorization registry. Upon receiving such a request, the registry makes an access control decision using information included in access control lists, as well as on auxiliary information provided by the iSHARE satellite. The outcome of this decision is encoded in a VC that includes the “capabilities” of the consumer, as well as a consumer-owned public key. These “capabilities” can encode access rights to a specific subset of the published data, such as data originating from a specific geographic location or from a specific sensor type. The communication between a Data consumer and a registry follows the corresponding, ongoing, standard developed by OpenID foundation.

From this point on, the Data consumer can make an appropriate NGSI-LD API call (as implemented by the FIWARE Context Broker) to access the stored data. The data consumer includes in the HTTP request headers the VC it obtained from the issuer, along with a “proof of possession”, which is a digital signature that can be verified using the public key bound to the VC and proves that the Data consumer is the legitimate owner of the provided VC.

An API call is initially handled by the VC verifier, which is implemented as a transparent HTTP proxy; the verifier validates the provided VC and verifies that it includes the required “capabilities” for accessing the requested data. If all checks succeed, then the request is forwarded to the FIWARE Context Broker.

Benefits & Impact

DARE project includes a diverse consortium.

ExcID gained expertise in iSHARE technology, which is a promising technology that fills a gap that currently exists in SSI-based solutions. ExcID has expanded its portfolio with an access control solution that can accommodate many of the use cases that are in its area of focus. ExcID’s access control solution targets enterprise systems and IoT solutions. ExcID’s contributions to DARE will be offered as a new product which is expected to increase ExcID revenue by 50% through sales, collaborations, and new projects.

The project offered Plegma Labs a chance to step into the promising world of data sharing. By entering this market, Plegma is set to draw in a new set of customers, expanding its reach and influence. Specifically, the interoperable data sharing components developed throughout the course of the DARE project enriched the company’s end-product since multiple IoT meters and sensors from different providers and systems can be integrated seamlessly through the context broker provided by i4Trust. Regarding Plegma Labs, the solution developed during the DARE project was deployed in 8 commercial building customers, hence significantly increasing the impact of the company offering in terms of data transparency, trust, and security. Looking into the future, the number of customers that are expected to adopt the solution through Plegma's platform is approximately 10 commercial buildings per year. This translates to approximately 200.000€ per year in revenue increase, leading to an expected growth of 600.000€ in 3 years. Thus the sales of Plegma will increase by around 30% through the next 3 years.

The participation of DOMX in the DARE experiment enabled the company to become familiar with SSI technologies and more specifically to incorporate data encoding and access control mechanisms with their data sharing infrastructure, thus improving the delivered privacy, data availability and interoperability. In addition, a new anomaly detection service has been developed together with StreamOwl. The developed system has been evaluated under targeted scenarios that have been identified to generate privacy and security concerns for end users of the consortium's service providers (GasOptions, CHTHON), which companies are both existing customers of DOMX. The successful delivery of the targeted scenarios will enable DOMX to attract new potential clients from the HVAC maintenance and facility management sectors, through the offering of improved existing and future products and services. The delivery of more efficient energy management and new preemptive maintenance services, will enable DOMX customers to further improve their energy efficiency and reduce their operational costs (up to 10%). DOMX foresees an increased revenue rate of >50% over the next 3 years, which will result through the increased customer acquisition rate by 30% and the customer retention rate by 10% per year.

StreamOwl had the opportunity to develop an innovative product for anomaly detection using the latest developments in Artificial Intelligence and, most importantly, to evaluate and validate the product in real-world use cases and data. The data were provided from DOMX's infrastructure and comprise IoT sensors physically deployed in several commercial and residential buildings. Moreover, the project gave the opportunity to strengthen the collaboration with DOMX and it is expected that it will result in a long-lasting partnership for joint projects and future collaboration. The development of a new product opens a new revenue stream for StreamOwl and enables the company to enter into the market of energy management and condition monitoring. It is expected that the revenue stream will comprise 10% of the existing revenues within the next 3 years and it is expected to grow by a 8% CAGR. Moreover, it is foreseen that the staff headcount will increase by 2 new members which will be devoted to the development and customization of the new product.

Added value through i4Trust

- i4Trust provided significant opportunities for networking and business through the i4trust bootcamp and the data spaces symposium events
- Excellent coaching and mentorship were provided through technical and business support sessions, as well as during follow up calls. i4Trust mentors helped us fine tune the used components so as to implement the desired functionality.
- i4Trust is an excellent source of knowledge related to data spaces. Its training material and the i4Trust B2B Data Sharing Playbook are a valuable source of information about this emerging concept. The provided sample material helped us test and debug our deployments.
- The provided components helped us to develop our data space. In particular, FIWARE Orion context broker, the Mintaka time-series component, and pre-defined data models for IoT devices, were leveraged in order to achieve our goal.
- i4Trust building blocks for Data Sovereignty and Trust played a pivotal role for the development of the access control component of our project. In particular, our registry and PEP leveraged software, protocols, and tools provided by i4Trust.

References

- https://medium.com/@excid/access-control-using-verifiable-credentials-and-the-ishare-framework-c0cebbe64900
- https://medium.com/@excid/enabling-iot-data-sharing-bce885cba9b7
- https://www.youtube.com/watch?v=etp7Luvzu6M

Authors & Contributors

Nikos Fotiou, CEO of ExcID, fotiou@excid.io

Spiros Chadoulos, Data Scientist, Plegma Labs, sc@pleg.ma

Stratos Keranidis, R&D Director, DOMX, stratos@domx.io

Categories

User(s):

Installation maintenance companies, Facility management services, 3rd party service providers

Key words:

Access Control, Data Spaces, Smart Energy, Verifiable Credentials

Disclaimer: In accordance with our Guidelines concerning the use of endorsements and Impact Stories in advertising, please be aware of the following: Impact Stories appearing on the i4Trust site and partner's site or in other digital or printed materials. It is possible to hand in text, audio or video submissions. They are individual experiences, reflecting real life experiences of those who have used our technology and/or services in some way or another. We do not claim that they are typical results that customers will generally achieve. i4Trust partner's reserves the right to revise the contents, make them shorter and adapt them as required.

i4Trust

DARE
(Data spAces for smaRt Energy)

Trustworthy and effective sharing of IoT device data

Do you have questions or want to know more?

CONTACT US

Founding Partners

FIWARE FOUNDATION

iSHARE

FundingBox

i4Trust has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement no 951975.

i4Trust – Data Spaces for effective and trusted data sharing

www.i4trust.org