

Igor KOROPIECKI, Krzysztof PIOTROWSKI

IHP – Leibniz Institute for High Performance Microelectronics, Frankfurt (Oder), Germany

THE SOVEREIGN RESIDENTIAL EDGE: A METHODOLOGY FOR CLASSIFYING DATA SPACE REQUIREMENTS AT USER PREMISES

Sharing data is required to create value, but the moment it leaves its source, the owner loses control. Data Spaces provide organizations with sovereignty mechanisms to maintain that control after sharing. In residential contexts, data sovereignty remains an afterthought, acknowledged in legislation but always on provider-controlled infrastructure. We argue that legal sovereignty does not translate to technical autonomy for the end-user: current architectures allow providers to access raw user data by design, relying on legal contracts rather than technical enforcement. We define the Sovereign Residential Edge (SRE) through three criteria: physical residency, administrative authority, and network autonomy. Using fragmentation analysis, we show that no existing concept captures all three simultaneously. We present a methodology grounded in reference architectures (SGAM, ISO/IEC 30141, IDS-RAM) to classify requirements for technically enforced data sovereignty at the residential level, identifying what current patterns address and what remains unaddressed for residents to participate in data spaces.

SOVEREIGN RESIDENTIAL EDGE: METODOLOGIA KLASYFIKACJI WYMAGAŃ DATA SPACE NA POZIOMIE UŻYTKOWNIKA KOŃCOWEGO

Udostępnianie danych napędza rozwój usług cyfrowych, lecz w momencie opuszczenia źródła właściciel traci kontrolę. Data Spaces zapewniają organizacjom mechanizmy suwerenności pozwalające utrzymać kontrolę. W kontekście rezydencjalnym suwerenność danych jest drugorzędna: prawo ją uznaje, lecz w praktyce dane są w rękach dostawcy. W artykule wykazano, że suwerenność prawna nie przekłada się na autonomię techniczną użytkownika końcowego, a obecne architektury umożliwiają dostawcom dostęp do surowych danych użytkownika. Proponujemy koncepcję Sovereign Residential Edge (SRE), zdefiniowaną przez trzy kryteria: fizyczną lokalizację danych, autonomię administracyjną oraz autonomię sieciową. Poprzez przegląd istniejących koncepcji wykazujemy, że żadna nie obejmuje wszystkich trzech kryteriów. Przedstawiamy metodologię opartą na architekturach referencyjnych (SGAM, ISO/IEC 30141, IDS-RAM), służącą do klasyfikacji wymagań dla technicznie wymuszonej suwerenności danych na poziomie rezydencjalnym, wskazując, które wzorce architektoniczne są już realizowane, a jakie luki pozostają do wypełnienia, aby mieszkańcy mogli uczestniczyć w przestrzeniach danych (Data Spaces).

1. INTRODUCTION

People increasingly depend on connected devices, especially in the energy sector, where data flows constantly between devices (smart meters, EVs, heat pumps, etc.) and service providers. By default, connected devices send data outward. The general architectural assumption is to generate data at the edge and process in the cloud. For organizations, *data spaces* [1] established mechanisms to maintain data control after sharing, which stays at the source and is shared under the owner's terms. For residents, this has not happened yet. Data leaves the premises as soon as it is generated and is processed on infrastructure outside resident control. The volume and granularity of data leaving user premises has increased. High-resolution smart meter data at sub-minute intervals, EV charging profiles, and heat pump telemetry give insights into daily routine patterns [2].

The EU Data Act [3] establishes legal rights over this data (access, portability, control), however the technical reality is that the service provider who operates the infrastructure has full access to raw data by design. Data spaces prove that organizations can share data without losing control. In this paper, we investigate how the same can be achieved for residents, using data spaces as a starting point. As an application domain, we focus on residential Energy Management Systems (EMS), where bidirectional

data flows, high measurement frequency, and diverse data types make the sovereignty problem urgent and technically demanding.

The Sovereign Residential Edge (SRE) definition builds on three technical requirements: physical residency of data and hardware (data not exposed to remote infrastructure), administrative root authority (user controls what software runs on the device), and offline-first operation (system functions without depending on external services).

2. RELATED WORK

Early attempts at user-controlled infrastructure started in the 2010s with personal cloud platforms (ownCloud, Tonido) that placed storage on user-owned hardware. These largely failed due to high hardware costs, poor usability, and eventual unusability as devices became unresponsive when connectivity was lost. The subsequent cloud era succeeded because the data was already centralized, offering enterprise-grade reliability without user-managed infrastructure. However, it introduced vendor lock-in, no technically guaranteed privacy, and limited or no offline capability. Edge and fog computing later moved processing closer to the user for latency reasons (MEC [4], AWS Outposts), but remain provider-managed. The resident has no administrative control.

Data spaces have matured in B2B contexts through initiatives such as IDSA [1] and Gaia-X, with proven sovereignty mechanisms (usage control, connector architecture, contract negotiation). In the energy sector, projects like Omega-X [5] implemented federated energy data spaces. However, in these architectures, residents participate as data sources through provider-operated platforms, not as sovereign participants. The need for personal data integration is acknowledged. IDSA established a Sub-working Group on Personal Data under its Architecture Working Group, focusing on how personal data can be securely integrated within the IDS ecosystem. Prometheus-X [6], primarily active in the education sector, developed Personal Data Intermediaries in collaboration with CozyCloud and SOLID to give individuals consent management over their data. However, the personal data stores remain cloud-hosted, the architecture does not address offline operation, and SOLID access control is permission-based, meaning the hosting provider retains technical access to stored data by default.

The building blocks for residential data sovereignty exist in isolation. Personal clouds provide physical residency, self-sovereign identity (SSI) provides identity control, Prometheus-X enables consent management, and digital home gateways [7] provide hardware at user premises. No single existing concept captures administrative root authority, resource-constrained operation, and data space interoperability under one definition. Table 1 maps existing concepts against three criteria derived from

Tabela 1. Istniejące rozwiązania suwerenności według kryteriów SRE
Table 1. Existing sovereignty-related concepts under the SRE criteria

Concept	Context	Physical Residency	Root Authority	Network Autonomy
Sovereign Cloud (Azure, AWS)	Enterprise	No (provider data center)	No	No (cloud connectivity)
Private Edge (MEC, Outposts)	Industrial IoT	Partial (operator-managed)	No	Partial (local buffering)
Personal Cloud	<i>Historical (2010s)</i>	Yes (user hardware)	Yes (user-administered)	No (cloud heartbeat)
SOLID	Decentralized Web	No (cloud-hosted Pods)	Partial (user chooses provider, no root acc.)	No (requires connectivity)
Digital Home Gateway	Smart Grid, Broadband	Yes (user premises)	No (provider-administ.)	Partial (local protocols)
SRE	Smart Grid Residential	Yes	Yes	Yes

this analysis. This fragmentation motivates the definition of the Sovereign Residential Edge presented in Section 3.

3. DEFINITION

The Sovereign Residential Edge (SRE) is a deployment model where the user's premises host infrastructure that simultaneously satisfies three criteria:

Physical residency, meaning that hardware and primary data store are physically located at the user's premises. Verified by checking whether storage location is within the user's legal property.

Administrative sovereignty, meaning that the user (or their delegate) holds exclusive root access to the device. Verified by checking whether user can authenticate as an administrator on the device.

Network autonomy, meaning that core functionality persists without internet access. Connectivity is treated as an enhancement. Verified by checking whether system operates when disconnected from the Internet.

When considering a residential energy scenario, the primary challenge for SRE-compliant architectures is that current data space designs bundle operational and informational access by design. The provider who deploys and maintains a connector can read, process, and export the raw data flowing through it. Sovereignty is delegated to legal contracts instead of the technology. In an example scenario, a Distribution System Operator (DSO) needs grid flexibility from a resident's EV battery. In current architectures, the DSO platform accesses raw consumption telemetry to determine available flexibility. In an SRE-compliant architecture, a local device processes the measurement data on premises and sends only a contract-compliant output to the DSO. The provider maintaining the device cannot access the raw measurements.

To systematically investigate current architectures, we propose a classification methodology grounded in established reference architectures.

4. METHODOLOGY

The assessment framework combines three reference architectures. Each addresses a different SRE dimension. SGAM [8] scopes the physical deployment, identifying components within the Customer Premises Domain at Station and Field Zones, but leaves administrative sovereignty unspecified at the residential level (out of scope for SGAM). ISO/IEC 30141 [9] defines trust boundaries between the User Domain and the Service Provider Domain, used to evaluate whether user devices are technically decoupled from provider infrastructure. IDS-RAM [1] provides the connector architecture and usage control model, used to evaluate whether policy enforcement can separate operational from informational access and whether it can function without permanent cloud connectivity.

Sources are drawn from categories including: standardization bodies (CENELEC/ETSI, ISO/IEC 30141), EU projects (Omega-X), industrial specifications (IDS-RAM, Gaia-X Trust Framework), and documentation (e.g. Home Assistant).

Requirements are extracted by identifying data exchange scenarios in each source and capturing the actor (who requires the data), the asset (what data is exchanged), and the constraint (what infrastructure assumptions are made). Each constraint is evaluated against the established criteria: where processing occurs (physical residency), who administers the infrastructure (administrative sovereignty), and what connectivity is assumed (network autonomy). Extracted requirements are classified along three dimensions: deployment tier (cloud, fog, edge, user premises), primary concern (sovereignty, offline capability, interoperability), and implementation maturity (specified, prototyped, deployed). The complete extraction protocol, classification, traceability and full taxonomy application will be presented in the full publication.

5. PRELIMINARY FINDINGS

To test the methodology, we applied the criteria to six architectures representing the deployment approaches spectrum: a cloud IoT platform (AWS IoT Core), a provider-managed edge deployment (MEC), an energy data space (Omega-X), a personal data store (SOLID), a utility-managed home gateway (Smart Meter Gateway), and an open-source home automation platform (Home Assistant).

All provider-managed systems (AWS IoT Core, Omega-X, MEC) lack administrative sovereignty regardless of where the hardware is physically located. All cloud-hosted systems (AWS IoT Core, Omega-X, SOLID) lack network autonomy. The Smart Meter Gateway provides physical residency and partial offline operation but is administered by the utility. Home Assistant is the only system where the user holds root access and operation is possible without connectivity, however it lacks data space sovereignty mechanisms such as usage control and contract negotiation. No analyzed architecture satisfies all three SRE criteria simultaneously. This preliminary analysis is limited. A comprehensive analysis across all source categories will be presented in the full publication.

6. CONCLUSIONS AND FURTHER STEPS

This paper defined the Sovereign Residential Edge in response to the absence of a concept that simultaneously captures physical residency, administrative sovereignty, and network autonomy, which are necessary for residents to participate in data spaces with technically guaranteed sovereignty. A classification methodology grounded in established reference architectures was outlined for identifying and evaluating data space requirements at the residential level. A preliminary execution of the methodology indicated that existing architectures satisfy at most two of the three SRE criteria simultaneously.

This work is part of a PhD investigating architectural patterns for data space integration in customer premises. In the next steps, the criteria will be used to evaluate existing platforms and architectures to identify specific constraints at the residential level.

REFERENCES

1. IDSA: Reference Architecture Model 4.0. Available at: <https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4> (last accessed on 23.04.2026).
2. Kua J., Hossain M.B., Natgunanathan I., Xiang Y.: Privacy Preservation in Smart Meters: Current Status, Challenges and Future Directions, MDPI Sensors, 2023.
3. European Commission: Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act). Official Journal of the European Union, December 2023.
4. Sabella D., Vaillant A., Kuure P., Raber U., Schotten, H.: Mobile-Edge Computing Architecture: The role of MEC in the Internet of Things, IEEE Consumer Electronics Magazine, 2016.
5. OMEGA-X: Orchestrating an interoperable sovereign federated Multi-vector Energy Data Space. Available at: <https://omega-x.eu/> (last accessed on 23.04.2026).
6. Prometheus-X. Available at: <https://prometheus-x.org/> (last accessed on 23.04.2026).
7. BSI: Technical Guideline TR-03109 Smart Meter Gateway. Available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/smart-metering_node.html (last accessed on 23.04.2026).
8. CEN-CENELEC-ETSI Smart Grid Coordination Group: Smart Grid Reference Architecture. November 2012.
9. ISO/IEC 30141:2018 Internet of Things (IoT) Reference Architecture. International Organization for Standardization, 2018.