CIRED 2020 Berlin Workshop (CIRED 2020)

22-23 September 2020

Theme 2: Opportunities and Challenges with Operation using Flexibility

Secure standards-based reference architecture for flexibility activation and democratisation

ISSN 2515-0855
doi: 10.1049/oap-cired.2021.0123
www.ietdl.org

Hrvoje Keko[1] ✉, Peter Hasse[2], Eloi Gabandon[3], Stjepan Sučić[1], Karsten Isakovic[2], Jordi Cipriano[3]

[1]*KONČAR – Power Plant and Electric Traction Engineering Inc., Zagreb, Croatia*
[2]*Fraunhofer – Fraunhofer-Institut für Offene Kommunikationssysteme – FOKUS, Berlin, Germany*
[3]*Centre Internacional de Mètodes Numèrics a l'Enginyeria (CIMNE), Building Energy and Environment Department, Lleida, Spain*
✉ *E-mail: hrvoje.keko@koncar-ket.hr*

Abstract: This study presents an open standards-based information system supporting democratisation and consumer empowerment through flexibility activation. This study describes a functional technical reference infrastructure: a secure, standard-based and viable communication backbone for flexibility activation. The infrastructure allows connection, registering, activation and reporting for different types of granular consumer flexibility. The flexibility sources can be directly controllable set points of chargers and stationary batteries, as well as controllable loads. The proposed communication system sees all these flexibility provisions as distributed energy resources in a wider sense, and the architecture allows consumer-level integration of different energy systems. This makes new flexibility sources fully available to the balancing responsible entities in a viable and realistically implementable manner. The proposed reference architecture, as implemented in the FLEXCoop project, relies on established open standards as it is based on the Open Automated Demand Response (OpenADR) and OAuth2/OpenID standards and the corresponding IEC 62746-10 standard, and it covers interfacing towards other relevant standards. The security and access implications are addressed by the OpenID security layer built on top of the OAuth2 and integrated with the OpenADR standard. To address the data protection and privacy aspects, the architecture is designed on the least knowledge principle.

1 Introduction

The power grid system of today sees increasing uncertainty. The main reason on the generation side is the renewable energy sources with non-controllable prime movers, while on the consumption side, electrification of mobility is one of the key drivers. The distribution networks are at the same time more active and the distribution system operators are required to perform tasks previously only seen at the transmission system operator. This includes ancillary services, redispatching, reactive power/voltage control and congestion management. Balancing the grid carries the costs – which are typically bundled in the grid operation cost and carried over to the final consumer. Perfect forecasting will surely remain impossible [1], hence, to fulfil the balancing needs, securing flexibility is necessary. Traditionally, flexibility for the automatic and manual frequency restoration reserve [2] is sought in the form of fully controllable and fast ramping resources such as hydropower plants. Flexibility can be provided on the demand side. Large energy consumers can offer the service of controllable loads to the system operator by participating in the balancing service markets. Examples include steel mills and mineral fertiliser factories. The flexibility is offered to the extent where it does not disrupt the primary service. This paper proposes a secure and open standards-based reference architecture to extend the flexibility towards the granular contributions at the end-user premises. Individually small, these contributions in larger numbers become significant. Here, the market roles are reversed, compared to wholesale and retail energy markets: the flexibility providers are the end users, and the flexibility consumers the balancing responsible entities.

An end-to-end software infrastructure from the flexibility consumers to the granular flexibility providers is required. Given the expectation of a large number of granular contributors, the intermediary entities – flexibility aggregators – will appear. Similar approaches have been discussed in a virtual power plant approach in [3–5]. This paper focuses on the underlying software architecture built around the Open Automated Demand Response (OpenADR) standard. To cover the data privacy and cybersecurity access control requirements at the application level, integration with the Open ID/OAuth2 standard is proposed and described.

2 OpenADR standard and its coverage

2.1 OpenADR and IEC 62746

The OpenADR [6, 7] is an open standard with a publicly available specification and architecture, designed in the early 2000s. As in many other American originating standards such as the DNP3 protocol [8], this standard is synthesised from practice, intensified during the Californian energy crisis of 2002 [9]. An updated version 2.0 of the standard has been established following the Organization for the Advancement of Structured Information Systems (OASIS) initiative [10]. In Europe, the OpenADR has been fully adopted as the IEC 62746-10 standard in January 2019 [11]. The IEC 62746 standard series specifies application-level service communication that can incentivise the responses from the customer-owned and customer-located distributed energy resources.

2.2 Smart grid user interface standard concepts

The OpenADR defines an implementation of a two-way signalling system, providing the servers that publish information to the (automated) clients subscribing to the information. It uses the

CIRED, Open Access Proc. J., 2020, Vol. 2020, Iss. 1, pp. 584–587

concept of virtual top nodes (VTNs) as servers and virtual end nodes (VENs) as automated clients. The servers VTNs are publishing the information while the clients VENs are its subscribers. These concepts come from the OASIS interoperability standard [10] as well as the IEC 62939 – SGUI (Smart Grid User Interface) [12]. The VEN has direct operational control of a set of resources and can be an energy consumer with controllable loads or a producer. The communication between the VTN and VEN is two-way. The VTN is a party whose role is an aggregation of the information and capabilities of multiple VENs. Direct (same-level) communication of different VENs is not supported (Fig. 1).

A VTN in one context can be a VEN in another context – as an aggregator – an (optional) mediator between the system operator and a large number of low-level VENs [13].

2.3 Semantic interpretation of OpenADR message payloads

The coverage of OpenADR/IEC 62746-10 excludes any market-specific contractual or business agreements as well as the interpretation of what the semantic of a generic event is. If a protocol is merely a data carrier, the data is interpreted at both ends so the semantic interpretation needs to be enforced implicitly or will lead to misinterpretations. The authors' experience confirms it is more efficient to explicitly and strictly enforce a semantic scheme and thus the adherence to the common semantic interpretation of the data [14]. In the CIM working groups, work is underway to standardise the data mappings [15, 16]. The FLEXCoop protocol implementation relies on Cerberus [17] library to strictly enforce adherence to a schema in JSON message payloads.

2.4 Gateways bridging the direct and open-ended control

The indirect control nature of OpenADR means that a gateway device is needed to register as a VEN and convert the OpenADR payloads to the direct telecontrol commands. Conversely, this gateway interprets the events downstream and passes the relevant information upstream. The opt-in nature points out another implicit requirement for the software infrastructure: the aggregator must implement a registry to keep track of numerous end-users and their resources. The registry can be a central instance or implemented in a federated manner. The available flexibility estimation is another challenging task. Forecasting and estimating the amount of available flexibility is beyond the scope of this paper, but typically, the end-user premises devices are used to extrapolate the available flexibility from ambient measurements. This estimates the baseline and provides a prediction of available flexibilities. The user premises device must handle numerous in-house protocols (e.g. ZigBee, Bluetooth Low Energy, Z-Wave, Modbus, custom protocols over an HTTP or Message Queuing Telemetry Transport interface) and function as a point of entry into a standardised system.

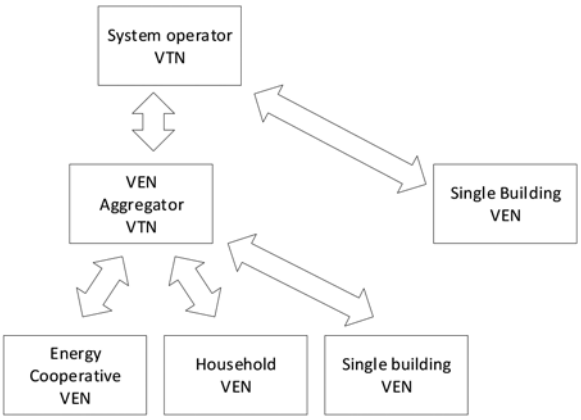

Fig. 1 *VTN and VEN concepts in the context of flexibility activation architecture*

3 Proposed reference architecture

Fig. 2 illustrates the proposed functional reference architecture to activate the granular demand response contributions.

The flexibility user (or customer) is a VTN communicating with aggregators as VENs. Regardless of the financial incentive scheme, the aggregator's middleware must keep track of the activations in a registry. The end-users entering the contract with the aggregator will expect a consumer-facing end-user software provided by the aggregator. To activate the demand response, the aggregator communicates, again, using OpenADR with a proper semantic messaging scheme, with the larger-scale telecontrol gateways interfacing with supervisory control and data acquisition systems, and with small-scale customer devices.

Fig. 3 illustrates the FLEXCoop [14] implementation. Functionally, the aggregator functionality is implemented in the *Message Oriented Middleware* with different applications communicating with respectively through it. The user premises

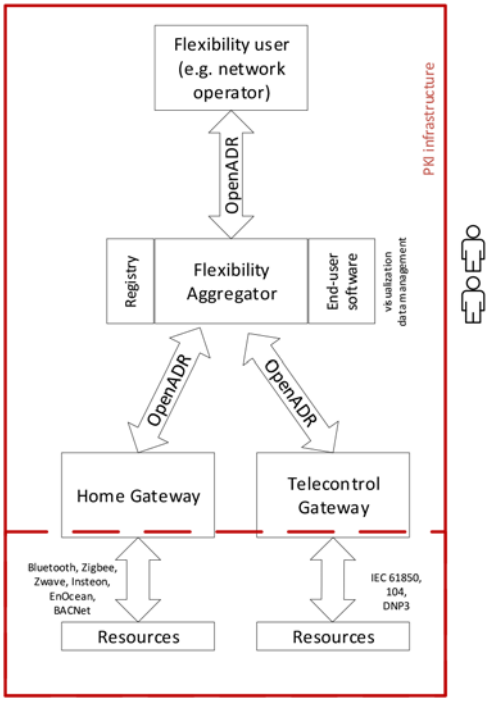

Fig. 2 *Proposed functional reference architecture*

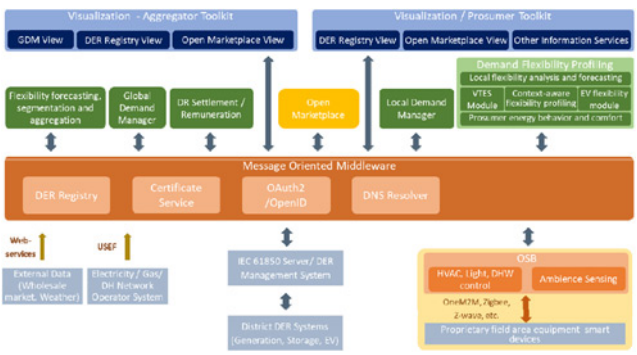

Fig. 3 *FLEXCoop implementation of the architecture*

device is called OSB: *Open Smart Box* and the end user-facing functions are implemented in Prosumer Toolbox.

In Fig. 3, other entry points communicating with the middleware are illustrated, as well as the profiling architecture, both out of the scope of this paper.

4 Data privacy and security concerns

4.1 OpenADR, security and privacy

Most automation protocols have been designed with dedicated air-gapped communication channels in mind which is not reasonable for a DR infrastructure that will operate over public networks instead. The OpenADR standard does not define transport mechanisms and only covers minimum cybersecurity mechanisms required to provide non-repudiation and mitigation of cyber-security risks. The standard only defines the procedure of fingerprint-based verification of the other party and XML messages signing, so it requires a public key infrastructure and transport layer security (TLS). The standard itself does not cover how the end users (the actual persons owning the DR resources) authenticate and have access to the system granted. Especially the provisioning of cryptographical keys and certificates is essential for such a distributed system which is also missing in OpenADR. The proposed reference standard expects the implementation of security and privacy measures, and this chapter illustrates these measures as implemented in the FLEXCoop solution.

4.2 Data privacy concerns

Demand response schemes have a high potential for privacy breaches. The FLEXCoop implementation addresses these concerns by implementing a security framework in both the software component communication layer (HTTPS REST APIs) and the software–hardware communication layer (based on OpenADR). Access to data stored in the system is granted to the different components on a mandate level. The components only get access to the minimum required data, and only for the data of the account, they are mandated for. The security framework separates personal data (names, addresses and other information linking the system user with a physical person), from the data the system generates or collects. The personal data is exclusively managed by the aggregators – who have contractual explicit permission to handle the personal data. This is based on a pseudo anonymisation process, assigning anonymous IDs to each customer. The aggregators (data handlers) are the only entities able to link this ID to the personal data, while not being able to access the system-generated data at the same time. The consistent use of reference IDs throughout the system enables the removal of all user data from the complete system if requested.

4.3 Software components authorisation and authentication

The FLEXCoop system uses Open ID/OAuth 2.0 as the delegation and authorisation framework. The OAuth 2.0 [18] is an open and widely used standard for access delegation, enabling the third-party application to obtain limited access to a service, through tokens issued by an authorisation server. OAuth 2.0 is directly related to OpenID Connect (OIDC), an authentication layer built on top of OAuth 2.0. In FLEXCoop implementation, most FLEXCoop software components are third-party applications and data handlers must grant access. The data handlers are energy cooperatives acting as aggregators. Furthermore, an OpenID provider is installed within the Middleware to provide access to the internal components with no user interaction to authenticated internal components such as the *Open Market Place*. Access to the user data is then granted only to the components that require them and only for the data the provider mandates them to. The OpenID

Role	Definition	FLEXCoop Mapping
Resource owner	An entity capable of granting access to a protected end-user.	End users or components without user interface.
Resource server	The server hosting the protected resources. Accepts and responds to protected users' requests using access tokens.	The Middleware
Client	Application requesting protected resource on behalf of the resource owner and with its authorization.	Software components with user interface.
Authorization server	The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.	The OpenID Servers.

Fig. 4 *FLEXCoop mappings of OpenID roles*

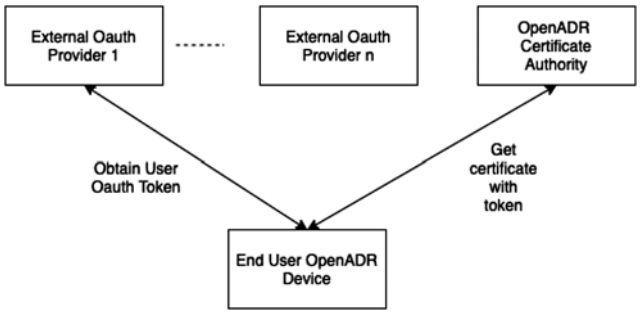

Fig. 5 *Token-based registration of user premises device*

user roles are mapped into the FLEXCoop platform, as shown in Fig. 4.

This deep implementation of OpenID into the system assures the least knowledge principle (the system components only access the information absolutely required to fulfil their functions), and seamless verification of the actual end users through tokens.

While the transmission security and non-repudiation of the messages are covered by the standard OpenADR protocol via the client certificates installed in the VENs and the data access at the application level is implemented as shown in Fig. 5.

To register a new user premises device at the household, the user is required to authenticate to the OAuth 2.0 server as indicated by the local device. As shown in Fig. 5, the VEN will then request a certificate from the certificate authority using the obtained OAuth 2.0 token that identifies the user. The generated certificate will be used in OpenADR messages subsequently. This extends the OpenADR VEN implementation to receive cryptographical key material in a secure way, change such material e.g. to assigned a VEN to a different DR system and check for revoked keys to keep the system secure.

5 Conclusion

In this paper, the scope of the OpenADR standard is briefly presented and then the key requirements for an open standards-based information system for democratisation and consumer empowerment through flexibility activation are discussed. These requirements are summarised in a functional reference architecture, which is illustrated as implemented in the FLEXCoop project. While the OpenADR standard can underpin the base of the communication, in practice two crucial extensions to OpenADR are needed to build a viable and secure flexibility activation system.

The implementation of a semantic scheme common to all components is called for, as well as tight integration with a security framework to ensure data privacy, interoperability and safety. Especially the key distribution and management for end-user devices are a blind spot in OpenADR which is a risk for security as interoperability between different OpenADR-based systems. The FLEXCoop solution solves these issues by enforcing

CIRED, Open Access Proc. J., 2020, Vol. 2020, Iss. 1, pp. 584–587

a common messaging schema and by implementing a security framework based on OAuth 2.0/OpenID, both for user access as well as in machine-to-machine communication. The security framework is explained in detail and this rounds up an implementation of a software architecture for wide-range secure flexibility activation.

6 Acknowledgements

The research leading to these findings has been supported by the FLEXCoop project. The FLEXCoop project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no. 773909.

7 References

1 Bessa, R. J., Miranda, V., Botterud, A., *et al.*: ''Good' or 'bad' wind power forecasts: a relative concept', *Wind Energy*, 2011, **14**, (5), pp. 625–636, doi: 10.1002/we.444
2 'ENTSO-E Operational Handbook: Load-Frequency Control and Performance'. https://www.entsoe.eu/publications/system-operations-reports/#continental-europe-operation-handbook (accessed Jun. 15, 2019)
3 Zajc, M., Kolenc, M., Suljanović, N.: '11 – virtual power plant communication system architecture', in Yang, Q, Yang, T, Li, W, (Eds). 'Smart power distribution systems', Academic Press, London, UK, 2019, pp. 231–250
4 Kolenc, M., Ihle, N., Gutschi, C., *et al.*: 'Virtual power plant architecture using OpenADR 2.0b for dynamic charging of automated guided vehicles', *Int. J. Electr. Power Energy Syst.*, 2019, **104**, pp. 370–382, doi: 10.1016/j.ijepes.2018.07.032
5 Nosratabadi, S.M., Hooshmand, R.-A., Gholipour, E.: 'A comprehensive review on microgrid and virtual power plant concepts employed for distributed energy resources scheduling in power systems', *Renew. Sustain. Energy Rev.*, 2017, **67**, pp. 341–363, doi: 10.1016/j.rser.2016.09.025
6 'OpenADR Alliance'. https://www.openadr.org/ (accessed May 31, 2019)
7 Keko, H., Tzanidakis, K., Malavazos, C., *et al.*: 'FLEXCoop D2.3 analysis of EU-wide interoperability standards and data models and harmonization requirements', D2.3, 2018
8 'Overview of DNP3 Protocol'. https://www.dnp.org/About/Overview-of-DNP3-Protocol (accessed Mar. 12, 2020)
9 'The California energy crisis', 2001 power engineering society summer meeting. Conf. Proc. (Cat. No. 01CH37262), Vancouver, Canada, 2001, vol. 1, pp. 570–572, doi: 10.1109/PESS.2001.970099
10 'OASIS Energy Interoperation TC | OASIS'. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=energyinterop (accessed June 01, 2018)
11 'IEC PAS 62746-10-1:2014 | IEC Webstore'. https://webstore.iec.ch/publication/7570 (accessed June 01, 2018)
12 'IEC TR 62939-1:2014 | IEC Webstore'. https://webstore.iec.ch/publication/7478 (accessed June 01, 2018)
13 Zupančič, J., Prislan, B., Lakić, E., *et al.*: 'Market-based business model for flexible energy aggregators in distribution networks'. 2017 14th Int. Conf. on the European Energy Market (EEM), Ljubljana, Slovenia, 2017, pp. 1–6, doi: 10.1109/EEM.2017.7981997
14 Martinez, G., Morcillo, L., Valalaki, K., *et al.*: 'FLEXCoop D6.4 FLEXCoop integrated DR optimization framework and pre-validation results – preliminary version', D6.4, 2020
15 'IEC 62325-301:2018 | IEC Webstore'. https://webstore.iec.ch/publication/31487 (accessed June 04, 2018)
16 'IEC 61968-11:2013 | IEC Webstore'. https://webstore.iec.ch/publication/6199 (accessed June 01, 2018)
17 'Welcome to Cerberus – Cerberus is a lightweight and extensible data validation library for Python'. https://docs.python-cerberus.org/en/stable/ (accessed March 26, 2020)
18 Hardt, D.: 'The OAuth 2.0 authorization framework', https://tools.ietf.org/html/rfc6749 (accessed March 20, 2020)