Exploring Vendor-Neutral SMART on FHIR Infrastructure for Secure Data Exchange in Research and Patient Care

Katja Hoffmann[1], Eveline Prochaska[1], Markus Wolfien[1,2] and Martin Sedlmayr[1]

[1]*Institute for Medical Informatics and Biometry, Faculty of Medicine Carl Gustav Carus, TUD Dresden University of Technology, Fetscherstraße 74, 01307 Dresden, Germany*

[2]*Center for Scalable Data Analytics and Artificial Intelligence, (ScaDS.AI), Dresden/Leipzig, Dresden, Germany*

Abstract

Health data is essential for advancing research and improving patient care, emphasizing the need for secure, interoperable infrastructures that enable seamless access to healthcare systems. SMART on FHIR is a framework that ensures secure data exchange by specifying APIs for authentication and authorization between applications and healthcare systems. Through a review of academic and non-academic sources, we identified open-source, vendor-neutral implementations of SMART on FHIR infrastructure, including the Alvearie Keycloak extension and the LinuxForHealth FHIR server as promising components. These solutions were prototypically implemented in a reference infrastructure to evaluate their feasibility. Despite their potential for experimental use, limitations in compatibility and functionality underscore the need for ongoing community-driven development to enhance interoperability, reduce costs, and foster innovation in healthcare.

Keywords

SMART on FHIR, Reference Implementation, Infrastructure, Vendor-neutral, Open-Source

1. Introduction

Health data serves as a foundation for advancing research, enhancing the quality of care, and developing AI models that support diagnostics and enable personalized therapies, while also empowering patients to access and use their own data. This underscores the pressing need for robust, secure data infrastructures that facilitate legal-compliant and secure access to health information.

Substitutable Medical Applications, Reusable Technologies on Fast Healthcare Interoperability Resources (SMART on FHIR) is an open standards-based framework developed to enable healthcare applications (apps) to interact seamlessly and securely with electronic health records (EHRs) and other health data systems [1]. SMART on FHIR leverages the internationally recognized Health Level 7 (HL7) FHIR standard for data exchange [2], and defines core specifications for authentication and authorization of both, user-facing client apps (*SMART App Launch*) [3] and headless or automated client apps (SMART/HL7 *FHIR Bulk Data Access*) [4]. Put differently, while FHIR defines data models (known as resources), and application programming interfaces (APIs) for interacting with these resources (**C**reate, **R**ead, **U**pdate, **D**elete, **S**earch, **E**xecute operations), SMART on FHIR specifies APIs for securely connecting third-party apps to EHRs or other health data systems and authorizing access to a subset of FHIR resources. The framework operates through three interconnected components: i) Resource server (hosts FHIR data and manages access to healthcare data using FHIR APIs), ii) Authorization

SWAT4HCLS 2025: 16th International Conference on Semantic Web Applications and Tools for Health Care and Life Sciences 2025
katja.hoffmann@tu-dresden.de (K. Hoffmann); eveline.prochaska@tu-dresden.de (E. Prochaska); markus.wolfien@tu-dresden.de (M. Wolfien); martin.sedlmayr@tu-dresden.de (M. Sedlmayr)
0000-0003-4765-0767 (K. Hoffmann); 0000-0002-7609-1565 (E. Prochaska); 0000-0002-1887-4772 (M. Wolfien); 0000-0002-9888-8460 (M. Sedlmayr)

server (provides secure authentication and issues access tokens to client applications based on user credentials and scopes), and iii) client application (the third-party app requesting access to FHIR data on behalf of a user). The communication between these components is based on OAuth 2.0 [5], which handles the authentication and authorization of requests, and OpenID Connect [6], which provides identity verification to ensure secure interactions (cf. Figure 1).

This framework allows an app written once to access standardized data from any EHR or health data system, provided the resource and authorization servers support the appropriate FHIR and SMART on FHIR specifications [7]. However, this poses a significant challenge. In the U.S., legislation mandates that EHR systems support the two key public APIs, namely *SMART App Launch* for secure access to individual patient data and *SMART HL7/FHIR Bulk Data Access* for large-scale data retrieval [8]. In contrast, Europe, including Germany, has seen limited adoption of solutions that fully support SMART on FHIR specifications, with many initiatives still in development or at early stages of implementation.

Implementing vendor-neutral, open-source infrastructure could help bridge this gap. Open-source solutions are critical for reducing costs, and enabling interoperability across healthcare sites. This study investigates the feasibility of leveraging existing vendor-neutral, open-source infrastructures to support the deployment of SMART on FHIR applications.

2. Materials and methods

We conducted a literature search of academic databases including *PubMed*, *Web of Science*, *IEEE Xplore*, and *Scopus* using the keywords “SMART-on-FHIR”, “implementation”, “infrastructure”, “open-source” and “vendor-neutral”. Manual review of the reference lists for eligible studies was performed and only guidelines, studies, and research articles written in English or German were included. Inclusion criteria required studies to focus on SMART on FHIR implementations, particularly open-source and vendor-neutral infrastructure solutions. The criteria for exclusion were as follows: (i) Non English or German written studies; (ii) Studies centered on the medical domain, clinical support systems or computational models (without focus on SMART on FHIR), iii) non open-source and vendor-neutral infrastructure solutions, iv) SMART-on-FHIR supporting EHRs, or future directions without concrete use or implementation of SMART on FHIR; and (v) duplicate studies.

In addition to peer-reviewed sources, we examined relevant non-academic resources, including the official website for the SMART Health IT project [7], HL7 FHIR Confluence [8], and discussions from the FHIR community on chat.fhir.org [9]. These were analyzed to identify open-source and vendor-neutral SMART on FHIR server implementations. We assessed the identified server implementations based on their feature set, quality and comprehensiveness of documentation, and the status of active development and maintenance. To demonstrate feasibility, we selected the most promising solution and developed a reference infrastructure using Docker Compose [10].

3. Results

No eligible studies were identified from the literature search in academic databases after applying the exclusion criteria. However, from non-peer-reviewed literature sources, we identified the following open-source and vendor-neutral SMART on FHIR server implementations (cf. Figure 1).

Authorization server

- *Alvearie Keycloak extension* [11], developed by IBM under the Alvearie healthcare initiative [12], is a set of extensions for Keycloak [13] to enable SMART App Launch.

- igia Keycloak extension [14], developed under the igia project [15], is a set of extensions for Keycloak [13] to enable SMART App Launch.

Keycloak itself is a highly customizable and extensible identity and access management solution designed to manage user authentication, authorization, and identity services for web applications, mobile apps, and APIs. Keycloak supports OAuth 2.0 [5] and OpenID Connect [6], which are essential for SMART on FHIR authentication and authorization. However, Keycloak does not natively support the SMART on FHIR specifications, requiring additional extensions to integrate SMART on FHIR capabilities.

Resource server

- *LinuxForHealth FHIR server* [16], developed by IBM under the Alvearie healthcare initiative [12], is a robust, scalable, and extensible FHIR server, supporting all resource types from HL7 FHIR version 4.3.0.
- *HAPI FHIR* [17] is a FHIR server of Smile Digital Health [18], supporting the complete HL7 FHIR standard.

We implemented a SMART on FHIR infrastructure deployment using Keycloak v22.0.1 [13] extended with a customized Alvearie Keycloak extension [19], alongside the LinuxForHealth FHIR server v5.1.1 [16] (cf. Figure 1). The deployment details, including source code, installation instructions, and developer documentation, are publicly available at https://gitlab.ukdd.de/pub/mihubx/smart-on-fhir-ibm-stack for reproducibility and further development. At the time of publication, the repository is at version 0.1.

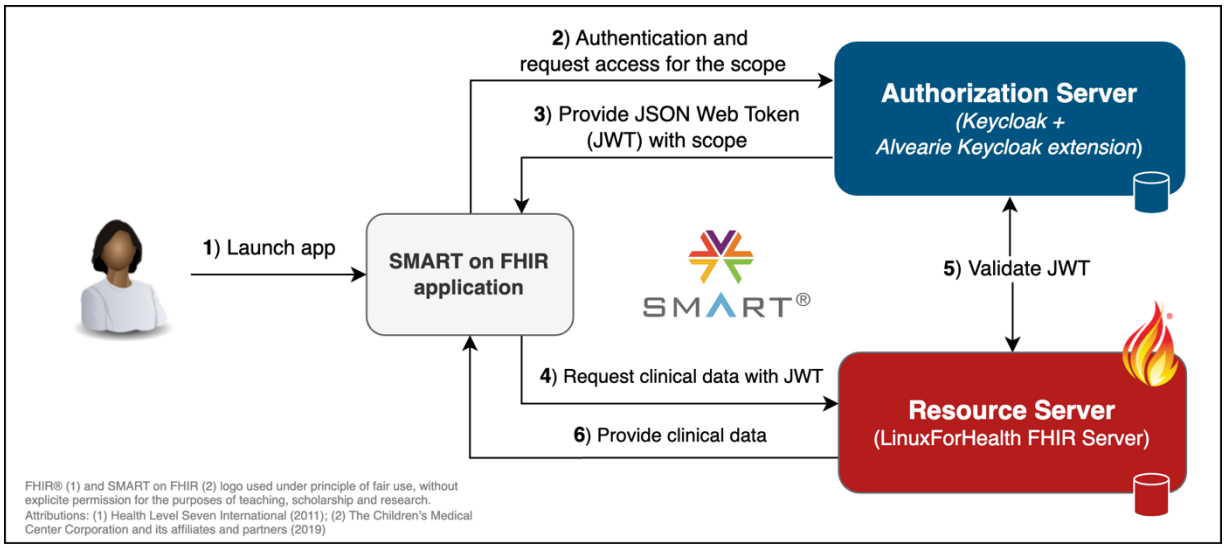

Figure 1: SMART on FHIR supporting reference implementation. The user initiates the app (1), which redirects them to an Authorization Server where they authenticate and consent to data access (2). The Authorization Server then issues an access token granting controlled access to specific FHIR data (3). With this token, the app retrieves the authorized data from the Resource Server (4), which validates the token (5) before providing the requested resources (6).

4. Discussion

Health data is essential for advancing research, improving care quality, supporting AI-driven diagnostics, and empowering patients to access and manage their own health information. This underscores the need for secure, interoperable, and compliant infrastructures for accessing and utilizing health data. The

SMART on FHIR framework provides standardized API specifications to facilitate secure, interoperable connections between healthcare applications and EHRs or other healthcare systems. However, realizing these benefits depends on accessible, vendor-neutral, and open-source solutions, which can enhance interoperability while reducing costs. In this study, we investigated the availability and usability of such solutions to support the deployment of SMART on FHIR applications across healthcare settings.

Our findings highlight the availability of open-source solutions for both Authorization and Resource Servers. Even though the GitHub repositories for both the *Alvearie Keycloak extension* [11] and *igia Keycloak extension* [14] have not released updates recently, development within the community persists. Notably, the *Alvearie Keycloak extension* shows ongoing engagements through forks, pull requests, and discussions within the FHIR community at https://chat.fhir.org [20] and the Keycloak community [21], indicating continued community engagement and development.

For this reason and due to the extensive server documentation, we opted for a vendor-neutral SMART on FHIR reference implementation based on *Alvearie Keycloak extension* as Authorization Server and *LinuxForHealth FHIR Server* [16] as Resource Server. However, this implementation is currently experimental and unsuitable for production environments. Limitations include compatibility issues, such as the Keycloak extension's lack of support for the latest Keycloak server version and the absence of a stable release for the LinuxForHealth server's *fhir-smart* module. Further constraints include that both the Keycloak extension and the LinuxForHealth FHIR Server support only *SMART on FHIR v1*, not the latest v2.2.0 [3].

Despite these constraints, we are confident in the potential of vendor-neutral, open-source SMART on FHIR infrastructures. They offer significant advantages such as enhancing interoperability across diverse healthcare systems, reducing vendor lock-in, and fostering innovation. These solutions can facilitate seamless and secure data exchange and enhance the accessibility of health information. This, in turn, can improve the quality of care, support the development of personalized therapies, and enable more efficient clinical research by ensuring that data can be shared and accessed securely across platforms. Moreover, open-source approaches can lower implementation costs, making advanced infrastructures more accessible across the healthcare sector. They also empower developers to create scalable, reusable applications that benefit healthcare providers, researchers, and patients alike.

Future work will focus on monitoring ongoing technical developments in this field, focusing on whether the components identified and utilized in this study are continuously updated and adapted. Additionally, emerging solutions will be assessed to address or mitigate the limitations identified, particularly for supporting the latest SMART on FHIR specifications and broader API functionalities.

5. Conclusion

This study demonstrates the feasibility of deploying a vendor-neutral, open-source SMART on FHIR infrastructure using currently available Authorization and Resource Servers. While certain limitations, such as lack of compatibility with the latest SMART on FHIR specifications and server versions, currently restrict the implementation for production use, ongoing community-driven development holds promise for addressing these gaps. Continued progress in this area can enhance interoperability, reduce costs, and foster innovation, ultimately benefiting both patient care and clinical research.

Acknowledgments

This work is part of the project "Medical Informatics Hub in Saxony (MiHUBx)", funded by the German Ministry of Education and Research (Grant number 01ZZ2101A).

Declaration on Generative AI

The authors acknowledge the use of OpenAI's ChatGPT, a large language model, for refining the language in this manuscript. All content was reviewed and edited by the authors to ensure scientific accuracy and integrity.

References

[1] J. C. Mandel, D. A. Kreda, K. D. Mandl, I. S. Kohane, R. B. Ramoni, SMART on FHIR: a standards-based, interoperable apps platform for electronic health records, J. Am. Med. Inform. Assoc. 23 (2016) 899–908.

[2] Hl7.org, health level seven international fast healthcare interoperability resources (hl7 fhir), n.d. URL: http://hl7.org/fhir/, (accessed December 15, 2023).

[3] Smart app launch implementation guide (v2.2.0: Stu 2.2), 2023. URL: http://hl7.org/fhir/smart-app-launch/ImplementationGuide/hl7.fhir.uv.smart-app-launch|2.2.0, (accessed September 28, 2024.

[4] Smart/hl7 bulk data implementation guide (v2.0.0: Stu 2.2), 2023. URL: https://hl7.org/fhir/uv/bulkdata/index.html, (accessed September 28, 2024.

[5] Oauth 2.0 rfc 6749, section 4.4: Client credentials flow, n.d. URL: https://datatracker.ietf.org/doc/html/rfc6749#section-4.4, (accessed April 19, 2024).

[6] Openid. openid. san ramon, ca: Openid foundation, 2023. URL: https://openid.net/connect/, (accessed December 18, 2023).

[7] smarthealthit.org, n.d. URL: https://smarthealthit.org/, (accessed November 10, 2024).

[8] Smart on fhir server implementations, 2021. URL: https://confluence.hl7.org/display/FHIR/SMART+on+FHIR+server+implementations, (accessed September 28, 2024).

[9] chat.fhir.org zulip channel "smart,", n.d. URL: https://chat.fhir.org/#narrow/stream/179170-smart, (accessed August 29, 2024).

[10] docker.com, docker compose, n.d. URL: https://docs.docker.com/compose/, (accessed January 19, 2014).

[11] Alvearie/keycloak-extensions-for-fhir (github repository), n.d. URL: https://github.com/Alvearie/keycloak-extensions-for-fhir, (accessed November 12, 2024).

[12] Alvearie healthcare initiative, n.d. URL: https://alvearie.io, (accessed November 14, 2024).

[13] Keycloak: Open source identity and access management, n.d. URL: https://www.keycloak.org, (accessed April 19, 2024).

[14] igia/igia-keycloak, n.d. URL: https://github.com/igia/igia-keycloak, (accessed November 14, 2024).

[15] Igia project, n.d. URL: https://igia.github.io, (accessed November 14, 2024).

[16] Linuxforhealth fhir server, n.d. URL: LinuxForHealthFHIRserver, (accessed November 14, 2024).

[17] Hapi fhir, n.d. URL: https://hapifhir.io, (accessed November 14, 2024).

[18] Smile digital health, n.d. URL: https://www.smiledigitalhealth.com, (accessed November 14, 2024).

[19] hoffmka/keycloak-extensions-for-fhir, n.d. URL: https://github.com/hoffmka/keycloak-extensions-for-fhir, (accessed November 14, 2024).

[20] chat.fhir.org zulip topic "keycloak for smart authz" in "smart" channel, n.d. URL: https://chat.fhir.org/#narrow/channel/179170-smart/topic/Keycloak.20for.20SMART.20authz, (accessed November 14, 2024).

[21] Keycloak discussion: 6753 smart on fhir repository, n.d. URL: https://github.com/keycloak/keycloak/discussions/26753, (accessed November 13, 2024).

A. Online Resources

The source code of the latest server deployment, including initial installation instructions and developer documentation, are available at https://gitlab.ukdd.de/pub/mihubx/smart-on-fhir-ibm-stack. At the time of publication, the repository is at version 0.1.