WP4 Data & Computation

Deliverable 4.4 API interfacing between technological modules

Edited by: < Marc-André Pitre & WP4 members>

Date: < 2024-28-03 >

CONFIDENTIAL

Introduction - Demystifying partner API interfacing in Secur-e-Health

The Secur-e-Health project stands as a pioneering initiative, aiming to revolutionize healthcare through secure data exchange and advanced analytics. This objective hinges on seamless communication between the diverse technological modules contributed by various partner companies. Application Programming Interfaces (APIs) serve as the critical bridge for this interoperability, facilitating data flow and enabling collaboration within the ecosystem.

This initial technical deliverable delves into the intricacies of partner API interfacing plans. It dissects the technical underpinnings of each partner's proposed API, explores potential integration hurdles, and identifies opportunities to leverage these APIs for efficient data exchange. By providing a comprehensive analysis, this document aims to:

- **Unify understanding:** Disseminate a clear technical understanding of each partner's API functionalities and data exchange mechanisms, ensuring all participants possess a shared knowledge base for integration efforts.
- **Foster collaboration:** Identify potential synergies between partner APIs, paving the way for collaborative data analysis and knowledge generation. By understanding API capabilities, researchers and developers can explore opportunities to combine functionalities and unlock new avenues for data-driven healthcare insights.
- **Address integration challenges:** Proactively identify and address potential integration hurdles, such as data format incompatibility or security concerns. A comprehensive analysis allows for early mitigation strategies, preventing delays and ensuring a smooth integration process.
- **Guide future development:** Inform future API design and standardization efforts within the project, ensuring efficient communication across the Secur-e-Health ecosystem. Insights gleaned from this analysis can guide future API development decisions, promoting interoperability and streamlining data exchange across the project.

This document serves as a foundation for ongoing discussions and collaborative API development within the Secur-e-Health project. Please note that this is a first version. As the project progresses, and partner API details evolve, this document will be updated to reflect the latest information and insights. Through continuous refinement, this technical deliverable will remain a valuable resource, guiding successful API integration and ultimately contributing to the overall success of the Secur-e-Health project.

Deep dive into Secur-e-Health partner API interfacing

This section delves into the nitty-gritty of API interfacing plans for various Secur-e-Health partners. We'll dissect the technical underpinnings, explore potential integration hurdles, and identify opportunities to harness the power of APIs for seamless data exchange within the project.

Solita: The FHIR champion

In the context of the planned Finnish use case, Solita is currently exploring integrations with several consortium partners. Due to the recent initiation of these discussions, the details remain fluid and subject to change.

Current integration plan:

- Solita leverages an Integration Platform equipped with a standardized **FHIR API**. This API might require some customization to fully support the specific use case.
- Bittium, a consortium partner, intends to utilize this API to transmit home care data points originating from their Medical Suite product. A demonstration showcasing this integration is planned for completion by next autumn, at the Secur-e-Health's annual review.

VTT Research Environment Integration:

- Data transfer from Solita's integration platform to VTT's research environment is under consideration. This integration might involve Mediconsult, another consortium partner. A dedicated planning meeting with Mediconsult is scheduled for the upcoming month to further explore this possibility. More details to come.

Almende: The secure health Vault

Almende is actively developing a cutting-edge secure health vault designed to store privately owned or maintained health data at the edge or within a private cloud environment. This novel technology will serve as the foundation for offering MPC-like services and privacy-enhancing technologies (PETs). Additionally, secure identity management will be incorporated to facilitate authorized data access. While API integration is envisioned for future development, with a target timeframe of March 2025, the current focus lies on gathering insights from technology providers possessing more mature solutions.

By collaboratively analyzing their offerings, Almende aims to solidify its plans and ensure alignment with the industry's most advanced technologies. More details to come in a second version of this document.

OFFIS & OnCare data exchange API - Connecting the dots between sensors and patient management.

OFFIS is actively developing an API to facilitate data exchange between its platform and OnCare's patient management system, another partner from the German consortium.

Current understanding:

- OnCare's patient management system allows patients to store post-treatment information and request recovery phase details, such as pain questionnaires.
- OFFIS utilizes a sensor system to gather patient recovery data, including IMU, EMG, and pressure sensor readings, which are subsequently stored and analyzed within the OFFIS cloud environment.

Data exchange rationale:

- Patient Outcome Measures (POM) data collected by OFFIS offers valuable insights for a comprehensive analysis by both parties.
- OnCare requires the ability to display OFFIS's analysis results to medical professionals, who can then leverage this information to determine the most appropriate treatment course.

Technical approach:

- An API is being specifically designed to enable the secure exchange of this medical patient data.
- A preliminary functional prototype has already been established, with ongoing development efforts underway.
- Given the nature of the data being exchanged, this API will not be publicly available.

IDENTOS: The gatekeepers of consent and authorization

IDENTOS offers a comprehensive set of authorization and consent management APIs that will play a pivotal role in the project's secure data access architecture. These APIs include industry standards such as OAuth2, OIDC, UMA2, and SMARTonFHIR.

- **OAuth2 and OIDC:** These widely adopted protocols enable secure authorization by delegating user authentication to a trusted identity provider (IdP). IDENTOS's implementation likely leverages these APIs to grant access tokens to authorized users after successful authentication at the designated IdP.
- **UMA2:** This API introduces an authorization server into the OAuth2 flow, providing more fine-grained control over access to protected resources. IDENTOS likely utilizes UMA2 to authorize access to specific data elements within partner systems based on user consent and predefined policies.
- **SMARTonFHIR:** This API facilitates standardized access to electronic health records (EHR) data stored in FHIR-compliant systems. IDENTOS's integration with SMARTonFHIR likely empowers users to grant controlled access to their EHR data within the project context.

Beyond these core APIs, IDENTOS provides integration adapters that streamline the incorporation of external components into their managed solution environment.

- **OIDC IDP integration:** These adapters enable the addition of external OIDC-compliant IdPs, such as Kelvin Zero (planned integration), to IDENTOS's authorization framework. This expands the range of supported authentication methods and potentially strengthens the security posture.
- **FHIR API integration:** IDENTOS's adapters can integrate existing FHIR APIs as protected resources. This allows for controlled access to data residing within these external FHIR systems, potentially including partner solutions like Solita's integration platform.

To facilitate partner testing and integration efforts, IDENTOS plans to establish a sandbox environment. This environment will provide a simulated setting for Secure-e-Health partners to experiment with a demo health consent flow. This will enable partners to test IDENTOS's authorization and consent functionalities within the project's specific context.

In summary, IDENTOS's suite of APIs and integration adapters positions them as a central hub for managing user access and consent within the project. Their planned integration with Kelvin Zero IDP and the sandbox environment further demonstrates their commitment to fostering a secure and collaborative data sharing ecosystem.

Linksight & ZorgTTP : Bridging the gap with pseudonymization

Linksight is actively working to integrate partner ZorgTTP's newly released pseudonymisation service into their product. This integration will leverage ZorgTTP's public APIs specifically designed for this purpose.

Leveraging ZorgTTP's pseudonymisation service:

- By incorporating ZorgTTP's pseudonymisation service, Linksight empowers its clients to link their datasets at the individual level while preserving privacy.
- This functionality facilitates collaborative data analysis on joint datasets without compromising sensitive personal information.

Technical approach:

- Linksight will utilize ZorgTTP's public APIs to interact with their pseudonymisation service. These APIs likely provide functionalities for data submission, pseudonymisation processing, and retrieval of pseudonymised results.

Privacy-enhancing technologies:

- Linksight emphasizes its use of modern cryptography-based privacy-enhancing technologies (PETs) in conjunction with ZorgTTP's pseudonymisation service. These PETs, such as homomorphic encryption and secure multi-party computation, enable collaborative data analysis while ensuring data privacy.

Overall benefit:

- The Linksight and ZorgTTP integration offers a secure and privacy-preserving solution for clients to perform collaborative data analysis on their combined datasets. This fosters valuable insights while safeguarding sensitive individual information.

ORTEC: Unveiling the U-Prevent API

ORTEC U-Prevent boasts a well-established API designed to seamlessly connect with various patient data source systems. This standardized interface facilitates the transfer of data between U-Prevent and the project's chosen data repository. We can provide comprehensive API documentation outlining the specific protocols and functionalities to ensure successful integration.

Current integration landscape:

- For now, there are no documented plans for U-Prevent to establish connections or integrations with other project partner solutions besides the designated patient data source system.
- Initial discussions explored the possibility of linking U-Prevent with MedRecord, but this avenue was not pursued further. It might be in the upcoming months and will be discussed in the second version of this document.

U-Prevent in the project context:

- ORTEC's participation in the program centers on U-Prevent's application within the Dutch use cases.
- The impact of MPC-analyzed local data on individual U-Prevent patient outcomes remains undefined. There seems to be a lack of focus on establishing a fully functional end-to-end workflow incorporating U-Prevent.

Conclusion

This deliverable has provided a preliminary overview of the planned API integrations between the various technological modules within the secure-e-health project. The information presented is based on current understanding and ongoing discussions with our partners. It is important to acknowledge that API specifications are subject to change as technical details are finalized. A more comprehensive Version 2 of this deliverable will be produced in the coming months to reflect this evolution.

In addition to the technical descriptions provided here, we also plan to develop visual aids such as flowcharts and diagrams to further illustrate the API interaction between project components. This will enhance clarity and facilitate a comprehensive understanding of the overall data flow within the secure-e-health ecosystem. These visual aids will be incorporated into the upcoming Version 2 of this deliverable.

We believe that a well-defined and standardized approach to API integration is essential for ensuring seamless communication and data exchange between the diverse project modules. The collaborative efforts described in this deliverable lay the foundation for achieving this objective. As work progresses and technical specifications are finalized, we will continue to refine our API integration strategy to guarantee a robust and secure data sharing environment.