NGI TRUST CHAIN

D1. STATE OF THE ART OVERVIEW, USE CASE ANALYSIS AND PRELIMINARY TECHNICAL SPECIFICATION OF THE SOLUTION

IM4DEC

08/09/2023 (submission date)

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

NGI TRUST CHAIN

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D1. STATE OF THE ART OVERVIEW, USE CASE ANALYSIS AND PRELIMINARY TECHNICAL SPECIFICATION OF THE SOLUTION

IM4DEC

Due date	08/09/2023
Submission date	08/09/2023
Team	OwnYourData, DEC112
Version	1.0
Authors	Christoph Fabianek, Jan Lindquist, Mario Murrent, Gabriel Unterholzer, Wolfgang Kampichler

Funded by the European Union

EXECUTIVE SUMMARY

UN convention Article 9 requires countries to take measures for the full and equal participation of persons with disabilities, including access to communication and information services. Despite this, there are still about 1 million deaf and hard of hearing persons in Europe who currently rely on outdated technology (e.g., fax) and help from others to make an emergency call.

DEC112 is a non-profit association that has designed and developed a standard-conform infrastructure (ETSI TS 103 479) for deaf emergency chats (ETSI TS 103 698). Since 2019, the association is now operating a system in Austria in collaboration with the Ministry of Interior that connects emergency chats to the appropriate emergency communication centre by utilising location information.

However, still a number of challenges exist that are addressed in the NGI TRUSTCHAIN funded project "IM4DEC - Identity Management for the Digital Emergency Call":

- Presenting a verified identity when delivering an emergency chat: replace current SMS verification with an eIDAS 2.0 compliant identity based on DIDs
- Operators struggle with chat from deaf persons: introduce an AI-based chatbot to train users and share this information with emergency organisations as basis for new training material
- Such data (identity, emergency information, training chats) are considered special category data under the GDPR and we will perform a formal DPIA (Data Protection Impact Assessment) for the end-to-end dataflow

The above goals are not only for the benefit of deaf people but also individuals oppressed by domestic violence can make use of this technology through the use of a silent emergency notification; already in operation since 2022 in Austria we will provide an SDK to include this functionality in an EU Digital Identity Wallet to get such functionality on every phone

EU Authorities addressed these topics in Regulation 2023/444 that require all member states to ensure accessible communication services to emergency services from 2025 onwards: With our initiative we want to make sure that such future solutions take special needs of the deaf community and oppressed individuals into consideration.

Funded by the European Union

Table of Contents

Funded by the European Union

LIST OF FIGURES

Funded by the European Union

LIST OF TABLES

Funded by the European Union

ABBREVIATIONS

ARF	Architecture and Reference Framework (for EUDI wallets)
API	Application Programming Interface
BCF	Border Control Function
CAD	Computer Aided Dispatch
CHE	Call Handling Equipment
D2A	Domain specific Data Agreement
D3A	Domain specific Data Disclosure Agreement
DEC	Digital Emergency Communication (previously: Digital Emergency Call)
DID	Decentralised Identifier
DIF	Decentralised Identity Foundation
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DRI	Decentralised Resource Identifier
ECC	Emergency Control Center
ECRF	Emergency Call Routing Function
ESRP	Emergency Service Routing Proxy
ETSI	European Telecommunications Standards Institute
EUDI	European Union Digital Identity
GPT	Generative Pre-trained Transformer
HTTP	Hypertext Transfer Protocol
ID	Identity
JSON	JavaScript Object Notation
JSON-LD	JavaScript Object Notation for Linked Data
LIS	Location Information Service
LoST	Location-to-Service Translation
NG	Next Generation (in Europe: NG112, in the US: NG911)

Funded by the European Union

OIDC	OpenID Connect
OYDID	Own Your Decentralised Identifier (`did:oyd` method)
PSAP	Public Safety Answering Point
PSQL	PostgreSQL (Relational Database Management System)
REST	REpresentational State Transfer
RDF	Resource Description Framework
SIP	Session Initiation Protocol
SHACL	Shape Constraints Language
SMS	Short Messaging Service
SOyA	Semantic Overlay Architecture
SSI	Self-Sovereign Identity
TLS	Transport Layer Security
VC	Verifiable Credential
VP	Verifiable Presentation
W3C	World Wide Web Consortium
YAML	Yet Another Markup Language

Funded by the European Union

1 Introduction

In Austria, dialling 0800 133 133 allows people to contact the police via fax or short message service (SMS). Officials don't have detailed data indicating how often this service is used or how successful it is, but people have repeatedly reported problems. For example, a former Austrian member of parliament's kitchen burned down because she couldn't contact the fire brigades in time. An obvious drawback is that any message received at the Vienna Police Department requires several steps and time until proper resources are dispatched. Organisations that support deaf and hard-of-hearing individuals have expressed the need for text to emergency services and location-based emergency call routing.

Technical standards that enable next-generation emergency calling or next-generation 1-1-2 (NG 1-1-2) are available, so it is a matter of implementing the technology. In 2016, a group of engineers started a private initiative, called Deaf Emergency Calling 1-1-2 (DEC112), to provide a better way to support deaf and hard-of-hearing people. For Austria, this means a solution that allows direct conversations between a person in need and the federal states' control centre and provides location information that can easily be integrated to the control room. The challenges with Austrian emergency services include different emergency numbers and the fact that emergency services are the responsibility of federal states using different call-handling equipment (CHE) or CAD systems. In technical terms, it means different services - at least for fire, ambulance, and police - and service regions for each federal state, combined with next-generation core services and standardised interfaces that make up an NG 1-1-2 architecture.

DEC112 open-source operation in Austria includes several main elements. The emergency services routing proxy (ESRP) is the base routing function for emergency calls, and the primary input to an ESRP is a SIP message, which means that only the call setup via SIP signalling is routed through intermediate functional elements. Media (audio, video, or text) is transmitted end to end. The ESRP maintains an interface to the emergency call routing function (ECRF) for location-based routing information. Emergency calls are routed to the appropriate PSAP based on the location of the caller. The functional element responsible for providing mapping information to querying entities is the ECRF. The ECRF supports the location to service translation (LoST) protocol by which location information and a service uniform resource name (URN) serve as input to a mapping function that returns a uniform resource identifier (URI) addressing the most appropriate PSAP for the caller's location.

Because DEC112 will integrate with different PSAP systems, and based on the workflow previously explained, the team moved on with the following ideas:

Funded by the European Union

- Choose the simplest standardised mechanism available for chat - the SIP SIMPLE instant messaging protocol.
- Implement a PSAP border device or gateway connecting to DEC112 backends
- Send a trigger message (adaptable to local needs) if a message arrives, which contains location, reference data (calling party) and a URL pointing to a local web user interface (UI) with a chat feature. The PSAP CPE or CAD receiving the trigger must support a UI web object that automatically connects to the border device via the URL.
- When integration is impossible, provide a web-based UI to display location, reference data and chat features that can be accessed via a browser

DEC112 implemented the mobile app with a proper backend to register users, considered a public part of DEC112. In addition, core ESRP and ECRF services, considered as emergency services IP network (ESInet), are part of DEC112 to interconnect the public side with the PSAP.

Since February 2019, anyone in Austria may use the DEC112 app to contact emergency services if that person has downloaded and properly installed the app. Properly installing the app requires going through the steps of two-factor authentication requiring a valid mobile number of the device hosting the application. Further, to ensure efficient processing of administrative issues associated with an emergency text, one should also provide additional personal data.

In the case of an emergency, an emergency chat requires just two clicks — one to open the app and another one to choose the required service by selecting one of the icons. Selecting a service immediately triggers a message sent to the proper PSAP including location, reference data and the configured name of the person in need.

OwnYourData is a non-profit association and helps individuals and organisations to achieve unrestricted access to their data for their own benefit. The association offers different services and products – all licensed as Open Source and according to the MyData principles:

- **Semantic Container:** enable secure and traceable data exchange between multiple parties; the solution is standards-based and offers a lightweight infrastructure to make open and commercial data available in an auditable and reproducible manner,
- **Own Your Decentralised Identifier:** the `did:oyd` Method provides a self-sustained and non blockchain-based environment to manage decentralised identifiers.
- **Semantic Overlay Architecture:** a data model authoring and publishing platform that also provides functionalities for validation and transformation.

Funded by the European Union

The project aims to implement and evaluate an important advancement for Decentralised Identifiers: DID Rotation together with relevant standardisation and validation for the DID Resolution process. Furthermore, it provides the technical (Registration Service) and legal (DPIA) basis for individuals to use DIDs. All of this embedded in the highly relevant emergency services domain to support minorities and the oppressed.

2 Motivation and Planned Functionalities

This chapter presents the performed work in the project regarding current status and requirements elicitation. In the course of the project the following steps were already performed, respectively are planned in the next months:

- research and familiarise ourselves with NGI TRUSTCHAIN and other funded projects
- identify relevant list of stakeholders and describe their needs as well as their environment and where they operate
- describe requirements (this document) and derive the Design Specification (D2, due in October 2023)
- setup a dedicated test system for deploying and verifying available components and iteratively feedback any learnings
- deploy solution with partners and other TRUSTCHAIN participants to collect further feedback

2.1 Stakeholder

Initially, a list of relevant stakeholders was compiled:

- **Deaf and hard of hearing persons** as users of the DEC112 App
  (tag: user)
- **Individuals with a government issued digital identity** in an EUDI ARF-compliant wallet
  (tag: cit - citizens)
- **Control rooms and emergency service providers** as users of the DEC112 Border and Viewer application
  (tag: cr - control room)
- **Organisations representing deaf and hard of hearing persons** for promoting the DEC112 solution
  (tag: org - organisation)
- **Government & politics** for establishing legal circumstances to operate emergency chats
  (tag: gov - government)
- **Public Safety industry** for integrating with the DEC system
  (tag: ps - public safety industry)
- **Community of volunteers** to develop and operate the DEC system
  (tag: com - community)

All requirements were mapped to at least one of those stakeholders to document source and motivation. During the course of the project multiple data flows will be implemented that demonstrate the interaction of above stakeholders.

2.2 Non-Functional Requirements

2.2.1 Performance and Scalability

Requirements that describe throughput under a given workload for a specific time frame in each setting.

ID	Tags	Description
perf_1	gov, org	The overall DEC112 system shall handle at least 100.000 registered users.
perf_2	gov, org	The overall DEC112 system shall handle at least 50 concurrent emergency chats.
perf_3	org	The chatbot shall handle at least 10 concurrent training chats.

Table 2.1: Performance and Scalability Requirements

2.2.2 Portability and Compatibility

Requirements to make sure that the system can be operated now and in the foreseeable future on the available platform infrastructure and also works together with adjacent systems.

ID	Tags	Description
port_1	ps, gov, com	Available standards and best practices for the respective areas should be identified and adhered to.
port_2	com	Data exchange between building blocks shall use JSON.
port_3	ps, com	Interfaces of the different components shall be clearly defined and documented.

Table 2.2: Portability and Compatibility Requirements

2.2.3 Reliability, Availability, and Maintainability

Requirements describing the accessibility of the system to the users at a given point in time and how to quickly recover from any failures.

ID	Tags	Description
rel_1	com	Components shall be easy to deploy and configure. (In this project Docker containers are the preferred way to make the developed software artefacts available.)
rel_2	com	All software components shall be documented.
rel_3	com	The system shall perform input validation.

Table 2.3: Reliability, Availability, and Maintainability Requirements

2.2.4 Privacy and Security

Requirements about privacy (safeguarding data) and security (authorization and protection) needs from different stakeholders.

ID	Tags	Description
priv_1	gov	All external data transfer shall be encrypted through TLS for communication over a network.
priv_2	gov	Consent information for data exchange (using Data Agreements) shall be documented and inseparably linked to the payload.
priv_3	gov, com	A privacy assessment shall be performed for the overall DEC112 system.

Table 2.4: Privacy and Security Requirements

2.2.5 Localisation

Specify requirements in line with the context of the target audience.

ID	Tags	Description
loc_1	com	The user interface shall support displaying in multiple languages.
loc_2	user, cit	The user interface shall be available at least in German, English.

Table 2.5: Localisation Requirements

2.2.6 Usability

Requirements that define the ease-of-use for the system.

ID	Tags	Description
usab_1	gov, user, cit	The user interface shall be designed to be usable also in stressful situations when performing an emergency chat.
usab_2	gov	Confirmation of the identity shall require the use of a government issued identity.
usab_3	user, cit	Texts should be written in an easy-to-understand language.

Table 2.6: Usability Requirements

2.3 Registration API

The DEC112 Registration API (RegAPI) is responsible for managing DEC112 registrations and to provide configuration information for DEC112 clients (DEC112 App).

ID	Tags	Description
reg_1	com	The RegAPI shall provide an API for DEC112 clients to retrieve local configuration data.
reg_2	com	The RegAPI shall provide an API for DEC112 clients to register new users.
reg_3	gov, cr, com	Registering new users shall require presentation of a government issued identity.
reg_4	ps	Information about the government issued identity shall be accessible in a control room.

Table 2.7: Registration API Requirements

2.4 Trigger SDK from Wallet

Requirements for an SSI wallet to trigger a silent emergency notification.

ID	Tags	Description
wal_1	com, gov	It shall be possible to create W3C DID for natural persons that uses a non-blockchain based trust registry in an EUDI ARF compliant wallet.
wal_2	com	The system shall support a workflow to create a W3C Verifiable Credential based on a government issued identity.
wal_3	com, cit	It shall be possible to transfer a W3C Verifiable Credential holding a government issued identity to an EUDI ARF compliant wallet.
wal_4	com, cit, cr	An EUDI ARF compliant wallet shall support the functionality to trigger a silent emergency notification when a valid W3C Verifiable Credential with a valid government issued identity is present.

Table 2.8: Trigger SDK from Wallet Requirements

Funded by the European Union

2.5 CHATBOT

A chatbot is used to improve the experience for training emergency chats.

ID	Tags	Description
bot_1	com, user	The chatbot shall use generative AI to provide a realistic emergency chat experience.
bot_2	user	The chatbot shall be integrated into the DEC112 environment to allow all users to train emergency chats.
bot_3	user, org, ps	The system shall enable users to consent to sharing a chat session with emergency organisations.
bot_4	com, gov, cr	Data Agreements shall be used to document the data exchange of chat sessions between the DEC112 association and emergency organisations.
bot_5	org, cr	Emergency organisations shall be able to use chatbot conversations for integration into internal training.

Table 2.9: Chat Bot Requirements

2.6 DID:OYD ADVANCEMENTS

The current limitation of not being able to seamlessly switch between DID methods (also known as DID Rotation) for an existing DID is addressed with the following requirements.

ID	Tags	Description
did_1	com, cit	Upon DID rotation the original DID must include a reference to the updated DID to enable a resolver switching between DID methods.
did_2	com, cit	Upon DID rotation the updated DID must include a reference to the original DID to allow full history lineage.
did_3	com, cit	Upon DID rotation there must be a proof that the original DID was deactivated to prohibit any forks.

Funded by the European Union

ID	Tags	Description
did_4	com, cit	Upon DID rotation the updated DID must include a proof that covers original and updated DID based on a private key from the original DID to document the legitimacy of the update.

Table 2.10: did:oyd Advancement Requirements

3 User Stories and Use Case Analysis

This chapter provides user stories based on the requirements from the previous chapter.

3.1 User Stories

Registration API

As a deaf person I want to be authenticated to be able to perform emergency communication using chat functionality so that I can get help.

As an emergency response organisation I want any incoming emergency communication to be associated with an identity so that misuse can be traced back.

Trigger DEC112 SDK from Wallet

As a person in an emergency situation I want to be able to perform a request for immediate help with the single press of a button so that nobody notices my request for help.

As a person in an emergency situation I want my identity and current location made available to the emergency response organisation so that they have all required information for a quick response at the scene.

As a person who might require immediate help in an emergency situation, I want to have the functionality provided as inconspicuously as possible on my smartphone, so that other people cannot easily take it away.

Chatbot

As a deaf person I want to be able to train emergency communication using chat functionality so that I can prepare for an emergency situation.

As a user of an emergency chat training system I want to have the call taker simulation as realistic as possible so that I can gain practical experience in handling crisis situations.

As an emergency response organisation, I want our call takers to receive specialised training in communicating with deaf individuals through emergency chat systems, so that they can more effectively address the unique needs of this community in crisis situations. A crucial component of this training is the inclusion of exemplary chat conversations.

As the DEC112 organisation we want to share training chat data with emergency

Funded by the European Union

response organisations only through methods that adhere to the strictest privacy regulations so that we ensure full legal compliance.

did:oyd Advancements

As controller of a DID I want to be able to seamlessly switch between DID methods (also known as “DID Rotation”) so that I’m not locked into a single DID method.

As a user I want to verify if a DID method supports all necessary properties for DID Rotation so that I can create an informed decision when choosing from the many available DID methods.

Funded by the European Union

3.2 Use Case Analysis

The following use cases will be used to showcase the functionality described above.

DEC112 Onboarding with ID Austria

To provide a verified identity in the DEC112 app (available for Android and iOS), the existing DEC112 Registration Element (Registration API) is updated to support the onboarding process using an existing eIDAS identity provider (in Austria the eIDAS conform "Bürgerkarte" and "Handy Signatur", and now the already available "ID Austria'' will develop into an eIDAS 2.0-conform identity provider).

Upon receiving a verified identity (using OIDC, Authorization Code Flow), SIP credentials are created in the SIP Service and stored on the DEC112 app so that emergency chats can be initiated.

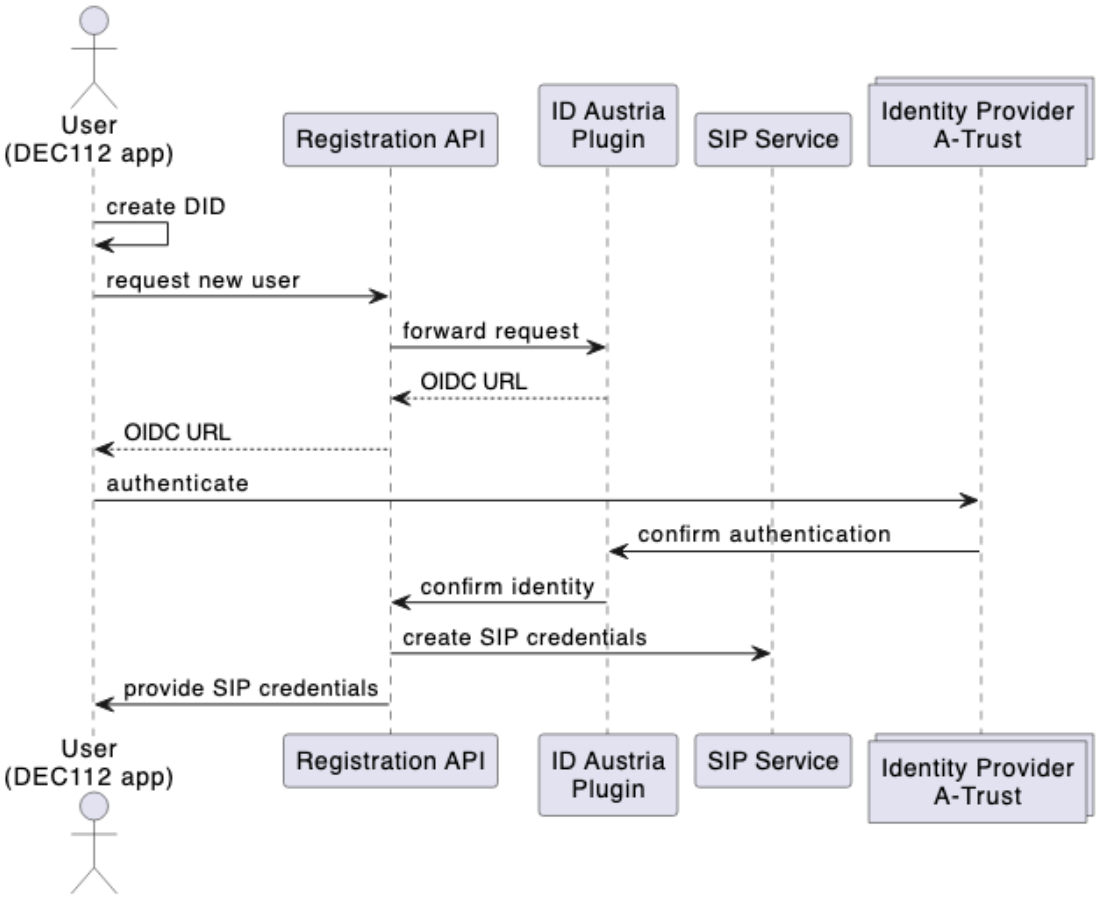

Figure 3.1: Onboarding with ID Austria

Triggering a Silent Emergency Notification from the Sphereon Wallet

To give as many people as possible access to emergency services, DEC112 and the Austrian Ministry of the Interior extended its services in April 2022 to offer a "Silent Emergency Notification": either in situations when you cannot talk (e.g., shooting in a bank) or also for individuals oppressed by domestic violence. Especially, for domestic violence the challenge is to have an unobtrusive app so that an aggressor does not remove the app from the victims smartphone.

In this use case we use a government issued identity (ID Austria) and OwnYourData acts as Issuer for a Verifiable Credential that holds personal data (name, address) and the signature certificate. Based on this identity SIP credentials are created and also added to the Verifiable Credential. The Verifiable Credential is added to an EU Digital Identity Wallet (we plan to use the wallet from Sphereon[1]) and through the DEC112 SDK a silent emergency notification can be triggered from within the wallet.

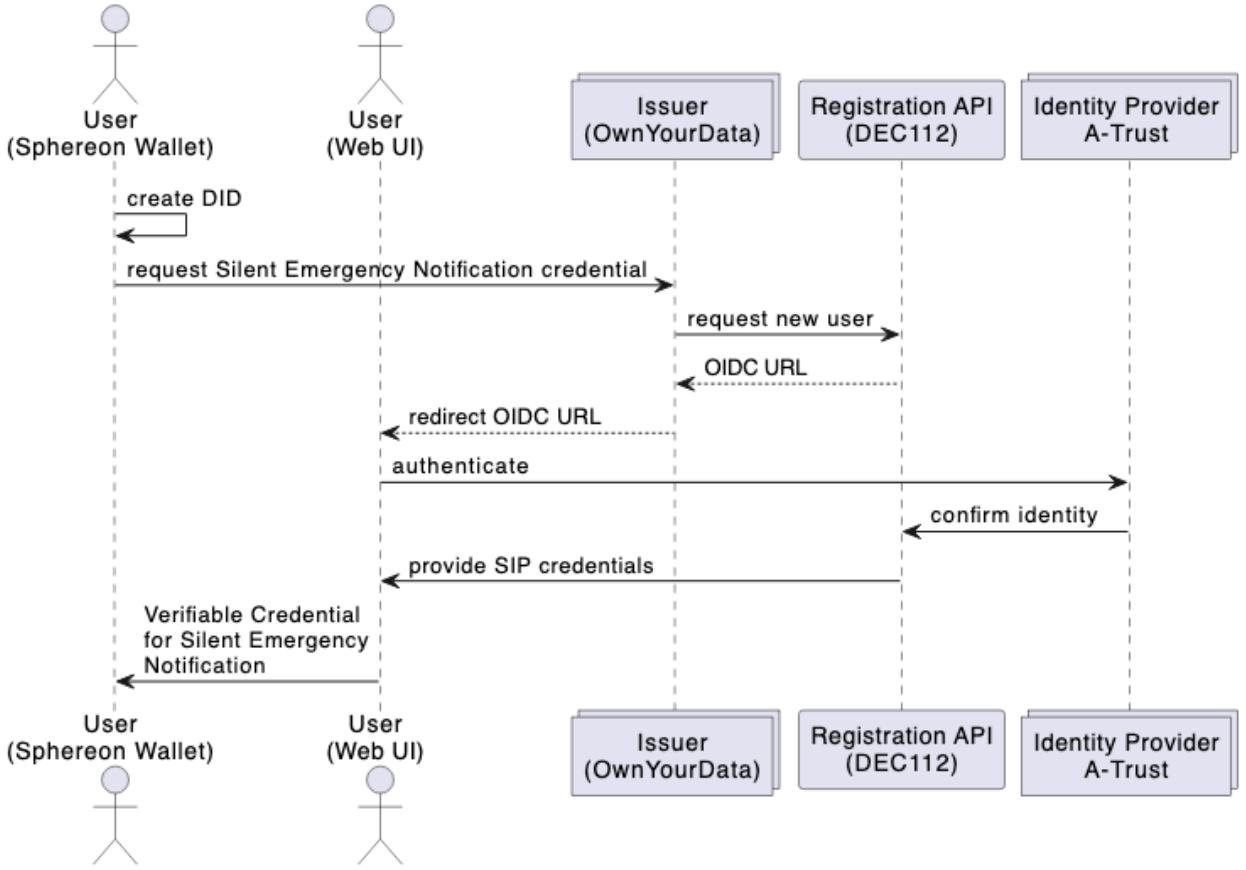

Figure 3.2: Silent Emergency Notification from Sphereon Wallet

[1] https://sphereon.com/sphereon-products/sphereon-wallet/

ChatGPT based Chatbot and Data Sharing

On the other end of an emergency chat is an operator in a control room that needs to be specifically trained on how to handle communication with a deaf person. With the advent of AI-based chatbots (e.g., ChatGPT) we want to provide functionality to simulate a control room operator and enable all DEC112 users to simulate emergency chats. Those chats can be - upon consent - shared with emergency service providers to increase the available training material for operators.

The whole process of collecting and sharing chat data is ensured to be GDPR compliant through a Data Protection Impact Assessment and using Data Agreements to document the data exchange.

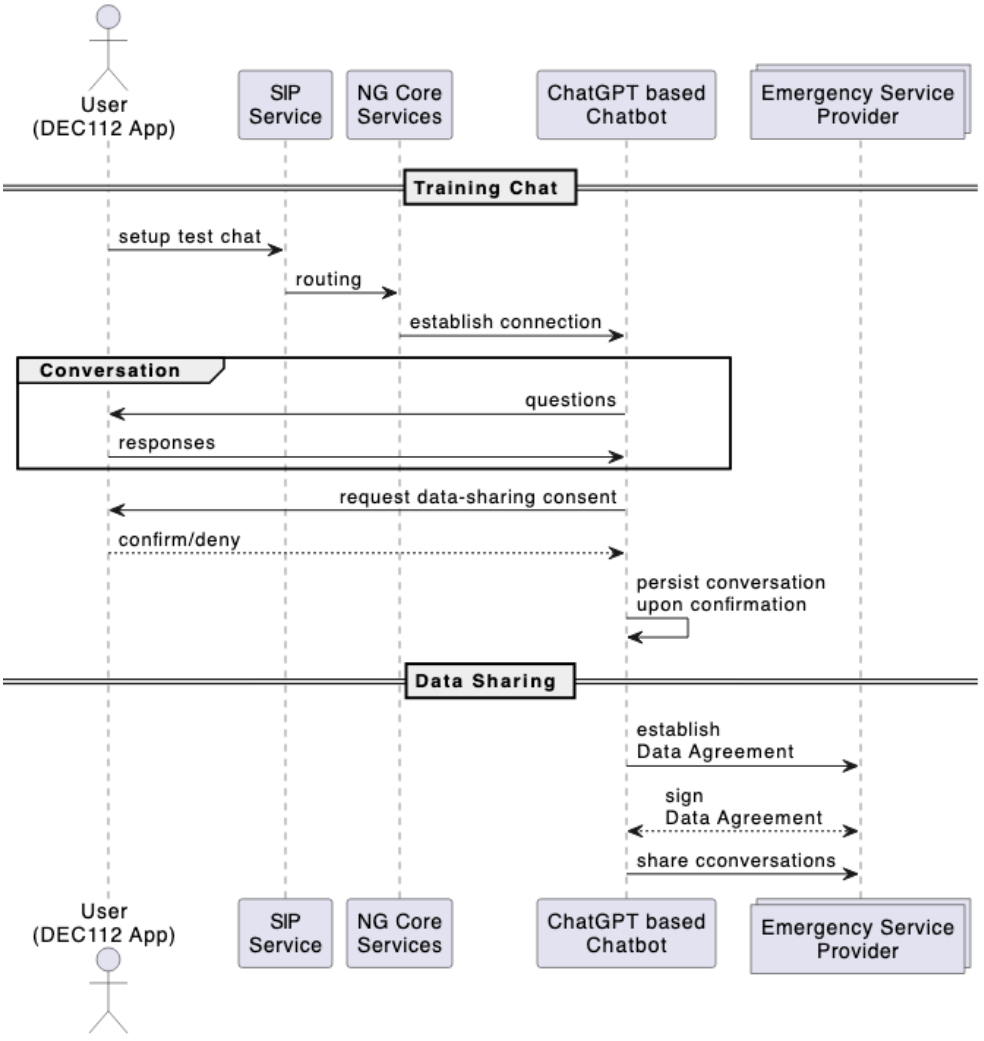

Figure 3.3: ChatGPT based Chatbot and Data Sharing

DID Rotation

DID Rotation refers to the process of changing (or "rotating") the underlying DID method for a given Decentralised Identifier. The concept is rooted in the best practices of cryptographic key rotation, where keys are changed periodically to reduce the risk of compromise. In the same way, periodically rotating a DID could reduce the risks associated with a specific DID method. And of course it avoids a lock-in situation into a given DID method.

Rotating a DID method involves a number of steps and Figure 3.4 depicts one possible approach that transforms an original DID `v1` into a new DID `v2'`. As detailed in the requirements section 2.6 it is necessary to take a number of precautions to ensure complete evidence when updating the DID method.

One specific challenge when performing a DID rotation is to ensure full compliance of both DID methods with relevant properties of the DID Core Specification[2]. To validate those properties the OwnYourData DID Lint service[3] will be extended with checks in the DID metadata and the resolution process. Only DID methods compliant with these checks are possible candidates for DID rotation. Currently, we plan to demonstrate DID rotation from the `did:oyd` to the `did:ebsi` method.

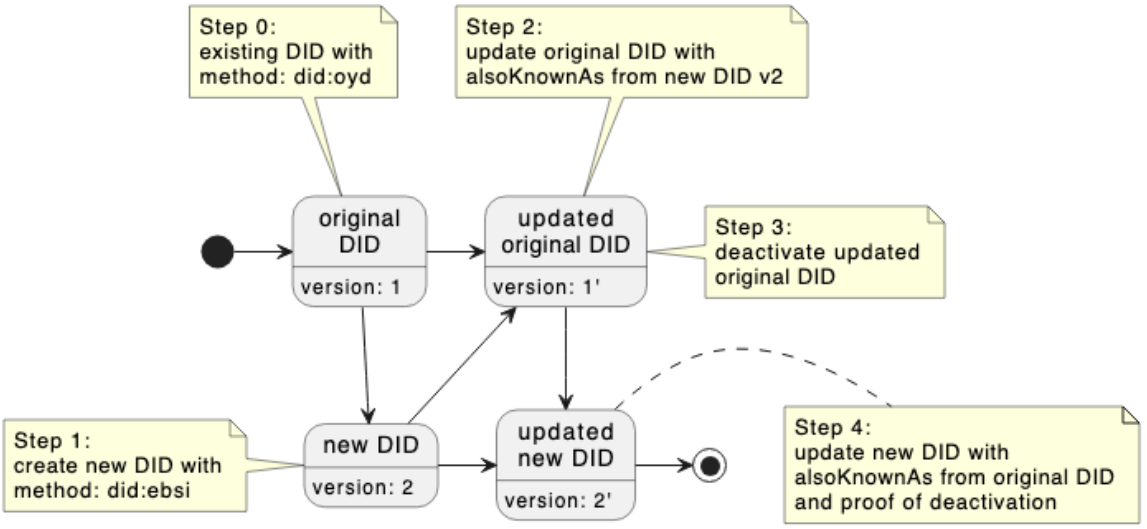

Figure 3.4: DID Rotation

[2] https://www.w3.org/TR/did-core/
[3] https://didlint.ownyourdata.eu/

4 State of the Art Analysis, Background, AND Innovation

This section is dedicated to the analysis of existing solutions, including developments, and demonstrating the innovation potential of the solution compared to what already exists.

4.1 State of the Art Analysis

In the course of the project the following standards were identified and are adhered to in developing the system:

- **JSON-LD** v1.1 a light-weight Linked Data format
  described in detail here: https://www.w3.org/TR/json-ld/
- **Decentralised Identifier** (DIDs) for managing identities of entities;
  described in detail here: https://www.w3.org/TR/did-core/
- **Verifiable Credentials** (VCs) expressing credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable
  described in detail here: https://www.w3.org/TR/vc-data-model/
- **ETSI TS 103 479** - Core elements for network independent access to emergency services; described in detail here:
  https://www.etsi.org/deliver/etsi_ts/103400_103499/103479/01.02.01_60/ts_103479v010201p.pdf
- **ETSI TS 103 698** - Lightweight Messaging Protocol for Emergency Service Accessibility with a focus on chat functionality; described in detail here:
  https://www.etsi.org/deliver/etsi_ts/103600_103699/103698/01.01.01_60/ts_103698v010101p.pdf

In addition, the following specifications were used or will be further developed:

- **Data Agreements** record conditions for an organisation to process data in accordance with a privacy regulation (e.g. GDPR)
  described in detail here:
  https://github.com/decentralised-dataexchange/automated-data-agreements/blob/main/docs/data-agreement-specification.md
- **did:oyd Method (OYDID)** a self-sustained environment to manage decentralised identifiers
  described in detail here: https://ownyourdata.github.io/oydid/

- **Semantic Overlay Architecture (SOyA)** data model authoring and publishing platform
  described in detail here: https://ownyourdata.github.io/soya/

4.2 Description of Background

4.2.1 DEC112 Infrastructure

Since 2019 DEC112 has been operating NG112 core services including the text-based DEC112 emergency communication in Austria and constantly and actively develops these services. Big parts of software components are available as Open-Source on Github[4].

The DEC112 system in Austria currently comprises three main functions: the mobile application (DEC112 App, described below), core services and several connections to Austrian emergency control centres. Interfaces between core services and other components (e.g., DEC112 App or control centres) are based on the standards ETSI TS 103 479 and ETSI TS 103 698.

The association operates an ECRF (Emergency Call Routing Function, see ETSI TS 103 479). An ECRF is a LoST (Location-to-Service Translation, see ETSI TS 103 479) protocol server where location information (either address or geo-coordinates) and URN (service name) are used as input and a URI is used to route an emergency call to the appropriate PSAP for the caller's location.

In addition, an ESRP (Emergency Service Routing Proxy, see ETSI TS 103 479) is part of the DEC112 core services. An ESRP is a SIP proxy server which selects routing for the next destination within the DEC112 core services based on location (using LoST query to the ECRF) and optional policy rules (e.g., the control centre's availability and/or workload). This routing decision is used to route an emergency call (e.g., from the DEC112 app) to the appropriate control centre.

The described routing process (involving both the ESRP and ECRF) is essential to direct emergency calls to the most appropriate control centre based on the user's need and location. The DEC112 app itself is not involved in the routing decision and therefore, does not need any information about any (potentially complex) structural properties of available control centres.

DEC112 PSAP is used to establish connections from SIP to other technologies. Given the fact that most established vendors of emergency call processing equipment are mainly focusing on traditional phone calls rather than text-based emergency communication, a technology-bridge is necessary to enhance those systems with

[4] https://github.com/DEC112

emergency chat capabilities. DEC112 PSAP provides services for processing SIP-based emergency calls. The most prominent of these, the chat service, is used to route emergency messages between the person making the emergency call and the control centre (mainly via the web-based DEC112 Viewer, accompanied by a trigger-based integration into existing call processing systems). Other services provide, for example, automated information for emergency callers (like chatbots).

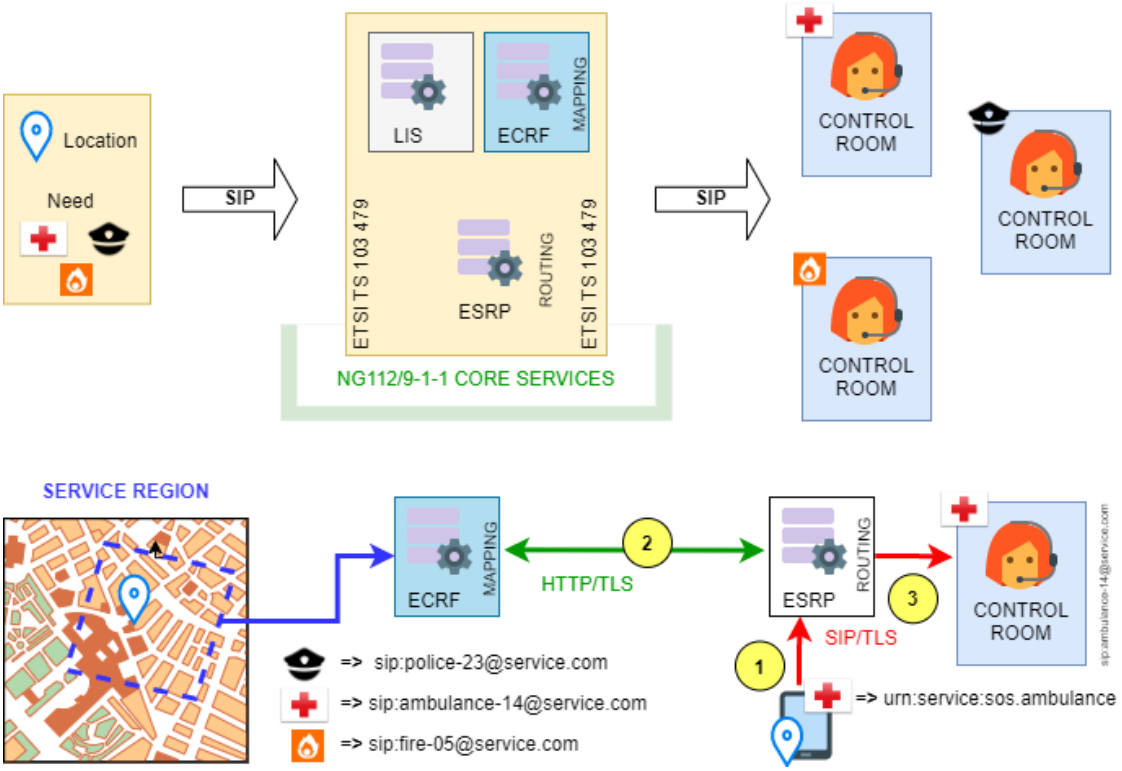

Figure 4.1: DEC112 Infrastructure Components

4.2.2 DEC112 App

A noteworthy and groundbreaking feature of the DEC112 2.0 app is its capability for deaf individuals to communicate directly with emergency call centres via a chat in case of emergencies. Utilising a text chat format, this app facilitates deaf individuals in easily accessing professional assistance when they need it most.

However, the DEC112 2.0 App doesn't just focus on communication; it also automatically sends health data and the user's current location to the emergency call centre. These central pieces of information significantly enhance the efficiency of emergency responses by providing rescuers with crucial information promptly.

In Austria, the app provides access to a wide range of emergency services, including

Funded by the European Union

the Fire Department (emergency number 122), Police (emergency number 133), Ambulance (emergency number 144), Mountain Rescue (emergency number 140), the European Emergency Number (emergency number 112), and even a silent emergency notification.

The DEC112 2.0 App stands out due to its intuitive, efficient, and secure design. Its user interface has been intentionally crafted to enable users to focus on the essentials during emergencies without being distracted by unnecessary elements.

Through the utilisation of GPS in your smartphone, the app accurately determines your location, ensuring precise and targeted assistance. Your personal data is treated with the utmost confidentiality—only being transmitted to the emergency call centre in the event of an actual emergency, while remaining solely stored on your device otherwise.

Moreover, the app features a training mode for emergency calls, allowing users to become familiar with its functions and procedures. This promotes a better understanding and increased confidence in using the app.

The DEC112 2.0 App represents a significant complement to the already established Deaf SMS service (0800 133 133) in Austria. It embodies progress in the realm of barrier-free communication and constitutes another step toward a more inclusive society, where all individuals, regardless of their specific needs, can be effectively safeguarded.

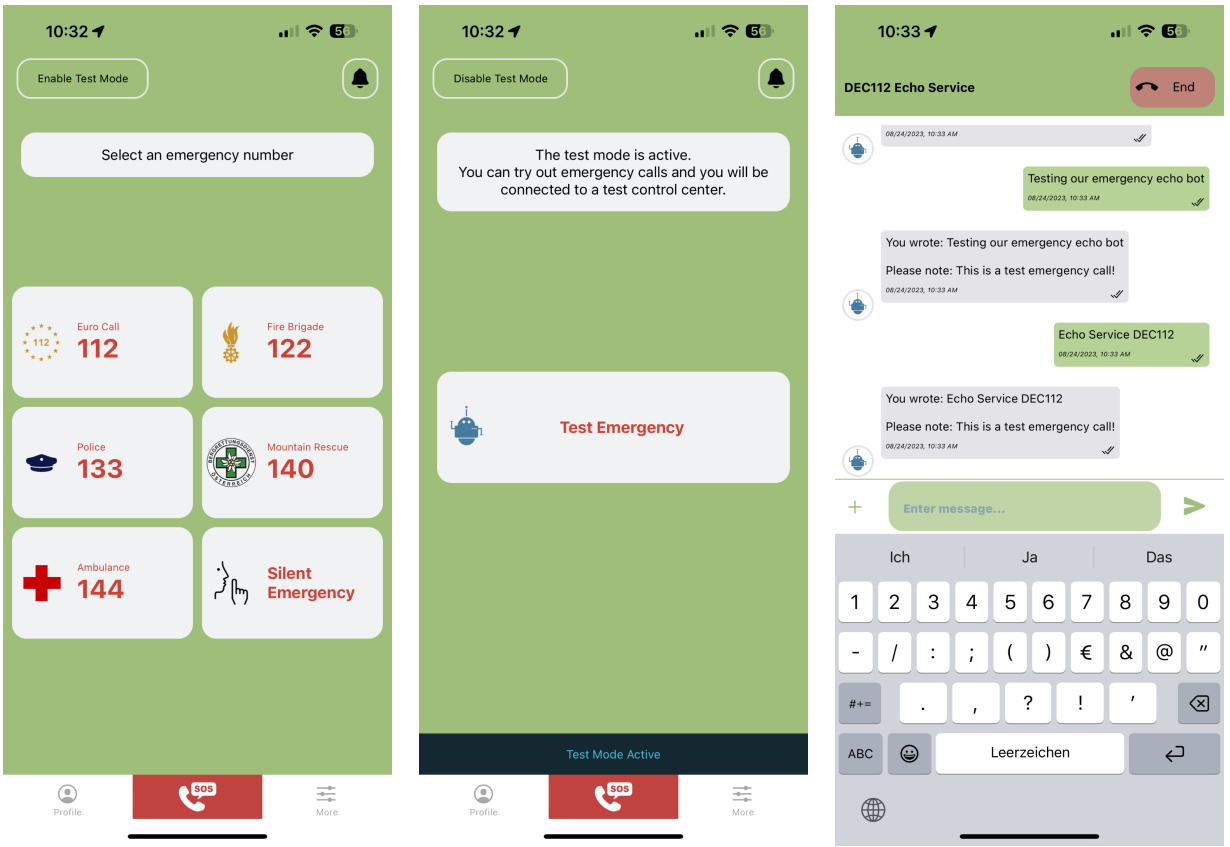

Figure 4.2: DEC112 App

4.2.3 Semantic Container

Semantic Containers provide a standardised infrastructure for data provisioning and allow data providers to efficiently distribute data without giving up control over its usage and monetization while providing data consumers with efficient and well-managed mechanisms to obtain and integrate data in a trustworthy and reproducible manner. By packaging data and processing capabilities into reusable containers, describing the semantics of the content and permissible usage, and providing uniform interfaces, a data set becomes a commodity with well-defined content, properties, quality, and usage policy, as well as clear ownership rights and a price tag.

The Semantic Container approach leverages existing container technologies such as Docker, which already provide scalable mechanisms for deploying complex software assemblies and use them as a foundation for an infrastructure for data discovery, provisioning, and integration. To create a suitable environment for the emergence of

Funded by the European Union

a commodity market around data, a set of rules for permissible usage of the data is captured in semantic descriptions, provides cryptographic methods to prove ownership rights, and applies blockchain technology to guarantee immutability. Complete audit trails of data sources and processing steps provide gapless provenance and facilitate reproducibility.

A W3C conform Community Group Specification is available here:
https://ownyourdata.github.io/semcon/

4.2.4 did:oyd Method (OYDID)

The aim of the did:oyd method is to provide a decentralised identifier (DID) that is not based on a distributed ledger. Many DID methods are based on blockchain technology and provide a trust anchor based on the respective governance of the used ledger for handling sensitive data. For certain aspects however, it could be interesting to have DIDs that don't require the full stack of a decentralised system. OYDID provides such a self-sustained environment for managing digital identifiers. The did:oyd method links the identifier cryptographically to the DID Document and through also cryptographically linked provenance information in a public log it ensures resolving to the latest valid version of the DID Document.

A W3C conform DID Method Specification is available here:
https://ownyourdata.github.io/oydid/

4.2.5 Semantic Overlay Architecture (SOyA)

SOyA allows data structures to be described in simple terminology. This description includes groups of data records with the same attributes, references between data records, and meta-attributes of these data structures.

Datasets are referred to as "bases", while meta-attributes are summarised in so-called "overlays". Overlays can contain information about attributes (e.g. detailed descriptions, permissible values, or formatting), but also transformations into other data structures.

For the exchange of these definitions of data structures, those structures can be stored in online repositories. When saving in such repositories, 2 versions are created:

- the original variant with the given names of the individual artefacts (i.e. of Structure, Base, and Overlay)
- a "frozen" variant where each name is replaced by a DRI; the DRI is a content-based address, which is also the unchangeable fingerprint of the content. This ensures that the previous version remains available if changes

are made later.

With the described definitions of data structures, concrete data can now be recorded. SOyA offers the following functions:

- Acquire: If the attributes are named accordingly in a simple JSON ("flat JSON"), a conversion into JSON-LD can take place automatically
- Validate: Existing data records can be checked for conformity using a Validate overlay
- Transform: you can switch between data structures with a transformation overlay; It is thus possible to retain existing data formats (legacy formats), while automatic mapping to new standards is guaranteed
- Capture: with automatically generated HTML forms based on the structure information, data can be conveniently visualised, recorded and processed

A W3C conform Community Group Specification is available here:
https://ownyourdata.github.io/soya/

4.2.6 Data Agreements

The ability to share and exchange data seamlessly across different organisations and systems is crucial for operational efficiency, cost reduction, and customer satisfaction. This is where data agreements come into play. Data agreements are essentially contracts that define the terms and conditions for data sharing between different entities from a source to a third-party. They set the usage policies for data access, ensuring that all parties involved adhere to the agreed-upon rules and regulations.

The Decentralized Identity Foundation[5] (DIF) has established a task force referred to as the "Data Agreement". This group is actively developing a specification that delineates the structure of data agreements. DIF's data agreements are rooted in the General Data Protection Regulation (GDPR) principles, and incorporate the recording of consent notices.

Further information about Data Agreements can be found here:
https://github.com/decentralised-dataexchange/automated-data-agreements/blob/main/docs/data-agreement-specification.md

4.3 Innovation Compared to the State of the Art

In recent years, the landscape of identity verification and management, especially within the realm of government-regulated sectors, has undergone tremendous

[5] https://identity.foundation/

shifts. Pioneering the next wave of innovations, several advancements distinctly set our IM4DEC project apart from the state of the art:

Documenting Government Issued Identities with Verifiable Credentials (VCs): Our solution leverages Verifiable Credentials, ensuring a digital proof that is not just trustworthy but also streamlined for modern applications.

Integration of eIDAS2 Conform Identities in Onboarding: The onboarding process, particularly for projects within the safety-critical infrastructure sector, demands utmost reliability and security. By integrating eIDAS2 conform identities, we ensure the integrity and validity of individuals using a safety critical service like the silent emergency notification. This alignment with the established eIDAS2 framework ensures compliance while enhancing the trustworthiness of our system.

EUDI AFR Compliant Wallets and Emergency Notifications: In a novel application of government-issued identity, we plan to integrate its use within an EUDI AFR compliant wallet. This not only consolidates identity verification but also seamlessly facilitates the triggering of silent emergency notifications, bridging the gap between personal identification and critical response mechanisms.

Generative AI for Training in Emergency Chats: Leveraging the power of generative AI, we have devised a platform that simulates emergency chats. This innovative approach trains users effectively, preparing them for real-world crises. Furthermore, the resulting chat protocols can be shared with relevant authorities using Data Agreements, enhancing transparency, and cooperation.

Robust Privacy Assessment of Processes: Recognizing the importance of data protection, especially in an age of digital vulnerabilities, we have undertaken a comprehensive privacy assessment of our initiative. This ensures that while we break new ground in innovation, the privacy and security of users and stakeholders are never compromised.

In conclusion, our efforts distinctly set the benchmark for combining technological advancements with practical, safety-critical applications, redefining the paradigm of government identity management and its intersection with emergency response mechanisms.

Funded by the European Union

5 Software Design and Analysis, Component Specification (Preliminary)

This chapter provides a technical description of the planned components and the overall architecture diagram.

5.1 Software Modules

5.1.1 Registration API

The Registration API (short: RegAPI) takes the request from a client (e.g., DEC112 app, SSI wallet, IoT sensor station) and generates SIP credentials after verifying the identity of the user triggering the request. The SIP credentials can then subsequently be used for initiating an emergency chat or a silent emergency notification.

RegAPI Components:

- **REST Endpoint:** the external interface of RegAPI and orchestrator of processes
- **Redis:** transient data store with a hashmap storage for objects being processed and publish/subscribe mechanisms for services to interact
- **IDA Service:** identity provider plugin in RegAPI to interact with A-Trust (the Austrian identity provider for the government issued identity "ID Austria")
- **SMS Service:** legacy plugin to verify a provided phone number through sending a 6-digit code to the user
- **SIP Service:** after an identity is verified (either through ID Austria or SMS code verification) SIP credentials are generated, stored in a hashed version in the Kamailio DB, and returned encrypted to the client

Security considerations:

- requests to the RegAPI require OAUTH2 authentication using DID Auth for clients that have DID support
- For mobile apps the API can be secured through app attestation:
    - Android: https://developer.android.com/google/play/integrity/overview
    - iOS: https://developer.apple.com/documentation/devicecheck/establishing_your_app_s_integrity

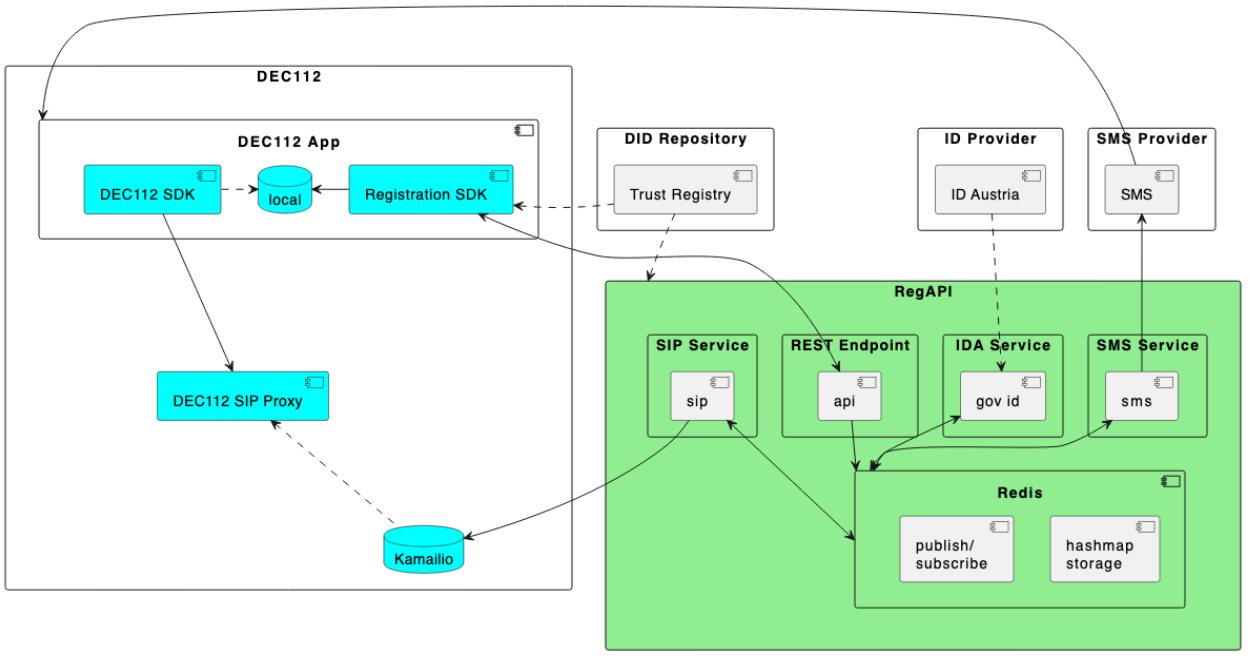

Figure 5.1: Registration API Components (green components are new developments, cyan components exist and might require adoptions)

5.1.2 Wallet

The Wallet is an alternative way for users to send a silent emergency notification using the SIP credentials created during the onboarding process and stored in a Verifiable Credential.

Wallet Components:

- **Issuer:** a web service hosted by OwnYourData (i.e., acting as issuer) is built based on the *OID4VC Issuer and Verifier Demo*[6]; it uses information from the Registration API (provides an ID Austria identity and creates SIP credentials), creates a Verifiable Credential, and allows transfer to an SSI Wallet
- **SSI Mobile Wallet:** based on the Sphereon SSI wallet a dedicated agent is developed that supports the `did:oyd` DID method, and processing of Verifiable Credentials that hold SIP credentials to initiated a silent emergency notification using the DEC112 SDK
- **SDK Crypto Extensions:** management of available DID methods is encapsulated in the SDK Crypto Extensions component and the component is extended to support the non-blockchain based `did:oyd` DID Method

[6] https://github.com/Sphereon-Opensource/OID4VC-demo

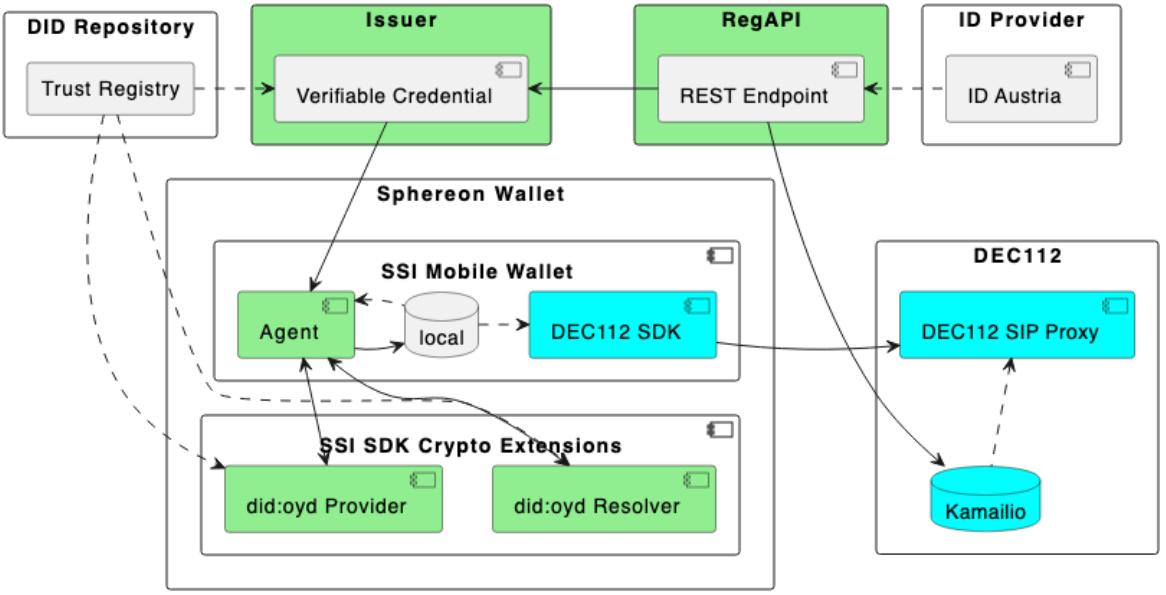

Figure 5.2: Wallet Components (green components are new developments, cyan components exist and might require adoptions)

5.1.3 Chatbot

The chatbot registers as an available endpoint for training chats (initiated in the DEC112 app with the "Test Emergency" button. It can also store conversations (upon consent from the user) and share it later using Data Agreements with an emergency response provider who can use it as additional training material for call takers.

Chatbot components:

- **DEC112 Endpoint:** the endpoint registers at the terminating ESRP and receives any incoming messages / publishes response using a websockets connection
- **Chatbot Service:** performs two functionalities
  - simulate call taker messages through the OpenAI provided ChatGPT API - see also Appendix C ChatGPT Privacy Analysis
  - orchestrate data exchange with other parties through Data Agreements
- **Emergency Service Provider:** this entity is covered in Austria by the Ministry of the Interior; to be able to demonstrate the functionality on a technical level, we will fully simulate this entity with a Semantic Container and in ongoing talks aim for integration in the overall process of the ministry

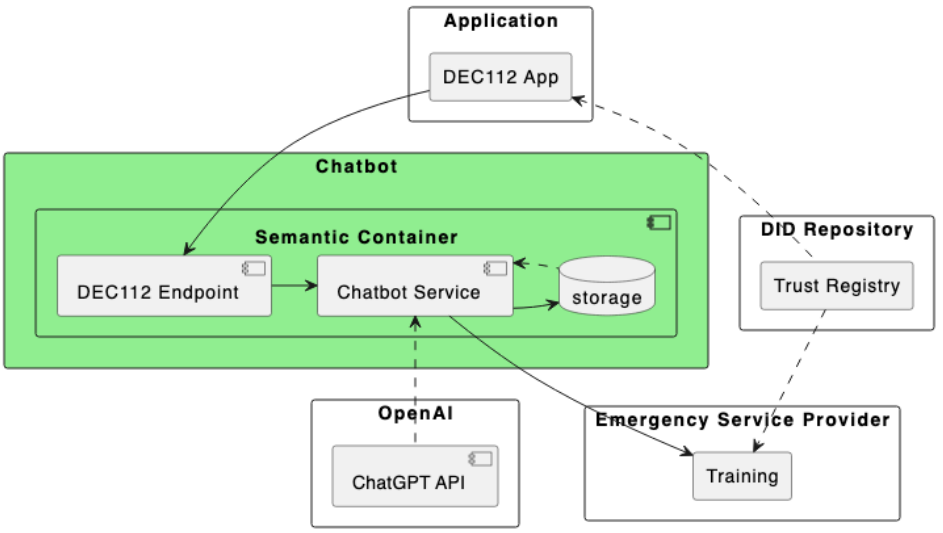

Figure 5.3: Chatbot Components (green components are new developments)

5.1.4 did:oyd Method

Own Your Decentralised Identifier (OYDID) is the umbrella term for all components associated with the did:oyd DID Method. It is a non-blockchain based DID method with the same cryptographic properties as a blockchain-based DID method. The focus in this project is on improving interoperability among DID methods through the demonstration of DID Rotation - the seamless switching between DID methods for a given DID Document.

OYDID components:

- **OYDID Tools:** provides a number of utilities to interact with the OYDID Repository - a command line tool, a Ruby Gem, and a JavaScript npm package
- **OYDID Repository:** central storage of all public data associated with a DID (DID Document, Logs, and Metadata)
- **Uniresolver and Uniregistrar:** community tools for interaction with the Self-Sovereign Identity space
- **DID Lint Service:** validating DID Documents and associated metadata for conformance to the DID v1.0 Core Spec based on the SOyA data modelling language using SHACL
- **SOyA Ecosystem:** online repository for SOyA structures and helper functions for data model management

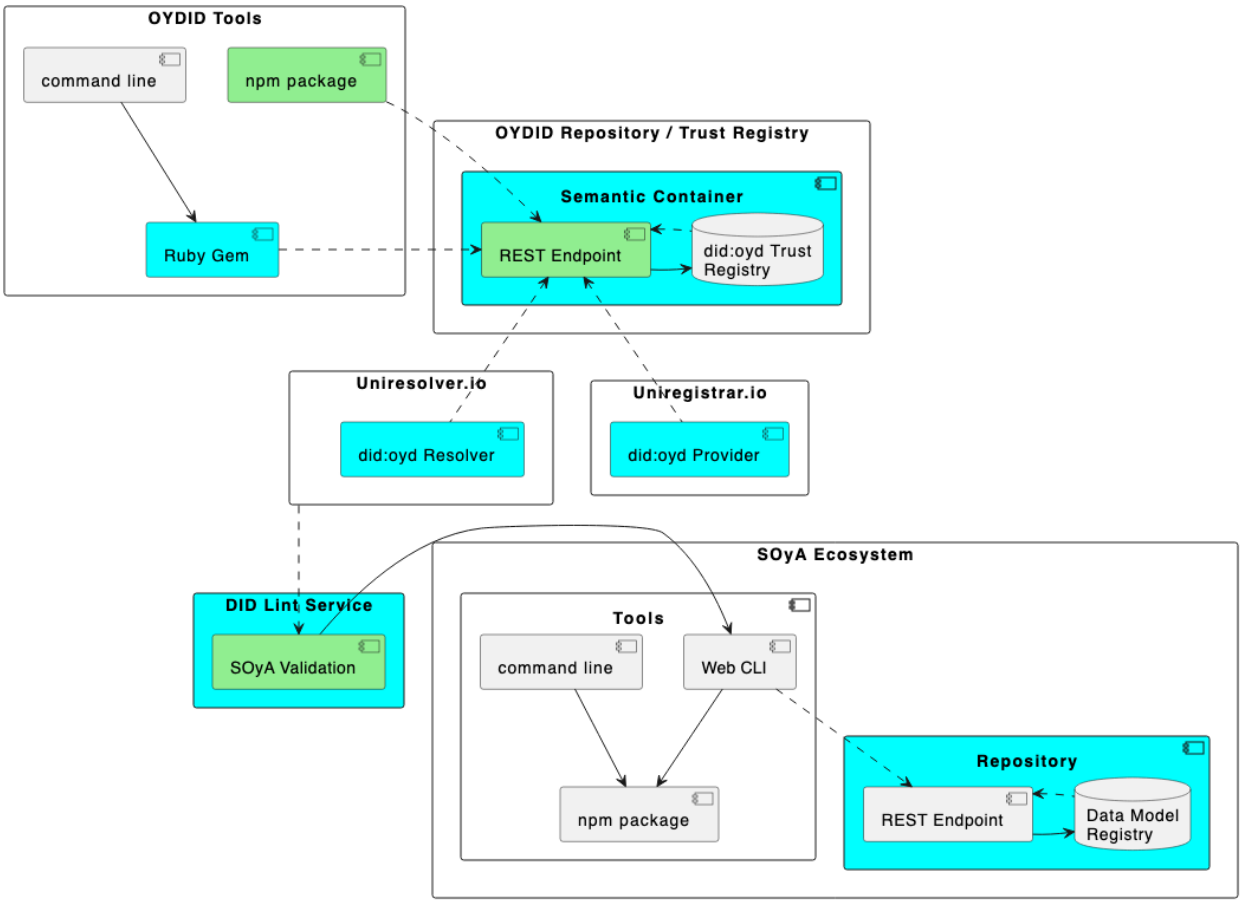

Figure 5.4: OYDID Components (green components are new developments, cyan components exist and might require adoptions)

5.2 Architecture Diagram

The architecture overview in Figure 5.5 depicts the main components of the IM4DEC solution. It highlights the components to be developed in the course of the project (in green colour) and also puts already existing components in context to demonstrate the overall functionality. Detailed information for each of the highlighted components are available in section 5.1 Software Modules.

The two main actors are the user at the top (using either the DEC112 app or the Sphereon wallet) and the call taker at the opposite end of the conversation. The DEC112 RegAPI (Registration API) will be extended by allowing a government issued ID in the onboarding process (Section 5.1.1), an SSI Mobile Wallet will be equipped with means to trigger a Silent Emergency Notification based on a government ID

and SIP credentials (Section 5.1.2), the chatbot simulates emergency personnel responses and additionally covers functionality for data exchange (Section 5.1.3), and finally a DID Trust Registry (focusing on did:oyd and did:ebsi DID methods) facilitates access to DID Documents associated with decentralised identifiers employed in the various use cases (Section 5.1.4).

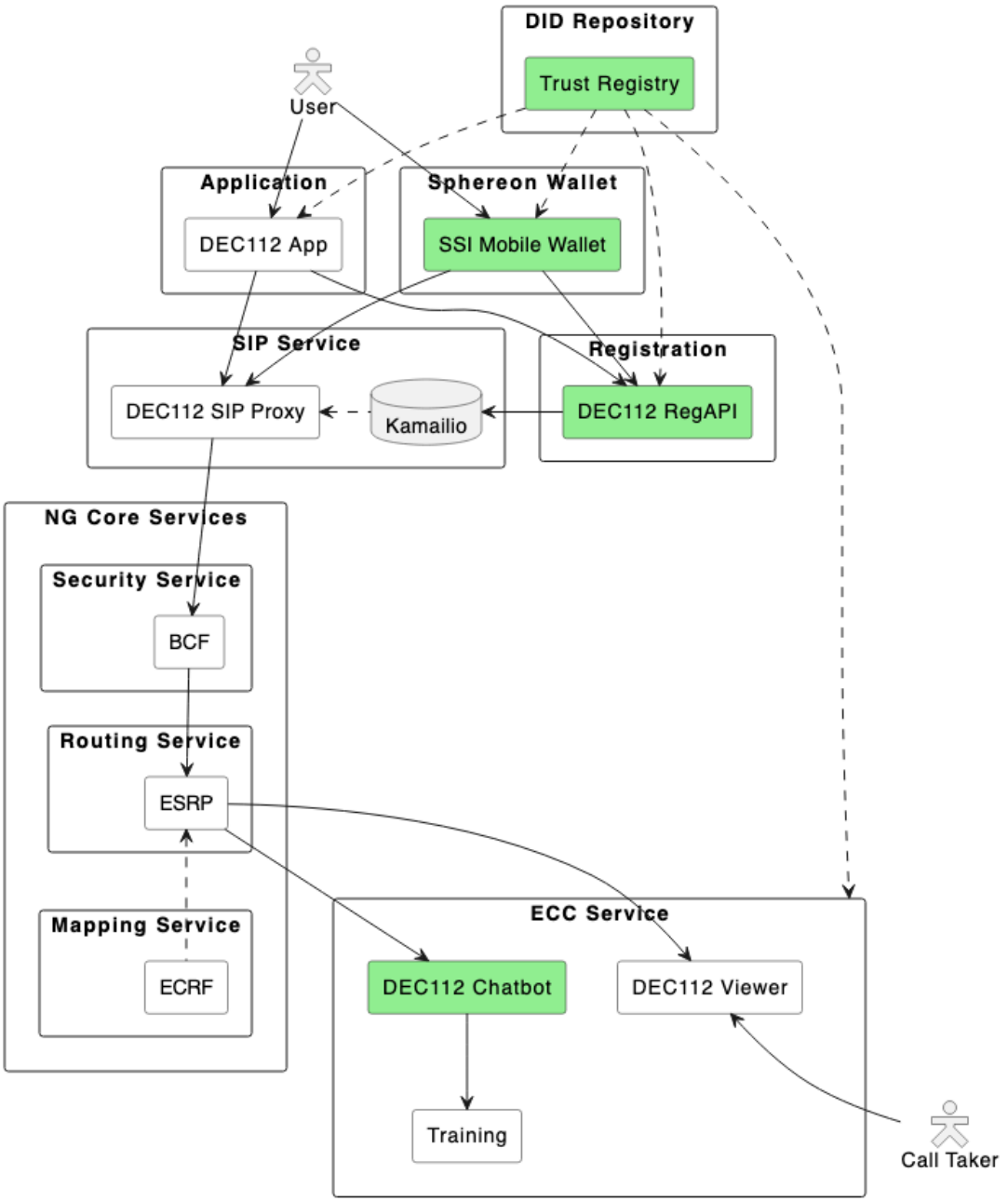

Figure 5.5: Architecture Overview

6 Detailed Work Plan for Implementation and Deployment (Preliminary)

The work plan for implementing IM4DEC during the 9-month funded project duration takes a stepwise approach and is depicted in Figure 6.1.

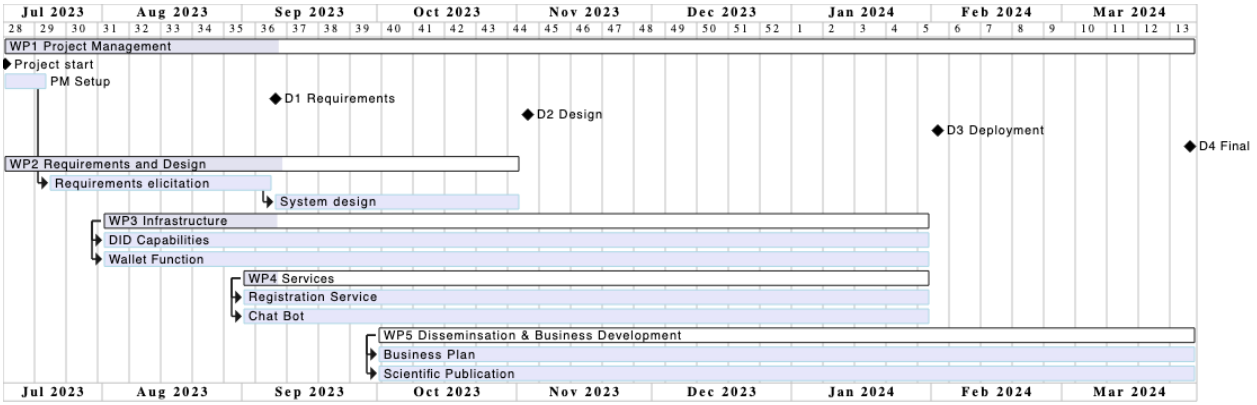

Figure 6.1: GANTT Chart

Work Package #1: Project Management (July 2023 - March 2024)

This WP spans the whole project duration and covers all administrative aspects of internal communication, organising meetings, and monitoring progress.

Work Package #2: Requirements and Design (July - October 2023)

Deliverables D1 & D2 for Requirements and Design are discussed, written, and reviewed in this WP. These documents describe the detailed features to be implemented and tested in the course of the project.

Work Package #3: Infrastructure (August 2023 - January 2024)

Infrastructure features specified in WP2 are implemented in WP3. This WP also includes packaging, documenting, and publishing the source code to make it easier for others to find and integrate the developed software artefacts.

Work Package #4: Services (September 2023 - January 2024)

Service features specified in WP2 using infrastructure artefacts developed in WP3 will be verified and demonstrated in various use cases in. This includes refining the deployment process, writing tutorials for aiding in adoption, and recording short videos for demonstration purposes.

Work Package #5: Dissemination & Business (October 2023 - March 2024)

WP5 describes the dissemination and business aspects of this project. The focus is here on promoting OwnYourData and DEC solutions in relevant communities. Additionally, a scientific paper will be published to share the findings and developments of the project.

6.1 Work Plan for Implementation

The main implementation tasks will be performed in work packages #3 and #4, running from August 2023 through January 2024. The four work streams we have identified are (1) Registration API, (2) Wallet, (3) Chat Bot, and (4) DID Enhancements.

The above work streams share the same development patterns of

- starting with requirements and user stories
  → this document,
- deriving a design
  → planned in WP2 and Deliverable D2,
- setting up a development and testing environment, implementing features, validating functionality based on pre-defined usage scenarios
  → performed in WP3 and WP4 and documented in Deliverable D3, and
- deploying components into our live system together with comprehensive documentation
  → executed in WP5 and Deliverable D4

6.2 Work Plan for Deployment

We plan regular deployments of the developed and updated software components in the course of the project. Our primary site for testing functionality and deploying off-chain storage is a Kubernetes cluster maintained by OwnYourData and services will generally be available as a sub-domain of data-container.net and ownyourdata.eu. For on-chain data we are looking into available services from Alastria as distributed ledger technology.

The live-system hosted redundantly in Germany and Austria is maintained by DEC112 and will receive updates only after thorough testing. The system status of the live system is available here: https://status.dec112.eu/

7 Conclusions

This document outlined the requirements and use cases identified in the initial design phase of the IM4DEC project. Based on a stakeholder analysis and the goals defined in the project proposal the main objectives were identified and non-functional as well as functional requirements were documented. Based on these requirements the design will be described in deliverable D2 Design.

Funded by the European Union

LINALTEC

DEC112 Privacy Report

Assessment

Date: 2023-08-31

LINALTEC AB
Assessment by:
Jan Lindquist (GDPR Privacy Advisor)
jan@linaltec.com
+46 730 694 942

Funded by the European Union

Executive Summary

This is an executive summary of the preliminary findings of the GDPR assessment of DEC112 association activities. This summary also covers the results of a DPIA assessment covered in a separate document

- A major vulnerability is registration API for new users and due to cleartext keys can be easily copied. Rate limitations should be in place to limit any potential attacks.
- Agreement between association and Ministry of Interior needs to be revised and association should have clear statements on what data can be transferred and historical data is discarded in case of disbanding the association.
- The DEC112 app needs a DPA with the association to make it clear the separation of responsibilities. The DEC112 app would be treated as an independent third-party.
- The usage of chatgpt should continuously be checked for any biases in chat simulations. Initial chat simulations look promising but need to be frequently checked if going live (simulation only).

Introduction

DEC112 association contracted Linaltec AB to perform a privacy assessment and provide a list of recommendations. Interviews were conducted with the following groups:

- Gabriel Unterholzer - chairman of the association as well as main developer, devops responsible.
- Mario Murrent - DEC112 app dev of mobile application and registration SDK
- Wolfgang Kampichler - standard responsible in ETSI and external partners, Ministry and political level
- Christian Fabianek - backend developer

This report is split into four areas: General Privacy Assessment, Routines, Data Breach Analysis and Systems Review. The General Privacy Assessment checks the risks surrounding the private data collected like cookie usage and privacy policy. The Routines section identifies the activities at DEC112 that handle personal information and need internal policies. The Data Break Analysis reviews IT related activities and potential data breach areas which raises the risk for GDPR penalties. The Systems Review checks for GDPR compliance of external systems and DEC112 association role in relation to these systems.

At the end of the report there is a summary of all the action points and recommended priority.

General Privacy Assessment

Risk Assessment

Companies need to assess the sensitivity of the data that is collected and determine if a threshold is reached where a larger risk assessment is required, this is called a Data Protection Impact Assessment (DPIA). A DPIA report identifies potential risks where top management decides the actions to mitigate any high-level risks.

To determine if a DPIA report is required a list of criteria are reviewed. If any of the criteria are yes, a DPIA should be conducted. Note this evaluation is only a guidance and each organisation may make their own decision to perform a DPIA.

Criteria for risk	Applicable?
Evaluation or scoring	No
Automated decision making	No
Systematic monitoring	No
Sensitive data	Yes (1)
Large scale data processing	No (2)
Datasets are matched/combined	No
Innovation use of technology	Yes (3)
Data relating vulnerable individual	Yes (4)

Note – For details on individual criteria refer to ICO guidelines[7].

DEC112 association is required to perform a DPIA due to the following reasons:

(1) Emergency chat sessions may include sensitive communication when using the app to inform health situations or personal injury. Additionally Apple Health and Google Health may be added to chat session which may include health conditions
(2) There are 20k registered users in the app. This is not considered a large scale.
(3) The usage of chatgpt is a new technology which needs additional care and understanding of how potentially sensitive personal information is processed. For example if chat is used by Open AI to train chatgpt.
(4) The target community are individuals with disabilities like hearing or speech impairments which is considered a vulnerable population.

Cookie Usage Analysis

An analysis was performed using Cookiebot (www.cookiebot.com) to determine what cookies are used and for which purpose (full cookiebot report shared separately).

[7] ICO Guidelines for Data Protection Impact Assessments: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Information Security Analysis

Several areas were reviewed to determine what threats that may occur and how to avoid data breaches which have large penalties in light of GDPR. Data breaches can occur not due to technical problems but simply using social engineering and stealing login credentials if not properly handled or losing a company computer.

Login Credentials

Credentials are not shared within the team. Not everybody has MFA implemented to prevent login credentials from being stolen and to prevent unauthorised login. Recommend consistent activation of MFA by team.

AP1: MFA needs to be implemented by whole team

When connecting with SSH custom certificates are used unique to each developer or devops.

Service Level Agreement

The SLA with both the ministry of interior and control centres with DEC112 association stipulates that all data shall be transferred or destroyed. Important to stipulate exact conditions such information is transferred or destroyed. The destruction of the data shall be documented. The potential transfer of DEC112 service to another entity also needs to be stipulated. For example transfer can be limited to registration information

AP2: Update of DEC112 association policy for covering 3 data handling scenarios: a) what data can be transferred, b) how to handle transfer of DEC112 operations to another entity and c) if DEC112 terminates SLA with ministry of interior steps for destructing collected information.

The SLA is missing a third party list and what are the privacy rights of an individual. The SLA is not clear what data can be transferred and needs clarification. The role of DEC112 being only a data processor or a data controller also needs to be clear. If for example, DEC112 through the app is a data controller for registration and communication it sets a clearer separation than what other data controllers may request for.

AP3: Update ministry of interior and control centre SLA with the latest list of third parties and clarify what data may be accessed.

Security Clearance

Providing emergency services deals with highly sensitive communication. The ministry of interior requires that all those with access to DEC112 are not in the police registry. The requirement is documented in the SLA.

AP4: Check everybody with access to DEC112 has copy of police registry

Violations

There is strong language in the SLA by the ministry of interior when there is misconduct and if it is proven that somebody intentionally jeopardised the DEC112 service they will be prosecuted. Important to have clear DEC112 association policy violations may be prosecuted.

AP5: Add policy to increase awareness of consequence of violations by any member

Privacy Policy

The privacy policy should convey in a clear language for deaf people to understand how their personal data is used. A review of the privacy policy showed that it is incomplete and needs updating. These are a sample of some websites with the structure and composition that is recommended for DEC112.

https://telldus.com/telldus-privacy-policy/

https://portal.life-guard.dk/website/privacypolicy

AP6: Update privacy policy with new template ensuring it is understood by target

When the privacy policy is updated a cookie analysis should be performed using Cookiebot (www.cookiebot.com) to determine what cookies are used and for which purpose. The following webpages will be analysed for cookie usage

https://www.dec112.at/en/web-privacy/

https://www.dec112.at/privacy/

Review of systems

This section is a review of the systems used by the DEC112 association. A complete inventory of the systems can be found in the "Third-party list" report. These systems were found to potentially handle personal information at a larger scale.

The following third-party systems are in the process of being phased out specially in considerations of the data transfer issues to non-EU countries.

- Google Firebase Crashlytics
- Sentry
- Google Analytics

AP7: Replacement of Google Firebase Crashlytics, Sentry and Google Analytics

Actions Summary

This is a summary of the actions and priority.

AP	Priority	Title	Description
AP1	M	Consistent usage of MFA	MFA needs to be implemented by whole team
AP2	M	DEC112 association policy on data handling	Update of DEC112 association policy for covering 3 data handling scenarios: a) what data can be transferred, b) how to handle transfer of DEC112 operations to another entity and c) if DEC112 terminates SLA with ministry of interior steps for destructing collected information.
AP3	M	Ministry of interior SLA update	Update ministry of interior and control centre SLA with the latest list of third parties and clarify what data may be accessed.
AP4	L	Police registry	Check everybody with access to DEC112 has copy of police registry
AP5	L	Policy on violations	Add policy to increase awareness of consequence of violations by any member

Funded by the European Union

AP6	M	Privacy policy update	Update privacy policy with new template ensuring it is understood by target group
AP7	L	Replace analytics and debugging tools	Replacement of Google Firebase Crashlytics, Sentry and Google Analytics

Table A.1: Actions and Priorities

Further Information: Understanding GDPR

Fundamental Rights

Like freedom of expression and religion every EU citizen has a fundamental right for protection of personal data. Here is the text in Article 8 which is the basis for GDPR.

Article 8

Protection of personal data

1. Everyone has the **right to the protection of personal data** concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Objectives

Each employee is responsible to raise questions relating to how an organisation manages internal routines that may have a GDPR impact. If the employee has a better understanding of GDPR and applies the knowledge on day to day activities, even in their private activities, they are better able to catch GDPR violations. The consequences of some of the data breaches occurring daily are huge financial impacts and in some cases threat to their own life. A good personal motivator to be interested is to ask the question if you trust how your personal data is being handled.

The objective of this section is to help each employee understand what to look for if any routines should be changed or check if any new services or systems are introduced. To help get a basic grasp of GDPR the following topics are covered:

1. What is considered personal data?
2. What principals should be followed to process personal data?
3. When is consent required?
4. What are the personal rights that need to be prepared to be answered?

What is considered personal data?

If no personal data is exchanged or if personal data is anonymized, then there is no GDPR concern and no risk of data breach risks.

What to look for when personal data is collected. Three types of personal data: identifiable, quasi-identifiable and sensitive. The quasi-identifiable example: even if no identifiable information is shared, if enough attributes like gender, data of birth and zip code are available it is possible with high accuracy to re-identify an individual. If sensitive information is collected with identifiable and quasi-identifiable attributes, then additional precautions are required and possibly a risk assessment like a DPIA is necessary.

Identifiable	**Quasi-identifiable**	**Sensitive**
Name ID (example driver's licence #) Physical address E-mail Photo IP address * GPS location **	(combination of attributes) Gender, date of birth and postcode	Ethnic background Political views Religion Physiological (DNA) Mental (medical diagnosis)

Note:
* an IP address can be tied to an individual and home. This is one reason to use VPN but need to also browse in private mode so cookies are not used which can re-identify you.
** GPS location can track where you visit and where you live and is considered personal data

There are more examples but this is a basic introduction of what is considered personal data.

What principals should be followed to process personal data?

All organisations that process personal data need to abide by the principles set by GDPR chapter 2. The principles help understand what to focus on when evaluating the practices of a system or routine. For example, how a privacy policy is written should reflect these principals.

- **Lawfulness, fairness and transparency:** Processes shall be done lawfully, fairly and in a manner that is transparent for the intended use.
- **Purpose limitation:** Processing of personal data shall have a legitimate purpose and limited to needs to fulfil the purpose. Additional data cannot be incompatible with the scope. For example, a cooking app shall not be collecting location information.
- **Data minimization:** To avoid collecting too much information the processing of personal data shall be minimised.

- **Data accuracy:** The collected personal data shall be accurate and be kept up to date.
- **Storage limitation:** The collected data shall be limited for the duration that is necessary.
- **Integrity and confidentiality:** Processes shall be done in a manner that ensures appropriate security of the data.
- **Accountable:** It shall be possible to demonstrate compliance to these principles.

When is consent required?

A legitimate purpose for processing personal data does not require a consent but if additional services are offered that go beyond the original purpose then a consent is required. For example, a web page may provide a news service but to store a cookie to track that pages you view and offer targeted ads requires a consent. The consent must be opt-in meaning choice cannot have a default of on. Unfortunately, frequently the option to opt-out is hidden. A good example is following notice with clear consent.

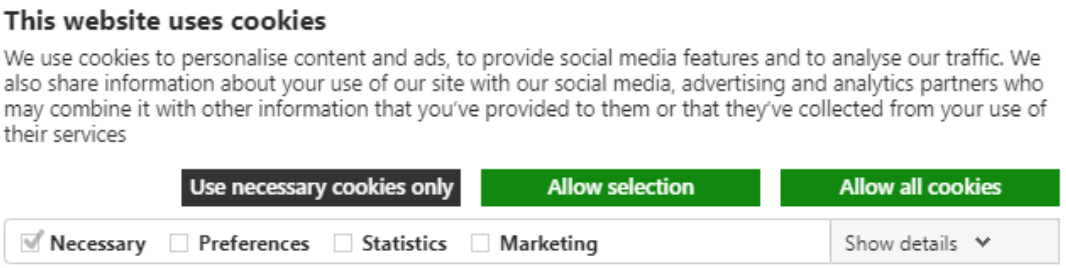

Figure A.1: Example of Well-Implemented Website Cookies Consent Interface

When checking out a service, it should not be misleading or hide how to consent. Below is an example of a misleading consent. **TIP:** Instead of typically clicking “agree” choose to “Manage settings” and scroll to the bottom. Typically most options are default off but you need to scroll to the bottom to “Save and continue” with them off. The marketing companies are making it just a little harder so 80% of the visitors simply select “I agree”. I call this death by consent so you do not care how personal data is collected for marketing purposes.

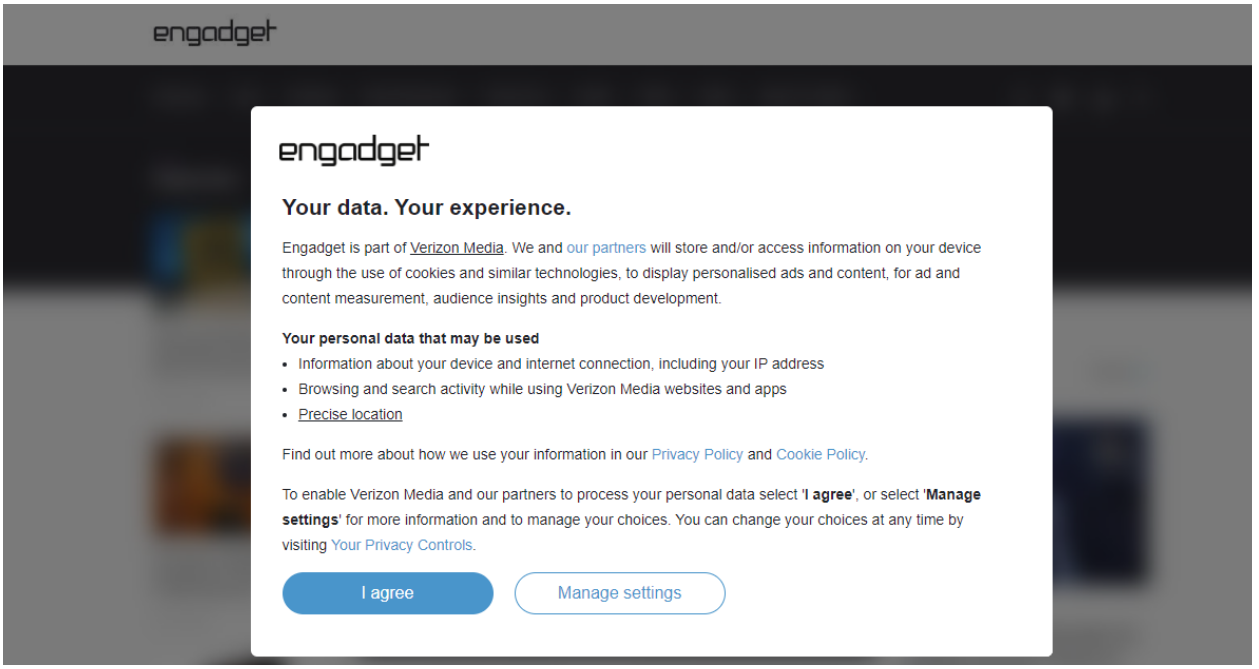

Figure A.2: Example of Poorly Designed Website Consent Interface

What are the personal rights that need to be prepared to be answered?

The final area to understand are the personal rights of an individual. The rights can be found in GDPR chapter 3 but before going into the rights good to be aware of some terms relating the roles surrounding data processing.

The individual is a Data Subject in GDPR terms. An organisation who has main responsibility for the Data Subjects personal data is called Data Controller. The Data Controller will not always or quite frequently rely on another company to collect the data on their behalf. The other company is a Data Processor. An organisation, Data Controller, needs to review the Data Processor routines and make sure the same processing principles and Data Subject rights are met.

The following table lists the rights of an individual, Data Subject, which an organisation, Data Controller, needs to be prepared to answer.

Rights	Description
The right to be informed	The individual has a right to be informed of any matters relating to processing of the personal data that may affect them. For example, in case of data breaches or changes to the privacy policy.
The right of access	The individual has a right to view their personal data.
The right to rectification	If the personal data is incorrect, they have the right to have it corrected.
The right to erasure	In the case they do not want the personal data to be kept they can request that the personal data is erased. *
The right to restrict processing	If the individual requires special consideration when processing the personal data to avoid exposure to any risks, they can request to restrict the access to the data.
The right to data portability	The individual has the right to not only access their personal right but right to move their data to another service provider. This is easier said than done due to compatibility issues.
The right to object	If any of their rights are impacted, they have a right to object
Rights in relation to automated decision making and profiling.	In case of automated decision making or profiling based on personal data which has direct impact they have the right to request to perform manual decision making.

Table A.2: GDPR Rights

* Not all personal data can be erased and there may be other legal requirements in a country where data must be kept for a longer period. For example, salary information must be kept for 7 years in Sweden. Even though personal data is kept for a longer period it is only for the purpose of fulfilling the legal requirement and the data cannot be used for any other purpose.

LINALTEC

DEC112 DPIA Report

Assessment

Date: 2023-08-31

LINALTEC AB
Assessment by:
Jan Lindquist (GDPR Privacy Advisor)
jan@linaltec.com
+46 730 694 942

Funded by the European Union

INTRODUCTION

Purpose

DEC112 provides emergency service based on text messages targeted for individuals with disabilities like hearing or speech impairment. DEC112 commits to manage compliance with applicable personal data protection legislation, contractual requirements and other internal policies.

This report is a Data Protection Impacts Assessment with intention to describe the processing of personal data and minimising the risks as much as possible.

Glossary

Term	Description
Data Protection Agency (DPA)	The Data Protection Agency is responsible for enforcement of GDPR. They are the point of contact for data breaches or questions.
Data Protection Impact Assessment (DPIA)	A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible.
Data Privacy Officer (DPO)	The Data Privacy Officer is appointed at DEC112 to manage all privacy questions and ensure the organisation is fulfilling training and security measures.
GDPR	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).
Individual	The term individual refers to the end-user who uses the coaching service.
Organisation	The term organisation refers to the whole DEC112 association members and subcontractors
Personal Identifiable Information (PII)	The term PII is used to refer to any personal identifiable information like email, name or driver's licence. Some PII data can be directly linked to an individual and some can be extrapolated like GPS location or physical characteristics.

Table B.1: DPIA Glossary

Scope

The resources that are in the scope of the DEC112 DPIA are:

- Software
  - DEC112 platform and application
  - 3rd party software suppliers
- Partners
  - Data processing agreements with DEC112 platform

Roles and Responsibilities

These are the roles at DEC112 and the responsibilities to provide accountability.

Role	Responsibility
Everybody	It is the responsibility of every employee and contractor to be observant of the privacy related irregularities and report them to the DPO immediately. The incident will be logged to best determine action.
Leadership team	Commit to the privacy policy and ensure the privacy program led by the DPO is being fulfilled.
IT admin	Ensure all access to private data is restricted based on role.
Platform Development	During the development phase limit the usage of real personal data.
Research	Research shall be performed on anonymized data but due to the level of detail of re-identify additional security measures shall be followed.
Data Protection Officer	Manage the privacy program and ensure adequate controls and training are in place minimising all privacy risks. Provide regular updates to the leadership of the privacy KPI's.

Table B.2: Roles and Responsibilities

Scope of Processing

Processing Overview

The following diagram represents the processing of the DEC112 solution. The main components are the DEC112 app and the DEC112 Core-Services. The Reg-API's components are gateways to the external services for the purpose of user verification. There are test simulation components to help to get individuals used to the app and interaction with operators during an emergency.

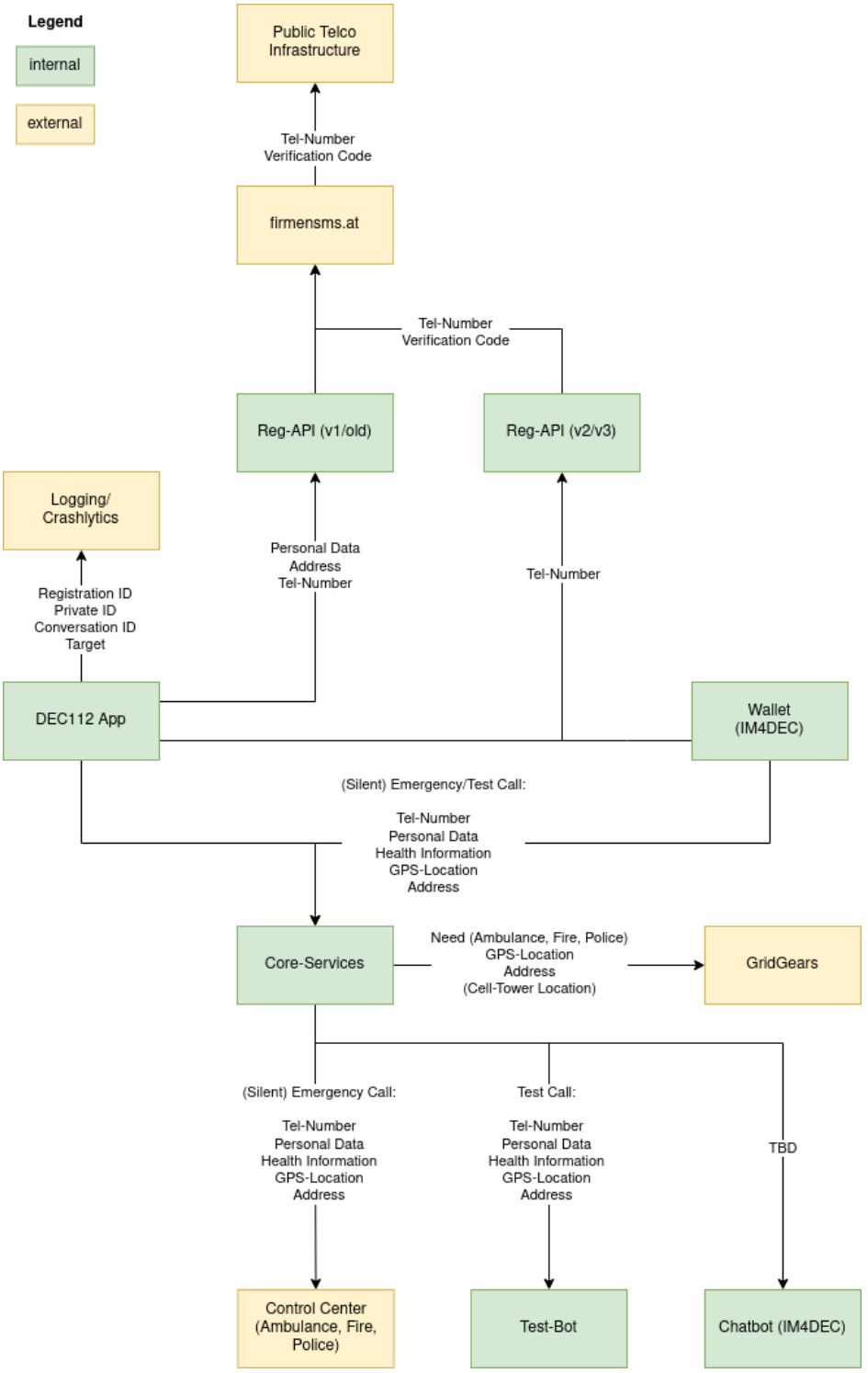

Figure B.1: Processing Overview

AP8: The DEC112 App is meant to be a 3rd party provider and a DPA should be in place.

These are the main flows when processing personal data:

1. Registering first time using the app
2. Emergency simulation with test bot or in the future chat-gpt
3. Emergency call

Data Subjects

The data processing is limited to individuals in Austria.

- Data will be collected when first registering with the DEC112 app.
- Data subjects may share additional information from Apple Health or Google Health during the registration.

Data Types

There are various different types of data to be processed by the system. The table below lists the data types and provides a definition for each.

Data Type	Definition	Example
Personal Data	The personal data has the following information: identifying, physical characteristics, demographics and medical health.	name, height, weight age, gender, disability (ex. hearing, speach), diagnosis, medical conditions, free text
Tracking	The tracking information comes in different forms: contact, location and computer device.	email, physical home address, mobile number, GPS coordinates, IP address, model, device id
Communication	The communication is limited to text, no voice. These occur during an emergency or simulation of an emergency.	Text messages

Table B.3: Data Types

Personal Data Classes

This section describes how personal data will be collected, used, transferred and if necessary, kept up to date. The privacy class are broken down into following classes:

- **PII**: Personal Identifiable Information

Specific information that references an individual, such as name or an identification number.

- **QII**: Quasi-Identifiable Information

Any piece of information (e.g. a geographical position in a certain moment or an opinion about a certain topic) that could be used, either individually or in combination with other quasi-identifiers, by someone that has knowledge about that individual with the purpose of re-identifying an individual in the dataset

- **SEN**: Sensitivity

The following type of information is considered sensitive: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Categories

The following table lists the data collected (right column) and Data Type Name, Personal Data Category and Privacy Class. Special attention is required for privacy class of type SEN (sensitive). Everybody in the organisation shall be able to identify processed personal specially sensitive information like disabilities. When they come across they should be extra cautious with the processing of the data. If unintentionally exposed, consider it a security incident and report it for remediation. recognize when they come across sensitive data that are not classified in the table.

Data Type Name	Personal Data Category (1)	Privacy Class	Data collected
Personal Data	Identifying	PII	name
	Physical characteristics	QII	height, weight
	Demographics	QII	age, gender
	Medical health	QII/SEN	disability (ex. hearing, speach), diagnosis, medical conditions, free text

Data Type Name	Personal Data Category (1)	Privacy Class	Data collected
Tracking	Contact	PII	email, physical home address, mobile number
	Location	QII	GPS coordinates
	Computer device	QII	IP address, model, device id
Communication	Text communication	SEN	Text communication

Table B.4: Data Categories

Note: (1) DPV related material for setting category. First link is a nice overview diagram. The second and third links are standards work in the W3C Data Privacy Vocabulary (DPV) community group.
https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf
https://dpvcg.github.io/dpv/#vocab-personal-data-categories
https://w3c.github.io/cg-reports/dpvcg/CG-FINAL-dpv-pd-20221205/

Data Retention

The data retention shall be strictly adhered to. The justification for retaining for the specified period is explained.

Data Type	Retention	Retention Justification	Retention Measure
Personal Data	All personal data is stored in the DEC112 app and is not deleted if an individual does not delete the app installed on their phone.	Individuals have full control of the app and are able to delete it at any time.	
Tracking (Contact, Computer device)	During registration some tracking information like phone number, device id and model are stored in the DEC112 backend. The information is stored as long as they are registered in the service.	DISCUSS	

Data Type	Retention	Retention Justification	Retention Measure
Communication	All emergency communications - once routing is established - are forwarded to the operator together with personal data and tracking information. The DEC112 backend stores the communication log for 2 years.	The communication is retained as long as necessary to troubleshoot communication.	

Table B.5: Data Retention

AP9: The backup of the app data has to consider the retention period and how to forget if there is a request.

Data Access/Use

Access to the data at DEC112 is broken down into the following roles.

Data Type	IT Admin	Research
Personal Data	yes	yes (1)
Tracking	yes	yes (1)
Communication	yes	yes (2)

Table B.6: Data Access/Use

Note (1) - Personal data has to be generalised to demographics so no re-identification is possible. For example, change birthdays to an age range like 40-50. Another example is statistics based on location, the aggregate number of individuals for a given region cannot represent less than 10 individuals. If the number of individuals in a region is lower than 10 then that region needs to be combined with another region to represent more than 10 individuals.

Note (2) - Text may be used for research and understanding performance of chat bots like chatgpt.

AP10: Reports created based on personal data and tracking requires a policy describing the generalisation of the information.

AP11: Usage of text communication for building chatbot like chatgpt has to be strictly controlled and anonymized. No names or addresses shall be included, nor personal data or tracking details. They shall be kept separate.

Data Sharing

The instances that data may be shared from DEC112 are the following:

1. Routing information is shared with the Ministry of Interior for the purpose of controlling which emergency service was used. One reason for sharing information is to identify and track fraudulent requests for emergency services and charge for falls dispatch. All emergency communications to the police require the police to respond.
2. The emergency communication is forwarded to the control centre on an instance basis. Once a session is terminated the DEC112 app does not keep a copy of the instance. The control centre retains information for 90 days but is dependent on their own policies.

Compliance with Data Protection Law

The following sets out the lawful bases for the processing of personal data identified.

Lawful Basis for Processing of Personal Data in Emergency Calls

The following lawful basis in Article 6 and Article 9 of the GDPR are appropriate to and suitable for the purposes of processing personal data for providing emergency services.

Article 6 (Lawfulness of processing)

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1(e); (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller).

Article 9 (Processing of special categories of personal data)

Processing is necessary for the purposes of providing emergency care during an emergency and medical diagnosis and treatment of the individual or other emergency if that is fire or police related.

Exercise of Data Subject Rights

An individual has the following rights and what are the actions taken.

Privacy Right	Description	Response	Internal routine
Right of access	Individual has the right to access all collected personal data.	DEC112 app provides access to all collected information.	
Right of rectification	Individual has the right to have any collected information rectified.	DEC112 app allows individual to make any correction.	
Right to be forgotten	Individual has the right to be forgotten	Through the DEC112 app individuals have the ability to remove or have all their data forgotten. To remove backend registration information, it needs to be communicated for a manual removal.	IT department
Right to restriction of processing	Under special circumstances the individual may request that personal data is not processed or removed. This may occur under circumstances when an individual wants to raise concerns with DPA.	Questions of restricting access shall be directed to the IT department and DPO shall be involved in order to determine nature of the request and establish reasonable reason for request.	IT department

Privacy Right	Description	Response	Internal routine
Right of portability	Individual has the right to request to port personal data to another service.	DEC112 app is not an open platform for data portability. Data source like Apple Health provided the portability if requested.	
Right to object	Individual has the right to object to processing of personal data and shall inform the organisation of the objection.	DPO shall be involved in order to determine the nature of the request and establish reasonable reason for request.	

Table B.7: Exercise of Data Subject Rights

AP12: The routines for right to be forgotten in the backend should documented

International Transfers

No personal data is transferred out of the EU except for application crash diagnostics used in Google Firebase Crashlytics.

Appointment of Data Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR.

Identify and Assess Risks

The table below sets out the risks that have been identified for the project and the levels for those risks if not mitigated. Overall risk score for each risk identified is calculated as the product of the risk likelihood score and the risk impact score (i.e. likelihood score X impact score). The following sets out the metrics used in documenting the risk assessment.

Likelihood	Score
Highly Unlikely	1
Unlikely	2
Possible	3
Likely	4
Highly Likely	5

Impact	Score
Negligible	1
Minor	2
Moderate	3
Major	4
Critical	5

Overall	Score
Low	1-7
Medium	8-14
High	15-25

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
1	Sharing of logs: Sharing of logs which may have personal information may be shared using Google Drive or Slack. Logs with potential emergency communication should be limited and deleted once addressed.	The likelihood is very limited with only 20% of communication being an emergency so sensitivity may be limited.	If sensitive communication is accessed it will be considered a security breach and needs reporting.	2	4	8
2	Chatgpt biases during simulated chat: The chatgpt may have biassed communication which may confuse or mislead an individual.	The responses will likely not be perfect.	These are only simulated chats and will be clearly communicated with individuals.	3	2	6
3	Fixed registration API keys: The registration API uses a fixed key used during registration of new users. After registration is performed a unique key is stored specifically for the device.	A man in the middle attack may be used to access the key.	Fake registration may cause sms spam which may affect reputation and high sms costs.	4	5	20

Funded by the European Union

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
4	Consistent usage of MFA: Production environment access should be only supported using MFA. Development environment may also need MFA in order to prevent injection of malicious code.	If a computer is hacked, stealing credentials is easy.	Depending on the level of privileges the whole system may be interrupted, corrupted or worse ransomware is installed.	3	5	15

Table B.8: Risk Assessment

Identify Measures to Reduce Risks

An evaluation of the identified risks in the previous section has been carried out and a series of measures have been detailed that seek to mitigate those risks to an acceptable level. The table below sets out these mitigation measures and an assessment of the risk impact due to their introduction.

No.	Risk	Mitigation	Likelihood Score	Impact Score	Overall Risk	Remaining risk to data subject
1	Sharing of logs	Reduction: Limit of sharing of logs to a single system and awareness to limit sharing sensitive communication.	2	4	8	Data breach space is reduced
2	Chatgpt biases during simulated chat	Reduction: Close evaluation during prototyping and feedback from users	3	2	6	Improved perception of users of chatbot.

No.	Risk	Mitigation	Likelihood Score	Impact Score	Overall Risk	Remaining risk to data subject
3	Fixed registration API keys	Sharing: The responsibility of the API is not with IM4DEC but should be highlighted as an issue Reduction: Cap on number of text messages should be set in case of abuse	4	5	20	Data subjects will still face inconvenience of SMS text messages but reduced by limiting how many text messages are sent.
4	Consistent usage of MFA	Reduction: require MFA and also increase security awareness [AP1]	3	5	15	Data breach is reduced by additional step in logging into system

Table B.9: Measures to Reduce Risks

Actions Summary

This is a summary of the actions and priority.

AP	Priority	Title	Description
AP8	H	DEC112 App DPA	The DEC112 App is meant to be a 3rd party provider and a DPA should be in place.
AP9	M	DEC112 App backup	The backup of the app data has to consider the retention period and how to forget if there is a request.
AP10	M	Policy for exporting usage reports	Reports created based on personal data and tracking requires a policy describing the generalisation of the information.

AP	Priority	Title	Description
AP11	M	Policy for usage of communication for creating chatbot	Usage of text communication for building chatbot like chatgpt has to be strictly controlled and anonymized. No names or addresses shall be included, nor personal data or tracking details. They shall be kept separate.
AP12	L	Policy for applying right to be forgotten	The routines for right to be forgotten in the backend should documented
AP13	M	Sharing of logs	Risk #1
AP14	L	ChatGPT biases during simulated chat	Risk #2
AP15	H	Fixed registration API keys	Risk #3

Table B.10: DPIA Action Summary

Appendix C - ChatGPT Privacy Analysis

This is the current status (as of 31. August 2023) of the ChatGPT Privacy Analysis that will be performed in the course of the project.

Overview

The association DEC112 plans to use ChatGPT, Large Language Models (LLMs) from OpenAI in order to improve the user experience. DEC112 is an emergency service for deaf people and recently expanded to support silent emergency notifications. Intention is to use ChatGPT for simulation purposes only for an emergency chat. Emergency chats are considered highly sensitive. ChatGPT will ONLY be used for simulation purposes and simulates responses from an operator. Clear indication that it is a simulation will be provided and the user will have the opportunity to rate conversations and consent to sharing chat data.

What is the DEC112 role in relation to OpenAI? OpenAI processes “customer data” and is defined as a Data Processor. Organisations using OpenAI services are Data Controllers and therefore need to be aware of the repercussions of using ChatGPT.

Executive Summary

These are the main findings so far of using ChatGPT in the IM4DEC project.

- ChatGPT API has a default of not using user data for training ChatGPT BUT the browser based ChatGPT is the contrary which is a major concern. Browser-ChatGPT requires users to opt out otherwise user data is used to train ChatGPT. A form has to be filled to explicitly make the request and it is necessary to indicate that it is not only browser but device since they are not synced.
- Preparing ChatGPT for simulating emergency conversations can be done in one of two methods which is described below.
- Additional procedures are required for how to handle conversations through a new policy so all those administering the DEC112 app and access to simulated or real conversation are aware of the risks and precautions to be taken.
- Regulator routines need to be established to ensure the answers from ChatGPT are trustworthy and ethical. Incorrect answers or abuse of the simulated conversation may expose DEC112 to bad press and litigation.

Analysis

OpenAI Policy Analysis

There are key questions relating to using ChatGPT which need answering in order to understand the consequences:

1. Are ChatGPT conversions kept confidential?
2. Are conversation histories used to train ChatGPT?
3. Any security considerations when using ChatGPT?

The policies are continuously being updated so analysis is a snapshot from July 26th, 2023. Quotes from the policies are included to better explain the conclusions in this analysis. There are also links to the original policy.

Open AI Privacy policy: https://openai.com/policies/privacy-policy

Claim 1: Input data is used for training the chatgpt model, opt-out is required

“As noted above, we may use Content you provide us to improve our Services, for example to train the models that power ChatGPT. See for instructions on how you can opt out of our use of your Content to train our models.”

Open AI - Data Controls FAQ: https://help.openai.com/en/articles/7730893-data-controls-faq

Claim 2: When opted-out input (conversation) is not used to train chatgpt
“Data controls offer you the ability to turn off chat history and easily choose whether your conversations will be used to train our models.”
“While history is disabled, new conversations won’t be used to train and improve our models,

Claim 3: Ensure no browser add-ons or malware on computer stores conversation
“Please note, this will not prevent unauthorised browser add-ons or malware on your computer from storing your history.”

Claim 4: Opting-out is on a device/browser basis. Need to opt-out independently.
“This setting does not sync across browsers or devices.”

same as Claim 1
“Our large language models are trained on a broad corpus of text that includes publicly available content, licensed content, and content generated by human reviewers. We don’t use data for

selling our services, advertising, or building profiles of people—we use data to make our models more helpful for people. **ChatGPT, for instance, improves by further training on the conversations people have with it, unless you choose to disable training.**

Claim 5: History can also be disabled and will be removed after 30 days.
While history is disabled, new chats will be deleted from our systems within 30 days"

Claim 6: There are plans by OpenAI to simplify opting-out
"We are working on a new offering called ChatGPT Business that will opt end-users out of model training by default. In the meantime, you can opt out from our use of your data to improve our services by filling out this form. Once you submit the form, new conversations will not be used to train our models."

Open AI - API data usage policies: https://openai.com/policies/api-data-usage-policies

Claim 7: Using the API by default the submitted data is not part of the training and requires opt-in
As of March 1, 2023

1. OpenAI **will not use data submitted by customers via our API to train** or improve our models, unless you explicitly decide to share your data with us for this purpose. You can
2. Any data sent through the API will be retained for abuse and misuse monitoring purposes for a maximum of 30 days, after which it will be deleted (unless otherwise required by law).

Claim 8: File endpoint is retained until user deletes the file
"Data submitted by the user through the Files endpoint, for instance to fine-tune a model, is retained until the user deletes the file."

How your data is used to improve model performance: https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance

Claim 2: same as claim 2
"...to turn off training for any conversations created while training is disabled or you can submit this form. Once you opt out, new conversations will not be used to train our models."

Data Processing Agreement
The data processing agreement (DPA) needs to be requested separately and is not provided directly so no link provided.

Claim 9: Requests from law enforcement or public authority will inform customer
"Customer. OpenAI will inform Customer if OpenAI becomes aware of:

a. any legally binding request for disclosure of Customer Data by a law enforcement authority, unless OpenAI is otherwise forbidden by law to inform Customer"
b. any notice, inquiry or investigation by an independent public authority established by a member state pursuant to Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer Data"

Summary

Here is a summary of the main points from OpenAI policies for consideration.

Claim 1: Input data is used for training the chatgpt model, opt-out is required.
Claim 2: When opted-out input (conversation) is not used to train ChatGPT.
Claim 3: Ensure no browser add-ons or malware on computer stores conversation.
Claim 4: Opting-out is on a device/browser basis. Need to opt-out independently.
Claim 5: History can also be disabled and will be removed after 30 days.
Claim 6: There are plans by OpenAI to simplify opting-out.
Claim 7: Using the API by default the submitted data is not part of the training and requires opt-in.
Claim 8: File endpoint is retained until the user deletes the file.
Claim 9: Requests from law enforcement or public authority will inform customers.

Guidelines for Using Generative AI Tools

The Canadian Cyber Security Guidance[8] provides a good set of guidelines. Much of the guidance is focused on the security aspects and mitigation. What concerns this analysis is how the AI tool is used. The following text comes from the guidance.

> **Security protections when using generative AI tools**
>
> The following security measures can help you generate quality and trusted content while mitigating privacy concerns:
>
> **Establish generative AI usage policies** — The policies should include the types of content that can be generated and how to use the technology to avoid compromises to your sensitive data. Your policies should also include the oversight and review processes required to ensure the technology is used appropriately. When creating solutions using generative AI, ensure practices lead to trustworthy and ethical behaviour. Be sure to implement the policies quickly and ensure they are communicated to staff.
> **Select training datasets carefully** — Obtain datasets from a trusted source and implement a robust process for validating and verifying the datasets, whether they're externally acquired or developed internally. Use diverse and representative data to avoid inaccurate and biassed content. Establish a process for outputs to be reviewed by a diverse team from across your organisation to look for inherent biases within the system. Continuously fine-tune or retrain the AI system with appropriate external feedback to improve quality of outputs.
> **Choose tools from security-focused vendors** — Ensure your vendors have robust security practices baked into their data collection, storage, and transfer processes.
>
> **Be careful what information you provide** — Avoid providing PII or sensitive corporate data as part of the queries or prompts. Determine whether the tool allows your users to delete their search prompt history.

Conclusion is that there has to be policies in place for the usage of the AI tools, a clear understanding of the training dataset and if search history can be deleted.

[8] https://www.cyber.gc.ca/en/guidance/generative-artificial-intelligence-ai-itsap00041

Using Own Data Analysis with ChatGPT

Model 1: Create snapshot of conversation and reuse in new conversations

With ChatGPT it is possible to create a backup of the communication with ChatGPT that can serve as a starting point for new communications. This allows starting new conversations from that backup and keeping them independent.

Model 2: Use own instance as plugin to ChatGPT

This approach requires more effort but gives more control over your own data. It is possible to add own data to ChatGPT without divulging any data through a plugin. There are many plugins already developed for ChatGPT that allow enhancing the functionality. ChatGPT uses a corpus for training that extends to September 2021. The method with plugins allows you to add your own data.
Here is an example of a Medium article on how to create a private ChatGPT with your own data[9].

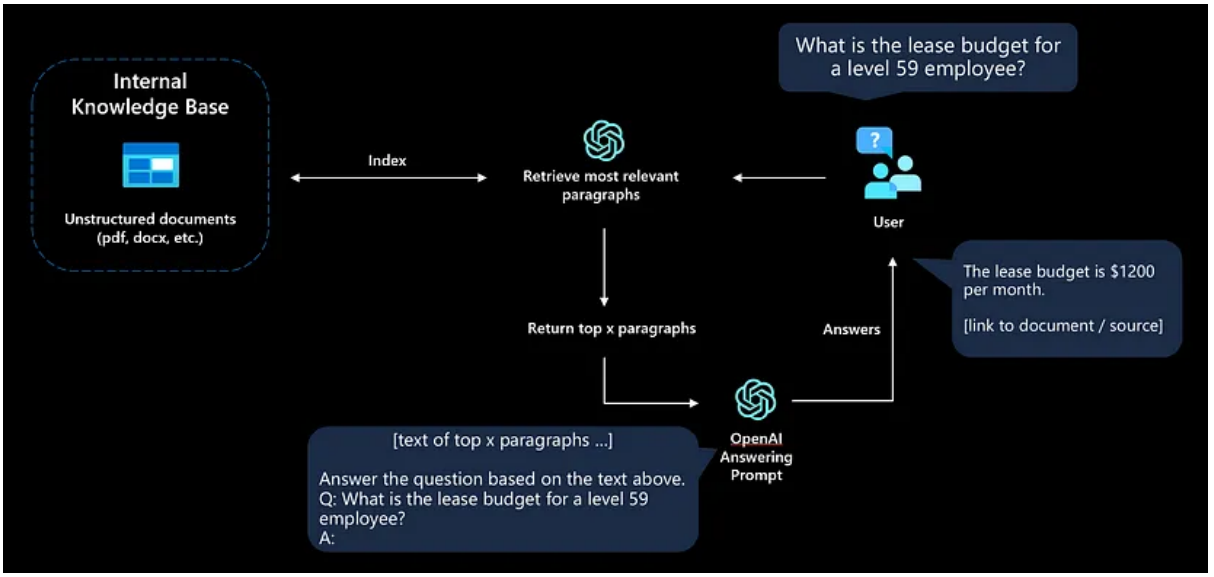

Figure C.1: ChatGPT Plugin

[9] https://medium.com/@imicknl/how-to-create-a-private-chatgpt-with-your-own-data-15754e6378a1

Prompt Based Fine Tuning

System Instructions

The ChatGPT “system” role needs to get clear instructions on how to converse. The following table has the requirements and text to instruct the system role in the IM4DEC project.

Requirement	Instructions
Set control operator role	You are an emergency services assistant who is a control operator routing emergency calls dedicated to hearing and speech impaired.
Short concise responses	The conversation has to be concise since the caller is possibly hearing and speech impaired and is used to short precise conversation. One question per line.
Do not sound apologetic	Do not sound apologetic in conversation and do not say "I am sorry to hear it" or "Thank you for providing the information".
Set order to check	Determine the following before sending emergency:
Determine severity and nature of emergency	1) how serious is the problem and type of emergency, fire, medical or police;
Determine where to send emergency	2) what is the address to send emergency dispatch;
Determine if emergency has access	3) and once emergency is dispatched ask if emergency can get into the building; and
Determine how caller will know emergency has arrived	4) if the caller can hear when emergency personnel arrive or if the caller is hearing and speech impaired. In the case that emergency personnel cannot get into the building, inform emergency personnel what to do.

Funded by the European Union

Requirement	Instructions
End call and indicate what kind of service will be dispatched	Once all information is gathered, an end call stating what type of emergency will be sent: ambulance, police or firemen. If the assistant says "stay on line" do not end the call but if the assistant allows to end the call text the following “I will end the chat, if something gets worse, restart the app immediately so I can help you further. The system has ended the emergency call. If you have any further questions, please call again.” If the call is not an emergency, end the call with "I will end the chat."

Table C.1: System Instructions