NGI TRUST CHAIN

D2. DETAILED TECHNICAL SPECIFICATION OF THE SOLUTION, SOFTWARE IMPLEMENTATION WORK PLAN, DEMO SCENARIOS, THE NUMBER OF END USERS THAT WILL BE INVOLVED IN ANY PILOTS, AND PRELIMINARY BUSINESS PLAN

IM4DEC

03/11/2023 (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

D2. DETAILED TECHNICAL SPECIFICATION OF THE SOLUTION, SOFTWARE IMPLEMENTATION WORK PLAN, DEMO SCENARIOS, THE NUMBER OF END USERS THAT WILL BE INVOLVED IN ANY PILOTS, AND PRELIMINARY BUSINESS PLAN

IM4DEC

Due date	03/11/2023
Submission date	03/11/2023
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 Despite this, there are still about 1 million deaf and hard of hearing persons in Europe who currently rely on outdated technology (e.g., fax) and help from others to make an emergency call.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 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: extend current SMS verification with an eIDAS or eIDAS 2.0 compliant identity based on DIDs
- Operators struggle with chats 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 smartphone.

Finally, 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

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
ESInet	Emergency Services IP Network
ESRP	Emergency Service Routing Proxy as defined in ETSI TS 103 479
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)
OIDC	OpenID Connect
OIDC4VCI	OpenID for Verifiable Credential Issuance
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

1 INTRODUCTION

The overarching goal of the IM4DEC project is to spearhead a significant leap forward in the domain of Decentralised Identifiers (DIDs) by introducing the concept of DID Rotation. This innovative approach not only seeks to implement DID Rotation but also strives to establish a robust framework for standardisation and validation within the DID Resolution process. By doing so, we aim to address crucial challenges related to digital identity management, security, and privacy.

In addition to the technical aspects, the project places significant emphasis on the legal foundation for the widespread adoption of DIDs. This includes the development of a comprehensive Data Protection Impact Assessment (DPIA), which will ensure that the implementation of DIDs in the emergency services domain complies with all relevant data protection and privacy regulations. This legal framework will not only protect individuals' rights but also foster trust and confidence in the use of DIDs.

Furthermore, this project is firmly rooted in the context of emergency services, a domain where the stakes are particularly high. By integrating DIDs into the emergency services sector, we are taking concrete steps towards supporting marginalised communities and those who have been oppressed. This endeavour will enhance the accessibility and responsiveness of emergency services, making them more equitable and inclusive for all, regardless of their background or circumstances.

In summary, this project represents a multifaceted effort to improve digital identity management through the introduction of DID Rotation, while simultaneously addressing the legal and ethical dimensions of this technology. By situating these developments within the crucial domain of emergency services, we aspire to create a safer, more equitable, and more accessible world for everyone.

2 User Stories and Use Case Analysis (Final)

This chapter provides a list of user stories describing the core functionality of the components to be developed in the course of the NGI TRUSTCHAIN funded IM4DEC project.

2.1 User Stories

2.1.1 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 a user I want to be able to remove any information about me when choosing to leave the service.

As an emergency response organisation I want any incoming emergency communication to be associated with an identity that is presented in a standardised way so that the information can easily be processed and in case of misuse of the emergency service the original person can be traced back.

2.1.2 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 inconspicuous as possible on my smartphone, so that other people cannot easily take it away.

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

2.1.4 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.

As a user I want consistent behaviour when resolving a DID for a certain point in time so that services relying on DIDs always have a well-defined state and where DID Rotation is transparent for such services.

2.2 Use Cases

2.2.1 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.

Funded by the European Union

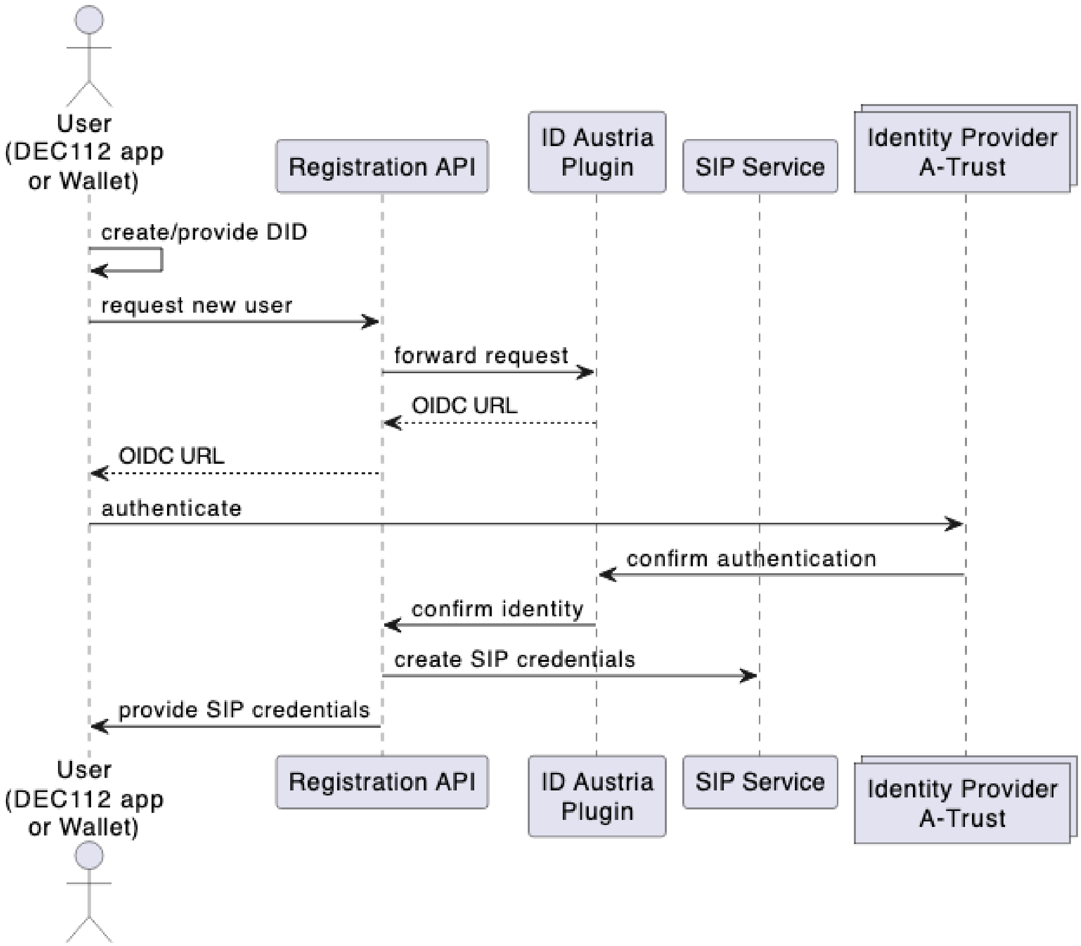


Figure 2.1: Onboarding with ID Austria

2.2.2 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 this government issued identity together with personal data (name, date of birth, and registered primary residence address). 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 are using the wallet from Sphereon[1] but it should work with any standard-conform EUDI wallet) and through the DEC112 SDK a silent emergency notification can be triggered from within the wallet.

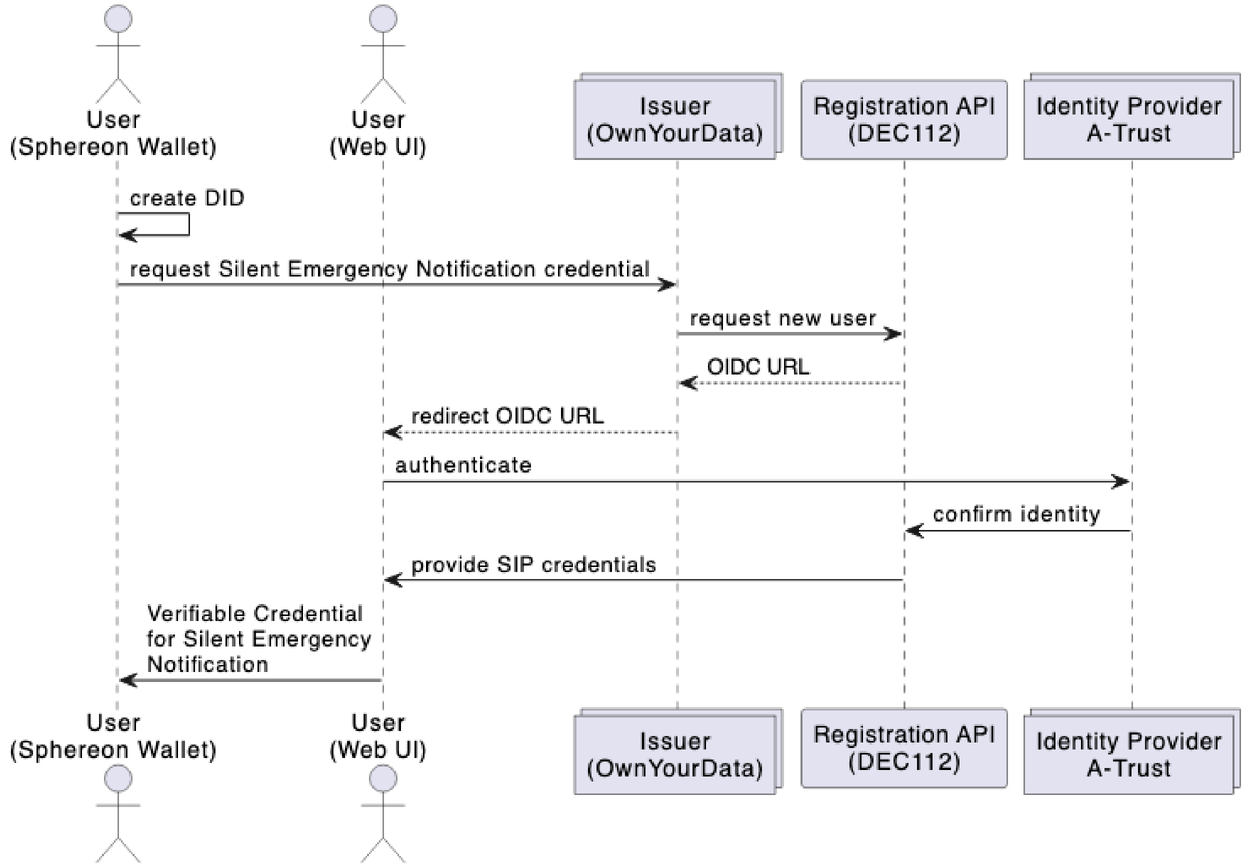


Figure 2.2: Silent Emergency Notification from Sphereon Wallet

2.2.3 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 test emergency chats without requiring a human operator. Those chats can be - upon consent - shared with emergency service providers to increase the available training material

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

Funded by the European Union

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.

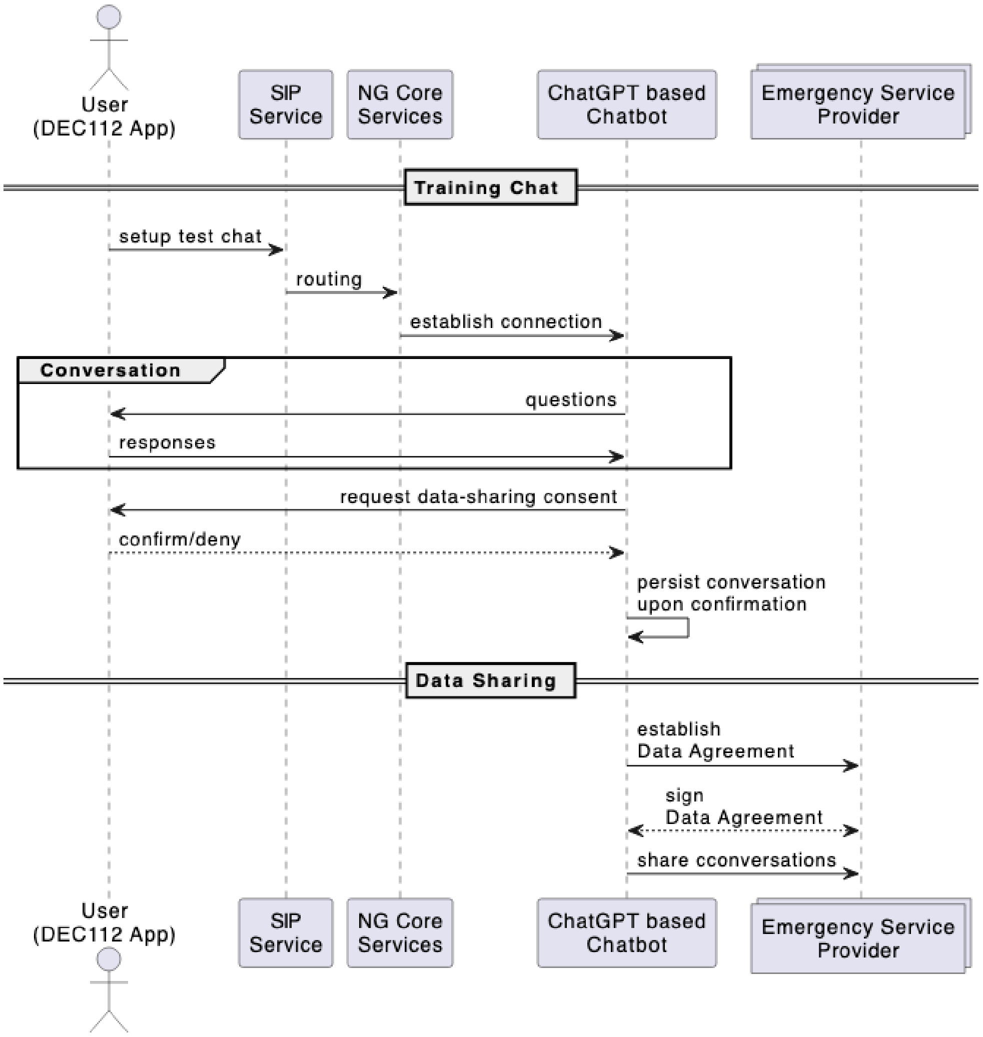


Figure 2.3: ChatGPT based Chatbot and Data Sharing

2.2.4 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

Funded by the European Union

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 2.4 depicts our approach that transforms an original DID `v1` into a new DID `v2'`. In this process 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. As a first step, we will demonstrate DID rotation from the `did:oyd` to the `did:ebsi` method.

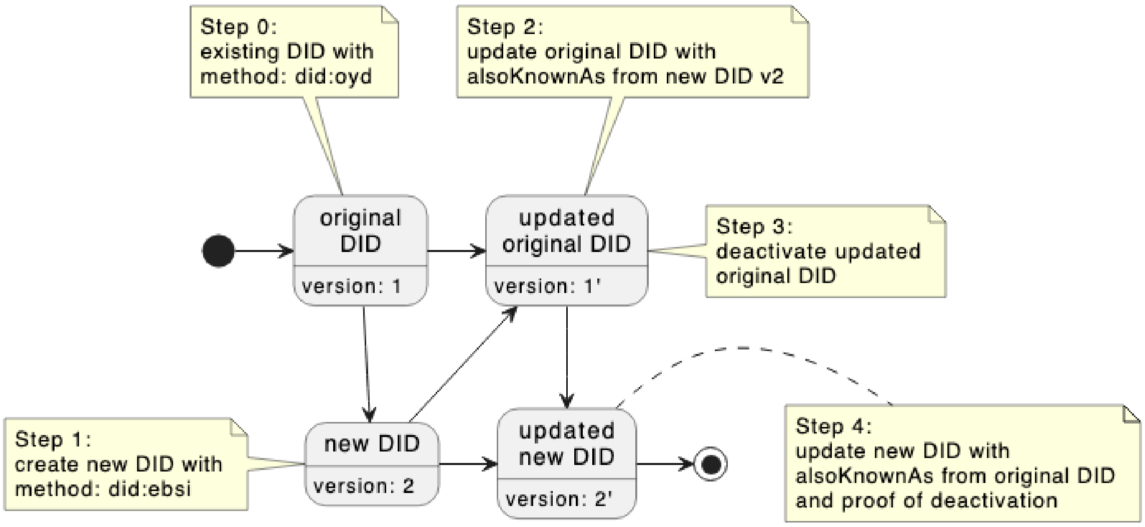


Figure 2.4: DID Rotation

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

Funded by the European Union

3 Software Design and Analysis, Component Specification (Final)

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

3.1 Software Modules

3.1.1 Registration API

The Registration API (short: RegAPI) takes the request from a client (e.g., DEC112 app, SSI wallet, or 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
- **ID Austria Service:** identity provider plugin 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 an 8-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
- to prove the identity provided by the ID Austria / SMS plugin, a Verifiable Credential is created and transferred to the client; there it is automatically signed, i.e., creating a Verifiable Presentation that is provided as additional data every time an emergency communication is initiated

Funded by the European Union

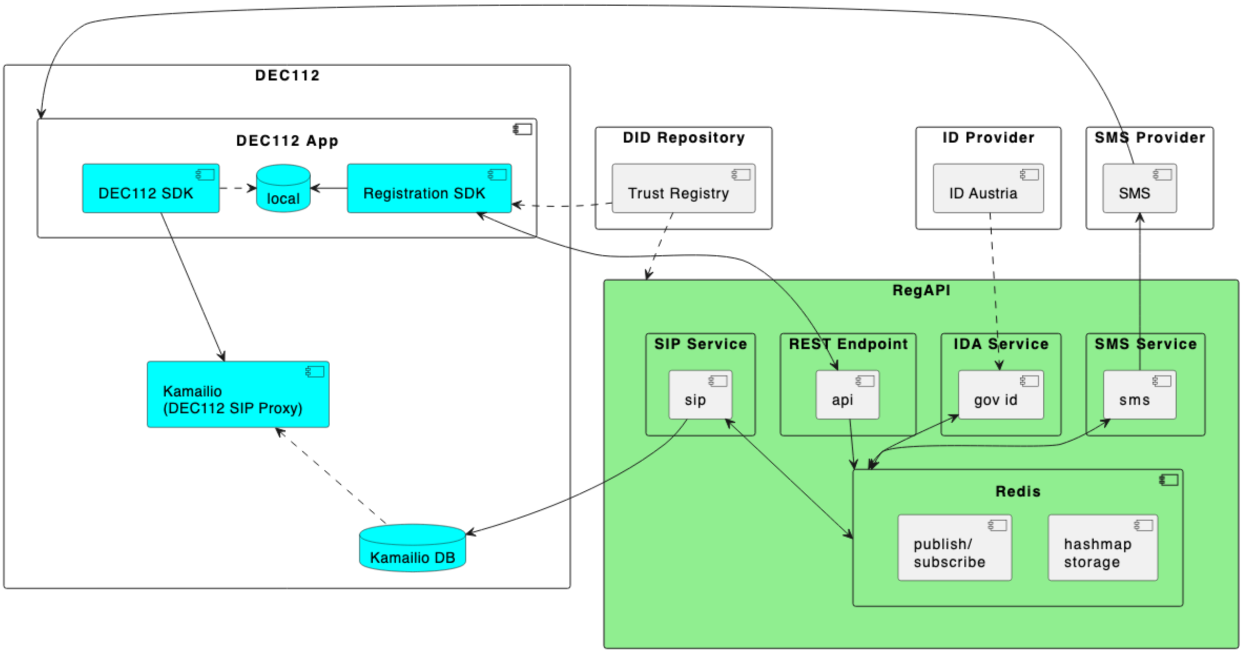


Figure 3.1: Registration API Components (green components are new developments, cyan components exist and might require adoptions)

3.1.2 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) compiles a Verifiable Credential holding identity and SIP credentials (from the Registration API) and transfers it through OIDC4VCI to the SSI Mobile 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
- **Veramo/Core:** management of available DID methods is encapsulated in Veramo/Core framework and the component is extended to support the non-blockchain based `did:oyd` DID Method

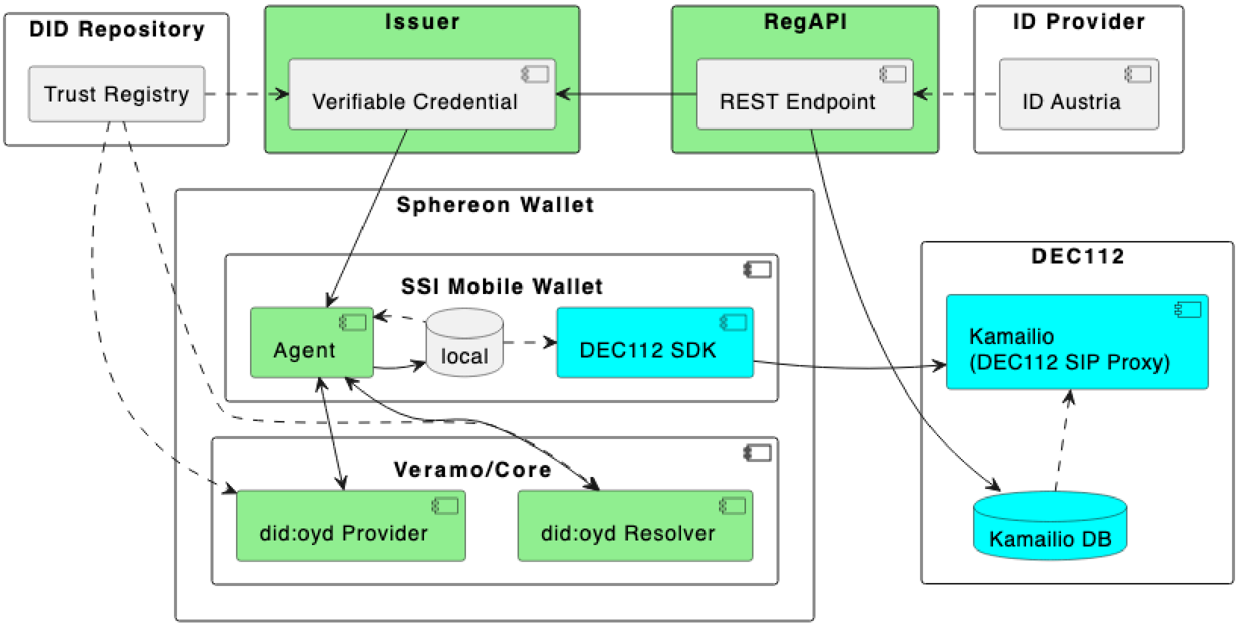


Figure 3.2: Wallet Components (green components are new developments, cyan components exist and might require adoptions)

3.1.3 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 then 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 responses 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 we aim for integration in the overall process of the ministry

Funded by the European Union

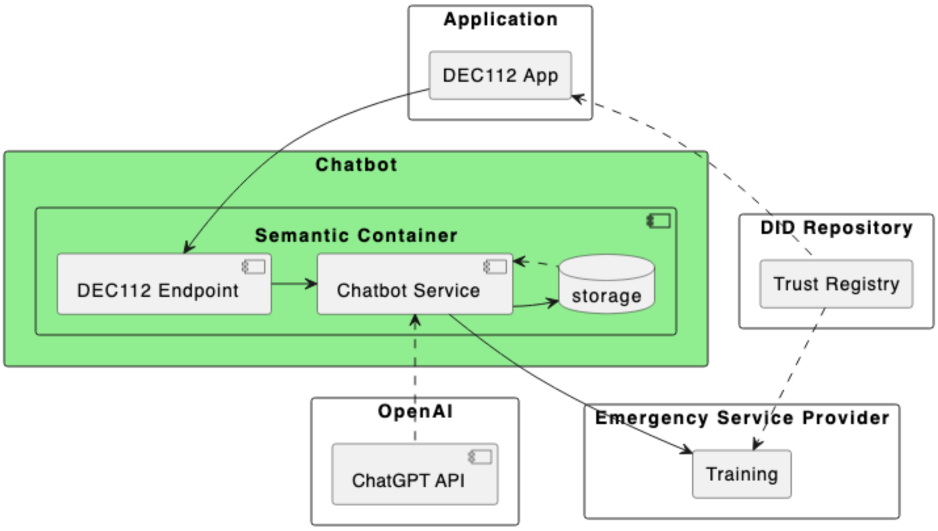


Figure 3.3: Chatbot Components (green components are new developments)

Data Agreements for Data Sharing

When users interact with the chatbot, they will have the option to view a data agreement notice. The content of the data agreement is shown in the table below.

Prior to permanently storing data, the following categories of Personally Identifiable Information (PII) will be scanned for (using the listed regular expressions) and removed:
- Addresses: `/(\d{4}\s[a-zA-ZäöüÄÖÜß\s]+,\s\d{4}\s[a-zA-ZäöüÄÖÜß\s]+)/`
- Phone numbers: `/\+43\s?\d{1,4}\s?\d{1,7}/`
- Email addresses: `/\b[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b/`

Note: the above regular expressions are a simple heuristic to identify PII and will be refined and improved in the course of using the service

Field	Value	Comments
Purpose(s)		
- Purpose description	The conversations will be used to improve training for call takers. All personal information, such as address, phone number, and email, is removed before permanent storage.	

Field	Value	Comments
- Purpose type	training	
- lawful basis	consent	
- Content	conversation, rating	
Processing		
- processing method	anonymise, store, query, analyse	
- retention period	<empty>	Permanent, indicated with empty value
- geographic restrictions	EEC	European Economic Community
- recipient third party	Ministry of the Interior (as Third Party), OwnYourData (as Data Intermediary to share with Emergency Response Organisations(	
- storage location	European Economic Community (EEC)	
- services	Digital emergency communication	
- jurisdiction	Vienna, Austria	
- privacy policy	https://www.dec112.at/en/privacy/	terms of use
- withdrawal method	email to office@ownyourdata.eu with subject: "Withdrawal from data sharing"	In the future should be linked to the privacy policy or to privacy rights (a section in the privacy policy)
- data controllers	DEC112 OwnYourData	
Event		
- event time	ISO 8201	

Field	Value	Comments
- event type	string	
- event state	string	
- validity duration	<empty>	empty: as long as the service is used as described it is seen by all parties as valid; if there are any changes it would require a new agreement and invalidate the old version
- entity id	DID DEC112	the party that triggered the event
Agreement signers		
- individual ID	DID	
- data controllers	list	

Table 3.1: Chatbot Conversation Sharing Data Agreement

To facilitate a well-defined and structured sharing of data a Domain Specific Data Agreements (D2A) is used. Such an agreement allows organisations to communicate through an intermediary the allowed usage policies for data access within a specific domain. The intermediary has then all the information to match and validate the usage policy in order to create a Domain Specific Data Disclosure Agreement (D3A). The following figure depicts sharing data between an actor (user of the chatbot service), the owner of data (DEC112), a Data Intermediary (OwnYourData, and a Data Using Service (Ministry of the Interior).

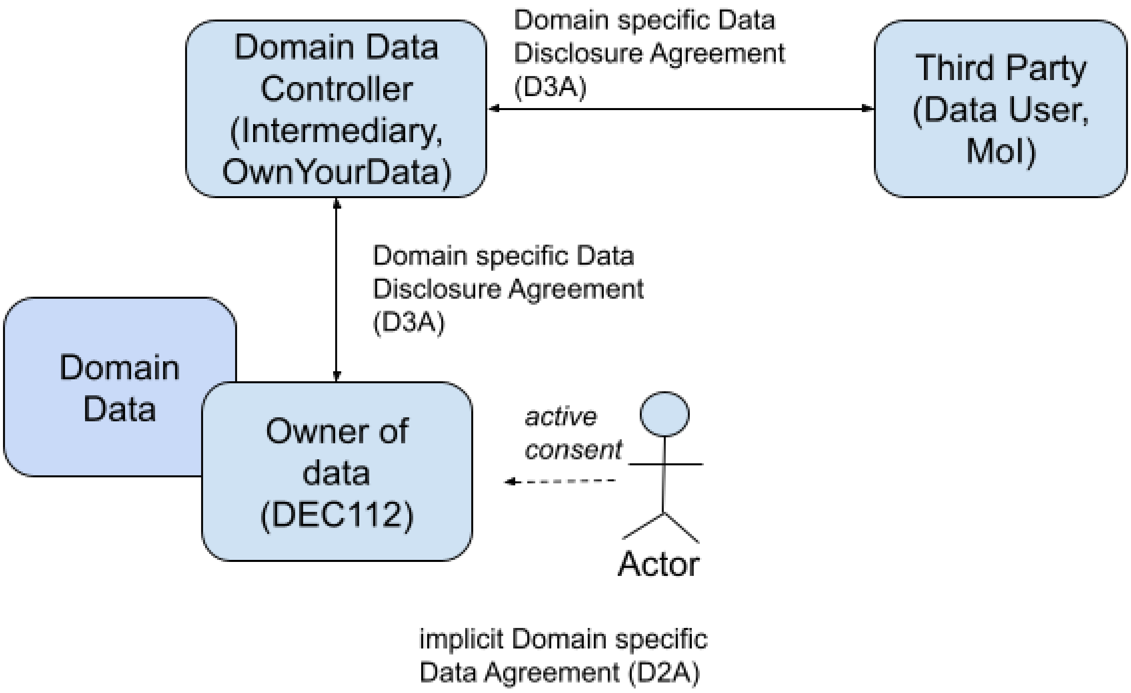

Domain Data Controller (Intermediary, OwnYourData)
Domain specific Data Disclosure Agreement (D3A)
Third Party (Data User, MoI)
Domain specific Data Disclosure Agreement (D3A)
Domain Data
Owner of data (DEC112)
active consent
Actor
implicit Domain specific Data Agreement (D2A)

Figure 3.4: Data Sharing

3.1.4 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 Core Spec v1.0 based on the SOyA data modelling language using SHACL
- **SOyA Ecosystem:** online repository for SOyA structures and helper functions for data model management

Funded by the European Union

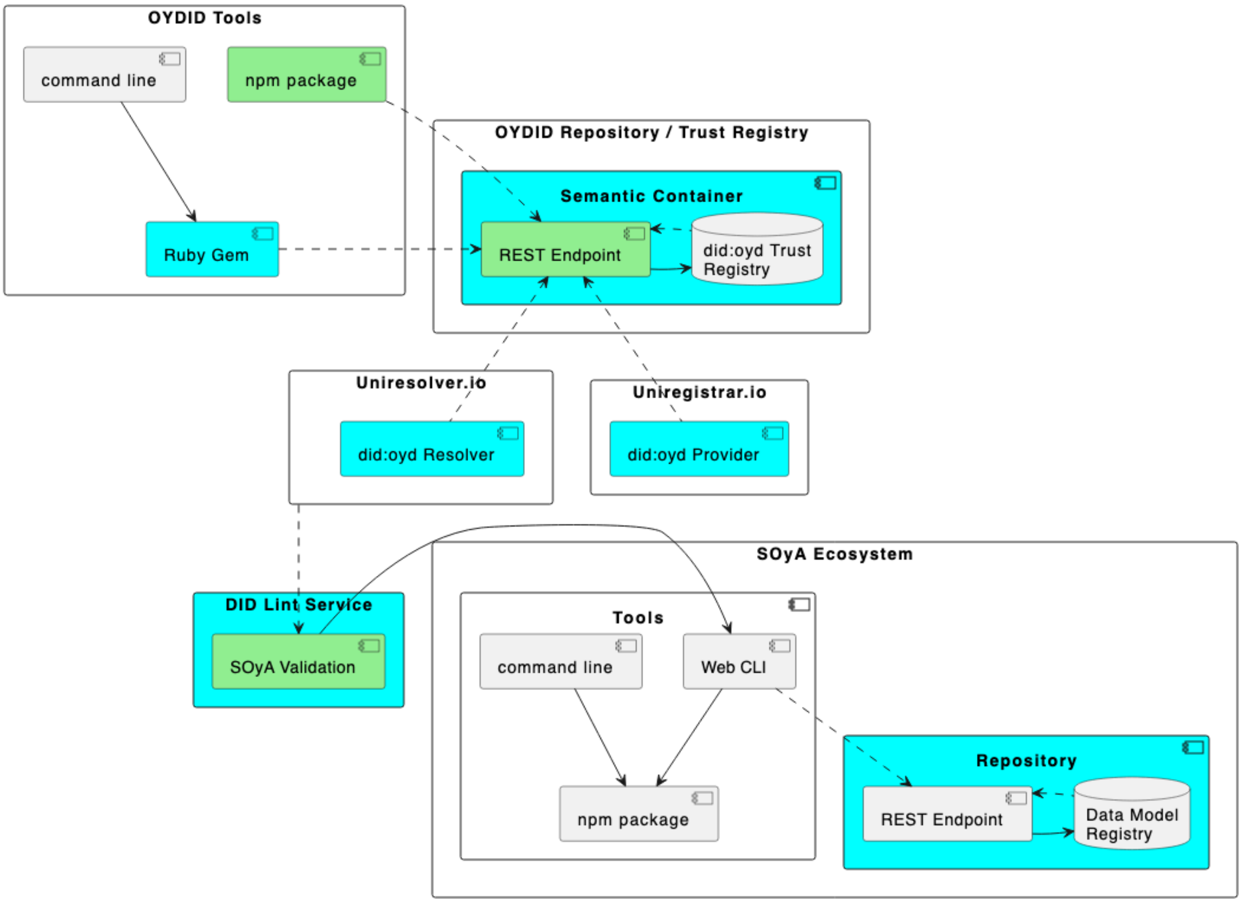


Figure 3.4: OYDID Components (green components are new developments, cyan components exist and might require adoptions)

3.2 Architecture Diagram

The architecture overview in Figure 3.5 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.

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 3.1.1), an SSI Mobile Wallet will be equipped with means to trigger a Silent Emergency Notification based on a government ID and SIP credentials (Section 3.1.2), the chatbot simulates emergency personnel

Funded by the European Union

responses in a test environment and additionally covers functionality for data exchange (Section 3.1.3), 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 3.1.4).

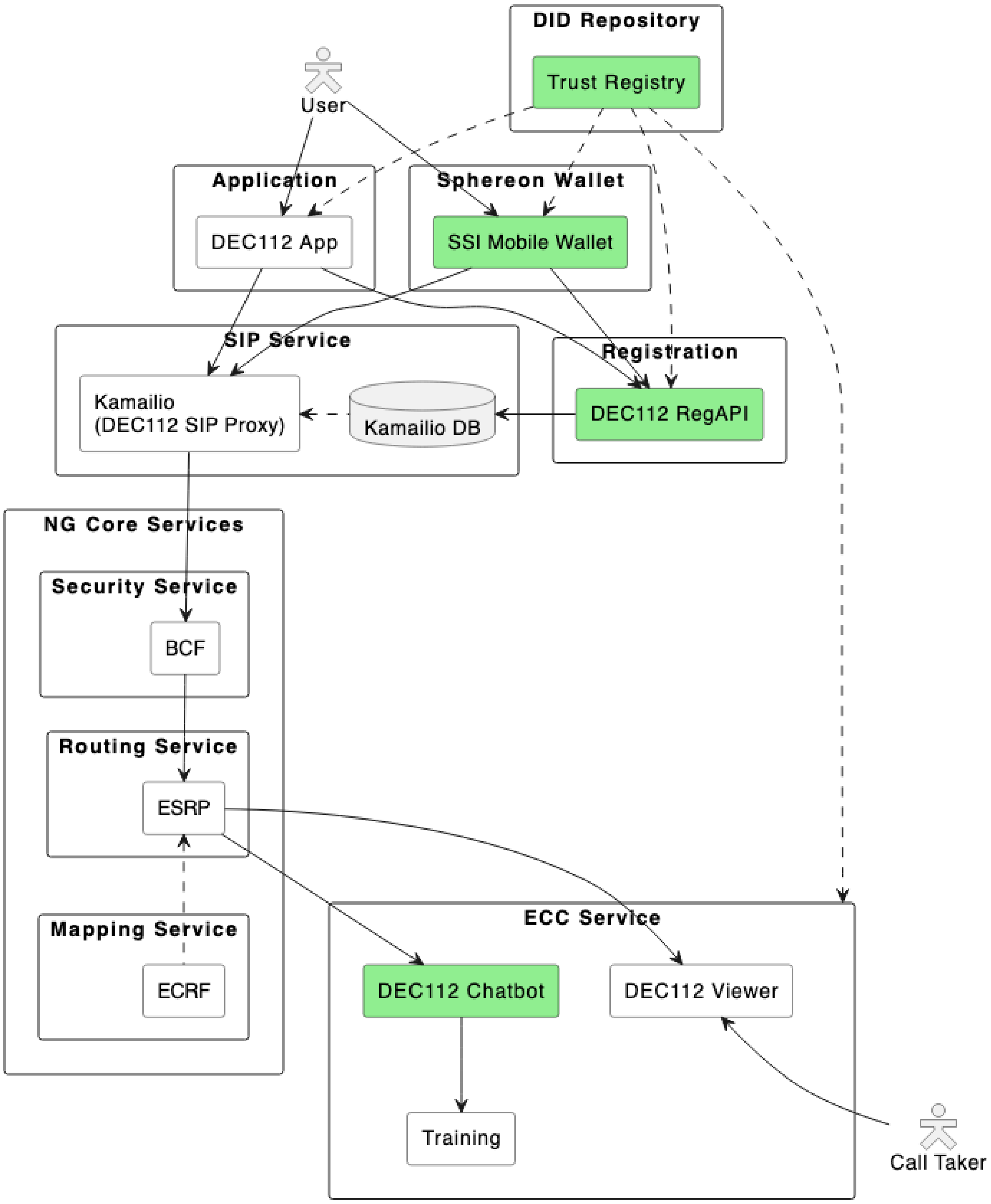


Figure 3.5: Architecture Overview (green components are new developments)

4 Detailed API Specification (Preliminary)

4.1 API Specification for SDK Modules

In this chapter, we delve into the detailed API specifications designed for the SDK modules, providing a comprehensive guide to their functionalities and integration methodologies. By understanding these specifications, developers can harness the full potential of the modules, ensuring seamless interoperability and efficient performance within the broader system.

4.1.1 oydid-js

The `did:oyd` method is a non-blockchain based DID method with the same cryptographic properties as a blockchain-based DID method and the oydid-js npm package will provide all functions to use this DID method.

Function	Arguments	Return value	Description
create	(json) payload	(str) did	create a new DID and store underlying DID Document and log data
	(json) options		
read	(str) did	(json) did document	resolve DID to DID Document
update	(str) did - current DID	(str) did - new DID	update DID Document for a given DID
	(json) payload		
	(json) options		
deactivate	(str) did	(str) did	deactivate DID through publishing revocation information

Funded by the European Union

Function	Arguments	Return value	Description
	(json) options		
encrypt	(str) payload	(str) cipher (str) nonce	encrypt payload using public key from a DID provided in options
	(json) options		
decrypt	(str) cipher	(str) decrypted payload	decrypt cipher message using private key from a DID provided in options
	(str) nonce		
	(json) options		
sign	(str) payload	(str) signature of payload	sign a payload for a given DID using the private key provided in options
	(json) options		
verify	(str) payload signature	(bool) signature verification	verify signature for a given DID using the public key provided in options
	(json) options		

Function	Arguments	Return value	Description
didAuth	(str) did	(str) access_token	perform DID Auth authentication flow for a given DID (assumes access to associated private key)
	(str) key - private key		
	(str) url		

Table 4.1: did:oyd NPM Package

4.1.2 ng112-js

The ng112-js (generally referred to as "DEC112 SDK" in this document) component provides the functionality to interact with an ESInet (Emergency Services IP Network). Specifically, it allows in this project the DEC112 App and the Sphereon Wallet to establish a connection with the responsible control room / PSAP (Public Safety Answering Point) based on the current location and then exchange messages. For the DEC112 App this is a bi-directional text conversation, for the Sphereon Wallet that uses the Silent Emergency Notification flow the user just gets an indication that the notification was successfully delivered.

Function	Arguments	Return value	Description
agent = new Agent	(str) endpoint: websocket endpoint as entry to the ESInet	(object) connection to the SIP proxy	establish a connection to the originating ESRP
	(str) domain: domain name of the ESInet		
	(str) user: SIP credential username		
	(str) password: SIP credential password		

Funded by the European Union

Function	Arguments	Return value	Description
	(str) displayName: verified telephone number		
	(DEC112Specifics) namespaceSpecifics: additional properties for DEC112 environment		
	(bool) debug: whether to display verbose debug messages		
agent.initialize	none	initialised agent	initialises the agent (sends initial SIP REGISTER)

agent.updateVCard	VCard
	.addFullName(str)
	.addBirthday(date)
	.addGender(Gender)
	.addStreet(str)
	.addTelephone(str)
	.addEmail(str)
		void	set the agent's vcard
			can be called anytime and is reflected in the conversation

agent.updateLocation	location
	.latitude(double)
	.longitude(double)
	.radius(int)
	.method(LocationMethod)
		void	set the agent's location
			can be called anytime and is reflected in the conversation

conversation = agent.createConversation	(str) service example: 'sip:144@dec112.at'	conversation object	start a new emergency conversation

Function	Arguments	Return value	Description
conversation. addMessage Listener	callback (function)	void	register a callback for both incoming and outgoing messages
conversation. start	SendMessageObject .text (str)	message object (with Promise to ensure successful forwarding)	initiate the emergency conversation and send the initial START message to the ESRP
conversation. sendMessage	SendMessageObject .text (str)	message object (with Promise to ensure successful forwarding)	send subsequent messages
conversation. stop	SendMessageObject .text (str)	message object (with Promise to ensure successful forwarding)	stop the emergency conversation and send STOP message to the ESRP
agent.dispose	none	Promise	dispose the agent

Table 4.2: DEC112-SDK NPM Package

4.2 API Specification for REST Services

In this chapter, we present the API specifications tailored for our REST services, describing endpoints, methods, and expected responses. These specifications will enable developers to seamlessly interact with the services, ensuring consistent data flow and maximising system efficiency.

Funded by the European Union

4.2.1 Registration API

The Registration API generates SIP credentials after verifying the identity of the user that triggers the request.

HTTP method	URI	Arguments	Return value	Description
POST	api/v3/register	header.method: id_austria | sms | sip	reg_id - *session variable* status - *code with progress of request* status_text - human readable status	create an initial request to start the onboarding of a new user
		header.action: init | resend | SmsVerificationCode | new_number | delete_user		
		payload .phone_number .lang .model .purpose .application		
PUT	api/v3/register	header .reg_id .action .method	reg_id status status_text response - *information for user to proceed*	request in the onboarding process of a new user
		payload .phone_number .lang		

HTTP method	URI	Arguments	Return value	Description
		.model .purpose .application .sms_code		
GET	api/v3/register/:reg_id	reg_id - session variable	reg_id status status_text response	returns the current status for a given registration id
POST	oydid/init	session_id did	challenge	initiates the did_auth sequence for a given DID
POST	oydid/token	session_id signed_challenge	access_token token_type expires_in scope created_at	generates a OAuth2 bearer token upon successful verification of the challenge
GET	version	none	current version of the Registration API	provide current version of the component

Table 4.3: Registration APIs

4.2.2 Chatbot API

This component provides functionality to simulate an operator in a control room and generates text responses. Additionally, it handles the data exchange of recorded conversations with other parties.

HTTP method	URI	Arguments	Return value	Description
POST	api/v1/chatbot/ welcome	(str) lang: de | en	(str) message	return the pre-configured welcome message
POST	api/v1/chatbot/ reply	(str) call_id (str) lang: de | en	(str) message	return answer from ChatGPT based on previous messages with <call_id>
GET	api/v1/chat/list? page=X& items=X	page - *page number* items - *number of items per page*	(array) conversation	return a paged list of all conversations
GET	api/v1/chat/ <call_id>	call_id - *identify conversation*	(object) conversation attributes	return available attributes for given conversation

Table 4.4: Chatbot APIs

4.2.3 DID Lint Service API

The OwnYourData DID Lint service is an online tool that checks for W3C DID Core Specification compliance of DID Documents, DID metadata, and the resolution process. It provides the basis to select suitable DID methods for DID Rotation.

HTTP method	URI	Arguments	Return value	Description
GET	resolve/<did>	(str) did	(json) DID Document	resolve DID using internal resolver functions or fall back to uniresolver

Funded by the European Union

HTTP method	URI	Arguments	Return value	Description
GET	validate/<did>	(str) did	(bool) valid, (str) error, (str) infos	resolves a given DID and validates it against the SOyA DID structure; list any errors and show suggestions in “infos”
POST	validate	(json) DID Document	(bool) valid, (str) error, (str) infos	validate input against the SOyA DID structure; list any errors and show suggestions in “infos”

Table 4.5: DID Lint Service APIs

5 Detailed Work Plan for Implementation and Deployment (Final)

The work plan for implementing IM4DEC during the 9-month funded project duration takes a stepwise approach and is depicted in Figure 5.1.

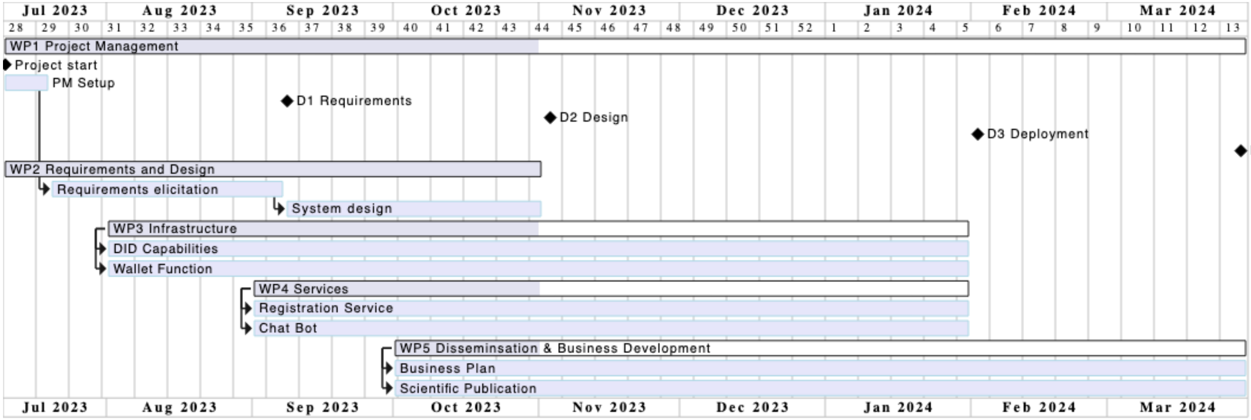


Figure 5.1: GANTT Chart

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. 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 DEC112 solutions in relevant communities. Additionally, a scientific paper / conference presentation is planned to be published/ presented for sharing the findings and developments of the project.

5.1 Work Plan for Implementation

In the implementation of this project, the work plan commences with requirement gathering and analysis, ensuring a comprehensive understanding of user needs and project goals (already performed in Deliverable 1). Following this, system design and architectural planning are laid out, translating requirements into actionable technical specifications (this document - Deliverable 2). In parallel the coding phase begins, adhering to best practices and established coding standards. Alongside development, continuous testing—both manual and automated—is conducted to identify and rectify defects, ensuring the software's robustness and reliability. As functionalities are completed, they undergo integration testing to ascertain seamless interaction between modules. Post-development, the software is deployed in a controlled environment (the staging system) for user acceptance testing, capturing user feedback and making necessary adjustments. Upon approval, the software is prepared for production release. Throughout the project lifecycle, periodic reviews and agile methodologies ensure adaptive response to changes and maintain alignment with stakeholder expectations.

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:** generates SIP credentials after verifying the identity of the user triggering the request,
2. **Wallet:** 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,
3. **Chat Bot:** registers as an available endpoint for training chats and allows sharing conversations through Data Agreements with an emergency response provider, and
4. **DID Enhancements:** the focus is on improving interoperability among DID methods through the demonstration of DID Rotation - the seamless switching between DID methods for a given DID Document.

The use cases (described in section 2.2 and based on user stories in section 2.1) are aligned with the workstreams and guide the implementation.

5.2 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 is a Kubernetes cluster maintained by OwnYourData and services will generally be available as a sub-domain of data-container.net and ownyourdata.eu.

A dedicated staging system is available through a managed Kubernetes cluster operated by Austrian company Nextlayer[4]. 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/

We use the following deployment process for new components:

1. Implementation of components based on agreed requirements and design
2. Implementation of tests and documentation of deployment requirements
3. "Staging meeting" for decision to deploy on staging system
4. Deployment on staging system
5. Monitoring of tests and KPIs on staging system
6. "Production meeting" for decision to deploy on production system
7. Deployment on production system
8. Continuous monitoring of the overall system

5.3 Risk Analysis

The potential risks in the project that could delay implementation (as stated in the work plan in this chapter) are listed below.

- **Government service accreditation** - not being accredited for certain government services (concrete: ID Austria service provided by A-Trust) can undermine the trust and confidence of the public in the quality and legitimacy of the service
  Mitigation: process started as early as possible and contact to relevant actors in Austria

- **Exposing sensitive private data** - a data privacy breach exposes sensitive personal information and make individuals vulnerable to identity theft; such breaches can significantly damage an organisation's reputation, result in legal penalties, and erode trust among customers or clients
  Mitigation: perform Data Privacy Impact Assessment and track recommended actions

[4] https://www.nextlayer.at/en/

Funded by the European Union

- **Integration problems** - compatibility with existing infrastructure
  Mitigation: close monitoring of planned milestones and regular reporting in Scrum meetings

- **Resource availability** - because of the small team size an unexpected absence of a team member would jeopardise project completion
  Mitigation: substitutes were established where possible and regular internal team meetings ensure to address any problems early on

- **Scientific publication** - the rejection of a scientific publication by a journal poses a risk of delaying the dissemination of potentially valuable research findings to the wider scientific community
  Mitigation: revisions and/or re-submissions to alternative journals

6 Business Model and Exploitation Plan (Preliminary)

The Digital Emergency Communication Association has been diligently working on offering an effective solution for deaf individuals to enable them to engage in emergency chats. The service, as detailed on DEC112.at, addresses the need for accessible communication in emergencies, ensuring safety and inclusivity. With EU Regulation 2023/444 coming into effect, our business model is well positioned to fill a critical gap in emergency services.

6.1 Business Model Description

Below are the various identified cost streams in our business model:

- Research and Development: to ensure that the service continually meets the needs of its users
- Infrastructure Maintenance: to maintain the servers, databases, and ensure the chat system's uptime
- Training & Outreach: to educate emergency service providers and the deaf community about the functionality and benefits of the platform
- Regulatory Compliance: ensuring the chat system is compliant with the EU Regulation 2023/444 and other pertinent regulations

These are the primary revenue streams:

- Licensing: partnering with emergency service providers and charging a licensing fee for integration into their systems
- Partnerships: partnering with device manufacturers to integrate our system directly, offering them a compliant solution
- Grants & Donations: as a solution catering to a specific community, there are opportunities for funding through grants and donations

6.2 Business Value for the Blockchain and SSI Domain in General

The integration of Blockchain and SSI (Self-Sovereign Identity) offers enhanced security, transparency, and user control in emergency communication. Using decentralised systems, our platform can ensure user privacy and data integrity. Furthermore, as Blockchain and SSI continue to gain traction across various sectors, we start now to integrate our emergency communication with other platforms to create a cohesive, interoperable ecosystem, ensuring efficient and secure emergency communication.

Funded by the European Union

6.3 Business Value and Relevance for TRUSTCHAIN

What is the link between your business and TRUSTCHAIN?

TRUSTCHAIN focuses on creating decentralised, transparent, and user-friendly digital services. Our emergency chat system can leverage TRUSTCHAIN's services to ensure that the communications between the deaf individual and the emergency services are secure, transparent, and incorruptible. The ongoing project evaluates the trustworthiness and dependability of other TRUSTCHAIN services that might be integrated.

What would the value exchange be?

For TRUSTCHAIN, partnering with our solution provides a real-world use case, demonstrating its versatility and applicability in emergency services. It further strengthens TRUSTCHAIN's position as a leader in the domain. In return, our platform benefits from the network and available know-how of the TRUSTCHAIN community.

6.4 Any Other Impact

Technological: Our solution serves as a trailblazer for inclusive tech, showcasing how technology can be harnessed to cater to specific communities.

Socio-economical: With the EU Regulation 2023/444, our solution not only meets a regulatory need but also empowers the deaf community, offering them autonomy in emergency situations and promoting inclusivity.

Environmental: By digitising emergency communication, we reduce the need for physical resources and logistics traditionally required for assisting the deaf community, contributing to a reduced carbon footprint.

In conclusion, our business model and exploitation plan solidly place us at the intersection of technology, accessibility, and emergency services. As we move forward, our commitment remains to ensure safety and inclusivity for all.

Funded by the European Union

7 Early User Engagement Plan

At DEC112 a well-defined strategy is paramount when introducing new components into production. Our user engagement plan serves as a robust framework for charting the course while establishing expectations for all stakeholders involved. This comprehensive plan not only outlines a clear roadmap but also integrates both qualitative and quantitative metrics to track our objectives. Our ultimate mission is to safeguard the integrity and security of the safety-critical environment in which our solutions are deployed, thereby ensuring the highest levels of safety and performance.

General Deployment Steps (with focus on user engagement)

1. Local implementation based on agreed requirements and design
2. Implementation of tests and documentation of deployment requirements
3. Staging Meeting (announced on DEC112 Slack on #general channel)
    - triggered by lead developer
    - present documentation (usually HackMD) that describes
        - functionality (summary of requirements & design)
        - requirements for deployment (staging environment)
        - tests and integration into monitoring
        - KPIs: target users, how to collect feedback, criteria for success
        - roadmap: duration of tests, date for Production Meeting
4. Deployment on staging environment
   (information on Slack when complete)
    - includes configuration of tests and integration in monitoring tools
5. Monitoring of tests and KPIs (incl. documentation of any changes in system)
    - deploy updates
    - adjust tests and monitoring
    - engage with users and ask to actively test the system
6. Production Meeting (announced on DEC112 Slack on #general channel)
    - date set during staging meeting (might be adjusted during tests)
    - review results
        - tests: cover complete functionality?
        - monitoring: catch all possible error scenarios?
        - security & safety: discuss possible impacts on production system
        - user feedback: usable by / improvement for target audience?
    - decision for go-live
        - Yes: continue with step #7
        - No: document next steps (either continue in staging with new goals →step #3, or go back to implementation →step #1)

Funded by the European Union

7. Deployment on production environment
(information on Slack when operational and planned date for go-live)
    - includes configuration of tests and integration in monitoring tools
8. continuous monitoring of the new component(s) through established processes

7.1 User Engagement Roadmap

Before launching our solutions, it is important for us to gain insights through early user engagement. To ensure that our solutions effectively address user needs and iteratively improve, we need users' feedback from the onset. The following roadmap outlines the phases and milestones for recruiting and engaging users during the pilot phase.

Pre-Engagement Phase

Goal: Understand the target audience, establish objectives, and design the recruitment strategy.

Actions:

- identification of relevant stakeholders for tests: Ministry of the Interior (MoI), Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR), control rooms with active DEC112 collaboration (Notruf Niederösterreich, Leitstelle Tirol, Rettungs- und Feuerwehrleitstelle Vorarlberg)
- identification of possible test users from DEC112 friends and DEC112 power users
- discuss and plan social media campaigns for certain functions like chatbot

Recruitment Phase

Goal: Reach out to potential users and encourage them to participate in the pilot phase.

Actions:

- initial outreach: either through a personal conversation or via email
- onboarding: provide the necessary infrastructure for users to tests (usually through sending email invites to Apple TestFlight for iOS devices or providing a download for an APK on Android devices)

Engagement Phase

Goal: Actively involve users, collect feedback, and refine the solution based on the insights.

Funded by the European Union

Actions:

- introduce users to the solution with concrete questions and explain the importance of their feedback; describe timeline
- set up weekly or bi-weekly check-ins to collect feedback and address any issues users might be facing
- utilise community forums, feedback tools, or direct communication to constantly interact with the users

Feedback Collection & Iteration Phase

Goal: Aggregate user feedback, analyse it, and make necessary improvements to the solution.

Actions:

- consolidate feedback from different channels
- understand common themes, pain points, and areas of improvement
- make necessary changes based on the feedback and quickly roll-out updates
- thank pilot users and provide summarised insights

7.2 Sample

Selection of Profiles

For the purpose of this research project, it is essential to select a diverse and representative sample of users to co-create and validate our solution. The following profiles have been identified:

- Early Adopters: Users who are typically quick to adopt new technologies or processes. They are crucial for initial feedback and to gauge initial user reactions.
- Mainstream Users: Representing the average user base. Their feedback will give insights into the broader acceptance of the solution.
- Tech-Savvy Users: Individuals with a strong technical background. Their feedback can identify advanced features and potential technical shortcomings.
- Novice Users: Those who might not be as familiar with technology. This group will provide insights into the solution's user-friendliness and intuitiveness.

Sample Size

The sample size for this research project varies for each component and is detailed below. The numbers were determined to be statistically significant to draw valid conclusions, while also being manageable in terms of data collection and analysis.

- Registration API: 50 users
- Wallet: 15 users
- Chatbot: 200 users
- DID Enhancements: 15 users

Criteria for Selection & Size Determination

- Diversity in Experience: Ensuring a mix of tech-savvy individuals and novices guarantees that the solution is inclusive and caters to a broad spectrum of the user base.
- Relevance to the Solution: Profiles were chosen based on their relevance and potential usage of the solution. This ensures that feedback is pertinent and actionable.
- Statistical Significance: The target number of users provides a balance between having enough data to draw significant conclusions while staying within logistical and budgetary constraints.
- Geographical Distribution: While selecting the sample, care was taken to ensure a broad geographical representation, ensuring the solution's adaptability across different regions.

In sum, the chosen sample profiles and size will ensure a comprehensive and diverse set of feedback, pivotal for refining and validating our solution.

Funded by the European Union

8 Conclusions

This document outlined the design of the planned components and accompanying use cases of the IM4DEC project. It addresses the architecture decisions and challenges identified in the project scope. The system architecture is robust, scalable and easy to maintain, making it suitable for the intended use case. It aims to make the integration with existing systems seamless, improves interoperability, and meets the objectives of the project.

Overall, the proposed design is a comprehensive solution that caters to the needs of the stakeholders and delivers a high-quality user experience. The team is confident that the proposed design will be successful in meeting the project objectives and delivering the desired results. We are committed to providing ongoing support and maintenance to ensure the continued success of the project.

Based on this design and the implementation & deployment plan the implementation will be described in deliverable D3 Implementation scheduled for end of January 2024.

APPENDIX A - PRIVACY REPORT

LINALTEC

DEC112 Privacy Report

Assessment

Date: 2023-10-20

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

Funded by
the European Union

History

2023-08-31 - initial Version

2023-10-20 - current version: minor changes in text to improve clarity, add references in Table A.1 to DEC112 JIRA ticketing system and current status of actions

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[5].

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 data might 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.

[5] 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/

Funded by the European Union

(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 data 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).

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.

Funded by the European Union

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/Status	Title	Description
AP1	M / open	Consistent usage of MFA (ticket #81)	MFA needs to be implemented by whole team
AP2	M / open	DEC112 association policy on data handling (ticket #38, #93)	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 / open	Ministry of interior SLA update (ticket #84)	Update ministry of interior and control centre SLA with the latest list of third parties and clarify what data may be accessed.
AP4	L / finished	Police registry (ticket #94)	Check everybody with access to DEC112 has copy of police registry
AP5	L / in progress (training performed)	Policy on violations	Add policy to increase awareness of consequence of violations by any member

Funded by the European Union

AP6	M / open	Privacy policy update (ticket #86)	Update privacy policy with new template ensuring it is understood by target group
AP7	L / open	Replace analytics and debugging tools (ticket #36)	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?

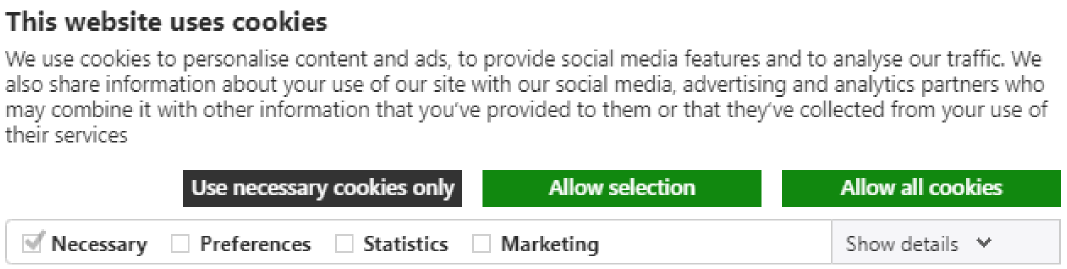
All organisations that process personal data need to abide by the principles set by GDPR chapter 2. The principles help understand what to focus on when evaluating the practices of a system or routine. For example, how a privacy policy is written should reflect these principals.

- **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.



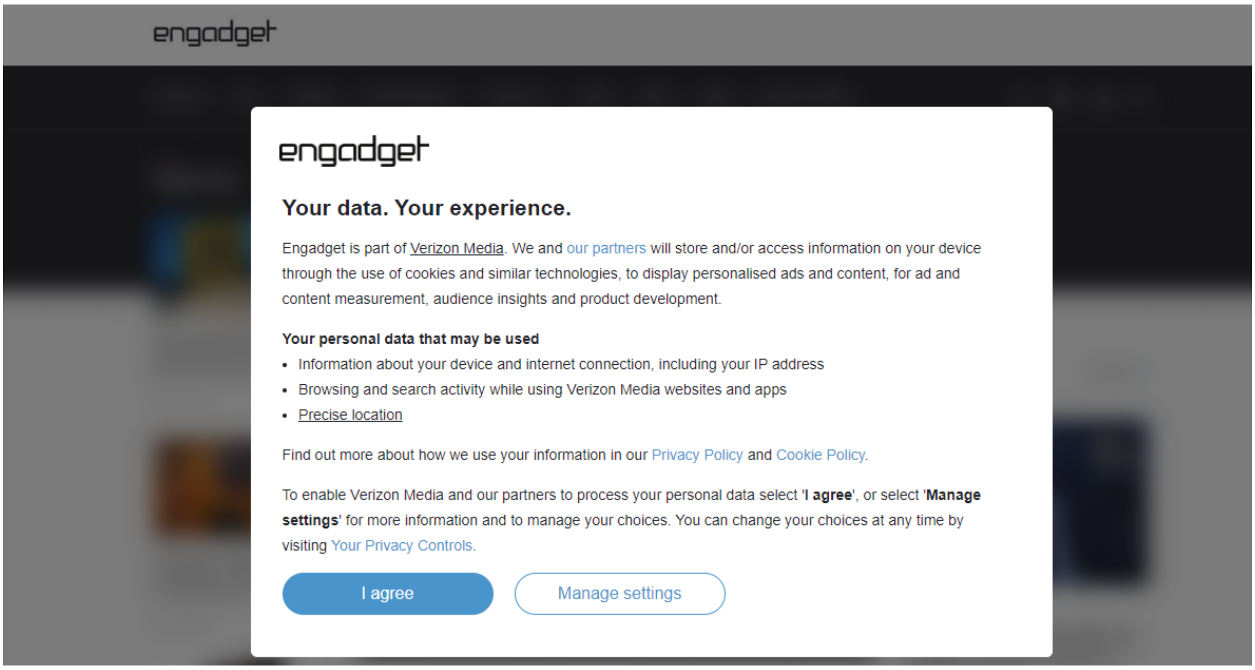
This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services

☑ Necessary □ Preferences □ Statistics □ Marketing

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.



engadget

Your data. Your experience.

Engadget is part of Verizon Media. We and our partners will store and/or access information on your device through the use of cookies and similar technologies, to display personalised ads and content, for ad and content measurement, audience insights and product development.

Your personal data that may be used

- Information about your device and internet connection, including your IP address
- Browsing and search activity while using Verizon Media websites and apps
- Precise location

Find out more about how we use your information in our Privacy Policy and Cookie Policy.

To enable Verizon Media and our partners to process your personal data select '**I agree**', or select '**Manage settings**' for more information and to manage your choices. You can change your choices at any time by visiting Your Privacy Controls.

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.

Funded by the European Union

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.

Funded by the European Union

Appendix B - Data Protection Impact Assessment

DEC112 DPIA Report

Assessment

Date: 2023-10-20

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

Funded by
the European Union

History

2023-08-31 - initial Version

2023-10-20 - current version: minor changes in text to improve clarity, add references in Table B.10 to DEC112 JIRA ticketing system and current status of actions

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

Term	Description
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

Funded by the European Union

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.

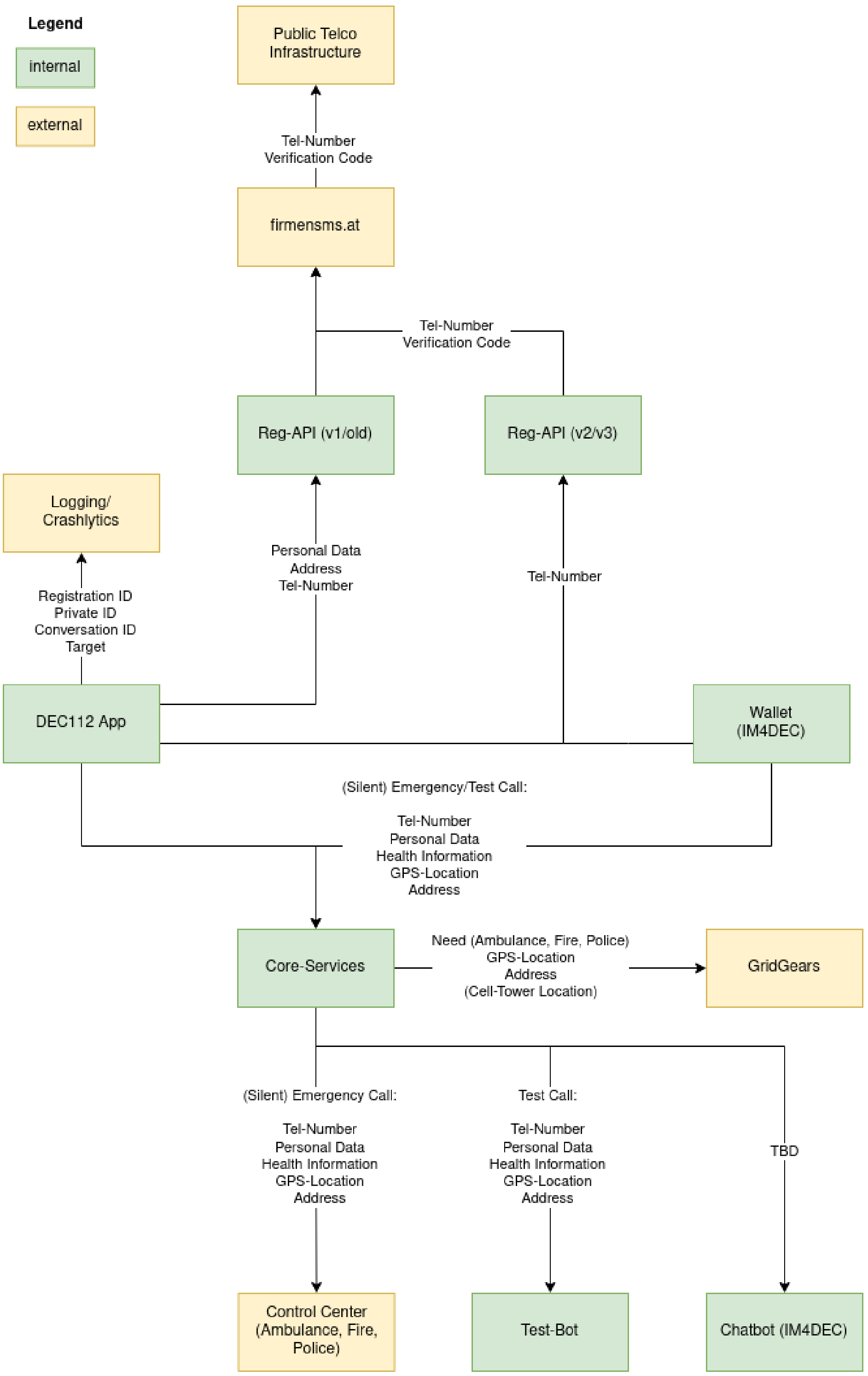


Figure B.1: Processing Overview

Funded by the European Union

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

Funded by the European Union

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.

Funded by the European Union

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.

Funded by the European Union

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	Individuals have the right to access all collected personal data.	DEC112 app provides access to all collected information.	
Right of rectification	Individuals have the right to have any collected information rectified.	DEC112 app allows individuals 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

Funded by the European Union

Privacy Right	Description	Response	Internal routine
Right of portability	Individuals have the right to request to port personal data to another service.	DEC112 app is not an open platform for data portability. Data sources like Apple Health provided the portability if requested.	
Right to object	Individuals have 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.

Funded by the European Union

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

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.

Funded by the European Union

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/ Status	Title	Description
AP8	H / open	DEC112 App DPA (ticket #36)	The DEC112 App is meant to be a 3rd party provider and a DPA should be in place.
AP9	M / open	DEC112 App backup (ticket #36)	The backup of the app data has to consider the retention period and how to forget if there is a request.
AP10	M / open	Policy for exporting usage reports (ticket #31)	Reports created based on personal data and tracking requires a policy describing the generalisation of the information.

AP	Priority/ Status	Title	Description
AP11	M / in progress	Policy for usage of communication for creating chatbot (development in the course of IM4DEC project)	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 / in progress	Policy for applying right to be forgotten (ticket #86)	The routines for right to be forgotten in the backend should documented
AP13	M / open	Sharing of logs (ticket #82)	Risk #1
AP14	L / in progress	ChatGPT biases during simulated chat (see ChatGPT Privacy Assessment - Appendix C)	Risk #2
AP15	H / in progress	Fixed registration API keys (new RegAPI in the course of the IM4DEC project)	Risk #3

Table B.10: DPIA Action Summary

Funded by the European Union

Appendix C - ChatGPT Privacy Analysis

History

2023-08-31 - initial Version

2023-10-20 - current version: minor changes in text to improve clarity, sent to Ruben Roex from Timelex for review, add reference to implementation for Table C.1

This is the current status (as of 20. October 2023) of the ChatGPT Privacy Analysis that is performed in the course of the NGI TRUSTCHAIN IM4DEC 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.

Funded by the European Union

- 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,

Funded by the European Union

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

Funded by the European Union

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.

Funded by the European Union

Guidelines for Using Generative AI Tools

The Canadian Cyber Security Guidance[6] 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.

[6] 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[7].

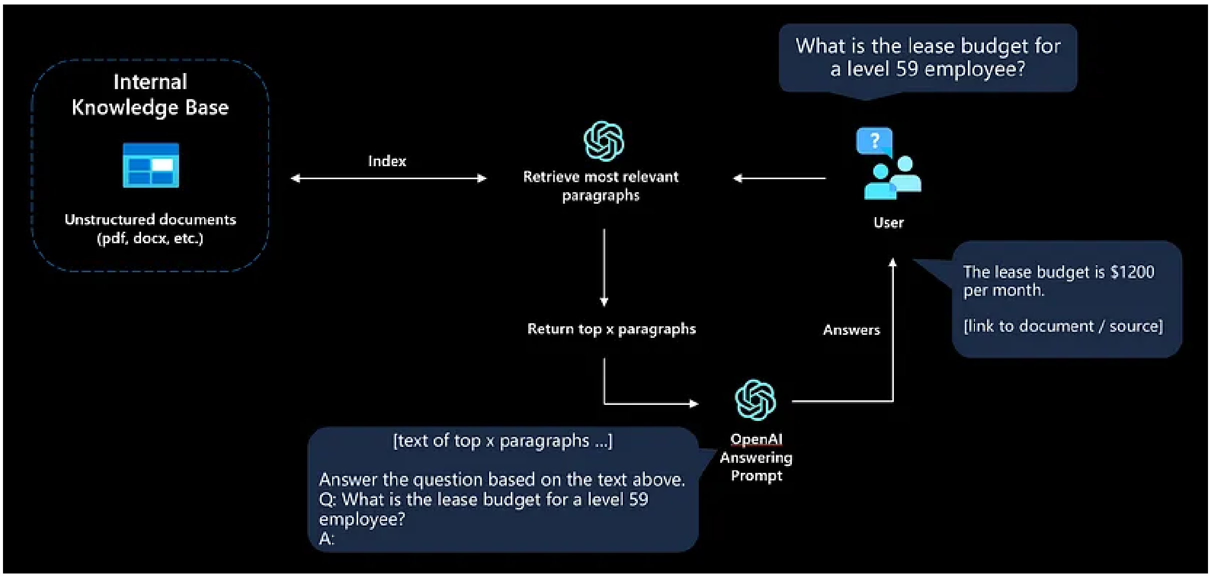

What is the lease budget for a level 59 employee?
Internal Knowledge Base
Unstructured documents (pdf, docx, etc.)
Index
Retrieve most relevant paragraphs
User
The lease budget is $1200 per month.
[link to document / source]
Return top x paragraphs
Answers
OpenAI Answering Prompt
[text of top x paragraphs ...]
Answer the question based on the text above.
Q: What is the lease budget for a level 59 employee?
A:

Figure C.1: ChatGPT Plugin

[7] 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.

Reference to current implementation on Github: https://github.com/OwnYourData/dc-chatbot/blob/main/config/textblocks/OAI_system_default_en.txt

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 hearing and speech impaired and is used to short precise conversations. Only ask one question at a time.
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 personnel:
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) once emergency personnel is dispatched ask if personnel 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 are they 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, end the call stating what type of emergency will be sent, ambulance, police or firemen. If the caller says “Stay on the line” do not end the call but otherwise end the call with the following text “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 conversation with “The system has ended the emergency call. If you have any further questions, please call again.”.

Table C.1: System Instructions

Funded by the European Union