NGI TRUST CHAIN

D3. 'IMPLEMENTATION, DEPLOYMENT IN AN APPROPRIATE TRUSTCHAIN PLATFORM, TESTING, DEMONSTRATION AND VALIDATION ROADMAP IN A REAL-LIFE APPLICATION (I.E., BANKING, EDUCATION, HEALTHCARE, UTILITIES, DEFENCE OR CROSS-BORDER TRAVEL).'

IM4DEC

26/01/2024 (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.

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

D3. 'Implementation, deployment in an appropriate trustchain platform, testing, demonstration and validation roadmap in a real-life application (i.e., banking, education, healthcare, utilities, defence or cross-border travel).'

>IM4DEC<

Due date	26/01/2024
Submission date	26/01/2024
Team	OwnYourData, DEC112
Version	1.0
Authors	Christoph Fabianek, Jan Lindquist, Gabriel Unterholzer

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 Despite this, there are still about 1 million deaf and hard of hearing persons in Europe who currently rely on outdated technology (e.g., fax) and help from others to make an emergency call.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

Funded by the European Union

List of Tables

Funded by the European Union

ABBREVIATIONS

ARF	Architecture and Reference Framework (for EUDI wallets)
API	Application Programming Interface
BCF	Border Control Function
CAD	Computer Aided Dispatch
CHE	Call Handling Equipment
CPE	Call Processing 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

Funded by the European Union

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

Funded by the European Union

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.

Funded by the European Union

2 Solution Description

Since 2019 DEC112 has been operating NG112 core services, including the text-based DEC112 emergency communication in Austria and constantly and actively develops these services. Big parts of software components are available as Open-Source on Github[1].

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

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

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

The described routing process (involving both the ESRP and ECRF) is essential to direct emergency calls to the most appropriate control centre based on the user's need and location. The app (using `ng112-js` as described in section 3.2.2) itself is not involved in the routing decision and therefore, does not need any information about any (potentially complex) structural properties of available control centres.

DEC112 PSAP is used to establish connections from SIP to other technologies. Given the fact that most established vendors of emergency call processing equipment (CPE) are mainly focusing on traditional phone calls rather than text-based emergency communication, a technology-bridge is necessary to enhance those systems with emergency chat capabilities. DEC112 PSAP provides services for processing SIP-based emergency calls. The most prominent of these, the chat service, is used to route emergency messages between the person making the emergency call and the control centre (mainly via the web-based DEC112 Viewer, accompanied by a trigger-based integration into existing call processing systems). Other services provide, for example, automated information for emergency callers (like chatbots as described in section 3.2.2). An overview of the DEC112 infrastructure components is depicted in Figure 2.1.

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

Funded by the European Union

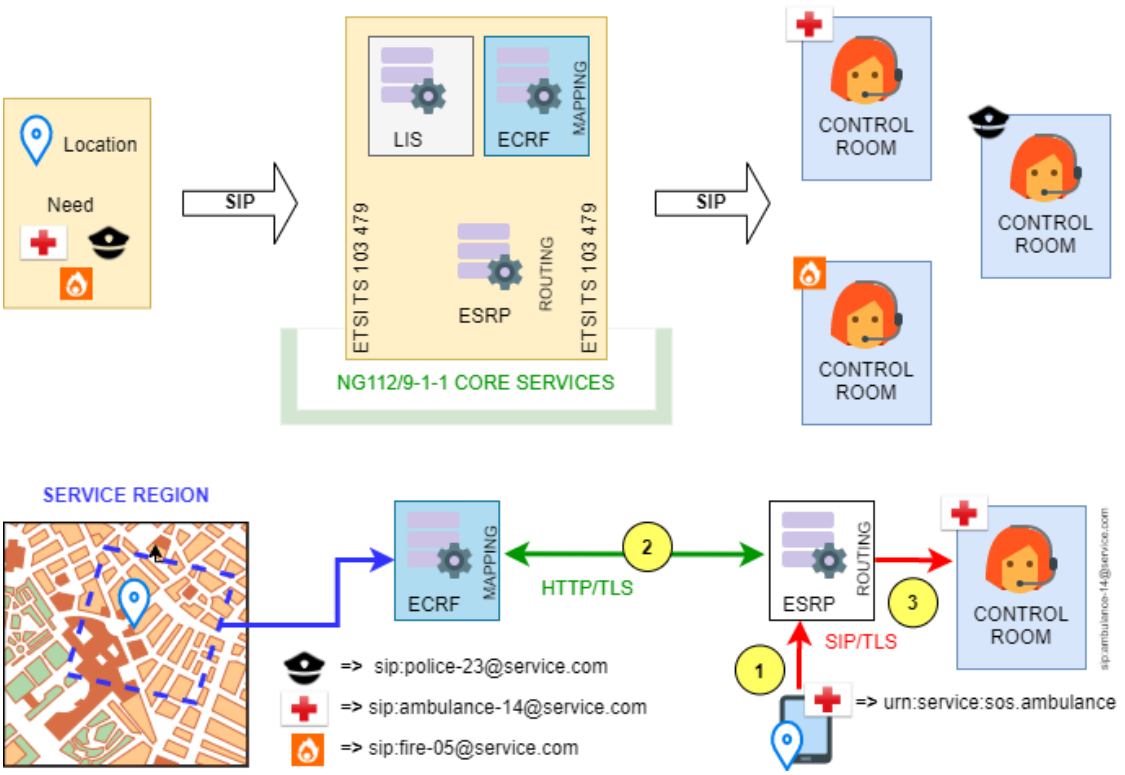

Figure 2.1: DEC112 Infrastructure Components

The following sections provide a list of use cases developed in the course of the NGI TRUSTCHAIN funded IM4DEC project.

2.1 DEC112 Onboarding with ID Austria

To provide a verified identity in the DEC112 app (available on Android and iOS), the existing DEC112 registration element (Registration API) was 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 compliant identity provider).

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

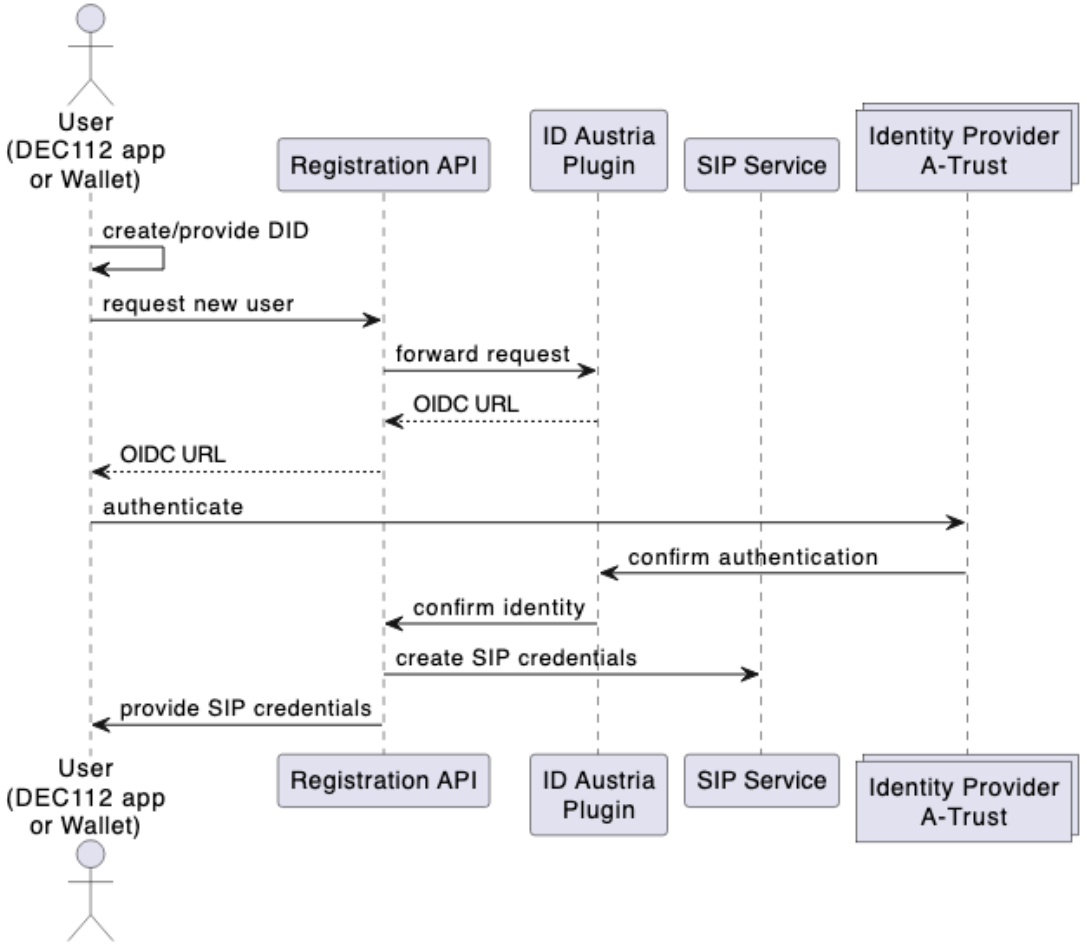

Figure 2.2: Onboarding with ID Austria

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, such that an aggressor does not remove the app from the victims smartphone.

In this use case we use a government issued identity (ID Austria) with OwnYourData

acting 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[2] 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.

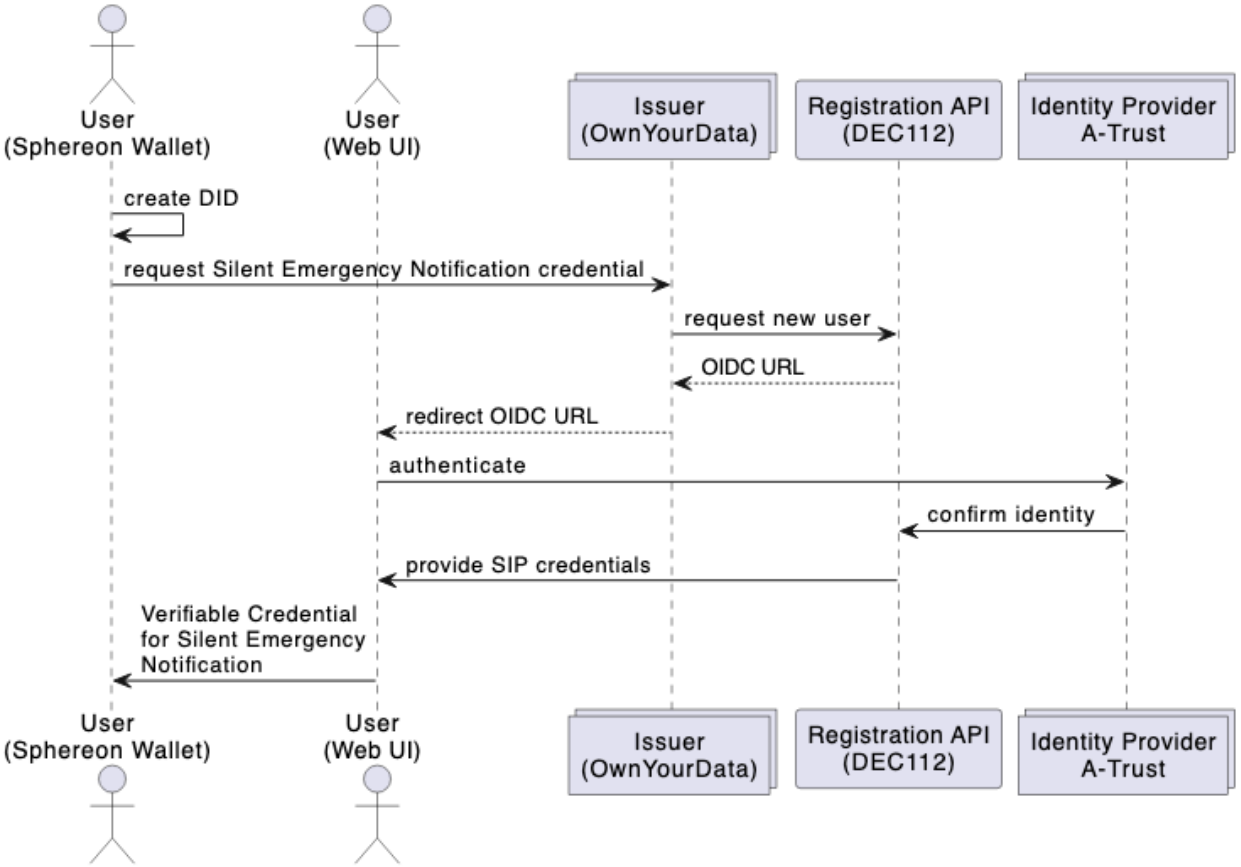

Figure 2.3: Silent Emergency Notification from Sphereon Wallet

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

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 text-based emergency communication. 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 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.

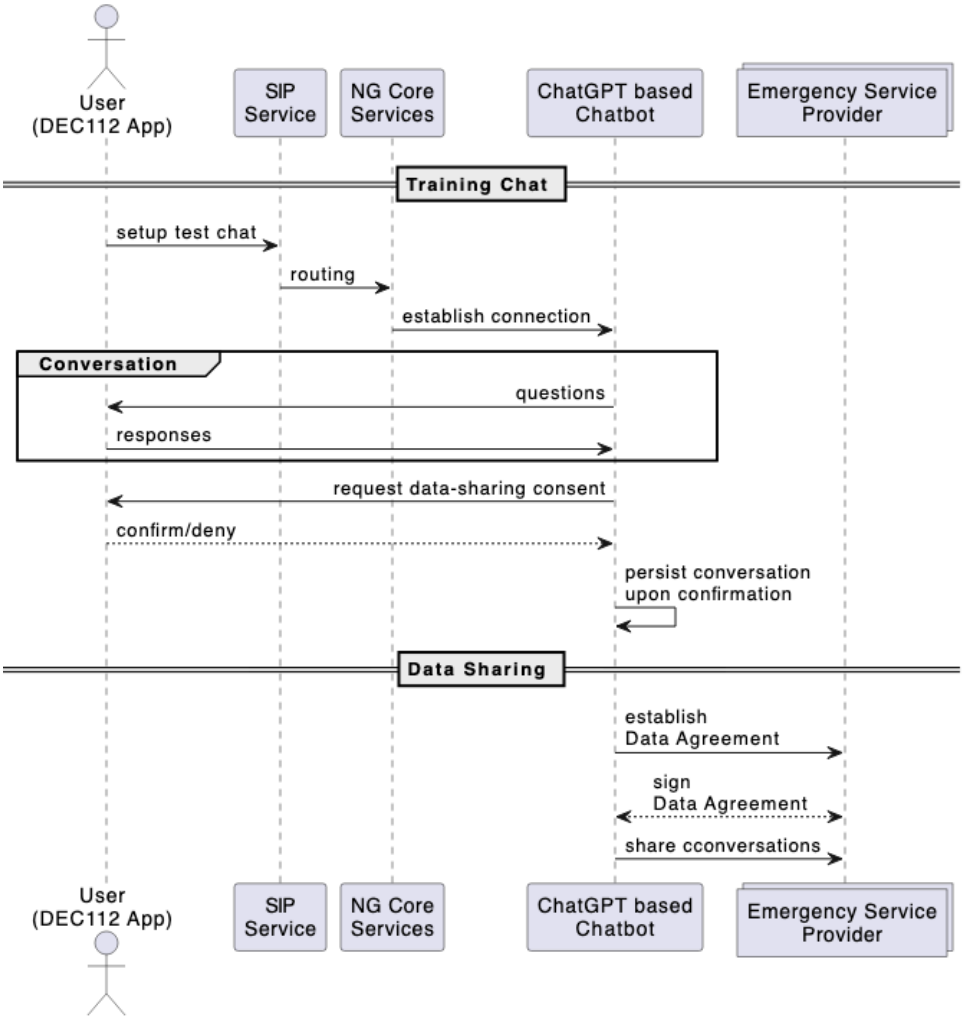

Figure 2.4: ChatGPT based Chatbot and Data Sharing

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 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 2.5 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[3]. To validate those properties the OwnYourData DID Lint service[4] 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.

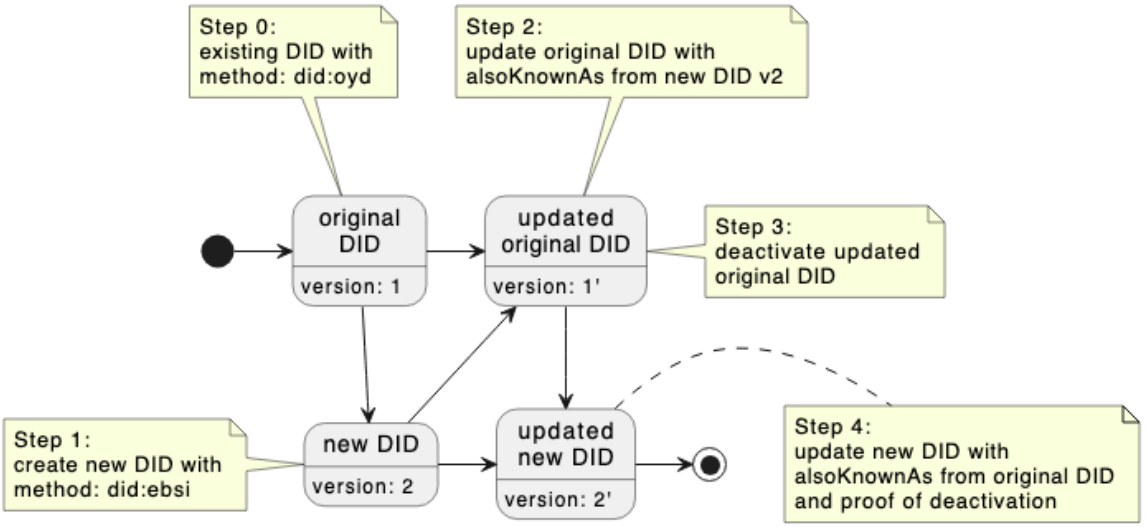

Figure 2.5: DID Rotation

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

3 Detailed API Specification (Final)

3.1 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.

3.1.1 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
	(json) options		
update	(str) did - current DID	(str) did - new DID	update DID Document for a given DID
	(json) payload		
	(json) options		

Function	Arguments	Return value	Description
deactivate	(str) did	(str) did	deactivate DID through publishing revocation information
	(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) message, (str) signature	(bool) signature verification	verify signature for a given DID using the public key provided in options
	(json) options		

Funded by the European Union

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 3.1: did:oyd NPM Package

3.1.2 ng112-js

The ng112-js (generally referred to as "DEC112 SDK" in this document) component provides 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		

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.update Location	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.create Conversation	(str) service example: 'sip:144@dec112.at'	conversation object	start a new emergency conversation

Funded by the European Union

Function	Arguments	Return value	Description
conversation.addMessageListener	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 3.2: DEC112-SDK NPM Package

3.2 API Specification for REST Services

In this section, 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.

3.2.1 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 3.3: Registration APIs

3.2.2 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 3.4: Chatbot APIs

3.2.3 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

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 3.5: DID Lint Service APIs

4 Software Code of the Solution

This chapter is about describing the implementation in detail. While D1 and D2 provided a logical view of the components and how they interact, this section is about the actual implementation of the solution. It explains how the solution works and how to use it, so that results can be reproduced and assessed.

4.1 Solution Architecture

The architecture overview in Figure 4.1 depicts the main components of the IM4DEC solution. It highlights the developed components 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 other end of the conversation. The DEC112 RegAPI (Registration API) was extended by allowing a government issued ID in the onboarding process, an SSI Mobile Wallet was equipped with means to trigger a Silent Emergency Notification based on a government ID and SIP credentials , the chatbot simulates emergency personnel responses in a test environment and additionally covers functionality for data exchange, 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.

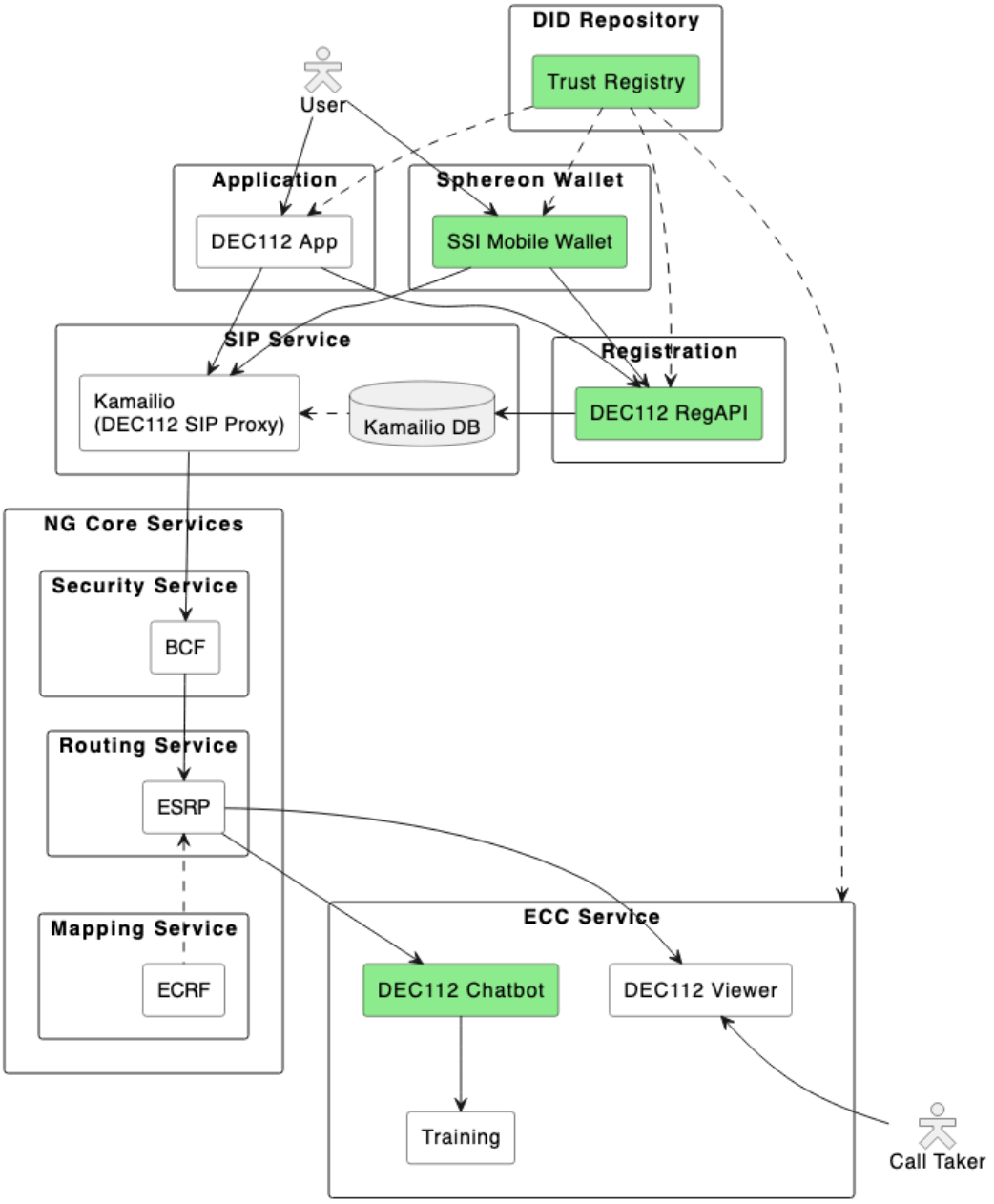

Figure 4.1: Architecture Overview (green components are new developments)

4.2 Program Modules Overview

This section presents a comprehensive examination of the various modules that constitute the core of our project. This overview is designed to provide insights into the functionality, interdependencies, and roles of the developed modules.

Name	Description	Language	Kind
OYDID Tools	a number of utilities to use and interact with OYDID Repository: command line tool, a Ruby Gem, and a JavaScript npm package, repository, UniResolver and UniRegistrar plugin	Ruby / Typescript	Script, Service, Package
DID Lint	validating DID Documents and associated metadata for conformance to the DID v1.0 Core Spec based on the SOyA data modelling language using SHACL	Ruby	Service
Sphereon Wallet	a privacy-preserving wallet based on open standards and open-source that gives you full and sole control over your own information: it enables you to manage your own data	Typescript	App
Veramo core	a JavaScript Framework for Verifiable Data that was designed to be flexible and modular which makes it an easy fit for a lot of complex workflows	Typescript	Library
Registration API	Deaf Emergency Call 112 API services that includes the backend API services with SMS, ID Austria, and SIP plugins	Ruby, SQL	Service
Onboarding Service	a web service that uses information from the Registration API (provides an ID Austria identity and creates SIP credentials), creates a Verifiable Credential, and transfers it to an SSI Wallet	Ruby	Service

Name	Description	Language	Kind
DEC112 SDK	library for integrating browser and node environments with existing NG112 or DEC112 infrastructure (covers standards ETSI TS 103 479 and ETSI TS 103 698, as well as DEC112 specific additions for text based emergency messages/calls)	Typescript	Library
ChatBot	registers as endpoint for training chats (initiated in the DEC112 app) and also stores conversations (upon consent from the user) to share it later using Data Agreements with an emergency response provider	Ruby	Service
Data Intermediary	basic functionality of a data intermediary as defined in the Data Governance Act	Ruby	Service

Table 4.1: Program Modules

4.3 Project Repositories

This section outlines the various code repositories and data storage locations used throughout the project.It provides clarity on the projects access protocols, and version control systems in place, ensuring a transparent and efficient management of project resources.

Repository Name	Link	Kind	Restrictions
oydid	https://github.com/OwnYourData/oydid https://www.npmjs.com/package/oydid	public	none
didlint	https://github.com/OwnYourData/didlint	public	none

Repository Name	Link	Kind	Restrictions
soya	https://github.com/OwnYourData/soya https://www.npmjs.com/package/soya-cli	public	none
ssi-mobile-wallet	https://github.com/OwnYourData/ssi-mobile-wallet	public	none
veramo	https://github.com/OwnYourData/veramo	public	none
RegAPI	https://github.com/dec112/dc-reg-api	public	none
RegAPI - SMS Plugin	https://github.com/dec112/dc-reg-sms	public	none
RegAPI - ID Austria Plugin	https://github.com/dec112/dc-reg-ida	public	none
RegAPI - SIP Plugin	https://github.com/dec112/dc-reg-sip	public	none
DEC Onboarding	https://github.com/OwnYourData/dc-dec_onboarding	public	none
DEC112 SDK	https://github.com/dec112/ng112-js https://www.npmjs.com/package/ng112-js	public	none
Chatbot	https://github.com/OwnYourData/dc-chatbot	public	none
Data Intermediary	https://github.com/OwnYourData/dc-intermediary	public	none

Table 4.2: Project Repositories

5 Implementation and Deployment in a Suitable TrustChain Platform

This chapter outlines the strategies and processes for implementing and deploying the project in a suitable environment. It details how the implementation aligns with the specific objectives of TrustChain and addresses the needs of the chosen sector.

5.1 Requirements for Deploying and Operating the Solution

The approach of OwnYourData and DEC112 in developing, testing, deploying and running software solutions is based on the following principles:

- Research available solutions for the given goal and choose available standards-based libraries and components to avoid reinventing the wheel
- Preferred development languages are currently Ruby, TypeScript, Python and R while we also include program languages are used in case specialised libraries need to be integrated (e.g., we use JAVA to integrate the Hermit OWL Reasoner)
- Our usual approach for validating implemented functionality and avoiding regression is to provide end-to-end test using the pytest framework
- We usually make our software not only available as Open Source under the MIT or GPL License on Github (using the https://github.com/OwnYourData and https://github.com/dec112 organisations) but also package it as ready to use Docker images on Dockerhub (https://hub.docker.com/u/oydeu)

Finally, we deploy our solutions on a managed Kubernetes cluster on sub-domains of dec112.eu (e.g., the Registration API component is available on https://regapi.staging.dec112.eu)

Hardware requirements for running those Docker images are quite modest but can vary from case to case. Semantic Containers (image oydeu/dc-base) and derived images run fine with only 256MB RAM and are provided for the linux/amd64 and usually also for the linux/arm64 CPU architecture. Currently, our servers are using the AMD EPYC 7702 server processors with 4 cores and 3,35 GHz / core. Nevertheless, it is possible to run our Docker images also on much more lightweight environments, e.g., we have deployments on Raspberry Pi 4 Model B with a 1.5 GHz 64-bit quad core ARM Cortex-A72.

5.2 How to Deploy

As already described above is the software developed for IM4DEC available as Docker images and can be deployed either locally or on servers with a simple docker run or can be pushed to Kubernetes to run as a pod instance. The list below describes configuration options / environment variables to be used for each of the images, gives an example command to start the image locally, and provides a link to example configurations for Kubernetes on Github.

Registration API

Docker image: https://hub.docker.com/r/oydeu/dc-regapi

Prerequisites:

- PostgreSQL instance: https://www.postgresql.org/
- Redis instance: https://redis.io/

Environment variables:

- REDIS_HOST – IP address of redis host
- DEFAULT_VC_OAUTH_APP – name of OAuth2 application to be used when authenticating with a DID as identity
- AUTH – TRUE or FALSE (default) if container should require authentication

Command to start image:

```
docker run -d --name regapi -p 3600:3000 \
      -e REDIS_HOST=192.168.178.60 \
      -e DEFAULT_VC_OAUTH_APP=oydid-vc \
      -e AUTH=TRUE \
      oydeu/dc-regapi
```

Kubernetes configuration:
https://github.com/dec112/dc-reg-api/blob/main/kubernetes/regapi-deploy.yaml

ID Austria Plugin

Docker image: https://hub.docker.com/r/oydeu/dc-decida

Prerequisites:

- Redis instance: https://redis.io/

Environment variables:

- REDIS_HOST – IP address of redis host
- IDA_CLIENT_SECRET – OIDC Secret provided when registering as E-ID service provider in Austria
- ISSUER_PRIVATE_KEY – private key for issuer DID to sign messages

Command to start image:

```
docker run -d --name decida -p 3620:3000 \
      -e REDIS_HOST=192.168.178.60 \
      -e IDA_CLIENT_SECRET=ida-secret \
      -e ISSUER_PRIVATE_KEY=issuer-password \
      oydeu/dc-decida
```

Kubernetes configuration:
https://github.com/dec112/dc-reg-ida/blob/main/kubernetes/ida-deploy.yaml

SIP Plugin

Docker image: https://hub.docker.com/r/oydeu/dc-decsip

Prerequisites:

- PostgreSQL instance: https://www.postgresql.org/
- Redis instance: https://redis.io/

Environment variables:

- REDIS_HOST – IP address of redis host
- SIP_SECRET – secret to encrypt SIP credentials

Command to start image:

```
docker run -d --name decsip \
      -e REDIS_HOST=192.168.178.60 \
      -e SIP_SECRET=secret \
      oydeu/dc-decsip
```

Kubernetes configuration:
https://github.com/dec112/dc-reg-sip/blob/main/kubernetes/sip-deploy.yaml

DEC112 Onboarding

Docker image: https://hub.docker.com/r/oydeu/dc-dec_onboarding

Prerequisites:

- PostgreSQL instance: https://www.postgresql.org/
- OAuth2 application configured on Registration API

Environment variables:

- ISSUER_PWD – private key for issuer DID to sign messages
- REGAPI_APPKEY – client-id from OAuth2 application to authenticate against Registration API
- REGAPI_APPSECRET – client-secret from OAuth2 application to authenticate

against Registration API

Command to start image:

```
docker run -d --name onboarding -p 3700:3000 \
     -e ISSUER_PWD=issuer-secret \
     -e REGAPI_APPKEY=client-id \
     -e REGAPI_APPSECRET=cliet-secret \
     oydeu/dc-dec_onboarding
```

Kubernetes configuration:
https://github.com/OwnYourData/dc-dec_onboarding/blob/main/kubernetes/onboarding-deploy.yaml

ChatBot Service

Docker image: https://hub.docker.com/r/oydeu/dc-chatbot

Prerequisites:

- PostgreSQL instance: https://www.postgresql.org/
- ChatGPT subscription: https://platform.openai.com/docs/introduction

Environment variables:

- OAI_ACCESS_TOKEN – access token from OpenAI
- WS_ENDPOINT – websocket endpoint to connect to ESInet

Command to start image:

```
docker run -d --name chatbot -p 3500:3000 \
     -e OAI_ACCESS_TOKEN="sk-..." \
     -e WS_ENDPOINT="wss://host:port/path?api_key=key" \
     oydeu/dc-dec_onboarding
```

Kubernetes configuration:
https://github.com/OwnYourData/dc-chatbot/tree/main/kubernetes

DID Lint Service

Docker image: https://hub.docker.com/r/oydeu/didlint

Prerequisites:

- PostgreSQL instance: https://www.postgresql.org/
- UniResolver instance: https://dev.uniresolver.io/

Environment variables:

- OAI_ACCESS_TOKEN – access token from OpenAI
- SOYA_DID_DRI – identifier for DID data model specified with SOyA

Command to start image:

```
docker run -d --name didlint -p 3200:3000 \
    -e SOYA_DID_DRI=zQmc76XfAkKxjFhHUANsq2yLxvt1FNkwHULChENskd9PJ9T \
    oydeu/didlint
```

Kubernetes configuration:
https://github.com/OwnYourData/didlint/tree/main/kubernetes

5.3 How to Run

This section provides a clear, step-by-step guideline to our developed algorithms, and components. It is intended for those who wish to reproduce our research, test the robustness of our findings, or further extend the scope of our project. With a blend of brevity and comprehensibility, we aim to make our research as accessible and replicable as possible.

Understanding the precise implementation of a research project is crucial, as it allows for the validation of results and the extension of the research by other scientists and researchers. Therefore, we have created a number of tutorials that describe the implemented functions:

Using the Registration API with the SMS flow

URL: https://hackmd.io/3lWxmrpAQjG76owztu13MA?view

Description: a step-by-step introduction how to perform the registration process using SMS to prove identity with a registered Austrian phone number

Using the Registration API with the ID Austria flow

URL: https://hackmd.io/7BhKMJIfRGC8sfGXaPgYCg?view

Description: a step-by-step introduction how to perform the registration process using ID Austria to prove identity using an Austrian issued government ID

Using the Registration API with the Sphereon Wallet

URL: https://hackmd.io/m1M_TCMuSU6Xj5AfMw4Lbg?view

Description: a step-by-step introduction how to perform the registration process using ID Austria with the Sphereon Wallet

Interacting with the ChatGPT based Chatbot and sharing conversations

URL: https://hackmd.io/Z8iuJGeYRLynxWPS7JpLwg?view

Description: walkthrough of the process to collect data with the DEC112 chatbot including giving consent, and subsequently sharing the conversation data through a Data Intermediary using Data Agreements

Identity Management with did:oyd

URL: https://github.com/OwnYourData/dc-intermediary/blob/main/tutorial/4_Identities/README.md

Description: creating and managing identities including rotation as well as attestation through Verifiable Credentials and Presentations

6 Testing and Demonstration Strategy

This chapter describes the testing plan to ensure the solution's functionality and efficacy. It includes strategies for demonstrating the solution in real-life scenarios and how it meets the practical needs of the intended sector. A clear roadmap of the pilot studies with real users and a detailed plan for validating the solution in a real-world application environment is presented that includes metrics and criteria for evaluating the success and effectiveness of the solution.

6.1 Requirements for Testing and Demonstrating the Solution

As already mentioned in the previous chapter are tests automated with pytest (https://docs.pytest.org/). Pytest provides a robust and flexible framework for writing and executing tests, allowing developers to easily define test cases and assertions. Its concise syntax and extensive plugin ecosystem enable the creation of comprehensive test suites with minimal effort. Additionally, pytest offers powerful features like test parametrization, fixtures, and test discovery, facilitating test reuse and reducing code duplication. The ability to run tests in parallel and generate detailed test reports further streamlines the testing process. By automating tests, developers can achieve faster feedback cycles, ensuring rapid detection and resolution of bugs, which ultimately leads to higher software quality and improved overall productivity.

The following requirements for available software and minimum version to run tests apply:

- python: v3.10
  - pytest: v7.3.1
  - pluggy: 1.0.0
- node: v16
- soya: v0.16.31
  make sure to install also the SOyA CLI with the following command:
  `npm install -g soya-cli@latest`

- oydid: v0.5.6
  make sure to install also the OYDID CLI with the following commands:
  (assuming a Debian-based distribution and BASH as shell)

```
apt-get update
apt-get -y install ruby-dev libsodium-dev
gem install oydid securerandom httparty ed25519 multibases \
    multihashes optparse rbnacl dag uri
mkdir -p ~/bin
```

```
wget https://raw.githubusercontent.com/OwnYourData/oydid/main/cli/oydid.rb -O
~/bin/oydid
chmod +x ~/bin/oydid
export PATH="$PATH:$HOME/bin"
```

The general structure of tests in the IM4DEC project is to group test cases in a `test_{function}.py` file and have associated directories with input data/execution and output data respectively. Here an example:

To test the "Chatbot" functionality there is:

- pytest file: `test_chatbot.py`
- input data and commands to run: `01_input` directory
- expected output data: `01_output` directory

When `test_services.py` is executed, it processes all files in the `03_input` directory by using as input data the content of `*.doc` files, running the command in `*.cmd` files and comparing the output to `*.doc` files in the `03_output` directory.

This directory structure allows to easily add more test cases without changing any of the test code in the *.py files. In case of errors it is also simple to reproduce individual steps by just running failed test cases on the command line.

Finally, to run tests it is first necessary to check out the necessary files from Github and go to the `pytest` directory (in the root of the Github repo). Additionally, we make use of environment variables for running tests either locally or in the production environment. To set these environment variables it is therefore mandatory to run a command to specify host and required credentials. In the various tests below this is marked as "prerequisite script".

6.2 How to Test

This section lists the tests performed for the logical components of the overall IM4DEC solution.

6.2.1 Tests for Registration API

Github Repository: https://github.com/dec112/dc-reg-api

Prerequisite Script: (run in the same directory where `pytest` is executed)

```
export DID="did:oyd:zQme9kivg2biykkgkqEfAKcDH4Fi1UWjZQAPyooYQy8Xhfo"
echo -n 'z1S5g1m6pB1tqP8yF1jkzXCoj2Zub4g57ErpXxSm8SWvRUJV' \
  > zQme9kivg2_private_key.enc
```

Table with functions for Registration API tests:

Function	pytest Script	# Tests
Coverage		
Configuration access	test_config.py	4
retrieve JSON configuration for root & user config, get OAuth2 token		
SMS flow	test_sms.py	3
trigger SMS registration flow		
ID Austria flow	test_ida.py	3
trigger ID Austria registration flow		

Table 6.1: Tests for Registration API

6.2.2 Tests for Chatbot

Github Repository: https://github.com/OwnYourData/dc-chatbot

Table with functions for Chatbot tests:

Function	pytest Script	# Tests
Coverage		
Conversation	test_general.py and test_ng112tester.py	4
setup full conversation incl. consent and statistical data collection		

Table 6.2: Tests for Chatbot

6.2.3 Tests for DID Rotation

Github Repository: https://github.com/OwnYourData/oydid

Table with functions for DID Rotation tests:

Function	pytest Script	# Tests
Coverage		
DID Rotation	test_rotation.py (in cli/pytest)	4
test resolving did:oyd rotated to did:ebsi, --followAlsoKnownAs flag, and handling in Uniresolver		

Table 6.3: Tests for DID Rotation

6.2.4 Tests for DID Linter

Github Repository: https://github.com/OwnYourData/didlint

Table with functions for DID Linter tests:

Function	pytest Script	# Tests
Coverage		
Command line resolver	test_did.py	2
resolve DIDs on the command line with oydid command		
DID Documents	test_ddo.py	12
validating aspects of DID Documents		
Context validation	test_context.py	9
tests for interpreting the JSON-LD context		

Table 6.4: Tests for DID Linter

6.3 Demonstration Strategy

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 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)
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

For the purpose of this research project our goals of user engagement for each component 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 conversations from at least 50 users
- DID Enhancements: 15 users

6.4 Evaluation Methodology

This section evaluates the project against KPIs defined in the TRUSTCHAIN Deliverable 3.7 "TrustChain Support to third parties - Guide for implementation v1.0" in section 2.5.4

KPIs towards sustainable business

#	KPI	Project Contribution
3.1	Market penetration potential? #of pilot users, # of potential customers, # of competitors, # of partners, etc.	Pilot users addressed in chapter 6.3 Demonstration Strategy and other KPIs in chapter 7: Business Model and Exploitation Plan
3.2	Business model defined? Details should be mentioned, such as # of Business Use Cases (BUCs), # of BM canvases, # of BUCs analysed	addressed in chapter 7: Business Model and Exploitation Plan
3.3	Profitability, e.g., ROI, NPV, payback period, etc.	only partially applicable since DEC112 and OwnYourData are non-profit organisations; relevant aspects addressed in chapter 7: Business Model and Exploitation Plan
3.4	Crypto strategy? Token type? Crypto distribution?	not applicable for IM4DEC

Table 6.5: KPIs towards sustainable business

KPIs related to the pilot studies

#	KPI	Project Contribution
5.1	User Experience (UEQ questionnaire)	planned to be addressed in D4
5.2	# of pilot users	estimates provided in D2 chapter 7 Early User Engagement Plan; final numbers will be listed in D4
5.3	User Engagement (# of transactions per user, freq. of use, etc.)	estimates provided in D2 chapter 7 Early User Engagement Plan; final numbers will be listed in D4
5.4	# of interested users in future business collaboration	planned to be addressed in D4; active collaboration with two other TRUSTCHAIN OC1 projects: DanubeTech and Sphereon
5.5	# of paying users	only partially applicable because this is a free service paid by the government; existing paid contract in Austria with Ministry of the Interior
5.6	List of use cases in the pilot	use cases described in chapter 2 Solution Description
5.7	User story: List of actions accomplished by users to complete the different use cases.	results from interviews and user tests will be provided in D4

Table 6.6: KPIs related to the pilot studies

Interoperability and standardisation

#	KPI	Project Contribution
6.1	Did you propose or could/will propose standards/drafts?	DEC112 is built on existing standards (specifically ETSI TS 103 479 and ETSI TS 103 698); in the course of the project we did not propose new standards
6.2	Describe international events on standardisation activities participated/contributed	invitation to present project results at the EENA 2024 conference in Valencia - the leading international conference hosted by European Emergency Number Association
6.3	What digital identity standards do you focus on?	W3C DID Core Spec v1.0
6.4	What standards related to credentials do you focus on?	W3C Verifiable Credentials Data Model v2.0
6.5	Which Blockchain network(s) and Smart Contract language(s), did you use?	the project aims to provide non-blockchain based solutions due to the performed DPIA for sensitive personal data handled in the course of emergency communication; for DID Rotation EBSI (European Blockchain Service Infrastructure) was used
6.6	Interoperability standards employed (syntactic interoperability)? Ontologies employed (semantic interoperability)?	Semantic Overlay Architecture (SOyA) used for syntactic interoperability; Ontologies employed: - SOyA Ontology (OWL) - DID Ontology (OWL) - SOyA DID Ontology (OWL, SHACL)

#	KPI	Project Contribution
6.7	What interoperable data formats or communication protocols were used if any in the implementation?	interoperable data formats: - Data Agreements (ISO 27560) - PIDF-LO (RFC 5491) - LoST (RFC 5222) communication protocols: - ETSI TS 103 479 - ETSI TS 103 698 - SIP (RFC 3261)
6.8	Importance of interoperability in your solution? E.g., # of cross-chain transactions?	interoperability for DID methods was demonstrated through DID Rotation; interoperability for emergency communication through adhering to ETSI standards → both forms of interoperability are crucial for wider adoption

Table 6.7: Interoperability and standardisation

Legal and ethical compliance

#	KPI	Project Contribution
7.1	All users are informed about the processing of their personal data. An information notice has been put in place.	yes, information is available online (https://www.dec112.at/en/privacy-idaustria/)
7.2	Users' consent is asked and stored whenever consent is the relevant legal basis to be used.	yes, users give consent during the registration process and specifically for data sharing in chatbot conversations
7.3	The purposes for processing personal data have been well-defined, specified and are communicated to the users and no personal data is processed beyond what is needed for these purposes.	yes, also a DPIA was performed (documented in Appendix B)

#	KPI	Project Contribution
7.4	Retention periods for users' personal data are well-defined and are communicated to the users.	yes, as part of the privacy statement on the website (https://www.dec112.at/en/privacy-idaustria/) retention period is 3 month
7.5	Personal data are kept accurate, complete and up to date.	yes, this is also in the self-interest of the user when actually performing emergency communication
7.6	The necessary technical measures are taken to protect the personal data processed. Personal data are encrypted in transfer and at rest, where appropriate.	yes, and documented in a Privacy Report (Appendix A) and a detailed Privacy Analysis for ChatGPT (Appendix C)
7.7	All processors engaged provide adequate assurances and guarantees as required and the appropriate data processing agreements have been completed and signed.	yes, evaluated in the Privacy Report (Appendix A)
7.8	The processes are put in place to ensure compliance with data subject rights (e.g., right of access, correction, erasure, limitation, opposition, etc.).	yes, documented in a Privacy Report (Appendix A)
7.9	Personal data are only transferred to third countries to the extent that adequate protection can be foreseen.	personal data is not transferred to third countries in the current setting; with data agreements dedicated consent for sharing data with third countries is possible
7.10	A record of processing activities is drawn up for the project and kept up to date.	yes, the processing activities are described in the DEC112 DPIA Report (Appendix B); the system keeps a timestamped log of all processing activities

#	KPI	Project Contribution
7.11	The necessary approvals and authorizations from the competent ethics and/or governmental bodies for the processing of personal data are sought and obtained.	yes, this is covered in the established contract with the Ministry of Interior Austria

Table 6.8: Legal and ethical compliance

KPIs related to the implementation

#	KPI	Project Contribution
10.1	Code simplicity (analyser used and results)	current standards in software development were adhered to but due to the complexity of components in different languages and heterogeneity in the overall solution dedicated code analysis for the overall solution was not performed (the software operates in a safety critical environment since 2019 and is monitored by the Austrian government)
10.2	Testability Coverage (method/tool used for testing and results)	for Ruby SimpleCov is used in the oydid gem, test coverage is 73%

Table 6.9: KPIs related to the implementation

7 Business Model and Exploitation Plan (Continuation)

Expanding on the preliminary business model and exploitation plan presented in D2, this section provides a more detailed and comprehensive analysis of the business model, including the project's value in the decentralised digital identity and blockchain domain, and its relevance to TrustChain.

7.1 Business Model

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 https://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.

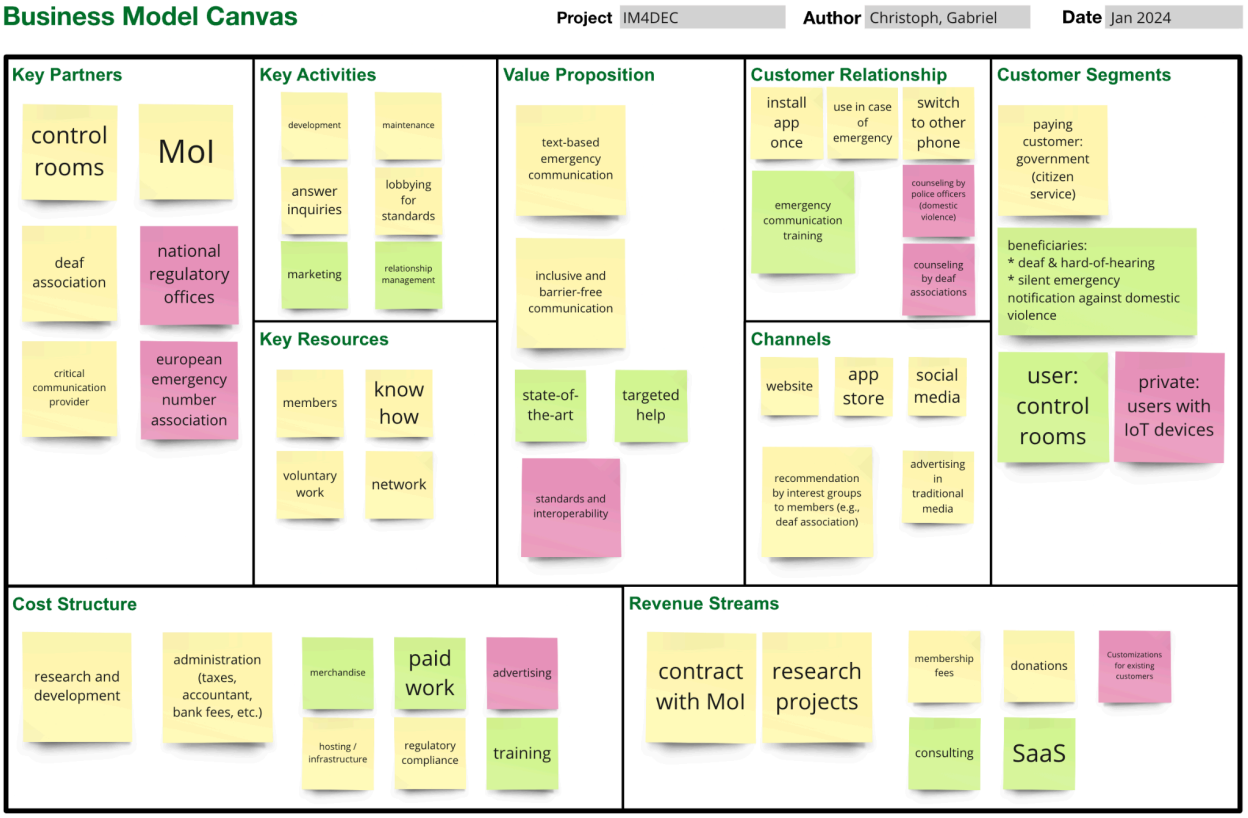

Figure 7.1: Business Model Canvas

The Business Model Canvas depicted in Figure 7.1 is the result of multiple team sessions to provide a comprehensive few of the business aspects of DEC112. Specifically we discussed cost and revenue streams and the remainder of the section provides a more detailed elaboration.

Below are the most relevant 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

Focusing on potential customers, our service targets a niche yet vital segment: around 1.8 million individuals who are deaf or are hearing impaired in Austria. However, the scope of our service transcends this group, extending to all Austrians who might find themselves in situations where a silent or text-based emergency call is necessary. This broadens our potential customer base significantly, encompassing the entire Austrian population.

When considering competitors, the landscape in Austria appears moderately competitive. There are a few organisations offering similar services (app-based emergency calling), but their number is limited to single digits. Furthermore, all competitors are just collecting additional data to an emergency, while still calling the emergency number via traditional phone call, whereas DEC112, in contrast, uses a multimedia IP infrastructure to forward emergency calls. This also allows for a direct integration of services into the respective emergency response centres, where DEC112 has already 6 control rooms connected, serving all 9 federal countries and covers fire, ambulance, police and mountain rescue services.

Regarding the role of partners we already have or anticipate forging alliances with a variety of entities, including emergency response centres, associations like the Deaf Association of Austria, and key organisations such as the Federal Ministry of the

Interior (BMI) and the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR). These partnerships will not only extend our reach but also enhance our credibility and operational efficiency. Combined with the fact of being a non-profit association, driven by innovation and not profit, DEC112 has already grown to an established entity in the Austrian landscape of emergency calling.

7.2 Exploitation Plan

This section outlines the exploitation plan for our research project, which is centred around further developing the innovative DEC112 text-based emergency communication system. The primary objective is to ensure that the outcomes of this research are effectively utilised to benefit society, particularly in enhancing the efficiency and accessibility of emergency response services. The exploitation plan is designed to maximise the impact of our findings and technological developments, ensuring their practical application and sustainability.

An initial market analysis was conducted and we identified the key stakeholders and potential beneficiaries, including emergency response units, healthcare providers, governmental agencies, and the general public. Special attention was given to regions with limited access to traditional emergency services (emergencies in mountains or other remote areas) and the use case of domestic violence where this technology could be particularly beneficial.

To ensure the effective use of our system, a concrete measure will be to develop comprehensive training programs for emergency responders and relevant stakeholders in the future. These programs will focus on the technical aspects of the system and data exchange between users and control rooms to improve emergency communication. Building this capacity is crucial for the successful adoption and further improvement of the system.

Increasing public awareness is also vital for the success of this project. We plan to conduct awareness campaigns to educate the community about the availability and benefits of the text-based emergency communication system. This will include the newly created ChatGPT-based chatbot and the data we collect through these campaigns in turn can be used to strengthen our relationship with control rooms through providing a possibility to exchange conversation data. Engaging with the public through workshops, social media, european conferences, and public demonstrations will also provide valuable feedback for continuous improvement of the system.

The long-term sustainability of the project will be ensured through a combination of governmental support, consulting in the area of emergency communication, and ongoing funding from stakeholders (including research grants). As the legal and

governance requirements in this domain mature and become mandatory in the EU, we will explore opportunities for scaling up and expanding the system's reach to other European countries.

7.3 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.

As a very concrete contribution to the SSI domain, a collaboration between OwnYourData and the UniResolver was initiated in the course of the project to provide DID Rotation for all DID methods. Through initial discussion in the DIF WG-ID bi-weekly calls it was agreed that an adapted resolution process for DID Rotation should be implemented right in the UniResolver.

7.4 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 help-seeking 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.

As a first tangible result an integration with the Sphereon Wallet was implemented and demonstrated: Users with a DEC112 Credential are now enabled to trigger a Silent Emergency Notification from the login screen.

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 TRUSTCHAINs position as a leader in the domain. In return, our platform benefits from the network and available know-how of the TRUSTCHAIN community.

8 Early Demo and/or Initial Experimental (or Analytical) Results

This chapter presents preliminary results of early demonstrations of the solution to illustrate its functionality and effectiveness.

8.1 Early Demos

In the current phase of our research project, we conducted a series of early demonstrations for various stakeholders to validate the functionality and effectiveness of our proposed solutions. These demonstrations were crucial in establishing the viability of using government-issued identities for authentication and data sharing in the emergency communication domain. Additionally, the use and further development of decentralised identifiers (specifically `did:oyd`), designed to apply self sovereign design principles and providing the infrastructure for user management and managing credentials, was a significant part of these early trials.

The primary objectives of these early demonstrations were to:

- **Test the Authentication Process:** Assess the efficiency and security of using government-issued identities for user authentication in emergency communication scenarios.
- **Demonstrate Integration into an EU Digital Identity Wallet:** Showcase the use of the DEC112-SDK in the Sphereon Wallet and trigger a Silent Emergency Notification using a credential stored in the wallet.
- **Assess Chatbot Functionality:** Evaluate the performance of the chatbot in simulating real-life emergency call takers, focusing on its ability to understand and respond to text-based emergency communications accurately and efficiently.
- **Evaluate Data Sharing Capabilities:** Determine the willingness of stakeholders to participate in facilitating the seamless sharing of conversation data between DEC112 and emergency response organisations with the optional use of a Data Intermediary.

We conducted a series of interviews with key stakeholders. These stakeholders included emergency response organisations (control rooms), government officials responsible for public safety, technology experts, and potential end-users of the system. The interviews aimed to gather diverse perspectives on the system's functionality, potential impact, and areas for improvement.

The interviews were conducted over a period of three weeks. Each interview lasted approximately 1 hour and was structured to cover a range of topics, including a

Funded by the European Union

presentation of the system and 5 prepared questions about the perceived benefits and challenges of the system, suggestions for enhancements, and overall impressions of the digital emergency communication platform and the chatbot.

8.2 Initial Results

In the critical phase of assessing the IM4DEC project solution, we engaged a diverse range of stakeholders, each bringing unique insights and expertise to the evaluation process. This inclusive approach ensured a comprehensive understanding of the system's impact from multiple perspectives. Our selected stakeholders included:

- **Emergency Response Organisations:** managers from the LWZ Vorarlberg (https://lwz-vorarlberg.at/) and Notruf NÖ (https://notrufnoe.com/) provided insights from a control room perspective
- **Public Safety Government Officials:** head of emergency call and control centre competence centre in the Ministry of Interior (https://www.bmi.gv.at/113/Sektion_II/start.aspx)
- **Governance and Technology Experts:** responsible managers from the Austrian telecom regulatory authority (https://www.rtr.at/rtr/Startseite.en.html)
- **Emergency Room Doctors:** medical professionals who treat patients from domestic violence in emergency room settings and report suspected cases in the hospital internal violence prevention program

These stakeholders collectively formed the backbone of our evaluation process, providing a well-rounded perspective on the system's functionality, challenges, and potential impact in the realm of digital emergency communication.

The following recommendations where a common theme in the feedback we received in the interviews:

- **Telephone Number Necessity:** Current processes in control rooms require a telephone number, and dispatchers want the option to call back.
- **ID Austria as Welcome Additional Information:** ID Austria is seen as a valuable extra piece of verified information.
- **Ease and Speed of ID Austria:** In initial tests, ID Austria is perceived as simpler and faster compared to the current SMS registration.
- **Automated and Silent Emergency Calls:** These are niche applications that should not be mixed with the text-based emergency call system.
- **Chatbot as a Training Tool:** Although the chatbot is viewed as an interesting training opportunity and generally acknowledged for its excellent performance, there are concerns about its deviation from a real emergency call and the potential mismatch of user expectations.

9 Integration with Global Objectives of TrustChain-Impact

This section analyses how the project contributes to the broader objectives of TrustChain. It highlights the project's role in fostering innovation and advancements within its specific sector.

9.1 KPIs towards a more trustworthy and privacy-aware evolution of the internet

#	KPI	Project Contribution
1.1	Which is the Trust Assessment Effectiveness, e.g., accuracy for labelling/inference of the trustworthiness subjects or for content, for your solution.	trustworthiness is key for delivering emergency calls and by using a government issued ID for onboarding we improve the overall trustworthiness of the system
1.2	How can you assess the privacy/anonymity of your solution? E.g., employing probabilistic metrics, anonymity set size, entropy, etc.	a Privacy Report (Appendix A) and a Data Protection Impact Assessment (Appendix B) was performed
1.3	Security guarantees on trustworthiness/privacy, e.g., security proofs.	the project scope did not encompass dedicated security proofing, although it is being undertaken by a team with over 10 years of experience in safety-critical emergency communication
1.4	Did you employ/ implement zero knowledge proof protocols?	was not in project scope / is not implemented
1.5	How does your solution improve security and privacy, compared with existing solutions?	through the focus on established standards (ETSI TS 103 479 and ETSI TS 103 698) along the technical delivery of an emergency call, using the latest established technologies (ID Austria, state-ot-the-art encryption standards), and performing a Privacy Report (Appendix A) and a Data Protection

#	KPI	Project Contribution
		Impact Assessment (Appendix B) we ensure the highest level of security and privacy currently available for text-based emergency communication for the deaf and hard-of-hearing community

Table 9.1: KPIs towards a more trustworthy and privacy-aware evolution of the internet

9.2 KPIs TOWARDS A MORE DECENTRALISED NGI

#	KPI	Project Contribution
2.1	Did you implement new decentralised computing technologies for storing and accessing data, e.g., via the OAI-PMH protocol, that achieve high reliability, availability, Quality of Service, and similar properties necessary to realise new decentralised services?	was not in project scope / is not implemented
2.2	Did you implement new decentralised social networks?	was not in project scope / is not implemented
2.3	Did you implement new decentralised publishing platforms?	was not in project scope / is not implemented
2.4	Did you implement new Digital Twin technologies that can help establish digital representation of the reality in specific circumstances where needed?	was not in project scope / is not implemented
2.5	How does your solution improve decentralisation, and how does	through the introduction of DIDs in the onboarding process for DEC112 services

#	KPI	Project Contribution
	that impact user experience, compared to existing solutions?	users are enabled to switch between service provider and are empowered to maintain their identity without relying on a third party; this even extends to the fact of switching DID providers through DID Rotation regarding user experience, a significant improvement in onboarding time is achieved by using ID Austria instead of SMS verification
2.6	Have you investigated the scalability of your decentralised solution?	The DEC112 app has now more than 29.000 users (as of Jan 2024) and design patterns as well as the components can easily handle a 10x increase in terms of users and call volume Due to thorough 24/7 (automated) end-to-end tests currently a call volume of 500.000 emergency calls is processed per year.

Table 9.2: KPIs towards a more decentralised NGI

9.3 KPIs towards new forms of human-centred interaction and immersive environments for NGI users

#	KPI	Project Contribution
4.1	Task Success rate. % of participants that successfully complete a task.	will be reported in D4
4.2	User Adoption Rate. How many new users does the tool have? What percentage represents the new users?	at the begin of the project DEC112 had about 20.000 registered users; as of Jan 15, 2024 there are now more than 29.000 users → this is an increase of about 45%

#	KPI	Project Contribution
4.3	User Satisfaction. How satisfied are the users with the solution? What is the % of satisfaction?	user satisfaction is only measured for the ChatGPT enabled chatbot and will be reported in D4
4.4	User error rate. How frequently users make mistakes during a specific task? Where do the users face difficulties with the product?	will be reported in D4
4.5	Time on task. How much time is the total learning time spent by the user to know how to use the solution?	no metrics are collected for time on task
4.6	Navigation vs. search What the users prefer to do? Is the navigation process clear? How often do the users use the search function?	not applicable for the DEC112 solution
4.7	System Usability Scale (SUS) questionnaire. How usable is your solution for the users? Net Promoter Score. What is the % of likelihood that the users recommend the solution?	neither System Usability Scale nor Net Promoter Score were evaluated for the DEC112 solution

Table 9.3: KPIs towards new forms of human-centred interaction and immersive environments for NGI users

9.4 KPIs TOWARDS A GREENER NGI

#	KPI	Project Contribution
8.1	Carbon footprint, e.g., greenhouse gas emissions comparing with existing solutions	through avoiding the use of blockchain a significant reduction in carbon footprint is achieved

#	KPI	Project Contribution
8.2	Consumption of energy	the solution is hosted on a managed Kubernetes cluster; we requested a statement of energy consumption from the hosting company and will provide the information in D4
8.3	Supply chain miles	not applicable for the provisioning of emergency communication services
8.4	Saving life, improving biodiversity	during 2023 the DEC112 service delivered 1.500 emergency calls
8.5	Waste reduction and recycling rates	not applicable for the provisioning of emergency communication services
8.6	Sustainable outcomes in economic, energy and/or the societal terms achieved	providing emergency communication services for the deaf community and people experiencing domestic violence is in line with the ESG goals and specifically the social aspects
8.7	Environmental sustainability standards and policies, e.g., Green Energy Generation Initiatives, Sustainable Development Goals	not applicable for the provisioning of emergency communication services
8.8	Addressing climate change? (yes/no)	not applicable for the provisioning of emergency communication services

Table 9.4: KPIs towards a greener NGI

9.5 KPIs TOWARDS INNOVATION

#	KPI	Project Contribution
9.1	Did you implement new innovative TRUSTCHAIN use cases?	yes, all use cases are described in chapter 2

Funded by the European Union

#	KPI	Project Contribution
9.2	Did you implement new innovative TRUSTCHAIN reasoning technologies?	was not in project scope / is not implemented
9.3	Did you make any inventions in the framework of your project, in terms of patents, copyrights, design rights, trademarks, trade secrets, etc?	no, was not in project scope
9.4	Which are the most disruptive technology components of your solution?	DID Rotation as described in section 2.4

Table 9.5: KPIs towards innovation

10 Any Other Impacts

This chapter discusses societal, environmental, legal and policy impacts.

Societal: Our solution serves as a trailblazer for inclusive tech, showcasing how technology can be harnessed to cater to specific communities, which in our case are people with disabilities and people suffering from domestic violenceFurthermore our technology facilitates the freedom of choice, which DID provider one may choose. With DIDs being a fundamental part of a person's identity, it's crucial that this identity is not bound to a single provider and can be freely migrated to other providers.

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.

Legal & Policies: 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.

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

11 Conclusions and Next Steps

In conclusion, the process of software implementation, deployment, testing, demonstration, and validation is an intricate and essential part of software development. This comprehensive document has described each phase of this process, demonstrating how they collectively contribute to the development of the TRUSTCHAIN OC1 project IM4DEC.

The implementation and deployment phases ensure that the developed software is correctly installed, configured, and made ready for use in the desired environment. Testing, a crucial step in guaranteeing the software's quality, ensures that the product is free from defects and performs as expected. We have explored various testing methodologies that allow us to identify and rectify errors and anomalies effectively.

Demonstration, an integral part of user engagement and feedback collection, allows us to present the functionalities of the software to the intended users and stakeholders. It gives users a firsthand experience of the software, enabling them to understand its capabilities and provide useful feedback.

Finally, the validation step confirms that the software meets the defined requirements and specifications. It ensures that the final result aligns with the initial design goals and fulfils the identified user needs.

As we move forward in our journey, it is crucial to remember that these steps are not isolated, but interconnected elements of a robust process. They reinforce each other, ensuring that our software not only functions as intended but also delivers significant value to its users as we will describe in Deliverable 4 - planned to be made available in March 2024.

LINALTEC

DEC112 Privacy Report

Assessment

Date: 2024-01-19

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

2024-01-19 - Current version: feedback from Ruben Roex (Timelex) incorporated. Added reference to EDPB as additional guidelines for performing DPIA.

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?
1. Evaluation or scoring	No
2. Automated decision making	No
3. Systematic monitoring	No
4. Sensitive data	Yes (1)
5. Large scale data processing	No (2)
6. Datasets are matched/combined	No
7. Data relating vulnerable individual	Yes (4)
8. Innovation use of technology	Yes (3)
9. Prevents using a service or a contract	No

Note – For details on individual criteria refer to either EDPB[5] or ICO guidelines[6].

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

[5] EDPB Guidelines on Data Protection Impact Assessment (DPIA) and determing whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

[6] 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/

(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.
(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.

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

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. Note: As a private citizen you protect yourself from this insight by using a VPN service. You also need to use private mode so cookies are not used as fingerprints which can re-identify you.
** GPS location can track where you visit and where you live and is considered personal data

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

What principals should be followed to process personal data?

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

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

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

When is consent required?

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

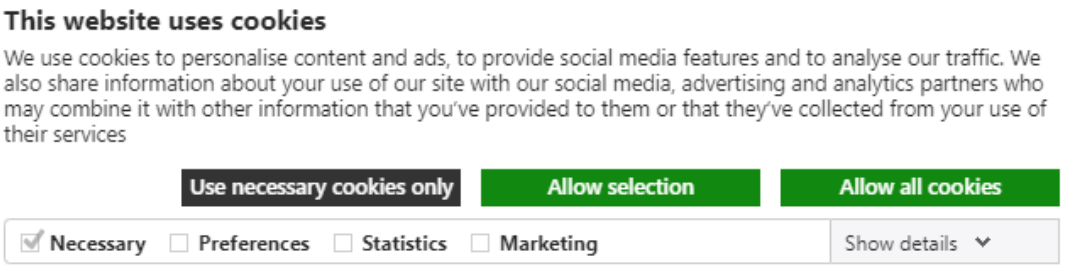

Figure A.1: Example of Well-Implemented Website Cookies Consent Interface

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

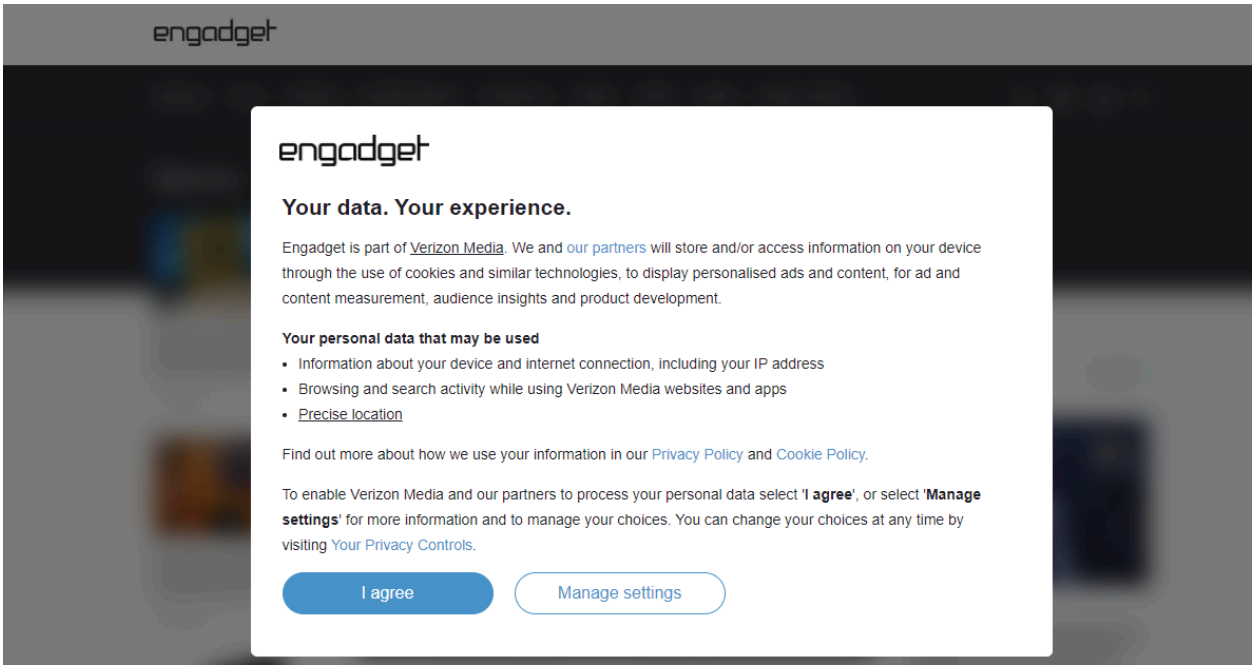

Figure A.2: Example of Poorly Designed Website Consent Interface

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

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

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

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

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

Table A.2: GDPR Rights

* Not all personal data can be erased and there may be other legal requirements in a country where data must be kept for a longer period. For example, salary information must be kept for 7 years in Austria. 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.

DEC112 DPIA Report

Assessment

Date: 2024-01-19

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

2024-01-19 - Current version: feedback from Ruben Roex (Timelex) incorporated. Clarified retention justification and security and privacy implementation responsible.

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 Protection 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.

Term	Description
Organisation	The term organisation refers to the whole DEC112 association members and subcontractors
Personal Identifiable Information (PII)	The term PII is used to refer to any personal identifiable information like email, name or driver's licence. Some PII data can be directly linked to an individual and some can be extrapolated like GPS location or physical characteristics.

Table B.1: DPIA Glossary

Scope

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

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

Roles and Responsibilities

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

Role	Responsibility
Everybody	It is the responsibility of every employee and contractor to be observant of the privacy related irregularities and report them to the DPO immediately. The incident will be logged to best determine action.
Leadership team	Commit to the privacy policy and ensure the privacy program led by the DPO is being fulfilled.
IT admin	Ensure all access to private data is restricted based on role.
Platform Development	During the development phase limit the usage of real personal data.
Research	Research shall be performed on anonymized data but due to the level of detail of re-identify additional security measures shall be followed.
Data Protection Officer	Manage the privacy program and ensure adequate controls and training are in place minimising all privacy risks. Provide regular updates to the leadership of the privacy KPI's. The role is assigned to the vice-president of DEC112.

Chief Technical Officer	The implementation of security requirements and ensuring the solution follows privacy-by-design is the responsibility of the president of DEC112.

Table B.2: Roles and Responsibilities

Scope of Processing

Processing Overview

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

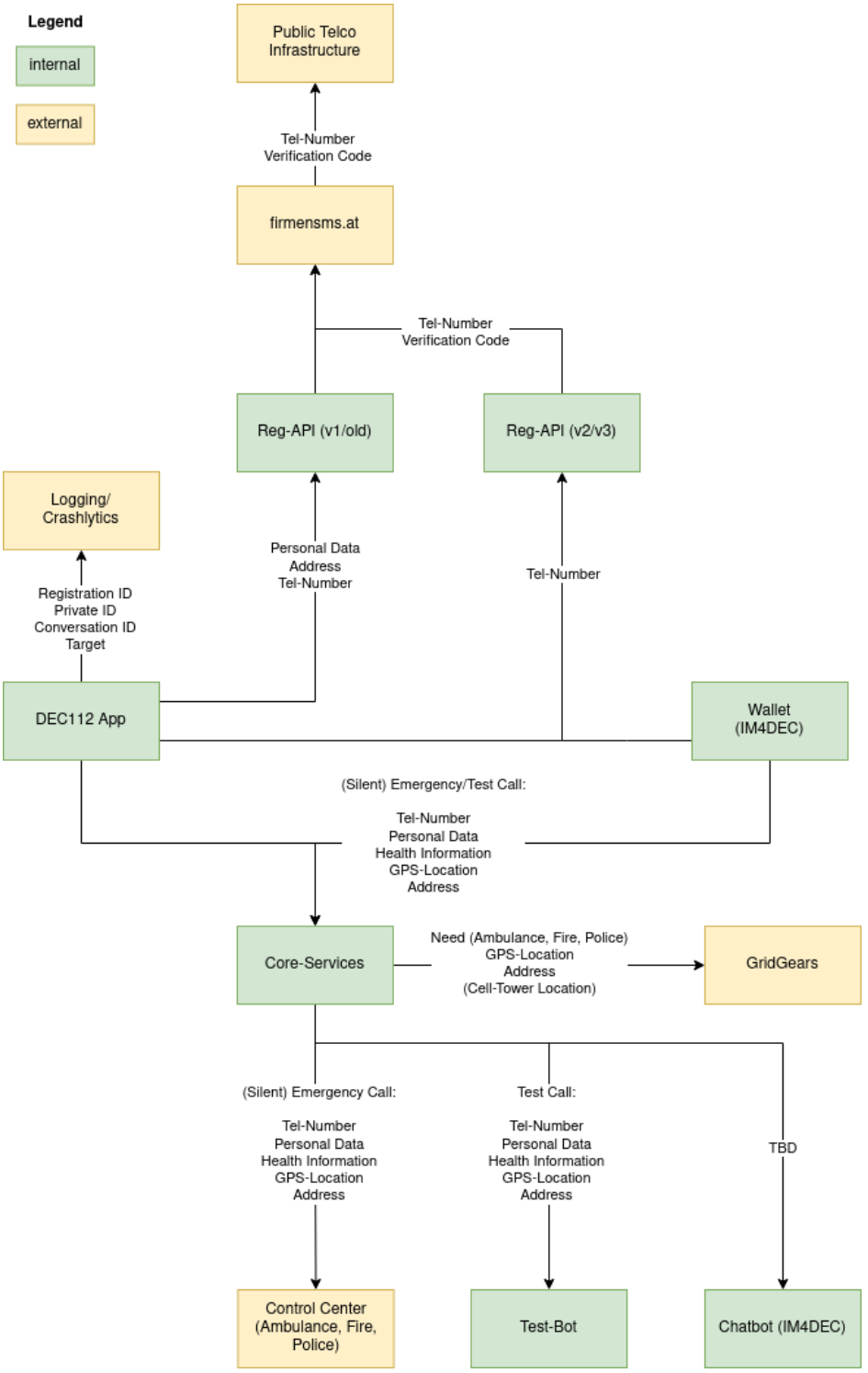

Figure B.1: Processing Overview

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

These are the main flows when processing personal data:

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

Data Subjects

The data processing is limited to individuals in Austria.

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

Data Types

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

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

Table B.3: Data Types

Personal Data Classes

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

- **PII**: Personal Identifiable Information

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

- **QII**: Quasi-Identifiable Information

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

- **SEN**: Sensitivity

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

Data Categories

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

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

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

Table B.4: Data Categories

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

Data Retention

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

Data Type	Retention	Retention Justification	Retention Measure
Personal Data	All personal data is stored in the DEC112 app and is not deleted if an individual does not delete the app installed on their phone.	Individuals have full control of the app and are able to delete it at any time.	
Tracking (Contact, Computer device)	During registration some tracking information like phone number and model are stored in the DEC112 backend. The information is stored for 24 hours. .	The registration information is only kept for a limited time in the system .	
Communication	All emergency communications - once routing is established -	The communication is retained as long as necessary to provide	

Data Type	Retention	Retention Justification	Retention Measure
	are forwarded to the operator together with personal data and tracking information. The DEC112 backend stores the communication log for 2 years.	evidence of delivering emergency service as part of contract with the Ministry of Interior. An example, the data is used to check potential abuses by callers when a call is not a real emergency.	

Table B.5: Data Retention

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

Data Access/Use

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

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

Table B.6: Data Access/Use

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

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

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

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

Data Sharing

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

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

Compliance with Data Protection Law

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

Lawful Basis for Processing of Personal Data in Emergency Calls

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

Article 6 (Lawfulness of processing)

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

Article 9 (Processing of special categories of personal data)

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

Exercise of Data Subject Rights

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

Privacy Right	Description	Response	Internal routine
Right of access	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

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.

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.

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

Appendix C - ChatGPT Privacy Analysis

History

2023-08-31 - initial Version

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

2024-01-19 - Current version: feedback from Ruben Roex (Timelex) incorporated. The new Terms of Use being released on February 15, 2024 introduces a data controller dedicated to the European Economic Area (EEA). The new "sharing publication policy" clarifies how the ChatGPT generated content shall be communicated externally.

This is the current status (as of 19. January 2024) 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.
- 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.

European Terms of Use: https://openai.com/policies/eu-terms-of-use

Analysis

OpenAI Policy Analysis

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

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

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

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

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

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

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

Claim 2: When opted-out input (conversation) is not used to train chatgpt

“Data controls offer you the ability to turn off chat history and easily choose whether your conversations will be used to train our models.”
“While history is disabled, new conversations won’t be used to train and improve our models,

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

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

same as Claim 1
“Our large language models are trained on a broad corpus of text that includes publicly available content, licensed content, and content generated by human reviewers. We don’t use data for selling our services, advertising, or building profiles of people—we use data to make our models more helpful for people. **ChatGPT, for instance, improves by further training on the conversations people have with it, unless you choose to disable training.**

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

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

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

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

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

Claim 8: File endpoint is retained until user deletes the file

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

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

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

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

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

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

Sharing Publication Policy: https://openai.com/policies/sharing-publication-policy
When using ChatGPT service and sharing the output it is important to abide by these practices:

a. The generated content should be attributed to organisation (DEC112) and clearly indicate content was AI-generated. Note - The badge to be used to indicate it is OpenAI generated can be found in the Brand guidelines.
b. The content should not violate the Content Policy which in essence shall not harm yourself or others

Summary

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

Claim 1: Input data is used for training the chatgpt model, opt-out is required.
Claim 2: When opted-out input (conversation) is not used to train ChatGPT.
Claim 3: Ensure no browser add-ons or malware on computer stores conversation.
Claim 4: Opting-out is on a device/browser basis. Need to opt-out independently.
Claim 5: History can also be disabled and will be removed after 30 days.
Claim 6: There are plans by OpenAI to simplify opting-out.

Claim 7: Using the API by default the submitted data is not part of the training and requires opt-in.
Claim 8: File endpoint is retained until the user deletes the file.
Claim 9: Requests from law enforcement or public authority will inform customers.

Guidelines for Using Generative AI Tools

The Canadian Cyber Security Guidance[7] 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.

[7] 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[8].

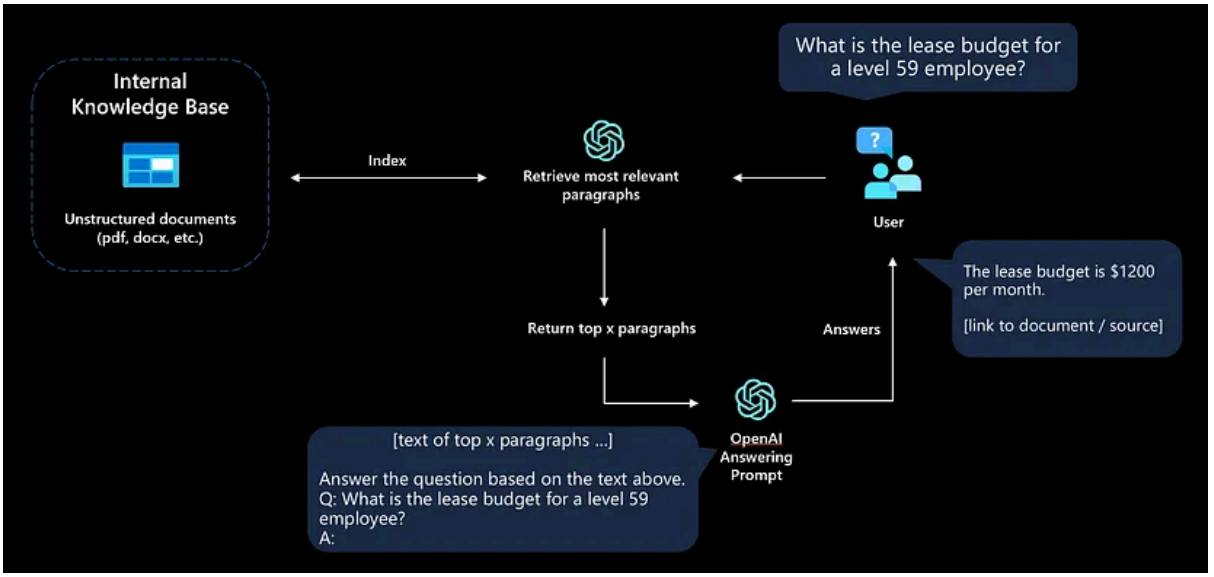

Figure C.1: ChatGPT Plugin

[8] 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.

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