

## NGI Funding for DECTS

18. May 2020 / 0 Comments / in OwnYourData, SemCon / by

Christoph Fabianek

The project DECTS (Deaf Emergency Chat and Training System) aims to provide deaf emergency calls and a training environment in several languages. With the help of a chatbot, deaf people can learn how to use the app and at the same time generate test data for training the control center personnel. The users can determine whether the entries are used as test data and there is documentation about origin, GDPR-compliant provision, and use of the data. The consent to the use of the data can also be changed and revoked later.

The teams from OwnYourData and DEC112 work together to implement this. In previous projects, an infrastructure was already set up in Austria for deaf emergency calls and the challenge now lies in international operations – for example when an Austrian tourist is on vacation in Copenhagen: in this case an emergency call is made via the DEC112 App registered in Austria and conveyed to the control center in Copenhagen.

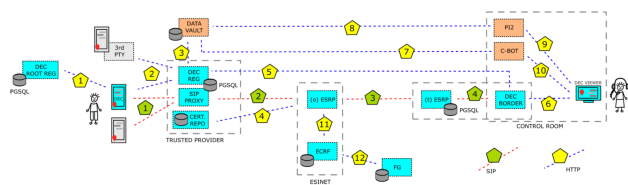
A chatbot is developed for the training environment that simulates a control center. In a test chat, structured information is queried and further questions arise when using certain keywords. In cooperation with emergency call centers, typical conversations were analyzed and so-called decision trees were created, which the chatbot automatically processes.

If a user consents to the further use of the chat protocol, this consent can be managed in the OwnYourData Data Vault. There the consent of the transfer of the data is documented and it is possible to query when the data was accessed. In particular, however, access can also be restricted or subsequently prohibited. Semantic containers are used as the

technology platform, which ensure data access is transparent and traceable.

Finally, personal data (emergency contacts, medical data and other information) can also be stored in the OwnYourData Data Vault, which is automatically provided to the control center in the event of an emergency chat. This personal data is referenced using a DID (Decentralized ID) and the data itself is stored encrypted. The Shamir's Secret Sharing scheme ensures that the data can only be read by the user and the control center, but cannot be accessed by OwnYourData or DEC112.

The system architecture for the project is shown in the graphic below, together with the data flows between the individual components. All parts are now at least available as prototypes and the first end-to-end tests were carried out in May.



## Share this entry



0

REPLIES