Leiden University Medical Center

H.J. van der Wijk[1], A. Kaldenhoven[2]
[1] Dept of Advanced Data Management, Leiden University Medical Center [2] ZorgTTP

Securing mobile device data in the LUMC Research-ICT architecture with TRES real-time reversible pseudonymization by ZorgTTP

Introduction

Mobile devices are an interesting opportunity for both care and research to collect a wide range of valuable health data, such as questionnaire data, measurements (heartrate, blood pressure), distance travelled and other sensor information. In the LUMC various healthcare apps have been developed, for example the Wound care app to determine whether a surgery wound may have become infected and Participatient, a modular app that currently can measure pain and can score the requirement of a catheter with the aim to reduce catheter infections.

The data collected by these apps is highly privacy sensitive and requires enhanced protection. Securing the data by pseudonymization, replacing identifying information with codes, is an important security measure.

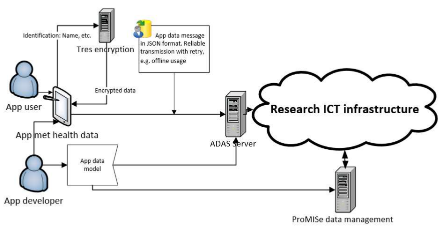
Pseudonymization architecture

TRES real-time encryption is being used in more than 30 research project to facilitate real-time pseudonymization and de-pseudonymization. Access to these services is granted to registered users and based on explicitly specified permissions[2]. App users however are not know beforehand. Apps are now supported with new TRES anonymous user functionality.

The TRES encryption server creates pseudonyms for the Identifying data elements, like names, and these replaces the information in the app. The app then constructs a message containing the pseudonym and the other data. This message is sent to the LUMC ADAS server and further processed for data management.

The new TRES anonymous users functionality provides a secure pseudonymization mechanism by granting encryption, but no decryption permission. Furthermore each user creates unique personal pseudonyms by using a personal encryption key.

The data collected in the app is sent as messages to the ADAS server, and from there can be processed by any application. Currently, integration into ProMISe data management is implemented, making the collected data available for research[6].


Identification: Name, etc.
Tres encryption
App data message in JSON format. Reliable transmission with retry, e.g. offline usage
Encrypted data
App user
App met health data
ADAS server
Research ICT infrastructure
App data model
App developer
ProMISe data management

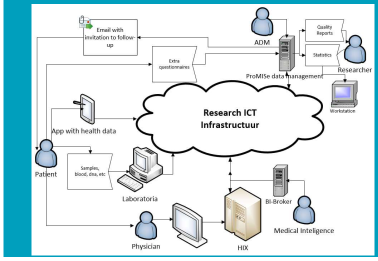
Conclusions

In collaboration with ZorgTTP, the TRES pseudonymization service has been successfully extended with the new functionality to support real-time pseudonymization on mobile devices. TRES can thereby now replaces directly identifying information within apps on mobile devices and can guarantee that no directly identifying information will be sent to the LUMC

This integration of TRES pseudonymization in mobile device health apps is a valuable measure for privacy protection, while at the same time the ability remains to link the data collected by the app to other information sources and to perform administrative tasks that require participants identity

Results

The LUMC has implemented a generic health research ICT infrastructure for collecting data from mobile devices with integration of TRES real-time pseudonymization



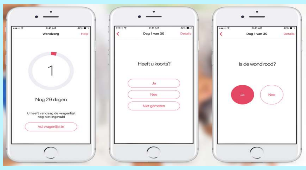
Analyses can very well be performed on this pseudonymized data. In addition, the pseudonym can be used to link the data to other information systems, if the patient approved for this.

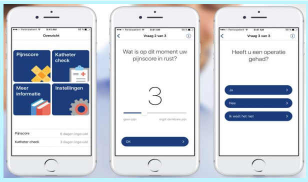
The resulting pseudonymization data is regular TRES data and therefore can be processed for linking and de-identification by any authorized TRES user like any other TRES data. The ProMISe data management server already provides integrated support for TRES and therefore can process this data naturally.

The TRES reversible pseudonym allows for administrative tasks, such as inviting participants for follow up or for new investigations. The TRES translate function allows safe linking and exchanging data between systems and projects based on these pseudonyms. This enables re-use of data, while keeping the data safe from unnecessary identification of the participants.

Wound care and Participatient app

The wound care app supports patients in wound healing by a daily questionnaire for 30 days. The answers to these questions will help to determine whether healing is progressing normally or not. Patients gain a better understanding when to contact their physician. They also are more involved in their healing process and will receive quicker medical attention when needed. Another benefit is that hospitals can learn from the collected data[3]





Participatient is a project to reduce infections in hospitals. With the development of new tools, patients are empowered to become active participants in the care process. The newly developed app daily collects relevant status information and provides the patient personalized feedback and background information. The app is modular to be able to support patients with multiple conditions and currently supports Pain score and Cather check. The gathered information can be discussed with a physician or nurse during consultation[4,5].

TRES pseudonymization

TRES stands for Trusted Reversible Encryption Service and is a real-time encryption service that has been developed in a collaboration of LUMC and ZorgTTP. The service provides encryption of any data element and is typically being used to replace identifying information with their encrypted value, thereby functioning as pseudonymization.

TRES can be fully integrated into any data management application. Combined with real-time en-/decryption, this provides seamless integration. The original data is automatically presented to authorized users and data is automatically encrypted upon data entry. TRES provides dynamic group permissions allowing the TTP to grant access to users based on their legal permission to access the identifying data.

References

1. https://en.wikipedia.org/wiki/Pseudonymization
2. https://www.zorgttp.nl/TRES
3. https://innovattic.com/portfolio/wondzorg/
4. https://innovattic.com/portfolio/patienten-participeren-participatient/
5. https://participatient.nl/
6. https://www.msbi.nl/ProMISe

Acknowledgments

This implementation has been realized in a close collaboration of LUMC and ZorgTTP which co-invested in the new TRES features and in collaboration with Innovattic for developing the apps. We are thankful to our colleagues from the LUMC IT department who provided expertise and support that greatly assisted in the realization of this architecture

Pseudonymization

"Pseudonymization is a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms"[1].

The purpose of pseudonymization is to make data records less identifying and therefore lower patient and legal objections to its use. Data in this form is suitable for extensive analytics and processing[1].

ZorgTTP Privacy & Vertrouwen

ZorgTTP, Houten, The Netherlands

innovattic

Innovattic, Delft, The Netherlands