RESEARCH NEWS

Telematics infrastructure

Future-proof security architecture for healthcare communications

Germany's telematics infrastructure (TI) aims to allow healthcare professionals to exchange patient data securely, rapidly and from anywhere. The platform for healthcare applications will soon see a new, flexible and therefore future-proof security architecture. The aim is to make it easier to exchange data between all parties involved as well as to facilitate access to specialist services. In conjunction with Bundesdruckerei, CompuGroup Medical, D-Trust GmbH and genua GmbH, the Fraunhofer Institute for Applied and Integrated Security AISEC has laid down the design foundations for gematik, who is responsible for the TI: Besides an architecture design based around zero trust principles and a migration plan, a demonstrator for the next-generation security architecture has also been developed. Proof of concept has also been done to demonstrate the feasibility of the architecture.

Electronic patient records, digital medication plans, e-prescriptions: These applications are all key elements of the telematics infrastructure (TI). The platform aims to deliver simple yet at the same time secure communication between medical practices, hospitals and other parties in the healthcare sector. Clinical information required for treating patients would then be available regardless of location. The national agency for digital medicine, gematik GmbH, is responsible for the TI. As well as the German Federal Ministry of Health (BMG), it counts medical associations, pharmacies, hospital and insurance groups among its stakeholders.

The telematics infrastructure is now set to have a new security architecture 2.0. TI 1.0 has so far been a standalone VPN-secured network that identifies users through smart cards for participation. However, the vast increase in TI users and ever-expanding digitalization bring with them new requirements in terms of scalability, availability, user-friendly security and mobile compatibility, which the existing security architecture can no longer meet.

Zero trust principles to verify every access

The new TI security architecture is to be based on zero trust principles. Zero trust means that the actors in a system do not trust each other in principle, but that trust is verified on a continuous basis. This means trust is re-established every time a service's

Contact
Thomas Eck | Fraunhofer-Gesellschaft, Munich, Germany | Science Communications | Phone +49 89 1205-1333 | presse@zv.fraunhofer.de
Tobias Steinhäußer | Fraunhofer Institute for Applied and Integrated Security AISEC | Phone +49 89 3229986-170 | Lichtenbergstrasse 11 | 85748 Garching near Munich, Germany | www.aisec.fraunhofer.de | tobias.steinhaeusser@aisec.fraunhofer.de

resources are accessed and expires again afterwards. For this to happen, reliable evidence must always be provided for communication between the parties, justifying this trust. Access control based on zero trust principles is thus a data-driven, fine-grained approach to information security, one that not only addresses external threats but also internal ones. The zero trust approach differs in this respect from traditional security design, which usually focuses on making company boundaries secure.

All parties integrated equally

"Our proposal for a TI security architecture 2.0 enables a zero trust approach without having to use proprietary components. Instead, the security architecture relies on the end devices that users of healthcare services already have and takes their security functions into account when authorizing individual access to a service. We explored options for various scenarios such as access by insured parties, medical practices or hospitals," explains Martin Seiffert, senior scientist in the Secure Systems Engineering department located at Fraunhofer AISEC in Berlin.

A further advantage of the new security architecture is that the user pool can be expanded. "With the existing VPN infrastructure, direct access to healthcare services is only available to service providers such as medical practices with a fixed location, using the VPN connector as a proprietary component. This access route is not suitable for service providers with no fixed location, or for insured parties. The design behind TI 2.0, however, allows for standard access mechanisms for all user groups, and also for using mobile devices," emphasizes Monika Kamhuber, a scientist from the Secure Operating Systems department at Fraunhofer AISEC in Garching.

Dynamic, versatile, adaptable set of rules

Another strength of the security architecture design is that when controlling access, not only is the identity of the user crucial, but additional factors such as the time and place of access, as well as security requirements for end devices, can be taken into account. The details specifically required for authorizing access to healthcare data are defined in a dynamic set of rules that evolve as technology advances: The set of rules rapidly integrates current developments in information security and changes relating to the use of healthcare services without having to update each individual service separately.

Access requirements can be defined for the various user groups and applications, depending on the risk, and adjusted again as appropriate. For example, tougher security requirements may be necessary for doctors accessing a large volume of patient data than for insured parties who are only looking to view their own personal data.

Special protection for sensitive patient data

The secure management of patient data and safeguarding data protection take top priority in sensitive environments such as healthcare. Against this background, the new

design from Fraunhofer AISEC and its partners tries to avoid the omnipotence of single actors by ensuring that no infrastructure component alone provides access to the healthcare services. So to access TI 2.0, besides proof of identity, verifying the presence of a one-time registered device can also be made a requirement so that stolen or manipulated proof of identity is not sufficient to gain access, nor is using a stolen registered end device.

"Because the telematics infrastructure is a network where primarily patients' personal healthcare data is processed, the TI 2.0 is subject to very high security requirements. Our architecture uses various standard components in the areas of identity and access management that are well-established within the context of zero trust, allowing us to meet these requirements," says Seiffert.

gematik GmbH has published the concept for TI 2.0 based on zero trust mechanisms, designed by Fraunhofer AISEC and its partners Bundesdruckerei, CompuGroup Medical, D-Trust GmbH and genua GmbH, online.

For more information, see here:
Feinkonzept Zero Trust Architektur für die Telematikinfrastruktur (gematik.de; in German only)

Fig. 1 Security architecture 2.0 for the telematics infrastructure (TI): Zero trust principles connect users such as insured parties, hospitals and medical practices (left) with healthcare applications, for example medication plans, e-prescriptions or electronic patient records (right).

© Fraunhofer AISEC