Solution Brief

Intel® Software Guard Extensions (Intel® SGX)

Maximum Security at the Processor Level: Intel® SGX Protects Electronic Patient Record

The Electronic Patient Record (ePA)

The electronic patient record (ePA) can store diagnoses, treatment data, medication plans, allergies and other health data. It is also possible to save individual health information, such as a diary of blood glucose levels, to it. Use of the ePA is voluntary and free of charge and is available uniformly across all statutory health insurance funds across sectors and cases. From 2022, additional information such as vaccination card, maternity log, the yellow booklet for the obligatory children's U-examinations and the dental bonus booklet can be stored on it.

Patients decide which documents are stored in the ePA and which doctor can access them for how long. For example, it can be specified that a doctor does not receive certain medical records even though they are allowed to use the ePA. As a rule, health insurance companies only get write access to the ePA. The duration of any authorization can range from one day to 18 months. In addition, patients will be able to appoint a representative to assist them in the use of ePA in medical care. All data belongs to the patients, and starting 2022 they will be able to transfer all contents of the ePA to another health insurance provider in case of a provider change.

Maximum security at the processor level

It takes innovative solutions to protect the security of highly sensitive data. Intel Software Guard Extensions (Intel SGX) fulfills extremely high security requirements while being completely transparent to the user. The AOK-specific implementation of the electronic patient record (ePA) in Germany is a prime example of the advantages of this approach.

In recent years, the requirements for protecting personal data have been strengthened, especially by the General Data Protection Regulation (GDPR) and the Patient Data Protection Act (PDSG). This is especially true for health-related information because this data is particularly sensitive – the collection, storage and processing are subject to the highest level of security precautions. Such special requirements can be implemented with reasonable effort in controlled environments like a doctor's practice or within a hospital. But it becomes a lot more difficult when insured persons and other service providers are involved. It was precisely this challenge that AOK – Die Gesundheitskasse, a statutory health insurance company, faced in the implementation of the electronic patient record (ePA). In addition to a strong focus on ease of use, the project participants particularly focused on data security. The ePA was approved by gematik in version 1.0 at the end of 2020 and has been in operation since January 1, 2021.

The concept of ePA

Since January 1, 2021, statutory health insurance has to provide an electronic patient file for each insured person at their request. PDSG states that the ePA must ensure data privacy and data security at all times without compromise in accordance with Paragraph 291a Social Code V and preserve the patient's self-determination information. While the majority of Germans are in favor of using an electronic patient record, as the study "Digital Health System" showed in April 2019, two-thirds of the surveyed feared data theft and abuse. For the numerous partners behind the overall concept of "electronic patient record," these requirements posed major challenges, as this is an environment that could be used by more than 70 million people.

The German concept of electronic patient records allows for a large number of parties to have access to the information to a varying degree. These access rights are not static. They change depending on time limits or granted and withdrawn authorizations by the insured. The ePA's "document management" component in particular has therefore been the most demanding in terms of security. While the patient data and documents can only be stored in encrypted form, the security requirements for processing are more difficult to solve, because the processing application must have access to the plain text data. The security concept of the ePA therefore requires a "Trusted Execution Environment" (TEE), which is a high-security virtual area that is particularly protected from access by processes and other system components.

AOK relies on partners and Intel SGX technology

The ePA requirements and the general legal framework apply to all statutory health insurances in Germany. However, due to the variety of providers, individual implementation timetables and concepts are permitted. Each health insurance can independently decide on an implementation concept and schedule as long as it meets the requirements for functionality and security, provides all specified interfaces, and adheres to the framework schedule. AOK, a community of eleven regional health insurances, chose Intel SGX technology to implement the TEE to meet the stringent integrity and confidentiality requirements of ePA. For technical project planning, service management and operation, AOK chose its long-standing partner ITSG. The x-tention group was commissioned to develop the ePA file system. Along with the digitization service provider Atos, the TEE was developed based on the Intel SGX architecture, built into Intel® Server processors. Finally, gematik commissioned Arvato to operate the telematics infrastructure. Additionally, gematik was responsible for providing the security specifications of the overall solution, based on the input of the Federal Office for Information Security (BSI).

AOK – The Health Fund

For more than 130 years, AOK has been synonymous with one of the largest health insurance organizations in Germany. About 61,500 employees in more than 1,218 branch offices throughout Germany guarantee a comprehensive and efficient service. With a market share of around 37 percent in terms of insured persons, AOK is one of the largest statutory health insurance companies.

Intel SGX: Safety at the highest level

The latest third generation Intel® Xeon® processors are equipped with Intel SGX technology. Intel SGX is an advanced security mechanism that can be used hand in hand with an existing infrastructure to better protect the most sensitive workloads or services. By using Intel SGX, the applications can protect code and data in isolated “enclaves”. The Xeon processor manages these enclaves itself, in memory spaces up to the terabyte range. After provisioning, other processes on the same system, or even on the same CPU core, even those with privileged “root” access, are prevented from accessing data and code within that enclave. In addition, Intel SGX solves a basic problem of Trusted Remote Computing: When a data owner wants data to be processed by a process that they cannot or do not want to control directly, they must rely on the owner of the process being trustworthy. In Intel SGX, a remote attestation server uses a hash value to verify that the code in the enclave matches the original code released by the developer, and attempts to plant manipulated code in the enclave can be detected and prevented.

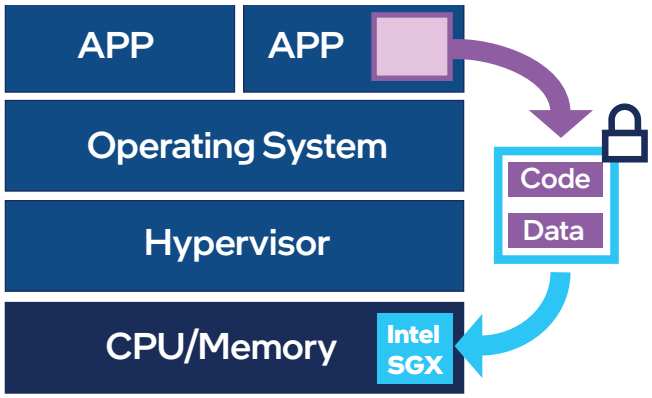

Figure 1. Intel SGX helps protect the most sensitive data by isolating it into enclaves up to 1 TB in size.

At the center of ePA: Document management

The entire electronic patient record includes numerous components. They take care of the connection of patients to the system, link medical practices and hospitals to the environment and handle the filing and archiving of the patient records. In the AOK implementation of ePA, the main task of Intel SGX is to protect the ePA file system. The file system combines authorization, document management and access gateway. It ensures that only authenticated and authorized users can interact with ePA. This also prevents individuals and institutions connected to the ePA from misusing patient data for profiling and evaluation, such as service providers or health insurance providers.

The project managers at AOK expect about 5,000 to 10,000 concurrent links to the ePA application, which means the same number of enclaves will be active in parallel. By using state-of-the-art server technologies, this number can be handled with a comparatively small number of servers and racks. The ePA file system is built with encrypted storage media. Once a patient has consented to the processing of their data, this data can be opened and decrypted within the Intel SGX enclave on the Intel Xeon processor. Once opened, approved applications, in this case the app “AOK Mein Leben”, are able access the document. When processing is complete, the enclave is closed, and the record is stored in encrypted form.

The actual medical records also contain various metadata, such as the access log to the file account of the insured person and policy documents for all access authorizations granted by the insured. The operating system communicates with the enclave through a kernel driver and is severely restricted by the hardware protection features of Intel SGX. The same applies to the code executed in the enclave. For example, the code is not allowed to make system calls; this

has to be done by the rest of the application connected to the enclave via the kernel driver. To be able to execute Intel SGX commands and run in an enclave, code must be signed and verified with a developer key.

Safe development methods as a basis

The developers of the ePA application, x-tention group and ATOS, use secure programming procedures based on best practices. Those cover various areas: most importantly, developers need to be specifically trained to work with Intel SGX in highly secure environments. The development environment is strictly isolated from other network areas and may only be used by specially authorized persons. Moreover, particularly strict quality assurance processes govern the entire process. As an example, the developed program code undergoes static analysis, and its interfaces are subject to internal and external penetration tests. Used Libraries are regularly and continuously examined for malware and secure programming techniques. In addition to the regular update cycles, there are also incident response plans in place that address critical vulnerabilities through emergency patches. Even the mechanisms by which software modules are continuously developed and deployed (Continuous Integration / Continuous Deployment) are implemented semi-automatically to enable additional checks before the roll-out.

Using Intel technology provides an additional layer of security. Intel tests its processors thoroughly and responds quickly to identified vulnerabilities. With Intel SGX technology, the ePA project has set the right course for overall security.

Concentrated processor power with HPE Moonshot and Intel Xeon processors

An application with very high security and availability requirements needs an equally secure operating environment. To achieve this, ITSG, as the operator of the complex application structure, very early on involved Hewlett Packard Enterprise (HPE) through the required public tender process. The aim was to provide a highly automated, secure, efficient and flexible operation of the ePA document management system. HPE contributed a key technology to the ePA implementation of AOK: ITSG chose the HPE m750 server chassis in the Moonshot form factor. The HPE Moonshot solution, similar to blade servers, consists of a central chassis that provides power and network connections via a backplane. However, Moonshot uses a much smaller form factor for the compute modules. This allows up to 45 ProLiant compute modules per chassis, including a redundant network switch. According to HPE, Moonshot enables up to 32% more users per server, with 25% less power required per each user. This extremely high packing density provides more than enough scalability for the expected growth of an ePA available to all German AOK members. AOK created optimal conditions in terms of space requirements, energy consumption and infrastructure operation in the data centers to ensure future growth was accounted for.

Conclusion

Expectations are high for the newly launched electronic patient record. It is expected to make treatments simpler and more flexible, assist in avoiding redundant examinations and give the patients absolute control and transparency over health-related information. In addition, the ePA must be supported by all statutory health insurance funds and allow seamless migration between the funds without loss of data from 2022 on. Through a competent and experienced consortium of service providers and manufacturers, AOK implemented its version of the ePA to the highest security standards, pivoting around Intel SGX technology, a guarantee of trusted and highly secure processor-level computing.

Solution Provided By: