M M S EXPERIENCE BEYOND DIGITAL

Dr. Ivan Gudymenko, IT Security Architect

Enemy in the Clouds

Confidential Computing Group@MMS

T · · Systems · Let's power higher performance

Student motivation to join our team

M M S EXPERIENCE BEYOND DIGITAL

"Joining your team has given me the curiosity to learn more about new technologies. The work environment is a source of motivation to work harder towards the resolution of business problems. What also amazed me is the sense of sharing, collaboration, and teamwork between the different members to work on new approaches for an ongoing project."

“I join this team because I believe the idea of securing our confidential data on the cloud while it’s being processed is an utmost security concern which we need to address as early as possible and as an emerging technology I want to be a pioneer in this field.”

“I wanted to learn about new methods that even ensure the security against strong attacker models”

Confidential Computing Motivation

M M S EXPERIENCE BEYOND DIGITAL

- Leverage the benefits of Cloud Computing
- Outsourcing the operations of infrastructure
  - retain the control over app, keys, etc
- Ensure privacy and security compliance (e.g. Gematik requirements)
- Separate infrastructure and application OPS

Figure from https://blog.keliweb.it/wp-content/uploads/2014/11/Cloud_Computing.jpg

T · · Systems · Let's power higher performance

Gematik Requirements: VAU

Die medizinische Versorgung ist generell gewährleistet, da als Ersatzverfahren (bei Ausfall von Diensten bzw. Störungen) auf das bisherige Papierformular (Muster 16) zurückgegriffen wird.

„Unzureichendes Verständnis bei Verschlüsselung"

Von den anderen 19 Ländern in Europa, in denen das E-Rezept bereits eingeführt ist, setzt kein einziges auf die „Ende-zu-Ende-Verschlüsselung". Das E-Rezept soll Mehrwert und echten Nutzen für den Versorgungsalltag bringen. Dafür muss es sowohl sicher als auch praktikabel sein.

Das E-Rezept ist durchgehend verschlüsselt – es wird sicher und verschlüsselt im Verschreibe- und Einlöseprozess übertragen, gespeichert und verarbeitet. Innerhalb der E-Rezept-Server (Fachdienst) wird eine „Vertrauenswürdige Ausführungsumgebung" (VAU) eingesetzt, um die Sicherheit während der Verarbeitung innerhalb des Dienstes zu garantieren. Hierdurch haben auch Administratoren des Betreibers keinen Zugriff auf die Daten. Die Hersteller von Prozessoren entwickeln diese Technologie laufend weiter; bei Confidential Computing in der Cloud ist sie bspw. zentraler Bestandteil.

Mit Ende-zu-Ende-Verschlüsselung könnte zukünftig z. B. kein in Köln ausgestelltes E-Rezept in Madrid eingelöst werden – was zwischen anderen europäischen Ländern bereits möglich ist und auch für deutsche Versicherte durch die Anbindung an den Europäischen Raum für Gesundheitsdaten künftig möglich werden soll.

What should be protected and why

- Application data
  - especially data-in-use!
- Code
- Secrets (tokens, passwords, master keys, etc)

Figure taken from https://de.freepik.com

Securing the 3 States of Data

M M S EXPERIENCE BEYOND DIGITAL

This is a challenge!

Data at rest

Data in transit

Data in use

Trust assumptions

M M S EXPERIENCE BEYOND DIGITAL

Conventional model:

trusting the underlying software

Operating System

VM Layer

BIOS/Firmware

Confidential Computing:

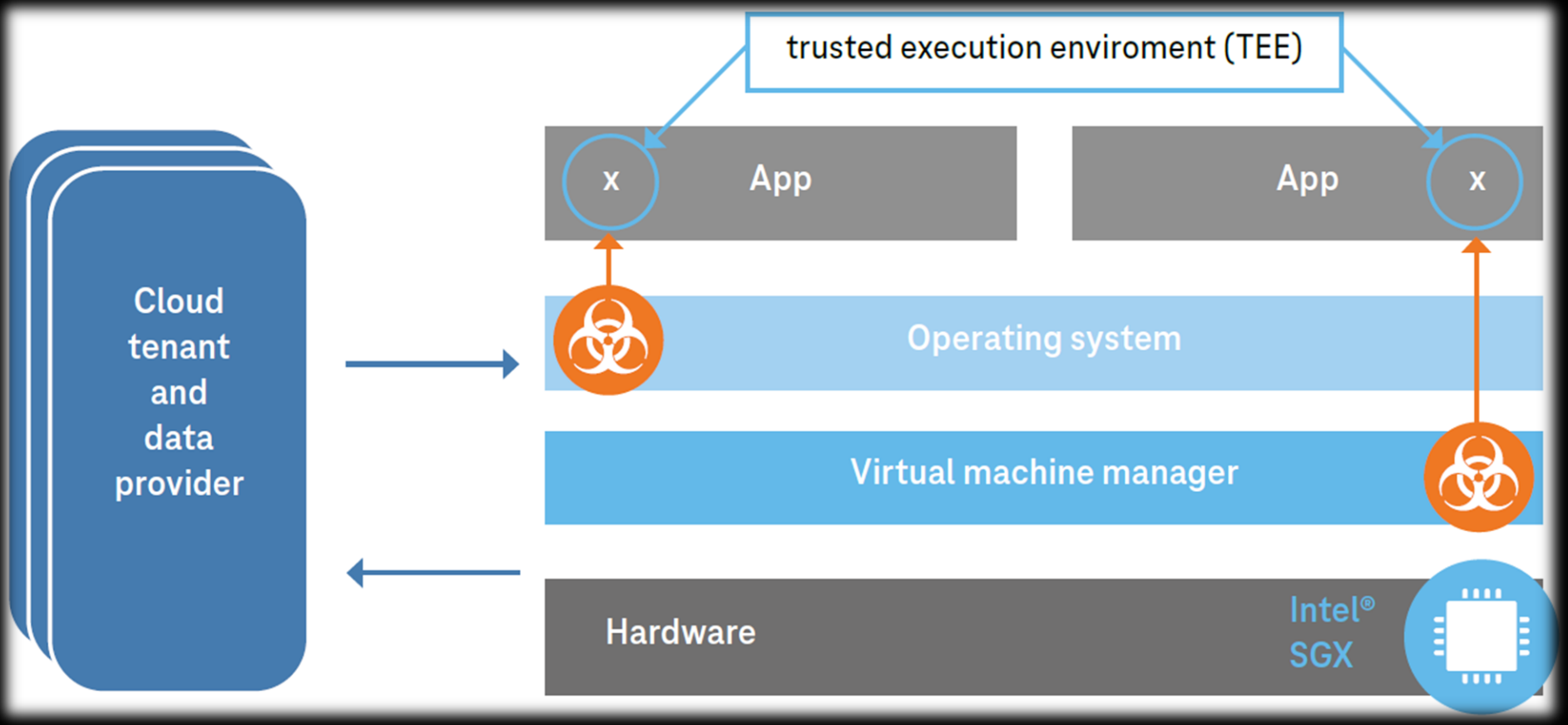
trusting only hardware (TEE)

TEE Hardware

(Intel SGX, AMD SEV, Arm TrustZone hardware)

Minimize attack surface

Trust anchor notion in confidential computing



Taken from whitepaper: Enemy in the clouds: protecting your cloud, assets from powerful adversaries

Examples of Trusted Execution Environments?

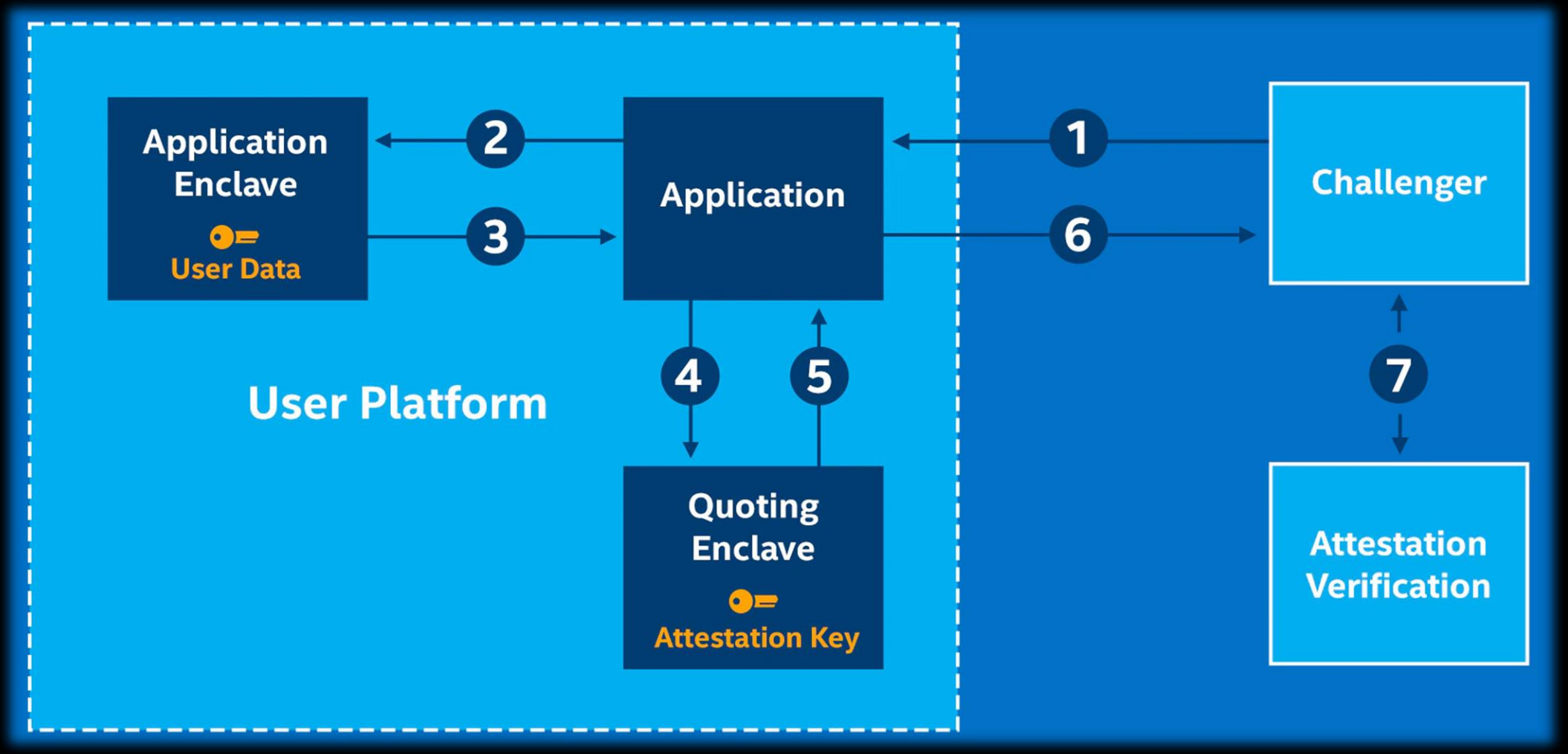
- Smart cards
- SIM Cards
- TPM (trusted platform modules)
- ...

The Notion of Attestation

- ensure execution in a secure container hosted by the trusted hardware
- is NOT code signing but rather measuring
- Software measuring (measurement hash)
  - compare the expected hash with the measured one

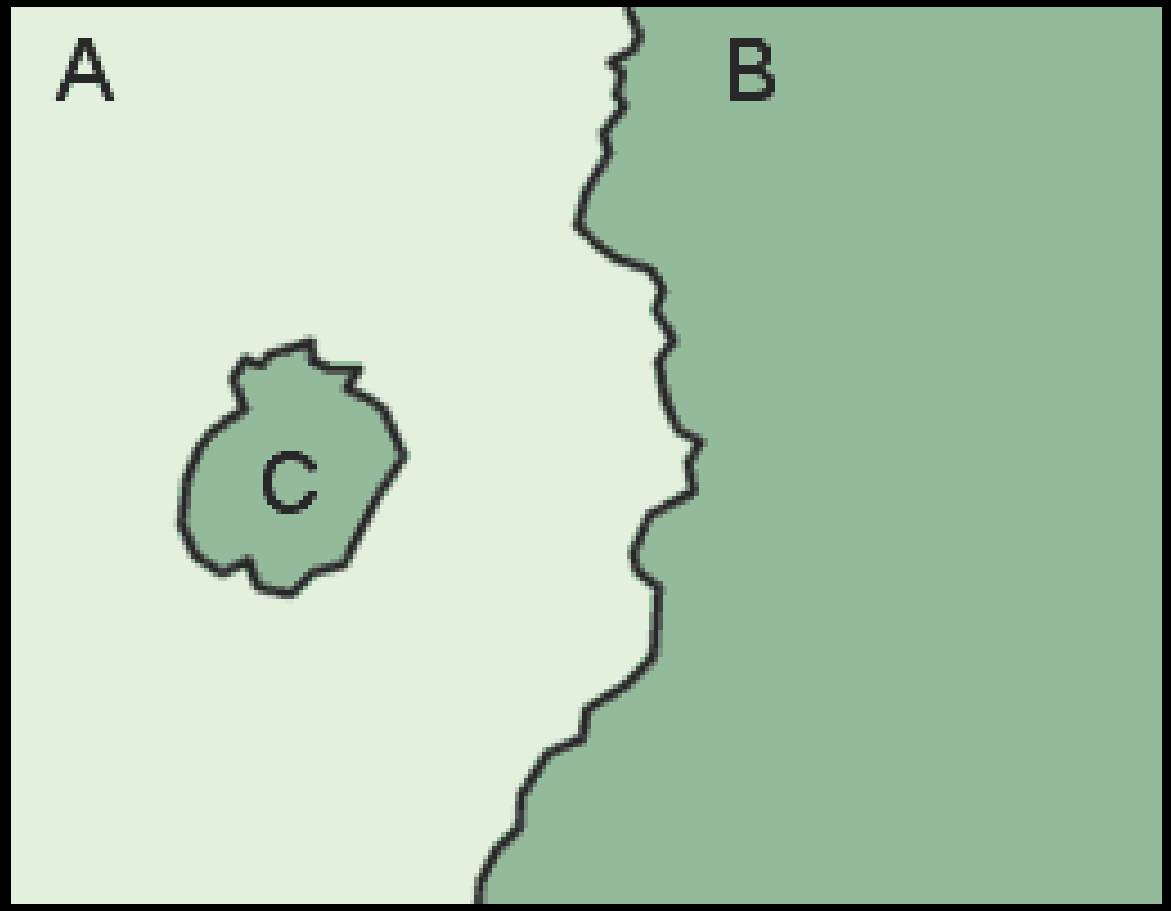
Figure taken from https://de.freepik.com

Example: Intel Attestation



https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/attestation-services.html

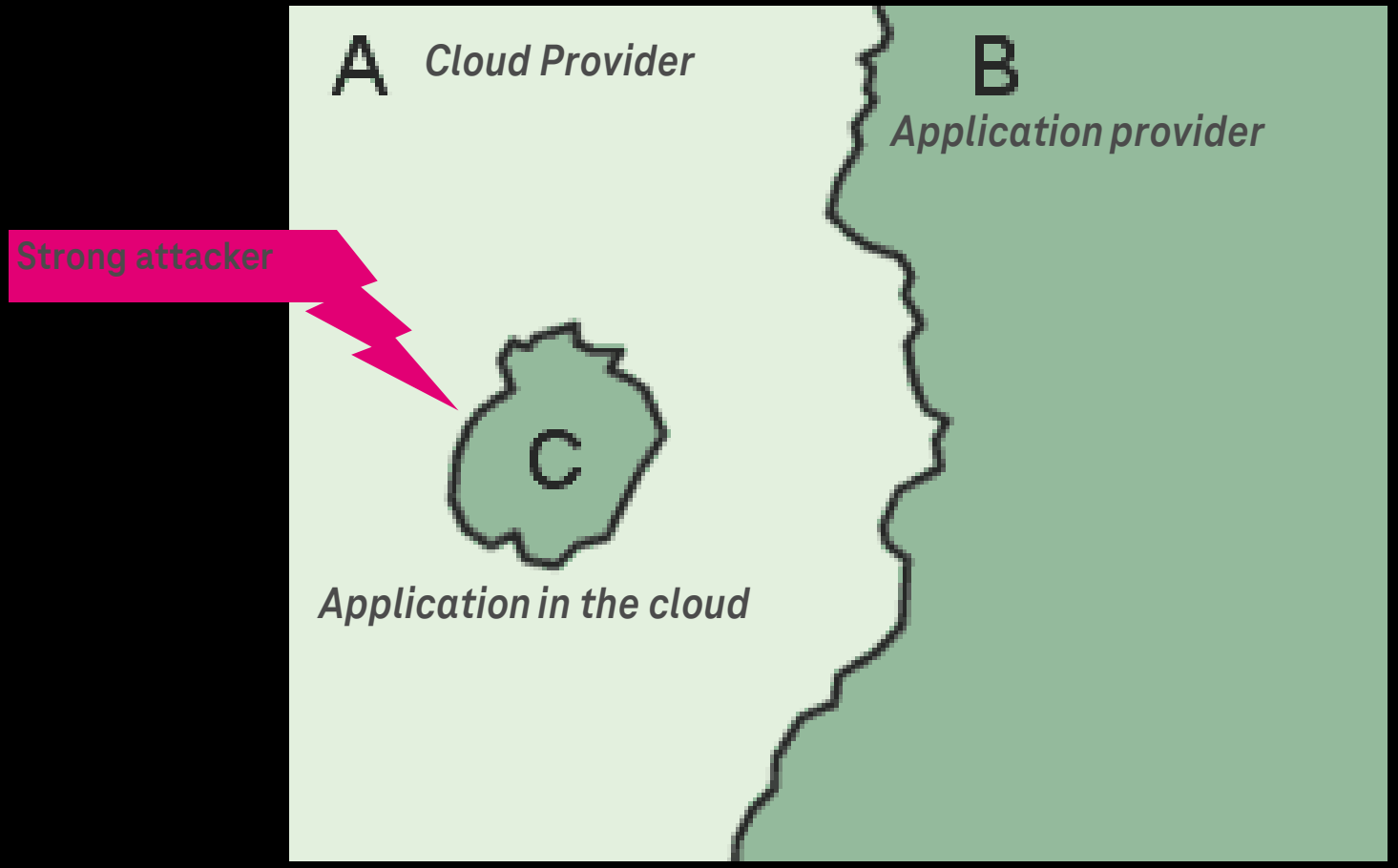
Secure Enclave and the metaphor of a security domain



Bildquelle: wiktionary.org

C represents a security domain of **B** in the environment under the control of **A**

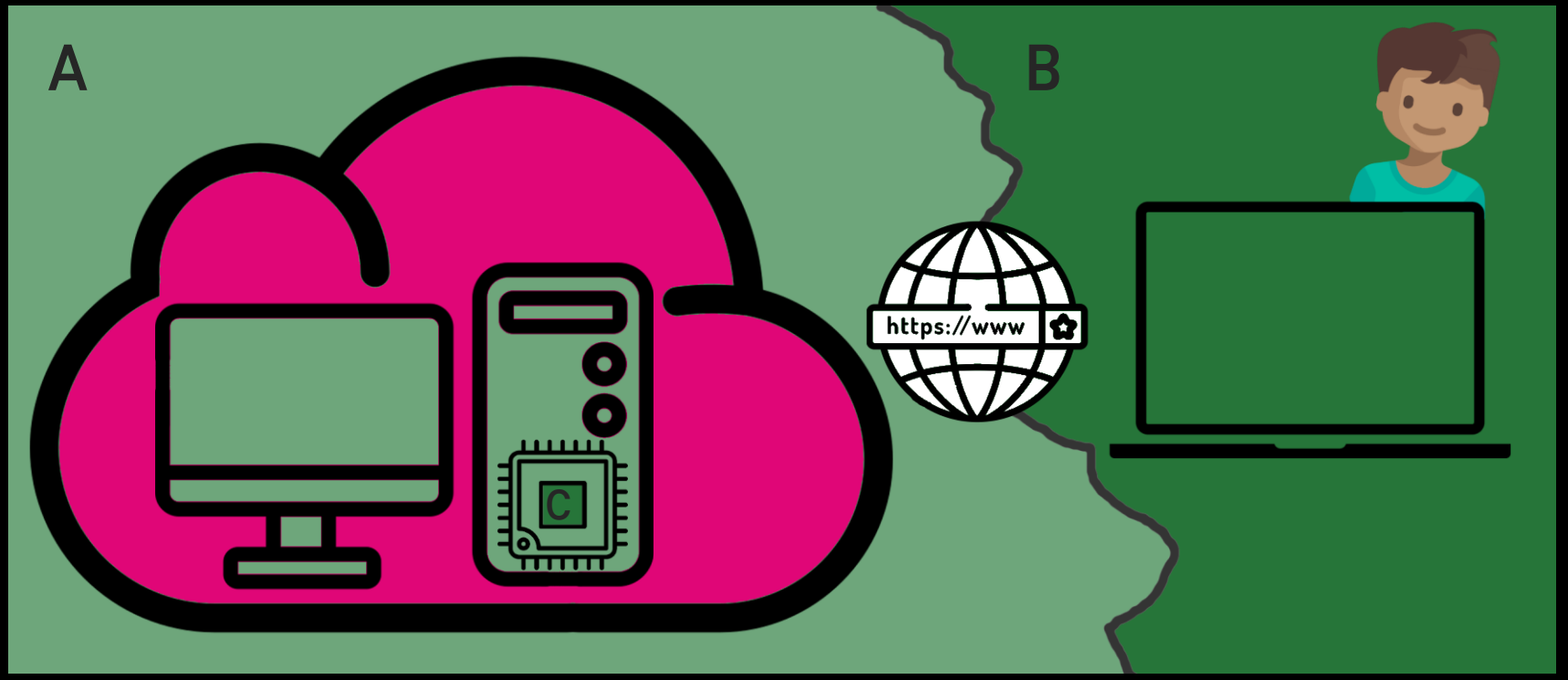
Secure Enclave and the metaphor of a security domain



Bildquelle: wiktionary.org

C represents a security domain of **B** in the environment under the control of **A**

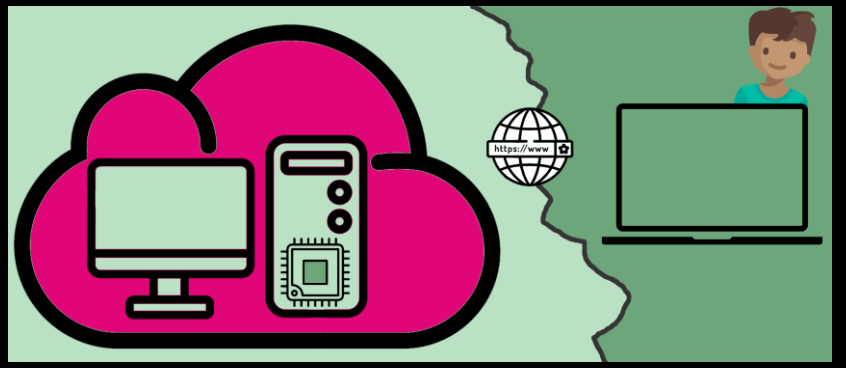
Secure Enclave and the metaphor of a security domain



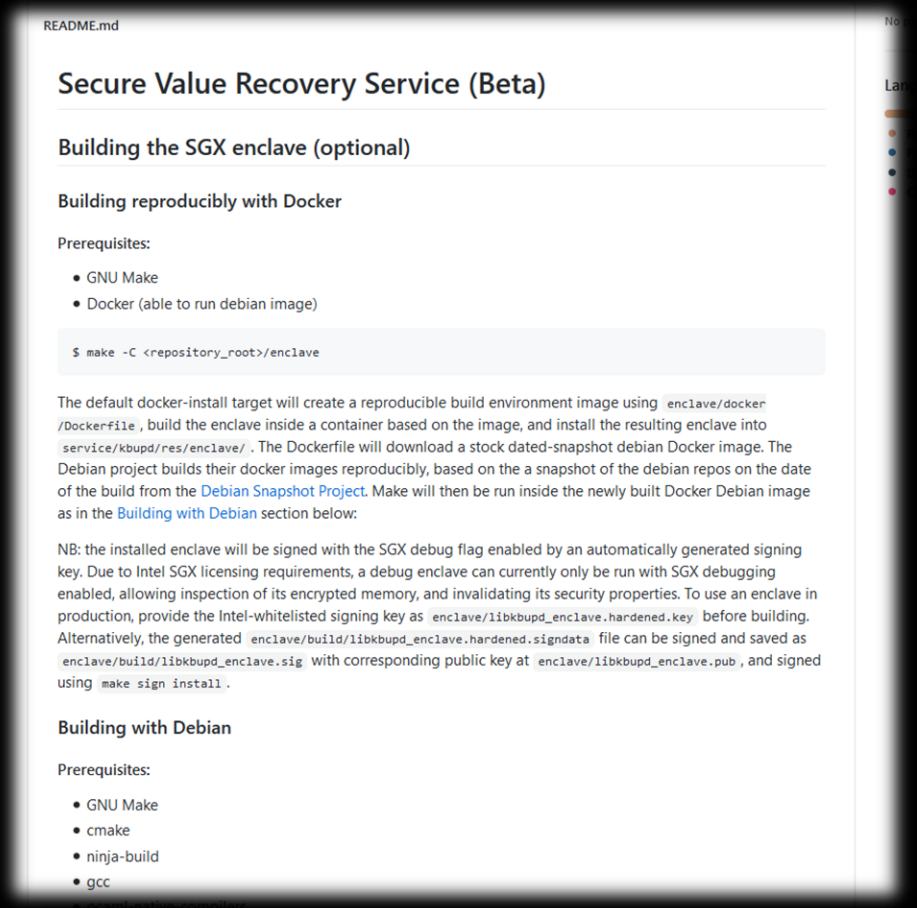
Symbole von freepik.com

Confidential Computing und Secure Enclaves

- **Secure Enclave: in essence a subclass of Trusted Execution Environment (TEE)**
- **Secure Enclaves to protect the *data in use (Confidentiality, Integrity)***
  - Relaxes the trust model against the cloud provider
  - Allows for additional security against administrators
- **Migration of legacy applications is possible**
  - A number of tools/frameworks/libraries are available
  - Migration of complex applications by partitioning out the security critical components into the enclave



Real-world use case: Signal Secure Value Recovery



README.md

Secure Value Recovery Service (Beta)

Building the SGX enclave (optional)

Building reproducibly with Docker

Prerequisites:

- GNU Make
- Docker (able to run debian image)

```
$ make -C <repository_root>/enclave
```

The default docker-install target will create a reproducible build environment image using `enclave/docker/Dockerfile`, build the enclave inside a container based on the image, and install the resulting enclave into `service/kbupd/res/enclave/`. The Dockerfile will download a stock dated-snapshot debian Docker image. The Debian project builds their docker images reproducibly, based on the a snapshot of the debian repos on the date of the build from the Debian Snapshot Project. Make will then be run inside the newly built Docker Debian image as in the Building with Debian section below:

NB: the installed enclave will be signed with the SGX debug flag enabled by an automatically generated signing key. Due to Intel SGX licensing requirements, a debug enclave can currently only be run with SGX debugging enabled, allowing inspection of its encrypted memory, and invalidating its security properties. To use an enclave in production, provide the Intel-whitelisted signing key as `enclave/libkbupd_enclave.hardened.key` before building. Alternatively, the generated `enclave/build/libkbupd_enclave.hardened.signdata` file can be signed and saved as `enclave/build/libkbupd_enclave.sig` with corresponding public key at `enclave/libkbupd_enclave.pub`, and signed using `make sign install`.

Building with Debian

Prerequisites:

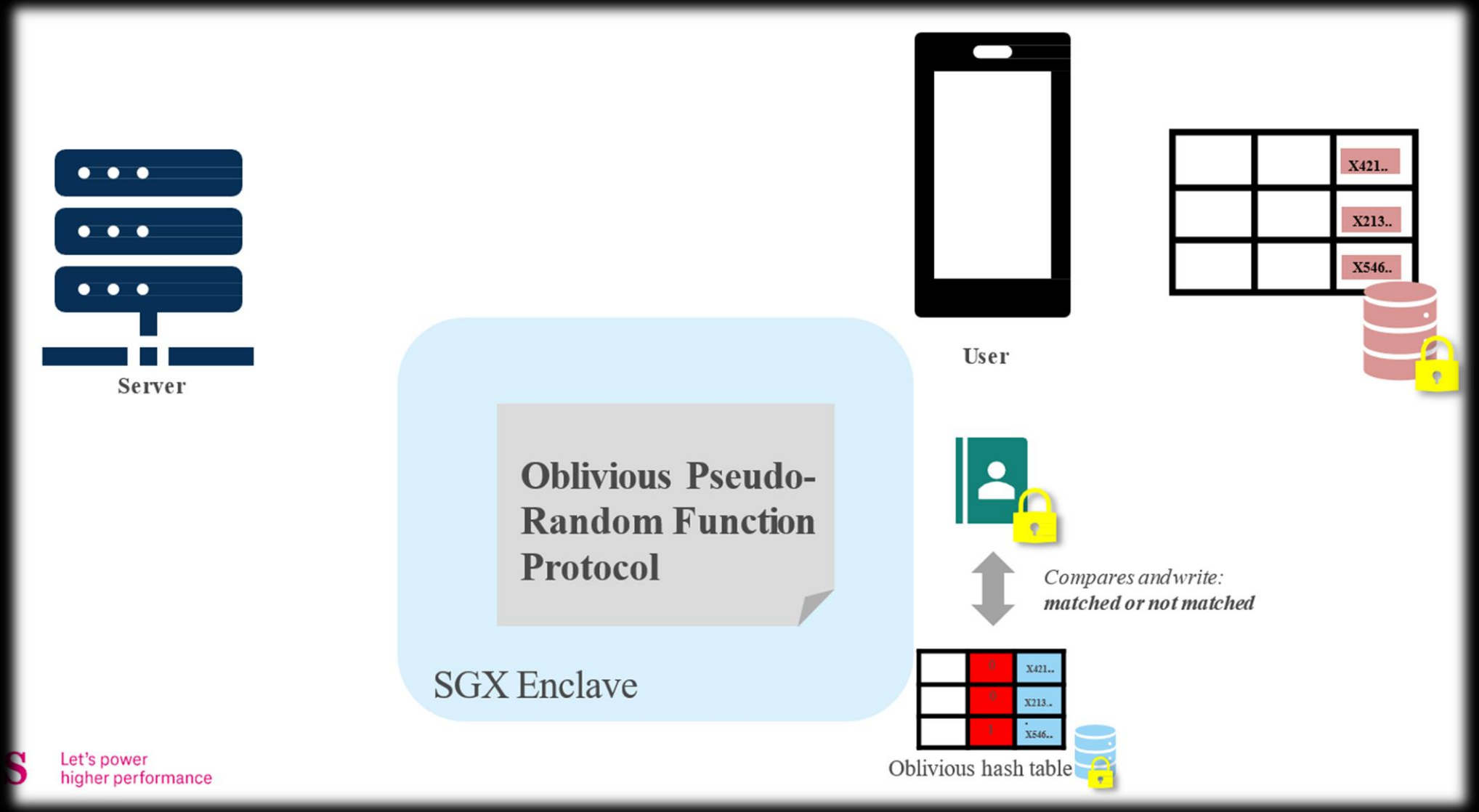
- GNU Make
- cmake
- ninja-build
- gcc

Signal

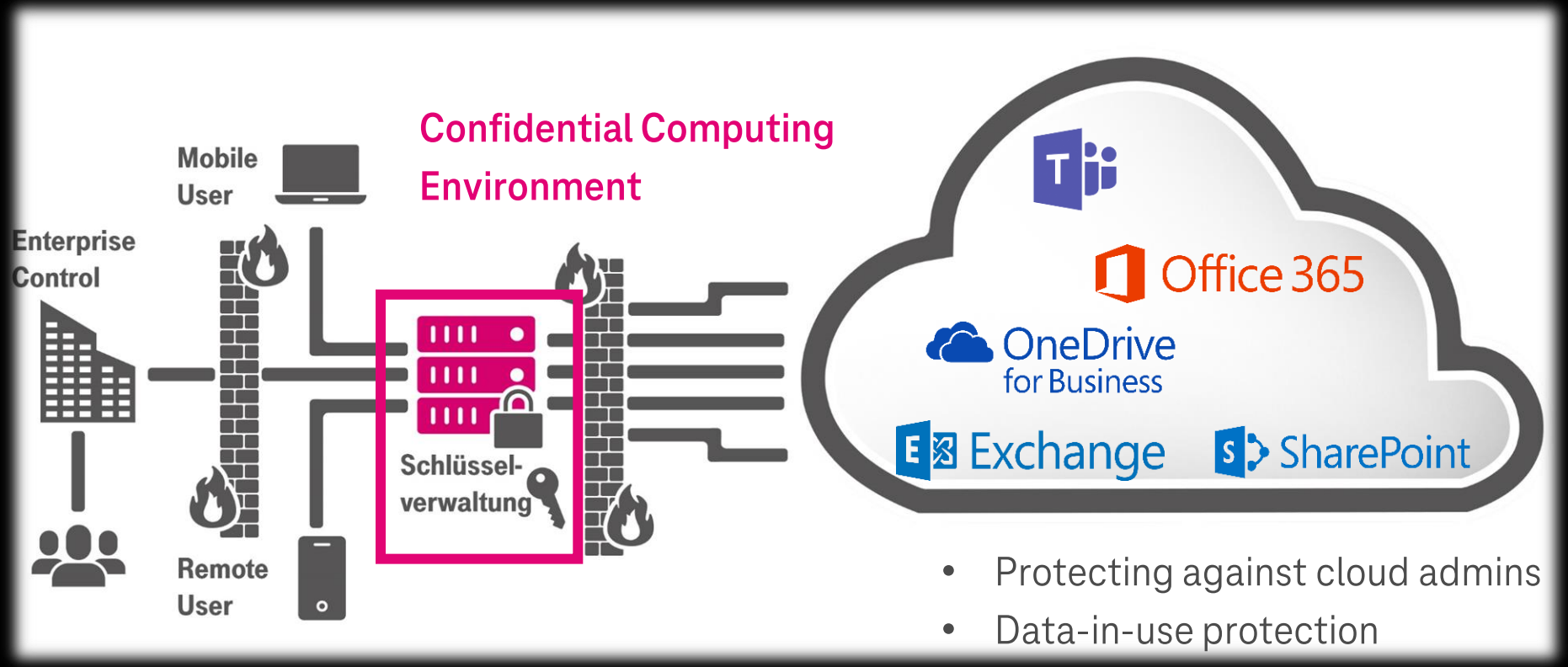
https://github.com/signalapp/SecureValueRecovery/blob/master/README.md

See also https://signal.org/blog/secure-value-recovery/

Signal Secure Value Recovery



Case Study: Cloud Encryption Proxy

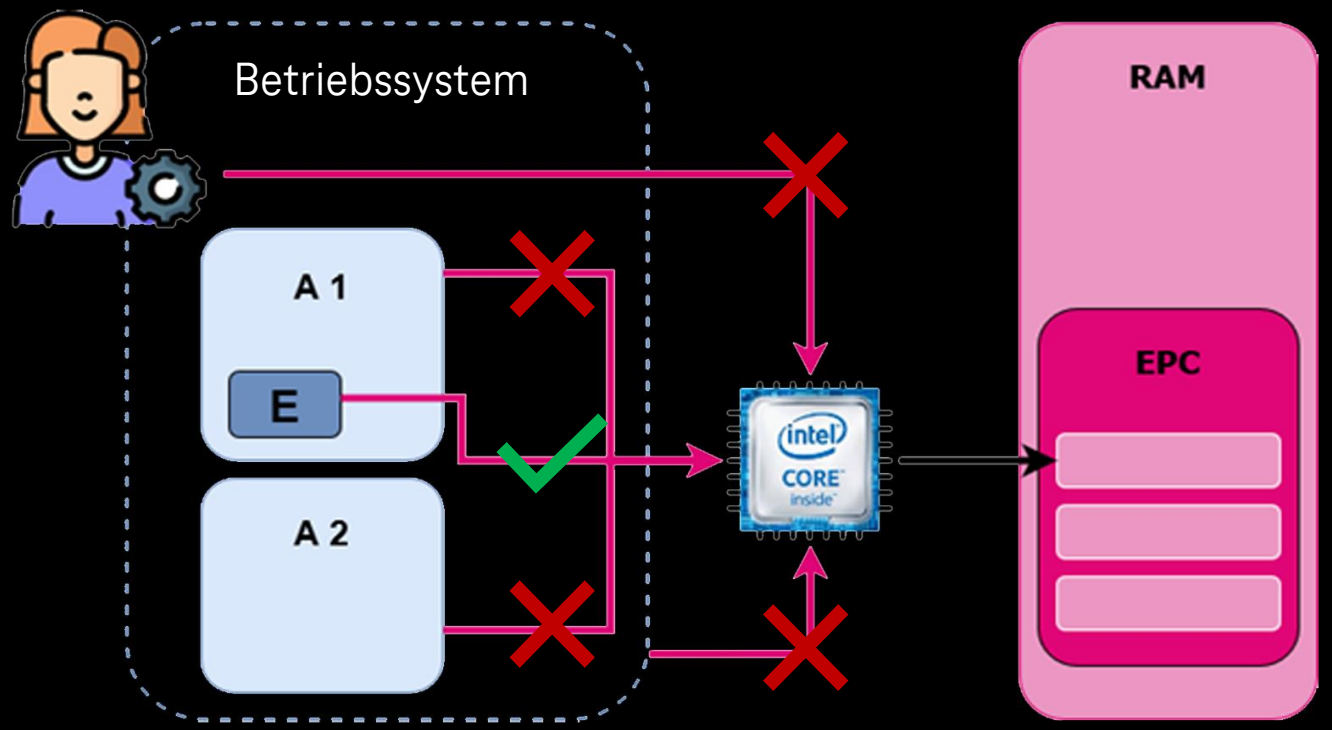


User view (plaintext)	Name: Max Müller Account: 1223123 Blutgruppe: AB Geburtsdatum: 15.06.1980

Name: Tp5. &ql fcj4&kL Account: 378338590 Blutgruppe: AB Geburtsdatum: 08.02.1980	**Data in the cloud (encrypted/ tokenized)**

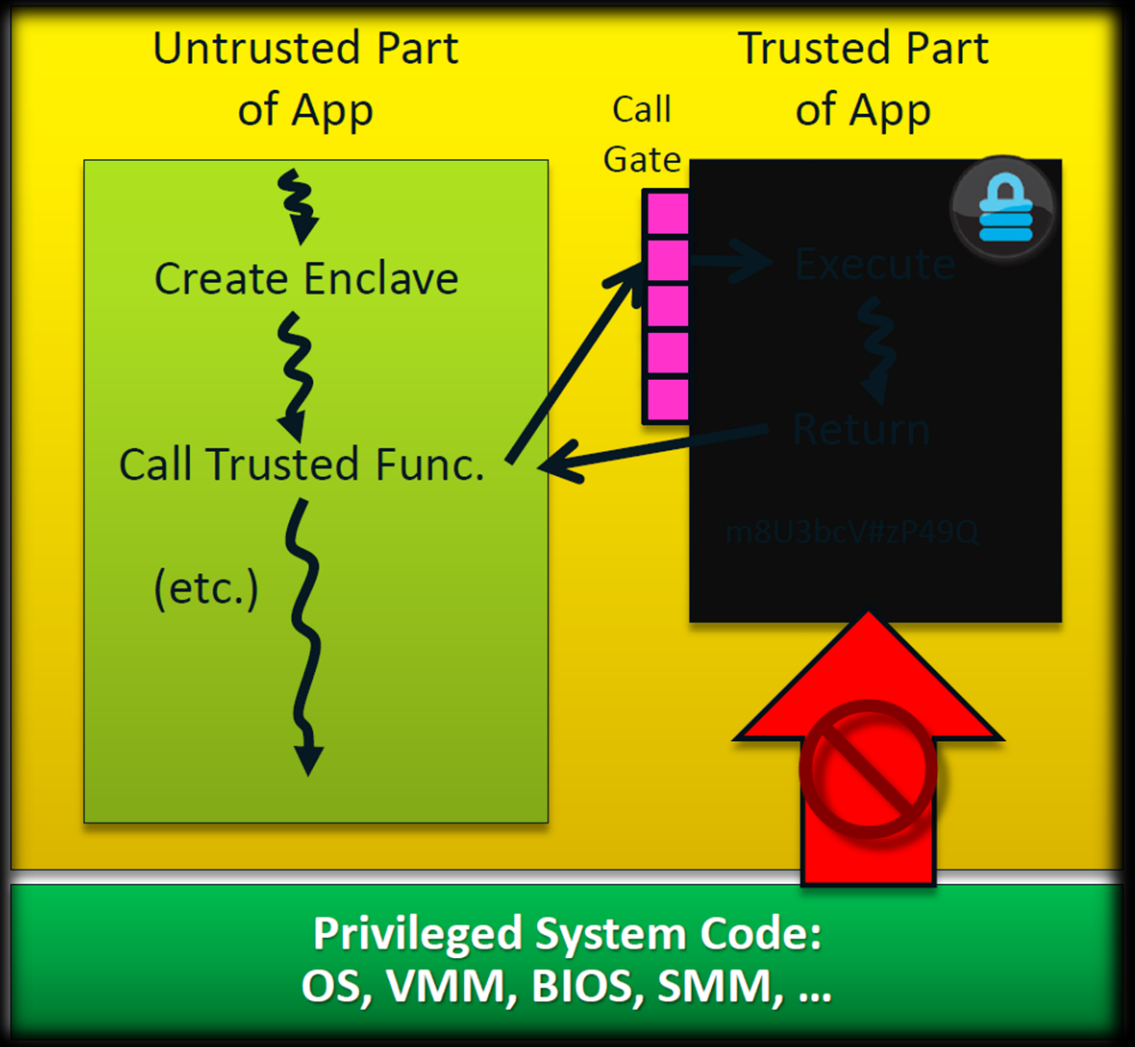
Intel SGX

- SGX = „Software Guard Extensions“
- Extended security-related instruction codes of certain Intel CPU
- Confidential memory areas rendering EPC (Enclave Page Cache); „SGX RAM“



Pictures from freepik.com, youtube.com

The notion of an enclave

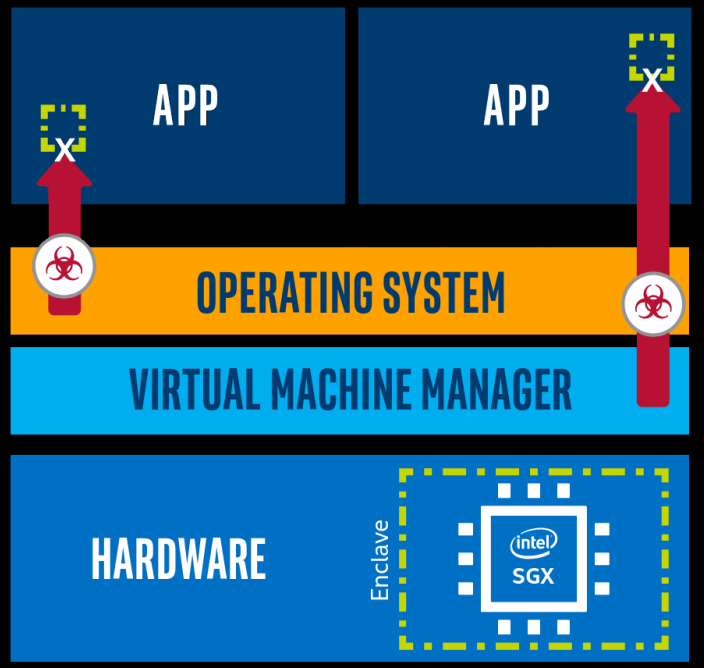


Taken from [Dror Caspi Intel software guard extensions (SGX)]

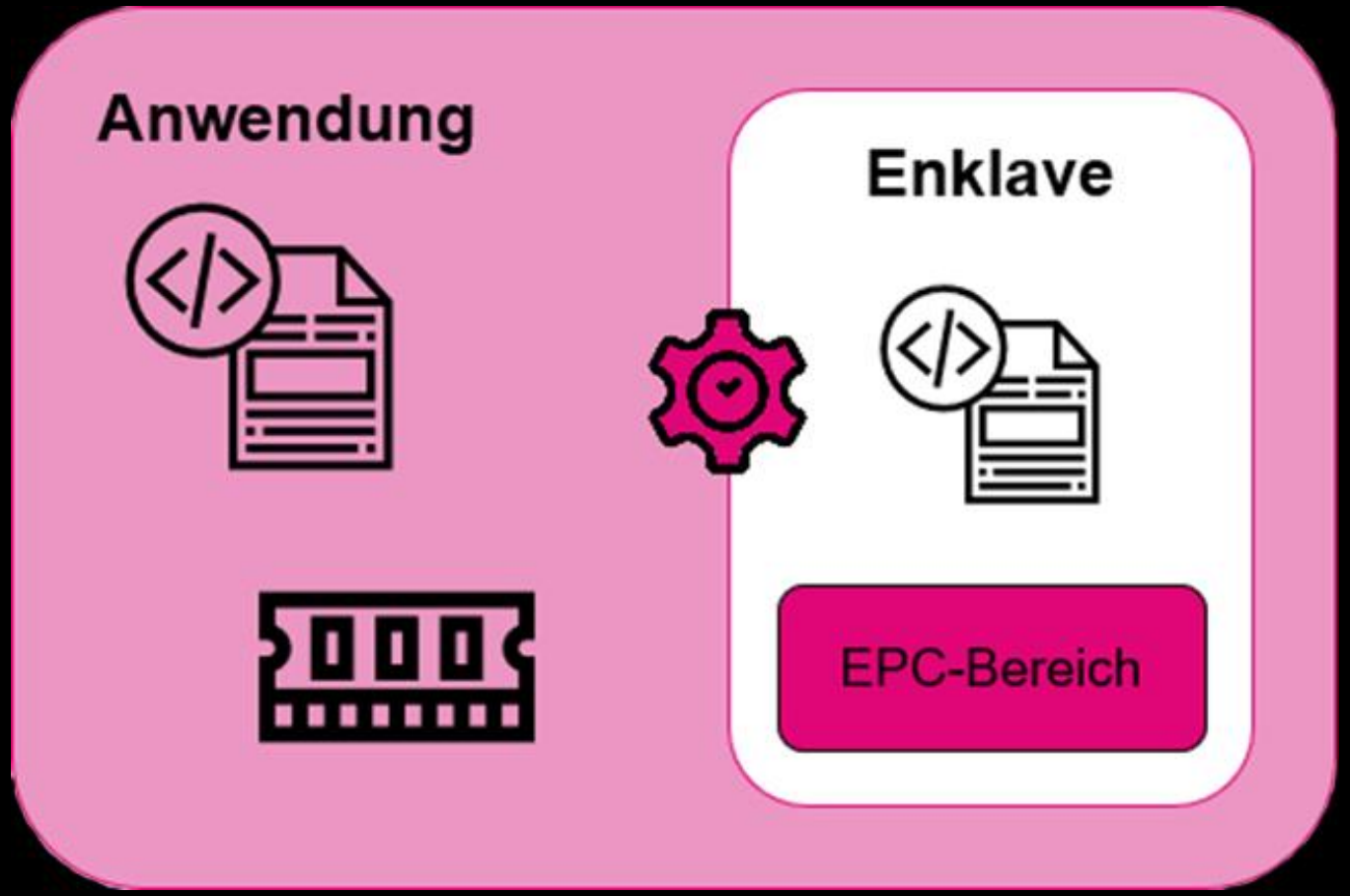
Intel SGX

- **Secure Enclaves to protect the *data in use (Confidentiality, Integrity)***
  - Execute the sensible data inside of secure enclave
  - Relaxes the trust model against the cloud provider
  - Allows for additional security against administrators
  - Espacially interesting in Cloud environment

- **Migration of legacy applications is possible**
  - A number of tools/frameworks/libraries are available
  - Migration of complex applications by partitioning the security critical components into the enclave



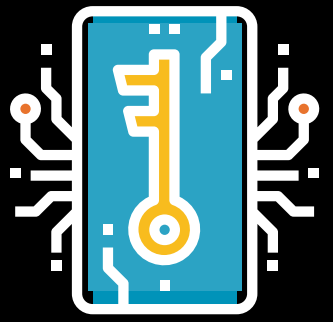
Creation of an SGX Application

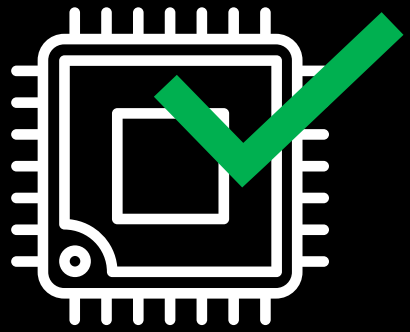


Symbole von freepik.com

Creation of an SGX Application

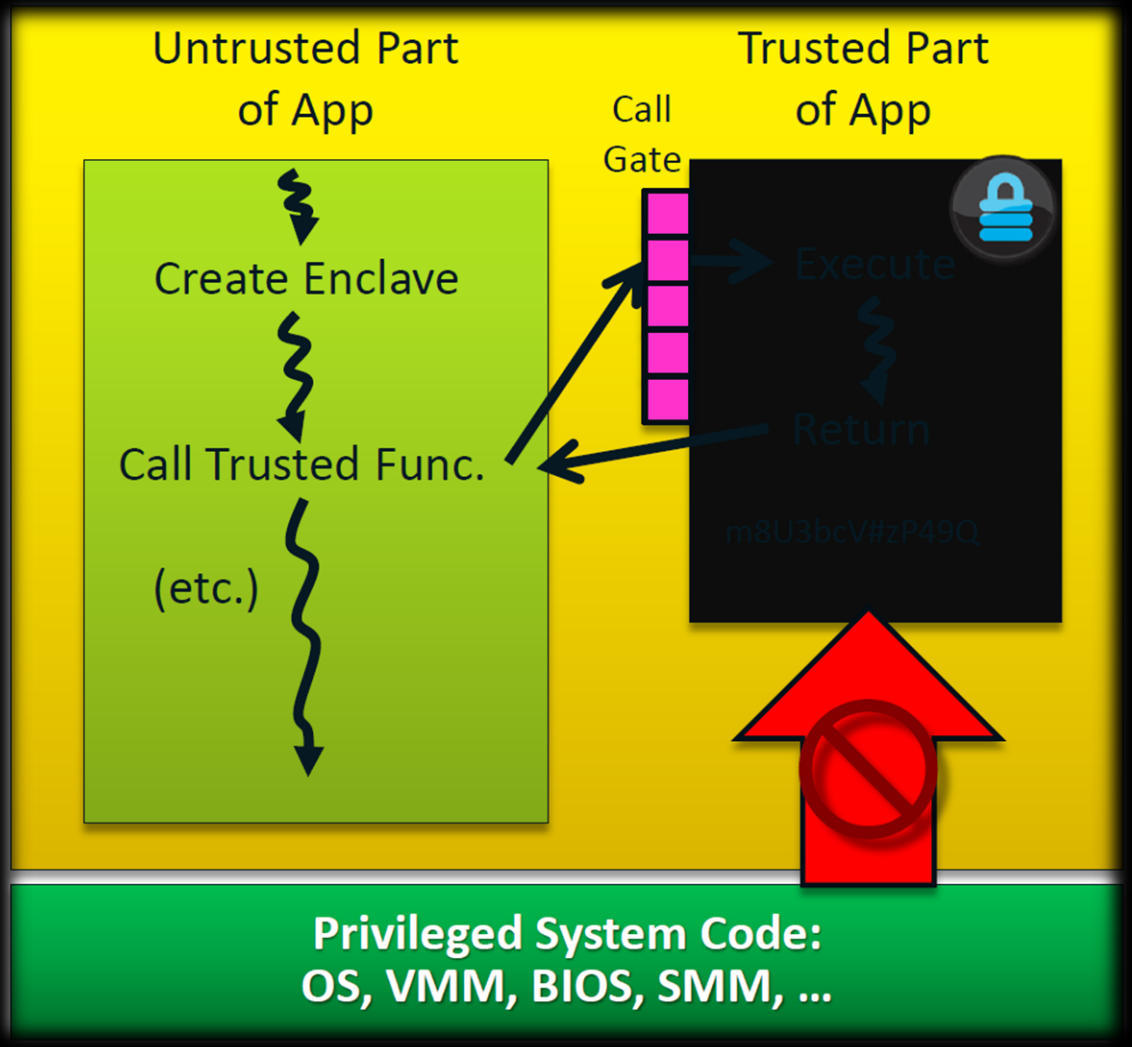
- EPC access only by the respective enclave
- No debugging
- Uninterrupted encryption
- Hardware based *root keys*
- Verification of the enclave and of the execution environment through remote attestation





Application partitioning and TCB implications

Recall:



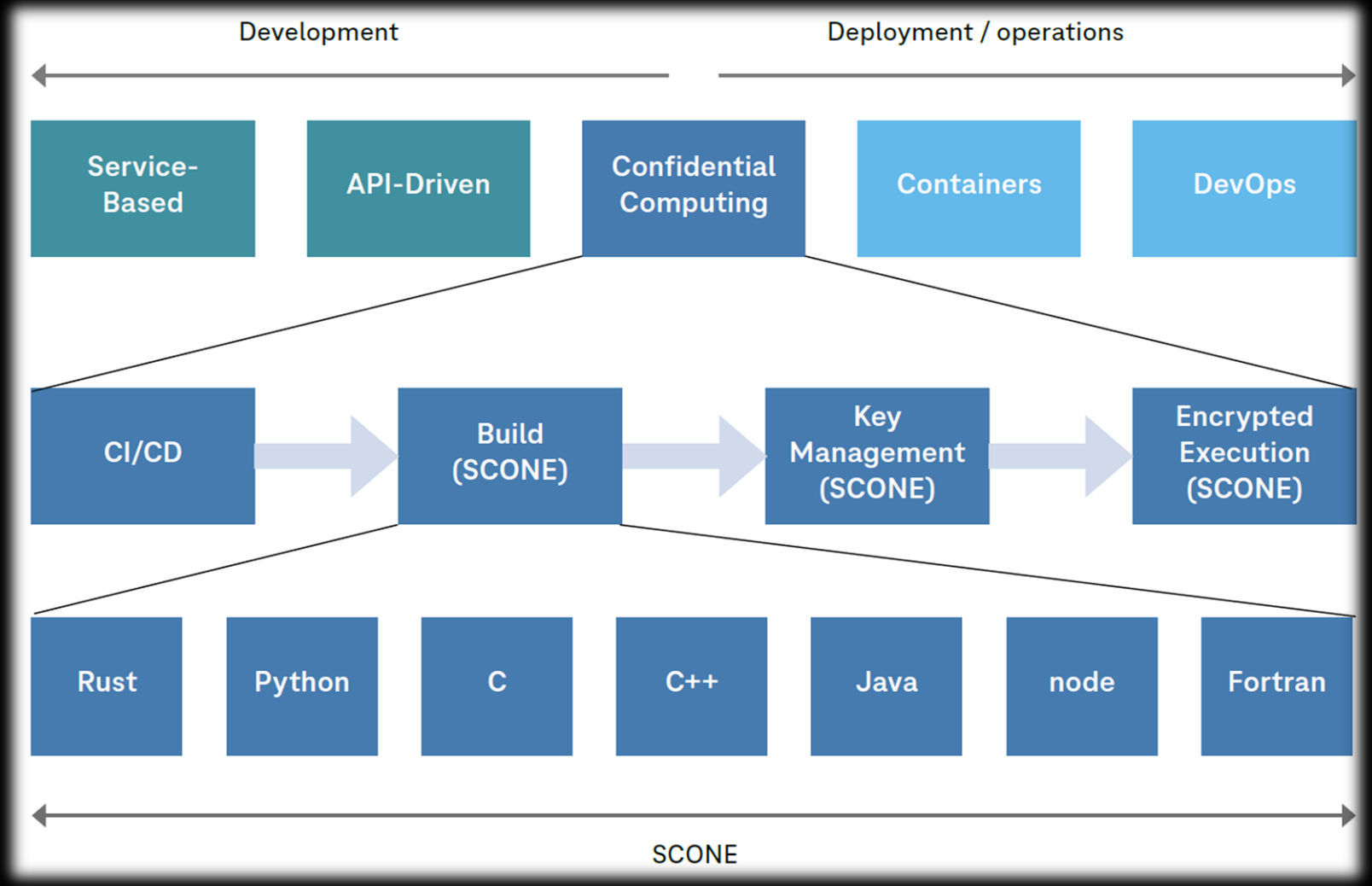
Taken from [Dror Caspi Intel software guard extensions (SGX)]

Application partitioning and TCB implications

M M S EXPERIENCE BEYOND DIGITAL

Confidential App design	Effort	TCB size	Approach/Lib
Partitioning	High	Small	Intel SDK („native“)
Without Partitioning	Low/Middle	Large	Scone, Ego, Gramine

Developing and Deploying Confidential Applications



DevSecOps

Taken from whitepaper: Enemy in the clouds: protecting your cloud, assets from powerful adversaries

M M S

EXPERIENCE
BEYOND
DIGITAL

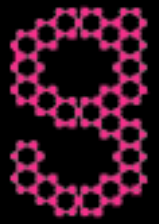
App Migration

Migrating the applications into the enclave infrastructure.

T · · Systems ·

Let's power
higher performance

Frameworks and tools to support app migration



GRAPHENE

Occlum

anjuna

Figures traken from: scontain.com, grapheneproject.io, occlum.io, anjuna.io

M M S EXPERIENCE BEYOND DIGITAL

A practical example

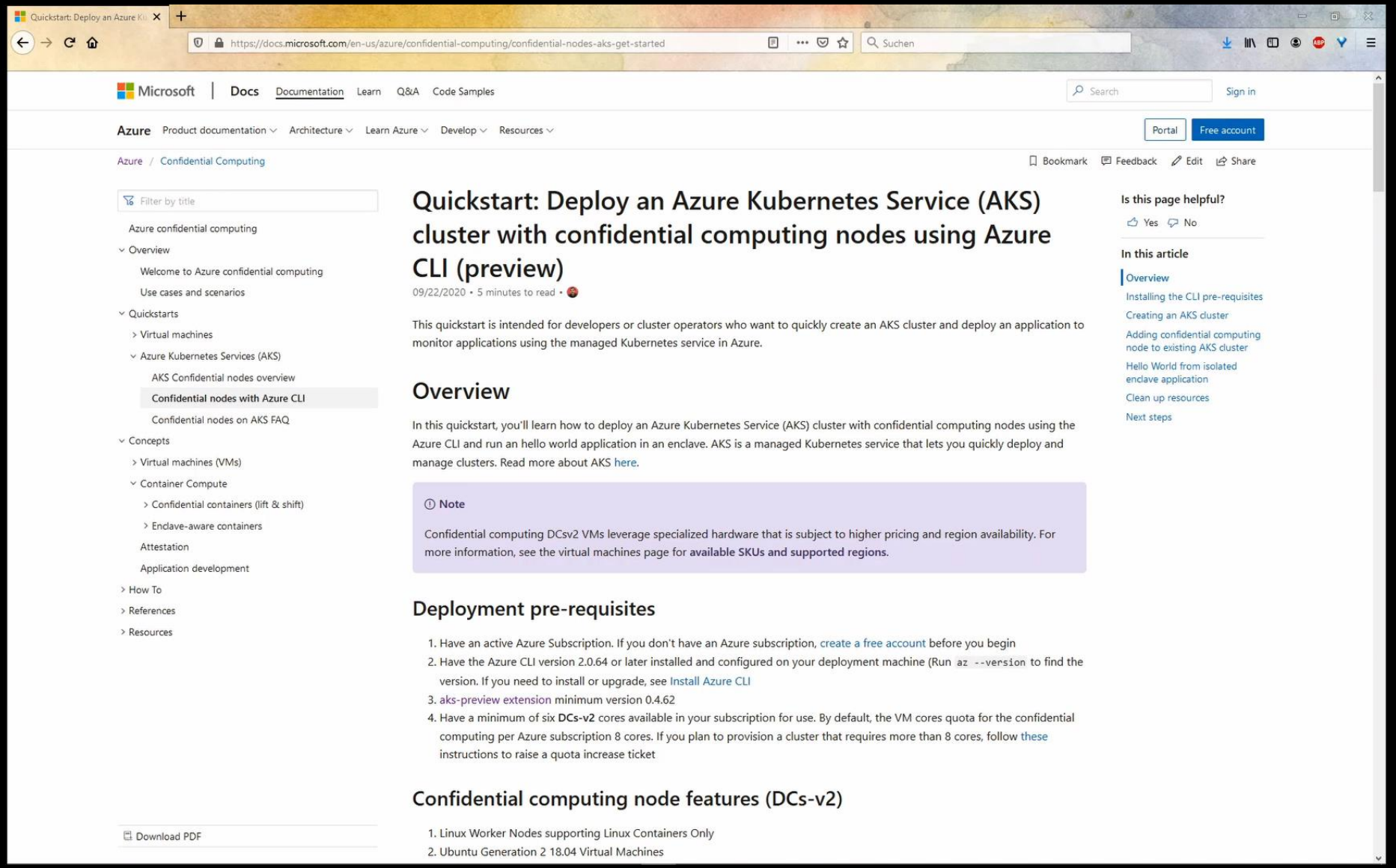
T · · Systems · Let's power higher performance

Confidential Patient Records in the Cloud

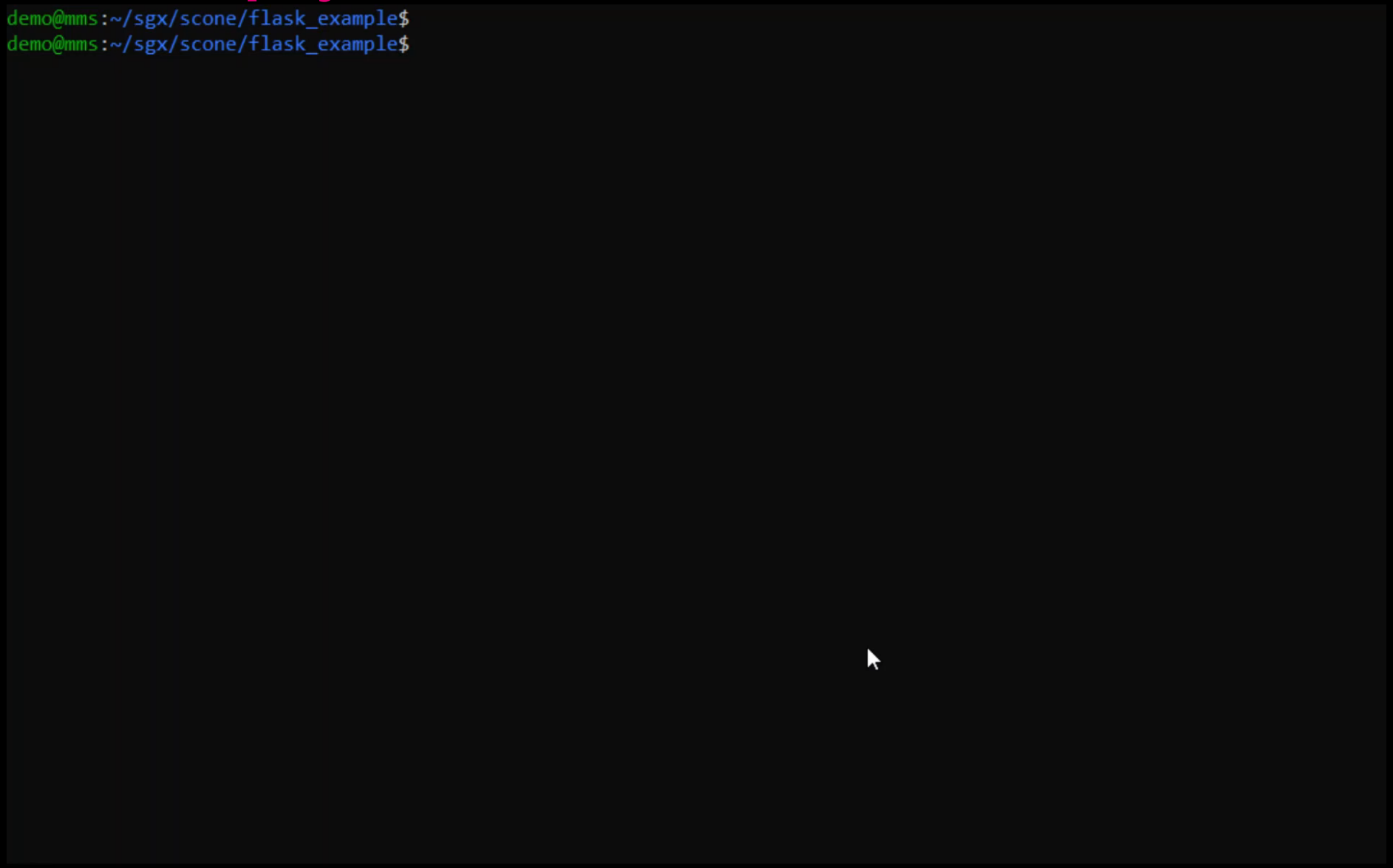
- Confidential Patient Records as a simple key-value database service in the public cloud
- Deployed on Azure Kubernetes Service (AKS) cluster with confidential computing nodes using Azure CLI

Picture source: https://www.ghs.org/wp-content/uploads/2015/11/medical-record.jpg

Demo: Deploy an AKS with CC nodes

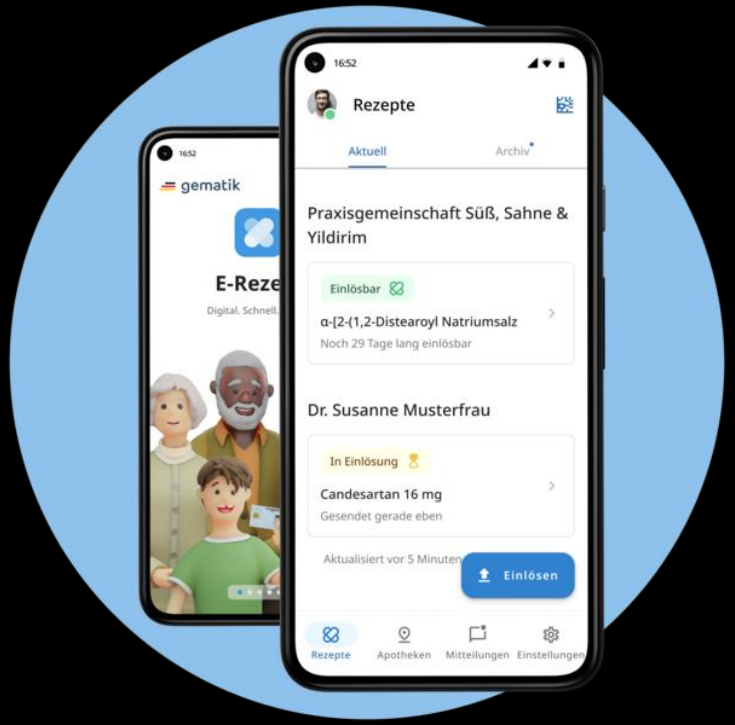


Demo: Application deployment in the enclave



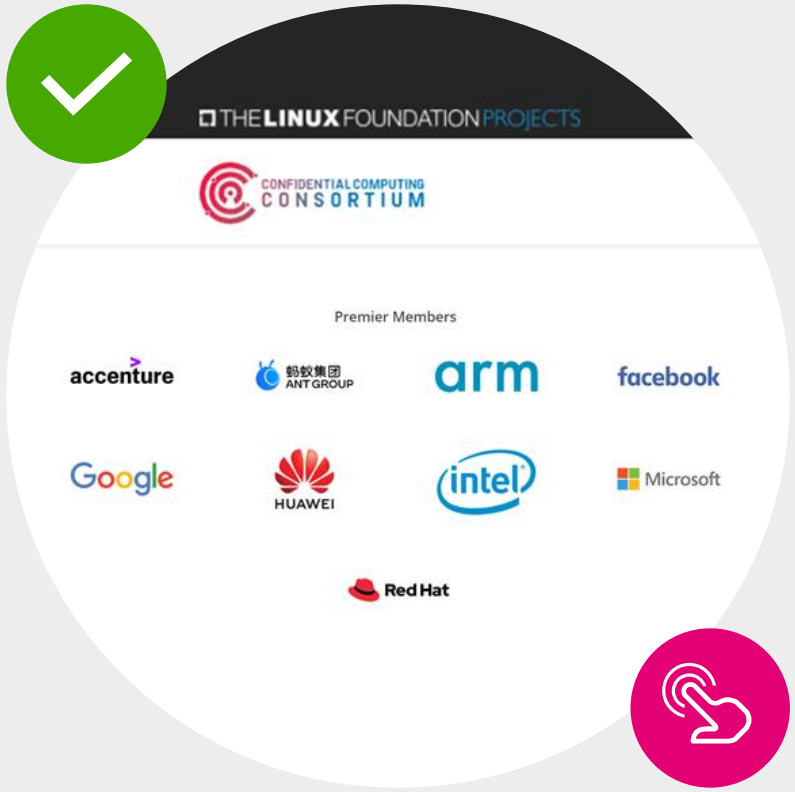
Typical use cases for Confidential Computing

- Digital Rights Management
- Cloud-based operation of e-prescriptions (eRezept)
- Handover of Ambulance Service → Hospital
- Outsourcing Organ Donation Data
- Key and Access Control Management (e.g. Vault)
- Privacy-preserving Data Analytics
- Federated Learning
- Multi-Party Computation
- Email Encryption Proxy



https://www.gematik.de/media/erezept/_processed_/7/e/csm_gematik_App_Mockup_Startseite_01_cj_e983d21f8e.png

Availability of Confidential Computing



Azure

Open Telekom Cloud

Confidential Compiting: Beyond Intel SGX

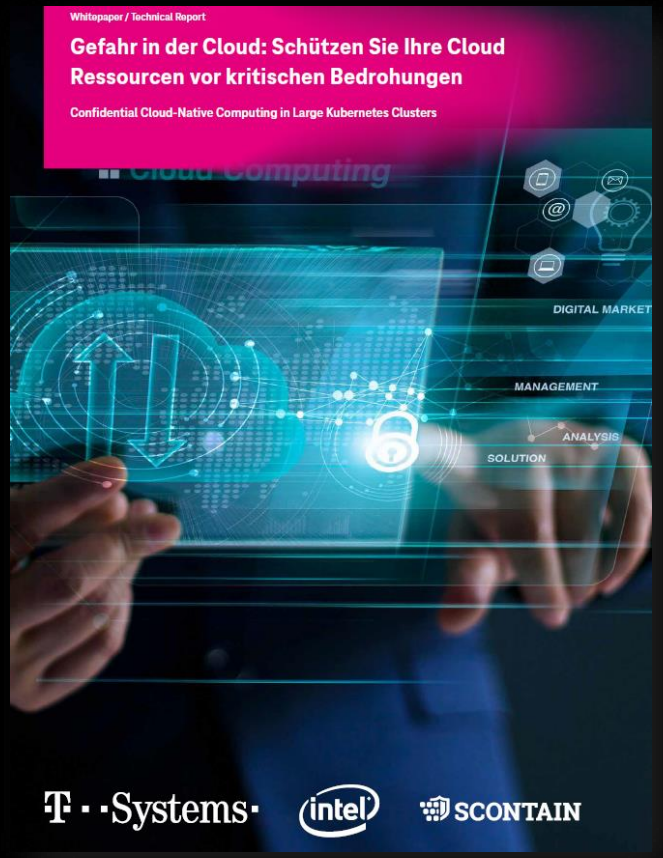
M M S EXPERIENCE BEYOND DIGITAL

- Intel SGX
- Intel TDX
- AMD SEV SNMP
- Arm TrustZone
- SGX and SEV are already available on e.g. Azure

Confidential Computing: an important innovation topic

https://www.youtube.com/watch?v=CCPI7C1lhh0

https://www.youtube.com/watch?v=pv6e1izDcj0



https://www.t-systems-mms.com/expertise/downloads/whitepaper-confidential-cloud-native-computing.html

M M S

EXPERIENCE
BEYOND
DIGITAL

Thank you

For your attention!

T · · Systems ·

Let's power
higher performance