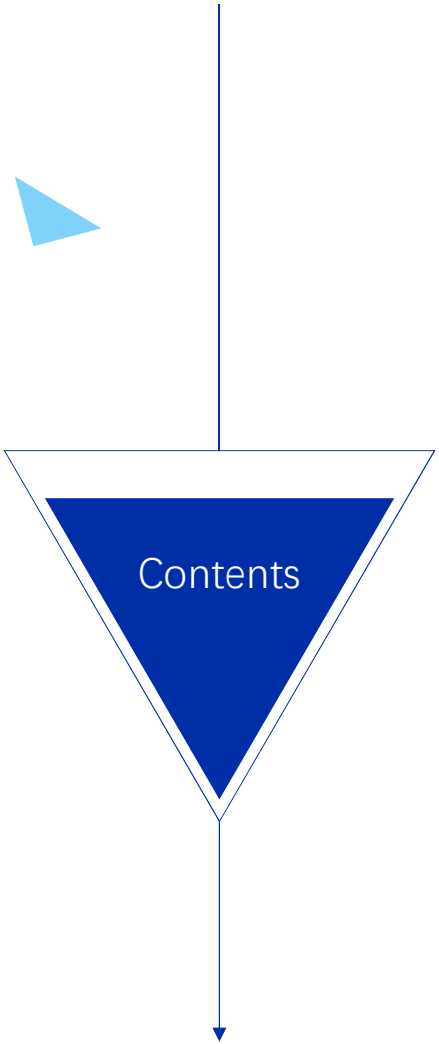
secGear

openEuler Unified Confidential Computing Framework

openEuler sig-confidential-computing maintainer Guijin Gao

openEuler



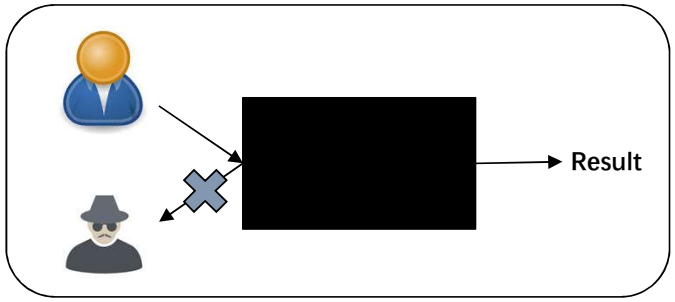
openEuler

1 What’s Confidential Computing

openEuler

What’ s Confidential Computing

Confidential computing technology emerges to resolve the problem that data-in-use is difficult to protect. Confidential computing can be simply abstracted as follows: Put running data into a black box, and an application can request related computations, but cannot take any confidential data out of the box.



Confidential computing hardware solutions are available on several chips:

- Intel: SGX、MKTME
- ARM: Trustzone
- RISC-V: keystone

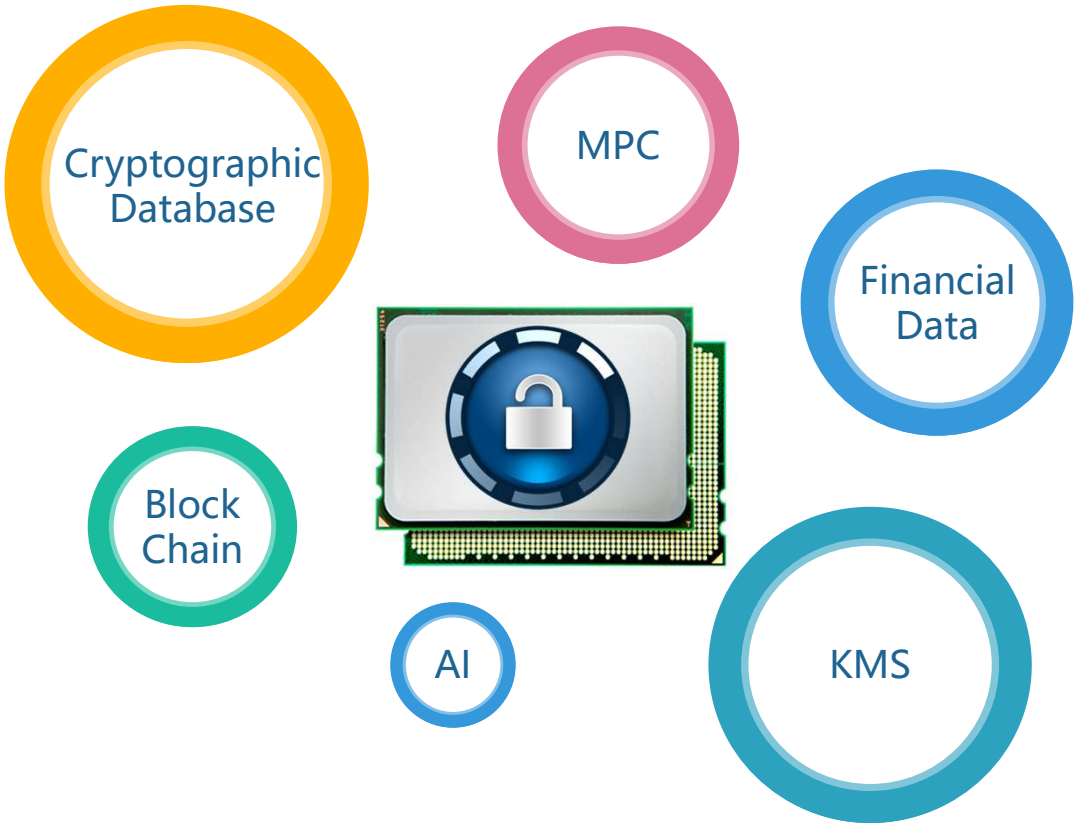
Design is different between different hardware architectures, for example:

The SGX partitions some memory addresses as secure containers to ensure the security of the memory in the addresses.

Trustzone, on the other hand, constructs two bounds, secure and insecure worlds, through time-division multiplexing of CPUs.

What’ s Confidential Computing

In the public cloud scenario, how to securely migrate private data to the public cloud is the focus of various industries. Confidential computing is a good fit.



openEuler

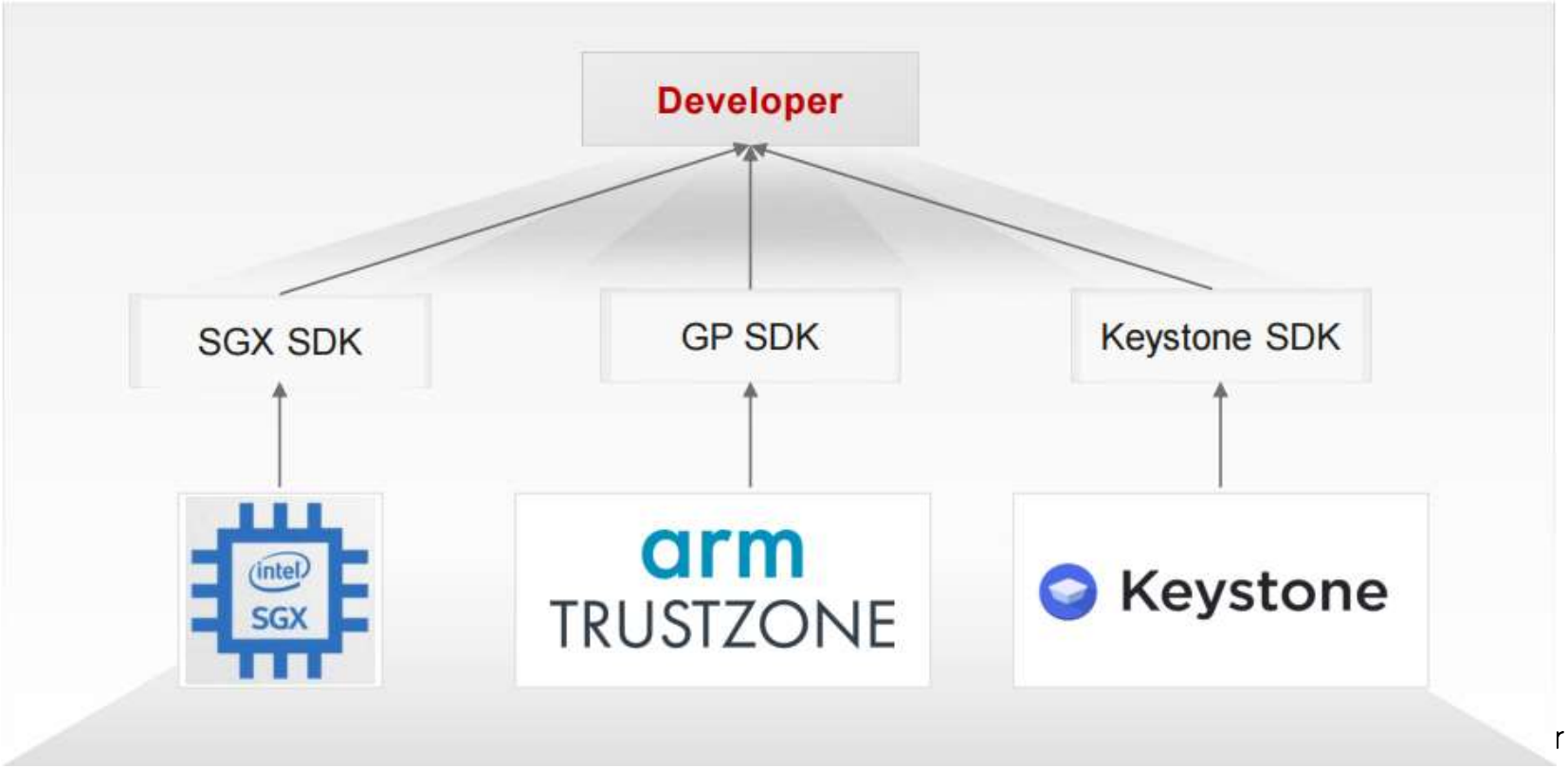
2 Multi-architecture Pain Points of Confidential Computing

openEuler

Multi-architecture Pain Points of Confidential Computing

Confidential computing involves a variety of industries, and different industries have different requirements for confidential computing frameworks. Confidential computing solutions developed by different chips vary from implementation principles to external interfaces.

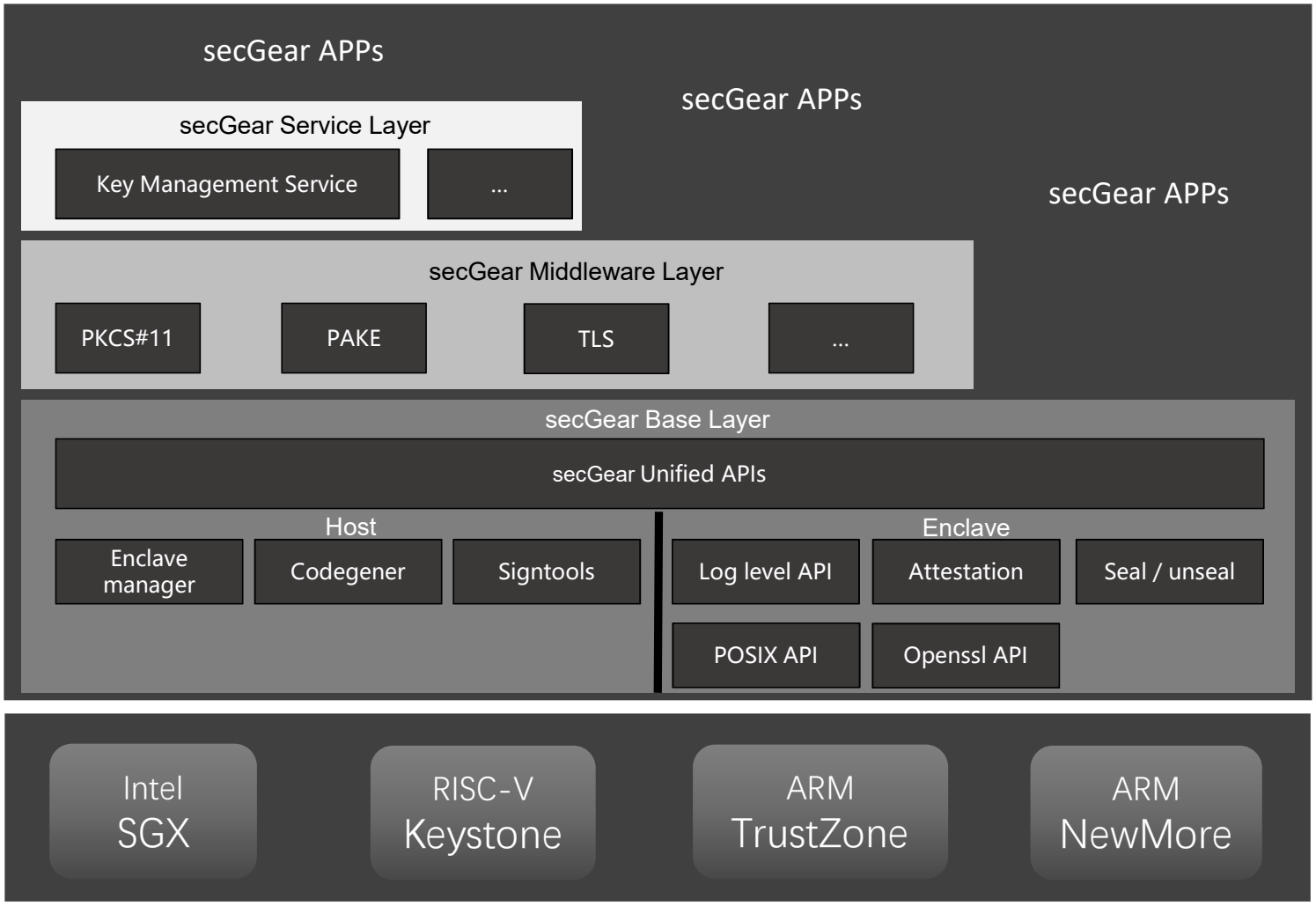
- Poor compatibility
- Ecological isolation
- High maintenance costs



3 secGear Framework

openEuler

secGear Framework



- **Service Layer**
  - key Management Service
- **Middleware Layer**
  - Provides the PKCS#11 key management interface.
  - PAKE Key Exchange Protocol
  - TLS Secure Link Protocol
- **Base Layer**
  - Lifecycle Management Interface
  - Intermediate code auxiliary generation tool
  - Provides data sealing and authentication capabilities
  - Supports standard C libraries and OpenSSL interfaces.

openEuler

secGear Framework

secGear Base Layer

secGear provides rich enclave development interfaces and tools at the base layer and supports C POSIX APIs and standard OpenSSL interfaces on the security side. Users can freely develop secure applications based on these interfaces. secGear tries to achieve the following objectives:

- The programming experience on the security side is the same as that on the non-security side.
- Consistent programming experience in different architectures

secGear Framework

secGear Base Layer Brings New Programming Experiences

Helloworld Item	Intel SGX	Trustzone Global Platform
Trusted App Creation	sgx_create_enclave	TEEC_InitializeContext TEEC_OpenSession TA_CreateEntryPoint TA_OpenSessionEntryPoint
Trusted App Destroy	sgx_destroy_enclave	TEEC_CloseSession TEEC_FinalizeContext TA_CloseSessionEntryPoint TA_DestroyEntryPoint
hello_world Calling	Write EDL file to call hello_world	Define CMD ID Construct parameters TEEC_InvokeCommand TA_InvokeCommandEntryPoint Call hello_world

Helloworld Item	secGear	
	Intel SGX	Trustzone Global Platform
Trusted App Creation	cc_enclave_create	
Trusted App Destroy	cc_enclave_destroy	
hello_world Calling	Write EDL file to call hello_world	

openEuler

secGear Framework

secGear Middleware Layer

The secGear provides rich security middleware components. Users can use these middleware to implement normal world program coding without being aware of security-side programming.

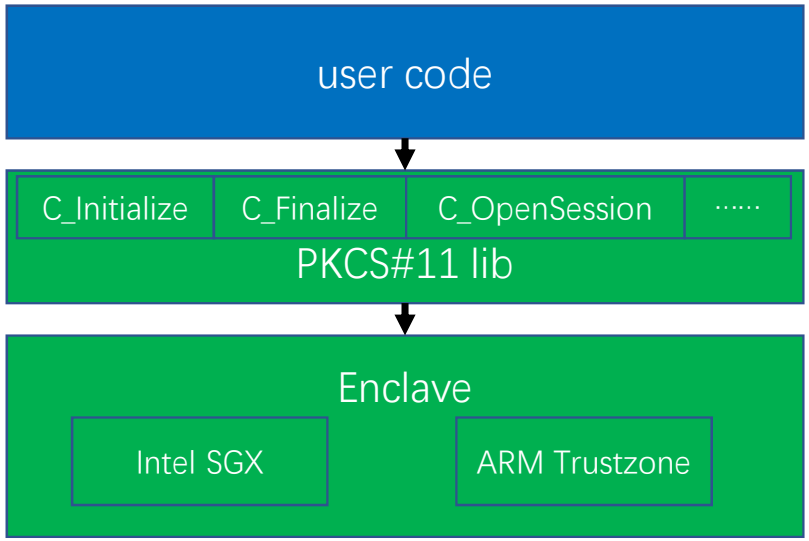
PKCS#11: uses the TEE environment as the backend encryption device and provides standard PKCS#11 interfaces.

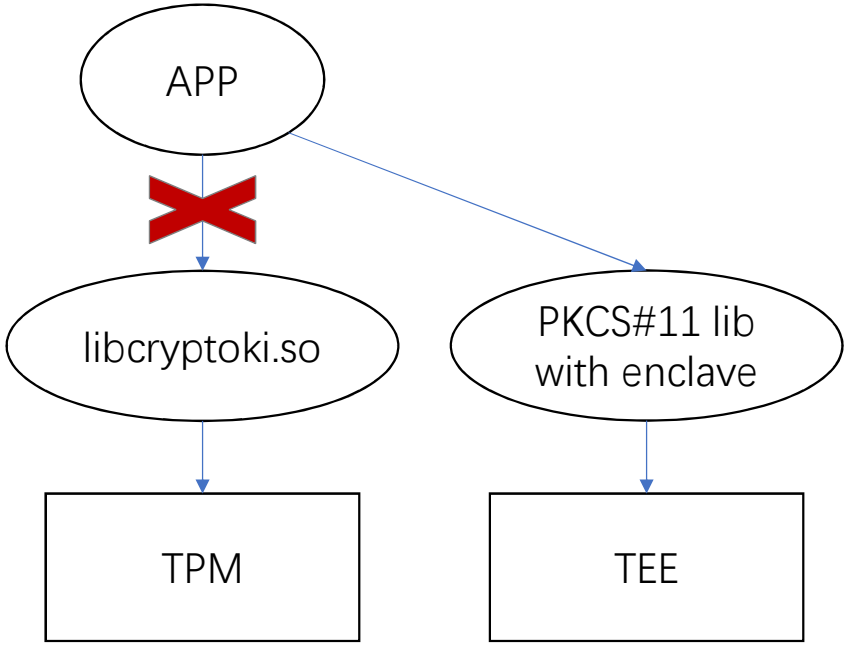
TLS: provides secure transmission protocols for direct interaction between the TEE and clients. TLS is widely used in scenarios such as secure database.

PAKE: PAKE provides a TEE-based key exchange protocol for device-cloud synergy scenarios.

secGear Framework

secGear Middleware Layer





openEuler

secGear Framework

secGear Service Layer

At the service layer, secGear provides services enhanced by enclave, including the key management service EKMS.

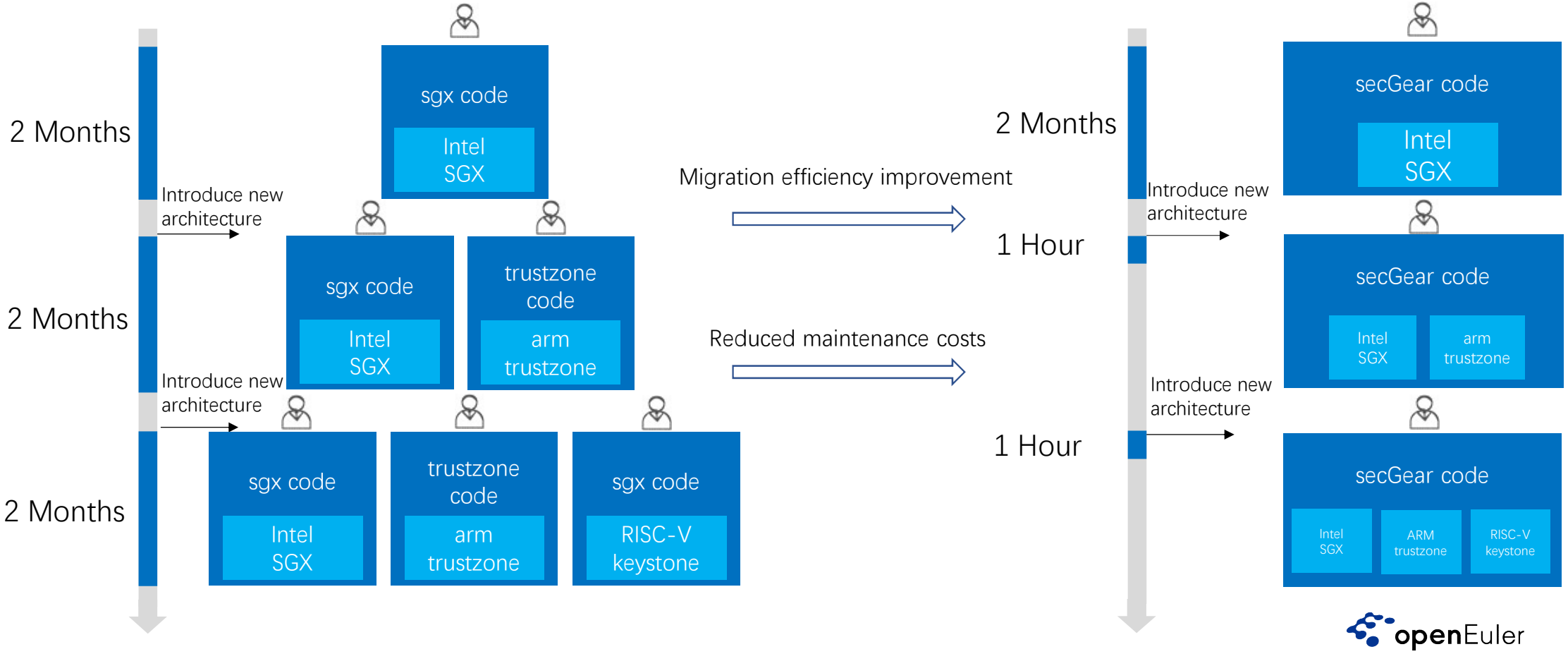
Scenario	Security analysis	EKMS Solution
Key storage	The key storage of many applications is costly, unsecure, and difficult to manage.	KMS provides highly reliable and secure centralized key generation, hosting, and subsequent management services based on enclave.
Sensitive data storage	Data encryption provides protection, but cannot ensure the security of the encryption key.	The EKMS provides multiple protection functions, such as data key management and permission control, after data keys are encrypted and stored.

4 secGear Makes Confidential Computing Simple

openEuler

secGear Makes Confidential Computing Simple

Developing confidential computing applications based on secGear greatly shortens the development, migration, and adaptation time and reduces maintenance costs.



secGear Makes Confidential Computing Simple

- Base Layer: standard interfaces and free development
- Middleware Layer: standard components and free integration
- Service Layer: standard services, ready to use

openEuler

Thank you!

openEuler

Welcome to follow

Sina Webo：openEuler Community　Twitter：openEuler　BiliBili：openEuler　WeChat public account：openEuler

Community

openEuler

https://openeuler.org

Code hosting

gitee

https://gitee.com/openeuler

WeChat group

Add the helper microsignal "openeuler123" to pull you into the group.

THANKS

openEuler