Confidential Computing on AWS

Urban Jurca

But first!

DEVOPS

DAYS LJUBLJANA

-> AWS User Group members get early bird discount! Send email to dodljubljana@gmail.com

-> Call for papers is open https://www.papercall.io/dod-ljubljana

Sept 28 2024

A little bit about me

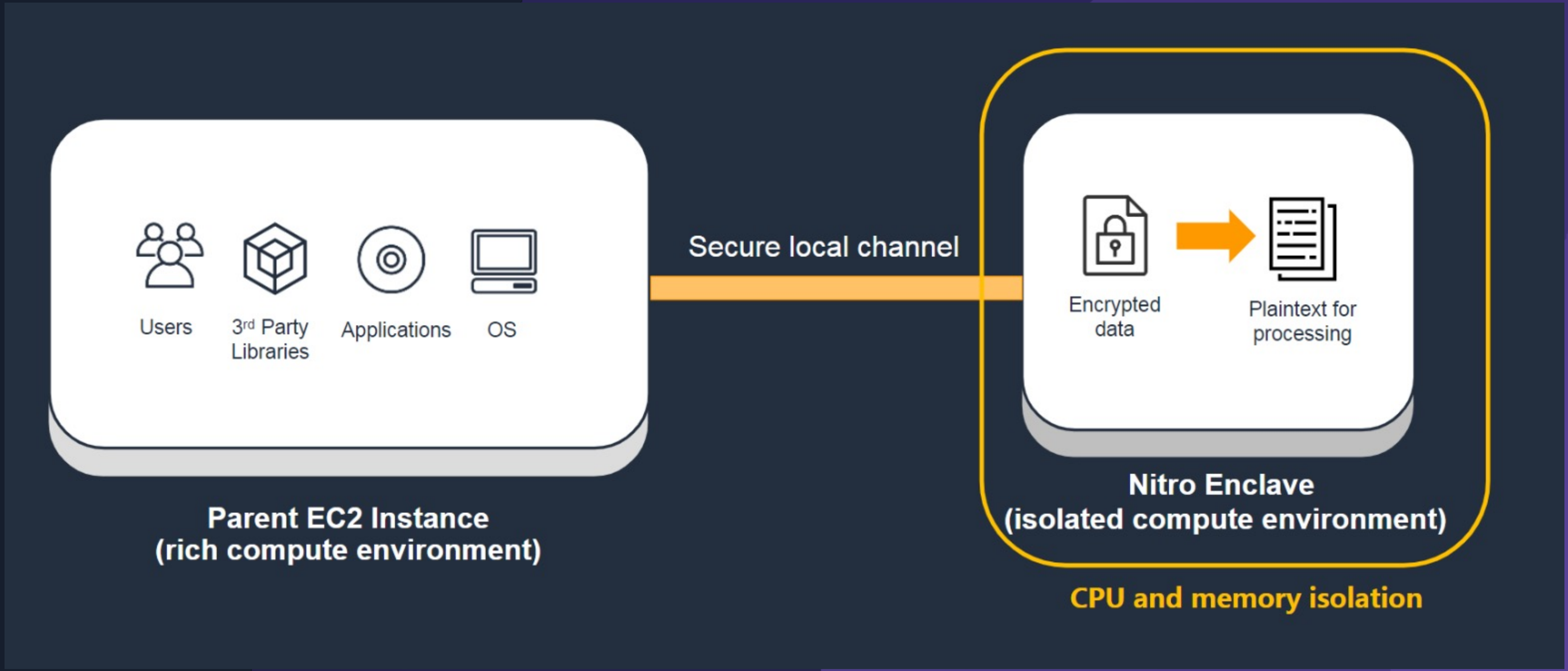
- DevOps consultant, specialized in exchange, custody and blockchain tech
- In a previous life: VP of Devops, Head of Infra
- Kitesurfer, avid MTBer, guitarist, dad!

Why do we need confidential computing

?

WTH is an AWS Nitro Enclave?

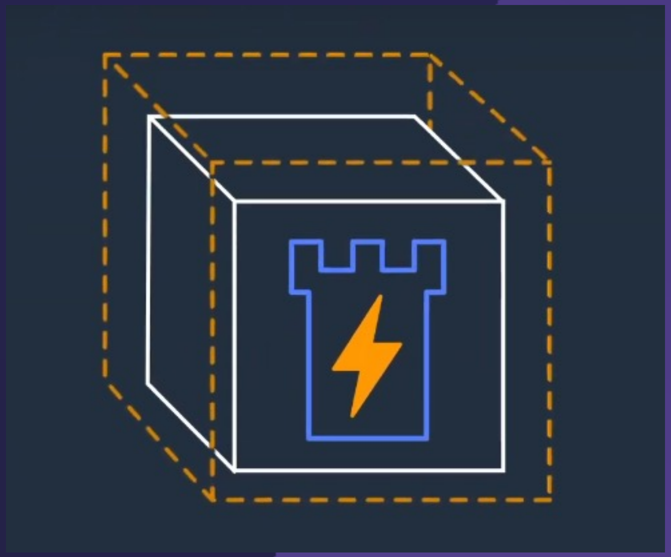
Enclave ➡️ isolated execution environment



WTH is an AWS Nitro Enclave?

Enclaves:

- Are separate, hardened, and highly-constrained virtual machines
- Provide only secure local socket connectivity with their parent instance
- Have no persistent storage, interactive access, or external networking
- Users cannot SSH into an enclave, and the data and applications inside the enclave cannot be accessed by the processes, applications, or users (root or admin) of the parent instance



Benefits

Additional isolation and security

Cryptographic attestation

Flexible

Use Cases

Securing Private Keys

Tokenization

MPC

Requirements and Considerations

- → Parent instance must be **Nitro** based
  - → Intel or AMD with at least 4 vCPUs
  - → long list of exclusions
- → Parent instance must run Linux or Windows
- → Enclave can only run Linux

Requirements and Considerations

** Limited region support

** Up to 4 enclaves per parent instance

** Enclave communicates only with its parent, no cross enclave communication

** Enclaves are active only while parent is running

** Hibernation not supported

Lets talk about concepts

Enclave

„An enclave is a virtual machine with its own kernel, memory, and CPUs. It is created by partitioning memory and vCPUs from a Nitro-based parent instance. An enclave has no external network connectivity, and no persistent storage. The enclave's isolated vCPUs and memory can't be accessed by the processes, applications, kernel, or users of the parent instance.“

Lets talk about concepts

Enclave ID

„An enclave ID is a unique identifier across AWS. It consists of the parent instance ID and an identifier for each enclave created by the instance. For example, an enclave created by a parent instance with an ID of i-1234567890abcdef0 could have an enclave ID of i-1234567890abcdef0-enc9876543210abcde.“

Lets talk about concepts

Parent instance

„The parent instance is the Amazon EC2 instance that is used to allocate CPU cores and memory to the enclave. The resources are allocated to the enclave for the duration of its lifetime. The parent instance is the only instance that can communicate with its enclave.“

Lets talk about concepts

Enclave image file

„An enclave image file (.eif) includes a Linux operating system, libraries, and enclave applications that will be booted into an enclave when it is launched.“

Lets talk about concepts

AWS Nitro Enclaves CLI

„The AWS Nitro Enclaves CLI (Nitro CLI) is a command line tool that is used to create, manage, and terminate enclaves. The Nitro CLI must be installed and used on the parent instance.“

Lets talk about concepts

AWS Nitro Enclaves SDK

„The AWS Nitro Enclaves SDK is an open-source library that you can use to develop enclave applications, or to update existing applications to run in an enclave. The SDKs also integrate with AWS KMS and provide built-in support for cryptographic attestation and other cryptographic operations.“

Lets talk about concepts

Cryptographic attestation

„Cryptographic attestation is the process that an enclave uses to prove its identity and build trust with an external service. Attestation is accomplished using a signed attestation document that is generated by the Nitro Hypervisor. The values in an enclave's attestation document can be used as a condition for an authorization decision by an external party. AWS KMS allows you to use attestation document values in conditions keys to grant access to specific cryptographic operations.“

Lets talk about concepts

Attestation document

„An attestation document is generated and signed by the Nitro Hypervisor. It contains information about the enclave, including platform configuration registers (PCRs), a cryptographic nonce, and additional information that you can define. It can be used by an external service to verify the identity of an enclave and to establish trust. You can use the attestation document to build your own cryptographic attestation mechanisms, or you can use it with AWS KMS, which provides built-in support for authorizing cryptographic requests based on values in the attestation document.“

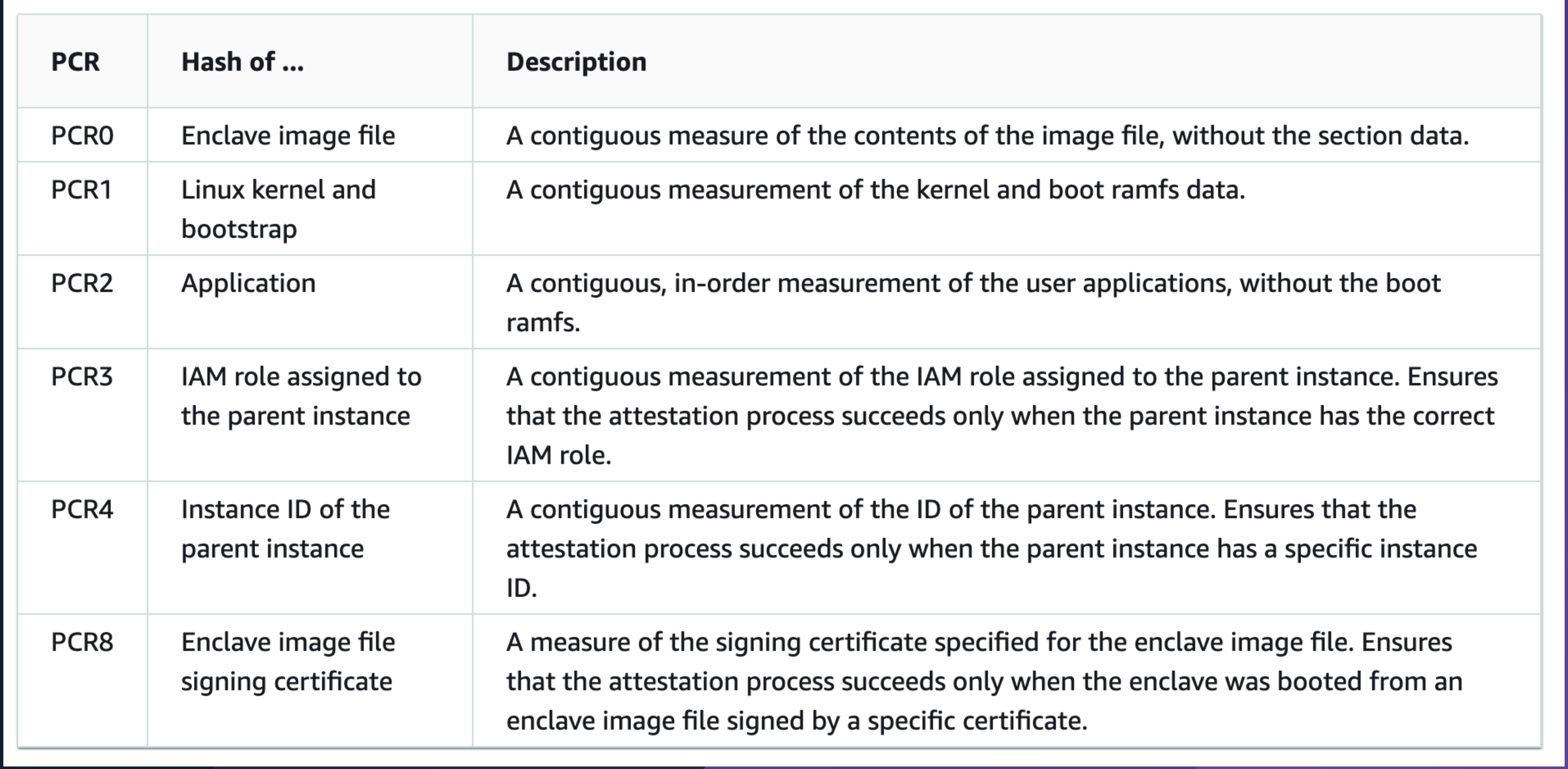
Lets talk about concepts

Platform configuration registers

„Platform configuration registers (PCRs) are cryptographic measurements that are unique to an enclave. Some PCRs are automatically generated when the enclave is created, and they can be used to verify that no changes have been made to the enclave since it was created. You can also manually create additional PCRs that can be used to ensure that the enclave is running on the instance on which you expect it to run. PCRs are included in the attestation document that is generated by the Nitro Hypervisor. You can use PCRs to create condition keys for AWS KMS keys. „

Lets talk about concepts

Platform configuration registers



PCR	Hash of ...	Description
PCR0	Enclave image file	A contiguous measure of the contents of the image file, without the section data.
PCR1	Linux kernel and bootstrap	A contiguous measurement of the kernel and boot ramfs data.
PCR2	Application	A contiguous, in-order measurement of the user applications, without the boot ramfs.
PCR3	IAM role assigned to the parent instance	A contiguous measurement of the IAM role assigned to the parent instance. Ensures that the attestation process succeeds only when the parent instance has the correct IAM role.
PCR4	Instance ID of the parent instance	A contiguous measurement of the ID of the parent instance. Ensures that the attestation process succeeds only when the parent instance has a specific instance ID.
PCR8	Enclave image file signing certificate	A measure of the signing certificate specified for the enclave image file. Ensures that the attestation process succeeds only when the enclave was booted from an enclave image file signed by a specific certificate.

Lets talk about concepts

KMS Proxy

„The KMS proxy is used by enclaves running in a parent instance to call AWS KMS through the parent instance's networking. The proxy ships with Nitro CLI and it runs on the parent instance. The proxy is required only if you use AWS KMS as your key management service and you perform AWS KMS operations (kms-decrypt, kms-generate-data-key, and kms-generate-random) using the Nitro Enclaves SDK. Sessions with KMS are established logically between AWS KMS and the enclave itself, and all session traffic is protected from the parent instance and from other enclaves.“

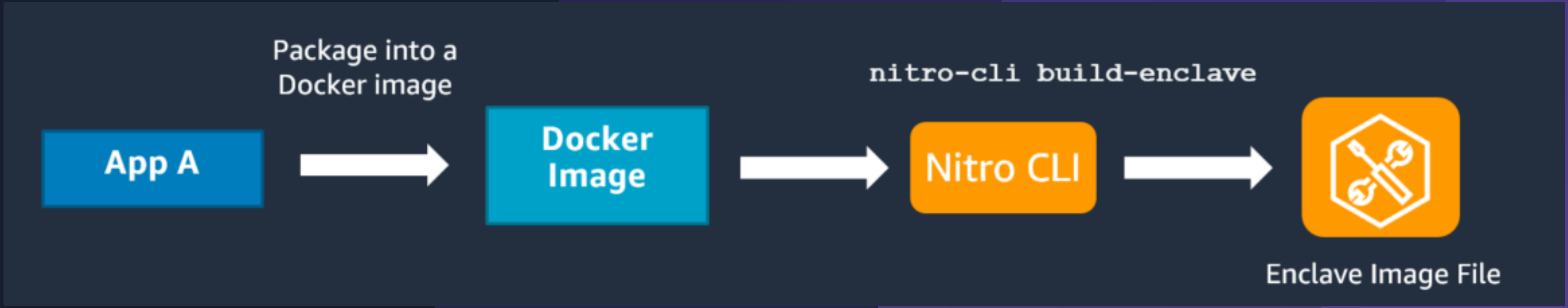
Lets talk about concepts

Vsock

„Vsock is a local communication channel between a parent instance and its enclaves. It is the only channel of communication that an enclave can use to interact with external services. An enclave launched from a parent instance will share the vsock with other enclaves launched from the same parent instance. An enclave's vsock address is defined by a context identifier (CID) that you can set when launching an enclave. Each enclave running on a parent instance gets a unique CID. The CID used by the parent instance is always 3.“

Demo time – Nitro CLI

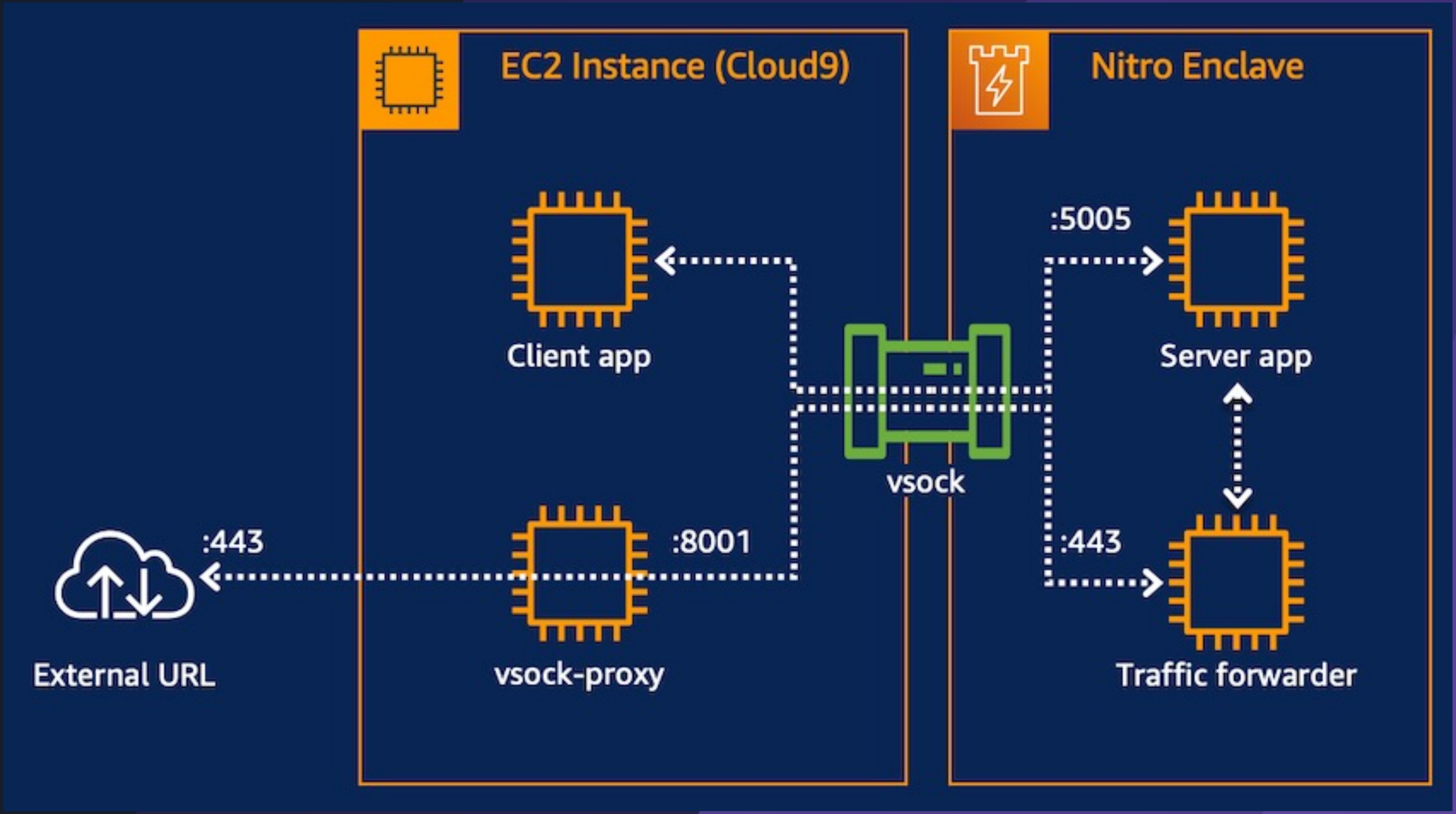
Build and run an Enclave!



```
nitro-cli build-enclave
```

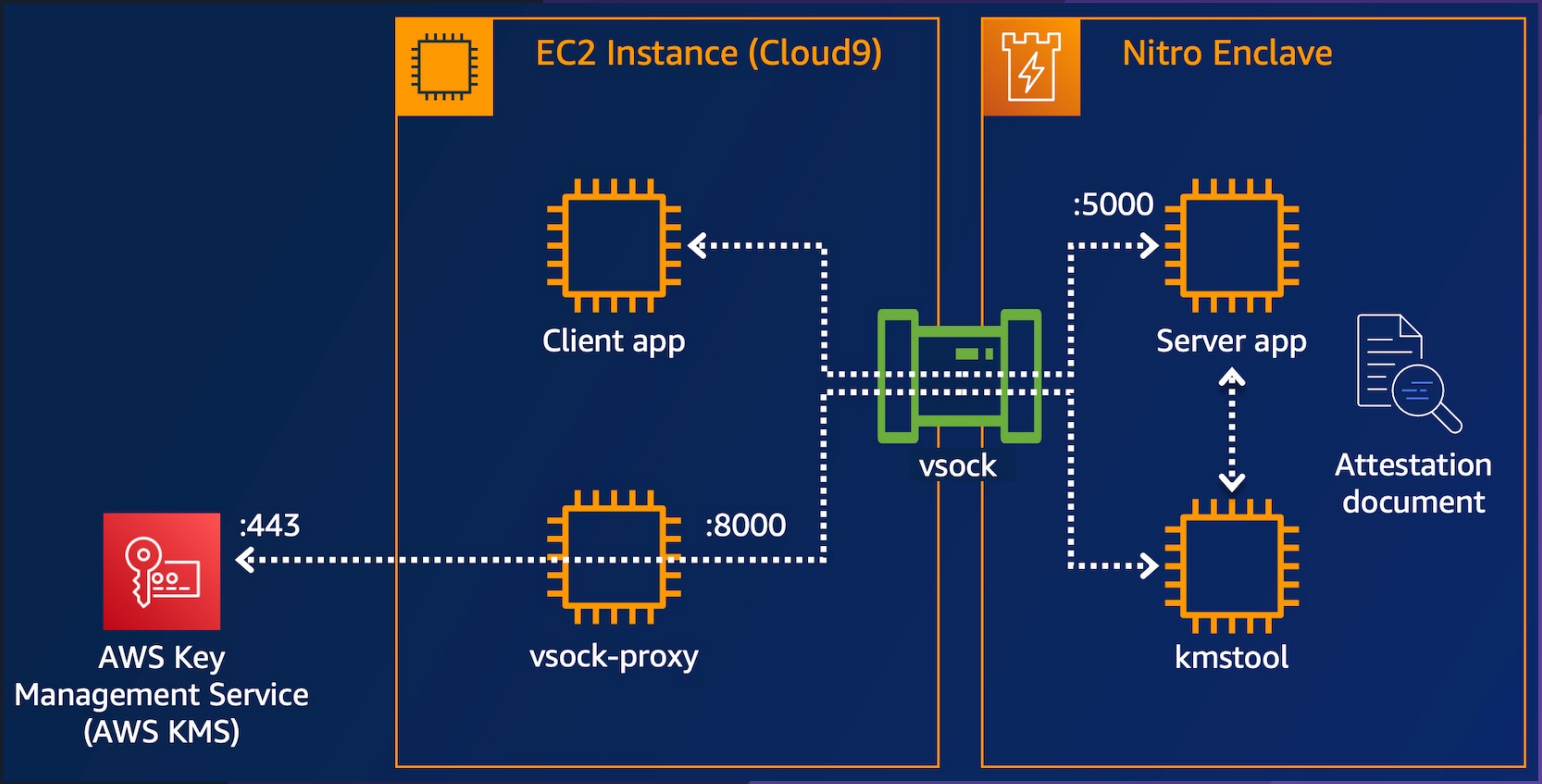
Demo time – Secure communication

Setup a secure local channel via vsock

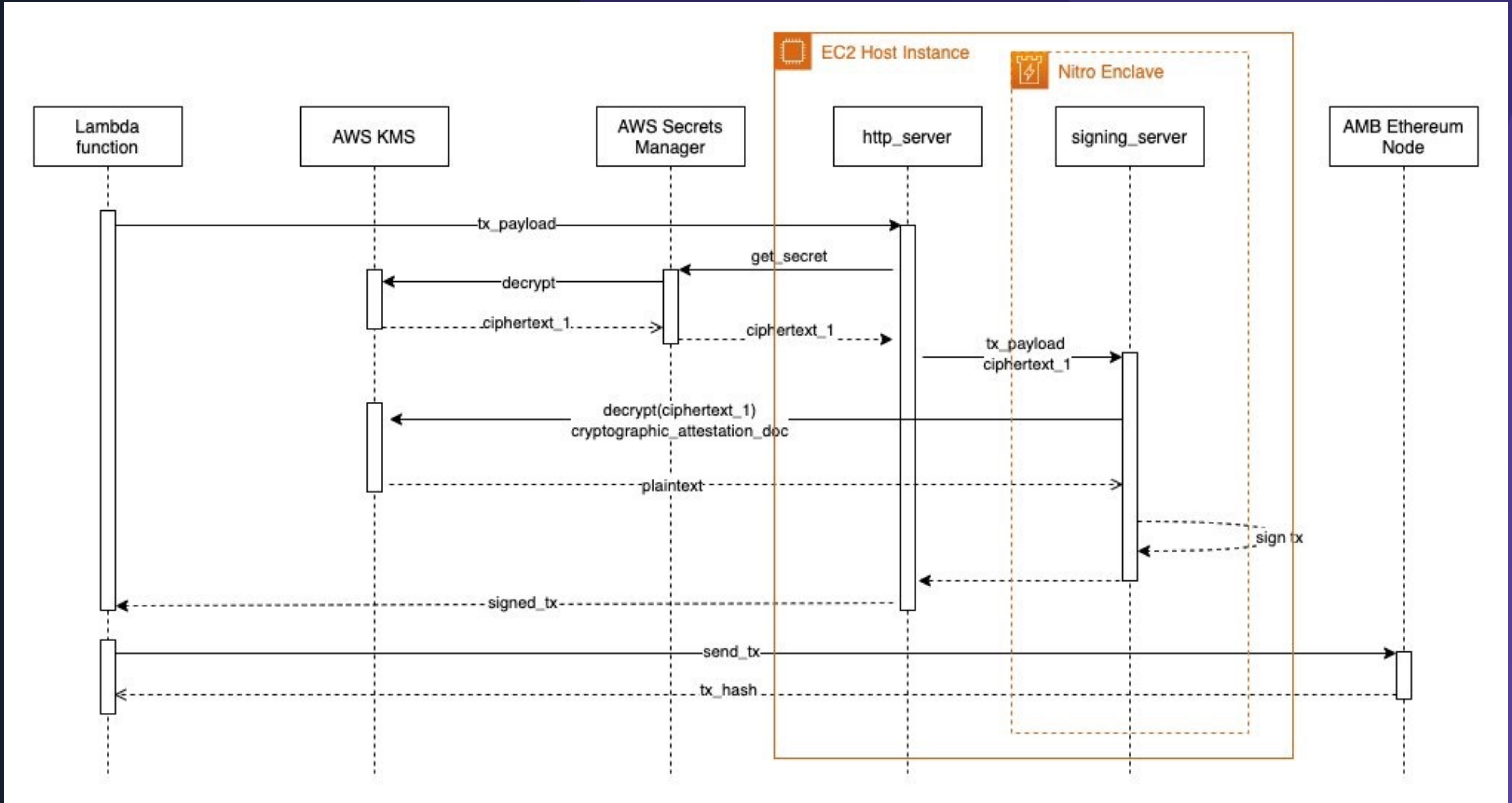


Demo time – Cryptographic attestation

Protect ze keys!



Real life example



Resources

- AWS Workshop https://github.com/aws-samples/aws-nitro-enclaves-workshop
- Nitro Enclaves for secure blockchain signing https://aws.amazon.com/blogs/database/part-1-aws-nitro-enclaves-for-secure-blockchain-key-management/