
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

CMP403

Enabling multi-party analysis of sensitive data using AWS Nitro Enclaves

Sudhir Reddy Maddulapally (he/him)
Sr. Specialist SA, Confidential Computing
AWS

J.D. Bean (he/him)
Principal Security Architect, EC2
AWS

Agenda

Fundamentals of multi-party computation (MPC)

Trust and attestation

Roles and responsibilities

Collaboration between untrusting parties

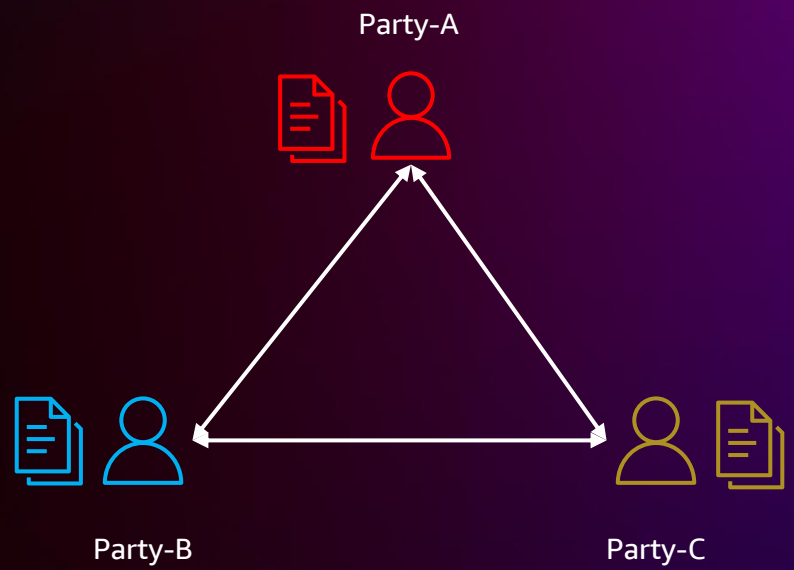
Demo

References

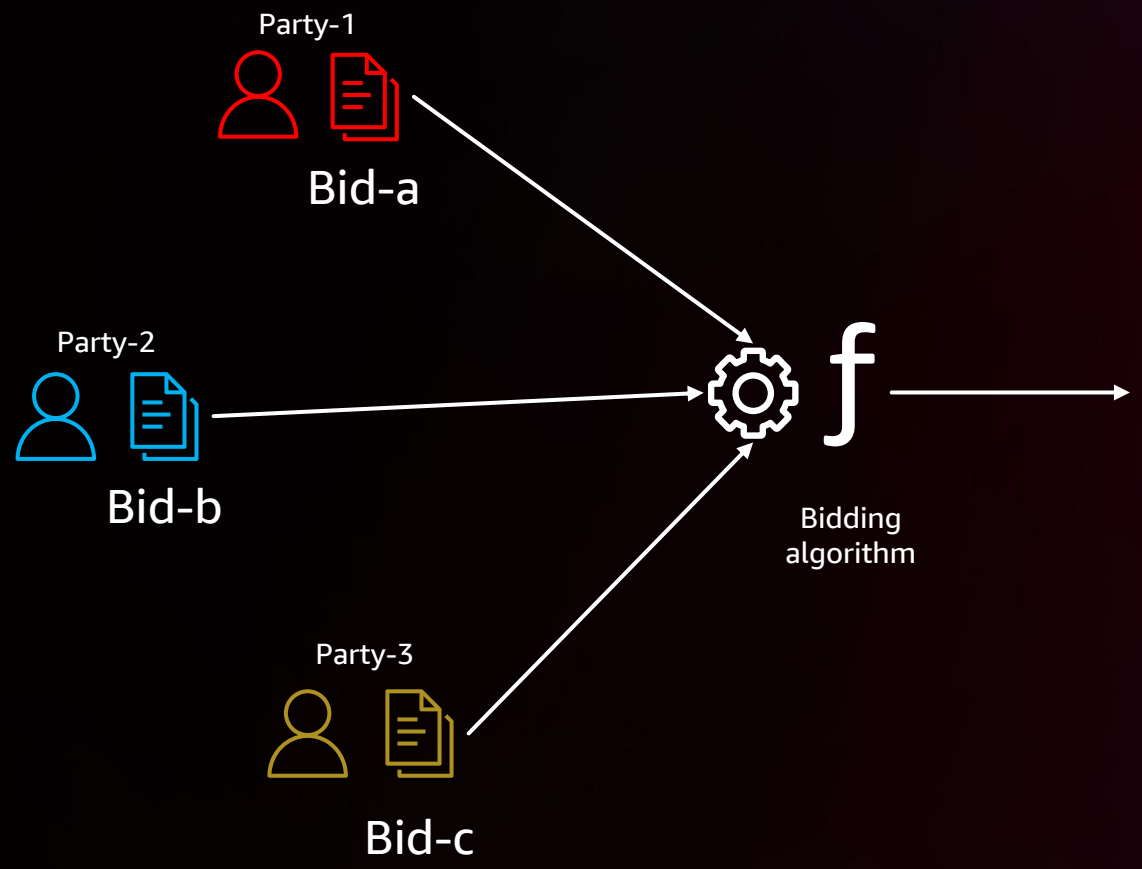
Fundamentals

What is multi-party computation (MPC)?

- MPC definition: At least 2 parties that hold the data or compute nodes
- SMPC without a trusted party
- MPC invented in 1987
- Fundamentals:
  - Security
  - Integrity of results/correctness
- Trust, secret sharing
- Collusion, adversarial, and other things
- Multi-party collaboration

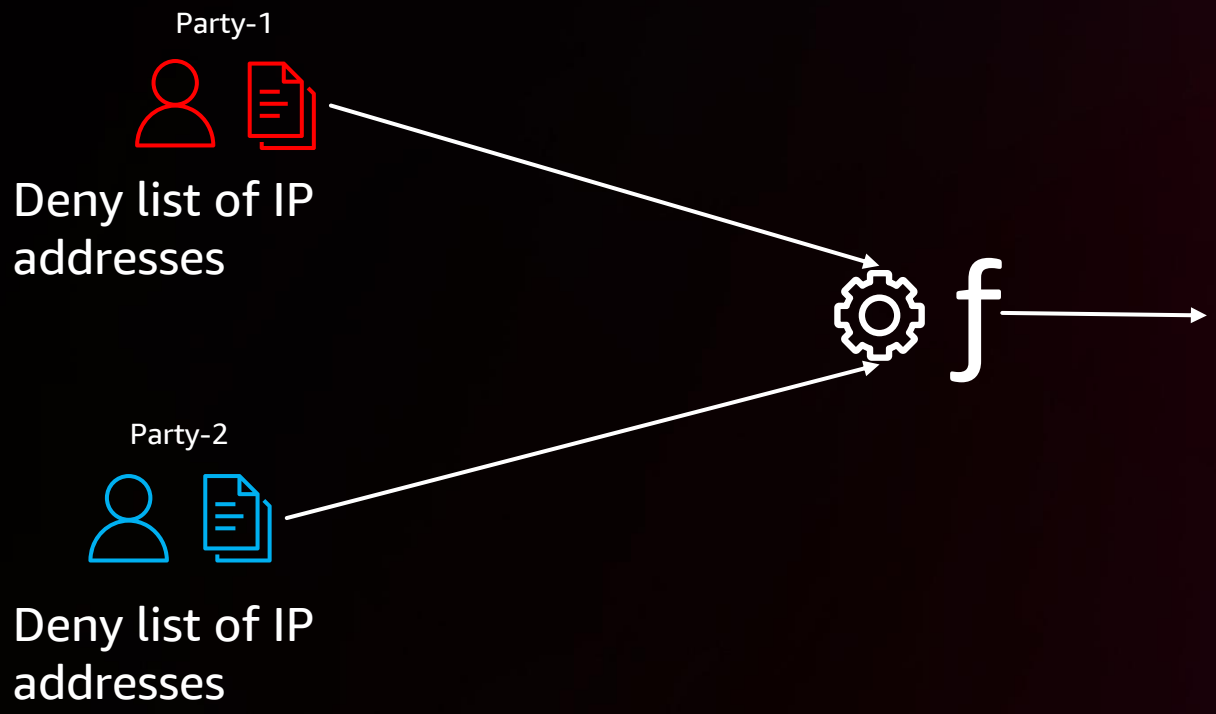


MPC – Bidding example



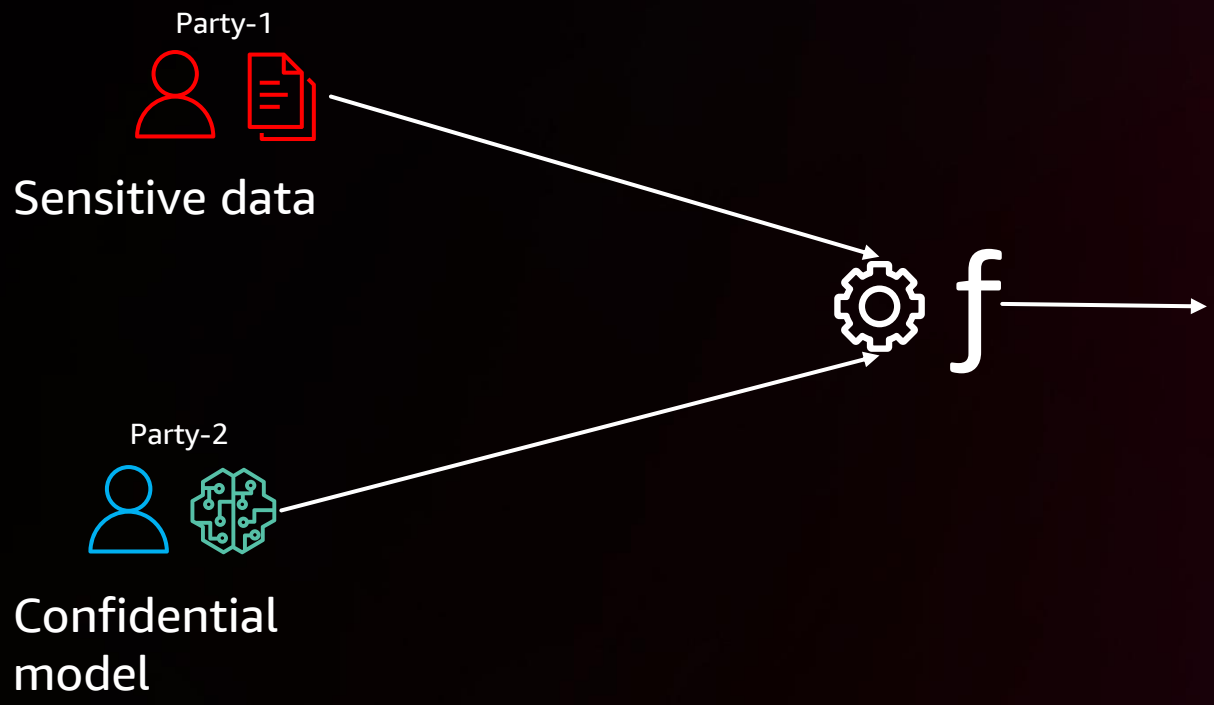
Goal: To calculate the winning bid without revealing bids to all parties

MPC – Data intersection example



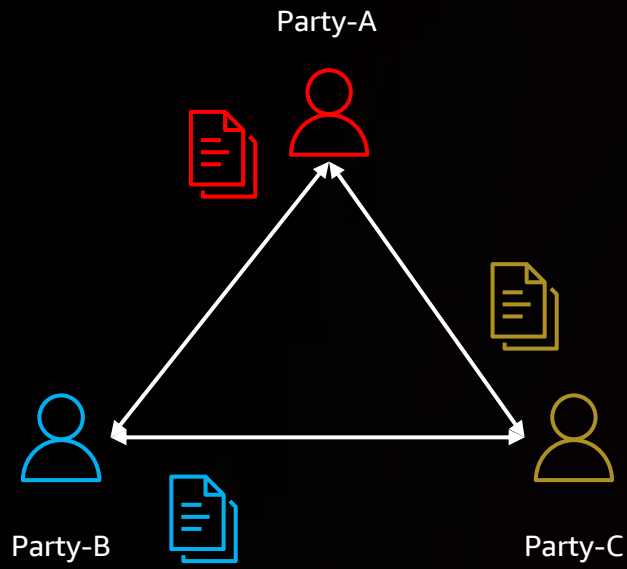
Goal: To check if certain IPs are already known to be on deny lists without revealing IPs to other parties

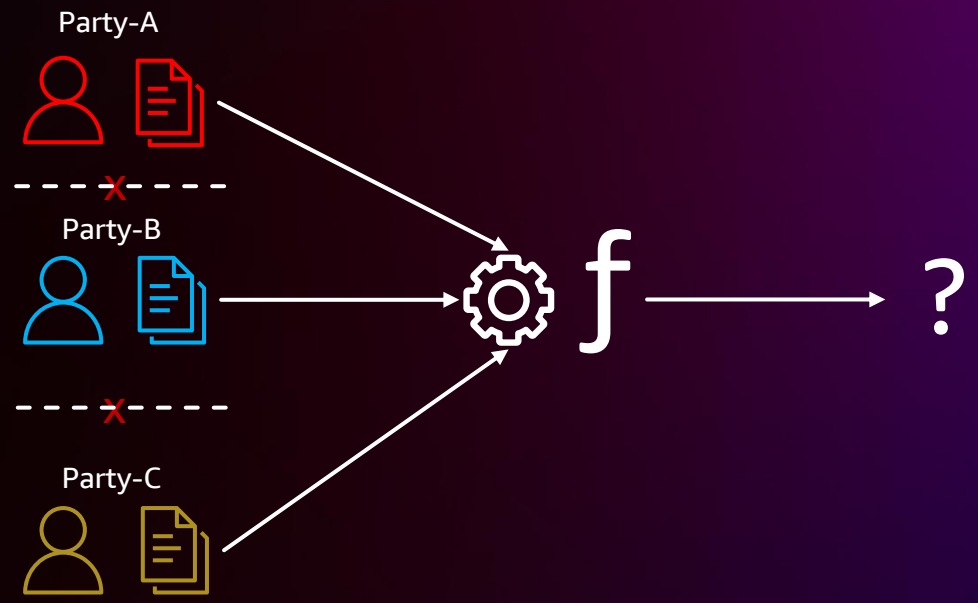
MPC – Sensitive AI/ML model example



Goal: To apply the model to the sensitive data without revealing the model details and the raw sensitive data

Multi-party computation example

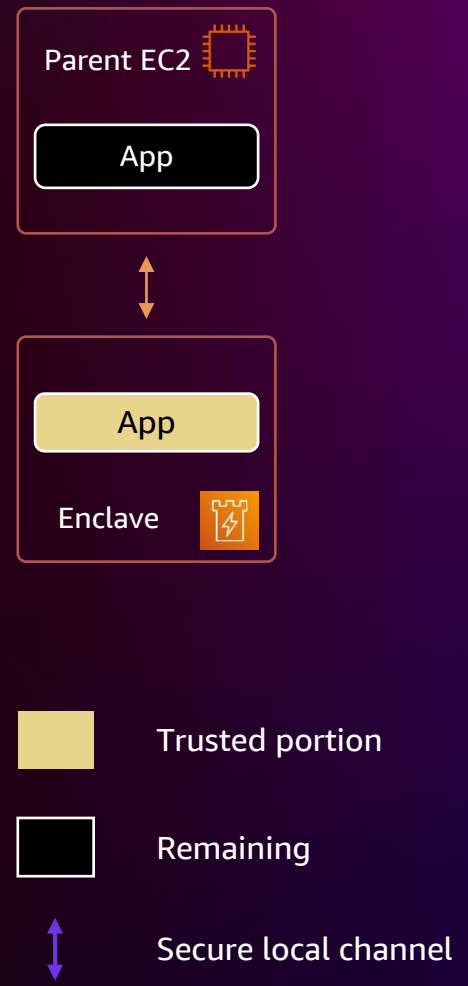




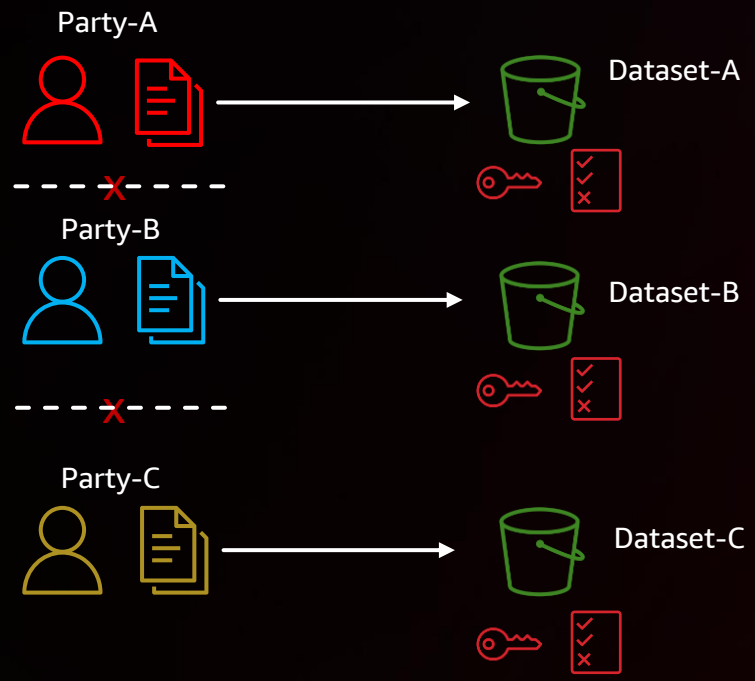
Trust and attestation

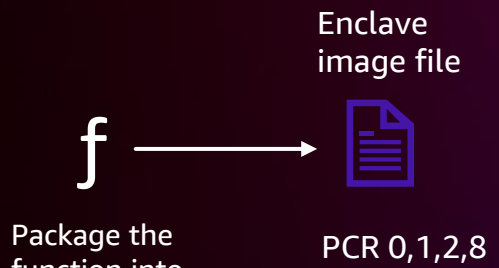
What is AWS Nitro Enclaves?

- Nitro Enclaves is an Amazon EC2 feature that allows you to create isolated execution environments, called *enclaves*, from EC2 instances
- Enclaves are separate, hardened, and highly constrained virtual machines
- Secure local channel connectivity with their parent instance
- No persistent storage, interactive access, or external networking
- Cryptographic attestation



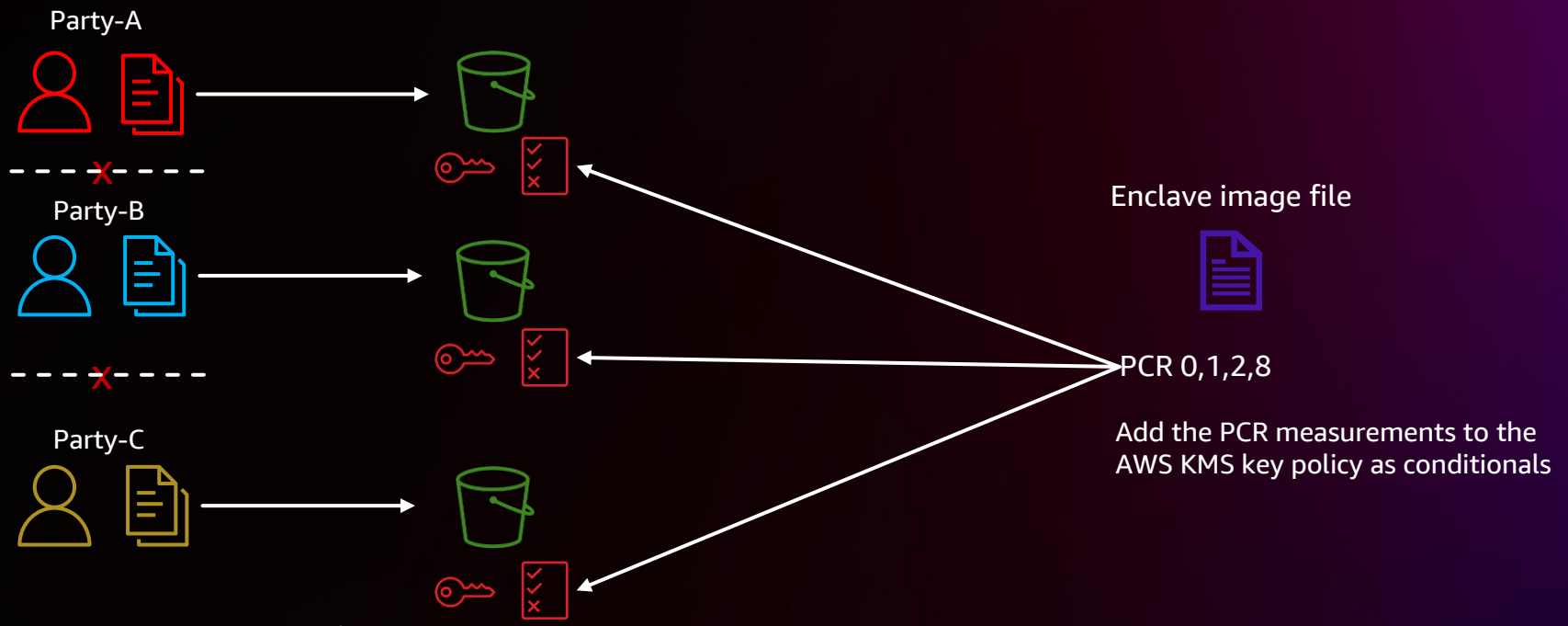
Generating enclave fingerprints





Broadcast the PCR measurements to all parties

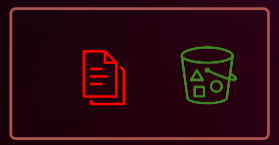
Conditionally allowing access based on PCRs




```
"Condition": {
  "StringEqualsIgnoreCase": {
    "kms:RecipientAttestation:PCR0":"EXAMPLEbc2ecbb68ed99a",
    "kms:RecipientAttestation:PCR1":"EXAMPLE050abf6b993c91",
    "kms:RecipientAttestation:PCR2":"EXAMPLEc300289e872e6a",
    "kms:RecipientAttestation:PCR8":"EXAMPLE34a884328944cd"
  }
}
```

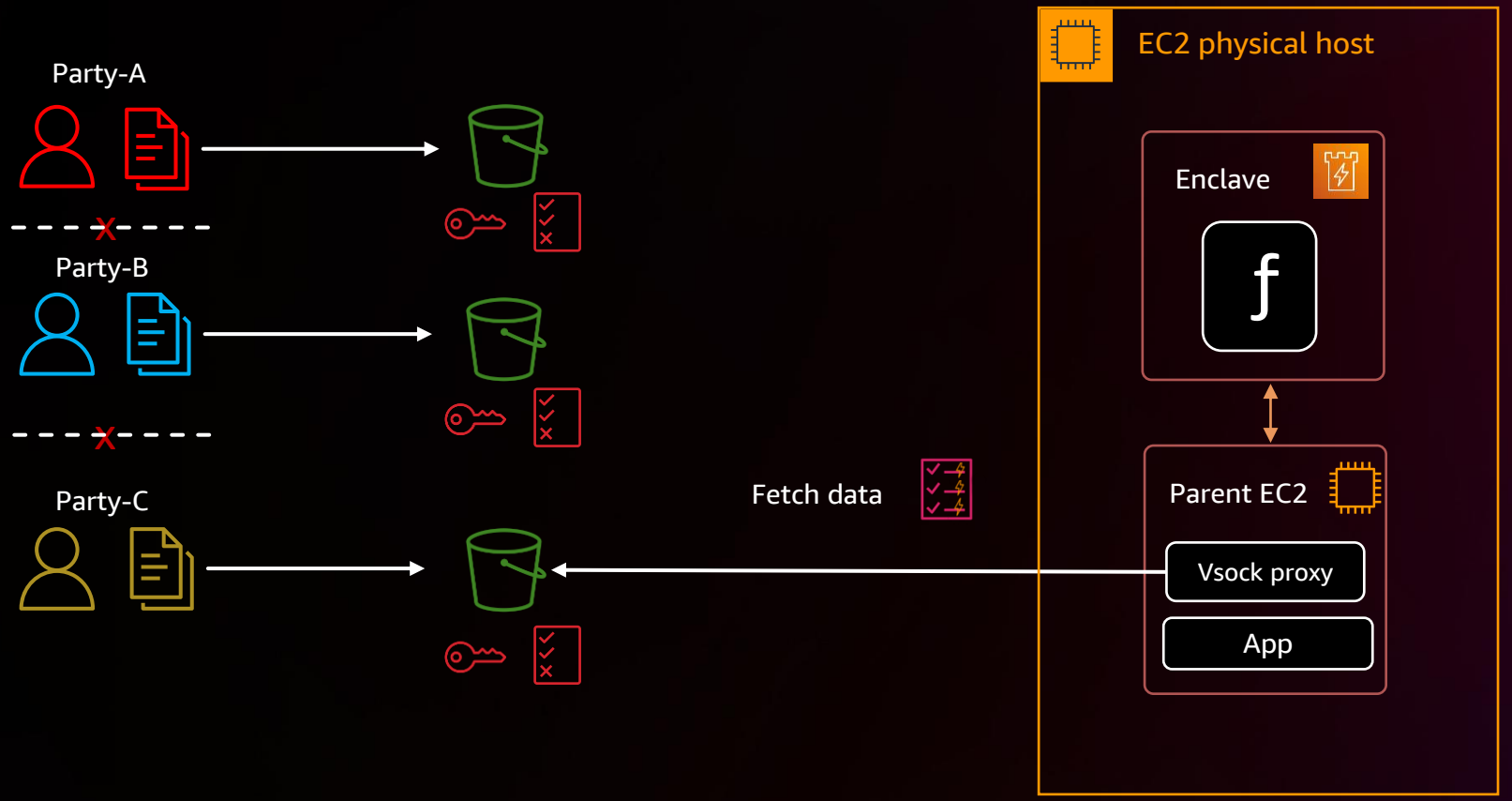
Roles and responsibilities

Roles

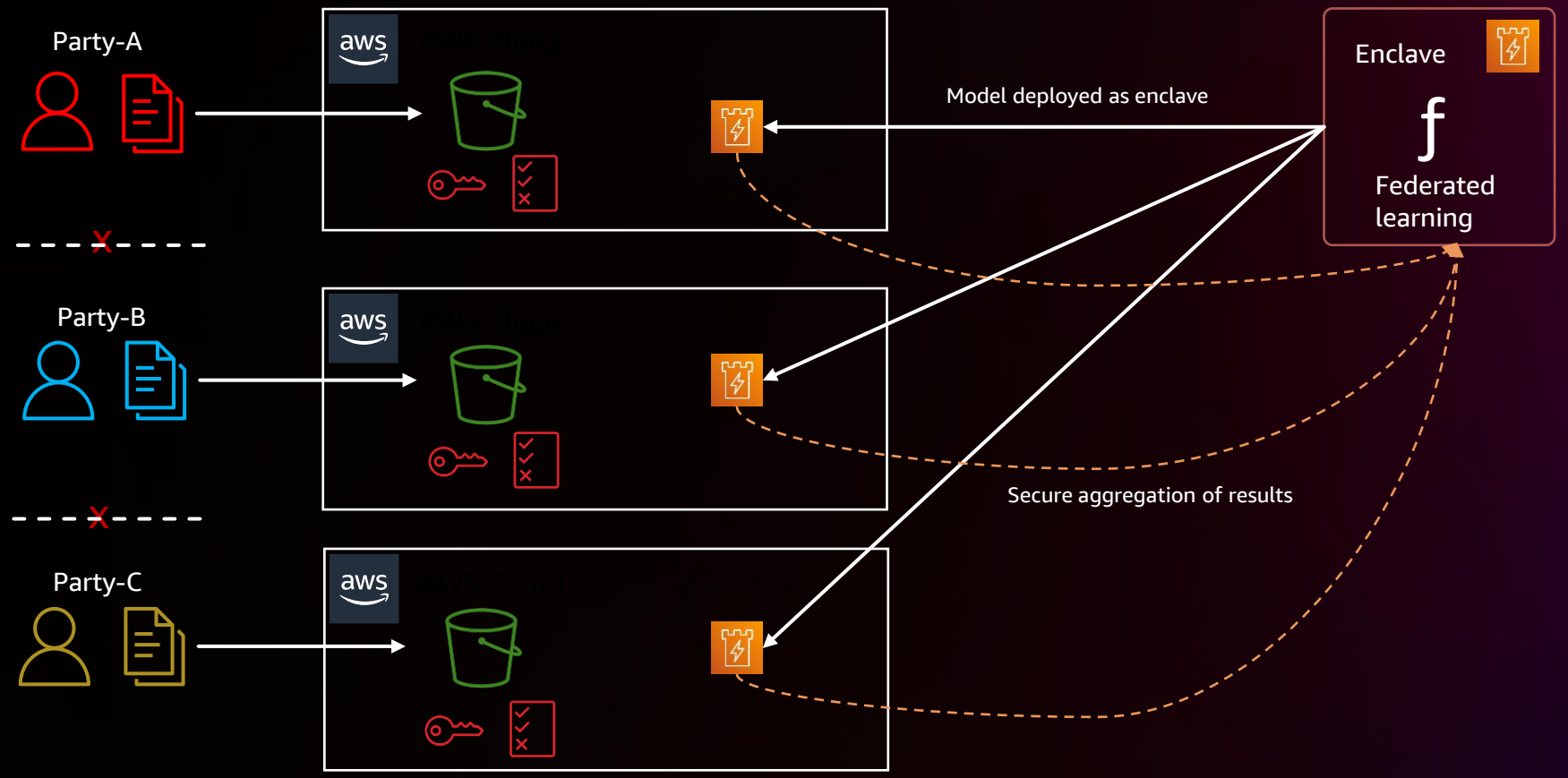
Data owner	Owns the sensitive data. Responsible for cryptographic key policy for the sensitive data.		
Platform owner	Hosts the sensitive computing environment.	Enclave 	Parent EC2 
Code developer	Develops the enclave code for computation to be performed.	Computation code 	EIF file 

Collaboration between untrusting parties

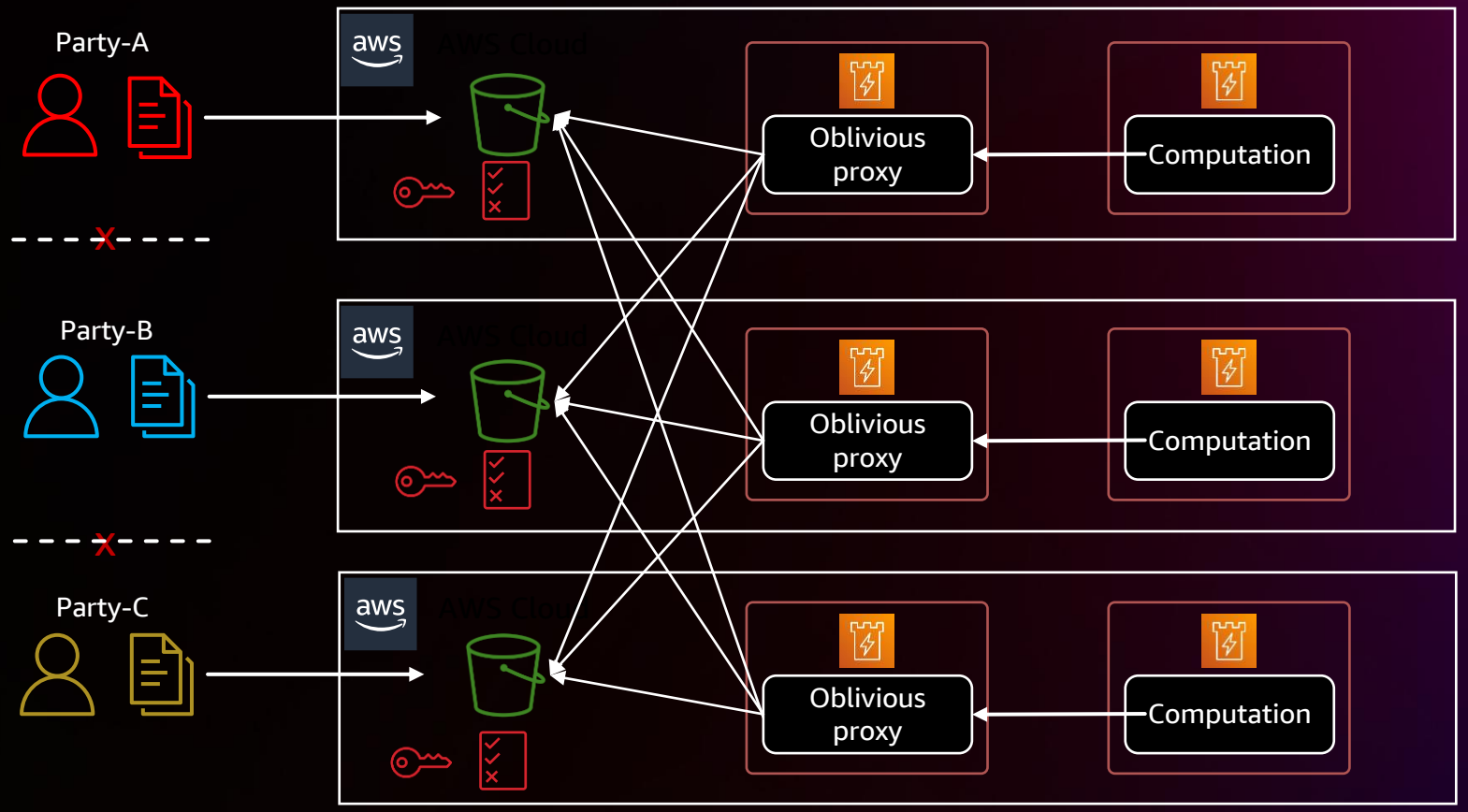
Sensitive data sharing



Computation by each party



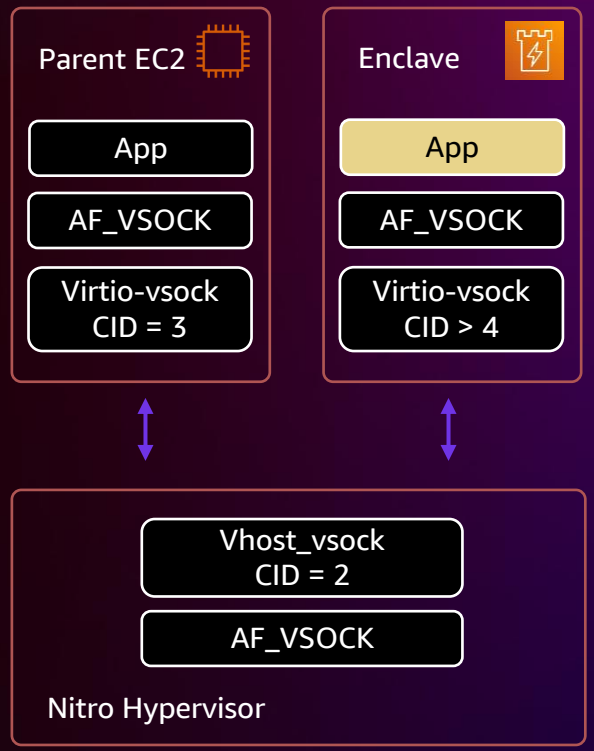
Oblivious data retrieval



References

What is a secure local channel?

- Vsock – Virtio vsock (VM sockets)
- POSIX socket API (socket, bind, listen, connect)
- SOCK_STREAM / SOCK_DRAM
- CID (context identifier) and port
  - Example, CID = 3 always points to parent EC2
  - Example, CID >4 can be specified when launching enclave
- Multiple vsock connections possible between enclave and parent EC2, however they all rely on one set of IO buffers



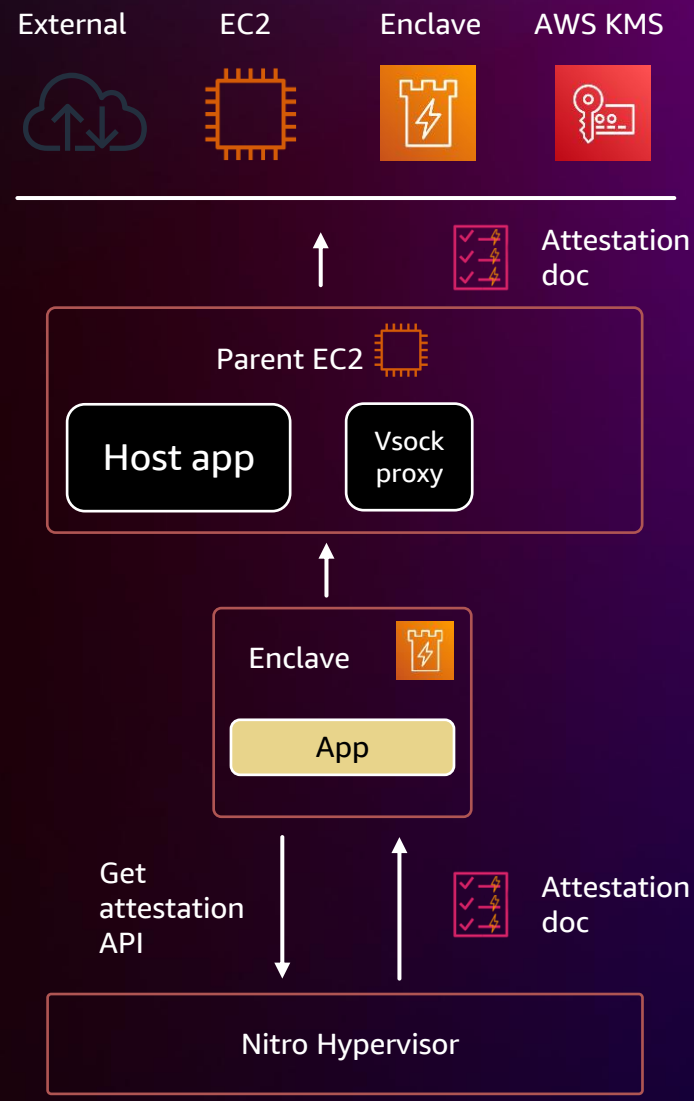
What are PCRs?

- An enclave's measurements include a series of hashes and platform configuration registers (PCRs) that are unique to the enclave
- An enclave has six measurements that are available out of the box
- 4 measurements set at EIF build time [0,1,2,8]
- 2 measurements set at enclave run time [3,4]

PCR	Hash of
PCR0	Enclave image file
PCR1	Linux kernel and bootstrap
PCR2	Application
PCR3	IAM role assigned to the parent instance
PCR4	Instance ID of the parent instance
PCR8	Enclave image file signing certificate

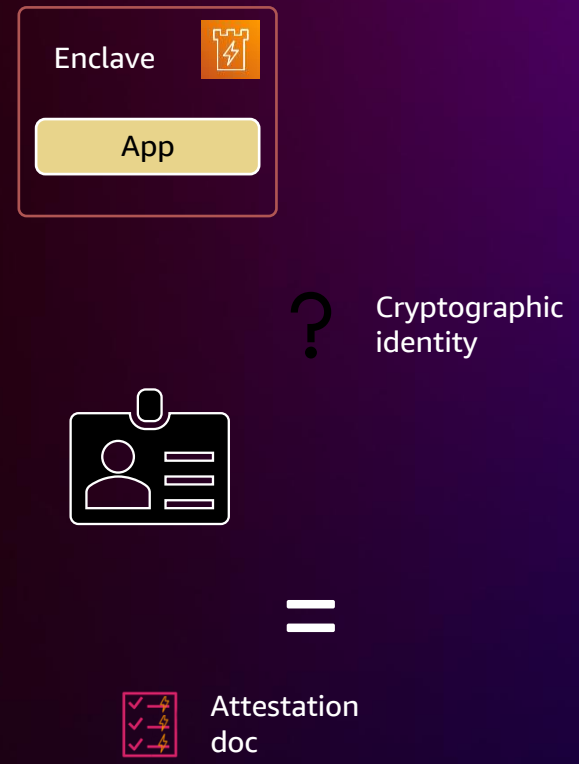
What is attestation?

- Enclave uses attestation as a mechanism to prove its identity and build trust
- Attestation can be used with an external service or another enclave
- Out-of-the-box integration with AWS Key Management Service (AWS KMS)



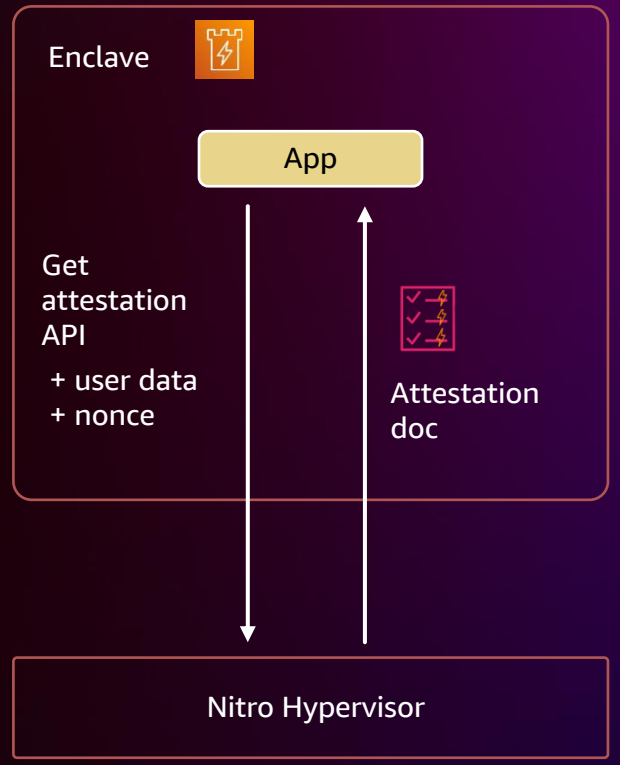
What is an attestation document?

- Issued by the Nitro Hypervisor as response to get-attestation-document API call included in the Nitro Enclaves SDK
- Concise Binary Object Representation (CBOR)-encoded and CBOR Object Signing and Encryption (COSE)-signed object using the COSE_Sign1 structure
- Includes the PCRs locked at the moment of generation
- Signed by the AWS Nitro Attestation PKI
- Services consuming the attestation have to
  - Verify signature
  - Parse the user data, PCRs, and nonce
  - Enforce the measurements-based access policies specific to the operation between the external service and enclave



What is an attestation document?

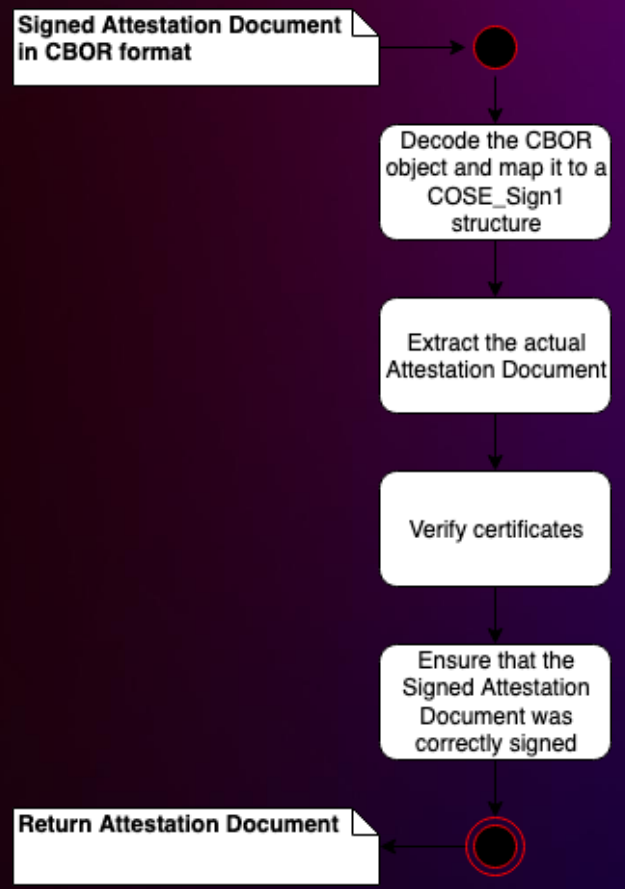
Module_id	Text	Issuing Nitro Hypervisor module ID
timestamp	Uint (8)	UTC time when document was created, in milliseconds since UNIX epoch
digest	digest	The digest function used for calculating the register values
pcrs	Bytes (32/48/64) [32]	Map of all locked PCRs at the moment the attestation document was generated
certificate	Cert	The infrastructure certificate used to sign this document, DER-encoded
cabundle	Cert [*]	Issuing CA bundle for infrastructure certificate
public_key	bytes .size (0..1024)	An optional DER-encoded key the attestation consumer can use to encrypt data
user_data	bytes .size (0..1024)	Additional signed user data, defined by protocol
nonce	bytes .size (0..1024)	An optional cryptographic nonce provided by the attestation consumer as a proof of authenticity



Verification of an attestation document

- Verification of an attestation document signature can be done with the certificate and CA bundle included
- Root certs are available for download at the below QR code

Nitro PKI root certs



Thank you!

Please complete the session survey in the **mobile app**