Joint work with the Coinbase cryptography team (and others)

- Arash Afshar
- Yi-Hsiu Chen
- Samuel Ranellucci

MPC for Custody (and more) at Coinbase

Yehuda Lindell

Head of Cryptography at Coinbase

- In this talk, we will describe CoreKMS Vault, a new key signing service at Coinbase
- Our description will not include exact deployment details, but rather the system and its capabilities
- Not all details are included, due to time constraints
- This talk contains a description of technology that Coinbase has available. Internal deployment of this technology may change over time.

Challenges of Asset Protection

Offline and Online Systems

- **Offline – an air-gapped system that holds the keys and signs**
    - Can be very high security
    - But security is not immediate:
        - How are transactions imported and signatures exported?
        - How is the physical environment protected and controlled?
    - Challenges regarding time to sign
- **Online – key held in online server**
    - Security challenges – an online machine with a highly lucratice target
        - Security risks: supply chain attack, insider access, zero days, etc.
    - Not suitable for large amounts
    - Immediate response time

Single Points of Failure (Attack)

- With such an extremely lucrative target, any single point of attack is dangerous
- Offline systems can be made very secure, but can also be a single point of failure (with a single place holding the key)
    - Can be mitigated well (multiple people and physical access controls)
    - Good mitigations can impact transaction signing time
- Offline systems work extremely well for infrequent operations (e.g., key generation ceremonies, infrequent transfers of funds out of freeze, etc.) but less so for ongoing operations

CoreKMS Vault

Design Principles

- **Flexibility**
  - Different products (custody, exchange, non-custodial, etc.)
  - Different security tradeoffs and response speed
- **Security**
  - No single environment with key access
  - Different entities with strong separation between them during entire lifecycle
  - Defense in depth throughout

Underlying Technology

- **We use MPC to obtain strong separation and flexibility**
- **Asset keys are shared amongst entities, and never brought together, throughout their entire lifecycle**
- **Backup is publicly verifiable and highly protected from loss and theft**

CoreKMS Vault Entity Types

- **Offline environment**
- **Human approvers**
- **MPC servers**

Entity Types

- **Offline environment**
  - An offline machine + a separate store of key shares
  - Physically secure location with strict access limitations
  - The offline environment holds ***only one share*** of the key

Entity Types

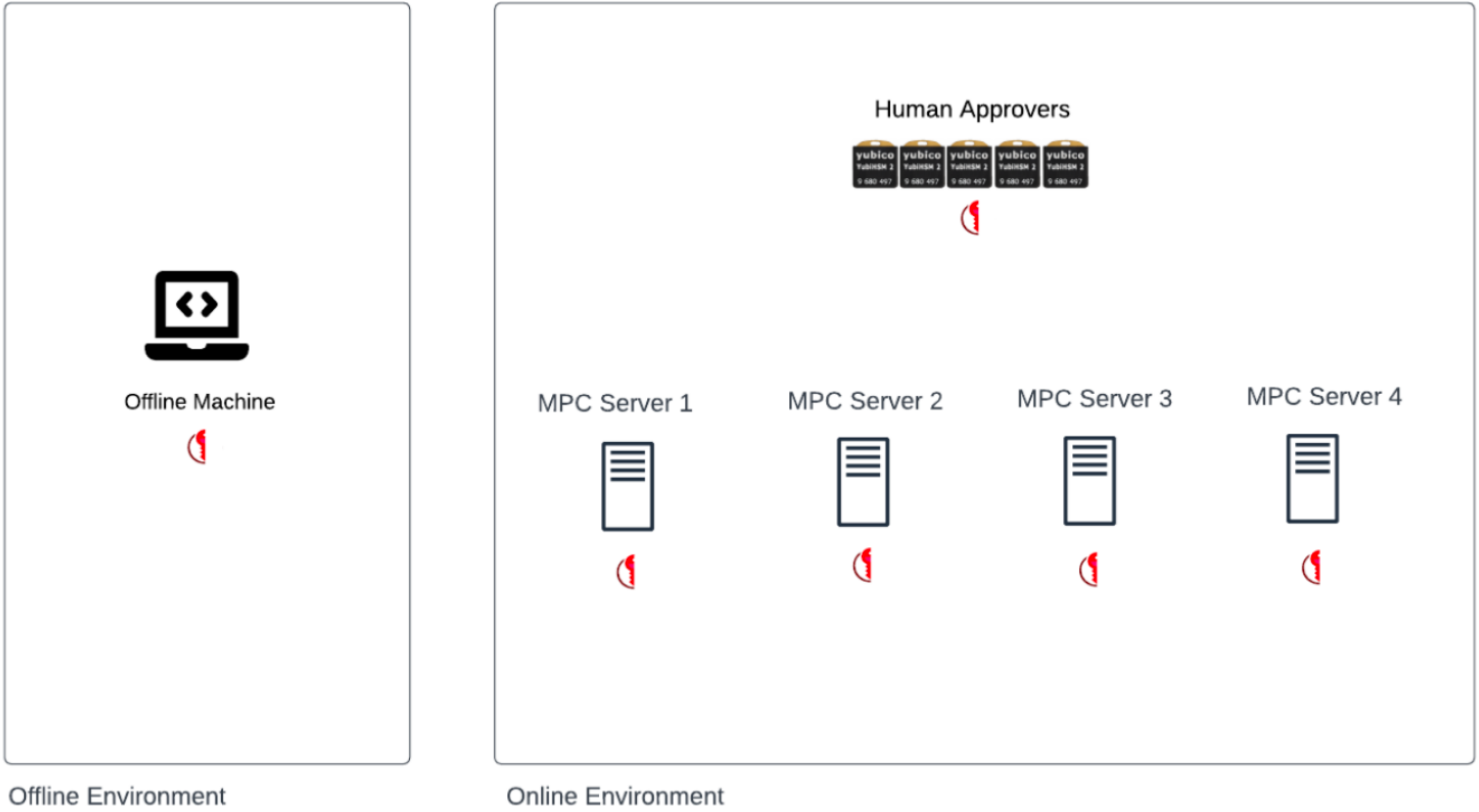
- **Human approvers**
  - Devices held by human operators (e.g., laptop, mobile)
  - Hold shares of a threshold decryption key (e.g., TDH2 by Shoup-Gennaro)
    - Generated via MPC at vault generation
  - One share of each asset-key is encrypted under the threshold encryption public key
  - Access structure defines quorum
    - System supports advanced access structures like (3-out-of-5) AND (4-out-of-10); any tree with AND, OR and threshold nodes
- **Human approver operations must be asynchronous (i.e., do not need to be online at the same time)**

Entity Types

- **Online MPC servers**
    - Servers who each hold their database of key shares
        - Each server holds its own share
    - Always online, and can interact with each other over multiple rounds

Entity Types – Security and Rationale

- **Strong separation with different types of entities**
    - Infrastructure for all three environments is completely different
    - Offline environment – without participation there isn't enough key material to sign online
    - Human approvers disconnected also means that there isn't enough key material to sign online
    - MPC servers can be completely locked down in the server infrastructure (and can also be separated, if desired)
- **Different instantiations can have different entity types, and different number of entities in each type**

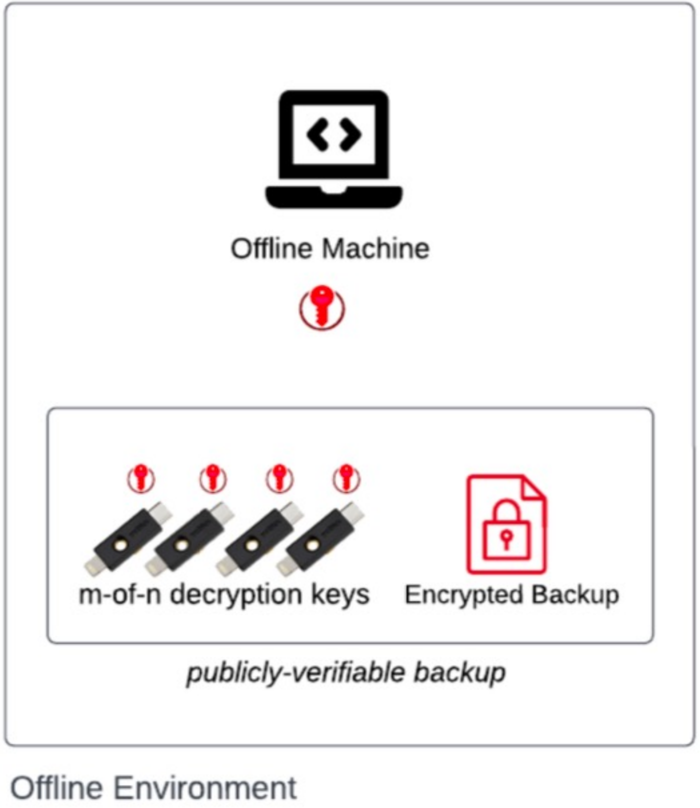

Human Approvers
yubico
yubico
yubico
yubico
yubico
Offline Machine
MPC Server 1
MPC Server 2
MPC Server 3
MPC Server 4
Offline Environment
Online Environment

Operations

- **Key generation and backup**
- **Signing**
- **Approver administration**

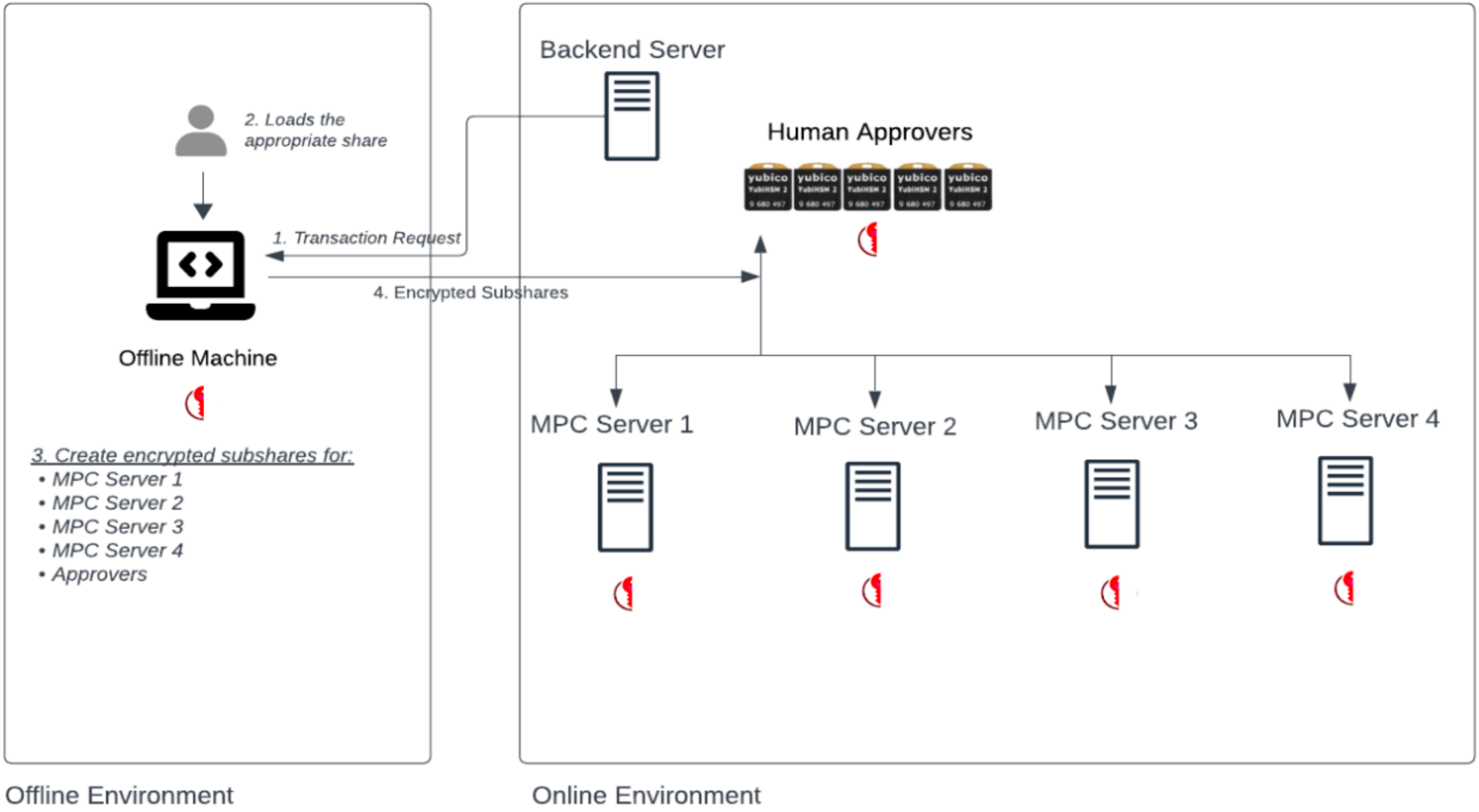
Key Generation and Backup

- **System with offline element**
    - Key generation ceremony in special offline environment (more secure than regular one)
    - Encrypt each entities' share under given public keys (offline signing environment, approvers, each MPC server)
- **System without offline element**
    - Use MPC protocol to generate key shares
- **At key generation, all shares are backed up using publicly-verifiable backup, with a quorum of backup entities required for any share**



Signing

- **Step 1 – offline environment**
  - Receives transaction request, loads key share
  - Subshares key share to all MPC servers plus human approvers
    - Encrypt under server public keys and approver threshold key
  - This subsharing is fresh and different in every transaction

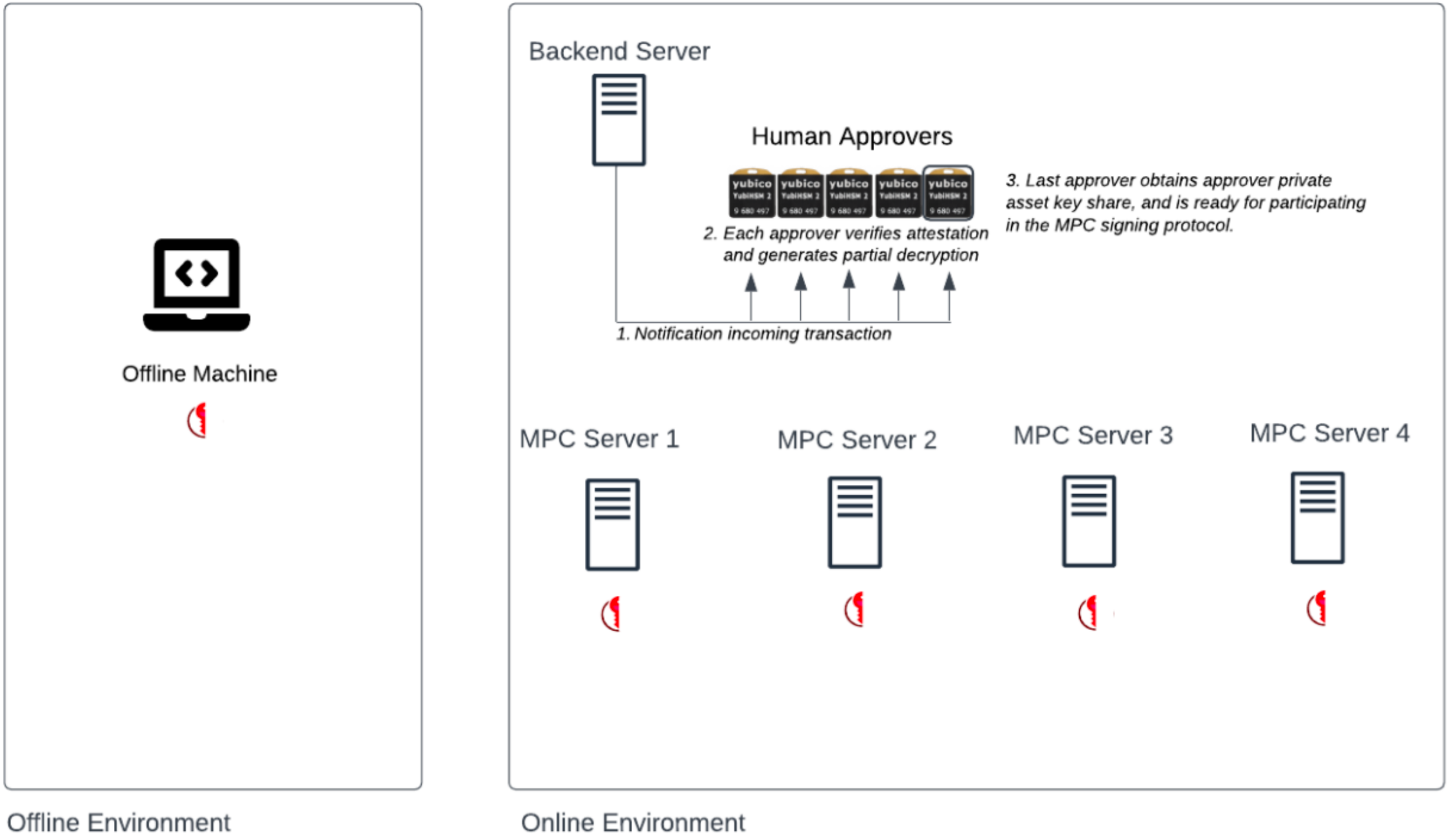


3. Create encrypted subshares for:

- MPC Server 1
- MPC Server 2
- MPC Server 3
- MPC Server 4
- Approvers

Signing

- **Step 2 – each human approver up to last in quorum**
  - Receives transaction request, *verifies transaction attestations*
  - Generates partial decryption of approver key share and offline subshare
  - Partial decryptions are *re-encrypted* under approver public keys
- **Last approver in the quorum**
  - Obtains the partial decryptions and finalizes to get shares (approver share and offline subshare)
  - Adds them together



Backend Server

Human Approvers

1. Notification incoming transaction

2. Each approver verifies attestation and generates partial decryption

3. Last approver obtains approver private asset key share, and is ready for participating in the MPC signing protocol.

Offline Machine

MPC Server 1

MPC Server 2

MPC Server 3

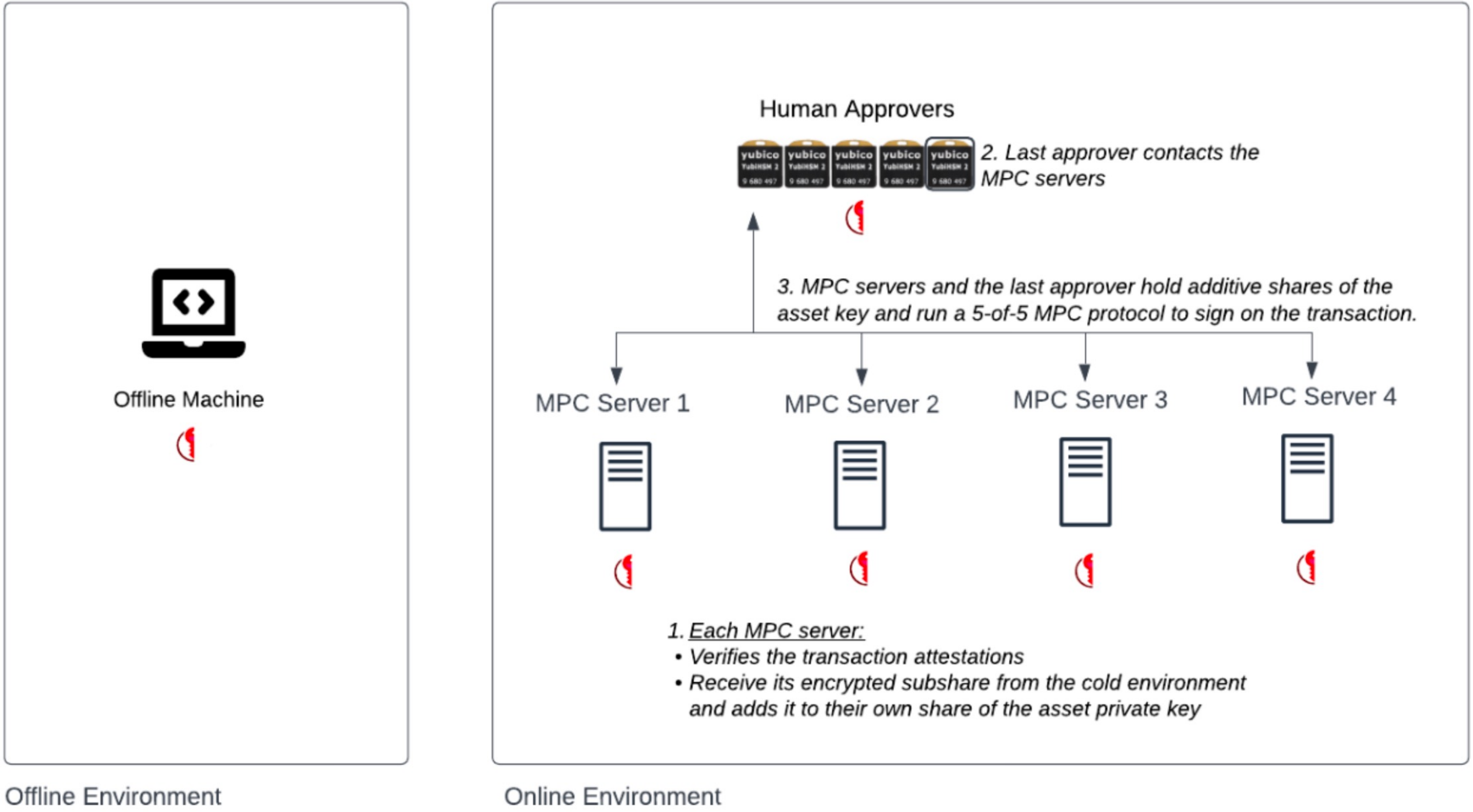
MPC Server 4

Offline Environment

Online Environment

Signing

- **Step 3 – MPC Signing**
  - Each MPC server receives offline environment’s subshare and adds to its own (also verifying all attestations)
  - MPC servers and last approver “agree” on the participants and the sharing (verify that the sum of all “public shares” is correct)
  - MPC servers and last approver run MPC to sign
  - MPC servers and last approver refresh the sharing of the asset key (excluding the offline share)
  - All state information is erased

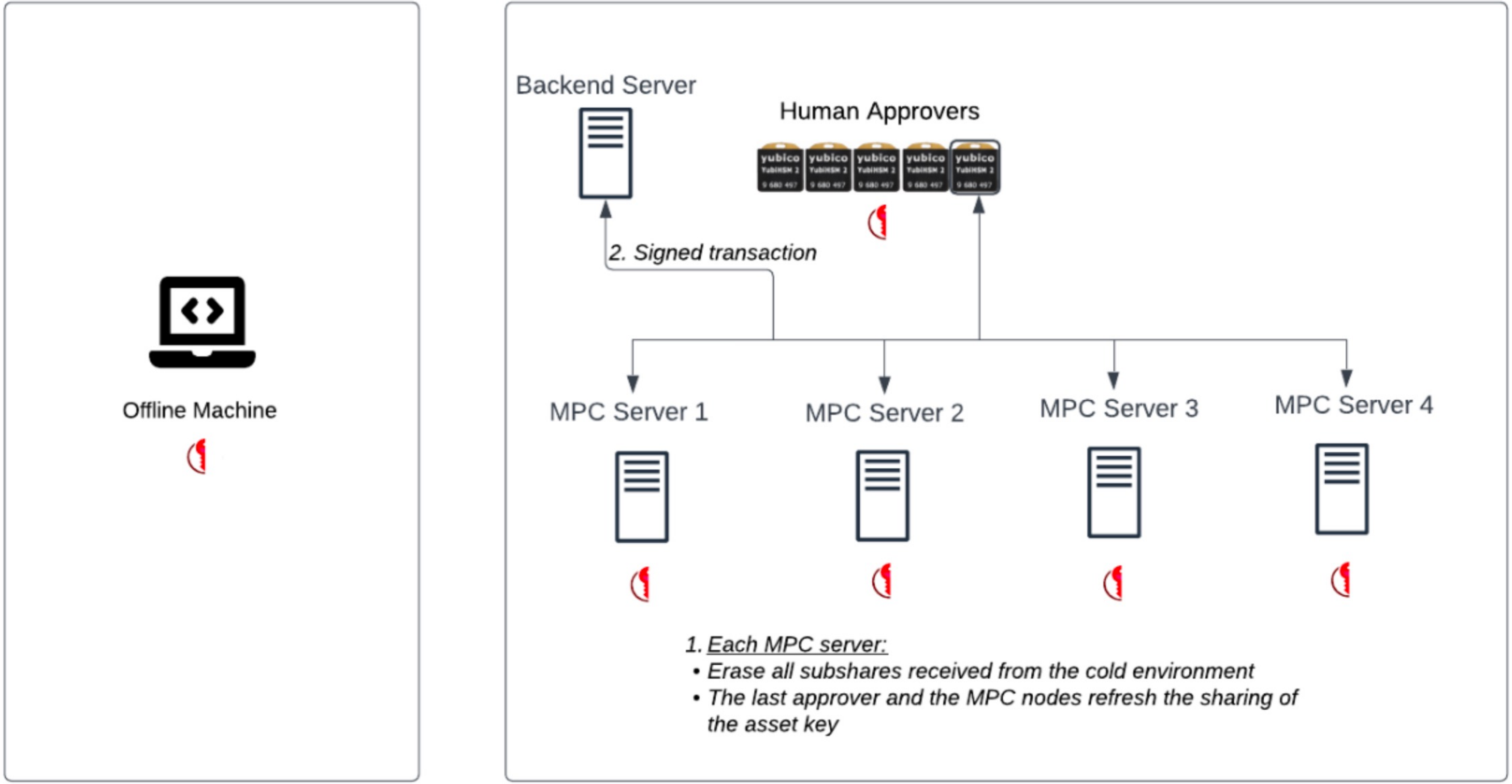


2. Last approver contacts the MPC servers

3. MPC servers and the last approver hold additive shares of the asset key and run a 5-of-5 MPC protocol to sign on the transaction.

1. Each MPC server:

- *Verifies the transaction attestations*
- *Receive its encrypted subshare from the cold environment and adds it to their own share of the asset private key*



Offline Machine

Backend Server

Human Approvers

2. Signed transaction

MPC Server 1

MPC Server 2

MPC Server 3

MPC Server 4

1. <u>Each MPC server:</u>

- *Erase all subshares received from the cold environment*
- *The last approver and the MPC nodes refresh the sharing of the asset key*

Offline Environment

Online Environment

Approver Administration

- **System also includes protocols for approver administration**
  - Add approver
  - Remove approver
  - Change approver quorum structure
  - Refresh approver threshold decryption key
- **All of the above via MPC**
- **All operations require signed admin quorum approval**

Properties

Security

- **A key cannot be brought to signing without approval from offline environment, a quorum of approvers, and all MPC servers**
  - Attestation verifications reduce risk of fraudulent transactions
  - Multiple attestation services can also be used
  - This is crucial for preventing **key misuse**
- **When using an offline environment, before being used, a key is never online in any form**
- **No single point of failure / attack**
  - Strong separation between machine types and machines
  - Makes it very hard to simultaneously corrupt all MPC servers and approvers

Achieving Flexibility and Speed

- **Can be deployed in multiple configurations and locations**
  - Important for MiCA compliance
- **Configurations**
  - **All entities – offline, human approvers, MPC servers**:
    - The number of human approvers, the access structure and where they are located can change, depending on the product and its needs
  - **MPC servers and human approvers**:
    - Same flow as above, but without offline
    - Faster than above, but still has element that can be disconnected
  - **MPC servers only**:
    - Fast response, always online; much more secure than classic online systems

Defense in Depth

- **All servers are heavily locked down**
- **Approver shares are encrypted with device secure enclave and external YubiHSMs**
- **Zero-trust approach to all devices in the system**
- **Controls around offline environment, approver operators, etc.**
- **And much more**

Thank You