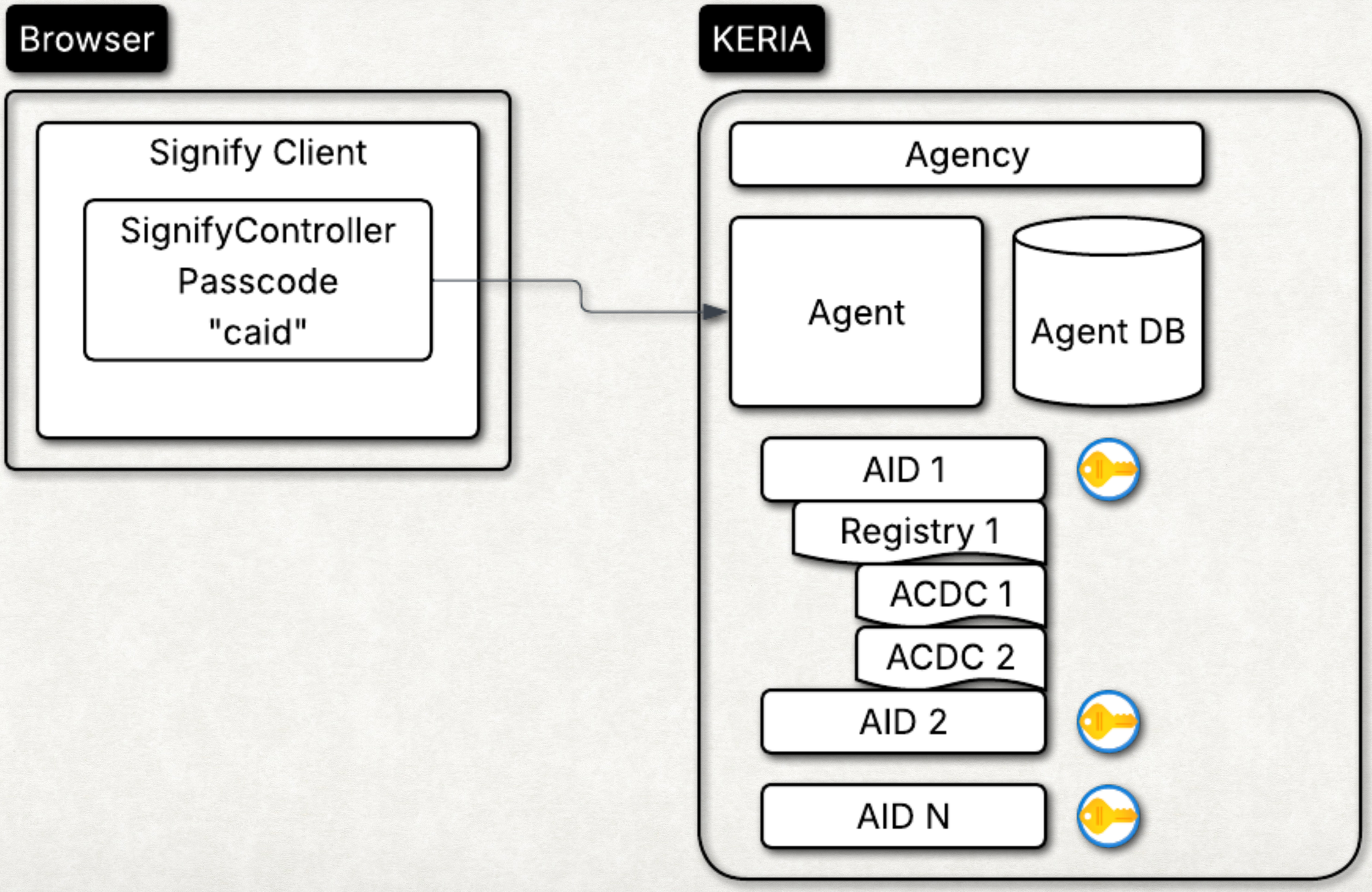


KERIA TUTORIAL

SIGNIFY ARCHITECTURE FRONT TO BACK

WHAT IS KERIA


Browser
KERIA
Signify Client
SignifyController
Passcode
"caid"
Agency
Agent
Agent DB
AID 1
Registry 1
ACDC 1
ACDC 2
AID 2
AID N

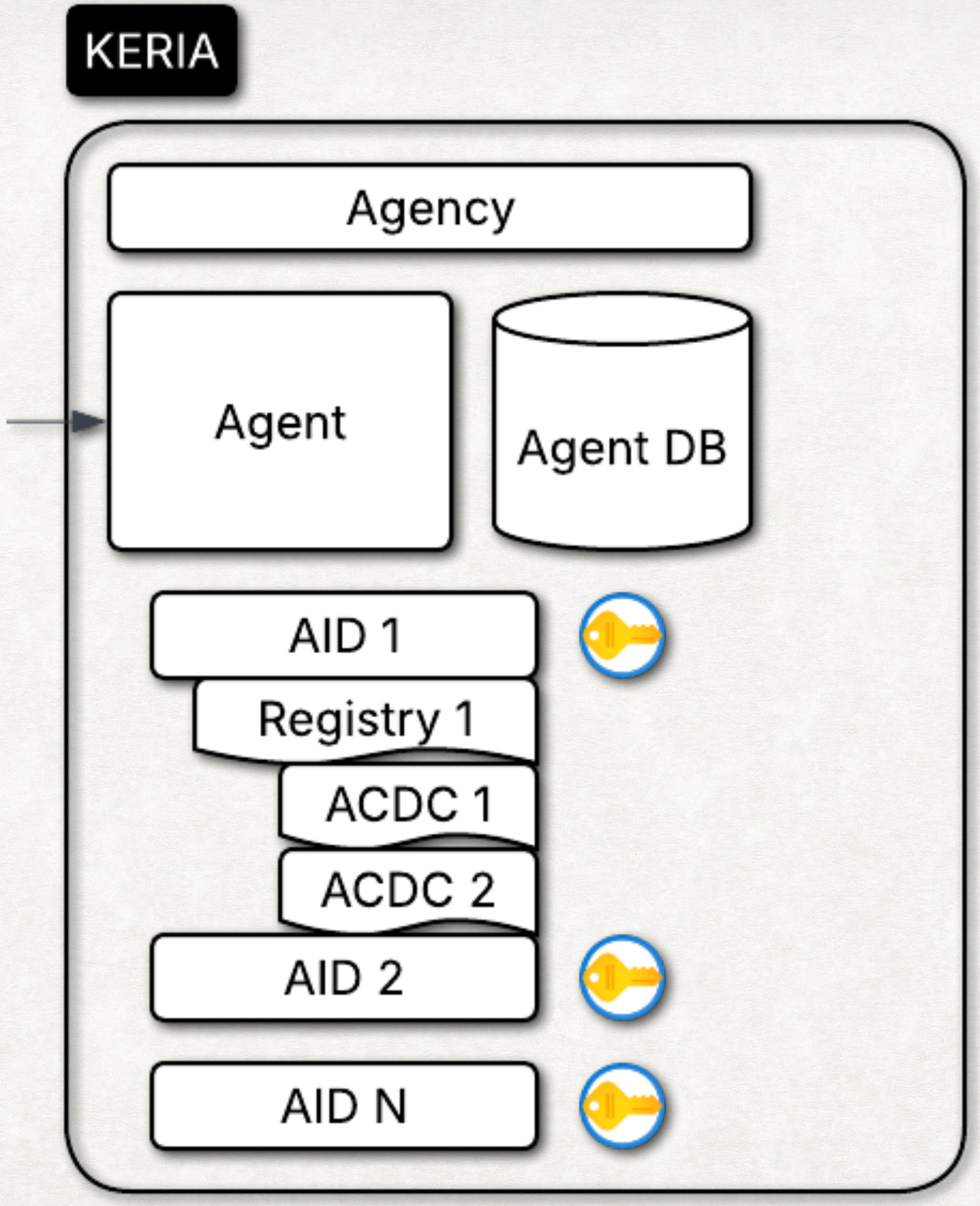
EDGE SIGNING ARCHITECTURE WITH AGENTS

LIGHTWEIGHT WALLET

- KERIA = KERI Agent
- The KERI Agent follows the SKWA Protocol
  - SKWA = Simple KERI for Web Auth
  - Original HackMD: https://hackmd.io/@SamuelMSmith/B1e03oGZY
  - Current WebOfTrust repo: https://github.com/WebOfTrust/skwa
- Basically, encryption key at the edge, identifier seed salts in the agent

WHAT IS THE AGENT?

Mailbox
Store and Forward
Mechanism



Delegation
Communication
Proxy

Cloud Storage for
Encrypted Key Seeds

Server Storage for
ACDCs, Contacts,
OOBIs, Challenges,
etc.

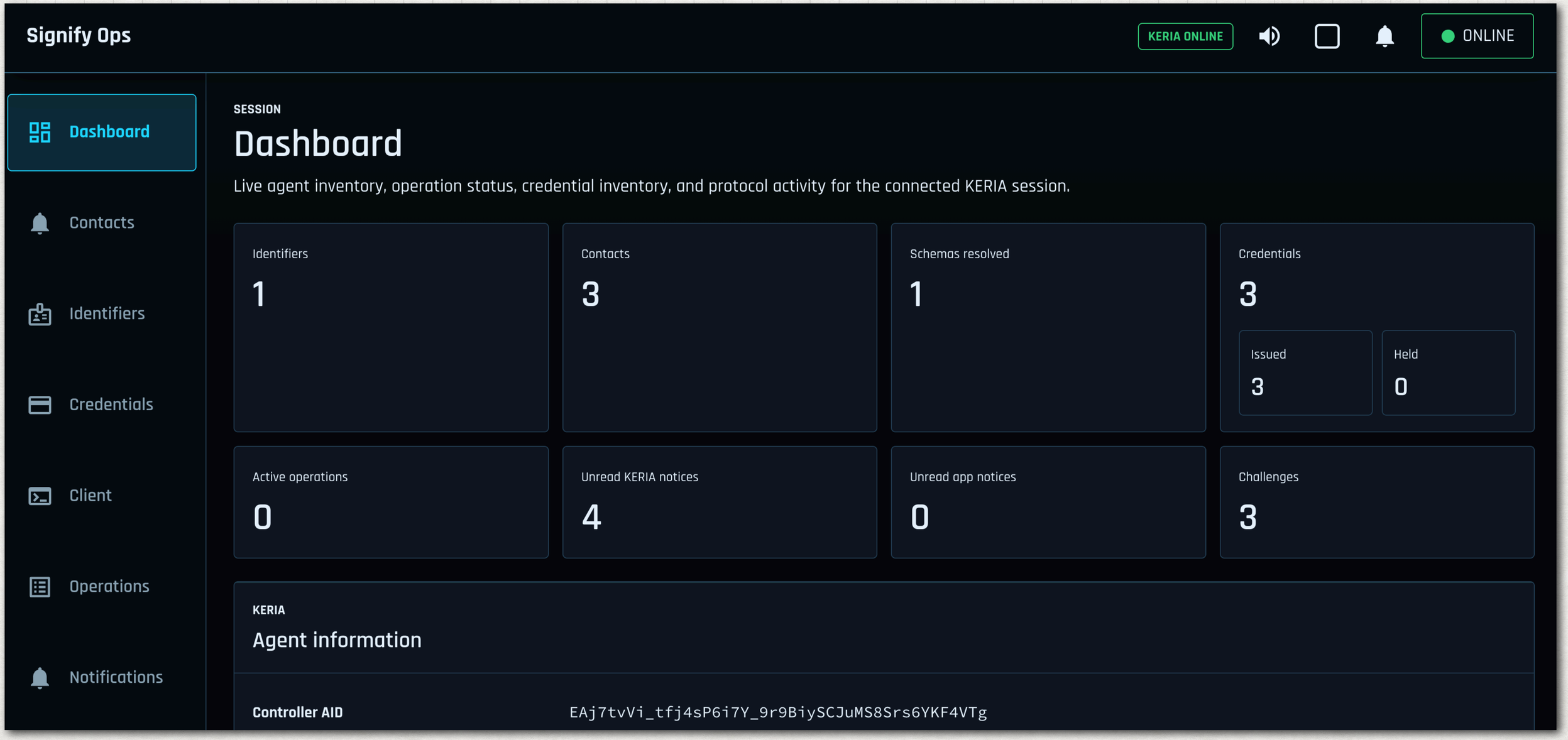
FEATURES OUTLINE

FUNCTIONALITY OVERVIEW

WHAT WE WILL COVER IN THIS PRESENTATION

- Client Creation - boot and connect
- Identifier Creation and Rotation
- OOBI Generation and Resolution
- Challenge Creation, Response, and Verification
- Credential Issuance, Grant, and Admit
- KERIA Configuration
- Signify Library Usage - latest is 0.3.0 as of April 21, 2026

DEMO


Signify Ops
KERIA ONLINE
ONLINE
Dashboard
Contacts
Identifiers
Credentials
Client
Operations
Notifications
SESSION
Dashboard
Live agent inventory, operation status, credential inventory, and protocol activity for the connected KERIA session.
Identifiers
1
Contacts
3
Schemas resolved
1
Credentials
3
Issued
3
Held
0
Active operations
0
Unread KERIA notices
4
Unread app notices
0
Challenges
3
KERIA
Agent information
Controller AID
EAj7tvVi_tfj4sP6i7Y_9r9BiySCJuMS8Srs6YKF4VTg

SIGNIFY ARCHITECTURE

SIGNIFY ARCHITECTURE

SIGNING AT THE EDGE

- Edge Controller - Signify Controller
- Signs Events
- Sends to delegated agent
- Agent is in KERIA!
- Agent handles identifiers, credentials, OOBIs, challenges, multisig, etc.
- Edge Libraries:
  - Signify TS, Signify Py

COMMON QUESTIONS, MISUNDERSTANDINGS, AND MISTAKES

WHAT IS THE PASSCODE?

WHERE ARE THE KEYS STORED?

WHAT IS ENCRYPTED AND DECRYPTED?

COMMON QUESTIONS, MISUNDERSTANDINGS, AND MISTAKES

AVOID THESE

- BAD: **Storing passcode in IndexedDB** / localStorage -> INSECURE
  - Any same-origin JS code can read and **exfiltrate**
  - If using Ionic/Capacitor use @evva/capacitor-secure-storage-plugin

COMMON QUESTIONS, MISUNDERSTANDINGS, AND MISTAKES

MISUNDERSTANDING

- Where are the keys stored?
  - Signify Controller key is edge encryption key
  - AID root salts are only ever unencrypted at the edge
  - AID root salts encrypted and stored in KERIA agent DB

COMMON QUESTIONS, MISUNDERSTANDINGS, AND MISTAKES

MISUNDERSTANDING

- CORS: by default CORS preflight OPTIONS requests are not handled
- Start KERIA with KERIA_AGENT_CORS=true
- ```
  KERI_AGENT_CORS=true keria start \
    --config-dir scripts \
    --config-file demo-witness-oobis \
    --name “keria" \
    --loglevel INFO
  ```
  ```

HOW IS MULTISIG HANDLED?

KERIA CONFIG

https://www.kentbull.com/posts/configuring-keripy-keria-controllers-witnesses/

Posts

2026-01-26 # Configuring KERIpy Controllers, Witnesses, and KERIA Agents

Configuring KERIpy Controllers, Witnesses, and KERIA Agents

Posted on 2026-01-26 :: Source Code:: #keri #keria #keripy #configuration #witnesses #controllers #agents #iurls #curls #durls #oobi

Configuring KERIpy Components, KERIA Agents, and Well-known URIs

KERIA CONFIGURATION POINTS

PHILOSOPHY AND GOTCHAS

- Philosophy: Config File First - Single File
  - Example in: keria/scripts/keri/cf/keria.json

```
{
  "dt": "2025-01-03T16:08:30.123456+00:00",
  "keria": {
    "dt": "2025-01-03T16:08:30.123457+00:00",
    "curls": ["http://127.0.0.1:3902/"]
  },
  "iurls": [
    "http://127.0.0.1:5642/oobi/BBilc4-L3tFUnfM_wJr4S4OJanAv_VmF_dJNN6vkf2Ha/controller?name=Wan&tag=witness",
    "http://127.0.0.1:5643/oobi/BLskRTInXnMxWaGqcpSyMgo0nYbalW99cGZESrz3zapM/controller?name=Wil&tag=witness",
    "http://127.0.0.1:5644/oobi/BIKKuvBwpmDVA4Ds-EpL5bt9OqPzWPja2LigFYZN2YfX/controller?name=Wes&tag=witness"
  ],
  "tocks": {
    "initer": 0.0,
    "escrower": 1.0
  }
}
```

LET'S ZOOM IN ON CONFIG

```
{
  "dt": "2025-01-03T16:08:30.123456+00:00",
  "keria": {
    "dt": "2025-01-03T16:08:30.123457+00:00",
    "curls": ["http://127.0.0.1:3902/"]
  },
  "iurls": [
    "http://127.0.0.1:5642/oobi/BBilc4-L3tFUnfM_wJr4S4OJanAv_VmF_dJNN6vkf2Ha/controller?name=Wan&tag=witness",
    "http://127.0.0.1:5643/oobi/BLskRTInXnMxWaGqcpSyMgo0nYbalW99cGZESrz3zapM/controller?name=Wil&tag=witness",
    "http://127.0.0.1:5644/oobi/BIKKuvBwpmDVA4Ds-EpL5bt9OqPzWPja2LigFYZN2YfX/controller?name=Wes&tag=witness"
  ],
  "tocks": {
    "initer": 0.0,
    "escrower": 1.0
  }
}
```

LET'S ZOOM IN ON CONFIG

```
{
  "dt": "2025-01-03T16:08:30.123456+00:00",
  "keria": {
    "dt": "2025-01-03T16:08:30.123457+00:00",
    "curls": ["http://127.0.0.1:3902/"]
  },
  "iurls": [
    "http://127.0.0.1:5642/oobi/BBilc4-L3tFUnfM_wJr4S4OJanAv_VmF_dJNN6vkf2Ha/controller?name=Wan&tag=witness",
    "http://127.0.0.1:5643/oobi/BLskRTInXnMxWaGqcpSyMgo0nYbalW99cGZESrz3zapM/controller?name=Wil&tag=witness",
    "http://127.0.0.1:5644/oobi/BIKKuvBwpmDVA4Ds-EpL5bt9OqPzWPja2LigFYZN2YfX/controller?name=Wes&tag=witness"
  ],
  "tocks": {
    "initer": 0.0,
    "escrower": 1.0
  }
}
```

NAMED AGENT CONFIG FOR CONTROLLER URLS - CURLS

```
{
  "dt": "2025-01-03T16:08:30.123456+00:00",
  "keria": {
    "dt": "2025-01-03T16:08:30.123457+00:00",
    "curls": ["http://127.0.0.1:3902/"]
  },
```

MUST have the named config blog so it will bind to ports specified in “curls” section

```
keria start --name "keria"
```

Default --name is “keria”

IURLS - OOBIS OF CONTACTS FOR AGENCY TO RESOLVE

```
  "keria": {
    "dt": "2025-01-03T16:08:30.123457+00:00",
    "curls": ["http://127.0.0.1:3902/"]
  },
  "iurls": [
    "http://127.0.0.1:5642/oobi/BBilc4-L3tFUnfM_wJr4S4OJanAv_VmF_dJNN6vkf2Ha/controller?name=Wan&tag=witness",
    "http://127.0.0.1:5643/oobi/BLskRTInXnMxWaGqcpSyMgo0nYbalW99cGZESrz3zapM/controller?name=Wil&tag=witness",
    "http://127.0.0.1:5644/oobi/BIKKuvBwpmDVA4Ds-EpL5bt9OqPzWPja2LigFYZN2YfX/controller?name=Wes&tag=witness"
  ],
  "tocks": {
    "initer": 0.0,
    "escrower": 1.0
  }
}
```

Bootstrap contacts for every agent in this KERIA server - this Agency

TOCKS - COROUTINE / HIO DOER RESCHEDULE TIME

```
11      ],
12      "tocks": {
13          "initer": 0.0,
14          "escrower": 1.0
15      }
16  }
```

Default is zero. Number of seconds, expressed as a float, to next scheduling

Long term processes expressed as coroutines.
Adjust for CPU and IO tuning.

DT - DATETIME - BADA-RUN

```
{
  "dt": "2025-01-03T16:08:30.123456+00:00",
  "keria": {
```

THIS IS REQUIRED!

Allows Best Available Data Acceptance, Read Update Nullify protection

Against config injection attacks.

KERIA checks this date time on startup to make sure it has the latest config.

Gets copied into each agent at agent boot time.

WHY USE KERIA?

WHY USE KERIA

IT IS A GOOD FIT WHEN...

- Lightweight wallet architecture useful
  - In-memory, edge signing
- Simple, multi-tenant architecture
- Many others use it
  - Provenant, Veridian, most GLEIF QVIs
- Simple Mailbox, Delegation Communication Proxy architecture

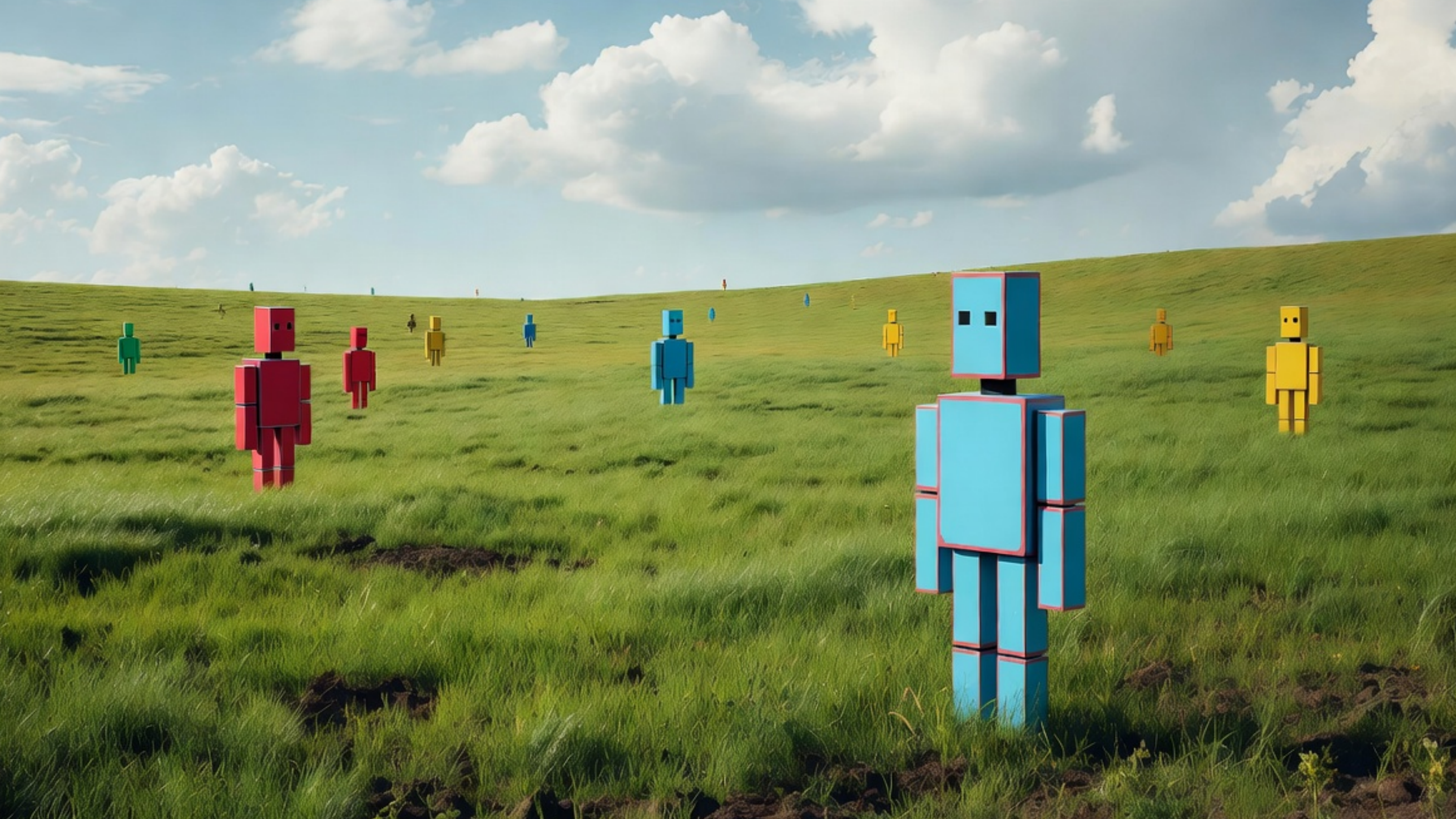
WHEN NOT TO USE KERIA

WHEN NOT TO USE KERI

IT IS A BAD FIT WHEN...

- Heavyweight wallet needed
- Doing an infrastructure only project
- Direct Mode
- Different Tenancy Architecture

CONFIGURING KERIA



END