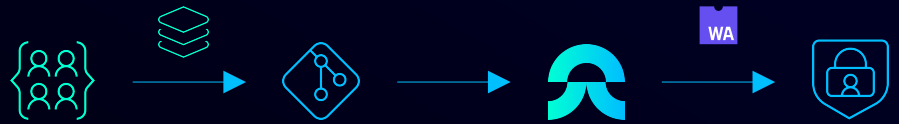
# Klave
# Trustless Confidential Computing Platform

# Klave

- Klave SDK
- GitHub integration
- WebAssembly
- Automatic deployments

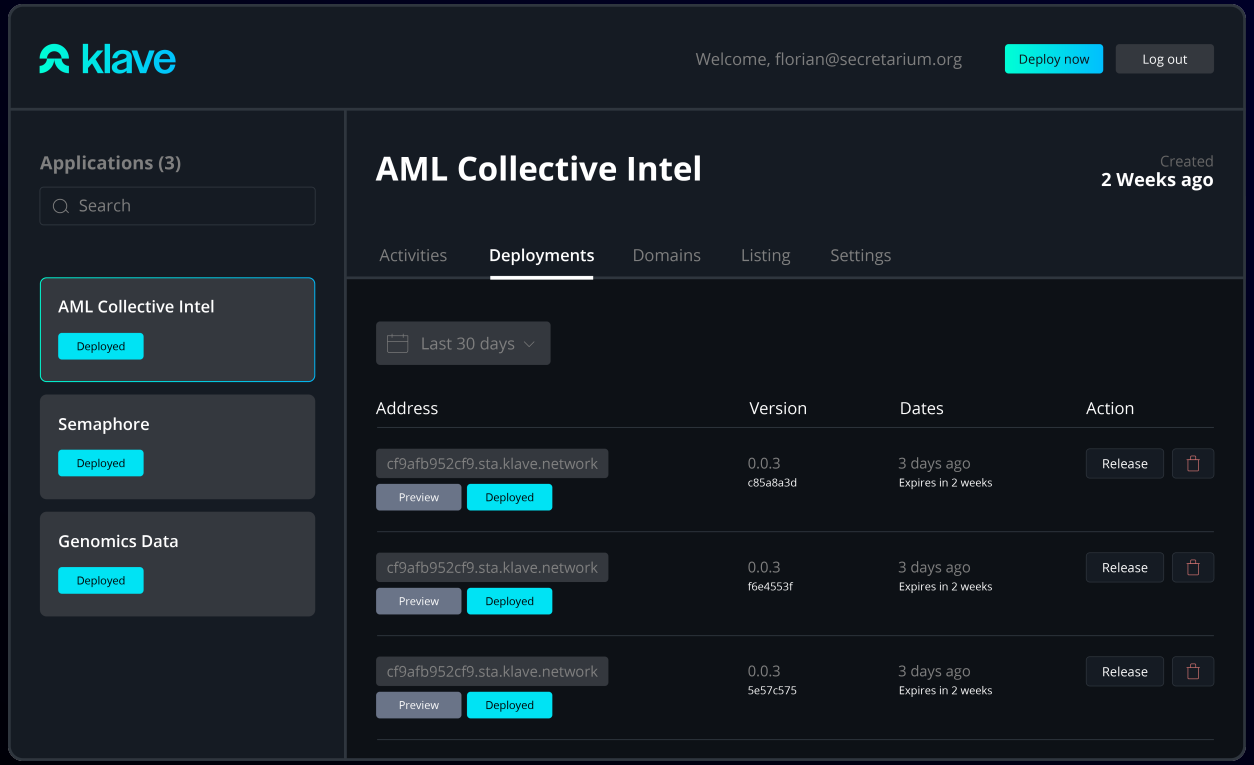


# Klave

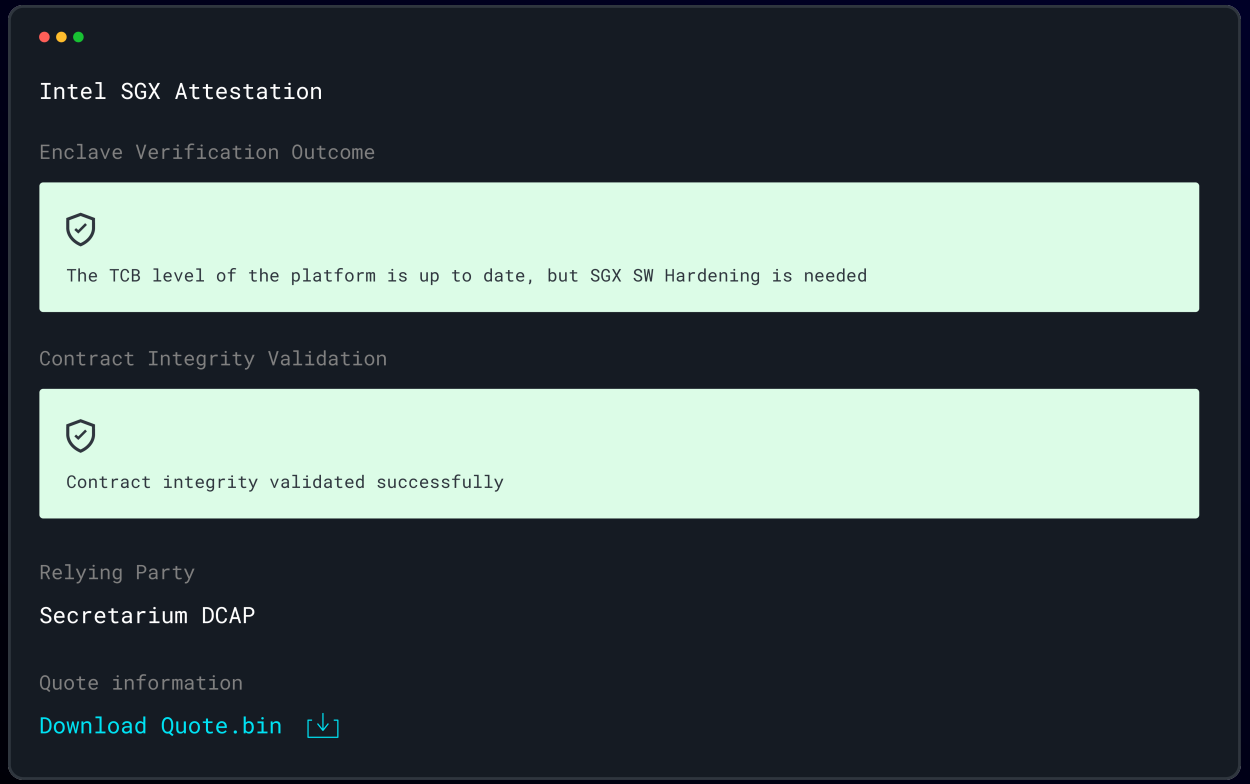
```
root@FG-XPS:~/demo# yarn create on-klave
yarncreate v1.22.19
[1/4] Resolving packages...
[2/4] Fetching packages...
[3/4] Linking packages...
[4/4] Building packages...

success Installed "create-on-klave@0.3.6" with binaries:
      - create-on-klave
      - create-trustless-app
✓ What is the package name?... my-trustless-app
✓ What is the name of your trustless application? My trustless application
✓ How would you describe the trustless application? A trustless application for the trustless network
✓ What is the name of the author?
✓ What is the email address of the author?
✓ What is the URL to the authors GitHub profile?
✓ What is the URL for the repository?

✓ Creating template files
✓ Installing dependencies
✓ Created an empty Git repository

✅ Successfully created a trustless application
Visit https://klave.com for the documentation on the trustless network
Done in 10.57s.
root@FG-XPS:~/demo#
```

```typescript
import { Notifier, Ledger, JSON } from '@Klave/sdk' ;
import { FetchInput, FetchOutput, StoreInput, StoreOutput, ErrorMessage }

const myTableName = "my_storage_table";

/**
 * @query
 * @param {FetchInput} input - A parsed input argument
 */
 export function fetchValue(input: FetchInput): void {

    let value = Ledger.getTable(myTableName).get(input.key);
    if (value.length === 0) {
        Notifier.sendJson<ErrorMessage>({
            success: false,
            message: 'key'${input.key} 'not found in table'
        });
    } else {
        Notifier.sendJson<FetchOutput>({
            success: true,
            value
        });
    }
}
```

# Klave


klave
Welcome, florian@secretarium.org
Deploy now
Log out
Applications (3)
Search
AML Collective Intel
Deployed
Semaphore
Deployed
Genomics Data
Deployed
AML Collective Intel
Created
2 Weeks ago
Activities
Deployments
Domains
Listing
Settings
Last 30 days
Address
Version
Dates
Action
cf9afb952cf9.sta.klave.network
Preview
Deployed
0.0.3
c85a8a3d
3 days ago
Expires in 2 weeks
Release
cf9afb952cf9.sta.klave.network
Preview
Deployed
0.0.3
f6e4553f
3 days ago
Expires in 2 weeks
Release
cf9afb952cf9.sta.klave.network
Preview
Deployed
0.0.3
5e57c575
3 days ago
Expires in 2 weeks
Release

# Klave


Intel SGX Attestation
Enclave Verification Outcome
The TCB level of the platform is up to date, but SGX SW Hardening is needed
Contract Integrity Validation
Contract integrity validated successfully
Relying Party
Secretarium DCAP
Quote information
Download Quote.bin

## Traditional computing

Trust boundary

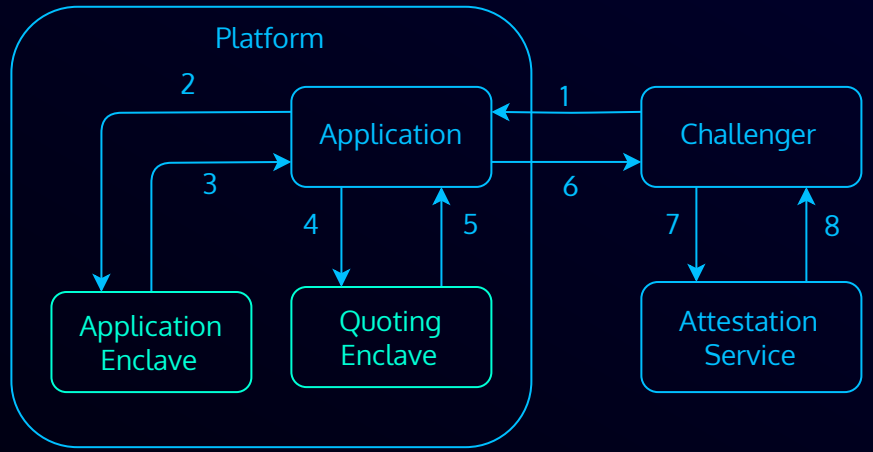
- Library
- Application
- Container
- Guest OS
- Hypervisor
- Host OS
- Firmware
- Infrastructure

## Confidential Computing

| Virtual Machine isolation | Container isolation | Application isolation | Library isolation |
|---|---|---|---|
| Trust boundary | Trust boundary | Trust boundary | Trust boundary |
| Library | Library | Library | Library |
| Application | Application | Application | Application |
| Container | Container | Container | Container |
| Guest OS | Guest OS | Guest OS | Guest OS |
| Hypervisor | Hypervisor | Hypervisor | Hypervisor |
| Host OS | Host OS | Host OS | Host OS |
| Firmware | Firmware | Firmware | Firmware |
| Infrastructure | Infrastructure | Infrastructure | Infrastructure |

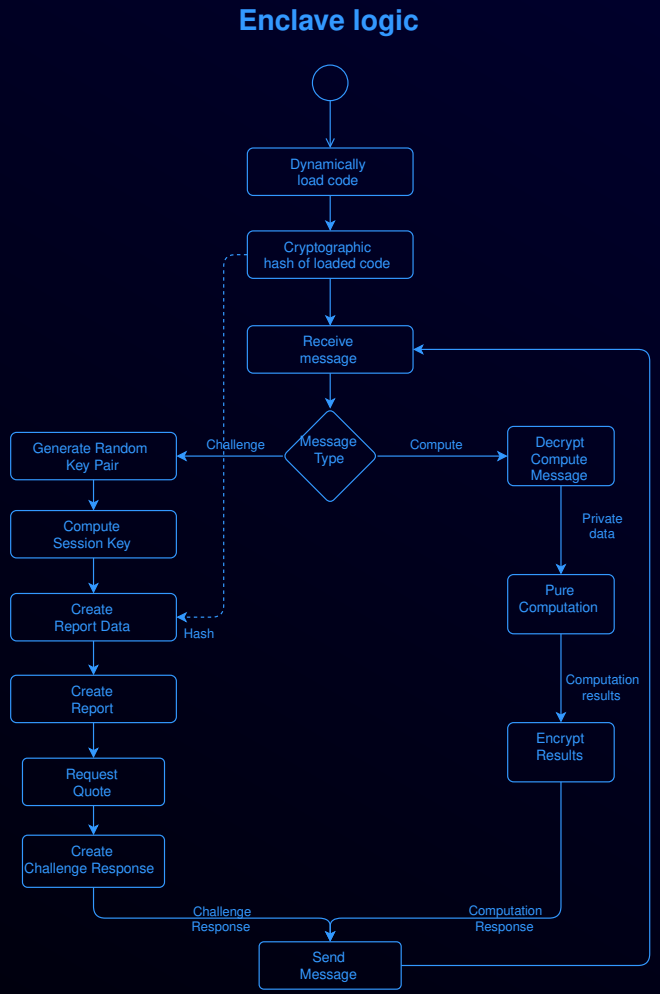
# Attestation

- 1, 2) Challenge (nonce)
- 3, 4) Generated report
- 5, 6) Signed report (quote)
- 7, 8) Verify quote



# Dynamic code

- Enclave is statically linked
- Report contains enclave measurement
- Dynamically loaded code are not part of the measurement
- Included in report data



# Technical concepts

Software development

Application domain

Cryptography

Confidential Computing

Formal verification

# Technical concepts

Software development

- Languages
- Toolchains
- Build systems

Application domain

Cryptography

Confidential Computing

Formal verification

# Technical concepts

Software development

Application domain

- ID
- Healthcare
- Digital cash

Cryptography

Confidential Computing

Formal verification

# Technical concepts

Software development

Application domain

Cryptography

- Algorithms
- Maths
- Computing advances

Confidential Computing

Formal verification

# Technical concepts

Software development

Application domain

Cryptography

Confidential Computing

- TEE implementations
- Threat model
- New field

Formal verification

# Technical concepts

Software development

Application domain

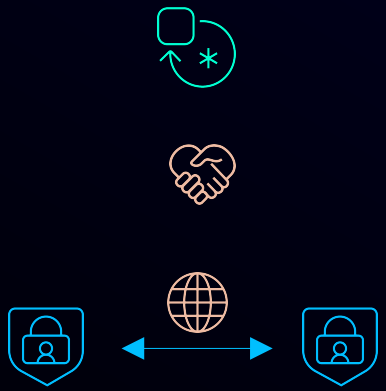
Cryptography

Confidential Computing

Formal verification

- Frameworks
- Ecosystem
- Accessible

# Verification



Deterministic builds

Messaging protocol

Enclave-to-Enclave communication

Data storage

Data migration

# App permissions

Data Linked to You

- Location
- Contact Info
- User Content
- Identifiers
- Usage Data
- Diagnostics

Data Not Linked to You

- Diagnostics

# App permissions

Data Linked to You

- Location
- Contact Info
- User Content
- Identifiers
- Usage Data
- Diagnostics

Data Not Linked to You

- Diagnostics

klave

- Verified by TU Dresden
- E2E encrypted
- No data shared with other apps
- App isolated storage
- User-controlled data migrations

klave

Klave.com

https://linkedin.com/in/rui-almeida-9a467321

# Thank you