A Transparent Certification Scheme Based on Blockchain for Service-Based Systems

Nicola Bena[1] Marco Pedrinazzi[1] Marco Anisetti[1] Omar Hasan[2] Lionel Brunie[2]

[1]Department of Computer Science, Università degli Studi di Milano

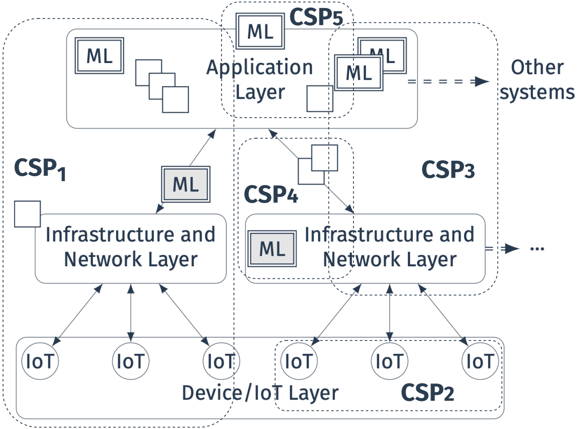
[2]LIRIS Lab, INSA Lyon

The work was partially supported by *i)* project MUSA - Multilayered Urban Sustainability Action - project, funded by the European Union - NextGenerationEU, under the National Recovery and Resilience Plan (NRRP) Mission 4 Component 2 Investment Line 1.5: Strengthening of research structures and creation of R&D "innovation ecosystems", set up of "territorial leaders in R&D" (CUP G43C22001370007, Code ECS00000037); *ii)* project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NextGenerationEU; *iii)* Università degli Studi di Milano via the program "piano sostegno alla ricerca" and "One Health Action Hub: University Task Force for the resilience of territorial ecosystems" – PSR 2021 – GSA – Linea 6; *iv)* SCUSI projet – Région Auvergne-Rhône-Alpes.

Scenario

Modern service-based systems

- confluence of cloud-edge-IoT
- multi-layer structure
- ML-based services and infrastructure
- dynamic, non-deterministic, and unpredictable behavior

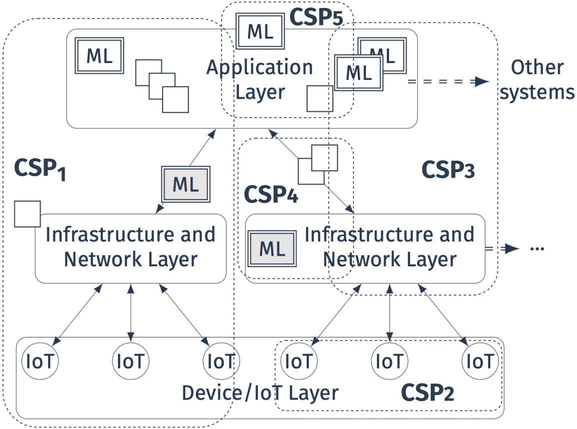


Scenario

Modern service-based systems

- impact of AI by 2030: $13 trillion[a]
- number of connected devices by 2023: 29.3 bln[b]
- economic impact of cloud-edge-IoT by 2025: $2.7–6.2 trillion[c]

[a] Source: McKinsey
[b] Source: Cisco
[c] Source: McKinsey

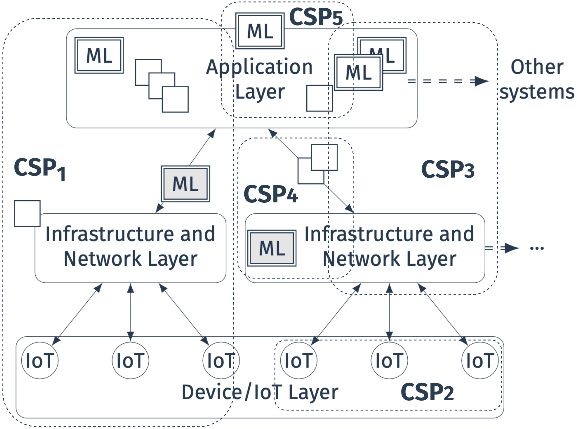


Scenario

Modern service-based systems

- increasing pervasiveness
- increasing risk for security, safety, and privacy
- lack of trustworthiness
  - full/partial lose of control on data/applications
  - lack of evidence about service operation and effectiveness

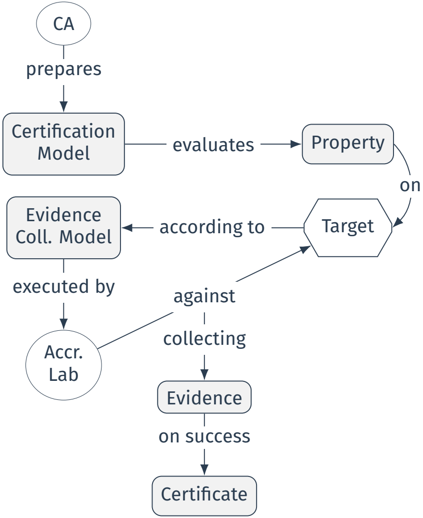
⟹ assurance based-certification to the rescue



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

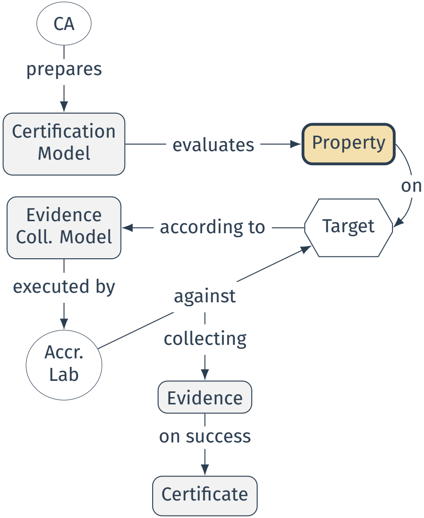
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

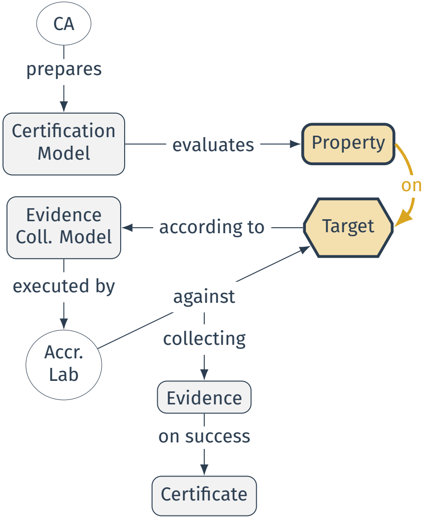
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

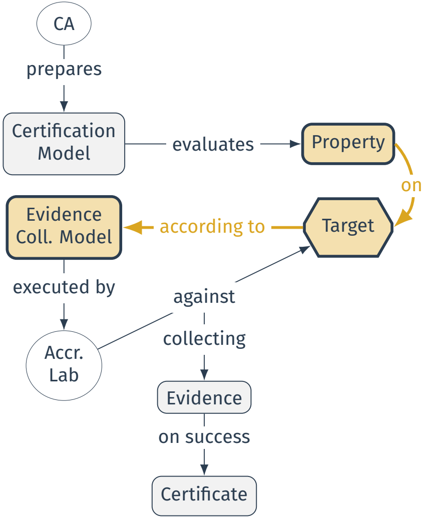
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

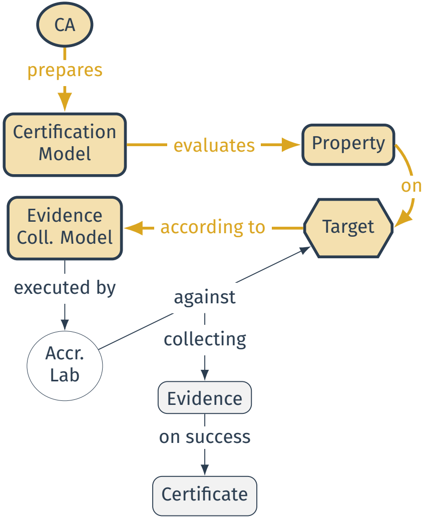
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

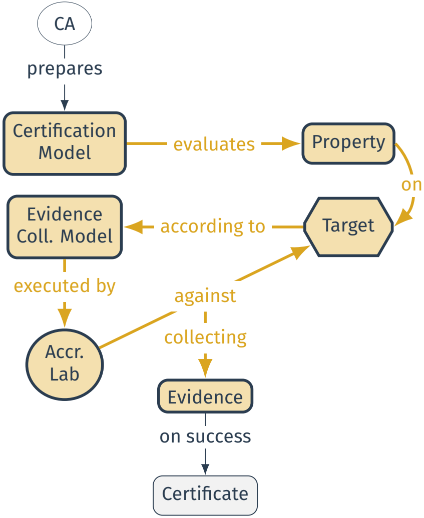
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

Certification scheme implements the certification (meta-)process, according to

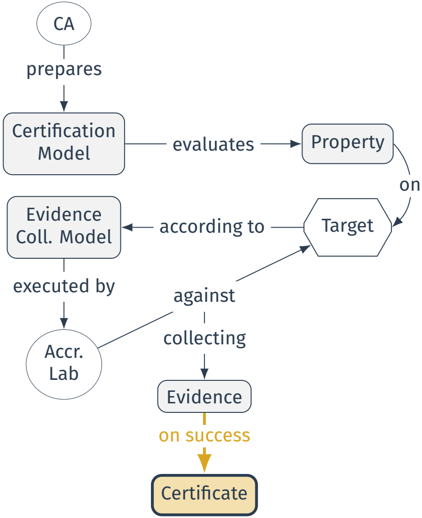
- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification Scheme

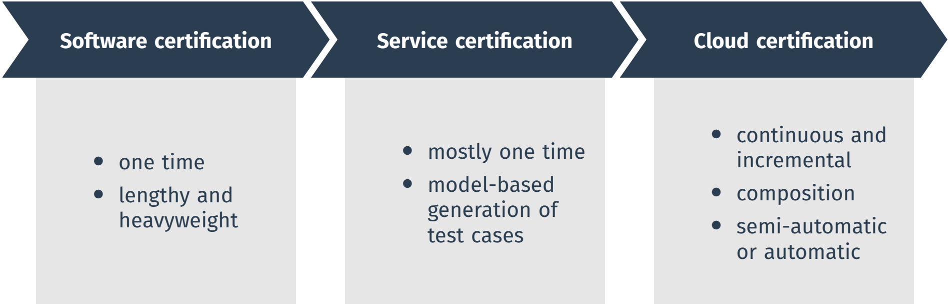
Certification scheme implements the certification (meta-)process, according to

- non-functional property
- target of certification
- evidence collection model
- certification model
- evidence
- certificate



Certification

Certification scheme details the certification process verifying that a target system behaves as expected and demonstrates one or more non-functional properties...



Software certification

- one time
- lengthy and heavyweight

Service certification

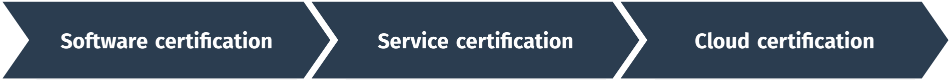
- mostly one time
- model-based generation of test cases

Cloud certification

- continuous and incremental
- composition
- semi-automatic or automatic

Certification

… but some assumptions remain the same



Software certification

- one time
- lengthy and heavyweight

Service certification

- mostly one time
- model-based generation of test cases

Cloud certification

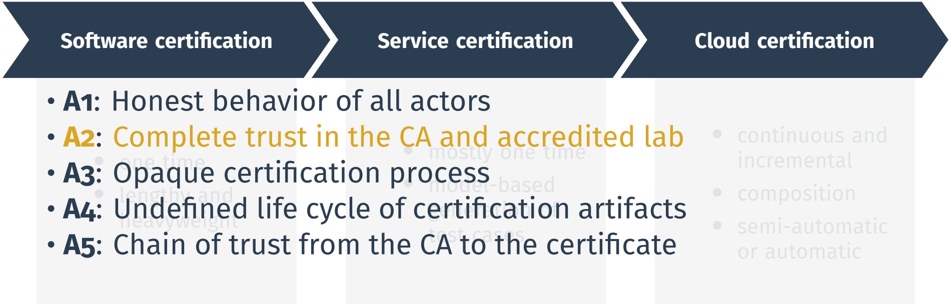
- continuous and incremental
- composition
- semi-automatic or automatic

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Certification

... but some assumptions remain the same

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate



Software certification

- one time
- lengthy and heavyweight

Service certification

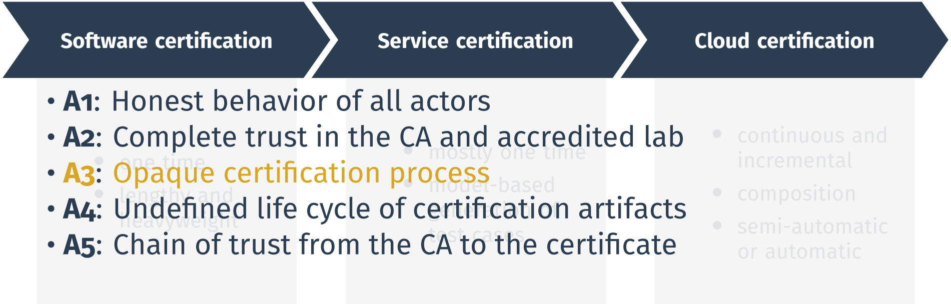
- mostly one time
- model-based
- generation of test cases

Cloud certification

- continuous and incremental
- composition
- semi-automatic or automatic

Certification

… but some assumptions remain the same



Software certification

- one time
- lengthy and heavyweight

Service certification

- mostly one time
- model-based generation of test cases

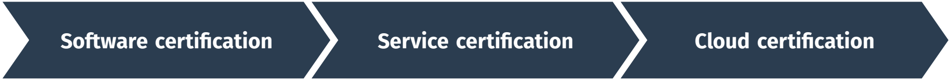
Cloud certification

- continuous and incremental
- composition
- semi-automatic or automatic

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Certification

... but some assumptions remain the same



Software certification

- one time
- lengthy and heavyweight

Service certification

- mostly one time
- model-based generation of test cases

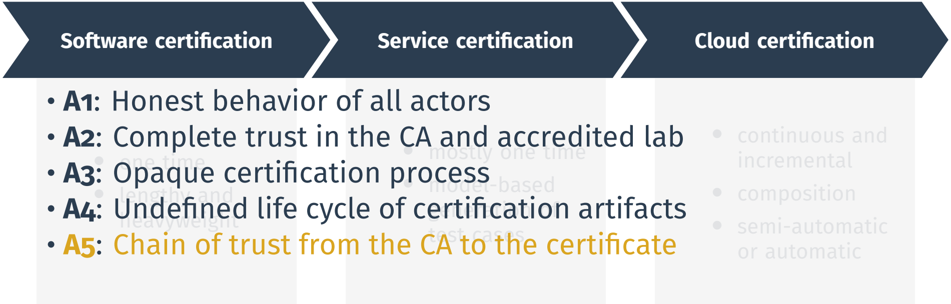
Cloud certification

- continuous and incremental
- composition
- semi-automatic or automatic

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Certification

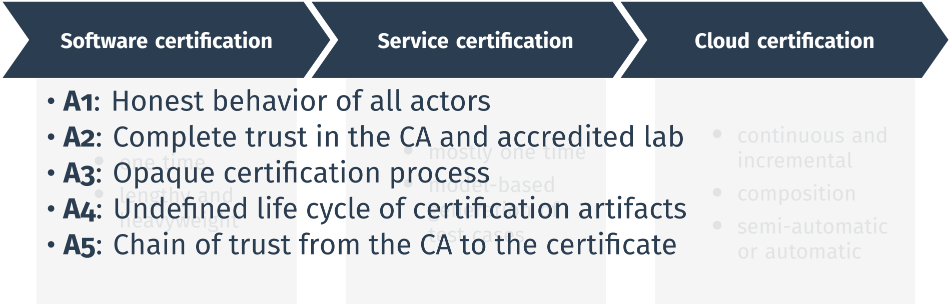
… but some assumptions remain the same



- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Certification

… but some assumptions remain the same



Software certification

- one time
- lengthy and heavyweight

Service certification

- mostly one time
- model-based generation of test cases

Cloud certification

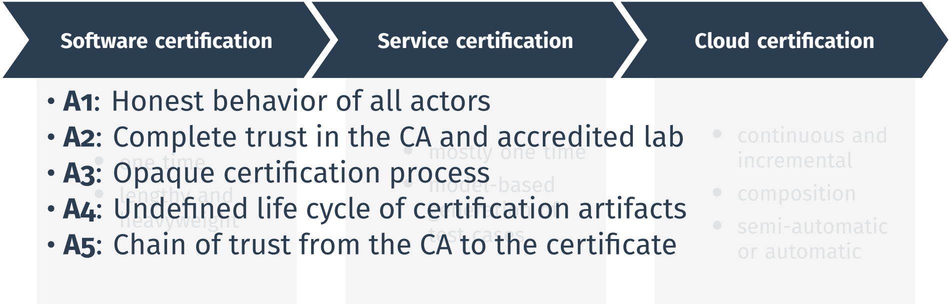
- continuous and incremental
- composition
- semi-automatic or automatic

- **A1:** Honest behavior of all actors
- **A2:** Complete trust in the CA and accredited lab
- **A3:** Opaque certification process
- **A4:** Undefined life cycle of certification artifacts
- **A5:** Chain of trust from the CA to the certificate

Are these assumptions acceptable in today's service world?

Certification

... but some assumptions remain the same



Software certification

- one time
- lengthy and heavyweight

Service certification

- mostly one time
- model-based
- generation of test cases

Cloud certification

- continuous and incremental
- composition
- semi-automatic or automatic

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Are these assumptions acceptable in today’s service world? NO!

Our Approach

⟹ Blockchain-based certification

Move the certification process and its actors to the blockchain

Our Approach

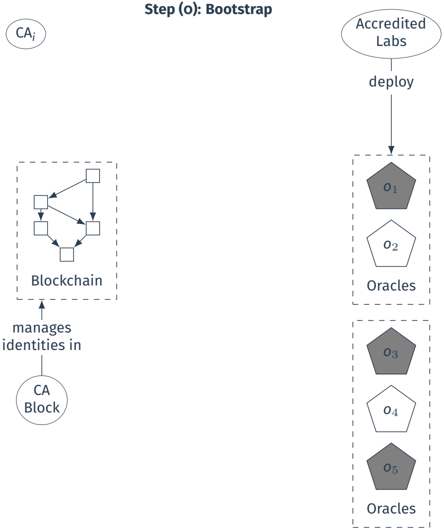
$\Longrightarrow$ Blockchain-based certification

Move the certification process and its actors to the blockchain

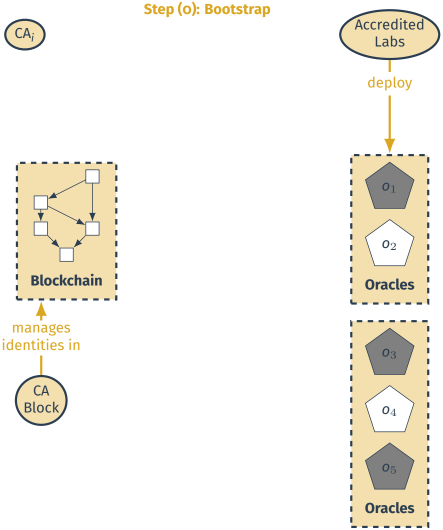
- certification model and certificate implemented as immutable, visible, and traceable smart contracts
- evidence is collected through *oracles*
- each probe is executed in multiple oracles (*fan-out*)
  - individual evidence is then retrieved through aggregation (*fan-in*)

Blockchain-Based Certification Process

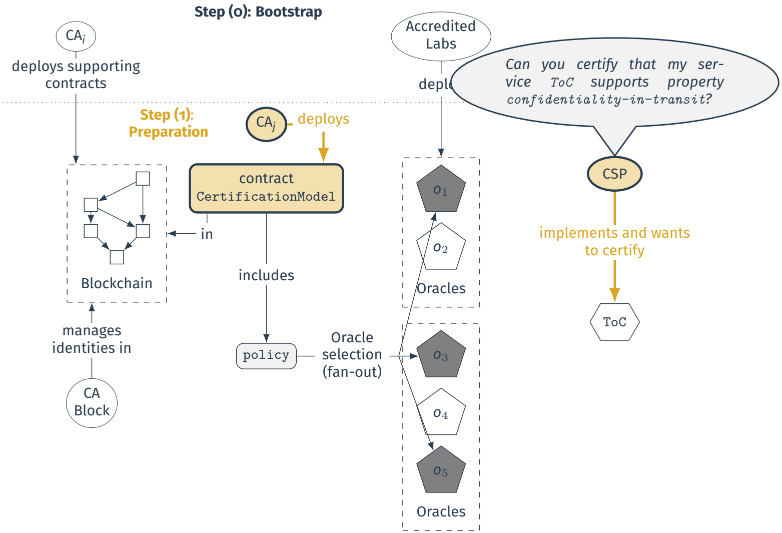
Step (0): Bootstrap



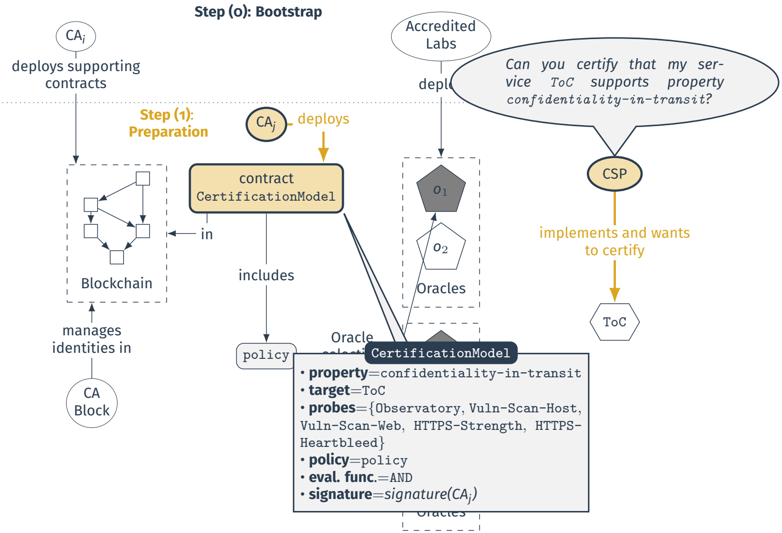
Blockchain-Based Certification Process



Blockchain-Based Certification Process


Step (0): Bootstrap
CA_i
deploys supporting contracts
Accredited Labs
depl
Can you certify that my service ToC supports property confidentiality-in-transit?
Step (1): Preparation
CA_j
deploys
contract CertificationModel
in
Blockchain
includes
manages identities in
CA Block
policy
Oracle selection (fan-out)
o_1
o_2
Oracles
o_3
o_4
o_5
Oracles
CSP
implements and wants to certify
ToC

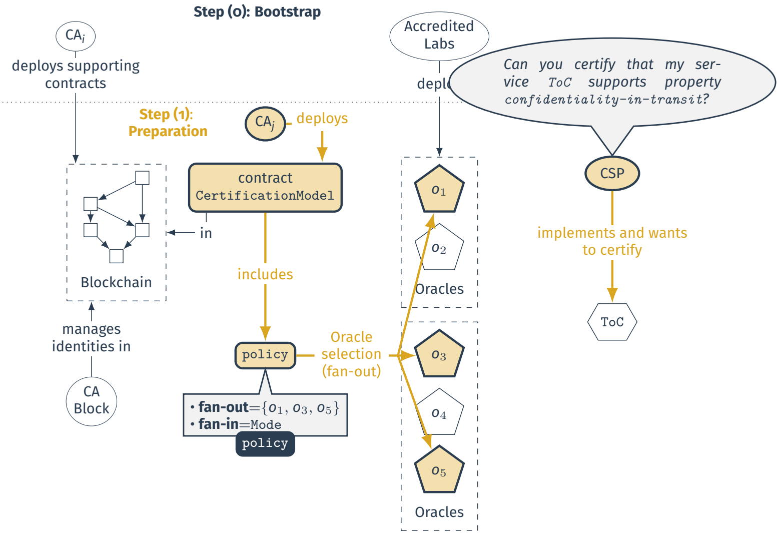
Blockchain-Based Certification Process



CertificationModel

- **property**=confidentiality-in-transit
- **target**=ToC
- **probes**={Observatory, Vuln-Scan-Host, Vuln-Scan-Web, HTTPS-Strength, HTTPS-Heartbleed}
- **policy**=policy
- **eval. func.**=AND
- **signature**=*signature*(CA_j)

Blockchain-Based Certification Process



Step (0): Bootstrap

CA$_i$

deploys supporting contracts

Accredited Labs

depl

Can you certify that my service `ToC` *supports property* `confidentiality-in-transit`*?*

Step (1): Preparation

CA$_j$

deploys

contract `CertificationModel`

in

Blockchain

manages identities in

CA Block

includes

`policy`

Oracle selection (fan-out)

- **fan-out**$=\{o_1, o_3, o_5\}$
- **fan-in**$=$`Mode`

`policy`

o_1

o_2

Oracles

o_3

o_4

o_5

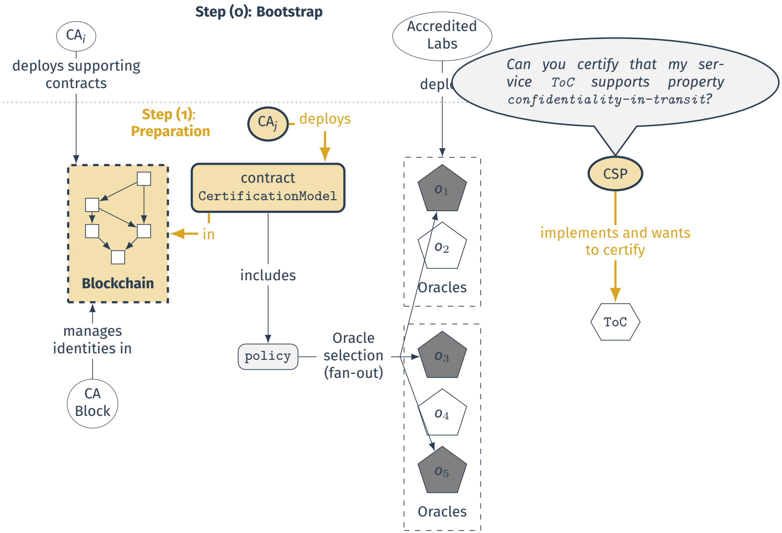
Oracles

CSP

implements and wants to certify

ToC

Blockchain-Based Certification Process



Step (0): Bootstrap

CA_i deploys supporting contracts

Accredited Labs depl

Step (1): Preparation

CA_j deploys

contract CertificationModel

in

Blockchain

manages identities in

CA Block

includes

policy

Oracle selection (fan-out)

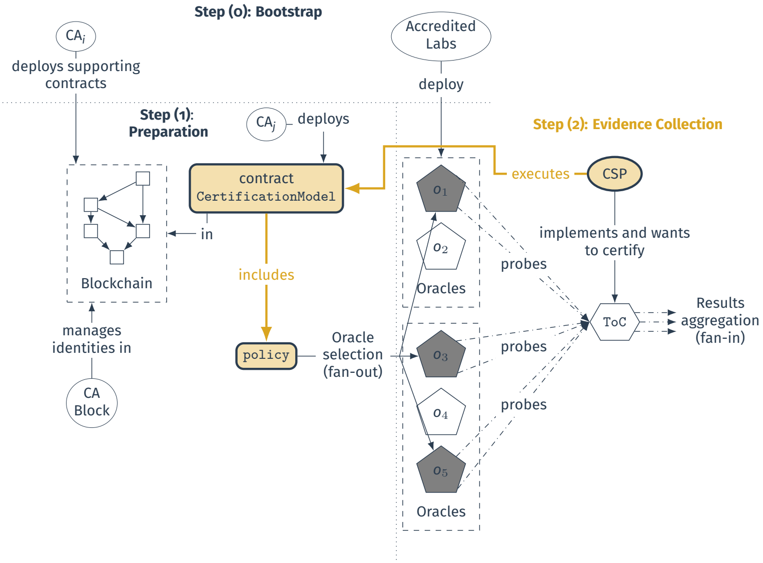
Can you certify that my service ToC supports property confidentiality-in-transit?

CSP

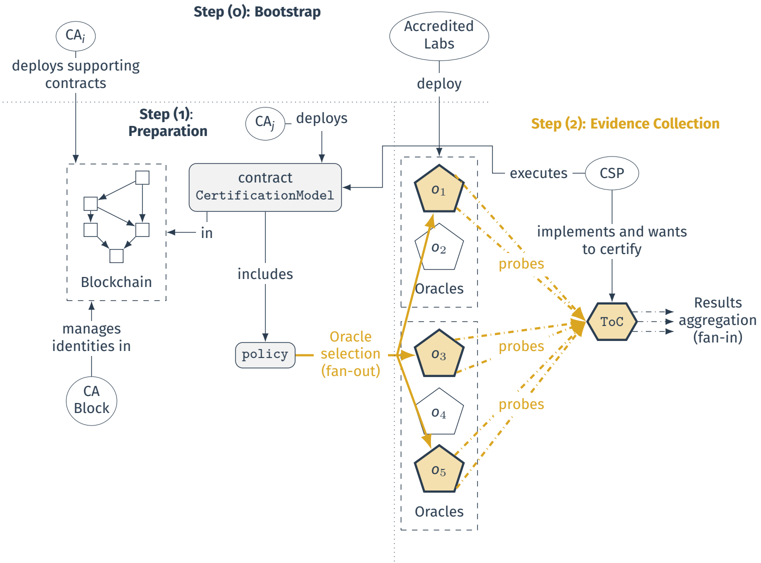
implements and wants to certify

ToC

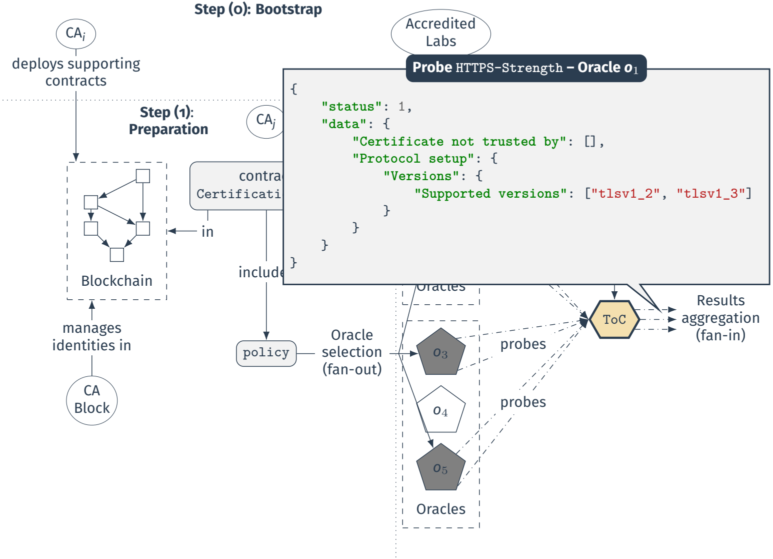
Blockchain-Based Certification Process



Blockchain-Based Certification Process



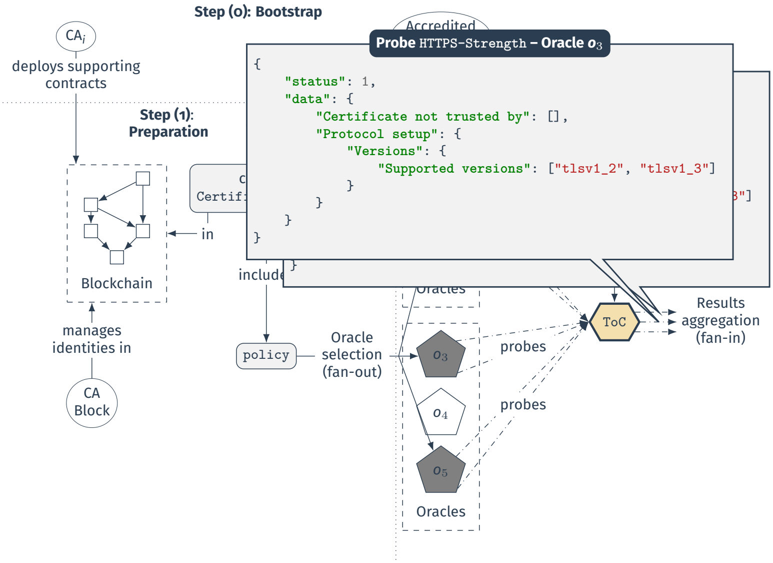
Blockchain-Based Certification Process



Probe `HTTPS-Strength` **– Oracle o_1**

```
{
    "status": 1,
    "data": {
        "Certificate not trusted by": [],
        "Protocol setup": {
            "Versions": {
                "Supported versions": ["tlsv1_2", "tlsv1_3"]
            }
        }
    }
}
```

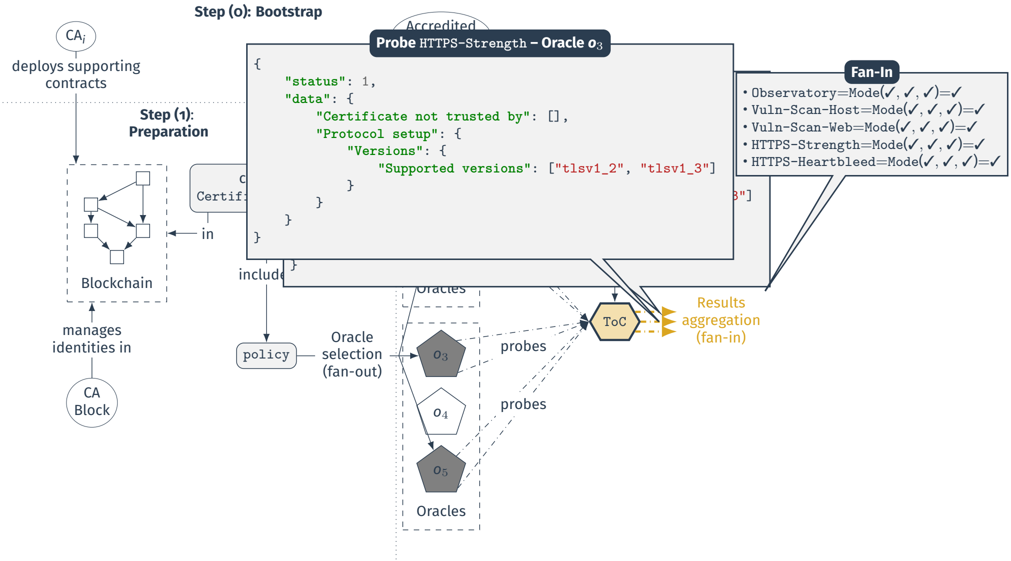
Blockchain-Based Certification Process



Probe `HTTPS-Strength` **– Oracle o_3**

```
{
    "status": 1,
    "data": {
        "Certificate not trusted by": [],
        "Protocol setup": {
            "Versions": {
                "Supported versions": ["tlsv1_2", "tlsv1_3"]
            }
        }
    }
}
```

Blockchain-Based Certification Process



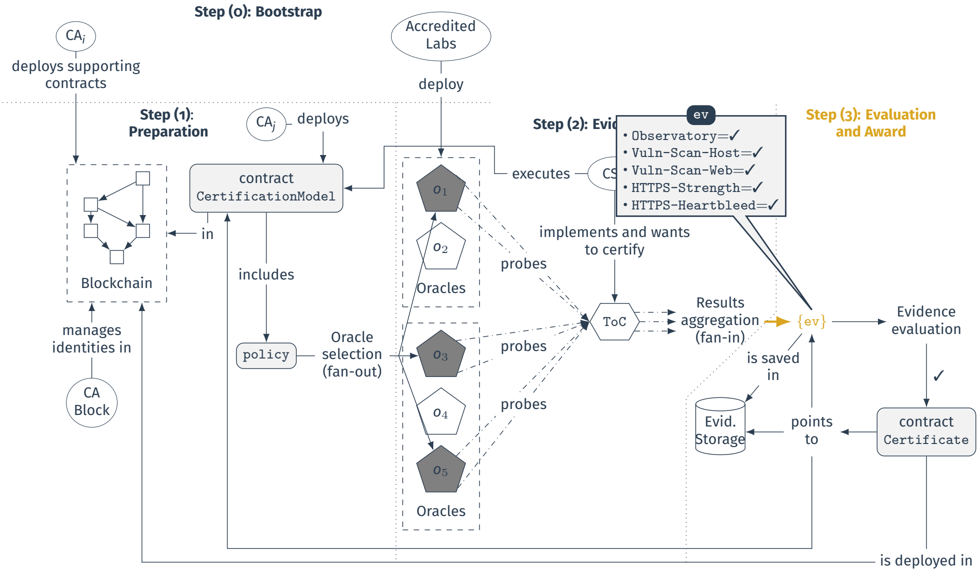
Probe `HTTPS-Strength` **– Oracle o_3**

```
{
    "status": 1,
    "data": {
        "Certificate not trusted by": [],
        "Protocol setup": {
            "Versions": {
                "Supported versions": ["tlsv1_2", "tlsv1_3"]
            }
        }
    }
}
```

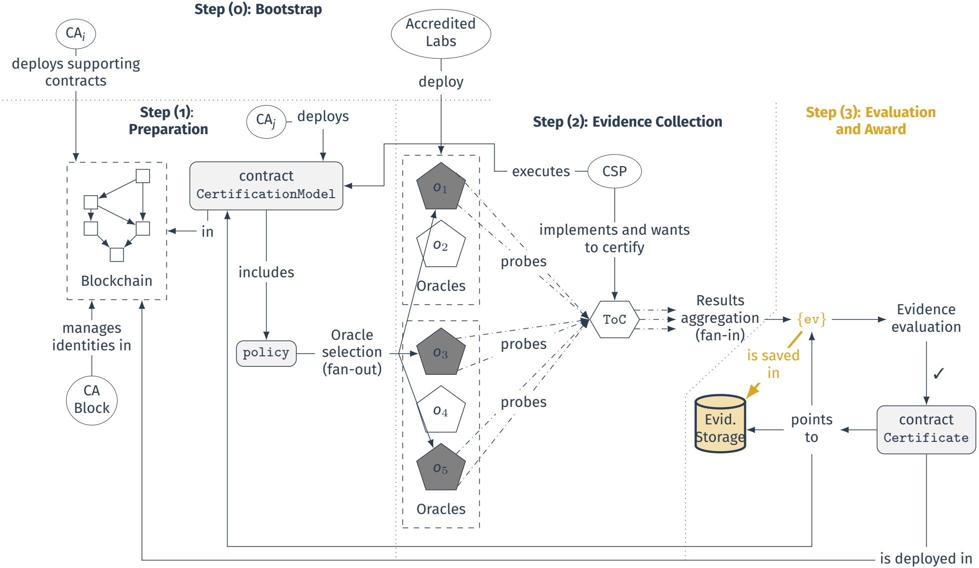
Fan-In

- `Observatory`=`Mode`(✓, ✓, ✓)=✓
- `Vuln-Scan-Host`=`Mode`(✓, ✓, ✓)=✓
- `Vuln-Scan-Web`=`Mode`(✓, ✓, ✓)=✓
- `HTTPS-Strength`=`Mode`(✓, ✓, ✓)=✓
- `HTTPS-Heartbleed`=`Mode`(✓, ✓, ✓)=✓

Blockchain-Based Certification Process



Blockchain-Based Certification Process



Step (0): Bootstrap

CA_i

deploys supporting contracts

Accredited Labs

deploy

Step (1): Preparation

CA_j deploys

contract CertificationModel

in

Blockchain

includes

policy

Oracle selection (fan-out)

manages identities in

CA Block

Step (2): Evidence Collection

o_1

o_2

Oracles

o_3

o_4

o_5

Oracles

executes

CSP

implements and wants to certify

probes

probes

probes

ToC

Results aggregation (fan-in)

Step (3): Evaluation and Award

{ev}

is saved in

Evid. Storage

Evidence evaluation

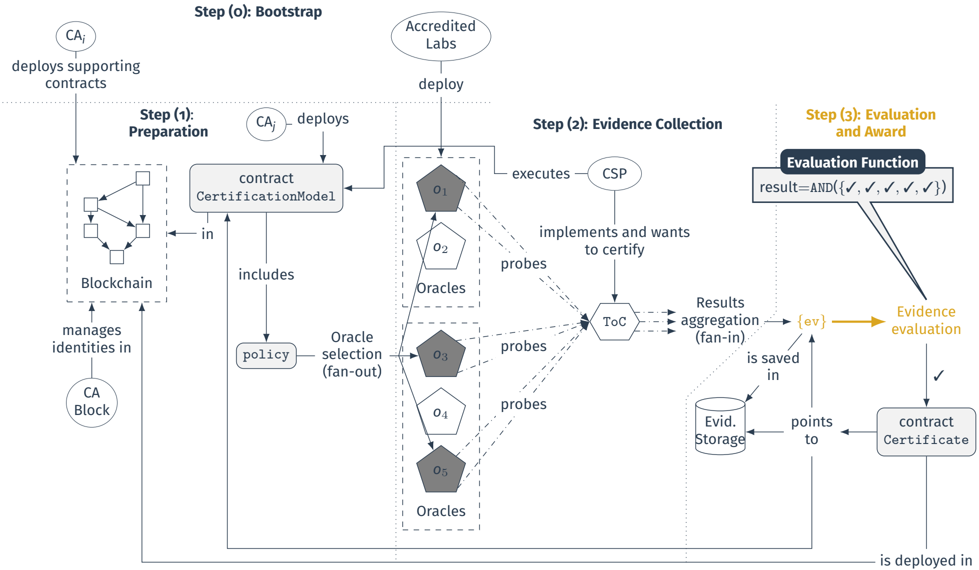
✓

contract Certificate

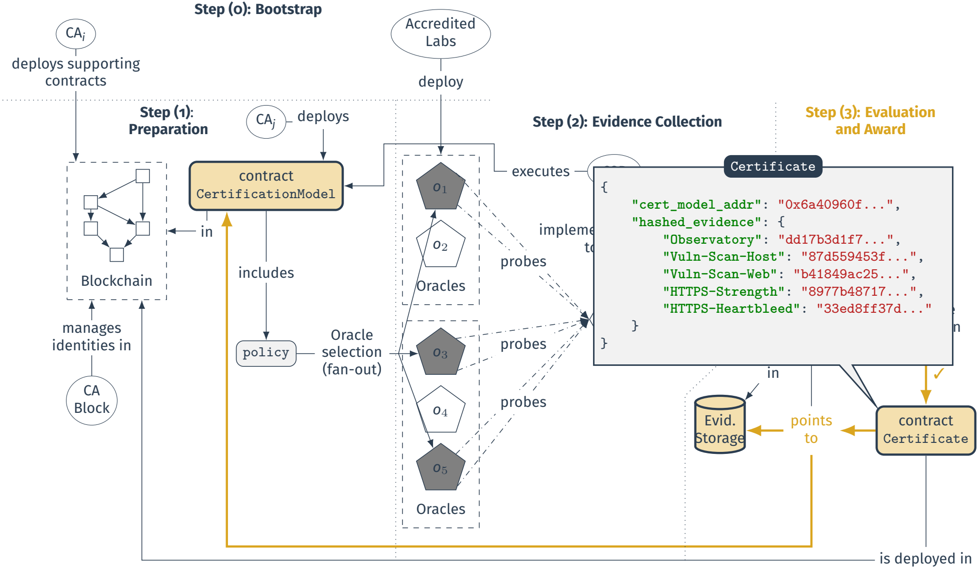
points to

is deployed in

Blockchain-Based Certification Process

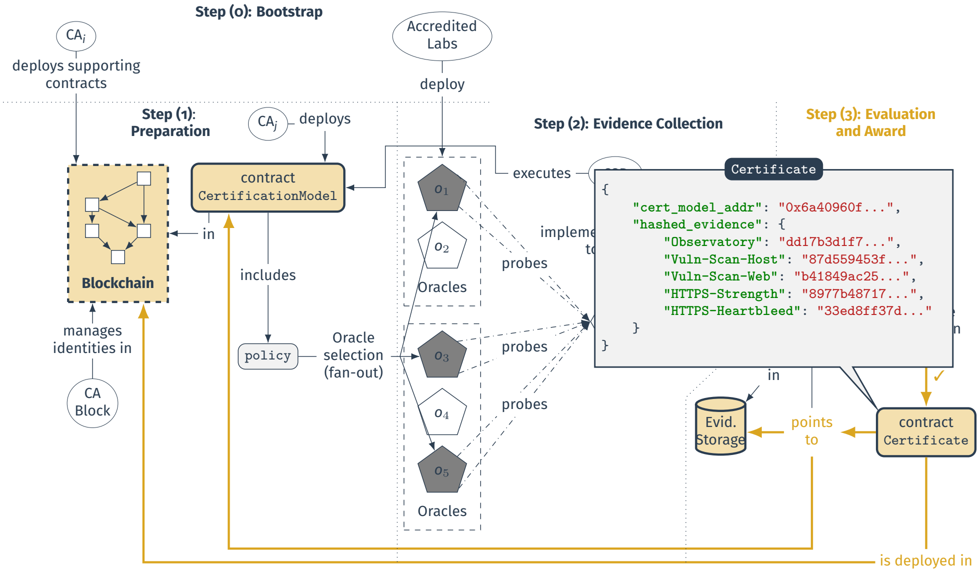


Blockchain-Based Certification Process



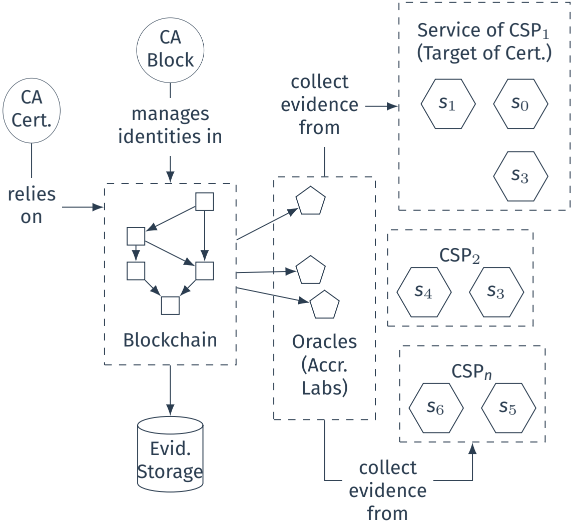
```
{
    "cert_model_addr": "0x6a40960f...",
    "hashed_evidence": {
        "Observatory": "dd17b3d1f7...",
        "Vuln-Scan-Host": "87d559453f...",
        "Vuln-Scan-Web": "b41849ac25...",
        "HTTPS-Strength": "8977b48717...",
        "HTTPS-Heartbleed": "33ed8ff37d..."
    }
}
```

Blockchain-Based Certification Process



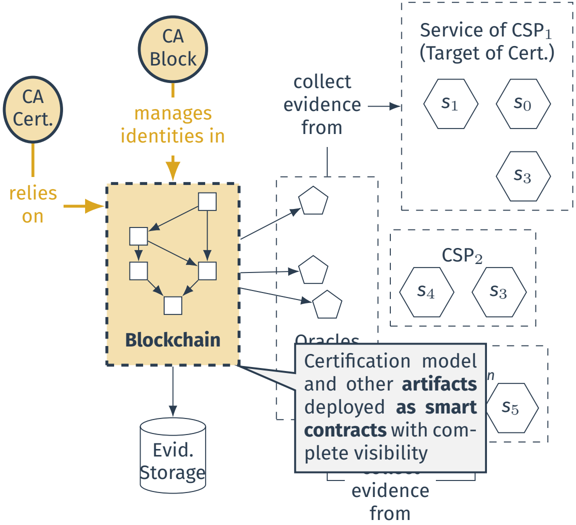
```
{
    "cert_model_addr": "0x6a40960f...",
    "hashed_evidence": {
        "Observatory": "dd17b3d1f7...",
        "Vuln-Scan-Host": "87d559453f...",
        "Vuln-Scan-Web": "b41849ac25...",
        "HTTPS-Strength": "8977b48717...",
        "HTTPS-Heartbleed": "33ed8ff37d..."
    }
}
```

Blockchain-Based Certification



- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

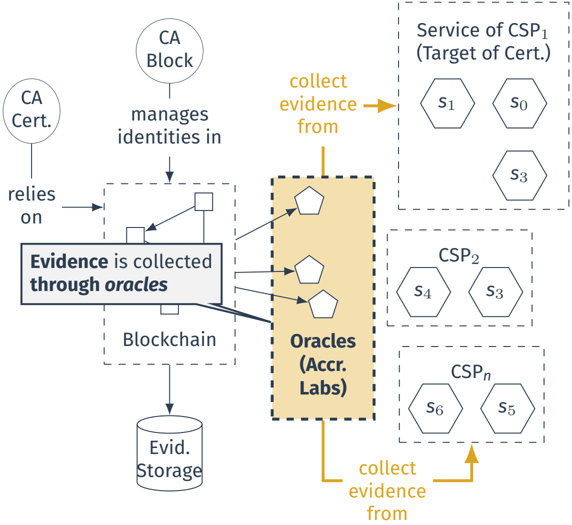
Blockchain-Based Certification



Certification model and other **artifacts** deployed **as smart contracts** with complete visibility

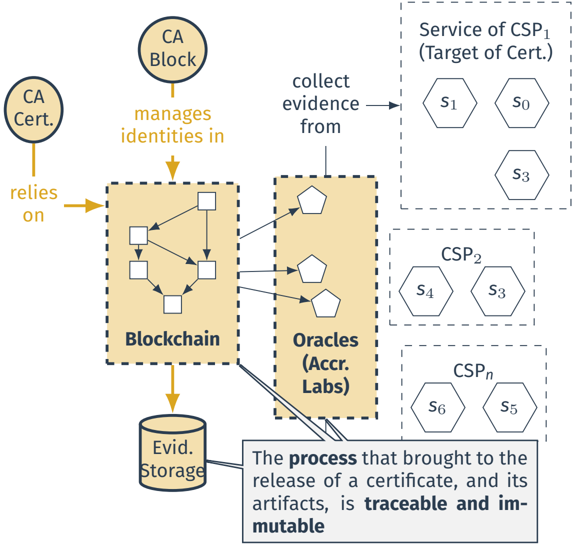
- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

Blockchain-Based Certification



- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

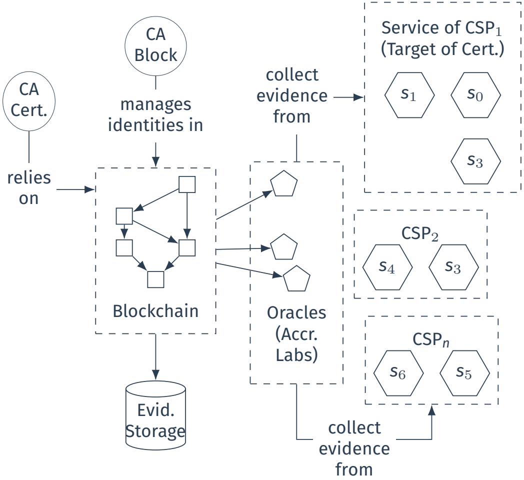
Blockchain-Based Certification



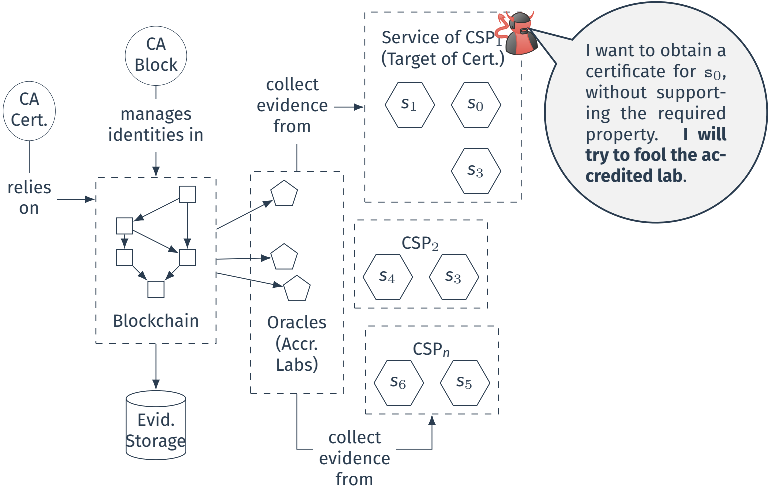
The **process** that brought to the release of a certificate, and its artifacts, is **traceable and immutable**

- **A1**: Honest behavior of all actors
- **A2**: Complete trust in the CA and accredited lab
- **A3**: Opaque certification process
- **A4**: Undefined life cycle of certification artifacts
- **A5**: Chain of trust from the CA to the certificate

What Happens When Actors are Misbehaving

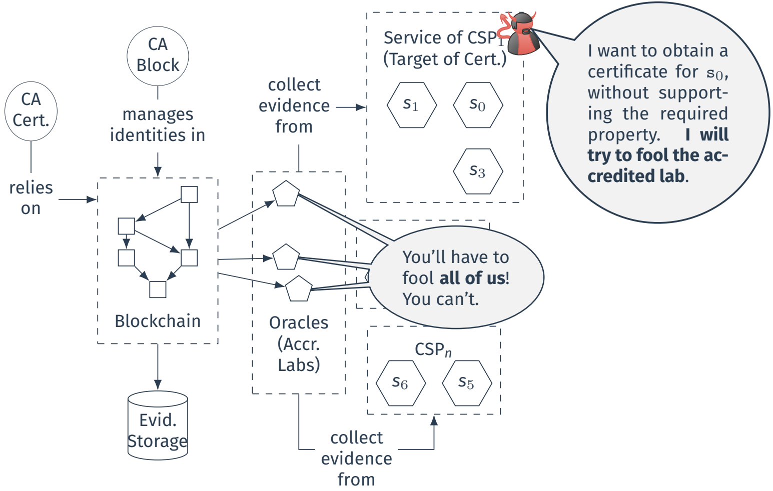


What Happens When Actors are Misbehaving: (1)



I want to obtain a certificate for s_0, without supporting the required property. **I will try to fool the accredited lab.**

What Happens When Actors are Misbehaving: (1)



CA Cert.

relies on

CA Block

manages identities in

Blockchain

Evid. Storage

collect evidence from

Oracles (Accr. Labs)

Service of CSP$_1$ (Target of Cert.)

s_1

s_0

s_3

CSP$_n$

s_6

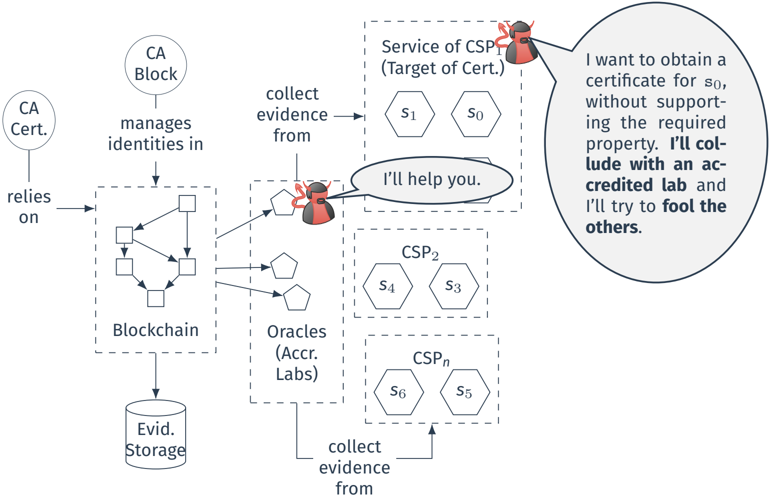
s_5

collect evidence from

I want to obtain a certificate for s_0, without supporting the required property. **I will try to fool the accredited lab.**

You'll have to fool **all of us**! You can't.

What Happens When Actors are Misbehaving: (2)



CA Cert.

relies on

CA Block

manages identities in

Blockchain

Evid. Storage

collect evidence from

Oracles (Accr. Labs)

Service of CSP$_1$ (Target of Cert.)

s_1

s_0

I'll help you.

CSP$_2$

s_4

s_3

CSP$_n$

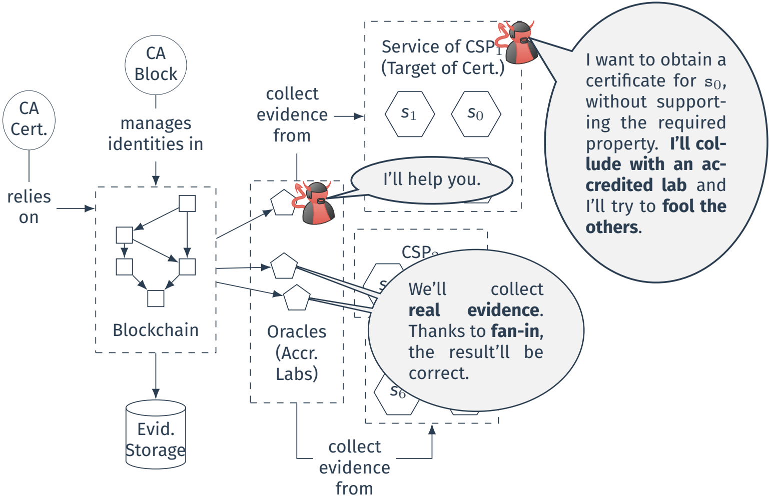
s_6

s_5

collect evidence from

I want to obtain a certificate for s_0, without supporting the required property. **I'll collude with an accredited lab** and I'll try to **fool the others**.

What Happens When Actors are Misbehaving: (2)



CA Cert.

relies on

CA Block

manages identities in

Blockchain

Evid. Storage

collect evidence from

Service of CSP$_1$ (Target of Cert.)

s_1

s_0

Oracles (Accr. Labs)

I'll help you.

CSP$_2$

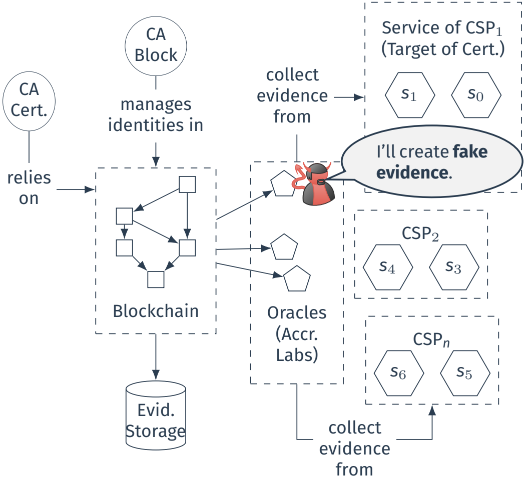
s_6

collect evidence from

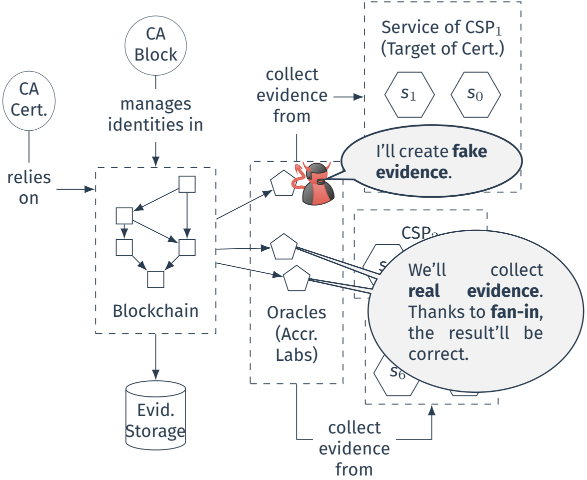
I want to obtain a certificate for s_0, without supporting the required property. **I'll collude with an accredited lab** and I'll try to **fool the others**.

We'll collect **real evidence**. Thanks to **fan-in,** the result'll be correct.

What Happens When Actors are Misbehaving: (3)



What Happens When Actors are Misbehaving: (3)



Smart Contracts

Name	Depl. Step	Usage Steps	Description
`CertificationModel`	Step (1)	Steps (1)–(3)	Certify a property on a target
`CertificationModelExecution`	Step (1)	Steps (1)–(3)	Execute a `CertificationModel`
`Certificate`	Step (3)	Step (3)	Final certification process artifact

Core contracts

Name	Depl. Step	Usage Steps	Description

`VRFv2SubscriptionManager,`
`VRFv2Consumer`
	Step (0)	Step (1)	Generate verifiable random numbers

`Probes`	Step (0)	Step (2)	Expose probes as functions then sent to oracles for execution
`Coordinator`	Step (0)	Steps (1), (2)	Define the *policy* for probes execution and retrieve their result

Supporting contracts

Gas Consumption (1)

Step	Gas used	Fee	
		ETH	€
Step (0): Bootstrap	8,932,049	0.41	1,288.920
Step (1): Preparation	5,136,015	0.235	741.141
Step (2): Evidence Collection	4,076,328	0.187	588.225
Step (3): Evaluation and Award	537,041	0.025	77.497
Total	18,681,433	0.857	2,695.783

- Fee $=$ *gas used* $\times$ *cost of a unit of gas*
- Cost of a unit of gas: ETH 45.85×10^{-9}
- ETH 1 $=$ €3,147.28 (as of March 2, 2024)
- *Sepolia* as blockchain testing network
- Probes implemented as HTTP calls

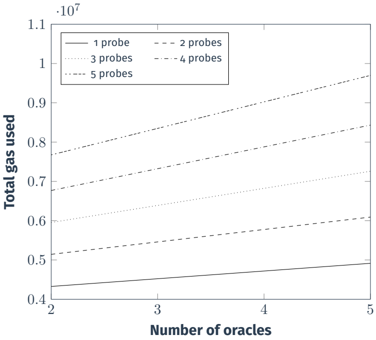
Gas Consumption (2)

Gas consumption varying the number of

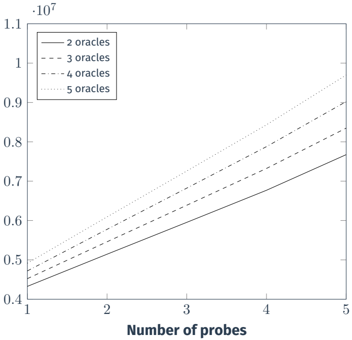
- probes in $\{1, ..., 5\}$
- oracles in $\{2, ..., 5\}$

Gas Consumption (2)

Gas consumption varying the number of probes and oracles



Varying the number of oracles



Varying the number of probes

$\Longrightarrow$ linear increase of gas consumption

Conclusions

Blockchain-based certification scheme and process

- relaxes old-fashioned assumptions
- complete visibility and traceability of certification artifacts

Future work

- improve oracle selection
  - stronger policies
  - reward–punishment