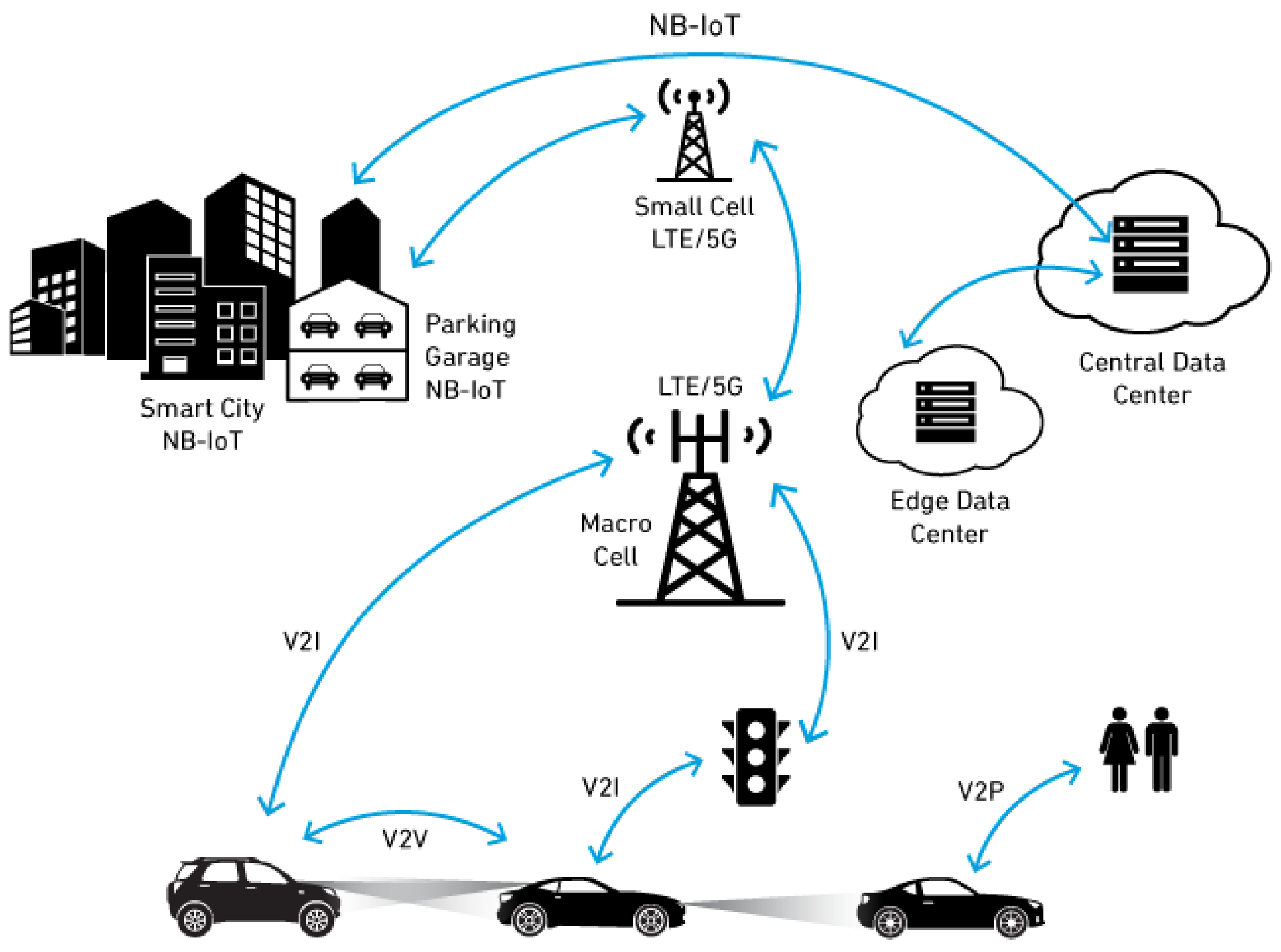
Scalable and Provably Secure Self-Revocation Protocols for V2X

Gianluca Scopelliti[1][2], Christoph Baumann[1], Fritz Alder[2], Eddy Truyen[2], Jan Tobias Mühlberg[2]

[1]Ericsson Security Research, Sweden, [2]KU Leuven, Belgium

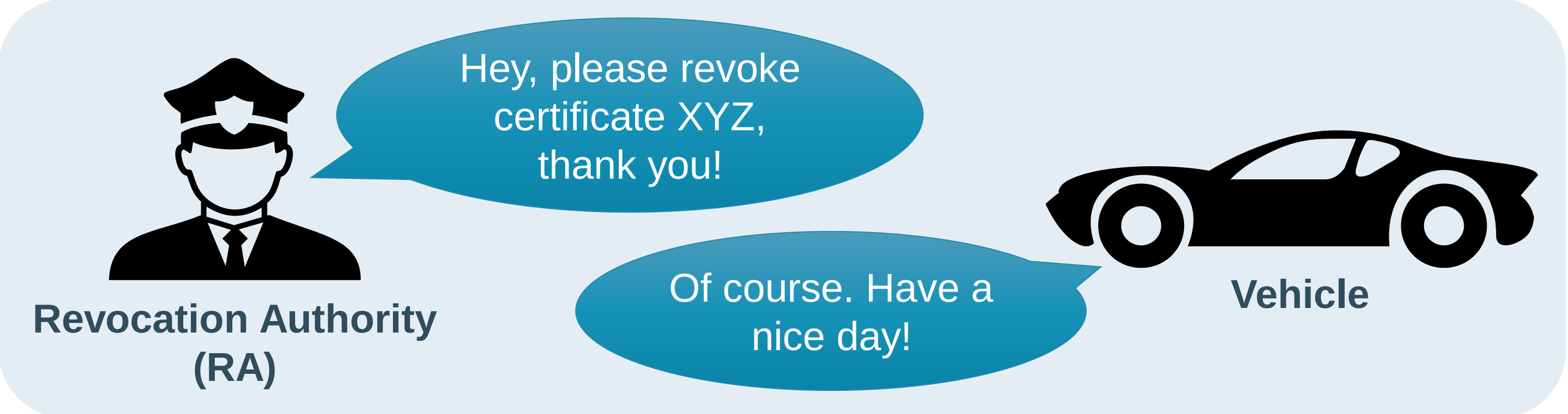
✉ gianluca.scopelliti@ericsson.com

V2X: Vehicle-to-Everything



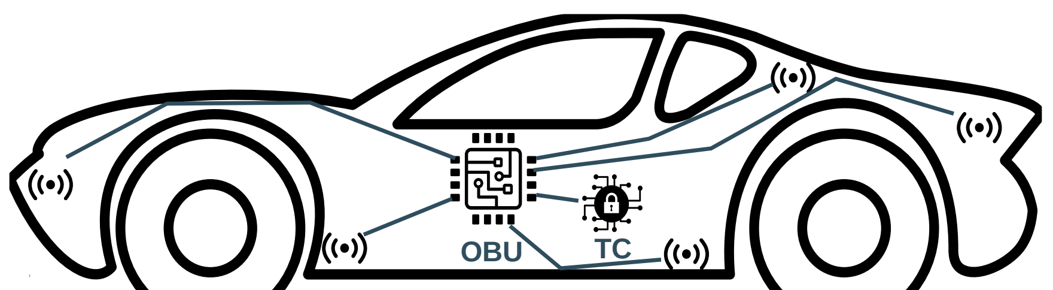
[1]

Self-Revocation of V2X credentials


Hey, please revoke certificate XYZ, thank you!
Of course. Have a nice day!
Revocation Authority (RA)
Vehicle

OBU: On-Board Unit

- Central processing
- Networking: V2V, V2I, V2P
- Can be **compromised**



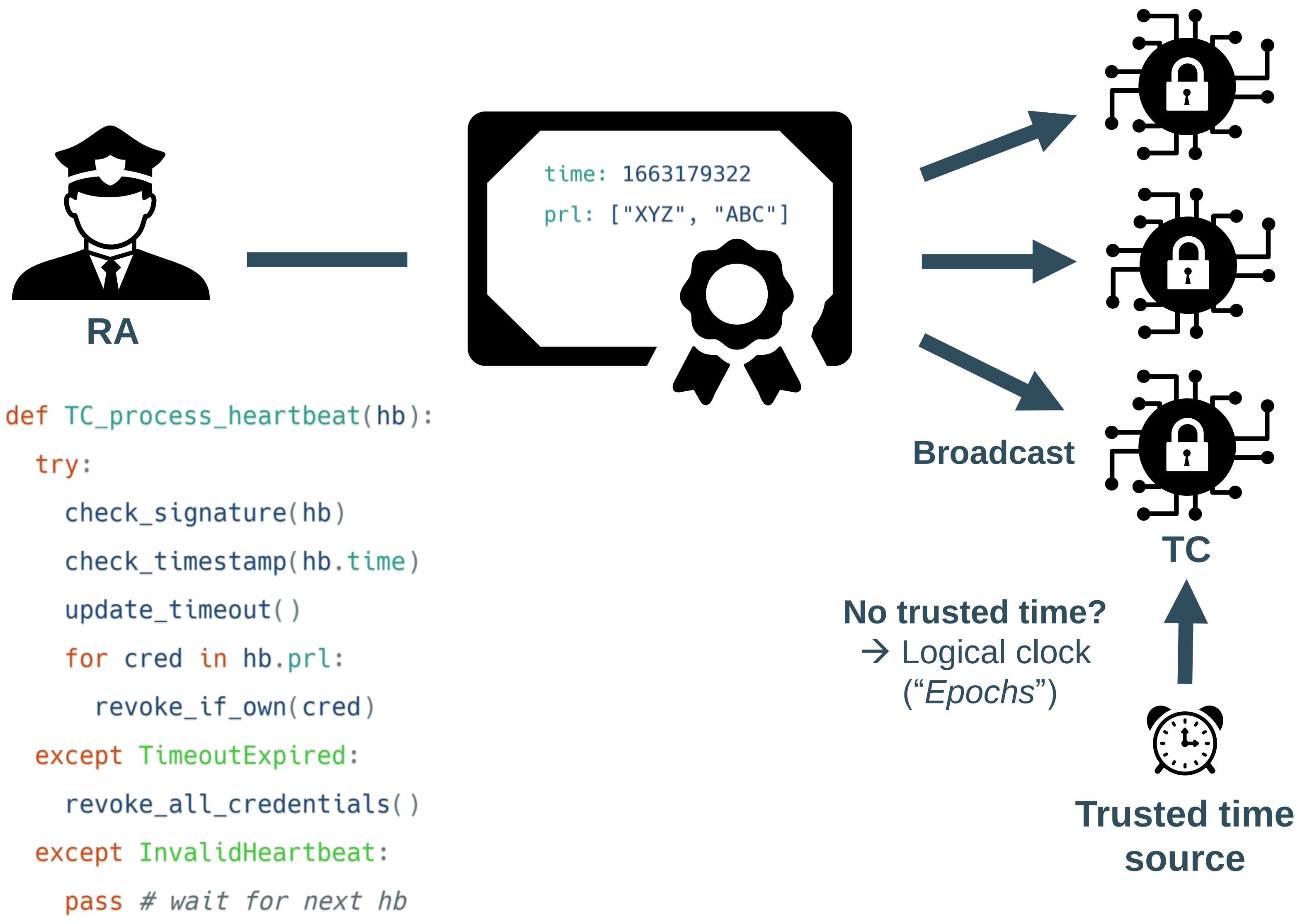
TC: Trusted Component

- Remote attestation
- Credential management

Examples of TCs: intel SGX, arm TRUSTZONE, TPM 2.0

[2,3]

Revocation message: Heartbeat

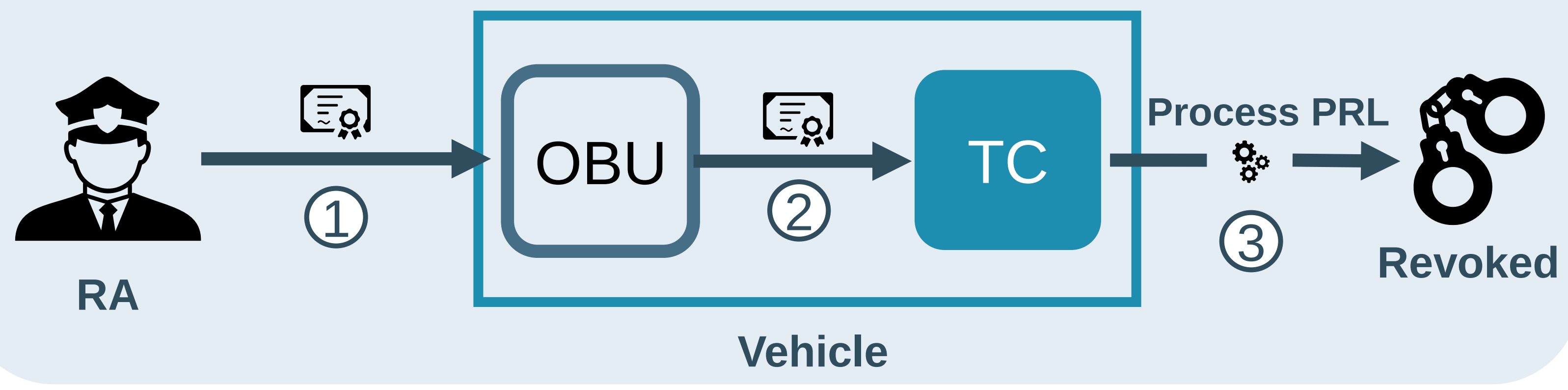


```
time: 1663179322
prl: ["XYZ", "ABC"]
```

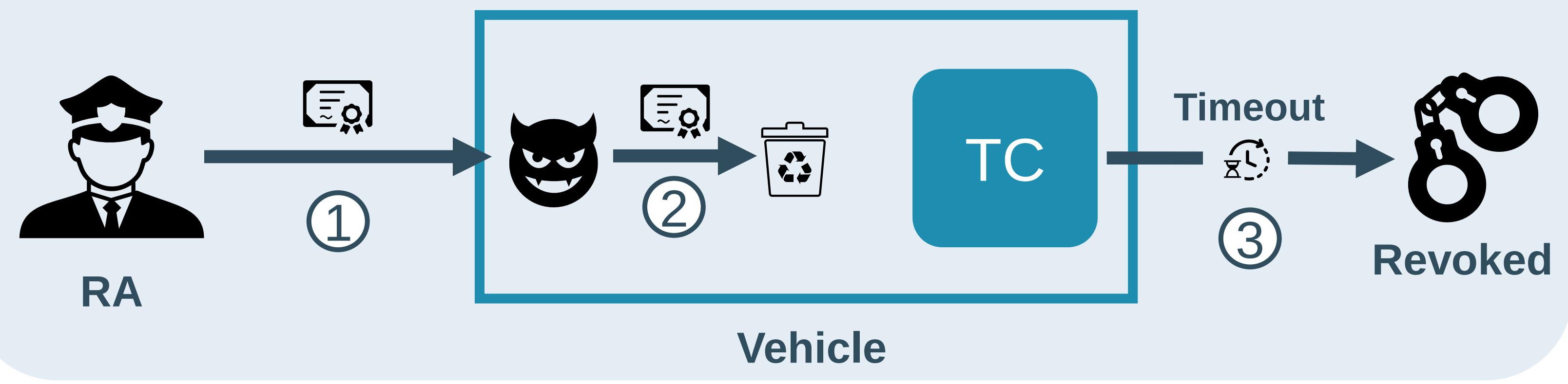
```
def TC_process_heartbeat(hb):
  try:
    check_signature(hb)
    check_timestamp(hb.time)
    update_timeout()
    for cred in hb.prl:
      revoke_if_own(cred)
  except TimeoutExpired:
    revoke_all_credentials()
  except InvalidHeartbeat:
    pass # wait for next hb
```

Revocation in practice

Scenario 1: Honest vehicle

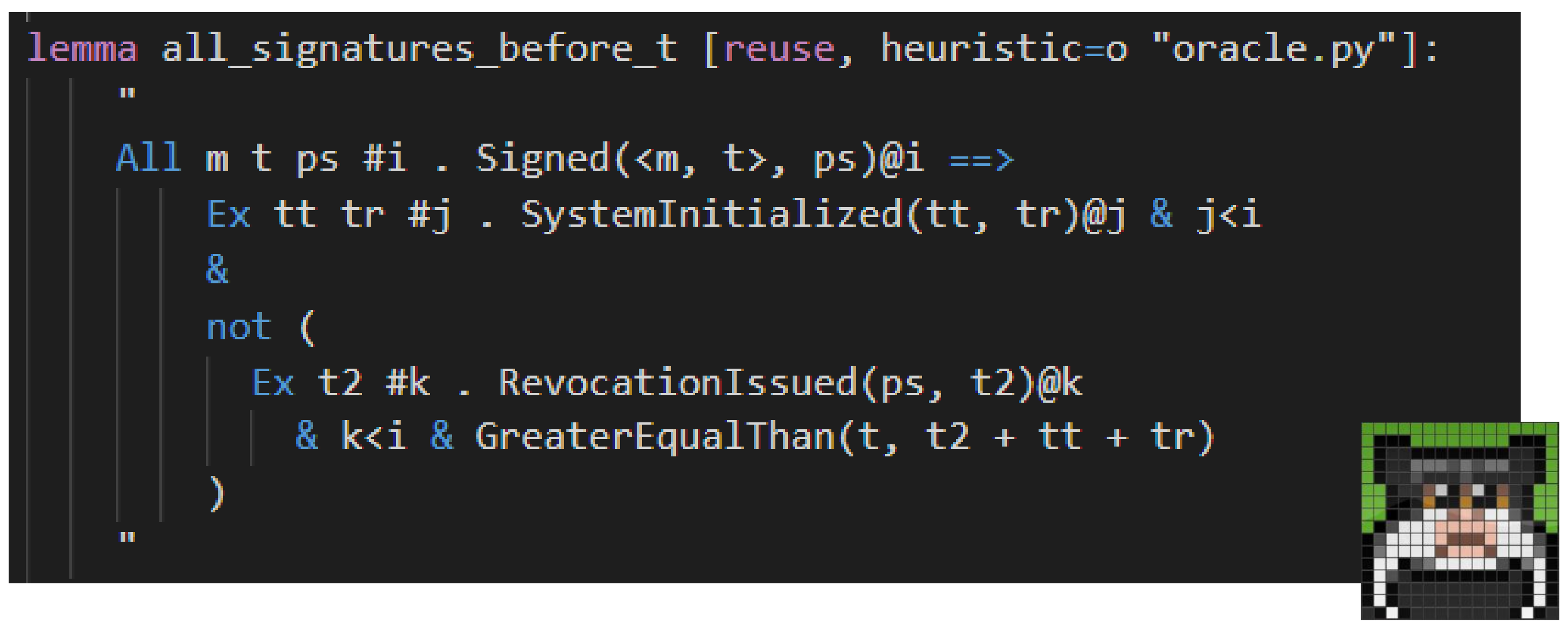


Scenario 2: Malicious vehicle



Formal verification: Tamarin prover

Property	Description
A	*Revocation is deterministic and completes within a fixed time*
B	*The revoked credential can be removed from the heartbeat after a fixed time*
C	*After a fixed time, other vehicles discard any message signed with the revoked credential*

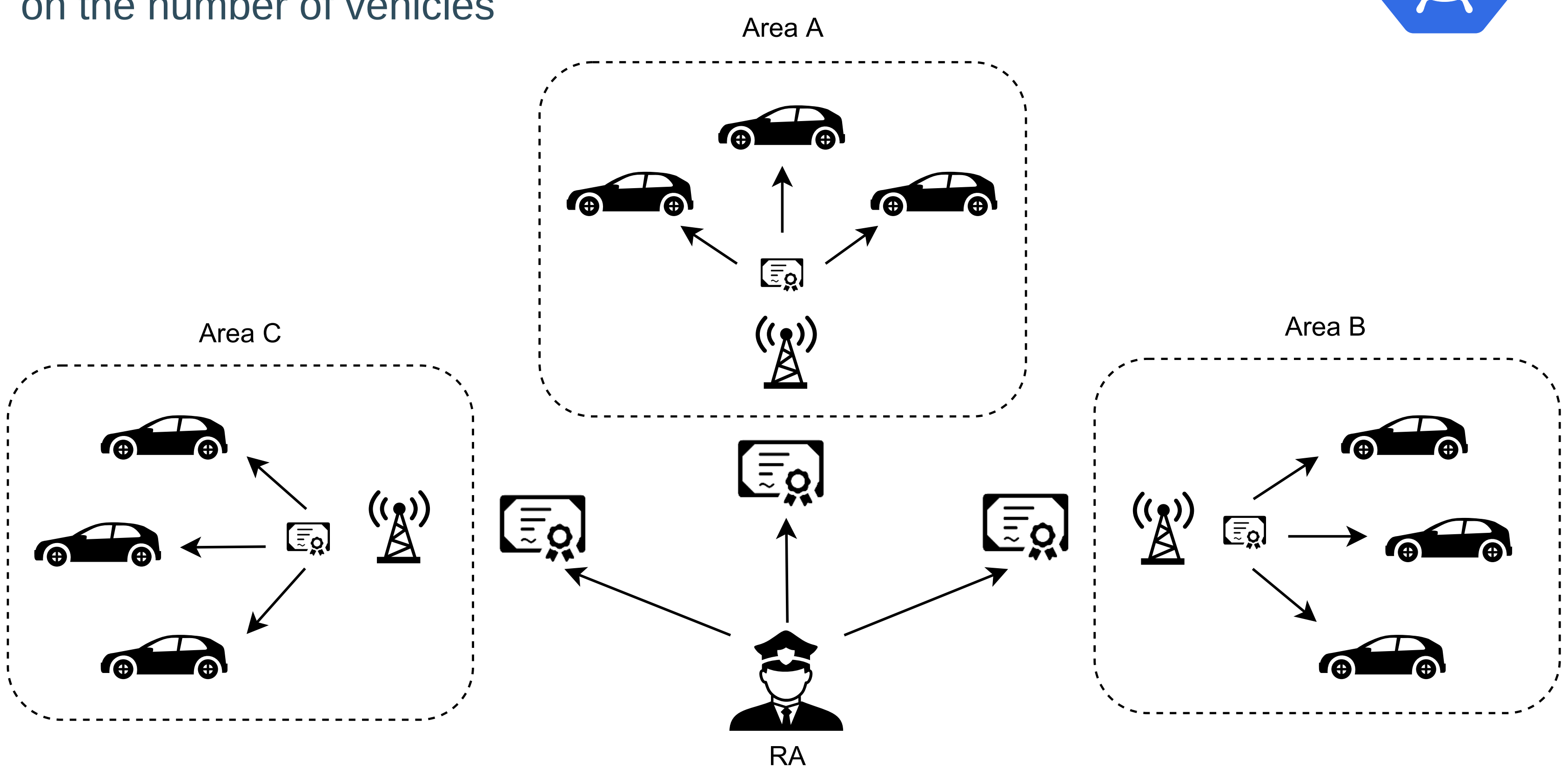


```
lemma all_signatures_before_t [reuse, heuristic=o "oracle.py"]:
    "
    All m t ps #i . Signed(<m, t>, ps)@i ==>
        Ex tt tr #j . SystemInitialized(tt, tr)@j & j<i
        &
        not (
          Ex t2 #k . RevocationIssued(ps, t2)@k
            & k<i & GreaterEqualThan(t, t2 + tt + tr)
        )
    "
```

Example: Property A with trusted time in TC

End-to-End Evaluation

Scalable: the number of heartbeats does not depend on the number of vehicles



References

[1] https://www.qorvo.com/design-hub/blog/v2x-in-the-connected-car-of-the-future

[2] Förster, D., Löhr, H., Zibuschka, J., & Kargl, F. (2015). REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks. In M. Conti, M. Schunter, & I. Askoxylakis (Eds.), Trust and Trustworthy Computing (pp. 193–208). Springer International Publishing.

[3] Whitefield, J., Chen, L., Giannetsos, T., Schneider, S., & Treharne, H. (2017). Privacy-enhanced capabilities for VANETs using direct anonymous attestation. 2017 IEEE Vehicular Networking Conference (VNC), 123–130.

5G HOSTS   DistriNet   fwo   ERICSSON