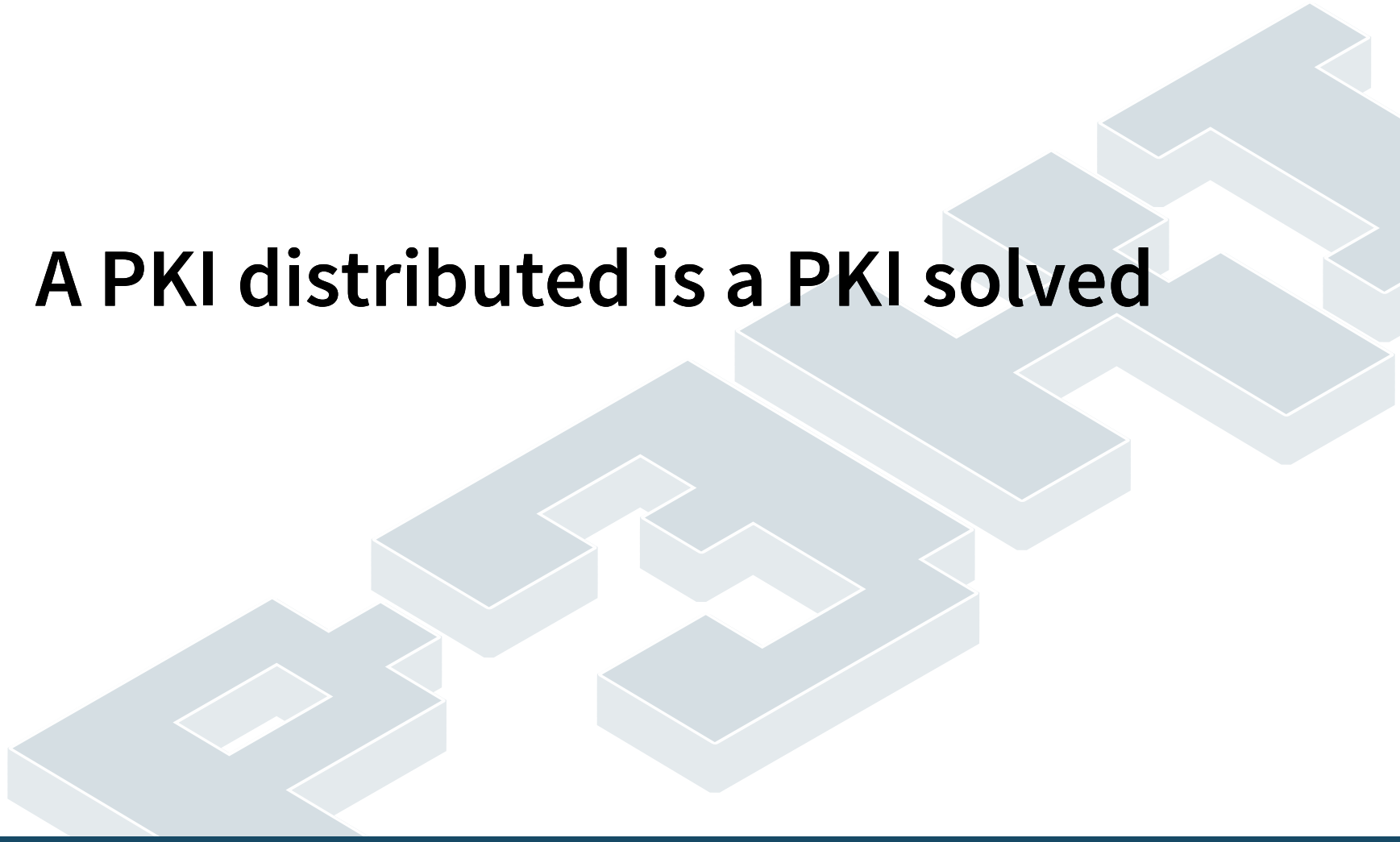
A PKI distributed is a PKI solved



A PKI decentralized is a PKI solved

Who we are

- Felix 'FX' Lindner
  Founder of P3KI & Recurity Labs
- Gregor 'hadez' Jehle
  Chief Everything Officer at P3KI

Ein Schwank aus der Geschichte

- FX@TollCollect.de
- ISO 20828 appears
- Years of research happen
- You receive: a new PKI!

The ISO 20828 Challenge: Independence from central CAs and connectivity

Size does matter

- Road networks are monsters
  DE: 13K+645K km, CN: 143K+6M km
- Needs to cover the whole country
- Distributed system of road-side infrastructure

Non-trivial number of moving targets

- The number of registered vehicles is staggering
  DE: 50M, USA:270M
- Efficient verification in maintenance scenarios
- Certificate management for V2x / C2x Communication

Mostly everything is federated

- Multi-layer hierarchy
  Germany: EU, federal, state, district, municipal
- Strategy: middle to high tiers
- Tactical: local

No infrastructure, no life

- Resiliency
- Resiliency
- Resiliency
- Resiliency

Why then have single points of failure?

- OCSP & CRL
- Central by design
- Can only be checked when online
- **ISO 20828 wanted to fix that!**

How they apply to other industries

Every non-trivial PKI faces the same challenges

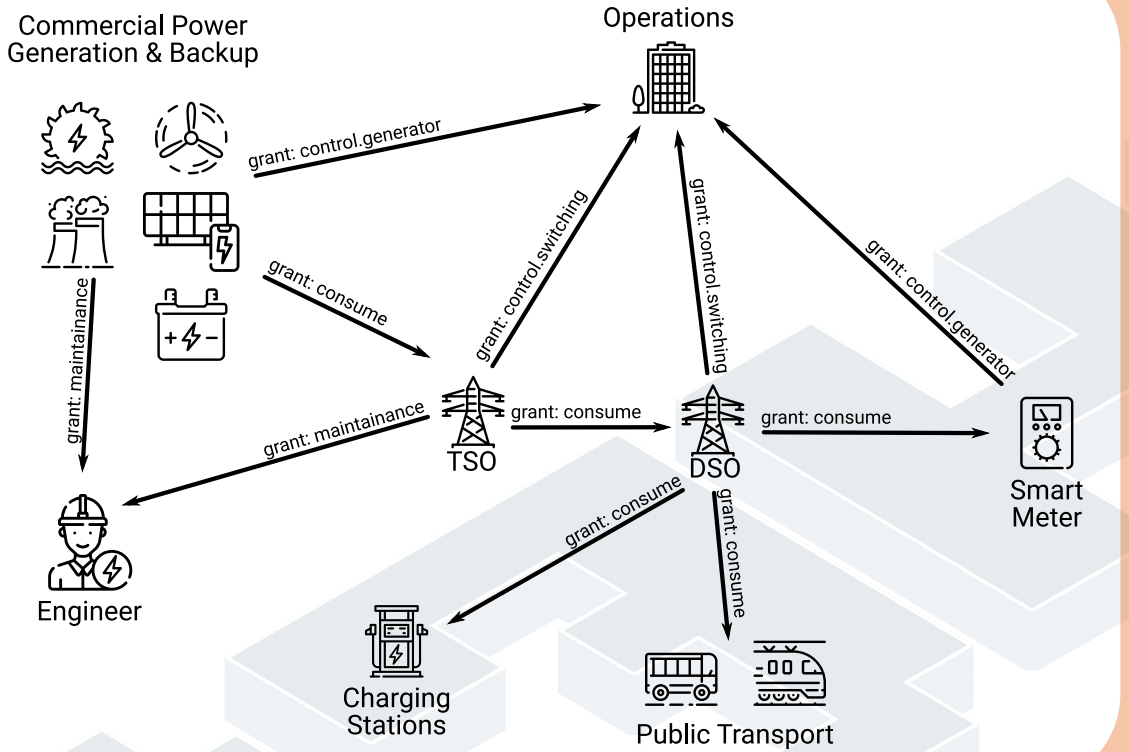
- Push towards decentralization
- Exponential growth in permission levels, roles, capabilities
- Need for resiliency
- We want better failure modes!

Cross-industry applications

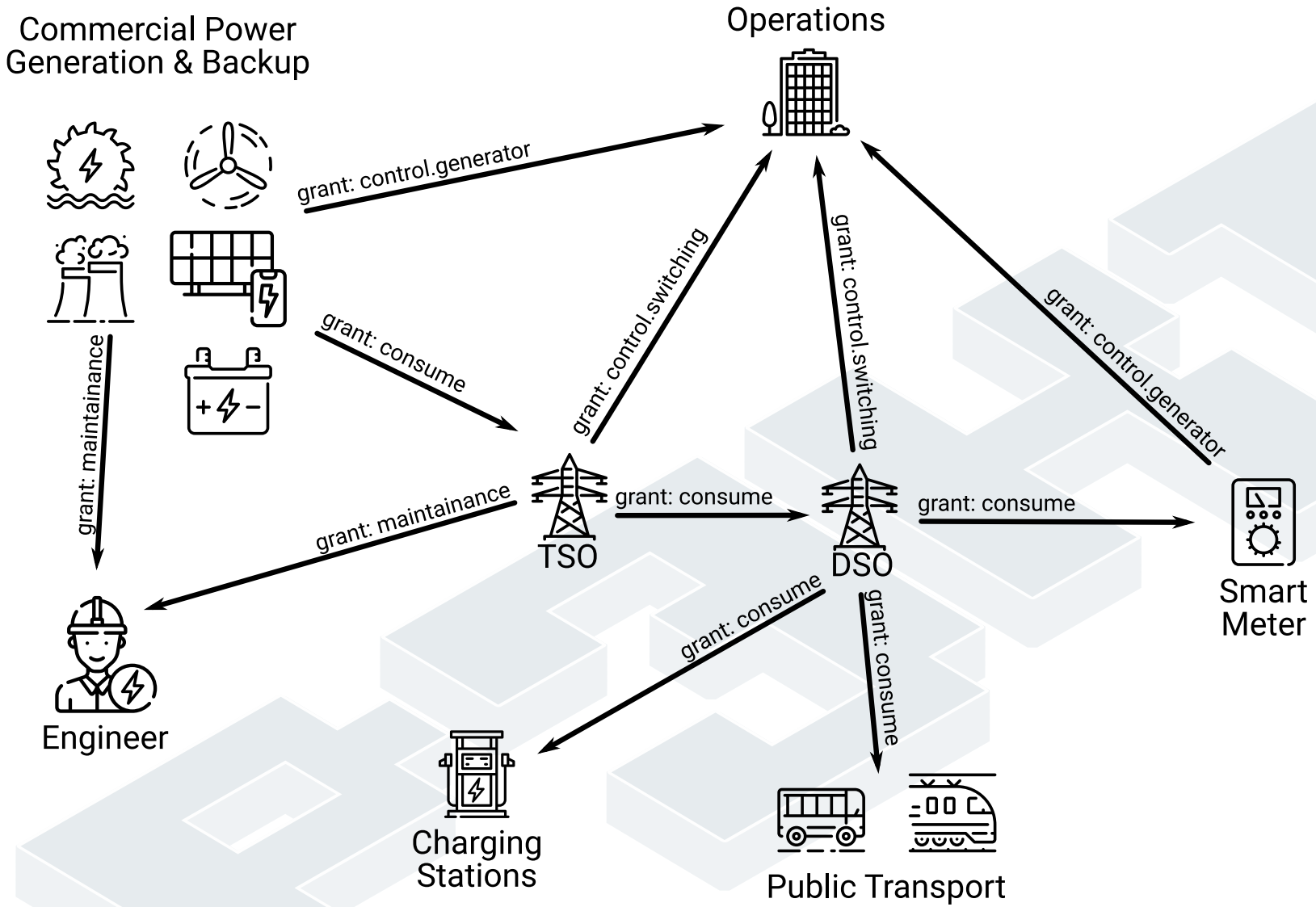
SCADA / ICS / IIoT

- Similar challenges to automotive sector regarding size
- Arguably more critical and dependent on resilience
- Replacements, provisioning & maintenance in the field
- More often than not: Resilient or boom scenario

SMART GRID

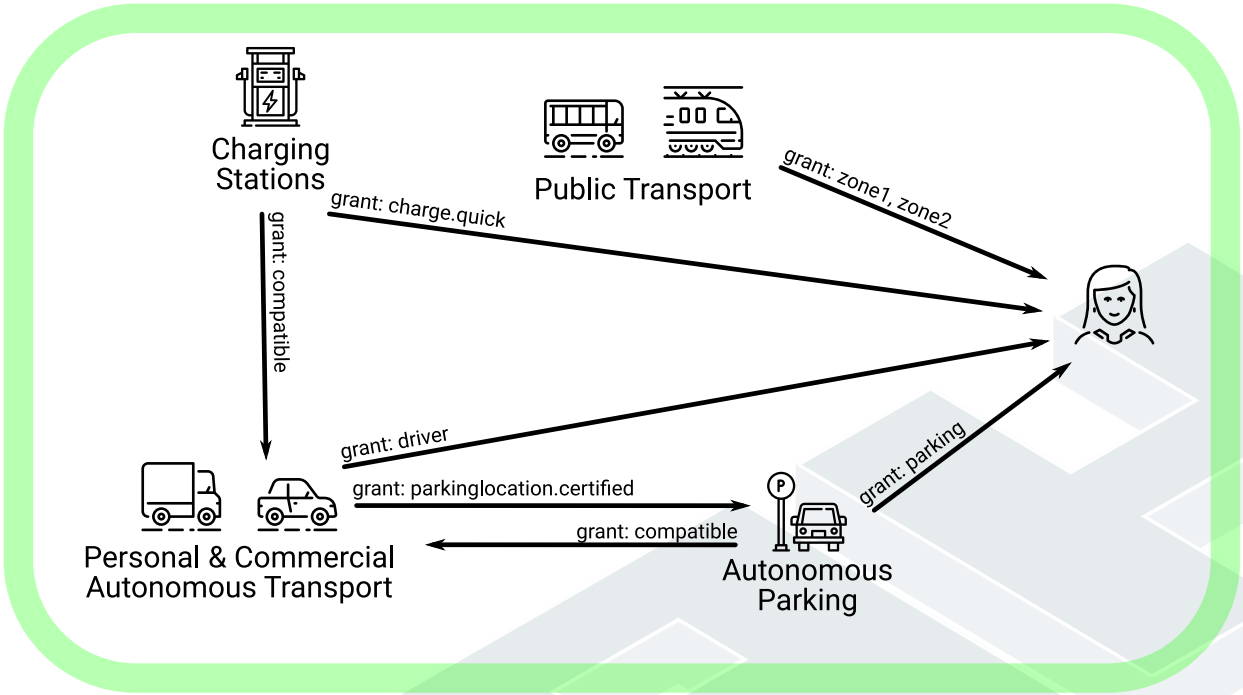

Commercial Power
Generation & Backup
Operations
grant: control.generator
grant: consume
grant: control.switching
grant: control.switching
grant: control.generator
grant: maintainance
grant: maintainance
TSO
grant: consume
DSO
grant: consume
Smart
Meter
Engineer
grant: consume
grant: consume
Charging
Stations
Public Transport

SMART GRID

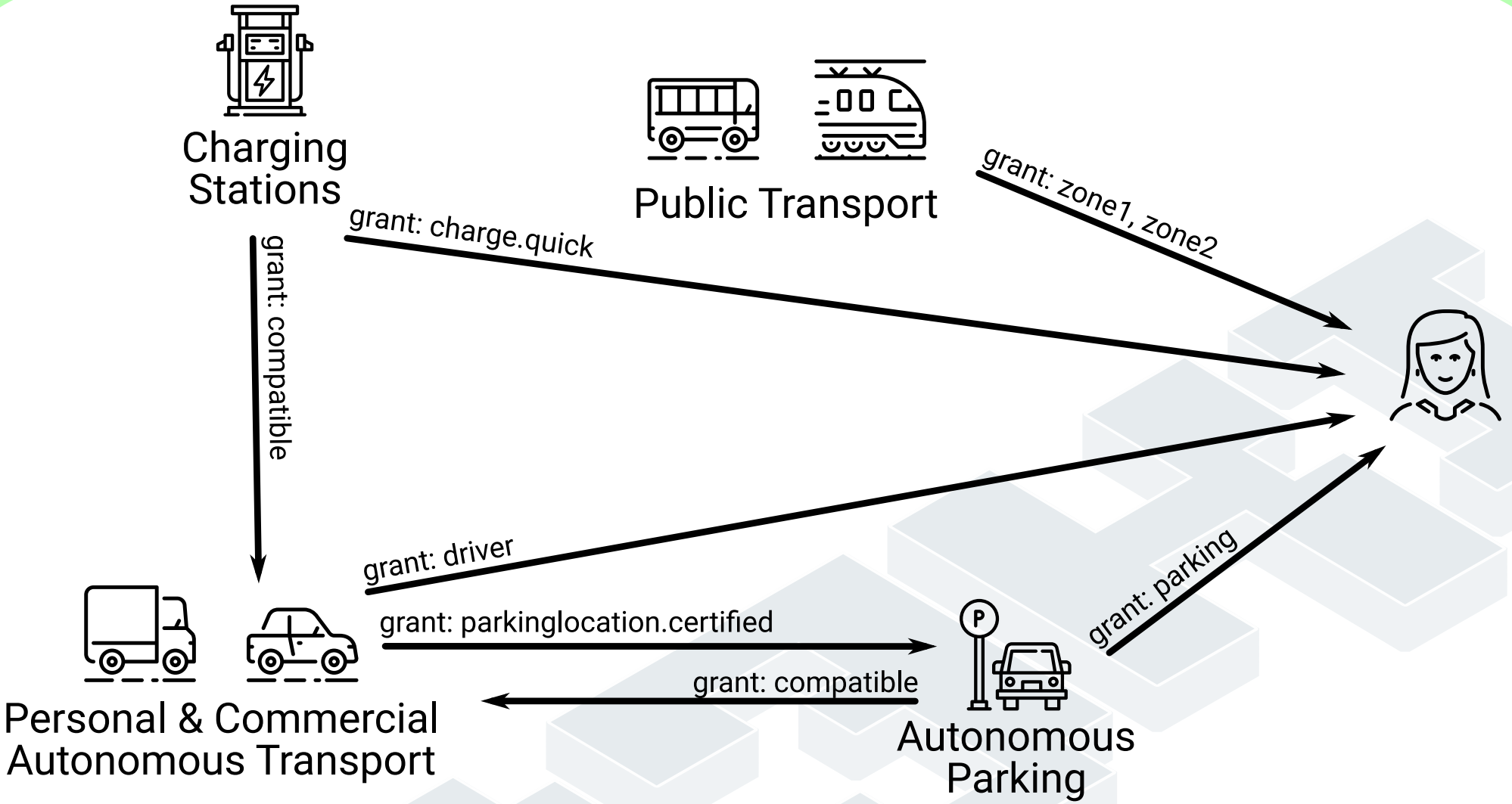

Commercial Power
Generation & Backup
Operations
grant: control.generator
grant: consume
grant: maintainance
grant: control.switching
grant: control.switching
grant: control.generator
grant: maintainance
grant: consume
grant: consume
TSO
DSO
Smart
Meter
Engineer
grant: consume
grant: consume
Charging
Stations
Public Transport

Automotive & Smart City

- V2x communication
- Autonomous driving and parking
- Car-sharing scenarios


Charging Stations
Public Transport
grant: charge.quick
grant: zone1, zone2
grant: compatible
grant: driver
grant: parkinglocation.certified
grant: compatible
grant: parking
Personal & Commercial Autonomous Transport
Autonomous Parking

SMART CITY

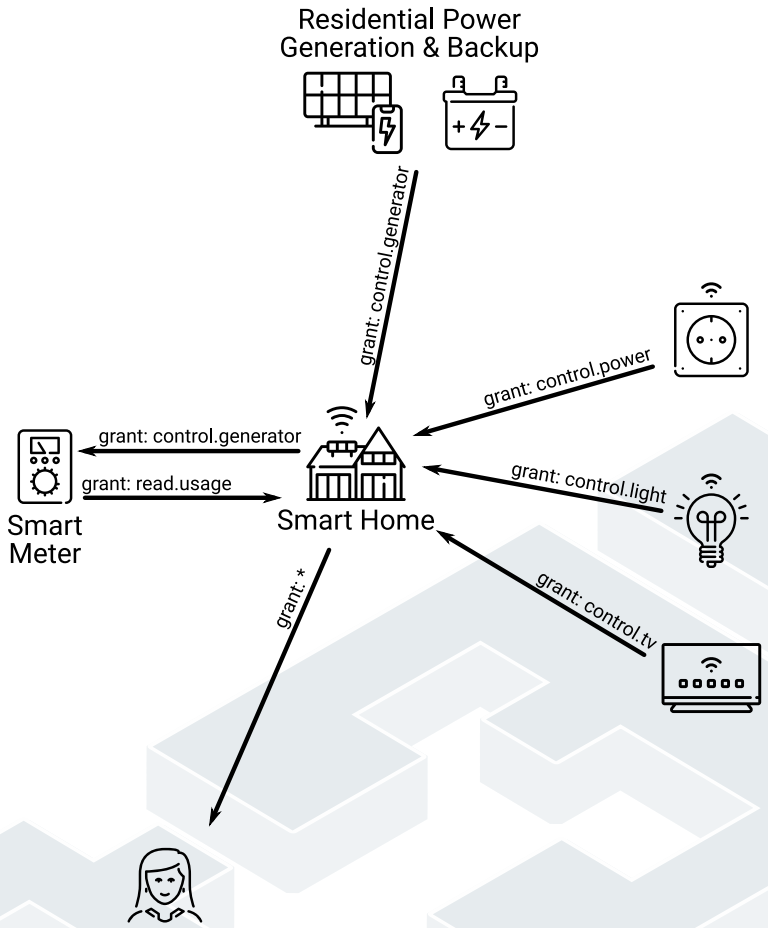

Charging Stations
Public Transport
grant: charge.quick
grant: zone1, zone2
grant: compatible
grant: driver
grant: parkinglocation.certified
grant: compatible
grant: parking
Personal & Commercial Autonomous Transport
Autonomous Parking

SMART CITY

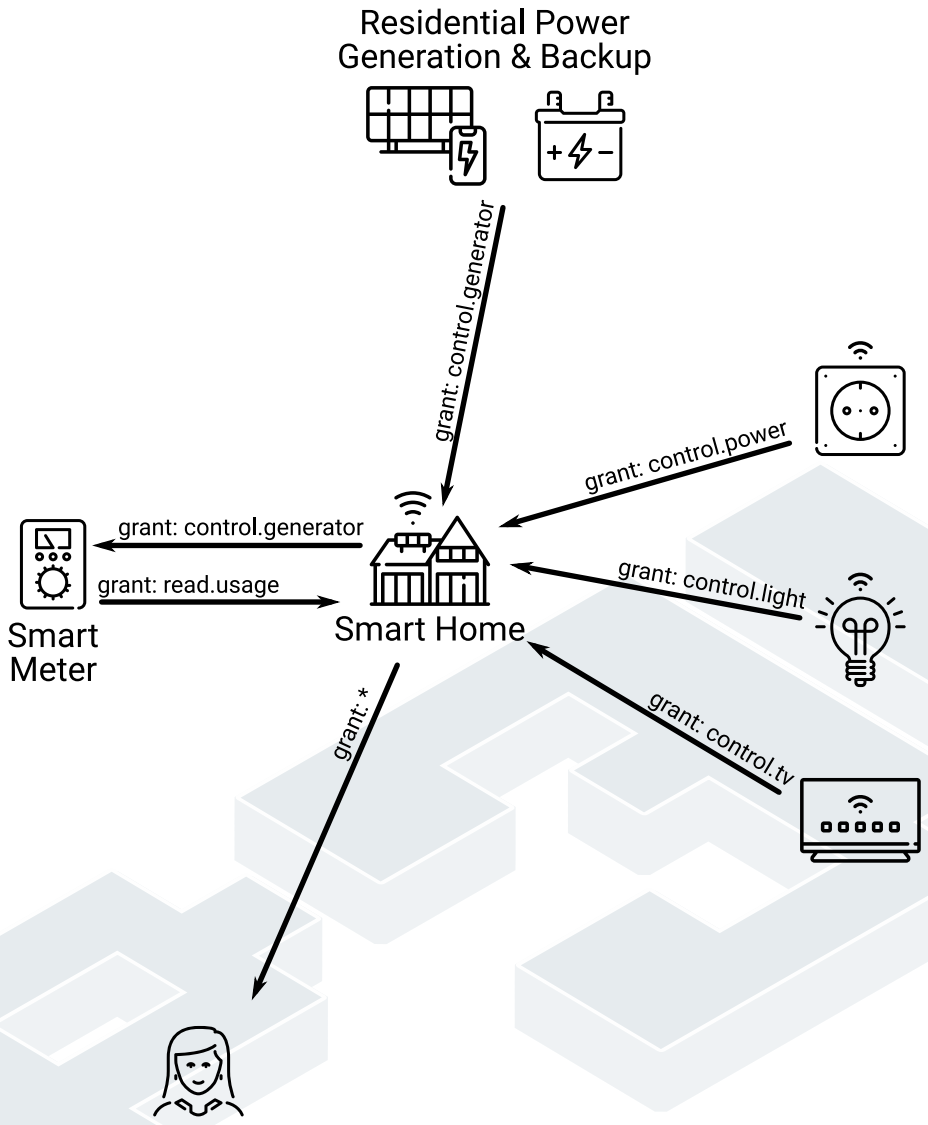
Internet of S...tuff

- IoT
  - Ridiculous device numbers
  - Arbitrarily complex networking
  - High price-pressure --> low performance platforms
- Smart Home & Building
  - Federated access control
  - Network on card applications
  - Must be resilient to outages

SMART HOME

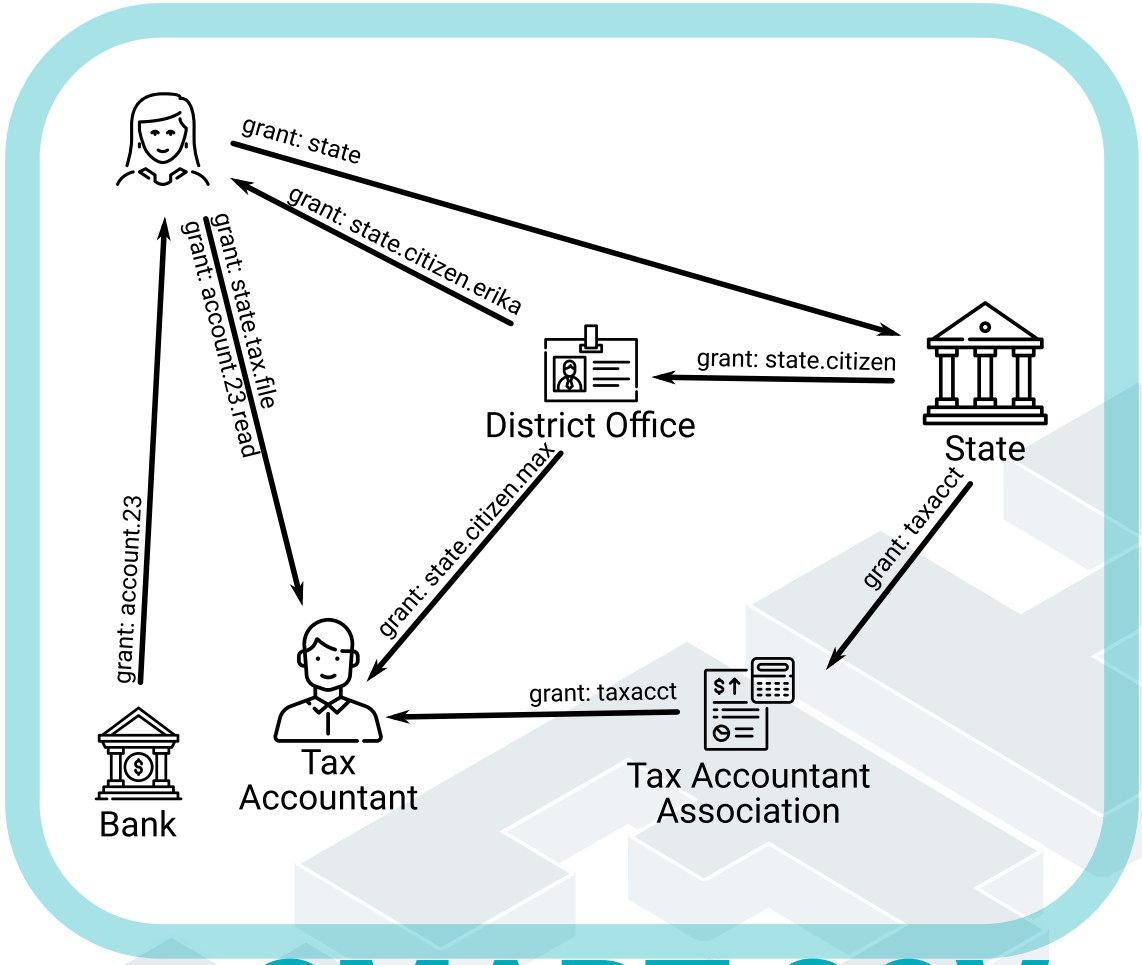

Residential Power
Generation & Backup
grant: control.generator
grant: control.power
grant: control.generator
grant: read.usage
Smart
Meter
Smart Home
grant: control.light
grant: *
grant: control.tv

SMART HOME

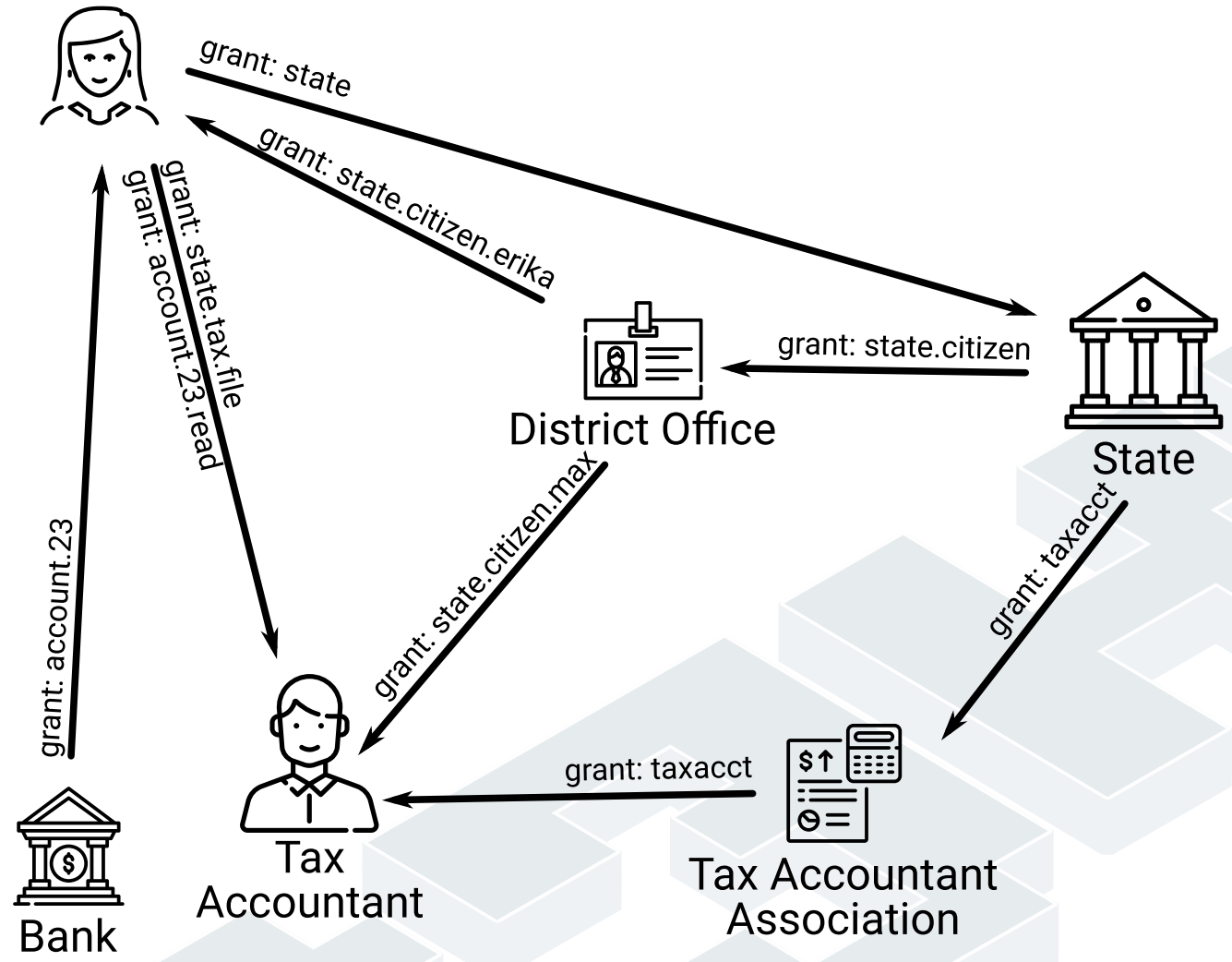

Residential Power
Generation & Backup
grant: control.generator
grant: control.power
grant: control.generator
grant: read.usage
Smart
Meter
Smart Home
grant: control.light
grant: *
grant: control.tv

eGOV: eIDAS / nPA / EU Citizen Card

- Common identity platform
- Based on FIDO
- Per-service sub-identities


grant: state
grant: state.citizen.erika
grant: state.tax.file
grant: account.23.read
grant: account.23
grant: state.citizen
District Office
State
grant: state.citizen.max
grant: taxacct
grant: taxacct
Bank
Tax
Accountant
Tax Accountant
Association

SMART GOV

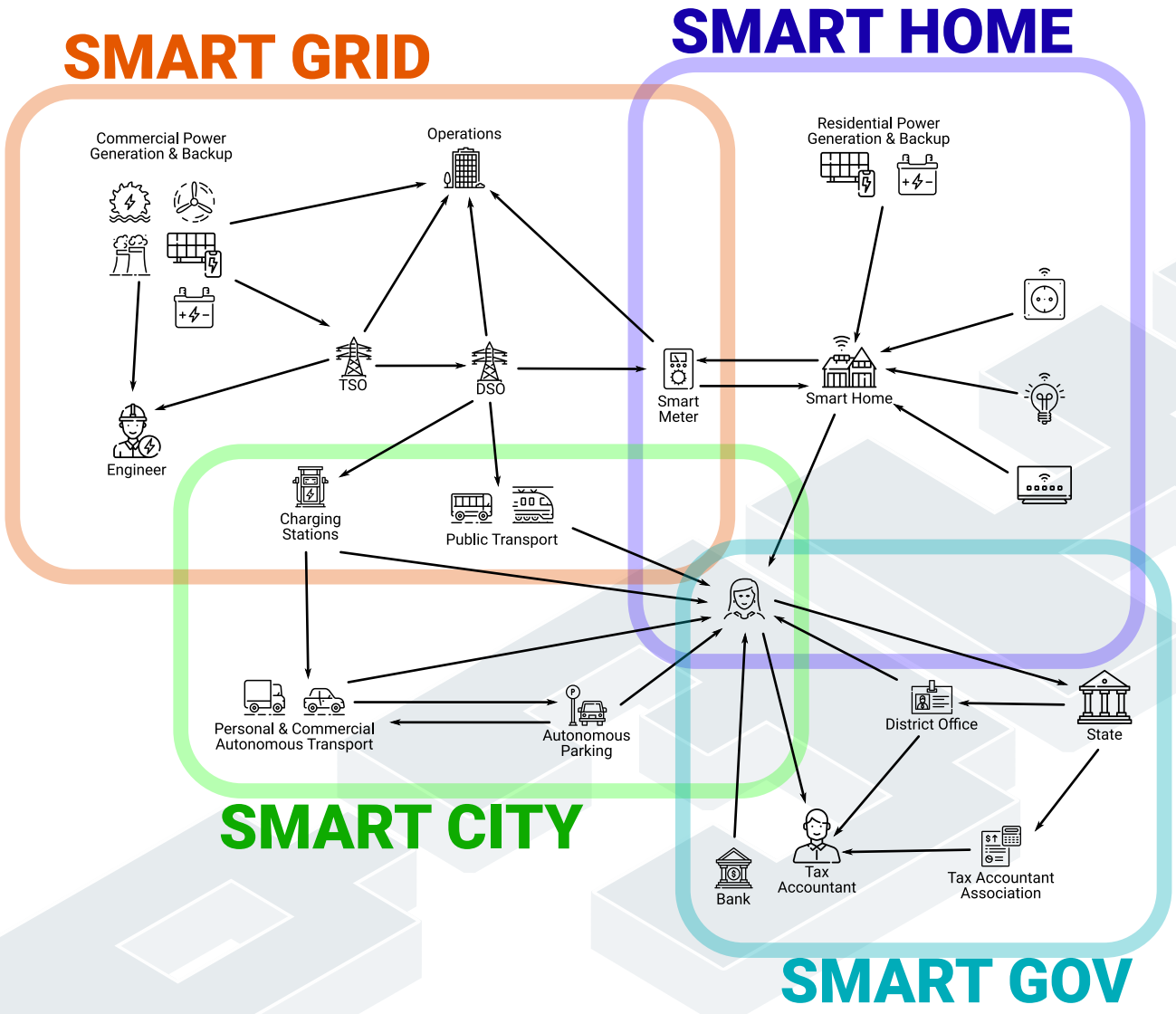

grant: state
grant: state.citizen.erika
grant: state.tax.file
grant: account.23.read
grant: account.23
grant: state.citizen
District Office
State
grant: state.citizen.max
grant: taxacct
grant: taxacct
Bank
Tax
Accountant
Tax Accountant
Association

SMART GOV

Tying it all together

- Common system to handle identity and delegation
- Scenarios defined by Trust Policy Language
- Interoperability without compromising privacy

Cross-domain access control & delegation



X.509 outage scenarios


September 3, 2011
It Was A Saturday Morning...
Revocation day

What no one wants to talk about

- Revoking intermediates requires central nodes (OCSP, CRL)
- Revocation prunes whole sub-trees

Ask yourself

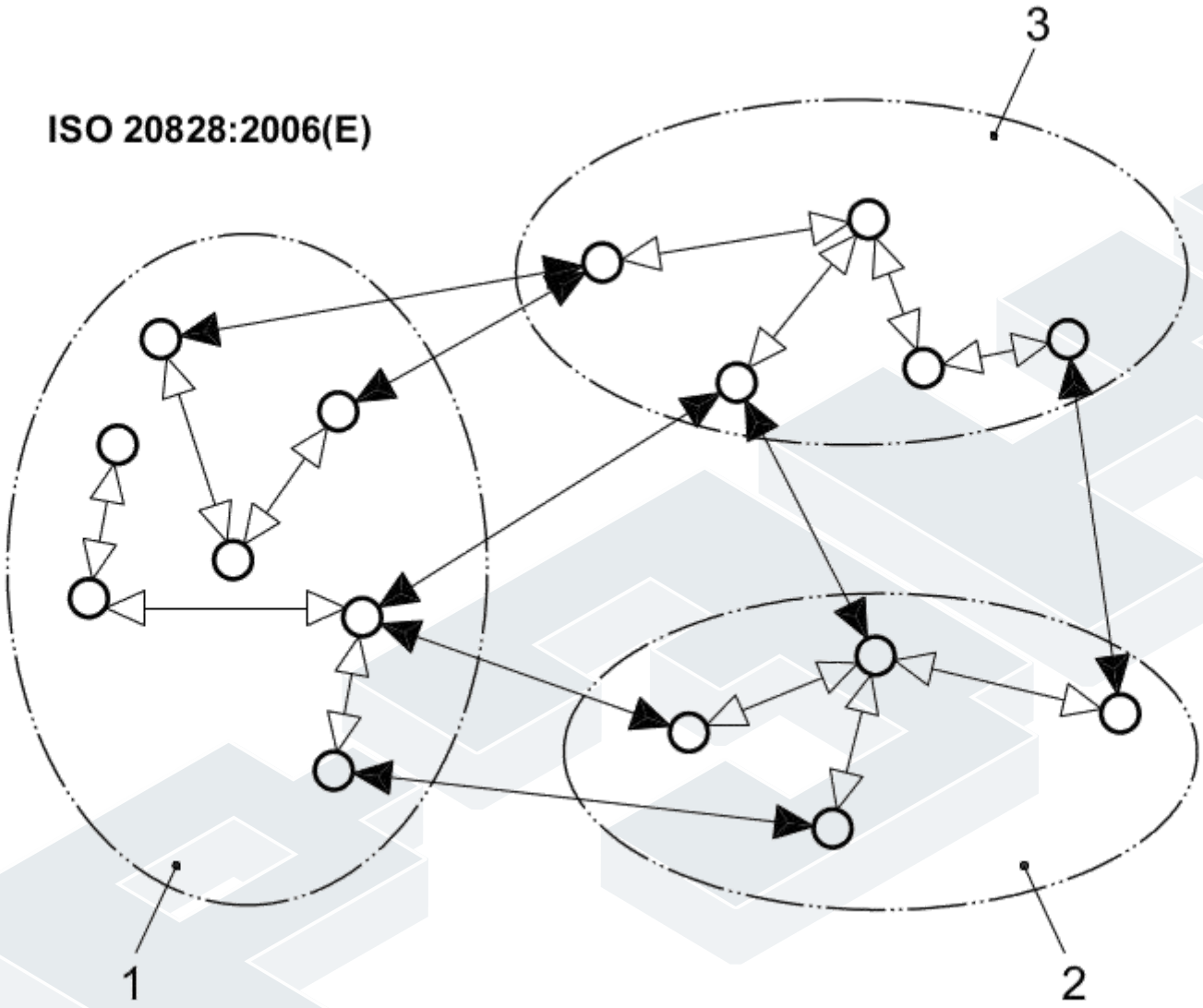
Did any of the companies responsible for large CA fuckups manage to retain their customers?

How ISO 20828 proposes to safe us all

ISO 20828
Requirements

- No shared overall infrastructure — Easily integrate into existing security systems with minimal impact
- Breaking a part does not break the whole
- Support low-resource devices
- Allow for mobile devices and sporadic communication

ISO 20828
Security Domains



P2P approach

- Nodes communicate with other nodes
- Able to proof to each other whether this is okay

Fine granular trust

- Permissions can be arbitrarily precise
- Delegate all or some of them

Federation

- Different permission levels based on hierarchy and device type
- Backup trust paths outside strict hierarchies
- Enable participants to make local decisions!

Trinity: A Generalization of 20828

Transport agnostic communication

The way you get the news does not matter. Pick the best one available at the time!

Trust Policy Languages

- Express permissions, roles, capabilities
- Arbitrary precision and sub-dividable expressions
- Extensible in the field
- Mathematically proven

Offline capabilities

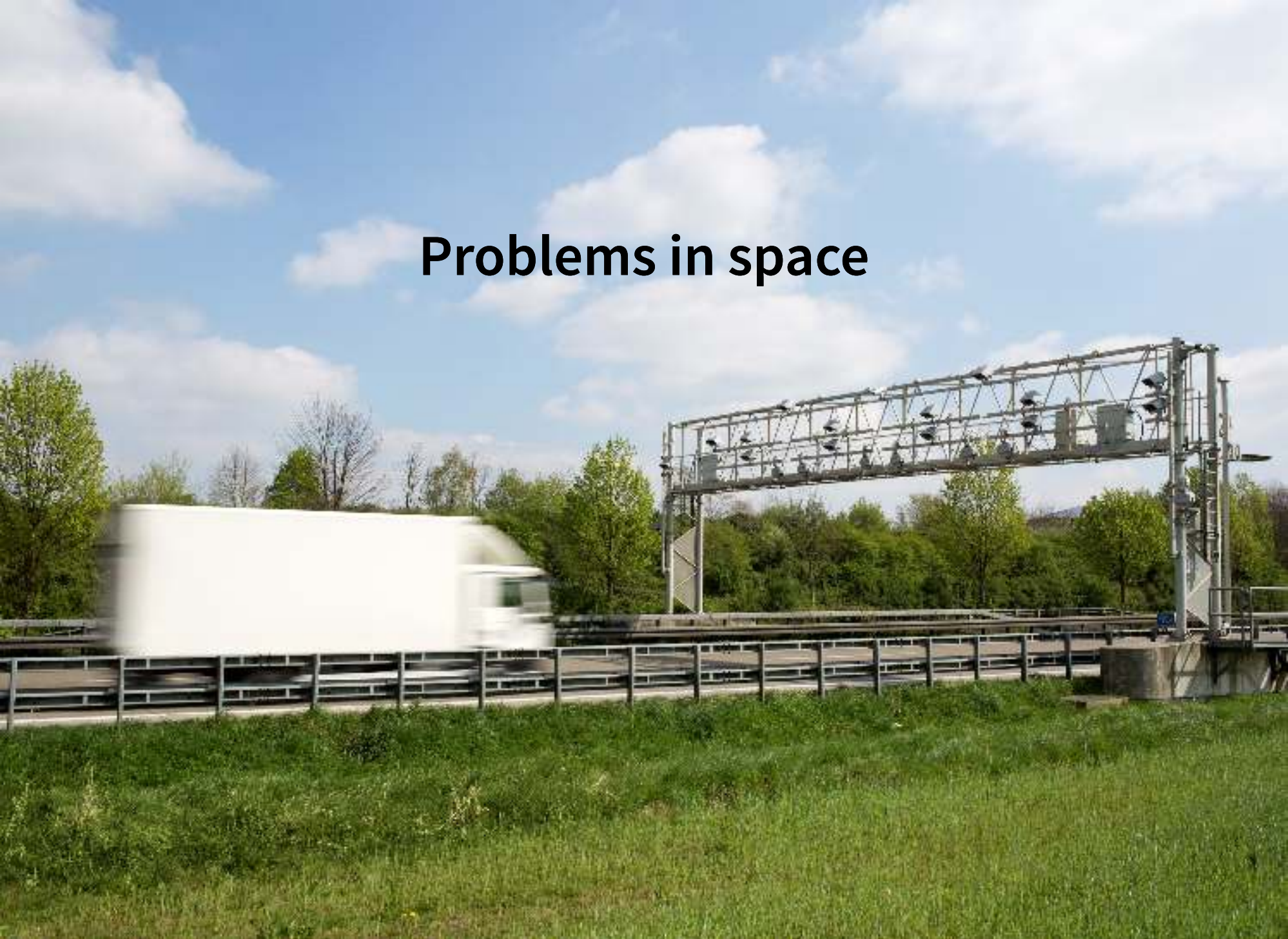
- Everything is offline verifiable
- Designed with store & forward networking in mind

How Toll Collect would work with Trinity

The problem space

Toll Collect is a tremendously complex distributed system

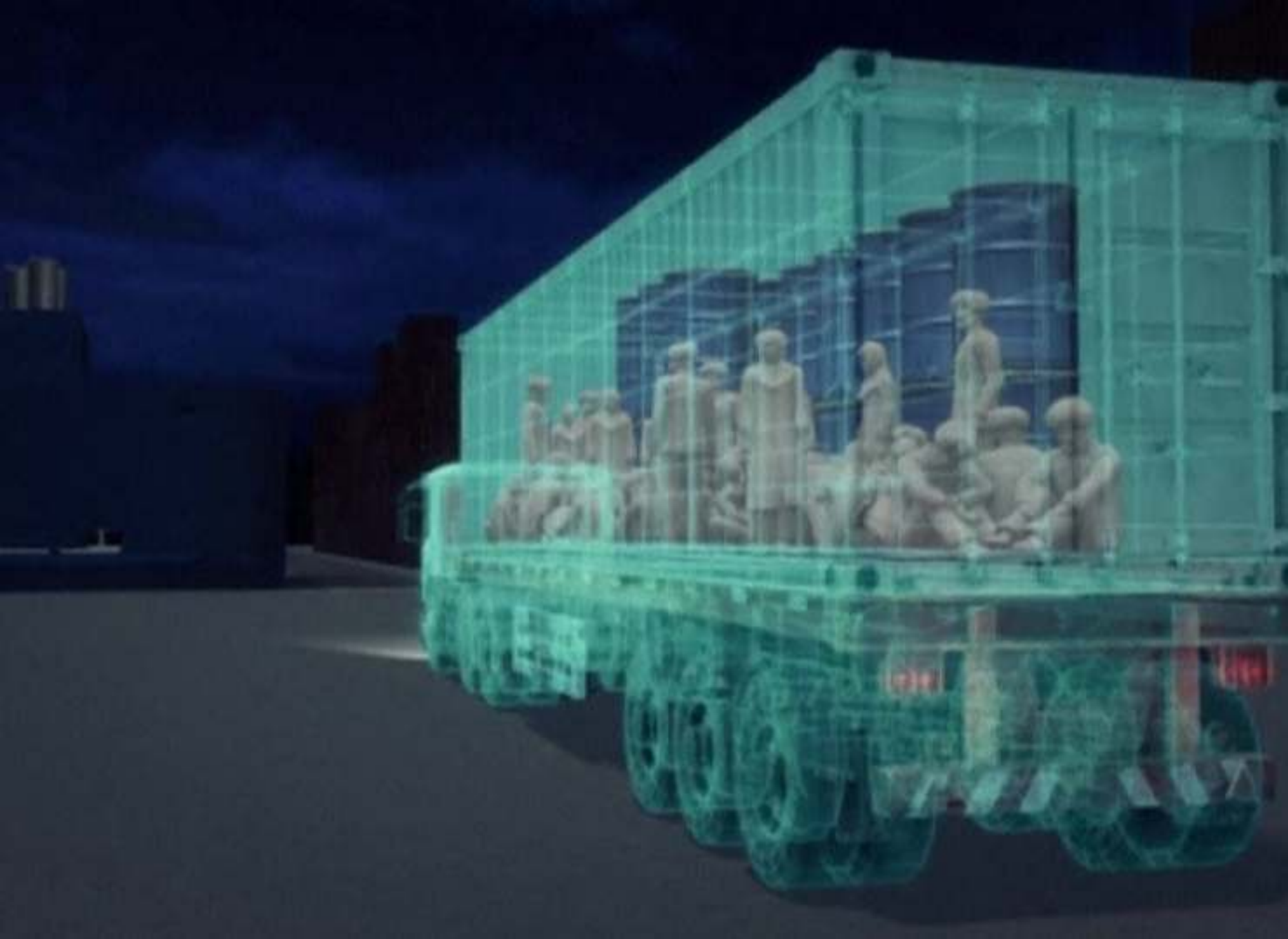
Problems in space



How it's done

- DSRC between vehicle and KonAu
- Cable to the backend
- Individual key per vehicle
  - Smartcard in vehicle
  - Stored in TC backend

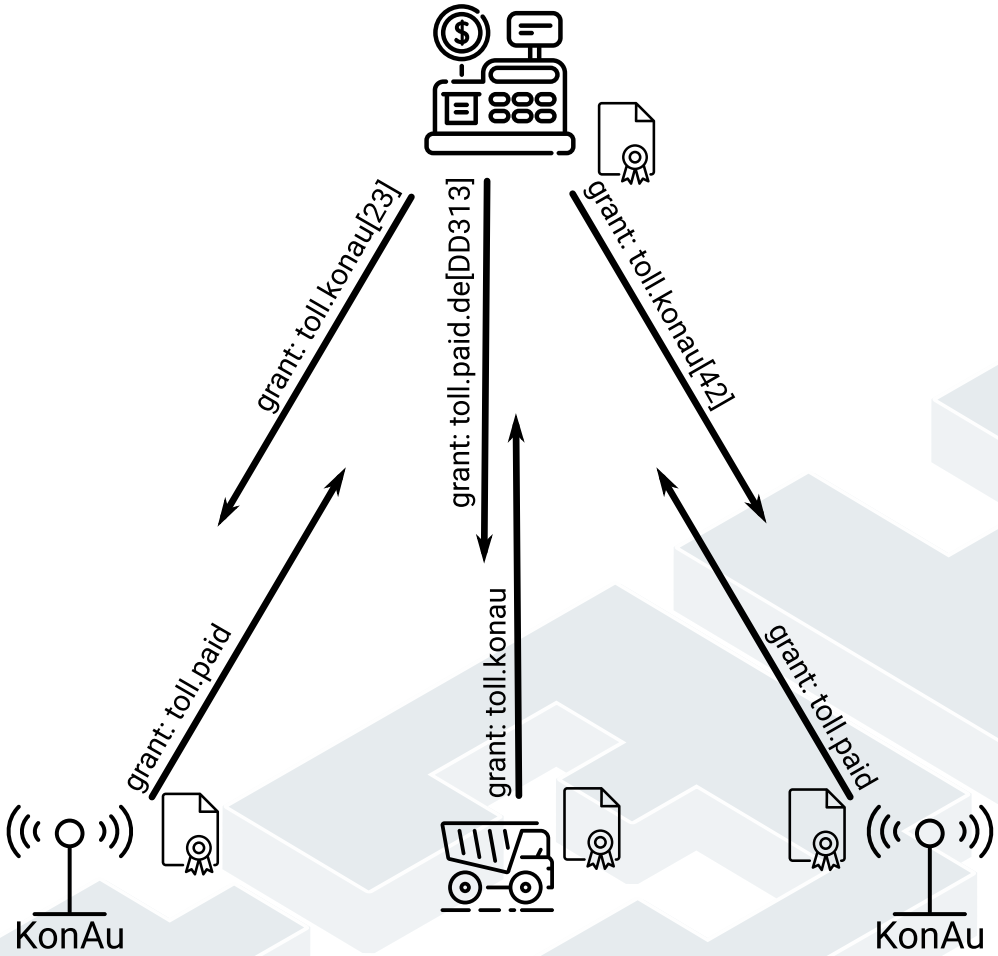
The obvious threat actors

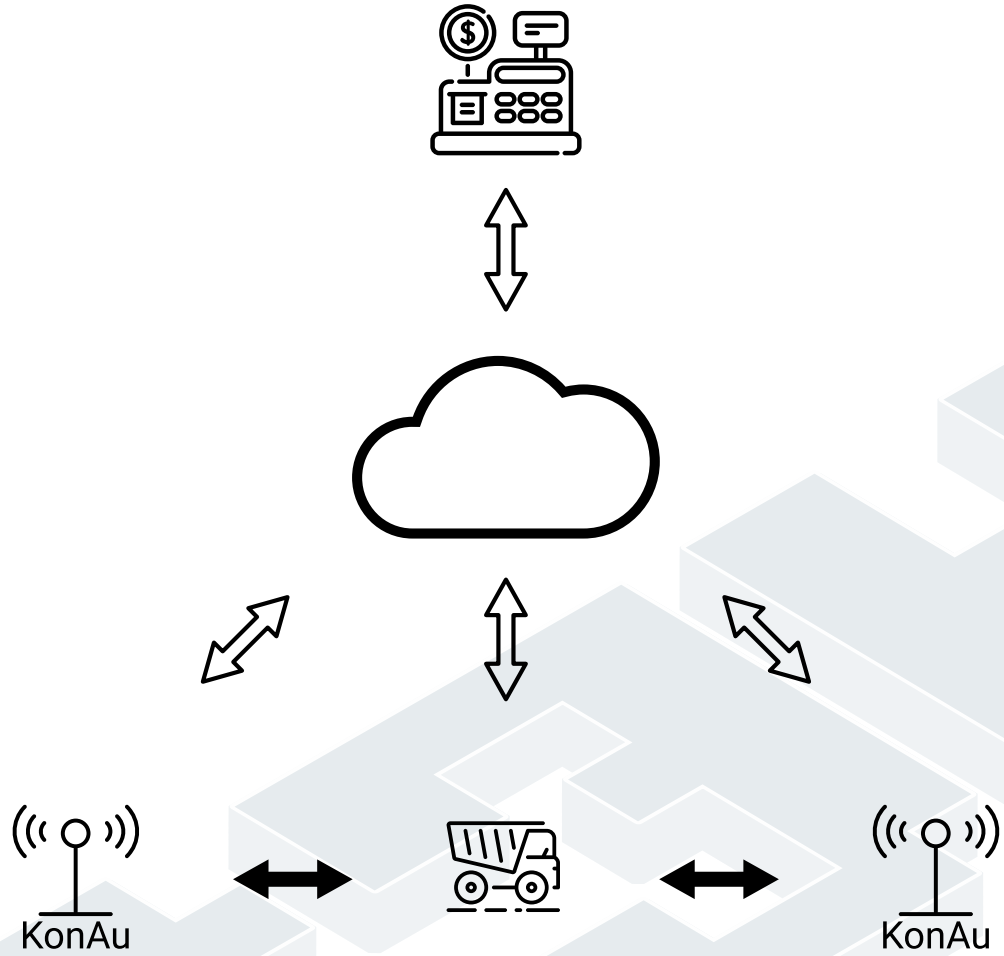


The non-obvious threat actors

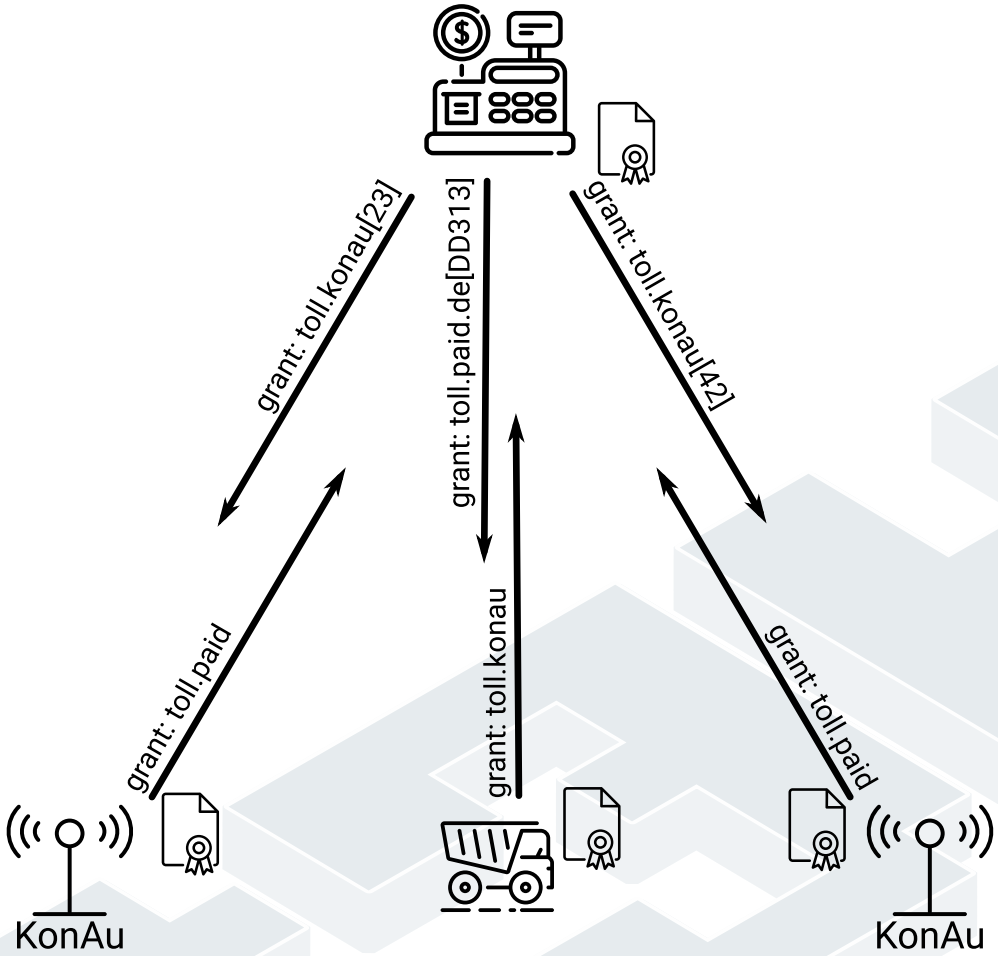

12
3
6
9

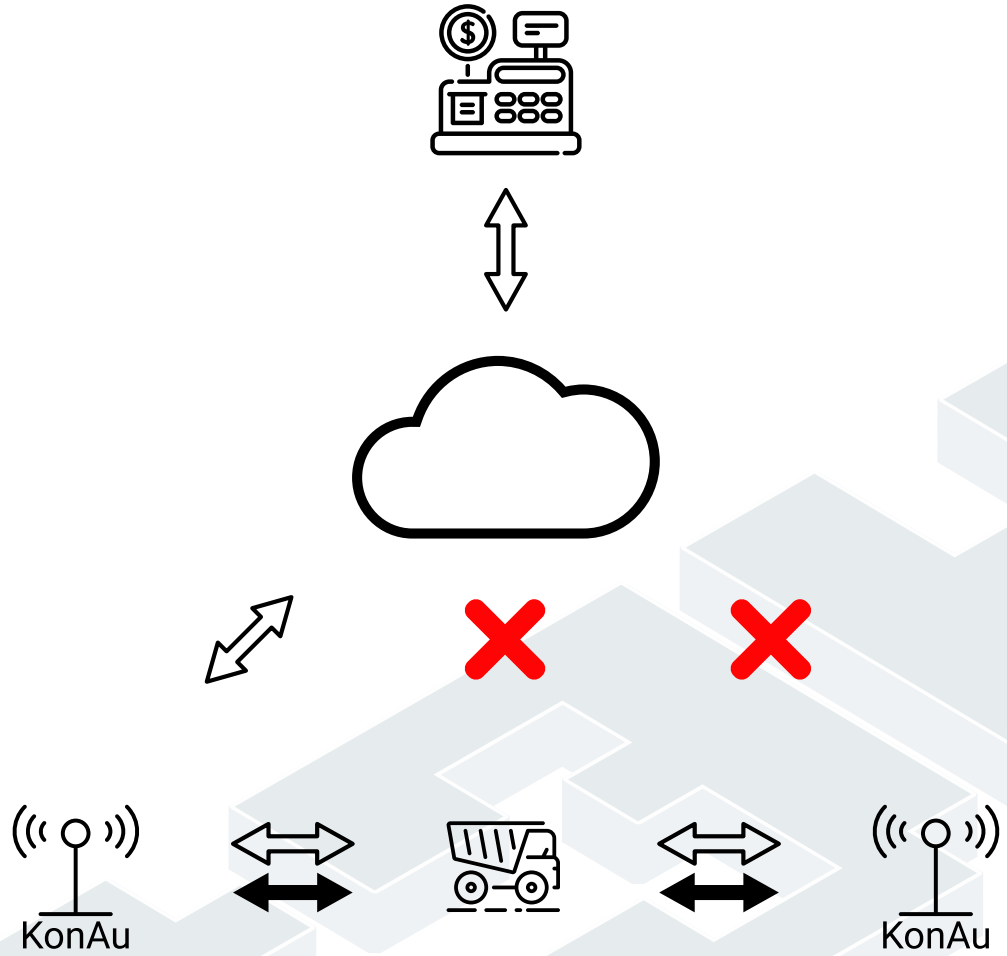
Happy Path

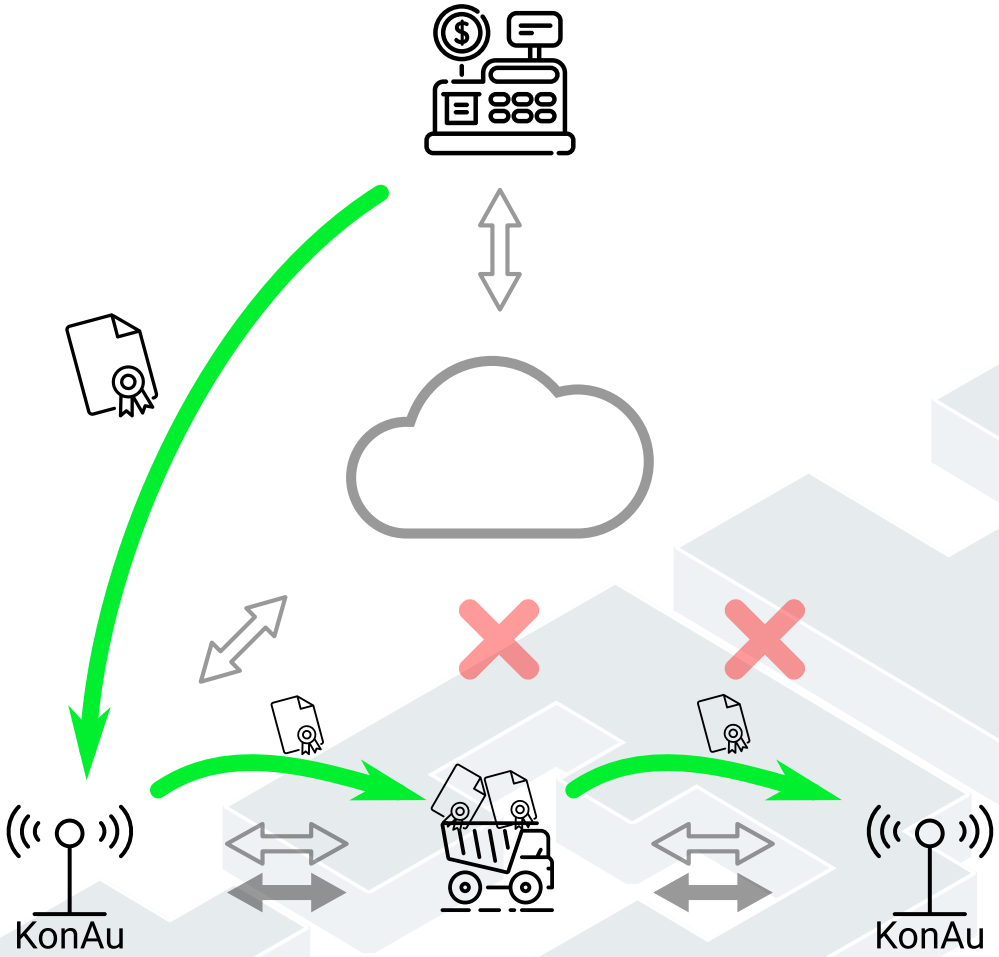

grant: toll.konau[23]
grant: toll.paid.de[DD313]
grant: toll.konau[42]
grant: toll.paid
grant: toll.konau
grant: toll.paid
KonAu
KonAu


KonAu
KonAu

Adversarial conditions
Graceful degradation to S&F networking


grant: toll.konau[23]
grant: toll.paid.de[DD313]
grant: toll.konau[42]
grant: toll.paid
grant: toll.konau
grant: toll.paid
KonAu
KonAu


KonAu
KonAu


KonAu
KonAu

Why this works

- Delegations are CRDTs
- Revocations don't exist explicitly
- Delegation changes are atomic

What's it actually good for!

Dezentralized mesh VPN w/ delegation

If you scale to IPv6, also scale your trust!

IPsec whitepaper @ p3ki.com

Globally delegatable SSO

Threat intel sharing

Change management


Revocation Day w/ P3KI Trinity

Thank you!

Gregor Jehle
gregor@p3ki.com

Felix 'FX' Lindner
fx@darklab.org

P3KI
trust yourself.

P3KI GmbH c/o Recurity Labs GmbH
Wrangelstr. 4, 10997 Berlin
contact@p3ki.com
+49 (0)30 695399933 (Berlin)
+49 (0)711 22051252 (Stuttgart)
@P3KI