escrypt
Embedded Security by ETAS

A Peer-to-Peer Approach to Digital Key Sharing for Vehicle Access & Control

Tony Rosati

Director of IOT Security, ESCRYPT

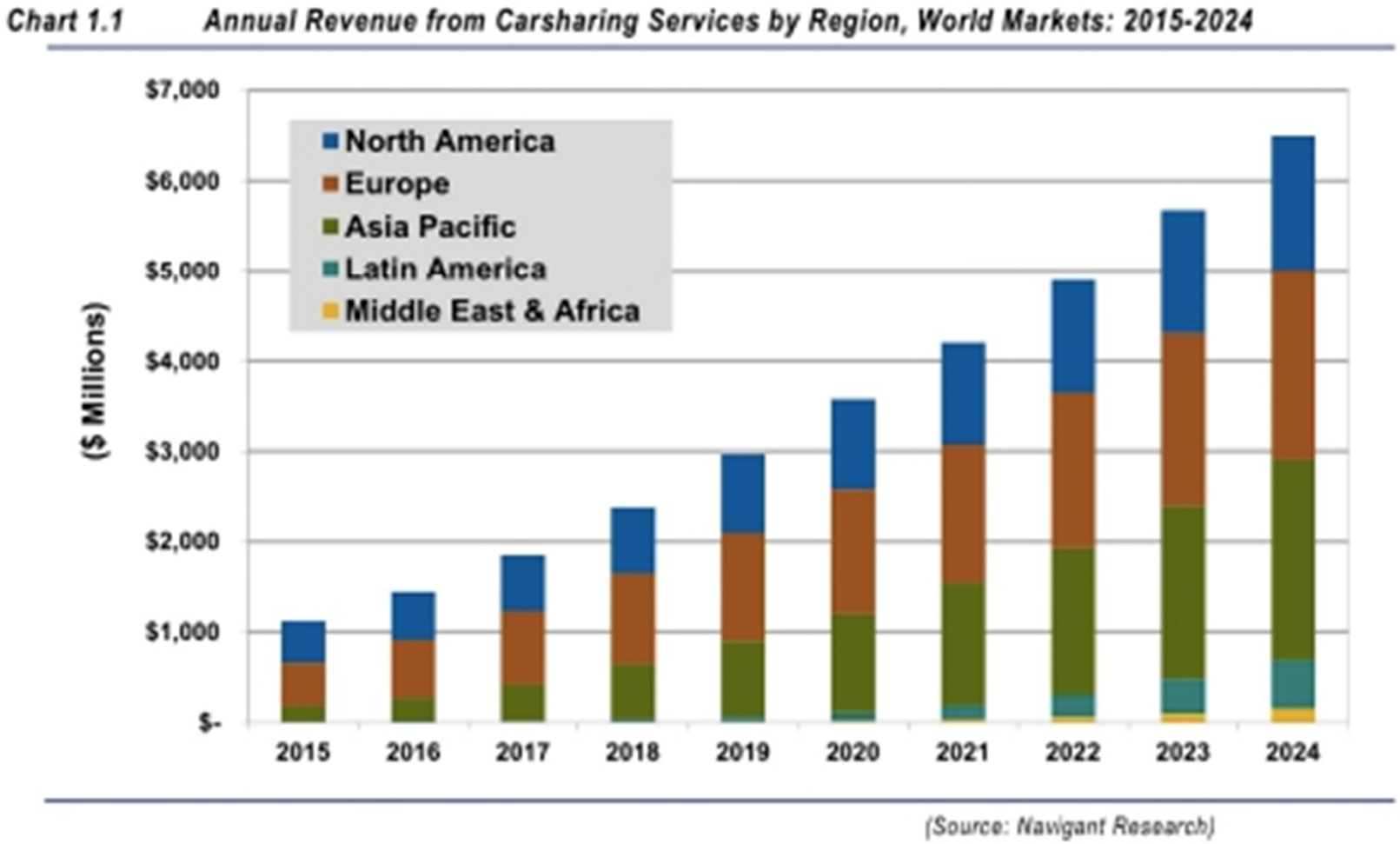
Agenda

- Motivation for Digital Key Sharing
- Architecture
- Security Model
- Security Analysis
- Future Work

Smartphone Access Control & Key Sharing

- No need to manage physical keys
- Desire/Need to use the Smartphone
  - Vehicle sharing
  - Security alerts
  - Control/Status

Car Sharing Growth



- Cars are increasingly too costly to own in the urban environment
- Cars sit unused most of the time
- Many new services:
  - BMW Drivenow,
  - Avis: Zip Car,
  - Daimler: Car2Go,
  - Uber,
  - Lyft

Smartphone/Vehicle Integration

Vehicle Access

- NFC and/or Bluetooth
- Security of the smartphone?

Enable

- Wireless Charging Bluetooth Handoff
- Vehicle personalization

Consumers Expect a Seamless User Experience

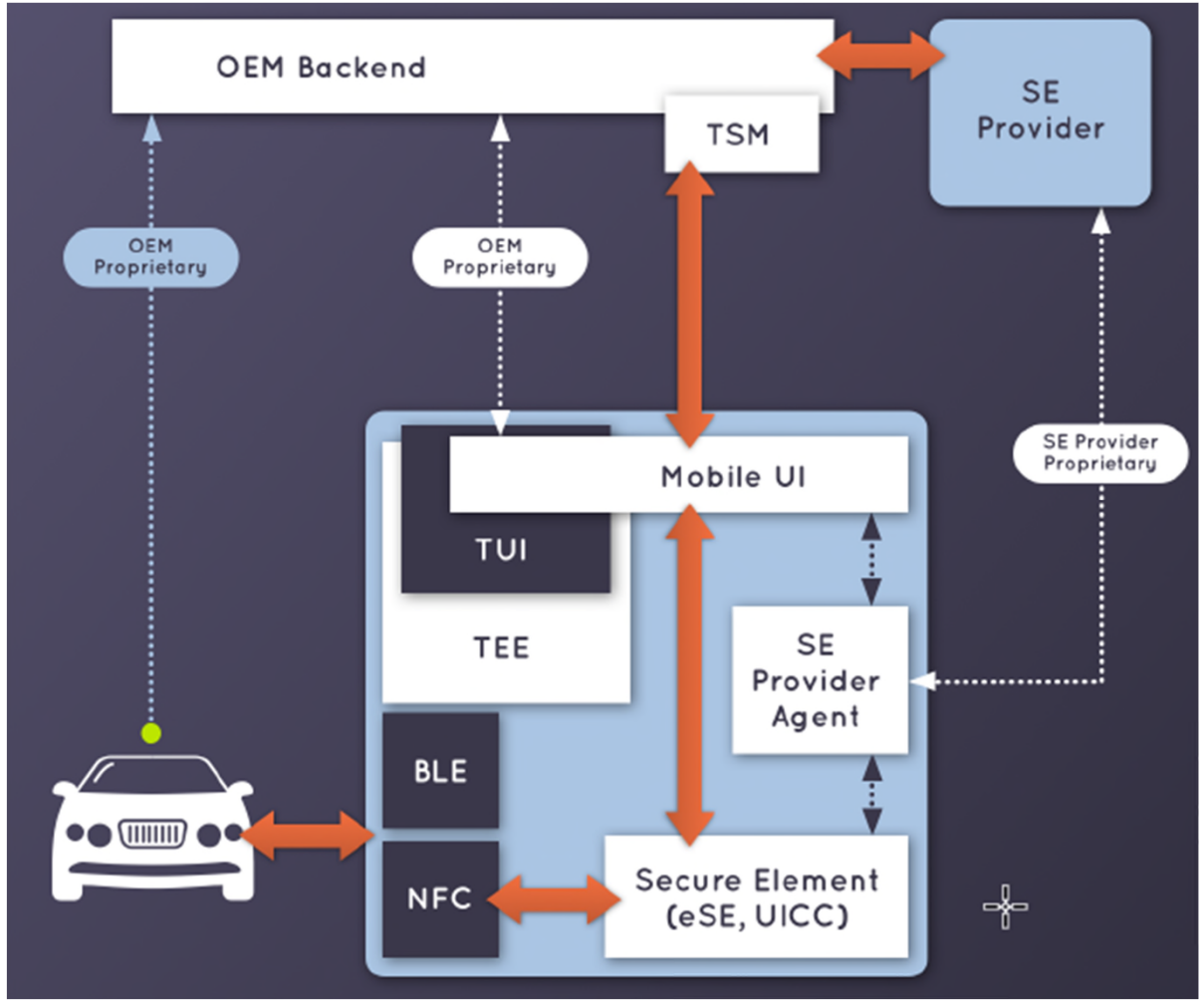
CONNECTIONS SUMMIT

escrypt
Embedded Security by ETAS

#Perfectly keyless #digital vehicle key #key management

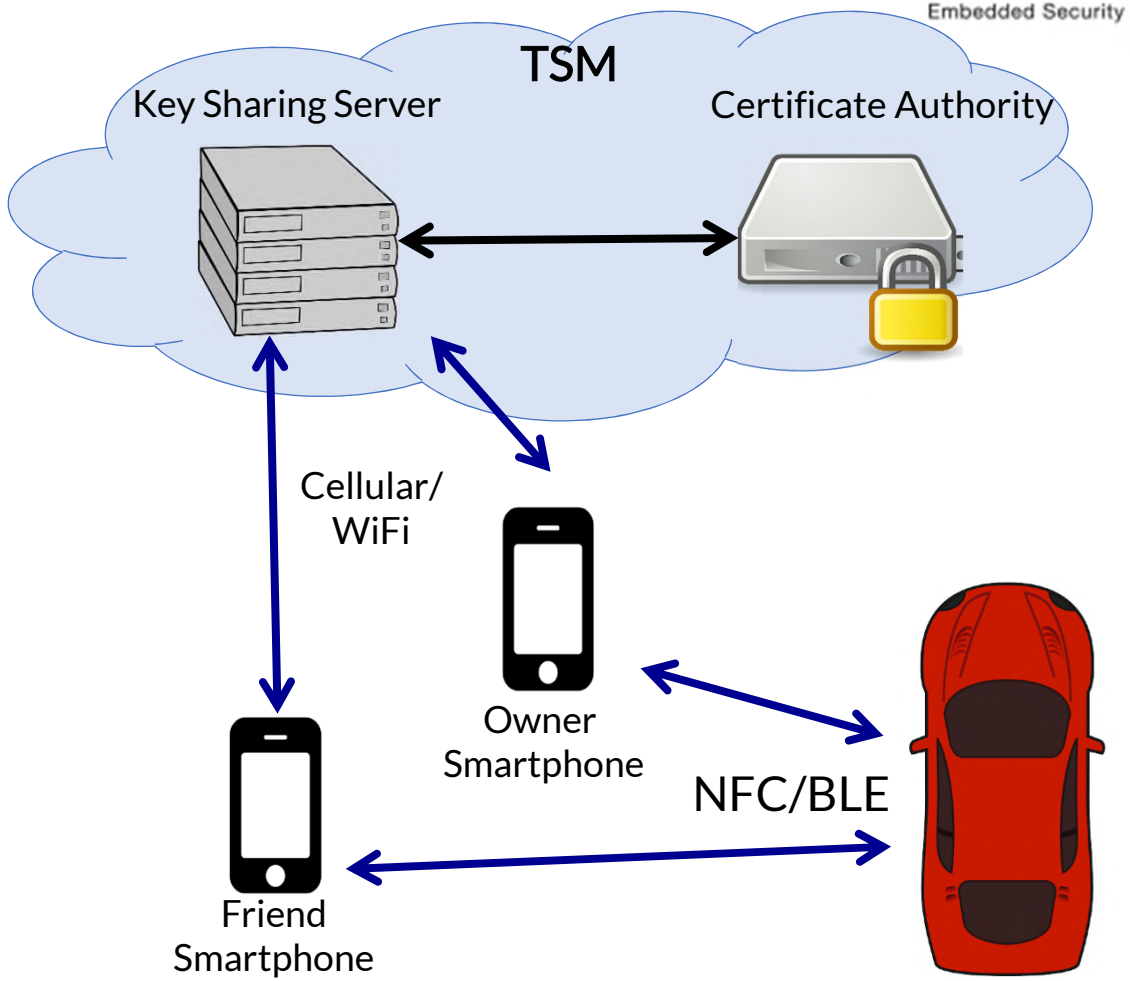
Perfectly keyless

Connected Car Consortium Model



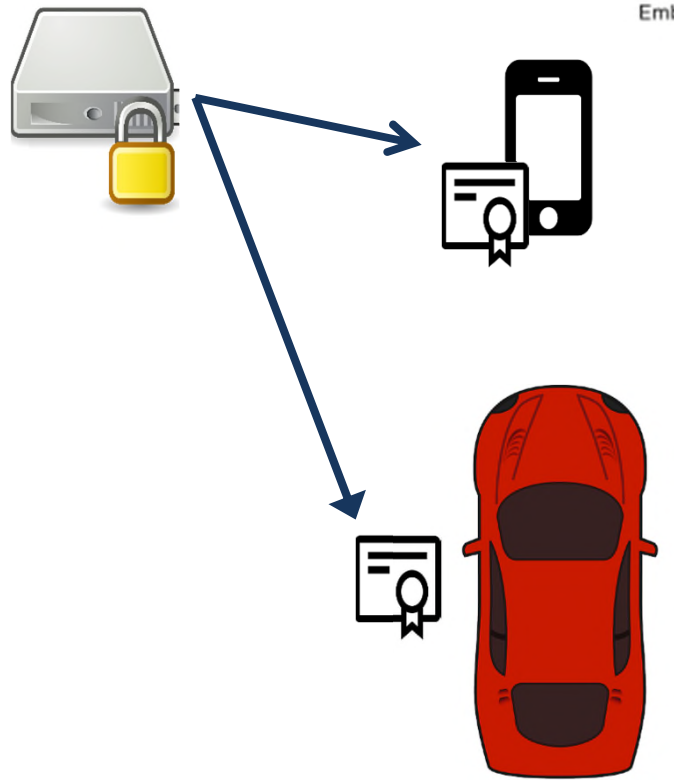
ESCRYPT CycurACCESS Architecture

- Leverage Public Key Infrastructure (PKI)
  - Enables efficient digital key sharing
    - Issue Identity Certificates
    - Massively scalable
- Leverage Mobile Platform Security
  - Secure Boot
  - Secure Key Store (hardware level attestation)
  - Sandboxing
  - Code Signing



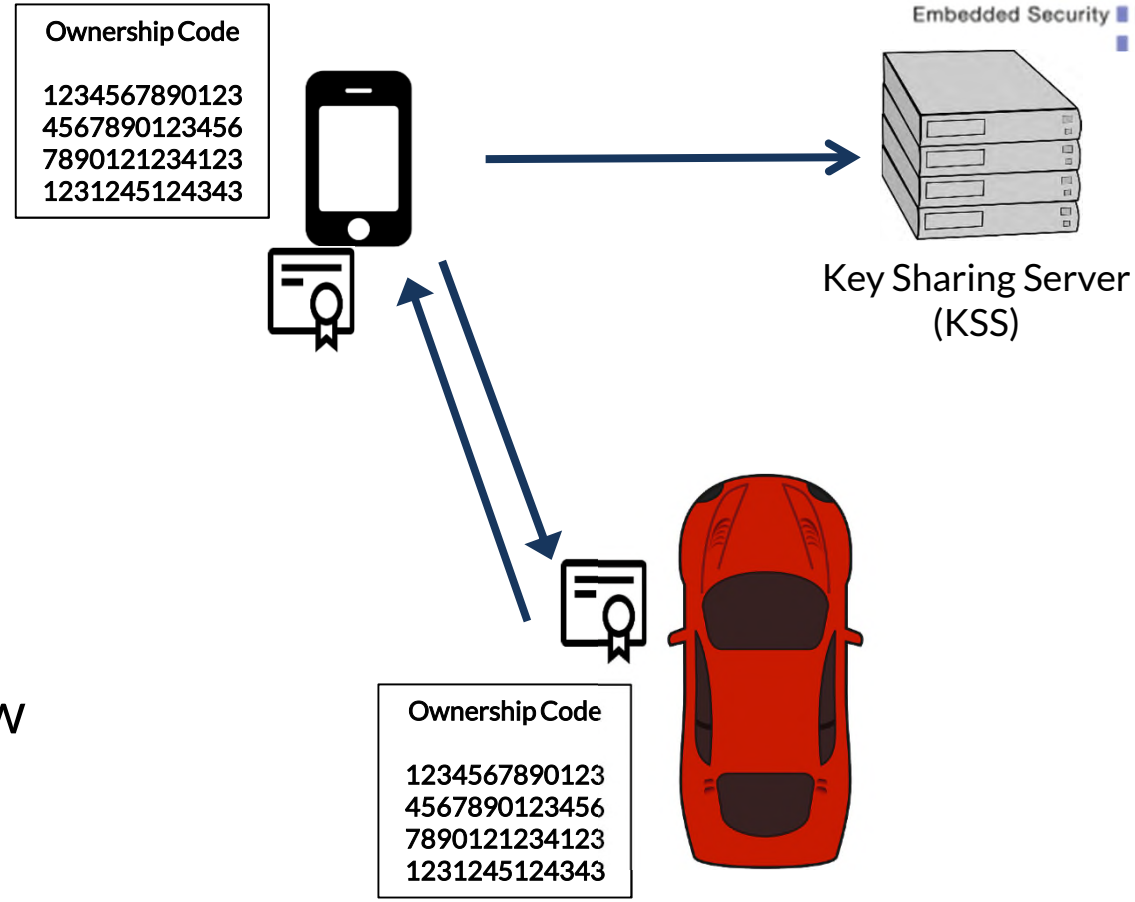
Proving Identity

- Certificate Authority provides a root of trust
- Identity certificates are issued to each user and each vehicle
  - Vehicle certificates issued in production
  - User Certificates issued at registration
- Entities in the system can now verify each other's identity securely and efficiently
  - Verification can be performed offline



Establishing Ownership

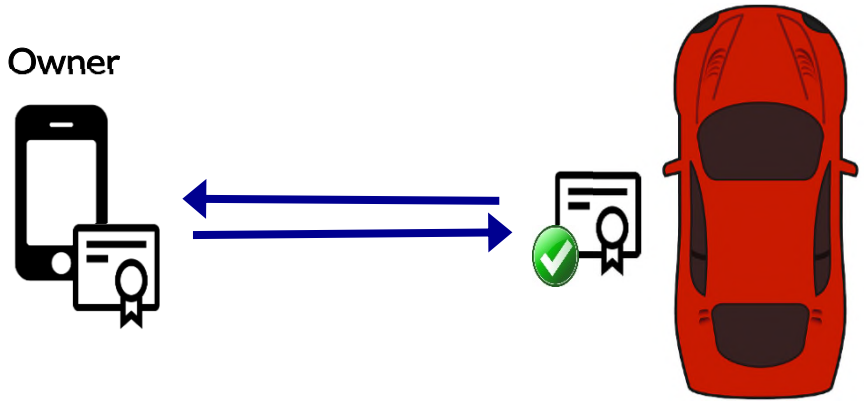
- Each vehicle is assigned a random Ownership Code during manufacture
- The owner and the vehicle exchange certificates & a challenge to prove identity
  - The owner sends the Ownership Code to the vehicle to prove ownership
  - If valid, vehicle stores new owner certificate for future use
- Vehicle generates and forwards signed “proof” to KSS via the owner to confirm new ownership



Gaining Access

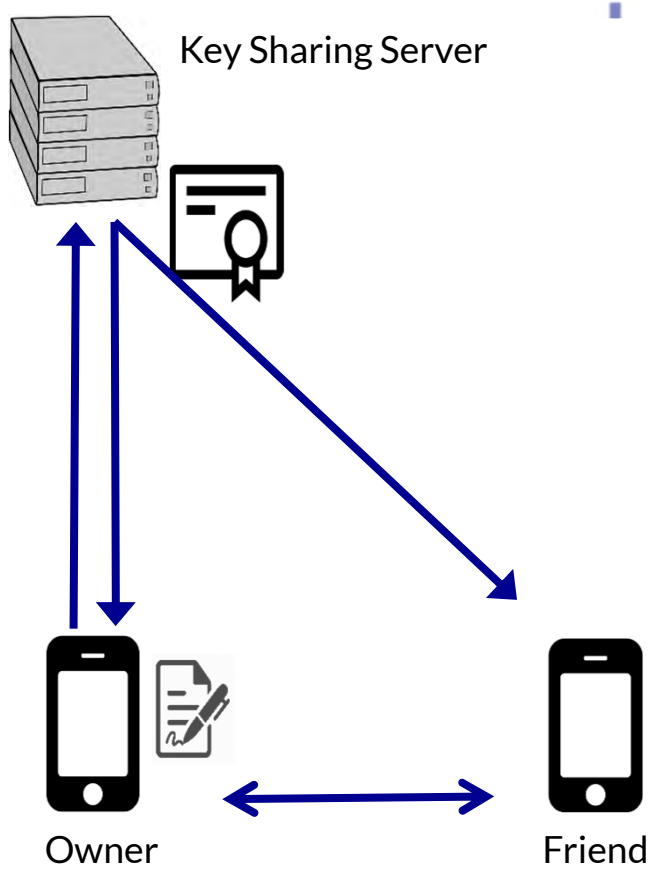
- To unlock the vehicle, the owner and vehicle begin by exchanging certificates & a challenge to prove identity

- The vehicle verifies the identity against stored owner certificate. If so, access is granted



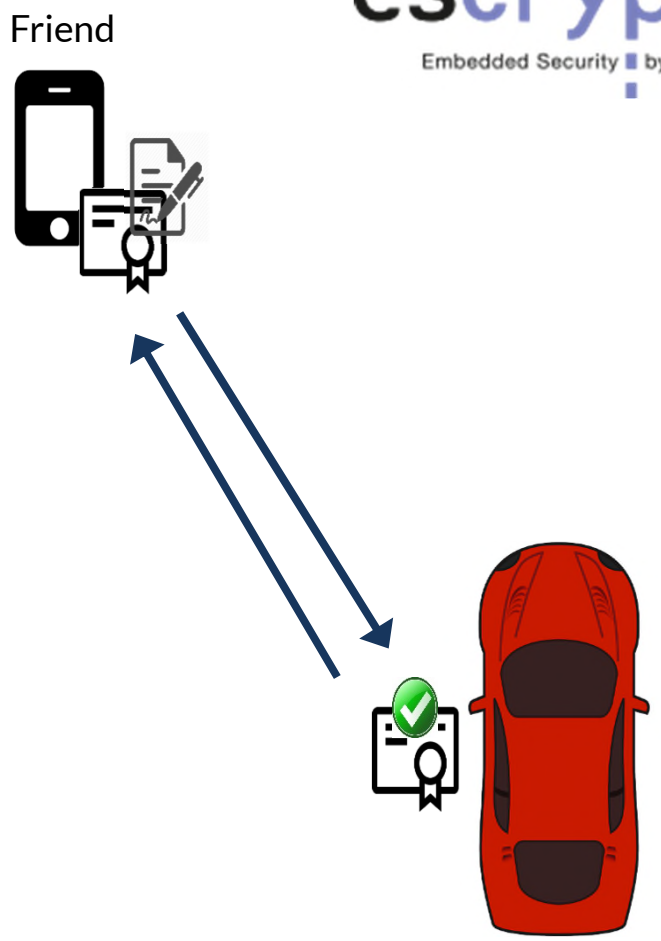
Key Sharing

- Owner creates and signs Sharing Permission containing Vehicle ID, serial number of friend's Identity certificate and any restrictions
- Owner forwards Sharing Permission to the friend via the KSS or P2P
- Note that the KSS does not have to be involved in this process



Shared Access

- To unlock the vehicle, the friend and vehicle begin by exchanging certificates & a challenge to prove identity
- The friend sends the Sharing Permission to the vehicle
- The vehicle verifies that the following is true of the Permission:
  - Issued for this vehicle
  - Issued to the friend
  - Signed by the owner
  - No restrictions are violated
- If checks pass, access is granted

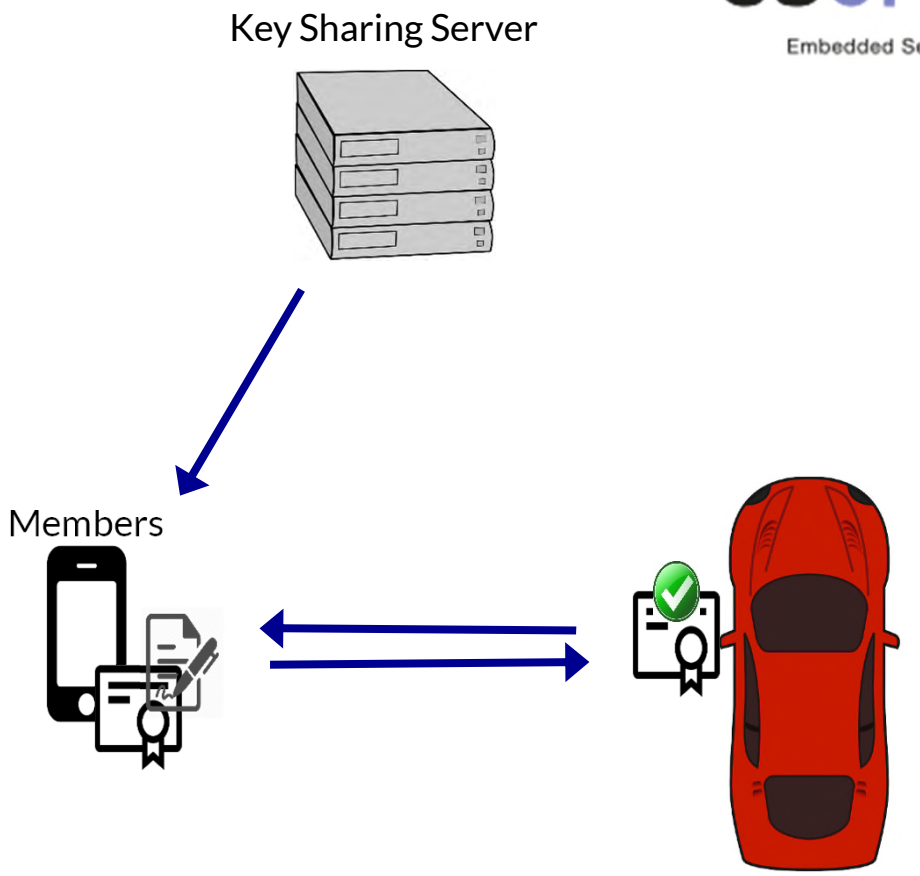


Car Sharing Service

- All vehicles are owned by the service
- All valid members are issued permissions

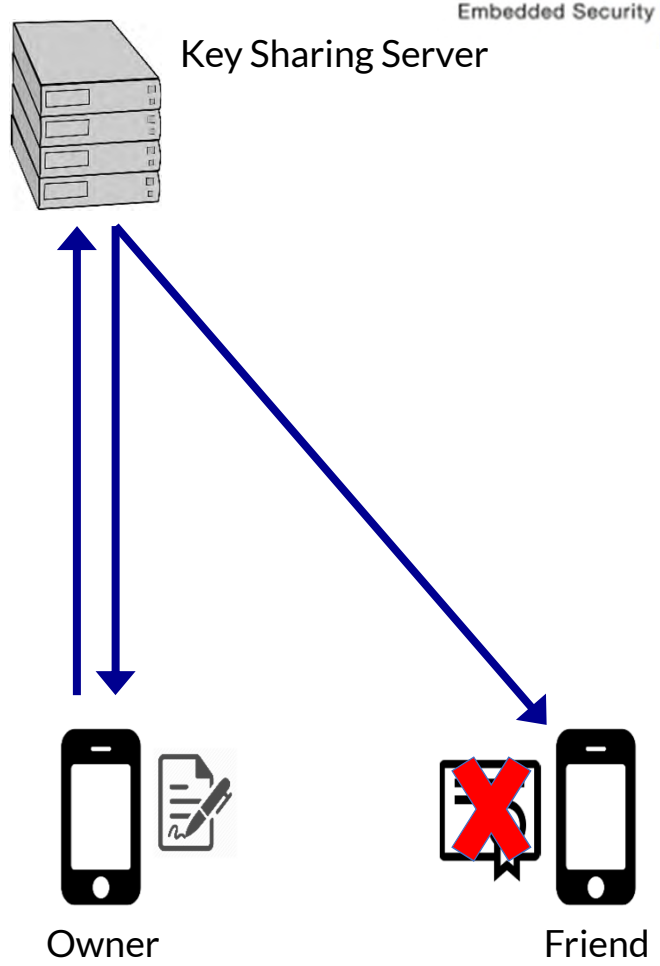
- The vehicle verifies that the following is true of the Permission:
  - Issued for this vehicle
  - Issued to the member
  - Signed by the service
  - No restrictions are violated
- If checks pass, access is granted

- How do we revoke bad actors?



Revoke a Permission

- To revoke a Permission, the owner generates a signed revocation request and forwards to the KSS
- If valid, the KSS generates a revocation notification and forwards to the friend's device
- Friend's device deletes the affected Permission



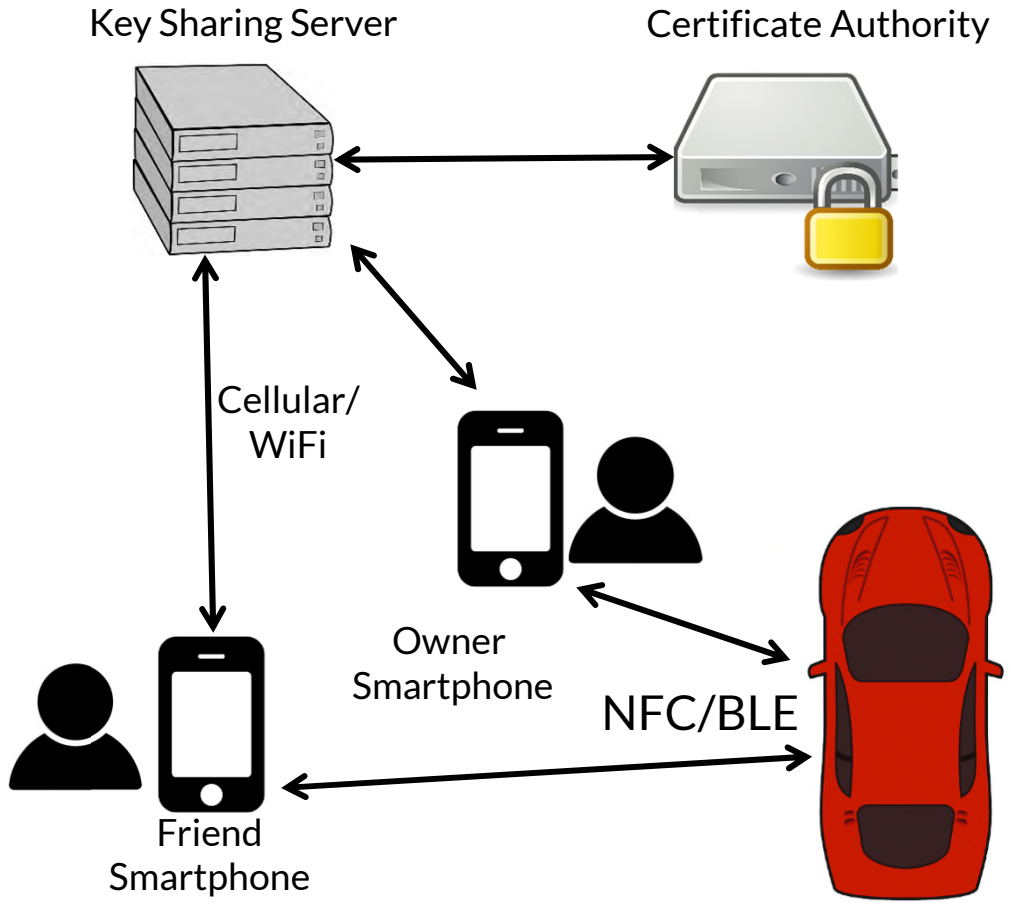
Dealing with Cheaters

- What if the friend is dishonest?
  - Friend takes their device offline to prevent the Permission from being deleted
- How does a car know that a permission is revoked?
- What can be done to mitigate this?

- Three ideas:
  - Next time the owner unlocks the vehicle, a list of recently revoked Permissions can be transferred to the vehicle
  - Permissions could require a periodic authorization from the KSS to remain valid. (Say every 24 hours)
  - A connected car receives revocations directly

Security Analysis/Threat Model

- Based on the work of Symeonidis et al.
- Main Features
  - Private keys are never transported & stored in SE
  - KSS compromise cant be used to gain or share access
  - Most operations are performed offline which limits the attack surface (ie Denial-of-Service)



Relay Attack

- Mitigation Strategies
  - Easy
  - User based preference
    - Smartphone screen off
  - Hard
  - RF Finger Print
  - Distance Bounding
    - Brands and Chaum 1994 – smart cards
    - Gambs et al 2016 – smartphones
      - Can detect adversary constantly > 1.5ms relay

Conclusion & Future Work

- A new approach digital Key Sharing
  - Using well-known PKI & modern smartphone security
  - Most operations are done offline to limit the attack surface
- Futures
  - Hardware level Key Attastation
  - Relay Attack Countermeasures

- Thank you
  - tony.rosati@escrypt.com