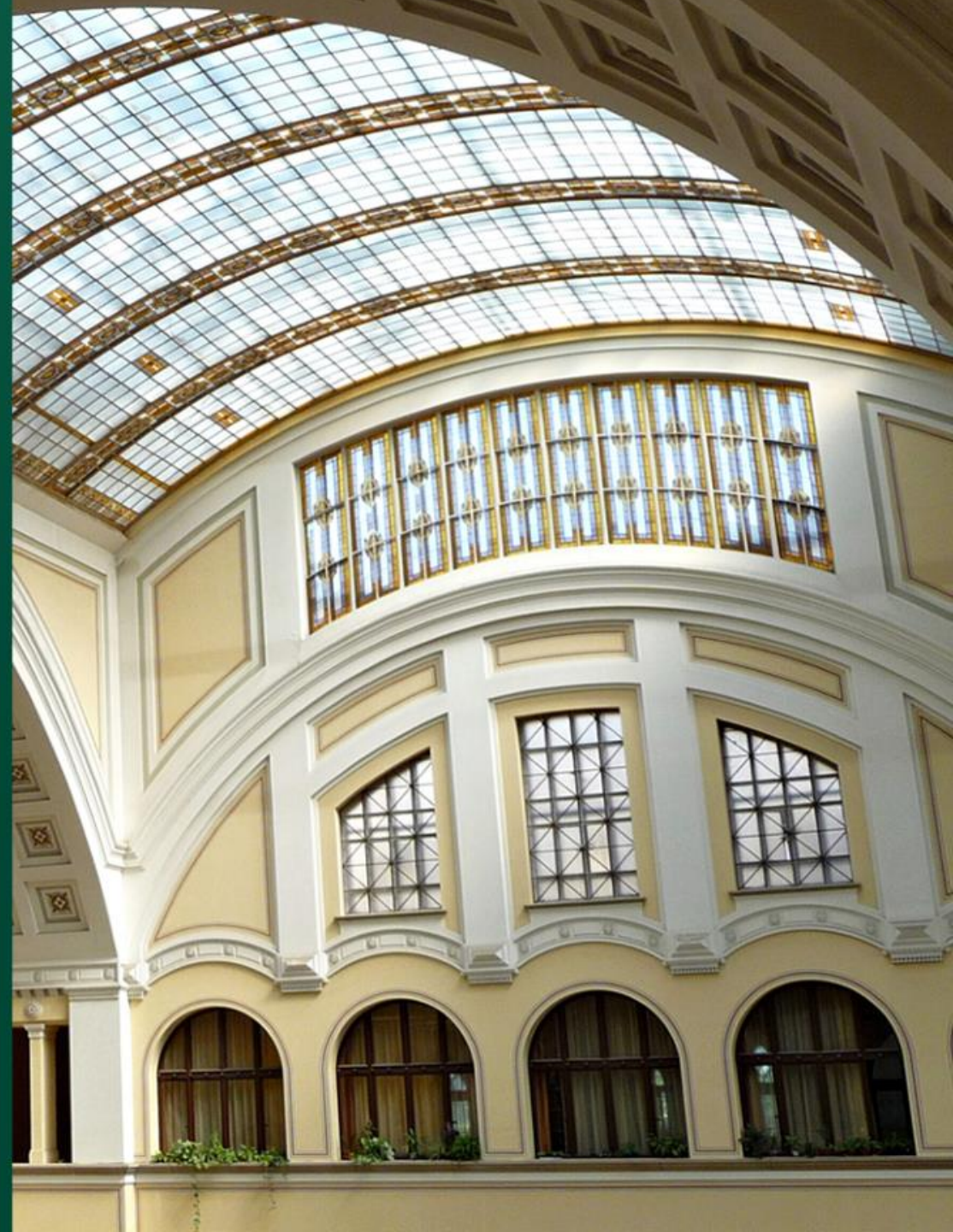
Hibrid anonim üzenetszórás

Kovács Szabolcs Zoltán

DEBRECENI EGYETEM



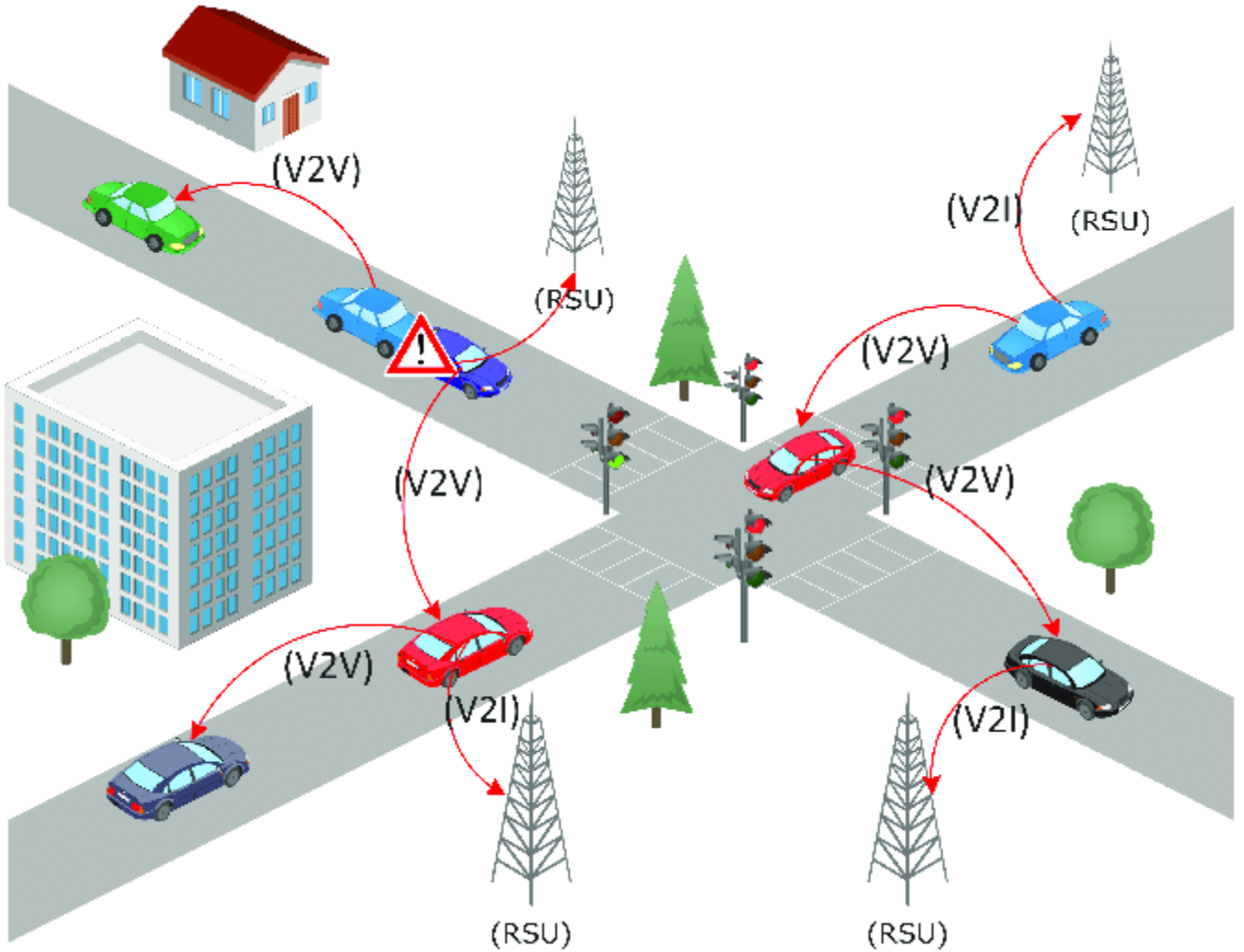
Tartalom

- Bevezetés
  - VANET
    - A VANET biztonsági követelményei
- Hibrid anonim üzenetszórás
  - Biztonsági célok
  - Implementáció és prototípus
  - Eredmények

DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

A járművek Ad-Hoc hálózata - VANET



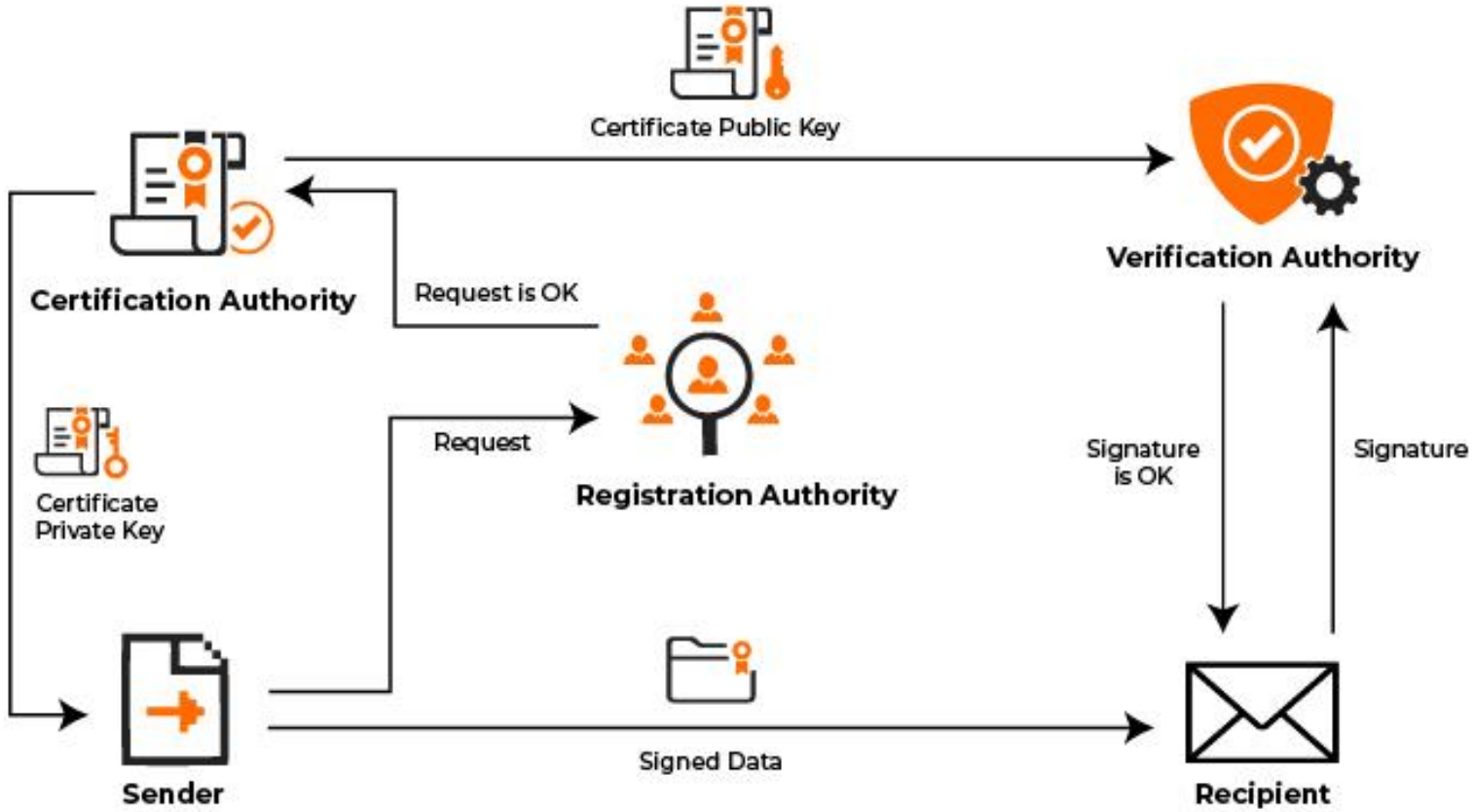
DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

Biztonsági elvárások

- **Jogosultság**: Biztosítani kell, hogy csak az arra jogosult résztvevők küldhessenek érvényes üzeneteket.
- **Feltételes anonimitás**: Egyrészről a V2V és a V2I kommunikációnak anonimnak kell lennie, másrészről az anonimitás visszavonható kell legyen.
- **Átláthatóság**: Egy fennhatóság tevékenységének átláthatónak kell lennie a hálózat összes résztvevője számára.
- **Hatékonyság**: Egy alkalmas biztonsági modellnek hatékonyan kell működnie mind a torlódások, mind az alacsony forgalom esetében.

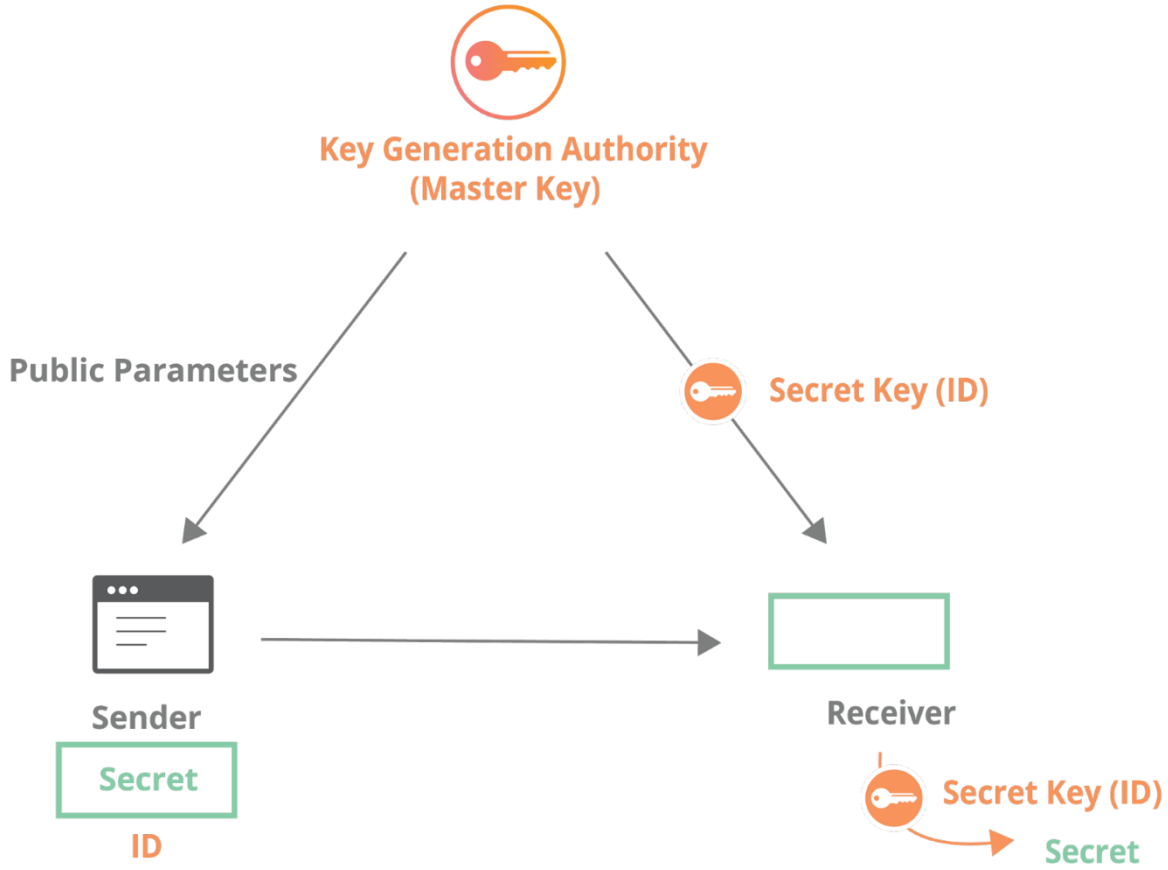
Nyilvános kulcsú infrastruktúra



DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

Identitás-alapú infrastruktúra



DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

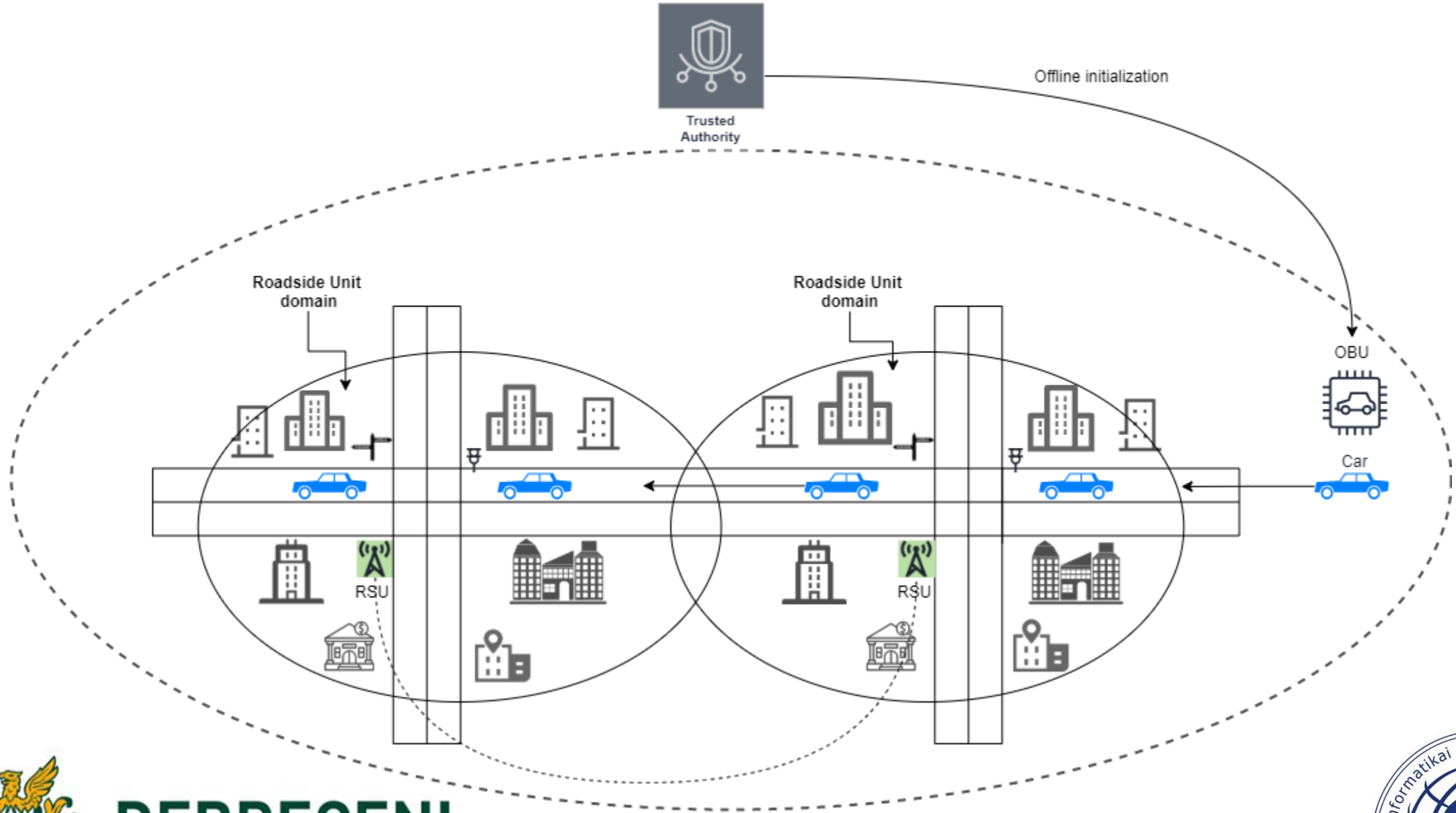
Hibrid anonim üzenetszórás

- **Lokálisan IBE:** ugyanazon TA alatt működő járművek identitás-alapú infrastruktúrában kommunikálnak

- **Globálisan PKI:** járművel, amelyek más TA fennhatósága alól érkeznek, tanúsítványokkal hitelesítik magukat

DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar



DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

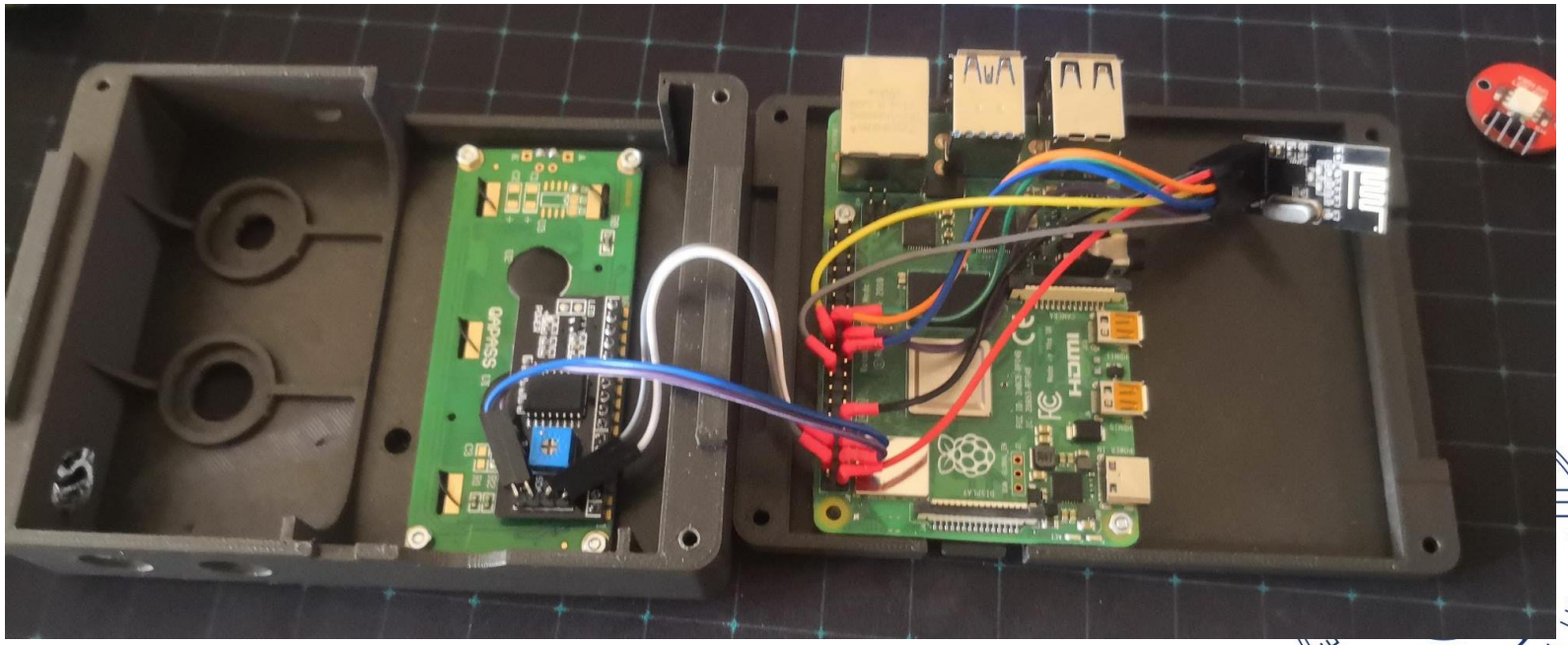
Implementáció és prototípus

- Választott programozási nyelv (Python és MicroPython).
- Az implementációhoz egy szabványgörbét használtunk, és az összes szükséges műveletet implementáltuk.
- Az implementáció hatékonyságának bizonyítása érdekében összeállítottam egy egyszerű prototípust alacsony számítási kapacitású eszközök felhasználásával.

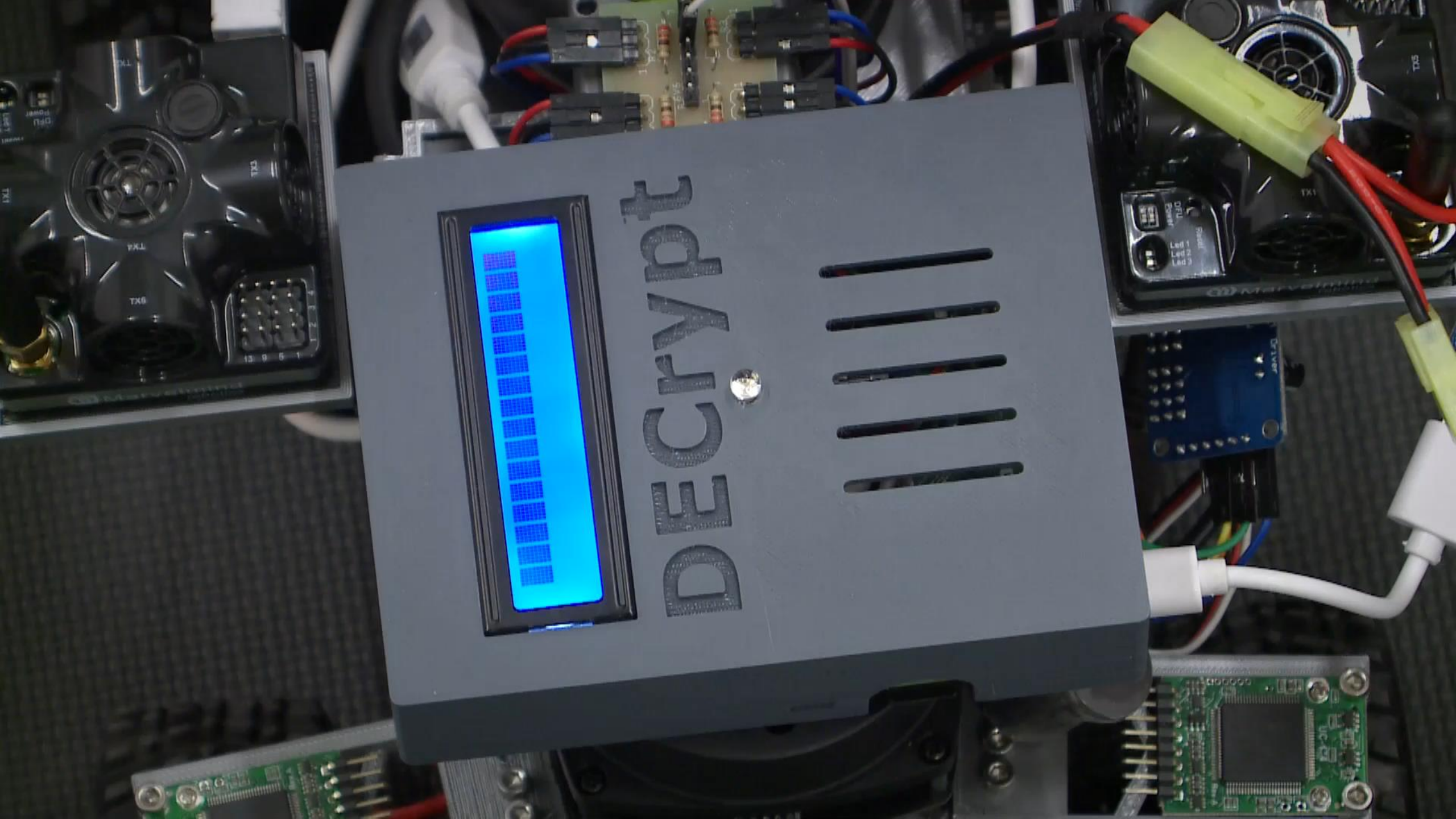
DEBRECENI EGYETEM

Debreceni Egyetem Informatikai Kar

Implementáció és prototípus



DEBRECENI EGYETEM


DECrypt

Köszönöm a figyelmet