



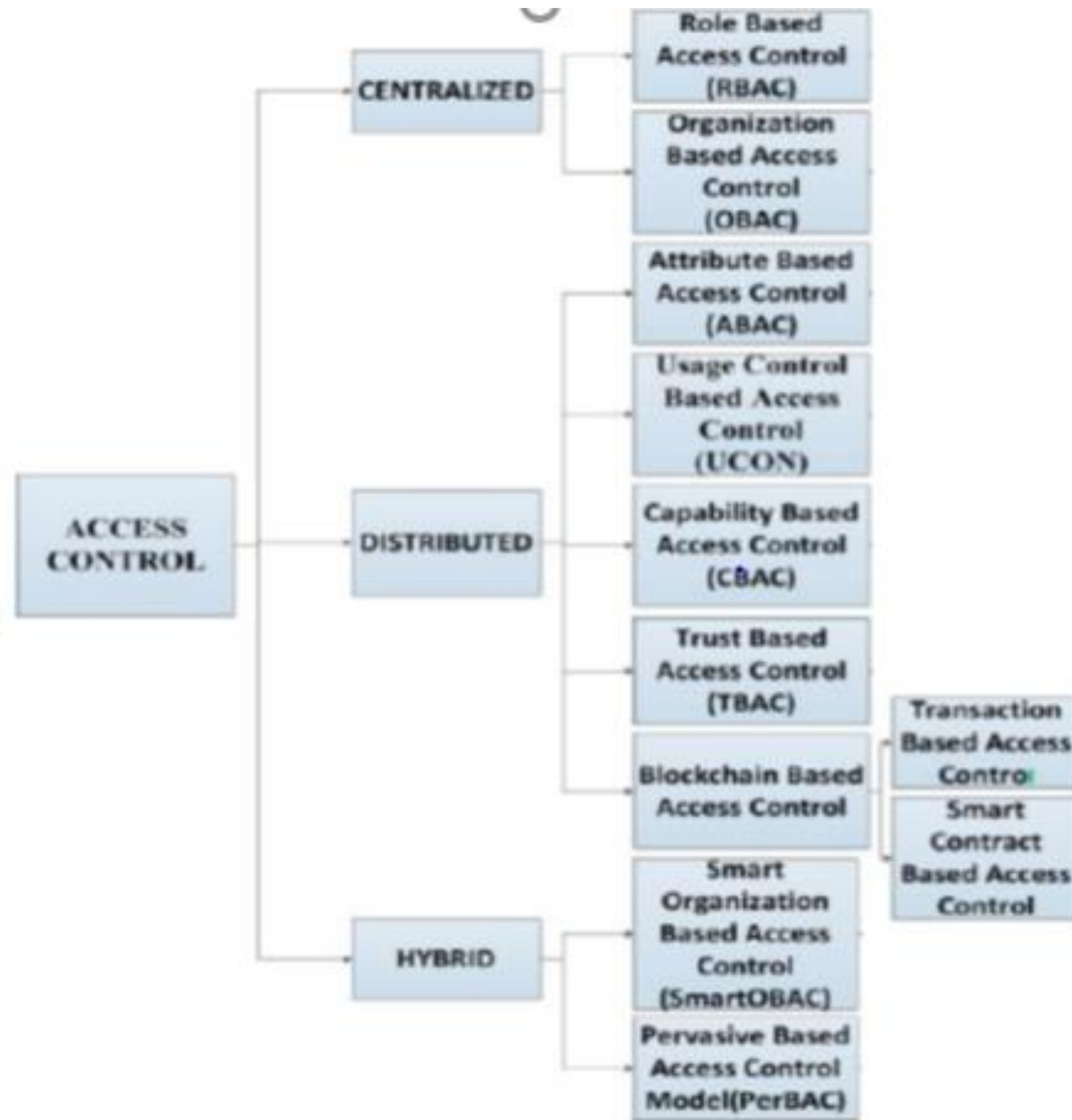
FRONT-END JOGOSÍTÁS-ELLENŐRZÉS



VILMOS ANDRÁS 2021. március 17.

(IA&A)
Bemutatkozás,
Azonosítás,
Engedélyezés

- A bemutatkozás a személy vagy a dolog identitásának jelzése
 - (pl. felhasználó név megállapítása)
- Az azonosítás az alany személyazonosságának [...] bizonyítása
 - (pl. a beírt és tárolt jelszó összehasonlítása).
- Az engedélyezés az erőforrásokhoz való hozzáférési jogok elbírálásának funkciója



IBAC (Identity Based Access Control – Személyiség alapú)

- A felhasználóknak egyedi, személyre szabott jogosítás készletük van.

RBAC (Role Based Access Control – Szerep alapú)

- A felhasználók jogosítása a szervezetben betöltött szerepükhöz kötődik.

ABAC (Attributes Based Access Control – Attribútum alapú)

- A jogosítások a felhasználók tulajdonságaihoz igazodnak (e.g.: kor, földrajzi hely, egészségügyi állapot, stb.)

TBAC (Trust Based Access Control – Bizalom alapú)

- A bizalom három elemre épül: tulajdonság, megfigyelés, ajánlás, és a köztük fennálló viszonyrendszerre

Blockchain

- Tokenizált jogosítás ellenőrzés
- Smart contract alapú jogosítás ellenőrzés

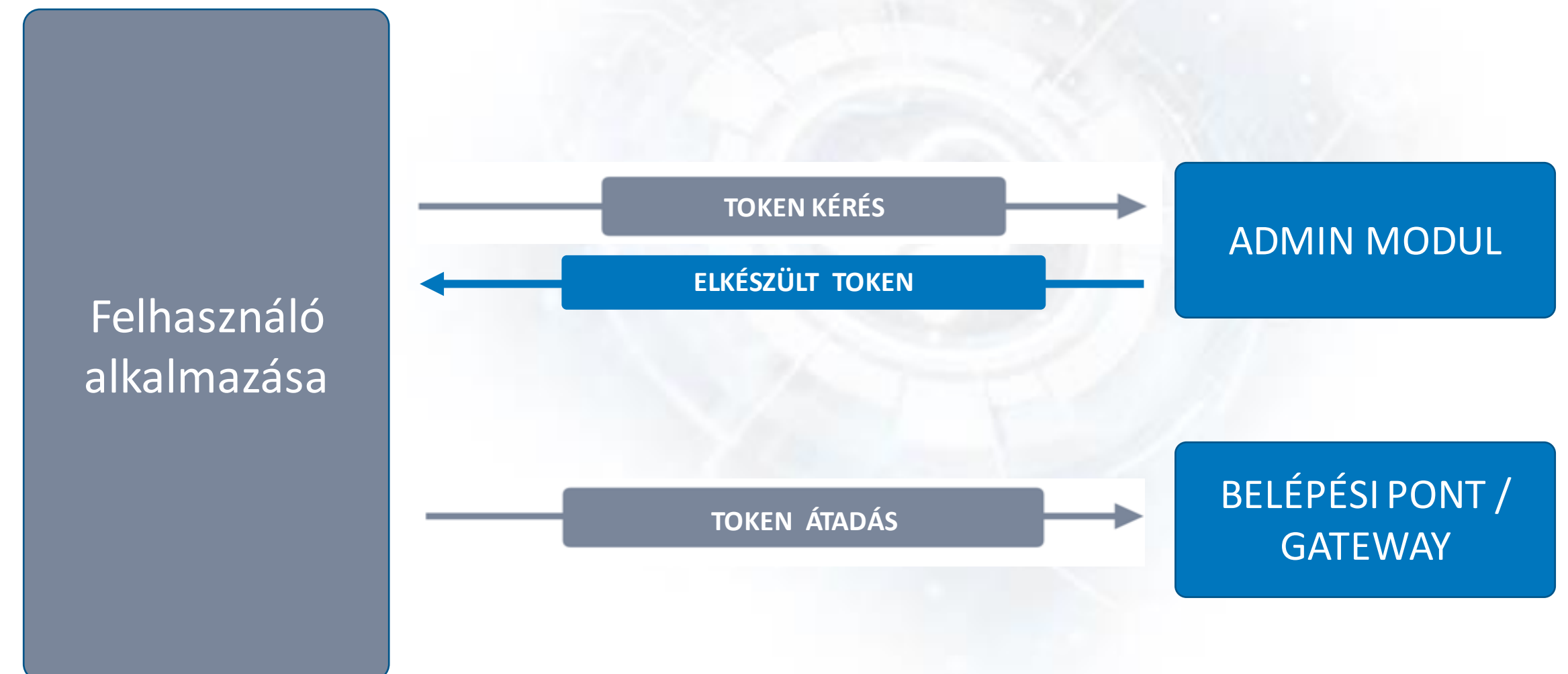
IoT JOGOSÍTÁS- ELLENŐRZÉS HIÁNYOSSÁGAI

- Skálázhatóság hiánya
 - Eszközök száma, felhasználók száma
- Túlzott erőforrás igény
- Egyetlen meghibásodási pont
 - Rendelkezésre állási kockázat
- Szükséges jogosítás elve nem biztosított
 - Nem elég részletes a jogosítás lebontás
- Együttműködő rendszerek korlátos interoperabilitása
- Jogosítás átadás nyomon követése hiányzik
- Nincs valós idejű jogosítás kibocsátás és visszavonás

CAPABILITY BASED ACCESS CONTROL – CBAC

TOKEN alapú jogosítás-ellenőrzés

- A „Capability” egy TOKEN, ami a birtokosának meghatározott hozzáférést biztosít egy entitáshoz
- A TOKEN, a birtokosának jogosultságait tartalmazza
- Aki elfogadja a TOKENT, az megismeri, hogy a birtokos milyen jogosításokkal rendelkezik
- A rendszernek nem kell foglalkoznia a jogosítási szabályokkal, csak a TOKEN megfelelését (aláírását) kell ellenőriznie.



A BIZTONSÁG A CBAC ESETÉN

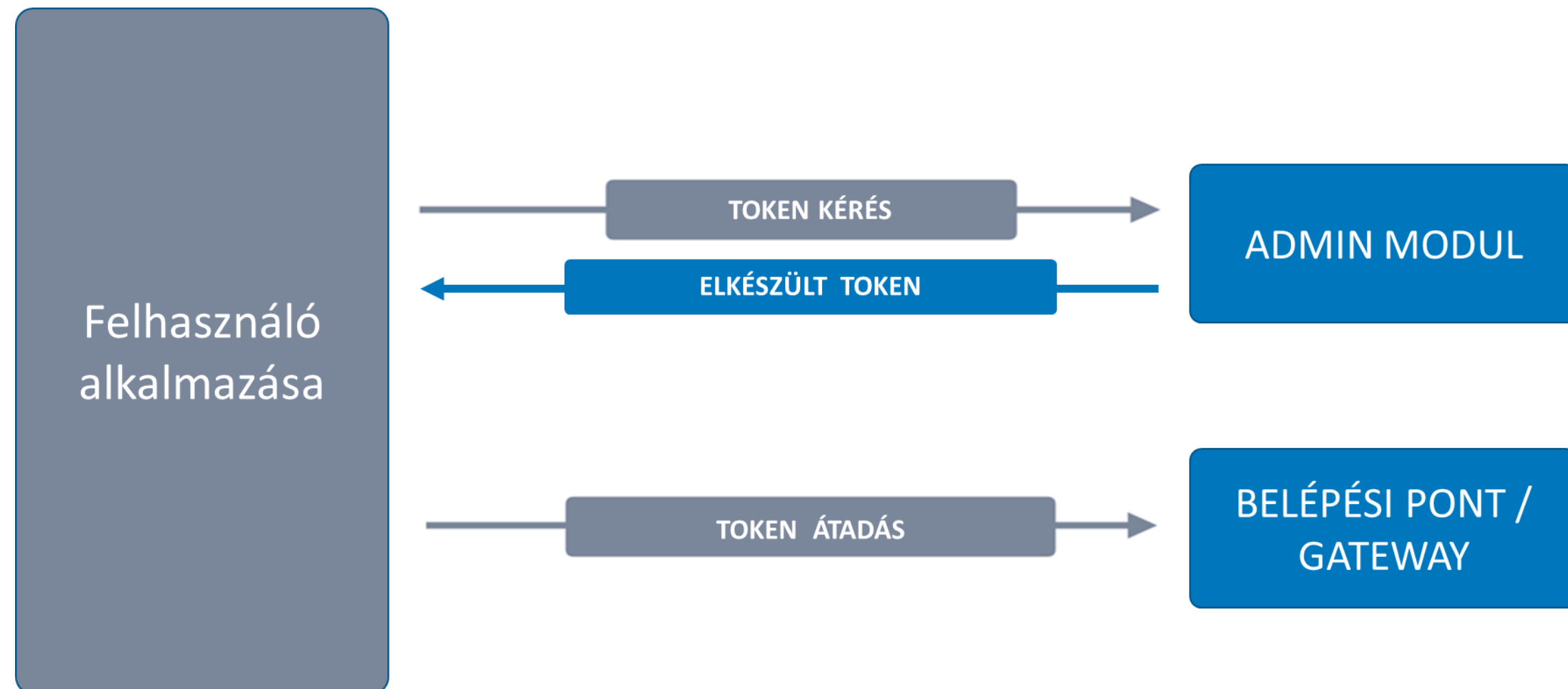
Maradvány biztonsági kockázatok:

- A TOKEN visszavonása
- A TOKEN védelme

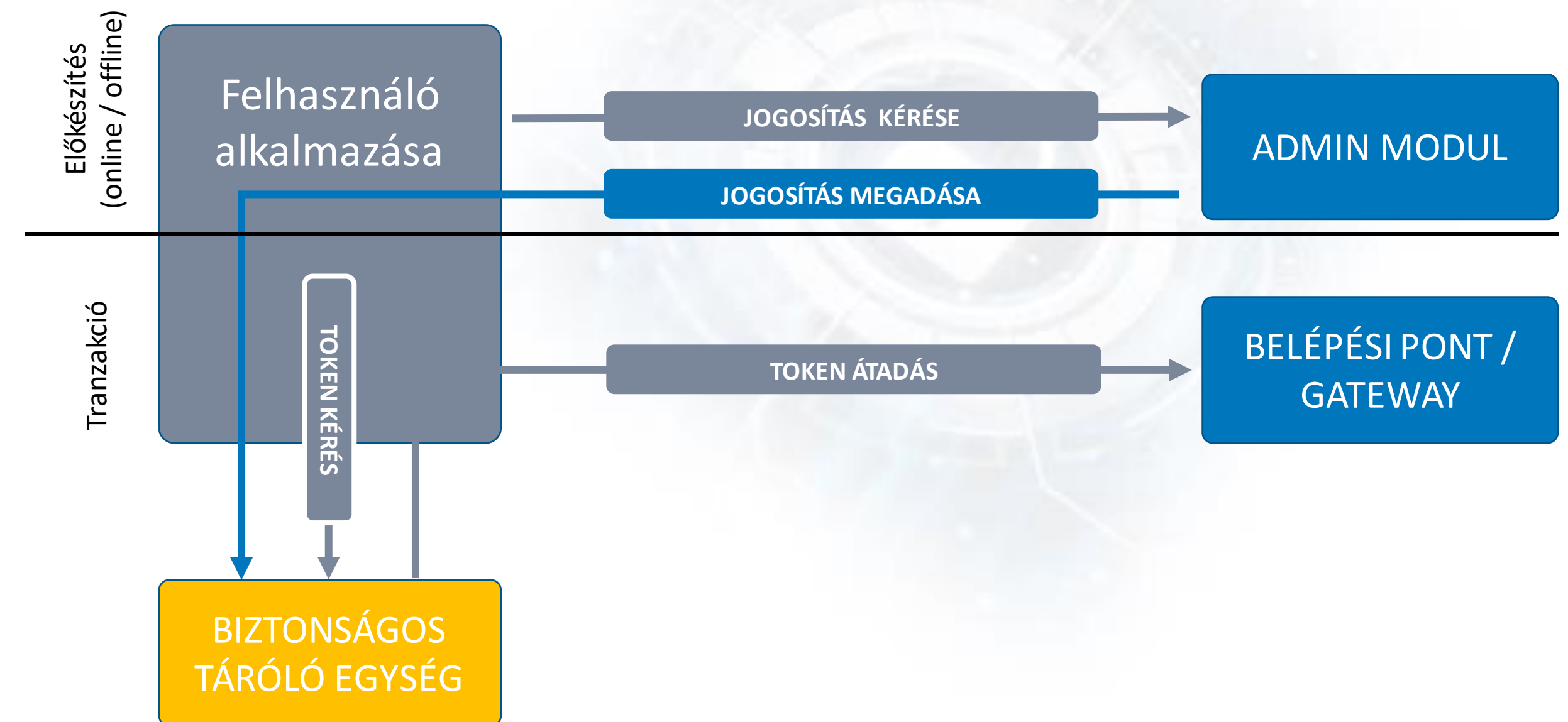
A megoldott biztonsági kihívások:

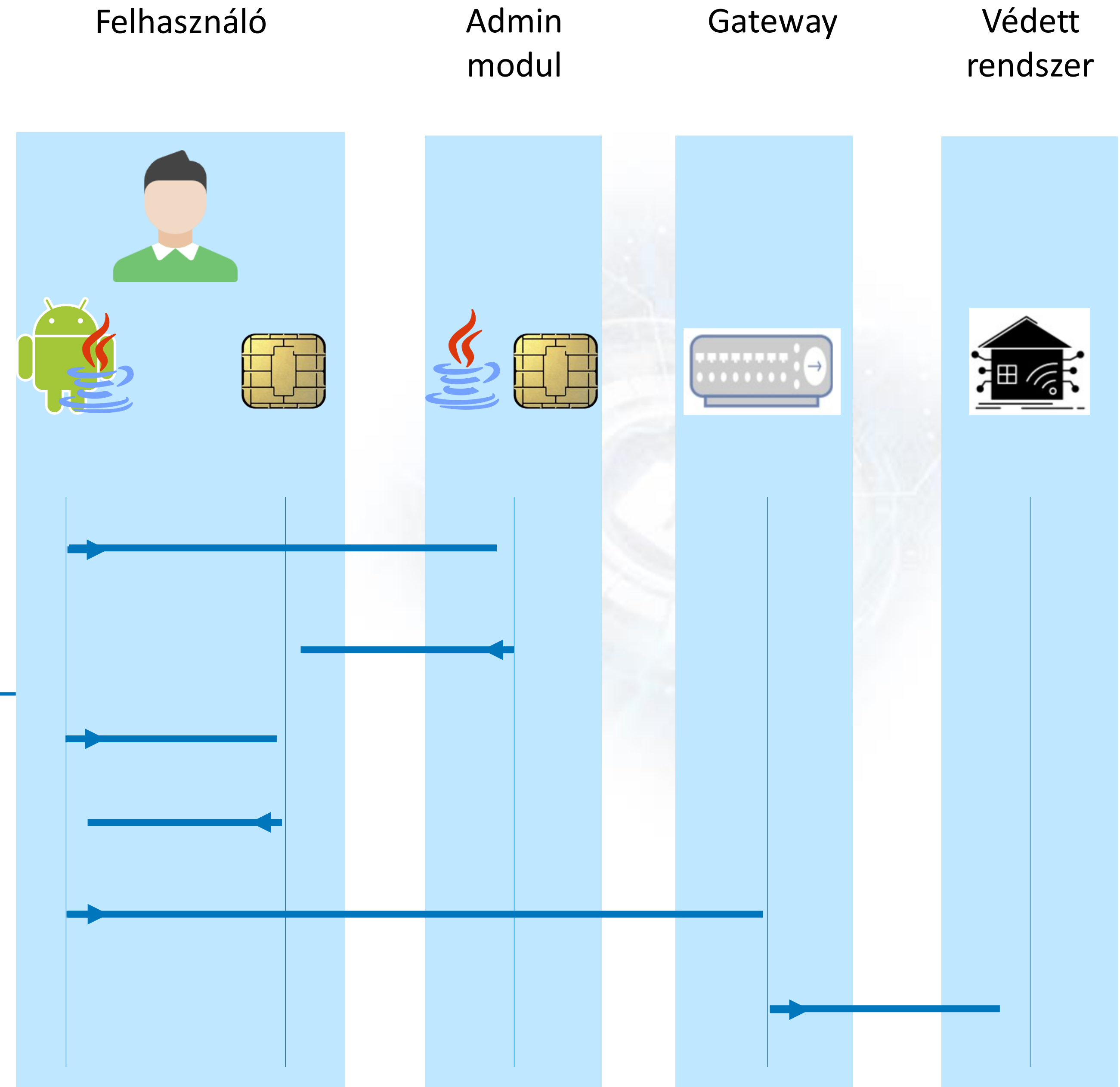
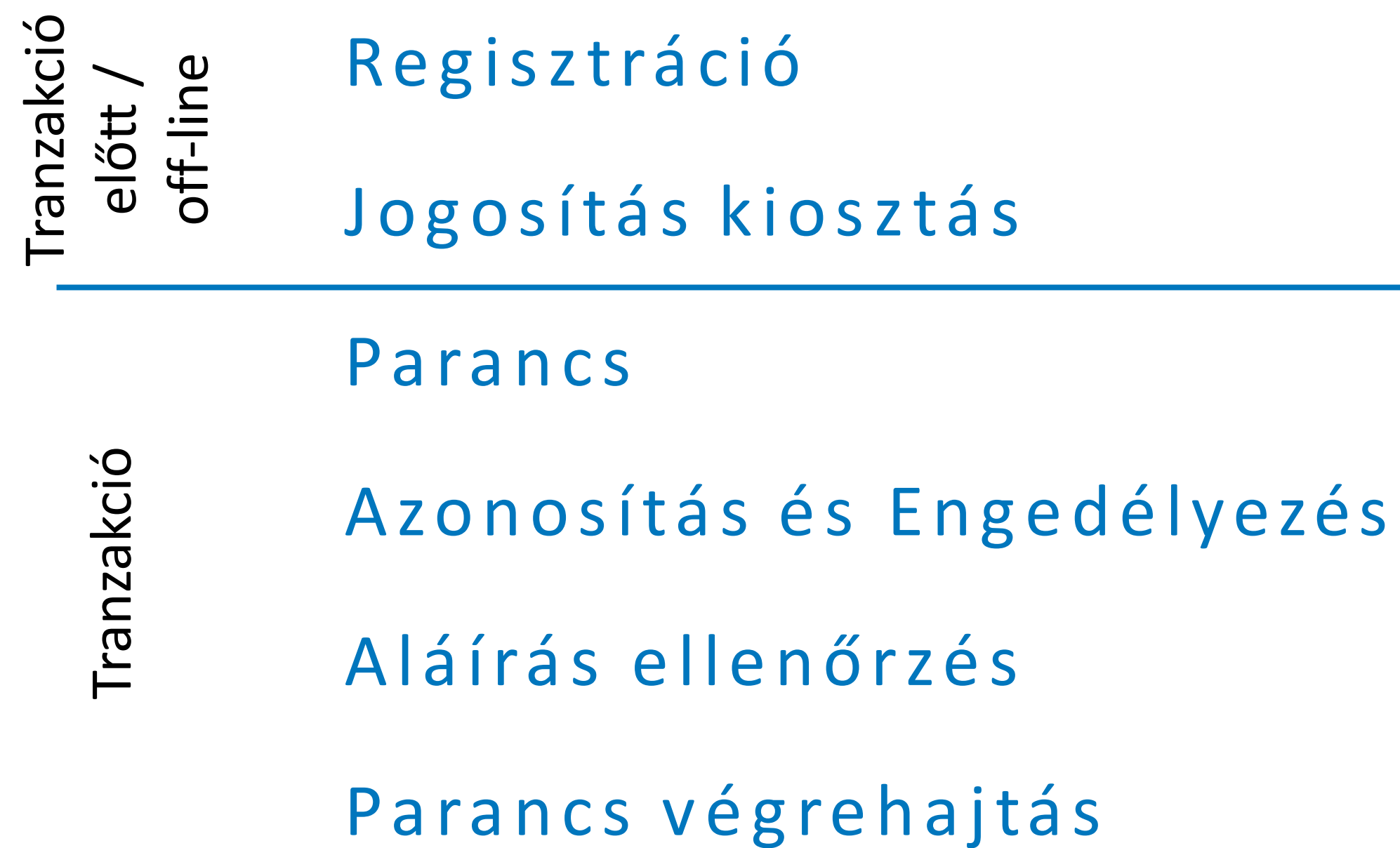
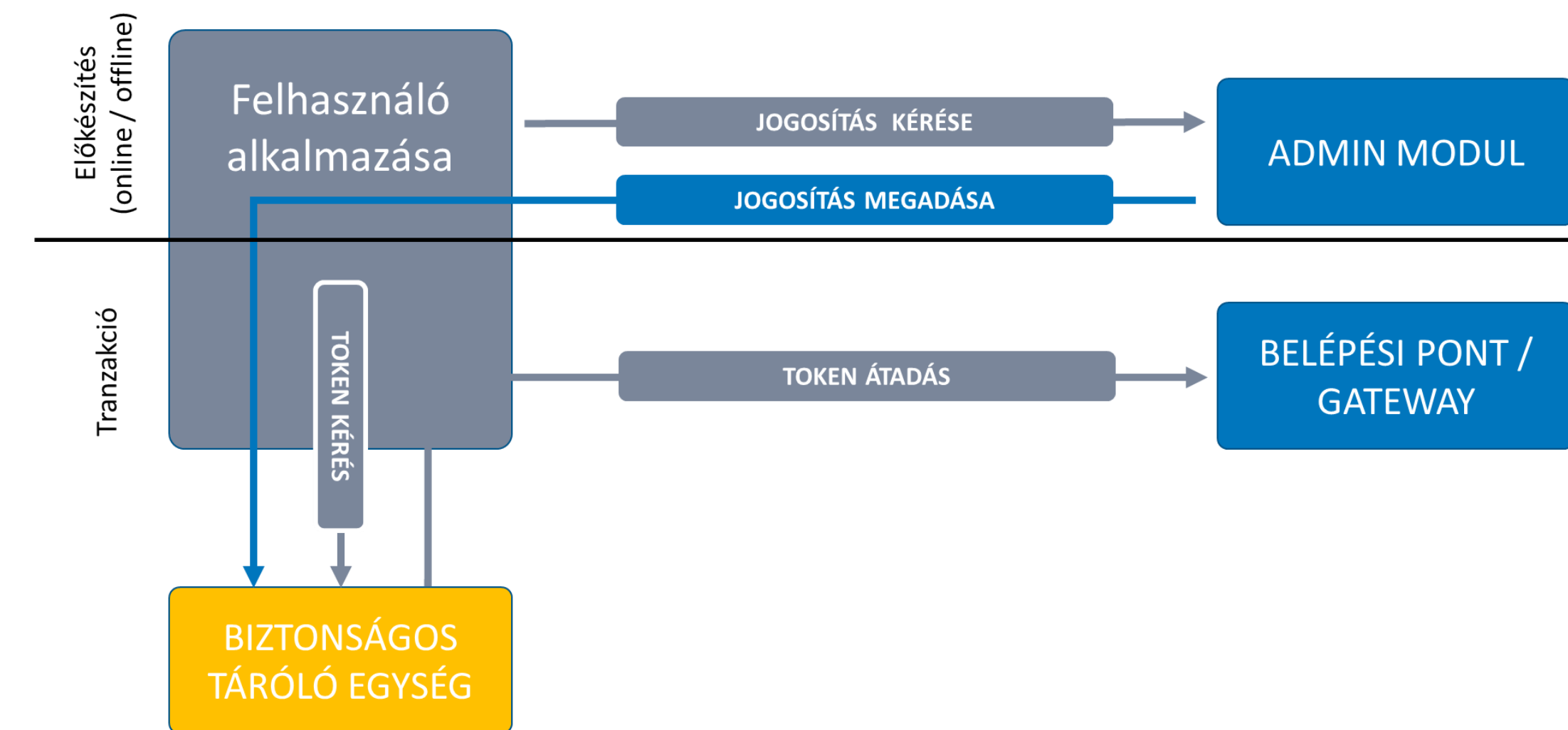
- Biztosítható a szükséges jogosítás elvének betartása
- Decentralizálható a jogosítás management
 - Támogatott a jogosítás átadása
- Erőforrás hiányos környezetben is megfelelő
- Azonosítás elválasztva a jogosítás-ellenőrzéstől, cross-domain alkalmazhatóság

CBAC



FEAC

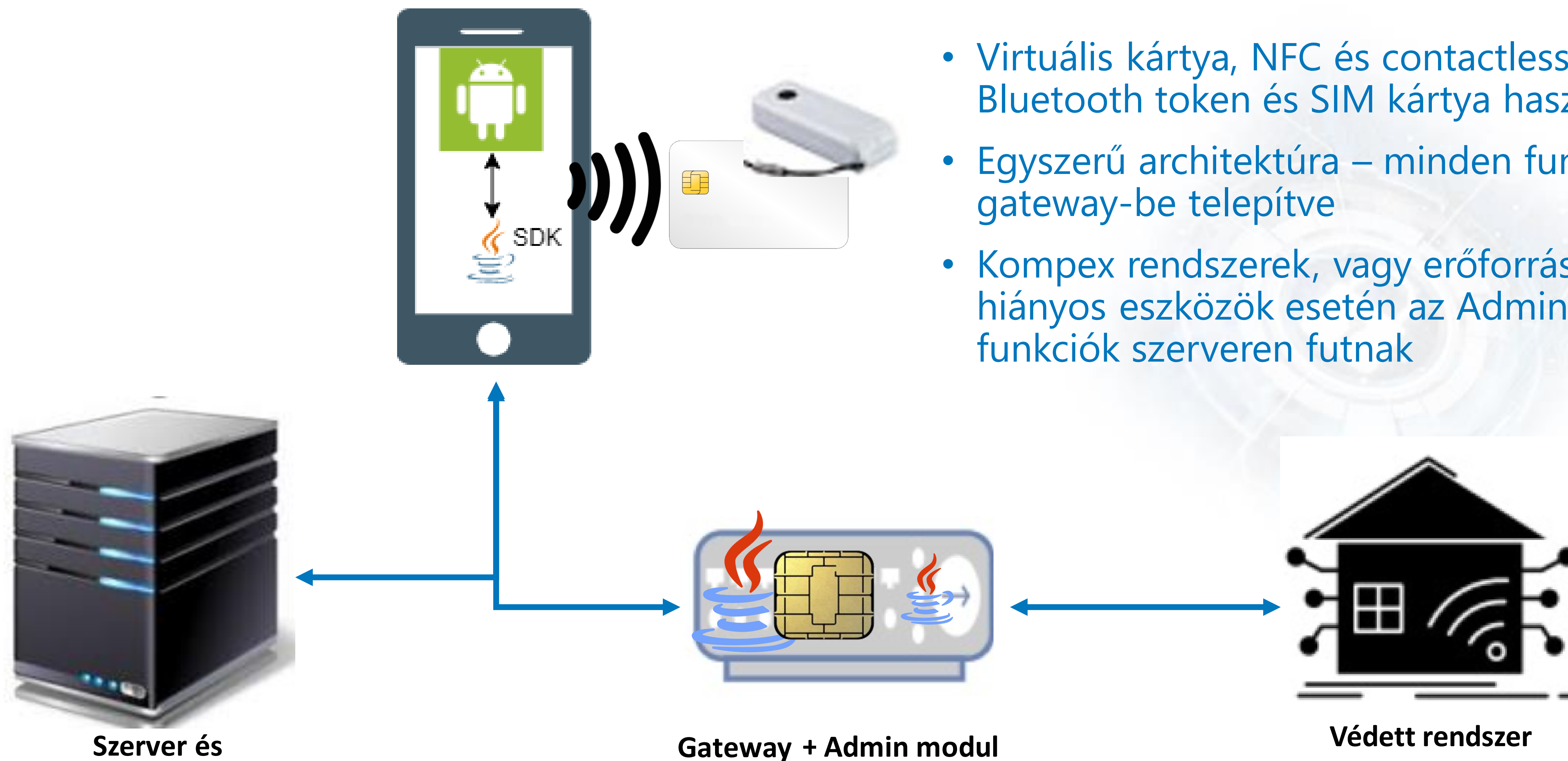




A FEAC BIZTONSÁGI ÉS EGYÉB JELLEMZŐI

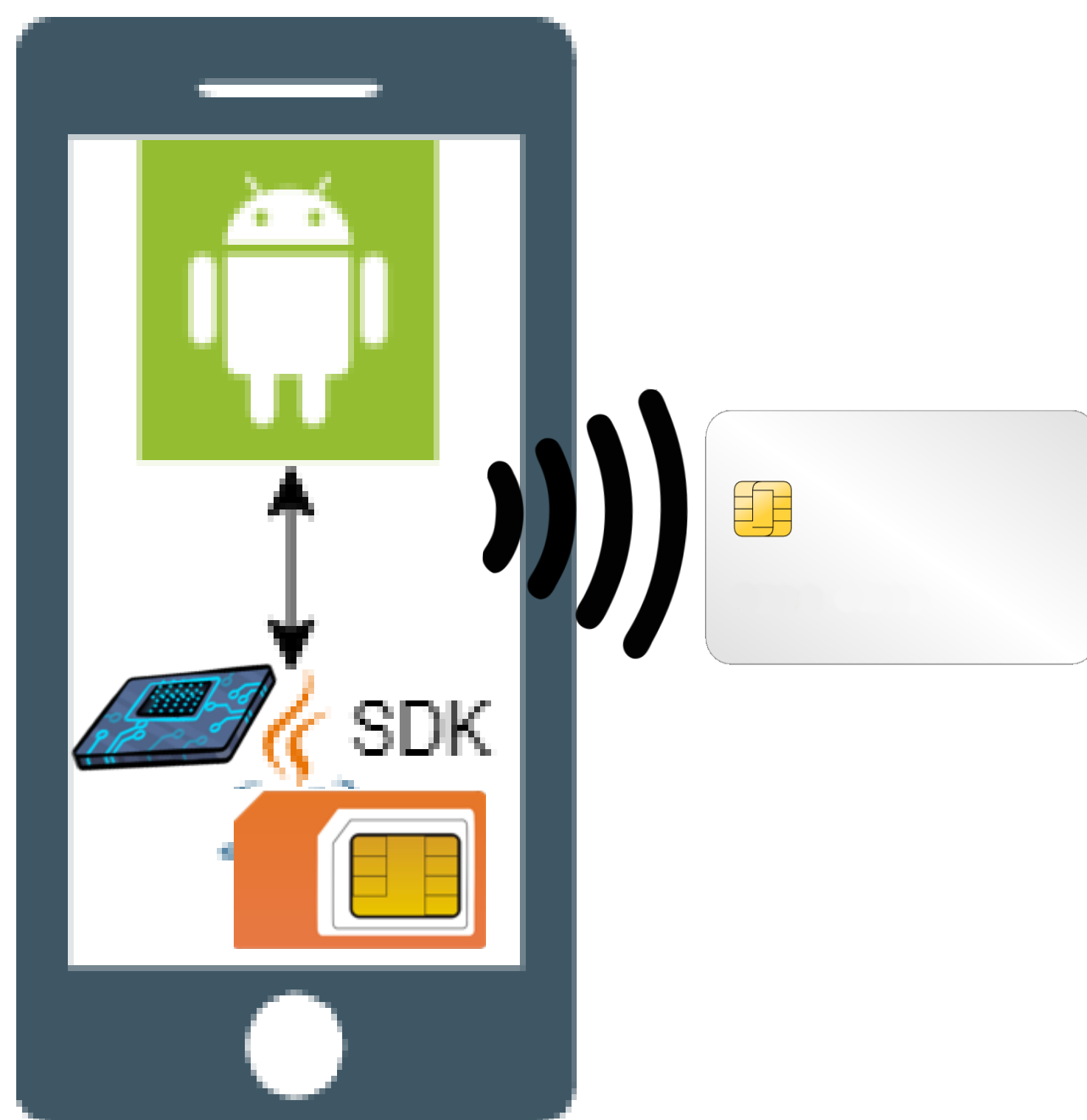
Maradvány kockázatok kivédve:

- TOKEN védelme
- A TOKEN visszavonása
- Smart kártya használata – legmagasabb szintű biztonság
- 2 faktoros azonosítás
- Nincs szerveren tárolt adat
- Felhasználói kontrol
- Auditálható jogosítás delegálás
- Felhasználó barátság
- Mobilitás
- Valós idejű jogosítás kiosztás/megvonás
- Átmeneti jogosítások
- Alacsony erőforrás igény
- Jó skálázhatóság



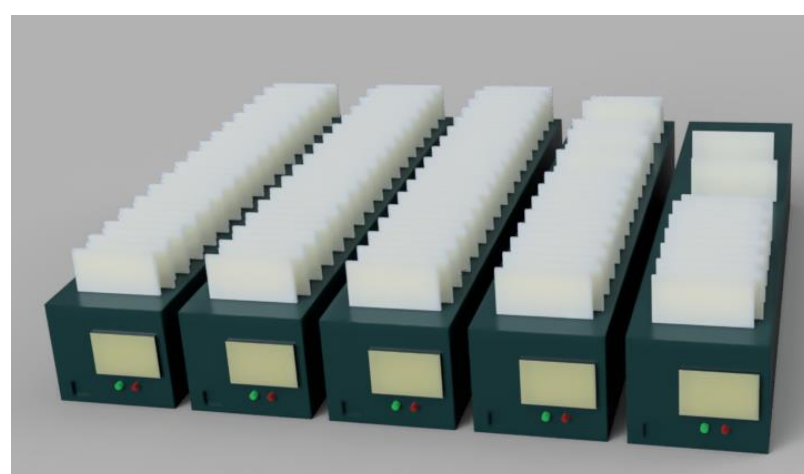
- Virtuális kártya, NFC és contactless kártya, Bluetooth token és SIM kártya használata
- Egyszerű architektúra – minden funkció a gateway-be telepítve
- Komplex rendszerek, vagy erőforrás hiányos eszközök esetén az Admin funkciók szerveren futnak

Front-End Jogosítás-Ellenőrzés SIM-mel vagy (eSE, TEE)



- Jogosultság ellenőrzés cardlet SIM kártyán külön SSD-ben
- A jogosítások OTA kibocsátása
- A jogosítás ellenőrzés végrehajtása a SIM kártyán
- A TOKEN elkészítése a SIM kártyán
- Biztonságos tranzakció a mobil alkalmazással

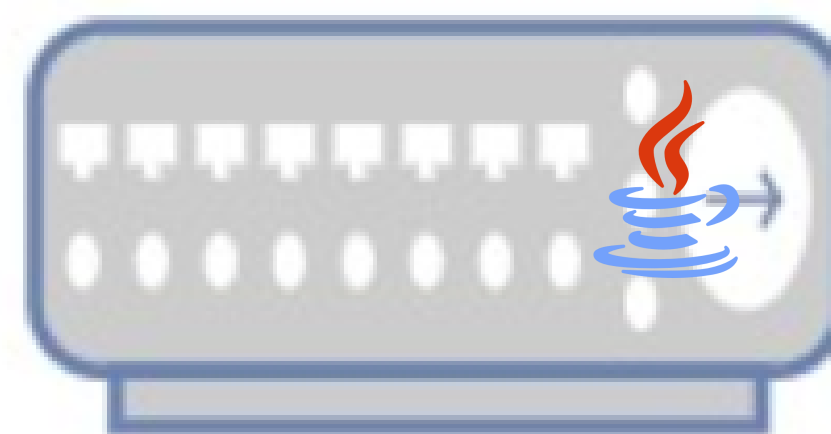
Front-End Jogosítás- Ellenőrzés Kártya Farmmal



Card Farm



Szerver és Admin modul



Gateway



Védett rendszer

- A Kártya Farm a felhőben van
- A Kártya Farmban nagyszámú kártya és a kártyákon több SSD van
- A felhasználók dedikált SSD-t kapnak, amit saját SE-ként használhatnak
- A kártyák 2F azonosítással érhetőek el
- Minden érzékeny adat a chipben van, semmi nincs a szerveren.

A FEAC egy nagyobb IoT architektúra részévé válik a H2020 IoTAC EU projektben.



CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS



M Ű E G Y E T E M 1 7 8 2



LIFE IS FOR SHARING.



Technische
Universität
Berlin



tecnalia Inspiring
Business



KÖSZÖNÖM A FIGYELMET!



INFORMÁCIÓ

<https://safepaysys.com>

KAPCSOLAT

vilmos@safepaysys.com