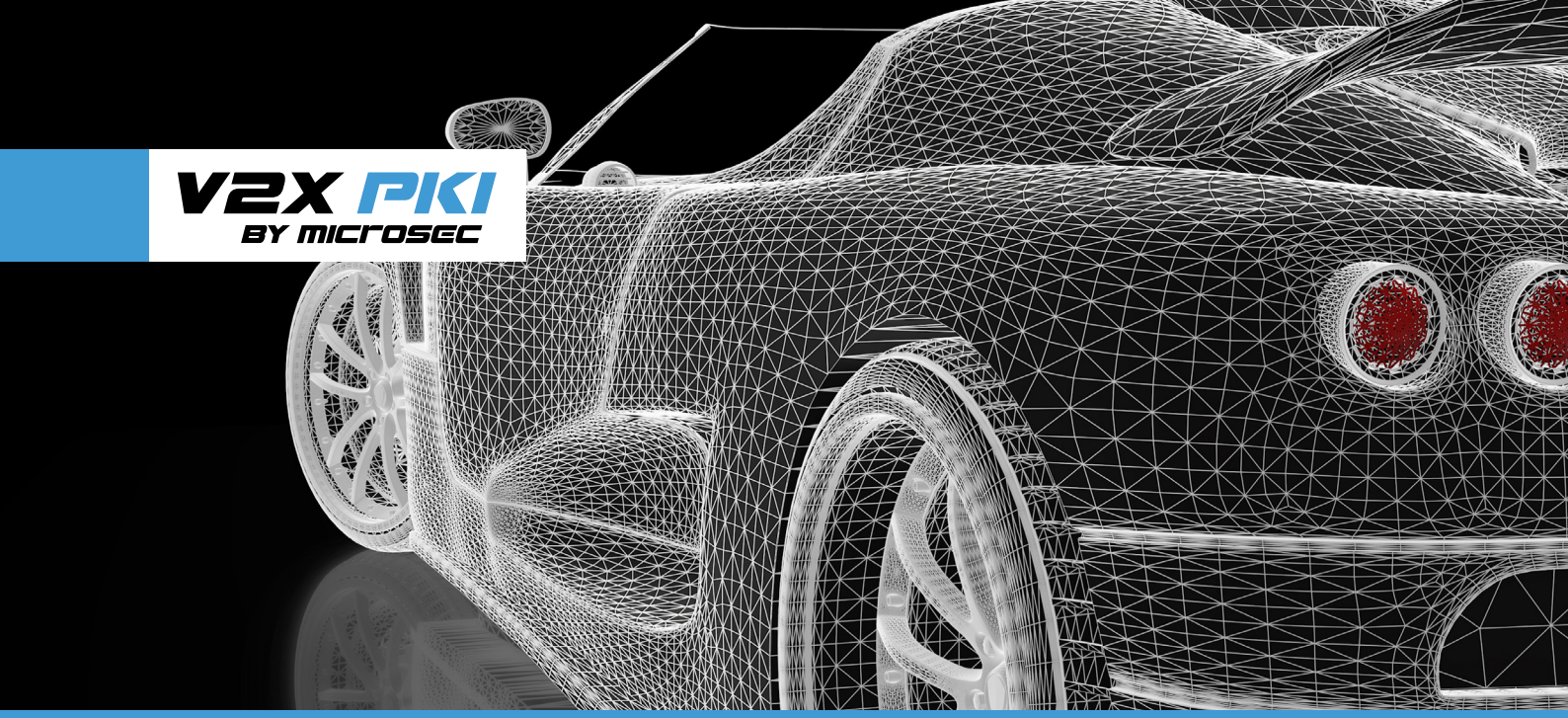
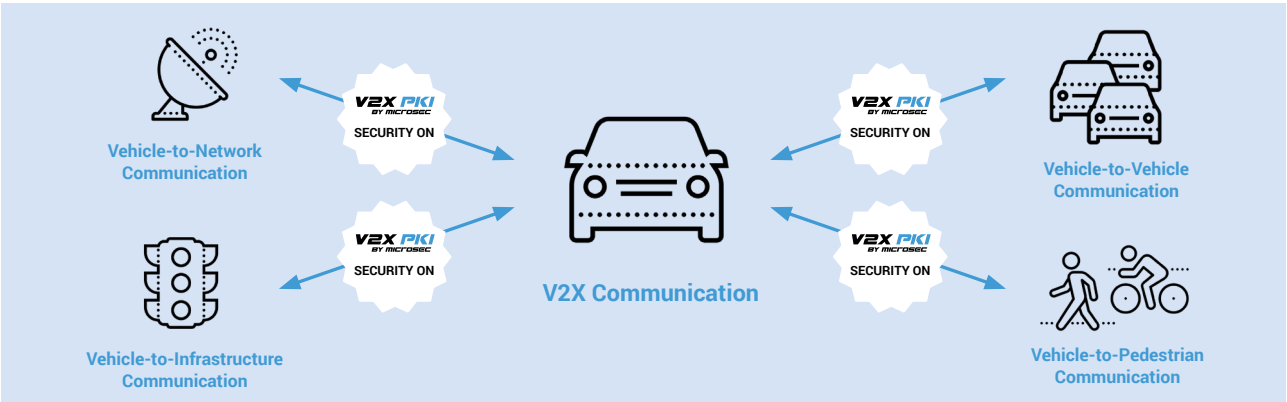


A V2X nyilvános kulcsú infrastruktúráról

Ha valaki IT-biztonsági vagy kapcsolódó szakterületen dolgozik, szinte biztosan hallotta már a PKI betűszót. Sokan tudhatják azt is, hogy ez a nyilvános kulcsú infrastruktúra kifejezést rövidíti, és sokan ismernek vonatkozó fogalmakat (tanúsítvány, hitelesítésszolgáltató stb.). Amivel már lényegesen kevesebben vannak tisztában, az a PKI számtalan felhasználási módja és területe. Az első asszociáció a kifejezéssel kapcsolatban általában az elektronikus aláírás és időbélyegzés megoldásokhoz kapcsolódik, ám a paletta ennél sokkal szélesebb: a nyilvános kulcsú infrastruktúra alkalmazható többek között a járművek közötti kommunikációban is.

A **Microsec V2X PKI** egy keretrendszer, amely garantálja a vehicle-to-everything (gépjármű és környezete közötti kommunikáció), azaz a V2X rendszerek biztonságát. Ezen környezetekben a nyilvános kulcsú infrastruktúra megoldások tanúsítványok révén a kommunikációban részt vevő felek engedélyeinek ellenőrzését szolgálják – a Microsec V2X PKI pedig a legkorszerűbb kriptográfiai megoldások alkalmazásával teszi ezt, többek között elliptikus görbén alapuló kriptográfiával (ECC), amely nagyobb biztonságot nyújt a széles körben alkalmazott RSA algoritmusénál.



A tanúsítványok használata a jogosulatlan felek adatcserébe való beavatkozásának elkerülése és a kommunikáció résztvevőinek biztonságos módon történő álnevesítése (pszeudonimizálása) érdekében szükséges. A V2X PKI mechanizmusának lényege röviden a következő: a hierarchia csúcsán egy Root CA található, amely tanúsítványokat bocsát ki két további szereplőnek, az Enrolment Authoritynek (EA) és az Authorization Authoritynek (AA). Az Enrolment Authority fő feladata a jármű vagy egyéb eszköz fedélzeti egységének (OBU) hitelesítése. A folyamat után egy ún. Enrolment Credentialt (EC) bocsát ki, amely hosszú távon azonosítja az eszközt. Az EC az Authorization Authority számára szükséges az ún. Authorization Ticketek kibocsátásához, amelyek rövidebb ideig érvényesek, és folyamatosan váltakoznak, így az álnevesítés célját szolgálják a vonatkozó szabványokban leírt módon.

Megfelelőség és tesztelés

A **Microsec V2X PKI** rendszer fejlesztése számos szabvány és specifikáció mentén történik, így az ezeknek való megfelelősége is biztosított. A keretrendszer több különböző szabványügyi szervezet követelményrendszerét is követi, többek között kompatibilis a következő, a V2X területén alapvető sztenderdekkel is:

- IEEE Std 1609.2 (IEEE Standard for Wireless Access in Vehicular Environments);
- ETSI TS 102 940 (ITS-S Security [PKI] Architecture and Application Groups);
- ETSI TS 102 941 (Trust and Privacy Management);
- ETSI TS 103 097 (Certificate and Message Structure Definitions for C2CPKI).

A Microsec ezenfelül részt vesz szakmai szervezetek (pl. az ETSI) munkájában, és folyamatosan követi a különböző szabványalkotási folyamatokat és draftokat, hogy amikor elkészül egy új követelményrendszer, az elsők között implementálhassa azt.

A Microsec V2X PKI gyakorlati tesztelésére létrehozása óta több alkalommal is sor került ETSI rendezvényeken is. A termék már a legelső ETSI Plugtests™ eseményeken – ahol a fent említett szabványok és specifikációk alapján a Microsec csapata a rendszert minden jelen lévő ITS gyártóval tesztelte – igen jól szerepelt, ezt jelzi a 2019–2020-as események 95%-os sikeraránya is. A végrehajtott tesztek között szerepelt a közúti veszélyek jelzése, útépítési munkálatokra való figyelmeztetés, illetve hosszirányú és kereszteződésben történő ütközési kockázat jelzése is.
A rendszer készen áll a használatra, V2X tanúsítványok által biztosítva a nyilvános kulcsú infrastrukturális keretrendszert ITS tesztpályák, gépjárműgyártók és -fejlesztők, illetve szállítási és okosváros infrastruktúrák kezelői számára egyaránt.
A Microsec V2X PKI képes tanúsítványokat kibocsátani többek között az útmenti egységek (RSU), fedélzeti egységek (OBU), tesztpályák és pilot projektek számára is. Lehetőség van továbbá akár egyedi PKI hierarchia vagy ehhez kapcsolódó tanácsadás igénylésére is.

Rövid útmutató V2X PKI tanúsítványok igényléséhez:

1. LÉPÉS Kérjük, látogassa meg regisztrációs oldalunkat a **https://v2x-pki.com** honlapon, és töltse ki a szükséges mezőket – beleértve a releváns tanúsítványtípusokat is. A V2X PKI rendszer üzemeltetői csapata ezután hamarosan felveszi Önnel a kapcsolatot az igénylés pontosítása végett.

2. LÉPÉS Az igénylés alapján a Microsec munkatársai a legmegfelelőbb működés érdekében az offline tanúsítványcsomag vagy a CA-ba történő regisztráció közül ajánlanak egy lehetőséget.

3. LÉPÉS Amennyiben praktikusabb, hogy a V2X PKI csapata generálja a tanúsítványokat, a nyilvános kulcs, a kulcs típusa (pl. NIST P-256), a kért PSID- és SSP párok (ha azok eltérnek a 36-01FFFC, 37-01FFFFFF és 141 értékektől) és opcionálisan a 250-től és 380-tól eltérő földrajzi régió megadása szükséges. Amennyiben az Igénylő a CA-ba kerül regisztrálásra, ugyanezen adatokat kell megadni, kiegészítve a kanonikus azonosítóval (Canonical ID).

4. LÉPÉS Ha ezek rendelkezésre állnak, és beüzemelésre kerültek, az infrastruktúra működésre készen áll, és az Igénylő el is kezdheti a tesztelést és a tanúsítványok használatát.

Kérjük, lépjen velünk kapcsolatba, és igényelje tanúsítványait a https://v2x-pki.com/ weboldalon!

A Microsecről

A Microsec zrt. 1984-es alapítása óta a hazai informatikai piac aktív szereplője. Minősített bizalmi szolgáltatóként (QTSP) az elektronikusan hiteles és bizonyító erejű okiratok, valamint az elektronikus aláírás technológiájára épülő üzleti megoldások terén nyújt kiemelkedő szolgáltatásokat. A V2X témakörhöz kapcsolódóan aktív tagja a European Telecommunications Standards Institute (ETSI), a CAR 2 CAR Communication Consortium (C2C-CC), valamint a 5G Automotive Association (5GAA) szervezetnek. A cég vonatkozó partnerkapcsolatai kiterjednek globálisan jegyzett V2X eszközgyártókra, autóipari beszállítókra és tesztközpontokra.