



NAV

NAV EBT rendszer ECC átállás

Czeglédi László

NAV Informatikai Intézete

2023.09.28.



Tervezett témák

- Jelenlegi működés
- Tervezett működés
- Tanúsítványok
- Új EBT kliens
- Mérföldkövek
- Egyéb
- Kérdések

Jelenlegi működés

„EBT” rendszer

- Pénzintézetek elektronikus megkeresési rendszere

Szakmai folyamatok

- VHR: Végrehajtás
- ELLTAM: Ellenőrzés támogatás

NAV EBT Kliens technológia

- Aláíró modul: EU DSS 2.0.1. verzió
- Támogatott futtató környezet: Java 1.6, 1.7
- Csak az RSA aláíró és titkosító kulcsok támogatottak

Tervezett működés

Szakmai folyamatok

- VHR: Végrehajtás
- ELLTAM: Ellenőrzés támogatás
- **CESOP: Pénzforgalmi szolgáltatók kötelező adatszolgáltatása a fizetési adatokról**

Tanúsítványok fejlődése

- ECC átállás

Új EBT kliens

- ECC tanúsítványok támogatása
- Technológiai megújítás

Tanúsítványok

Tanúsítvány típusok

- Általánosan használt: RSA (Rivest, Shamir and Adleman algorithm) 2048, 3072, 4096 bit
- Újabb: ECC (Elliptic-curve cryptography) 256 bit

ECC átállás

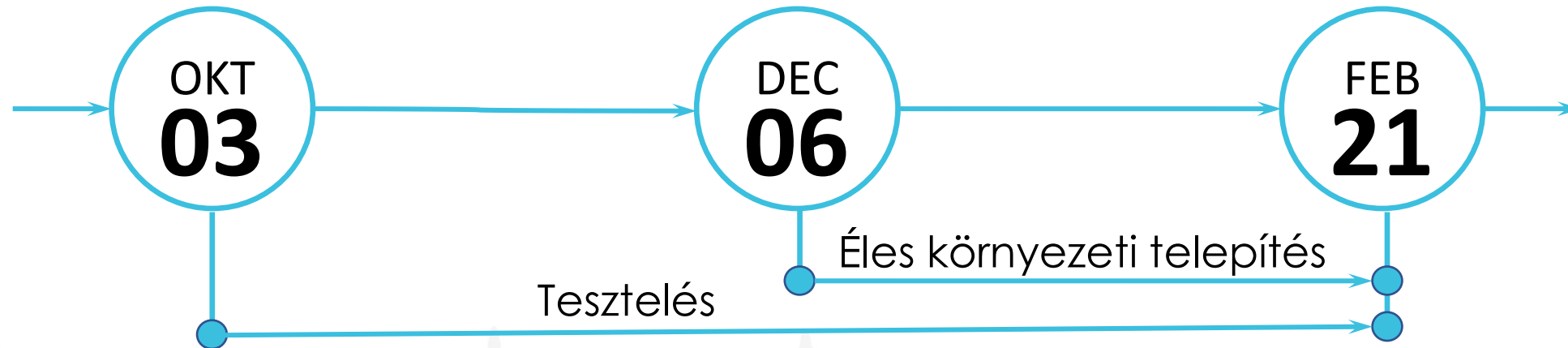
- ETSI TS 119 312 V1.4.2 (2022-02) ajánlás javasolja az RSA kulcsok kivezetését és ECC-vel helyettesítését.
- A NISZ több ütemben vezeti ki a NAV részéről is használt RSA aláíró kulcsokat, az egyik mérföldkő 2023.09.21 volt, a következő 2024.03.20, utána csak **ECC alapú aláíró tanúsítványok** használhatók.
- NISZ **RSA 3072-bit alapú, titkosító tanúsítványok** még használhatók, de célszerű ECC-re váltani.
- Piaci hitelesítésszolgáltatók: saját átállási menetrend

Új EBT Kliens

NAV EBT Kliens technológia

- Aláíró modul: EU DSS **5.12**
- Támogatott futtató környezet: Java 8+ (JDK **8, 11, 15, 17**)
- Spring keretrendszer: **5.3.x**
- RSA és **ECC** aláíró és titkosító kulcsok támogatottak
- **Maven** alapú szoftver projekt menedzsment
- NAV külső **nexus** repository-ba publikált artifact-ok

Mérföldkövek



- ECC képes EBT szerver telepítése **teszt** környezetben
- Új EBT Kliens publikálása
- Tesztelés kezdete: az új EBT klienssel és a független beszállítókkal

- ECC képes EBT szerver telepítése **éles** környezetben
- A pénzügyintézetek ECC aláíró és titkosító kulcsot is használhatnak **éles** környezetben
- Az új EBT kliensek is használhatók az **éles** környezetben

- NAV ECC aláíró és titkosító kulcsok telepítése **éles** környezetben
- ETSI EN 319 132 kompatibilitás aktiválása
- Már csak az új EBT kliens használható

Mérföldkövek I.

2023.10.03.

- ECC képes EBT szerver telepítése **teszt** környezetben
- Az EBT szerver a teszt környezetben már az ETSI EN 319 132-1 – V1.1.1 ajánlásnak megfelelő XAdES aláírás üzenetet küld: például SigningCertificateV2, SignatureProductionPlaceV2, and SignerRoleV2 elemek a korábbi SigningCertificate, SignatureProductionPlace és SignerRole elemek helyett
- EBT Kliens publikálása
- Tesztelés kezdete:
az új EBT klienssel és a független beszállítókkal

Mérföldkövek II.

2023.12.06.

- ECC képes EBT szerver telepítése **éles** környezetben.
- Az EBT szerver az éles környezetben még az ETSI EN 319 132-1 – V1.1.1 ajánlást megelőző formátumú XAdES aláírás üzenetet küld (például SigningCertificate, SignatureProductionPlace és SignerRole elemek), így a régi klienssel kompatibilis marad.
- A pénzüintézetek ettől a dátumtól kezdve ECC aláíró és titkosító kulcsot is használhatnak **éles** környezetben.
- Az új EBT kliensek is használhatók az **éles** környezetben, az ETSI EN 319 132-1 – V1.1.1 ajánlásnak megfelelő formátumban is küldhetnek.

Mérföldkövek III.

2024.02.21.

- NAV ECC aláíró és titkosító kulcsok telepítése **éles** környezetben
- Az EBT szerver az **éles** környezetben az ETSI EN 319 132-1 – V1.1.1 ajánlásnak megfelelő XAdES aláírás üzenetet küld: például SigningCertificateV2, SignatureProductionPlaceV2, and SignerRoleV2 elemek a korábbi SigningCertificate, SignatureProductionPlace és SignerRole elemek helyett
- Ettől a dátumtól kezdve a NAV ECC tanúsítványok és az ETSI EN 319 132-1 – V1.1.1 ajánlásnak megfelelés miatt a régi EBT kliensek nem lesznek használhatók, már **csak az új EBT kliens használható.**

Egyéb

NAV Teszt tanúsítványkiadó

- 2023 tavaszán lejárt a NAV EBANKTITOK (RSA) nevű tanúsítványkiadó érvényessége.
- Bekonfigurálásra került a NAV EBANKTITOK2 (továbbra is RSA, 4096 bit) tanúsítványkiadó, ez használható tesztelésre.
- ECC-s teszt tanúsítványok a piaci tanúsítványkiadóktól igényelhetők.

ECC titkosítás

- Az ECC kulcsok felhasználásával történő titkosítás némileg eltér az RSA kulcsokkal történő titkosítástól. Az erre vonatkozó leírást a frissítésre kerülő EBT_KKK2_Kripto_Interfész_specifikáció fogja tartalmazni.

Független beszállítók tesztelése

- Az EBT klienst használó pénzintézetek mellett várjuk és hívjuk a független beszállítókat, fejlesztőket, integrátorokat is a tesztelésre!

Kérdések



A fejlesztés, tesztelés, üzemeltetés során felmerülő technikai kérdéseket, észrevételeket továbbra is az alábbi címen várjuk:

ebt_teszt@nav.gov.hu

Köszönjük a figyelmet!



Nemzeti Adó-
és Vámhivatal

nav.gov.hu