Tisztelt Érdeklődő!

Az alábbiakban a HUNGUARD Kft. tanúsítási tevékenységével kapcsolatos jogszabályokat, mértékadó, szakmai előírásokat és elvárásokat találja.

Információbiztonsággal kapcsolatos EU-s joganyagok

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2019/881 RENDELETE (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2554 RENDELETE (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (DORA)
- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/ 1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

Információbiztonsággal kapcsolatos hazai jogszabályok

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről
- 26/2020. (VIII. 25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól

Az elektronikus aláírási termék tanúsítására vonatkozó legfontosabb jogszabályok

- Az Európai Parlament és a Tanács 910/2014/EU rendelete (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (eIDAS)
- A BIZOTTSÁG (EU) 2016/650 VÉGREHAJTÁSI HATÁROZATA (2016. április 25.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 30. cikkének (3) bekezdése és 39. cikkének (2) bekezdése alapján a minősített aláírást és bélyegzőt létrehozó eszközök biztonsági értékelésére vonatkozó szabványok megállapításáról

- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 137/2016. (VI. 13.) Korm. rendelet az elektronikus ügyintézési szolgáltatások nyújtására felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről.
- 541/2020. (XII. 2.) Korm. rendelet a bizalmi szolgáltatások esetében a személyes jelenléttel egyenértékű biztosítékot nyújtó, nemzeti szinten elismert egyéb azonosítási módszerekről1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól
- 227/2023. (VI. 8.) Korm. rendelet a minősített elektronikus aláírást és minősített elektronikus bélyegzőt létrehozó eszközök megfelelőségértékelési tevékenységére irányuló kijelöléséről, valamint a kijelölt szervezetek tevékenységének különös szabályairól

Információbiztonsággal kapcsolatos irányadó követelmények

- NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53 Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-53A Revision 4: Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- NIST SP 800-53A Revision 5: Assessing Security and Privacy Controls in Federal Information Systems and Organizations
- NIST SP 800-53B Control Baselines for Information Systems and Organizations
- ETSI TS 101 533-1 V1.3.1 (2012-04) Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

Információbiztonsággal kapcsolatos MNB ajánlások

- A Magyar Nemzeti Bank 4/2021. (III.30.) számú ajánlása a hitelintézetek digitális transzformációjáról
- A Magyar Nemzeti Bank 12/2020. (XI.6.) számú ajánlása a távmunka és távoli hozzáférés informatikai biztonsági követelményeiről
- A Magyar Nemzeti Bank 11/2020. (X.20.) számú ajánlása a pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeiről
- A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről
- A Magyar Nemzeti Bank 7/2020. (VI.3.) számú ajánlása a külső szolgáltatók igénybevételéről
- A Magyar Nemzeti Bank 4/2019. (IV.1.) számú ajánlása a közösségi és publikus felhőszolgáltatások igénybevételéről

Az elektronikus aláírási termékekkel szemben támasztott irányadó követelmények forrásai

Az alább részletezett általános követelmények konzisztens részrendszerét kell az egyes aláírási termékek tanúsítása során irányadónak tekinteni. A konzisztens részrendszert meghatározzák az aláírási termék specifikumai (pl. SmartCard, PC-ben szoftver, kriptográfiai hardver modul stb.), valamint a funkcióval és az alkalmazással szemben meghatározott kockázatelemzés.

- ETSI TS 119 101 V1.1.1 (2016-03) Policy and security requirements for applications for signature creation and signature validation
- EN 419241-1:2018 Trustworthy Systems supporting Server Signing - Part 1: General System Security Requirements
- EN 419241-2, Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing
- CEN/TS 419261:2015 Security requirements for trustworthy systems managing certificates and time-stamps
- EN 419221-5, PP Cryptographic Module for Trust Services (note: TS 419 221-6 – provides conditions for use of EN 419 221-5 as a qualified electronic signature or seal creation Device)

Bizalmi szolgáltatók eIDAS megfelelését megalapozó követelmények

- ETSI EN 319 401 V2.3.1 (2021-05) General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.3.1 (2021-05) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.4.1 (2021-11) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 V1.2.1 (2013-05) Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI TS 119 431-1 V1.2.1 (2021-05) Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 511 V1.1.1 (2019-06) Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques
- ETSI TS 119 461 V1.1.1 (2021-07) Policy and security requirements for trust service components providing identity proofing of trust service subjects

Kriptográfiai modulra vonatkozó speciális irányadó követelményrendszer

- EN ISO/IEC 19790:2020 Information technology -- Security techniques – Security requirement for cryptographic modules
- A NIST FIPS (Federal Information Processing Standard) kiadványai közül a FIPS-140 kiadvány határozza meg azt a szabványt, amelyet állami szerveknek kell az Egyesült Államokban felhasználniuk, ha kriptográfia alapú biztonsági rendszereket akarnak használni érzékeny, vagy értékes adatok védelmére, a FIPS PUB 140-2 európai szabványosítása az ISO/IEC 19790; az újabb verzió a FIPS PUB 140-3 Security Requirements for Cryptographic Modules.

- ISO/IEC 24759:2017 Information technology — Security techniques — Test requirements for cryptographic modules

- A kriptográfiai modulokban megvalósított kriptográfiai algoritmusokkal kapcsolatban alapvető követelmény, hogy szabványos és biztonságosnak minősített algoritmusoknak kell lenniük, ezeket meghatározó dokumentumok pl.:
  - NIST SP 800-131A Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019
  - ETSI TS 119 312 V1.4.2 (2022-02) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
  - SOG-IS Crypto Working Group SOG-IS Crypto Evaluation Scheme Version 1.2
  - FIPS PUB 186-4, 2013 Digital Signature Standard (DSS)
  - NIST SP 800-56A Rev. 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
  - NIST SP 800-56B Rev. 2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography
  - NIST SP 800-56C Rev. 2 Recommendation for Key-Derivation Methods in Key-Establishment Schemes

A Nemzeti Média- és Hírközlési Hatóság iránymutatásai (elérhetők az NMHH honlapján)

- EF/26838-8,9,10,11,12,13/2011 számú határozat a felhasználható biztonságos kriptográfiai algoritmusokról, valamint a hozzájuk tartozó paraméterekről a mellékletekben foglaltaknak megfelelően.
- Ajánlás elektronikus archiválási szolgáltatások nyújtásához felhasznált megbízható rendszerekre vonatkozó biztonsági követelményekre, NHH, 2007.07.07.
- Ajánlás Eljárásrendi követelményekre elektronikus aláírás felhasználásával végzett elektronikus archiválási szolgáltatások szolgáltatói számára, NHH, 2007.07.07.
- Elektronikus archiválási szolgáltatásokkal kapcsolatos hatósági tájékoztató, NHH, 2007.07.07.

Kapcsolódó, a tanúsítást támogató egyéb nemzetközi dokumentumok

- EN ISO/IEC 15408-1:2020 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- EN ISO/IEC 15408-2:2020 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- EN ISO/IEC 15408-3:2020 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- ISO/IEC TR 19791:2010 Information technology — Security techniques — Security assessment of operational systems
- EN ISO/IEC 18045:2020 Information technology -- Security techniques -- Methodology for IT security evaluation
- EN ISO/IEC 27002:2017 Information technology — Security techniques — Code of practice for information security controls
- MSZ ISO/IEC 27001:2022 Információbiztonság-irányítási rendszerek. Követelmények
- ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management
- ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Nagyon sok jogszabályban[1] – külön definíció nélkül – szerepel az informatikai rendszer zártságának követelménye, ezért kiemeljük a zárt elektronikus információs rendszerrel szembeni elvárásokat:

Egy elektronikus információs rendszer akkor tekinthető zártnak[2], ha…

1. Az informatikai rendszer zárt, teljes körű, folytonos és kockázatokkal arányos védelmet biztosít a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából /lásd 2013. L. törvény – a továbbiakban IBTV - 1. § 15/, az alábbi értelmezések mellett:

[1] a villamos energiáról szóló 2007. évi LXXXVI. törvény 43. § (4)
a földgázellátásról szóló 2008. évi XL. törvény 100. § (1b)
az elektronikus hírközlésről szóló 2003. évi C. törvény 142. § (3)
víziközmű-szolgáltatásról szóló 2011. évi CCIX. törvény 63. § (5)
a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 67/A. § (1)
az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 12/A. § (1)
a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 94. § (4)
a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény 12. § (12)
31/2016. (IX. 2.) NGM rendelet 1 melléklet 7/a
[2] Az elvárás jogszabályi megjelenése a 42/2015. (III. 12.) Korm. rendelet 5/A § (2)-ban található

- zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem / IBTV (1. § 48) /,
- teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem / IBTV (1. § 44) /,
- folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem / IBTV (1. § 21) /,
- kockázatokkal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével / IBTV (1.§ 31) /

  Az elvárásoknak megfelelő részletes követelményrendszer megtalálható az IBTV-hez kapcsolódó 41/2015. (VII. 15.) BM rendelet 3.-4. mellékletében.

2. A védelem fenti általános elvárásai mellett az informatikai rendszer működtetésének teljes életciklusában folyamatosan teljesülnek az alábbiak:
   - a jogosult általános (emberek és program entitások) és privilegizált (speciális jogokkal felruházott) felhasználók (pl. rendszergazdák) kizárólag a szigorúan szabályozott szerepkörüknek megfelelően férhetnek a védendő információkhoz és az azokat kezelő rendszer elemeihez, kezdeményezhetnek aktivitásokat, valamint kizárólag meghatározott privilegizált felhasználók adhatnak szabályozott szerepkörüknek megfelelően és ellenőrzött módon hozzáférési jogosultságokat;
   - a rendszer megfelelő műszaki és eljárásrendi megoldásokkal nyomon követi a védendő információk minden változtatását, melyek biztosítják, hogy még a jogosult általános és privilegizált felhasználók sem tudják törölni vagy módosítani a napló vagy egyéb nyomon követést biztosító információkat;
   - az informatikai rendszer összes külső interfésze szabályozott és kontrollált;
   - a szabályozások és eljárások garantálják a rendszer biztonsági szintjének folyamatos fenntartását (pl. szoftverfrissítések, üzemeltetés).