Tisztelt Érdeklődő!

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

Információbiztonsággal kapcsolatos hazai jogszabályok

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 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
- 45/2018. (XII. 17.) 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)
- 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.
- 1/2018. (VI. 29.) ITM rendelet a digitális archiválás szabályairól
- 451/2016. (XII. 19.) Korm. rendelet az elektronikus ügyintézés részletszabályairól

Információbiztonsággal kapcsolatos irányadó követelmények

- A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár alábbi részhalmaza /mely alapvetően a KIB 25-ös – MIBÉTS – ajánlás továbbfejlesztése/:
    - Termékekre vonatkozó értékelési módszertan
    - Összetett termékekre vonatkozó értékelési módszertan
    - Rendszerekre vonatkozó értékelési módszertan
- NIST SP 800-53 Revision 4: 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
- ETSI TS 101 533-1 V1.3.1 (2012-04) Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

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
- CEN/TS 419241:2014 Security Requirements for Trustworthy Systems supporting Server Signing
- CEN/TS 419261:2015 Security requirements for trustworthy systems managing certificates and time-stamps

Bizalmi szolgáltatók eIDAS megfelelését megalapozó követelmények

- ETSI EN 319 401 V2.2.1 (2018-04) General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 V1.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 V2.2.2 (2018-04) 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 V1.1.1 (2016-03) Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

Kriptográfiai modulra vonatkozó speciális irányadó követelményrendszer

- ISO/IEC 19790 Information technology -- Security techniques -- Methodology for IT security evaluation (mely megfelel az amerikai FIPS PUB 140-2 szabványnak)
- A NIST FIPS (Federal Information Processing Standard) kiadványai közül a FIPS-140-2 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, ennek európai szabványosítása az ISO/IEC 19790.
    a. FIPS 140-3 Security 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.:

- ENISA (The European Union Agency for Network and Information Security) **Algorithms, Key Size and Protocols Report** c. 2016
- FIPS PUB 186-4, 2013 Digital Signature Standard (DSS)
- NIST SP 800-56B Revision 2 Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
- **NIST SP 800-131A Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019**
- ETSI TS 119 312 V1.3.1 (2019-02) Electronic Signatures and Infrastructures (ESI); **Cryptographic Suites**

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 hazai ajánlások

A Közigazgatási Informatikai Bizottság 25. számú ajánlása: a Magyar Informatikai Biztonsági Ajánlások (MIBA) ajánlássorozata, amely három fő területre fókuszálva 12, önállóan is használható dokumentumban került megjelentetésre. A MIBA az ITB 8., 12., és 16. számú ajánlásait váltja fel, azok kibővítése és jelentős kiegészítése révén.

- A KIB 25. számú ajánlása: Magyar Informatikai Biztonsági Ajánlások (MIBA) 1.0 verzió:
  - A KIB 25. számú ajánlása: 25/2. kötet: Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS) 1.0 verzió
  - A KIB 25. számú ajánlása: 25/2-1. segédlet: MIBÉTS - Modell és Folyamatok 1.0 verzió
  - A KIB 25. számú ajánlása: 25/2-2. segédlet: MIBÉTS – Útmutató a Megbízók számára 1.0 verzió
  - A KIB 25. számú ajánlása: 25/2-3. segédlet: MIBÉTS – Útmutató a Fejlesztők számára 1.0 verzió
  - A KIB 25. számú ajánlása: 25/2-4. segédlet: MIBÉTS – Útmutató Értékelőknek 1.0 verzió
  - A KIB 25. számú ajánlása: 25/2-5. segédlet: MIBÉTS – Értékelési módszertan 1.0 verzió
- A Közigazgatási Informatikai Bizottság 28. számú ajánlása: Az E-Közigazgatási Keretrendszer projekt eredményeként létrehozott Követelménytár alábbi részhalmaza /mely alapvetően a KIB 25-ös – MIBÉTS – ajánlás továbbfejlesztése:
  - Termékekre vonatkozó értékelési módszertan

- Összetett termékekre vonatkozó értékelési módszertan
- Rendszerekre vonatkozó értékelési módszertan

A fenti KIB 25 és KIB 28 ajánlások jelentős részét a HUNGUARD Kft. dolgozta ki!

Kapcsolódó, a tanúsítást támogató egyéb nemzetközi dokumentumok

- MSZ ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- MSZ ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- MSZ ISO/IEC 15408-3:2008 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
- ISO/IEC 18045:2008 Information technology -- Security techniques -- Methodology for IT security evaluation
- ISO/IEC 27002:2013/Cor 2:2015, Information technology — Security techniques — Code of practice for information security controls
- MSZ ISO/IEC 27001:2014 Információbiztonság-irányítási rendszerek. Követelmények
- ISO/IEC 27004:2016 Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005 Information technology — Security techniques — Information security risk management
- ISO/IEC 27017 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:

[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

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:

    - 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).

[2] Az elvárás jogszabályi megjelenése a 42/2015. (III. 12.) Korm. rendelet 5/A § (2)-ban található