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

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
- 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
- CEN 14167-1:2003 munkacsoport egyezmény: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures (kivezetve)
- CWA 14170: 2004 Security requirements for signature creation applications (kivezetve)– magyar kivonat
- CWA 14171: 2004 General guidelines for electronic signature verification (kivezetve)– magyar kivonat

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

Kriptográfiai algoritmusokra vonatkozó elvárások /A Nemzeti Hírközlési Hatóság határozatai/

- 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 26. számú ajánlása: A Magyarországon elektronikus azonosításra, hitelesítésre, aláírásra és elektronikus azonosítók hordozására alkalmas eszközök követelményei (HUNeID) 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 15408-1:2002 (=Common Criteria)

- Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 1. rész: Bevezetés és általános modell (idt ISO/IEC 15408-1:1999)
- MSZ ISO/IEC 15408-2:2003
- Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 2. rész: A biztonság funkcionális követelményei (idt ISO/IEC 15408-2:1999)
- MSZ ISO/IEC 15408-3:2003
- Informatika. Biztonságtechnika. Az informatikai biztonságértékelés közös szempontjai. 3. rész: A biztonság garanciális követelményei (idt ISO/IEC 15408-3:1999)
- ISO/IEC 18045:2005: Information technology -- Security techniques -- Methodology for IT security evaluation
- Information technology -- Security techniques -- Methodology for IT security evaluation
- A Közös értékelési módszertan (CEM) a Közös szempontok (CC) társdokumentuma. Célja, hogy leírja azokat a tevékenységeket, melyeket egy értékelő elvégez egy CC szerinti értékelés folyamán.
- ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls
- MSZ ISO/IEC 27001:2014 Információbiztonság-irányítási rendszerek. Követelmények

Egyéb követelmények – a zárt elektronikus információs rendszerrel szembeni elvárások

Egy elektronikus információs rendszer akkor tekinthető zártnak, 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).