Az auditált elektronikus hírközlő eszköz és működtetésének minimum követelményei, auditálásának módja, valamint az ilyen eszköz útján végzett ügyfél-átvilágítás végrehajtása

1.1 Az elektronikus hírközlő eszköz akkor auditálható és működtethető, ha legalább az alábbi informatikai biztonsági követelményeknek megfelel:

a) elemei azonosíthatók és dokumentáltak,

b) üzemeltetési folyamatai szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek,

c) változáskezelési folyamatai biztosítják, hogy a rendszer paraméterezésében és a szoftverkódban bekövetkező változások csak tesztelt és dokumentált módon valósulhassanak meg,

d) adatmentési és adatvisszaállítási rendje biztosítja a rendszer biztonságos visszaállítását, továbbá a mentés-visszaállítás az üzemeltetési szabályzat szerinti gyakorisággal és dokumentáltan tesztelt,

e) a felhasználói hozzáférés mind alkalmazási, mind infrastruktúra szinten szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött,

f) a felállított végfelhasználói hozzáférések egységes, zárt rendszert alkotnak, biztosítják az azonosítási folyamat megvalósulását, továbbá felhasználóinak tevékenysége naplózott, a rendkívüli eseményekről automatikus figyelmeztetések generálódnak,

g) a hozzáférést biztosító kiemelt jogosultságok szabályozottak, dokumentáltak és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzöttek, a kiemelt jogosultságokkal elvégzett tevékenység naplózott, a napló fájlok sérthetetlensége biztosított és a kritikus rendkívüli eseményekről automatikus figyelmeztetések generálódnak,

h) a távoli hozzáférés szabályozott, dokumentált és az üzemeltetési szabályzat szerinti gyakorisággal ellenőrzött,

i) a vírusok és más rosszindulatú kódok és cselekmények elleni védelem biztosított,

j) egyéb adatkommunikációja és rendszerkapcsolatai dokumentáltak és ellenőrzöttek, az adatkommunikáció bizalmassága, sérthetetlensége és hitelessége biztosított,

k) a katasztrófa-helyreállítási terv rendszeresen tesztelt,

l) karbantartása szabályozott és megfelel a pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló kormányrendeletben meghatározottaknak,

m) adathordozóinak védelme szabályozott, megfelelően korlátozott, és a korlátozások rendszeres felülvizsgálatokkal és ellenőrzésekkel fenntartott,

n) saját kontrolljai és az üzemeltetési szabályzat gondoskodnak a rendszerelemek és a kezelt információk sértetlenségéről és védelméről, valamint

o) biztosított a megfelelő szintű fizikai védelem, az elkülönített környezet és az egyes biztonsági események detektálása.

1.2 A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában gondoskodik arról, hogy

a) az ügyféllel felépített elektronikus átviteli csatornán keresztül folyó távadat-átvitel megfelelően biztonságos, titkosított, bizalmas, sértetlen és hiteles legyen,

b) az ügyfél megkapja a szolgáltatás igénybevételének feltételeiről való tájékoztatást, beleértve a szolgáltatás biztonságára vonatkozó ügyféloldali felelősséget is,

c) a szolgáltató oldali azonosításban csak a szükséges mértékben és csak olyan személy vegyen részt, aki a valós idejű ügyfél-azonosítás végrehajtásához szükséges jogi, technikai és biztonsági oktatásban részesült,

d) az elektronikus hírközlő eszközre, és az azonosítási és hitelesítési folyamatra vonatkozó olyan vizsgálati jelentéssel rendelkezzen, amely igazolja, hogy ezek informatikai védelme a biztonsági kockázatokkal arányos, és megfelel a 1.1 pontban foglalt követelményeknek,

e) a jogi szabályozás, az alkalmazott technológia vagy az üzleti folyamat vonatkozásában történt változás esetén, de legalább kétévente, a vizsgálati jelentést megújítsa,

f) a *d)* pontban meghatározott vizsgálati jelentést olyan, az Európai Gazdasági Térség valamely tagállamában bejegyzett szervezet állítsa ki, amely szervezetnél a vizsgálatban igazolhatóan részt vevő személy rendelkezik legalább

fa) az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Systems Auditor (CISA),

fb) az Information Systems Audit and Control Association (ISACA) által kiadott Certified Information Security Manager (CISM),

fc) az International Information Systems Security Certification Consortium Inc. által kiadott Certified Information Systems Security Professional (CISSP), vagy

fd) az Információbiztonsági irányítási rendszerekre vonatkozó ISO/IEC 27001 Vezető Auditor (Lead Auditor)

képesítéssel és minősítéssel, valamint

g) az ügyfél kérésére az ügyfél számára lehetővé tegye az azonosításával, hitelesítésével és a nyilatkozatával kapcsolatos adatoknak az adatkezelés céljának megfelelő ideig történő tartós tárolását, és a tárolt adatok változatlan formában és tartalommal történő megjelenítését.

2.1 A foglalkoztatott az auditált elektronikus hírközlő eszköz útján végzett valós idejű ügyfél-átvilágítást (a továbbiakban: valós idejű ügyfél-átvilágítás) egy erre a célra elkülönített és felszerelt helyiségben végzi.

2.2 A szolgáltató visszakereshető módon rögzíti

a) a helyiségbe belépő személyét,

b) a helyiségből kilépő személyét, valamint

c) a be- és kilépés időpontját.

2.3 A valós idejű ügyfél-átvilágítást csak a szolgáltató olyan foglalkoztatottja végezheti, akinek az e tevékenység ellátásával összefüggő képzését a szolgáltató előzőleg biztosította, és aki a képzést követően eredményes vizsgát tett.

2.4 A szolgáltató az auditált elektronikus hírközlő eszköz vonatkozásában biztosítja az ügyfél átvilágítására és hitelesítésére vonatkozó biztonságos feltételeket, amennyiben

a) az ügyfél az átvilágítási és hitelesítési feltételeket részletesen megismerte és ahhoz kifejezetten hozzájárult,

b) a távoli azonosítás és hitelesítés legalább kétfaktoros – amelyek közül egyik kép- és hangátvitelt lehetővé tevő elektronikus hírközlő eszköz –, és a faktorai legalább két eltérő technológián alapulnak,

c) a távoli azonosítás és hitelesítés másik faktora legalább fokozott biztonságú elektronikus aláíráson, biometrikus azonosítási eszközön, az ügyfél azonosítására alkalmas telefonszámon, elektronikus fizetési eszközön vagy más, megbízható szolgáltató által korábban elvégzett átvilágításon és hitelesítésen alapul,

d) a valós idejű kép- és hangátvitelt lehetővé tévő elektronikus hírközlő eszköz képfelbontása és a kép megvilágítása alkalmas az ügyfél nemének, korának, arcjellemzőinek felismerésére és az ügyfél által bemutatott fényképes azonosító okmánnyal való összevetésre, az okmányban foglalt adatok és a bemutatott okmány biztonsági elemeinek azonosítására,

e) az átvilágítási és hitelesítési folyamat szabályozott és folyamatosan ellenőrzött,

f) az átvilágítás megfelelőségét további, második szintű ellenőrzés követi a szolgáltatón belül.

3.1 A szolgáltató a valós idejű ügyfél-átvilágítás során a szolgáltató és az ügyfél között létrejött teljes kommunikációt, az ügyfél valós idejű ügyfél-átvilágítással kapcsolatos részletes tájékoztatását és az ügyfél ehhez történő kifejezett hozzájárulását visszakereshető módon kép- és hangfelvételen rögzíti.

3.2 A valós idejű ügyfél-átvilágítást végző foglalkoztatott felszólítja az ügyfelet arra, hogy

a) úgy nézzen bele a kamerába, hogy arcképe felismerhető és rögzíthető legyen,

b) érhető módon közölje a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolvány vagy vezetői engedély okmányazonosítóját, és

c) úgy mozgassa a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolványát vagy vezetői engedélyét, hogy az azon található biztonsági elemek és adatsorok felismerhetők és rögzíthetők legyenek.

3.3 A valós idejű ügyfél-átvilágítást végző foglalkoztatott köteles megbizonyosodni arról, hogy a valós idejű ügyfél-átvilágításhoz használt kártyaformátumú személyazonosító igazolvány vagy vezetői engedély alkalmas a valós idejű ügyfél-átvilágítás elvégzésére, így

a) kártyaformátumú személyazonosító igazolvány vagy vezetői engedély egyes elemei és azok elhelyezkedése megfelel az okmányt kiállító hatóság előírásainak,

b) az egyes biztonsági elemek – különösen a hologram, a kinegram vagy ezekkel megegyező más biztonsági elemek – felismerhetők és sérülésmentesek,

c) a kártyaformátumú személyazonosító igazolvány vagy vezetői engedély rendelkezik gépi adatolvasást lehetővé tevő mezővel,

d) a kártyaformátumú személyazonosító igazolvány vagy vezetői engedély okmányazonosítója megegyezik az ügyfél által közölt okmányazonosítóval, felismerhető és sérülésmentes.

3.4 A valós idejű ügyfél-átvilágítást végző alkalmazott köteles megbizonyosodni arról, hogy

a) az ügyfél arcképe felismerhető és azonosítható az általa bemutatott kártyaformátumú személyazonosító igazolványon vagy vezetői engedélyen látható arckép alapján, és

b) a kártyaformátumú személyazonosító igazolványon vagy vezetői engedélyen megtalálható adatok megegyeznek az ügyfélről a szolgáltatónál rendelkezésre álló adatokkal.

3.5 A szolgáltató a valós idejű ügyfél-átvilágítás során az ügyfél által bemutatott kártyaformátumú személyazonosító igazolvány vagy vezetői engedély adatait összeveti nyilvánosan hozzáférhető nyilvántartás vagy olyan nyilvántartás adataival, amelynek kezelőjétől törvény alapján adatigénylésre jogosult.

3.6 A szolgáltató egy számokból és egyéb jelekből álló, központilag, véletlenszerűen generált azonosítási kódot küld az ügyfélnek az ügyfél választása szerint az ügyfél azonosítására alkalmas e-mail címre vagy SMS-ben mobil telefonszámra, amely kódot az ügyfél a valós idejű ügyfél-átvilágítás befejezéséig a szolgáltató által választott kommunikációs formában küld vissza a szolgáltatónak.

4.1 A szolgáltató a 3. pontban meghatározottak elvégzését követően az ügyfélre irányadó, Pmt. szerinti nyilatkozatok megtételére és okiratok bemutatására hívja fel az ügyfelet.

4.2 A szolgáltató az 4.1. pont alapján bemutatott okiratok adatait összeveti nyilvánosan hozzáférhető nyilvántartás vagy olyan nyilvántartás adataival, amelynek kezelőjétől törvény alapján adatigénylésre jogosult.

5.1 A szolgáltató megszakítja a valós idejű ügyfél-átvilágítást, amennyiben

a) az ügyfél a valós idejű ügyfél-átvilágítás során visszavonja az adatrögzítéshez adott hozzájárulását,

b) az ügyfél által bemutatott okmányok, illetve okiratok fizikai és adattartalmi követelményei nem adottak,

c) az ügyfél, az általa bemutatott okmányok, illetve okiratok vizuális azonosításának feltételei nem adottak,

d) a szolgáltató nem tudja elkészíteni a hang- és képfelvételt,

e) az ügyfél nem, nem teljes egészében vagy hibásan küldi vissza az azonosítási kódot,

f) az ügyfél nem vagy a foglalkoztatott számára észlelhetően befolyás alatt tesz nyilatkozatot, vagy

g) az eljárás során azzal kapcsolatban bármilyen ellentmondás vagy bizonytalanság lép fel.

5.2 Pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, illetve körülmény felmerülése esetében, a szolgáltató az 5.1 pontban írt feltételek fennállása ellenére is elvégzi a valós idejű ügyfél-átvilágítást, amelyet követően haladéktalanul bejelentést tesz a pénzügyi információs egységnél.

5.3 A szolgáltató az 5.1 pont *a)* alpontja esetében, amennyiben nem merül fel pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény, illetve körülmény, haladéktalanul törli a hozzájárulás visszavonásáig birtokába jutott ügyféladatokat.

6. A valós idejű ügyfél-átvilágítást a foglalkoztatott közvetlen vezetőjének a valós idejű ügyfél-átvilágítás egészére kiterjedő ellenőrzése zárja le.

7. A szolgáltató a valós idejű ügyfél-átvilágítás rendszerét úgy alakítja ki, hogy azt a fogyatékos személyek jogairól és esélyegyenlőségük biztosításáról szóló törvény szerinti fogyatékos személy is igénybe tudja venni.