Műszaki leírás és követelmények

A Bankszövetség által indított Egységes Digitális ESG Platform beszerzés tenderben

A Bankszövetség, mint ajánlatkérő a nyertes ajánlattevő által leszállítandó és üzemeltetendő Közös Digitális ESG Platformmal, és nyertes ajánlattevővel kapcsolatban az alábbi elvárásokat fogalmazza meg:

I. A Közös Digitális ESG Platformra vonatkozó általános elvárások:

1. A Közös Digitális ESG Platformnak meg kell felelnie a mindenkori releváns MNB ajánlásoknak és bankszektorra vonatkozó törvényi előírásoknak, különösen, de nem kizárólagosan a fenntartható finanszírozás és az egységes vállalati felelősségvállalás ösztönzését szolgáló környezettudatos, társadalmi és szociális szempontokat is figyelembe vevő, vállalati társadalmi felelősségvállalás szabályairól és azzal összefüggő egyéb törvények módosításáról szóló 2023. évi CVIII. törvény („**ESG tv.”)** rendelkezéseinek, valamint a Pillér 3-as/EU Taxonomy adatigények, továbbá a GDPR rendelkezéseinek.

2. A Közös Digitális ESG Platformnak alkalmasnak kell lennie arra, hogy az Ügyfelek máshol kitöltött kérdőíveiket – ideértve az SZTFH ESG Platformon kitöltött kérdőívet is – feltölthessék a rendszerbe (mintha ott töltötték volna ki) és továbbküldhessék az általuk megjelölt Résztvevő Hitelintézet részére.

3. A Közös Digitális ESG Platformon elérhető kérdőív egységes szerkezettel és tartalommal tartalmazza az MNB Ajánlás 1. számú mellékletében szereplő minimum kérdéssort, valamint a Pillér 3-as[1] és a Taxonómia rendelet[2] adatigényeket, melyet a kötelező adatszolgáltatás során az Ügyfelek megválaszolnak és azt a Résztvevő Hitelintézetekkel megoszthatják.

4. A Közös Digitális ESG Platformnak képesnek kell lennie a mindenkori MNB Ajánlásoknak történő megfelelés keretében akár a vállalkozás típusától függő, eltérő tartamú kérdéssorok alkalmazására is.

5. A kérdőív önkéntesen, banki elvárás nélkül is elérhető, kitölthető legyen az Ügyfelek számára.

6. A Közös Digitális ESG Platformnak magyar mellett angol nyelven is rendelkezésre kell állnia.

7. A Közös Digitális ESG Platform és a kérdőív kialakítási formája online felület. Az egyes válaszok lehetnek szabadszavasak, értékkészletek és számértékek.

8. A kérdőívnek is az értékkészletes mezőknek is paraméterezhetőnek kell lennie a későbbi módosítások átvezetéséhez, továbbá annak érdekében, hogy a kérdéssor tartalma Résztvevő Hitelintézetenként módosítható vagy kiegészítő legyen.

9. A kérdésekhez biztosítani kell alátámasztó dokumentum csatolásának a lehetőségét is (legalább az alábbi formátumokban: excel, word, pdf, jpg)

---

[1] A hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról szóló, 2013. június 26-i 575/2013/EU európai parlamenti és tanácsi rendelet (CRR) 449a. cikke.

[2] Az Európai Parlament és a Tanács (EU) 2020/852 rendelete (2020. június 18.) a fenntartható befektetések előmozdítását célzó keret létrehozásáról, valamint az (EU) 2019/2088 rendelet módosításáról.

10. A Közös Digitális ESG Platformnak alkalmasnak kell lennie arra, hogy az Ügyfelek az egyes kérdésekhez magyarázó információkat tudjanak megadni (mértékegység átváltás, hivatkozás jogszabályi helyre, képletezés stb.)

11. A mezőkre vonatkozóan logikai és formai ellenőrzéseket is kell tudni definiálni, adott esetben értékkészletet definiálni hozzá.

12. Elvárt a validációs logikák alkalmazása, azaz a Közös Digitális ESG Platform a rögzítés során azonosítsa az invalid/hiányzó válaszokat, a mentés során érvényesítse a teljeskörűség igényét (ne lehessen hiányos/nyilvánvalóan invalid adatokat tartalmazó űrlapot véglegesíteni).

13. Kétirányú Bank-Ügyfél, Ügyfél-Bank kapcsolat kialakítása a Közös Digitális ESG Platform által.

- Egyrészt az Ügyfél megadhatja melyik Résztvevő Hitelintézettel osztja meg a kitöltött kérdőívét.
- Másrészt a Bank felől induló kérések kezelésére is alkalmas legyen, azaz a résztvevő Résztvevő Hitelintézet is kezdeményezheti az adatigényt alátámasztó dokumentáció megküldését, melynek jóváhagyására az Ügyfél jogosult.

14. A Közös Digitális ESG Platformot úgy kell megtervezni és kialakítani, hogy:

- Egyidőben akár 500 felhasználót ki tudjon szolgálni.
- Skálázható módon legalább 600.000 Ügyfél adatait tudja tárolni.
- Az adatokat a jogszabályban előírt, minimum a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény 57. § alapján meghatározott 8 évre visszamenőleg tárolja.
- A Közös Digitális ESG Platformon keresztüli lekérdezések visszakövethető és letagadhatatlan módon történjenek.
- Az adatátadások titkosított csatornán történjenek és az adatállományok sértetlensége biztosított legyen, azaz a tagbankok az adatokat megmásíthatatlan módon kapják meg.
- A jogosultság kezelést a szükséges és elégséges elv mentén, szeparáció mellett kell biztosítani.
- Az adatvédelmi elvárásokat be tudja tartani (beépített és alapértelmezett adatvédelem érvényesülése és érintetti jogok gyakorlásának elősegítése).

15. A Résztvevő Hitelintézetek felé kialakításra kerülő adatcsatorna és adatfile típus(ok) a tagok számára elfogadható kompatibilitással és adatbiztonsági szinttel rendelkezzen.

- Elfogadott adatkommunikációs megoldások API, MQ. Ezek előzetes kialakítása elvárt a nyertes ajánlattevő részéről.
- A Résztvevő Hitelintézetek által elfogadott és alkalmazandó kriptográfiai algoritmusok alkalmazása elvárt:
    - Felhős adattárolás esetében a következő szimmetrikus kulcsú algoritmusok elvártak: AES-256 vagy erősebb.
    - Az adatok integritását és forrásának hitelességét biztosító, kulcs generáló algoritmusok közül a következők egyikét tudjuk elfogadni: SHA-256, SHA-384, SHA-512/224, SHA-512/256, SHA-512/384, SHA3-224, SHA3-256, SHA3-384

- Digitális aláírás és időbélyegző esetén elvárt az eIDAS szerinti minősített tanúsítvány alkalmazása.

16. 1 Ügyfél, 1 beszámolási időszakra (1 évre) 1 db kérdőívet tölt ki. Naptári éven belül, amennyiben évközben az Ügyfél új beszámolója elérhetővé válik, 2 db kérdőívet tölthet ki továbbá a saját kérdőívét módosíthatja.

17. Egy adott időpontban egy adott üzleti év vonatkozásába egy érvényes dokumentum lehet a rendszerben.

18. A visszakövethetőség biztosítása érdekében az érvényét vesztő dokumentumokat is tárolni szükséges 8 évig.

19. A Közös Digitális ESG Platformnak 7/24-ben elérhetőnek kell lennie (99%-os elérhetőség és működőképesség mellett, ide nem értve az előre bejelentett karbantartásokat, amelyek mértéke legfeljebb évi 36 óra).

20. A Közös Digitális ESG Platform kapcsán elvárás az Ügyfélkitöltést támogató ESG szakmai vonal kialakítása, különösen a chatbot, továbbá oktatási anyagok és kalkulátorok elkészítése és rendelkezésre bocsátása. Opcionális elvárás, és értékelési előnyt jelent, ha a kérdéssor kitöltéséhez ajánlattevő tud a chatboton túl telefonos kitöltési tanácsadási támogatást is biztosítani.

II. A nyertes ajánlattevővel szembeni elvárások:

1. A nyertes ajánlattevő köteles elvégezni a Közös Digitális ESG Platformot igénybe vevő Ügyfelek azonosítását az irányadó adatvédelmi jogszabályok betartásával. Az ügyfélazonosítás során szükséges a felhasználói szerepkörök megkülönböztetése, legalább ügyintéző és cégképviseletre jogosult szerepek tekintetében. Az ügyfélazonosítás során a felhasználók személyes adatainak kezeléséért a nyertes ajánlattevő önálló adatkezelőként felel. A Résztvevő Hitelintézet felé történő adattovábbítás kapcsán nyertes ajánlattevő köteles gondoskodni a megfelelő adatkezelési tájékoztató elérhetőségéről, illetve az adattovábbítás jogi feltételeinek megteremtéséről (az adatkezelési tájékoztatóban külön ki kell térni arra, hogy kinek, milyen céllal, milyen határidővel kerülnek átadásra adatai).

2. A Közös Digitális ESG Platformot üzemeltetője által kialakított általános szerződési feltételekben vagy üzletszabályzatban, illetve adatkezelési tájékoztatóban rögzítésre kerüljön, hogy a Közös Digitális ESG Platformon megtett nyilatkozatok fizikai átadását a nyertes ajánlattevő, mint a Közös Digitális ESG Platformot üzemeltetője biztosítja, az adatok címzettjeként feltüntetve az adott Résztvevő Hitelintézetet. Az ajánlatban ajánlattevő mutassa be a kérdőív adatok saját célú felhasználására vonatkozó terveit és koncepcióját (ha van ilyen). A saját célú felhasználás lehetséges, amennyiben ajánlattevő ennek jogi kereteit az általános szerződési feltételekben vagy üzletszabályzatban kialakítja. Amennyiben egy Ügyfél a kérdőívben megadott adatok saját célú felhasználásra a nyertes ajánlattevőnek felhatalmazást ad, erről a tényről az Ajánlatkérő és az érintett Résztvevő Hitelintézet kapjon tájékoztatást nyertes ajánlattevőtől vagy a a Közös Digitális ESG Platformon keresztül.

3. Nyertes ajánlattevőnek a Résztvevő Hitelintézetek belső ellenőrzése számára jogosultságot kell biztosítania az adatok, folyamatok ellenőrzésének lefolytatására.

4. Az ajánlattevő rendelkezzen a Közös Digitális ESG Platform működtetéséhez szükséges minden hatósági engedéllyel (ha van ilyen).

5. Nyertes ajánlattevő köteles megfelelni a Hpt. szerinti kiszervezett szolgáltatással szembeni elvárásoknak, a DORA rendelet IKT szolgáltatásra vonatkozó releváns rendelkezéseinek, továbbá MNB 1/2025 és 2/2025 információbiztonsági ajánlásainak.

6. Nyertes ajánlattevőnak folyamatos támogatást és opcionálisan folyamatos tesztelési lehetőséget kell biztosítania a szerződéses időszakban.

7. Nyertes ajánlattevőnek képesnek kell lennie a Közös Digitális ESG Platform implementációját elvégezni mind a 9 Résztvevő Hitelintézetnél, továbbá az egyedi igények teljesítésére is az egyes Résztvevő Hitelintézetekkel kötött külön szerződés alapján.

III. Közös Digitális ESG Platform elvárt működési folyamatának leírása és általános elvárások

Kérjük, hogy ajánlatukat az alábbiakban részletezett folyamatleírásra és elvárásokra tekintettel tegyék meg.

1. Fázis - Közös Digitális ESG Platform Ügyfél általi elérésének folyamata:

A platform felületén megvalósuló folyamatok (több megoldás kezelése):

1.1 Ügyfél előtt ismert, hogy hitelfelvételekor elvárt az MNB által meghatározott ESG minimum kérdéssor, valamint a Pillér 3-as/EU Taxonomy adatigények kitöltése, ezért önként felkeresi a Közös Digitális ESG Platformot.

1.2 A Résztvevő Hitelintézet vagy a Résztvevő Hitelintézet kezdeményezésére a Közös Digitális ESG Platform küldi meg elektronikus levélben az Ügyfélnek a weboldal elérési útját tartalmazó linket a kitöltésre vonatkozó felkéréssel.

A Közös Digitális ESG Platform elérését, kialakítását érintő elvárás:

- A nyertes ajánlattevő a tagbankok számára térítés ellenében, az Ügyfelek részére ingyenesen biztosítja a webes felület elérését.
- A kommunikáció során lehetőség legyen magyar mellett az angol nyelv kiválasztására.
- A Közös Digitális ESG Platformnak követnie kell a Bankszövetség arculati elvárásait és el kell fogadnia a Bankszövetség Etikai Kódexét.

2. Fázis - Ügyfélregisztráció a Közös Digitális ESG Platformon

A Közös Digitális ESG Platform felületén megvalósítandó folyamatok:

2.1 A nyertes ajánlattevő, mint a Közös Digitális ESG Platform szolgáltatója ügyfélazonosítást végez. Ennek jogszabályok szerinti működését biztosítani szükséges. A Platform-felhasználók személyes adatainak kezeléséért a nyertes ajánlattevő a felelős, önálló adatkezelőként.

2.1.1 Az Ügyfélnek a jogszabály szerinti adatkezelési tájékoztatót kell elfogadnia a Résztvevő Hitelintézet felé történő adattovábbításra szóló meghatalmazás során. Ennek jogszabályi feltételeit biztosítani szükséges. (Kinek, milyen céllal, etc. kerülnek átadásra adatai.)

2.1.2 A nyertes ajánlattevő által kialakított ÁSZF és ÜSZ-ben, illetve Adatkezelési tájékoztatóban kerüljön rögzítésre, hogy a Közös Digitális ESG Platformon megtett nyilatkozatok fizikai átadását a nyertes ajánlattevő biztosítja, az adatok címzettjeként feltüntetve az érintett Résztvevő Hitelintézetet.

2.1.3 A Közös Digitális ESG Platformon az érintett cég regisztrációját kizárólag a cég képviseletére jogosult személyek végezhessék el, biztosítva, hogy kizárólag az adott vállalat képviselője küldheti be az adatokat. MFA, multi faktoros azonosítás elvárt. További jó megoldást jelent az azonosításra az úgynevezett harmadik feles (third party) megoldás beépítése (pl. DÁP, Ügyfélkapu) a Közös Digitális ESG Platformba, mely által biztosított, hogy ne „akárki" tölthesse ki a kérdőívet. Legyen lehetséges a képviseleti jog igazolása meghatalmazás feltöltésével is.

2.2 A szabályos működéshez szükséges Ügyfél nyilatkozatok elektronikus úton történnek meg.

2.2.1 GDPR szerinti adatvédelmi nyilatkozat (ha az alkalmazott jogalap miatt szükséges).

2.2.2 adattovábbítást jóváhagyó nyilatkozat.

2.2.3 képviseleti jogról való nyilatkozás.

2.2.4 a rögzített adatok hitelességéről szóló nyilatkozat.

2.3 Egy Ügyfél csak egy alkalommal regisztrálhat.

A regisztrációs felület kialakítása során megjelenő elvárás:

- Ügyfélazonosítás.
- Biztonság / A multi faktoros azonosítás elvárt a regisztráció során. További elfogadható megoldást a harmadik feles azonosítás (pl. DÁP-os/ügyfélkapu).
- Nyilatkozatok, kérdőívek tárolása.
- Nyilatkozatok, kérdőívek módosításának biztosítása.
- Nyilatkozatok, kérdőívek között visszakereshetőség biztosítása.
- Nyilatkozatok megfelelőségének ellenőrzése.

3. Fázis - Ügyféladatok rögzítése a Közös Digitális ESG Platformon

A Közös Digitális ESG Platformon felületén megvalósítandó folyamatok:

3.1 Az adatok vonatkoztatásának időpontjának (üzleti év) kiválasztása.

3.2 1 ügyfél, 1 beszámolási időszakra 1 db kérdőívet tölt ki. Naptári éven belül, amennyiben évközben az ügyfél új beszámolója elérhetővé válik, 2 db kérdőívet tölthet ki továbbá a saját kérdőívét módosíthatja.

3.3 Egy adott időpontban egy adott üzleti év vonatkozásába egy érvényes dokumentum lehet a rendszerben. A visszakövethetőség biztosítása érdekében az érvényét vesztő dokumentumokat is tárolni szükséges 8 évig.

3.4 A felhasználó (Ügyfél) a felületen manuálisan rögzíti az információkat, azokhoz manuálisan rögzít alátámasztó dokumentumokat. Ellenőrzést követően jóváhagyja a rögzült adatokat. Ekkor - a beépített logikai vizsgálatok és a teljeskörűség megvizsgálását követően - a bevitt adatok véglegesítésre kerülnek, azok beküldésre kész állapotba kerülnek.

3.5 Elvárás a feltöltött adatok kiexportálásának biztosítása. Ennek keretében az Ügyfél letölti a platformra rögzített adatait a saját IT környezetébe.

3.6 Elvárás, hogy az Ügyfelek korábbi kérdőívei visszakereshetőek és megtekinthetőek legyenek.

3.7 Elvárás az adatok több lépcsőben megvalósuló rögzítésének biztosítása köztes állapotok mentésével és azok visszatöltésének biztosításával.

3.8 Elvárás a logikai ellenőrzések futtatása kérésre, illetve mentés előtt mindig, hibaüzenetek kiírása felületre, navigálás a hibás mezőre.

3.9 Elvárás a kérdőív leadás-véglegesítés nélküli mentése. (A kérdések megválaszolása után az Ügyfél eltárolja a kérdőívet a felületen, melyet tudnia kell szerkeszteni későbbi időpontokban.)

3.10 Elvárás a mentett kérdőív újra szerkesztésének folytatása (mentett adatok rendelkezésre állnak). Ez esetben látszódjon, hogy ki és mikor módosított (mentett) utoljára.

3.11 Elvárás, hogy amennyien az Ügyfél módosítja a korábban már lezárt, Résztvevő Hitelintézet által feldolgozott kérdéssorát, úgy arról az érintett Résztvevő Hitelintézet értesítést kapjon. *(„Új érvényes dokumentum készült ….. tárgyévet érintően.”)*

3.12 Az Ügyfél kérdőív beérkezéséről hiteles időbélyegző készüljön. Szintén rögzítésre kerüljön a hozzájárulást adó személye (felhasználó azonosítója).

<u>Az Ügyféladatok rögzítése során felállított elvárás:</u>

- Kizárólag az érintett cég képviseletét ellátó személyek tudjanak a cég nevében eljárni, melynek szabályait az Ügyfél rögzíti.
    - Azonosítást a nyertes ajánlattevő végzi. (MFA, multi faktoros azonosítással.)
    - Lehetőségként legyen biztosítva az adat rögzítésre (rögzítő), valamint a kérdőív jóváhagyására, véglegesítését eredményező (jóváhagyó) jogkörök különválasztása.
- Az adott tevékenység naplózásra kerüljön, ez által biztosítva az időbeli visszakövethetőséget, továbbá az adatrögzítő személy(ek) tevékenységét.
- Az ugyanazon időszakra vonatkozó kérdőívek elkülönítése, tárolása is biztosított legyen (módosítás esetén).
- Adatok egyszerű, felhasználóbarát módon kialakított mentése/visszatöltése biztosítva legyen.
- Biztosítva legyen a hosszútávú adattárolás – archiválás.
- Ügyfél és felhasználó azonosítás a törvény által előírtak szerint a lehető legkevesebb személyes adat felhasználásával történjen.

- Opcionálisan az ügyfelek technikai támogatása telefonos ügyfélszolgálaton keresztül megvalósuljon.
- Rendszer integritásvédelme. A Közös Digitális ESG Platform képes legyen felismerni a fájlokban bekövetkezett nem várt vagy nem engedélyezett változásokat, amelyek jelezhetnek egy rosszindulatú tevékenységet vagy behatolást. A Közös Digitális ESG Platform napi szinten készít egy lenyomatot a rendszerfájlok állapotáról, valamint a futtatott programkódokról. Ha eltérést talál, a nyertes ajánlattevőnek, mint rendszerüzemeltetőknek emailt küld a részletekről. Az emailben érkezett értesítések feldolgozásáért a nyertes ajánlattevő, mint rendszerüzemeltető felel.

4. Fázis - Ügyféladatok elérése a Résztvevő Hitelintézetek által

A Közös Digitális ESG Platformon megvalósítandó folyamatok:

4.1 Az Ügyfél a Közös Digitális ESG Platformról indítva, vagy a Résztvevő Hitelintézet digitális bekérdezése nyomán a Közös Digitális ESG Platform biztonságos csatornán küldi meg az általa kiválasztott Résztvevő Hitelintézet számára a hozzáférést lehetővé tevő „kulcsot” (adatai elérését biztosító engedélyt). Elfogadott adatkommunikációs megoldások API, MQ. Ezek előzetes kialakítása elvárt a nyertes ajánlattevő részéről.

4.2 A Résztvevő Hitelintézet elektronikus rendszeren keresztül küldi meg adott ügyfel(ek)re vonatkozó dokumentum igényét a nyertes ajánlattevőnek, mint a Közös Digitális ESG Platform szolgáltatójának. A nyertes ajánlattevő az általa véglegesített státuszban letárolt, az adott Résztvevő Hitelintézet számára hozzáférési engedélyt kapott Ügyfél kérdőíveket továbbítja elektronikus válasz csomagjában, időbélyegző és a Közös Digitális ESG Platform digitális aláírásával ellátva a Résztvevő Hitelintézet felé.

4.3 Elvárás, hogy a Közös Digitális ESG Platform lehetőséget biztosítson a Résztvevő Hitelintézetnek, mint felhasználónak a felületen történő adatbekérdezésre/lekérdezésre.

4.4 A nyertes ajánlattevő biztosítson tömeges és egyedi, rendszeres és eseti adattranszfer lehetőséget biztonságos API kapcsolaton keresztül.

4.5 A Résztvevő Hitelintézetek egyedileg és tömegesen, az adószámokat megadva is tudjanak visszajelzést küldeni az Ügyfelek felé a Közös Digitális ESG Platformon keresztül. Ez a módszer szolgálna arra, hogy az Ügyfelek figyelmét felhívja a kérdőívek kitöltésére, vagy a dokumentumhiány(ok)ra.

4.6 Elvárás a historikus adatok elérése a Résztvevő Hitelintézet által. Az Ügyfél által a Résztvevő Hitelintézet részére adott hozzáférés az Ügyfél összes tárolt, korábbi évekre vonatkozó kérdőívére is vonatkozik.

4.7 Amennyiben az Ügyfél visszavonja korábban adott hozzáférését, úgy az érintett Résztvevő Hitelintézet csak a visszavonás időpontjának évére vonatkozó, valamint az azt megelőző időszak adataihoz férhessen hozzá.

4.8 Elvárás, hogy a hozzáférés visszavonásának tényéről a Résztvevő Hitelintézet és az Ügyfél is tájékoztatást kapjon.

4.9 A Résztvevő Hitelintézetek számára lehetőség biztosítása, hogy alátámasztó dokumentációt kérjenek az Ügyfél által rögzített adatokról.

4.10 A Közös Digitális ESG Platform tegye lehetővé, hogy Ügyfél minden egyes alkalommal, amikor egy Résztvevő Hitelintézet véglegesített kérdéssorához hozzáférési engedélyt kap nyilatkozzon az adatkezelési tájékoztató megismeréséről, és legyen lehetőség egyedi adatkezelési tájékoztatók feltöltésére és Ügyfél általi megismerésére (Az így átadott információkat az adott Résztvevő Hitelintézet milyen céllal fogja felhasználni, azokat meddig fogja tárolni, milyen módon tudja a meghatalmazását megszűntetni. Az átadás során személyes adatok nem kerülnek a Bank felé továbbításra, valamint a nyilatkozatát a Platform felületéről minimum 8 évig le tudja tölteni.)

4.11 A dokumentumokat nyertes ajánlattevő eIDAS szerinti megfelelően aláírással, azaz legalább fokozott biztonságú időbélyegzővel és hiteles aláírással együtt továbbítja a Résztvevő Hitelintézet részére.

5. Az Ügyféladatok Résztvevő Hitelintézetek felé történő továbbítására vonatkozó elvárás:

- Biztonságos adattovábbítás. Az adatcsomag titkosítása.
- Az adatok átadásáról, mind az Ügyfél, mind a címzett Résztvevő Hitelintézet igazolást kap.
- A leadott kérdőívek és hozzá tartozó dokumentumok elérése, megtekintése a felületen – keresési funkciók segítségével biztosított legyen.
- A Résztvevő Hitelintézetnek legyen lehetőségük tömeges bekérdezések útján ellenőrizni, hogy az ügyfeleik adtak-e le kérdőívet és ha igen, mikor.
- A front-end felületre a bankok is be tudjanak lépni. A bankoknak lehetőséget kell biztosítani, hogy az ügyfelek által kitöltött kérdőíveket le tudják tölteni, valamint az üzleti funkciókat a bankok elérhessék biztonságos csatornán (pl. API, MQ) keresztül.

6. Rendszerintegrációval szemben támasztott részletes technikai követelmények

Egyidejű/szinkron integráció, API követelmények

- Minden külső rendszer felé történő szinkron integrációnak HTTPS/REST alapúnak kell lennie.
- A preferált üzenetformátum a JSON, benne előre definiált schema objektum leírókkal

Hitelesítés és engedélyezés (Authentication & Authorization)

- Minden API-nak engedélyeznie kell a hitelesítést.
- A bank támogatja az API-kulcsot, az Oauth-kódot és az ügyfél-hitelesítési engedélyt.
- A hálózati térben minden kommunikációt a hívó felek között mTLS-szel kell biztosítani.
- Az API-kat általában megbízható IdP-k által kibocsátott JWT hordozó tokenekkel kell védeni.
- Az ismeretlen kibocsátótól származó tokeneket el kell utasítani.
- Az API kliensek több felhasználási esetben (m2m / alkalmazott / ügyfél) szereznek hozzáférési tokeneket az IdP-ktől, és hordozó token API-hívásokként használják őket.
- Mivel a hívás különböző API-rétegeken halad át, az eredeti hozzáférési tokent használják az összes hívás során (ugyanaz a biztonsági kontextus).
- A tokenek a legkisebb jogosultság elvét követik: API-k meghívása a legspecifikusabb hozzáférési token használatával - az alkalmazottak és ügyfelek hozzáférési tokenjei előnyben részesítendők az m2m hozzáférési tokennel szemben.

- Minden API-szolgáltatónak ellenőriznie kell az összes bemenetet, és nem hagyatkozhat a korábbi felekre az ilyen ellenőrzések végrehajtása során, mert előfordulhat, hogy ezt nem teszik meg, vagy az API-t egy másik fél (érvényes ügyfél vagy támadó) hívhatja meg és a feltételezett ellenőrzések nem hajthatók végre (Zero Trust).

Aszinkron integráció

- A bank támogatja és biztosítja a streaming I Kafka üzenetkezelési megoldásokat.
- KAFKA esetében az üzeneteknek AVRO formátumban kell lenniük, és szükséges előre definiált schema-t használni a schema validáció miatt.

7. Biztonsági követelmények

A Közös Digitális ESG Platformnak meg kell felelnie az alábbi biztonsági követelményeknek:

Adattitkosítás

- Minden érzékeny adatot titkosítani kell nyugalmi állapotban (at rest) minimum AES-256 titkosítással.
- Az adatátvitel során (in transit) TLS 1.3 vagy újabb protokollt kell alkalmazni megfelelő cipher suite konfigurációval.
- A kriptográfiai kulcsokat biztonságos kulcskezelő rendszerben kell tárolni, periodikus rotációval.

Adatmegőrzés és -törlés

- A rendszernek támogatnia kell az adatmegőrzési szabályoknak megfelelő automatizált adattörlés végrehajtását.
- Az adatok törlését biztonságos, visszaállíthatatlan módon kell végrehajtani, megfelelő naplózással.
- A rendszernek biztosítania kell a "törléshez való jog" (GDPR) támogatását éles adatokon.

Hitelesítés

- Minden rendszeradminisztrációs és privilegizált hozzáférés esetén többfaktoros hitelesítést (MFA) kell alkalmazni.
- A felhasználói jelszavaknak bonyolultságára biztosítani kell konfigurálható jelszókomplexitási megoldást.

Jogosultságkezelés

- A rendszernek szerepköralapú hozzáférés-szabályozást (RBAC) kell implementálnia.
- A legkisebb jogosultság elvét (least privilege) kell alkalmazni minden felhasználó és rendszerkomponens esetében.
- A rendszernek támogatnia kell a feladatkörök szétválasztását (segregation of duties) a kritikus funkciók esetében.

Naplózás

- A rendszernek naplóznia kell a biztonsági eseményeket, úgymint ki és bejelentkezési események, authorizációs rendszer módosításai, konfiguráció módosítása, rendszer leállítása, újraindítása, hibák.
- Az üzemeltetési és biztonsági naplóbejegyzéseket logikailag szét kell választani.

Biztonságos Konfiguráció (Hardening)

- Minden rendszerelemet dokumentált biztonsági konfigurációs alapelvek szerint kell beállítani.

8. Szoftverfejlesztés követelményei

Biztonságos Szoftverfejlesztési Életciklus (SSDLC)

- A fejlesztés során követni kell a nyelv- és platform-specifikus biztonsági legjobb gyakorlatokat:
- OWASP Top 10 kockázatok kezelése
- CERT Secure Coding Standards
- Nyelv-specifikus biztonsági irányelvek (pl. Java Secure Coding Guidelines)
- Az implementáció során kiemelt figyelmet kell fordítani az alábbi védelmi mechanizmusokra:
- Bemeneti adatok validálása minden érintett rétegben
- File feltöltés esetén vírusvédelem bekötése
- Output encoding alkalmazása XSS ellen
- Parametrizált lekérdezések használata SQL injection ellen
- Biztonságos session kezelés (lejárat, invalidáció, fixáció elleni védelem)
- CSRF elleni védelem
- Biztonságos hibakezelés és naplózás (érzékeny információk kiszivárgásának elkerülése)
- Időalapú támadások (timing attacks) elleni védelem
- Cache-elés és memóriakezelés biztonságos implementálása

Kódellenőrzés és Tesztelés

- Minden kódot az alábbi biztonsági ellenőrzéseknek kell alávetni fejlesztés során:
- Statikus kódelemzés (SAST) automatizált eszközökkel
- Dinamikus alkalmazásbiztonsági tesztelés (DAST)
- Interaktív alkalmazásbiztonsági tesztelés (IAST) ahol lehetséges
- Függőségvizsgálat (SCA) a külső komponensek sérülékenységeinek azonosítására
- Manuális kódellenőrzés a kritikus biztonsági funkcióknál
- A biztonsági tesztelési eredményeket dokumentálni kell, a talált problémákat súlyosság szerint priorizálva kell kezelni.
- Kritikus és magas kockázatú biztonsági problémákat kötelezően javítani kell üzembe helyezés előtt.

Függőségkezelés

- Minden külső komponenst, könyvtárat és keretrendszert nyilván kell tartani és rendszeresen ellenőrizni kell biztonsági szempontból.
- Csak megbízható forrásból származó, aktívan karbantartott és ismert sebezhetőségekkel nem rendelkező komponensek használhatók.
- A külső komponensek verziószámát és frissítési folyamatát dokumentálni kell.

API Biztonság

- Minden API-t a következő biztonsági kontrollokkal kell ellátni:
- Erős hitelesítés minden végponton
- Jogosultságkezelés minden API műveletnél
- Input validálás minden paraméteren

- Rate limiting és throttling a túlterheléses támadások ellen
- API dokumentáció, amely nem fed fel érzékeny implementációs részleteket
- REST API-k esetén az OWASP API Security Top 10 kockázatokat kezelni kell.

Titokkezelés (Secrets Management)
- Tilos a kódba ágyazni érzékeny adatokat (jelszavak, API kulcsok, titkosítási kulcsok).
- A titkok rotációját automatizált módon kell biztosítani.

Biztonságos konfiguráció és hardening
- Egy részletes konfigurációs baseline-t kell létrehozni, amely dokumentálja az összes biztonsági beállítást.
- A biztonsági konfigurációkat rendszeresen ellenőrizni kell az eltérések (drift) felderítésére.

Felhő szolgáltatások igénybevételének követelményei
- Az alkalmazni kívánt felhőszolgáltató biztonságát és megfelelőségét előzetesen jóvá kell hagyatni a megrendelővel.
- A nyújtott felhőszolgáltatás alkalmazásba vételét követően feleljen meg az MNB érvényes, felhőszolgáltatások igénybevételéről szóló ajánlásában foglalt követelményeknek.

Nyertes ajánlattevővel szemben elvárás a fenti követelményeknek való megfelelést igazoló fejlesztési dokumentáció és/vagy audit jelentés átadása Ajánlatkérő részére.

9. **Egyéb nem elvárt, azonban a folyamatok hatékonyságát növelő szolgáltatások, amelyek biztosítása az értékelés során előnyt jelent**:

9.1 A fenntarthatósági adatok előzetes feldolgozása:

A Közös Digitális ESG Platform feltöltött és véglegesített kérdéssor adatain - transzparens módon felállított értékelési szempontrendszer alapján kialakított algoritmus mentén - a Közös Digitális ESG Platform szolgáltatója, vagy a vele szerződésben lévő partnere előzetes értékelést végez. Ezt teheti komplex értékelést alkalmazva, vagy külön E, S, G komponensekre bontva. Az értékelés az Ügyfél és az Ügyfél által meghatalmazott Résztvevő Hitelintézetek számára legyen csak megismerhető. Ez nem publikus adat. Ezen előzetes értékelés nem váltja ki a Résztvevő Hitelintézet kockázatkezelése által végzett elemzést.

9.2 Adatelemzést lehetővé tévő megoldások (BI) támogatása, biztosítása.

***

A jelen műszaki leírásban nem definiált fogalmak a tender felhívásban meghatározott jelentéssel bírnak.

A műszaki leírás a tender felhívás elválaszthatatlan részét képezi. A felhívás és a műszaki leírás közötti ellentmondás esetén a jelen műszaki leírás az irányadó.

Budapest, 2025. 07. 02.