

Technikai és biztonsági tájékoztatás

Concorde Értékpapír Zrt.



Tartalomjegyzék

Bevezető.....	3
Internetes weboldalak használata.....	3
Elektronikus elérhetőségek védelme	6
Elektronikus dokumentumok	7
Videókonferencia megoldás.....	8
Teendők technikai és biztonsági problémák és incidensek esetén.....	9

Bevezető

A dokumentum célja, hogy a Concorde Értékpapír Zrt. (továbbiakban Concorde) által publikusan és az ügyfelek részére szolgáltatott informatikai szolgáltatásainak rendszerkövetelményeit meghatározza, valamint a szolgáltatások biztonságos használatáról tájékoztasson. A Concorde a szolgáltatásainak kialakítása során a különböző hatóságok (MNB, NAIH) hatályos ajánlásait és elvárásait vette figyelembe és közvetíti a felhasználók felé.

Felhívjuk a szolgáltatások felhasználóinak figyelmét, hogy a felhasználók felelősége a használt készülékek, eszközök és felhasználói hozzáférések (felhasználói név, jelszó) megfelelő szintű biztonsági védelméről gondoskodni!

Internetes weboldalak használata

A Concorde Értékpapír Zrt (Concorde) az ügyfelek részére az alábbi internetes weboldalakat, alkalmazásokat üzemelteti:

- www.con.hu : Publikus vállalati portál
- www.mycd.hu : Ügyfélportál
- www.con.hu/onlineszamlanyitas/ : Online számlanyitás

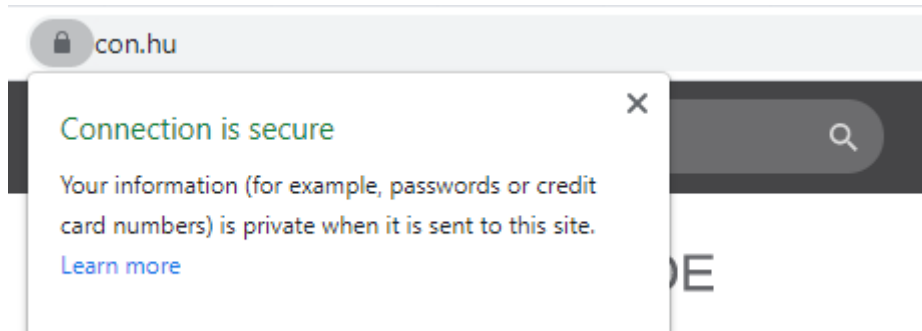
A Concorde internetes weboldalai a legelterjedtebb böngészők használatával tekinthetők meg:

- Chrome
- Edge
- Firefox
- Safari

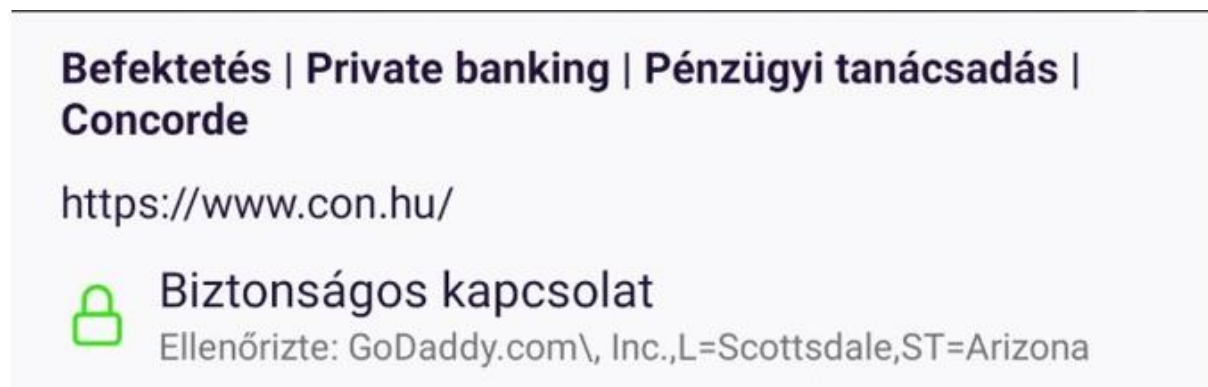
A Concorde a felsorolt internetes böngészőkre optimalizálta weboldalait és alkalmazásait. A weboldalak megtekinthetők a böngésző fejlesztője által támogatott aktuális és azoknak korábbi, de egy évnél nem régebbi verzióival.

Az Ön adatainak biztonságának érdekében és a weboldalak alkalmazások kérjük, hogy használjon a böngésző alkalmazásokból legfrissebb verziót és azoknak frissítéseit, új verzióit rendszeresen telepítse!

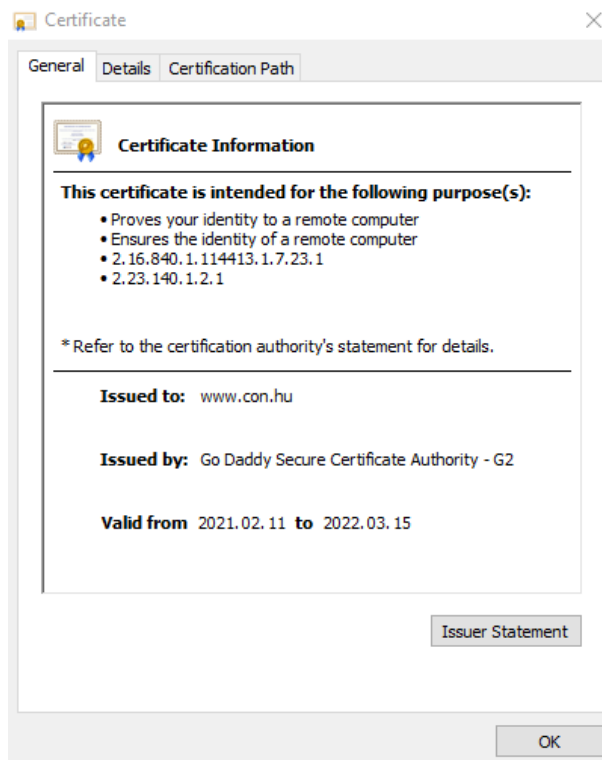
Ön a Concorde weboldalait minden esetben titkosított kommunikációs csatornán keresztül érheti el. Erről úgy győződhet meg, ha az oldal címsora „https” -sel kezdődik, és a weboldal URL -je mellett megjelenik egy lezárt lakat képe, például:



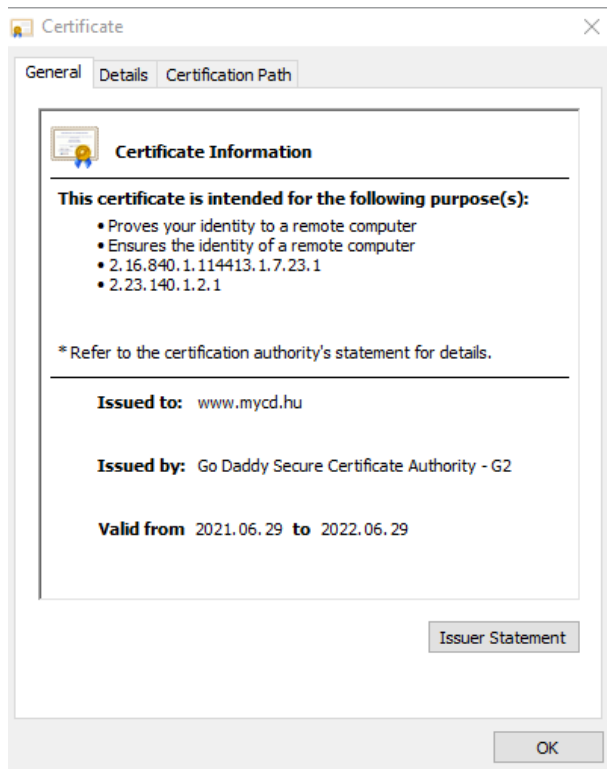
vagy mobil böngésző esetén:



A Concorde a kommunikációs csatorna titkosításához minimum RSA 2048 Bit -es SSL tanúsítványt használ, melyeket hiteles tanúsítvány kiadóktól szerez be (GoDaddy, Sectigo).



www.con.hu SSL tanúsítvány



www.mycd.hu SSL tanúsítvány

A weboldalak (www.con.hu, www.mycd.hu, www.con.hu/onlineszamlanyitas/) megtekintése és használata során kérjük ellenőrizze a tanúsítványok kiállítását (Issued to) valamint azok érvényességét (Valid from, valid to).

Kérjük az internetes böngésző használata során mindig ellenőrizze a titkosított csatorna használatát és a weboldal tanúsítványát!

A Concorde weboldalai az ügyfél eszközein csak minimális mértékben tárolnak adatokat. A weboldalak használata során csak a munkamenet kezeléshez (session) szükséges információk kerülnek (Süti - cookie) rögzítésre. A weboldalak automatikusan megjelenítik ezen információk kezeléséhez szükséges hozzájárulást tartalmazó funkciót. Részletesebb információ a Concorde adatvédelmi tájékoztatójában található:

https://www.con.hu/documents/adatvedelmi_tajekoztato.pdf

A weboldalon cookie-kat használunk, amik segítenek minket a lehető legjobb szolgáltatások nyújtásában. Weboldalunk további használatával jóváhagyja, hogy cookie-kat használjunk.

ELFOGADOM

Kérjük, amennyiben hozzájárul a süti kezeléséhez fogadja el weboldalunkon azok használatát!

Az Ügyfélportál és az Online számlanyitás felület automatikusan, 10 perc inaktivitás után kilépteti a felhasználót az alkalmazásokból. A böngésző bezárása esetén pedig 30 perc inaktivitás után lezárja a munkamenetet. Az Ön biztonsága érdekében az alkalmazásokból minden esetben jelentkezzen ki.

Számítógépét, okostelefonját bekapcsolva ne hagyja őrizetlenül, és a használat felfüggesztésekor vagy befejezésekor lépjen ki az éppen látogatott weboldalról, vagy a használt programból, lehetőleg zárja a képernyőt!

Rendszeresen törölje az internethasználat során keletkező ideiglenes fájlokat (különösen nyilvános helyeken, pl. internetkávézóban), illetve állítsa be böngészőjét ezek automatikus törlésére, tárolásuk tiltására!

Az ügyfélportál hozzáféréshez szükséges jelszavak kezelése során kérjük az alábbi szabályokat minden körülmények között tartsa be:

- A rendszer megköveteli a komplex jelszavak használatát. A jelszó hossza minimum 8 karakter, melyben kis és nagybetűnek és minimum 2 számnak kell szerepelnie.
- Törekedjünk olyan jelszó megadására, mely nem kapcsolható hozzánk
- A szolgáltatás igénybevételéhez használt azonosítót, jelszót ne adjuk meg senkinek
- A jelszavakat csak biztonságos formában tároljuk, például. jelszókezelő alkalmazás segítségével. A felhasználói jelszavakat csak titkosított formában tároljuk
- A Concorde nem ismeri az Ön felhasználói jelszavát, azokat csak titkosított formában tárolja. A Concorde soha nem kéri semmilyen csatornán a felhasználóktól, hogy osszák meg a jelszavakat. Kérjük jelszavát ne ossza meg senkivel!
- Kérjük, hogy a felhasználói jelszót rendszeresen változtassa meg. Amennyiben arról értesül, hogy felhasználói hozzáférést kompromitáltak, akkor haladéktalanul változtassa meg felhasználó jelszavát és jelezze azt a Concorde elérhetőségein.
- Javasoljuk, hogy minden rendszerhez használjon egyedi, generált jelszót. Lehetőleg ne használja különböző rendszerekhez ugyanazt a jelszót, mert így nagyobb a lehetősége a visszaéléseknek.
- Amennyiben elfelejtené jelszavát, lehetősége van új jelszó igénylésére. Az új jelszót a Concorde ügyfélszolgálaton keresztül, telefonon kérheti. Biztonsági okokból kollégánk Önt azonosítani fogja és új, átmeneti hitelesítő jelszót fog küldeni a korábban megadott telefonos elérhetőségére.
- 3 sikertelen bejelentkezési kísérlet után a rendszer átmenetileg 1 órára letiltja a hozzáférést. Amennyiben elfelejtette jelszavát kérjük hívja az ügyfélszolgálatot új jelszó igényléséhez.
- Saját érdekében kérjük, hogy jelszavát ne tárolja internetes böngészőkben!

Elektronikus elérhetőségek védelme

Ügyfeleink személyes elérhetőségeit az online számlanyitási és azonosítási folyamat során ellenőrizzük. Az Ön mobil telefonszámának és email címének felhasználásáról egy egyszer használatos hitelesítő kód küldésének segítségével győződünk meg.

A Concorde kiemelt funkciók végrehajtásához (pl. adatmódosítás) is mobil telefonszámra küldött SMS hitelesítő kód segítségével ellenőrzi az Ön közreműködését csalás és visszaélések megelőzése miatt.

A Concorde biztonsági megfontolásból az elérhetőségek változásáról emailben értesítést küld az Ön részére. Amennyiben nem Ön kezdeményezte a módosítását, kérjük haladéktalanul jelezze ezt a Concorde ügyfélszolgálatának elérhetőségein! Kérjük ellenőrizze, hogy elektronikus levelező rendszere nem kezeli a Concorde által küldött leveleket levélszemétként!

Felhívjuk figyelmét, hogy az ön birtokában lévő személyes eszközök és hozzáférési információk védelme az Ön felelőssége!

Eszközeinek és személyes elérhetőségeinek védelme érdekében kérjük gondoskodjon azok megfelelő védelméről az alábbiak végrehajtásával:

- Ne használjon publikusan elérhető számítógépet és hálózatot
- Eszközeit mindig lássa el jelszavas védelemmel és azokat használat után mindig kapcsolja ki, vagy zárolja le
- Telepítsen eszközeire vírus és kártékony kód elleni védelmet
- Rendszeresen telepítse az eszközein található szoftverek biztonsági frissítéseit
- Használjon eszközei védelmére tűzfal megoldást

Elektronikus dokumentumok

PDF dokumentumok megtekintése és védelme

A Concorde által emailben küldött PDF állományok megnyitását különböző, ingyenesen is elérhető szoftverekkel tudja elolvasni. Javasoljuk az Adobe Reader szoftver használatát, de, alternatív megoldásként a friss verziójú böngészőkben is megtekinthetők a PDF állományok az Acrobat Reader beépülő modul megléte esetén:

- Mozilla Firefox (v52 és újabb verziók)
- Google Chrome (2015. szeptemberi és újabb verziók)
- Apple Safari (v12 és újabb verziók)
- Microsoft Edge

A Concorde által emailben küldött PDF állományok jelszóval védett állapotban kerülnek kiküldésre. Az állományok megnyitásához szükséges jelszóképzési mód is emailben kerül átadásra.

Hash kód, digitális aláírás, időbélyegző

A Concorde által emailben küldött ügyfélszámla szerződéseket tartalmazó PDF állományok digitális aláírással és időbélyeggel vannak ellátva, valamint a dokumentumból generált ún. „hash” kód is átadásra kerül az ügyfél részére az azonosítás után emailben.

Az **időbélyeg** az elektronikus dokumentumhoz végérvényesen hozzárendelt, vagy azzal logikailag összekapcsolt olyan adat, amely igazolja, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában létezett. A dokumentum időbélyegzővel való ellátását a Concorde független külső időbélyegző szolgáltatótól (Microsec, E-SZIGNO) veszi igénybe, mely harmadik fél által is igazolja az adott időpontban létező dokumentum tartalmát.

A **„hash” kód** egy adott beviteli adatból generált egyedi karaktersorozat. Ismert állapotban generálva fájlok hash kulcsát szavatolható, hogy egy esetleges a fájlban történt változás utólag megállapítható, tehát a fájlok integritása ellenőrizhető. Két eltérő nevű, de azonos tartalmú fájl egyezősége megállapítható. A Concorde által készített számlaszerződéstervezetről és a végleges, aláírt szerződésről SHA1 algoritmussal készít „hash” kódot és lenyomatot. A videokonferenciás azonosítás során ezt a kódot kell Önnek visszaolvasnia, hogy igazolható legyen a szerződésre történő hivatkozás. Ön ellenőrizni tudja a lenyomat egyezőségét azt „hash” kód készítésére alkalmas szoftverrel (pl. Total Commander vagy Windows parancssori utasítással: certutil -hashfile <file> SHA1).

A **digitális aláírás** a nyílt kulcsú titkosítású rendszerek egy lehetősége, amellyel a hagyományos aláírást tudjuk helyettesíteni az informatika világában. Igazolni lehet vel az aláíró személyét, és azt, hogy a dokumentum az aláírás óta nem változott meg. A Concorde a digitális aláíráshoz mindig névre szóló, minősített tanúsítványokat használ, melyet publikus tanúsítvány kezelő szolgáltatótól szerez be (Netlock).

Kérjük mindenképpen ellenőrizze az Ön részére átadott ügyfélszámla szerződés tartalmát, valamint annak változatlanóságát a „hash” kód és az időbélyegzők segítségével. Kérjük ellenőrizze azt is, hogy a szerződés megfelelően, digitális tanúsítvánnyal is cégszerűen alá lett írva a Concorde részéről!

Videókonferencia megoldás

Zoom alkalmazás

A regisztrált potenciális ügyfeleit a Concorde egy videokonferenciás egyeztetésen keresztül azonosítja, melyhez a Zoom megoldást (www.zoom.us) használja.

A Zoom alkalmazást az alábbi módokon használhatja:

- Asztali és laptop számítógépen futtatott Zoom kliens alkalmazással
- Okostelefonon futtatott Zoom kliens alkalmazással
- Internet böngészőben futtatott Zoom klienssel (bővebb információ a böngészők használatáról az Internetes böngészők használata fejezetben)

A Zoom kliens a www.zoom.us weboldáról, valamint a mobil alkalmazás áruházakból (Android Play Store, iOS App Store) töltheti le és telepítheti.

A Concorde javasolja, hogy a Zoom alkalmazásokból mindig a legfrissebb verziót használja a kapcsolódáshoz.

Kérjük, hogy az Ön eszközein futó alkalmazásokat csak biztonságos forrásból töltsse le és telepítse, azt a kapcsolódás előtt frissítse. Kérjük, hogy minden esetben vírusirtó szoftver segítségével ellenőrizze a telepített alkalmazást!

Kapcsolódási feltételek

A videókonferencia során végrehajtott ügyfélazonosításhoz és szóbeli szerződéskötéshez a következő feltételek szükségesek az Ön eszközén:

- Legfrissebb verziójú telepített zoom alkalmazás
- Nagyfelbontású (HD) kamera
- Mikrofon
- Hangszóró / fülhallgató

Kapcsolódás Zoom videókonferenciához

Az online szerződéskötés és azonosítás során Ön értesítő email értesítést kap a konferencia kapcsolódási információiról. A levélben küldött linke kattintva, vagy a Zoom alkalmazás indításával a levélben küldött „Meeting Id” és „Passcode” kapcsolódási adatok megadásával.

Kérjük az emailben küldött kapcsolódási információkat ne ossza meg senkivel, azokat ne továbbítsa és gondoskodjon a dokumentumban leírt „Elektronikus elérhetőségek védelme” módon elérhetőségeinek biztonságáról!

Videókonferencia adatok kezelése

A Concorde a Zoom alkalmazás használata során a videófelvételeket törvényi előírások miatt rögzíti és az aktuális jogszabályban meghatározott ideig megőrzi. A videófelvétel rögzítése után a kapcsolódó állományokat a Concorde időbélyegzővel látja el, hogy független harmadik féllel is biztosítsa a rögzített állományok integritását.

A Zoom alkalmazás kapcsolódáskor értesítő üzenetben tájékoztatja a felhasználót a Concorde adatkezeléséről a videóhívás során rögzített adatokról. A videókonferencia elindulása után a Zoom alkalmazás automatikus hang üzenet lejátszásával is tájékoztatja a felhasználót a konferencia rögzítéséről.

Kérjük olvassa el a tájékoztatás és amennyiben egyetért vele, járuljon hozzá azok elfogadásához. A videókonferencia rögzítése és elkezdése csak az Ön hozzájárulása után indul!

Csalások megelőzése

A jelenlegi technológiai megoldások már lehetővé teszik az élőkamerás felvételek hamisítását is, pl. ún. „deepfake” megoldással. A „deepfake” egy olyan algoritmus, amely képes akár valós időben is olyan hamisított videót létrehozni, amelyen a kellő adatmennyiség birtokában, bármilyen tetszőleges személy valóságként megjeleníthető. A Concorde munkatársai, ennek kiszűrése érdekében különböző instrukciókkal láthatják el a videókonferencián részt vevő ügyfelet, amelyek segítségével megfigyelhetik az esetleges „deepfake” algoritmusra utaló jeleket.

Kérjük közreműködésével segítse kollégánkat a lehetséges csalásokat kiszűrő intézkedések végrehajtása során!

Teendők technikai, biztonsági problémák és incidensek esetén

Amennyiben problémát tapasztal, az esetleges csalások és visszaélések megelőzése érdekében kérjük haladéktalanul értesítse ügyfélszolgálatunkat az www.con.hu/kapcsolat/ oldalon található elérhetőségeken.