



Biztonság, követhetőség, egyszerű kapcsolódás – az STH alapelvei

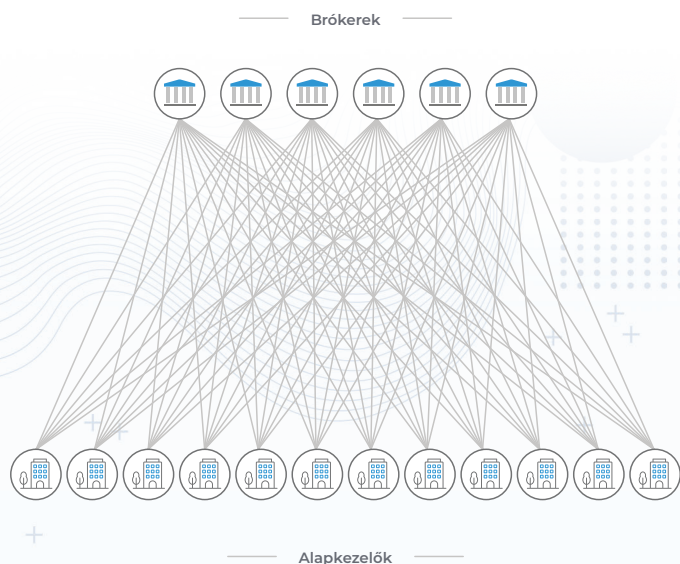
Közeleg a T+1-felkészülés első fontos megfelelési mérföldköve. Az ESMA ütemezése szerint 2026. december 7-től az allokációk és visszaigazolások cseréjében az elektronikus, szabványosított kommunikációs csatornák és a nemzetközi üzenetszabványok alkalmazása válik elvárttá. Az STH készen áll az ehhez szükséges intézményközi kommunikáció támogatására.

Az STH kialakításakor a biztonság, a követhetőség és az üzemeltethetőség egyaránt meghatározó szempont volt. Az alábbiakban kifejtjük azokat az architektúrális és üzleti döntéseket, amelyekkel az STH támogatja a piaci szereplők T+1-re való átállását.

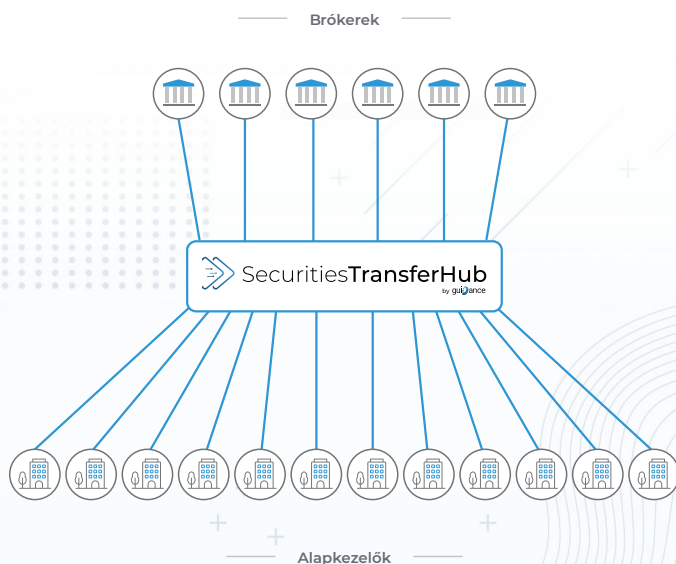
Közös kapcsolódási modell az STH-val

Az STH-val az intézmény egyszer csatlakozik a szolgáltatáshoz, és ezen keresztül éri el a már csatlakozott partnereket. Nem szükséges minden partnerkapcsolathoz külön technológiai és üzemeltetési megoldást fenntartania.

Partnerenkénti kapcsolatok



STH-kapcsolódási modell



A szolgáltatás a kapcsolódás mellett központi naplózást, visszaigazolást, monitoringot, riasztási rendszert, előre meghatározott és egységes csatlakozási folyamatot és szakmai támogatást nyújt.

Szempont	Partnerenkénti kapcsolatok	STH-kapcsolódási modell
Kapcsolódás	Minden partnerrel külön-külön	Egy kapcsolódás az STH-hoz
Szolgáltatás kiajánlás	Szükséges, minden partner számára, akár különböző módokon	Nem szükséges, minden partner kliensként kapcsolódik az STH-hoz
Működési szabályok	Partnerenként kialakítva, akár eltérő módokon, akár eltérő felületeken	Közös kapcsolódási modell, egy felhasználói felületen
Naplózás és státuszok	Több rendszerben kezelve	Központilag követhetők
Új partner csatlakozása	Újabb egyedi kialakítás	A meglévő modell újrahasználható
Támogatás	Résztvevőnként szervezett	Központi szolgáltatói támogatás
Költségszerkezet	Partnerenként felmerülő bevezetési és üzemeltetési költségek	Kiszámítható szolgáltatási díj

Az STH értéke tehát nem egy újabb adatátviteli technológiában rejlik. A kommunikációt közösen használt, támogatott szolgáltatássá alakítja, amelyben a résztvevők azonos kapcsolódási és működési szabályokat alkalmazhatnak.

Az adatátvitel csak az első lépés – az SFTP-kapcsolat határai

A felkészülés során több intézmény számára az SFTP tűnhet a leggyorsabban megvalósítható alternatívának. Széles körben ismert, kiforrott technológiáról van szó, használatához pedig a legtöbb pénzügyi intézménynél rendelkezésre áll a szükséges szakértelem. Egy korszerű, a DORA és az MNB informatikai biztonsági elvárásaihoz illeszkedő SFTP-kapcsolat kialakítása azonban már nem feltétlenül egyszerű feladat.

Egy ilyen kapcsolatnál a kockázatokkal arányos technikai és szervezési kontrollokat is ki kell alakítani. Ide tartozhatnak a korszerű titkosítási algoritmusok, a biztonságosan kezelt SSH-kulcspárok és szükség esetén egy további hitelesítési faktor, az IP-alapú hozzáférés-korlátozás, a kulcsok életciklus-kezelése, a naplózás és monitorozás, valamint az állományok integritásának ellenőrzőösszeggel (checksum) történő igazolása. Mindezek kialakítása és folyamatos működtetése jelentős informatikai adminisztrációval járhat, a felhasználói oldalon pedig kerülőmegoldásokhoz vezethet.

Az SFTP adatátviteli technológiaként önmagában a fájl biztonságos továbbítását biztosítja. A technikai naplókban - megfelelő üzemeltetési hozzáféréssel és szakértelemmel - megállapítható, hogy az átvitel sikeres volt-e. Az azonban nem feltétlenül derül ki, hogy a fogadó fél feldolgozta-e az állományt, miért utasította el, vagy szükség van-e beavatkozásra. Az érkező üzenetek észlelése, a feldolgozási státuszok és hibák követése, a visszaigazolások kezelése, valamint a szervezeten belüli jogosultságkezelés külön megoldást igényel. Egy szervezetek közötti SFTP-kapcsolat ezeket üzleti folyamatszinten nem biztosítja.

A hiányzó funkciók természetesen egyedi fejlesztésekkel, scriptekkel és kiegészítő alkalmazásokkal pótolhatók. Ebben az esetben azonban minden partnerkapcsolatot meg kell tervezni, fejleszteni, tesztelni és később üzemeltetni. Az SFTP-re épülő megoldás így könnyen elveszítheti azt az előnyét, hogy gyorsan és alacsony költséggel vezethető be.

Modern API-k az adatátvitelben – szinkron vagy aszinkron?

Az STH üzenetküldési és -lekérdezési interfészét platform- és programozási nyelvtől független [OpenAPI-specifikációk](#) írják le. Ezek egyértelműen rögzítik a végpontokat, az adatstruktúrákat, a biztonsági követelményeket és a lehetséges válaszokat.

Az STH tervezésekor a webhook jellegű push API-t, a Server-Sent Events (SSE) technológiát, a WebSocket-et és a long pollingot is megvizsgáltuk, mint a piacon előforduló technológiai megoldásokat.

A webhook jellegű push API minden résztvevőnél folyamatosan elérhető, védett fogadó végpontot igényelne. Az SSE és a WebSocket ezzel szemben kliens által kezdeményezett, tartós kapcsolatot használ: az SSE egyirányú szerver–kliens eseményfolyamra, a WebSocket kétirányú, valós idejű kommunikációra alkalmas. Ezek elsősorban sűrű eseményforgalomnál előnyösek. Az STH elkülönülő, aszinkron üzleti üzeneteinél azonban a megbízható várakoztatás, a kézbesítés követhetősége és a feldolgozás visszaigazolvatósága fontosabb a folyamatos, valós idejű kapcsolatnál. A tartós kapcsolatok emellett külön újracsatlakozási, proxy-, tűzfal- és skálázási kezelést igényelnek.

Ezek alapján az STH a long polling mellett döntött. A kliens mTLS-sel hitelesített HTTPS-kérést indít, amely üzenet érkezésekor azonnal, egyébként a beállított időkorlát elérésekor tér vissza. A még át nem vett üzenetek az STH szerveroldali várólistáján maradnak, így a címzett átmeneti kiesése alatt is később lekérhető. Az üzenet metaadatai és az életciklus-státuszok alapján a megszakadások, az ismételt lekérdezések és az ellenőrzött újraküldések követhetők.

Szempont	WebSocket	SSE	Long-polling
Elsődleges felhasználás	Gyakori, valós idejű interakció	Folyamatos esemény- vagy adatfolyam	Elkülönülő, aszinkron üzenetek
Vállalati hálózati illeszthetőség	Extra proxy- és tűzfalkonfigurációt igényelhet	A hosszú kapcsolatot köztes eszközök megszakíthatják vagy pufferelehetik	Szabványos HTTPS-forgalomként egyszerűbben kezelhető
Küldés és visszaigazolás	Egy csatornán megoldható, de egyedi üzenetprotokoll szükséges	A küldéshez és visszaigazolóshoz külön API kell	Egységes REST API-n keresztül kezelhető
Üzenetek várakoztatása	Külön szerveroldali várólista szükséges	Külön eseménytárolási és visszajátszási logika szükséges	Tökéletesen illeszthető központi szerveroldali várólistához
Átmeneti klienskiesés	Újracsatlakozási és visszajátszási logikát igényel	Automatikusan újracsatlakozhat, de az üzleti események pótlását külön kell kezelni	A kliens a következő lekérdezéskor átveheti a várakozó üzeneteket
Illeszkedés az üzleti use-case-hez	A szükségesnél összetettebb kapcsolati modell	Az egyirányúság és a tartós kapcsolat miatt kevésbé megfelelő	Jól támogatja a várakoztatást, az ismételt fogadást és a követhető kézbesítést

Az STH, mint működési modell

Az STH kialakítása összefoglalva nem egyszerűen egy adatátviteli technológia kiválasztásáról szolt. A biztonságos REST API, az aszinkron üzenetkezelés, a szerveroldali várakoztatás, az életciklus-státuszok és a központi kapcsolódási modell együtt teszik lehetővé a megbízható és követhető intézményközi kommunikációt.

Ezek a döntések azt szolgálják, hogy a csatlakozó intézményeknek ne partnerenként kelljen kialakítaniuk ugyanazokat a biztonsági, hibakezelési és üzemeltetési megoldásokat.

Az STH így nemcsak a közelgő megfelelési mérföldkőre való felkészülést támogatja, hanem hosszabb távon is egységes alapot kínál az értékpapírpiazi szereplők közötti kommunikációhoz.

TOVÁBBI INFORMÁCIÓ ÉS CSATLAKOZÁSI DOKUMENTÁCIÓ: [STHSERVICE.EU](https://sthservice.eu)



SecuritiesTransferHub

by guidance