

## **E mail titkosítás az üzleti életben ma már követelmény!**

### **Ön szerint ki tudja elolvasni bizalmas email leveleinket?**

Egy email szövegében elhelyezett információ annyira biztonságos, mintha ugyanazt az információt nyílt postai levelezőlapra adnánk fel.

A ma elterjedt titkosítási megoldások bevezetése a levelezőpartnerek nagy száma esetén azonban bonyolult, sok munkaórát és jelentős anyagi ráfordítást igényel. A külső partnerek mindegyikének képesnek kéne lennie arra, hogy a titkosítást feloldó nyilvános kulcsokat kezelni tudja. A titkosítást feloldó szoftvert pedig minden partnerhez el kellene juttatni, ami igen nehézkes, sok esetben nem is lehetséges.

### **A megoldandó feladat**

Biztonságos email kommunikációt szeretnénk tehát folytatni bármely partnerünkkel anélkül, hogy a nekik külön titkosító szoftvert kellene telepíteniük és a titkosítással bármely egyéb módon bajlódniuk.

Az adatok biztonsága és hozzáférhetetlensége, az adatvédelemmel kapcsolatos jogi előírások és az ipari kémkedés elleni védekezés miatt ugyanakkor nélkülözhetetlen valamilyen titkosító megoldás használata.

Ennek megfelelően a feladat tehát a következő:

- Titkosított email-ek kiküldése a vállalati levelező rendszerből úgy történjen, hogy azok elolvasásához a címzett
  - gépén ne kelljen hardvert telepítenie
  - gépén ne kelljen szoftvert telepítenie
  - ne bajlódjon a kulcsok kezelésével
  - a kiküldött titkosított levél a felhasználó postafiókjában tárolódjon
  - egy egyszerű webmail szolgáltatáshoz elegendő tudással kezelni tudja a titkosított leveleit is
  
- Válaszok fogadása biztonságos csatornán történik
  - automatikusan használható biztonságos válaszcsatorna biztosítása, hogy a címzetteknek ne kelljen a válaszok biztonságával foglalkozni u
  - ugyancsak egyszerű kezeléssel

## A megoldás !

A Group Technologies iQ.Suite megoldásának WebCrypt modulja egyszerű és megbízható módszert nyújt az ügyfelekkel és az üzleti partnerekkel való email kommunikációra. Az iQ.Suite a Crypt modul kiegészítőjeként telepítendő. Gyorsan és zökkenőmentesen integrálódik a levelezőrendszerbe és anélkül teszi lehetővé a titkosított emailek azonnali kölcsönös küldését és fogadását, hogy a külső partnernek hardver vagy szoftvereszközt kellene telepítenie. A titkosított emailek ehelyett a WebCrypt portál egy biztonságos portján keresztül regisztrálódnak.



## Hogyan működik?

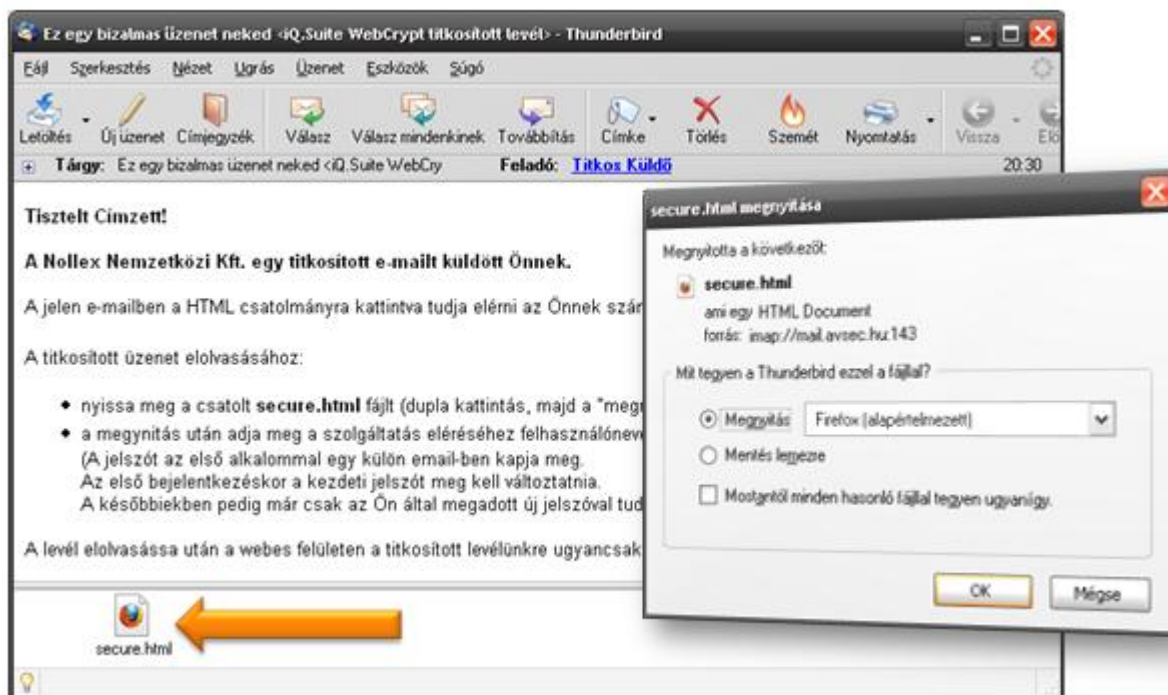
A felhasználó a szokásos módon elküldi a titkosított emailt. A címzett egy szokványos emailt kap, amelybe csatolt állományként van beillesztve a teljesen titkosított üzenet. Ezt bármikor megnyithatja és megtekintheti a küldő WebCrypt portálján keresztül, amelyhez csak egy felhasználói névre és jelszóra van szüksége. A biztonság érdekében a címzettek bármikor, gond nélkül megváltoztathatják saját jelszavukat.

A titkosított melléletek elmentésére és titkosított válasz küldésére természetesen szintén lehetőség van. Mivel minden tartalom a címzettnél marad és nincs elmentve a küldő WebCrypt szerverén, ezért:

- a rendszer tehát NEM az ingyenes levelezőportálokhoz hasonlóan működik, ahol ha a jelszót ellopják, elolvashatják az online tárolt (titkos) levelezést

- a küldő részéről tárhely probléma nem merül fel, hiszen minden titkosított levelet a címzettek tárolnak
- a címzett mindig bizonyos lehet, hogy titkosított levelét csakis ő tudja megnyitni

## A titkosított e mail bármely e mail klienssel olvasható!



## Hol, mire használhatjuk a titkosított emailek kiküldését?

A titkosított email leveleket számos területen használhatjuk. Gondoljon csak arra, hova küldenek ki manapság bizalmas információkat postai levélben, vagy kikkel szeretne bizalmasan levelezni a jövőben, stb.

Néhány gondolatébresztő példa az eddigi tapasztalatainkból:

- elektronikus **bérjegyzék** kiküldése a saját dolgozók számára
- elektronikus **számlalevelek, értesítők** kiküldése
- bizalmas **árlisták, árajánlatok, szerződések** kiküldése ügyfelek, partnerek felé
- bizalmas **megrendelések** fogadása, elküldése
- stb.

## Milyen előnyökhöz jutunk a titkosított email levelek használatával?

A titkosított email levelek használatának számos előnye adódik, többek között:

- **bárminek** (akinek tudja az email címét) küldhet titkos levelet
- titkos csatornán keresztül kapja meg a **válaszokat is**
- csakis a címzett tudja elolvasni az üzenetet, **még a rendszergazdája sem!**
- **óriási költségcsökkentést eredményez** a postai levelezést kiváltva
- titkosított levél kiküldéséhez **nem kell bonyolult műveleteket megtanulni** elvégezni - sőt, gyakorlatilag elegendő akár csak a levél tárgyába beírni egy adott kulcsszót, pl: **<titkosan>**, és a levél titkosítva megy a címzettnek
- a bizalmas levelek **automatikusan titkosítódnak** akár tartalmuk alapján is: a rendszer képes figyelni a kimenő levelek tartalmait (címzett, szöveg, csatolmány típusa és/vagy tartalma, szövege), és adott címzett, tartalom, vagy egyéb email jellemző találat esetén automatikusan titkosítva küldi ki a levelet

## Az iQ.Suite WebCrypt email titkosító rendszer szolgáltatásai, további előnyök

- A szellemi tulajdon és a bizalmas adatok védelme, ugyanakkor a kommunikáció hatékonyságának növelése
- Biztonságos email forgalom PGP, S/MIME vagy PKI struktúrák nélkül
- A külső partnernek nem kell hardver vagy szoftvereszközt telepítenie
- Azonnali titkosított levélküldési és fogadási lehetőség bármely partnerrel Korlátlan nyelvi támogatás (felhasználó szintű nyelvválasztás)
- Gyors és zökkenőmentes integráció az intézményi hálózattal és az iQ.Suite Crypttel Komplex, szabály alapú titkosítási lehetőségek
- A rendszergazda sem tudja elolvasni a titkosított leveleket
- Nincs szükség a levelezési útvonal megváltoztatására
- A titkosítási előírások központi meghatározása
- Központosított, integrált és automatikus felhasználó kezelés
- Kényelmesen használható web portál, az intézményi arculathoz szabható kezelői felülettel és biztonságos hozzáféréssel
- Többszintű menedzsment-jogosultság kezelés
- HelpDesk támogatói funkciók
- A terhelés változásával összhangban jól skálázható architektúra (HEAD + NODE szerverek)
- A titkosan kiküldött levelek a címzettnél tárolódnak
- A titkosításhoz használt személyes kulcsok a cég adatbázis-szerverén, biztonságban tárolódnak

## Hardware és software követelmények

### Támogatott levelező szerverek

Gyakorlatilag bármely levelező rendszerhez hozzákapszolható, így például az alábbiakhoz is:

MS Exchange, IBM Lotus Domino, SMTP

### Támogatott email kliensek

Gyakorlatilag bármely email klienssel vagy webes email szolgáltatással\* használható, így például az alábbiakkal is:

- bármely POP3/SMTP kliens
- bármely IMAP kliens
- Microsoft Outlook, Mail, Outlook Express
- Lotus Notes
- Webes kliensek (pl. freemail.hu, citromail.hu)

\* tekintve sokszínűségüket, a webes email szolgáltatások nem kerültek teljes körűen tesztelésre

**Ha biztonságban akarja tudni e mailjeit, adatait használja az iQ.Suite WebCrypt email titkosító rendszert!**

**Hívja tanácsadónkat!**