

Meghívó előzetes piaci konzultációra

a KIFÜ QKD eszközök és adathálózati aktív eszközök beszerzésére irányuló
közbizottsági eljárásaihoz

1 Ajánlatkérő adatai

Hivatalos név: Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ)

Postai cím: 1134 Budapest, Váci út 35.

Kapcsolattartó neve: dr. Kepes Eszter, beszerzési referens

Telefon: +36 30 149 3193

e-mail: kozbeszerzes@kifu.gov.hu

2 A konzultáció célja:

Jelen konzultáció tárgya:

- közbizottsági eljárás előkészítése, a piaci lehetőségek felmérése, megismerése;
- a résztvevő gazdasági szereplők előzetes tájékoztatása a fentiekben megjelölt tárgyban megindítani tervezett közbizottság kapcsán az ajánlatkérői elvárásokról, a műszaki leírás tervezett tartalmáról, a beszerzés céljáról és körülményeiről;
- valamint a lefolytatni tervezett közbizottsági eljárás becsült értékének megállapítása.

Minden a konzultáción résztvevő gazdasági szereplő kérdéseket intézhet és javaslatokat tehet a műszaki tartalom racionalizálása, pontosítása körében. Az érdeklődő gazdasági szereplők a konzultációt megelőzően a konzultáció menetére vonatkozó szabályok szerint intézhetnek kérdéseket.

3 A tervezett beszerzés:

A KIFÜ, mint ajánlatkérő a QCIHungary projekt keretében QKD és azokkal együttműködő adathálózati aktív eszközöket tervez beszerezni. Ajánlatkérő célja a beszerzendő eszközökkel több olyan pont-pont adatkommunikációs összeköttetés kiépítése, melynek végpontjain az adathálózati aktív eszközök végzik az adatok titkosító kódolását és dekódolását szimmetrikus kulcsú algoritmusokkal, amihez a QKD (Quantum Key Distribution) berendezések által szolgáltatott titkosító kulcsokat használják.

3.1 Adatkommunikációs összeköttetések

Az adatkommunikációs összeköttetések közt Magyarországon belüli vidéki, valamint Budapesten belüli viszonylatok szerepelnek:

- Budapest – Győr
- Budapest – Szeged ill. Budapest – Nagykanizsa (ugyanazon QKD készülékekkel, egyszerre csak az egyik működik majd)
- Budapest KIFÜ Victor Hugo u. adatközpont (XIII. kerület) – KIFÜ Wigner FK adatközpont (XII. kerület, Csillebérc)
- BME campuson belül (két épület közt)

- ELTE campuson belül (két épület közt)

A fenti adatkapcsolati összeköttetések közül Ajánlatkérő négyhez tervez beszerezni titkosító eszközpárt.

3.1.1 Vidéki összeköttetések paraméterei

Budapest – Győr

Szakasz	Hossz [km]	Becsült csillapítás @ 1550 nm [dB]
Budapest – BG1	48	14
BG1 – BG2	28	8
BG2 – Győr	73	20

Budapest – Szeged

Szakasz	Hossz [km]	Becsült csillapítás @ 1550 nm [dB]
Budapest – BS1	76	21
BS1 – BS2	56	15
BS2 – BS3	28	8
BS3 – Szeged	68	19

Budapest – Nagykanizsa

Szakasz	Hossz [km]	Becsült csillapítás @ 1550 nm [dB]
Budapest – BN1	43	11
BN1 – BN2	61	17
BN2 – BN3	64	18
BN3 – BN4	56	16
BN4 – BN5	32	9
BN5 – Nagykanizsa	63	18

3.2 Ajánlatkérő elvárásai a szállítandó eszközökkel szemben

Az itt megfogalmazott előzetes elvárások nem az ajánlatkérés követelményei, hanem a piackutatás tárgykörének behatárolását szolgálják. Az ajánlatkérés követelményeit – többek közt – a jelen piackutatás eredményei alapján fogja ajánlatkérő specifikálni.

3.2.1 Minden termékcsoportra érvényes elvárások

- kereskedelmi forgalomban kapható, sorozatgyártású termékek
 - dokumentációval
 - gyártói támogatással
- a készülékek szabványos 19 hüvelykes távközlési rack keretbe szerelhetők

3.2.2 QKD eszközök

- a QKD rendszer által biztosított kulcsbitsorozat véletlenszerű, erről maga a QKD rendszer gondoskodik, külső forrás használata nélkül
- a kulcsok kiosztása során a kvantumfizikai jellemzőben hordozott információt távközlési (ITU-T G.652) fényvezető szálon továbbítják
- ha az adatkommunikációs végpontok túl távol vannak egymástól, akkor több QKD készülékpár sorba köthető, és az így felépülő QKD rendszer az egyes szakaszokon működő készülékpárok

által szolgáltatott kulcsbitsorozatból származtatja az adatkommunikációs végpontokon kiadandó kulcsbitsorozatot

3.2.3 Titkosító kódolók

- távközlő adathálózat forgalmát titkosítják és fejtik vissza az összeköttetés végpontjain
- olyan szimmetrikus kulcsú titkosító algoritmust használnak, ami a jelenlegi tudományos ismeretek szerint kvantumszámítógép használatával sem kriptóanalizálható sikeresen
- IPsec protokoll szerint kódolják és dekódolják az IP csomagokat, vagy MACsec protokoll szerint kódolják és dekódolják az Ethernet kereteket, vagy egyéb módon kódolják és dekódolják az Ethernet ill. az OSI rétegmodellben az alatti adatfolyamot
 - ajánlatkérő mindháromból tervez beszerezni egy-egy eszközpárt
- a titkosító algoritmus kulcsát a QKD rendszertől az összeköttetés két végpontján kapott azonos véletlen bitsorozatból származtatják

3.3 Ajánlatkérő által megismerni kívánt információk

3.3.1 QKD eszközök

Kérjük, röviden mutassa be a fenti célokra javasolt QKD eszközöket, azok fő műszaki jellemzőit!

Hogyan történik a véletlen bitsorozat generálása?

Mi a kulcsok megosztásának, ill. a fizikai paramétereiből való származtatásának módja?

Képes-e a QKD eszközpár olyan fényvezető szálon működni, amin más, szabványos adatátvitel (Ethernet vagy WDM) is zajlik egyidejűleg? Ha igen, akkor ez hogyan befolyásolja a QKD működését?

Mekkora intenzitással képes egy QKD eszközpár kulcsokat szolgáltatni? Milyen jellemzők, körülmények korlátozzák ezt?

Hogyan lehet több QKD eszközpárt egymással sorban összekapcsolni a nagyobb hatótávolság elérése céljából? Ehhez szükségesek-e további eszközök? Mik a köztes csomópontokra vonatkozó feltételek?

Mi a kulcsbitsorozat származtatásának módja sorba kötött QKD eszközpárokból álló rendszer esetén?

Befolyásolja-e – és ha igen, akkor hogyan – a QKD eszközpárok sorba kötése a rendszer által szolgáltatott kulcsbitsorozat intenzitását?

Milyen intézkedéseket alkalmaz a QKD rendszer az illetéktelen hozzáférés detektálására, megakadályozására?

Kérjük, mutassa be a rendszer ETSI (vagy más) szabványoknak megfelelő interfészeit!

Milyen felületen szolgáltatja a QKD rendszer a kulcsbitsorozatokat? Mik az interfész ill. protokoll fő jellemzői?

Milyen adathálózati titkosító eszközökkel tud együttműködni, különös tekintettel az előző fejezetben említett 3 csoportba sorolható titkosítókra? Melyiknek milyen interfészen képes a kulcsbitsorozatokat átadni? Melyik ETSI szabványnak felel meg az együttműködés?

Milyen felületen, milyen módon lehet a rendszer elemeit beállítani, vezérelni?

Milyen felületen, hogyan lehet a rendszer működési paramétereit, állapotát, a benne történt eseményeket lekérdezni?

3.3.2 Titkosító kódolók

Kérjük, röviden mutassa be a fenti célokra javasolt adathálózati titkosító kódolókat, azok fő műszaki jellemzőit!

Milyen felületen képes a kódoló QKD rendszertől titkosító kulcsbitsorozatokat átvenni? Mik az interfész ill. protokoll fő jellemzői?

Melyik gyártók QKD eszközeivel tud együttműködni? Melyiktől milyen interfészen képes a kulcsbitsorozatokat átvenni? Melyik ETSI szabványnak felel meg az együttműködés?

Hogyan történik a QKD rendszertől kapott titkosító kulcsok felhasználása?

Milyen felületen, milyen módon lehet a rendszer elemeit beállítani, vezérelni?

Milyen felületen, hogyan lehet a rendszer működési paramétereit, állapotát, a benne történt eseményeket lekérdezni?

4 A konzultáció menete:

A konzultáció helyszíne: Ajánlatkérő székhelye, 1134 Budapest, Váci út 35., azonban Ajánlatkérő lehetőséget biztosít az online jelenlétre is.

Tájékoztatjuk a gazdasági szereplőket, hogy az előzetes piaci konzultáción történő részvétel regisztrációhoz kötött. A konzultáción kizárólag az érdeklődésüket a megjelölt határidő lejártáig jelző, és ennek folytán az Ajánlatkérő által regisztrált gazdasági szereplők által megjelölt személyek vehetnek részt.

A konzultáción történő részvételi szándékukat az érdekelt gazdasági szereplők 2023. május 19. napján 14:00 óráig a kobzeszerzes@kifu.gov.hu elektronikus levélcímen tudják jelezni, az alábbi információk megadásával:

- gazdasági szereplő neve;
- gazdasági szereplő címe;
- gazdasági szereplő e-mail címe;
- gazdasági szereplő képviselőjében a konzultáción résztvevő személyek neve.

Ezen időpontig az érdeklődő gazdasági szereplőknek lehetőségük van továbbá a fent megjelölt címre a tervezett beszerzés, valamint a műszaki leírás vonatkozásában kérdéseket feltenni. A regisztrációs időpontig feltett kérdéseket Ajánlatkérő a konzultációk keretében válaszolja meg, azonban a feltett kérdések és az arra adott válaszok tartalmát minden érdeklődő megismerheti a konzultációt követően készített jegyzőkönyv részeként.

A piaci konzultáció pontos időbeosztásáról Ajánlatkérő a regisztráció határidejének lejártát követően fogja tájékoztatni az érdeklődőket. Ajánlatkérő a gazdasági szereplőkkel külön-külön kíván konzultációt tartani. **Az érintett gazdasági szereplőkkel történő konzultáció sorrendje a részvételi szándék jelzésének sorrendje szerint történik.**

Ajánlatkérő előzetes szándékai szerint egy konzultációs fordulót kíván tartani, de fenntartja magának a jogot, hogy a szükség esetén újabb konzultációs forduló(ka)t tartson.

Az újabb konzultációs forduló(k) megtartásáról az Ajánlatkérő egyrészt a részvételi szándékukat jelző gazdasági szereplőket közvetlenül értesíteni fogja, másrészt az esetleges újabb forduló(ók)ról a honlapján közleményt fog közzétenni.

A piaci konzultációról jegyzőkönyv készül, amelyeket a konzultációt követően a meghívó közzétételével azonos felületen közvetlenül, térítésmentesen, elektronikusan bárki számára elérhetővé tesz Ajánlatkérő, továbbá közvetlenül is megküldi a konzultáción résztvevőknek.

Ajánlatkérő a jegyzőkönyvek pontossága érdekében a konzultáción hangfelvételt kíván rögzíteni..

Fentiekre is tekintettel, Ajánlatkérő kéri Gazdasági Szereplőket, hogy a konzultáción nyilatkozattételre jogosult (cégképviselőre jogosult vagy megbízott) személyek jelenlétének biztosítására törekedni szíveskedjenek.

Keltezés elektronikus aláírás szerint.

Tisztelettel,

Dr. Spaller Endre
elnök