Verejná konzultácia

k návrhu výzvy na predloženie ponúk do výberového konania na vydanie individuálnych povolení na používanie frekvencií z frekvenčného pásma 3,6 GHz formou elektronickej aukcie.

Údaje o respondentovi

Názov / meno:

Huawei Technologies (Slovak), s.r.o.

Adresa:

Einsteinova 23, 851 01 Bratislava
Sky Park Offices, Bottova7939/2A, 811 09 Bratislava

Kontaktná osoba:

Cui Yu

Štát:

Slovenská Republika

Tel.: +421 907 606 668 ***Fax.:***

e-mail:

cuiyu@huawei.com

Odpoveď na verejnú konzultáciu k návrhu výzvy na predloženie ponúk do výberového konania na vydanie individuálnych povolení na používanie frekvencií z frekvenčného pásma 3,6 GHz formou elektronickej aukcie.

Spoločnosť Huawei je poctená príležitosťou vyjadriť sa k tejto dôležitej konzultácii k budúcej dostupnosti a pridelení spektra. Dúfame, že naše odporúčania podporia základ jasného regulačného rámca pre výberové konanie pre pridelenie spektra.

Nakoľko istá časť odbornej verejnosti môže preferovať čítanie odpovedí v Anglickom jazyku, ponechali sme ju v texte nižšie. V každom prípade je však Slovenská jazyková varianta tou, ktorá je za našu stranu záväznou pre túto verejnú konzultáciu.

Huawei welcomes the opportunity to comment on this important consultation on the future spectrum availability and assignment. We hope the remarks in this reply will support a definition of a clear regulatory framework for an assignment procedure.

Because some part of the professional community might prefer to read the answers in English language, we have kept them for reference – in any case, the Slovak language version prevails.

V bode “4 Výberové konanie” je okrem iného uvedený ako cieľ výberového konania zabezpečenie požadovanej kvality služieb a podpory inovácií. Veríme, že na dosiahnutie tohto cieľa je potrebné okrem iného dosiahliadnuť aj na primeranú bezpečnosť siete pracujúcej na ponúkanom frekvenčnom pásme.

Z tohto dôvodu navrhujeme pod bod 5.1 – Podmienky pridelenia frekvencií doplniť nasledové požiadavky, ktoré navrhujeme doplniť i do jednotlivých individuálnych povolení:

Besides other objectives, point "4 Selection procedure" defines the goal to ensure the required quality of service and to promote innovation. We believe that, in order to achieve this objective, it is also necessary, to take in to consideration and to ensure the adequate security of the networks operation under the offered frequency bands.

Due to this reason, we propose to add additional requirements as listed below under point 5.1 – Conditions for the allocation of frequencies. We propose to include these requirements also in to individual authorisations issued to each operator for the auctioned frequency bands.

1. S cieľom zabezpečiť primeranú úroveň zabezpečenia 5G sietí musia prevádzkovatelia takýchto sietí predložiť dôkaz o vhodnom zabezpečení siete, predložením príslušných správ z auditov tretích strán, ktoré potvrdzujú súlad so súčasnými verziami medzinárodne uznávanej normy. Tieto správy sa musia predložiť prvýkrát do [dátum – odporúča sa od 01. 09. 2025] a potom v pravidelných intervaloch nie dlhších ako dva roky. Rozsah auditovaných bezpečnostných opatrení musí zahŕňať aspoň nasledovné oblasti: návrh siete 5G, jej prevádzku, údržbu a riešenie problémov, riadenie prístupu, riadenie rizík v dodávateľskom reťazci, ako aj bezpečnosť vývoja a životného cyklu sieťových prvkov 5G implementovaných v sieti prevádzkovateľa (vrátane bezpečného návrhu, systém riadenia verzií, sledovanie zmien, audit zdrojového kódu, bezpečnostné testovanie, vzdelávanie zamestnancov, proces nápravy zraniteľnosti, nezávislosť jednotlivých bezpečnostných záplat, riadenie bezpečnosti informácií, automatizovaný proces zostavenia (komplilovania), kontrolované prostredie pre zostavenie softvéru, manažment informácií o zraniteľnostiach, ochrana integrity softvéru, unikátny identifikátor vydaného / uvoľneného softvéru, informácie o bezpečnostných opravách, presnosť dokumentácie, kontakt k otázkam bezpečnosti, správa zdrojového kódu, neustále zlepšovanie, bezpečnostná dokumentácia) bez ohľadu na to, či tieto funkcie vykonáva prevádzkovateľ alebo dodávateľ prevádzkovateľa. Akýkoľvek nesúlad s požiadavkami uvedených noriem sa musí odôvodniť.

1. *In order to ensure an appropriate level of security for 5G networks, operators of such networks must provide evidence of network security management maturity, by submitting appropriate reports from third-party audits attesting conformity to the current versions of an internationally recognized standard. The evidence must be provided for the first time by [date – recommended as of 01.09.2025.] and thereafter at regular intervals of no more than two years. The scope of the audited security measures must include at least 5G network design, operation, maintenance and troubleshooting, access control, supply chain risk management as well as development and lifecycle security for 5G network elements implemented in the operator’s network (including security by design, version control system, change tracking, source code review, security testing, staff education, vulnerability remedy process, vulnerability remedy independence, information security management, automated build process, build environment control, vulnerability information management, software integrity protection, unique software release identifier, security fix communication, documentation accuracy, security point of contact, source code governance, continuous improvement, security documentation), regardless if these functions are conducted by the operator, or operator’s supplier. Any non-conformity with a requirement from the aforementioned standards must be justified.*

2. Okrem toho prevádzkovatelia takýchto sietí musia spĺňať štandardy uvedené v Prílohe číslo 1 a musia po prvýkrát predložiť vyhlásenie o zhode spolu s dokumentmi dokazujúcimo zhodu do [dátum– odporúča sa od 01. 09. 2025] a potom pravidelne predkladať vyhlásenie o zhode v intervaloch nie dlhších ako dva roky. Každý nesúlad s voliteľnými ustanoveniami noriem uvedených v dodatku musí byť v každom prípade odôvodnený.

2. *Additionally, operators of such networks must comply with the standards listed in Appendix 1 and need to submit a declaration of conformity together with evidence of conformity for the first time by [date - recommended as of 01.09.2025] and thereafter at regular intervals of no more than two years. Any non-conformity with optional provisions of the standards listed in the appendix must be justified in each case.*

3. Dôkaz o zhode opísaný v bodoch 1 a 2 sa môže poskytnúť vo forme osvedčení vydaných v súlade s príslušným európskym certifikačným systémom podľa nariadenia (EÚ) 2019/881 (zákon o kybernetickej bezpečnosti).

3. *The evidence of conformity as described in points 1 and 2 can be provided in the form of certificates issued in accordance with appropriate European certification scheme pursuant to Regulation (EU) 2019/881 (Cybersecurity Act).*

Príloha 1 / Appendix 1:

3GPP TS 33.116, Security Assurance Specification (SCAS) for the MME network product class
3GPP TS 33.117, Catalogue of general security assurance requirements
3GPP TS 33.216, Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
3GPP TS 33.250, Security assurance specification for the PGW network product class
3GPP TS 33.511, Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
3GPP TS 33.512, 5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
3GPP TS 33.513, 5G Security Assurance Specification (SCAS); User Plane Function (UPF)
3GPP TS 33.514, 5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
3GPP TS 33.515, 5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
3GPP TS 33.516, 5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
3GPP TS 33.517, 5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
3GPP TS 33.518, 5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
3GPP TS 33.519, 5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class

S pozdravom,

Cui Yu
Managing Director
Huawei Technologies (Slovak), s.r.o.