TECNOLOGIE
TELEMATICHE
TRASPORTI
TRAFFICO
TORINO

5T S.R.L.
Corso Novara 96 — 10152 Torino (IT)
T +39 011 227 4101
info@5t.torino.it / direzione5t@legalmail.it
www.5t.torino.it
C.F. - P.IVA 06360270018
C.C.I.A.A. TORINO 2825/1992
CAP. SOCIALE € 100.000,00 i.v.

Torino, 30 maggio 2024
Prot. n. 286/2024

Spett.le
Concorrente

Oggetto: APPALTO 5T S.R.L.

GARA EUROPEA A PROCEDURA APERTA PER L'APPALTO DI PROGETTAZIONE, FORNITURA, INSTALLAZIONE, ASSISTENZA IN GARANZIA E POST GARANZIA DI ROAD-SIDE UNIT V2I E TELECAMERE DI MONITORAGGIO

C.I.G. B1905CBBE6

CUP C14E20005260006 - "PROGETTO CTE NEXT; PIANO DI INVESTIMENTI PER LA DIFFUSIONE DELLA BANDA ULTRA LARGA FSC 2014- 2020"
CUP C15C22007220001 - "MAAS4ITALY - RAFFORZAMENTO MISURA PNRR M1C1 - INVESTIMENTO 1.4: SERVIZI DIGITALI E ESPERIENZA DEI CITTADINI" SUB-INVESTIMENTO 1.4.6. "MOBILITY AS A SERVICE FOR ITALY" - PIANO NAZIONALE COMPLEMENTARE PNC-A.1-N1

Chiarimento n. 2

Un Concorrente ha inoltrato la seguente richiesta di chiarimento:

Quesito n.1

Con riferimento al documento di Capitolato Tecnico, paragrafo 6.6, punto 'q': si intende 'firma e verifica' invece di 'crittografia e verifica', potete confermare?

Quesito n.2

Pensiamo inoltre che al sottopunto 'ii. ritardo firma massimo: 50 microsecondi? ci sia un errore di battitura in quanto 50 microsecondi significherebbero circa 20 000 firme al secondo. Si intendeva 50 millisecondi, potete confermare?

In merito alla richiesta di chiarimento la Stazione Appaltante specifica quanto segue.

Risposta di 5T a quesito n.1

La stazione appaltante conferma che è possibile intendere il punto 'q' come "firma e verifica" specificando quanto segue.

La crittografia è una disciplina di cui la "firma digitale" è un sottoinsieme, pertanto tali concetti non vanno interpretati come mutuamente esclusivi, come invece ci sembra di evincere dal quesito del Concorrente.

Il riferimento al concetto di "firma digitale" è infatti desumibile dal fatto che si cita la tecnica ECDSA, cioè una famiglia di algoritmi di firma digitale basati su crittografia a curve ellittiche. Queste sono usate dalle RSU per firmare i messaggi da trasmettere ai veicoli al fine di consentire a questi ultimi di identificare l'ente che emette i messaggi come ente fidato, autorizzato al servizio e per esso responsabile.

D'altro canto, concordiamo sul fatto che la dicitura usata nel Capitolato, "crittografia e verifica ECDSA", possa essere astrattamente interpretata anche come "(cifratura) e (verifica firma digitale)". Tuttavia, a quanto ci risulta, la cifratura dei messaggi è un processo crittografico non usato nella comunicazione tra RSU e veicoli, non sussistendo alcun requisito di confidenzialità e/o riservatezza. Di conseguenza, nella redazione del Capitolato, si era ritenuta sufficientemente esaustiva la formula usata.

***

Risposta di 5T a quesito n.2

La stazione appaltante conferma e ribadisce quanto riportato a capitolato, puntualizzando quanto segue.

Ai fini della presente procedura, per "ritardo di firma" si deve intendere il tempo che trascorre dalla ricezione del messaggio da front-end a RSU, fino alla generazione del messaggio firmato e pronto per essere trasmesso ai veicoli sul canale radio.

Il requisito di ritardo di firma non superiore a 50 microsecondi è volto a limitare la latenza introdotta dalla RSU tra la generazione del contenuto di un messaggio (p. es. stato fasi semaforiche negli SPATEM) e la sua effettiva trasmissione ai veicoli, affinché mantenga la migliore corrispondenza possibile con la realtà che il messaggio descrive.

Il ritardo di firma non è quindi l'inverso della frequenza alla quale la RSU gestisce (e firma) i messaggi, come sembra ipotizzare il Concorrente, Difatti, per questo parametro non è stato specificato un requisito minimo più stringente di quanto già richiesto dalle specifiche di riferimento, secondo le quali la massima frequenza "teoricamente" richiesta per l'invio dei messaggi ITS ai veicoli è attualmente di 10Hz, cioè 10 msg/s (numero raggiunto solo in casi particolari, quindi ben inferiore ai 20'000 messaggi al secondo riportati nel quesito dal Concorrente,

Il requisito richiesto risulta inoltre, dalle indagini di mercato condotte, supportato da prodotti di mercato già da qualche tempo disponibili.

Si richiama infine che, in base al Capitolato, le RSU richieste devono disporre di modulo hardware per la sicurezza (HSM) con funzionalità di accelerazione crittografica, quindi tendenzialmente più veloce della crittografia puramente software che, oltre a non garantire le medesime prestazioni di velocità, non sarebbe, per quanto ci risulta, conforme ai requisiti dei servizi PKI descritti nel Capitolato.

Con i migliori saluti,

Firma

Il RUP Ing. Luca Bonura

Firmato digitalmente da
Luca Bonura
CN = Bonura Luca
C = IT