

CAPITOLATO TECNICO

SISTEMI DI MONITORAGGIO E LOCALIZZAZIONE DI APPARATI RADIOMOBILI (LOTTO 8)

**PER L'ATTUAZIONE DEL PROGETTO DI ASSISTENZA EMERGENZIALE
"HOME/2017/ISFB/AG/EMAS/0054 - FALCO" GRANT AGREEMENT N.
HOME/2017/ISFB/AG/EMAS/0054**

CUP: F59I18000000006

Sommario

1	Struttura del documento	4
2	Sigle acronimi e definizioni	5
3	Contesto tecnologico	6
4	Oggetto della fornitura	6
4.1	Requisiti generali della fornitura	9
4.2	Certificazione del fornitore	10
4.3	Servizio di Help Desk telefonico.....	10
4.4	Servizi di manutenzione.....	10
4.4.1	Livelli di servizio (SLA)	11
4.4.2	Penali.....	11
4.4.3	Disponibilità scorte	12
4.5	Formazione	12
5	Caratteristiche della fornitura e criterio di aggiudicazione	13
5.1	Definizione dell'offerta tecnica.....	14
5.2	Definizione dell'offerta economica.....	15
6	Sistema Imsi Catcher / WiFi – requisiti	16
6.1	Unità tattica WiFi	17
6.2	Gestione dei dati raccolti.....	19
6.3	Caratteristiche tecniche di valutazione: unità integrata trasportabile.....	20
6.3.1	Requisiti riferiti al funzionamento in modalità passiva	20
6.3.2	Requisiti riferiti al funzionamento in modalità attiva	21
6.3.3	Requisiti riferiti alle soluzioni implementative adottate	24
6.3.4	Requisiti riferiti all'interfaccia locale e data management.....	26
6.4	Caratteristiche tecniche di valutazione: unità tattica WiFi.....	29
6.5	Caratteristiche tecniche di valutazione: affidabilità e servizi	31
7	Presentazione dell'offerta tecnica	32
8	Presentazione dell'offerta economica	32
9	Documentazione relativa ai prodotti.....	34
9.1	Documentazione di gestione del sistema	34
9.2	Documentazione del software.....	34
10	Verifica di conformità	34
10.1.1	Verifica di funzionalità del sistema	35



10.1.2	Precollaudò in fabbrica	35
10.1.3	Verifica di conformità	35
ALLEGATO	36

1 Struttura del documento

Il presente documento descrive la fornitura oggetto di gara in merito a due sistemi IMSI Catcher e relativi accessori. Il fornitore dovrà produrre una proposta tecnico-economica omnicomprensiva, ovvero che includa tutte le attività e i materiali a corredo, necessari per la messa in funzione dei sistemi. Gli stessi dovranno essere integrati in opportuni kit trasportabili.

La fornitura, come di seguito specificato, consta dei sistemi di monitoraggio e localizzazione e dei servizi ad essi associati.

Il presente documento è strutturato nei seguenti capitoli:

- Nel capitolo 3 è descritto il contesto in termini di caratteristiche applicative e di ambienti tecnologici.
- Nel capitolo 4 vengono elencate le componenti, i servizi oggetto della fornitura e le certificazioni richieste al fornitore.
- Nel capitolo 5 viene esposto il criterio di aggiudicazione e formulazione dei punteggi.
- Nel capitolo 6 e relativi paragrafi, a valle di una breve descrizione funzionale dell'apparecchiatura, vengono descritti i requisiti di valutazione
- Nei capitoli 7 e 8 è descritta la modalità di presentazione dell'offerta tecnica ed economica rispettivamente.
- Nel capitolo 9 è riportata la descrizione della documentazione a corredo della fornitura.
- Nel capitolo 10 vengono illustrati tempi e fasi per la verifica di conformità.

2 Sigle acronimi e definizioni

Nell'ambito del presente Capitolato Tecnico sono stati usati i seguenti acronimi:

ACRONIMO	DESCRIZIONE
BTS	Base Transceiver Station
DF	Direction Finding, localizzazione radiogoniometrica del terminale con analisi direzionale ed apprezzamento distanziometrico della posizione
EIRP	Acronimo di Equivalent Isotropic Radiated Power ad indicazione delle potenze radio emesse dai trasmettitori
GPS	Global Position System
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
LOS	Line of sight (collegamenti radio in visibilità ottica delle due terminazioni)
IMSI Catcher	Sistema di localizzazione e monitoraggio dei telefoni radiomobili
MTBF	Mean Time Between Failure
MS	Mobile System
Nodo	Nel presente documento con questo termine viene indicata l'unità fisica con cui il sistema provvede alla simulazione di una cella di radiocopertura. Se ad esempio il sistema ha un'architettura che consente la simultanea realizzazione in aria di tre celle, si parlerà di un sistema composto da tre nodi
POI	Point of Interest
AP	Access Point
MAC	Media Access Control
P_E	Punteggio Economico attribuito all'offerta
P_T	Punteggio Tecnico attribuito all'offerta
RAT	Radio Access Technology
RRC	Radio Resource Control
SDR	Software Defined Radio
SLA	Service Level Agreement
TTFF	Time To First Fix, tempo richiesto da un ricevitore GPS per acquisire il segnale satellitare, i dati di navigazione e calcolare la posizione (c.d. fix).
VOX	Voice Operated eXchange – soluzione di interruzione della trasmissione in assenza di segnale vocale utile
Y	Punteggio totale attribuito all'offerta

3 Contesto tecnologico

Negli ultimi decenni le operazioni di *Law Enforcement* sono state caratterizzate da un ricorso sempre crescente a dispositivi dall'elevato contenuto tecnologico. Si tratta di una strategia investigativa per il contrasto alla criminalità organizzata, transfrontaliera nonché del terrorismo, che richiede un costante rinnovamento delle dotazioni.

L'efficacia di tali sistemi risiede nella capacità delle soluzioni impiantistiche individuate di superare diversi fattori critici operativi tra cui:

- **Esigenze di occultamento dei dispositivi con implicazioni sui fattori di forma e sulle dimensioni in generale.**
La possibilità di installare i dispositivi nei pressi del target aumenta considerevolmente le possibilità di cattura delle informazioni ma accresce anche il rischio di *discovery* da parte dell'indagato con conseguente fallimento dell'intera operazione investigativa. Il contenimento delle dimensioni dei dispositivi agevola l'individuazione del sito di installazione.
- **Autonomia dei dispositivi e contenimento in generale degli assorbimenti energetici.**
La rapidità con cui le operazioni devono essere condotte.
- **Portata operativa della strumentazione.**
Intesa in termini di distanza di cattura delle informazioni rispetto alla sorgente. Il fattore distanza consente di limitare il rischio di *discovery* del dispositivo seppure garantendo adeguati livelli qualitativi del segnale catturato.
- **Qualità del segnale captato.**
Tanto a fini investigativi quanto forensi, la qualità del segnale e la sua intellegibilità giocano un ruolo strategico nel buon esito delle operazioni.

La presente fornitura si inserisce in tale contesto ed è mirata al potenziamento delle strutture del Servizio di Polizia Scientifica e del Servizio Centrale Operativo con l'acquisizione di sistemi di localizzazione e monitoraggio dei telefoni radiomobili in tecnologia 2G/3G/4G-LTE/5G con funzionalità WiFi integrate.

Relativamente alle funzionalità 5G, la fornitura si intende già inclusiva degli oneri di upgrade dei moduli di uno dei due sistemi, che saranno implementata in seguito al rilascio dei servizi commerciali da parte degli operatori nazionali.

4 Oggetto della fornitura

La presente fornitura è identificata come Lotto 8.

Il presente documento definisce i requisiti realizzativi e valutativi per la procedura di gara mirata all'acquisizione di n.2 Imsi Catcher realizzati in tecnologia trasportabile e modulare, ogni apparato può essere composto da più moduli che interagiscono con un'unica consolle di controllo in grado di pilotare contemporaneamente, in un'unica interfaccia grafica, le operazioni di censimento e localizzazione dei terminali (tale modulo è denominato "unità integrata trasportabile" nel resto del documento). Detta unità integrata trasportabile dovrà essere allocata in un unico contenitore rugged, tipicamente un trolley, in

grado di agevolarne il trasporto ed il trasferimento tra i diversi veicoli utilizzati in missione. Per ciascuno di detti sistemi, deve essere prevista la capacità integrata di monitorare, censire e localizzare terminali operanti in tecnologia 2G 3G 4G 5G¹ e WiFi in modalità passiva (scansione della rete) e attiva (simulazione della rete e affiliazione dei terminali a scopo di localizzazione e censimento)².

La soluzione offerta deve prevedere per ciascun Imsi Catcher una unità utilizzabile anche separatamente, in grado di operare in maniera autonoma con capacità integrata di censimento e localizzazione dei terminali nonché di ampliamento della modalità attiva al fine di eseguire attacchi MITM (Man In The Middle) sulle connessioni dati (almeno in tecnologia WiFi) come meglio specificato nel seguito del documento con riferimento al modulo "unità tattica WiFi".

Si precisa che una delle due **unità integrate trasportabili** (nel seguito del documento denominata "unità advanced") dovrà essere corredata delle seguenti prestazioni aggiuntive:

- funzionalità attive atte alla implementazione di attacchi MITM operanti sulla connettività dati dei terminali target (anche sulle connessioni dati radiomobili ed almeno in tecnologia 2G/3G)
- upgrade dei moduli con l'integrazione almeno delle funzionalità di monitoraggio e localizzazione di terminali radiomobili in tecnologia 5G in seguito al rilascio dei servizi commerciali dagli operatori nazionali.

Alla data della stesura del presente documento, non sono state definite le specifiche implementabili relative allo standard 5G. Quando il 3GPP completerà la standardizzazione del 5G e tale standard verrà pubblicato, entro e **non oltre 12 mesi** a partire da tale data, e comunque **non oltre 6 mesi** dal lancio commerciale in Italia dei servizi 5G, sarà obbligo del fornitore adeguare l'apparato "advanced" a tale tecnologia **senza nessun onere economico aggiuntivo per questa Amministrazione** e formando il suo personale all'impiego.

I sistemi, che verranno descritti in dettaglio nei loro componenti nei seguenti capitoli, comprendono:

- unità centrale IMSI Catcher 2G/3G/4G-LTE/WiFi; l'unità, eventualmente realizzabile anche come assemblaggio meccanico di uno o più cestelli, si intende comprensiva del ricevitore GPS, dei nodi di simulazione delle stazioni radio base, del sistema di scansione e dei moduli radio-goniometrici utili all'espletamento del Direction Finding, del sistema di scansione passiva di reti e dispositivi WiFi a/b/g/n 2,4 Ghz e 5 Ghz e di memorizzazione oltre che di catalogazione delle unità nonché del loro MAC; l'unità integrata trasportabile "advanced" dovrà essere oggetto upgrade al 5G come sopra specificato;

¹ Le capacità 5G sono richieste su uno solo dei due sistemi in fornitura.

² Relativamente alle reti WiFi, il modulo integrato nell' Unità Integrata Trasportabile deve essere in grado, senza simulare un particolare hot spot e quindi senza andare in trasmissione, di monitorare la presenza degli hot spot che coprono l'area in cui è collocato lo strumento e deve poter censire le affiliazioni dei terminali ivi presenti su tali hot spot. Tali prestazioni si intendono riferite alle reti wireless 802.11 nelle due bande commercializzate.

- in caso di sistema modulare con unità estraibili, deve essere previsto un PC portatile per ognuno dei moduli, necessario per la gestione del sistema e l'esecuzione delle attività di monitoraggio e localizzazione; nel seguito del documento denominato anche "PC di gestione" o "interfaccia locale";
- dotazione di backup (costituita da un PC aggiuntivo e un HD immagine predisposto con tutto il software necessario);
- modulo radiogoniometrico; sottosistema, integrato con l'IMSI Catcher, utile alla esecuzione della localizzazione dei terminali;
- antenne e cavetterie varie;
- contenitore per il trasporto mobile degli apparati succitati;
- manuale d'installazione (formato cartaceo ed elettronico);
- manuale d'uso (formato cartaceo ed elettronico);
- cartografia nazionale geo-referenziata ed in formato elettronico;
- kit di alimentazione per autoveicolo;
- kit di alimentazione tramite batterie ricaricabili.

Per ogni sistema deve essere prevista un'unità tattiche WiFi dedicata alla raccolta (anche mediante il ricorso ad una modalità attiva di simulazione delle reti) di informazioni elettroniche su reti wireless 802.11 ognuna delle quali comprendenti:

- Unità portatile per la scansione attiva di reti e dispositivi WiFi a/b/g/n 2,4 Ghz e 5 Ghz e di memorizzazione oltre che di catalogazione dei dispositivi presenti nel range operativo, dei loro MAC nonché degli SSID associati a ciascuno di essi in qualità di reti già note al terminale;
- PC portatile per la gestione del sistema e l'esecuzione delle attività di monitoraggio nel seguito del documento denominato anche "PC di gestione" o "interfaccia locale";
- antenne e cavetterie varie;
- contenitori per il trasporto mobile degli apparati succitati;
- manuale d'installazione (formato cartaceo ed elettronico);
- manuale d'uso (formato cartaceo ed elettronico);
- kit di alimentazione per autoveicolo;
- kit di alimentazione tramite batterie ricaricabili.

Tutto il materiale consegnato dovrà essere etichettato secondo lo schema riprodotto di seguito, visibile anche dagli imballaggi esterni.

Progetto HOME/2017/ISFB/AG/EMAS/0054 – “FALCO”



Co-funded by the
Internal Security
Fund of the
European Union



MINISTERO
DELL'INTERNO

Fondo Sicurezza Interna 2014-2020

Gli apparati devono essere consegnati presso la sede della Direzione Centrale Anticrimine sita in Roma, Via Tuscolana 1548

4.1 Requisiti generali della fornitura

La fornitura deve conformarsi ai requisiti di seguito indicati.

La mancata rispondenza ad uno dei seguenti punti costituirà motivo d'esclusione:

- Il fornitore deve consegnare i prodotti secondo i quantitativi indicati, nuovi di fabbrica e costruiti con parti nuove.
- Il fornitore deve consegnare tutti i prodotti con software preinstallato, comprensivi di licenze e manuali d'uso, patch di sistema e di sicurezza aggiornati almeno alla data di firma del contratto.
- In relazione alle apparecchiature e ai servizi offerti l'Amministrazione prenderà in considerazione solo prodotti hardware di costruttori d'apparecchiature elettroniche che abbiano una struttura produttiva i cui sistemi d'assicurazione della qualità siano stati certificati conformi alle norme della serie UNI-EN ISO 9001:2015 da un ente accreditato, nazionale od internazionale.
- Il sistema deve essere munito dei marchi di certificazione riconosciuti da tutti i paesi dell'Unione Europea e deve essere conforme alle norme relative alla compatibilità elettromagnetica.
- Il fornitore deve garantire la conformità del sistema alle normative CEI o ad altre disposizioni internazionali riconosciute e, in generale, alle vigenti norme legislative, regolamentari e tecniche disciplinanti i componenti e le modalità di impiego delle apparecchiature medesime ai fini della sicurezza degli utilizzatori.
- Per ciascun prodotto il fornitore deve consegnare una copia della manualistica tecnica completa, edita dal produttore; la documentazione deve essere in lingua italiana o inglese.
- Il fornitore deve consegnare una dichiarazione scritta che garantisce l'interoperabilità e la compatibilità dei componenti che costituiscono la soluzione proposta.

4.2 Certificazione del fornitore

Il fornitore deve presentare idonea documentazione attestante il possesso, per i materiali in fornitura, di idonea certificazione in corso di validità di rispondenza alle normative della serie UNI-EN ISO 9001:2015.

Il mantenimento della validità della certificazione viene richiesto anche per tutto l'arco della durata della manutenzione.

4.3 Servizio di Help Desk telefonico

Il fornitore deve far fronte a richieste e quesiti che si presenteranno sia nel corso dell'installazione che durante l'utilizzo dei sistemi. A tal fine è richiesto un servizio di supporto telefonico, in orario 09:00-18:00 e 5 giorni su 7 per tutta la durata del contratto (36 mesi), da attuarsi con un numero unico messo a disposizione dal fornitore.

4.4 Servizi di manutenzione

La durata del servizio di manutenzione incluso nell'offerta è di 36 mesi, fatti salvi i semestri aggiuntivi inclusi nell'offerta come descritto al requisito Q.15 (v. paragrafo 6.5), che decorreranno dalla data di comunicazione dell'esito favorevole della verifica di funzionalità del sistema.

I livelli minimi di servizio richiesti sono i seguenti:

DESCRIZIONE	RICHIESTA MINIMA
Durata	36 mesi
Modalità	On Site con intervento o recupero del sistema
Tempo di intervento	Ritiro entro 8 ore lavorative dalla segnalazione
Copertura settimanale	5 gg su 7

Le eventuali spese di spedizione del sistema saranno totalmente a carico del fornitore; il ritiro del sistema deve avvenire nella sede concordata con l'Amministrazione nella richiesta di intervento. Il mezzo di comunicazione delle richieste di intervento è il messaggio e-mail all'indirizzo unico messo a disposizione dal fornitore; ai fini del calcolo dei tempi di intervento farà fede la data/ora di invio della richiesta. Il fornitore deve mettere a disposizione dell'Amministrazione un numero di rete fissa (preferibilmente un numero verde) con cui fornire informazioni circa gli interventi di assistenza.

L'intervento del fornitore, ai fini del computo degli SLA di cui al successivo paragrafo 4.4.1, si riterrà concluso provvisoriamente alla riconsegna dell'apparato nella sede concordata con l'Amministrazione. Farà fede la bolla di ricezione della spedizione. L'accettazione dell'intervento sarà comunque subordinata al superamento con esito positivo di una selezione di test estratti dal piano di collaudo contenente almeno le verifiche di cui ai requisiti R.1, R.4, R.8, R10 (se l'intervento ha interessato il modulo "unità tattica WiFi" devono essere considerati almeno i requisiti R34 ed R39). In caso di verifica di funzionalità con prestazioni

non conformi a quelle di riferimento, l'intervento sarà riaperto e gli ulteriori giorni necessari al ripristino saranno addizionati ai precedenti ai fini del computo degli SLA.

La fornitura di semestri aggiuntivi di prolungamento del servizio di manutenzione in garanzia costituirà elemento di valutazione dell'offerta.

Per la manutenzione in garanzia, come per i semestri aggiuntivi eventualmente inclusi nell'offerta, saranno adottati i livelli di servizio (SLA) di seguito specificati.

Nel periodo di manutenzione in garanzia si intendono inclusi anche gli aggiornamenti software degli applicativi associati al prodotto nella configurazione offerta.

Qualsiasi aggiornamento deve essere assicurato anche ai dispositivi di backup inclusi nella fornitura (PC di gestione aggiuntivo, HD immagine etc...).

4.4.1 Livelli di servizio (SLA)

Il servizio di manutenzione deve essere accessibile dal lunedì al venerdì dalle ore 9.00 alle ore 18.00 (esclusi sabato, domenica e festivi) e sarà attivato durante il normale orario lavorativo mediante mail o chiamata telefonica da parte del personale utilizzatore di questa Amministrazione (a cui seguirà comunque la mail di segnalazione).

Il servizio di manutenzione deve essere erogato con le seguenti modalità:

- tempo di prima risposta telefonica: con riferimento al servizio di *Help Desk* telefonico e di manutenzione in garanzia, un tecnico qualificato deve richiamare entro 1 ora lavorativa la persona di riferimento indicata dall'utilizzatore al momento della chiamata;
- tempo di intervento on-site o ritiro dell'apparecchiatura: qualora il problema non sia risolvibile da remoto, entro 8 ore lavorative dalla chiamata dell'Amministrazione;
- i tempi di ripristino della normale operatività del sistema devono rispettare i seguenti vincoli:
 - o l'80% degli interventi devono essere risolti entro 5 giorni lavorativi;
 - o il resto degli interventi devono essere risolti entro 10 giorni lavorativi.

Gli interventi effettuati dovranno eliminare gli inconvenienti che hanno determinato la richiesta di riparazione e ripristinare le normali condizioni di funzionamento.

Deve essere redatta una nota d'intervento, da consegnare sia in formato cartaceo che elettronico, mediante la quale il fornitore deve mantenere traccia delle azioni necessarie al ripristino del sistema per consentire all'Amministrazione di controllare l'attività svolta.

Il fornitore deve adoperarsi, per quanto possibile, al recupero degli archivi presenti sulle apparecchiature da sostituire.

4.4.2 Penali

Il mancato rispetto dei termini previsti per l'esecuzione della fornitura e per i servizi di assistenza e manutenzione, comporterà l'applicazione di penali così come descritto nel contratto.

4.4.3 Disponibilità scorte

Il fornitore sarà contrattualmente impegnata ad assicurare la disponibilità di pezzi di ricambio/assistenza per almeno 6 anni successivi dalla scadenza del periodo di garanzia.

4.5 Formazione

Il fornitore deve erogare un servizio di formazione rivolto al personale tecnico dell'Amministrazione, con lo scopo di fornire una adeguata conoscenza delle tecnologie offerte, tale da consentire la gestione delle apparecchiature e dei prodotti software previsti nell'ambito della fornitura.

La formazione deve essere volta all'approfondimento di temi riguardanti l'utilizzo e la gestione dei prodotti oggetto di fornitura³ comprendendo le caratteristiche e le funzionalità, con particolare riferimento alle configurazioni hardware e software adottate. Inoltre deve comprendere le comuni problematiche riscontrabili nell'implementazione della tecnologia nell'ambiente applicativo dell'Amministrazione.

Il fornitore deve erogare due sessioni di formazione, provvedendo alla fornitura della documentazione didattica per i discenti, sia su supporto cartaceo, sia su supporto elettronico.

Una prima sessione di 5 giorni sarà destinata al personale operatore individuato dall'Amministrazione e si terrà presso la sede dell'Amministrazione con un numero massimo di 15 partecipanti.

Gli obiettivi minimi del primo pacchetto di formazione devono includere:

- a. addestramento teorico sulle tecnologie impattate dal sistema;
- b. addestramento tecnico/pratico circa l'utilizzo del sistema il cui contenuto minimo deve prevedere le funzionalità descritte ai paragrafi 6.3.1, 6.3.2, 6.4;
- c. Superamento di un esame pratico relativo alle tematiche affrontate ai punti a e b.

Una seconda sessione di 5 giorni dovrà prevedere la formazione avanzata e deve essere erogata a n.2 (due) discenti, con personale certificato sui prodotti offerti, e tenuta presso il fornitore stesso. Il pacchetto proposto deve comprendere le spese di vitto, alloggio e trasporto (voli in classe economy inclusi) per i n.2 (due) discenti.

Gli obiettivi minimi del secondo pacchetto di formazione devono includere:

- a. richiami teorici sulle tecnologie;
- b. richiami tecnico/pratici all'utilizzo;
- c. formazione tecnico/pratico per l'espletamento autonomo da parte dell'Amministrazione di interventi di manutenzione di primo livello (es: sostituzione e riconfigurazione dei moduli di sistema, upgrade firmware ...);
- d. superamento di un esame pratico relativo alle tematiche affrontate ai punti a, b e c.

³ La formazione deve intendersi estesa all'"unità integrata trasportabile" "unità tattica WiFi" e estensione delle funzionalità 5G del sistema advanced.

Per ogni partecipante al corso deve essere rilasciato un attestato che certifichi il superamento del corso.

Il completo e corretto espletamento dell'attività formativa sarà certificato mediante apposita Relazione sull'addestramento svolto redatta a cura del fornitore ed accettata dal personale dell'Amministrazione, nella quale verranno indicati l'oggetto, i destinatari e la durata dell'addestramento svolto nonché gli esiti delle prove pratiche di cui al punto d.

L'attività di formazione deve essere conclusa, salvo diverso accordo con l'Amministrazione, entro un tempo massimo di 4 (quattro) mesi dalla data di accettazione della fornitura a cura di un profilo professionale corrispondente a Sistemista Senior con comprovata esperienza nell'utilizzo del sistema oggetto della fornitura. In esito al rilascio dell'upgrade per le funzionalità 5G, la fornitura deve includere una sessione formativa aggiuntiva presso l'Amministrazione finalizzata alla formazione degli operatori addetti all'impiego in campo e contenente eventuali ulteriori contenuti legati alla gestione degli interventi di primo livello di manutenzione.

Entrambi i programmi delle sessioni formative devono essere approvati dall'Amministrazione prima della loro erogazione.

5 Caratteristiche della fornitura e criterio di aggiudicazione

La gara sarà aggiudicata a favore del concorrente che presenterà l'offerta economicamente più vantaggiosa ai sensi dell'art. 95 comma 2 del D.lgs. 50/2016, da individuare sulla base dei parametri e con i pesi di seguito indicati:

CRITERIO	PUNTEGGIO MASSIMO
Punteggio tecnico	70
Punteggio economico	30
TOTALE	100

Il punteggio totale sarà determinato dalla somma algebrica del punteggio tecnico (P_T) e del punteggio dell'offerta economica (P_E), calcolato applicando la seguente formula:

$$Y = P_T + P_E$$

La commissione giudicatrice procederà alla valutazione delle offerte tecniche e all'attribuzione del relativo punteggio con riguardo alle caratteristiche tecniche migliorative rispetto a quanto previsto dal Capitolato Tecnico in base ai criteri indicati nelle tabelle di valutazione tecnica riportate nel seguito.

La gara verrà aggiudicata all'offerta che consegnerà la massima valutazione totale. Tutti i calcoli saranno troncati alla seconda cifra decimale arrotondata all'intero più vicino secondo i seguenti esempi:

- 5.565 diviene 5.57
- 5.654 diviene 5.65

A parità di punteggio complessivo l'aggiudicazione avverrà a favore dell'offerente che avrà ottenuto il maggiore punteggio tecnico.

5.1 Definizione dell'offerta tecnica

I requisiti di carattere tecnico sono suddivisi in due tipologie contraddistinte dalle lettere **R** e **Q** seguite da un numero progressivo che ne facilita il riferimento. Alle diverse lettere sono associate le seguenti tipologie di richieste:

- **R.# requisiti mandatori:** il rispetto di tali requisiti è **obbligatorio**, pena l'esclusione dalla gara. Per tali requisiti, in quanto abilitanti alla partecipazione, non è prevista una pesatura di valutazione. Il fornitore deve rispondere a tali requisiti indicandone la conformità.
- **Q.# requisiti migliorativi:** il rispetto di tali requisiti **non è obbligatorio ma concorre alla valutazione dell'offerta** secondo il peso associato nella matrice di valutazione. Il fornitore che vorrà rispondere a tali quesiti deve indicare il valore/soluzione caratterizzanti l'offerta secondo le richieste formulate nel testo.

Il rispetto di un requisito minimo, anche se non attribuisce un punteggio migliorativo, deve essere dichiarato, pena esclusione.

In alcune tabelle saranno presenti quesiti contrassegnati con la lettera "I" seguita da un numero progressivo (**I.#**). Si tratta di quesiti informativi in cui il fornitore è tenuto ad indicare dettagli circa la soluzione tecnica adottata.

Con riferimento ai requisiti migliorativi opzionali quotabili, qualora il punteggio debba premiare la soluzione in proporzione alla prestazione inferiore fornita in comparazione con le altre offerte, ove espressamente indicato con il suffisso "INV" nel riquadro destinato alla definizione dei punti disponibili per il requisito, l'attribuzione del punteggio avverrà su scala lineare sulla base della relazione:

$$P = \frac{V_{\min} + V_{\max} - V}{V_{\max}} * P_{\max}$$

Dove:

- P è il punteggio assegnato
- P_{\max} è il massimo punteggio assegnabile per il quesito in questione

- V_{max} , V_{min} , V sono rispettivamente i valori espressi dal fornitore con soluzione che riporta il valore massimo, fornitore con valore minimo e risposta del fornitore in esame. Alcuni o tutti i valori suddetti potranno eventualmente coincidere in relazione al numero e al valore delle offerte pervenute.

Qualora invece il punteggio debba premiare la soluzione in proporzione alla miglior prestazione fornita in comparazione con le altre offerte (suffisso "LIN" presente nel riquadro che definisce il punteggio massimo disponibile), sarà adottata la seguente formula:

$$P = \frac{V_{min}}{V_{min} + V_{max} - V} * P_{max}$$

Il punteggio relativo all'offerta tecnica (P_T) sarà calcolato come la somma di tutti i punteggi associati ai requisiti tecnici. Tutti i calcoli saranno troncati alla seconda cifra decimale arrotondata all'intero più vicino secondo i seguenti esempi:

- 5.565 diviene 5.57
- 5.654 diviene 5.65

5.2 Definizione dell'offerta economica

Il punteggio relativo all'offerta economica (P_E) sarà calcolato sulla base della seguente formula di tipo lineare che tiene conto dei prezzi minimo e massimo offerti:

$$P_E = \frac{P_{min} + P_{max} - P}{P_{max}} * 30$$

Dove:

- P_E è il punteggio economico assegnato all'offerta in esame;
- P_{min} è il prezzo offerto minimo pervenuto;
- P_{max} è il prezzo offerto massimo pervenuto;
- P è il prezzo dell'offerta in esame.

Tutti i calcoli saranno troncati alla seconda cifra decimale arrotondata all'intero inferiore secondo i seguenti esempi:

- 5.565 diviene 5.57
- 5.654 diviene 5.65

6 Sistema Imsi Catcher / WiFi – requisiti

L'impiego sistematico dei sistemi radiomobili di comunicazione fa sì che la loro localizzazione e il loro monitoraggio sia di importanza strategica nello svolgimento delle attività di Polizia Giudiziaria.

Il sistema in oggetto deve essere in grado di acquisire lo stato della radio copertura del territorio in cui viene attivato e di simulare il funzionamento di una qualsiasi cella radio, utilizzata dai gestori telefonici per l'erogazione dei servizi radiomobili 2G/3G/LTE-4G-5G⁴. Tale operazione è propedeutica alla rilevazione dei terminali presenti all'interno della sua area di operatività (ossia l'area coperta dal segnale di "simulazione" generato dal sistema). La potenza erogata dalla cella clonata deve essere uno dei parametri configurabili dall'operatore.

L'utilizzo del sistema, previsto su tutto il territorio nazionale nell'ambito di scenari operativi dinamici, ne rende indispensabile la trasportabilità (il sistema essendo prevalentemente utilizzato all'interno di un veicolo sarà sottoposto ad inevitabili sollecitazioni meccaniche e termiche) e i ridotti consumi energetici (la potenza assorbita deve poter essere sostenuta dal gruppo alternatore-batteria di un normale veicolo commerciale).

In ragione della necessità di dover operare il monitoraggio e la localizzazione, anche in ambienti *indoor* o comunque non accessibili ai veicoli (seppure nel rispetto del requisito generale di integrazione delle prestazioni richieste in un unico kit), è richiesto che gli apparati demandati alla localizzazione di dispositivi cellulari prevedano la possibilità di ricorrere all'uso in sinergia di dispositivi tattici.

Nell'ambito delle reti radiomobili di tipo cellulare, tali dispositivi tattici dovranno poter essere configurati con i dati ricavati dal sistema IMSI Catcher (finora denominato unità integrata trasportabile) in relazione alla forzatura dei terminali target nella trasmissione su canali specifici, poi facilmente individuabili con il dispositivo tattico fornito a corredo⁵.

Nell'ambito delle reti WiFi, il dispositivo tattico dovrà beneficiare delle informazioni ricavate dal sistema Imsi Catcher in relazione alle reti WiFi individuate nell'area indoor di interesse. Questo al fine di poter conoscere a priori le reti hot spot da simulare in modalità attiva con il dispositivo tattico wireless fornito (finora denominato unità tattica wifi).

Per quanto sopra esposto si rende necessario il funzionamento del sistema in due differenti modalità operative denominate "passiva" ed "attiva" non mutuamente esclusive, come di seguito descritte⁶.

⁴ Il riferimento al 5G resta da intendersi valido per il solo sistema "advanced" e con disponibilità a decorrere dalla definizione dello standard e dell'entrata in commercio dei servizi 5G da parte degli operatori nazionali italiani.

⁵ La funzionalità di localizzazione deve essere comunque erogabile dal sistema senza l'ausilio del terminale in questione, da intendersi opzionale e di ausilio per task specifici (es. applicazioni indoor).

⁶ Tali funzionalità si intendono estese anche alle reti 5G, al netto della clausola di rilascio delle stesse in esito alla standardizzazione e commercializzazione dei servizi 5G.

- In modalità passiva il sistema deve consentire la scansione, l'analisi e la registrazione dei dati di copertura radiomobile delle celle 2G/3G/LTE-4G/5G nonché hot-spot WiFi rilevabili nell'area di utilizzo, offrendo la possibilità di passare alla modalità attiva su una o più celle rilevate.
- In modalità attiva il sistema deve effettuare, anche su RAT differenti, la contemporanea simulazione di stazioni radio 2G/3G/LTE-4G/5G. La modalità attiva sulle reti WiFi non è richiesta obbligatoriamente integrata nel sistema di localizzazione e monitoraggio ma deve essere implementata almeno nei sistemi tattici a corredo della fornitura (Unità tattica WiFi).

In tale modalità si devono poter acquisire informazioni circa l'identificazione dei *Mobile System* presenti nell'area coperta dallo strumento (es: procedura di IMSI *attach*); le informazioni devono poter essere archiviate, elaborate ed estratte dal sistema. I terminali mobili presenti nell'area di copertura devono essere censiti e rilasciati alla rete reale.

In modalità attiva e sui terminali selezionati, deve poter essere possibile procedere alla affiliazione permanente alla stazione radiomobile simulata dal sistema, rendendo di fatto le utenze invisibili alla rete reale e quindi impossibilitati a fare e ricevere telefonate.

Per agevolare tale modalità di funzionamento ed altre policy mirate su taluni terminali/utenze selezionati dall'operatore, deve poter essere possibile marcare alcune utenze/terminali come "target". Tra le funzionalità minime offerte dal sistema deve essere prevista la possibilità di avviare la localizzazione radiogoniometrica del terminale con analisi direzionale ed apprezzamento distanziometrico della posizione (modalità denominata anche *DF Direction Finding*).

Il sistema dovrà inoltre integrare delle funzionalità in grado di raccogliere in modalità passiva, le informazioni relative ad apparati WiFi nelle bande 2,4 Ghz e 5 Ghz (a/b/g/n). Le informazioni rilevate durante la scansione wireless dovranno essere integrate con le analoghe informazioni rilevate effettuando la scansione della rete cellulare e rese disponibili sulla stessa interfaccia grafica. In tale ottica i formati dei dati e le rispettive GUI dell'unità IMSI Catcher e dell'unità tattica devono essere compatibili ad effettuare inter lavoro nello scambio dei dati e nelle successive fasi di filtraggio ed estrazione (es. ricavare da missioni diverse IMSI IMEI e MAC address rilevati in comune) così da approssciare l'associazione dei MAC address agli IMEI/IMSI.

6.1 Unità tattica WiFi

La presenza di interfaccia WiFi su device portatili quali smartphone, tablet, notebook e la capillare distribuzione sul territorio di punti di accesso (hot spot) talvolta libero, resi disponibili sia da soggetti pubblici che privati, favorisce l'uso di tale tecnologia per l'accesso ad Internet e ai social network (Whatsapp, Twitter, Facebook,...). In virtù di ciò, la localizzazione e il monitoraggio di apparati che fanno uso dell'interfaccia WiFi per l'accesso alla rete, ricopre un'importanza crescente nello svolgimento delle attività di Polizia Giudiziaria.

Premesso ciò, la fornitura in oggetto dovrà comprendere numero due unità tattiche dedicate alla raccolta di informazioni elettroniche su reti Wireless 802.11. Ognuno dei due sistemi, deve:

- essere in grado di clonare un access point WiFi erogando connettività internet al posto della rete hot spot originaria;
- essere in grado di eseguire attacchi selettivi sulla rete WiFi esistente per eseguire Deny of Service (DoS) e favorire l'aggancio del target sulla rete fake;
- Clonare un Access Point;
- Catturare l'handshake tra terminale e hotspot;
- Effettuare il jamming selettivo della rete WiFi per singolo canale o per intero hotspot;
- Avere un ingombro inferiore nei tre lati uguale o inferiore a 200X150X100 mm;
- Peso inferiore a 2 Kg per l'unità tattica e 2kg per il pacco batteria;
- Essere dotato di espansione di memoria tramite Slot SD e di una card slot mini Sim.

Inoltre dovrà essere dotata di

- Connettori esterni per antenne WiFi e GPS;
- Interfaccia Ethernet 100/1000;
- Modem LTE;

Inoltre ogni unità tattica dovrà essere alloggiata in un apposito case rugged in grado di contenere anche gli accessori qui di seguito elencati :

- Antenne WiFi omnidirezionali con guadagno pari o superiore a 6 dBi in numero almeno pari al doppio rispetto al numero di connettori di cui è dotata ciascuna unità;
- Antenne WiFi direttive con guadagno pari o superiore a 10 dBi in numero almeno pari al doppio rispetto al numero di connettori di cui è dotata ciascuna unità;
- Antenne WiFi omnidirezionali con base magnetica e guadagno pari o superiore a 4 dBi in numero almeno pari al doppio rispetto al numero di connettori di cui è dotata ciascuna unità;
- Power Supply: devono essere forniti due alimentatori completi di cavo per garantire il backup);
- Batteria di capacità sufficiente a garantire all'unità un'autonomia di funzionamento almeno pari a 4 ore in regime di funzionamento;
- Carica batterie per le batterie al punto precedente;
- Cavi di collegamento in numero almeno pari al doppio rispetto a quelli necessari per la completa operatività dell'unità;
- SD Card con capacità almeno pari a 128 Gb;
- Contenitore per mini SIM card e Card SD;
- Terminale tipo smartphone caratterizzato da : processore almeno octa core (Quad-core 2.3 GHz + Quad-core 1.6 GHz), Ram almeno 4 Gb, Risoluzione display almeno pari a 1440 x 2560 pixel espandibile in memoria almeno fino a 200 Gb, Card Sd di espansione di capacità almeno superiore a 128 Gb (qualora la gestione dell'unità tattica wifi possa essere svolta con APP dedicata, il terminale deve essere configurato con wardware e firmware/SO utile a garantirne l'eseguitività).

La gestione dell'unità tattica dovrà avvenire tramite apposita interfaccia grafica. Tra le funzionalità configurabili :

- Tempo di funzionamento sui canali a 2,4 Ghz e 5 Ghz;
 - Prospetto riepilogativo delle reti rilevate, reti simulate, terminali presenti in rete e terminali affiliati all'hot spot emulato con tutte le relative informazioni circa le frequenze utilizzate, MAC address, canali usati etc...;
 - Prospetto per la gestione di attacchi MITM;
 - Parametri di connessione remota utilizzata per la gestione del modulo tattico;
 - Parametri dell'interfaccia Ethernet;
 - Parametri del modem LTE;
 - Export/Import della configurazione;
 - Export/Import delle missioni;
 - Export/Import delle regole di attacco
- Tutte le funzionalità di attacco MITM volte al supporto delle attività di intercettazione telematica, si intendono realizzate previo controllo dell'identità dell'operatore e con esplicito riferimento ad un decreto di intercettazione (si faccia riferimento al paragrafo 6.4).

6.2 Gestione dei dati raccolti

Il sistema deve gestire, sia un cruscotto in grado di rappresentare in tempo reale i dati dei telefoni e degli apparati WiFi censiti nel corso delle misure, sia un *tool* di ricerca *off-line* a valle delle misure effettuate.

Le particolari metodologie operative condotte in campo, richiedono un'architettura di base dati in grado di evidenziare agevolmente apparecchi e utenze che siano state già oggetto di censimento in precedenti rilevamenti ma, al tempo stesso, la base di dati deve consentire diversi livelli di aggregazione dei dati rilevati in campo nelle diverse sessioni di misura.

Prescindendo dalla particolare nomenclatura e soluzione adottata, devono essere gestiti almeno i seguenti livelli di aggregazione dei dati di seguito riportati secondo un'alberatura gerarchica⁷:

- **Task:** è il macro contenitore in cui sono contenuti tutti i dati di una particolare indagine;
- **Missione:** è il contenitore dei dati raccolti in un insieme di misurazioni condotte da una squadra operante nel territorio in riferimento ad un dato task. Più squadre possono lavorare con diverse missioni allo stesso task;
- **Luogo:** è il più basso livello di aggregazione e descrive la località in cui, nell'ambito di una data missione di un dato caso, sono state condotte misure.

I livelli di aggregazione devono essere gestiti sia nel cruscotto di visualizzazione dei dati di cattura in tempo reale, sia nei *tool* di post analisi dei dati raccolti. In quest'ultimo caso devono poter essere implementate ricerche⁸ articolate con più criteri di selezione.

⁷ La nomenclatura della struttura dei dati è puramente indicativa. La stessa struttura gerarchica è da intendersi non vincolante, purché il sistema consenta di isolare i dati raccolti in termini di "caso investigativo" distinguendo le singole uscite operative effettuate con lo strumento nell'ambito dello stesso "caso" in termini di luogo in cui si opera e uscita degli operatori.

Circa il cruscotto di analisi in tempo reale dei dati di cattura deve poter essere abilitata in maniera configurabile la rilevazione di telefoni già visti aggregando dati della sola missione in corso, di più missioni, di un solo caso o di tutti i dati presenti sul sistema. Altra prestazione minima è l'evidenza in tempo reale di fenomeni di cambio SIM o cambio terminale (ossia gli eventi di cattura di IMEI già censiti ma con altra IMSI e viceversa).

Le funzionalità sopra esposte devono intendersi disponibili sia nell'unità integrata trasportabile (imsi catcher trasportabile 2G/3G/4G – WiFi), sia nell'Unità tattica wifi circa i dati censiti nelle reti wireless, che, nel sistema advanced, per i terminali 5G (fatta salva la clausola temporale di rilascio dello standard e di avvio commerciale dei servizi 5G sul territorio nazionale).

6.3 Caratteristiche tecniche di valutazione: unità integrata trasportabile

Nei paragrafi successivi i concetti esposti nell'introduzione del presente capitolo circa un ipotetico utilizzo applicativo dei sistemi vengono esplosi nel dettaglio dei requisiti tecnici di fornitura.

6.3.1 Requisiti riferiti al funzionamento in modalità passiva

Con riferimento allo scenario d'impiego descritto al capitolo 6, il sistema deve essere in grado di erogare in modalità passiva le seguenti prestazioni minime

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
R.1	La modalità passiva deve consentire la scansione e l'analisi dei dati di copertura radiomobile rilevati nel sito di utilizzo in tutte le tecnologie supportate 2G/3G/LTE-4G e 5G (quando disponibile e per il solo sistema "advanced") dai gestori di servizi radiomobili presenti sul territorio nazionale. Tale modalità deve essere operativa anche per le reti WiFi rilevate. In tal caso oltre al rilevamento degli hot-spot, il sistema deve procedere ad associarvi i terminali rispettivamente affiliati con le relative informazioni di connettività a corredo (banda di freq. Canale, Mac, SSID noti al terminale etc...). Il sistema deve conservare le coordinate GPS dei siti in cui è stato rilevato un dato SSID così da consentire l'analisi incrociata delle reti WiFi incontrate sul territorio con le reti WiFi note ai terminali monitorati. La modalità di scansione deve essere gestibile in parallelo alla modalità attiva senza sottrarre al sistema nodi utili per il catching dei terminali mobili. In altri termini la scansione deve poter procedere anche durante l'uso in modalità attiva di tutti i nodi di simulazione offerti dal sistema fornendo la possibilità di aggiornare il parco delle celle clonate nel corso della sessione in ragione, ad esempio, degli spostamenti intervenuti e quindi del mutato ambiente radio in cui il sistema si trova ad operare.	
Q.1	Il punteggio verrà assegnato alla soluzione che consenta il salvataggio dei risultati di scansione e la sua geo-referenziazione con possibilità di richiamo per la configurazione dei cloni sui nodi in tempo reale senza necessità di reiterazione di un ciclo di scansione. I dati dovranno poter essere esportati in formato elettronico gestibile dalle più diffuse suite di office automation disponibili in ambiente Windows (es: file txt, .xml, .xls etc...).	Punti

⁸ A titolo esemplificativo: si devono poter isolare apparecchi che si presentano nello stesso luogo in missioni diverse piuttosto che apparecchi che risultino sempre presenti insieme ad un dato telefono in diverse sessioni di misura eseguite in luoghi diversi



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
	<ul style="list-style-type: none"> - Possibilità di salvataggio e richiamo dei risultati di scansione (Punti 0,7). - Presentazione dei risultati di scansione pregressa con ordine di selezione calcolato in base alla prossimità geografica del sistema rispetto alla posizione in cui è stata eseguita la scansione stessa (Punti 0,3). 	1
R.2	<p>Il sistema deve essere in grado di passare alla modalità attiva su una delle celle rilevate/proposte in fase di scansione senza soluzione di continuità nell'utilizzo dell'apparecchiatura. Il sistema non deve quindi necessitare della chiusura e riavvio del software di gestione o della ripetizione di operazioni di log-in. Il software fornirà all'operatore l'elenco delle celle simulabili secondo un criterio di preferibilità che consenta di indirizzare la scelta manuale verso la selezione dei migliori cloni ai fini della efficacia di cattura dei terminali mobili a parità di nodi utilizzati. Il criterio adottato per il ranking deve essere descritto.</p>	
Q.2	<p>Il punteggio sarà assegnato alla soluzione offerta in grado di configurare il modulo tattico WiFi con i dati di rete wifi da simulare e le caratteristiche dei target da acquisire così come rilevato dal modulo Imsi catcher (unità integrata trasportabile) in esito alla scansione passiva operata in modalità WiFi</p>	Punti 1
I.1	<p>Il fornitore, ove supportate, deve indicare le eventuali altre funzionalità implementate dal sistema in modalità passiva, con dettaglio per singola RAT delle informazioni/funzionalità gestite, della eventuale possibilità di esportazione dei dati e dei formati in cui questi saranno resi disponibili.</p>	

Tabella 1 – Funzionamento in modalità passiva

6.3.2 Requisiti riferiti al funzionamento in modalità attiva

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
R.3	<p>Il sistema deve essere in grado di simulare le stazioni di radio-copertura cellulare in tutte le tecnologie radiomobili presenti sul territorio nazionale 2G/3G/LTE-4G e 5G (quando disponibile e per il solo sistema "advanced") nelle rispettive bande oggetto di licenza.</p>	
Q.3	<p>Il punteggio sarà assegnato alla soluzione in grado di implementare nel sistema imsi catcher trasportabile la funzionalità attiva anche su reti wireless. Per l'assegnazione del punteggio, tali funzionalità devono essere inclusive delle tecniche di attacco adottate dall'Unità tattica WiFi (MiTM, DoS etc...) meglio descritte al paragrafo 6.4 Caratteristiche tecniche di valutazione: unità tattica WiFi.</p> <p>In tal caso il sistema deve essere equipaggiato anche con un modulo per la connettività almeno 4G alla rete radiomobile al fine di consentire materialmente l'instradamento del traffico verso le destinazioni simulate o desiderate dal target oggetto di attacco.</p>	Punti 6
R.4	<p>La simulazione delle celle di radio-copertura deve poter avvenire anche su più RAT simultaneamente. Il fornitore deve indicare il numero massimo di nodi contemporaneamente simulabili per RAT. I nodi devono essere realizzati in tecnologia singleRAN/SDR/MSR. Per il solo sistema "advanced" e relativamente all'integrazione del 5G, sarà ritenuto accettabile l'utilizzo di un nodo discreto dedicato.</p> <p>Il numero minimo di nodi contemporaneamente simulabili richiesto deve essere pari ad almeno 3. La funzionalità WiFi potrà essere implementata in un modulo a parte. Qualora fosse sviluppata integrata</p>	

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
	<p>nei precedenti, la sua attivazione non deve interferire con la possibilità di operare in WiFi e, contemporaneamente, con almeno 3 clonazioni di celle radiomobili.</p> <p>Per ogni modulo l'impostazione della RAT in cui avviene la simulazione di cella deve poter essere eseguita dall'operatore in campo senza la necessità di alcuna installazione hardware o software, ma semplicemente per mezzo di una configurazione del sistema in tempo reale per mezzo del PC di gestione/interfaccia locale.</p>	
Q.4	<p>Il punteggio sarà assegnato alla soluzione offerta il cui sistema IMSI Catcher "unità integrata trasportabile" sia in grado di implementare un attacco MITM in tecnologia 3G o superiore.</p> <p>In tal caso il sistema deve essere equipaggiato anche con un modulo per la connettività almeno 4G alla rete pubblica al fine di consentire materialmente l'instradamento del traffico verso le destinazioni simulate o desiderate dal target oggetto di attacco. Se condivisibile dai moduli cellulari e WiFi, può essere utilizzato lo stesso modulo di connettività descritto al precedente quesito opzionale previsto in ambito WiFi.</p> <p>Per la descrizione della operatività degli attacchi MITM si rimanda a quanto riportato nel paragrafo 6.4 Caratteristiche tecniche di valutazione: unità tattica WiFi.</p>	<p style="text-align: center;">Punti</p> <p style="text-align: center;">6</p>
R.5	<p>A supporto della configurazione in modalità attiva dello strumento, il sistema deve proporre, a valle della prima scansione, un set di celle ottimale da sottoporre a simulazione, lasciando comunque la possibilità all'operatore di selezionare altre combinazioni di celle.</p> <p>Allo spostamento dello strumento durante il funzionamento in modalità attiva deve conseguire l'adeguamento del set ottimale di celle da riprodurre sui nodi tenendo conto ad esempio delle nuove adiacenze. A tal fine lo strumento deve poter procedere alla scansione in background fornendo risultati aggiornati al contesto radio in cui il sistema è inserito a seguito degli spostamenti condotti o comunque al mutato ambiente radio.</p>	
Q.5	<p>Il punteggio verrà assegnato al fornitore che preveda una modalità attiva configurabile anche in modalità automatica. Per modalità attiva automatica si intende la possibilità di configurare lo strumento affinché avvii in sequenza la scansione e la simulazione delle celle con selezione dei cloni basata sul criterio di massima efficacia di cattura dei terminali mobili. La RAT, le bande ed i gestori oggetto di clonazione devono essere configurabili. Le due fasi, quella di scansione e quella di simulazione e cattura dei terminali, devono inoltre poter essere separate da un comando dell'operatore⁹.</p>	<p style="text-align: center;">Punti</p> <p style="text-align: center;">1</p>

⁹ Si consideri la situazione operativa in cui per esigenze tattiche non sia opportuno procedere alla scansione in prossimità del target; l'avvio automatico della cattura, senza la possibilità del rinvio da parte dell'operatore, porterebbe a registrare apparati che non appartengono all'area strettamente prossima al target, introducendo rumore nel data base delle rilevazioni.

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI
R.6	Il sistema deve consentire all'operatore di modificare la configurazione dei cloni anche nel corso di una sessione di acquisizione in modalità attiva rendendo selezionabile sia la cella di cui modificare i parametri di simulazione che la cella obiettivo da riprodurre (devono poter essere selezionabili anche quelle rilevate in scansione). La modifica di uno dei nodi non deve perturbare il funzionamento degli altri.
R.7	La potenza erogata dai nodi simulatori di cella deve essere uno dei parametri configurabili dall'operatore. Indicare il <i>range</i> nominale supportato dallo strumento per singola RAT. Per ciascuna RAT la potenza massima configurabile deve essere di almeno 10W.
I.2	Il fornitore deve indicare le sensibilità dei ricevitori nelle diverse RAT con i corrispondenti valori di <i>data rate</i> e <i>bit error rate</i> di riferimento a cui sono stati testati.
R.8	<p>Tutti i terminali mobili nelle tecnologie 2G/3G/LTE-4G e 5G (quando disponibile e solo per il sistema "advanced") commercializzate sul territorio nazionale e presenti nell'area di copertura del sistema, inclusi i dispositivi concepiti per la sola navigazione dati (c.d. tablet, dongle o chiavetta internet), dovranno essere censiti dallo strumento (le informazioni minime acquisite sono IMSI ed IMEI del terminale).</p> <p>Nella modalità attiva di base (ossia quella mirata alla sola rilevazione dei terminali mobili presenti nell'area coperta dal sistema), a valle dell'acquisizione dei dati di identità del terminale, i MS dovranno essere rilasciati alla rete reale.</p>
R.9	<p>Modalità di funzionamento "target". In modalità attiva il sistema deve agganciare, censire e rilasciare i terminali. Sui terminali censiti come "target" deve essere possibile impostare l'affiliazione permanente del terminale alla BTS simulata.</p> <p>In modalità attiva, a fronte di un qualsiasi MS identificato, ossia che si è agganciato alla cella simulata ed è stato quindi censito nella consolle di gestione dello strumento, il sistema deve consentire all'operatore di marcare l'utenza come "target" per potervi applicare le policy descritte circa tale modalità di funzionamento.</p> <p>Il sistema deve rendere configurabili le policy da applicare in automatico sui singoli target censiti (solo monitoraggio con alerting, controllo del terminale, silent call etc...).</p>
R.10	<p>Modalità "localizzazione" (o DF, Direction Finding). Il sistema, con riferimento ad almeno un'utenza marcata come target, deve poter procedere alla definizione approssimata della sua posizione. Il numero minimo di terminali gestiti in tale modalità deve essere almeno 1.</p> <p>Il sistema deve fornire la misura della potenza ricevuta dal terminale target sul nodo simulato e la stima della distanza presunta a cui il terminale si trova. A tal fine deve essere in grado di indurre in trasmissione il MS.</p>
I.3	Il fornitore deve indicare il numero massimo di MS contemporaneamente gestibili in modalità "localizzazione" (o DF).
I.4	Il fornitore deve esplicitare, per RAT, il principio di funzionamento con cui realizza le funzioni di <i>Silent Call</i> o altra modalità di forzatura alla trasmissione da parte del terminale mobile (sms, cicli di misure di potenza...).
R.11	<p>Il sistema deve rendere visualizzabile il canale/bearer radio (frequenza e relativo numero/codice di scrambling) su cui il terminale è indotto alla trasmissione ai fini del direction finding.</p> <p>Questo al fine di poter consentire ad esempio l'utilizzo combinato dell'IMSI Catcher con altri dispositivi anche non proprietari ma utilizzabili per una localizzazione fine del target in ambienti indoor mediante scansione passiva delle frequenze.</p>



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
Q.6	Il punteggio è assegnato qualora il sistema sia in grado, su comando dell'operatore, di produrre una chiamata su uno dei telefoni censiti in fase di cattura. Più precisamente, selezionato il terminale dalla schermata di cattura dei terminali, deve essere possibile attivarne la suoneria, vibra call o comunque l'opzione di segnalazione di chiamata entrante sull'utenza configurata sul terminale.	<p style="text-align: center;">Punti</p> <p style="text-align: center;">1</p>
I.5	Il fornitore deve indicare le possibili combinazioni di tecnologia di partenza e arrivo in cui il sistema è in grado di indurre il terminale ad effettuare il <i>downgrade</i> radio (es: 3G→2G, 4G→3G ...5G quando disponibile e sul solo sistema "advanced"), qualora tale prestazione sia fornita dalla soluzione proposta.	
R.12	In modalità "localizzazione" il modulo radiogoniometrico di cui si avvale il sistema non deve avere bisogno di ulteriori veicoli e <i>software</i> , ma deve essere integrato nello stesso programma di gestione dell'apparato. A livello <i>hardware</i> , deve avere bisogno al più dell'aggiunta della sola antenna direttiva.	

Tabella 2 – Funzionamento in modalità attiva

6.3.3 Requisiti riferiti alle soluzioni implementative adottate

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
R.13	<p>Il contenitore che ospita l'unità centrale ed il PC di controllo/gestione deve essere un trolley con guscio rinforzato (nel documento denominato anche portapacchi standard da auto per trasporto apparecchiature).¹⁰</p> <p>Lo stesso deve pertanto essere predisposto per consentire i cablaggi necessari all'utilizzo del sistema con tutti i moduli attivi allocati al suo interno (dovrà pertanto essere dotato di patch panel per alimentazione, networking, collegamenti radio etc...) e con involucro chiuso.</p> <p>La disposizione dei connettori per il cablaggio verso l'esterno (alimentazione, antenne , etc..) deve essere ingegnerizzata con nicchie interne preservando le connessioni da sporgenze , urti e strappi accidentali.</p>	
Q.7	<p>Il volume complessivo del contenitore non deve superare i 130 litri. La dimensione massima del contenitore (altezza, profondità o larghezza) non deve superare i 90 cm e la somma delle tre dimensioni non deve superare i 180 cm.</p> <p>Fermi restanti i limiti sopra esposti, il punteggio è assegnato su scala lineare riferita al volume secondo la formula descritta al par.5.1 con aggiudicazione del massimo punteggio alla soluzione con il minor volume. Indicare il volume in litri e le dimensioni in cm.</p>	<p style="text-align: center;">Punti</p> <p style="text-align: center;">4</p> <p style="text-align: center;">INV</p>
Q.8	<p>Il peso complessivo del sistema non deve superare i 40 kg.</p> <p>Fermi restanti i limiti sopra esposti, il punteggio è assegnato su scala lineare riferita al peso secondo la formula descritta al par.5.1 con aggiudicazione del massimo punteggio alla soluzione con il minor peso. Indicare il peso in Kg.</p>	<p style="text-align: center;">Punti</p> <p style="text-align: center;">4</p> <p style="text-align: center;">INV</p>

¹⁰ L'utilizzo del sistema su vetture non predisposte ed assegnate all'apparecchiatura in maniera stabile comporta la necessità di smontaggio ed installazione presso vetture differenti; l'alloggiamento dei moduli del sistema in un unico trolley ne aumenta la robustezza meccanica e ne facilita il trasporto.



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
I.6	Per ciascun modulo del sistema deve essere indicato il parametro MTBF (<i>Mean Time Between Failure</i>).	
R.14	Il modulo di scansione della rete radiomobile deve essere integrato nel sistema, sia dal punto di vista di assemblaggio meccanico che in termini di modulo software integrato alla GUI di cattura dei telefoni.	
R.15	Il fornitore dovrà adottare un'architettura scalabile in termini di nodi/stazioni radio base simulabili su ciascuna tecnologia rispetto alla configurazione oggetto di offerta. La soluzione architetture deve essere tale che i moduli aggiuntivi successivamente acquistabili siano gestibili sulla stessa consolle di gestione del sistema originario.	
R.16	Il fornitore deve indicare l'intervallo di temperature in cui è garantita la corretta operatività e lo stoccaggio del sistema. Detti intervalli devono includere rispettivamente il range 0°+45°C per il funzionamento e -20°+70°C per l'immagazzinamento. Il sistema deve poter gestire il surriscaldamento come evento non distruttivo e monitorabile.	
Q.9	Il punteggio è assegnato alla soluzione che, al raggiungimento della prossimità della massima temperatura tollerabile, provvede alla notifica all'operatore con un allarme prima dello shutdown/blocco di protezione.	Punti 2
R.17	Alimentazione: il sistema deve poter essere alimentato dalla tensione di rete e dalla tensione della batteria del veicolo su cui è installato. Il sistema, qualora ne preveda l'inserimento, deve essere fornito corredato di 2 <i>inverter</i> per l'impiego veicolare con le seguenti caratteristiche minimali: ingresso 12V DC, uscita 220 V AC, potenza $\geq 1,3 * P_{max}$ [W] ¹¹ , tipologia ad onda sinusoidale pura (<i>pure sine wave inverter</i>).	
R.18	Il fornitore deve indicare l'assorbimento di corrente nelle condizioni di utilizzo a massimo regime (modalità attiva con tutte le celle simulate impostate alla massima potenza trasmittiva). Il sistema deve poter funzionare alla massima potenza anche con l'autovettura in sosta con il motore al minimo regime e per un periodo di almeno cinque minuti. In caso di spegnimento del motore e/o calo di tensione, il sistema deve poter gestire l'eventuale arresto del funzionamento senza riportare danni.	
R.19	L'antenna radiogoniometrica, in dotazione, deve avere la dimensione massima (tra altezza, lunghezza e profondità) non superiore a 30 cm.; le antenne stilo omnidirezionali in dotazione devono avere la dimensione massima inferiore a 10 cm e devono essere adatte all'utilizzo su veicoli non specializzati (ad esempio con supporto ad attacco magnetico).	
R.20	Tutti i componenti oggetto della fornitura devono essere consegnati completi di quanto necessario per il loro utilizzo (cavi di alimentazione, cavi di connessione, adattatori, materiali di consumo di prima dotazione, ecc.).	
R.21	La soluzione proposta deve essere orientata alla riduzione dell'impatto visivo a valle della installazione presso i veicoli dell'Amministrazione e collocando all'esterno le antenne trasmittenti. All'esterno del veicolo devono essere installate al più 3 antenne trasmittenti.	
R.22	Per favorire l'utilizzo sotto copertura del sistema, le antenne trasmissive, oltre ad essere fornite singolarmente, devono essere fornite anche in versione integrata all'interno di un manufatto trasparente alle onde radio. Il sistema dovrà essere corredato di apposito miscelatore che renda possibile l'utilizzo simultaneo di tutti i nodi attivi (anche se ciascuno è impostato su frequenze diverse). Il sistema radiante,	

¹¹ P_{max} è la massima potenza assorbita dal sistema in configurazione attiva con tutti i nodi in trasmissione con il massimo livello di segnale. Nel computo di tale potenza devono essere inclusi i consumi del PC con cui si realizza la consolle di controllo, nonché gli altri apparati inclusi nella fornitura necessari al funzionamento delle configurazioni possibili (es. miscelatore per ricorso ad antenna integrata unica sul tetto)

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI
	da applicarsi sul tetto all'esterno del veicolo, deve assumere la forma di antenna a pinna di squalo tipica delle antenne radio di serie dei SUV della serie X BMW. Conservandone le proporzioni e la forma l'antenna così ottenuta deve essere al più il 30% più grande rispetto a quella di serie
R.23	<p>Caratteristiche di protezione meccanica.</p> <p>L'utilizzo del sistema in uno scenario operativo outdoor, su veicolo o a spalla (in caso di eventuali moduli estraibili portatili), richiede resistenza alle sollecitazioni meccaniche. Le apparecchiature destinate all'uso su veicolo, devono essere in grado di sopportare le sollecitazioni e gli urti tipici degli automezzi senza che ciò causi degrado del loro funzionamento. Il sistema deve aderire alle normative di resistenza della serie ETSI 300 019 parte 2-5, specifiche T5.1 "Protected Installation" indicandone la classe di protezione certificata.</p>
R.24	<p>L'unità centrale deve integrare un ricevitore GPS. Tra le caratteristiche minime se ne richiede una sensibilità minima di -150dBm ed un TTFF (time to first fix) minore di un minuto.</p> <p>Il sistema GPS deve essere testato per garantire la sua efficace utilizzabilità anche durante il funzionamento in modalità attiva dell'IMSI Catcher con i nodi settati alla massima potenza.</p>
R.25	<p>Localizzazione Fine.</p> <p>Il sistema deve essere equipaggiato con uno smartphone android o IOS comprensivo di APP dedicata al pilotaggio di un ricevitore radio. Il ricevitore, periferica Bluetooth del palmare, deve poter essere sintonizzato dall'APP sulla frequenza e sul canale logico in cui è forzato un target in silent call durante il direction finding. Questo deve essere possibile almeno in tecnologia 2G e 3G. Il ricevitore deve essere corredato di antenna direttiva di dimensioni inferiori o uguali a 5x16x16cm.</p> <p>L'APP deve restituire in maniera acustica e grafica una misura qualitativa dell'intensità di segnale in base all'orientamento e alla prossimità del target.</p>
R.26	<p>Le funzionalità attive correlate ad attacchi MITM sia sul sistema imsi catcher trasportabile (qualora realizzate) che sull'unità tattica wireless, devono poter essere attivate sui sistemi a valle dell'inserimento e tracciamento dell'operatore che esegue l'attività, dati del decreto autorizzativo.</p> <p>Si faccia riferimento al paragrafo 6.4 Caratteristiche tecniche di valutazione: unità tattica WiFi</p>

Tabella 3 – Soluzioni implementative

6.3.4 Requisiti riferiti all'interfaccia locale e data management

Il sistema deve essere fornito corredato di due unità di interfaccia locale per consentire un'immediata sostituzione in caso di rottura di quella in uso. Entrambe devono avere le stesse caratteristiche e *suite software* di dotazione per consentirne un'immediata intercambiabilità.

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI
R.27	<p>Il PC di gestione utilizzato come interfaccia locale deve essere dimensionato affinché possa supportare le funzionalità del sistema nelle condizioni di impiego al massimo regime elaborativo (scansione su tutte le RAT, funzionamento attivo simultaneo su tutti i nodi e contemporanea attivazione del Direction Finding, attacchi MITM ove previsti), soddisfacendo comunque i requisiti minimi di seguito indicati:</p> <ul style="list-style-type: none"> processore: di prestazioni pari o superiori a intel i-7, clock 1.7 GHz o superiore, cache 6MB L3(o



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
	<p>altro con prestazioni equivalenti o superiori)</p> <ul style="list-style-type: none"> • Certificazione di resistenza circa le condizioni d'uso estreme: MIL-STD-810 o superiore • Certificazione di protezione alla penetrazione di corpi solidi e polveri: IP65 o superiore • RAM 8G espandibile • Hard disk 1 TB o superiore • Lettore/masterizzatore DVD, Dual Layer RW standard +/- • Tastiera QWERTY e sistema operativo in lingua italiana • Monitor: LCD $\geq 15''$ • Scheda Grafica: 2GB dedicata DDR3 • Connettività: Ethernet 10/100/1000; WiFi; Bluetooth; USB 3.0 • Batteria: ioni di litio con numero di celle ≥ 6 (autonomia di almeno 4h) • Accessori: alimentatore con adattatore per auto 	
Q.10	<p>Il fornitore deve indicare l'eventuale presenza nella soluzione proposta delle seguenti funzionalità di georeferenziazione delle misure, alle quali saranno attribuiti i punteggi indicati:</p> <ul style="list-style-type: none"> - il <i>software</i> di gestione è integrato con il modulo GPS e dotato di cartografia nazionale geo-referenziata aggiornabile. Il software deve riportare su mappa la posizione in cui si trova il sistema durante il suo impiego. (Punti 1) - con il sistema attivo in modalità "localizzazione" il software di gestione fornisce su mappa indicazioni circa la posizione stimata del MS <i>target</i>. (Punti 2) - il sistema deve essere in grado di rappresentare su mappa i segmenti di percorso in cui sono stati rilevati gli SSID di interesse (punti 2) 	<p>Punti 5</p>
R.28	<p>Il sistema deve agevolare le attività di analisi dell'operatore durante le sessioni di monitoraggio. Con riferimento a quanto riportato al paragrafo 6.2 Gestione dei dati raccolti si riportano di seguito i requisiti minimi utili al supporto analitico alle attività condotte dagli operatori in tempo reale, durante la missione.</p> <p>Tutti i dati raccolti devono poter essere esportati in formato non proprietario coadiuvando l'attività di <i>reporting</i>. Tra le prestazioni minime si richiede:</p> <ul style="list-style-type: none"> • la visualizzazione in tempo reale dei dati raccolti circa i terminali agganciati (sulla base delle informazioni scambiate in aria dal terminale IMSI/TIMSI/IMEI/SSID/Channel, Mac Address e SSID associato). • evidenza delle utenze che sono state già censite nell'ambito di più sessioni di misura con aggregazione delle informazioni programmabile sui livelli descritti al paragrafo citato. Questo deve valere anche circa i Mac Address rilevati in WiFi con riporto delle diverse SSID in cui il MAC è stato censito. • evidenza delle utenze già censite per le quali sia avvenuto un cambio SIM o apparato; in altri termini terminali che sono stati già censiti (stesso IMEI) con altra SIM inserita (diverso IMSI) o, viceversa, di SIM già censite (stesso IMSI) ma installate su terminali diversi (diverso IMEI). • in tutti i casi di cattura di utenze già censite in sessioni diverse devono poter essere evidenziate (in tempo reale e durante la sessione di cattura ancora in corso) le missioni in cui sono avvenute le catture precedenti (es: nome missione e data /ora di cattura, posizione GPS del sistema...) • evidenza di utenze appartenenti a liste <i>target</i> preimpostate entrate in aggancio con lo strumento (con segnalazione acustica e visiva sul sistema di gestione) <p>Nei dati di cattura in tempo reale devono poter essere distinguibili i dati di nuovi censimenti dalle ripetizioni di attach di utenti già censiti e ricaduti nell'area di competenza dell'apparato nell'ambito della stessa sessione di cattura.</p>	



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
R.29	Il sistema deve fornire indicatori in tempo reale circa le performance di cattura dei singoli nodi impostati in modalità attiva; ciascun nodo impostato nella clonazione deve essere identificabile rendendo possibile un apprezzamento qualitativo delle singole performance.	
R.30	<p>Con riferimento ai dati di cattura, il software di gestione deve supportare anche funzionalità di post-analisi dei dati raccolti con possibilità di impostazione di query e livello di aggregazione dei dati configurabile (singolo task, missione e luogo o combinazioni di questi).</p> <p>Deve poter essere possibile porre condizioni di filtraggio sul numero di catture per luogo, missione, task, date orari o presenza di altre utenze note.</p>	
R.31	<p>Il <i>software</i> associato al sistema deve fornire supporto alla preparazione delle sessioni di misura.</p> <p>Si richiede il caricamento dell'anagrafica delle utenze target di interesse (descrivere le possibilità di anagrafica gestite quali, ad esempio, campi alfanumerici, fotografie, modalità di caricamento...) consentendone la selezione/impostazione come <i>target</i> su base IMEI e/o IMSI e/o SSID.</p>	
Q.11	Il punteggio sarà assegnato alla soluzione che, per agevolare il data entry delle utenze target di interesse, preveda il completamento automatico del codice IMEI ed il riconoscimento del TAC ¹² con facoltà di aggiornamento del database.	<p>Punti</p> <p>1</p>
Q.12	<p>Il soddisfacimento dei seguenti requisiti consentirà l'aggiudicazione di punteggio aggiuntivo in base alla conformità con le caratteristiche indicate di seguito:</p> <ul style="list-style-type: none"> - gestione delle principali funzionalità di scansione e cattura con un'interfaccia locale implementata su <i>tablet</i> o <i>smartphone</i> al fine di aumentarne la possibilità di occultamento d'uso. In tal caso, <i>software</i> e terminale dovranno essere inclusi nella fornitura. (Punti 3) - dall'interfaccia grafica ed il relativo <i>software</i> di navigazione deve essere possibile il tracciamento su mappa dei percorsi eseguiti durante le misure. Deve essere possibile attivarne e disattivarne la visualizzazione. Il tracciamento deve essere possibile sia in corso del solo censimento dei terminali presenti sia nel corso del direction finding. (Punti 2) - caricamento delle stazioni radio base nelle tecnologie 2G/3G/LTE-4G e 5G (quando disponibile e solo sul sistema "advanced") con la rappresentazione del cono di radio-copertura presunto. Il formato dei dati da inserire e le caratteristiche di visualizzazione sono rappresentati in allegato. (Punti 1) - possibilità di selezionare i POI (<i>point of interest</i>) da visualizzare sulla cartografia (ad esempio estraendoli dalle anagrafiche delle utenze <i>target</i>, come indirizzi, luoghi significativi pre-anagrafati, posizioni dello strumento in cui sono avvenuti gli agganci delle utenze target con filtro sull'utenza di riferimento). Deve poter essere possibile tracciare aree di interesse sulla cartografia. (Punti 1) - rappresentazione su mappa dei posizionamenti da cui lo strumento ha rilevato/agganciato i <i>target</i>, facilitando così la pianificazione di ulteriori passaggi di cattura nelle zone di interesse. (Punti 1) - rappresentazione su mappa di figure quali rettangoli, cerchi, poligoni. (Punti 1) 	<p>Punti</p> <p>9</p>

¹² Modello del terminale radiomobile



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER - WIFI	
I.7	Con riferimento al supporto dell'operatore in termini di pianificazione ed effettuazione delle sessioni di cattura, il fornitore deve descrivere altri eventuali <i>tool</i> di rappresentazione grafica o elaborazione delle informazioni raccolte ed inclusi nella soluzione proposta.	
I.8	<p>Funzioni diagnostiche. Il fornitore deve descrivere gli indicatori supportati nel modulo di gestione per la valutazione delle prestazioni dello strumento. A mero titolo esemplificativo:</p> <ul style="list-style-type: none"> • contatori/tassi di richieste di IMSI <i>attach</i> in rapporto ai tassi di acquisizione dei terminali mobili; una forbice elevata potrebbe ad esempio suggerire di ridurre la velocità di movimento del veicolo durante l'uso dello strumento in modalità attiva • possibilità di generazione ed estrazione di file log in modalità "<i>debug</i>" in modo da consentire, ad esempio, l'analisi del comportamento in rete, le mimiche protocollari a livello RRC. Per limitare la mole di dati acquisiti deve essere possibile modulare il range di azione della modalità <i>debug</i> (tempo di attivazione, IMSI, IMEI, SSID, Host su cui operare). 	
Q.13	<p><i>Operation & Maintenance</i> Il punteggio è attribuito se la soluzione offerta prevede per il sistema l'instaurazione di sessioni di tele-gestione. In tale ambito l'operatore deve poter attivare una modalità di funzionamento con controllo remoto che consenta al fornitore o ad un operatore dell'Amministrazione di interagire con il sistema acquisendo le informazioni di configurazione, i <i>log</i>, nonché consentire eventuali <i>upgrade firmware</i>. Eventuali software applicativi da installare presso le postazioni dell'operatore remoto devono essere a corredo della fornitura e compatibili con l'ambiente Windows.</p>	<p>Punti 3</p>
R.32	L'interfaccia locale/PC di gestione deve poter interagire con il sistema di monitoraggio e localizzazione includendo almeno la possibilità di connessione Ethernet e WiFi.	

Tabella 4 – Interfaccia locale

6.4 Caratteristiche tecniche di valutazione: unità tattica WiFi

Nei paragrafi successivi i concetti esposti al paragrafo 6.1 circa l'ambito applicativo di riferimento vengono esplosi nel dettaglio dei requisiti tecnici di fornitura.

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER – WIFI E SISTEMI ANALISI ATTIVA RETI WIFI	
R.33	<p>L'interfaccia grafica di gestione dell'unità tattica wifi deve essere unica ed integrata di tutte le funzionalità atte all'utilizzo dell'apparecchiatura; amministrazione utenze, scansione passiva, modalità attiva e attacchi MITM.</p> <p>Per favorire l'uso tattico indor dell'apparecchiatura, la gestione delle principali funzionalità di scansione e cattura deve poter essere implementata su un'interfaccia locale su tablet o smartphone. Software e terminale dovranno essere inclusi nella fornitura.</p>	
R.34	L'unità tattica, in modalità passiva, deve erogare almeno le seguenti funzioni: di scansione delle reti WiFi presenti, riconoscimento di reti già viste in altre missioni, censimento dei terminali e dei relativi mac, riconoscimento di terminali già censiti, affiliazione dei terminali alle diverse reti attive nell'area, correlazione ai terminali censiti delle SSID a questi note.	



Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER – WIFI E SISTEMI ANALISI ATTIVA RETI WIFI	
	<p>I dati di cattura in fase passiva devono poter essere aggregati per SSID; per ogni terminale agganciato deve essere rappresentato il livello di segnale. I dati di primo e ultimo aggancio, tipo di terminale, protocolli/AP/indirizzo mail utilizzati dal terminali grazie alla relativa cattura del traffico. Devono essere censiti anche i terminali non agganciati a nessun Hot Spot ma con wifi attivo.</p> <p>La gestione dei dati per il modulo WiFi deve essere implementata con gli stessi livelli di aggregazione previsti per l'unità integrata trasportabile (caso, missione, luogo, vedi paragrafo 6.2).</p>	
R.35	<p>Il sistema deve essere in grado di emulare hot-spot in tutte le bande disponibili. In caso di reti protette da cifratura, il sistema deve essere in grado di superare almeno la crittografia WEP.</p> <p>Il sistema deve quindi essere in grado di catturare gli handshake tra hot spot e terminale con lo scambio di credenziali.</p>	
Q.14	<p>Il punteggio sarà assegnato alla soluzione in grado di superare la cifratura WPA e WPA2</p>	<p>Punti 5</p>
R.36	<p>La potenza radio in WiFi per l'SSID clonato deve poter essere regolata. Il valore massimo deve essere paria da almeno 400mW.</p>	
R.37	<p>Con riferimento alla gestione dei dati raccolti in fase di censimento delle reti e dei terminali, la soluzione offerta deve:</p> <ul style="list-style-type: none"> • Consentire l'export in formati standard (almeno csv) • Fornire maschere di interrogazione che consentano l'effettuazione di query sui terminali censiti correlando tali informazioni almeno con i luoghi, tempi, ssid di aggancio. 	
R.38	<p>Il sistema deve poter gestire la popolazione di un database di terminali target a cui associare un profilo, foto, e policy da applicare in caso di rilevamento di un terminale di interesse investigativo.</p>	
R.39	<p>Per favorire l'aggancio di dato target ad un SSID fake appositamente realizzato dal sistema, la soluzione proposta deve essere in grado di:</p> <ul style="list-style-type: none"> • operare un jamming selettivo sul MAC/Canale dell'hot spot presso cui è accampato il terminale target stesso • forzare lo sgancio dalla rete hot-spot reale del target 	
Q.15	<p>Il punteggio sarà assegnato in relazione alle prestazioni di attacco supportate dalla soluzione offerta:</p> <ul style="list-style-type: none"> • Dns poisoning/redirection : punti 2 • http redirection : punti 2 • https downgrade : punti 2 • java script injection : punti 2 • mirroring pagine di accesso ai sociale per cattura credenziali di account: punti 3 	<p>Punti 11</p>

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER – WIFI E SISTEMI ANALISI ATTIVA RETI WIFI
R.40	<p>L'utilizzo delle funzionalità di attacco deve essere subordinato a due fattori imprescindibili:</p> <ul style="list-style-type: none"> • il riconoscimento dell'operatore che sta eseguendo l'operazione. Ad ogni attivazione dell'attacco devono essere inserite le credenziali dell'operatore • la sussistenza di un decreto autorizzativo associato alla missione. In una data missione le funzioni di attacco possono essere utilizzate solo se sono stati definiti i campi descrittivi del decreto (procura, PP, etc...). • ad ogni impiego delle funzionalità di attacco MITM le informazioni suddette devono essere oggetto di log • il file di log deve essere inalterabile salvo la sua corruzione in modalità rilevabile. <p>Il fornitore deve pertanto sviluppare il sistema includendo nel software di gestione la realizzazione di un gruppo di utenze, l'encryption delle password degli operatori e la relativa gestione tutelata a valle della loro attivazione.</p> <p>Il super user crea o resetta gli account degli operatori. L'operatore al primo utilizzo sarà obbligato al cambio password. In caso di smarrimento la password , deve essere previsto un meccanismo di self-recovery (es: domande segrete); in caso di fallimento la password non sarà recuperabile in alcun modo se non attraverso il reset da parte del super-user.</p>
R.41	<p>Altre caratteristiche obbligatorie per la soluzione proposta:</p> <ul style="list-style-type: none"> • Avere un ingombro nei tre lati uguale o inferiore a 200X150X100 mm • Peso inferiore a 3 Kg per l'unità tattica e 3kg per il pacco batteria • Essere dotato di espansione di memoria tramite Slot SD e di una card slot mini Sim <p>Inoltre dovrà essere dotata di</p> <ul style="list-style-type: none"> • Connettori esterni per antenne WiFi e GPS • Interfaccia Ethernet 100/1000 • Modem LTE

6.5 Caratteristiche tecniche di valutazione: affidabilità e servizi

Id.	FUNZIONALITA' RICHIESTE SISTEMA IMSI CATCHER – WIFI E SISTEMI ANALISI ATTIVA RETI WIFI	
Q.16	<p>Sarà assegnato un punteggio aggiuntivo per ciascun semestre di proroga della garanzia/manutenzione incluso nell'offerta (fino ad un massimo di 10 punti anche qualora il fornitore offra più di due semestri aggiuntivi di manutenzione/garanzia). Indicare il numero dei semestri aggiuntivi.</p> <p>5 punti per ogni semestre aggiuntivo</p>	<p>Punti</p> <p>10</p>

Tabella 5 – Affidabilità e Servizi

7 Presentazione dell'offerta tecnica

Lo schema di offerta tecnica richiesto dovrà essere conforme a quanto riportato di seguito:

1. Presentazione del fornitore.
2. Sistema proposto.

Relazione Tecnica descrittiva della fornitura proposta con dettaglio delle caratteristiche tecniche delle componenti. In particolare il fornitore dovrà produrre una descrizione dei sistemi in moduli logico/funzionali e la relativa allocazione nei moduli fisici di cui la soluzione stessa si compone.

Compilazione delle tabelle riportate nel paragrafo 6.3, 6.4, 6.5 e relativi sottoparagrafi. Ai fini di una più agevole valutazione delle offerte, le risposte ai quesiti posti nei paragrafi seguenti dovranno essere riportate in tabelle che ne riproducono la struttura, introducendo il testo nei rispettivi riquadri e fornendo i richiami alle sezioni della Relazione Tecnica in cui la materia è trattata in maniera estesa. Si precisa che tutte le soluzioni proposte dovranno essere nella piena disponibilità del fornitore, senza oneri aggiuntivi per l'Amministrazione e che quanto descritto nella Relazione Tecnica e in risposta ai quesiti costituirà di per sé dichiarazione di impegno del fornitore all'esecuzione nei tempi e modi descritti nella documentazione stessa consegnata.

3. Help Desk.

Descrizione della modalità di erogazione del servizio di Help Desk.

4. Manutenzione.

Descrizione delle modalità con cui il fornitore intende garantire i livelli di servizio richiesti.

5. Formazione.

Dettaglio del programma e modalità dei corsi da erogare.

La relazione tecnica dovrà essere redatta in modo da porre in evidenza gli elementi necessari alla commissione giudicatrice per l'attribuzione dei punteggi.

La relazione tecnica dovrà essere firmata siglata in ogni pagina e sottoscritta per esteso, a pena d'esclusione, all'ultima pagina dal legale rappresentante del concorrente (o da persona munita da comprovati poteri di firma).

Il numero di pagine, esclusa la copertina, l'indice, dovrà essere massimo 100. I parametri di redazione dei documenti saranno: Carattere Calibri, stile normale, corpo 11, per le tabelle corpo 10, dimensioni foglio A4.

8 Presentazione dell'offerta economica

L'offerta economica deve essere redatta secondo i seguenti schemi:

SOCIETA	(DA REPLICARE IN CASO DI RTI)
CODICE FISCALE	(DA REPLICARE IN CASO DI RTI)

OGGETTO			
Requisito	Q.TA'	IMPORTO UNITARIO	IMPORTO TOTALE
<p>Sistema completo.</p> <p>Il fornitore deve riportare il costo per la fornitura del sistema completo così come descritto al paragrafo 4</p>			
<p>Sistema completo "advanced".</p> <p>Il fornitore deve riportare il costo per la fornitura del sistema completo così come descritto al paragrafo 4</p>			
<p>Servizio di Help Desk telefonico.</p> <p>Il fornitore deve riportare il costo per la fornitura del servizio di <i>help desk</i>.</p>			
<p>Formazione</p> <p>Il fornitore deve riportare il costo per l'erogazione del pacchetto di formazione come descritto al paragrafo 4.5.</p>			
<p>Manutenzione Sistema completo.</p> <p>Il fornitore deve riportare il costo del servizio di manutenzione in garanzia, come descritto al paragrafo 4.4.</p> <p>Il fornitore deve precisare il numero di annualità di manutenzione che intende erogare.</p>			
<p>Manutenzione Sistema completo "advanced".</p> <p>Il fornitore deve riportare il costo del servizio di manutenzione in garanzia, come descritto al paragrafo 4.4.</p> <p>Il fornitore deve precisare il numero di annualità di manutenzione che intende erogare.</p>			
<p>Altro.</p> <p>Il fornitore deve indicare eventuali costi non incluse nelle precedenti voci, indicandone uno per ogni riga.</p>			
TOTALE (IVA esclusa)			
Oneri per la sicurezza previsti dall'art. 26, comma 6), del D. L.vo n. 81/2008			

Tabella 6 – Offerta economica

9 Documentazione relativa ai prodotti

Il fornitore deve fornire almeno una copia della documentazione tecnica e della manualistica d'uso e installazione relativa alle apparecchiature hardware ed ai prodotti software, di base ed applicativi, oggetto della fornitura. La documentazione deve essere redatta in lingua italiana o inglese e deve essere fornita sia in formato cartaceo (manuali) che su supporto elettronico (CD-ROM).

9.1 Documentazione di gestione del sistema

Al termine della consegna e dell'implementazione dei materiali, il fornitore deve rilasciare dettagliata documentazione relativa a:

- Procedure per la conduzione del sistema:
 - Lista operazioni importanti per la corretta gestione del sistema;
 - Indicazione delle attività critiche di gestione;
- Procedure operative da seguire in caso di fault del sistema:
 - Criteri di valutazione del fault;
 - Procedure da attuare in caso di guasti più gravi;
 - Elenco dei contatti.

9.2 Documentazione del software

Dovrà essere fornita tutta la documentazione prodotta, relativa ai sistemi software, oggetto della fornitura (*technical reference, operator & service guide, installation guide, tuning guide etc.*).

La documentazione deve essere redatta in lingua italiana o inglese e deve essere fornita su supporto cartaceo (manuali) ed elettronico (CD-ROM).

Deve inoltre essere prodotta, a cura del fornitore, una completa e circostanziata documentazione di fornitura, installazione, collaudo e configurazione relativa:

- alle operazioni d'installazione e configurazione effettuate sulla console;
- agli eventuali problemi incontrati;
- alle soluzioni adottate.

10 Verifica di conformità

Il fornitore deve approntare al collaudo il sistema, oggetto della fornitura, entro 90 (novanta) giorni solari decorrenti dalla data di comunicazione dell'avvenuta esecutività del contratto. Entro tale termine il sistema deve essere completamente configurato e operativo.

A tal fine il fornitore deve procedere a:

- effettuare il precollaudo in fabbrica con il rilascio del relativo statino;
- produrre il piano di test;
- rendere funzionanti le componenti software e hardware previste dalla fornitura;

- configurare le componenti software di gestione e controllo secondo le specifiche richieste dall'Amministrazione, fornendone adeguata documentazione.

10.1.1 Verifica di funzionalità del sistema

Le attività di verifica di funzionalità sono dirette a verificare la conformità della fornitura con l'offerta tecnica presentata dal fornitore, nonché, per quanto da questa non previsto, alle specifiche e alle indicazioni del presente documento.

10.1.2 Precollauda in fabbrica

Il sistema deve essere sottoposto alle prove di precollauda in fabbrica a cura del fornitore ed il relativo statino di collauda deve essere reso disponibile all'Amministrazione. Tali prove dovranno essere mirate a riscontrare la completa funzionalità del sistema, oltrech  a prevedere un esplicito riferimento all'esecuzione di test inerenti i requisiti di seguito specificati, corredati da adeguata documentazione sulle modalit  di esecuzione/certificazione e sui risultati ottenuti. In particolare, in riferimento alle funzionalit  riportate nel paragrafo 6.3, si richiede di documentare i seguenti punti: R.1, R.4, R.7, I.2, R.8, I.5, R.9, R.10, R.34, R.35, R.39.

Il superamento del precollauda in fabbrica   condizione necessaria per l'approntamento al collauda.

10.1.3 Verifica di conformit 

Il fornitore deve produrre, entro 20 (venti) giorni dall'approntamento al collauda, un piano di test che deve essere approvato dall'Amministrazione, le verifiche, oltre al rispetto delle funzionalit  previste dal piano di test proposto dal fornitore riguarderanno l'esecuzione di prove da effettuarsi in campo con la simulazione degli scenari operativi di impiego con automezzi messi a disposizione dall'Amministrazione.

Dieci giorni lavorativi prima dell'approntamento al collauda il fornitore deve consegnare il sistema presso i locali dell'Amministrazione per essere sottoposto alle prove di verifica della funzionalit .

Il fornitore garantir  tutta l'assistenza necessaria e metter  a disposizione dell'Amministrazione tutte le apparecchiature, gli strumenti ed i terminali radiomobili necessari all'effettuazione delle verifiche di funzionalit .

Le prove verranno eseguite con le modalit  previste nel piano di test proposto dal fornitore ed accettato dall'Amministrazione, fatta salva la facolt  della Commissione di collauda di richiedere ulteriori verifiche o integrazioni.

ALLEGATO

Con riferimento al requisito Q.12 del lotto 1 di seguito si riporta il maggior dettaglio circa le prestazioni minime richieste per il modulo cartografico integrato nel software di gestione dell'apparato.

Nella figura 1 è riportato, a scopo esemplificativo, l'aspetto con cui dovranno essere rappresentati gli elementi grafici di seguito descritti. Per preservare un livello adeguato di leggibilità della cartografia deve essere possibile abilitare e disabilitare in maniera selettiva la visualizzazione su mappa degli elementi cartografici. Ciascun elemento grafico avrà inoltre un riempimento con parziale trasparenza, al fine di non coprire completamente la topografia e la toponomastica sottostante anche quando ne viene abilitata la visualizzazione.

Tracciamento su mappa dei percorsi eseguiti: deve essere possibile abilitare e disabilitare il tracciamento dei percorsi eseguiti durante il funzionamento in modalità attiva dello strumento. Il sistema memorizzerà il percorso seguito e l'operatore potrà scegliere di visualizzarne o meno il tracciato al fine di verificare la presenza di aree scansionate o meno nel territorio di interesse.

I percorsi restano memorizzati e quindi visualizzabili nel contesto del "task" "missione" "luogo". Ossia all'avvio dell'utilizzo dello strumento viene creato / riaperto un "task", e viene creata / riaperta una "missione" e viene definito il "luogo" al fine di catalogare e gestire i dati rilevati (si faccia riferimento al paragrafo 6.2 Gestione dei dati raccolti). Ogni volta che in tale contesto viene innescata la modalità "attiva" di funzionamento, il sistema incrementa la collezione dei punti di tracciato eseguito. Alla chiusura del lavoro, ad esempio per apertura di un nuovo task/missione/luogo, il tracciato visualizzabile è azzerato.

Point of Interest (POI): il modulo deve consentire all'operatore di introdurre sulla cartografia elementi grafici che contraddistinguano luoghi di interesse investigativo (abitazioni, punti di frequentazione del target, luogo del crimine...). L'abilitazione della loro visualizzazione su mappa (in figura 1 è stato scelto ad esempio un rombo rosso) deve abilitare anche la lettura del campo di testo descrittivo appositamente inserito. Per salvaguardare la leggibilità della mappa le informazioni associate saranno leggibili all'interazione con il mouse (sovrapposizione del simbolo o sua selezione) con il simbolo. Il sistema deve prevedere una funzione di data entry per l'inserimento dei POI. Il POI è un dato globale del livello di aggregazione "task". Ad esempio, se in una missione viene creato un nuovo POI, questo sarà visibile ed utilizzabile in tutte le successive "missioni" e "luoghi" che saranno realizzate nello stesso task.

Punti di aggancio dei target: il sistema memorizzerà le posizioni data e ora in cui sono stati agganciati i telefoni target. L'abilitazione della loro visualizzazione consentirà di verificare la posizione dello strumento su mappa ed al passaggio del mouse sarà possibile evidenziare alcune delle informazioni salienti dell'evento (alias del target, IMSI, IMEI, data e ora della cattura). I punti di aggancio del target sono dati globali del "task". Un aggancio di un target deve poter essere visualizzato in tutte le sessioni di lavoro

Aree di interesse su mappa: sulla base delle informazioni ricevute dai gestori di rete o da fonti di investigazione, è necessario poter rappresentare sulla cartografia delle aree geografiche di interesse. Il sistema deve consentire pertanto il tracciamento di poligoni o comunque l'evidenziazione di aree.

Rappresentazione dei ponti radio: deve essere possibile il caricamento della banca dati delle BTS, nodeB ed e-nodeB (2G/3G/4G) dell'intero territorio nazionale di tutti i gestori. Il modulo cartografico del software di gestione deve abilitare la visualizzazione selettiva delle celle dei singoli operatori, per tecnologia e consentendo la visualizzazione selettiva delle celle.

Le celle saranno rappresentate con il cono teorico di irraggiamento così come fornito dai gestori di rete e rappresentato nel file csv di caricamento di seguito esemplificato. Per la rappresentazione deve essere adottato un cono di irraggiamento con apertura angolare di 120° e puntamento ottenuto con vertice nelle coordinate GPS fornite in tabella e direzione indicata in gradi in verso orario con lo 0° in direzione Nord.

Le celle saranno rappresentate di default con un raggio di copertura pari a 1000 metri in modo da limitarne le sovrapposizioni in area urbana. Per mantenerne una adeguata leggibilità anche in aree rurali, dove risultano intervallate da maggiori distanze, deve essere possibile impostarne il raggio di copertura ad ampiezze maggiori.

Di seguito è riportato un esempio del file da cui deve essere effettuato il caricamento.



csv2_prova_voda.csv
v



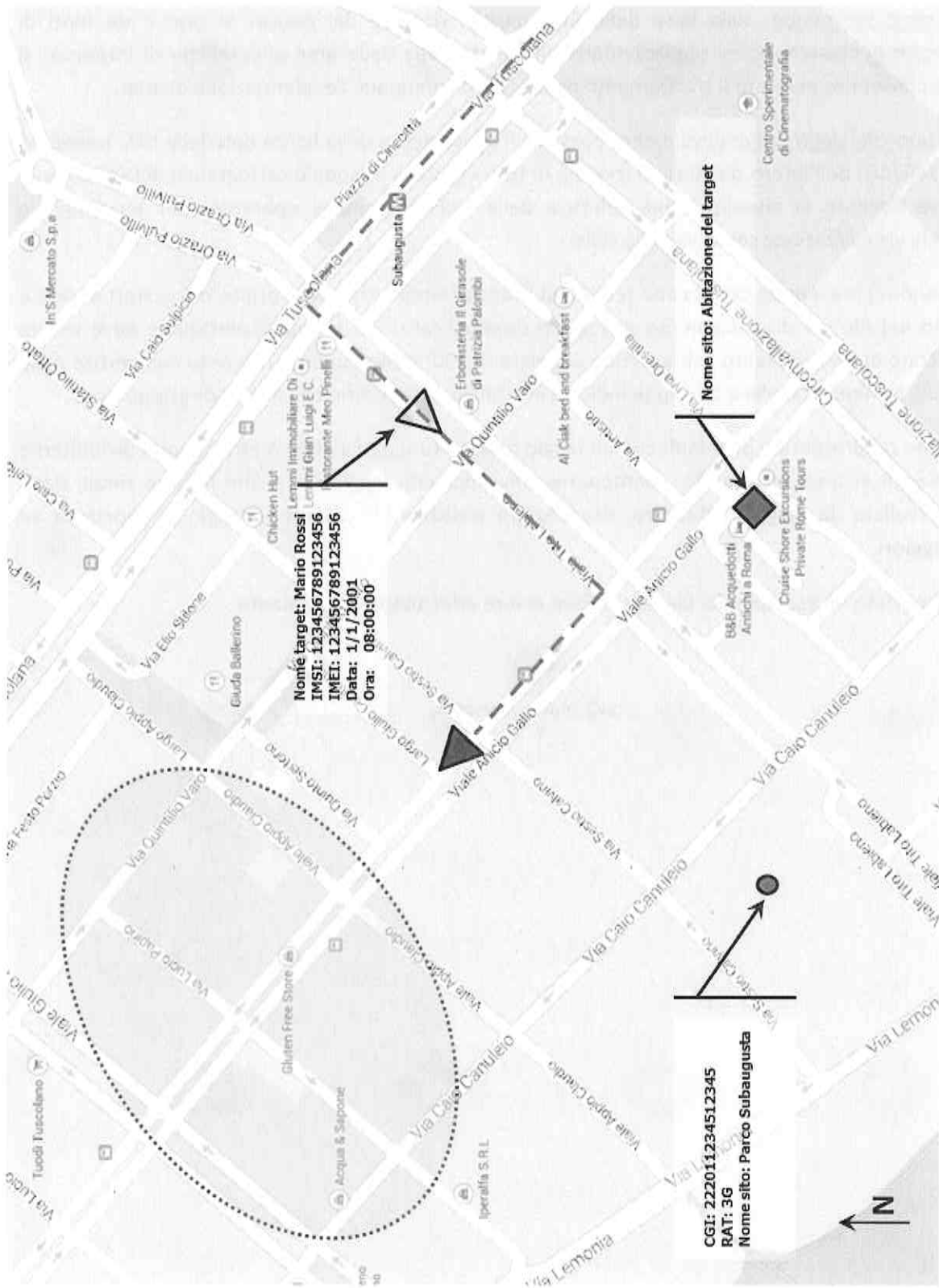


Figura 1

