1. Attivazione del Servizio IT-Alert

L'attivazione del "servizio IT-Alert" richiede che, nel rispetto degli standard 3GPP TS 23.041 V15.3.0 (2018-09) "Technical realization of Cell Broadcast Service (CBS)", ogni operatore di telefonia realizzi e mantenga in operatività h24 presso le proprie sedi almeno una coppia di entità CBC (Cell Broadcast Centre), finalizzata al trasferimento immediato dei messaggi ricevuti dalle corrispondenti entità CBE (Cell Broadcast Entity) alle proprie infrastrutture di rete, e da qui, in modalità broadcast, a tutti i dispositivi cellulari ad esse agganciati (**Figura *1***).

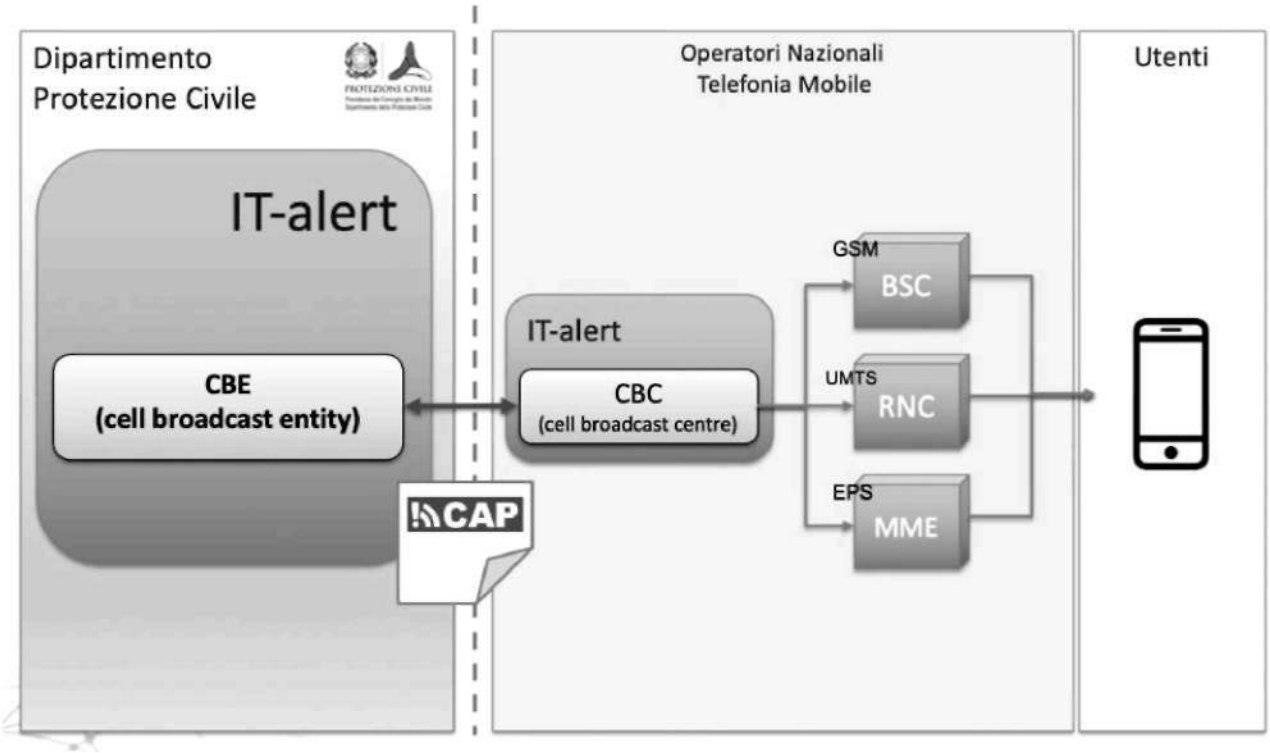

Figura 1. Servizio IT-Alert. Schema della catena di trasmissione.

Di seguito i requisiti utente e di sistema che dovranno essere rispettati per la realizzazione delle entità CBC:

1. Ogni sottosistema CBC deve essere realizzato facendo riferimento agli standard 3GPP TS 23.041 “Technical realization of Cell Broadcast Service (CBS)”. I requisiti mirano a raggiungere le caratteristiche della V15.3.0 (2018-09) degli standard, pur nella consapevolezza che ciascun operatore potrà implementare tale versione in tempi diversi e successivi all’entrata in operatività del servizio IT-Alert. La prestazione di invio di messaggi Cell Broadcast (CBS) dovrà comunque essere garantita entro le scadenze previste per tutte le tecnologie (2G, 3G, 4G e 5G) per le quali ciascun operatore è titolare di diritti d'uso per frequenze nazionali.

2. Ogni sottosistema CBC deve distribuire i messaggi a tutti i nodi della rete dell’operatore telefonico in modo che, per ogni tecnologia operativa, questi vengano inoltrati contemporaneamente, in modalità broadcast, a tutte le celle delle BTS attive comprese nell’area target e, di conseguenza, ai dispositivi cellulari in quel momento connessi.

3. Ogni sottosistema CBC deve raggiungere tutti i nodi della rete telefonica e ripetere il messaggio verso tutte le utenze attive nelle celle selezionate, comprese le utenze dei “roamers”, degli MVNO e degli MNO che condividono la rete di accesso radio.

4. Ogni sottosistema CBC deve accettare in ingresso il formato CAP come definito nella versione 1.2 dello standard Oasis e dettagliato nella specifica nazionale CAP-IT.

5. Ogni messaggio, contenente al massimo 93 caratteri (con riferimento agli alfabeti di 7 bit di cui allo standard tecnico 3GPP TS 22.038), deve essere inviato ai dispositivi cellulari attivi nell’area target entro 3 minuti dall’istante di ricezione da parte del CBC, ed essere ripetuto, per tutto il periodo di validità, secondo la frequenza prevista. L’invio di messaggi di lunghezza superiore a 93 caratteri (sempre con riferimento agli alfabeti di 7 b–it) non deve eccedere di 3 minuti il tempo tecnico di trasmissione.

Eventuali criticità che dovessero emergere in fase di realizzazione saranno prese in considerazione per una eventuale modifica dei requisiti di timing.

6. Per ogni messaggio ricevuto da CBE ogni sottosistema CBC deve restituire in tempo reale un messaggio di “corretta ricezione” o di “errore”.

7. Per ogni messaggio ricevuto, ottenuto l’esito della trasmissione dagli elementi della rete di accesso radio, ogni Operatore deve restituire un report con le informazioni relative al messaggio (identificativo univoco, tipo, contenuto, inizio e fine invio, ripetizioni), nonché l’elenco contenente il codice CGI/e CGI, la tecnologia, la posizione della BTS e la direzione di irradiazione delle celle a cui, per ogni tecnologia, è stato inviato il messaggio per la trasmissione e l’esito della trasmissione.

8. Ogni sottosistema CBC deve essere connesso con il Dipartimento della Protezione Civile attraverso link privati ad alta affidabilità.

9. Il testo e tutte le meta-informazioni di ogni messaggio, tra cui l’area target, il periodo di validità e la frequenza di ripetizione, dovranno essere ricavati dalla decodifica del messaggio CAP-IT ricevuto. Allo stesso modo, il CBC dovrà inviare le informazioni di risposta nello stesso formato.

10. Le entità CBC di uno stesso operatore devono essere realizzate per lavorare in alta affidabilità e disponibilità continua h24, ed essere installate presso due nodi geograficamente distribuiti. Il presente requisito non preclude tuttavia soluzioni per l'implementazione del CBC che prevedano la condivisione con più reti dello stesso operatore o di più operatori e/o la virtualizzazione in cloud privato ovvero l'esternalizzazione del servizio CBC, fermo restando l'onere per l'operatore al rispetto delle specifiche del presente documento e delle prescrizioni di sicurezza applicabili agli operatori quali infrastrutture critiche. Al fine di assicurare le attività di prevenzione e monitoraggio, l'eventuale collocazione della funzione CBC fuori dei confini nazionali dovrà essere valutata e autorizzata di caso in caso.

11. Ogni CBC dovrà accettare solo messaggi certificati provenienti da fonti autorizzate. Le rispettive chiavi pubbliche e/o i certificati digitali saranno scambiati in modo sicuro con ciascun operatore.

12. Al fine di evitare ogni possibilità di invio di messaggi Cell Broadcast che non siano stati debitamente autorizzati, è fatto carico a ciascun operatore di adottare opportuni sistemi di sicurezza per proteggere l'accesso ai sottosistemi CBC conformemente alle prescrizioni di cui all'articolo 4 del decreto del MISE del 12 dicembre 2018, recante misure di sicurezza ed integrità delle reti di comunicazione elettronica e notifica degli incidenti significativi, pubblicato nella Gazzetta Ufficiale, Serie Generale n.17 del 21-01-2019.

13. Presso le sedi di installazione delle entità CBC ogni Operatore dovrà consentire l'installazione degli apparati di rete e delle connessioni necessarie per la ricezione dei messaggi. Agli Operatori è dato il compito di fornire l'hosting degli apparati (raffrescamento e continuità energetica) e di consentire l'accesso per tutti i successivi interventi di manutenzione secondo un protocollo da concordarsi tra le parti.

14. La comunicazione verso e dalle entità CBC avverrà secondo il pattern Publish/Subscribe. Il CBE esporrà un broker a cui tutti i CBC si dovranno registrare e restare in attesa di messaggi. Al ricevimento di un messaggio dalla coda, i CBC dovranno processarlo e, successivamente, inviare la risposta al CBE tramite il broker stesso.

15. Prima dell'inoltro sulla rete cellulare ogni CBC dovrà verificare la doppia firma digitale associata al messaggio CAP-IT con cui gli è stato trasmesso.

2. Attivazione dei messaggi IT-Alert

Ogni entità CBC realizzata come descritto in precedenza dovrà processare due tipi di messaggi:

- Messaggi Broadcast: sono i messaggi che devono essere inoltrati sulla rete cellulare;
- Connection Test: sono i messaggi per la verifica dello stato di funzionamento delle entità CBC (non devono essere propagati sulla rete).

Per discriminare tra i due tipi di messaggi è necessario fare riferimento ai seguenti campi dello standard CAP-IT:

- Alert.msgType: identificativo CAP del tipo di messaggio;
- Alert.status: identificativo CAP dello stato del messaggio;
- Alert.scope: identificativo CAP della visibilità del messaggio;
- Alert.restriction: identificativo CAP della eventuale lista di restrizioni di visibilità del messaggio.

La **Tabella *1*** riporta la valorizzazione dei campi nei due casi.

Messaggio IT-ALERT	Alert.msgType	Alert.status	Alert.scope	Alert.restriction
Messaggio Broadcast	. Alert . Update . Cancel	Actual	Public	-
Connection Test	Alert	Test	Restricted	CBC

Tabella 1. Valorizzazione dei campi del tracciato CAP-IT per la discriminazione dei messaggi "broadcast" e dei messaggi "test connection".

Tutti i messaggi che avessero una diversa combinazione di questi campi dovranno essere rifiutati dal CBC con un opportuno messaggio di risposta di tipo "Error".

*CC.1 **Messaggio Broadcast***

La formalizzazione delle comunicazioni prevede che ogni messaggio inviato da un'entità CBE sia ricevuto da tutte le entità CBC in ascolto.

In **Figura** *2* è schematizzato il flusso dei messaggi fra CBE e CBC nel caso di invio di un Messaggio Broadcast:

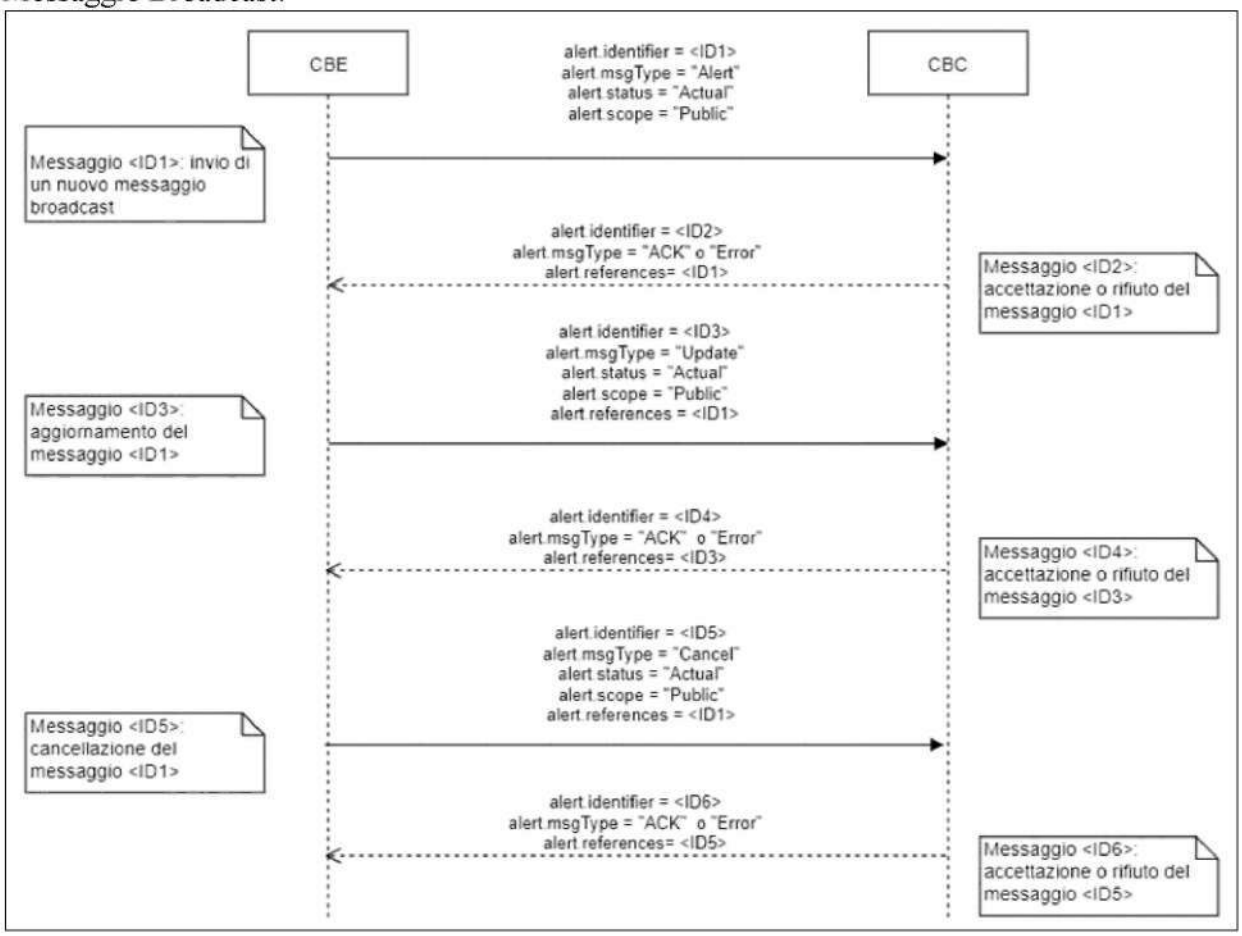

Figura 2. Servizio IT-Alert. Schema del flusso dei messaggi fra CBE e CBC nel caso di invio di un messaggio Broadcast.

Dopo i controlli preliminari dettagliati alla lettera f), è previsto che ogni entità CBC risponda all'entità CBE con un messaggio di corretta ricezione (acknowledge) o di rifiuto (error), a loro volta formalizzati in un nuovo messaggio CAP-IT.

La valorizzazione dei diversi campi è riportata in **Tabella** *2*.

TIPO DI MESSAGGIO	Campi del formato CAP-IT	valori
Nuovo Messaggio Broadcast	<Alert.identifier>	ID1
	<Alert.msgType>	Alert
	<Alert.status>	Actual
	<Alert.scope>	Public
Corrispondente accettazione o rifiuto	<Alert.identifier>	ID2
	<Alert.msgType>	"ack" o "error"
	<Alert.references>	ID1
Aggiornamento di un messaggio	<Alert.identifier>	ID3
	<Alert.msgType>	Update
	<Alert.status>	Actual
	<Alert.scope>	Public
	<Alert.references>	ID1
Corrispondente accettazione o rifiuto	<Alert.identifier>	ID4
	<Alert.msgType>	"ack" o "error"
	<Alert.references>	ID3
Cancellazione di un messaggio	<Alert.identifier>	ID5
	<Alert.msgType>	Cancel
	<Alert.status>	Actual
	<Alert.scope>	Public
	<Alert.references>	ID1
Corrispondente accettazione o rifiuto	<Alert.identifier>	ID6
	<Alert.msgType>	"ack" o "error"
	<Alert.references>	ID5

Tabella 2. Valorizzazione dei diversi campi del tracciato CAP-IT nel caso di Messaggio Broadcast

α.2 Test Connection

In **Figura** *3* è schematizzato il flusso dei messaggi fra CBE e CBC nel caso di "test connection".

Figura 3. Servizio IT-Alert. Schema del flusso dei messaggi fra CBE e CBC nel caso di Test Connection.

La valorizzazione dei diversi campi è riportata in **Tabella** *3*.

TIPO DI MESSAGGIO	Campi del formato CAP-IT	valori
Nuovo messaggio Test Connection	<Alert.identifier>	ID1
	<Alert.msgType>	Alert
	<Alert.status>	Test
	<Alert.scope>	Restricted
	<Alert.restriction>	CBC
Corrispondente accettazione o rifiuto	<Alert.identifier>	ID2
	<Alert.msgType>	"ack" o "error"
	<Alert.references>	ID1

Tabella 3. Valorizzazione dei diversi campi del tracciato CAP-IT nel caso di Test Connection.

3. Contenuti dei messaggi IT-Alert

Le procedure di Protezione Civile che dovranno essere seguite per l'invio di ogni singolo messaggio IT-Alert devono, in primo luogo, individuare la sua tipologia, definendo i nove item riportati in **Tabella *4***, tra cui le soglie di attivazione per il loro trigger. Le procedure le soglie e trigger sono stabiliti d'intesa con le Regioni e le Province autonome.

art.	Item	Opzioni
01	Fase	• Test • Previsionale • Monitoraggio • Emergenza • Esercitazione • …
02	Rischio	• Idrogeologico e Idraulico • Tsunami • Temporali • Generico • …
03	Tipo	• Automatico • Manuale
04	Trigger	• Test • Emissione stato di allerta Idrogeologica e Idraulica • Attivazione sistema SIAM • Superamento soglie strumentali • Emergenza conclamata • Esercitazione
05	Area TARGET	• Aree pre-definite o Nazione o Regioni o Province o Comuni o Zone Allerta o Fasce Costiere

		• Poligonale libera
06	Time Start	• Data Emissione • Inizio periodo di Validità • Attivazione • Immediata
07	Time End	• Fine periodo di validità
08	Frequenza di ripetizione	• Valori pre-definiti • Valori liberi
09	Lingue	• Italiano • Inglese • Tedesco • etc.

Tabella 4. Possibili valorizzazioni dei nove Item individuati per la definizione della tipologia di messaggio IT-Alert

I testi di ogni messaggio saranno contenuti in un apposito campo del tracciato CAP-IT (info.description) che sarà ripetuto all'occorrenza in diverse lingue.

Lo standard tecnologico a cui, dal 2012, hanno aderito tutti i produttori di dispositivi cellulari, definisce le regole per la ricezione e la presentazione dei messaggi di testo sui dispositivi degli utenti, che avviene come una "notifica", ovvero attraverso un "pannello modale" (che prende il sopravvento sul display), che contiene il testo e attende un click di conferma.

Ogni pannello, oltre a una intestazione fissa, può contenere fino a 93 caratteri di testo (spazi inclusi).

Per messaggi più lunghi lo standard consente la possibilità di concatenare fino a 15 pannelli che si presentano, in sequenza, a seguito dei "tap" dell'utente sul tasto OK.

Oltre al semplice testo, lo standard afferma che l'apparato ricevente deve poter processare anche un identificativo URL di una risorsa Internet o un numero telefonico che siano presenti nel testo del messaggio.

4. Gestione della richiesta per l'attivazione dei messaggi IT-Alert;

Tutte le informazioni necessarie per la gestione della richiesta di attivazione di un'istanza di messaggio IT-Alert avverrà tramite protocollo CAP-IT.

Ogni file che incapsulerà un messaggio CAP-IT valido sarà quindi definito da un tracciato standard XML che conterrà tutti gli estremi del messaggio secondo lo schema definito e sarà composto da un segmento <Alert>, da uno o più segmenti <Info> e, per ciascuno, uno o più segmenti <Area> e <Parameter> (**Figura *4***)

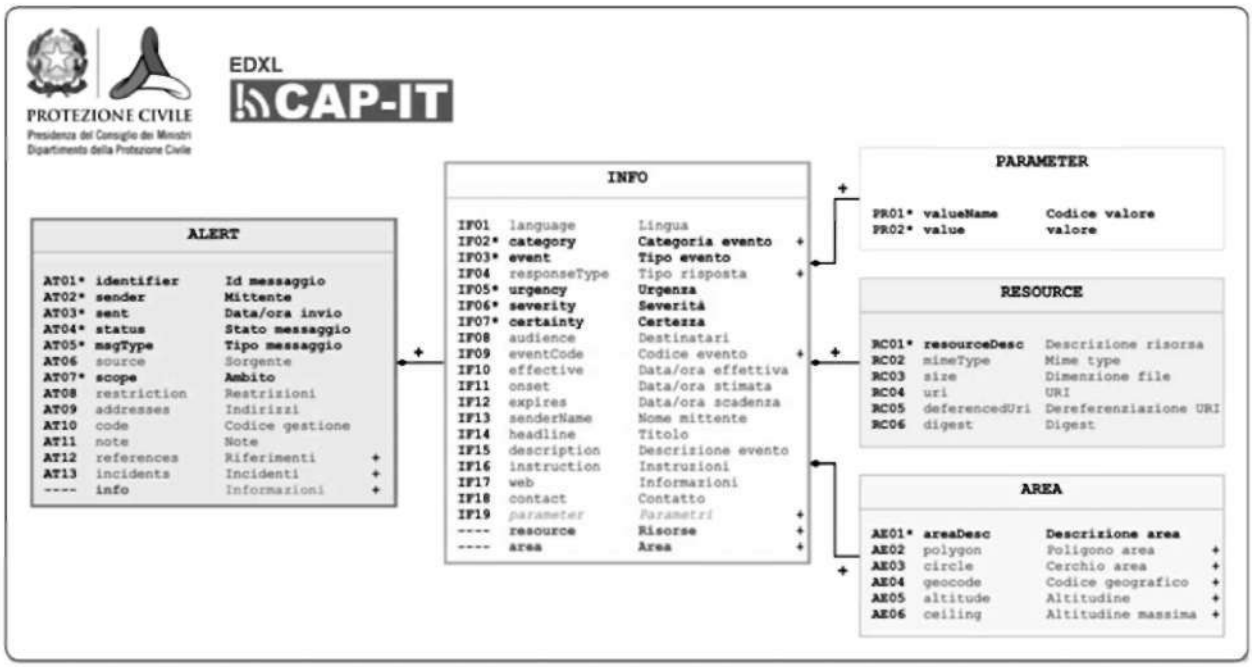

Figura 4 Richiesta attivazione messaggi IT-Alert. Schema CAP-IT

Ogni CBC dovrà ricavare le informazioni tramite la mappatura dei campi del tracciato CAP riportata in **Tabella *5***.
Viene usata la seguente convenzione tipografica:

- **Obbligatorio**: il grassetto è utilizzato per i campi del CAP-IT obbligatori
- *Condizionale*: l'Italico è utilizzato per i campi del CAP-IT condizionali
- Opzionale: il carattere normale è utilizzato per i campi del CAP-IT opzionali

Campo CAP-IT	Possibili valorizzazioni	Note
Alert.identifier	• 55f91a3f-48de-4d4b-88b0-b010fb252d28	Identificativo alfanumerico univoco del messaggio in formato GUID. Deve essere valorizzato e viene utilizzato dal CBC per i seguenti scopi: • Il CBC deve usare tale identifier nelle risposte, ACK o ERROR, copiandolo nel campo Alert.references per dare riscontro al CBE • In caso il messaggio sia stato accettato, il CBC deve mantenere l'informazione che questo messaggio è stato correttamente processato e, nel caso lo ricevesse nuovamente, dovrà rispondere con un ACK ma non processare nuovamente il messaggio stesso.
Alert.sender	• DPC-CBE-RM • DPC-CBE-SV • TIM-CBC-RM • TIM-CBC-BO • VOD-CBC-MI • VOD-CBC-FI • WI3-CBC-RM • WI3-CBC-MI • ILD-CBC-MI • ILD-CBC-RM	Il campo è valorizzato con l'identificativo univoco del mittente in formato testuale e serve ad effettuare la verifica della firma del messaggio. Ogni CBC ed ogni CBE saranno identificati da un codice univoco. L'entità che invia dovrà impostare il proprio identificativo nel campo Alert.sender. Nel caso dei messaggi inviati dal CBE, qualunque problema in questi passaggi comporta lo scarto del messaggi e la relativa risposta ERROR.
Alert.status	• "actual" • "test"	Il CBC dovrà considerare solo messaggi in cui Alert.status è valorizzato con "actual" o "test".
Alert.msgType	• "Alert"	"Ack" ed "error" sono tipi di messaggi

Campo CAP-IT	Possibili valorizzazioni	Note
	• "update" • "cancel" • "ack" • "error"	inviati dal CBC in risposta ad un messaggi inviato dal CBE.
Alert.references	• 55f91a3f-48de-4d4b-88b0-b010fb252d28	Il campo è valorizzato se il messaggio è di tipo <Alert.msgType>: • Update • Cancel • Ack • Error Il campo è valorizzato se il messaggio è di tipo <Alert.status>: • Test Il campo deve contenere l'identificativo univoco del messaggio CAP a cui si riferisce.
Alert.scope	• Public • Restricted	Il campo indica la visibilità del messaggio. E' impostata a Public per l'invio dei messaggi Broadcast ed a Restricted per i messaggi di Test Connection
Alert.restriction	• CBC	Il campo deve essere valorizzato solo per i messaggi di tipo Test Connection quindi con Alert.scope = Restricted e riporta la dicitura convenzionale CBC.
info.language	• it-IT (Italiano); • en-EN (inglese) • Etc.	Lingua del messaggio, specificata secondo il codice internazionale RFC 3066. Essendo un campo obbligatorio, se non è valorizzato, si intende it-IT.
info.eventCode	• EAN (EU-Alert level 1) • RMT (required monthly report)	Se specificato, definisce univocamente il canale da usare per la trasmissione broadcast.

Campo CAP-IT	Possibili valorizzazioni	Note
info.urgency	• Immediate • Expected • Future • Past • Unknown	Ai fini della trasmissione broadcast è condizionale in quanto, sebbene sarà comunque valorizzato nel CAP-IT, deve essere ignorato dal CBC nel caso in cui nello stesso messaggio sia valorizzato il campo <info.eventCode>
info.severity	• Extreme • Severe • Moderate • Minor • Unknown	Ai fini della trasmissione broadcast è condizionale in quanto, sebbene sarà comunque valorizzato nel CAP-IT, deve essere ignorato dal CBC nel caso in cui nello stesso messaggio sia valorizzato il campo <info.eventCode>
info.certainty	• Observed • Likely • Possibile • Unlikely • Unknown	Ai fini della trasmissione broadcast è condizionale in quanto, sebbene sarà comunque valorizzato nel CAP-IT, deve essere ignorato dal CBC nel caso in cui nello stesso messaggio sia valorizzato il campo <info.eventCode>
info.description	"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris…."	Testo da inviare nel messaggio esposto nel formato UTF-8 nella lingua definita nel campo <info.language>. Gli apparati cellulari "pagineranno" il testo suddividendolo in pannelli da 93 caratteri.
info.onset	2019-06-09T22:11+01:00	Data e ora di inizio delle trasmissioni nel formato "Date Time" YYYY-MM-DDThh:mm:ssXzh:zm. Se non presente, l'invio si intende immediato.
info.expires	2019-06-09T23:11+01:00	Data e ora in cui si devono cessare la ripetizione del messaggio espressa nel

Campo CAP-IT	Possibili valorizzazioni	Note
		formato "Date Time" YYYY-MM-DDThh:mm:ssXzh:zm.
area.polygon	LAT1,LON1 LAT2,LON2 LAT3,LON3 LATn,LONn LAT1,LON1	Coordinate dei vertici (v) in formato WGS84, di una poligonale chiusa, convessa, espresse come numeri decimali separati da spazio. L'ultimo punto della poligonale deve essere uguale al primo (cfr. "criteri per l'individuazione delle aree target"). Almeno uno fra polygon, circle o geocode deve essere valorizzato.
area.circle	LATc,LONc KM	Coordinate del centro (c) in formato WGS84 e il raggio (r) espresso in chilometri di un'area target circolare (cfr. "criteri per l'individuazione delle aree target") Almeno uno fra polygon, circle o geocode deve essere valorizzato.
area.geocode	• "Comune di Roma; • "area di allertamento LIG-B"; • "Provincia di Napoli" • Etc	"codice" di una o più "features" note a priori, precedentemente inserite all'interno di appositi vocabolari controllati (cfr. "criteri per l'individuazione delle aree target") Almeno uno fra polygon, circle o geocode deve essere valorizzato.
parameter	• <valueName>repetition</valueName><value>250</value> • <valueName>repetition</valueName><value>1440</value> • etc	Eventuale indicazione del periodo di ripetizione dell'invio del messaggio. Se presente, deve avere la forma: <parameter> <valueName>repetition</valueName> <value>value</value> </parameter>

Campo CAP-IT	Possibili valorizzazioni	Note
		Dove value è espresso come un numero intero di secondi compreso nell'intervallo [0..4095].
Alert.note	• invalid-sender-id • Server-error • Invalid-format • …	Il campo è valorizzato solo nei messaggi di errore inviati dal CBC.

Tabella 5. Mappatura tra campi del tracciato CAP-IT e informazioni di interesse/supportate dai CBC.

5. Modalità di autorizzazione della richiesta di attivazione di un messaggio IT-Alert;

Prima dell'inoltro di un messaggio sulla rete cellulare, ogni CBC dovrà verificare la doppia firma digitale associata al formato CAP-IT con cui gli è stato trasmesso.

Le comunicazioni avverranno secondo il protocollo TLS 1.2.

Ogni macchina inclusa nella rete dovrà, una tantum, generare una propria coppia di chiavi pubblica e privata. Con la chiave pubblica verrà generato un apposito certificato dalla Certification Authority che verrà resa disponibile all'interno della rete. Questo certificato varrà per le comunicazioni TLS, per verifica delle firme dei messaggi e per la firma dei messaggi di risposta.

A livello software, la sicurezza del messaggio dal CBE al CBC viene garantita da una doppia firma del messaggio CAP-IT che deve essere verificata da parte del CBC prima dell'invio fisico sulla rete. La doppia firma rappresenta la certificazione del sistema (automatico, semi

automatico o manuale) che in origine ha scatenato il messaggio e del CBE che lo ha ricevuto, processato ed inoltrato al CBC.

Per implementare questa doppia firma, il messaggio CAP-IT viene incapsulato in un apposito tag xml denominato <it_Alert></it_Alert>, contenente al suo interno:

2. Il messaggio cap originale, con l'aggiunta di un attributo *"id"* al tag <Alert> necessario per poterlo "riferire";
3. Le firme <ds:Signature></ds:Signature> che fanno riferimento al tag xml che incapsula il vero e proprio cap <Alert></Alert>;

Lo schema riportato in **Figura *5*** rappresenta la struttura dei tag del messaggio che verrà ricevuto dal brocker.

```
<it_alert>
    <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2" id="cbe cap it alert">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
</it_alert>
```

Figura 5. Srvizio IT-Alert. Struttura dei tag XML del messaggio CAP-IT inviato dal CBE.

L'operazione di verifica delle firme restituisce il documento xml che rappresenta il solo CAP-IT (senza il tag che lo incapsula e, ovviamente, senza le firme).

Analogamente, le risposte dal CBC verso il CBE dovranno essere firmate. In questo caso la firma sarà singola. Lo schema dei tag XML è rappresentato in **Figura *6***:

```
<it_alert>
    <alert xmlns="urn:oasis:names:tc:emergency:cap:1.2" id="cbe cap it alert">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
</it_alert>
```

Figura 6. Servizio IT-Alert. Struttura dei tag XML del messaggio CAP-IT di risposta dal CBC.

6. Modalità di invio dei messaggi IT-Alert;

Tulle le regole tecniche per la realizzazione del servizio IT-Alert sono raccolte nello standard ETSI TS 102 900 V1.2.1 (2012-01) "European Public Warning System (EU-Alert) using

the Cell Broadcast Service" a cui l'intero progetto si riferisce, e che contiene le indicazioni per uniformare il protocollo di comunicazione tra tutti i paesi europei.

Come riportato in **Tabella *6***, Il protocollo EU-Alert è utilizzato in Italia per l'invio di cinque tipologie di messaggi.

#	Tipo	messaggio	Disattivazione notifiche
1	IT-Alert level 1	Messaggi di allerta a maggiore severità	No
2	IT-Alert level 2	Messaggi di allerta a severità media	Si
3	IT-Alert level 3	Messaggi di allerta a bassa severità	Si
4	IT-Monthly test	Messaggio specifico per il test mensile	Si
5	IT-Excercise	Messaggio specifico per le esercitazioni	Si

Tabella 6. Classificazione dei tipi di messaggio secondo l'interpretazione italiana dello standard EU-Alert

I messaggi di tipo 1, 2 e 3, sono i veri e propri messaggi di allerta utili per informare i cittadini di una situazione di pericolo imminente e sono contraddistinti da tre livelli di gravità decrescente.

Per i messaggi di allerta di livello 1, ovvero a maggiore severità, le notifiche non possono essere disattivate ed il messaggio sarà comunicato a prescindere dalle opzioni di ricezione disposte sull'apparato ricevente.

Per tutti gli altri tipi di messaggio ogni utente finale può disattivare dal proprio dispositivo cellulare la ricezione delle notifiche.

A parità di tutti gli altri campi valorizzati nel tracciato CAP-IT, il CBC discriminerà il messaggio in base al campo <info.event> o, in alternativa, in base alla combinazione dei campi <info.severity>, <info.urgency> e <info. certainty> e lo invierà attraverso opportuni canali a priori definiti.

Oltre questo, il CBC selezionerà il canale di invio anche a fronte della valorizzazione del campo info.language.

La **Tabella *7*** mostra la corrispondenza tra i tipi di messaggio dello Standard EU-Alert e la valorizzazione dei campi del tracciato .XML del formato CAP-IT.

Nelle ultime due colonne i canali di trasmissione rispettivamente nel caso della sola lingua italiana e nel caso di più lingue:

		Message identifier				
Standard EU-Alert	CAP-IT info.event	CAP-IT info.severity	CAP-IT info.urgency	CAP-IT info.certainty	Canale di trasmissione per messaggi relativi alla sola lingua italiana	Canale di trasmissione per messaggi relativi a più di una lingua
EU-Alert Level 1	EAN	-	-	-	4370	4383
EU-Alert Level 2	-	Extreme	Immediate	Observed	4371	4384
EU-Alert Level 3	-	Extreme	Immediate	Likely	4372	4385
EU-Monthly Test	RMT	-	-	-	4380	4393

Tabella 7. Corrispondenza tra i tipi di messaggio dello Standard EU-Alert e la valorizzazione dei campi del tracciato CAP-IT.

L'individuazione dell'area target, ovvero dell'area geografica a cui si intende inviare il messaggio (a tutte le utenze cellulari in essa attive) è definita nei segmenti "<Area>" del tracciato CAP.

Compito dei CBC è quello di attivare, ad ogni occorrenza e per tutte le tecnologie, tutte le celle installate presso le stazioni radio base (BTS) presenti nell'area indicata.

In ogni segmento la dimensione e la forma dell'area target possono essere definite mediante tre differenti metodi (**Figura *7***, **Figura *8*)**:

- <area.polygon>: il messaggio CAP-IT conterrà le coordinate dei vertici (v) in formato WGS84, di una poligonale chiusa, convessa, espresse come coppie LAT,LON di numeri decimali separati da spazio

- <area.circle>: il messaggio CAP-IT conterrà le coordinate LAT,LON del centro (c) e il raggio (r) espresso in chilometri.

- <area.geocode>: il messaggio CAP-IT conterrà il riferimento al "nome" di una o più "features" note a priori, precedentemente inserite all'interno di appositi vocabolari controllati (es: "Comune di Roma", "area di allertamento LIG-B", "Provincia di Napoli", ecc.).

I "vocabolari controllati" saranno resi disponibili agli Operatori con cadenza periodica, e conterranno, oltre al nome di ogni singola area target, anche la poligonale geografica che la rappresenta sul territorio.

Atteso che, in ogni caso, l'area target non sarà perfettamente sovrapponibile all'area di copertura delle celle e che una data area geografica può essere servita anche da celle/BTS ubicate all'esterno dei confini che descrivono l'area, il CBE invierà a ciascun CBC una poligonale già "estesa" rispetto all'area effettiva di interesse per l'invio dei messaggi IT-Alert affinché vengano individuate ed attivate tutte le celle che ragionevolmente offrono copertura all'interno dell'area di interesse ("Poligonale netta").

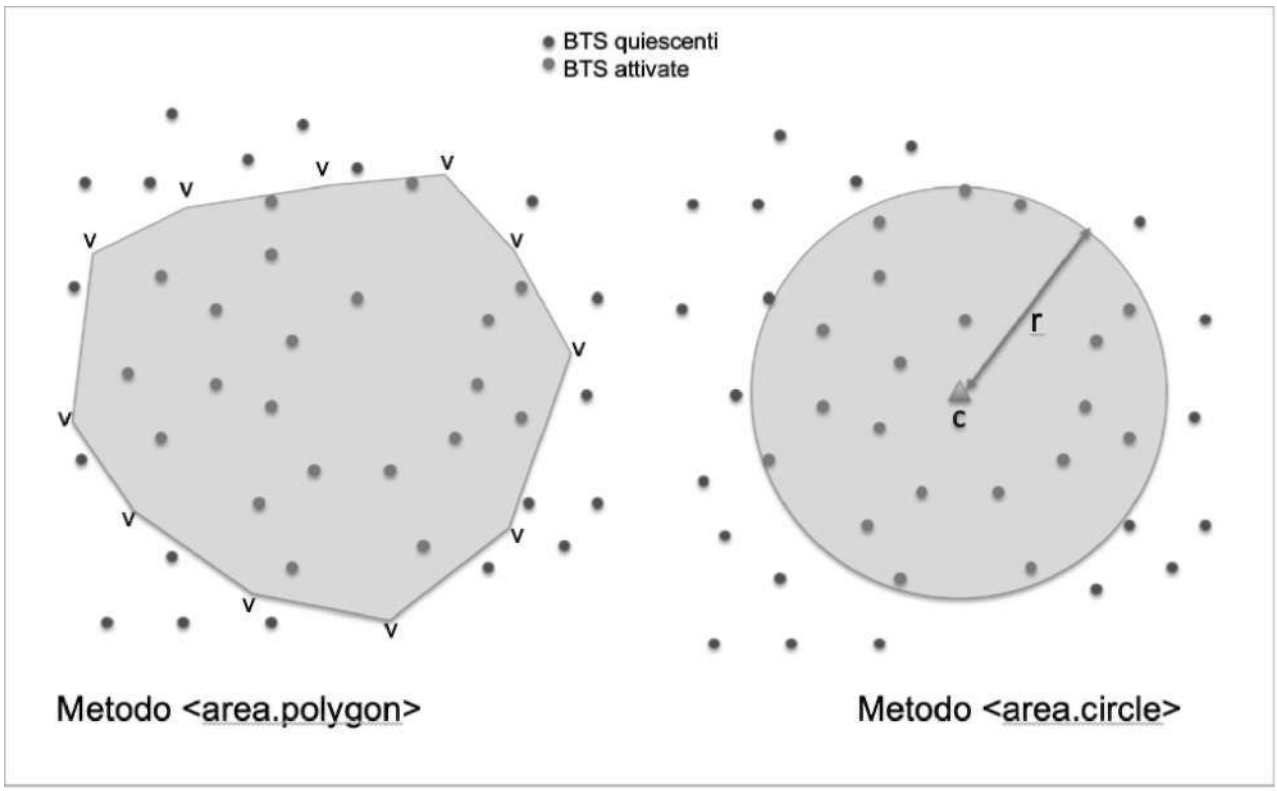

Figura 7. Messaggi IT-Alert. Definizione delle aree target con i metodi <area.polygon> e <area.circle>.

Per gli scopi del servizio, l'eventuale allertamento anche di utenti all'esterno dell'area target, in funzione dell'estensione e della forma dell'area di copertura delle celle individuate risulta, infatti, accettabile.

Nel caso dei messaggi automatici o semi-automatici l'area target nominale (corrispondente al nome della feature) nel corrispondente vocabolario sarà sempre associata a una figura geometrica opportunamente estesa, in modo che si possa massimizzare la copertura delle utenze all'interno di essa (**Figura 8)**.

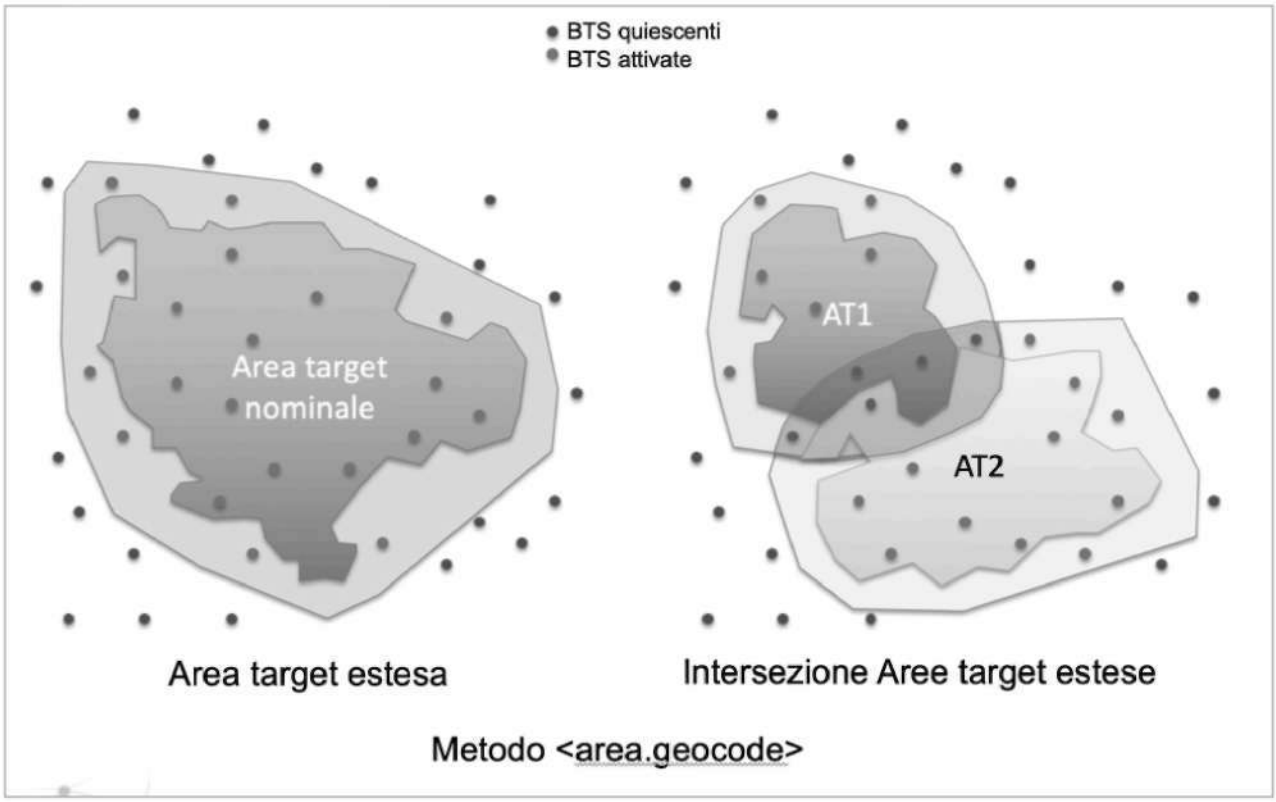

Figura 8. Piattaforma IT-Alert. Definizione delle aree target con il metodo <area.geocode>.

7. Rispetto della normativa in materia di protezione dei dati personali;

Il servizio IT-Alert viene erogato attraverso l'invio di messaggi con la tecnologia Cell Broadcast, come definita dagli standard ETSI TS 102 900 e 3GPP 23041. In particolare, il funzionamento del servizio non è basato sul numero dell'utente che deve ricevere il messaggio, essendo, invece - come specificato al paragrafo 2 dello standard 3gpp 23041 - un servizio analogo a quello televisivo, che consente l'invio generalizzato (broadcast o "radiodiffusione circolare") di messaggi a tutti gli apparati in grado di riceverli all'interno di una determinata area geografica.

Tale specificità tecnica pone il servizio IT-Alert al di fuori dello scopo della normativa sulla Privacy, non essendo necessaria, per chi invia il messaggio, alcuna informazione circa il ricevente, inclusi il numero di telefono, nominativo, etc. L'assenza di riscontro circa la ricezione del messaggio, rafforza l'assenza di qualunque violazione della privacy degli utenti.

È comunque fatto divieto di utilizzare dati comunque ricavabili dalla gestione del Servizio che non siano strettamente necessari per il funzionamento dei Servizio stesso e per gli scopi previsti dalla legge.