Sommario

REQUISITI TECNICI

Il presente documento ha per oggetto la definizione e la descrizione dei requisiti tecnici del sistema di allarme antirapina, di seguito denominato "Videoallarme", escludendo qualsiasi altra tipologia di allarmi (quali ad es. antintrusione, tamper, mancanza di rete, etc.), e costituisce parte integrante del Protocollo Quadro.

Attraverso il Videoallarme si ottengono segnalazioni di allarme nonché la visione e l'eventuale controllo delle immagini provenienti dai sistemi di videosorveglianza, installati presso gli esercizi commerciali/imprese, associati con le Confederazioni firmatarie, o presso gli esercizi commerciali/imprese non associati.

Il Videoallarme, attivabile esclusivamente tramite la volontà diretta del soggetto sottoposto ad azione criminale (attraverso la semplice pressione sul pulsante di comando), deve essere in grado di collegarsi con la Piattaforma installata presso le Sale/Centrali operative delle Forze di polizia e di trasmettere le immagini in tempo reale.

Il Videoallarme prevede il collegamento dei sistemi installati presso gli esercizi commerciali/imprese il cui flusso telematico, in caso di allarme, viene inviato direttamente alle sale operative delle Forze di polizia competenti per gli esercizi commerciali, ferma restando la possibilità di inoltrare l'allarme alle Sale/Centrali operative delle Forze di polizia attraverso la sala controllo dell'istituto di vigilanza autorizzato ai sensi dell'art.134 del Tulps.

Il Sistema di Videoallarme potrà avvalersi anche delle tecnologie standard di geolocalizzazione della refurtiva, attivate dall'utente/fruitore sottoposto ad azione criminale, con allarme filtrato e inoltrato dall'istituto di vigilanza autorizzato ai sensi dell'art.134 del Tulps, all'atto della conclamazione del reato.

In caso di Videollarme antirapina è fatto divieto di veicolare il flusso degli stessi a postazioni diverse da quelle previste dal presente disciplinare tecnico.

Restano salve le disposizioni riguardanti la normativa sul procurato allarme.

In caso di comprovata violazione delle disposizioni del presente disciplinare, il Comitato provinciale per l'ordine e la sicurezza pubblica potrà valutare la sospensione dell'autorizzazione all'utilizzo del sistema di Videoallarme antirapina con conseguente disattivazione del collegamento verso le Sale/Centrali operative delle Forze di polizia dell'esercizio commerciale interessato.

Le specifiche tecniche proposte nel presente documento sono da intendersi vincolanti.

Le variazioni degli indicati requisiti tecnologici devono essere concordate tra le Parti ed a tal fine viene istituito un apposito Tavolo tecnico permanente, che si riunisce con cadenza almeno semestrale, presieduto dall'Ufficio di Coordinamento e Pianificazione delle Forze di Polizia e con la partecipazione dell'Ufficio per l'Amministrazione Generale, della Direzione Centrale Servizi Tecnico Logistici e della Gestione Patrimoniale, della Direzione Centrale Anticrimine, nonché degli Uffici Operazioni e Sistemi Informativi del Comando Generale dell'Arma dei Carabinieri.

Analogamente, in relazione al progressivo evolversi delle tecnologie di trasmissione delle segnalazioni di allarme in forma multimediale, potrà essere attivato un tavolo tecnico dedicato, per lo studio e l'approfondimento delle modalità di implementazione del sistema.

INTEGRAZIONE CON I SISTEMI ESISTENTI PRESSO LE SALE/CENTRALI OPERATIVE

Il presente protocollo prevede l'integrazione con i sistemi informatici esistenti presso le Sale/Centrali operative delle Forze di polizia, presso le quali dovranno essere resi disponibili i flussi video in tempo reale provenienti dalle telecamere installate presso gli esercenti, per il tramite delle Sale controllo degli istituti di vigilanza, ovvero direttamente dagli esercizi commerciali/imprese, per la visualizzazione ed eventuale presa in carico degli stessi all'interno dei rispettivi applicativi.

ARCHITETTURA

L'architettura di sistema è descritta nel documento allegato (all.1 - schema esplicativo collegamenti).

Si riportano di seguito i vari aspetti caratterizzanti il sistema.

1. **CARATTERISTICHE DEL SISTEMA AUDIO/VIDEO E DELLA REGISTRAZIONE PRESSO GLI ESERCENTI**

Le caratteristiche del sistema Audio/Video e della registrazione delle immagini dei sistemi installati presso gli esercizi commerciali/imprese devono essere le seguenti:

a. risoluzione di ciascun video registrato non inferiore a 1280x720 pixel;
b. supporto della registrazione audio, non inferiore a 16 bit;
c. rappresentazione delle immagini a colori e in modalità day&night;
d. visualizzazione di una rappresentazione di tipo "full-motion" e la visione diretta di ogni particolare che prende parte all'evento criminoso in tempo reale non meno di 15 fps;
e. conservazione, presso l'esercente, dei filmati (audio + video) conformemente alla normativa vigente in materia di protezione dei dati personali;
f. informazioni di data/ora relativi al filmato ripreso. L'informazione su data/ora deve avere precisione minima al secondo e deve prevedersi un meccanismo di controllo e/o gestione a garanzia della precisione richiesta.

2. **SICUREZZA DELLE REGISTRAZIONI**

Il sistema Audio/Video, installato presso l'esercizio commerciale/impresa e utilizzato per la registrazione e la conservazione dei filmati, nel rispetto delle disposizioni in tema di tutela dei dati personali e in particolare del provvedimento in materia di videosorveglianza dell'8 aprile 2010, dovrà obbligatoriamente:

a. consentire l'estrazione delle informazioni registrate (audio e video) da parte degli Organi di Polizia Giudiziaria, garantendo la non ripudiabilità, la completezza e l'inalterabilità dei dati raccolti;
b. consentire l'accesso, presso l'esercente, ai dati attraverso un collegamento rapido con un generico personal computer, dotato del necessario software di lettura e assolutamente immodificabile nei contenuti;

c. includere un file di log, costantemente aggiornato e non modificabile da terzi, contenente la registrazione degli accessi e delle operazioni effettuate; tale file di log dovrà essere reso disponibile agli Organi di Polizia Giudiziaria;
d. essere protetto con efficaci misure (es. dispositivi con doppia chiave o con apertura ritardata del vano di alloggiamento del videoregistratore).

3. CARATTERISTICHE DELLE MODALITÀ DI INTERCONNESSIONE/ INTERFACCIAMENTO CON LE SALE/CENTRALI OPERATIVE DELLE FORZE DI POLIZIA

a. Il flusso video deve essere inviato mediante sistemi e protocolli per la comunicazione sicura su Internet che proteggano l'integrità, la riservatezza dei dati scambiati e ne garantiscano l'autenticazione (almeno con utilizzo del protocollo HTTPS).

b. I segnali videoallarmati verso le Sale/Centrali operative delle Forze di polizia devono essere convogliati attraverso un unico collegamento fisico per il tramite di una Sala Controllo di un Istituto di Vigilanza, ovvero direttamente verso ciascuna Sala/Centrale operativa delle Forze di polizia, quindi, rispettivamente:
- uno per la Sala operativa della Questura;
- uno per la Centrale operativa del Comando Provinciale/Gruppo dell'Arma dei Carabinieri,
che gestiranno l'intervento secondo le ordinarie procedure operative e le competenze ripartite sulla base del Piano coordinato di controllo del territorio previsto a livello provinciale.

c. Il punto di accesso delle Sale operative delle Forze di polizia deve avviare la registrazione del video in ingresso immediatamente, in caso di allarme, indipendentemente dalla successiva presa in carico da parte dell'operatore di Sala/Centrale operativa.

Il sistema tecnologico di acquisizione e gestione dei flussi multimediali (Media Server) utilizzato dalle Sale/Centrali operative delle Forze di polizia deve poter conservare in memoria le immagini allarmate (audio + video) pervenute e consentire il trattamento dei dati personali, in linea con le disposizioni del decreto legislativo del 18 maggio 2018, n.51.

Per la Polizia di Stato, il Media Server di ogni Questura espone su Internet *web services* adeguatamente protetti.

Per l'Arma dei Carabinieri, il Media Server "interno" di ogni Comando Provinciale/Gruppo si interfaccia in locale, presso la DMZ della Centrale operativa, con il Media Server "esterno", messo a disposizione dal soggetto privato fornitore del servizio (singolo esercente o istituto di vigilanza ex art. 134 TULPS).

Il Media Server "esterno" dovrà esporre web services, adeguatamente protetti, analoghi a quelli previsti dalla Polizia di Stato (vedasi punto precedente) funzionali a ricevere lo streaming video; sullo stesso dovranno pervenire esclusivamente gli "streaming" allarmati (è fatto divieto di veicolare su tali server i video "non allarmati").

Gli oneri di approvvigionamento e manutenzione degli apparati allocati presso ogni Comando Provinciale/Gruppo sono a carico del soggetto privato fornitore del servizio.

d. Le immagini trasmesse alla postazione di Sala/Centrale operativa delle Forze di Polizia dovranno avere le seguenti caratteristiche minime:
- risoluzione con un formato DCIF (minima 1.280x720 pixel);

- formato delle immagini in modalità colore 24 bit/pixel, pari a 32 ML di colori e in B&W notturna (8bit/pixel, 512 livelli di grigio), con algoritmo standard di compressione;
- frame rate non inferiore a 15 fps;
- standard Codifica Audio G.711.

e. Per le finalità del videoallarme antirapina, la connettività Internet delle Sale operative delle Forze di polizia è predisposta senza oneri per le stesse. Il collegamento sarà di tipo a banda larga, riservato e protetto con sistemi di protezione predisposti dalle Forze di polizia.

f. Il sistema dovrà rendere disponibili le seguenti funzionalità:
- allarme completo dell'identificativo dell'esercizio commerciale/impresa e dell'identificativo della sorgente del flusso video;
- informazioni dell'esercente commerciale, corredato di campo note e di fotografie dell'esercente, ed eventualmente di collaboratori, nonchè della planimetria dell'esercizio commerciale;
- videoallarme completo di audio, ove presente, attivato esclusivamente in caso di allarme, proveniente dalle telecamere installate dall'esercizio commerciale/impresa;
- in assenza di attivazione del videoallarme antirapina, presso le Sale operative delle Forze di polizia NON devono giungere le immagini delle telecamere.

4. PROCEDURE DI ACCREDITAMENTO

4.1 NULLA OSTA TECNICO

Nelle more della realizzazione della nuova architettura di collegamento, per poter procedere all'installazione del sistema, ciascuna ditta deve ottenere un Nulla Osta Tecnico di conformità al Protocollo d'Intesa 2019 (nel seguito: N.O.T. 2019) attraverso due fasi distinte e consequenziali:

1. *Verifiche amministrative*.
   a) in caso di istituto di vigilanza: la Questura verifica il possesso della prevista autorizzazione rilasciata ai sensi dell'art.134 TULPS;
   b) in assenza di autorizzazione ai sensi dell'art.134 del TULPS, la Forza di polizia che riceve la richiesta di attivazione, secondo le ordinarie procedure:
      - verifica l'iscrizione nell'apposito albo degli installatori della camera di commercio;
      - raccoglie la dichiarazione di installazione a regola d'arte presentata dall'installatore.

2. *Verifiche tecniche*.
   A livello territoriale, l'Arma dei Carabinieri provvede al rilascio del Nulla Osta Tecnico attraverso l'Ufficio TAES Legionale.

Le novità introdotte dal Protocollo d'Intesa del 2019 impongono, per i soggetti privati fornitori del servizio già in possesso di un Nulla Osta Tecnico di conformità al Protocollo d'Intesa 2009/2013 (nel seguito: N.O.T. 2009 e N.O.T. 2013 ove applicabile), l'ottenimento di un N.O.T. 2019 che certifichi l'avvenuto adeguamento dei sistemi al presente disciplinare.

I soggetti privati fornitori del servizio non in possesso del "vecchio N.O.T." devono invece avviare le procedure per l'acquisizione del N.O.T. 2019.

Si riporta, di seguito, l'iter da seguire per l'ottenimento di un N.O.T., distinto per Polizia di Stato e Arma dei Carabinieri, nei seguenti tre casi:

A. Il soggetto privato fornitore del servizio è in possesso del N.O.T. 2009/2013 ed ha apparati installati nella DMZ della Questura o del Comando Provinciale;
B. Il soggetto privato fornitore del servizio è in possesso del N.O.T. 2009/2013 ma non ha apparati installati in Questura o in DMZ della Questura o del Comando Provinciale;
C. Il soggetto privato fornitore del servizio non è in possesso del N.O.T. 2009/2013.

Polizia di Stato

Nel caso A:
l'installatore, entro un anno dalla sottoscrizione del presente accordo, deve ritirare il materiale presente nelle Sale operative (postazione videoallarme) e predisporre l'apposito interfacciamento verso il MediaServer installato nella Questura competente territorialmente.

Nel caso B e C:
l'installatore provvede a predisporre l'apposito interfacciamento verso il MediaServer della Questura competente territorialmente.

Arma dei Carabinieri

Il soggetto privato fornitore del servizio deve avanzare al Comando Generale dell'Arma dei Carabinieri, Ufficio Sistemi Informativi, richiesta di ottenimento del N.O.T. 2019:

- nei casi A e B (la ditta ha già ricevuto un N.O.T. 2009/2013) l'esito positivo dei test di integrazione con il nuovo software CC112-NUE determina automaticamente il rilascio del N.O.T. 2019 (a cura del predetto Ufficio Sistemi Informativi). Il soggetto privato fornitore del servizio, nel caso abbia già degli apparati installati nelle DMZ delle Centrali Operative periferiche, dovrà provvedere all'adeguamento di tali impianti secondo le caratteristiche tecniche previste dal presente disciplinare entro 180 gg dall'ottenimento del N.O.T. 2019;
- nel caso C (la ditta non ha un N.O.T. 2009/2013), successivamente all'esito positivo del test di integrazione con il software CC112-NUE effettuato presso il Comando Generale dell'Arma, la ditta dovrà presentare alle articolazioni tecniche Legionali dell'Arma dei Carabinieri gli apparati che intende installare localmente, al fine di ottenere il N.O.T 2019.

4.2 MODALITÀ DI COMUNICAZIONE CON LE ARTICOLAZIONI TECNICHE PERIFERICHE DELL'ARMA DEI CARABINIERI

Le articolazioni tecniche periferiche dell'Arma dei Carabinieri:

- ricevono, con lettera formale, da parte del soggetto privato fornitore del servizio il progetto di video-allarme;
- esaminano il progetto presentato, al fine di verificarne la coerenza con i dettami del disciplinare tecnico;
- rispondono alla ditta proponente rilasciando il Nulla Osta Tecnico (N.O.T.) al progetto, ovvero rigettando lo stesso per non conformità (modello di risposta in all.2-modello di concessione-rifiuto di N.O.T.).

4.3 MANDATO (solo per l'Arma dei Carabinieri)

Una volta in possesso del N.O.T.:

- le "associazioni di categoria/singoli esercenti non associati" attivano le loro procedure interne per conferire al soggetto privato/soggetti privati fornitore del servizio l'incarico ad operare anche sulla base di eventuali protocolli/accordi territoriali ;
- il soggetto privato fornitore del servizio che abbia ricevuto il N.O.T. da parte delle articolazioni periferiche dell'Arma dei Carabinieri ed il mandato da parte di un'associazione di categoria/esercente non associato è autorizzato ad interfacciarsi con le Centrali operative dell'Arma dei Carabinieri.

5. INSTALLAZIONE DEGLI APPARATI IN SALA/CENTRALE OPERATIVA

Il soggetto privato fornitore del servizio provvederà ad interfacciarsi con i rispettivi software in dotazione alle Forze di polizia (ICT per la P.d.S. e "CC112-NUE" per l'Arma dei Carabinieri). Eventuali casistiche particolari (da specificare) dovranno essere rimesse alle valutazioni delle singole Amministrazioni Centrali.

5.1 ATTIVITÀ (solo per l'Arma dei Carabinieri)

Il soggetto privato fornitore del servizio, in accordo a quanto riportato nell'allegato all.1. – schema esplicativo collegamenti:

- consegna ed installa in Sala/Centrale Operativa un router con connettività ad internet flusso ADSL/HDSL (nello schema riportati come "routers xDSL verso le aziende convenzionate");
- consegna ed installa, in ciascuna Comando Provinciale/Gruppo interessato, un "Media Server video allarme anti rapina" dotato di due interfacce di rete. La prima di queste sarà collegata al predetto router secondo un indirizzamento privato, mentre la seconda interfaccia - cablaggio a cura della ditta - sarà collegata all'Hub/switch già disponibile in Sala/Centrale operativa (indicato nello schema come "DMZ Switch"), utilizzando un IP appartenente al range assegnato ad ogni Comando Provinciale/Gruppo ('all.3 – indirizzamenti Arma CC' per l'Arma dei Carabinieri).

Se il numero di porte dell'hub/switch non fosse sufficiente o il suddetto hub/switch non fosse presente, la ditta dovrà consegnare un nuovo switch che sostituisce/integra il precedente.

NOTA: "il Video Server interno alla rete delle Forze di polizia (su cui viene installato il WS "alerter" al quale sarà notificato l'invio del flusso allarmato, vedasi paragrafo successivo) non deve essere fornito, perché già nella disponibilità delle Forze di polizia".

Gli oneri di installazione e manutenzione degli apparati ricadono sul soggetto privato fornitore del servizio accreditato per l'installazione del proprio sistema di video allarme.

5.2 INTEGRAZIONE CON IL SOFTWARE "CC112- NUE"

I "Media Server - video allarme anti rapina" per l'Arma dei Carabinieri riceveranno dai singoli sistemi di video allarme tutte le informazioni di cui necessitano ed inoltreranno al "Video Server interno" (indirizzi IP in cit. all.3) esclusivamente una notifica (attestante l'arrivo di un flusso video allarmato), mediante invocazione del Web Service c.d. "alerter" (all.4 Specifiche Tecniche WS Alerter), il quale attiverà un meccanismo che permetterà ai server dell'Arma di prelevare in tempo reale il flusso video e riversarlo all'interno della rete Intranet. Se si rendesse necessaria la

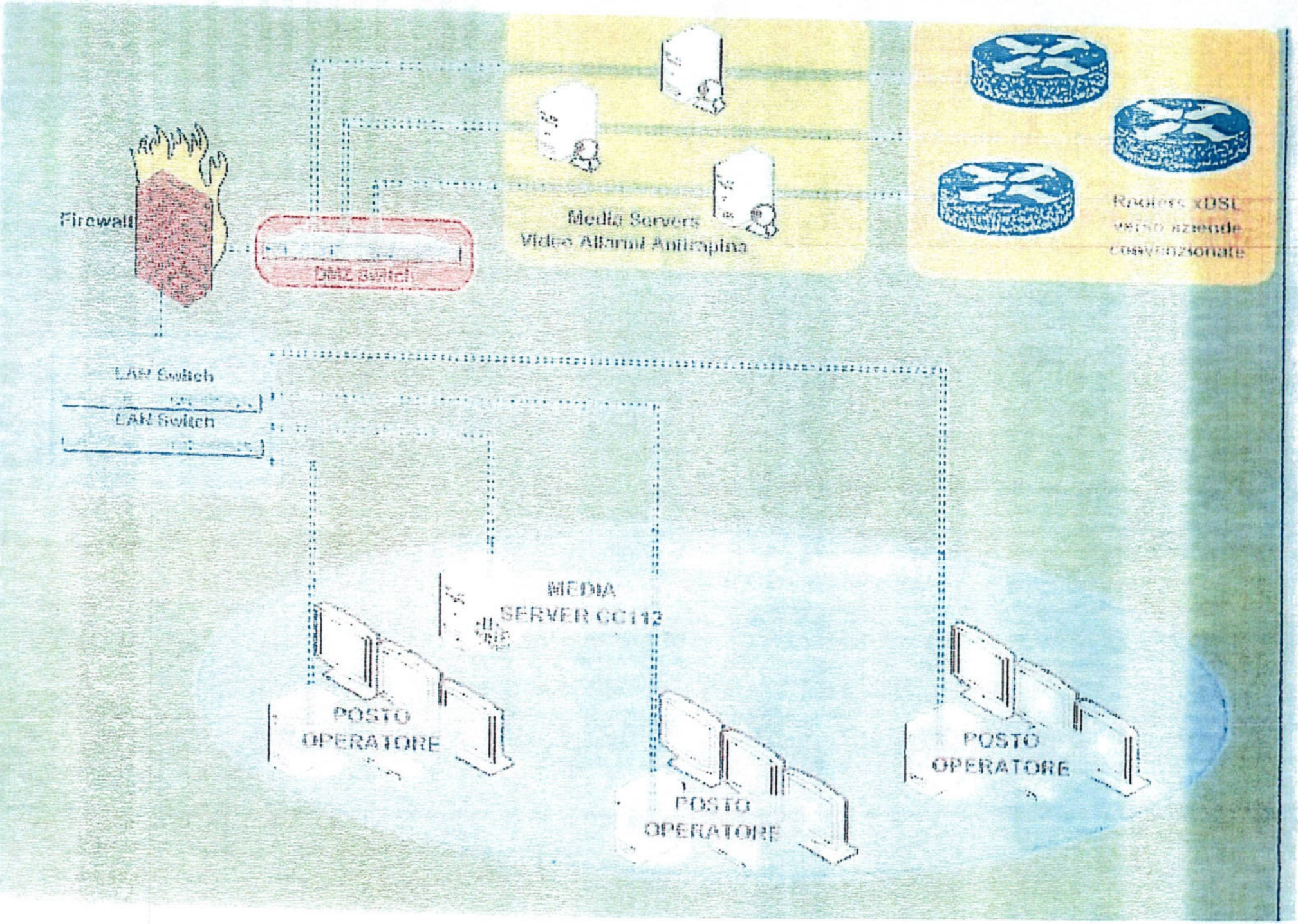
configurazione dei firewall posti a valle dell'Hub/switch, le articolazioni periferiche dell'Arma dei Carabinieri contatteranno i rispettivi organi tecnici per l'ausilio del caso.

6. ATTIVAZIONE DEI SINGOLI SISTEMI DI VIDEO-ALLARME NEI SOFTWARE "I.C.T." E "CC112-NUE"

L'esercente chiede l'attivazione del servizio alla Questura e al Comando dei Carabinieri territorialmente competente, mediante la compilazione del modulo di attivazione (all.5 - modulo di attivazione) che dovrà indicare:

- i dati identificativi dell'esercizio commerciale/impresa;
- i dati identificativi degli addetti alla vendita (potenzialmente chiamati ad attivare il pulsante del videoallarme);
- dichiarazione di installazione effettuata a regola d'arte da parte dell'installatore;
- dichiarazione di iscrizione all'apposito albo della Camera di Commercio;
- l'eventuale istituto di vigilanza incaricato del servizio.

Nella fase transitoria (1 anno) è ammessa la presentazione della domanda di attivazione da parte del soggetto privato fornitore del servizio accreditato secondo le modalità di cui al N.O.T 2009 e N.O.T 2013 ove applicabile; nelle more restano operative le precedenti modalità.


Firewall
DMZ Switch
Media Servers
Video Allarmi Antirapina
Routers xDSL
verso aziende
convenzionate
LAN Switch
LAN Switch
MEDIA
SERVER CC112
POSTO
OPERATORE
POSTO
OPERATORE
POSTO
OPERATORE

INTESTAZIONE REPARTO

versione del 30 giugno 2019

OGGETTO: Sistema di video-allarme antirapina

Rif. : richiesta di accreditamento prot. n. _____ del _____

ALLA SPETT.Le ditta

_____

_____

^.^.^.^.^.^.^.^.^.^.^.^

NON si concede il Nulla Osta Tecnico all'installazione dell'impianto di video allarme anti-rapina di cui al progetto trasmesso con la richiesta in riferimento per il seguente motivo:

_____

_____

SI concede il Nulla Osta Tecnico all'installazione dell'impianto di video allarme anti-rapina di cui al progetto trasmesso con la richiesta in riferimento. In proposito si evidenzia che:

a. codesta ditta è autorizzata ad effettuare l'installazione del sistema presso le C.O. di questo Comando Legione dal momento in cui avrà ricevuto, da parte di un'associazione di categoria/ esercente non associato, il **mandato** ad attivare un sistema di video allarme, (purchè in regola con le disposizioni per lo svolgimento di lavori non classificati in aree riservate);
b. codesta Ditta si impegna sin d'ora, pena revoca dell'autorizzazione testè concessa, a consentire, in caso di richiesta dell'Amministrazione, l'accesso al proprio sistema per l'eventuale attestazione di ulteriori flussi video provenienti da fonti video diverse (es: altri sistemi di video allarme antirapina, telecamere urbane etc...);
c. il sistema di video-allarme dovrà essere interfacciato con il software "CC112" inoltrando al "Media Server CC112" esclusivamente i flussi di videostreaming allarmati in formato compatibile con "Microsoft Media services" – protocollo RTSP (come previsto da capitolato tecnico). Il flusso video dovrà essere corredato da un "Codice Unico Apparato" che, per ogni esercizio commerciale che aderirà al progetto, sarà definito dal responsabile della C.O. al quale dovrà essere consegnato il **modulo di attivazione** allegato.
Nota: la ditta si impegna sin d'ora, pena revoca dell'autorizzazione testè concessa, ad attuare tutte le necessarie predisposizioni tecniche per continuare a garantire l'operatività del sistema.

GRUPPO FIRMA

Numero Sede	Comando	Indirizzo	SUBNET SERVER DI VIDEO ALLARME ANTI-RAPINA	GATEWAY	IP MEDIA SEVER CC112
1	Agrigento	P.zza Aldo Moro 2	192.168.1.128 /25	192.168.1.129	192.168.1.13
2	Alessandria	P.zza Vittorio Veneto 2	192.168.2.128 /25	192.168.2.129	192.168.2.13
3	Ancona	Via Della Montagnola 81/a	192.168.3.128 /25	192.168.3.129	192.168.3.13
4	Aosta	P.zza Roncas 1	192.168.4.128 /25	192.168.4.129	192.168.4.13
5	Arezzo	Via Gen. Carlo Alberto Dalla Chiesa 12	192.168.5.128 /25	192.168.5.129	192.168.5.13
6	Ascoli Piceno	Via Circonvallazione 10	192.168.6.128 /25	192.168.6.129	192.168.6.13
7	Asti	Via Zangrandi 6	192.168.7.128 /25	192.168.7.129	192.168.7.13
8	Avellino	Via Roma 104	192.168.8.128 /25	192.168.8.129	192.168.8.13
9	Bari	Lungomare N. Sauro 43	192.168.9.128 /25	192.168.9.129	192.168.9.13
10	Belluno	Viale Europa 9	192.168.10.128 /25	192.168.10.129	192.168.10.13
11	Benevento	Via Meomartini 9	192.168.11.128 /25	192.168.11.129	192.168.11.13
12	Bergamo	Circonvallazione Delle Valli 31	192.168.12.128 /25	192.168.12.129	192.168.12.13
13	Biella	Via F.lli Rosselli 96/BIS	192.168.13.128 /25	192.168.13.129	192.168.13.13
14	Bologna	Via Del Bersaglieri 3	192.168.14.128 /25	192.168.14.129	192.168.14.13
15	Bolzano	Via Dante 30	192.168.15.128 /25	192.168.15.129	192.168.15.13
16	Brescia	P.zza Tebaldo Brusato 19	192.168.16.128 /25	192.168.16.129	192.168.16.13
17	Brindisi	Via Bastioni S. Giorgio 3	192.168.17.128 /25	192.168.17.129	192.168.17.13
18	Cagliari	Via Nuoro 9	192.168.18.128 /25	192.168.18.129	192.168.18.13
19	Caltanisetta	Via Leone XIII 97	192.168.19.128 /25	192.168.19.129	192.168.19.13
20	Campobasso	Corso Mazzini 97	192.168.20.128 /25	192.168.20.129	192.168.20.13
21	Caserta	Via Laviano Cap. Luigi 13	192.168.21.128 /25	192.168.21.129	192.168.21.13
22	Castello di Cisterna (Gruppo)	Via Cosimo Micceli 8	192.168.22.128 /25	192.168.22.129	192.168.22.13
23	Catania	P.zza Verga 8	192.168.23.128 /25	192.168.23.129	192.168.23.13
24	Catanzaro	Piazzale Trieste 1	192.168.24.128 /25	192.168.24.129	192.168.24.13
25	Chieti	Via Amiense 102	192.168.25.128 /25	192.168.25.129	192.168.25.13
26	Como	Via Borgovico 171	192.168.26.128 /25	192.168.26.129	192.168.26.13
27	Cosenza	Viale Eusento SNC	192.168.27.128 /25	192.168.27.129	192.168.27.13
28	Cremona	Viale Trento Trieste 58	192.168.28.128 /25	192.168.28.129	192.168.28.13
29	Crotone	Via IV Novembre 4	192.168.29.128 /25	192.168.29.129	192.168.29.13
30	Cuneo	C.so Soleri 7	192.168.30.128 /25	192.168.30.129	192.168.30.13
31	Enna	Via Montesalvo 83	192.168.31.128 /25	192.168.31.129	192.168.31.13
32	Ferrara	Via Del Campo 40	192.168.32.128 /25	192.168.32.129	192.168.32.13
33	Firenze	Borgo Ognissanti 48	192.168.33.128 /25	192.168.33.129	192.168.33.13
34	Foggia	Via Guglielmi 4	192.168.34.128 /25	192.168.34.129	192.168.34.13
35	Forlì	Corso Mazzini 78	192.168.35.128 /25	192.168.35.129	192.168.35.13
36	Frascati (Gruppo)	Viale V. Veneto 40	192.168.36.128 /25	192.168.36.129	192.168.36.13
37	Frosinone	Viale Mazzini 131	192.168.37.128 /25	192.168.37.129	192.168.37.13
38	Genova	Via Gobetti 5	192.168.38.128 /25	192.168.38.129	192.168.38.13
39	Gorizia	C.so Verdi 17	192.168.39.128 /25	192.168.39.129	192.168.39.13
40	Grosseto	Via Ferrucci 32	192.168.40.128 /25	192.168.40.129	192.168.40.13
41	Imperia	V.le Matteotti 46	192.168.41.128 /25	192.168.41.129	192.168.41.13
42	Isernia	Viale 3 Marzo 1970 2	192.168.42.128 /25	192.168.42.129	192.168.42.13
43	La Spezia	Via C.A. Dalla Chiesa 1	192.168.43.128 /25	192.168.43.129	192.168.43.13
44	L'Aquila	Via Beato Cesidio 6	192.168.44.128 /25	192.168.44.129	192.168.44.13
45	Latina	Largo Caduti di Nassiriya 1	192.168.45.128 /25	192.168.45.129	192.168.45.13
46	Lecce	Via Lupiae 5	192.168.46.128 /25	192.168.46.129	192.168.46.13
47	Lecco	Corso Carlo Alberto 62	192.168.47.128 /25	192.168.47.129	192.168.47.13
48	Livorno	Via Fabbicotti 1	192.168.48.128 /25	192.168.48.129	192.168.48.13
49	Lodi	Piazza Caduti di Nassiriya 3	192.168.49.128 /25	192.168.49.129	192.168.49.13
50	Lucca	Cortile degli Svizzeri 4	192.168.50.128 /25	192.168.50.129	192.168.50.13
51	Macerata	Via XX Settembre 2	192.168.51.128 /25	192.168.51.129	192.168.51.13
52	Mantova	Via Chiassi 29	192.168.52.128 /25	192.168.52.129	192.168.52.13
53	Massa Carrara	Via Angelini 14	192.168.53.128 /25	192.168.53.129	192.168.53.13
54	Matera	Via Dante 17	192.168.54.128 /25	192.168.54.129	192.168.54.13
55	Messina	Via Monsignor D'Arrigo 13	192.168.55.128 /25	192.168.55.129	192.168.55.13
56	Milano	Via Moscova 21	192.168.56.128 /25	192.168.56.129	192.168.56.13
57	Modena	Via Pico della Mirandola 30	192.168.57.128 /25	192.168.57.129	192.168.57.13
58	Monreale (Gruppo)	Via Biagio Giordano 1	192.168.58.128 /25	192.168.58.129	192.168.58.13
59	Monza	Via Volturno 35	192.168.59.128 /25	192.168.59.129	192.168.59.13
60	Napoli	Via Morgantini 4	192.168.60.128 /25	192.168.60.129	192.168.60.13
61	Novara	Via Baluardo Lamarmora 8	192.168.61.128 /25	192.168.61.129	192.168.61.13
62	Nuoro	Via S. Onofrio 3	192.168.62.128 /25	192.168.62.129	192.168.62.13
63	Oristano	Via F. Loffredo 10/A	192.168.63.128 /25	192.168.63.129	192.168.63.13
64	Ostia (Gruppo)	Via A. Zambrini 48	192.168.64.128 /25	192.168.64.129	192.168.64.13
65	Padova	Via Rismondo 4	192.168.65.128 /25	192.168.65.129	192.168.65.13

66	Palermo	Via Muro di San Vito	192.168.66.128 /25	192.168.66.129	192.168.66.13
67	Parma	Strada Fondarie 10	192.168.67.128 /25	192.168.67.129	192.168.67.13
68	Pavia	Via D. Sacchi 31	192.168.68.129 /25	192.168.68.129	192.168.68.13
69	Perugia	Via Ruggia, 9	192.168.69.128 /25	192.168.69.129	192.168.69.13
70	Pesaro	Via Salvo D'Aquisto 2	192.168.70.128 /25	192.168.70.129	192.168.70.13
71	Pescara	Via G. D'Annunzio 149	192.168.71.128 /25	192.168.71.129	192.168.71.13
72	Piacenza	Via Beverora 48	192.168.72.128 /25	192.168.72.129	192.168.72.13
73	Pisa	Via Guido Da Pisa 1	192.168.73.128 /25	192.168.73.129	192.168.73.13
74	Pistoia	Viale Italia 78	192.168.74.126 /25	192.168.74.129	192.168.74.13
75	Pordenone	Via del Carabiniere 2	192.168.75.128 /25	192.168.75.129	192.168.75.13
76	Potenza	Via Pretoria 300	192.168.76.128 /25	192.168.76.129	192.168.76.13
77	Prato	Via Pablo Picasso 30	192.168.77.128 /25	192.168.77.129	192.168.77.13
78	Ragusa	P.zza Caduti di Nassiriya 3	192.168.78.128 /25	192.168.78.129	192.168.78.13
79	Ravenna	Viale Pertini 11	192.168.79.129 /25	192.168.79.129	192.168.79.13
80	Reggio Calabria	Via Aschenetz 3	192.168.80.128 /25	192.168.80.129	192.168.80.13
81	Reggio Emilia	C.so Cairoli 8	192.168.81.128 /25	192.168.81.129	192.168.81.13
82	Rieti	Via Giulio de Julis 2	192.168.82.128 /25	192.168.82.129	192.168.82.13
83	Rimini	Viale Carlo Alberto Dalla Chiesa 15	192.168.83.129 /25	192.168.83.129	192.168.83.13
84	Roma	Piazza S. Lorenzo in Lucina 6	192.168.84.128 /25	192.168.84.129	192.168.84.13
85	Rovigo	Via Silvestri 29	192.168.85.128 /25	192.168.85.129	192.168.85.13
86	Salerno	Via R. Masri 99	192.168.86.129 /25	192.168.86.129	192.168.86.13
87	Sassari	Via Rockefeller 52	192.168.87.128 /25	192.168.87.129	192.168.87.13
88	Savona	C.so Ricci 30	192.168.88.128 /25	192.168.88.129	192.168.88.13
89	Siena	Largo Salvo D'Acquisto 1	192.168.89.128 /25	192.168.89.129	192.168.89.13
90	Siracusa	Via Tica 142/m	192.168.90.128 /25	192.168.90.129	192.168.90.13
91	Sondrio	Largo Sertoli 5	192.168.91.128 /25	192.168.91.129	192.168.91.13
92	Taranto	Viale Virgilio 25	192.168.92.128 /25	192.168.92.129	192.168.92.13
93	Teramo	Piazza Del Carmine 3	192.168.93.128 /25	192.168.93.129	192.168.93.13
94	Terni	Via Giuseppe Lombardo Radice 6	192.168.94.128 /25	192.168.94.129	192.168.94.13
95	Torino	Via Valfrè 5/bis	192.168.95.128 /25	192.168.95.129	192.168.95.13
96	Trapani	Via Orlandini 27	192.168.96.128 /25	192.168.96.129	192.168.96.13
97	Trento	Via Barbacovi 24	192.168.97.128 /25	192.168.97.129	192.168.97.13
98	Treviso	Via Carnarotta 24	192.168.98.128 /25	192.168.98.129	192.168.98.13
99	Trieste	Via Dellistna 54	192.168.99.128 /25	192.168.99.129	192.168.99.13
100	Udine	Viale Trieste 28	192.168.100.128 /25	192.168.100.129	192.168.100.13
101	Varese	Via Aurelio SAFFI 55	192.168.101.128 /25	192.168.101.129	192.168.101.13
102	Venezia	Castello 4693/a	192.168.102.128 /25	192.168.102.129	192.168.102.13
103	Verbania	Via Gen. Carlo Alberto Dalla Chiesa 1	192.168.103.128 /25	192.168.103.129	192.168.103.13
104	Vercelli	Via Gioberti 57	192.168.104.128 /25	192.168.104.129	192.168.104.13
105	Verona	Via S. D'Aquisto 6	192.168.105.128 /25	192.168.105.129	192.168.105.13
106	Vibo Valentia	Via Gen. Pellicanò 19	192.168.106.128 /25	192.168.106.129	192.168.106.13
107	Vicenza	Via Muggia 2	192.168.107.128 /25	192.168.107.129	192.168.107.13
108	Viterbo	Via S. Camillo De Lellis 20	192.168.108.128 /25	192.168.108.129	192.168.108.13
109	Torre Annunziata	Piazza Enrico de Nicola 12	192.168.109.128 /25	192.168.109.129	192.168.109.13
110	Gioia Tauro (Gruppo)	Via strada provinciale 111	192.168.110.128 /25	192.168.110.129	192.168.110.13
111	Lamezia Terme (Gruppo)	Via Guglielmo Marconi 66	192.168.111.128 /25	192.168.111.129	192.168.111.13
112	Locri (Gruppo)	Via Cosmano S.N.	192.168.112.128 /25	192.168.112.129	192.168.112.13
113	Fermo	Via Beni 5	192.168.113.128 /25	192.168.113.129	192.168.113.13

1. SCOPO

Lo scopo del servizio "alerter" descritto in questo documento è quello di consentire al sistema di "Video Allarme Anti Rapina" di notificare ai sistemi in dotazione alle Centrali Operative dei Carabinieri l'arrivo di un flusso video allarmato.
In seguito a tale notifica, i sistemi delle Forze di Polizia effettueranno una chiamata al video server esterno (posizionato in DMZ) fornito dalle società civili (nel seguito denominato "*Media Server video allarme anti rapina*") per acquisire l'allarme stesso.

2. WEB SERVICE

Attraverso questo servizio, il "*Media Server video allarme anti rapina*" potrà inviare ai server locali installati nella rete Intranet delle Forze di Polizia un comando di "attivazione della registrazione" notificando, contestualmente, l'arrivo di una segnalazione di allarme alle Sale/Centrali Operative.

Grazie a questa nuova modalità non si dovrà effettuare un "push" verso i server delle Sale/Centrali Operative delle FF.PP., ma si attiverà un meccanismo per il quale saranno i server delle FF.PP. a prelevare in tempo reale il flusso video e riversarlo all'interno della rete Intranet.

Mediante questa nuova modalità, sarà possibile gestire i flussi audio/video di seguito descritti:

- MMS/HTTP
- RTSP
- RTMP

Le tipologie di Codec utilizzabili, quindi, potranno essere quelli di seguito descritti:

- Windows Media Video;
- MPEG2;
- H264.

La tecnologia di realizzazione del Web Services descritto nel presente documento è "Web Service 1.2", al fine di rendere compatibili la maggior parte dei linguaggi di sviluppo attualmente in uso.

Il WS è strutturato come di seguito descritto:

	DESCRIZIONE	Note
Id	Codice Univoco Identificativo del sistema di video allarme	Parametri sempre obbligatori. Nel caso in cui i parametri restanti fossero non popolati, si intende che si sta inviando solo un allarme e la relativa posizione (variabile nel tempo) senza correlarvi un flusso video.
Timestamp	Data Ora di attivazione dell'allarme (timestamp dal 1° gennaio 1970)	
IpAddress	Indirizzo Ip Sorgente del Server da cui si preleva il flusso Video	
NMEA	Coordinate Geografiche del punto da cui proviene l'allarme (standard GPRMC). Coincide con il luogo dell'obiettivo, tranne nel caso in cui provenga da un oggetto mobile collegato al medesimo "codice univoco".	
Protocol	Protocollo utilizzato per il flusso video (MMS, RTSP, RTMP)	Parametri da popolare obbligatoriamente se si intende trasferire anche un flusso di video streaming, altrimenti restano vuoti.
Port	Porta del sorgente	
Uri	Indirizzo per esteso dove andare a prelevare la fonte video live (ad es.: mms://172.16.100.10/videoAlert)	
Parameters	Eventuali parametri che devono essere lanciati per prelevare il flusso Video	
CallbackUri	Eventuale Url del sistema mittente da lanciare una volta terminato il flusso Video per notificare, ad es., l'esito (positivo o negativo) dell'acquisizione del filmato	

Di seguito viene descritto il WSDL per interfacciarsi con il sistema "Alerter":

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:tm="http://microsoft.com/wsdl/mime/textMatching/" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:mime="http://schemas.xmlsoap.org/wsdl/mime/" xmlns:tns="http://carabinieri.it.org/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:http="http://schemas.xmlsoap.org/wsdl/http/" targetNamespace="http://carabinieri.it.org/" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:types>
    <s:schema elementFormDefault="qualified" targetNamespace="http://carabinieri.it.org/">
      <s:element name="BeginAlert">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="message" type="tns:Message" />
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:complexType name="Message">
        <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="Id" type="s:string" />
          <s:element minOccurs="1" maxOccurs="1" name="Timestamp" type="s:int" />
          <s:element minOccurs="0" maxOccurs="1" name="Protocol" type="s:string" />
          <s:element minOccurs="1" maxOccurs="1" name="Port" type="s:int" />
          <s:element minOccurs="0" maxOccurs="1" name="Uri" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="IpAddress" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="Parameters" type="s:string" />
          <s:element minOccurs="0" maxOccurs="1" name="CallbackUri" type="s:string" />
        </s:sequence>
      </s:complexType>
      <s:element name="BeginAlertResponse">
        <s:complexType>
          <s:sequence>
            <s:element minOccurs="1" maxOccurs="1" name="BeginAlertResult" type="tns:Response" />
          </s:sequence>
        </s:complexType>
      </s:element>
      <s:complexType name="Response">
        <s:sequence>
          <s:element minOccurs="1" maxOccurs="1" name="Result" type="s:boolean" />
          <s:element minOccurs="0" maxOccurs="1" name="Description" type="s:string" />
        </s:sequence>
      </s:complexType>
    </s:schema>
  </wsdl:types>
  <wsdl:message name="BeginAlertSoapIn">
    <wsdl:part name="parameters" element="tns:BeginAlert" />
  </wsdl:message>
  <wsdl:message name="BeginAlertSoapOut">
    <wsdl:part name="parameters" element="tns:BeginAlertResponse" />
  </wsdl:message>
  <wsdl:portType name="ErmesAlerterSoap">
    <wsdl:operation name="BeginAlert">
      <wsdl:input message="tns:BeginAlertSoapIn" />
      <wsdl:output message="tns:BeginAlertSoapOut" />
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="ErmesAlerterSoap" type="tns:ErmesAlerterSoap">
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="BeginAlert">
      <soap:operation soapAction="http://carabinieri.it.org/BeginAlert" style="document" />
      <wsdl:input>
        <soap:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal" />
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="ErmesAlerterSoap12" type="tns:ErmesAlerterSoap">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="BeginAlert">
      <soap12:operation soapAction="http://carabinieri.it.org/BeginAlert" style="document" />
      <wsdl:input>
        <soap12:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal" />
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="ErmesAlerter">
    <wsdl:port name="ErmesAlerterSoap" binding="tns:ErmesAlerterSoap">
      <soap:address location="http://localhost:59305/ErmesAlerter.asmx" />
    </wsdl:port>
    <wsdl:port name="ErmesAlerterSoap12" binding="tns:ErmesAlerterSoap12">
      <soap12:address location="http://localhost:59305/ErmesAlerter.asmx" />
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

ErmesAlerter.wsdl

SISTEMA DI VIDEO-ALLARME ANTIRAPINA
MODULO DI ATTIVAZIONE

Alla Questura di _____
Al Comando Provinciale dei Carabinieri di _____

Il sottoscritto _____ nato a _____ il _____
residente in _____via_____ n.___, in qualità di _____
dell'esercizio commerciale _____ C.F. - partita IVA _____
situato in _____ via _____ n._____

COMUNICA

di voler attivare un dispositivo di video-allarme antirapina collegato con le Forze di Polizia in virtù del Protocollo d'intesa siglato tra il Ministero dell'Interno e le Associazioni di categoria.
A tal proposito fornisce i recapiti telefonici di pronto contatto:

1. Sig. _____ tel. _____ cell. _____ ;
2. Sig. _____ tel. _____ cell. _____ .

In caso di necessità ed in assenza del sottoscritto, le chiavi dell'esercizio sono custodite dal Sig. _____abitante in _____ via _____ n._____ tel./cell._____ .

In merito all'installazione dell'impianto di video-allarme antirapina dichiara quanto segue:

a) di aver incaricato la società _____ .
Allega la seguente documentazione:
   1) Iscrizione alla camera di commercio della società incaricata;
   2) Dichiarazione di regolare installazione anche ai sensi della normativa sul trattamento del dato personale;
   3) Indirizzo IP statico ____.____.____.____ .

(oppure)

b) di aver incaricato l'Istituto di vigilanza _____con licenza rilasciata dalla Prefettura di _____in data _____ .
Allega la seguente documentazione:
   1) Dichiarazione di regolare installazione anche ai sensi della normativa sul trattamento del dato personale;
   2) Indirizzo IP statico ____.____.____.____ ;
   3) Recapiti telefonici di pronto contatto:
   Sig. _____ tel. _____ cell. _____

Il sottoscritto:

1. dichiara - ai sensi del Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 - di essere stato informato che i dati personali contenuti nella presente dichiarazione saranno trattati, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presente dichiarazione viene resa;
2. è a conoscenza del fatto che l'adesione al sistema di video-allarme antirapina non costituisce canale preferenziale e che le Forze di polizia interverranno nel più breve tempo possibile, compatibilmente con le risorse disponibili al momento;

2a - conferma che l'impianto è stato realizzato secondo le istruzioni pubblicate all'indirizzo www.poliziadistato.it /XXXXX
2b - conferma che l'impianto ha ottenuto il Nulla Osta Tecnico dal Comando Generale dell'Arma dei Carabinieri per il collegamento con le relative Centrali operative.

Luogo e data _____

IL RICHIEDENTE

_____

Il presente modulo potrà consegnato a mano e/o esser trasmesso via mail agli indirizzi reperibili sul sito istituzionale

(spazio riservato alle Forze di Polizia)

Codice unico d'identificazione assegnato all'apparato _____

Luogo e data _____

Gruppo Firma

_____