



Prefettura di Grosseto



Prefettura Grosseto
Prot. Ingresso del 18/03/2016
Numero: **0013239**
Classifica: A1.12.B01

RINNOVO E AGGIORNAMENTO DEL PROTOCOLLO D'INTESA DEL 27 APRILE 2010



TRA

PREFETTURA – UFFICIO TERRITORIALE DEL GOVERNO DI GROSSETO
CAMERA DI COMMERCIO DI GROSSETO
CONFCOMMERCIO DI GROSSETO
CONFESERCENTI DI GROSSETO
CONFARTIGIANATO IMPRESE DI GROSSETO
CONFEDERAZIONE NAZIONALE DELL'ARTIGIANATO
E DELLA PICCOLA E MEDIA IMPRESA DI GROSSETO

VISTO il Protocollo d'Intesa del 14 luglio 2009 in tema di video allarme antirapina stipulato tra il Ministro dell'Interno e i rappresentanti delle Associazioni di categoria Confcommercio Imprese per l'Italia e Confesercenti, al fine di realizzare un sistema di video allarme antirapina, nell'intento di aumentare il livello di tutela degli operatori commerciali, anche mediante l'impiego delle più moderne tecnologie;

TENUTO CONTO dell'art. 7 del medesimo Protocollo, che rimette ai Prefetti la sottoscrizione con i rappresentanti provinciali delle Associazioni di categoria di mirati protocolli in conformità agli indirizzi delineati a livello nazionale e volti alla massima diffusione ed allo sviluppo operativo del sistema;

TENUTO CONTO CHE il suddetto Protocollo prevede, in particolare, l'attivazione presso gli esercizi aderenti alle citate Associazioni, di un sistema di allarme antirapina controllato con telecamere – configurato secondo i requisiti tecnici indicati nel Capitolato Tecnico allegato al Protocollo medesimo – che interagisce direttamente con gli apparati ed i sistemi in essere presso le Sale e le Centrali Operative della Polizia di Stato e dell'Arma dei Carabinieri, dislocate sul territorio;

[Handwritten signatures and initials]



Prefettura di Grosseto



CONSIDERATO che in data 12 novembre 2013 il predetto Protocollo è stato rinnovato, per ulteriori anni 3 ed integrato in alcune sue parti;

VISTA la nota in data 17 novembre 2014, con la quale il Ministero dell'Interno – Gabinetto del Ministro, nel richiamare la direttiva ministeriale “Arrestiamo ... furti e rapine” del 17 dicembre 2013 e nel rappresentare l'esigenza di accompagnare l'attività di prevenzione e contrasto ai reati predatori, anche con interventi di natura pattizia volti a rafforzare il partenariato pubblico-privato, ha trasmesso il nuovo “Disciplinare Tecnico” che sostituisce ed integra il precedente;

ATTESO CHE in data 27 aprile 2010 è stata data piena ed integrale esecuzione, nella provincia di Grosseto, al Protocollo Nazionale con la sottoscrizione del Protocollo d'Intesa tra il Prefetto pro tempore di Grosseto, il Presidente della Camera di Commercio, il Presidente della ASCOM – Confcommercio di Grosseto, il Presidente dell'Associazione Confesercenti e il Presidente della Confartigianato Imprese di Grosseto;

ATTESO ALTRESI' CHE in data 10 aprile 2013, con atto aggiuntivo sottoscritto dal Prefetto di Grosseto pro tempore e dal Direttore della Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa di Grosseto, in esecuzione dell'art. 7, comma secondo, del suddetto Protocollo d'Intesa, la locale C.N.A. ha aderito alla convenzione in tema di video allarme antirapina, stipulata in data 27 aprile 2010 con le altre associazioni di categoria;

CONSTATATO il diffondersi ed il moltiplicarsi di fenomeni di microcriminalità che colpiscono in particolare le imprese del commercio;

CONSIDERATO che i reati predatori costituiscono un fenomeno di particolare allarme sociale e che la percezione del rischio e la domanda di sicurezza nel settore sono in aumento, con la conseguente necessità di potenziare le misure di prevenzione e contrasto già apprestate;



RAVVISATA quindi la necessità di rinnovare la convenzione attuativa del 27 aprile 2010 e di aggiornarne i contenuti;

TANTO PREMESSO SI CONVIENE QUANTO SEGUE

Art. 1

Rinnovo e aggiornamento del Protocollo d'Intesa del 27 aprile 2010

Il Prefetto della Provincia di Grosseto, il Presidente della Camera di Commercio, il Presidente della ASCOM – Confcommercio di Grosseto, il Presidente dell'Associazione Confesercenti – Unione Provinciale Commercianti di Grosseto, il Presidente della Confartigianato Imprese di Grosseto, il Presidente della Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa di Grosseto, convengono che il Protocollo d'Intesa siglato il 27 aprile 2010 in tema di video allarme antirapina, integrato dall'atto aggiuntivo al suddetto Protocollo, siglato in data 10 aprile 2013, si intende rinnovato per la durata di cui all'art. 3, modificato ed integrato in alcune sue parti.

Costituisce parte integrante del presente documento il nuovo Disciplinare Tecnico, di cui all'art. 2 del rinnovato Protocollo Nazionale, predisposto dal Ministero dell'Interno - Dipartimento della Pubblica Sicurezza, d'intesa con i rappresentanti delle associazioni di categoria firmatarie, che sostituisce il precedente. Lo stesso definisce sia i requisiti tecnologici del sistema di allarme antirapina denominato "videoallarme", sia le modalità per l'adeguamento degli impianti già esistenti, per le nuove attivazioni e per la registrazione dei filmati.

Art. 2

Impegni delle parti

Ai fini dell'attuazione del presente Protocollo d'Intesa, le parti assumono i seguenti impegni:

1. confermano i vincoli derivanti dalla sottoscrizione del Protocollo d'Intesa del 27 aprile 2010;
2. la Prefettura favorisce lo sviluppo operativo del sistema di video allarme antirapina;



Prefettura di Grosseto



3. le Forze di Polizia assicurano, nell' ambito dell' attività di formazioni degli operatori economici, l'assistenza da parte di proprio personale la cui comprovata esperienza nel settore investigativo consenta agli operatori commerciali l'adozione di più efficaci misure di autoprotezione;
4. le Associazioni sottoscrittrici del presente Protocollo:
 - curano la diffusione dei contenuti informativi, relativi al presente Protocollo, ai propri associati;
 - promuovono la formazione degli imprenditori;
 - promuovono la diffusione di sistemi di sorveglianza e di sicurezza, di nuove tecnologie e dell'utilizzo degli strumenti di pagamento elettronico, quali mezzi per la limitazione dell'uso del contante, a fini di contrasto alla criminalità diffusa.

Le parti si impegnano infine ad aggiornare di comune accordo i programmi congiunti di informazione e di formazione.

Art. 3 **Durata**

Il presente Protocollo entra in vigore alla data di sottoscrizione dello stesso ed ha la durata di anni tre, con possibilità di tacito rinnovo.

Grosseto, 18 marzo 2016

Il Prefetto di Grosseto
Anna Maria Manzone

Il Presidente della Camera di Commercio, Industria, Artigianato e Agricoltura
Riccardo Breda



Prefettura di Grosseto

p. Il Presidente della ASCOM Confcommercio

Il Direttore Gabriella Orlando

p. Il Presidente della Ass.ne CONFESERCENTI - Unione Provinciale Commercianti

Il Direttore Gloria Faragli

p. Il Presidente della CONFARTIGIANATO Imprese

Il Segretario Generale Mauro Ciani

p. Il Presidente della C.N.A. Associazione Artigiani Piccole e Medie Imprese

Il Direttore Generale Renzo Alessandri

ALLEGATI:

1. Protocollo d'Intesa sottoscritto in data 27.4.2010 tra la Prefettura di Grosseto e la Camera di Commercio, la ASCOM - Confcommercio di Grosseto, l'Associazione Confesercenti e la Confartigianato Imprese di Grosseto;
2. Atto aggiuntivo sottoscritto in data 10.4.2013 tra la Prefettura di Grosseto e la confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa di Grosseto;
3. Atto di rinnovo del Protocollo d'Intesa siglato in data 12.11.2013 tra il Ministero dell'Interno e le Associazioni di categoria Confcommercio Imprese per l'Italia e Confesercenti il 12.11.2013;
4. Protocollo d'Intesa sottoscritto tra il Ministero dell'Interno con Casartigiani, CNA (Confederazione Nazionale Artigianato e Piccola e Media Impresa) e Confartigianato Imprese il 12.11.2013;
5. Nuovo Disciplinare Tecnico - edizione 2014 - predisposto dal Ministero dell'Interno - Dipartimento della Pubblica Sicurezza, d'intesa con i rappresentanti delle associazioni di categoria firmatarie.



ALL N-1

Prefettura di Grosseto
Ufficio Territoriale del Governo

Il Prefetto della Provincia di Grosseto, il Presidente della Camera di Commercio, il Presidente della ASCOM – Confcommercio di Grosseto, il Presidente dell'Associazione Confesercenti – Unione Provinciale Commercianti di Grosseto, il Presidente della Confartigianato Imprese di Grosseto,

VISTO

il Protocollo d'intesa sottoscritto in data 14 luglio 2009 tra il Ministro dell'Interno e i rappresentanti delle Associazioni di categoria Confcommercio Imprese per l'Italia e Confesercenti in materia di videoallarme antirapina, allo scopo di aumentare il livello di tutela della sicurezza degli operatori economici, anche mediante l'impiego dei più moderni strumenti tecnologici, ed in particolare l'art. 7 del medesimo Protocollo, che rimette ai Prefetti la sottoscrizione con i rappresentanti provinciali delle Associazioni di categoria di mirati protocolli in conformità agli indirizzi delineati a livello nazionale e volti alla massima diffusione ed allo sviluppo operativo del sistema;

DATO ATTO

che la Prefettura di Grosseto, in attuazione del disposto del predetto art. 7, ha già operato con lettera n. 36716/Area I del 22 settembre 2009, apposita diffusione del Protocollo Nazionale nei confronti delle Rappresentanze provinciali delle confederazioni di categoria firmatarie del Protocollo Nazionale e, per il tramite della locale Camera di Commercio, nei confronti delle altre associazioni di categoria ed esercenti non consociati, e che in conseguenza di quanto precede è pervenuta richiesta di adesione al Protocollo da parte della Confartigianato Imprese di Grosseto;

CONVENGONO QUANTO SEGUE

Art. 1 – Principi generali

Con il presente Protocollo è data piena ed integrale esecuzione al Protocollo d'Intesa in tema di videoallarme antirapina (d'ora in avanti denominato "Protocollo Nazionale"), sottoscritto in data 14 luglio 2009 dal Ministro dell'Interno, dal Presidente della Confcommercio Imprese per l'Italia e dal Presidente della Confesercenti, che si unisce in copia quale parte integrante del presente protocollo operativo.



Luy
66

Prefettura di Grosseto
Ufficio Territoriale del Governo

Art. 2 - Modalità di presentazione ed esame delle istanze di attivazione dei collegamenti

Le richieste di attivazione del collegamento da parte di esercenti aderenti alle Associazioni firmatarie dovranno pervenire attraverso le Associazioni di appartenenza alla Forza di Polizia competente da individuarsi secondo il criterio che segue:

- per il comune capoluogo, ove sono presenti la Polizia di Stato e l'Arma dei Carabinieri, l'istanza potrà essere presentata, a scelta, alla Questura o al Comando Provinciale dell'Arma dei Carabinieri. La Forza di Polizia che riceverà la richiesta opererà le verifiche di compatibilità tecnica di cui al successivo comma 3 e la trasmetterà successivamente all'altra Forza di Polizia per le analoghe verifiche di propria competenza. Tanto sul presupposto che "i segnali video allarmati dovranno indistintamente essere veicolati verso entrambe le Forze di Polizia presenti", come previsto dal capitolato tecnico.
- nei restanti comuni della provincia, ove non sono presenti con propri presidi entrambe le FF.PP., l'istanza andrà presentata al locale Comando Carabinieri competente per territorio.

Le richieste di attivazione del collegamento da parte di esercenti non aderenti alle predette Associazioni dovranno pervenire alla competente Forza di Polizia attraverso la locale Camera di Commercio.

Le predette istanze dovranno essere corredate da idonea documentazione comprovante la conformità dei materiali ai requisiti tecnici di cui al Progetto allegato al Protocollo Nazionale, per la preventiva valutazione di competenza delle componenti specializzate della Zona Telecomunicazioni della Polizia di Stato e dell'Ufficio Logistico dei Comandi di Legione Carabinieri, ai sensi dell'art. 3, comma 4, del Protocollo Nazionale.

Art. 3 - Adempimenti delle Associazioni di categoria firmatarie

Le Associazioni firmatarie si impegnano:

- a portare a conoscenza, anche dei nuovi associati, i contenuti del presente Protocollo e del Protocollo Nazionale;
- a costituire il tramite per la presentazione delle istanze di adesione da parte degli esercenti interessati, fornendo ad essi assistenza ed ogni utile supporto conoscitivo, anche relativamente all'attuazione dei principi e delle regole stabiliti dal Garante per la protezione dei dati personali in materia di videosorveglianza, ovvero al divieto di controllo a distanza dei lavoratori di cui all'art. 4 della Legge 20 maggio 1970, n. 300;
- a collaborare, per gli aspetti di competenza, all'attività di monitoraggio svolta dall'Osservatorio di cui al successivo art. 6.



Prefettura di Grosseto
Ufficio Territoriale del Governo

by
66

Art. 4 - Adempimenti delle Forze di Polizia

- La Questura ed il Comando Provinciale dell'Arma dei Carabinieri si impegnano:
- ad individuare e comunicare alle Associazioni firmatarie ed alla Camera di Commercio, Industria, Artigianato e Agricoltura i nominativi di un referente per la trattazione delle istanze di collegamento alle rispettive centrali operative;
 - ad avere la massima cura nella gestione ed utilizzo del materiale tecnico ad esse conferito in comodato gratuito in conformità all'art. 3 del Protocollo Nazionale, segnalando tempestivamente ai fruitori eventuali anomalie di funzionamento o guasti che possono limitare o compromettere il servizio reso, al fine di consentire ad essi la sollecita adozione di iniziative idonee a rimuovere l'inconveniente segnalato;
 - ad informare gli esercizi che si avvalgono di altri sistemi già installati e collegati con le rispettive centrali operative, dell'obbligo di uniformare, entro 24 mesi, i requisiti tecnici degli apparati ai dettami tecnici di cui al Capitolato allegato al Protocollo Nazionale del 14 luglio 2009.

Art. 5 - Adempimenti dei fruitori

- I fruitori si impegnano:
- ad informare tempestivamente la competente Forza di Polizia di eventuali guasti od avarie degli impianti installati nel proprio esercizio e delle iniziative in atto per il sollecito superamento dell'inconveniente;
 - a comunicare alla competente Forza di Polizia il nominativo dei soggetti responsabili e incaricati dell'utilizzazione degli impianti.

Art. 6 - Osservatorio sull'attuazione del Protocollo

E' costituito presso la Prefettura - U.T.G. di Grosseto un Osservatorio, per il monitoraggio del sistema e per l'acquisizione degli elementi di informazione di cui all'art. 8 del Protocollo Nazionale, anche ai fini della loro successiva trasmissione al Dipartimento della Pubblica Sicurezza.

L'osservatorio, presieduto dal Vice Prefetto Vicario o, in sua vece, da altro dirigente della Prefettura-Ufficio Territoriale del Governo di Grosseto, è composto da funzionari e ufficiali delle Forze di Polizia e da rappresentanti delle Associazioni firmatarie appositamente designati.



Prefettura di Grosseto
Ufficio Territoriale del Governo

Art. 7 - Adesione alla convenzione da parte di altri soggetti

Il presente Protocollo è sottoscritto dai Presidenti della ASCOM Confcommercio di Grosseto, dell'Associazione Confesercenti - Unione Provinciale Commercianti di Grosseto, della Confartigianato Imprese di Grosseto e della Camera di Commercio, Industria, Artigianato e Agricoltura di Grosseto.

Lo stesso è aperto all'eventuale successiva adesione, con sottoscrizione del presente Protocollo, da parte di altre Associazioni di categoria o di singoli fruitori non aderenti alle predette Organizzazioni. Le istanze di adesione dei singoli fruitori, indirizzate al Prefetto di Grosseto, dovranno essere presentate tramite la Camera di Commercio, Industria, Artigianato e Agricoltura.

Grosseto, 27 aprile 2010

Il Prefetto di Grosseto

dott. Giuseppe Linardi

Il Presidente della Camera di Commercio, Industria, Artigianato e Agricoltura

dott. Giovanni Lamioni

Il Presidente della ASCOM Confcommercio

sig. Claudio Chiti

Il Presidente della Ass.ne CONFESERCENTI - Unione Prov.le Commercianti

sig. Pierferruccio Lucheroni

Il Presidente della CONFARTIGIANATO Imprese

dott. Giovanni Lamioni



CONFCOMMERCIO
IMPRESE PER L'ITALIA



1

PROTOCOLLO D'INTESA

Il Ministero dell'Interno, con sede a Roma, piazza del Viminale 1, rappresentato dal Ministro dell'Interno On. Roberto Maroni

Confcommercio Imprese per l'Italia, con sede in Roma, piazza G.G. Belli 2, rappresentata dal Presidente dott. Carlo Sangalli

Confesercenti, con sede in Roma, Via Nazionale 60, rappresentata dal Presidente dott. Marco Venturi

- VISTI gli artt. dal 133 al 141 del Titolo IV "Delle guardie particolari e degli istituti di vigilanza e di investigazione privata", del regio decreto 18 giugno 1931, n. 773 "Testo unico delle Leggi di Pubblica Sicurezza";
- VISTO il D.P.R. 4 agosto 2008, n. 153 recante modifiche al regio decreto 6 maggio 1940, n. 635 "Regolamento per l'esecuzione del T.U. 18 giugno 1931, n. 773, delle leggi di pubblica sicurezza", in materia di guardie particolari, istituti di vigilanza e investigazioni private;
- VISTO l'art. 13 della legge 1 aprile 1981, n. 121 "Nuovo ordinamento dell'Amministrazione della pubblica sicurezza", secondo cui "Il Prefetto ha la responsabilità generale dell'ordine e della sicurezza pubblica nella provincia e sovrintende all'attuazione delle direttive emanate in materia";
- VISTI l'art. 17 della legge 26 marzo 2001, n. 128 e l'art. 7 del decreto legge 23 maggio 2008, n. 92 recante "misure urgenti in materia di sicurezza pubblica" convertito con modificazioni dalla legge 24 luglio 2008, n. 125 nonché le correlate direttive ministeriali concernenti i piani coordinati di controllo del territorio;
- VISTO l'art. 39 della legge 16 gennaio 2003, n. 3, secondo cui il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno può stipulare convenzioni in materia di sicurezza "con soggetti pubblici e privati

Patto allo. n. 128
e n. 125



dirette a fornire, con la contribuzione degli stessi soggetti, servizi specialistici, finalizzati ad incrementare la sicurezza pubblica”;

- VISTI** gli artt. 11 e 13 del decreto legislativo 30 giugno 2003, n. 196 (codice in materia di protezione dei dati personali);
- VISTA** la circolare ministeriale n. 558/A/421.2/70/456 dell'8 febbraio 2005 avente per oggetto: “Sistemi di videosorveglianza. Definizione di linee guida in materia”;
- VISTO** il Protocollo d'Intesa siglato il 30 giugno 2003 tra il Ministero dell'Interno e Confcommercio, Confesercenti e Comufficio, avente lo scopo di promuovere il progetto denominato Securshop, che prevedeva “*un sistema di allarme controllato - con telecamere - dei locali commerciali, attivabile con semplice pressione sul pulsante di comando ed in grado di collegarsi con le sale e centrali operative delle Forze di polizia e di trasmettere, in caso di rapina all'interno dei locali, le immagini in tempo reale*”;
- CONSIDERATO** che si rende necessario, anche alla luce delle nuove tecnologie, migliorare e perfezionare il protocollo d'intesa suddetto, pur valido nella sua impostazione generale, sia per quanto concerne gli aspetti degli adempimenti procedurali sia sotto il profilo tecnologico;
- RILEVATO** di dover promuovere la massima diffusione di una progettualità che abbia lo scopo di aumentare i livelli di tutela degli operatori economici in generale, con particolare riferimento a quelli aderenti alle categorie rappresentate dalle Confederazioni di cui sopra;
- RITENUTO** che a tal fine occorre assicurare su tutto il territorio adeguati sistemi e appropriati servizi ad essi connessi, nel rispetto comunque del vincolo inderogabile di



CONFCOMMERCIO
IMPRESERPERL'ITALIA



uniformità a livello nazionale dei profili tecnologici e funzionali,

CONVENGONO QUANTO SEGUE

Art. 1

Generalità

La presente convenzione sostituisce quella stipulata il 30 giugno 2003 e stabilisce i criteri generali della collaborazione in tema di videoallarme antirapina tra Ministero dell'Interno e Confcommercio Imprese per l'Italia e Confesercenti.

Al progetto di cui agli articoli successivi potranno aderire, oltre alle suddette Confederazioni ed alle loro rappresentanze locali e di categoria, anche le altre organizzazioni di categoria e gli esercenti non consociati, tutti di seguito denominati *fruitori*.

Art. 2

Architettura del sistema

Il sistema di videoallarme antirapina - configurato secondo i requisiti tecnici indicati nell'allegato capitolato che costituisce parte integrante del presente protocollo - dovrà interagire direttamente con gli apparati in essere presso le sale e le centrali operative della Polizia di Stato e dell'Arma dei Carabinieri, conformemente ai principi predisposti dal Garante per la protezione dei dati personali in materia di videosorveglianza.

Art. 3

Scelta delle imprese fornitrici

Gli impianti saranno concessi alle Forze di polizia in comodato d'uso gratuito dai *fruitori*, tramite le imprese fornitrici degli apparati e dei servizi da loro indicate.



CONFEDERAZIONE
IMPRESE PER L'ITALIA



Le Confederazioni firmatarie potranno delegare le loro rappresentanze locali e di categoria nella scelta delle imprese fornitrici degli apparati e dei servizi.

Gli oneri concernenti le linee telefoniche per i necessari collegamenti, l'installazione e il collaudo delle apparecchiature, gli interventi d'urgenza, la manutenzione ordinaria e straordinaria, l'adeguamento e l'aggiornamento degli strumenti tecnologici nonché la formazione degli addetti alle sale e alle centrali operative competono ai *fruitori* che potranno avvalersi eventualmente delle imprese da loro prescelte.

I materiali offerti dai *fruitori* a loro richiesta dovranno essere preventivamente sottoposti all'esame delle componenti specializzate delle Zone Telecomunicazioni della Polizia di Stato e dell'Ufficio Logistico dei Comandi di Legione Carabinieri, per verificare la loro rispondenza ai requisiti contenuti nel capitolato tecnico suddetto.

Art. 4

Adeguamento degli impianti esistenti

I *fruitori* avranno cura di far uniformare - d'intesa con le imprese fornitrici degli apparati e dei servizi da loro indicate - entro 24 mesi i sistemi finora installati alla medesima architettura ed ai requisiti tecnici di cui al capitolato, verificandone congiuntamente lo stato di attuazione dopo 12 mesi.

Art. 5

Funzionalità del sistema

In caso di concreta ed esclusiva possibilità di rapina l'esercente potrà attivare l'allarme per inviare le immagini, in tempo reale alle postazioni delle sale e delle centrali operative della Polizia di Stato e dell'Arma dei Carabinieri per gli interventi di competenza.

La trasmissione delle immagini potrà avvenire anche utilizzando le connessioni fisiche di rete del "centro di controllo", gestito da istituto di vigilanza privata - eventualmente incaricato dai *fruitori* - di integrare il sistema attraverso le tipiche attività riconducibili alla cd. "sicurezza secondaria" che non richiedono l'esercizio di potestà autoritative squisitamente di polizia.



CONFCOMMERCIO
IMPRESE PER L'ITALIA



Le immagini della rapina non dovranno in ogni caso essere visualizzate da parte dei cennati istituti e, ai fini info-investigativi, dovranno essere custodite opportunamente dall'esercente, secondo le prescrizioni del Garante per la protezione dei dati personali.

Art. 6

Adempimenti relativi alle nuove attivazioni

I fruitori dovranno comunicare alla Prefettura e alle Forze di polizia, ai fini delle opportune verifiche sulla conformità amministrativa, ogni nuova attivazione nonché la ditta prescelta - in possesso di abilitazione di sicurezza, qualora richiesta in conformità all'art. 41 del DPCM del 3 febbraio 2006 "Norme concernenti la protezione e la tutela delle informazioni classificate" - per l'installazione dei dispositivi e la fornitura dei relativi servizi in ambito territoriale, la data dell'accesso e le generalità del personale tecnico, parimenti dotato dell'abilitazione di cui sopra qualora richiesta, incaricato delle attività tecniche.

Art. 7

Diffusione del protocollo

Il Ministero dell'Interno e le Confederazioni si impegnano a diffondere e rendere efficace il presente protocollo, informando rispettivamente le Prefetture, il Dipartimento della Pubblica Sicurezza e il Comando Generale dell'Arma dei Carabinieri nonché le rappresentanze locali e di categoria di Confcommercio Imprese per l'Italia e Confesercenti per consentire una fattiva reciproca collaborazione.

I Prefetti favoriranno la massima diffusione e lo sviluppo operativo del sistema, sottoscrivendo con i rappresentanti provinciali delle associazioni di categoria mirati protocolli conformi ai cennati indirizzi.

Art. 8

Monitoraggio del sistema e risoluzione delle problematiche

Le Prefetture, d'intesa con le rappresentanze locali e di categoria delle Confederazioni interessate, effettueranno - con cadenza annuale - il monitoraggio del sistema per verificare la percentuale degli esercenti aderenti, l'andamento della delittuosità nei confronti delle suddette categorie, l'efficacia e l'efficienza del sistema, ai fini delle iniziative da assumere in sede territoriale, rappresentando al Dipartimento della Pubblica



CONFCOMMERCE
IMPRESSE PER L'ITALIA



Sicurezza le problematiche o le proposte suscettibili di interventi a livello centrale o di valenza nazionale, da valutare con le Confederazioni, le quali potranno in ogni caso chiedere d'iniziativa l'esame congiunto di aspetti di interesse comune.

Art. 9

Entrata in vigore e durata

Il presente protocollo d'intesa entra in vigore dopo 120 giorni dalla data di sottoscrizione; allo scopo di consentire la predisposizione della tecnologia necessaria per la funzionalità del sistema, e ha la durata di 4 anni, con possibilità di tacito rinnovo entro il 31 ottobre 2013.

Roma, 14 luglio 2009

Confcommercio
Imprese per l'Italia
Il Presidente
dott. Carlo Sangalli

Confesercenti

Il Presidente
dott. Marco Venturi

Il Ministro dell'Interno
On. Roberto Maroni



PER COPIA CONFORME
IL COLLABORATORE AMM.VO
Dott. Maria Rosaria SOAVE



CONFCOMMERCE
UNIONE PER L'ITALIA



Progetto per un sistema di allarme antirapina controllato con telecamere integrato con le Sale/Centrali Operative delle Forze di Polizia Requisiti tecnici

PREMESSA

Il presente documento ha per oggetto la realizzazione di un sistema di allarme antirapina - di seguito denominato *Videoallarme* - mediante il controllo con telecamere dei locali commerciali, attivabile con semplice pressione sul pulsante di comando, in grado di collegarsi con le sale/centrali operative delle Forze di Polizia e di trasmettere le immagini in tempo reale e registrate.

Il videoallarme è un sistema che prevede il collegamento degli esercizi commerciali alle sale/centrali operative con collegamento telematico anche per il tramite di un centro di controllo, qualora presente gestito da istituto di vigilanza privata.

Il centro di controllo, nell'ambito dell'architettura del videoallarme, riveste il ruolo di concentratore dei collegamenti ovvero degli allarmi provenienti dagli esercizi commerciali, per poi instradarli verso le sale/centrali operative della Polizia di Stato e dell'Arma dei Carabinieri ad ognuna tramite un unico collegamento telematico. Il centro di controllo, nei casi di allarme per rapina, avrà esclusivamente un ruolo di transito del flusso del video allarme, senza rivestire compiti di filtraggio e trattazione dell'informazione.

L'implementazione del sistema è improntato alla *gestione intelligente* degli eventi, quest'ultima da intendersi quale gestione delle informazioni conforme ai sistemi presenti e in modo tale da rendere minimo l'intervento dell'operatore nella gestione degli allarmi.

Le specifiche tecniche proposte nel presente documento sono da intendersi come *requisiti minimi*, nel senso che si potranno implementare soluzioni tecnologiche migliorative (trasmissione dell'audio in tempo reale alla sala/centrale operativa, formato immagine di dimensioni superiori, etc.), purché tali da garantire gli obiettivi prefissati in termini di prestazioni, sicurezza e gestibilità nell'ottica dell'ottimizzazione dei costi.



CONFEDIRETTORI
IMPRESSE PER L'ITALIA



INTEGRAZIONE CON I SISTEMI ESISTENTI PRESSO LE SALE/ CENTRALI OPERATIVE

Necessità vincolante in fase di progettazione del sistema in argomento è l'integrazione con i sistemi informatici esistenti presso le sale/centrali operative delle FF.PP., presso le quali dovranno essere resi disponibili i flussi video allarmati "live", provenienti dalle telecamere installate presso l'esercizio per il tramite del Centro di Controllo ovvero direttamente, per la "contestualizzazione" degli stessi all'interno dei rispettivi applicativi (SCT - Sistema per il Controllo del Territorio e CC112 - Sistema di gestione interventi) e la relativa gestione "intelligente".

Inoltre è richiesto l'interfacciamento dei citati flussi video con i sistemi di visualizzazione su grande schermo esistenti presso le Sale/Centrali Operative, dove i nuovi segnali provenienti dalle telecamere dovranno essere resi disponibili in formato compatibile con la matrice video preesistente, opportunamente estesa mediante aggiunta di elementi necessari (hardware, software) facenti parte della fornitura.

ARCHITETTURA

L'architettura di sistema viene descritta secondo la presente segmentazione:

CARATTERISTICHE DEL SISTEMA AUDIO/VIDEO E DELLE REGISTRAZIONI PRESSO GLI ESERCIZI COMMERCIALI

- Alta risoluzione, in ogni caso non inferiore ad un formato immagine VGA pari a 307.200 pixel (640x480 pixel). Eventualmente sarà possibile considerare l'impiego di complessi di ripresa con definizione dell'ordine del megapixel, purché aderenti al profilo di missione richiesto e alle performance derivanti da specifiche tecniche che costituiscono vincolo di comunicazione.
- Supporto della registrazione audio (WAVE compatibile con campionamento almeno a 16 bit).
- Rappresentazione delle immagini a colori e in modalità day&night.
- Visualizzazione fino al limite di una rappresentazione di tipo "full motion" (visione diretta di ogni particolare che prende parte all'evento criminoso in tempo reale).
- Conservazione dei filmati (audio + video) per almeno 7 giorni h 24 (conformemente a quanto previsto dal paragrafo 3.4 del Provvedimento generale sulla videosorveglianza del 29 aprile 2004 del Garante per la protezione dei dati personali), con risoluzione almeno VGA ad un frame rate pari a 25 fps e sensibilità microfonica pari a -54db.



CONFEDERAZIONE
IMPRESE PER L'ITALIA



- 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.
- Algoritmo di compressione compreso nelle famiglie MPEGx, MJPEG.
- Videoregistrazione delle immagini allarmate (audio e video) di ciascuna telecamera e conservazione in memoria per almeno 7 giorni consecutivi.
- Compatibilità del software con i sistemi operativi utilizzati presso le Sale/Centrali operative.
- Nel caso in cui l'esercente usufruisca (o intenderà farlo in un secondo momento) anche di altri servizi di sorveglianza - autonomamente attivati sulla base di specifici contratti con il medesimo istituto di vigilanza che svolge le funzioni di Centro di Controllo nell'ambito della rete di cui al presente capitolato - il sistema dovrà supportare una duplice modalità di invio dell'allarme. In tale ipotesi, dovranno essere installati due tasti d'allarme, ai quali corrispondono due differenti funzionalità:
 1. allarme antirapina: il flusso di video-allarme generato viene veicolato attraverso il Centro di Controllo, ma viene direttamente transitato alla sala/centrale operativa, allertando le competenti Forze di Polizia;
 2. allarme generico (per le altre situazioni di diversa natura di cui al relativo contratto stipulato con gli istituti di vigilanza): il flusso di video-allarme è veicolato solo al Centro di Controllo per gli interventi del caso.Il flusso dati e le linee trasmissive nell'ipotesi 1 di cui sopra, dovranno sempre essere improntate alle specifiche tecniche riportate nel presente capitolato.

SICUREZZA DELLE REGISTRAZIONI

Il supporto di memoria di massa, utilizzato per la registrazione e conservazione dei filmati per le finalità d'impiego da parte dell'Autorità Giudiziaria, dovrà obbligatoriamente essere:

- asportabile da parte degli Organi di Polizia Giudiziaria e conseguentemente sostituibile con analogo apparato, a carico dell'Associazione di categoria ovvero dell'esercente, per garantire a quest'ultimo la continuità del servizio di video-allarme;
- leggibile attraverso un collegamento rapido ad un generico personal computer, dotato del necessario software di lettura, ma "assolutamente immodificabile nei contenuti" (ovvero solo il sistema installato presso l'esercente deve poter essere in grado di scrivere e registrare contenuti sul supporto di memoria in argomento);
- monitorabile, in locale o da remoto, attraverso la registrazione in un file di log di tutte le variazioni di stato di funzionamento dello stesso supporto (tale file di log dovrà essere reso disponibile agli Organi di Polizia Giudiziaria contestualmente al sequestro del supporto);
- custodito con efficaci misure di protezione (es. dispositivi di apertura ritardata del vano di alloggiamento del videoregistratore).



CARATTERISTICHE DEI FLUSSI AUDIO/VIDEO ALLARMATI DESTINATI ALLE SALE/CENTRALI OPERATIVE

Trasferimento delle immagini su protocollo IP (IPver04 compatibile).

- I segnali video allarmati verso le sale/centrali operative delle FF.PP. devono essere convogliati con un unico collegamento fisico (eventualmente per il tramite di un Centro di Controllo), obbligatoriamente a "filo" (la "policy di sicurezza" adottata dalle strutture militari, al momento, vieta la connessione telematica da/verso l'esterno su reti wireless), ovvero un unico punto di accesso al sistema presente su ciascuna sala/centrale operativa: uno per la sala operativa della Questura e uno per la centrale operativa del Comando Provinciale dell'Arma CC. Tale collegamento, punto nevralgico del sistema, dovrà garantire l'efficienza del servizio che si intende offrire all'esercente.
- I segnali video allarmati dovranno indistintamente essere veicolati verso entrambe le Forze di polizia presenti.
- Le immagini che verranno trasmesse alla postazione di sala/centrale operativa dovranno avere le seguenti caratteristiche minime:
 - media risoluzione con un formato QVGA, corrispondente ad un numero di pixel pari a 76.800 (320x240 pixel);
 - formato delle immagini in modalità colore (24 bit/pixel, pari a 16 ML di colori) e in B&W notturna (8 bit/pixel, 256 livelli di grigio), con algoritmo standard di compressione della famiglia MPEGx / MJPEG;
 - frame rate non inferiore a 2 fps.
- La capacità relativa alla banda passante va calcolata riguardo alle necessità di accesso dei sistemi periferici tenendo conto che il massimo ritardo consentito per tutte le trasmissioni, e per ogni telecamera facente parte di un singolo sistema periferico, non sia superiore al valore di 1500 millisecondi espresso come tempo di latenza (parametro legato alla capacità della banda dell'infrastruttura di telecomunicazioni e migliorabile in funzione della stessa).

Deve essere garantita la trasmissione contemporanea di videoallarmi provenienti da diversi esercizi commerciali. Il collegamento sarà di tipo a larga banda, riservato e protetto con sistemi firewall.

SISTEMI DI GESTIONE E CONTROLLO PRESSO LE SALE/CENTRALI OPERATIVE

Laddove presente il sistema SCT/CC112, le funzionalità del sistema dovranno essere integrate nella postazione operatore già presente secondo le modalità successivamente meglio descritte e per il tramite di:



CONFEDOMMERCA
MARCHESSE PER L'ITALIA



- un apparato attivo ove attestare i flussi video eventualmente provenienti dal centro di controllo, da fornirsi sempre a cura delle Associazioni di categoria o dell'esercente non consociato;
- un video server dedicato alla ricezione dei segnali video da posizionarsi all'esterno delle reti intranet di ciascuna Forza di polizia (DMZ - DeMilitarized Zone); da fornirsi sempre a cura delle associazioni di categoria o dell'esercente non consociato (per la P. di S. n° 103 videosever; per l'Arma n° 109 videosever).

In particolare, il protocollo di scambio dati dovrà essere basato su standard SOAP/XML, che consente l'identificazione del problema e l'inserimento in automatico dell'evento nella coda (ordine cronologico secondo il quale arrivano i videoallarmi) del sistema SCT e del sistema CC112. I relativi campi della scheda evento, uguali per tutte le sale/centrali operative, dovranno essere modulati sulla base di quelli già definiti e descritti per gli eventi attualmente gestiti. In ogni caso, dovranno comprendere tutti gli elementi identificativi e referenziali dell'esercizio da cui proviene l'allarme.

Per il corretto abbinamento dell'allarme all'esercizio associato e la sua completa gestione da parte dell'operatore di sala/centrale, è necessaria una fase preliminare di codifica. Deve pertanto essere definito un protocollo di interscambio informazioni, tra i vari attori del progetto, che consenta:

- la stipula del contratto di servizio, l'invio delle informazioni alle due FF.PP. interessate al progetto per il tramite delle Prefetture (dati anagrafici dell'esercizio e dell'esercente e dati tecnici identificativi dell'apparato);
- la codifica delle suddette informazioni da parte degli organi tecnici delle FF.PP. nel sistema SCT/CC112 e l'attribuzione di un codice univoco dell'impianto.

Si dovrà prevedere la trasmissione alle FF.PP. dei dati anagrafici degli esercizi e degli esercenti autorizzati in formato elettronico (formato CSV).

POSTAZIONE DI GESTIONE DEI FLUSSI VIDEO ALLARMATI

Si ribadisce che in tutte le centrali operative dei Carabinieri e nelle sale operative della Polizia di Stato, ove è presente e disponibile SCT/CC112, tutti i flussi video dovranno essere interfacciati al sistema per la gestione diretta su ogni posto operatore presente in sala/centrale operativa. Saranno a carico dell'Associazione di categoria o dell'esercente non consociato tutte le implementazioni necessarie per consentire una corretta integrazione, previo coordinamento con i referenti designati rispettivamente dal Questore e dal Comandante Provinciale dei Carabinieri.



CONFEDIRETTORE
SINDACATO



Le sale/centrali operative, a seguito di pervenuto allarme, dovranno poter svolgere le seguenti attività:

- visualizzare e memorizzare le immagini dal vivo in tempo reale;
- archiviare le informazioni di controllo (es. LOG degli accessi);
- gestire gli allarmi.

Nell'eventualità che all'interno della/e sala/e operative della Polizia di Stato e centrale/i operative dei Carabinieri fossero già presenti strumenti di visualizzazione su schermi panoramici (schermi al plasma, videowall, videoproiettori, ecc.) disponibili per l'impiego con l'applicazione specifica e tecnicamente interfacciabili, il progettista - incaricato dall'Associazione di categoria o dall'esercente non consociato - dovrà prevedere l'impiego di tali apparati.

In caso di indisponibilità di postazione SCT/CC112, dovrà essere fornita una "postazione di gestione", composta da un personal computer con case middle tower (o in alternativa da rack, in funzione delle scelte progettuali), dotato delle seguenti caratteristiche minime:

CARATTERISTICHE	RICHIESTO
BAPCO SYSMARK 2007 RATING.	Il PC dovrà essere in grado di raggiungere almeno 160 punti
NR Processori/ CORE	1/2
RAM Installata	2 GB
RAM MAX	2 GB
Velocità RAM	533 MHz
Capacità disco fisso Installato	Nr. 2 HD 320 GB configurati in modalità Raid 1
Interfaccia Disco Fisso	SATA
Velocità rotazione	7.200 RPM
Chipset Grafico	Non integrato
RAM Installata	512MB non condivisa
Risoluzione Max	1280x1024
Bus grafico	PCIx
Masterizzatore	DVD +-RW
Velocità supportate	Dichiarare il valore
Velocità Rete /Standard	100 /1000- Ethernet
Porte (Quantità e Tipo)	1 parallela 1 seriale 4 USB 2.0 retro 2 USB 2.0 avanti 1 RJ-45 2 VGA 1 microfono 1 cuffia



CONFESERCENTI
IMPRESSE PER L'ITALIA



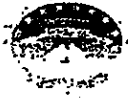
Slot di espansione	2 PCI
Tastiera e Mouse	Italiana 108 tasti, 2 tasti con scroll
Monitor doppio Tipo /Dimensione	LCD 21" TFT 1280 x 1024 Dot pich non superiore a 0,297 mm, con amplificazione incorporata
UPS	Con funzione di stabilizzazione e continuità della alimentazione elettrica per almeno 20 minuti e comunque di capacità non inferiore a 600VA
Sistema operativo	Windows 2008 Server (tassativo)
Software in dotazione	Ms Office Professional, Antivirus

- n.1 stampante di rete laser colori A4 con tavolino porta stampante:

CARATTERISTICHE	RICHIESTO
TECNOLOGIA	Laser colori
RISOLUZIONE STAMPA B/N	600 x 600 dpi
RISOLUZIONE STAMPA Colori	1200 x 1200 dpi
FORMATO CARTA	A4 -
VELOCITA' DI STAMPA B/N	28 pagine/minuto
VELOCITA' DI STAMPA Colori	16 pagine/minuto
RAM Installata	128 MB
SUPPORTI DI STAMPA	Carta normale, buste, lucidi, etichette
INTERFACCE	Hi-Speed USB
ALIMENTAZIONE CARTA	vassoio da 250 fogli
RUMOROSITA'	In stampa max 66 dB, Riposo max 54 dB

Le postazioni di gestione con le necessarie configurazioni ed abilitazioni, dovranno essere equipaggiate con un applicativo software, con licenza d'uso, che:

- svolga la funzionalità di videosever per la gestione dei flussi video live MPEGx, o MJPEG (in funzione delle configurazioni) ed audio MPEG1;
- svolga la funzione di DVR per la registrazione dei flussi video MPEGx o MJPEG (in funzione delle configurazioni) ed audio ricevuti a seguito di allarme;
- visualizzi in modalità videosplit "n" flussi video allarmati contemporanei live o registrati selezionabili dall'utente o pre-impostati;
- gli "allarmi video" dovranno essere registrati e tenuti disponibili, per esigenze investigative, per almeno 7 giorni e non cancellati se non da personale abilitato;
- visualizzi una cartografia interattiva a livelli multipli navigabili che permetta di selezionare (tramite modalità drag & drop) le telecamere da visualizzare sul videosplit;
- permetta la visualizzazione e la gestione dei flussi video allarmati entranti con segnalazione acustica;



CONFEDERAZIONE
IMPRESARIATI TELECOM



- veicoli le informazioni attraverso la rete IP;
- gestisca l'accesso degli utenti;
- gestisca profili utenti diversi con livelli di autorizzazione diversi (amministrazione, manutenzione, visione live, visione playback, esportazione filmati, ecc.).

La "postazione di gestione" risulterà autorizzata (a livello di configurazione, comunque modificabile) alla visualizzazione ed all'esportazione delle immagini registrate.

ADESIONE AL SISTEMA DA PARTE DI ESERCENTE NON AFFILIATO ALLE ASSOCIAZIONI DI CATEGORIA

Il sistema dovrà consentire l'adesione anche di esercenti non affiliati alle associazioni di categoria.

Questi potranno avvalersi di un centro di controllo gestito dall'istituto di vigilanza privata, qualora abbiano conferito a quest'ultimo la gestione del complessivo flusso di video-allarme. In tale ipotesi il sistema locale sarà strutturato secondo i requisiti tecnici sinora descritti, compreso il diretto transito dell'allarme antirapina alla sala/centrale operativa delle Forze di polizia.

Qualora gli esercenti non affiliati alle associazioni di categoria non intendano avvalersi di un centro di controllo gestito dall'istituto di vigilanza privata, le specifiche tecniche del sistema locale rimangono inalterate, mentre il flusso trasmissivo viene modificato come di seguito indicato:

- viene abolito il collegamento wireless (GPRS/UMTS tra l'esercente ed il centro di controllo);
- viene instaurato un collegamento di tipo fisico (es: HDSL) tra esercente e Forze di polizia con oneri a carico del primo. Il flusso video sarà attestato, qualora ci sia disponibilità di porte, sugli stessi apparati attivi (router) forniti dalle associazioni di categoria e veicolati sulle precedentemente citate postazioni di gestione attestate in DMZ. In caso contrario dovrà essere fornito anche il router contestualmente al collegamento.

Occorre, infine, che l'esercente provveda, con oneri a proprio carico, a segnalare tempestivamente alle Forze di polizia il verificarsi di guasti al sistema di allarme.

INSTALLAZIONE, ASSISTENZA E MANUTENZIONE

Ogni installazione presso le sale/centrali operative dovrà essere sottoposta a preventiva verifica di funzionalità da parte del personale tecnico delle competenti



CONFEDERAZIONE
IMPRESE PER L'ITALIA



Zone Telecomunicazioni della Polizia di Stato e dell'Ufficio Logistico dei Comandi di Regione Carabinieri, congiuntamente ai tecnici dell'impresa fornitrice ovvero della struttura tecnica individuata dalle Confederazioni, con facoltà di delegare le loro rappresentanze locali e di categoria, ovvero dagli esercenti non consociati.

Per le apparecchiature assegnate in comodato d'uso all'Amministrazione, corredate di idonea documentazione tecnica relativa all'architettura e alle specifiche tecniche del sistema, dovrà essere fornito un servizio di assistenza e manutenzione correttiva, preventiva ed evolutiva per il quale sarà individuato un servizio di help desk.

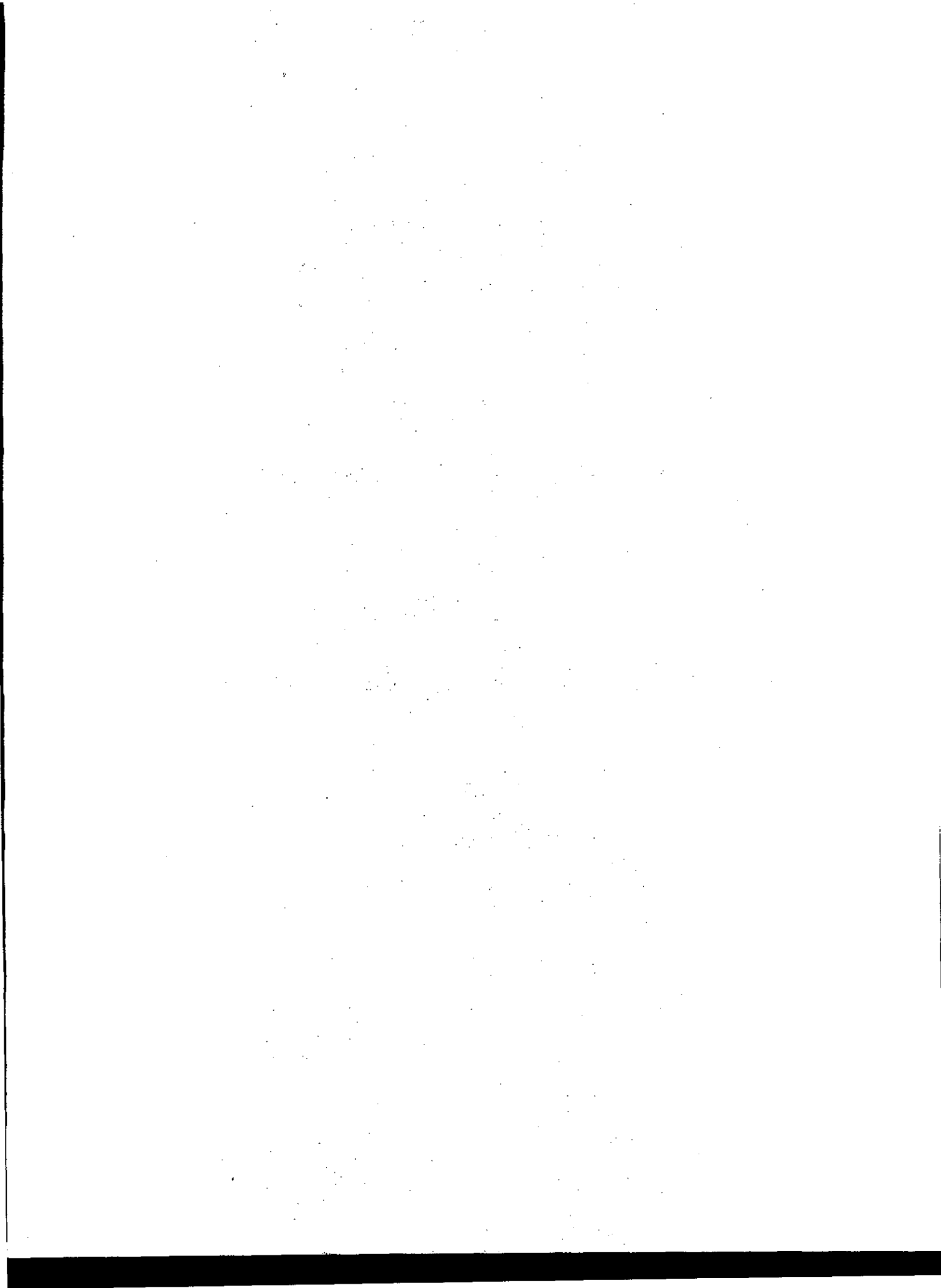
FORMAZIONE ED ADDESTRAMENTO

Alle Confederazioni o loro rappresentanze locali e di categoria ovvero agli esercenti non consociati competono gli oneri inerenti alla formazione degli addetti alle sale e alle centrali operative. Per tale incombenza potranno avvalersi anche delle imprese da loro prescelte.

Si dovranno prevedere almeno 2 giorni di affiancamento all'utente, uno per ciascuna sala/centrale operativa per:

- addestramento all'utilizzo delle procedure;
- configurazioni (fine-tuning) dei parametri di sistema, per soddisfare eventuali richieste degli operatori;
- verifica della completa funzionalità del sistema;
- verifica del corretto utilizzo del sistema da parte degli operatori.

Dovrà essere altresì previsto un affiancamento on-the-job di almeno 1 giorno per ciascuna sala operativa da parte di personale specializzato - parimenti in possesso di abilitazione di sicurezza, qualora richiesta in conformità all'art. 41 del DPCM del 3 febbraio 2006 "Norme concernenti la protezione e la tutela delle informazioni classificate" - in grado di correggere eventuali errori di utilizzo degli operatori nella fase iniziale di conduzione e di funzionamento dell'impianto.





Prefettura di Grosseto
Ufficio Territoriale del Governo

ATTO DI ADESIONE

VISTO il Protocollo d'Intesa sottoscritto in data 14 luglio 2009 dal Ministro dell'Interno, dal Presidente della Confcommercio Imprese per l'Italia e dal Presidente della Confesercenti in tema di video allarme antirapina;

VISTA la convenzione stipulata in data 27 aprile 2010 tra il Prefetto pro tempore di Grosseto, il Presidente della Camera di Commercio, il Presidente della ASCOM - Confcommercio di Grosseto, il Presidente dell'Associazione Confesercenti e il Presidente della Confartigianato Imprese di Grosseto, con la quale è stata data piena e integrale esecuzione nella provincia di Grosseto all'art. 7, comma secondo, del citato Protocollo d'Intesa;

VISTO l'art. 7 della suddetta convenzione che prevede l'eventuale successiva adesione, con relativa sottoscrizione, da parte di altre Associazioni di categoria o di singoli fruitori non aderenti alle predette Organizzazioni;

VISTA la nota prot. n. 4R/89/6/13 in data 18 marzo 2013 con la quale il dott. Renzo Alessandri - Direttore della C.N.A. di Grosseto - ha chiesto di poter aderire alla convenzione stipulata presso questa Prefettura il 27.4.2010

CONSIDERATA l'opportunità di promuovere la massima diffusione di uno strumento condiviso che ha lo scopo di aumentare i livelli di tutela degli operatori economici in genere

DETERMINA

l'adesione della Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa alla convenzione stipulata in data 27 aprile 2010 presso questa Prefettura di esecuzione dell'art. 7, comma secondo, del Protocollo d'Intesa in tema di video allarme antirapina.

Grosseto, 10 aprile 2013

Il Prefetto di Grosseto

Marco Valentini

Il Direttore della

Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa

Renzo Alessandri



MINISTERO
DELL'INTERNO



CONFCOMMERCIO
IMPRESSE PER L'ITALIA



CONFESERCENTI

PROTOCOLLO QUADRO

Rinnovo e aggiornamento
del Protocollo d'Intesa del 14 luglio 2009

tra

Il Ministero dell'Interno

e

Confcommercio Imprese per l'Italia

e

Confesercenti

VISTO il Protocollo d'Intesa del 14 luglio 2009 in tema di video allarme antirapina – in scadenza il 31 ottobre 2013 – siglato tra il Ministro dell'Interno *pro tempore* ed i Presidenti di Confcommercio Imprese per l'Italia e Confesercenti;

CONSIDERATA la necessità di rinnovare il Protocollo d'Intesa del 14 luglio 2009 e di aggiornarne i contenuti;

ATTESO che permangono gravi fenomeni di criminalità perpetrati ai danni delle imprese del commercio, del turismo e dei servizi (di seguito denominati "operatori o imprese commerciali"), in particolare laddove viene movimentato denaro contante;

CONSTATATO anche il diffondersi ed il moltiplicarsi di fenomeni di microcriminalità che colpiscono in particolare le imprese del commercio;

CONSIDERATO che i reati predatori costituiscono un fenomeno di particolare allarme sociale e che la percezione del rischio e la domanda di sicurezza nel settore sono in aumento, con la conseguente necessità di potenziare le misure di prevenzione e contrasto già apprestate;

RAVVISATA la necessità di rafforzare il livello di protezione degli operatori del commercio secondo linee di indirizzo basate su una più stretta collaborazione tra Istituzioni pubbliche, Forze di polizia, associazioni di categoria ed operatori commerciali;

...preziosamente premesso, si conviene quanto segue:

Articolo 1
(Premesse)

Le Premesse fanno parte integrante del presente Protocollo.

Articolo 2
(Rinnovo e aggiornamento del Protocollo d'Intesa del 14 luglio 2009)

- 1 Il Ministero dell'Interno, Confcommercio Imprese per l'Italia e Confesercenti (di seguito "parti"), convengono che il Protocollo d'Intesa siglato il 14 luglio 2009, in tema di video allarme antirapina e menzionato in premessa, si intende rinnovato di tre anni e modificato ed integrato in base a quanto di seguito esposto.
- 2 Un nuovo disciplinare tecnico organizzativo sostituisce l'allegato al Protocollo del 2009, definisce ed aggiorna tra le parti le funzionalità del sistema di video allarme antirapina, la scelta delle imprese fornitrici, nonché l'adeguamento degli impianti e gli adempimenti relativi alle nuove attivazioni.
- 3 Le Prefetture favoriscono lo sviluppo operativo del medesimo sistema, sottoscrivendo con le articolazioni territoriali delle Confederazioni Protocolli conformi ai suddetti indirizzi.

Articolo 3
(Impegni delle parti)

- 1 Ai fini dell'attuazione del presente Protocollo Quadro, le parti assumono i seguenti impegni:
 - a) Confermano i vincoli derivanti dalla sottoscrizione del Protocollo d'Intesa del 14 luglio 2009;
 - b) il Ministero dell'Interno:
 - predispone idoneo materiale informativo e divulgativo concernente le buone prassi da seguire per ridurre il rischio di furti e rapine e per consentire agli operatori economici commerciali di fornire agli organi investigativi ogni utile informazione volta all'individuazione dei responsabili di tali reati;
 - assicura l'assistenza, nell'attività di formazione degli operatori economici, di personale delle Forze di polizia, la cui comprovata esperienza nel settore investigativo consenta agli operatori commerciali l'adozione di più efficaci misure di autoprotezione;
 - c) le Confederazioni parti del presente Protocollo:
 - curano la diffusione dei contenuti informativi, relativi al presente Protocollo, ai propri associati;

- promuovere la partecipazione degli imprenditori;
- sensibilizzare gli enti locali e le associazioni territoriali a stipulare analoghi accordi con il C.P.E.;
- promuovono la diffusione di sistemi di sorveglianza e di sicurezza, di nuove tecnologie e dell'utilizzo di strumenti di pagamento elettronico, quali mezzi per la limitazione dell'uso del contante, per il contrasto alla criminalità diffusa.

Infine, le parti si impegnano ad aggiornare di comune accordo i programmi congiunti di informazione e di formazione.

Articolo 4
(Durata)

Il presente Protocollo entra in vigore alla data di sottoscrizione dello stesso ed ha la durata di anni tre.

Verona, 12 novembre 2013

Ministero dell'Interno
Il Ministro *[Firma]*

Confcommercio Imprese per l'Italia
Il Delegato dal Presidente *[Firma]*

Confesercenti Nazionali
Il Segretario Generale *[Firma]* **CONFESERCENTI**



CASARTIGIANI
L'ARTIGIANATO FA BENE



Confederazione Nazionale
dell'Artigianato e della Piccola
e Media Impresa



PROTOCOLLO QUADRO
per la Legalità e la Sicurezza delle Imprese

tra
Il Ministero dell'Interno,
Casartigiani,
CNA Confederazione Nazionale dell'Artigianato e della Piccola e Media
Impresa
e
Confartigianato Imprese

ATTESO che sussistono gravi fenomeni di criminalità perpetrati ai danni delle imprese artigiane, e delle micro, piccole e medie imprese, in particolare laddove viene movimentato denaro contante;

CONSTATATO il diffondersi di fenomeni di microcriminalità che colpiscono le imprese sopra richiamate;

CONSIDERATO che i reati predatori costituiscono un fenomeno di particolare allarme sociale e che la percezione del rischio e la domanda di sicurezza nel settore sono in aumento, con la conseguente necessità di potenziare le misure di prevenzione e contrasto;

RAVVISATA la necessità di rafforzare il livello di protezione delle imprese artigiane, e delle micro, piccole e medie imprese, secondo linee di indirizzo basate su una più stretta collaborazione tra queste, le Associazioni di categoria, le Istituzioni pubbliche e le Forze dell'Ordine.

Tanto premesso, si conviene quanto segue:

Articolo 1
(Premesse)

Le Premesse fanno parte integrante del presente documento.

Articolo 2

(Iniziative per prevenire la criminalità)

1. Il Ministero dell'Interno, Casartigiani, CNA e Confartigianato Imprese (di seguito "parti"), convengono di stipulare il presente Protocollo Quadro, definito in base a quanto di seguito esposto e finalizzato a promuovere i sistemi di videosorveglianza e di sicurezza anche attraverso la predisposizione di un disciplinare tecnico in tema di videoallarme antirapina.
2. Il disciplinare tecnico organizzativo definirà le funzionalità del sistema di video allarme antirapina, i criteri per la scelta delle imprese fornitrici, nonché le modalità per l'adeguamento degli impianti eventualmente già esistenti e gli adempimenti relativi alle nuove attivazioni.
3. Le Prefetture favoriranno lo sviluppo operativo del sistema, sottoscrivendo con le articolazioni territoriali delle Confederazioni Protocolli conformi ai suddetti indirizzi.

Articolo 3

(Impegni delle parti)

1. Ai fini dell'attuazione del presente Protocollo Quadro, le parti assumono i seguenti impegni:

a) il Ministero dell'Interno:

- predispone idoneo materiale informativo e divulgativo concernente le buone prassi da seguire per ridurre il rischio di furti e rapine e per consentire agli operatori delle imprese di fornire agli organi investigativi ogni utile informazione volta all'individuazione dei responsabili di tali reati;
- assicura l'assistenza, nell'attività di formazione degli operatori economici, di personale delle Forze dell'Ordine, la cui comprovata esperienza nel settore investigativo consenta agli operatori delle imprese, l'adozione di più efficaci misure di autoprotezione;

b) le Confederazioni aderenti al presente Protocollo:

- curano la diffusione dei contenuti informativi ai propri associati;
- promuovono la partecipazione degli imprenditori alle attività di formazione finalizzate alla prevenzione della criminalità;
- sensibilizzano le rispettive articolazioni territoriali a stipulare analoghi accordi con le Prefetture.
- promuovono la diffusione di sistemi tecnologicamente avanzati di sorveglianza e di sicurezza nonché l'utilizzo di strumenti di pagamento

elettronico, quali mezzi per la limitazione dell'uso del contante, per il contrasto alla criminalità diffusa.

2. Le parti si impegnano ad individuare congiuntamente misure che possano incentivare le imprese ad adottare strumenti di protezione più efficaci.

3. Infine, le parti si impegnano ad aggiornare di comune accordo i programmi di informazione e di formazione.

Articolo 4
(Durata)

Il presente Protocollo entra in vigore alla data di sottoscrizione dello stesso ed ha la durata di anni tre.

Verona, 12 novembre 2013.

Il Ministero dell'Interno
Il Ministro On. Angelino Alfano

Casartigiani
Il Presidente Dott. Giacomo Basso

CNA Confederazione Nazionale
dell'Artigianato e della Piccola e Media
Impresa Il Vice Presidente Nazionale
Dott.ssa Alessia Zaninello

Confartigianato Imprese
Il Presidente Dott. Giorgio Merletti

ALL. 5



Protocollo Quadro per la legalità e la sicurezza delle Imprese (videoallarmi antirapina) tra Ministero dell'Interno, Confcommercio Imprese per l'Italia e Confesercenti sottoscritto in data 14 luglio 2009 e rinnovato in data 12 novembre 2013.

Protocollo Quadro per la legalità e la sicurezza delle Imprese (videoallarmi antirapina) tra Ministero dell'Interno, Casartigiani, CNA Confederazione Nazionale dell'Artigianato e della Piccola e Media Impresa e Confartigianato Imprese sottoscritto in data 12 novembre 2013.

DISCIPLINARE TECNICO

**PROGETTO PER UN SISTEMA DI ALLARME ANTIRAPINA
E ANTIAGGRESSIONE INTEGRATO PER LA TUTELA
DELL'INCOLUMITÀ FISICA DI SOGGETTI A RISCHIO,
CONTROLLATO CON TELECAMERE INTEGRATE
CON I SISTEMI PRESSO LE SALE/CENTRALI
OPERATIVE DELLE FORZE DI POLIZIA.**

Indice

REQUISITI TECNICI

Premessa	pag.	5
----------------	------	---

ARCHITETTURA

1. Caratteristiche del sistema audio/video e della registrazione presso i fruitori.....	“	8
2. Sicurezza delle registrazioni	“	10
3. Caratteristiche del sistema da installare presso le Sale/centrali operative delle forze di Polizia	“	11
4. ACCREDITAMENTO DELLA DITTA	“	13
Polizia di Stato	“	14
Arma dei Carabinieri	“	15
5. INSTALLAZIONE DEGLI APPARATI IN SALA/CENTRALE OPERATIVA		17
6. ATTIVAZIONE DEI SINGOLI SISTEMI DI VIDEO-ALLARME NEI SOFTWARE “S.C.T. E CC112NG”	“	19

ALLEGATI

All. 1 - Schema esplicativo collegamenti	“	23
All. 2 - Modello di concessione - rifiuto di NOT	“	25
All. 3 - Indirizzamenti Arma dei Carabinieri	“	27
All. 4 - Specifiche Tecniche WS Alerter	“	29
All. 5 - Modulo di Attivazione	“	33
All. 6 - Disciplinare Tecnico del 14 luglio 2009	“	35

REQUISITI TECNICI

PREMESSA

Il presente documento ha per oggetto il mantenimento e l'integrazione dei requisiti tecnici del sistema di allarme antirapina denominato Videoallarme le cui caratteristiche tecniche di base sono indicate nell'Allegato Disciplinare Tecnico "Requisiti Tecnici" del *Protocollo d'Intesa del 14 Luglio 2009* rinnovato il 15 novembre 2013. Attraverso il sistema di Videoallarme, si ottiene il controllo e la visione delle immagini provenienti dagli apparati di videoregistrazione e dalle annesse telecamere, installati presso gli esercizi commerciali, gli operatori economici e le Associazioni di strada (tutti definiti fruitori), attivabili tramite la volontà diretta del soggetto sottoposto ad azione criminale (come ad esempio con la semplice pressione sul pulsante di comando), in grado di collegarsi con la Piattaforma installata presso le Sale/Centrali Operative delle Forze dell'Ordine e di trasmettere le immagini in tempo reale e registrate.

Il Videoallarme è un sistema che prevede il collegamento dei fruitori alle Sale/Centrali Operative con collegamento telematico che nel caso dell'allarme antiaggressione passa, qualora presente, attraverso un Centro di Monitoraggio.

Il Centro di Monitoraggio, nell'ambito dell'architettura del Videoallarme riveste il ruolo di concentratore dei collegamenti audio e dati dei pre-allarmi provenienti dagli utenti, nella funzione di preventiva verifica della potenziale minaccia criminale, per il successivo instradamento, all'atto della conclamazione concreta del reato, verso le Sale/Centrali Ope-

rative della Polizia di Stato e dell'Arma dei Carabinieri, ad ognuna tramite un unico collegamento telematico.

Il Centro di Monitoraggio o gli Istituti di Vigilanza Privata, eventualmente incaricati dagli utenti/fruitori, al fine di integrare il sistema attraverso le tipiche attività riconducibili alla cd. "sicurezza secondaria", nei casi di "videoallarme per rapina" o di "violenza sulla persona" che richiedono l'esercizio di potestà autorizzative squisitamente di Polizia, avranno esclusivamente un ruolo di transito passivo del flusso telematico del Videoallarme Antirapina, senza rivestire compiti di filtraggio e trattazione dell'informazione e delle immagini. Le immagini della rapina o della violenza sulla persona non dovranno in ogni caso essere visualizzate dai censurati Istituti di Vigilanza Privata e, ai fini info investigativi, dovranno essere custodite opportunamente dall' esercente, secondo le prescrizioni del Garante per la Protezione dei dati e le norme sulla tutela dei Lavoratori.

L'implementazione del sistema è improntata sulla gestione intelligente degli eventi, quest'ultima da intendersi quale gestione delle informazioni conformemente ai requisiti dei sistemi per le Sale/Centrali Operative delle Forze di Polizia, riferite al Protocollo d'Intesa del 14 luglio del 2009, in modo tale da rendere minimo l'intervento dell'operatore, nella gestione degli allarmi.

L'Operatore di Sala/Centrale Operativa, potrà avvalersi anche delle tecnologie standard di geo-localizzazione e telecomunicazione (*apparati GPS/Wireless standard, Smartphone, etc.*), attivate dall'utente/fruitori in mobilità, sottoposto ad azione criminale di aggressione, con allarme filtrato e inoltrato dal Centro di Monitoraggio, all'atto della conclamazione del reato stesso, con funzioni integrate nei sistemi ed utili alla deterrenza ed alla repressione degli atti criminosi contro la persona.

L'operatore di Sala/Centrale Operativa, potrà avvalersi anche delle tecnologie standard di geo-localizzazione della refurtiva (apparati GPS/Wireless, occultati in oggetti civetta, quali gioielli, orologi, telefonini, mazzette di soldi, etc.), integrate nei sistemi ed utili alla deterrenza ed alla repressione degli atti criminosi contro la persona e il patrimonio della stessa, attivabili contestualmente alla generazione volontaria del Videoallarme ed all'asporto forzato dei valori rubati.

Le specifiche tecniche proposte nel presente documento, sono da intendersi come requisiti minimi, nel senso che si potranno implementare soluzioni tecnologiche migliorative (come ad esempio trasmissione dell'audio in tempo reale alla Sala/Centrali Operative delle Forze dell'Ordine, formato immagine di dimensioni superiori, etc.), purché tali da garantire gli obiettivi prefissati in termini di prestazioni, sicurezza e gestibilità nell'ottica anche dell'ottimizzazione dei costi operativi delle Forze di Polizia.

Per quanto non espressamente previsto dal presente disciplinare, si ritengono valide le disposizioni del protocollo d'intesa sottoscritto il 14 luglio 2009.

INTEGRAZIONE CON I SISTEMI ESISTENTI PRESSO LE SALE/CENTRALI OPERATIVE

Necessità vincolante in fase di progettazione del sistema in argomento è 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 allarmati "live", provenienti dalle telecamere installate presso gli utenti/ fruitori, per il tramite dell'allarme generato dal Centro di Monitoraggio, ovvero direttamente, per la "conte-

stualizzazione” degli stessi all’interno dei rispettivi applicativi (nuovo SCT Sistema per il Controllo del Territorio e CC112NG) e la relativa gestione “intelligente”; conformemente alle prescrizioni elaborate dal Garante per la protezione dei dati personali in materia di video sorveglianza.

ARCHITETTURA

L’architettura di sistema è descritta nel documento allegato (*anx. 1. - schema esplicativo collegamenti*).

Si riportano di seguito i vari aspetti caratterizzanti il sistema.

1. CARATTERISTICHE DEL SISTEMA AUDIO/VIDEO E DELLA REGISTRAZIONE PRESSO I FRUITORI

Le caratteristiche del sistema Audio/Video e della registrazione della immagini dei sistemi installati presso i fruitori sono le seguenti:

- 1) Alta risoluzione, in ogni caso non inferiore ad un immagine VGA pari a 307.200 pixel (*640x480 pixel*). Eventualmente sarà possibile considerare l’impiego di complessi di ripresa con definizione dell’ordine del megapixel, purché aderenti al profilo di missione richiesto e alle performance derivanti da specifiche tecniche che costituiscono vincolo di comunicazione.
- 2) Supporto della registrazione audio (*WAVE compatibile almeno a 16 bit*).
- 3) Rappresentazione della immagini a colori e in modalità day&night.
- 4) Visualizzazione fino al limite di una rappresentazione di tipo “full motion” (*visione diretta di ogni particolare che prende parte all’evento criminoso in tempo reale*).

- 5) Conservazione dei filmati (*audio+video*) per almeno 15 giorni h24 (*conformemente a quanto previsto dal paragrafo 3.4 del Provvedimento dell'8 aprile 2010 del Garante per la protezione dei dati personali*), con risoluzione almeno VGA pari a 25 fps e sensibilità microfonica pari a -54 db.
- 6) Informazioni di data/ora relativi al filmato ripreso.
- 7) 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.
- 8) Algoritmo di compressione compreso nelle famiglie MPEGx, MJPEG, H.264, WMV.
- 9) Compatibilità del Software con sistemi operativi utilizzati presso le Sale/Centrali Operative.
- 10) Nel caso in cui l'operatore usufruisca (o intenda farlo in un secondo momento) anche di altri servizi di sorveglianza - autonomamente attivati sulla base di specifici contratti con il medesimo Istituto di Vigilanza Privata, aventi anche le connessioni con il Centro di Monitoraggio nell'ambito della rete di cui al presente disciplinare - il sistema dovrà supportare una duplice modalità di invio dell'allarme. In tale ipotesi dovranno essere installati due tasti di allarme ai quali corrispondono due differenti funzionalità:
 - a) Allarme antirapina: il flusso di videoallarme generato, viene veicolato attraverso il Centro di Monitoraggio sotto forma di riscontro dell'allarme e di gestione dei dati dell'utente, ma viene direttamente transitato (senza alcun filtro da parte del personale addetto

alla gestione dei pre-allarmi e da parte dei cennati Istituti di Vigilanza Privata) alla Sala/Centrale Operativa, allertando le competenti Forze di Polizia;

b) Allarme generico (per altre situazioni di diversa natura di cui al relativo contratto stipulato con gli Istituti di Vigilanza Privata o con Centrali di Controllo (ad es. Istituti Bancari): il flusso di videoallarme è veicolato solo al Centro di Monitoraggio per gli interventi del caso nel trattamento del pre-allarme e, solo qualora si verifichi una situazione di emergenza/soccorso, devono essere coinvolte le competenti Forze di Polizia, con la trasmissione del flusso video.

Il flusso dati e le linee trasmissive nelle suddette ipotesi, dovranno sempre essere improntate alle specifiche tecniche riportate nel presente disciplinare.

- 11) Nel caso in cui l' esercente/fruitore usufruisca (o intenda farlo in un secondo momento) anche di altri servizi di sicurezza - già attivati sulla base di specifiche autorizzazioni da parte delle Forze di Polizia - potrà, previa autorizzazione di quest'ultime, richiederne l'integrazione delle funzioni di Videoallarme

2. SICUREZZA DELLE REGISTRAZIONI

Il supporto di memoria di massa, utilizzato per la registrazione e conservazione dei filmati per le finalità d'impiego da parte dell'Autorità Giudiziaria, dovrà obbligatoriamente essere:

- 1) Asportabile da parte degli Organi di Polizia Giudiziaria e conseguentemente sostituibile con analogo apparato, a carico dell'Associazione di Categoria ovvero dell' esercente, per garantire a quest'ultimo la continuità del servizio di Videoallarme;

- 2) Leggibile attraverso un collegamento rapido ad un generico personal computer, dotato del necessario software di lettura e “assolutamente immodificabile nei contenuti” (le registrazioni devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste)
- 3) Monitorabile, in locale o da remoto, attraverso la registrazione in un file di log di tutte le variazioni di stato del funzionamento dello stesso supporto (tale file di log dovrà essere reso disponibile agli Organi di Polizia Giudiziaria, contestualmente al sequestro del supporto);
- 4) Custodito con efficaci misure di protezione (es. dispositivi con doppia chiave o con apertura ritardata del vano di alloggiamento del videoregistratore).

3. CARATTERISTICHE DEL SISTEMA DA INSTALLARE PRESSO LE SALE/ CENTRALI OPERATIVE DELLE FORZE DI POLIZIA

Trasferimento delle immagini su protocollo IP (IP ver. 04 compatibile):

- 1) I segnali videoallarmati verso le Sale/Centrali Operative delle Forze di Polizia devono essere convogliati attraverso un unico collegamento fisico (eventualmente per il tramite anche di un Centro di Monitoraggio), obbligatoriamente a “filo” (*la “policy di sicurezza” adottata dalle strutture militari, al momento, vieta la connessione telematica da/verso l’esterno su reti wireless*), ovvero un unico punto di accesso al sistema presente su ciascuna Sala/Centrale Operativa delle Forze di Polizia: uno per la Sala Operativa della Questura e uno per la Cen-

trale Operativa del Comando Provinciale dell'Arma dei Carabinieri. Tale collegamento, punto nevralgico del sistema, dovrà garantire l'efficienza del servizio che si intende offrire all' esercente.

- 2) I segnali videoallarmati dovranno indistintamente essere veicolati verso entrambe le Forze di Polizia presenti, che gestiranno l'intervento secondo le ordinarie procedure operative in atto.
- 3) Il Media Server di cui al paragrafo 5 deve avviare la registrazione del video in ingresso immediatamente, indipendentemente dalla successiva presa in carico da parte dell'operatore di Sala o Centrale operativa. Il Media Server deve poter conservare in memoria, per almeno 15 giorni consecutivi, le immagini allarmate (audio+video) pervenute
- 4) Le immagini che verranno trasmesse alla postazione di Sala/Centrale Operativa delle Forze di Polizia dovranno avere le seguenti caratteristiche minime:
 - a) Risoluzione con un formato DCIF (528x384 pixel);
 - b) 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 della famiglia MPEG2, H.264, WMV.;
 - c) Frame rate non inferiore a 15 fps;
 - d) Standard Codifica Audio G.711.
- 5) La capacità relativa alla banda passante va calcolata riguardo alle necessità di accesso dei sistemi periferici, tenendo conto che il massimo ritardo consentito per tutte le trasmissioni, e per ogni telecamera facente parte di un singolo sistema periferico, non sia superiore a 1500 millisecondi espresso come tempo di latenza (*parametro le-*

gato alla capacità della banda dell'infrastruttura di telecomunicazioni e migliorabile in funzione della stessa)

- 6) Deve essere possibile la visualizzazione su mappa cartografica o ibrida della posizione di un allarme completo delle Coordinate geografiche (LAT, LON) con la relativa visualizzazione delle immagini alle Sale/Centrali Operative di entrambi le Forze di Polizia.
- 7) Deve essere garantita la completezza delle informazioni dell'utente/fruttore corredate anche di campi note e di fotografia nel caso di antiaggressione.

Deve essere garantita la trasmissione contemporanea di videoallarmi provenienti da diversi fruitori. Il collegamento sarà di tipo a banda larga, riservato e protetto con sistemi firewall.

4. ACCREDITAMENTO DELLA DITTA

4.1 NULLA OSTA TECNICO

Per poter procedere all'installazione del proprio sistema, ciascuna ditta deve ottenere un Nulla Osta Tecnico di conformità al Protocollo d'Intesa 2013 (*nel seguito: N.O.T. 2013*) attraverso due fasi distinte e consequenziali:

1. Verifica del sistema a livello centrale, per ciascuna Forza di polizia, da effettuarsi presso una sede individuata da ciascuna Forza
2. Verifica del sistema a livello periferico per il rilascio del Nulla Osta Tecnico a cura della competente articolazione regionale.

Ciò premesso, le novità introdotte dal Protocollo d'Intesa del 2013 impongono, per le ditte già in possesso di un Nulla Osta Tecnico di conformità al Protocollo d'Intesa 2009 (*nel seguito: N.O.T. 2009*), l'ottenimento di un N.O.T. 2013 che certifichi l'avvenuto adeguamento dei sistemi al

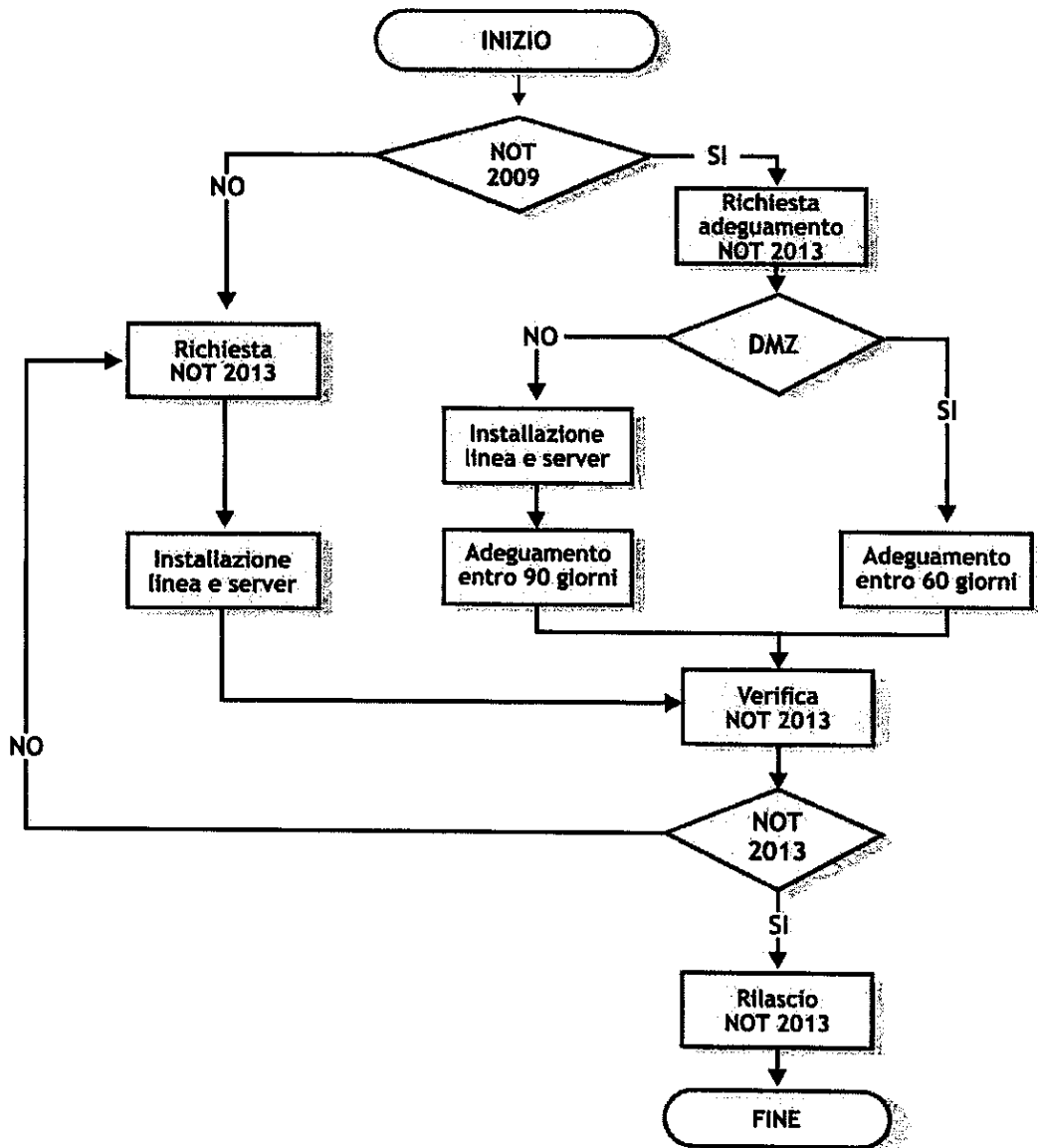
presente disciplinare. Le ditte non in possesso del ‘vecchio’ N.O.T. devono invece avviare le procedure per l’acquisizione del N.O.T. 2013.

Si riporta, di seguito l’iter da seguire per l’ottenimento di un N.O.T. 2013, distinto per Arma dei Carabinieri e Polizia di Stato nei seguenti tre casi:

- A. La ditta è in possesso del N.O.T. 2009 ed ha apparati installati nella DMZ della Questura o del Comando Provinciale
- B. La ditta è in possesso del N.O.T. 2009 ma non ha apparati installati in DMZ della Questura o del Comando Provinciale
- C. La ditta non è in possesso del N.O.T. 2009

Polizia di Stato

Come si può desumere dal diagramma, nei primi due casi la ditta deve avanzare, per ogni sede periferica, richiesta di adeguamento del N.O.T. 2009 al N.O.T. 2013 e, secondo tempistiche differenti, provvedere a dare comunicazione via posta elettronica certificata alle Forze di polizia competenti circa l’esito positivo dei propri test di verifica; qualora ciò non avvenga, la ditta è tenuta ad avviare l’intero iter di acquisizione del N.O.T. 2013. Ricevuta la comunicazione di test positivo, l’Amministrazione provvederà a verificare l’avvenuto adeguamento rilasciando un documento **“Nulla Osta Tecnico di Avvenuto Adeguamento al Protocollo d’Intesa del 2013”**, che permetterà il procedimento di adeguamento del parco tecnologico esistente. Tale adeguamento è applicabile ai soli Sistemi di Videollarme Antirapina presenti presso le Sale/Centrali Operative delle Forze di Polizia, installati prima della data di sottoscrizione del presente documento.



Arma dei Carabinieri

La ditta deve avanzare al Comando Generale dell'Arma dei Carabinieri, Ufficio Sistemi Telematici, richiesta di ottenimento del N.O.T. 2013:

- nei casi A e B (la ditta ha già ricevuto un NOT 2009) l'esito positivo dei test di integrazione con il nuovo software CC112NG determina automaticamente il rilascio del N.O.T. 2013 (a cura del predetto Uf-

ficio Sistemi Telematici). La ditta, 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 NOT 2013;

- nel caso C (*la ditta non ha un NOT 2009*), successivamente all'esito positivo del test di integrazione con il software **CC112** effettuato presso il Comando Generale dell'Arma, la ditta dovrà presentare alle articolazioni tecniche Legionali dell'Arma gli apparati che intende installare localmente, al fine di ottenere il NOT 2013.

4.2 MODALITÀ DI COMUNICAZIONE CON LE ARTICOLAZIONI TECNICHE PERIFERICHE DELLA POLIZIA DI STATO E DELL'ARMA DEI CARABINIERI

Le articolazioni tecniche periferiche della Polizia di Stato e dell'Arma dei Carabinieri (quando previsto):

- ricevono, con lettera formale, da parte della ditta proponente 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 (NOT) al progetto, ovvero rigettando lo stesso per non conformità (modello di risposta in anx.2-modello di concessione-rifiuto di NOT).

4.3 MANDATO

Una volta in possesso del NOT:

- la ditta e le "associazioni di categoria/ singoli esercenti non associati", attivano le loro procedure interne per conferire alla ditta stessa l'incarico ad operare (mandato);

- la ditta che abbia ricevuto il NOT da parte delle articolazioni periferiche delle FF.PP. ed il mandato da parte di un'associazione di categoria/esercente non associato è autorizzata ad effettuare le installazioni presso le Sale/Centrali Operative (purché in regola con le disposizioni per lo svolgimento di lavori non classificati in aree riservate).

5. INSTALLAZIONE DEGLI APPARATI IN SALA/CENTRALE OPERATIVA

La ditta accreditata installerà il proprio sistema presso la Sala/Centrale Operativa della competente Questura/Comando Provinciale, provvedendo ad interfacciarsi con i rispettivi software in dotazione alle Forze di polizia (Nuovo SCT per la P.d.S. e "CC112NG" per l'Arma dei Carabinieri).

Eventuali casistiche particolari dovranno essere rimesse alle valutazioni delle singole Amministrazioni Centrali.

5.1 ATTIVITÀ

La ditta, in accordo a quanto riportato nell'allegato anx.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 Questura/Comando Provinciale interessata, 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 disponi-

bile in Sala/Centrale Operativa (indicato nello schema come “DMZ Switch”), utilizzando un IP appartenente al range assegnato ad ogni Questura/C.do Provinciale (‘anx.3 - indirizzamenti Arma CC’ per l’Arma dei Carabinieri; per la Polizia di Stato si fa riserva di fornire analogo documento anx.3bis) - 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 FF.PP. (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 FF.PP.”.

Gli oneri di installazione e manutenzione degli apparati ricadono sulla società accreditata per l’installazione del proprio sistema di video allarme.

5.2 INTEGRAZIONE CON I SOFTWARE “NUOVO SCT E CC112NG”

I “Media Server - video allarme anti rapina” per Polizia di Stato/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. anx.3 e anx.3bis) esclusivamente una notifica (attestante l’arrivo di un flusso video allarmato), mediante invocazione del Web Service c.d. “alerter” (anx.4 Specifiche Tecniche WS Alerter), il quale attiverà un meccanismo che permetterà ai server delle FF.PP. 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 delle FF.PP. contatteranno i rispettivi organi tecnici per l’ausilio del caso.

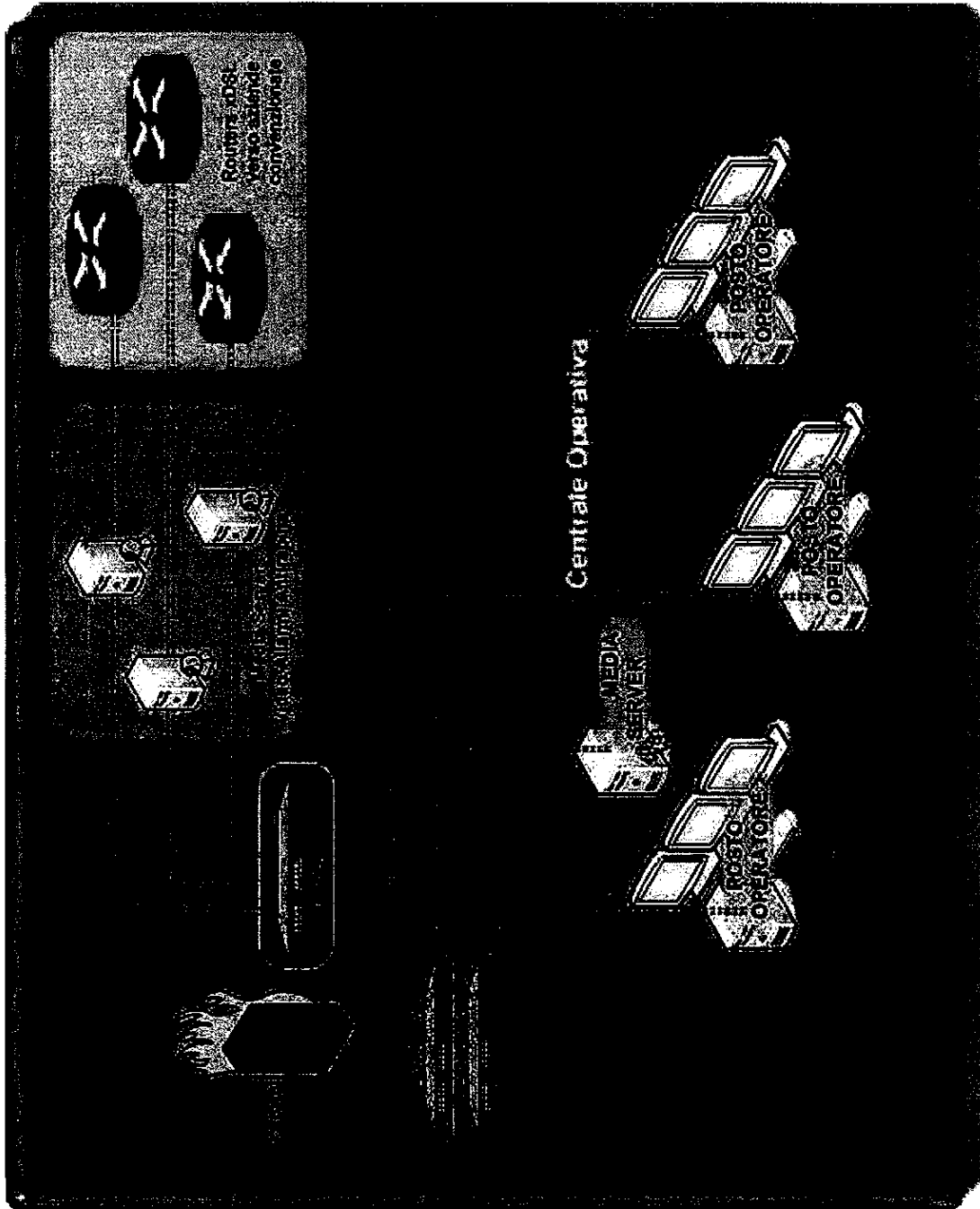
6. ATTIVAZIONE DEI SINGOLI SISTEMI DI VIDEO-ALLARME NEI SOFTWARE “S.C.T.” E “CC112NG”

“L’associazione di categoria / singolo esercente non associato” o, in alternativa, la ditta accreditata, chiede l’attivazione del sistema alla Questura o al Comando dei Carabinieri territorialmente competente, mediante la compilazione del modulo di attivazione in anx.5 - modulo di attivazione che conterrà i dati identificativi dell’esercizio;

La Questura o il Comando dei Carabinieri territorialmente competente che riceve il predetto a mezzo posta elettronica certificata il modulo di attivazione:

- a) genera, utilizzando i sistemi informatici di rispettiva competenza, un “codice univoco” secondo la seguente regola di “naming”: codice di 12 cifre alfanumeriche (le prime 2 saranno obbligatoriamente “PS” per la Polizia di Stato e “CC” per i Carabinieri);
- b) restituisce, a mezzo posta elettronica certificata, il modello di richiesta “accettato” e completato con il codice univoco precedentemente generato.

Allegato 1



Allegato 2 - Modello di concessione - rifiuto di NOT

INTESTAZIONE

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 la Sala Operativa di questa Questura/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 "Nuovo SCT"/ "CC112" nella versione corrente alla data delle attività inoltrando al "Video Server" (Nuovo SCT/CC112) esclusivamente i flussi di videostreaming allarmati in formato compatibile così 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 Questura/C.O. al quale dovrà essere consegnato il **modulo di attivazione** allegato.

Nota: il software "Nuovo SCT" e "CC112" sono progressivamente in via di evoluzione; nel momento in cui una delle Questure/C.O. ove è stato attestato il sistema di video allarme anti rapina sarà soggetta a centralizzazione (o comunque ad attività di modifica), la ditta sarà contattata dall'organo tecnico della Questura/Arma competente a definire i dettagli tecnici necessari a continuare a garantire l'arrivo dei flussi di video-allarme al software di centrale anche nelle nuove versioni.

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

Allegato 3 - Indirizzamenti Arma dei Carabinieri

Numero Sede	Comando	Indirizzo	SUBNET SERVER DI VIDEO ALLARME ANTI-RAPINA	GATEWAY	IP MEDIA SEVER CC 112
1	Agrigento	P.zza Aldo Moro 2	192.168.1.128 /26	192.168.1.129	192.168.1.13
2	Alessandria	P.zza Vittorio Veneto 2	192.168.2.128 /26	192.168.2.129	192.168.2.13
3	Ancona	Via Della Montagnola 81/a	192.168.3.128 /26	192.168.3.129	192.168.3.13
4	Aosta	P.zza Roicas 1	192.168.4.128 /26	192.168.4.129	192.168.4.13
5	Arezzo	Via Gen. Carlo Alberto Dalla Chiesa 12	192.168.5.128 /26	192.168.5.129	192.168.5.13
6	Ascoli Piceno	Via Circonvallazione 10	192.168.6.128 /26	192.168.6.129	192.168.6.13
7	Asti	Via Zangrandi 6	192.168.7.128 /26	192.168.7.129	192.168.7.13
8	Avellino	Via Roma 104	192.168.8.128 /26	192.168.8.129	192.168.8.13
9	Bari	Lungomare N. Sauro 43	192.168.9.128 /26	192.168.9.129	192.168.9.13
10	Belluno	Viale Europa 9	192.168.10.128 /26	192.168.10.129	192.168.10.13
11	Benevento	Via Neomarina 9	192.168.11.128 /26	192.168.11.129	192.168.11.13
12	Bergamo	Circonvallazione Delle Valli 31	192.168.12.128 /26	192.168.12.129	192.168.12.13
13	Biella	Via F.lli Rosselli 88/B/5	192.168.13.128 /26	192.168.13.129	192.168.13.13
14	Bologna	Via Dei Borsaglieri 3	192.168.14.128 /26	192.168.14.129	192.168.14.13
15	Bozzano	Via Dante 30	192.168.15.128 /26	192.168.15.129	192.168.15.13
16	Brescia	P.zza Tebaldo Brusato 19	192.168.16.128 /26	192.168.16.129	192.168.16.13
17	Brindisi	Via Bastoni S. Giorgio 3	192.168.17.128 /26	192.168.17.129	192.168.17.13
18	Cagliari	Via Nuoro 9	192.168.18.128 /26	192.168.18.129	192.168.18.13
19	Caltanissetta	Via Leone XIII 97	192.168.19.128 /26	192.168.19.129	192.168.19.13
20	Campobasso	Corso Mazzini 97	192.168.20.128 /26	192.168.20.129	192.168.20.13
21	Caserta	Via Leviano Cap. Luigi 13	192.168.21.128 /26	192.168.21.129	192.168.21.13
22	Castello di Cisterna (Gruppo)	Via Cosimo Miccoli 8	192.168.22.128 /26	192.168.22.129	192.168.22.13
23	Catania	P.zza Verga 8	192.168.23.128 /26	192.168.23.129	192.168.23.13
24	Catanzaro	Piazzale Trieste 1	192.168.24.128 /26	192.168.24.129	192.168.24.13
25	Chieti	Via Amintore 102	192.168.25.128 /26	192.168.25.129	192.168.25.13
26	Como	Via Borgovico 171	192.168.26.128 /26	192.168.26.129	192.168.26.13
27	Cosenza	Viale Bisemio SNC	192.168.27.128 /26	192.168.27.129	192.168.27.13
28	Cremona	Viale Trento Trieste 58	192.168.28.128 /26	192.168.28.129	192.168.28.13
29	Crotone	Via IV Novembre 4	192.168.29.128 /26	192.168.29.129	192.168.29.13
30	Cuneo	C.so Soleri 7	192.168.30.128 /26	192.168.30.129	192.168.30.13
31	Enna	Via Montesalvo 83	192.168.31.128 /26	192.168.31.129	192.168.31.13
32	Ferrara	Via Del Campo 40	192.168.32.128 /26	192.168.32.129	192.168.32.13
33	Firenze	Borgo Ognissanti 48	192.168.33.128 /26	192.168.33.129	192.168.33.13
34	Foggia	Via Guglielmi 4	192.168.34.128 /26	192.168.34.129	192.168.34.13
35	Forlì	Corso Mazzini 78	192.168.35.128 /26	192.168.35.129	192.168.35.13
36	Frascati (Gruppo)	Viale V. Veneto 40	192.168.36.128 /26	192.168.36.129	192.168.36.13
37	Frosinone	Viale Mazzini 131	192.168.37.128 /26	192.168.37.129	192.168.37.13
38	Genova	Via Gobetti 5	192.168.38.128 /26	192.168.38.129	192.168.38.13
39	Gorizia	C.so Verdi 17	192.168.39.128 /26	192.168.39.129	192.168.39.13
40	Grosseto	Via Ferrucci 32	192.168.40.128 /26	192.168.40.129	192.168.40.13
41	Imperia	V.le Matteotti 46	192.168.41.128 /26	192.168.41.129	192.168.41.13
42	Isernia	Viale 3 Marzo 1970 2	192.168.42.128 /26	192.168.42.129	192.168.42.13
43	La Spezia	Via C.A. Dalla Chiesa 1	192.168.43.128 /26	192.168.43.129	192.168.43.13
44	L'Aquila	Via Beato Celsidio 5	192.168.44.128 /26	192.168.44.129	192.168.44.13
45	Latina	Largo Caduti di Nassirya 1	192.168.45.128 /26	192.168.45.129	192.168.45.13
46	Lecce	Via Lupiae 8	192.168.46.128 /26	192.168.46.129	192.168.46.13
47	Lecco	Corso Carlo Alberto 62	192.168.47.128 /26	192.168.47.129	192.168.47.13
48	Livorno	Via Fabbicotti 1	192.168.48.128 /26	192.168.48.129	192.168.48.13
49	Lodi	Piazza Caduti di Nassirya 3	192.168.49.128 /26	192.168.49.129	192.168.49.13
50	Lucca	Corfite degli Svizzeri 4	192.168.50.128 /26	192.168.50.129	192.168.50.13
51	Macerata	Via XXI Settembre 2	192.168.51.128 /26	192.168.51.129	192.168.51.13
52	Mantova	Via Chival 29	192.168.52.128 /26	192.168.52.129	192.168.52.13
53	Massa Carrara	Via Angelini 14	192.168.53.128 /26	192.168.53.129	192.168.53.13
54	Matera	Via Dante 17	192.168.54.128 /26	192.168.54.129	192.168.54.13
55	Messina	Via Monsignor D'Amico 13	192.168.55.128 /26	192.168.55.129	192.168.55.13

Allegato 3 - Indirizzamenti Arma dei Carabinieri

Numero Sede	Comando	Indirizzo	SUBNET VIDEO ALLARME ANTI-RAPINA	SERVER DI GATEWAY	IP MEDIA SEVER CC112
56	Milano	Via Moscova 21	192.168.56.128/26	192.168.56.129	192.168.56.13
57	Modena	Via Pio delle Mirandole 30	192.168.57.128/26	192.168.57.129	192.168.57.13
58	Monreale (Gruppo)	Via Blegio Giordano 1	192.168.58.128/26	192.168.58.129	192.168.58.13
59	Monza (Gruppo)	Via Voltumo 35	192.168.59.128/26	192.168.59.129	192.168.59.13
60	Napoli	Via Morgantini 4	192.168.60.128/26	192.168.60.129	192.168.60.13
61	Novara	Via Balduino Lamerzora 8	192.168.61.128/26	192.168.61.129	192.168.61.13
62	Nuoro	Via S. Onofrio 3	192.168.62.128/26	192.168.62.129	192.168.62.13
63	Oristano	Via F. Loffredo 10/A	192.168.63.128/26	192.168.63.129	192.168.63.13
64	Ostia (Gruppo)	Via A. Zambrini 48	192.168.64.128/26	192.168.64.129	192.168.64.13
65	Padova	Via Rispondo 4	192.168.65.128/26	192.168.65.129	192.168.65.13
66	Palermo	Via Muro di San Vito	192.168.66.128/26	192.168.66.129	192.168.66.13
67	Parma	Strada Fondere 10	192.168.67.128/26	192.168.67.129	192.168.67.13
68	Pavia	Via D. Secchi 31	192.168.68.128/26	192.168.68.129	192.168.68.13
69	Perugia	Via Ruggia 9	192.168.69.128/26	192.168.69.129	192.168.69.13
70	Pesaro	Via Salvo D'Acquisto 7	192.168.70.128/26	192.168.70.129	192.168.70.13
71	Pescara	Via G. D'Annunzio 149	192.168.71.128/26	192.168.71.129	192.168.71.13
72	Piacenza	Via Beveroni 48	192.168.72.128/26	192.168.72.129	192.168.72.13
73	Pisa	Via Guido De Pisa 1	192.168.73.128/26	192.168.73.129	192.168.73.13
74	Pistoia	Viale Italia 78	192.168.74.128/26	192.168.74.129	192.168.74.13
75	Pordenone	Via dei Carabinieri 2	192.168.75.128/26	192.168.75.129	192.168.75.13
76	Potenza	Via Pretoria 300	192.168.76.128/26	192.168.76.129	192.168.76.13
77	Prato	Via Pablo Picasso 30	192.168.77.128/26	192.168.77.129	192.168.77.13
78	Ragusa	Piazza Caduti di Nassirya 3	192.168.78.128/26	192.168.78.129	192.168.78.13
79	Ravenna	Viale Pertini 11	192.168.79.128/26	192.168.79.129	192.168.79.13
80	Reggio Calabria	Via Aschenetz 3	192.168.80.128/26	192.168.80.129	192.168.80.13
81	Reggio Emilia	C.so Cairoli 8	192.168.81.128/26	192.168.81.129	192.168.81.13
82	Rieti	Via Giulio de Julis 2	192.168.82.128/26	192.168.82.129	192.168.82.13
83	Rimini	Viale Carlo Alberto Dalla Chiesa 15	192.168.83.128/26	192.168.83.129	192.168.83.13
84	Roma	Piazza S. Lorenzo In Lucina 8	192.168.84.128/26	192.168.84.129	192.168.84.13
85	Rovigo	Via Silvestri 28	192.168.85.128/26	192.168.85.129	192.168.85.13
86	Salerno	Via R. Mauri 89	192.168.86.128/26	192.168.86.129	192.168.86.13
87	Sassari	Via Rockefeller 52	192.168.87.128/26	192.168.87.129	192.168.87.13
88	Savona	C.so Ricci 30	192.168.88.128/26	192.168.88.129	192.168.88.13
89	Siena	Largo Salvo D'Acquisto 1	192.168.89.128/26	192.168.89.129	192.168.89.13
90	Siracusa	Via Tica 149/m	192.168.90.128/26	192.168.90.129	192.168.90.13
91	Sondrio	Largo Serbelli 5	192.168.91.128/26	192.168.91.129	192.168.91.13
92	Taranto	Viale Virgilio 25	192.168.92.128/26	192.168.92.129	192.168.92.13
93	Teramo	Piazza Del Carmine 3	192.168.93.128/26	192.168.93.129	192.168.93.13
94	Terni	Via Giuseppe Lombardo Radice 5	192.168.94.128/26	192.168.94.129	192.168.94.13
95	Torino	Via Valfra 5/bis	192.168.95.128/26	192.168.95.129	192.168.95.13
96	Trapani	Via Orlandini 27	192.168.96.128/26	192.168.96.129	192.168.96.13
97	Trento	Via Barbecovi 24	192.168.97.128/26	192.168.97.129	192.168.97.13
98	Treviso	Via Comerota 24	192.168.98.128/26	192.168.98.129	192.168.98.13
99	Trieste	Via Dell'Isola 54	192.168.99.128/26	192.168.99.129	192.168.99.13
100	Udine	Viale Trieste 28	192.168.100.128/26	192.168.100.129	192.168.100.13
101	Varese	Via Aurelio SAPI 55	192.168.101.128/26	192.168.101.129	192.168.101.13
102	Venezia	Castello 4893/a	192.168.102.128/26	192.168.102.129	192.168.102.13
103	Verbania	Via Gen. Carlo Alberto Dalla Chiesa 1	192.168.103.128/26	192.168.103.129	192.168.103.13
104	Vercelli	Via Gioberti 57	192.168.104.128/26	192.168.104.129	192.168.104.13
105	Verona	Via S. D'Acquisto 6	192.168.105.128/26	192.168.105.129	192.168.105.13
106	Vibo Valentia	Via Gen. Polliciano 19	192.168.106.128/26	192.168.106.129	192.168.106.13
107	Vicenza	Via Muggia 2	192.168.107.128/26	192.168.107.129	192.168.107.13
108	Viterbo	Via S. Camillo De Lellis 20	192.168.108.128/26	192.168.108.129	192.168.108.13
109	Torre Annunziata	Piazza Enrico De Nicola 12	192.168.109.128/26	192.168.109.129	192.168.109.13

Allegato 4 - Specifiche Tecniche WS Alerter

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 Sale e Centrali Operative della Polizia di Stato e dell’Arma dei Carabinieri l’arrivo di un flusso video allarmato.

In seguito a tale notifica, i sistemi delle singole Forze di polizia effettueranno una chiamata al video server esterno (posizionato in DMZ) fornito dalle confederazioni (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 al server locale installato nella rete Intranet della Sala/Centrale operativa un comando di “attivazione della registrazione” notificando, contestualmente, l’arrivo di una segnalazione di allarme alla Sala/Centrale Operativa.

Grazie a questa nuova modalità non si dovrà effettuare un “push” verso il server della Sala/Centrale Operativa, ma si attiverà un meccanismo per il quale sarà quest’ultimo server 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 standard di compressione utilizzabili, quindi, potranno essere quelli di seguito descritti:

- Windows Media Video;
- MPEG2;
- H.264 (MPEG-4 Parte 10/AVC).

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:

Id	Codice Univoco identificativo del sistema di video allarme	Parametri sempre obbligatori. Nel caso in cui un parametro resti non popolato, si intende che si sta inviando solo un allarme e la relativa posizione (variable nel tempo) senza coinvolgere un flusso video.
Timestamp	Data Ora di attivazione dell'allarme (timestamp dal 1° gennaio 1970).	
Titolare	Informazioni sull'esercente	
Ubicazione	Indirizzo dell'esercente	
Telefono	Telefono di riferimento dell'esercente	
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".	Parametri da popolare obbligatoriamente se si intende trasferire anche un flusso di video streaming, altrimenti restano vuoti:
Protocol	Protocollo utilizzato per il flusso video (MMS, RTSP, RTMP)	
Port	Porta del sorgente	
ID Telecamera	Identificativo della telecamera, per ogni telecamera	
Tipo Telecamera	Tipologia della telecamera (fissa, mobile, dome), per ogni telecamera	
Uri	Indirizzo per esteso dove andare a prelevare la fonte video live (ad es.: <u>mms://172.16.100.10/videoAlert</u>), per ogni telecamera	
Parameters	Ulteriori parametri	
CallbackUri	Eventuale Uri del sistema mittente da lanciare una volta terminato il flusso Video per notificare, ad es., l'esito (positivo o negativo) dell'acquisizione del filmato.	
Foto	Foto del mittente del servizio da trasmettere nello scenario di acquisizione	
Note	Campo note per la comunicazione di informazioni utili	

NOTA:

I campi relativi a 'Titolare', 'Ubicazione', 'Telefono' permettono al Nuovo SCT di popolare la scheda contatto senza la necessità di gestire, localmente, un DB con l'anagrafica degli esercenti.

Si fa riserva di trasmettere il WSDL per interfacciarsi con il sistema "Alerter".

3. SUPPORTO DI METODI AGGIUNTIVI

Si richiede inoltre, da parte del Media Server - Video allarme anti rapina, il supporto dei metodi di seguito elencati e descritti nel dettaglio, al fine di permettere, all'operatore di Sala/Centrale Operativa, specifiche azioni:

- 0. TVCC.requestVideo, per richiedere il playback del video
- 1. TVCC.exportVideo, per richiedere l'export del video
- 2. TVCC.requestPtz, per richiedere il brandeggio di una specifica video camera

Di seguito, si indica con TVCC il Media Server video allarme anti rapina.

Metodo 'TVCC.requestVideo'

Descrizione	Richiede l'acquisizione dei flussi video.			
	Obb.	Nome	Tipo	Descrizione
Campi Ingresso	*	<u>idCamera</u>	string	Identificativo telecamera cui si richiede il live
	*	<u>StartDateTime</u>	string	Data ora inizio video in millisecondi (xsd:dateTime YYYY-MM-DTHH:mm:ss SSS)
	*	<u>EndDateTime</u>	string	Data ora fine video in millisecondi (xsd:dateTime YYYY-MM-DTHH:mm:ss SSS)
	*	<u>User</u>	<Credential>	Identificativo del sistema ICT.
	Obb.	Nome	Tipo	Descrizione
Campi in Uscita	*	<u>Result</u>	string	URL di accesso al registrato

Tabella 1 - Integrazione TVCC: il metodo TVCC.requestVideo

Metodo 'TVCC.exportVideo'

Descrizione	Richiede l'acquisizione dei flussi video.			
	Obb.	Nome	Tipo	Descrizione
Campi Ingresso	*	<u>idCamera</u>	string	Identificativo telecamera cui si richiede il live
	*	<u>StartDateTime</u>	string	Data ora inizio video in millisecondi (xsd:dateTime YYYY-MM-DTHH:mm:ss SSS)
	*	<u>EndDateTime</u>	string	Data ora fine video in millisecondi (xsd:dateTime YYYY-MM-DTHH:mm:ss SSS)
		<u>Format</u>	string	Indica il formato del file da esportare
		<u>Reason</u>	string	Motivo dell'export (note operative, ecc.)
	*	<u>User</u>	<Credential>	Identificativo del sistema ICT.
		Obb.	Nome	Tipo
Campi in Uscita	*	<u>Result</u>	string	URL di accesso al file registrato

Tabella 2 - Integrazione TVCC: il metodo TVCC.exportVideo

Metodo 'TVCC.requestPtz'

Il sistema TVCC integrato deve consentire il brandeggio da remoto delle proprie telecamere esponendo un metodo, il cui schema è descritto nella tabella successiva, attraverso il quale ICT invierà dei comandi PTZ predefiniti attraverso il protocollo http del tipo:

http://IP_TVCC_SERVER/ptz/camera=<ID_TVCC>&comando=<comandoPTZ>

con i valori del <comandoPTZ> sono indicati nel capitolo delle strutture dati

Descrizione	Richiede l'acquisizione dei flussi video.			
Campi In Ingresso	Obb.	Nome	Tipo	Descrizione
	*	<u>idCamera</u>	string	Identificativo telecamera a cui si richiede il video live
*	<u>comandPTZ</u>	string	URL contenente il comando del brandeggio.	
Campi In Uscita	Obb.	Nome	Tipo	Descrizione
	*	<u>Result</u>	string	"True" o "False"

Tabella 3 - Integrazione TVCC: il metodo TVCC.requestPtz

AUTOC	Descrizione	Parametro PTZ
PTZ Movement UP	Effettua il movimento della telecamera verso l'alto	UP
PTZ Movement Down	Effettua il movimento della telecamera verso il basso	DOWN
PTZ Movement Up_plus	Effettua un movimento più grande della telecamera verso l'alto	UPPLUS
PTZ Movement Down_plus	Effettua un movimento più grande della telecamera verso il basso	DOWNPLUS
PTZ Movement Sx	Effettua un movimento della telecamera verso Sinistra	SX
PTZ Movement Dx	Effettua un movimento della telecamera verso Destra	DX
PTZ Movement Sx_plus	Effettua un movimento più ampio della telecamera verso Sinistra	SXPLUS
PTZ Movement Dx_plus	Effettua un movimento più ampio della telecamera verso Destra	DXPLUS
Zoom ZoomIn	Effettua uno zoom in della telecamera	ZIN
Zoom ZoomOut	Effettua uno zoom out della telecamera	ZOUT
ZoomC ZoomIn	Effettua uno zoom in progressivo della telecamera	ZINC
ZoomC ZoomOut	Effettua uno zoom out progressivo della telecamera	ZOUTC
Zoom Stop	Effettua uno stop dello Zoom	ZSTOP
Home Set_Home	Vai alla posizione predefinita della telecamera	HOME

4. WSDL

Ciascuna Forza di polizia fa riserva di fornire il WSDL per interfacciarsi con il sistema "Alerter".

Allegato 5 - Modulo di attivazione
INTESTAZIONE
SISTEMA DI VIDEO ALLARME ANTI-RAPINA
- MODULO DI ATTIVAZIONE -

ALLA QUESTURA/COMANDO _____ **di** _____

Il sottoscritto _____ nato a _____ il _____
residente in _____ via _____ n. _____, in qualità di responsabile
dell'esercizio _____ situato in _____ via _____ n. _____
(denominazione)

COMUNICA

di aver conferito mandato alla società _____ di attestare presso il proprio
esercizio un sistema di video allarme anti-rapina collegato con le Forze dell'Ordine in virtù del-
l'omonimo protocollo d'intesa siglato tra il Ministero dell'Interno e le associazioni di categoria.
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 _____ nr. _____ tel./cell _____

Il sottoscritto:

1. dichiara, ai sensi dell'art. 13 della legge 30 giugno 2003 n.196, di essere stato informato che i
dati personali contenuti nella presente dichiarazione saranno trattati, anche con strumenti in-
formatici 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 né implica la certezza dell'intervento immediato da parte delle Forze del-
l'Ordine, che interverranno nel più breve tempo possibile compatibilmente con le risorse dispo-
nibili al momento.

Luogo e data _____

IL RICHIEDENTE

~~~~~  
(spazio riservato alle Forze dell'Ordine)

**Codice unico d'identificazione** assegnato all'apparato:

\_\_\_\_\_

Luogo e data \_\_\_\_\_

Gruppo Firma

\_\_\_\_\_

---

## Allegato 6 - Disciplinare tecnico del 14 luglio 2009

---



COMMISSIONE  
N. 1000/2008



### Progetto per un sistema di allarme antirapina controllato con telecamere integrato con le Sale/Centrali Operative delle Forze di Polizia Requisiti tecnici

#### PREMESSA

Il presente documento ha per oggetto la realizzazione di un sistema di allarme antirapina - di seguito denominato *Videoallarme* - mediante il controllo con telecamere dei locali commerciali, attivabile con semplice pressione sul pulsante di comando, in grado di collegarsi con le sale/centrali operative delle Forze di Polizia e di trasmettere le immagini in tempo reale e registrate.

Il videoallarme è un sistema che prevede il collegamento degli esercizi commerciali alle sale/centrali operative con collegamento telematico anche per il tramite di un centro di controllo, qualora presente gestito da istituto di vigilanza privata.

Il centro di controllo, nell'ambito dell'architettura del videoallarme, riveste il ruolo di concentratore dei collegamenti ovvero degli allarmi provenienti dagli esercizi commerciali, per poi instradarli verso le sale/centrali operative della Polizia di Stato e dell'Arma dei Carabinieri ad ognuna tramite un unico collegamento telematico. Il centro di controllo, nei casi di allarme per rapina, avrà esclusivamente un ruolo di transito del flusso del video allarme, senza rivestire compiti di filtraggio e trattazione dell'informazione.

L'implementazione del sistema è improntato alla *gestione intelligente* degli eventi, quest'ultima da intendersi quale gestione delle informazioni conforme ai sistemi presenti e in modo tale da rendere minimo l'intervento dell'operatore nella gestione degli allarmi.

Le specifiche tecniche proposte nel presente documento sono da intendersi come *requisiti minimi*, nel senso che si potranno implementare soluzioni tecnologiche migliorative (trasmissione dell'audio in tempo reale alla sala/centrale operativa, formato immagine di dimensioni superiori, etc.), purché tali da garantire gli obiettivi prefissati in termini di prestazioni, sicurezza e gestibilità nell'ottica dell'ottimizzazione dei costi



CONFEDIREZIONE  
RAI/ISCOM/ISCOM



### **INTEGRAZIONE CON I SISTEMI ESISTENTI PRESSO LE SALE/ CENTRALI OPERATIVE**

Necessità vincolante in fase di progettazione del sistema in argomento è l'integrazione con i sistemi informatici esistenti presso le sale/centrali operative delle FF.PP., presso le quali dovranno essere resi disponibili i flussi video allarmati "live", provenienti dalle telecamere installate presso l'esercizio per il tramite del Centro di Controllo ovvero direttamente, per la "contestualizzazione" degli stessi all'interno dei rispettivi applicativi (SCT - Sistema per il Controllo del Territorio e CC112 - Sistema di gestione interventi) e la relativa gestione "intelligente".

Inoltre è richiesto l'interfacciamento dei citati flussi video con i sistemi di visualizzazione su grande schermo esistenti presso le Sale/Centrali Operative, dove i nuovi segnali provenienti dalle telecamere dovranno essere resi disponibili in formato compatibile con la matrice video preesistente, opportunamente estesa mediante aggiunta di elementi necessari (hardware, software) facenti parte della fornitura.

### **ARCHITETTURA**

L'architettura di sistema viene descritta secondo la presente segmentazione:

#### **CARATTERISTICHE DEL SISTEMA AUDIO/VIDEO E DELLE REGISTRAZIONI PRESSO GLI ESERCIZI COMMERCIALI**

- Alta risoluzione, in ogni caso non inferiore ad un formato immagine VGA pari a 307.200 pixel (640x480 pixel). Eventualmente sarà possibile considerare l'impiego di complessi di ripresa con definizione dell'ordine del megapixel, purché aderenti al profilo di missione richiesto e alle performance derivanti da specifiche tecniche che costituiscono vincolo di comunicazione.
- Supporto della registrazione audio (WAVE compatibile con campionamento almeno a 16 bit).
- Rappresentazione delle immagini a colori e in modalità day&night.
- Visualizzazione fino al limite di una rappresentazione di tipo "full motion" (visione diretta di ogni particolare che prende parte all'evento criminoso in tempo reale).
- Conservazione dei filmati (audio + video) per almeno 7 giorni h 24 (conformemente a quanto previsto dal paragrafo 3.4 del Provvedimento generale sulla videosorveglianza del 29 aprile 2004 del Garante per la protezione dei dati personali), con risoluzione almeno VGA ad un frame rate pari a 25 fps e sensibilità microfonica pari a -54db.



MINISTERO  
D'INTERNO



Progetto per un sistema di allarme antirapina  
controllato con telecamere integrato con le  
Sale/Centrali Operative delle Forze di Polizia  
Requisiti tecnici

PREMESSA

Il presente documento ha per oggetto la realizzazione di un sistema di allarme antirapina - di seguito denominato *Videoallarme* - mediante il controllo con telecamere dei locali commerciali, attivabile con semplice pressione sul pulsante di comando, in grado di collegarsi con le sale/centrali operative delle Forze di Polizia e di trasmettere le immagini in tempo reale e registrate.

Il videoallarme è un sistema che prevede il collegamento degli esercizi commerciali alle sale/centrali operative con collegamento telematico anche per il tramite di un centro di controllo, qualora presente gestito da istituto di vigilanza privata.

Il centro di controllo, nell'ambito dell'architettura del videoallarme, riveste il ruolo di concentratore dei collegamenti ovvero degli allarmi provenienti dagli esercizi commerciali, per poi instradarli verso le sale/centrali operative della Polizia di Stato e dell'Arma dei Carabinieri ad ognuna tramite un unico collegamento telematico. Il centro di controllo, nei casi di allarme per rapina, avrà esclusivamente un ruolo di transito del flusso del video allarme, senza rivestire compiti di filtraggio e trattazione dell'informazione.

L'implementazione del sistema è improntato alla *gestione intelligente* degli eventi, quest'ultima da intendersi quale gestione delle informazioni conforme ai sistemi presenti e in modo tale da rendere minimo l'intervento dell'operatore nella gestione degli allarmi.

Le specifiche tecniche proposte nel presente documento sono da intendersi come *requisiti minimi*, nel senso che si potranno implementare soluzioni tecnologiche migliorative (trasmissione dell'audio in tempo reale alla sala/centrale operativa, formato immagine di dimensioni superiori, etc.), purché tali da garantire gli obiettivi prefissati in termini di prestazioni, sicurezza e gestibilità nell'ottica dell'ottimizzazione dei costi



COMANDO PROVINCIALE  
FORZE DI POLIZIA



**CARATTERISTICHE DEI FLUSSI AUDIO/VIDEO ALLARMATI DESTINATI  
ALLE SALE/CENTRALI OPERATIVE**

Trasferimento delle immagini su protocollo IP (IPver04 compatibile).

- I segnali video allarmati verso le sale/centrali operative delle FF.PP. devono essere convogliati con un unico collegamento fisico (eventualmente per il tramite di un Centro di Controllo), obbligatoriamente a “filo” (la “policy di sicurezza” adottata dalle strutture militari, al momento, vieta la connessione telematica da/verso l'esterno su reti wireless), ovvero un unico punto di accesso al sistema presente su ciascuna sala/centrale operativa: uno per la sala operativa della Questura e uno per la centrale operativa del Comando Provinciale dell'Arma CC. Tale collegamento, punto nevralgico del sistema, dovrà garantire l'efficienza del servizio che si intende offrire all' esercente.
- I segnali video allarmati dovranno indistintamente essere veicolati verso entrambe le Forze di polizia presenti.
- Le immagini che verranno trasmesse alla postazione di sala/centrale operativa dovranno avere le seguenti caratteristiche minime:
  - media risoluzione con un formato QVGA, corrispondente ad un numero di pixel pari a 76.800 (320x240 pixel);
  - formato delle immagini in modalità colore (24 bit/pixel, pari a 16 ML di colori) e in B&W notturna (8 bit/pixel, 256 livelli di grigio), con algoritmo standard di compressione della famiglia MPEGx / MJPEG;
  - frame rate non inferiore a 2 fps.
- La capacità relativa alla banda passante va calcolata riguardo alle necessità di accesso dei sistemi periferici tenendo conto che il massimo ritardo consentito per tutte le trasmissioni, e per ogni telecamera facente parte di un singolo sistema periferico, non sia superiore al valore di 1500 millisecondi espresso come tempo di latenza (parametro legato alla capacità della banda dell'infrastruttura di telecomunicazioni e migliorabile in funzione della stessa).

Deve essere garantita la trasmissione contemporanea di videoallarmi provenienti da diversi esercizi commerciali. Il collegamento sarà di tipo a larga banda, riservato e protetto con sistemi firewall.

**SISTEMI DI GESTIONE E CONTROLLO  
PRESSO LE SALE/CENTRALI OPERATIVE**

Laddove presente il sistema SCT/CC112, le funzionalità del sistema dovranno essere integrate nella postazione operatore già presente secondo le modalità successivamente meglio descritte e per il tramite di:



MINISTERO DELL'INTERNO  
CORPO NAZIONALE DI POLIZIA



- un apparato attivo ove attestare i flussi video eventualmente provenienti dal centro di controllo, da fornirsi sempre a cura delle Associazioni di categoria o dell'esercente non consociato;
- un video server dedicato alla ricezione dei segnali video da posizionarsi all'esterno delle reti intranet di ciascuna Forza di polizia (DMZ – DeMilitarized Zone); da fornirsi sempre a cura delle associazioni di categoria o dell'esercente non consociato (per la P. di S. n° 103 videosever; per l'Arma n° 109 videosever).

In particolare, il protocollo di scambio dati dovrà essere basato su standard SOAP/XML, che consente l'identificazione del problema e l'inserimento in automatico dell'evento nella coda (ordine cronologico secondo il quale arrivano i videoallarmi) del sistema SCT e del sistema CC112. I relativi campi della scheda evento, uguali per tutte le sale/centrali operative, dovranno essere modulati sulla base di quelli già definiti e descritti per gli eventi attualmente gestiti. In ogni caso, dovranno comprendere tutti gli elementi identificativi e referenziali dell'esercizio da cui proviene l'allarme.

Per il corretto abbinamento dell'allarme all'esercizio associato e la sua completa gestione da parte dell'operatore di sala/centrale, è necessaria una fase preliminare di codifica. Deve pertanto essere definito un protocollo di interscambio informazioni, tra i vari attori del progetto, che consenta:

- la stipula del contratto di servizio, l'invio delle informazioni alle due FF.PP. interessate al progetto per il tramite delle Prefetture (dati anagrafici dell'esercizio e dell'esercente e dati tecnici identificativi dell'apparato);
- la codifica delle suddette informazioni da parte degli organi tecnici delle FF.PP. nel sistema SCT/CC112 e l'attribuzione di un codice univoco dell'impianto.

Si dovrà prevedere la trasmissione alle FF.PP. dei dati anagrafici degli esercizi e degli esercenti autorizzati in formato elettronico (formato CSV).

#### **POSTAZIONE DI GESTIONE DEI FLUSSI VIDEO ALLARMATI**

Si ribadisce che in tutte le centrali operative dei Carabinieri e nelle sale operative della Polizia di Stato, ove è presente e disponibile SCT/CC112, tutti i flussi video dovranno essere interfacciati al sistema per la gestione diretta su ogni posto operatore presente in sala/centrale operativa. Saranno a carico dell'Associazione di categoria o dell'esercente non consociato tutte le implementazioni necessarie per consentire una corretta integrazione, previo coordinamento con i referenti designati rispettivamente dal Questore e dal Comandante Provinciale dei Carabinieri.





INFORMATICA  
PROSPERITÀ



Le sale/centrali operative, a seguito di pervenuto allarme, dovranno poter svolgere le seguenti attività:

- visualizzare e memorizzare le immagini dal vivo in tempo reale;
- archiviare le informazioni di controllo (es. LOG degli accessi);
- gestire gli allarmi.

Nell'eventualità che all'interno della/e sala/e operative della Polizia di Stato e centrale/i operative dei Carabinieri fossero già presenti strumenti di visualizzazione su schermi panoramici (schermi al plasma, videowall, videoproiettori, ecc.) disponibili per l'impiego con l'applicazione specifica e tecnicamente interfacciabili, il progettista - incaricato dall'Associazione di categoria o dall'esercente non consociato - dovrà prevedere l'impiego di tali apparati.

In caso di indisponibilità di postazione SCT/CC112, dovrà essere fornita una "postazione di gestione", composta da un personal computer con case middle tower (o in alternativa da rack, in funzione delle scelte progettuali), dotato delle seguenti caratteristiche minime:

| CARATTERISTICHE                 | RICHIESTO                                                                                                      |
|---------------------------------|----------------------------------------------------------------------------------------------------------------|
| BAPCO SYSMARK 2007 RATING.      | Il PC dovrà essere in grado di raggiungere almeno 160 punti                                                    |
| NR Processori/ CORE             | 1/2                                                                                                            |
| RAM Installata                  | 2 GB                                                                                                           |
| RAM MAX                         | 2 GB                                                                                                           |
| Velocità RAM                    | 533 MHz                                                                                                        |
| Capacità disco fisso Installato | Nr. 2 HD 320 GB configurati in modalità Raid 1                                                                 |
| Interfaccia Disco Fisso         | SATA                                                                                                           |
| Velocità rotazione              | 7.200 RPM                                                                                                      |
| Chipset Grafico                 | Non integrato                                                                                                  |
| RAM Installata                  | 512MB non condivisa                                                                                            |
| Risoluzione Max                 | 1280x1024                                                                                                      |
| Bus grafico                     | PCIx                                                                                                           |
| Masterizzatore                  | DVD +-RW                                                                                                       |
| Velocità supportate             | Dichiarare il valore                                                                                           |
| Velocità Rete /Standard         | 100 /1000- Ethernet                                                                                            |
| Porte (Quantità e Tipo)         | 1 parallela<br>1 seriale<br>4 USB 2.0 retro<br>2 USB 2.0 avanti<br>1 Rj-45<br>2 VGA<br>1 microfono<br>1 cuffia |



CONFERENZA  
UNIVERSITARIA



|                                    |                                                                                                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Slot di espansione                 | 2 PCI                                                                                                                                        |
| Tastiera e Mouse                   | Italiana 108 tasti, 2 tasti con scroll                                                                                                       |
| Monitor doppio<br>Tipo /Dimensione | LCD 21" TFT 1280 x 1024 Dot pitch non superiore a 0,297 mm, con amplificazione incorporata                                                   |
| UPS                                | Con funzione di stabilizzazione e continuità della alimentazione elettrica per almeno 20 minuti e comunque di capacità non inferiore a 600VA |
| Sistema operativo                  | Windows 2008 Server (tassativo)                                                                                                              |
| Software in dotazione              | Ms Office Professional, Antivirus                                                                                                            |

- n.1 stampante di rete laser colori A4 con tavolino porta stampante:

| CARATTERISTICHE            | RICHIESTO                               |
|----------------------------|-----------------------------------------|
| TECNOLOGIA                 | Laser colori                            |
| RISOLUZIONE STAMPA B/N     | 600 x 600 dpi                           |
| RISOLUZIONE STAMPA Colori  | 1200 x 1200 dpi                         |
| FORMATO CARTA              | A4 -                                    |
| VELOCITA' DI STAMPA B/N    | 28 pagine/minuto                        |
| VELOCITA' DI STAMPA Colori | 16 pagine/minuto                        |
| RAM Installata             | 128 MB                                  |
| SUPPORTI DI STAMPA         | Carta normale, buste, lucidi, etichette |
| INTERFACCE                 | Hi-Speed USB                            |
| ALIMENTAZIONE CARTA        | vassoio da 250 fogli                    |
| RUMOROSITA'                | In stampa max 66 dB, Riposo max 54 dB   |

Le postazioni di gestione con le necessarie configurazioni ed abilitazioni, dovranno essere equipaggiate con un applicativo software, con licenza d'uso, che:

- svolga la funzionalità di videosever per la gestione dei flussi video live MPEGx, o MJPEG (in funzione delle configurazioni) ed audio MPEG1;
- svolga la funzione di DVR per la registrazione dei flussi video MPEGx o MJPEG (in funzione delle configurazioni) ed audio ricevuti a seguito di allarme;
- visualizzi in modalità videosplit "n" flussi video allarmati contemporanei live o registrati selezionabili dall'utente o pre-impostati;
- gli "allarmi video" dovranno essere registrati e tenuti disponibili, per esigenze investigative, per almeno 7 giorni e non cancellati se non da personale abilitato;
- visualizzi una cartografia interattiva a livelli multipli navigabili che permetta di selezionare (tramite modalità drag & drop) le telecamere da visualizzare sul videosplit;
- permetta la visualizzazione e la gestione dei flussi video allarmati entranti con segnalazione acustica;



MINISTERO  
DELL'INTERNO



- veicoli le informazioni attraverso la rete IP;
- gestisca l'accesso degli utenti;
- gestisca profili utenti diversi con livelli di autorizzazione diversi (amministrazione, manutenzione, visione live, visione playback, esportazione filmati, ecc.).

La "postazione di gestione" risulterà autorizzata (a livello di configurazione, comunque modificabile) alla visualizzazione ed all'esportazione delle immagini registrate.

**ADESIONE AL SISTEMA DA PARTE DI ESERCENTE  
NON AFFILIATO ALLE ASSOCIAZIONI DI CATEGORIA**

Il sistema dovrà consentire l'adesione anche di esercenti non affiliati alle associazioni di categoria.

Questi potranno avvalersi di un centro di controllo gestito dall'istituto di vigilanza privata, qualora abbiano conferito a quest'ultimo la gestione del complessivo flusso di video-allarme. In tale ipotesi il sistema locale sarà strutturato secondo i requisiti tecnici sinora descritti, compreso il diretto transito dell'allarme antirapina alla sala/centrale operativa delle Forze di polizia.

Qualora gli esercenti non affiliati alle associazioni di categoria non intendano avvalersi di un centro di controllo gestito dall'istituto di vigilanza privata, le specifiche tecniche del sistema locale rimangono inalterate, mentre il flusso trasmissivo viene modificato come di seguito indicato:

- viene abolito il collegamento wireless (GPRS/UMTS tra l'esercente ed il centro di controllo);
- viene instaurato un collegamento di tipo fisico (es: HDSL) tra esercente e Forze di polizia con oneri a carico del primo. Il flusso video sarà attestato, qualora ci sia disponibilità di porte, sugli stessi apparati attivi (router) forniti dalle associazioni di categoria e veicolati sulle precedentemente citate postazioni di gestione attestate in DMZ. In caso contrario dovrà essere fornito anche il router contestualmente al collegamento.

Occorre, infine, che l'esercente provveda, con oneri a proprio carico, a segnalare tempestivamente alle Forze di polizia il verificarsi di guasti al sistema di allarme.

**INSTALLAZIONE, ASSISTENZA E MANUTENZIONE**

Ogni installazione presso le sale/centrali operative dovrà essere sottoposta a preventiva verifica di funzionalità da parte del personale tecnico delle competenti



CONFEDERAZIONE  
CONFESERCENTI



Zone Telecomunicazioni della Polizia di Stato e dell'Ufficio Logistico dei Comandi di Regione Carabinieri, congiuntamente ai tecnici dell'impresa fornitrice ovvero della struttura tecnica individuata dalle Confederazioni, con facoltà di delegare le loro rappresentanze locali e di categoria, ovvero dagli esercenti non consociati.

Per le apparecchiature assegnate in comodato d'uso all'Amministrazione, corredate di idonea documentazione tecnica relativa all'architettura e alle specifiche tecniche del sistema, dovrà essere fornito un servizio di assistenza e manutenzione correttiva, preventiva ed evolutiva per il quale sarà individuato un servizio di help desk.

#### **FORMAZIONE ED ADDESTRAMENTO**

Alle Confederazioni o loro rappresentanze locali e di categoria ovvero agli esercenti non consociati competono gli oneri inerenti alla formazione degli addetti alle sale e alle centrali operative. Per tale incombenza potranno avvalersi anche delle imprese da loro prescelte.

Si dovranno prevedere almeno 2 giorni di affiancamento all'utente, uno per ciascuna sala/centrale operativa per:

- addestramento all'utilizzo delle procedure;
- configurazioni (fine-tuning) dei parametri di sistema, per soddisfare eventuali richieste degli operatori;
- verifica della completa funzionalità del sistema;
- verifica del corretto utilizzo del sistema da parte degli operatori.

Dovrà essere altresì previsto un affiancamento on-the-job di almeno 1 giorno per ciascuna sala operativa da parte di personale specializzato - parimenti in possesso di abilitazione di sicurezza, qualora richiesta in conformità all'art. 41 del DPCM del 3 febbraio 2006 "Norme concernenti la protezione e la tutela delle informazioni classificate" - in grado di correggere eventuali errori di utilizzo degli operatori nella fase iniziale di conduzione e di funzionamento dell'impianto.



Stampato presso la Tipografia della  
**DIREZIONE CENTRALE DELLA POLIZIA CRIMINALE**  
Viale dell'Arte, 81 - 00144 Roma  
Tel. 06.465.41669 - Fax 06.465.41670