



MINISTERO
DELL'INTERNO



CONFCOMMERCIO
IMPRESE PER L'ITALIA



CONFESERCENTI

PROTOCOLLO QUADRO VIDEO -ALLARME ANTIRAPINA

Il Ministero dell'Interno, con sede a Roma, piazza del Viminale n. 1, rappresentato dal Ministro dell'Interno Dott. Matteo Piantedosi;

Confcommercio Imprese per l'Italia, con sede in Roma, piazza G.G. Belli n.2, rappresentata dal Vice Presidente Dott.ssa Patrizia Di Dio, giusta delega del Presidente Carlo Sangalli;

Confesercenti con sede in Roma, Via Nazionale n.60, rappresentata dal Presidente Dott.ssa Patrizia De Luise;

- Visto il Protocollo d'Intesa stipulato il 30 giugno 2003 tra il Ministero dell'Interno e Confcommercio, Confesercenti e Comufficio, 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"*;
- VISTO il Protocollo d'intesa stipulato il 14 luglio 2009, in tema di video-allarme antirapina tra il Ministero dell'Interno e Confcommercio Imprese per l'Italia e Confesercenti, rinnovato il 12 novembre 2013 per la durata di tre anni;
- VISTO il Protocollo Quadro video-allarme antirapina stipulato il 12 dicembre 2019, concernente i criteri generali di collaborazione in tema di video-allarme antirapina tra il Ministero dell'Interno e Confcommercio Imprese per l'Italia e Confesercenti;
- RAVVISATA la attuale necessità di rafforzare i livelli di protezione degli esercizi commerciali o imprese, assicurando la più efficace sinergia tra Istituzioni pubbliche, Forze di polizia e Associazioni di categoria, anche avvalendosi di nuove tecnologie, attesa la domanda di sicurezza nel settore delle imprese e degli esercizi commerciali (nel prosieguo denominati "Esercenti");
- CONSIDERATE le specificità territoriali e settoriali che caratterizzano l'imprenditoria italiana e il terziario di mercato in particolare;
- RAVVISATA pertanto l'opportunità di proseguire i rapporti di sinergica collaborazione avviati con il richiamato Protocollo Quadro sottoscritto in data 12 dicembre 2019;

CONVENGONO QUANTO SEGUE

Art.1 (Premesse)

Le premesse fanno parte integrante del presente Protocollo Quadro.

del documento), comunicandone gli esiti al Dipartimento della Pubblica Sicurezza – Ufficio per il coordinamento e la pianificazione delle attività delle Forze di polizia.

Art. 8
(Clausola finanziaria)

All'attuazione del presente Protocollo Quadro si provvede con le risorse economiche, di personale e strumentali finanziate a legislazione vigente, senza oneri aggiuntivi per il bilancio dello Stato.

Art. 9
(Clausola finale)

Il presente Protocollo Quadro potrà essere oggetto di aggiornamento in relazione ai sopravvenuti interventi normativi in materia ed agli eventuali atti di indirizzo emanati dal Ministero dell'Interno.

Il Disciplinare tecnico allegato al presente Protocollo-Quadro potrà essere aggiornato in base alla implementazione di nuove piattaforme tecnologiche da parte delle Forze di polizia.

Le Confederazioni potranno richiedere l'esame congiunto di aspetti di interesse comune o di nuove esigenze correlate.

Per quanto non espressamente previsto dal presente Protocollo Quadro si fa riferimento alla normativa vigente.

Art. 10
(Durata)

Il presente Protocollo Quadro ha la durata di tre anni a decorrere dalla data di sottoscrizione.

Roma, 22.02.2024

Confcommercio - Imprese per l'Italia

La Vice Presidente

Di Dio

Confesercenti

La Presidente

De Luse

Il Ministro dell'Interno

Piantedosi

REQUISITI TECNICI

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

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

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

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

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

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

Restano salve le disposizioni riguardanti la normativa sul procurato allarme.

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

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

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

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

3. CARATTERISTICHE DELLE MODALITÀ DI INTERCONNESSIONE/ INTERFACCIA- MENTO CON LE SALE/CENTRALI OPERATIVE DELLE FORZE DI POLIZIA

- a. Il flusso video deve essere inviato mediante sistemi e protocolli per la comunicazione sicura su Internet che proteggano l'integrità, la riservatezza dei dati scambiati e ne garantiscano l'autenticazione (almeno con utilizzo del protocollo HTTPS).
- b. I segnali videoallarmati verso le Sale/Centrali operative delle Forze di polizia devono essere convogliati attraverso un unico collegamento fisico per il tramite di una Sala Controllo di un Istituto di Vigilanza, ovvero direttamente verso ciascuna Sala/Centrale operativa delle Forze di polizia, quindi, rispettivamente:
 - uno per la Sala operativa della Questura;
 - uno per la Centrale operativa del Comando Provinciale/Gruppo dell'Arma dei Carabinieri, che gestiranno l'intervento secondo le ordinarie procedure operative e le competenze ripartite sulla base del Piano coordinato di controllo del territorio previsto a livello provinciale.
- c. Il punto di accesso delle Sale operative delle Forze di polizia deve avviare la registrazione del video in ingresso immediatamente, in caso di allarme, indipendentemente dalla successiva presa in carico da parte dell'operatore di Sala/Centrale operativa.

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

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

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

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

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

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

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

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

Polizia di Stato

Nel caso A:

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

Nel caso B e C:

l'installatore provvede a predisporre l'apposito interfacciamento verso il MediaServer della Questura competente territorialmente.

Arma dei Carabinieri

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

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

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

Le articolazioni tecniche periferiche dell'Arma dei Carabinieri:

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

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

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

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

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

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

INTESTAZIONE REPARTO

versione del 30 giugno 2019

OGGETTO: Sistema di video-allarme antirapina

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

ALLA SPETT.LE ditta

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

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

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

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

Nota: la ditta si impegna sin d'ora, pena revoca dell'autorizzazione testè concessa, ad attuare tutte le necessarie predisposizioni tecniche per continuare a garantire l'operatività del sistema.

GRUPPO FIRMA

66	Palermo	Via Muro di San Vito	192.168.66.128/25	192.168.66.129	192.168.66.13
67	Parma	Strada Fondaria 10	192.168.67.128/25	192.168.67.129	192.168.67.13
68	Pavia	Via D. Sordani 31	192.168.68.128/25	192.168.68.129	192.168.68.13
69	Perugia	Via Ruggia 9	192.168.69.128/25	192.168.69.129	192.168.69.13
70	Pesaro	Via Salvo D'Acquino 2	192.168.70.128/25	192.168.70.129	192.168.70.13
71	Pescara	Via G. D'Armando 143	192.168.71.128/25	192.168.71.129	192.168.71.13
72	Piacenza	Via Bevanon 46	192.168.72.128/25	192.168.72.129	192.168.72.13
73	Pisa	Via Guido De Pisa 1	192.168.73.128/25	192.168.73.129	192.168.73.13
74	Pistoia	Viale Italia 76	192.168.74.128/25	192.168.74.129	192.168.74.13
75	Pordenone	Via del Carabiniere 2	192.168.75.128/25	192.168.75.129	192.168.75.13
76	Potenza	Via Piratola 300	192.168.76.128/25	192.168.76.129	192.168.76.13
77	Prato	Via Paolo Piccini 30	192.168.77.128/25	192.168.77.129	192.168.77.13
78	Ragusa	P.zza. Card. de Nardis 3	192.168.78.128/25	192.168.78.129	192.168.78.13
79	Ravenna	Viale Perini 11	192.168.79.128/25	192.168.79.129	192.168.79.13
80	Reggio Calabria	Via Ascheretti 3	192.168.80.128/25	192.168.80.129	192.168.80.13
81	Reggio Emilia	Via Canali 6	192.168.81.128/25	192.168.81.129	192.168.81.13
82	Rieti	Via Giulio de Julia 2	192.168.82.128/25	192.168.82.129	192.168.82.13
83	Rimini	Viale Carlo Alberto Dalla Chiesa 16	192.168.83.128/25	192.168.83.129	192.168.83.13
84	Roma	Piazza S. Lorenzo in Lucina 6	192.168.84.128/25	192.168.84.129	192.168.84.13
85	Rovigo	Via Sfricini 21	192.168.85.128/25	192.168.85.129	192.168.85.13
86	Salerno	Via R. Mauri 99	192.168.86.128/25	192.168.86.129	192.168.86.13
87	Sassari	Via Roccaforte 52	192.168.87.128/25	192.168.87.129	192.168.87.13
88	Savona	Via Ricci 10	192.168.88.128/25	192.168.88.129	192.168.88.13
89	Siena	Largo Salvo D'Acquino 1	192.168.89.128/25	192.168.89.129	192.168.89.13
90	Siracusa	Via Tico 1450m	192.168.90.128/25	192.168.90.129	192.168.90.13
91	Sondrio	Largo Gentili 6	192.168.91.128/25	192.168.91.129	192.168.91.13
92	Taranto	Viale Virgilio 28	192.168.92.128/25	192.168.92.129	192.168.92.13
93	Teramo	Piazza Dei Carmine 3	192.168.93.128/25	192.168.93.129	192.168.93.13
94	Terni	Via Giuseppe Lombardi Radice 6	192.168.94.128/25	192.168.94.129	192.168.94.13
95	Torino	Via Valce 5/5a	192.168.95.128/25	192.168.95.129	192.168.95.13
96	Trapani	Via Ortonelli 27	192.168.96.128/25	192.168.96.129	192.168.96.13
97	Trento	Via Badacchini 24	192.168.97.128/25	192.168.97.129	192.168.97.13
98	Treviso	Via Garzarotti 24	192.168.98.128/25	192.168.98.129	192.168.98.13
99	Trieste	Via Dell'Alba 54	192.168.99.128/25	192.168.99.129	192.168.99.13
100	Udine	Viale Tosti 28	192.168.100.128/25	192.168.100.129	192.168.100.13
101	Varese	Via Aurelia SAFFI 55	192.168.101.128/25	192.168.101.129	192.168.101.13
102	Venezia	Castello 4692a	192.168.102.128/25	192.168.102.129	192.168.102.13
103	Verbania	Via Gen. Carlo Alberto Dalla Chiesa 1	192.168.103.128/25	192.168.103.129	192.168.103.13
104	Vercelli	Via Obizzi 57	192.168.104.128/25	192.168.104.129	192.168.104.13
105	Verona	Via S. D'Acquino 8	192.168.105.128/25	192.168.105.129	192.168.105.13
106	Vibo Valentia	Via Gen. Polipani 18	192.168.106.128/25	192.168.106.129	192.168.106.13
107	Vicenza	Via Muggia 2	192.168.107.128/25	192.168.107.129	192.168.107.13
108	Vitarbo	Via S. Carmelo De Lese 20	192.168.108.128/25	192.168.108.129	192.168.108.13
109	Torre Annunziata	Piazza Enrico da Nicola 12	192.168.109.128/25	192.168.109.129	192.168.109.13
110	Giola Tauro (Gruppo)	Via strada provinciale 111	192.168.110.128/25	192.168.110.129	192.168.110.13
111	Lamezia Terme (Gruppo)	Via Guglielmo Marconi 65	192.168.111.128/25	192.168.111.129	192.168.111.13
112	Locri (Gruppo)	Via Cosmano S.N.	192.168.112.128/25	192.168.112.129	192.168.112.13
113	Fermo	Via Bari 5	192.168.113.128/25	192.168.113.129	192.168.113.13

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

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions xmlns:tc="http://microsoft.com/wadl/xhtml2/xml" xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:tns="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:tns1="http://carabinieri.it.org/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:s="http://www.w3.org/2001/XMLSchema" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
  xmlns:ht="http://schemas.xmlsoap.org/wsdl/http/" targetNamespace="http://carabinieri.it.org/" xmlns:wsp="http://schemas.xmlsoap.org/wsdl/"
  <wsdl:types>
    <xs:schema elementFormDefault="qualified" targetNamespace="http://carabinieri.it.org/">
      <xs:element name="BeginAlert">
        <xs:complexType>
          <xs:sequence>
            <xs:element minOccurs="1" maxOccurs="1" name="message" type="tns:Message" />
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:complexType name="Message">
        <xs:sequence>
          <xs:element minOccurs="0" maxOccurs="1" name="Id" type="s:string" />
          <xs:element minOccurs="1" maxOccurs="1" name="Timestamp" type="s:int" />
          <xs:element minOccurs="0" maxOccurs="1" name="Protocol" type="s:string" />
          <xs:element minOccurs="1" maxOccurs="1" name="Port" type="s:int" />
          <xs:element minOccurs="0" maxOccurs="1" name="Uri" type="s:string" />
          <xs:element minOccurs="0" maxOccurs="1" name="IpAddress" type="s:string" />
          <xs:element minOccurs="0" maxOccurs="1" name="Parameters" type="s:string" />
          <xs:element minOccurs="0" maxOccurs="1" name="CallbackUri" type="s:string" />
        </xs:sequence>
      </xs:complexType>
      <xs:element name="BeginAlertResponse">
        <xs:complexType>
          <xs:sequence>
            <xs:element minOccurs="1" maxOccurs="1" name="BeginAlertResult" type="tns:Response" />
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:complexType name="Response">
        <xs:sequence>
          <xs:element minOccurs="1" maxOccurs="1" name="Result" type="s:boolean" />
          <xs:element minOccurs="0" maxOccurs="1" name="Description" type="s:string" />
        </xs:sequence>
      </xs:complexType>
    </xs:schema>
  </wsdl:types>
  <wsdl:message name="BeginAlertSoapIn">
    <wsdl:part name="parameters" element="tns:BeginAlert" />
  </wsdl:message>
  <wsdl:message name="BeginAlertSoapOut">
    <wsdl:part name="parameters" element="tns:BeginAlertResponse" />
  </wsdl:message>
  <wsdl:portType name="ErmasAlerterSoap">
    <wsdl:operation name="BeginAlert">
      <wsdl:input message="tns:BeginAlertSoapIn" />
      <wsdl:output message="tns:BeginAlertSoapOut" />
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="ErmasAlerterSoap" type="tns:ErmasAlerterSoap">
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="BeginAlert">
      <soap:operation soapAction="http://carabinieri.it.org/BeginAlert" style="document" />
      <wsdl:input>
        <soap:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal" />
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="ErmasAlerterSoap12" type="tns:ErmasAlerterSoap">
    <soap12:binding transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="BeginAlert">
      <soap12:operation soapAction="http://carabinieri.it.org/BeginAlert" style="document" />
      <wsdl:input>
        <soap12:body use="literal" />
      </wsdl:input>
      <wsdl:output>
        <soap12:body use="literal" />
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="ErmasAlerter">
    <wsdl:port name="ErmasAlerterSoap" binding="tns:ErmasAlerterSoap">
      <soap:address location="http://localhost:59305/ErmasAlerter.asmx" />
    </wsdl:port>
    <wsdl:port name="ErmasAlerterSoap12" binding="tns:ErmasAlerterSoap12">
      <soap12:address location="http://localhost:59305/ErmasAlerter.asmx" />
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```



ErmasAlerter.wsdl

