Offre Technique et Commerciale

Mise à disposition d'une application mobile multisupport d'alerte et d'information de la population dans le cadre de l'Euro 2016

Objet	Offre technique et financière pour la mise à disposition d'une application mobile multisupport d'alerte et d'information de la population dans le cadre de l'Euro 2016
Diffusion	Ministère de l'Intérieur
Rédacteur	
Vérificateur	
Approbateur	

Evolutions

Edition	Date	Objet de l'évolution

TABLE DES MATIÈRES

1 RAPPEL DU BESOIN 4

2 PRÉSENTATION DE DEVERYWARE 4

1.1 ACTIVITÉ 4

1.2 NOS PRINCIPAUX CLIENTS 5

3 PROPOSITION TECHNIQUE 6

3.1 PRÉSENTATION GÉNÉRALE DE LA SOLUTION 6

3.2 DISPOSITIF 7

3.3 POSTE 1 – PRODUCTION DE LA SOLUTION 7

3.4 POSTE 2 – UNITÉ 1 8

3.4.1 Infrastructure 8

3.4.2 Tierce Maintenance Applicative et assistance client 9

4 MÉTHODOLOGIE ET ORGANISATION PROJET 11

4.1 DÉMARCHE QUALITÉ, SÉCURITÉ ET ENVIRONNEMENT 11

4.2 L'ORGANISATION PROJET DEVERYWARE 12

4.2.1 Phase de Préparation 12

4.2.2 Phase de développement et exploitation 12

4.2.3 Phase de Formation 13

4.2.4 Phase de maintenance applicative et assistance client 13

4.3 ORGANISATION SPÉCIFIQUE AU PROJET SAIP 13

4.3.1 Équipes projet 13

4.3.2 Responsable de la contractualisation 14

4.3.3 Meetings et revues 15

5 PROPOSITION FINANCIÈRE 16

5.1 PRESTATION POUR LA PÉRIODE DU 20 MAI AU 15 JUILLET : 16

5.2 COÛT POUR 15 JOURS CALENDAIRES DE PRESTATIONS 17

5.3 SIGNATURES ET ACCORD 17

6 POLITIQUE DE SÉCURITÉ DE L'ÉDITEUR 18

ANNEXE 1 : MATRICE DE CONFORMITÉ 19

ANNEXE 2 : DESCRIPTIF SUCCINCT DES TRAVAUX RÉALISÉS POUR LE DÉVELOPPEMENT D'UN DISPOSITIF D'ALERTE DE LA POPULATION 28

ANNEXE 3 : PROTOCOLE SSI DÉFINIS ENTRE LES PARTIES 32

1 RAPPEL DU BESOIN

L'alerte des populations est inscrite dans le code de la sécurité intérieure depuis la fin des années cinquante. Depuis 2011, l'administration rénove son réseau national d'alerte et l'a nommé SAIP (système d'alerte et d'information des populations) sous la responsabilité de la Sécurité civile. En lien avec les préfectures de département.

Le système d'alerte n'ayant de sens que s'il peut toucher un maximum de gens concernés par le phénomène en cours. **L'Etat a fait le choix de garantir l'alerte multicanal.**

Les événements terroristes dramatiques de l'année 2015 ont mis en évidence la nécessité pour le Gouvernement de disposer d'un **outil de communication mobile d'alerte, non seulement pour les risques naturels et industriels, mais également en cas d'attentats.**

Le Premier ministre a demandé au service d'information du gouvernement (SIG de développer, dans un délai court et si possible pour **l'Euro 2016**, une application mobile d'alerte et d'information des populations en cas de crise majeur.

2 PRÉSENTATION DE DEVERYWARE

1.1 ACTIVITÉ

Créée en 2003, le groupe Deveryware est une société française indépendante, ouverte à l'international avec ses filiales Deveryware Afrique, Deveryware Iberia, Deveryware Amérique du Nord, qui emploie 84 personnes et réalise un chiffre d'affaires de 14 M€, essentiellement pour la sécurité de l'État et des entreprises.

[redacted]

Deveryware est un prestataire spécialisé intervenant en appui des opérateurs de communications électroniques français pour agréger les données des opérateurs et proposer

des traitements et représentations sophistiquées consultables et pilotables aisément.

[redacted]

Deveryware est membre actif du GICAT, elle contribue à la gouvernance de plusieurs pôles de compétitivité et du défi sécurité de l'Agence Nationale de la Recherche (ANR), et participe à la gouvernance du Conseil des industries de la confiance et de la sécurité (CICS), pilier de la filière industrielle nationale de sécurité incarnée par le COFIS. Membre de l'association européenne de l'appel d'urgence (EENA) en tant que Vice-Chairman, le Groupe Deveryware travaille aussi à la normalisation Télécom européenne auprès de l'ETSI et s'assure ainsi de l'intégration des standards les plus innovants de demain dans la gestion de crise et de l'urgence au niveau européen.

Fort de son savoir-faire dans la localisation et de son expérience réussie sur le territoire français, Deveryware participe à de nombreux projets collaboratifs de recherche et développement subventionnés par la Commission Européenne (FP7, H2020) l'Agence Nationale de la Recherche (ANR-défi 9 Sécurité) et le Fonds Unique Interministériel (FUI) et est adhérent de deux pôles de compétitivité (System@tic et Cluster Safe) à la gouvernance desquels elle participe. Dans ce cadre, *Deveryware* a pu proposer le fruit de ses travaux de recherche et développement issus du projet Européen « ISAR+ » et répondant au besoin exprimé par l'administration.

1.2 NOS PRINCIPAUX CLIENTS

Deveryware est un acteur majeur dans la fourniture de prestations de haut niveau de fiabilité et de sécurité auprès

[redacted]

Par ailleurs, Deveryware a pour clients des grands comptes et des entreprises de tous horizons, notamment :

- des transporteurs et logisticiens spécialisés dans les transports de chargements de grande valeur, pour la surveillance des véhicules et des marchandises ;
- des intégrateurs spécialisés dans des applications de haute sécurité ;
- des sociétés de télésurveillance, de sécurité et d'assistance
- [redacted]

3 PROPOSITION TECHNIQUE

3.1 PRÉSENTATION GÉNÉRALE DE LA SOLUTION

A la demande du Service d'Information du Gouvernement (SIG) et de la Direction Générale de la Sécurité Civile et de la gestion de Crise (DGSCGC), Deveryware propose sa réponse à l'expression de besoin Euro 2016.

La solution Deveryware se compose d'une plateforme de traitement de données géolocalisées [redacted]

Dans la cadre de cette proposition nous allons développer une application mobile avec son back office afférent pour la gestion des alertes et informations à destination des citoyens ayant téléchargées l'application mobile.

Le dispositif permettra :

- De diffuser des messages d'alerte ou de vigilance sur l'ensemble du territoire de la République. Une autorité pourra diffuser une alerte vers des zones (cercle, polygone, département, zone de défense), et des vigilances vers des départements. Il sera possible d'adjoindre des sons aux messages émis,
- De respecter totalement la vie privée du citoyen : aucune donnée personnelle ne sera nécessaire à l'enregistrement et à l'usage de l'application, aucune donnée de localisation ne sera transmise vers des serveurs. Tous les traitements liés à la géolocalisation seront traités à bord du smartphone,
- De ne pas consommer excessivement l'énergie bord,
- De diffuser un message auprès de 5% de la population française, soit 3,3 millions d'utilisateurs potentiels,
- De mettre à disposition le message, après validation par l'autorité, à l'ensemble des utilisateurs dans un délai court inférieur à une minute. Le message sera présenté à l'utilisateur sur son smartphone dans un délai de 10 minutes au maximum.
- De s'appuyer sur les senseurs de localisation les plus précis disponibles au moment de l'émission de l'alerte.
- De disposer d'une architecture sécurisée :
  - Mécanisme d'identification et d'authentification forte de l'utilisateur
  - Chiffrage des échanges
  - Capacité à faire face aux attaques classiques de type DDoS

  [redacted]
- D'historiser et retrouver des évènements passés

Une matrice de conformité est présentée en Annexe 1.

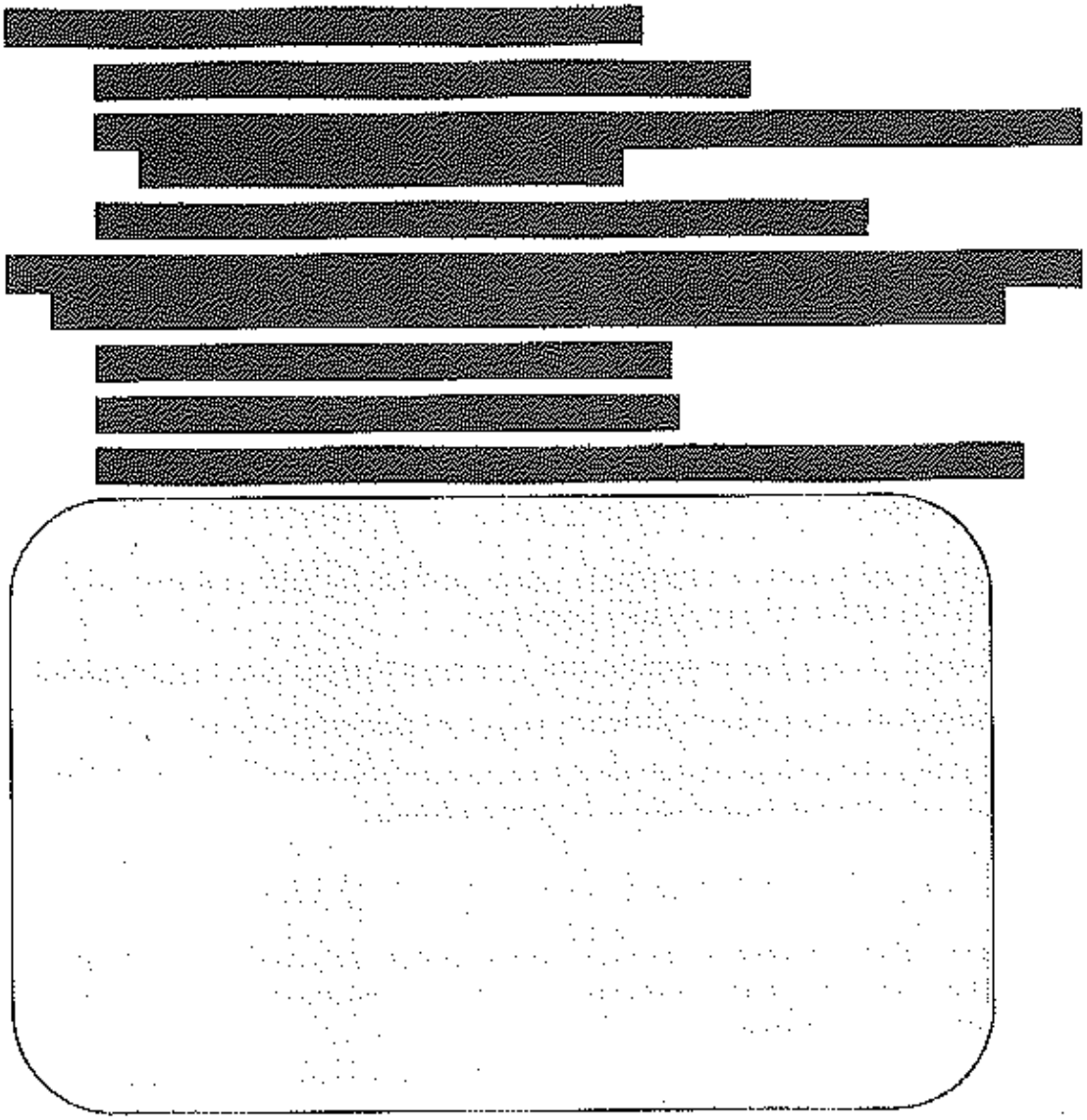
3.2 DISPOSITIF

3.3 POSTE 1 – PRODUCTION DE LA SOLUTION

L'offre du dispositif d'alertes et d'information géolocalisées des populations par le biais de smartphones, repose sur une architecture constituée de :

- un back office permettant pour la définition et l'émission des messages d'alerte,
- une application mobile « SAIP », disponible sous IOS et Androïd, pour la réception des messages
- serveurs spécifiques

Le principe fonctionnel macroscopique est le suivant :



Le concept et la technologie embarquée par Deveryware font l'objet d'un dépôt de brevet.

3.4 POSTE 2 – UNITÉ 1

3.4.1 Infrastructure

3.4.1.1 Hébergement

L'hébergement de l'application SAIP est assuré par l'opérateur de Cloud Computing Numergy.

Numergy dispose d'une infrastructure sécurisée et garantit légalement le contrôle de la localisation des données d'alerte sur le sol européen. Il est rappelé qu'aucune donnée utilisateur de l'application SAIP n'est collectée.

- Les datacenters sont localisés en France.
- La sécurité physique et logique est assurée par 3 Datacenters.
- L'infrastructure est redondée, chaque client est cloisonné dans son environnement.
- Les actions sont tracées.
- La sécurité active est assurée par la proactivité et la détection en temps réel des attaques.
- Taux de disponibilité de 99.9%.
- Numergy est certifié ISO9001 et ISO27001, nous pouvons fournir leurs certificats.

Deveryware a accès à la matrice d'escalade de Numergy en cas de problème.

3.4.1.2 Haute Disponibilité et Gestion de la charge sur les services exposés sur Internet

Deveryware a sélectionné 2 Prestataires pour absorber le trafic Internet, assurer une disponibilité de 100% et comme bouclier anti DDoS:

- Cedexis: Un aiguilleur de de trafic DNS permettant l'orchestration de plusieurs CDN.
- OptimiCDN: Une solution Multi-CDN, basée sur EdgeCast et Level3.

Pour ces 2 prestataires nous pouvons fournir des documents complémentaires détaillant les niveaux de sécurité et de disponibilité des services proposés.

3.4.1.3 Exploitation et Administration du Système d'information

Deveryware a dédié plusieurs « tenants » pour le projet SAIP (dev/integ, preprod, prod). L'application SAIP est donc totalement cloisonnée. Deveryware est en charge de l'exploitation de ces « tenants ».

Deveryware opère les services de Numergy en utilisant la méthode Infrastructure As A code (création de VM, Firewall ...). Toutes les modifications sont tracées et versionnées.

L'installation système et applicative est industrialisée, automatisée, relue et versionnée.

L'infrastructure est auditée régulièrement avec des outils de détection de vulnérabilités.

Les serveurs sont installés avec un soin particulier concernant : la politique de mise à jour, de backup, de gestion de logs, de détection d'intrusions ...

Un service de supervision assure la surveillance de chaque brique du système d'information et alerte les exploitants en cas de problèmes (une astreinte & un plan d'escalade sont mis en place pour assurer une disponibilité optimale, détaillés au chapitre suivant)

3.4.2 Tierce Maintenance Applicative et assistance client

Deveryware propose une **Tierce Maintenance Applicative (TMA)** comprenant les prestations suivantes :

- Correction de toutes anomalies bloquantes : est déclarée « bloquante » une anomalie qui empêche un testeur de poursuivre le processus de test (par exemple : la page des CGU n'est pas accessible, je ne peux valider son contenu)
- Correction de toutes les anomalies majeures : est déclarée « majeure » une anomalie empêchant l'usager de bénéficier des pleines fonctionnalités du dispositif. (par exemple : une alerte émise à T0 n'est pas distribuée). Ces anomalies sont traitées en priorité.
- Formation de l'administration
    - 1 session de formation initiale sur site de l'administration, à l'utilisation de l'émetteur d'alertes pour les formateurs (1/2 journée)
    - 1 session de formation sur site de Deveryware, à l'utilisation de l'émetteur d'alertes pour les formateurs (1/2 journée)
    - des sessions de rattrapage en vidéoconférence sont possibles
    - Fourniture d'un guide de prise en main rapide de l'éditeur d'alerte
- Mises à jour plateforme serveur
    - développement serveur
    - Tests
    - Pilotage PO
- Exploitation des plateformes (équipe Ops - 2 ressources mobilisées à temps partiel)

Durant la période du marché, les équipes de l'administration bénéficieront d'un soutien assuré par le service d'**Assistance Clients (AC)** de Deveryware. Une organisation spécifique a été mise en place pour la gestion de l'exploitation de la plateforme via un process de gestion des incidents avec deux niveaux d'escalades ainsi que des astreintes :

- Le niveau 1, premier contact pour le client, est composé de personnels en poste fixe.

[redacted]

[redacted]
identifié par l'utilisateur. Pour ce dernier cas, l'Assistance Client escalade au niveau 2.

- Le niveau 2 (N2) gère les évènements nécessitant une analyse approfondie. Dans le cas particulier du SAIP, le niveau 2 fait partie de l'équipe qui a développé le dispositif. [redacted]
- Lorsque l'incident est identifié, le contact RSSI de l'administration est informé selon le protocole défini entre les deux parties, et joint en annexe 3.

Pour accéder à l'assistance client les moyens suivants sont à disposition exclusive de l'administration :

[redacted]

La procédure de demande d'assistance est la suivante :

[redacted]

4 MÉTHODOLOGIE ET ORGANISATION PROJET

4.1 DÉMARCHE QUALITÉ, SÉCURITÉ ET ENVIRONNEMENT

Afin de garantir à ses clients des produits et services à la hauteur de leurs attentes, DEVERYWARE s'est engagée depuis plusieurs années dans une démarche de qualité orientée satisfaction de ses clients, et a été la seule entreprise de géolocalisation à avoir obtenu la double certification ISO 9001 & ISO 14001.

Les démarches qualité, sécurité et environnement apparaissent aujourd'hui comme des outils de de management efficaces et stratégiques pour faire face aux exigences des clients, à la concurrence, et aux exigences réglementaires.

Dans sa volonté de déployer une stratégie globale QSE, DEVERYWARE entame actuellement une démarche visant à certifier la sécurisation de ses systèmes d'information via la mise en place de la norme ISO 27001. L'objectif est d'assurer la cohérence de l'ensemble du dispositif de sécurité couvrant à la fois les dimensions techniques (matériels, logiciels, etc.) et organisationnelles (personnels, sites, procédures, etc.).

En effet, l'intégration des trois systèmes de management est une démarche assurant la pérennisation de l'activité et également l'amélioration des résultats. Elle permet de créer un équilibre entre la volonté de satisfaire les clients, de maîtriser les risques liés à la sécurité et d'intégrer au mieux les enjeux environnementaux.

Les projets sont conçus et développés conformément au processus [redacted] de l'ISO 9001.

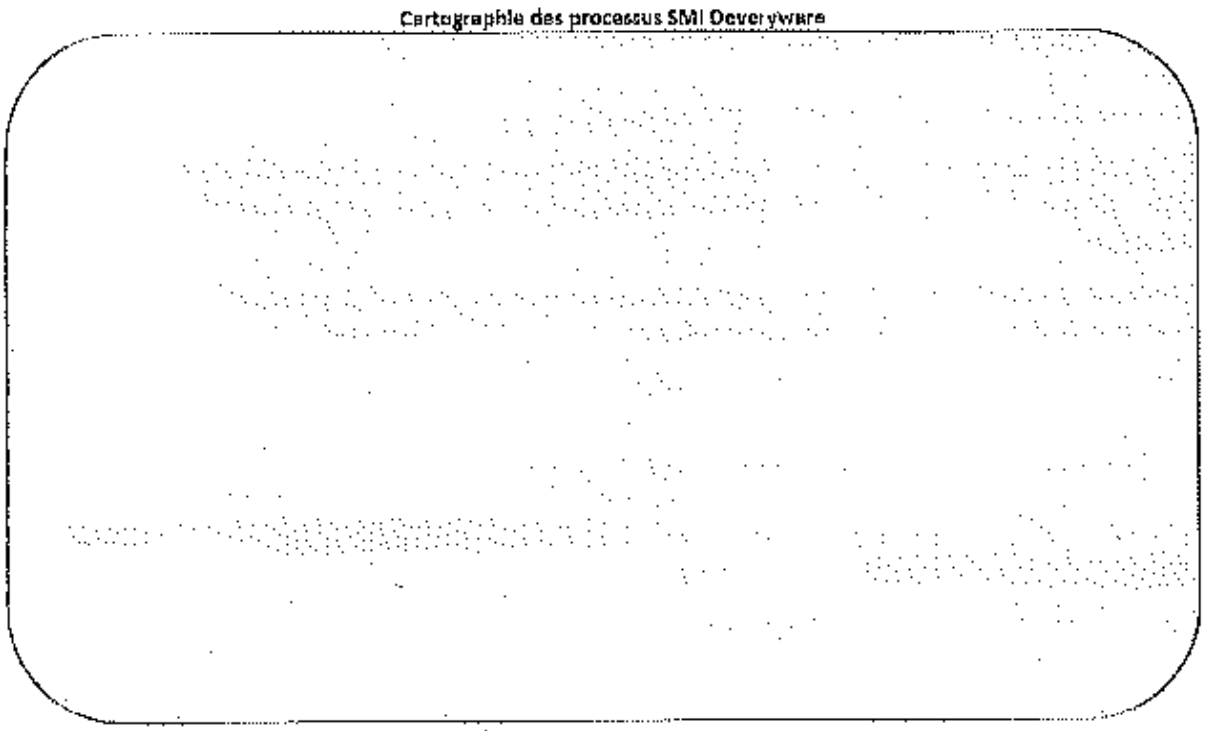


Figure 1 : cartographie de l'ensemble des processus certifiés de Deveryware

4.2 L'ORGANISATION PROJET DEVERYWARE

Deveryware assure la maîtrise d'œuvre du projet, elle assure :

- La conception et le développement du produit (participation à l'ergo-design)
- Le suivi de l'avancement des lots
- La définition et instruction des indicateurs projets pour préparation du reporting
- Le pilotage des sous-traitants
- La maîtrise des risques, des performances et des délais
- L'évolution logicielle
- L'assistance téléphonique (diagnostic d'un dysfonctionnement, assistance dans l'exploitation des applications, complément de formation au logiciel, etc.)

Le déroulement du projet suit une planification rigoureuse avec des jalons de validation et de livraison. L'objectif étant d'identifier toutes les tâches nécessaires à la réalisation du produit et à la conduite de projet.

Le projet est découpé en lots de travaux qui sont ainsi affectés aux entités les plus compétentes pour les réaliser. Les principales caractéristiques d'un lot sont : l'objectif de performance, le respect des coûts, le respect des délais, la définition des responsabilités.

La mise en place de l'organisation du projet se traduit par la diffusion de l'ensemble des expressions de besoins constituant des lots et par leur signature en tant qu'engagement sur le scope du lot de chacun des responsables de lot désigné. Dans le cas de la sous-traitance, le contrat et le bon de commande entre Deveryware et le sous-traitant, s'appliquent.

4.2.1 Phase de Préparation

C'est la phase d'initialisation et de construction du projet.

L'objectif de cette phase est de décrire l'organisation affectée au projet et le découpage en lots, chaque lot ayant des objectifs de performances, coûts délais et une responsabilité désignée.

La phase de préparation aboutit à la mise en place des équipes assurant la maîtrise d'œuvre, à la décomposition du projet en sous-tâches et à la définition des principales responsabilités.

Elle se termine par la revue de lancement de projet.

4.2.2 Phase de développement et exploitation

Elle est réalisée conformément au processus [redacted] » de l'ISO 9001.

Une équipe interne sous le pilotage du directeur technique travaille sur la partie serveur d'alerte et architecture du dispositif.

Deveryware travaille en équipe intégrée avec ses sous-traitants habituels pour la fourniture standard de certains lots. L'un concerne certains travaux sur le développement mobile, l'autre concerne l'évolution de l'interface graphique du back-Office.

Deveryware est responsable des étapes suivantes :

- Des spécifications techniques et fonctionnelles des composants du dispositif,
- De la conception des applicatifs ; des ateliers de travail réguliers ont été mis en place entre l'administration et Deveryware
- Du développement du dispositif
- De l'intégration et de la validation des composants du dispositif

Cette phase se termine par la recette client.

4.2.3 Phase de Formation

La formation est coordonnée et réalisée par le Product Manager auprès de l'administration. Elle est réalisée selon le processus [redacted]

4.2.4 Phase de maintenance applicative et assistance client

Elle est réalisée selon le processus [redacted]
L'organisation est décrite au chapitre 3.4.2 « Tierce Maintenance Applicative et assistance client »

4.3 ORGANISATION SPÉCIFIQUE AU PROJET SAIP

4.3.1 Équipes projet

L'organisation mise en place pour la réalisation du projet est une organisation matricielle classique :

Product Manager, responsable du projet	[redacted]
Responsable technique du projet	[redacted]
Responsable sous-traitance et gestion de projet	[redacted]
Product Owner partie Mobile	[redacted]
Product Owner partie backoffice	[redacted]
Product Owner partie Serveur	[redacted]
Responsable UX	[redacted]
Responsable Assistance Client	[redacted]

Le responsable du projet assure les rôles de pilotage du projet, de gestionnaire de contrat, aidé par un chef de projet responsable de la sous-traitance.

Le chef de projet établit le planning du projet, sur la base du référentiel des jalons, en cohérence avec les jalons contractuels et suivant les directives du responsable du projet.

Le responsable technique du projet propose et met en œuvre la solution technique.

Les PO pilotent la conception et la réalisation du produit conformément aux exigences du Product Manager en respectant les contraintes de qualité et de délais.

Le responsable UX propose l'ergonomie et le design du produit dans la première partie du projet, dans l'attente de la mise à disposition des éléments de design par l'administration.

L'équipe de développement application « SAIP », pilotée par le PO Mobile est constituée de :

- Un Scrummaster
- Quatre développeurs (2 androïd, 2 iOS)
- Un lead test

L'équipe de développement BO, pilotée par le PO Back office, est constituée de :

- Un Scrummaster
- Quatre développeurs

Une équipe « Serveurs » pilotée par le directeur technique :

- Un Architecte technique
- Un Responsable Mobile
- Un Référent Qualité Logicielle
- Deux Référents Exploitation
- Quatre développeurs

Cette équipe est responsable :

- de l'étude, de la documentation et mise en place de l'architecture serveur.
- De la définition des formats d'échange et/ou API avec le mobile
- De la réalisation des tests de charge côté serveur
- Du Développement côté Serveur

L'ensemble des équipes développent selon la méthodologie agile Scrum décrite dans le référentiel méthodologique de maîtrise des développements ref. « [redacted]

Pour les tâches réalisées avec des sous-traitants, Deveryware se réserve la maîtrise des éléments clés, en particulier la conception et validation de l'architecture.

Le sous-traitant est vu comme une équipe intégrée à Deveryware, et respecte donc strictement les règles méthodologiques appliquées aux équipes Deveryware. Le suivi détaillé du travail réalisé est totalement intégré au processus qualité de l'entreprise.

4.3.2 Responsable de la contractualisation

Le responsable de la contractualisation est le responsable du projet, Product Manager. Conformément au processus [redacted] le responsable du

projet aidé de son chef de projet, traitera tous les aspects contractuels client ou sous-traitant se rapportant au projet.

4.3.3 Meetings et revues

Le responsable du projet aidé de son chef de projet, organise les Comité de suivi et Comité de pilotage réguliers nécessaire à la bonne conduite du projet.

Le suivi du projet est effectué selon le processus [redacted] ».

Désignation	Responsabilité	Participants	Fréquence	Objet
COPIL	Responsable du projet	Client, acteurs projets	Non retenu vu la durée du marché	
Revue de projet	PO	Client, suivant thème	Suivant contrat	Avancement général Avancement des actions Planning Risques
Réunion sous-traitance	Responsable sous-traitance. Chef de projet	Chef de projet Sous-traitants	Suivant contrat Sous-traitant	Avancement technique Avancement des actions
Comité de suivi interne	PO	Equipes projet	Mensuelle	Avancement général Avancement des actions Planning Risques

6 PROPOSITION FINANCIÈRE

La proposition concerne la mise à disposition pour l'administration d'une application mobile d'alerte et d'information de la population et des services associés, destinée à couvrir une période du 20 mai au 15 juillet. L'offre inclut le maintien en condition opérationnelle du dispositif complet par période de 15 jours pour une durée de renouvellement de 45 jours maximum.

Le Poste 1 fera l'objet d'une facturation comprenant un acompte de 40% à l'issue de la vérification d'aptitude au bon fonctionnement (VABF)

Le poste 2 fera l'objet d'une facturation sur sa totalité à terme échu pour la période couvrant du 20 mai au 15 juillet 2016.

5.1 PRESTATION POUR LA PÉRIODE DU 20 MAI AU 15 JUILLET :

Poste 1 : Coût de production du dispositif	durée	Total HT

Poste 2 - Unité d'œuvre 1	durée	Total HT
Poste 2 - Unité d'œuvre 1 : Infrastructure - hébergement		
hébergement		
CDN (OptimiCDN/Cedexis)		
Poste 2 - Unité d'œuvre 1 - TMA		
TMA serveurs		
Astreinte 24h/24 7j/7		
Astreinte de niveau 1 - assistance client		
Astreinte de niveau 2 - DevOps		
Total Poste 2 - Unité d'œuvre 1 - Euros HT		

Grand Total Poste 1 et Poste 2 unité d'œuvre 1	**366 230,00 €**

5.2 COÛT POUR 15 JOURS CALENDAIRES DE PRESTATIONS

Les prestations éventuellement commandées sont à régler à terme échu dans leur totalité.

Poste 2 - Unité d'œuvre 2 : coût total pour 15 jours	[redacted]
Poste 2 - Unité d'œuvre 2 - TMA	
TMA serveurs pour 15 jours de prestations	
Poste 2 - Unité d'œuvre 2 - Infrastructure - hébergement	
hébergement	
CDN double	
Poste 2 - Unité d'œuvre 2 - Astreinte	
Astreinte de niveau 1 - assistance client	
Astreinte de niveau 2 - DevOps	
Total Poste 2 - Unité d'œuvre 2 - Euros HT	**6 247.00 €**

5.3 SIGNATURES ET ACCORD

Pour Deveryware SA

[redacted]

6 POLITIQUE DE SÉCURITÉ DE L'ÉDITEUR

Deveryware est une société dont le cœur de métier repose sur des technologies interconnectées au travers de l'Internet, et donc accessibles de l'extérieur afin de permettre un travail en réseau avec ses clients, ses partenaires, ses fournisseurs ou bien ses personnels. La croissance exponentielle des technologies de l'information, notamment dans le domaine des outils nomades (ordinateurs portables, téléphones mobiles, technologies « sans fil »), crée une vulnérabilité des systèmes internes de l'entreprise vis-à-vis d'attaques potentielles. Cette menace s'exerce sur tous les critères de la sécurité des systèmes d'information : la confidentialité, l'intégrité, la disponibilité, l'authentification, et la non-répudiation.

Principal fournisseurs des ministères [redacted] en solutions de géolocalisation de mobiles, Deveryware est particulièrement sensibilisé à la problématique de la sécurité des systèmes et réseaux d'information. Le cadre général régissant la SSI chez Deveryware est exprimé dans le document de référence « [redacted]

Ce document de politique de sécurité est un des éléments fondateurs qui définit les objectifs à atteindre et les moyens mis en place par l'entreprise pour y parvenir. Deveryware s'est notamment appuyé sur le document PSSI lors des négociations d'accès aux services des opérateurs de télécommunication en France et à l'étranger et pour guider notre choix des hébergeurs qui sont tous certifiés ISO 27001.

ANNEXE 1 : MATRICE DE CONFORMITÉ

La présente matrice de conformité reprend point par point les exigences de l'expression de besoin Euro 2016 du 21 avril 2016, et indique la conformité complète (C), partielle (PC) ou non-conformité (NC) du dispositif proposé dans la présente offre.

Ref EB	Exigence	Conformité	Dispositif Deveryware
Page1 – Poste 1 - I	La solution technique du titulaire doit permettre l'envoi par l'administration de messages d'alerte pour partie pré-enregistrés et leur réception par les usagers ayant téléchargé gratuitement l'application, dans la zone géographique ciblée par cette alerte.	C	Le dispositif permet à partir d'un éditeur en webservice de diffuser sur une zone géographique déterminée par l'autorité, un message pré-enregistré ou rédigé, et sa diffusion sur les smartphones présents sur la zone de diffusion, grâce à une application gratuitement disponible sur les stores.
Page 1 – Poste 1 -II	1) La solution technique ne doit nécessiter aucune constitution de base de données d'informations personnelles;	C	L'application est pleinement fonctionnelle sans nécessité de création de compte, d'enregistrement de données personnelles d'aucune sorte.
Page 1 – Poste 1 -II	2) Horodatage: Chaque message est horodaté au jour et à l'heure exacte locale (format: hh:mm) de l'envoi du message;	C	La date et l'heure du message de chaque alerte reçue sont clairement lisibles par l'usager
Page 1 – Poste 1 -II	3) Les message d'alerte, leur contenu, (quelle que soit la langue utilisée), leur design, et leur aspects graphiques sont à la charge de l'administration. A titre d'information, les types d'alertes et les contenus afférents sont joints au présent document;	C	Cette exigence ne s'applique qu'à l'application mobile, ainsi qu'aux logos utilisés sur l'IHM du webservice.
Page 1 – Poste 1 -II	4) l'alerte reçu par l'usager doit être visuelle et en fonction des situations, sonore ou silencieuse;	C	Le choix est déterminé par l'autorité émettant le message. Par défaut il n'y a pas de signal sonore accompagnant une alerte ORSEC
Page 1 – Poste 1 -II	5) Un serveur de diffusion de message d'alerte vers les applications des dispositifs mobiles mettant à disposition des utilisateurs les messages d'alerte géolocalisés (soit un cercle défini par un centre et un rayon, soit une zone fermée définie par une succession de points)	C	Une interface de création et de diffusion de messages d'alerte sur des zones géographiques de type circulaires ou polygonales fait partie du dispositif développé.
Page 1 – Poste 1 -II	6) L'interface de mise à disposition de l'administration doit permettre l'envoi de messages de manière simple et ergonomique	C	

Page 1 – Poste 1 -II	7) le dispositif développé doit être capable recevoir des messages d'un système extérieur en vue d'une diffusion vers l'application SAIP (application SAIP mobile)	C	Le système est conçu de manière être ouvert à d'autres plateformes pour échange de données d'alerte, au travers d'une API. Cette capacité ne faisant pas partie du périmètre du marché, elle n'a pas été testée.
Page 1 – Poste 1 -II	8) Le traitement de la géolocalisation au sein du terminal mobile est effectué localement, aucune information de géolocalisation ou donnée personnelle ne remonte au serveur de diffusion de l'alerte	C	Tous les traitements de localisation sont réalisés à bord du smartphone, aucune donnée n'est transmise en dehors du terminal.
Page 1 – Poste 1 -II	9) l'application comporte des bibliothèques de consignes de comportement fournies par l'administration. Chaque alerte renvoie vers le contenu, qui lui est associé	C	Les bibliothèques de consignes fournies par l'administration sont présentes à bord du smartphone pour garantir une disponibilité même en absence de réseau, et la consigne pertinente est présentée avec l'alerte reçue.
Pages1 à 2 Poste 1 -II	*1) Grâce à la géolocalisation:* Les personnes ayant téléchargé l'application, pour peu qu'elles aient consenti à autoriser la géolocalisation, doivent pouvoir recevoir les messages d'alerte les concernant lorsqu'ils sont présents dans la zone impactée par un attentat ou par un phénomène dangereux, en cours ou imminent, susceptible de mettre leur vie en danger s'ils n'adoptent pas les bons comportements de sauvegarde (rappelés dans les informations complémentaires jointes à l'alerte).	C	Un usager choisit si le mobile peut utiliser ou non sa localisation pour déterminer sa présence sur la zone de danger qu'il a reçue. S'il est localisé sur zone de danger une alerte explicite visuelle et sonore (sauf « alerte attentat ») l'informe de la situation.
Page 2 Poste 1 -III	*1) Grâce à la géolocalisation:* Cette alerte doit pouvoir être reçue dès que l'utilisateur pénètre dans la zone concernée. Le système informe l'utilisateur qu'il sort de la zone concernée et le prévient dès qu'il re-pénètre le périmètre de sécurité. L'application permet de localiser le dispositif mobile par rapport à la zone de diffusion de l'alerte avec une précision de 300 m à minima.	C	Une alerte est émise sur entrée en zone de danger, une information transmise sur sortie de cette même zone. La localisation est dépendante des conditions de réception et ne peut être garantie selon les zones géographiques. L'offre technique détermine la meilleure localisation possible en fonction des capteurs et senseurs disponibles au moment du calcul du point.
Page 2 Poste 1 -III	*1) Grâce à la géolocalisation:* La géolocalisation doit permettre à l'utilisateur de bénéficier des alertes concernant la zone géographique où il se trouve à chaque instant, mais que l'administration ne doit pas accéder à ces informations de géolocalisation.	C	Aucune donnée de localisation n'est exploitée en dehors du dispositif mobile, les zones de danger sont transmises au terminal qui vérifie localement s'il est présent ou non sur la zone considérée.
Page 2	*2) Via un paramétrage pré-déterminé par l'utilisateur:*	C	L'utilisateur peut choisir des codes postaux ou noms de

Poste 1 -III	L'utilisateur qui a téléchargé l'application doit pouvoir paramétrer la réception d'alerte émise par l'administration pour des zones géographiques de son choix. Ce paramétrage consiste alors à la pré-sélection par l'usager de zones géographiques spécifiques, (par exemple, lieu de travail, lieu de résidence secondaire...).		communes pour lesquels il souhaite recevoir une information en cas de survenue d'une alerte ORSEC.
Page 2 Poste 1 -III	*2) Via un paramètrage pré-déterminé par l'utilisateur:* Les notifications de l'application, pour cette catégorie, devront être clairement différenciées des alertes géolocalisées visées au paragraphe précédent, de manière à ce qu'il n'y ait pas de confusion possible, et une stricte hiérarchie entre l'alerte géolocalisée – qui nécessite un comportement réflexe de mise en sécurité – et l'information pour les zones géographiques sélectionnés, que ce soit la vigilance ou le relais d'alertes intervenant sur les communes renseignées par le détenteur de l'application	C	Les alertes sur géolocalisation (je suis au sein d'une zone de danger) sont clairement différenciées (sirène (sauf « alerte attentat »), fenêtre préemptive, vibration, pleine page de l'application) des informations d'alertes se déroulant sur des lieux favoris distants (liste de lieux + pictogrammes)
Page 2 Poste 1 -III	*2) Via un paramètrage pré-déterminé par l'utilisateur:* Une même personne pourrait référencer jusqu'à 8 communes différentes, le code postal servant alors de référentiel.	C	Le dispositif permet la gestion de 8 communes distinctes
Page 2 Poste 1 -III	*2) Via un paramètrage pré-déterminé par l'utilisateur:* L'alerte reçue doit être affichée sous une forme différente afin de ne pas être confondue avec l'alerte impérative concernant l'utilisateur du fait de sa présence dans une zone de danger.	C	Les alertes sur géolocalisation (je suis au sein d'une zone de danger) sont clairement différentiées (sirène (sauf « alerte attentat »), fenêtre préemptive, vibration, pleine page de l'application) des informations d'alertes se déroulant sur des lieux favoris distants (liste de lieux + pictogrammes)
Page 2 Poste 1 -III	*Exigences de disponibilité de l'application:* 1) La disponibilité de l'application doit tendre au maximum vers une disponibilité totale (24 heures sur 24 et sept jours sur sept)	C	Le dispositif est conçu pour être fonctionnel 24 heures sur 24 et sept jours sur sept. En cas de défaillance technique, le marché comprend une assistance de niveau 1 et 2
Page 2 Poste 1 -III	*Exigences de disponibilité de l'application:* 2) L'application déployée doit être opérationnelle sur l'ensemble du territoire national (France métropolitaine et départements et collectivités d'outre-mer), et cela dans les limites qu'offrent les magasins d'application.	C	L'application sera disponible sur l'ensemble des stores français, voire internationaux sur demande. A noter l'exception des Antilles Françaises, pour lesquelles un store spécifique doit être envisagé, Google ne permettant pas toujours la mise à disposition d'application française sur cette zone géographique
Page 2	*Exigences de disponibilité de l'application:*	C	Le dispositif est dimensionné pour permettre la diffusion d'un message d'alerte vers 3,3M d'utilisateurs, sur l'ensemble du

Poste 1 -III	3) L'hypothèse de volumétrie du téléchargement volontaire de l'application est de 5 % de la population française. Il peut donc être fixé comme limite supérieure. Compte tenu de la population en métropole et d'outre-mer, cela correspond à 3,3 M d'utilisateurs potentiels		territoire national.
Page 2 Poste 1 -III	*Exigences de disponibilité de l'application:* 4) Le temps de distribution d'une alerte pour 200 000 personnes présentes sur une zone de danger est de moins de dix minutes	C	Le dispositif est dimensionné pour qu'une alerte soit distribuée en moins de 10 minutes sur une population de 200 000.
Pages 2 et 3 Poste 1 -III	*Exigences de disponibilité de l'application:* 5) L'application doit être téléchargeable à tout moment via les magasins et « stores » applicatifs d'un maximum de fournisseurs, et obligatoirement via les services de téléchargement d'applications d'Android (Google) et iOS (Apple), dans les limites qu'offrent les magasins d'application.	C	L'application sera disponible sur l'ensemble des magasins français Apple Store et Google Play, voire internationaux sur demande. A noter l'exception des Antilles Françaises, pour lesquelles un store spécifique doit être envisagé, Google ne permettant pas toujours la mise à disposition d'application française sur cette zone géographique
Page 3 Poste 1 -III	*Exigences de disponibilité de l'application:* 6) L'application sera disponible pour un maximum de systèmes d'exploitation, et obligatoirement via deux principaux systèmes d'exploitation leader du marché, Android et iOS (Apple)	C	Le dispositif est disponible sous iOS et Android.
Page 3 Poste 1 -III	*Exigences de disponibilité de l'application:* 7) À partir de la validation du message d'envoi par l'autorité, celui-ci doit être mis à disposition des utilisateurs en moins de une minute.	C	Le message est mis à disposition des usagers en moins de dix secondes.
Page 3 Poste 1 -III	*Exigences de disponibilité de l'application:* 8) L'application ayant vocation à rester active (en premier plan ou arrière-plan), son impact sur la consommation d'énergie doit rester faible	C	Le concept du dispositif fait que la consommation de l'application doit être largement inférieure à 5% si aucune alerte n'est active. Ce point est un des constituants du brevet protégeant le dispositif
Page 3 Poste 1 -III	*Exigences de disponibilité de l'application:* 9) Le titulaire doit assurer la comptabilité du système en cas d'upgrade d'Android et iOS (Apple)	C	Le marché intègre un lot de tierce maintenance applicative qui couvre des évolutions d'iOS et Android (une majeure et une mineur par an et par OS)
Page 3 Poste 1 -IV	*Caractéristiques concernant le déclenchement de l'alerte* Le titulaire est informé que, dans un premier temps, seul le COGIC (Centre opérationnel de gestion interministériel de crise, Rue de	C	Le dispositif est conforme en ce point, sur cette exigence très particulière et liée au contexte de l'Euro 2016. Chaque poste opérateur pourra interagir sur les évènements créés par les

	Miromesnil à Paris) sera habilité à utiliser l'application de diffusion des alertes. Dans ce cadre, dix accès simultanés sur poste fixe sont nécessaires. Ces accès ne seront pas nécessairement différenciés, chaque poste devra pouvoir avoir accès et gérer les alertes émises par les autres postes.		autres postes, et chaque poste peut gérer un évènement distinct sur une zone géographique distincte des autres postes (cas de groupes de gestion de crise gérant un lieu par poste)
Page 3 Poste 1 -IV	*Caractéristiques concernant le déclenchement de l'alerte* Un déploiement ultérieur au niveau national, pouvant couvrir jusqu'à 500 points d'émission, (données prévisionnels non contractuels) doit être possible	C	L'architecture fondamentale du dispositif permet de gérer une organisation hiérarchique de type nationale (échelon national, préfectures, mairie) avec un cloisonnement strict entre chaque compte
Page 3 Poste 1 -V	Autres caractéristiques attendues: 1) l'application doit permettre d'accéder aux conseils sur les comportements à adopter face aux événements divers auxquels on peut faire face. Ces conseils sont actuellement repris par le site internet www.risques.gouv.fr. ... ... En complément et pour éviter la congestion du réseau internet pendant la crise, une bibliothèque simplifiée de fiches de risques sera téléchargée sur chaque terminal et accessible durant la crise au sein de l'application, sans besoin de connexion opérationnelle.	PC	Seul l'accès aux fiches comportementales liées aux risques est pris en charge par le dispositif.
Page 3 Poste 1 -V	*Autres caractéristiques attendues:* *2) L'architecture de la solution technique doit pouvoir répondre* Un serveur de diffusion de message d'alerte vers les applications des terminaux mobiles met à disposition de tous les téléphones les messages d'alerte géolocalisés (soit un cercle défini par un centre et un rayon, soit une zone fermée définie par une succession de points)	C	Le dispositif met en œuvre un serveur de diffusion de messages d'alerte géolocalisés, capable de servir l'ensemble des mobiles utilisant l'application SAIP
Page 3 Poste 1 -V	*Autres caractéristiques attendues:* *2) L'architecture de la solution technique doit pouvoir répondre* L'application ne doit pas impacter significativement la consommation data et la batterie de bord;	C	Le dispositif breveté permet de maintenir la consommation batterie à un pourcentage très inférieur à 5% par jour en période sans incident. En cas d'alerte, le niveau de consommation reste très faible.
Page 3 Poste 1 -V	*Autres caractéristiques attendues:* *2) L'architecture de la solution technique doit pouvoir répondre* Si une nouvelle alerte est publiée, l'application vérifie si le possesseur du téléphone est concerné ou pas, soit au titre de sa	C	Le dispositif permet à chaque terminal mobile doté de l'application SAIP de vérifier s'il est concerné par une alerte le menaçant directement, ou bien sur un de ses lieux favoris.

	position physique, soit au titre de ses choix de paramétrages d'information;		
Page 3 Poste 1 -V	*Autres caractéristiques attendues:* *2) L'architecture de la solution technique doit pouvoir répondre* Le traitement de la géolocalisation est effectué localement, rien ne remonte aux serveurs de diffusion de l'alerte de l'administration;	C	Tous les traitements de localisation sont réalisés à bord du smartphone, aucune donnée n'est transmise en dehors du terminal.
Page 4 Poste 1 -V	*Autres caractéristiques attendues:* *2) L'architecture de la solution technique doit pouvoir répondre* En cas d'alerte, le terminal, affiche le message d'alerte. Le système continue à consulter la liste pour vérifier si un message modificatif d'alerte a été émis	C	Le dispositif permet l'affichage d'une alerte sur évènement dès que l'usager est détecté présent sur une zone de danger. Il permet en outre de détecter la survenue d'un nouveau message relatif au premier évènement pour l'afficher en remplacement du premier message, comme suite logique.
Page 4 Poste 1 -V	3) Une personne qui reçoit une alerte géolocalisée ou une information par paramétrage doit pouvoir avoir la possibilité, si elle le souhaite, de la retransmettre à des proches, via les réseaux sociaux. C'est la « viralisation » de l'alerte. Cette retransmission doit pouvoir se faire au niveau des écrans d'alerte (source citée).	C	Le dispositif permet sur demande de l'usager de renvoyer l'alerte, depuis le niveau des écrans d'alerte, vers le compte twitter ou facebook de l'usager, afin de faciliter la dissémination de l'alerte.
Page 4 Poste 1 -V	L'application téléphonique doit donc offrir la possibilité, optionnelle, d'enregistrer ses différents profils sur les principaux réseaux sociaux, dont Facebook et Twitter.	C	La solution permet la dissémination des messages d'alerte sur Facebook et Twitter selon des mécanismes classiques d'émission ne nécessitant pas la détention des profils par l'application SAIP.
Page 4 Poste 1 -V	Le téléchargement et l'installation de l'application par un l'utilisateur de l'application SAIP, doit être l'occasion de l'éclairer et de recueillir son consentement, conformément aux meilleures pratiques en cours.	C	L'usager qui lance l'application pour la première fois se voit proposer les CGU puis peut accepter ou refuser de recevoir des notifications, accepter ou refuser de laisser l'application SAIP utiliser la géolocalisation bord.
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 1) La mise en oeuvre de mécanismes d'identification et d'authentification efficaces de l'utilisateur chargé d'émettre l'alerte (notamment via les solutions préconisées par l' ANSSI);	C	[redacted]
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 2) Le chiffrement des échanges en utilisant des solutions préconisées par l'ANSSI (durcissement des configurations serveurs,	C	[redacted]

	pare-feux et chiffrement IP).		[redacted]
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 3) La sécurisation de la solution technique de manière à pouvoir faire face aux attaques classiques de type DDoS (déni de service). L'utilisation de pare-feux et des répartiteurs de charges pourront contribuer à absorber certaines attaques.	C	Mise en place d'une solution d'aiguillage DNS (Cedexis) et d'un double CDN (OptimiCDN) pour absorber et faire face aux attaques DDoS. [redacted]
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 4) Aucune remontée sur la position géographique des connexions au serveur d'alerte, sur le nombre de requêtes à intervalle donnée, sur les paquets et leur contenu.	C	Aucune information n'est remontée des smartphones, et aucune sonde d'analyse de flux utilisateurs n'est mise en place.
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 5) L'impossibilité de toute décompilation du code et de rétro-ingénierie d'une partie de l'architecture informatique de l'administration;	C	La décompilation du code mobile est astreinte aux limites des outils du marché. Le dispositif issu de ce marché ne reposant pas sur l'architecture informatique de l'administration cette exigence est respectée.
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 6) Une obligation de moyen de rendre difficile l'usurpation d'identité et d'usage malveillant de l'application (comme un déclenchement par un tiers de fausses alertes)	C	Le dispositif propose une triple sécurité reposant sur : - la notification par push d'une alerte identifiée de façon unique - l'analyse de correspondance de l'identifiant de l'alerte notifiée et du message d'alerte en base - signature de l'alerte par certificat SHA2
Page 4 Poste 1 -VI	*Sécurité et hébergement. Il est attendu du titulaire :* 7) La mise en œuvre à compter de la notification du marché, des mesures administratives et techniques nécessaires à l'homologation de la solution technique aux exigences du système SAIP. Ces démarches sont réalisées en étroite collaboration avec l'administration.	C	Deveryware se tient à la disposition de l'administration pour travailler à l'homologation de la solution technique.
	Sécurité et hébergement. Il est attendu du titulaire : Le système d'information utilisé dans le cadre de la prestation devra être dédié au profit du Ministère de l'Intérieur ('tenant' dédié).	C	Deveryware a créé un tenant dédié au ministère de l'Intérieur chez Numergy/ OpenStack
	Sécurité et hébergement. Il est attendu du titulaire :	C	Un fichier binaire des applications Android et iOS sera remis

	La société DEVERYWARE s'engage à communiquer le code de son application afin de permettre une analyse statique.		aux autorités pour analyse statique
	Afin de permettre la mise en œuvre de la gestion d'incident SSI, la société DEVERYWARE s'engage à fournir un contact technique dans le cadre de l'astreinte SSI.	C	Un contact technique associé à l'astreinte SSI sera désigné.
Page 4 Poste 1 -VII	*Hébergement de la solution technique du titulaire* : L'hébergement de la solution technique est à la charge du titulaire. L'ensemble des actions du titulaire dans sa mission d'hébergement doit garantir une continuité de service et une disponibilité de l'application totales. A ce titre, il peut par exemple proposer un hébergement de secours.	C	Pendant la durée du marché le service d'hébergement sera géré par nos soins avec l'assentiment des SSI du ministère de l'intérieur.
Page 4 Poste 1 -VII	*Hébergement de la solution technique du titulaire* : Toutefois, le titulaire est informé qu'à terme, les services de la direction des systèmes d'information et de communication (DSIC) du Ministère de l'intérieur pourront assurer l'hébergement.	C	Le dispositif est très simplement transposable sur les moyens techniques de la DSIC.
Pages 4 et 5 Poste 1 -VII	*Hébergement de la solution technique du titulaire* : Précision sur le(s) cahier(s) de test et la démarche de qualité concernant la vérification d'aptitude au bon fonctionnement de l'application mobile : Le titulaire transmet aux agents de l'administration toute information pertinente leur permettant de vérifier l'aptitude au bon fonctionnement de l'application mobile, et cela dans les règles de l'art.	C	Nous nous engageons à apporter notre soutien aux phases de test de l'administration et à leur fournir tous les éléments nécessaires
Page 5 Poste 2	*Poste 2: Maintenance corrective et évolutive de la solution technique du titulaire, accompagnement et formation:* 1) Le titulaire met en œuvre une solution de maintien en condition opérationnelle de l'application, et de l'ensemble des éléments d'infrastructure permettant un fonctionnement normal de la solution applicative.	C	La maintenance en condition opérationnelle est assurée pendant toute la durée du marché, et pour un maximum de 45 jours au-delà si des bons de commande venaient à être émis.
Page 5	3) Le titulaire met à disposition de l'administration une solution d'accompagnement des utilisateurs du dispositif émetteur de	C	Une session de formation de formateurs est planifiée pour le lundi 23 mai après-midi, et un guide de prise en main rapide

Poste 2	l'alerte. Cet accompagnement se traduira par une session de formation des personnels du COGIC pressentis pour utiliser le dispositif pendant la durée du marché, et par la remise d'un guide d'usage de l'émetteur.		sera fourni au format numérique. L'administration pourra le dupliquer et l'utiliser auprès de ses personnels sans restrictions. En cas de besoin, une assistance client de niveau 1 peut porter assistance 24h sur 24 et 7jours sur 7 pour la prise en main du dispositif.
Page 5 Poste 2	4) Le titulaire met à disposition un outil de gestion de suivi des anomalies, qui permettra aux agents de l'administration utilisant le dispositif (émetteur ou récepteur) lors des phases de recette ou de service régulier, de communiquer sur des anomalies rencontrées, et de préciser le niveau de criticité de l'anomalie.	C	L'administration aura accès à l'outil de gestion des anomalies de l'entreprise et pourra y instruire les dysfonctionnements constatés durant les phases d'évaluation et au-delà.
Page 5 Poste 2	5) Centre de support aux utilisateurs (émetteurs de l'alerte) ou hotline: À ce titre, le titulaire propose une solution de support à l'utilisateur en temps réel. Les interlocuteurs doivent connaître les principales caractéristiques de l'application et de l'infrastructure de l'application. Le support utilisateur intègre un dispositif d'astreinte 24h/24, sept jours sur sept.	C	Un service de support client de niveau 1 et niveau 2 est mis en place afin d'assurer une astreinte 24h/24 7jours/7.

ANNEXE 2 : DESCRIPTIF SUCCINCT DES TRAVAUX RÉALISÉS POUR LE DÉVELOPPEMENT D'UN DISPOSITIF D'ALERTE DE LA POPULATION

Cette annexe présente à titre d'information une vision macroscopique des différentes tâches qui ont conduit au développement d'un système d'alerte et d'information de la population, dans le cadre de travaux de recherche et développement.

Développement application mobile

Sprint 1

- Mise en place de l'environnement de développement.
- Installation et paramétrage des outils:
  - [redacted] Création du projet, gestion des comptes.
  - [redacted] Mise à jour avec les dernières bibliothèques utiles.
  - [redacted] Installation et configuration.
  - [redacted] Installation et configuration.
  - [redacted] Installation et configuration.
  - [redacted] Installation et configuration.
- Serveur de DEV
  - Paramétrage et accès à un compte NUMERGY.
  - Création d'une VM.
- [redacted] – développement du script de déploiement pour l'Intégration Continue sur le serveur de DEV.
- Ateliers expression de besoin / estimation backlog
- Création des stores DW, des outils de reporting qualité

Sprint 2

- Alertes sur position (2 OS)
- Intégration crashlytics (2OS)
- Gestion de zones circulaires
- Design Deveryware

Sprint 3

- Alertes sur position : gestion de zones polygonales
- Alertes sur abonnement : gestion des communes
- Publication par le serveur
- Intégration design SIG

Sprint 4

- Consolidation alertes sur abonnement / polygones
- Gestion multilingue

- Intégration des alertes sonores
- Gestion des fiches de comportements
- Gestion des notifications (sur zone, sur fin de crise)
- Intégration design
- Résorption dette technique

Sprint 5

- Utilisation et contenu mobile
- Gestion des abonnements : réception des messages
- Sortie de zone
- Notification code postal
- Gestion de fin de crise
- Dissémination réseaux sociaux
- Cheminement – menu burger
- Gestion GCM
- Gestion soumission messages

Développement BackOffice

Sprint 1

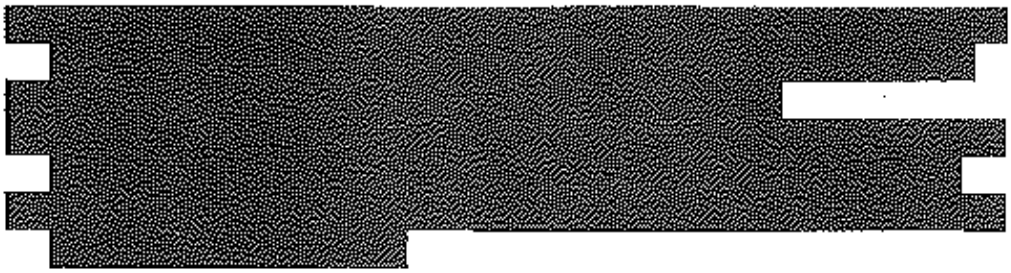
- Mise en place de l'environnement de développement.
- Installation et paramétrage des outils:
  - [redacted] -- Création du projet, gestion des comptes.
  - [redacted] - Mise à jour avec les dernières bibliothèques utiles.
  - [redacted] - Installation et configuration.
  - [redacted] - Installation et configuration.
  - [redacted] - Installation et configuration.
  - [redacted] - Installation et configuration.
- Serveur de DEV
  - Paramétrage et accès à un compte NUMERGY.
  - Création d'une VM.
- [redacted] – développement du script de déploiement pour l'Intégration Continue sur le serveur de DEV.

Sprint 2

- Description d'une alerte : niveau, catégorie, gestion des erreurs, environnement multilingue
- Liste des alertes : historique des alertes clôturées, Tableau des alertes courantes, recherche textuelle étendue sur langue anglaise,
- Mécanismes de diffusion nationale

Sprint 3

- Gestion des communes :

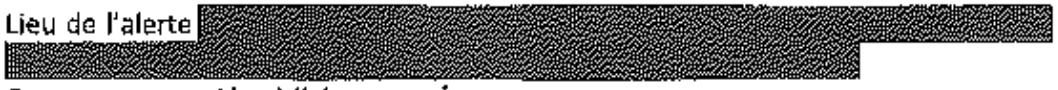


- Messages prédéfinis :

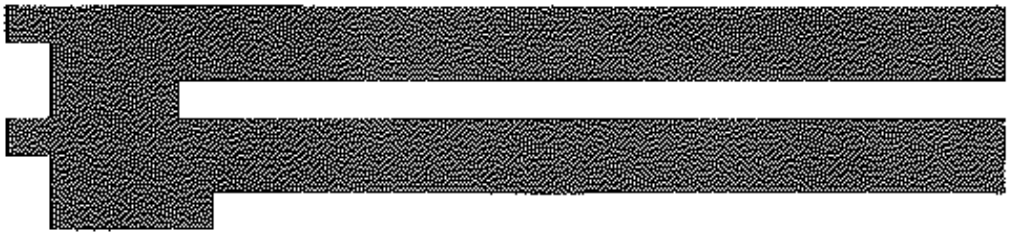
- Son associé à l'alerte : liste de choix pour chaque message d'alerte, présélection sur « pas de son »

Sprint 4

- Lieu de l'alerte



- Communes associées à l'alerte :



- Habillage du site
- Mise en place du logo définitif et du nom de l'application.
- Mise en place du logo et du nom de l'autorité en charge de saisir les alertes.
- Habillage de l'écran de connexion.

Sprint 5 :

- Consolidation
- Finition habillage site
- Testing – correction

Développement architecture dispositif

- étude et conception architecture du dispositif
- définition et mise en place des environnements virtuels « intégration continue », « intégration », « pré production », « production » pour les parties serveur
- construction de l'usine logicielle du projet serveur et mobile (iOS, Androïd)
- développement du robot de déploiement des environnements
- mise en place des espaces de collaboration des équipes (voix, vidéo, wiki, messagerie instantanée, email)
- définition de l'architecture, et documentation

- spécification du format des alertes
- intégration, et configuration du système de gestion de files de messages
- définition et développement du processus de scellé pour les alertes
- modélisation des zones (cercles, polygones)
- configuration et installation des certificats pour les environnements « intégration continue », « intégration », « pré production »
- définition du modèle de stockage
- développement communication [redacted]
- intégration d'un service de partage de fichiers
- intégration service web de publication
- intégration des outils de supervision
- définition et mise en œuvre des VPN d'accès

Lot « opérations » et SSI

- Installation / Configuration / Automatisation des serveurs webs
- Installation / Configuration / Automatisation du système de partage du fichier [redacted] alerte
- Installation VPN pour l'environnement de production [redacted]
- Choix d'une solution haute-disponibilité de CDN
- Installation de l'architecture CDN
- Configuration DNS & Certificats
- Mise en place d'une solution de supervision système et réseau
- Mise en place d'une solution de sauvegarde

ANNEXE 3 : PROTOCOLE SSI DÉFINIS ENTRE LES PARTIES