

## SOLUTION SHAPPER

**Shapper** est un générateur d'applications mobiles natives. Shapper se pilote sur le principe d'une solution "cloud" accessible depuis un navigateur web, sans connaissance en programmation, permettant ainsi :

- la **création d'une application mobile** native pour smartphones et tablettes iOS (iPhone, iPad) et Android, accessible depuis les stores publics ou privés,
- le choix du **design graphique** pour personnaliser l'App à ses couleurs,
- la définition des **fonctionnalités intégrées** à l'App,
- la **gestion du contenu et des fonctions** en temps réel.

L'application mobile générée par Shapper peut s'adresser au grand public, être orientée "métier" ou les deux à la fois avec une partie publique et une partie privée.

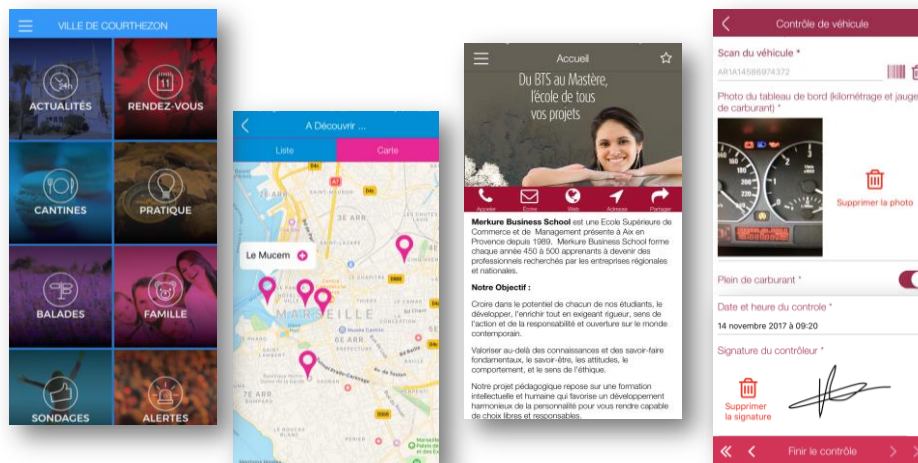
Les applications générées via Shapper, permettent aux organismes d'accroître leur communication (informer, alerter, fédérer, interagir, ...) n'importe où, n'importe quand. Les organismes ciblés sont par exemples des PME, des collectivités territoriales, des commerçants, des associations, des organisations souhaitant mettre en œuvre une stratégie mobile.

Auprès de grands comptes, Shapper, plateforme de création d'applications sans connaissance en programmation (appelée également les NC/LC App c'est-à-dire les « No-Code / Low-Code » App) suscite une attention, un intérêt croissant par les unités métiers de l'entreprise et une double opportunité pour les DSI :

- Favoriser une meilleure coopération entre l'IT et les métiers de l'entreprise, basée sur une approche pragmatique.
- Libérer des budgets et ressources en développement pour d'autres projets.

car Shapper offre :

- une rapidité de mise en œuvre,
- une agilité d'adaptation en fonction des retours terrains,
- des coûts plus faibles en investissement et exploitation,
- une stratégie adaptée et étendue d'habilitations, pour proposer des fonctions et services différenciés selon les profils utilisateurs aussi bien pour l'administration de la plateforme, que pour chaque application
- une architecture sécurisée permettant l'interopérabilité avec des sources ou systèmes d'information externes
- un avantage « métier » et concurrentiel en matière de productivité et de qualité de service.



## ETENDUES FONCTIONNELLES

Shapper propose des applications natives iOS (Apple) & Android (Google) avec une grande étendue fonctionnelle pour proposer aux mobinautes une application en adéquation avec leurs attentes :

- Administrable en ligne via un Back Office Web. Gestion des droits par gestion de rôles
- Gestion multilingue
- Gestion du contenu – Editeur de texte (WYSIWYG)
- Gestion de l'arborescence sans limite
- Affichages variés : Page, Liste, Grille, Bannière, Cardview, ...
- Affichage de points d'intérêts, Géolocalisation
- Affichage d'adresse avec itinéraire
- Partage de contenu : réseaux sociaux/Mail/SMS
- Gestion des mobinautes, Compte avec profil personnalisable
- Contenus et fonctions publics et privés (gestion des habilitations par groupe de mobinautes)
- Campagne d'annonces via interstitiel et bandeaux
- Vues graphiques
- Moteur de recherche interne
- Gestion des favoris
- Clic to Call / Clic to Mail
- Navigateur web intégré
- Visionneuse PDF
- Player Vidéos Youtube
- Envoi de notifications push via listes de diffusion paramétrables (critères profil mobinaute)
- Statistiques de consultation
- Scan de QR Code pour un accès direct au contenu
- Formulaire personnalisés avec divers types de données (texte, liste à choix unique ou multiple, date, heure, numérique, case à cocher, photos, scan de code, signature numérisée, position GPS, ...)
- Gestion Beacons et/ou Géofencing (Message de proximité, Offre promotionnelle, Parcours découverte, ...)
- Cache local pour consultation hors-ligne
- E-boutique, catalogue, gestion de panier, système de fidélité
- Système de paiement via carte bancaire et achat in-app
- Connecteurs bidirectionnels de données via webservices
- ...

## APPROCHE PROJET

Le début des études et de la conception de la solution Shapper remonte à 2014. La première version commercialisable date de fin 2016. Après une phase importante en matière de modélisation conceptuelle afin de bâtir une architecture modulaire, évolutive et sécurisée. La méthodologie projet s'appuie aujourd'hui sur une approche Agile avec des cycles itératifs (backlog) permettant d'implémenter et de mettre en production de nouvelles fonctionnalités régulièrement. Cela permet de répondre aux demandes, besoins et contraintes des clients.

## ARCHITECTURE LOGICIELLE

La solution Shapper est conçue en s'appuyant sur des technologies standards et reconnues s'articulant sur une architecture logicielle modulaire orientée objet permettant de garantir :

- La répartition de la solution en modules logiciel interdépendant
- La sécurisation de la solution, des données et des flux
- La scalabilité assurant une montée en charge
- L'évolutivité fonctionnelle de la solution

La modularité des couches applicatives serveur permet de séparer et répartir (load-balancing) les traitements suivants en plusieurs strates :

- Couche données Database
- Couche données fichiers (illustrations, PDF, ...)
- Couche webservices de communication avec les applications mobiles
- Couche webservices connecteurs
- Couche web Back Office (BO)
- Couche web Front Office

La solution Shapper est développée dans le respect des normes des constructeurs afin de respecter l'expérience utilisateur sur chaque système d'exploitation.

Les langages utilisés sont :

- Objective-C, Swift pour iOS, architecture MVC
- Java, Kotlin pour Android, architecture MVC
- PHP, architecture MVC
- HTML5 et CSS3
- JavaScript, et le Framework jQuery
- MySQL, pour les bases de données
- Framework: CodeIgniter, Cake PHP

Les applications sont développées avec les composants et bibliothèques standards afin de garantir au maximum les compatibilités avec les versions ultérieures des OS mobiles.

## **EXIGENCES APPLIQUEES A LA SOLUTION SHAPPER**

### **Exigence de performance**

Une attention particulière est définie du point de vue des performances, afin d'obtenir :

- Des temps de réponse et de chargement rapides (en fonction des débits de la connectivité)
- La capacité de supporter la montée en charge d'utilisation (consultation, stockage)

### **Exigence ergonomique**

La solution propose aux utilisateurs des interfaces simples, intuitives et optimisées pour permettre une navigation aisée à travers le back office et l'application.

La priorité ergonomique est de présenter un accès rapide aux informations et fonctionnalités et de privilégier des saisies rapides

Le succès d'une solution est largement dû à son ergonomie. Afin que les utilisateurs adoptent rapidement la solution, elle s'appuie sur les grands principes des interfaces préconisés par les constructeurs, les usages, les tendances et la rapidité de saisie des informations.

### **Exigence d'évolutivité et de maintenabilité**

A travers les choix conceptuels et techniques, la solution est à la fois pérenne et évolutive dans le temps aussi bien sur les aspects fonctionnels que technologiques.

L'implémentation de la solution facilite la maintenance préventive et corrective ainsi qu'une possibilité de montée en charge.

Les contraintes imposées sont :

- Simplicité, modularité et factorisation du code
- Utilisation de composants et technologies standards

- Documentation technique, Code lisible et commenté
- Architecture technique flexible pour assurer les capacités d'ouverture

## Exigence de sécurité

Synertic accorde une importance prioritaire dans la sécurisation des solutions qu'elle conçoit et réalise et notamment la solution Shapper. Cette exigence permet de garantir une :

- Surface d'attaque minimaliste
- Intégrité des données échangées
- Confidentialité des données sensibles
- Fiabilité maximale

afin de réduire les risques tels que :

- Destruction et falsification de données
- Vol de données
- Détournement applicatif
- Indisponibilité
- Résultats non-conformes
- Erreurs en cascade
- ...

Une démarche sécurité applicative est systématiquement opérée via une approche « **Security by Design** », c'est-à-dire que la sécurité est appréhendée comme une fonctionnalité de la solution et donc prise en compte dans l'ensemble des phases projet.

Des inspections « Sécurité » sont effectuées régulièrement à chaque phase ou fin de processus d'itération.

- Revue de spécification
- Revue de conception
- Revue de code
- Revue de recette (tests d'intrusion et de vulnérabilité)

L'analyse sécuritaire a pour but d'aider les spécifications conceptuelles en matière de sécurité. Les objectifs d'une analyse sécuritaire sont :

- Identifier les ressources
- Aider à identifier les vulnérabilités de la solution
- Évaluer les menaces et failles relatives à la solution
- Réduire les risques globaux à l'égard de la sécurité
- Permettre d'établir la base des spécifications de conception en matière de sécurité

Un référentiel de bonnes pratiques est utilisé lors de la phase de réalisation, parmi lesquelles :

- Contrôle et validation des saisies utilisateur
- Contrôle systématique des codes de retour
- Exécution avec le moins de privilèges possibles
- Interception des exceptions
- Gestion du transactionnel
- Non stockage d'informations sensibles ou confidentielles en 'clair'
- Contrôle et évaluation des capacités des ressources techniques avant les traitements complexes
- Gestion appropriée des messages d'erreur et de logs pour éviter les messages utiles pour un attaquant
- Prévoir l'échec et échouer en mode sécurisé. Gestion des cas improbables et des exceptions
- Gestions des modes dégradés
- Traçabilité des actions et des échanges
- ...

## HEBERGEMENT SOLUTION SHAPPER

---

Les solutions et services Shapper sont hébergés sur des plates-formes avec une qualité de service de haut niveau grâce à des accords passés avec la société Digital Network opérant plusieurs datacenters à niveau de tolérance maximale. L'infrastructure hébergée dédiée à la solution Shapper est localisée dans

- un Datacenter à Aix en Provence, région PACA (France)
- répliqué dans un Datacenter à Gravelines, région Hauts-de-France (France)
- sauvegardé dans un Datacenter à Strasbourg, région Grand Est (France)

Le service comprend :

- L'hébergement des services connectés, modules et systèmes nécessaires à la solution sur la plateforme technique du Datacenter
- La supervision quotidienne intégrant les actions d'infogérances des serveurs et éléments réseaux hébergeant les services de la solution
- La sauvegarde des données et systèmes
- L'administration et le Support technique



## LES INFRASTRUCTURES

Les infrastructures reposent sur une approche basée sur 4 critères : la performance, la disponibilité, la simplicité et la flexibilité.

L'ensemble de ces critères est piloté par une même gouvernance : la sécurité

- **Disponibilité** : chaque unité est composée de plusieurs serveurs RAID Hardware, double alimentation, équipés de 2x10 Gb/s connectés à 2 réseaux 10 Gb/s (un réseau de stockage + un réseau de production privé isolé dans un Vrack). L'ensemble des équipements réseaux desservants ces infrastructures est redondant.
- **Performance** : chaque unité est équipée de 48 à 512 cœurs physiques et connectée à des stockages réseau ZFS redondants de 26 TB composés de deux baies redondantes de 44 disques complétés par des SSD utilisés en cache ainsi que deux têtes (maître et esclave) afin d'assurer une haute disponibilité du stockage. L'affectation des ressources reste limitée à 75% afin d'assurer une performance maximale.
- **Flexibilité** : il est possible de modifier en quelques minutes la capacité des services d'infrastructure de manière à s'adapter à la croissance des clients.

### Le PRA

Situé au sein du Datacenter OVH de Gravelines, les infrastructures PRA sont connectées via un réseau privé 10 Gb/s aux infrastructures de production. Elles reposent sur les mêmes briques technologiques mais utilisent volontairement une approche d'infrastructure totalement différente : afin d'assurer une compartimentation aussi bien pour des raisons d'apparition de bug que de sécurité, les infrastructures PRA utilisent un stockage local mixte (Disques dur & SSD NVMe), ainsi qu'une approche par répartition au lieu d'une approche clusterisée.

### Le Backup

Situé au sein du Datacenter OVH de Strasbourg, les infrastructures de backup sont connectées via un réseau privé 10 Gb/s aux infrastructures de PRA et de production.

L'infrastructure de backup est composée de serveurs équipés chacun de 12 disques SAS de 6To en RAID 10 afin d'assurer un niveau de redondance maximal (niveau similaire à la production) ainsi que

d'un SSD monté en LSI cachecade sur le contrôleur RAID afin d'assurer des performances lecture/écriture optimales lors des backups.

3 niveaux de backup sont exécutés :

- 1) Hyperviseur : toutes les 24H les instances sont intégralement backupées sur le site de Strasbourg avec une rétention glissante de 7 jours.
- 2) Stockage : Un snapshot ZFS des disques des instances est effectué à intervalle régulier (h-1, h-6, j-1, j-2, j-3)
- 3) Système : Un backup au niveau applicatif (rdiff-backup avec une rétention standard de 30 jours upgradable à plusieurs années, dumps base de données est exécuté toutes les 24H

## DATACENTERS

### Sécurité :

- Périmètres sécurisés via des clôtures équipées de barbelés.
- Système de vidéo-surveillance et de détection de mouvement en continu
- L'activité à l'intérieur et à l'extérieur des Datacenters est monitorée et enregistrée sur des serveurs sécurisés.
- Des équipes de surveillance se relaient 24H/24 et 7j/7.
- L'accès aux datacenters n'est pas autorisé aux clients.
- L'accès aux datacenters se fait via un badge RFID nominatif auquel sont associés les droits d'accès.
- Pour accéder aux locaux, chaque employé doit soumettre son badge à une vérification et traverser un sas sécurisé.

La gestion de la sécurité, l'évaluation des risques et les traitements associés s'appuient principalement sur les normes ISO 27002 et ISO 27005.

### Gestion des risques incendie

Chaque salle de chaque datacenter est équipée d'un système de détection et d'extinction d'incendie ainsi que de portes coupe-feu. Les installations des extincteurs portatifs et mobiles, sont faites dans le cadre du respect de la règle APSAD R4. Tous les datacenters possèdent le certificat de conformité N4.

### Alimentation électrique

Chaque datacenter est alimenté par deux arrivées électriques indépendantes l'une de l'autre. Ils sont également équipés d'onduleurs 250 KVA chacun, ainsi que de groupes électrogènes d'une autonomie initiale de 48H afin de pallier toute panne des réseaux de fourniture d'électricité.

### Réseau

Chaque datacenter est équipé au minimum de 2 arrivées réseaux indépendantes. Chaque datacenter dispose de 2 salles réseaux jumelles capables chacune de prendre le relais de l'autre.

Les infrastructures reposent sur le réseau OVH : un réseau mondial d'une capacité de plus de 12 Tb/s à travers le monde disposant de son propre réseau de fibre optique géré via des équipements DWDM.

Les infrastructures exploitent également la technologie vRack (baie virtuelle) qui permet à Digital Network de bâtir des infrastructures complexes multi-datacenters à base de réseaux publics et privés dédiés sécurisés au travers de liens allant de 1 Gb/s à 40 Gb/s.

Le transit IP est conforme à la norme DCI (Digital Certified Infrastructure), anciennement DCN (Digital Certified Network) qui impose l'utilisation d'un minimum de 3 opérateurs de transit IP indépendants en sus des accords de Peering inter-réseaux.

L'infrastructure réseau repose essentiellement sur des produits Cisco, Ciena et Arista.



Généralement limités à 2KVA par baie (capacité électrique et/ou refroidissement), la densité électrique ainsi que la capacité de refroidissement des Datacenters, permettent d'utiliser une valeur standard de 14KVA par baie upgradable à **24 KVA**, tout en conservant une **démarche écologique**.

C'est la technologie **InfrastruXure ISX d'APC** qui a été choisie pour équiper les salles. Contrairement aux salles traditionnelles, il n'y a pas besoin de faux-plancher : la climatisation qui est verticale, permet un refroidissement uniforme des infrastructures hébergées en évitant la création de dépressions et des « points chauds » qui restent le gros point faible des systèmes de refroidissement classiques.

L'air est aspiré à l'avant et rejeté à l'intérieur du cube dans un couloir d'air chaud fermé. Ce système unique offre actuellement le meilleur rendement en matière de refroidissement et de consommation électrique.

## INFOGERANCE ET SUPPORT TECHNIQUE

L'ensemble des instances dédiées à la solution Shapper bénéficient des services d'infogérance de Digital Network 24/24 et 7/7.

Dans ce cadre, les équipes techniques ingénieries et sécurité de Digital Network opèrent en temps réel les infrastructures des clients. Les opérations d'infogérance comprennent notamment les éléments suivants :

- Le maintien en conditions opérationnelles des serveurs et des services associés
- La veille sécurité et l'application des patches (fréquence hebdomadaire)
- Audits sécurité des plateformes (fréquence semestrielle)
- Audits sécurité des instances infogérées (fréquence trimestrielle)
- Mises à jour (fréquence hebdomadaire à bi-hebdomadaire)
- Exploitation de la journalisation, maintenances correctives et préemptives
- Vérification de la bonne exécution des procédures (backups, etc.)
- Monitoring multi-niveaux (système & hyperviseur) des instances (ram, cpu, charge, io-disques, services, etc.)
- Monitoring externe via un tiers de confiance reconnu (Pingdom) sur les aspects temps de réponse et disponibilité.
- Traitement des incidents en escalade à 3 niveaux 24/24 et 7/7, 365 jours par an. La GTI (Garantie de Temps d'Intervention) du support technique sur incident majeur ou critique est de

15 min 24/7 avec un temps de résolution incident moyen constaté sur les 5 dernières années de moins de 10 minutes.

## SECURITE

Les instances supports de la solution Shapper sont protégées par des systèmes de sécurité multiniveaux incluant notamment :

- Protection Anti-DDOS Système de mitigation multi-points répartie sur 7 datacenters & 3 continents de 4 TB/s
- Un pré-firewall Arista 7508R avec une capacité de pre-firewalling de 1.2 Tbps/1.8 Bpps
- Un firewall composé de vRouters d'une capacité unitaire de 200 Gb/s / 100 Mpps permettant un filtrage en amont.
- Shield : une solution s'exécutant sur les vRouters capables de mitiger les attaques par amplification (DNS, NTP...)
- Armor : s'exécute sur les vRouters complétées par des cartes FPGA capables de mitiger les attaques perfectionnées.
- Firewall hyperviseur : permettant de mettre en place des règles de filtrage en amont des instances.
- Firewall local : situé sur chaque instance permettant un filtrage indépendant de toute infrastructure externe.
- Restrictions locales sur les services : en sus du firewall : permet de limiter les services aux seuls bastions autorisés.
- Différentes sondes et systèmes locaux et déportées permettant de réagir à certaines attaques.

Note : l'administration des instances s'effectue uniquement au travers de bastions et de proxys dédiés à cet effet.