



PROJET « RAINBOW BUTTON »

FACILITER LA MISE EN ŒUVRE DE LA PORTABILITÉ DES DONNÉES PERSONNELLES
ET EN FAIRE UNE OPPORTUNITÉ POUR L'INNOVATION ET LA RELATION CLIENTS

Description du projet en vue d'un prototypage – V3 – Avril 2017

Synthèse et objectif de la note

Le projet provisoirement nommé « Rainbow Button » réunit 10 entreprises (Crédit Coopératif, Enedis, Engie, GRDF, Maif, Mgen, Orange, RMW-groupe BNP Paribas, Société Générale) et la Fing autour d'un objectif, la définition d'un cadre commun de mise en œuvre du nouveau « droit à la portabilité » qui :

- réduit la complexité pour chaque entreprise en partageant des éléments de spécification et de design,
- assure l'effectivité de ce droit en le rendant « lisible » par les individus et en rendant sa mise en œuvre aussi cohérente que possible d'une entreprise à l'autre,
- et par conséquent, fasse de sa mise en œuvre une opportunité pour l'innovation, la relation clients et la confiance.

Au terme de 4 ateliers de co-conception, les participants se sont accordés sur le périmètre du projet et les objectifs de mise en œuvre, en vue d'un prototypage et d'un test avant la fin 2017. Ceci permettra aux entreprises participantes, et pourquoi pas à d'autres, de prendre leurs décisions sur une mise en œuvre « grandeur réelle » en 2018.

1. Le contexte	2
2. Périmètre fonctionnel du projet Rainbow Button	2
3. Les actions d'accompagnement	4
4. Le contenu du prototype	4
5. Les étapes suivantes	5
Annexe 1 : exemple de dialogue utilisateur (scénario 1)	6
Annexe 2 : exemple de dialogue utilisateur (scénario 2)	6
Annexe 3 : description des tâches	8

1. Le contexte

Selon les autorités européennes de protection des données personnelles (G29) et le Contrôleur européen de la protection des données (EDPS), le « droit à la portabilité » introduit par le Règlement général sur la protection des données (GDPR) est un « nouveau droit » qui « offre aux individus un chemin facile pour récupérer *et réutiliser* leurs données personnelles par eux-mêmes ». Toutes les données générées par l'activité des clients sont concernées, y compris les données captées et les données transactionnelles. Elles doivent être mises à disposition facilement, gratuitement (en général), « dans un format structuré, d'usage commun et lisible par des machines. » L'utilisateur peut vouloir les télécharger chez lui, ou les mettre directement à disposition d'un tiers.

Pour les régulateurs eux-mêmes, l'enjeu de la portabilité est la création de valeur fondée sur d'autres utilisations des données, à l'initiative et sous le contrôle des individus (ex. analyse des consommations d'énergie par une application tierce, pour identifier des scénarios d'économie). Il ne faut pas la confondre avec la notion de *switching* présente dans d'autres réglementations sectorielles, dont l'objet est la concurrence, mais qui utilise également le terme de portabilité (du numéro de mobile, du compte bancaire, ...).

2. Périmètre fonctionnel du projet Rainbow Button

► Données concernées

Le projet ne définit pas le périmètre des données que chaque entreprise proposera dans le cadre de la « portabilité » en fonction de son analyse du GDPR et des réglementations sectorielles. Il est cependant conseillé de ne pas limiter *a priori* ce périmètre et d'y intégrer les données contractuelles, transactionnelles et d'utilisation qui ont le plus de sens pour les clients et utilisateurs. D'un point de vue juridique, la Cnil et le G29 ont précisé 4 critères d'éligibilité des données à la portabilité :

- les données concernent l'individu (elles sont « à caractère personnel ») ;
- elles sont traitées par des moyens automatiques ;
- elles ont été collectées ou produites sur la base d'un consentement ou d'un contrat, et/ou elles ont été fournies par l'individu ;
- leur portabilité n'affecte pas les droits et libertés d'autres individus.

► Scénarios d'usage

Le projet intègre les deux scénarios d'usage prévus par le Règlement, et un troisième optionnel :

1. Téléchargement des données sur la machine de l'utilisateur :
 - Déclenché par l'utilisateur à partir de « l'espace client » de l'entreprise « contrôleur des données » (P-DC, « *Present Data Controller* »).
 - Permet le téléchargement de tout ou partie des données proposées dans un format « structuré, d'usage commun et lisible par des machines » (type CSV).
 - Le dialogue utilisateur doit permettre à l'utilisateur de comprendre qu'il devient seul responsable du devenir des données qu'il a téléchargées.
2. Transmission des données à une application tierce :
 - Déclenchée par le client à partir de l'application tierce, qui précise les données demandées.
 - La requête de l'application tierce déclenche un dialogue qui doit être entièrement géré par l'entreprise qui contrôle les données (P-DC) avec identification-authentification, consentement explicite, *disclaimer* (informations et avertissement sur le transfert de responsabilités vis-à-vis des données).

Ce circuit s'appuie sur les procédures existantes chez chaque P-DC. Il ne doit naturellement pas permettre à l'application tierce de prendre connaissance des informations d'identification-authentification des clients et utilisateurs. A noter que d'un point de vue technique, le standard OAuth, très utilisé, répond précisément à ces spécifications.

- Sur la base du consentement, les données sont mises à disposition de l'application tierce, idéalement au travers d'une API, mais des formes « dégradées » (téléchargement...) sont également possibles.
- A partir de ce moment, le gestionnaire de l'application tierce assume la responsabilité de « contrôleur des données » sur les données qu'il a reçues (N-DC, « *New Data Controller* »).

3. (optionnel) Transmission des données à un « cloud personnel » détenu par l'utilisateur :
- Déclenché par le client à partir de son « cloud personnel » *ou* à partir de l'espace client de l'entreprise P-DC.
 - Le circuit reste à décrire mais ressemblera vraisemblablement à celui décrit au cas 2. ci-dessus.

► L'expérience utilisateur

Le Rainbow Button permettra aux entreprises (P-DC, N-DC) de proposer une expérience utilisateur intelligible et cohérente. A cette fin :

- Des éléments graphiques et signalétiques communs seront définis ;
- Les différents scénarios seront spécifiés afin de proposer un parcours client cohérent, même si chaque entreprise pourra vouloir l'adapter ;
- Un vocabulaire et des textes « juridiques » communs (consentement, disclaimer) seront proposés aux entreprises, charge à elles de les adapter si besoin.

► Le Rainbow Button comme « label »

L'objectif est également de faire du Rainbow Button une forme de « label » qui démontre par la preuve la volonté des entreprises impliquées de faire de la mise en œuvre du droit à la portabilité une opportunité pour l'innovation, la relation clients et la confiance. Dans ce but :

- Un travail sera fait sur le nom du label (qui ne restera vraisemblablement pas « Rainbow Button »), en cohérence bien sûr avec le travail graphique ;
- La Cnil, déjà associée au projet, sera consultée sur les conditions de réussite d'un tel label ;
- Côté « P-DC » (contrôleurs de données actuels), une gouvernance légère permettra d'approuver ou non l'utilisation du label et de ses attributs par de nouvelles entreprises.

La question s'est posée d'étendre ce processus d'approbation aux applications tierces (N-DC). Il s'avère cependant prématuré de le faire, la situation des entreprises et leur appréciation du GDPR variant fortement sur ce point. Il a donc été décidé :

- De prévoir dans les spécifications 3 niveaux de qualification des N-DC et des applications qu'ils proposent, que chaque P-DC peut interpréter à sa manière :
 - Application proposée par un fournisseur inconnu ;
 - Application proposée par un fournisseur identifié et authentifié *via* une autorité reconnue ;

- Application « qualifiée » *via* un processus propre à une entreprise ou un secteur.
- Ainsi, une entreprise peut choisir :
- D'accepter ou de refuser des requêtes issues de fournisseurs inconnus (le GDPR ne prévoit pas une telle distinction, mais certaines réglementations sectorielles semblent le faire) ;
 - De différencier le traitement de chaque demande, par exemple en adaptant le dialogue utilisateur ;
 - Ou de ne faire aucune distinction.
- En revanche, il a été décidé de ne pas créer un processus commun de labellisation des applications tierces, qui nécessiterait la mise en place d'un dispositif lourd et coûteux.

3. Les actions d'accompagnement

Afin de favoriser la reconnaissance et la diffusion du Rainbow Button, le projet prévoit :

- De produire les spécifications en Anglais et de les partager à l'international, en profitant des actions des partenaires dans ce domaine (participation de la Fing à la communauté « MyData », actions d'Orange dans des organismes de standardisation etc.) ;
- De conserver un dispositif de collaboration léger en vue :
 - De promouvoir le Rainbow Button en direction des régulateurs, de fédérations professionnelles, d'associations de consommateurs ou de médias (en s'appuyant sur les ressources internes des partenaires) ;
 - De réaliser des bilans de la mise en œuvre et de l'usage ;
 - De discuter d'éventuelles évolutions du périmètre, des fonctions, de la gouvernance, etc. ;
 - D'approuver les nouvelles entreprises (P-DC) souhaitant exploiter le label.

4. Le contenu du prototype

Le prototype qui sera réalisé en 2017 déclinera le Rainbow Button dans deux contextes différents :

- Celui de l'énergie, en se raccordant au projet en cours chez les « distributeurs » (Enedis et GRDF) : ce projet visera une mise en œuvre réelle, sur la base de « vraies » données ;
- Un autre secteur ou une autre entreprise (à définir sur la base de la présente note), sous forme de maquette fonctionnelle sur la base de données fictives.

Ces deux réalisations déclineront chacune les 2 scénarios « Téléchargement » et « Transmission à une application tierce », idéalement dans un contexte utilisateur « Web » et « Mobile » ; il est souhaitable que la maquette décline également le scénario de transmission des données à un « cloud personnel ».

S'agissant du scénario 1 « téléchargement », un modèle sur tableur sera réalisé pour permettre aux utilisateurs de visualiser simplement les données reçues. Pour le scénario 2 « application tierce », une simulation avec une application tierce sera réalisée.

Les deux réalisations seront testées auprès de groupes d'utilisateurs.

L'annexe 3 décrit les tâches à réaliser.

5. Les étapes suivantes

En cas d'accord d'un nombre suffisant de partenaires, l'objectif est :

- De finaliser les spécifications fonctionnelles, ainsi que le travail sur le nom et les éléments graphiques (1^{er} semestre 2017)
- De produire et tester le prototype (2^e semestre 2017).

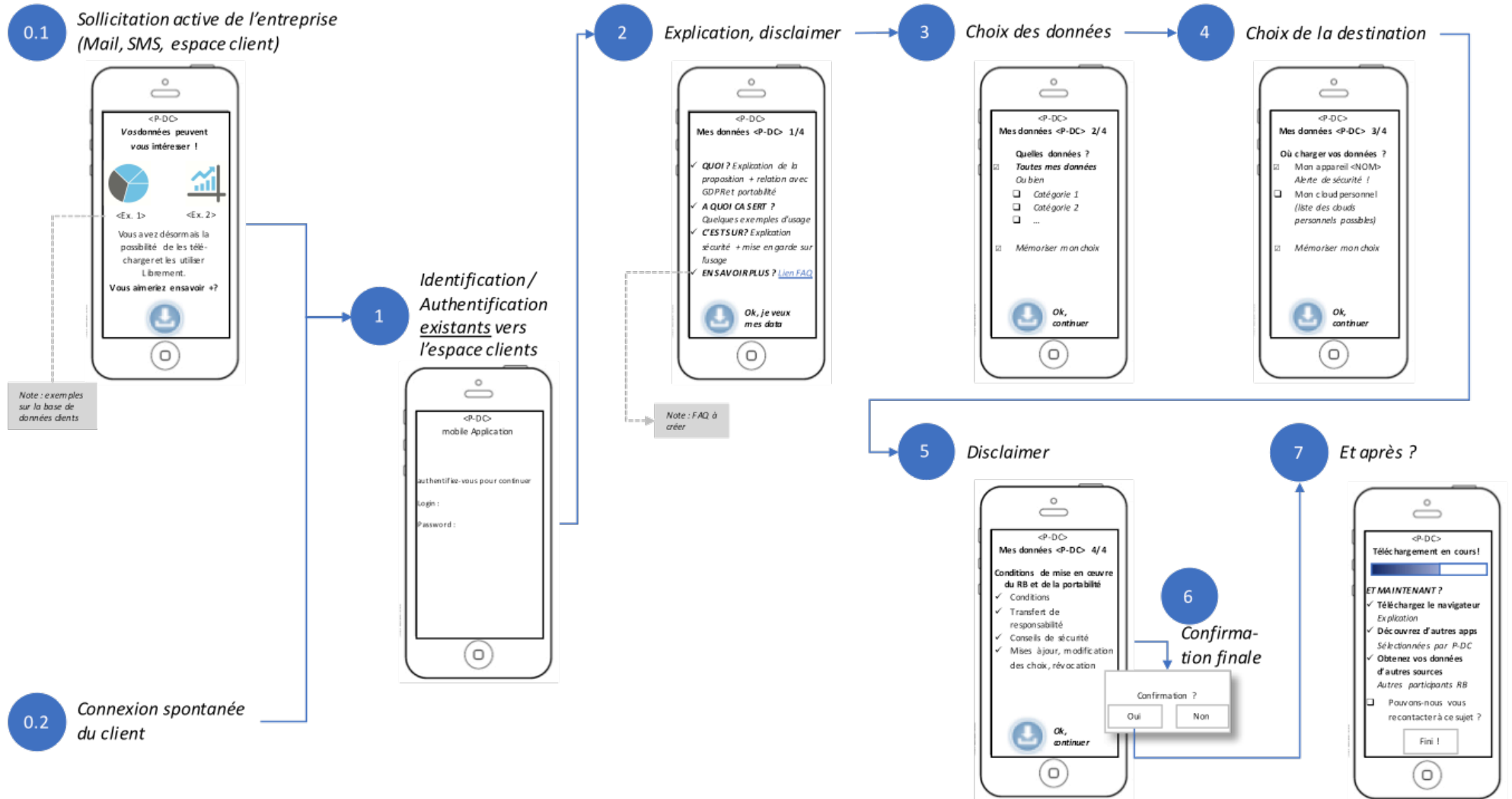
A partir de ces réalisations et des retours utilisateurs, des « lignes directrices » seront produites. Elles comprendront :

- La description du « label », ses éléments graphiques et signalétiques et ses règles d'utilisation ;
- La description des scénarios d'usage et de l'expérience utilisateur associée ;
- La description technique de la mise en œuvre ;
- Le vocabulaire et les textes juridiques-types.

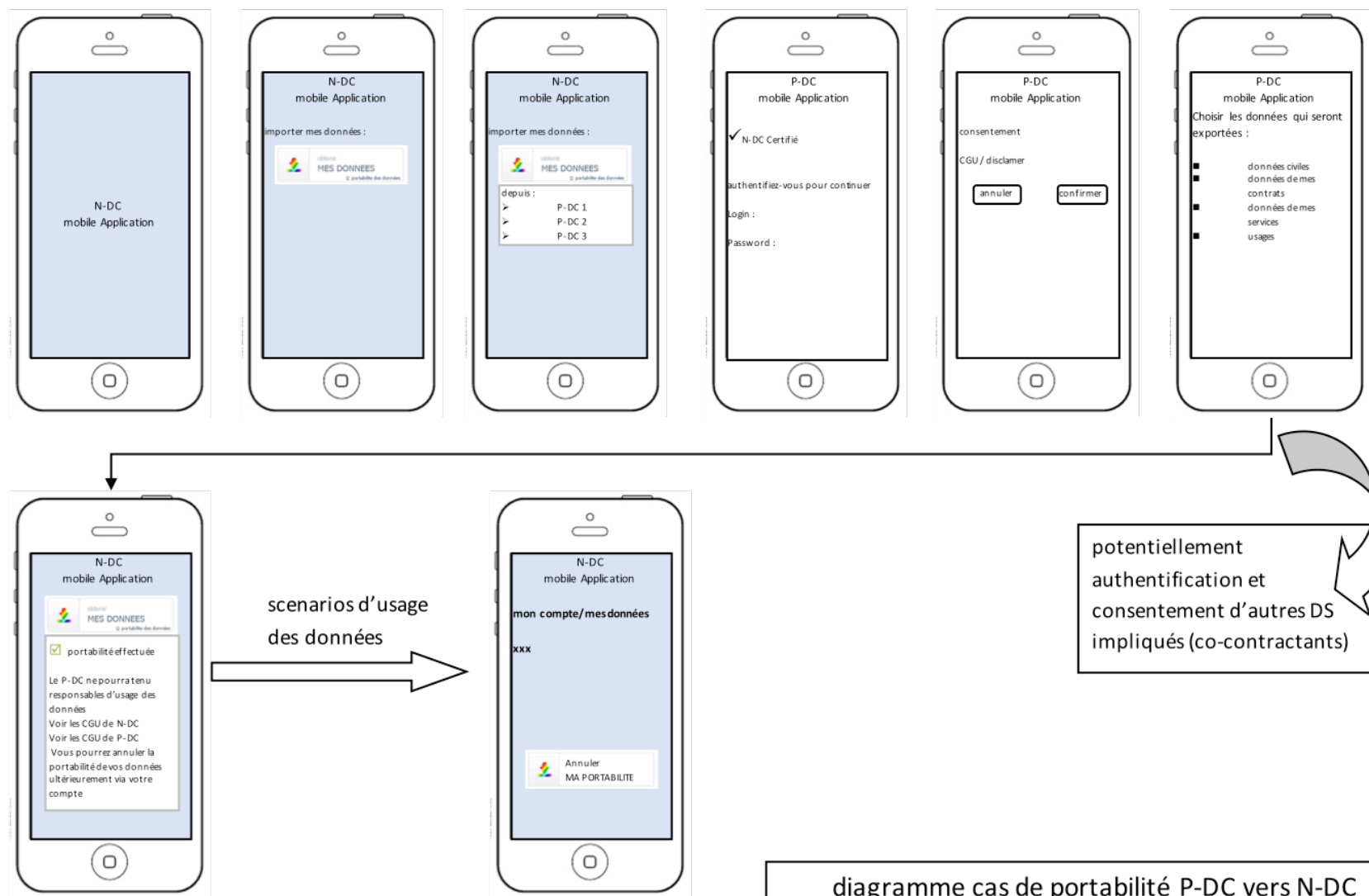
Un bilan (fin 2017) permettra aux entreprises partenaires de se positionner sur la suite, et notamment sur leur propre mise en œuvre du Rainbow Button.



Annexe 1 : exemple de dialogue utilisateur (scénario 1)



Annexe 2 : exemple de dialogue utilisateur (scénario 2)



Annexe 3 : description des tâches

	Tâches communes	Par entreprise
Identification et documentation des données mises à disposition, ainsi que de leur mode de mise à disposition.	- Définition d'une méthode - Schéma de documentation des données <i>Responsable : Fing.</i>	- Identification et documentation des données « portables » - Description des formats de mise à disposition (Energie) Mise à disposition des données
Label et signalétique : nom, éléments graphiques et signalétiques	- Trouver un nom - Réaliser le travail graphique - Prendre contact avec Cnil, Afnor, CFONB sur le fonctionnement des labels <i>Responsable : Orange (vérifie si dispose d'un budget pour sous-traitance graphique).</i>	Décliner le label et la signalétique sur son espace clients
Expérience utilisateur	Spécifications types (scénario 1 « téléchargement » et 2 « application tierce ») <i>Responsable : le groupe de travail Rainbow Button.</i>	- Scénario 1 : mise en œuvre dans l'espace clients - Scénario 2 : mise en œuvre du dialogue d'identification-authentification, « disclaimers » et transmission des données
Description technique	Spécifications types <i>Responsable : le groupe de travail Rainbow Button.</i>	Mise en œuvre
Textes juridiques type	Production des textes types <i>Responsable : un sous-groupe de juristes des entreprises partenaires.</i>	Adaptation en fonction de l'entreprise

Prototype « énergie »	Mise en cohérence des spécifications types avec le travail déjà réalisé par le secteur <i>Responsables : Fing, Enedis, GRDF.</i>	Mise en œuvre Enedis / GRDF
Maquette fonctionnelle « autre secteur ou entreprise »	Simulation d'une application tierce <i>Responsables : Fing, l'entreprise ou les entreprises partenaire(s).</i>	- Réalisation de la maquette adaptée au contexte de l'entreprise ou des entreprises partenaires (contextes « Web » et « Mobile ») - Modèle sur tableur de visualisation des données téléchargées
Tests utilisateurs	- Tests et comptes-rendus - Retour sur les spécifications en fonction des retours utilisateurs <i>Responsable : Orange, Fing et les entreprises engagées dans le prototype et la maquette.</i>	
Document « lignes directrices »	- Production et validation du document. - Traduction en Anglais. <i>Responsable : le groupe de travail Rainbow Button.</i>	
Description des tâches et contraintes associées à un futur déploiement réel dans les entreprises	- Travail commun à partir de l'expérience du prototype et de la maquette - Production d'un document <i>Responsable : le groupe de travail Rainbow Button.</i>	Validation par entreprise (et en fonction du secteur)