



« RAINBOW BUTTON » project

Enabling personal data portability and turning it into an opportunity for innovation
and customer relationship

executive summary – V1 – May 2017

In a nutshell

The « Rainbow Button » project has been initiated end of 2016 by 8 leading companies (Crédit Coopératif, Enedis, Engie, GRDF, Maif, Mgen, Orange, Société Générale) and the FING association, in order to define a common framework for the deployment of the « portability right » as described in the GDPR and the guidelines to data portability provided by WG29 in April 2017. The goals are:

- to decrease the complexity for companies through common specifications, guidelines and design,
- to ensure an efficient deployment of this new right, making it usable by end-users, providing a common and consistent experience from one service to another, and preventing misuse or abuse,
- and consequently, to make it an opportunity for innovation, customer relationship and trust.

After 4 co-design workshops, the participants have defined a project scope, key steps that can be shared in a common framework, potential deployment scenarios implicating different level of involvement from participants (financial and human). A prototype will be produced to demonstrate the benefits. The aim is also to spread the initiative through Europe, and possibly towards European or Global standardization bodies.

1. Context	2
2. What is the Rainbow Button ?	2
3. A common user experience for a better understanding.....	3
4. A label for trust and understanding.....	3
5. Next steps.....	4
Annex A: Typical use cases	5
Annex B: Common steps for the Rainbow Button framework	10

1. Context

According to European authorities in charge of Personal Data protection (Article 29 Data Protection Working Party) and the European Data Protection Supervisor (EDPS), the « right to data portability » introduced by the General Data Protection Regulation (GDPR) is a « new right » which *“allows for data subjects to receive the personal data that they have provided to a controller [...] and to transmit those data to another data controller¹.”* *“The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.”* All data generated by the activity of end-users are concerned, included *“data provided knowingly and actively”* as well as *“the personal data generated by his or her activity”*. The portability feature must be provided for free, easily, with a reasonable delay (*“within one month of receipt of the request”*, with a maximum of 3 months in some complex cases), and must use a *“structured, commonly used and machine-readable format”* format. The data subject must be able to download the data, or transfer them to another data controller.

The regulators confirm that the right to data portability is at the heart of the creation of a data ecosystem and the services of tomorrow, based on new data usages initiated and controlled by the data subjects. The target is not limited to switching services (churn), but really to spark the creation of a new range of services based on data.

2. What is the Rainbow Button ?

► Data concerned

The initiative does not define the perimeter of the data each company will provide for portability: it will depend on analysis by each company, possibly taking into account sector-specific regulations. It is however recommended not to limit this perimeter, therefore including contractual, transactional and usage-based data that make sense for end-users. From a regulation point of view, WG29 have defined that the data are not only “provided by” the data subject submitted via online forms:

“In accordance with Article 20(1)(a) of the GDPR, in order to fall under the scope of data portability, processing operations must be based:

- either on the data subject’s consent;*
- or, on a contract to which the data subject is a party.”*

► Usage scenarios

The project integrates two scenarios requested by the European regulation:

1. “Download”:

Initiated by the user from his/her customer account, it provides a feature to download data (all data, or categories chosen by the user,) into a structured, commonly used and readable format. The interaction with the user must make him/her understand that s/he will be the only responsible for the future usage of his/her downloaded data.

2. “Connect” from one Data Controller to another:

Initiated by the user from a third-party service provided by a “Destination Data Controller” (D-DC), the request requires an interaction with the data subject to select its “Source Data Controller” (S-DC), authenticate itself with this S-DC, and express an explicit consent for portability. The experience must provide legal information, disclaimer, and inform the user about the responsibilities of each Data Controller.

¹ Source: Article 29 Data Protection Working Party, “Guidelines on the right to data portability”, WP242 rev.01, April 2017

In technical terms, the OpenId Connect standard (including OAuth) is used to perform the authentication and consent phase, delivering a token to the “Destination Data Controller” (D-DC). The portability API consumes this token to deliver the information directly between the S-DC and the D-DC.

A third scenario, which will not be implemented in the initial stage, introduces the principle of a Personal Cloud, which can help users to efficiently manage their personal information, as well as create a real Data ecosystem based on services running on this Personal Cloud (refer to “MesInfos” project²):

3. « Connect to Personal Cloud »:

Initiated by the Data Subject from his/her Personal Cloud or his/her customer account with a Data Controller, the principle is similar to the « Connect » scenario, but with a Personal Cloud acting as the D-DC. This model would mix the benefits of both approaches (download & connect).

3. A common user experience for a better understanding

The “Rainbow button” framework is used by S-DC and D-DC to create a consistent, clear and understandable user experience for portability:

- Common buttons or graphical elements are defined and used by data controllers
- The scenarios have steps common to the data controllers (refer to annex B). The authentication of users is specific to each data controller, but the consent screens have a similar structure and some common design elements, including the label.
- A common terminology and vocabulary for presentation of service and consent page is proposed

4. A label for trust and understanding

With the framework comes a “Label”, which will illustrate the willing to provide a comprehensive implementation of the right to data portability.

- A work will be done on the name of the Label (which will most probably not remain “Rainbow button”);
- CNIL (France’s Data Protection Authority), already member of the project, will share best practices on creating and managing successful labels;
- A light governance mechanism will manage the label, the framework and its usage rules.

One of the challenges of portability is to avoid “phishing” situations, whereby third-party services request large sets of personal data and/or use the received data in unlawful ways, resulting in the opposite of why the GDPR has been made: a total loss of Personal data for the end-user. Some participants have argued that sector-specific regulations, such as DSP2 for the banking sector, explicitly aim at preventing such situations.

The governance should help to approve Source Data Controllers that can use “Rainbow Button” assets, but also Destination Data Controllers that can be part of a “Connect” model. It could allow for 3 levels of qualification for D-DCs:

² <http://mesinfos.fing.org/english/>

- level 0: unknown data controller
- level 1: identity of data controller has been verified
- level 2: level 1 + verification of D-DC processes and commitments on some elements (security, deletion of data, design, clear display, etc.)

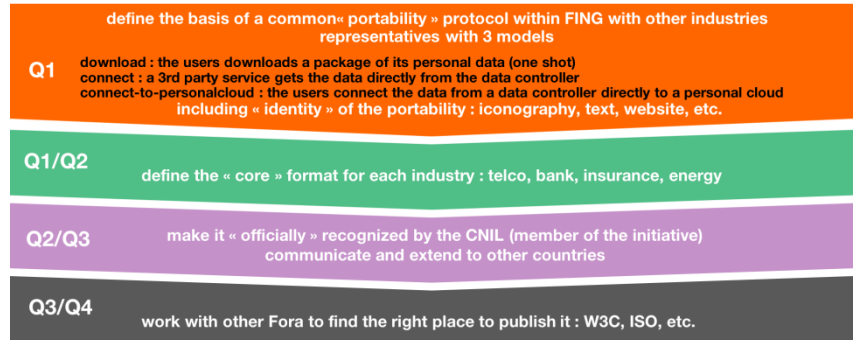
5. Next steps

The project will deliver:

- June 2017: specifications of the framework, including protocol, formats, in english to share internationally
- July 2017: graphical resources, template, legal texts
- October 2017: demonstrator and user tests

a one-year approach

january 2017



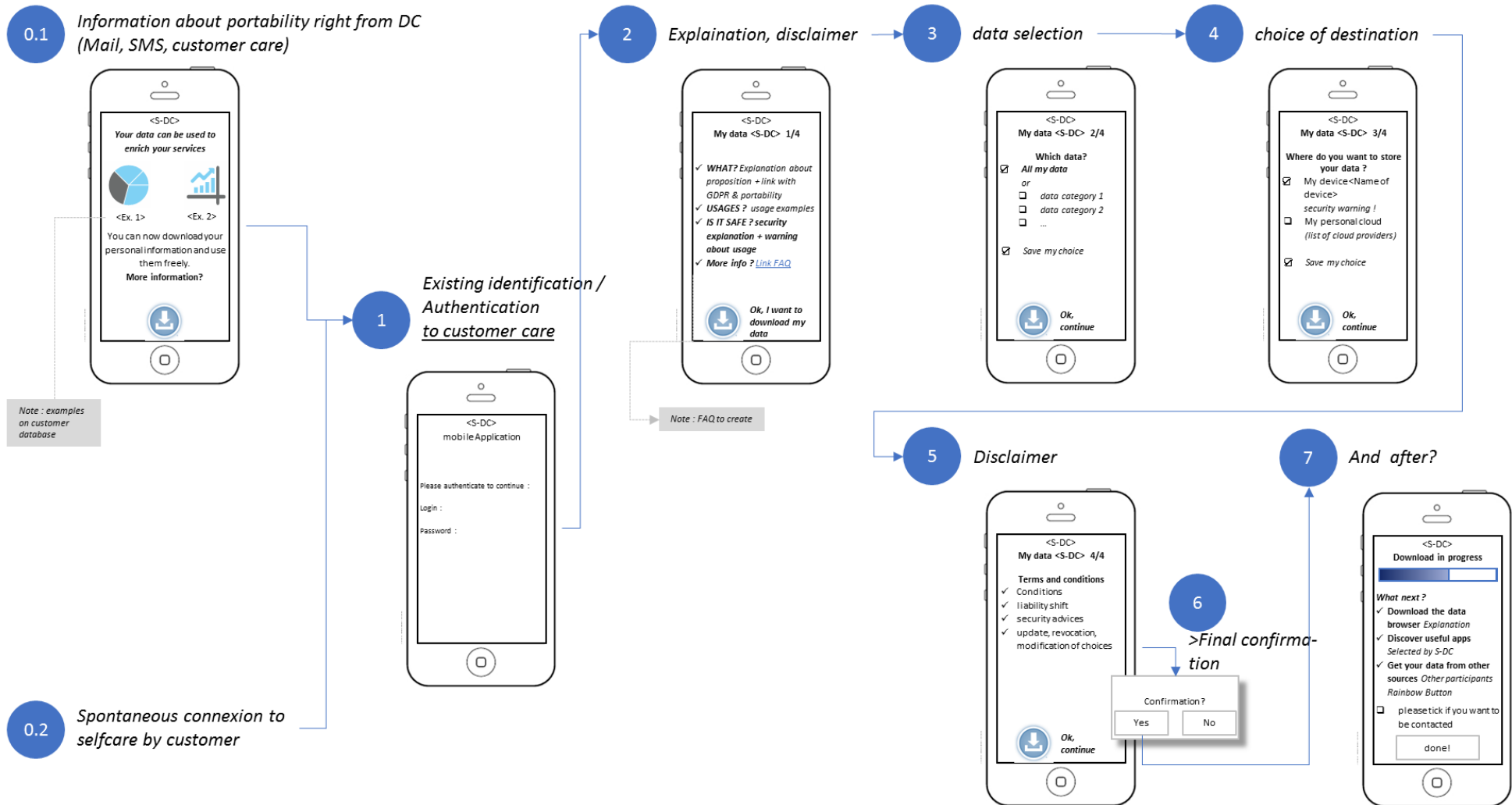
december 2017

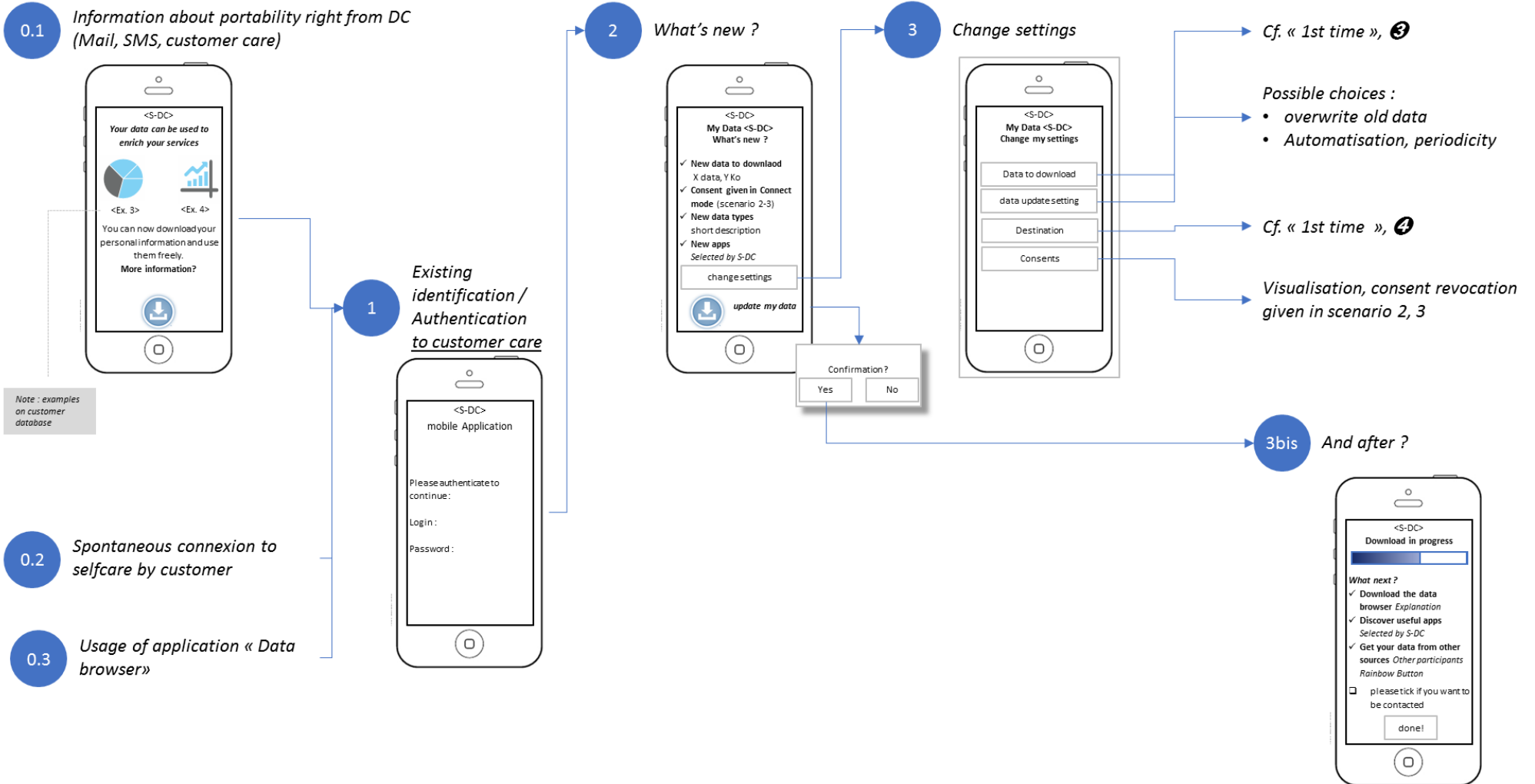
Annex A: Typical use cases

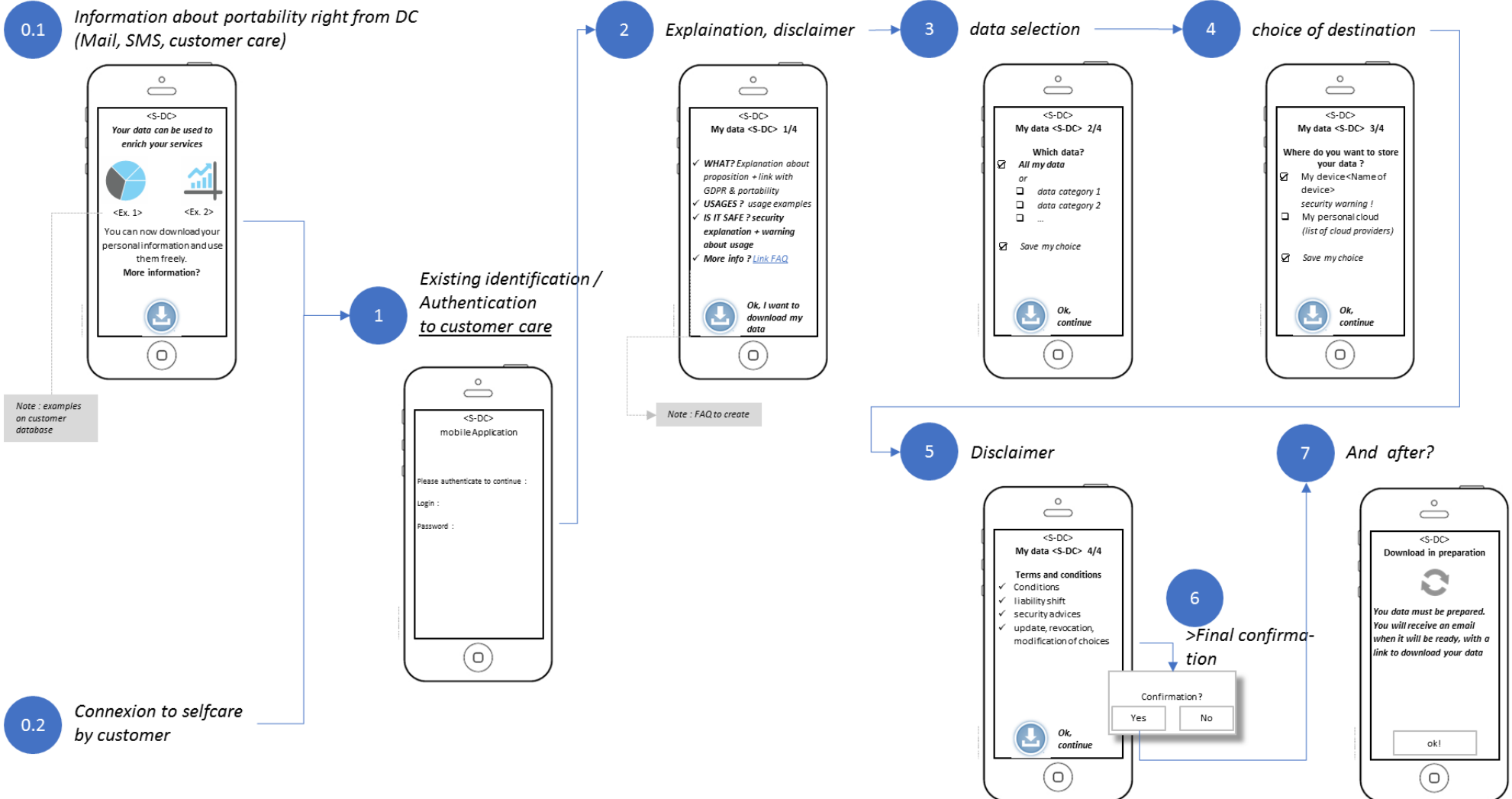


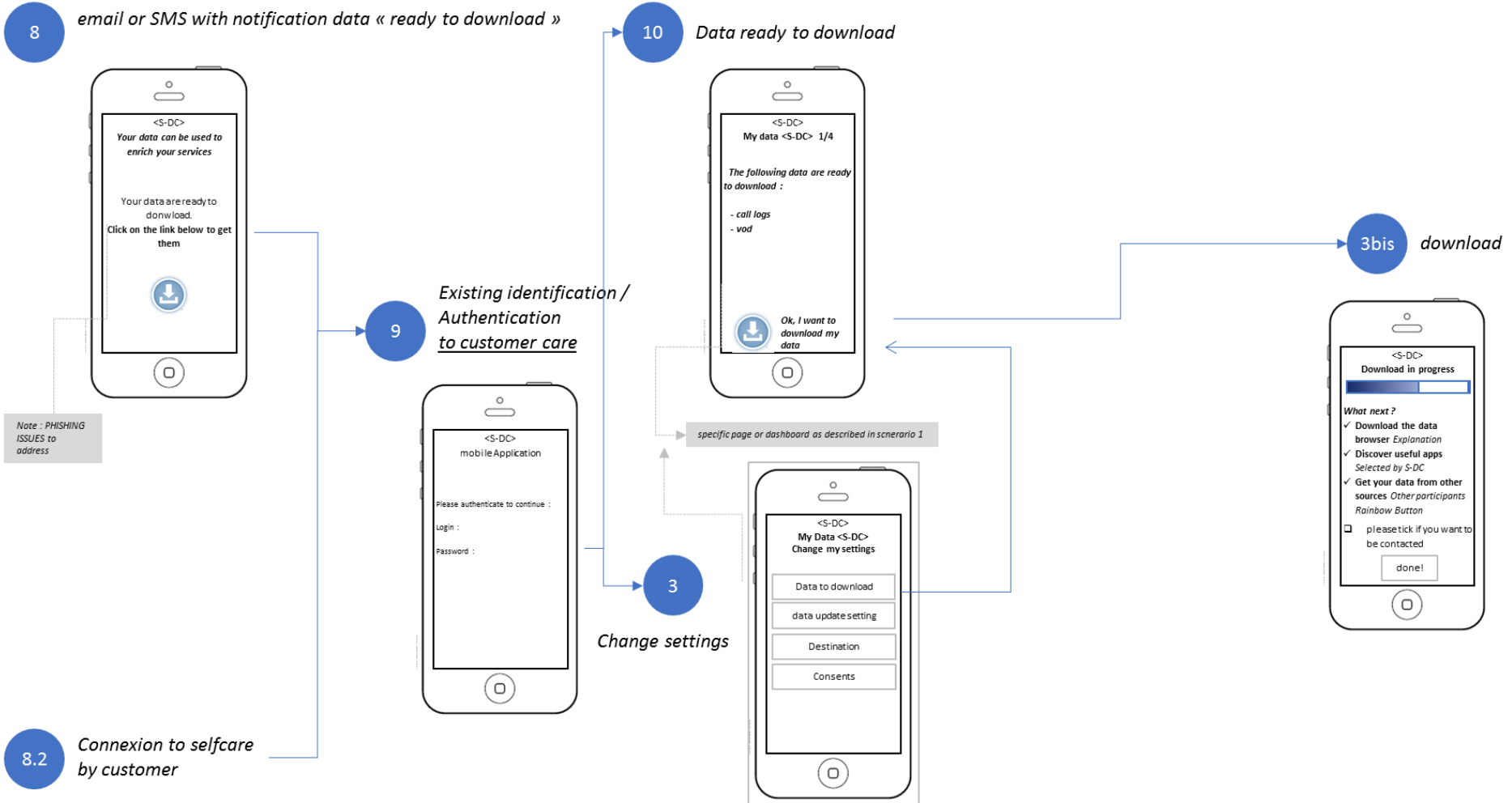
RAINBOW BUTTON – Usage scenario #1 (1/2) : Download (S-DC → DS), 1st time, data directly available

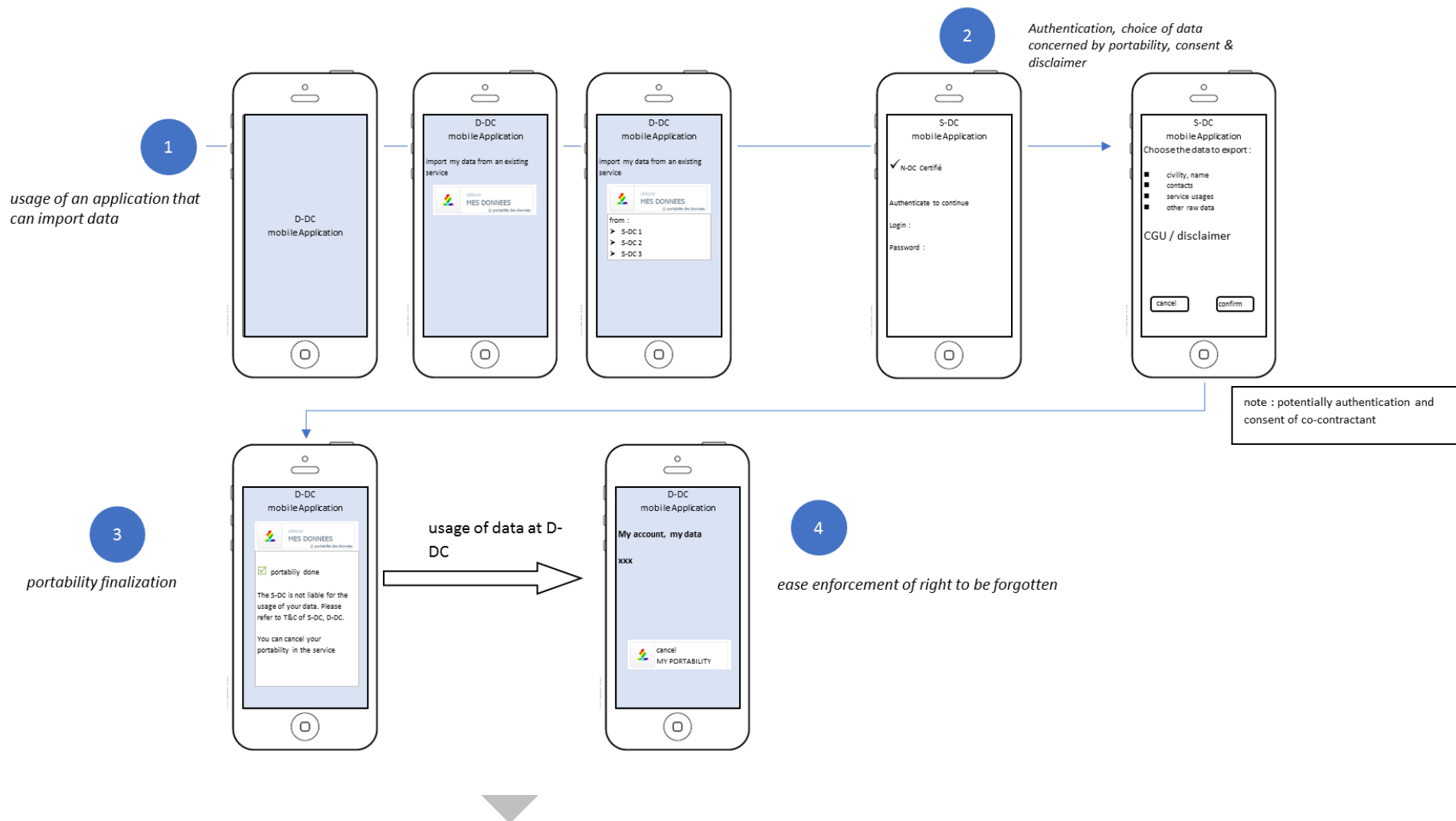
Version 2
April 2017











Annex B: Common steps for the Rainbow Button framework

This annex describes the steps of the usage scenario that are common to the different members of a “Rainbow Button” framework. Those steps require either specification or design.

Step #1: Portability (Rainbow) Button

Button that is displayed to the end-user to start a « portability » request. It is adapted to the 3 scenarios: « Download », « Connect », « Connect To Cloud »

Step #2: “ Discovery” of Data Controllers

There can be 2 types of mechanisms:

- directory of S-DC, that a D-DC can use to guide the end-user to select a source of data and to facilitate the selection of DC by a D-DC. The directory could contain url of privacy policies/terms, technical url of apis, keys
- automatic detection of D-DC, made by sharing cookie at a central level, as for the “youronlinechoices” ad tracker activation/deactivation mechanism (not initially implemented).

Step #3: technical call to start portability

Technical call to S-DC who can be based on technical url from step 2.

Step #4: Authentication of Destination Data Controller.

The S-DC has to authenticate the caller of the portability request. It is likely to be based on OAuth/OpenId connect mechanism, meaning that keys has been delivered to the D-DC. Those secrets can be delivered to anyone, or to a short list of verified D-DC, as described above (Level 0, 1, 2) .

Step #5: Consent

The consent screen displayed by the S-DC has a standardized design and iconography, to simplify the understanding by the end-user.

A specific icon or text can inform the user about the level of D-DC (level 0,1,2)

Step #6: Disclaimer

The text displayed on the consent, or before starting the portability request, is very important for the understanding of the roles and responsibilities of each actor (S-DC, D-DC and Data Subject). A common disclaimer can help the data subject to figure out who is responsible for what after a portability request is fulfilled.

Step #7: Data description

It is currently difficult to map all the categories of Personal Data that can be concerned by portability. The possibilities are endless, and it might become difficult for the end-user to understand which data are concerned by a specific portability scenario. Some categories are standardized, so that the D-DC knows which one to request to a S-DC: the same terminology will be used to describe the data it concerns, the technical elements to request them will be common to all Rainbow Button members.

Step #8: Technical transfer of data

Relying on token delivery thanks to OAuth, the Rainbow Button Source Data Controllers will align the exposition point of their portability API(s), so that it is easier for another Data Controller to integrate and access them.

Two kinds of transfer can occur:

- A synchronous transfer, that answers directly with data;
- An asynchronous transfer, that will answer first a url to call back later, after the data a collected internally. The D-DC will require some minutes, hours or days later the API to effectively get the data.

Those mechanisms, the format, the protocol, the error types, the messages, are shared through the framework.

Step #9: Acknowledgement (end of portability)

The Rainbow Button framework defines the text that must be displayed to the Data Subject after a portability procedure: it standardizes the text of the status (successful, unsuccessful, reasons, etc.), messages to display when the transfer is asynchronous and reminds the consequences in term of responsibilities.

Step #10: Cancellation of portability

Everybody has already experienced the fact we want to try a service, and to do so we have to create an account. After having tested it during some minutes, we see it does not correspond to what we expected, but the data have already been copied, and potentially spread.

With the cancellation, Rainbow Button members are strongly engaged into the right to be forgotten: they propose with a highly visible experience the possibility to delete the freshly imported Personal Data using portability, so that the Data Subject can be sure that at the end of a “test”, its data have been deleted.

Step #11: Portability receipt / history

The Rainbow Button members provide a portability history, so that the user can verify who accessed the data and when. It might be particularly useful in a second step, for periodic data portability requests.