Identity Assurance Research Brief
GDS Customer Insight and Usability
Nov 2012

1. Introduction to GDS

The Government Digital Service (GDS) is a new organisation that has been created through a merger of the Cabinet Office Digital Delivery and Digital Engagement teams with Directgov, the "one-stop shop" for online government. It is the aim of GDS to be the centre for digital government in the UK, building and championing a 'digital culture' that puts the user first and delivers the best, low-cost public services possible.

GDS is responsible for implementing the recommendations set out in the 2010 review of Directgov, undertaken by Martha Lane Fox. These recommendations called for the overhaul of 750 separate government websites, to be replaced by a single Internet "front-door" to public services on the web.

2. Project Background

When members of the public transact with government online – for example when applying for a provisional driving licence or completing their tax self assessment - they need to **prove their identity** for the transaction to be successful. This relies on accurate and up-to-date back end systems (which verify an individual's personal details) and an easy to use interface that supports the user task at hand.

Registration and authentication with government currently deters customers from accessing services online. This has been attributed to factors such as:

- The effort required of the user to go through the initial registration and subsequent login procedure, which are known to be complex and counter-intuitive.
- The fact that this process might have to be repeated at an individual service level – even though the customer might perceive all government services as being provided by the "*one government*".
- The burden of responsibility placed on the user to remember complex user IDs, passwords and activation codes.

From an internal perspective, citizens tend to update their personal details with government as and when they need to. It is not a priority for citizens and as a result it is common for government records to be out of date. This presents an issue for digital verification as the input from the user (e.g. new home address) does not match the record held by government (e.g. old home address) and therefore the system returns a data mis-match. From a user's perspective this means that they cannot move forward with their online task as the back end system doesn't recognise their details.

As a result GDS is leading on a project to investigate a **new model for online authentication**, which is intended to improve the overall user experience. The core focus of this research project is to understand the current landscape e.g. how people authenticate themselves online, explore how the new model might work in the future, how well the concept is received by citizens and in particular to investigate how the customer experience can be optimised.

When members of the public transact with government online – for example when applying for a provisional driving licence or completing their tax self assessment - they need to **prove their identity** for the transaction to be successful. This relies on accurate and up-to-date back end systems (which verify an individual's personal details) and an easy to use interface that supports the user task at hand.

Registration and authentication with government currently deters customers from accessing services online. This has been attributed to factors such as:

- The effort required of the user to go through the initial registration and subsequent login procedure, which are known to be complex and counter-intuitive.
- The fact that this process might have to be repeated at an individual service level – even though the customer might perceive all government services as being provided by the "*one government*".
- The burden of responsibility placed on the user to remember complex user IDs, passwords and activation codes.

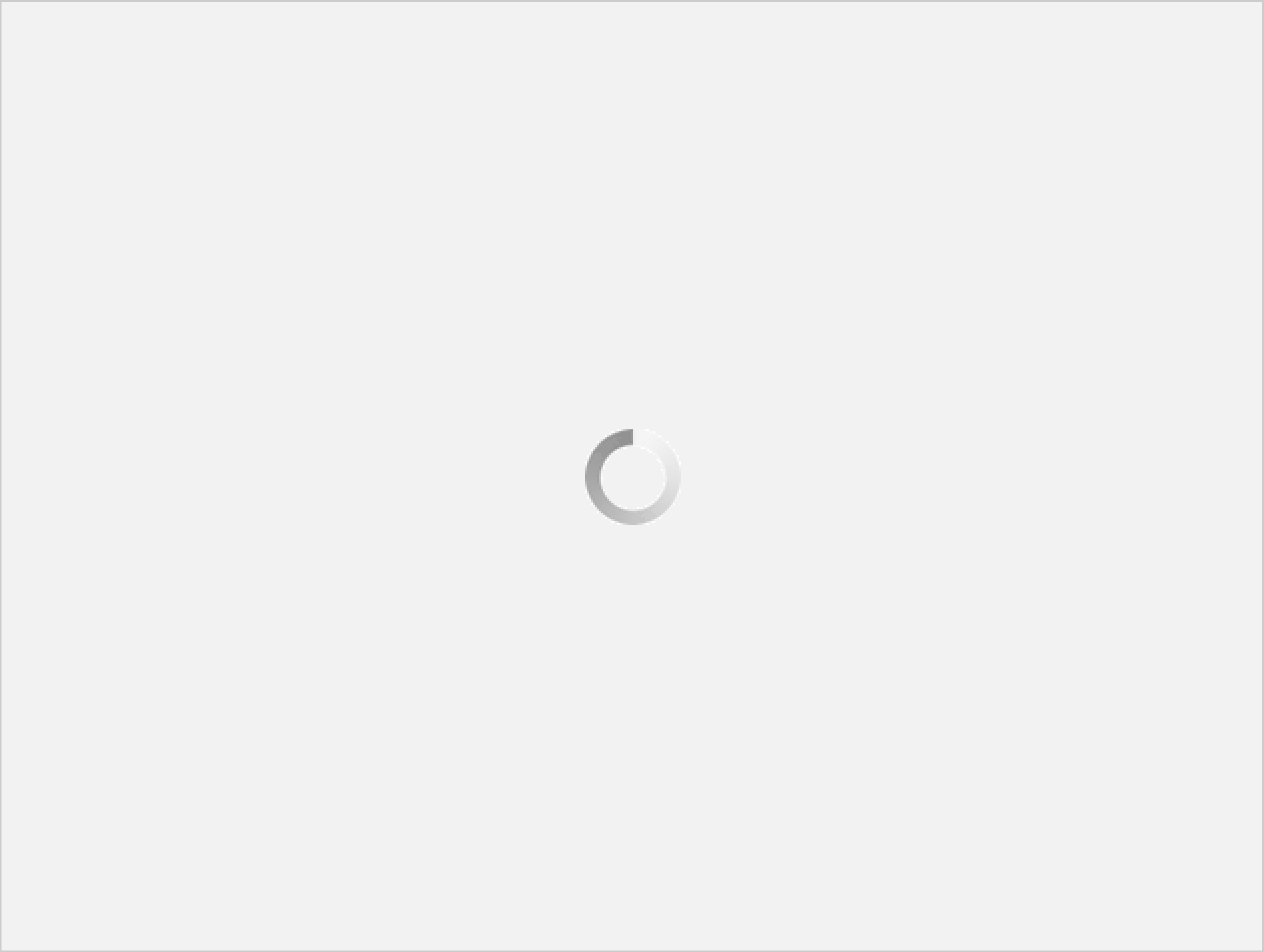
From an internal perspective, citizens tend to update their personal details with government as and when they need to. It is not a priority for citizens and as a result it is common for government records to be out of date. This presents an issue for digital verification as the input from the user (e.g. new home address) does not match the record held by government (e.g. old home address) and therefore the system returns a data mis-match. From a user's perspective this means that they cannot move forward with their online task as the back end system doesn't recognise their details.

As a result GDS is leading on a project to investigate a **new model for online authentication**, which is intended to improve the overall user experience. The core focus of this research project is to understand the current landscape e.g. how people authenticate themselves online, explore how the new model might work in the future, how well the concept is received by citizens and in particular to investigate how the customer experience can be optimised.

3. New identity assurance model

In the proposed new model government will not own an individual’s data. Instead government will work with trusted identity assurance providers that have current data sets and greater expertise in data management. This is explained by the illustration below:

Figure 1 – Illustration of new identity assurance concept



In this model citizens navigate through GOV.UK to access a particular government service/transaction. The user will arrive at a page on GOV.UK and will be asked to log-in to an identity provider”. The user will then be asked to select a trusted provider, such as their bank, to verify their identity. It is the identity provider’s role to check and verify the individual’s identity on behalf of government. The user has a choice of identity provider. Once a user’s identity has been confirmed, the user is able to move through the process and complete the transaction. The “identity provider” acts as the doorway into the transaction.

It is accepted that this is a new concept for most mainstream users of Government services. To date several high profile private sector companies have agreed to work with major Government departments to develop the scheme. It is important to note that this is not a *government only* solution. The concept of ‘open identity’ is already being used in the market place and this project reflects current industry thinking and future advancements. **However it is not a concept that will be familiar to the average UK citizen**. Most people will not have experienced this type of mechanism before and it is therefore essential to test the concept and its execution to understand how it can best be optimised.

4. Benefits of the new model

Internally it is believe that there are several key benefits to adopting this approach. It is not however known whether these benefits will resonate with members of the public. The key benefits are described below:

Only one digital identity – Citizens will be able to use and re-use registration details that they have set up elsewhere (e.g. with their bank) to transact with government. This means that they will have fewer log-in details to recall. It also means that they won’t have to keep re-registering with different government departments.

Higher success rates – The identity providers will have more up to date records than those held by government. This means that a higher proportion of people’s details will be recognised and verified online. In addition, the quality of authentication given by the identity provider will remove the need for government to verify citizens in a face-to-face context. This will enable the end-to-end transactions to take place digitally.

Control & choice– Citizens will be in control of their own data. They will get to decide which identity providers vouch for their identity.

Personal data stores – Data is a valuable commodity. Traditionally data is held by large organisations and these organisations are constantly under threat from hackers who want to steal people’s identities. To increase security the industry is moving towards a concept of distributed personal data stores. This means that everyone will have their own personal data store, which is held separately from everyone else’s data. It is believed that a structure of this nature will deter criminals from committing identity theft. For example, if a hacker manages to access a large database then they will have access to thousands of people’s identities. In a world of personal data stores the hacker would have to use the same amount of energy to hack into one personal data store, but if successful, they would only acquire one identity. The incentive to commit identity fraud is therefore greatly reduced.

5. Business Objectives

This project aims to address the points discussed in section 2 and thus define a customer experience for accessing public services that will overcome (or at least aim to address) the current deterrents. The proposed solution will:

- Empower the customer by allowing them the choice to use the accredited identity provider service of their choice, as appropriate for the transaction
- Be simple and intuitive for ALL users: such as negating the need to register with each digital service; negating the need for a customer to remember login details for each and every digital service
- Build trust with the customer by providing a suitably secure mechanism for accessing public services
- Encourage the customer to conduct further transactions online

6. Research Objectives

We are looking to commission two pieces of research. The key objectives of the first phase of research are to provide **evidence based research answering the following questions**:

i, Overall reaction to the concept

- What language / models enable people to understand the concept?
- What are their first impressions?
- Which services do they feel more/less comfortable using it on?
- What are the perceived benefits?
  - listen out for any financial benefits for government and tax payers
- How motivating are the perceived benefits?
- Would the idea encourage people to do more transactions online?
- What are the potential barriers to use?
- What are people's key concerns?

ii, What identity verification mechanisms do they use are the moment? E.G Verify by Visa, Post Office, Paypal, Facebook, Twitter etc.

- How do they feel about these types of identity providers?
- Do they trust some more than others? Why etc
- Which ones would they use to verify themselves with government?
- Would some services be more suitable than others?
- What do they understand about where their data is stored? Does this matter?
- Understand general feelings towards security?

iii, Communicating/educating the user

- How do we educate people about the potential change in authentication for online government services?
- How can they be encouraged to use the service?
- What messages should be used?

- What methods should be used to communicate the messages (vox pops, avitars, leaflets, mail shots, point of sale etc).
- At what point should methods be employed e.g. avatars, vox pops on screen, leaflets at Post Offices etc.
- Is it appropriate for partners to help educate on the change?
- Which partners would be suitable/which would not?

Please note that in addition to this research we will also conduct usability testing, to be carried out in parallel with this piece of work.

Phase 2

Secondly, a quantitative survey is required to measure the outputs of the qualitative work and to get a picture of the UK's usage of identity verification and their attitudes towards it.

7. Methodology phase 1

Given the nature of this research, we would anticipate a qualitative approach. We are keen to hear agency thinking on the most suitable methodology or combination of methodologies for confidently answering the research questions outlined above.

The overall approach will need to be agreed with the project team.

8. Test Stimulus phase 1

GDS would like the successful agency to support them with the production of test stimulus for this project. This is likely to be a difficult concept for respondents to grasp, particularly as they won't have had much/any exposure to this type of mechanisms in real life.

GDS will lead on the production of a clickable prototype to test reactions to the customer experience, but will look to the agency in question to support and advise on the best way to structure any other test material.

The agency should recommend how any test materials can be most usefully employed to help us achieve our objectives. The project team believes that the success of this project will partly hinder on the use of creative and compelling stimulus, which will help to convey the idea to the public. The project team is open-minded about the type and nature of test stimulus and will look to the competing agencies to recommend suggestions.

9. Recruitment phase 1

The agency should recommend an approach to recruitment and sourcing of a sample with characteristics they feel would be appropriate to include in the study given the research questions outlined in Section 6. Initial thinking suggests the following characteristics would be of interest in this study:

- Representative spread of the population >16 in the UK to enable testing on a number government services.
- Spread on exposure/awareness to verification providers.
- Spread of attitudes to online data security, and confidence in data sharing online.
- They do not reject the idea of authenticating/transacting online.
- Customers that have a footprint with the government now and will do so in the future e.g. benefit claiming customers and customers applying for car tax.
- Those people who may find it difficult to use online services, for whatever reason.

11. Bidders Capability Profile / Skills and experience phase 1

The agency must have research expertise and experience in:

- Eliciting people's needs, motivations and goals
- Knowledge of authentication processes
- Concept development expertise, particularly navigational concepts and early designs
- Ability to apply this insight to the design of successful online user journeys

12. Budget phase 1

The budget for the qualitative research is £30-40K including VAT. We are looking for an appropriate methodology that meets the requirements of the brief and provide a cost effective research solution.

13. Phase 2 - methodology, sample and budget

It is proposed that the second phase will be carried out using a face-to-face omnibus survey, covering a representative sample of the UK.
The budget available for phase 2 is £30K including VAT.