Data Standards Body

Consumer Experience Working Group

Noting Paper 280: CX of Authentication Uplift

Publish Date: _13 December 2022_
Feedback Conclusion Date: _27 January 2023_

Contacts:
Bikram Khadka, Consumer Experience Designer
Holly McKee, Consumer Experience Designer
Michael Palmyre, Consumer Experience Lead

Overview

In 2019, a single authentication model was determined through CX research[1] and community consultation to be appropriate for the CDR: the 'Redirect with One Time Password' (OTP) flow. No other flows are currently supported. Following the Government's response to the Inquiry into Future Directions for the CDR, as well as the Independent Information Security Review, the Data Standards Body (DSB) is now conducting Consumer Experience (CX) research to inform which authentication approaches should be supported by the technical and CX standards.

The purpose of this noting paper is to share the DSB's general CX research approach to authentication uplift with the community. We invite community feedback on this work and recommend you read this noting paper if you would like to:

- Provide views on the preliminary scope and priorities for authentication uplift
- Suggest other authentication approaches for the DSB to consider
- Comment on the general approach to CX assessment of authentication approaches

This paper and consultation will not delve into technical considerations. It focuses on CX research goals and the preliminary scope for authentication uplift, as well as various methods, measures, and metrics being used to assess alternative authentication approaches.

While this paper centres on CX research, the preliminary scope and focus will inform the general scope for CDR authentication uplift. Given the DSB is prioritising authentication uplift as foundational to future CDR expansion including action initiation, community feedback is invited on the preliminary scope and priorities for authentication uplift, as well as any other issues or items that the DSB should consider.

[1] In 2019, the 'Redirect with One Time Password' method was assessed in CX research against two alternative approaches: 'Redirect to Known' and 'Decoupled'. The outcome of that research can be viewed in this public report. To find out more about authentication in general, see here.

Background

Several factors have triggered the review of CDR authentication:

- In December 2021, the Government noted support for the Inquiry into Future Directions for the CDR's recommendation to review the approach to authentication. The Inquiry stated that 'the convenience and consumer experience of different authentication mechanisms should be considered' when assessing how to expand CDR authentication support.
- The Independent Information Security Review published in July 2022 separately highlighted that the current approach to CDR authentication does not meet minimum security requirements, and adjustments are warranted.
- The CDR community have also requested changes to the current CDR authentication model, which the DSB is considering as part of this work (see CR405, CR554 and CR542).

As the CDR matures and evolves, consumers will need to authenticate to provide a wider range of outcomes, including those that may be enabled by payment and action initiation functionality. Along with shifts in technology and consumer behaviour, the changing nature of CDR will alter the channels, contexts, and triggers for consumer consent and authorisation. CDR authentication will need to adapt and evolve accordingly to support stronger methods of customer authentication and cross-channel experiences.

In response to these factors, the DSB is now conducting CX research to help identify appropriate authentication approaches to support enhanced CDR value propositions. This aims to provide consumers with more choice and freedom when authenticating themselves while maintaining financial grade security.

Goals and Scope

Goals

The CX of authentication uplift research aims to:

- Identify appropriate authentication approaches to support in the CDR;
- Provide CX input to assessing proposed authentication approaches;
- Identify an appropriate balance between security, consumer experience, and value delivery;
- Provide CDR consumers with intuitive, informed, and trustworthy consent experiences that provide positive outcomes

Scope

To support stronger methods of customer authentication and cross-channel experiences, the preliminary scope for CX research includes the following overlapping areas:

- Augmentation of the Redirect with One Time Password (OTP) model
- App to app and web to app
- Decoupled and Client-Initiated Backchannel Authentication (CIBA)
- Step up and Multi-factor Authentication (MFA)
- Fast Identity Online (FIDO) passkeys
- Biometrics

As noted in the beginning of the paper, these areas represent the scope for CX research but will also inform the general scope for CDR authentication uplift. The DSB invites community feedback on this preliminary scope and prioritisation. Justifications for any alternative approaches are also welcome, along with views on how these should be prioritised.

Research approach

Elements rather than methods

Authentication methods providing financial grade security are regularly developed and revised. Instead of testing every available method, the DSB is looking at the various elements that make up any authentication approach. This will help support a scalable, flexible, and interoperable approach to authentication uplift. Three widely recognised elements of authentication that the DSB will focus on include:

- **Channel:** where authentication is performed. For example: mobile, desktop, or kiosk
- **Modality**: the inputs used for authentication, such as biometrics or a pin code
- **Authentication method**: how authentication is performed. Out of many factors of authentication method, these 3 are mostly recognised:
- **Knowledge based:** Something the user knows, such as a password, a passphrase, a PIN code, or a mother's maiden name
- **Inherence based:** Something that the user is, as represented by a fingerprint, DNA fragment, voice pattern, hand geometry etc.
- **Possession based:** Something the user possesses, such as a USB token, a phone, a smart card, a software token, or a navigator cookie
- **Notification method**: The different ways a user may be alerted about the authentication requirement, such as a push notification or email notification

Research Methodology & Structure

Data collection

Data collection for authentication uplift research is occurring using various research methods. This includes both moderated and unmoderated testing. The proposed research methodology and structure are as follows:

Moderated sessions include:

- Screeners
- Interviews
- Prototype tests
- In-depth interviews
- Post-task surveys

Unmoderated sessions include:

- Screeners
- Prototype tests
- Post-task surveys

Screening surveys: Screening surveys are conducted to recruit participants relevant to the research. These ask questions relating to demographics, backgrounds, accessibility requirements, digital literacy, but also attitudes and behaviours relating to the problem space, including technology use and adoption.

Moderated sessions: These activities involve 1 on 1 moderated sessions with research participants held over 90 minutes per person. Participants engage with a prototype and answer questions about authentication via an interview and a post task survey. The moderated sessions provide qualitative insights, such as ease of use, familiarity, and perceptions regarding security.

Unmoderated sessions: 30-minute unmoderated sessions with participants are conducted using a research platform called *Maze*. As part of these sessions, participants complete tasks using a prototype at their own pace, followed by a post task survey. This activity gathers more quantitative metrics, such as time to completion.

Measures and Metrics

Research Outputs

This section outlines the various outputs being used to inform the development of technical and CX standards for authentication uplift, including what alternative authentication approaches to support:

- **Global Performance:** this artefact is used to showcase the overall performance for an authentication approach
- **System Usability Scale (SUS):** this measure is used to evaluate the usability and ease of use of an authentication approach
- **Behavioural Archetypes:** this artefact categorises general behaviours, attitudes, and thematic responses to the CDR ecosystem and elements of authentication
- **Fogg Model Diagram:** this uses BJ Fogg's behavioural model to predict the likelihood of adoption of a specific authentication approach based on a participant's ability, motivation, and how compelling the prompt is seen to be

Global Performance

Global Performance is a measure used by the CX research team to define success for various authentication approaches. The Global Performance score is assessed using five separate measures:

- Recall & input
- Familiarity & completion
- Comfort & control
- Purpose & outcome
- Expectations

Each of these five measures consist of 3 different metrics as demonstrated in the 'Measures and Detailed Metrics' table below. These are collected throughout the moderated test and then collated to determine a quantifiable outcome for each measure. These 5 measures are then reflected on a five-point radial graph, demonstrating the global performance for the respective authentication model.

Measures and Detailed Metrics

Recall &/input	**Familiarity & completion**	**Comfort & control**	**Purpose & outcome**	**Expectations**
Information a user needs to recall	Familiarity	User feeling in control	Benefit awareness	User security expectations
User perception of length	Brand influence	Awareness of next step	Sensitivity of value proposition (incl. data)	Perceived security
Number of user inputs	Current authentication models	Trustworthiness	Level of positive friction	Sector

Each detailed metric can be explained as follows:

- **Information a user needs to recall:** how much information a user is required to recall to successfully authenticate (e.g. Customer ID, lengthy and complicated codes or passwords)
- **User perception of length:** how long did the user perceive the length of time it took them to authenticate, and how appropriate they found this duration to be
- **Number of user inputs:** how many fields a user was required to successfully input throughout the authentication process
- **Familiarity:** how familiar a user is with a specific authentication approach, and how often they have previously used it
- **Brand influence:** if a user's level of trust is influenced by the brand they are authenticating with (e.g. do they place more trust in a major established entity)
- **Current authentication models:** what model/s the participant currently uses
- **User control:** what element/s of the authentication approach provide the user with control
- **Awareness of next step:** can the user accurately anticipate each step based on the information provided
- **Trustworthiness:** how trustworthy did the user find the authentication approach
- **Benefit awareness:** was the user aware of the benefit of the authentication approach based on the use case
- **Sensitivity of value proposition:** was the user influenced by the value proposition (e.g. did they feel more or less likely to authenticate based on the perceived level of value they would receive)
- **Level of positive friction:** did the user feel the authentication approach was easy enough for them to complete but hard enough for a malicious actor to exploit
- **User security expectations:** did the authentication approach meet or exceed the user's expectations regarding security
- **Perceived security:** how secure did the user perceive the authentication approach to be, and what elements contributed to this perception
- **Sector:** was the user influenced by the sector of the use case (e.g. was the user more or less trusting of a specific authentication approach for banking data vs energy data)

System Usability Scale

The System Usability Scale (SUS) is a Likert scale of 10 questions. Participants rank each question from 1 to 5 based on how much they agree with the statement. A score of 5 means they strongly agree, while a score of 1 means they strongly disagree. Once data is collected and synthesised, a score can range from 0 to 100. The average SUS score is 68, but this should not be interpreted as 68% of a maximum score. The general view regarding the SUS is that:

- A score of 80.3 or higher is well performing and bodes well
- A score of around 68 is average and needs some work to improve
- A score of 51 or less is problematic and needs addressing

SUS is not used as a diagnostic and will not highlight any *specific* problems with a flow, but it can give an indication on how usable a product is in general.

Behavioural Archetypes

User archetypes help segment and succinctly describe different drivers, behaviours, and needs observed through research. The archetypes below have been developed by the DSB to represent common behavioural and attitudinal themes relating to data sharing.

There are four identified CDR archetypes, each of which has specific needs for how authenticating to share CDR data should work to be trustworthy and comprehensible.

Sceptics are less trusting of organisations and/or technology. They generally value control and are averse to sharing data based on past experiences.

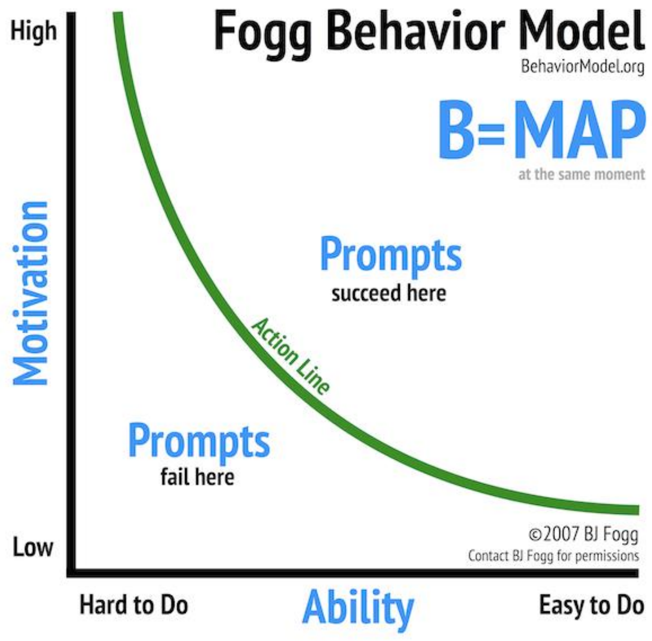
Assurance Seekers want additional assurance before proceeding. They may be apprehensive about new experiences and technologies but generally value familiarity and external references and support.

Sense-makers need to understand how the process works. They generally value additional information and can trust the process if given enough valuable detail.

Enthusiasts are excited to get the benefits of authenticating to share CDR data. They generally value simple experiences once trust is established.

Fogg Behaviour Model

In the discipline of Behaviour Design, the Fogg Behaviour Model suggests that a Behaviour (**B**) occurs when Motivation (**M**), Ability (**A**), and a Prompt (**P**) converge at the same moment. This can be summarised in the formula: **B=MAP**.



Using an Accredited Data Recipient's (ADR)'s CDR value proposition and authentication as the Prompt (P), CX research seeks to understand how Motivated (M) and Able (A) participants are to adopt the CDR process simulated in the prototype.

Ability criteria

The Fogg Behaviour model defines Ability as a function of the scarcest of the following resources at a given moment:

- Time
- Money
- Physical effort
- Mental effort
- Non-routine

Motivation criteria

- Sensation
- Expectation
- Belonging

Action line

The Fogg Behaviour Model suggests that if a participant scores below the line of action for both Ability and Motivation, then the combination may be insufficient to result in adoption of the proposed approach. This 'Action line' is indicated on the above diagram with the green line. If the participant score passes the action line threshold, then the conditions are likely conducive to them acting on the prompt and adopting the proposed approach – such as the authentication method being tested. The CX of authentication uplift research will use aspects of the Fogg Behaviour Model, tailored to the needs of the research, to help illustrate the propensity to adopt a proposed approach to authentication. For more details about criteria and metrics in general, read our page on CX metrics.

Feedback

Community feedback on this paper is invited **by Friday 27 January 2023**. In line with the DSB's approach to maintaining transparency, CX reports on authentication uplift research will be published as part of this consultation thread. When developing a response to this paper, please consider the following:

- Do you agree with the preliminary scope for authentication uplift research?
- Are there other authentication approaches, models, or elements that the DSB should consider – including any authentication approaches that you may be looking to support in the future? If so, you are invited to provide a justification for any alternative approaches and your views on their priority.
- Will the preliminary scope and approach to authentication uplift sufficiently support a broad range of consumers, demographics, contexts, and needs? If not, what considerations should be made? This may include factors relating to, for example, location, use cases, accessibility, inclusivity, and digital literacy.
- Do you agree with the measures and metrics being used to assess the CX of various authentication approaches? If not, what alternative methodologies and considerations should the DSB consider?
- The DSB has commenced a separate consultation on accessibility uplift following an independent review. Are there any factors relating to accessibility uplift, such as relevant Web Content Accessibility Guidelines (WCAG), that may impact or be relevant to authentication uplift? Relevant issues are invited to be raised as part of feedback to this noting paper, or in the dedicated accessibility uplift consultation in Noting Paper 279.