Authentication regulations for payment services

Some countries require financial services and e-commerce sites to use certain multiple forms of authentication for payment services - e.g. Strong Customer Authentication in the UK and Payment Services Regulations in the EU. It would be useful for the understanding document to reflect these requirements to assist with adoption.

UK Finance industry body has published a paper on the challenges of authentication for disabled and vulnerable customers.

In UK and EU payments must authentication using 2 independent sources through a combination of two out the three categories:

- Knowledge: something you know e.g.
    - Password
    - PIN
    - Knowledge-based challenge questions
    - Passphrase
    - Memorised swiping path

- Possession: something you have for example through a Card, phone, token e.g.
    - Possession of a device evidenced by an one time password (OTP) generated by, or received on a device
    - Possession of a device evidenced by a signature generated by a device
    - Card or device evidenced by QR code scanned from an external device
    - App or browser with possession evidenced by device binding
    - Card evidenced by a card reader
    - Card with possession evidenced by a dynamic card security code

- Inherence: something you are for example through biometrics e.g.
    - Fingerprint scanning
    - Voice recognition
    - Hand & face geometry
    - Retina & iris scanning
    - Keystroke dynamics
    - Angle at which device is held

Whether an authentication method would be considered a cognitive function test often comes down to how it is implemented. Without clearer guidance payment services platforms are unlikely to adopt the accessible authentication requirements as they must

balance it against their regulators requirements and their duty to protect customers from fraud.

Proposed Examples of passing :

1. Passphrase

Pass: Customers must enter a passphrase into an input field. Copy & paste is not blocked on the inputs, so the user's browser or extension can identify the purpose of the inputs and automatically fill in the username and password.

Failure: Customers must enter specific characters from a passphrase. Customers must select characters from a dropdown list so that it is not possible to use copy and paste.

2. OTP

Pass: Customer is sent a OTP passcode to their device which can be pasted into the input field

Failure: Customer must generate a OTP passcode of a device in their possession and transcribe it into the payment system which could be on a separate device.

3. Possession of a device

Pass: Customer is sent a notification to their personal device to authorise a payment. Customer must enter their device's authentication mechanism (e.g. PIN, fingerprint, facial recognition) to authorise payment

Fail: Customer receives a phone call on their phone number stored on an account and must speak or enter a code presented on screen for a limited period of time.

Areas than need clarification:

The current understanding document implies that transcription is always a cognitive function test unless it is possible to copy/paste. However, this is based around transcription of characters. Authentication methods can also include transcription through speaking characters or words (e.g. through phone verification), through replicating a swiping or drawn path (e.g. making a shape by connecting doc),r through handwriting (e.g. signature recognition) or through a photograph (e.g. scanning a QR code). Transcription tasks are often used instead of a knowledge based task and so may still be a more accessible alternative to other authentication methods. While all transcription tasks may be cognitive function tests,

some may be more difficult to individuals than others as they involve different cognitive tasks.. This could be addressed by adding

“Where authentication by transcription cannot be avoided, then users should be provided with a choice of mechanisms to enter the information.”

The understanding document does not differentiate between user-generated PINs and system generated PINs. Many authentication methods require customers to unlock a device or app using their PIN. While some devices allow customers to unlock with biometrics, it is in the users domains to choose whether to use these. Suggest:

“authentication methods that require the user to enter a PIN number created by themselves or their standard authentication method to unlock a device are not considered a cognitive function test.”

There should be some reference to time limits within authentication methods as the impact of a cognitive function test can be greater if the test must be performed in a time limited. Many non-cognitive function authentication methods are more likely to include timeouts for security purposes.

.