Great Southern Bank

7 November 2023

Feedback regarding DP 327 Authentication Uplift Phase 1

Great Southern Bank welcomes the opportunity to provide feedback on the Decision Proposal 327. Please find our feedback below.

Section 5.1 Levels of Assurance

Consultation questions

1. **Are there any reasons, or scenarios, when MFA must be required?**

   MFA is mandatory to support TDIF Credential Level 2. But the complex enrolment options for MFA may impact the customer experience.

2. **Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?**

   TDIF CL equates to NIST authenticator level. Data standards can retain the TDIF CL and uplift the security by keeping CL2 (MFA).

3. **Where retention of TDIF is supported, are there any clauses in the TDIF role requirements that should not or must not apply to the Data Standards?**

   No.

4. **Are there any specific accessibility requirement that should be considered in addition to the success criteria 3.3.8 and 3.3.9 of the WCAG 2.2?**

   No.

Section 5.2 Restricted Credentials

Consultation questions

1. **What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why? The 2022 Independent Health Check recommended that entropy for OTP use should be increased and OTPs shouldn't be used by themselves, but only in multifactor authentication scenarios because of the phishing risk and issues with delivery of OTP through common mechanisms like SMS and email.**

   Agreeing the security risk related to single factor OTP authentication and risk involved with email and SMS channels. Integration with authenticators will be a brand-new development for CDR platform. But if DSB, proceeding for the same, recommending go for common authenticators like- google or Microsoft or OTP apps.

2. **Should email-based OTP delivery be classified as a Restricted Credential list in accordance with NIST guidance for either or both online and offline customers?**

Yes. OTP channel should be a medium that tied to a specific device and email will not be eligible for this. It can be moved to restricted credential list.

3. **Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?**

   As per NIST guidance, potential security risk associated with SMS delivery such as device [swapping], SIM change, number porting, or other abnormal behavior before using the PSTN3to deliver an out-of-band authentication secret, cannot be monitored/identified by DH. One simple option is to display customers registered mobile number (masked with only 4 digits) and get verified by customer before delivering OTP, even though this will transfer some part of security risk to end user. Another option is to use OTP apps instead of SMS, but this also involve development effort.

4. **How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?**

   Restricted credentials and its associated security risk assessments can be published. Also propose a migration plan to block the restricted credentials.

Section 5.3 Uplift the 'Redirect with OTP' flow

Consultation questions

1. **Should the Redirect with OTP flow require a second factor of authentication, including for offline customers? An example may be introducing an additional PIN code secret that is established for CDR data sharing purposes.**

   Introducing a new pin or any other way of MFA can be over complicate the auth mechanism. Instead, suggesting to provide an option to member to validate the mobile number, in which OTP is going to deliver(either by displaying the last 4 digits of mobile number and request member to verify or request member to enter last 4 digits of mobile number). This will help to enhance the customer trust on OTP delivery.

2. **Should OTPs be only delivered to a channel the customer has already established to receive authentication secrets?**

   As of now, GSB is sharing the OTP via SMS (single channel) for member authentication. The mobile number registered against the member identity only will be considered for the OTP delivery. GSB authentication mechanism, prompt customer to enter the last 4 digits of registered mobile number and validate the same before delivering OTP. This additional step ensures the logged in customer completely aware about the mobile number in which the OTP is going to get delivered.

Section 5.4 X2App (Web2App and App2App) Interaction Flows

Consultation questions

1. **Is it reasonable to require Data Holders to support App2App when the Data Holders is dealing with online customers that have the DH app installed?**

   DSB recommendation is to support X2APP if DH app available in customer device, else support redirection flow with OTP for authentication. Deep linking/push notifications for DH app from ADR redirect URL, requires brand new development/enhancement in DH app side. Also, the *current implementation is supporting the CDR authentication and authorization is completely isolated from non-CDR auth flow. So, linking this process with other digital services of DH will be extremely complex. GSB understand this process will standardize the CDR with non-CDR platforms but wanted to highlight the complexity related to this recommendation.*

Section 5.5 Transition Roadmap: phasing in of authentication uplift obligations.

Consultation questions

1. **Are the dates proposed for Phase 1 achievable?**

   No. CDR should propose the sector based uplift options, considering the current capacity of DH. Data holders who are maintaining the CDR platform as separate entity from other digital channels, should get options to continue the same (without sharing biometrics /MFA with online channels).

2. **Do you propose any other enhancements to the uplift of authentication for the CDR?**

   No.

Section 5.6 Non-Functional Requirements (NFR)

Consultation questions

1. **Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?**

   Yes. For banking sector performance requirements are in place post authorization API invocations only. If the same extending to authorization flow, then the auth methods should be considered.

2. **Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?**

   No