BIZA·IO

DP 327: Authentication Uplift

Proposal Response

Introduction

This document outlines Biza's response to the Consumer Data Standards Decision Proposal 327: Authentication Uplift Phase 1

References

The following documents were used and are referenced during preparation of this analysis:

Document Name	Date (Version)	URL
TDIF: Role Requirements	March 2022 (4.6)	https://www.digitalidentity.gov.au/sites/default/files/2022-03/TDIF%2005%20Role%20Requirements%20-%20Release%204.6%20%28Doc%20Version%201.9%29.pdf
2022 Independent Health Check (IHC)	June 24, 2022	https://github.com/ConsumerDataStandardsAustralia/standards/issues/258
OAuth 2.0 for Native Apps	October 2017	https://www.rfc-editor.org/rfc/rfc8252.html#section-7.2

5.1 Levels of Assurance

5.1 Options for Consideration

Biza is highly supportive of options which strengthen CDR authentication towards Action Initiation while allowing data sharing authentication to align with the authentication experiences that Consumers are using in their digital channels.

We agree with the statement that CDR Data Sharing is not a low-risk transaction and our interpretation of TDIF aligns with the Option 3 recommendation of LoA 3 resulting in a requirement of CL2 authenticators. As a market leader in Holder solutions we are of the opinion we can provide a number of pragmatic observations.

Firstly, we have observed that the energy sector has significantly weaker authentication patterns on their digital channels than the banking sector, so are cautious to suggest a forcing of CL2 for data sharing across all industries. Our initial observations within the Non-Bank Lending sector indicate the level of maturity is more aligned with energy than banking on this front.

Secondly, achieving CL2 for offline consumers is difficult without introducing a memorised secret, risking adding pre-authorisation signup friction, a move we do not believe is the intent of the existing Rules & Standards.

Thirdly we also note that without a memorised secret in play, the provisions for achieving CL2 are quite limited (MF OTP, MF Crypto Software and MF Crypto Device). Our observations of solutions in market are that a vast proportion of the smaller banking population does not have these capabilities. At least some of this is due to a heavy reliance on their core banking vendor for user authentication, which is predominantly password and SMS based OTP. If this base recommendation, along with others in this proposal, could have a significant “chilling” effect on the ability for competition to be maintained in vendor choices. Put another way, such tight coupling of “existing digital experience” and uplifting of requirement could result in existing incumbent (and deficient) solutions being further embedded.

Conversely, reusing the memorised secret of the Holder’s current digital channel (i.e. their internet banking password) is currently explicitly banned by the Standards, which inherently means that, without change, the holder would be forced to create a new “CDR Pin” if they needed a memorised secret to achieve CL2. We do not believe *either* of these options would result in a favourable Consumer outcome.

Our overall suggestion, in the short term, would be to alter the proposal for requiring LoA 3 to a SHOULD for Data Sharing for Online Consumers. This allows and indeed requires holders with this capability already to adopt and align while also allowing smaller organisations to rely upon “valid technical reasons” why it is not possible right now. This would facilitate an orderly adoption of a more suitable solution which may include leap frogging directly to authenticators which achieve CL3 (i.e. MF Crypto Device).

5.1.3 2022 IHC Recommendations

Recommendation 4: Credential Level Normative References

Biza supports the CDS authentication standards aligning with the TDIF to maximise Australian standards compatibility and leave potential for utilising TDIF accredited authenticators in the CDR. We caution on adding concurrent references to both TDIF and NIST as it may lead to ambiguity or confusion if either source is updated independently. Further we believe alignment towards TDIF *rather* than NIST is most appropriate in an Australian context and is likely easier managed in the context of the Cyber Incident Management Arrangements for Australian Governments[1].

Recommendation 10: Permit Strong Authentication

Biza supports the proposal to allow stronger authentication mechanisms as per our points above. With this stated we are concerned about the following statement in the proposal:

> *Data Holders may only support authenticators commensurate to their existing digital channels to ensure there is consistency across channels and customers are already enrolled for the Data Holder's preferred authenticators.*

While we appreciate the standards enforcing cross channel consistency to alleviate undue friction within the CDR this statement may have the effect of forcing changes to organisations outside of the CDR scope as the CDR requirements grow.

We support a world where consistency is preferred and expected, but see many reasons where CDR leaders would prefer to run *ahead* of existing channels. On this basis we feel the ecosystem would be best served with standards wording that encourages and promotes advanced (and possibly separate) authenticators beyond that adopted by existing digital channels. By taking this approach the CDR could be a valuable consumer validation pathway (i.e. provide value to organisations with respect to existing digital channels). This is especially evident for smaller banking customers who have deployed CDR solutions side by side in an environment where they have very little control over the authenticators in use within existing digital experiences.

Recommendation 12: Require Credential Level 2

Biza supports adding an immediate SHOULD for CL2 for Data Sharing for Online Consumers to permit and strongly recommend upgrading, but feels like there is further consultation and clarification required before making this provision a MUST.

Specifically:

1. Whether the use of the digital channel password is still in effect? And if so, clarification on whether the introduction of a standalone memorised secret ("CDR Pin") is acceptable.
2. In the case the holder doesn't currently have an authenticator achieving CL2, whether they can require, as a standalone, one for CDR purposes?

[1] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/cyber-incident-management-arrangements-australian-governments

Q1: Are there any reasons, or scenarios, when MFA must be required?

The enhancement of the CDR to Write actions is the most obvious high risk use case. We question whether it is appropriate that Write actions be permissible within the ecosystem for Consumers who are unable to validate to CL3 (i.e. should offline users be *permitted* to conduct write actions at all?).

In addition, and with a focus on data sharing, we believe Data Sharing involving direct Personally Identifiable Information (PII) may be a candidate for MFA. This is particularly relevant given an active proposal by a participant for the introduction of a Date Of Birth into the existing CDR endpoints.

Q2: Should the Data Standards retain reference to TDIF Credential Levels or consider aligning to NIST Authentication Assurance Levels?

We support alignment to TDIF, not NIST, as we feel it is most appropriate in an Australian CDR context and ensures compatibility with TDIF credential providers.

Q3: 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?

Biza is not aware of any TDIF role requirements that should be excluded from the CDS.

Q4: Are there any specific accessibility requirements that should be considered in addition to the success criteria 3.3.8 and 3.3.9 of the WCAG 2.2?

While Biza is not aware of accessibility requirements for authentication outside what is already defined in 3.3.8 and 3.3.9 we feel it is always appropriate to conduct consumer research on accessibility patterns that are most suitable. Consideration should also be given on the need for an OTP Device to have sufficient screen readability, our basic testing on this front indicates that some existing OTP generator applications have poor accessibility for those with visual impairments.

5.2 Restricted Channels

Constraining supported authenticator channels and delivery methods

Biza supports Option 2 with the Data Standards defining an exclusion list of Restricted Credentials. It may be worth nuancing constraining authenticator channels based on *action* and *sector* combinations.

Q5: What authenticators or authentication channels should be precluded, if any, from an allowed list of authentication methods and why?

In the interests of reducing vectors of attack, particularly phishing, the existing CDR restriction of disallowing using their digital channel password access should be continued *but* this has a strong probability of increasing friction in order to achieve CL2. This is particularly the case in deployments where MFA is not currently widely adopted (i.e. energy).

Consideration should be given to the workflow associated with establishing the aforementioned "CDR Pin" in the context of contacting a call centre for Consumers who may not want or be able to setup an appropriate MFA mechanism (i.e. do not possess a mobile phone).

Q6: 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?

As a provider of a majority of the active Data Holders in the Energy sector we note that the only reliable contact method many Energy retailers possess is an email and therefore this is the only mechanism available for OTP delivery.

In our experience, classifying email OTP as a restricted credential for Banking would make sense, but would be highly disruptive to the Energy sector. Considering email as a restricted credential without an alternative (a TDIF requirement) would currently result in double jeopardy situation as it would not be possible to add new authenticators for CDR purposes (as they would not align with existing digital channels).

Q7: Should SMS-based OTP delivery be classified as Restricted Credentials in accordance with NIST guidance for either or both online customers?

By brand count, SMS-based OTP is the prevalent OTP mechanism used by Banking sector participants. As a consequence restricting SMS-based OTP delivery would be challenging without a relaxation of the digital user experience alignment requirements.

Q8: How should section 4.3.9 Restricted Credentials of TDIF be applied to the Data Standards?

To enforce the TDIF restricted credentials guidance, we suggest the following:

1. Clear CX Standards on how Holders should alert consumers of the risk of their weaker credential and how to use a stronger mechanism. Consistent messaging will be critical.
2. Guidance on Holders being able to support stronger alternative authenticators that aren't aligned to their digital channels where their incumbent digital channel has no support for other alternative credentials.

5.3. Uplift the 'Redirect with OTP' flow

2022 IHC, Recommendation 3: OTP Channel Choice

It is unlikely that a standardised requirement for OTP channel choice could work for offline consumers and these consumers are likely the most vulnerable to the threats addressed by encouraging an explicit OTP channel choice.

Biza supports deferring a decision on this recommendation until additional context is learned through other forms of authentication uplift/strengthening and better consultation on how this uplift should work with offline Consumers.

2022 IHC Recommendation 5: Set A Minimum OTP Length Of At Least 6

Biza supports changing the minimum OTP length to 6 digits.

2022 IHC, Recommendation 6: Remove The Maximum OTP Length

Biza supports extending the maximum to 10 digits as long as the WCAG 3.3.8 requirements for allowing copying and pasting of the OTP are prescribed in the standards to avoid the cognitive burdens of manually remembering and copying a 10-digit OTP.

2022 IHC, Recommendation 8: OTP Pseudo-randomness

The Standards update of:

> *Data Holders MUST generate random OTPs in accordance with [TDIF] CSP-04-02- 03j.*

Seems confusing when viewed purely in the context of the TDIF requirement:

> *The Applicant MUST generate random Authentication secrets with at least 20 bits of entropy.*

Biza reads the intent of the decision proposal as wanting to add a requirement to initialise Pseudo-random Number Generators with at least 20 bits of quality entropy, but viewing the proposed standards addition that is very unclear.

If the 20 bits of randomness was to apply to the OTP generated secret, then the suggested 6-digit OTP minimum length and OTPs generated from numbers only (10^6 or 1,000,000 possibilities) above does not conform to the 2^{20} bits (1,048,576 possibilities) of secret entropy that CSP-04-02-03j requires.

Q9: Should the Redirect with OTP flow require a second factor of authentication, including for offline customers?

Biza has experienced many energy holders which only have one reliable factor (email or mobile) across their customer base, even for online consumers. A requirement to add a second factor would likely force the setup of a CDR PIN or deployment of authenticators that currently do not exist for a large portion of energy consumers.

This is especially important for offline customers, as the redirect with OTP flow is critical to the continued support of authenticating these consumers in the CDR.

Q10: Should OTPs be only delivered to a channel the customer has already established to receive authentication secrets?

This has large implications for the offline Consumer base, as mentioned above, and given these offline Consumers are most vulnerable to the risks, Biza feels like restricting these should be delayed until appropriate consultation occurs.

5.4. X2App (Web2App and App2App) Interaction Flows

Specifically on X2App interactions we believe there are a number of clarifications worthwhile stating. We note that there is many different variations of these terms and encourage a standardised definition and consistent messaging.

URI Schemes

The use of Claimed https Scheme app to app support appears the best and most supported mobile option. This allows authorisation endpoints to be seamlessly intercepted by application flows when an app is installed or otherwise fall back to web based flows. The other schemes prescribed by RFC8252 (Private-use URI scheme and Loopback URI scheme) are likely to be problematic as a single issuer can only advertise a single authorisation endpoint using an OpenID Discovery Document. This results in limited ability to determine if an authorisation server supports an App2App environment or is purely a Web endpoint.

Claimed https scheme is supported by iOS and Android versions to circa 2015 and appears to be the clear choice with regards to App2App standardisation while still allowing a good user experience for Web fall back. The same reasoning can be applied to standardisation of the URI scheme used in redirect uris back to ADR software products (Relying Parties)

Disallowing entering of “customer id” in all proposed options

The following statement:

> *With all options it is proposed that the consumer must not be required to enter any user identifier (customer ID etc) irrespective of whether the consumer is establishing once-off or ongoing consent.*

This inclusion is likely to present issues for Data Holders that have multiple apps for individual business units (i.e. Personal vs. Corporate) but a single brand within the CDR. The technical reason for this restriction is the combination of a single issuer per Data Holder Brand and a single authorisation endpoint for the issuer.

Existing Data Holders are already deployed which capture the Customer ID in order to route to the relevant system. In an App2App world this would involve a redirect based on the Customer ID but in the proposal this has been disallowed. Holders may be required to significantly rework their solution which may, in fact, have been designed to be a single brand following guidance from the Data Standards Body and/or the ACCC.

Our read of this proposal is that it is probably too ambitious given that design choices have been made based on information Australian Government representatives have previously provided. Put another way some organisations *never wanted* to have a single brand but were forced to do so. We note that in energy a similar problem exists but the prevalence of separate digital experiences based on Consumer type is lower.

App2App vs. Web2App vs. Web2Web

While App2App is the most desirable flow when a CDR authorisation is initiated on the user’s primary mobile device, Biza encourages the ecosystem to continue to support Web2App and Web2Web scenarios as a first class citizen.

Disproportionally focusing on App2App may inadvertently add friction to alternative flows, be problematic for Business Consumers and potentially cater to a younger demographic rather than the entire Australian population.

Options for consideration

For maximum support for offline and online consumers and CDR arrangements being authorised on a diverse set of devices, Biza also supports Option 3.

At a high level, we propose the following:

1. Mandate Claims https URI Scheme for authorise endpoints and redirect uris so that fallback experience to Web is seamless regardless of user agent.
2. For Web flows, allow:
    a. backchannel push notification to mobile apps to allow MF Crypto type authentication approvals
    b. support for MF OTP credentials if a push based Web2App flow is not available
    c. when neither MF Crypto or MF OTP authenticators are available, either:
        i. have CX standards that specify how Holders can install an additional authenticator to strengthen their authentication and the risks involved (without interfering with rules prescription around offline customers)
        ii. fallback to email/SMS single factor OTP for offline customers or where no step up is possible.

Q11: Is it reasonable to require Data Holders to support preferred interaction flows, such as x2App, where the Data Holder is dealing with an online customer who has the DH app installed?

Biza is of the position that while we should strive for strengthening of the CDR authentication mechanisms, the Data Standards should not force uplift of existing digital channels that are outside of the CDR's purview. This is especially important for digital channels from incumbent vendors that Data Holders have little influence over.

Having a clearly defined preference in terms of flows and authenticators would be very helpful, particularly if it includes SHOULDs where there is considerable CX benefit to adoption of those flows.

We caution against forcing these uplifts on existing digital channels rather than allowing extensions and strengthening of existing Holder authentication in a separate mobile app specific to CDR while creating CX standards to allow communication to the user that these stronger options exist in consent flow.

5.5 Transition Roadmap

Q12: Are the dates proposed for Phase 1 achievable?

Having now been a delivery partner of every major sectorial activation deadline our default position is that alignment of Phase 1 of this proposal with sectoral activation *is not* helpful for implementers.

Beyond this more vendor specific statement our view is that the size and scope of this change means it is currently not possible to fully assess a reasonable timeline for implementation. Our suggestion would be to proceed with experimental Standards without an FDO so that implementors had the time to review and provide a reasonable assessment of the work required.

Q13: Do you propose any other enhancements to the uplift of authentication for the CDR?

Broadly speaking Biza has nothing additional to add to the uplifts proposed for authentication. We note that the focus of this proposal has been on *authentication* not *authorisation* and that the workflow changes as a result of the authentication uplift could result in poor user experiences once principal and account selection comes into scope.

We recommend the DSB consider a further authorisation uplift Decision Proposal to clarify expected Consumer workflows beyond “pre account selection” stage.

5.6. Non-Functional Requirements (NFR)

2022 IHC, Recommendation 7: Guidance for Defending Against Enumeration Attacks

Biza supports making applying the TDIF CSP-04-03-02 rate limiting requirements to the CDR Standards. We would expect all holders *already* have such rate limiting in place as this would be found in even the most trivial penetration testing.

Q14. Should NFRs or performance requirements on Data Holders be considered based on authentication method or interaction flow?

Biza does not currently have suggestions for additional NFRs or performance requirements that aren't already covered by the consent flow in the CDR metrics V5 endpoint.

Q15. Should any other service level agreements be defined for authentication methods, or the delivery of authentication secrets out of band?

It is probably worthwhile considering an SLA regarding the latency of "push" notifications in the decoupled / Web2App scenarios. We note that this may be difficult to metricise without precise definition of what this auth flow option is.

About Biza.io

Biza.io (Biza) are the market leaders in Data Holder solutions to the Consumer Data Right and are the only pure-play CDR vendor in Australia providing these solutions. Biza.io has been involved in the Data Standards setting process since the very beginning and its personnel remain the largest non-government contributors to consultations. In addition to its participation within the CDR, Biza.io is also a contributing member of the Financial-grade API (FAPI) Working Group, contributors to the FAPI 1.0 information security profile and co-authors of the Grant Management for OAuth 2.0 specification.

About Our Customers

By November 2023, Biza will be responsible for providing the Data Holder infrastructure for more than 50% of the mandated Energy Retailers as recently published by the ACCC[2] accounting for more than 75% of the entire Australian Consumer market within the Energy sector. In addition, Biza delivers the Data Holder obligations for approximately 20% of the Data Holders within the Banking sector.

[2] https://cdr-support.zendesk.com/hc/en-us/articles/7975868764431-Energy-Data-Holders-with-Consumer-Data-Sharing-Obligations-Commencing-1-November