AGL Energy Limited
T 02 9921 2999
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 14120 MCMC
Melbourne VIC 8001

Data Standards Body

Treasury

Submitted via upload to github.com.

15 November 2023

Consumer Data Right – Decision Proposal 327 – Authentication Uplift Phase 1

AGL Energy Limited (**AGL**) welcomes the opportunity to provide a response to the *Decision Proposal 327 – Authentication Uplift Phase 1 consultation paper* dated 3 October 2023 (**Consultation Paper**).

AGL has been a consistent supporter of the Consumer Data Right (**CDR**) and its goal to enable consumers to have access to, and control over, their data. As such, AGL welcomes proposals to better protect CDR data, make it easier for consumers to authenticate using their existing Data Holder applications for a seamless consumer experience, and enhance trust in CDR interactions.

However, AGL has a number of concerns in respect of how the Data Standards Board's (**DSB's**) recommendations account for the differing levels of digital maturity offered by Data Holders across different sectors. In particular, the significant challenges posed to sectors other than the more digitally mature ADRs, by the requirement for the authentication uplifts to be implemented before the end of 2024. AGL is also concerned that the authentication requirements of its offline customers (which represent a sizable proportion of the customer base within the energy sector) have not been adequately considered.

As an overarching comment, AGL is concerned that it is not adequately resourced to fully access the impacts and implications of the proposed changes set out in the Consultation Paper within the time provided for consultation, noting that the referenced credential levels and authentication standards do not currently exist in the energy sector, and represent a significant change in approach for the energy sector as a whole. AGL also expects that this means that the energy sector as a whole will struggle to engage the necessary resources for the implementation of these changes, given the constrained resourcing environment (both technical and financial) to assess, design and implement the proposed changes prior to the end of 2024.

Despite this limitation, AGL has sought to provide a response within the required timeframe, although it should be noted that a deeper level of engagement with the technical aspects of the Trusted Digital Identity Framework (**TDIF**) and National Institute of Science and Technology (**NIST**) standards than those set out in the current Consultation Paper still requires further review.

In summary, AGL's respectful view is:

- authentication uplift should be aligned and delivered on a sector by sector basis;
- the energy sector needs more time to digitally mature and it is both fair and reasonable that energy sector is allowed the same time as was given to the banking sector;
- the introduction of the authentication uplift should be aligned with utilisation of CDR within the energy sector, ideally only once the energy sector uptake and maturity is commensurate with volumes observed in the banking sector today;

- authentication standards for offline consumers need to be addressed concurrently with the online authentication standards as both are CDR consumers and energy sector has a far larger proportion of offline consumers when compared with the banking sector; and
- in relation to the Levels of Assurance (**LoA**) to be stated in the Data Standards for Authentication, Option 2 (Allow LoA 2 or above for online customers) is the closest scenario presented by the DSB that might cater to the above points.

General Responses to the Consultation Paper

This section sets out AGL's responses to specific questions asked in the Consultation Paper and its responses to certain proposals in the Consultation Paper, excluding items for which AGL has no response.

Appendix 1 sets out AGL's response to the specified Consultation Questions.

1. Table of Contents – 4. Discounted Options

No response, except as set out in relation to "Offline customers" under 5. Identified Options below.

5. Identified Options – Phase 1

5.1 Levels of Assurance (Options 1 to 3)

For consultation questions, see our responses in Appendix 1.

AGL does not support Option 1, given that it restricts heightened levels of assurance and consumer data protection for consumers in circumstances where better levels of assurance might be readily available, and where consumers already expect it.

AGL's proposed Option

AGL supports **Option 2** presented by the DSB: allow LoA 2 or above for online customers.

AGL supports the flexibility for Data Holders to implement additional levels of authentication in accordance with their existing digital channels, in line with convention *CDS-DC-0014.*[1]

Option 2 also provides the necessary flexibility for Data Holders to address overlapping regulatory obligations with respect to authentication, such as the Australian Communications and Media Authority (**ACMA**) authentication requirements for the telecommunications sector.[2] Without this flexibility, there is the potential for the DSB authentication standards to conflict with other regulatory requirements.

The flexibility provided by Option 2 will accommodate consumers requiring (and expecting) greater levels of authentication and identity proofing, such as in the banking sector, as well as accommodating sectors where consumers do not have the same expectations (or requirement) and where substantially higher levels of assurance and identify proofing may be a detriment to improved CDR utilisation. This differentiation also parallels the consumer's experience today. For example, consumers do not undergo such stringent authentication hurdles when they seek to compare or acquire energy sector products online using existing product comparison services that exist outside of the CDR regime.

Considerations relevant to Option 3

In contrast, Option 3 (requiring LoA 3 or above) represents a substantial departure from consumer expectations when managing or comparing energy products online.

It is AGL's opinion that Option 3 may create barriers for CDR consumers in the energy sector, and rather than improving utilisation, may have a chilling effect on CDR take-up. Furthermore, given this option exceeds authentication and identity proofing requirements in the energy sector today, the DSB's recommended changes have the potential to create barriers for all consumers seeking online energy services and products,

[1] https://cdr-support.zendesk.com/hc/en-us/articles/900004894483

[2] For example, the multi-factor authentication requirements set out in *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (Cth).

affecting all digital channels for consumers rather than just those available through the CDR via an accredited data recipient (**ADR**).

AGL notes the prevailing expectation that the offering of an app is the qualifying factor to require 'App2App MFA with biometrics'. This appears to conflict with existing Consumer Data Standards which state that Data Holders may only support authenticators (ie one-time password mechanism) that "align to existing and preferred channels for the customer" and do not "introduce unwarranted friction into the authentication process".[3] The consultation paper does not appear to contemplate the not-uncommon scenario where the existing apps offered by Data Holders do not fit within definitions mapped out within the TDIF, alongside restrictions imposed by the Consumer Data Standards.

Practical impact of implementation of Option 3

Further to this point, if the Consumer Data Standards were to state the DSB's recommended authentication changes under Option 3 (namely, App2App MFA with biometrics) for energy sector Data Holders, such changes would have **profound** impacts on every aspect of AGL's existing digital infrastructure.

Option 3 appears to advocate for the deprecation of all existing authentication processes that utilise SMS and email based OTP messaging. To date, AGL has made substantial investments in CL1 authentication systems and processes, particularly in the last 12 months, in support of the implementation of the consumer data right, and if those systems and processes are replaced with another authentication method, this will impose significant incremental costs, in addition to the need to write off the investment that has been implemented. The corollary to this point is that the resources required to implement the authentication uplifts predicated by Option 3 are scarce and AGL is concerned that it would be able to meet the implementation timelines considering many Data Holders would be competing for the same resources.

AGL respectfully encourages the DSB to reconsider how this Option is framed and to clearly state, for each sector, which authenticators are endorsed, how Data Holders' existing digital channels will be acknowledged under this Option, and why Data Holders implementing existing obligations now must decommission those solutions.

Further clarity on Option 3

AGL also seeks clarity on those requirements of Option 3 that appear to be in conflict, for example, the requirement that "Data Holders must support at least one valid authenticator under CL2, or above" (paragraph 5.1 of the Consultation Paper, following "What this means…") and "Data Holders may only support authenticators commensurate to their existing digital channels to ensure there is consistency across channels and customers" (paragraph 5.1.1 of the Consultation Paper). AGL currently supports CL1 across its digital channels and would require significant changes to its systems and processes to implement a Level of Assurance (**LoA**) that is equivalent to CL2 in the expected timeframe.

Offline Customers

Lastly, it is very important that the energy sector's offline consumers, as legitimate CDR consumers, are concurrently provided with appropriate authentication standards so as not to be disadvantaged (or potentially locked out, noting that if, for example, CL2 is mandated under Option 3, offline consumers will have no ability to authenticate). This is particularly relevant to the energy sector where the proportion of offline consumers is much greater than in the banking sector.

While AGL recognises that the DSB is not proposing the deprecation of support for offline customers as part of the initial phase of consultation, it is important to note the implications of any future proposed deprecation. Any proposed change that effectively prevents offline customers from accessing the CDR would be

[3] See https://consumerdatastandardsaustralia.github.io/standards/#authentication-flows.

inconsistent with the requirements of the *Competition and Consumer (Consumer Data Right) Rules 2020* (**CDR Rules**) (Schedule 4, clause 2.3). AGL respectfully suggests it is not feasible or realistic for energy sector Data Holders to onboard their offline consumers to be online consumers as suggested by the DSB. Further, if the Data Standards Chair purports to make any Consumer Data Standards that are inconsistent with the CDR Rules (in that they are not fit to permit offline customers as required under the CDR Rules) these actions are likely to be outside of the powers of the Data Standards Chair set out in Div 6, Part IVB of the *Competition and Consumer Act 2010* (Cth), and may (among other potential implications) result in the resulting Consumer Data Standards not being considered *binding data standards* under section 56FA(3) of the Act.

5.2 Restricted Credentials (Options 1 to 4)

For consultation questions, see our responses in Appendix 1.

AGL supports **Option 1: Allow Data Holders to support any suitable authenticator defined by TDIF (no restrictions)**.

AGL respectfully encourages the DSB to adopt a single framework, specifically the TDIF without further alterations or caveats. It is AGL's position that the TDIF has carefully constructed a standard for measuring authentication and credential levels and represents best practice.

By eliminating or restricting some aspects of the TDIF, the DSB, and the CDR regime by extension, may become out of step with the Government's own standards of best practice. This is important because future federal legislation relating to cyber security more broadly, could very likely impose TDIF as a standard upon organisations that are also Data Holders, resulting in expectations that they meet two parallel, and potentially conflicting, standards of best practice. In particular, it is worth nothing the proposed introduction of an accreditation regime for accredited identity service providers as part of the latest form of proposed digital identity legislation. AGL encourages the DSB to consider close alignment with the digital identity framework, as any deviation from the standards adopted through that framework is likely to give rise to unnecessary complications and cost implications for organisations using or adopting multiple frameworks.[4]

AGL does not support Options 2, 3, and 4 for the reasons outlined above.

5.3 Uplift the 'Redirect with OTP' Flow

For consultation questions, see our responses in Appendix 1.

5.4 X2App (Web2App and App2App) Interaction Flows (Options 1 to 3)

For consultation questions, see our responses in Appendix 1.

AGL supports **Option 1: Data Holder determined framework**, because it best accommodates the differing levels of digital maturity between the CDR sectors (for example the energy sector compared to the banking sector), and allows the authentication uplift to be tailored to the requirements and expectations of energy sector consumers specifically. The reasons behind this are discussed throughout this consultation response.

AGL does not support Options 2 and 3.

5.5 Transition Roadmap: phasing in of authentication uplift obligations

For consultation questions, see our responses in Appendix 1.

5.6 Non-Functional Requirements (NFR)

For consultation questions, see our responses in Appendix 1.

[4] As available at https://www.digitalidentity.gov.au/have-your-say/2023-digital-id-bill-and-rules-submissions.

6. Current Recommendations

AGL offers no comment here.

7. Implementation Considerations (Questions 1 to 6)

1. Do this paper's recommendations adequately tend to the security and consumer experience issues raised to date, or are there other options that need to be considered?

It is AGL's respectful position that the DSB's proposed authentication uplift approach and alterations to existing authentication standards do not fully take into account the different levels of digital maturity between CDR sectors, the requirements and expectations of CDR consumers in each sector (noting that the use profile of consumers in those sectors may vary significantly), and as a result, is not aligned with the capabilities and requirements of the energy sector.

AGL respectfully requests the DSB consider the following:

- The energy sector must support offline customers for the very legitimate objective of inclusivity within a sector whose chief product is classed as an essential service.
- Offline customers represent a far greater proportion of the energy sector's customer base than would be the case in the banking sector. Offline customers are legitimate CDR consumers for the purpose of the CDR Rules, the CCA and the *Consumer Data Right (Telecommunications Sector) Designation 2022*.
- Maintaining support for offline customers creates two parallel streams of protection for CDR consumers: one, which in the DSB's current advocacy does not address the requirements of offline customers; and another which seeks the highest threshold protections for CDR consumers to be implemented for online customers only.
- The outcome of this approach will result in the best protections being available for some CDR consumers while others are treated to a far lower standard of protection (or in the worst case, may be precluded from participating in the CDR), simply by virtue of demographic or chosen energy retailer.
- AGL does not believe it is possible to argue consistently that all current CDR consumers and all future offline customers are adequately protected, while also requiring substantially higher levels of authentication and corresponding investment for only one category of CDR consumers.
- AGL does not believe it is not realistic for energy sector Data Holders to onboard all of their offline customers as online customers through processes external to the CDR, as suggested by the DSB. Even if it were a realistic proposition, this is a proposal that is well outside the DSB's role and powers under the CCA, and may well result (as set out above) in a category of CDR consumers simply being restricted from the ability to access the CDR regime, despite being considered within scope under the current form of the CDR Rules.

Furthermore, AGL is concerned the introduction of heightened authentication standards and increasing identity proofing levels has the effect of introducing, by proxy, 'Know Your Customer' style regulation into the energy sector, where such regulation is not currently applicable. This exceeds the remit of the CDR regime well beyond the scope of the legislation, and is inconsistent with all current consumer expectations when dealing with energy sector products and retailers. For example, AGL respectfully suggests that a requirement for Identity Proofing Level 4 (IP4) in order to select a competitor energy product through CDR (in the context of action initiation), when the same can be achieved using existing online channels without such onerous hurdles, will severely undermine the success of CDR regime itself, and action initiation use cases that may arise.

To address these concerns, AGL's strong recommendation is that the DSB reconsider expectations of consistency across sectors given the inherent differences between sectors clearly precludes such consistency. AGL encourages the DSB to consider introducing any future phases of authentication uplift **sector by sector**,

taking into account consumer expectations, capability and cost implications, given each sector is vastly different and has different consumer expectations. Failing to do so will place unwarranted additional pressure onto the energy sector which is still in the process of delivering to existing obligations.

2. Which options (if any) are supported?

AGL has outlined which positions are supported in the response above.

3. If no options are supported, what alternatives exist to address the identified issues?

AGL has provided alternatives in its responses above wherever applicable.

4. Do you agree with the proposal to support certain approaches now and alternatives in a subsequent phase of authentication uplift?

AGL is concerned that by relying on multiple phases of implementation, the result is an expectation of continual investment by Data Holders. AGL encourages the DSB to consider that acquiring the necessary skills and resources (including capital investment) is challenging particularly in a marketplace where there are competing business imperatives and other participants are competing for the same scarce resources. This issue is heightened by the changes proposed under this paper, particularly given the potential that AGL will effectively be writing off CDR investments it has delivered in the last 12 months (with respect to the delivery of One-Time Passwords, as we have noted on page 4 above).

Across the energy sector overall, it is estimated that only 307 consumers accessed CDR in the month of October[5]. AGL's strong recommendation is that consumer participation in the CDR attains *substantially* higher levels of utilisation in the energy sector (commensurate with the numbers of active participants in the banking sector) before considering requiring further investment. At that time, AGL strongly encourages the DSB to implement a single, future-fit uplift for authentication for write access.

5. What unforeseen impacts (if any) could these recommendations have?

AGL has discussed such unforeseen impacts in its responses throughout this response.

6. What timeframes for implementation would need to be considered?

Like most other Data Holders in the energy sector, AGL is currently 100% focused on the delivery of its existing CDR obligations and is not able to absorb any further alteration or introduction of scope until after its mandated Tranche 2 deadline of May 2024. To provide a more targeted response on timeframes for the implementation of DSB's recommended option (App2App MFA with biometrics), AGL would need at a minimum three months to assess the new standards, including the acquisition of specialised consultants it does not currently employ. This activity cannot commence until after May 2024.]

Once a detailed understanding of the implementation roadmap is defined, it is likely AGL would require a further 12-18 months to become compliant with those new standards. A realistic timeframe for delivery, subject to the availability of published standards, would be Q4 2025 to Q1 2026.

AGL's response is continued in the Appendix section below.

[5] AEMO supplied performance metrics, unique NMI's invoked with Secondary Data Holder for the calendar month of October 2023

We are happy to discuss further if you have any queries in relation to AGL's response, please contact Andrew Ferris, CDR Manager at aferris@agl.com.au.

Yours sincerely,

Gino Fragapane
Head of Connections and Billing

Appendix A

Consultation questions

The following responses are provided in addition to the broad commentary set out in the body to AGL's response to the Consultation Paper.

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

With respect to read access in the energy sector, it is AGL's position that current standards are adequate. AGL recommends that MFA be introduced alongside action initiation.

Aligning to existing protections outside of the CDR framework, AGL notes that multi-factor authentication (**MFA**) is implemented for AGL's telecommunications customers (pursuant to the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*) and for those customers flagged under AGL's Family and Domestic Violence policy.

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

AGL supports the adoption of one framework to leverage definitions for the sake of consistency and simplicity. Aligning to some aspects of multiple standards will lead to unnecessary complexity, particularly if other organisations regulated in other areas of the economy, such as digital identity service providers, maintain a different position.

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?

AGL offers no comment here.

4. 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?

AGL offers no comment here.

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

AGL supports the inclusion of all authenticators mapped out in the TDIF for each credential level.

6. 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?

AGL does not support this option for read access. At the very least, it is necessary to retain email-based OTP delivery for offline energy sector consumers. It is AGL's position that existing mechanisms of authentication (including email) meet consumer expectations and offer adequate protection.

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

See AGL's response in question 6 above relating to email-based delivery.

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

As per the response in question 6 above, AGL's position is that all authentication channels within a specified Credential Level should be available for use, as dictated by the target level of assurance required for a given digital interaction.

9. 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?

Noting AGL's existing implementation for MFA for telco customers and those flagged under AGL's Family and Domestic Violence Policy, AGL supports the inclusion of a second factor of authentication for action initiation only and believes that existing standards of authentication are suitable for read access.

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

AGL supports this proposal.

11. 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?

AGL supports the introduction of provisions to *allow* x2App interaction flows with MFA authentication wherever this aligns to the Data Holders' existing digital channels.

Should the DSB implement changes that *require* the provision of x2App interaction flow with MFA, this would have the effect of all energy sector applications necessarily being pushed to the same standards as banking sector apps, irrespective of consumer expectations, use cases or cost-benefit analysis.

This would substantially inhibit take up and utilisation of the AGL app, and may result in more customers remaining offline customers, given that consumers:

- will be required to succeed multiple layers of authentication and identity proofing that are not required elsewhere in the energy sector;
- may be forced to download and register with their current retailer's app when they may be seeking to leave that retailer, which is not required elsewhere in the energy sector, adding friction to the authentication process (in a manner that is potentially inconsistent with CDR Rule 4.24); and
- would be forced to re-register and consent to share greater levels of personal information with their energy retailer than is shared currently, irrespective of whether they are interested in utilising the CDR regime or not.

For these reasons, it is not reasonable to *require* energy sector Data Holders who have an app to support x2App MFA authentication.

12. Are the dates proposed for Phase 1 achievable?

It is AGL's position that the dates proposed for Phase 1 are not realistic or achievable for any energy sector Data Holder. Further, AGL makes the following observations:

- Following AGL's own learning from the progressive delivery of '*complex request*' obligations to date, these obligations are especially complex and multifaceted and we note that AGL sought and was granted an extension of 12 months for delivery. It is very likely that most second tier retailers (ie larger retailers, as defined in Schedule 4 of the CDR Rules) will be deploying these functions well after May 2024**.**
- AGL notes Treasury has proposed several additional changes to the function and support for complex requests. Should these proposed changes be implemented, it is likely that full deployment of complex requests is further delayed, given the corresponding re-solutioning, and re-build effort that will be necessary.
- Reviewing and considering *finalised* authentication requirements and accompanying standards will require around 3 months of detailed planning and assessment to create a roadmap for implementation and acquire funding. This activity is likely to involve the engagement of specialised consultants and cannot be initiated until the latter of finalised requirements and/or the deployment of 'complex requests' scheduled for May 2024.

- Once AGL's roadmap is created, deployment is estimated to require *a further* 12 to 18 months before compliance can be achieved.

For these reasons it is AGL's **strong recommendation** that any uplift for authentication, in the energy sector specifically, first meets the following prerequisite conditions:

- **Utilisation of CDR overall in the energy sector matches those same volumes observed in the banking sector today**.[6] This represents a *substantial* increase, by several orders of magnitude, on current observed rates of take up in the energy sector. A total of 307 unique NMI's accessed CDR in October across the energy sector.[7] It is critical that the utility of the CDR regime to consumers in the energy sector is proven before Data Holders are required to allocate further significant resources and funding.
- **All first and second tier energy retailers (i.e. all initial retailers and larger retailers, as defined in Schedule 4 of the CDR Rules) have deployed both simple and complex request tranches of obligations for at least 12 months**. This will allow users to explore the benefits of a CDR framework that covers the energy sector holistically and allow Data Holders the *critical* time necessary to bed down systems, solutions and integration. Given the banking sector was afforded this opportunity, we ask that the DSB grant this same consideration to the energy sector, noting that much of the sector will continue to be in the midst of implementing functionality well into 2024.

It is AGL's position that the above conditions are fair, reasonable, and will provide the best outcomes for CDR consumers.

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

AGL offers no comment here.

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

AGL offers no comment here.

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

AGL offers no comment here.

[6] Referencing Data Holder Performance, 5.6M Session Count and 14.6M High Priority API invocations, observed in last 30 days from 3rd November 2023.

[7] AEMO supplied performance metrics, unique NMI's invoked with Secondary Data Holder for the calendar month of October 2023.