Data Standards Body

Technical Working Group

Decision Proposal 182 - Information security uplift for Write

Contact: James Bligh, Mark Verstege

Publish Date: 13th May 2021

Feedback Conclusion Date: 25th June 2021

Context

The information security profile for the Consumer Data Right (CDR) has been developed for the read operations currently included in the CDR regime.

The profile has, however, been developed with a view to being used for write operations and is therefore based on the Read/Write profile (now called Advanced Security profile) created by the Financial-grade API (FAPI) working group of the OpenID Foundation.

A write profile was originally used for three reasons:

- It was deemed that a higher base level of information security was preferable to protect consumer data shared under the CDR regime
- The extensibility mechanisms of the standards allow for voluntary exposure by data holders of write APIs. There was a strong preference to ensure that the information security profile was not a barrier to the use of the extensibility mechanisms.
- It was anticipated that the regime may, in the future, be extended to write (or action initiation) operations.

Even though the CDR information security profile was based on write oriented normative standards, consultations have not previously focused on the applicability of the profile for write operations.

Now that the final version of the FAPI Advanced Security profile has been published, and FAPI 2.0 is nearing Implementer's Draft status, guidance from the community of how the CDR information security profile should evolve is being requested. Also, feedback is being sought on specific concerns with the suitability of the profile to support write operations that would prevent voluntary extension to write operations.

Any feedback provided will help inform the prioritisation of future standards consultations.

Decision To Be Made

This proposal is seeking to determine the specific areas of uplift to the CDR information security profile that should be consulted on by the DSB in the short and medium term. This includes the standards related to both the Consumer Data Standards and the CDR Register.

Identified Options

For this decision proposal specific options are not included. Instead, questions are being asked to help frame and direct feedback from the CDR community.

Note that, feedback on DSB consultations is expected to be made public so that all participants can consider the content and integrate it with their own understanding of the problem being considered. We are, however, aware that feedback on security issues can be confidential in nature. Where this is the case the confidential information that supports your feedback can be provided by email. Any confidential details on specific vectors or vulnerabilities will be kept confidential and only the general implications of the feedback and the resulting recommendations for change to the standards will be published publicly.

Question 1 – What are the existing gaps or concerns with the information security profile?

The DSB would like to understand if any concerns or risks exist with the current version of the information security profile for the current CDR scope, that have not previously been addressed via consultation. If any such concerns or risk exist that have not yet been consulted on then the DSB would see the consultation on options for resolution of these issues as a high priority.

Question 2 – What gaps or concerns with the information security profile would prevent voluntary extension to write operations by a data holder?

It is anticipated that specific issues will need to be addressed in the information security profile before write operations are adopted by data holders and that this is more likely for higher risk operations. The DSB would like to understand the specific issues that will need to be addressed so that consultation on these issues can be scheduled at the appropriate time.

Question 3 – What aspects of version 1.0 of the FAPI Advanced Security profile, if any, should be prioritised for adoption by the CDR?

A specific consultation regarding the adoption of the more recently published version of the FAPI profiles has been scheduled by the DSB. In advance of this consultation it would be helpful to understand if there are specific aspects of the FAPI profiles that should be included as a high priority.

Question 4 – What priority should be given to transitioning to FAPI 2.0?

A specific consultation regarding the adoption of the FAPI 2.0 profile version has been scheduled by the DSB. In advance of this consultation, it would be helpful to understand whether adoption of FAPI 2.0 should be considered with priority ahead of FAPI 1.0 Final alignment, or whether co-existence of FAPI 1.0 and FAPI 2.0 support should be considered. What other issues should be considered such as vendor supportability, staged adoption of FAPI 2.0 and implementation timeframes?

Question 5 – What additional patterns or normative standards should be considered for adoption to reduce the risk of write operations?

There are a number of patterns to reduce the risk profile of various write actions that are widely adopted in digital channels. The use of transactional signing, step-up authentication, decoupled authentication and push to approve of an action via another channel and complex protocols such as 3D Secure v2 in the credit card industry are all examples of patterns that reduce transactional risk.

The DSB is seeking recommendations on the types of patterns or international standards that the DSB should consider.

Question 6 – What additional changes, if any, that should be considered for maximising international operability?

Increasingly, operability across adjacent regimes such as the CDR is anticipated. The DSB would like to understand the specific issues that will need to be addressed to facilitate read and write operations across international regulatory standards.

Question 7 – What steps could be taken by the DSB to assure the efficacy of the information security profile?

Validation of the information security profile is important so that CDR participants can engage in the regime with confidence. What specific actions could be undertaken to increase participant confidence and improve the credibility of the information security profile?

Current Recommendation

There is no recommendation contained in this proposal. Open feedback is being sought to help steer future proposals and recommendations for consultation.

Implementation Considerations

As no specific changes are being proposed there are no direct implementation considerations that have been identified by the DSB.

Any feedback that the community may have on implementation concerns and issues with timing of implementation of any of the issues raised by this proposal are still welcome.