August 8, 2022

Saudi Central Bank (SAMA)
King Saud Bin Abdulaziz Street
PO Box 2992 Riyadh, 11169 Saudi Arabia

RE: OpenID Foundation's FAPI Adoption Recommendation

To Whom It May Concern,

It was my, and other representatives of the OpenID Foundation, pleasure to meet Abdulelah Alanqry at Identiverse 2022 in June. We appreciate Abdulelah sharing a comprehensive overview of the Saudi Open Banking initiative including the adoption of FAPI being led by SAMA.

During the conversations at Identiverse, we understood SAMA's reluctance to mandate a draft specification, especially in a highly regulated sector. Additionally, there is also a reluctance to implement a strong 'regime' of conformance and certification where either the profile and/or conformance suite are still in draft.

FAPI 2 should be the recommended security profile for open API (e.g., open banking/finance) standards and ecosystems. However, as FAPI 2 is still an "Implementers Draft", ecosystems looking to implement open banking/finance before the end of 2022, we recommend the following is adopted as the official security profile:

- FAPI 1 Advanced.
- Mandating the PAR option within FAPI 1 Advanced (to enable an easier migration path to FAPI 2) as the method for parameter passing for authorization grants.

This profile can simply be stated as "FAPI 1 Advanced with PAR", so there is no need for any standards body or ecosystem to create any new FAPI profile or derivative.

The benefits of this approach are:

1. Providers and relying parties are implementing a security profile which is mature, well defined and widely used, which will give all parties assurance.
2. There are a large number of vendor solutions supporting this profile, which will speed up implementation for providers and relying parties.
3. There is a robust and comprehensive conformance suite, which will enable a much higher level of conformance in any ecosystem.
4. Both the profile and the conformance suite are actively maintained and supported by the OpenID Foundation, which significantly reduces the work for any other standards body in this regard.

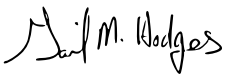
5. There is a relatively simple upgrade path to FAPI 2 for both providers and relying parties, which makes any solution future proof and supports interoperability between ecosystems.

As soon as FAPI 2 and the corresponding conformance suite are finalised, and as soon as the OIDF are able to validate and publish FAPI 2 certifications, then we recommend that standards bodies, ecosystems and implementers migrate to FAPI 2.

The proposed adoption and migration path is detailed in an attached paper which is a comparison of available FAPI profiles and recommendations for new markets looking to implement FAPI as their security profile. The paper was developed by the FAPI Working Group co-chairs and a number of contributors.

The OpenID Foundation looks forward to continuing to work with SAMA on its successful adoption and rollout of FAPI including FAPI conformance and certification. Please let us know if you have any questions regarding the proposed approach.

Best regards,



Gail Hodges
Executive Director
OpenID Foundation