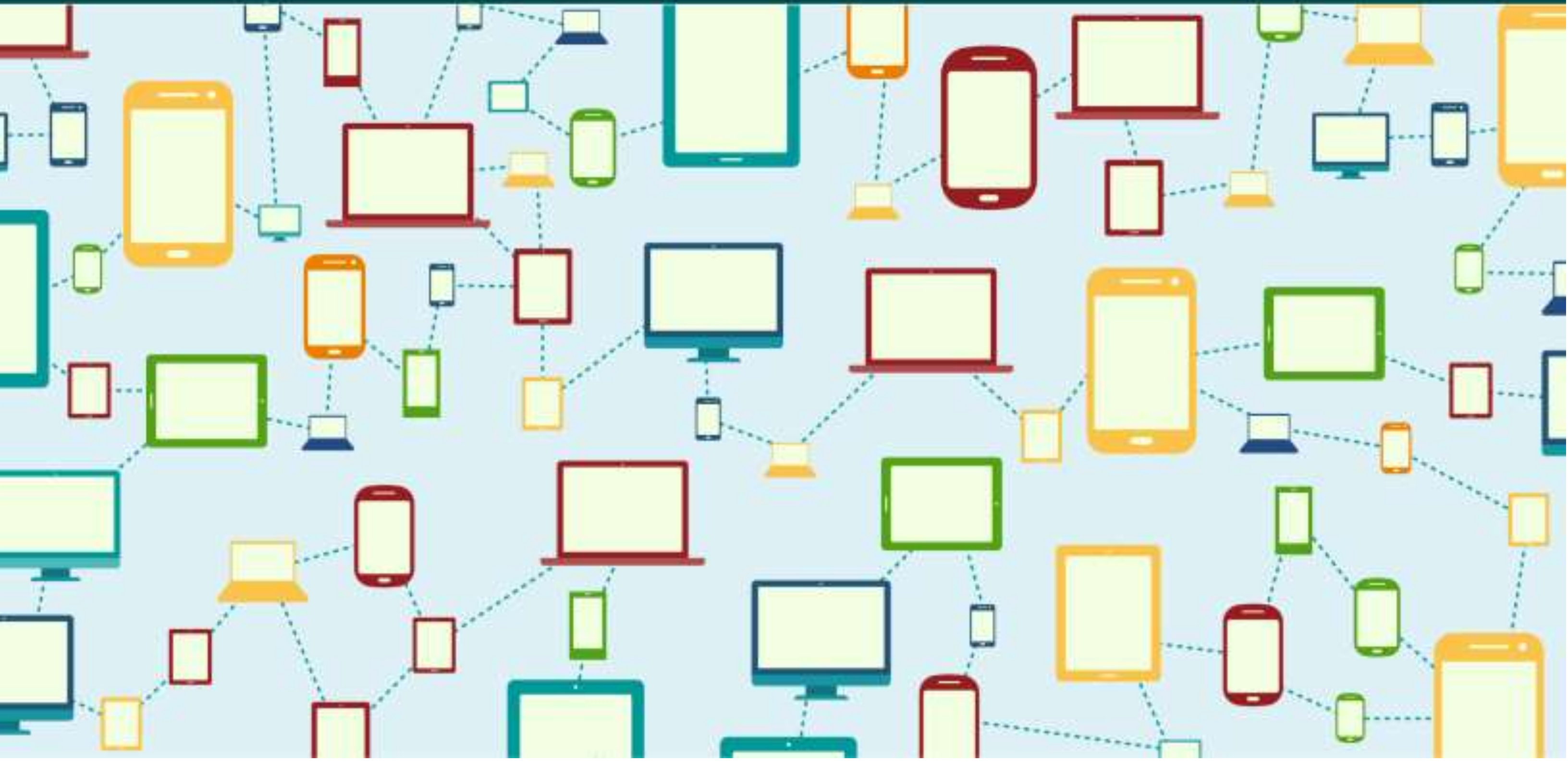

Recommended Account Recovery Practices for FIDO Relying Parties

February 2019

Editors: Hidehito Gomi, Yahoo! JAPAN
Bill Leddy, VISA
Dean H. Saxe, Amazon

Introduction

In 2019, strong customer authentication is expected to ramp up rapidly, driven by support from regulatory initiatives such as Payment Services Directive 2 (PSD2), industry standards such as those from FIDO Alliance and the World Wide Web Consortium (W3C) and also through platform vendors. But adoption will be limited without mechanisms to recover accounts when authenticators are lost. The entire ecosystem is only as strong as the weakest link, so account-recovery mechanisms and policies must be clearly defined. These approaches need to provide secure and acceptable user experiences. This document briefly summarizes recommended practices for all service providers (also referred to as Relying Parties or RPs), including banks and merchants.

The FIDO Alliance recommends the following two-step strategy for managing account recovery:

1. **Multiple authenticators per account (reduction of account-recovery needs)**
2. **Re-run identity proofing / user onboarding mechanisms (actual execution of account recovery)**

These best practices are described in more detail below. This strategy reduces the need for account recovery through multiple authenticators, while maintaining identity and authentication assurance levels required by the business during account recovery. Consistent use of these practices across RPs will provide a consistent consumer experience that reinforces FIDO security and adoption.

1. Multiple Authenticators

The primary mechanism to reduce higher-friction account-recovery mechanisms is by encouraging users to register multiple authenticators on their accounts. The loss or breakage of a single FIDO authenticator is minimally impactful to the user when an additional authenticator is readily available. FIDO authenticators such as FIDO-enabled USB keys (FIDO Security Keys) or mobile phones can be used for this purpose. For example, a user could have their personal computer and mobile device connected to their banking account. If one is ever lost, damaged or replaced, the user can log in with the other device.

Roaming authenticators, like USB keys, are particularly useful for this purpose. Users can register a FIDO Security Key as an additional authenticator across all their accounts, but keep it locked in their desk drawer at home, or another safe place. If they ever lose their primary authenticator (e.g., phone or security key), they can use the additional device to authenticate, retaining account access and avoiding further account-recovery mechanisms.

Google’s Advanced Protection is a good example of this approach. The user is required to enroll two FIDO Security Keys for any given service (https://google.com/advancedprotection/) to maintain consistent access. Note that the additional authenticators to be registered and the registration processes should ensure the resulting assurance level to be at the same or higher assurance level while satisfying an RP’s security policies and requirements.

RPs should strongly encourage account holders to add additional authenticators when the account is created or when the account with no additional authenticator is identified; if the user defers they can be prompted later. For example, the RP can suggest enrolling an additional authenticator during routine account communications – such as when users are asked to confirm their contact information is still current. RPs must provide a mechanism for users to report the loss or breakage of a registered authenticator, such as a specific interface on their web site to manage authenticators. RPs should revoke the credentials of the lost authenticators in response to users’ requests after confirming this request is true.

2. Re-run Identity Proofing / User Onboarding Mechanisms

If an additional authenticator is unavailable, lost, or broken, RPs may fall back to identity proofing of their users using a mechanism at the same or higher assurance level as the initial account bootstrapping. This can be the same method used to create accounts or could be a mechanism set up after the account was created.

Mechanisms for identity proofing users can be found in the National Institute of Standards and Technology (NIST) 800-63A Digital Identity Guidelines (https://pages.nist.gov/800-63-3/). Identity proofing can range from in-person proofing of identity documents to remote proofing or use of a trusted referee. The RP must determine the best fit for their needs based upon risk and the tolerance for customer friction.

Just like account creation, the requirements for identity proofing depend on the requirements of the RP. For example, an online fantasy game is very different from a retirement account. The RP must select the appropriate choice between security and customer friction. Customers may expect higher security requirements for accessing their private financial accounts and also expect less friction when accessing accounts they consider less risky. No matter what mechanisms for identity proofing may be selected to recover an account, RPs should ensure that they obtain user consent to perform identity proofing and provide personal data needed to prove their identity for recovering an account. Note that FIDO authenticators by design do not reveal any personally identifiable information.

In some cases, such as anonymous or pseudonymous accounts established with no identity proofing, RPs may be unable to offer identity proofing-based account-recovery mechanisms, leading to account abandonment. For some users, this may be preferable to being identifiable. However, anonymous or pseudonymous accounts may be recovered using a protocol such as the Delegated Account Recovery protocol developed at Facebook, (https://github.com/facebook/DelegatedRecoverySpecification) which allows a user to demonstrate continuous control of an account at a trusted service provider without revealing any personally identifying information. In this scenario, the RP relies on the trusted service provider to store a recovery token indicating a user's privilege to reclaim access to their account, thus preserving the anonymity/pseudonymity of the account. Depending on the value of the account and the trust an RP places in the trusted service provider, this might be sufficient as a standalone mechanism, or it could be combined with independent mechanisms to achieve the desired level of assurance.

Alternatively, RPs may allow both anonymous and/or identified accounts with the consumer accepting the risk of account loss on anonymous accounts. In these cases, RPs should inform the user of the risk of account loss, allowing the user to make an informed decision about the risks.

Finally, RPs may offer other recovery mechanisms that are designed to meet their needs and requirements for account recovery. Weaker mechanisms may lower the bar for account recovery by providing a weaker pathway to user identity-proofing or authentication, but this approach would also reduce the value of the FIDO implementation. Implementing weaker account-recovery options is not recommended by the FIDO Alliance.

3. Conclusion

Using multiple authenticators is the recommended best practice to reduce the need for account recovery. This is the most secure and easy option for RPs to manage account recovery for users, and minimizes the risk of the having to perform identity proofing for account recovery.

However, there are cases where this method is not sufficient. For such situations, there are other options for account-recovery methods, but these must be selected based on the RP's use cases, requirements and policies. If an RP has an identity-proofing or authentication method for account recovery, they can use those and leverage their current investment. If this option is not available, account-recovery methods leveraging a trusted service provider could be used.

It ultimately is up to the RP to select the appropriate options that balance account risk and user experience while meeting security policies.

4. Acknowledgements

The editors acknowledge the following contributors for their valuable feedback and comments:

- Alexei Czeskis, Google
- Max Hata, NTT DOCOMO
- Brad Hill, Facebook
- Giridhar D. Mandyam, Qualcomm
- James Manger, Telstra
- Hideo Nishimura, NTT Labs
- Andrew Shikiar, FIDO Alliance
- David Treece, Yubico
- Elizabeth Votaw, Wells Fargo