Making 2SKD Work for People

Jeffrey Goldberg
Julie Haugh
Jessy Irwin
The three Js
under the protection of Umbrella Bear
Two-Secret Key Derivation

Two user secrets to derive Key Encryption Key
Master Password

- Created by user
- Stored only in user’s head
- Difficult to steal
- Not so difficult to guess
Account Key

- Created by client
- Stored only on user’s devices
- Possible to steal (from user’s device)
- Impossible to guess
Why 2SKD

The hash* we store is uncrackable

We store an SRP verifier and an encrypted AES key encryption key
A new kind of secret

- Unfamiliar to users
- How should user treat it?
- How to help users not lose it?
- Two ways to be fully locked out of own data
Video 1: Setting up a Team

Chena the Psycho Dog …

1. Creates a new team
2. Sets up her own account info
3. Is assigned an Account Key
4. Creates a Master Password
5. Signs in
6. Saves Emergency Kit
7. Creates data
What kind of account do you need?

Family

Team

Already have an account? Sign in
Spreading the Account Key

- Each client will hold an Account Key locally
- Signup through browser means in browser local store
- Better to get it in other clients as well
Video 2: Enrolling 1Password for Mac

In 1Password Mac, Chena

1. Starts in Preferences > Teams
2. Clicks to add a new team
3. Selects “manual” to add details
4. Decides again “manual”
5. Scans QR code
6. Enters Master Password
7. Checks her Team data
Video 3: Morgan joins

1. Chena invites Morgan
2. Morgan signs up
3. Chena confirms signup
4. Morgan creates data in Personal Vault
Rabbit-Hunters is using 1Password!

Chena the Psycho Dog ([jeff+chena@agilebits.com](mailto:jeff+chena@agilebits.com)) wants you to join Rabbit-Hunters on 1Password.

Grrr. Woof woof.

1Password is here to help you...

- Never lose a password again
Account recovery

- Team/Family Organizers have all vault keys
- Organizers don’t always have access to vault data
- We, AgileBits, do not have any of these keys
- There is no recovery possible if Organizers lose Account Key or forget Master Password
The road to recovery starts here.

Your Rabbit-Hunters account on 1Password has been placed into recovery mode. You can now create a new secret Account Key and choose a new Master Password.

Once you proceed, you won’t be able to use your account until your Team Admin finishes the recovery process. We’ll send you another email when you
Will people treat Account Keys properly

- Will our users understand that it is a secret?
- Will they understand that it is their secret? (For example, it not like a license key, which would be our secret)
- Can we do more to prevent catastrophic data loss?
Usable Security is a moving target.

We cannot rest on our laurels.