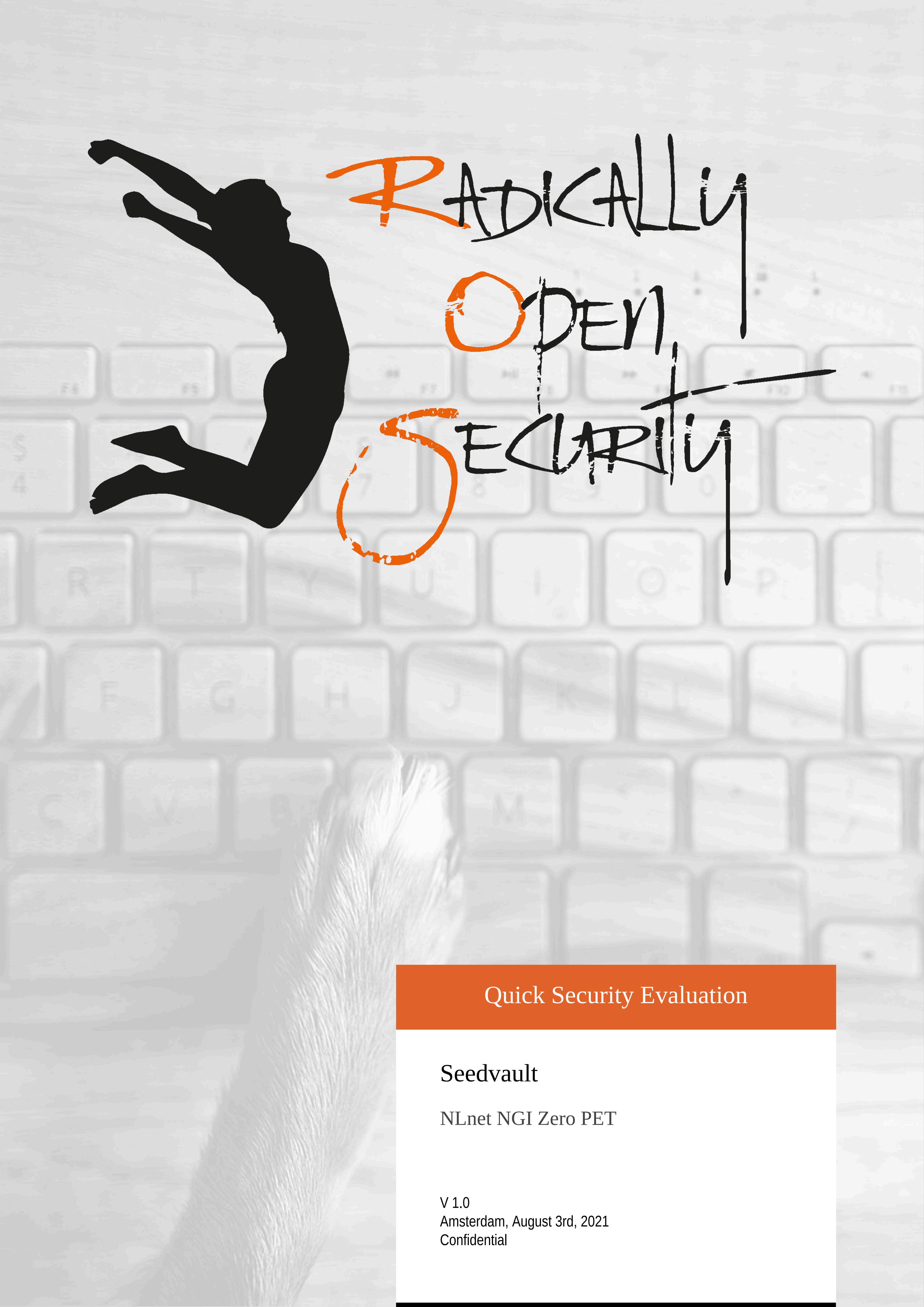

Radically Open Security

Quick Security Evaluation

Seedvault

NLnet NGI Zero PET

V 1.0
Amsterdam, August 3rd, 2021
Confidential

1 Introduction

As part of the NLnet projects your project **Seedvault** has received a basic quick security evaluation from Radically Open Security. The goal of the review is to provide advice and input to consider in the further development of your project. The selected project gets 2 persondays from ROS for a quick security evaluation. This was split to one day of evaluation in January 2021 and one day at a later phase of the project in July and August 2021.

2 Security Evaluation For Seedvault

Tasks Performed

- Reviewed the previous project communication.
- Reviewed the seedvault-LFB design document.
- First review of the project repository in January 2021.
- Discussion with representative of the project in the ROS chat and via video conference.
- Overview of code dependencies.
- Brief study of cryptographic code dependencies.
- In-depth discussion of cryptographic design, thread model and related questions via video conference.
- Second review of the project repository in July and August 2021.
- Overview of public Github issues.
- Brief look at documentation, changelogs and recommended software.
- Public participation on two Github issues GH74 and GH138 as asked by the developers.

Security Considerations

- There are known problems with integrity guarantees for backups due to lacking Android APIs. Additionally, the Seedvault application currently does not offer user-triggered verification checks (issue #12).
- Discussed some of the externally proposed changes with regards to the encryption schemes and key usage, specifically allowing regular full disk encryption passphrases, using smartcards and hardware tokens as well as offering a mode completely without encryption. To summarize, it is currently recommended to stay with the existing security model (issue #18).
- Attack scenario with temporary physical access to an unlocked smartphone with Seedvault (issue #17).
- Discussed strengths and weaknesses of the multi-layered key derivation scheme (issue #8).
- Generally discussed the requirements on random number generator output at Seedvault key generation (issue #2).
- Generally discussed attack scenarios involving compromised smartphone devices such as malware in backups (issue #6).

Recommendations - First Analysis

- Consider the NovaCrypto dependency as essential to the project security and introduce documentation and review steps for upgrades that reflect this (issue #9).
- Introduce some automated testing that compares the NovaCrypto BIP39 output to equivalent operations of a second, widely used crypto library to spot discrepancies.
- Update the existing cryptographic design document to match the current state in terms of employed mechanisms such as compression and describe all key derivations.
- Include documentation and configuration to limit information leakage through the long-lived SQL cache layer.

Recommendations - Second Analysis

- After the replacement of the NovaCrypto BIP39 library, similar recommendations as before apply to the new Zcash/kotlin-bip39 library dependency.
- It is recommended to add some documentation on the risks of using third party software, especially together with the secret BIP39 key (issue #21).
- Some of the public documentation of cryptocurrency software and hardware wallets may be helpful when determining UI/UX patterns or recommendations to the user with regards to the BIP39 word handling.

3 Contact details

Your pentester for this project:

- Christian Reitter
  Christian Reitter is an IT Security Consultant with experience in the area of software security and security relevant embedded devices. After his M. Sc. in Computer Science, he has worked as a developer and freelance security consultant with a focus on fuzzing research. Notable published research includes several firmware vulnerabilities in popular cryptocurrency hardware wallets, including remote theft of secret keys and circumvention of 2FA protection. He has also discovered multiple memory issues in well-known smartcard driver stacks.

If you have any questions about this advice, please contact us at info@radicallyopensecurity.com

For more information about Radically Open Security and its services please visit our website: www.radicallyopensecurity.com.

4 Disclaimer

This evaluation is not to be considered a full audit or pentest. It is important to understand the limits of ROS' services. ROS does not (and cannot) give guarantees that something is secure. Additionally, the above advice is obviously incomparable to a full-blown security audit as performed by ROS or any other professional security company, which takes orders of magnitude more time and effort. (Such an audit may be necessary in the future still, and we would be happy to work with you on that).

We recommend for now you treat our feedback as a discreet sanity check by knowledgeable friends; it is not the intention to publicly claim that Radically Open Security audited your code and found it to be safe or 'found no problems'. Rather, the intention is the reverse: we aim to help you capture obvious flaws within the very limited terms of this deal, and to protect the general audience from irresponsible projects putting them at risk. NGI Zero takes the public interest very seriously and wants to have at least a rough understanding of the maturity of your work - hopefully this will guide your own behaviour in terms of any claims you make.

There is no shame in clearly messaging to users that your project is still in an early stage, that they use it at their own risk and that there are no guarantees - being honest with your users can only ever be a good thing.

Front page image by PickPik (https://www.pickpik.com/), "Dogs paw on the wooden keyboard", Image styling by Patricia Piolon, royalty-free stock photo.