The Federated Open Key Service (FOKS)

Maxwell Krohn (max@ne43.com)

March 14, 2025

Abstract

This paper presents FOKS (Federated Open Key System), a decentralized key management system designed to provide secure and flexible key distribution across federated networks. We describe the system architecture, security model, and implementation details.

1 Introduction

2 Background

3 System Architecture

4 Security Model

5 Implementation

6 Evaluation

7 Related Work

The initial inspiration for FOKS is the SUNDR project [2], which first originated the idea of a fork-consistent blockchain of edits facilitated by a untrusted server. Like Keybase [1], FOKS applies this basic architecture to the problem of key distribution, rather than the data those keys might secure. Many other projects have riffed on this, from CONIKS [3], to the SEAMless work out of Microsoft Research, to the widespread adoption of Key Transparency Signal, WhatsApp and iMessage. The question of federation has largely been ignored, as these sytems all shared the basic architecture of a single upstream server.

8 Conclusion

References

[1] Chris Coyne and Maxwell Krohn. Keybase.io. `https://keybase.io`, 2014. Accessed: 2024.

[2] Jinyuan Li, Maxwell Krohn, David Mazières, and Dennis Shasha. Secure untrusted data repository (SUNDR). In *6th Symposium on Operating Systems Design & Implementation (OSDI 04)*, San Francisco, CA, December 2004. USENIX Association.

[3] Marcela S Melara, Aaron Blankstein, Joseph Bonneau, Edward W Felten, and Michael J Freedman. Coniks: Bringing key transparency to end users. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 383–398, Washington, D.C., 2015. USENIX Association.