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. The basic problem addressed is that of of two parties sharing end-to-end encrypted data across the internet, where both parties have several devices. They might rotate devices, form mutable teams with other users, or even teams of teams in an arbitrary graph. In any setting, they need to share secret key material to facility symmetric encryption, and this material must rotate whenever devices are replaced, or team membership changes. This is a very natural problem but one that still lacks an adequate solution. Morever, we believe such a system should exist that does not lock these users into a particular provider, but instead, should allow for federation and independeent management of server resouces, as we see in HTTP and SMTP. We describe the system architecture, security model, and implementation details of a system that achieves secure, federated key exchange, and enables useful applications like end-to-end encrypted data sharing and git hosting.

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 [3], 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 [4], to the SEAMless [2] 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] Keybase. Available at `https://keybase.io`.

[2] Melissa Chase, Apoorvaa Deshpande, Esha Ghosh, and Harjasleen Malvai. SEEMless: Secure end-to-end encrypted messaging with less trust. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1639–1656, 2019.

[3] 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.

[4] 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, 2015.