1. Projektziel

Im Rahmen unserer Produktentwicklung sind wir auf das OPAQUE Protokoll gestoßen und waren begeistert davon. Es erlaubt Username/Password-basierte Authentifizierung, ohne dass jemals das Password in seiner originalen Form an den Server geschickt wird. Dies basiert auf moderner Kryptographie, genauer gesagt dem OPRF Konstrukt. Weiters lässt sich das Protokoll als Basis für Ende-zu-Ende-Verschlüsslung verwenden und eröffnet ApplikationsentwicklerInnen somit neue Möglichkeiten.

Das von uns entwicklete Software Package ermöglicht es, das OPAQUE-Protokoll mittels weniger Zeilen JavaScript Code (Web, Node & ReactNative) einzurichten.

Das Kernteam der Naisho GmbH besteht aus Susanne Kristufek, Bettina Ecker (Freelancerin), Stefan Oestreicher und Nikolaus Graf. Wir arbeiten an der Software Applikation Serenity, die es erlaubt end-to-end verschlüsselt als Team an Dokumenten zu arbeiten und diese zu verwalten.

2. Projektendergebnisse

1	*Projektzwischenbericht*	*CC BY-SA 4.0*	*netidee.at/opaque*
2	*Projektendbericht*	*CC BY-SA 4.0*	*netidee.at/opaque*
3	*Entwickler_innen-DOKUMENTATION*	*MIT*	*https://github.com/serenity-kit/opaque/blob/main/CONTRIBUTING.md* *https://github.com/serenity-kit/react-native-opaque/blob/main/CONTRIBUTING.md*
4	*Anwender_innen-DOKUMENTATION*	*CC BY-SA 4.0*	*https://opaque-auth.com/*
5	*Veröffentlichungsfähiger Einseiter / Zusammenfassung*	*CC BY-SA 4.0*	*netidee.at/opaque*
6	*Dokumentation Externkommunikation zur Erreichung Sichtbarkeit /Nachhaltigkeit (als Teil des Endberichtes)*	*CC BY-SA 4.0*	*netidee.at/opaque*
7	*Opaque Package veröffentlicht in eine Github repository und publiziert auf NPM* ** Dieses Package erlaubt die Software in Websites einzubetten als auch in Node Server backend* ** Das Package ist mit Typescript typisiert und enthält eine solid Testsuite* ** Das Package enthält ein CLI Command*	*MIT*	*https://github.com/serenity-kit/opaque* *netidee.at/opaque*

	um einen Server private key zu generieren"		
8	*Opaque Package für React Native veröffentlicht in eine Github repository und publiziert auf NPM. Die p256 Variante wurde als separates Repository angelegt.* ** Dieses Package erlaubt die Software in React Native clients einzubetten und unterstützt iOS und Android* ** Das Package ist mit Typescript typisiert und enthält eine solid Testsuite*	*MIT*	*https://github.com/serenity-kit/react-native-opaque* *https://github.com/serenity-kit/react-native-opaque-p256* *netidee.at/opaque*
9	*Dieses Package enthält das Script um eines der Opaque Beispiele lokal zu erstellen.*	*MIT*	*https://github.com/serenity-kit/create-opaque* *netidee.at/opaque*

3. Geplante weiterführende Aktivitäten nach netidee-Projektende

Ein wichtiger Teil wird die Bekanntmachung und Verbreitung der Open Source Library.

Die nächste konkrete Aktivität ist ein Opaque als Teil eines Vortrags auf der ReactSummit Konferenz in Amsterdam am 14. Juni 2024. Derselbe Vortrag wird dieses Jahr auf diversen Meetups und Konferenzen einreichen.

Außerdem planen wir, sowohl die Open Source Library als auch die Dokumentation weiterhin zu pflegen. Dies ist auch eine Notwendigkeit, da wir die Library bereits für die Authentifikation in unserem Hauptprodukt Serenity verwenden.

4. Anregungen für Weiterentwicklungen durch Dritte

Unsere Lösung ist nun einfach in JavaScript-Systeme integrierbar. Dies erlaubt es Unternehmen, welche JavaScript (Node) oder Rust im Backend einsetzen, das Package zu integrieren und somit eine sichere Authentifizierung zu ermöglichen.

Potentielle Weiterentwicklungsmöglichkeiten sehen wir vor allem darin Opaque auch für diverse andere Programmiersprachen e.g. Python, Go zu portieren. Des weitern wäre es spannend, noch einfachere und bessere Erklärung und Visualisierung der OPAQUE-Protokolls in der Dokumentation.