Peer Review for William Godfrey

Manual Code Review:

Adherence and Implementation of the Protocol:

This is a really thorough and accurate Angular implementation of the protocol. I believe that it covers most of the requirements and
For example, I've seen through my code review that the following are satisfied:

- WebSocketService handles WebSocket connections. Also reconnection logic and server failover.
- UserService handles user-specific data like fingerprints and public keys.
- Implementation of various message types.
- Proper use of cryptography. Symmetric and asymmetric.
- Client discovery. Mechanism for finding other clients, through RecipientService.
- File transfer functionality.

Static Analysis:

Some of my key findings through TSLint and static analysis were the following:

- The use of the \`any\` type, reduces type safety. (for example "processSignedData(message: any)". Lack of explicit return types on some functions. All leading to some general type unsafety.

Vulnerabilities

- The CustomSanitizationService bypasses Angular's XSS protections.
- Because the counter in SignedDataService is stored within the local storage, it could be manipulated. Could lead to replay attacks.

Recommendations and Conclusion:

1. Use more specific types, instead of 'any'.
2. Enhance security, through using a more secure method for storing the message counter. Such as encrypted storage or server side management.
3. Implement more robust error handling, in WebSocket and some of the cryptographic functions.