**BoringSSL vs MbedSSL**

**Initial Remarks**

BoringSSL and mbedTLS (formerly known as PolarSSL) are both open-source cryptographic libraries that provide SSL/TLS and other cryptographic functionalities. Here are the key differences between BoringSSL and mbedTLS:

1. Origin and Forking: BoringSSL is a fork of OpenSSL created by Google to meet the specific needs of its projects. It focuses on code simplicity, maintainability, and performance. BoringSSL includes modifications and additions that are specific to Google's use cases. MbedTLS, on the other hand, is an independent project initially developed by PolarSSL and later acquired by ARM (now owned by NXP Semiconductors). It was designed specifically for embedded systems and IoT devices.
2. Codebase and Features: BoringSSL and mbedTLS have different codebases and feature sets. BoringSSL aims to provide a minimal and streamlined library with a focus on security, performance, and maintainability. It may not prioritize maintaining full compatibility with OpenSSL. MbedTLS is designed to be a lightweight and efficient library suitable for resource-constrained environments. It offers a wide range of cryptographic functionalities and supports various protocols, including SSL/TLS, DTLS, and IPsec.
3. Development and Community: BoringSSL is primarily maintained by Google engineers and benefits from contributions within the Google development community. It follows its own development processes and priorities. MbedTLS is developed by a dedicated team at ARM/NXP and has its own community of users and contributors. It places a strong emphasis on the embedded systems and IoT community.
4. Platform Support: Both BoringSSL and mbedTLS support multiple platforms, including Linux, Windows, macOS, and embedded systems. However, mbedTLS places a strong focus on embedded systems, IoT devices, and resource-constrained environments. It provides platform-specific optimizations and features tailored for these environments.
5. Licensing: BoringSSL is released under the Apache License 2.0, which is a permissive license. MbedTLS is dual-licensed, offering both an Apache License 2.0 and a GPLv2 license.
6. Industry Adoption: BoringSSL is primarily used by Google and integrated into various Google projects and services. It may have limited adoption outside of the Google ecosystem. MbedTLS is widely used in embedded systems, IoT devices, and security-focused applications. It has a strong presence in the embedded systems and IoT community and is integrated into various products and projects.

When choosing between BoringSSL and mbedTLS, consider your specific requirements, platform support, licensing preferences, and the level of compatibility needed with existing software. If you are working on a project that aligns with Google's use cases and prioritizes simplicity and performance, BoringSSL may be a suitable choice. If you need a lightweight and efficient library tailored for embedded systems and IoT, mbedTLS might be a better fit.

**Testcase Directories:**

1. 20220421\_170646\_boringssl-f0451ca-mbedtls-2.2.1-update-1\_tgt-0\_all
2. 20220421\_171656\_boringssl-f0451ca-mbedtls-2.2.1-update-1\_tgt-1\_all
3. 20220511\_172345\_boringssl-f0451ca-mbedtls-2.2.1-update-1-rank-1-03454\_tgt-0\_all
4. 20220511\_173318\_boringssl-f0451ca-mbedtls-2.2.1-update-1-rank-1-03454\_tgt-1\_all
5. 20220511\_174130\_boringssl-f0451ca-mbedtls-2.2.1-update-1-rank-2-2d5b7\_tgt-0\_all
6. 20220511\_175102\_boringssl-f0451ca-mbedtls-2.2.1-update-1-rank-2-2d5b7\_tgt-1\_all