Open Enclave SDK Project Review 2022

As a project of the Confidential Computing Consortium (CCC) in the [Incubation](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fconfidential-computing%2Fgovernance%2Fblob%2Fmaster%2Fproject-progression-policy.md%23incubation-stage&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608492265%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=W3Gg5kh3i5MGjjfkK2m7iDMFSkczl9wzmXuZQzmioGA%3D&reserved=0) stage, the [Open Enclave SDK](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fopenenclave%2Fopenenclave&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608502262%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=NA8PSWNZQYb4kpV8x2d2IcVTgF%2FqenohzODPHbg7Dh0%3D&reserved=0) has published a [growth plan](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fopenenclave%2Fopenenclave%2Fpull%2F3448%2Ffiles&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608502262%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=rResx77QvC0ryyQvUIgLD08dOqMHJxJeIpzs1Dd4A%2Bc%3D&reserved=0) for reaching the [Graduation](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fconfidential-computing%2Fgovernance%2Fblob%2Fmaster%2Fproject-progression-policy.md%23graduation-stage&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608512254%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=EXTi%2FxOs6mC9waZj4SEyn1f1ZVdOFFXPISBOCvN5B3Y%3D&reserved=0) stage in accordance with CCC Technical Advisory Council mentorship. This report summarizes updates of the project information since its annual report a year ago and progress against the growth plan over the last year.

1. Updated and additional information for the project submission template since the last annual report:

* List of project official communication channels
  + [https://chat.openenclave.io/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fchat.openenclave.io%2F&data=04%7C01%7CSimon.Leet%40microsoft.com%7C94a8eeba10294fcb043d08d885031766%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637405595608572220%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=UIm%2FY8e%2BXozixM71hbTruIfgYEhGxPxIArhFCLAYpXs%3D&reserved=0) (Home Server: openenclave.modular.im) is deprecated. The Open Enclave SDK conducts its public communication through the [oesdk@lists.confidentialcomputing.io](mailto:oesdk@lists.confidentialcomputing.io) mailing list.
* List of 3rd party dependencies – The following new dependencies were added
  + [LLVM compiler-rt](https://github.com/openenclave/openenclave/tree/master/3rdparty/compiler-rt): Library that provides various builtin functions for a variety of architectures
    - License: Apache-2.0
  + [libgcov:](https://github.com/openenclave/openenclave/tree/master/3rdparty/libgcov) Profiler that is part of compiler-rt
    - License: Apache-2.0
  + [OpenSSL:](https://github.com/openenclave/openenclave/tree/master/3rdparty/openssl) Crypto library
    - License: Apache-2.0
  + [Intel SGX-SSL:](https://github.com/openenclave/openenclave/tree/master/3rdparty/openssl) Intel’s OpenSSL libraries for SGX(on Linux) which contain LVI mitigated implementations for OpenSSL
    - License: BSD 3-clause "New" or "Revised" License
  + [Intel SGX SDK for Linux:](https://github.com/openenclave/openenclave/tree/master/3rdparty/sgxsdk) Contains the header files retrieved from the Intel SGX SDK for Linux, that are needed for compiling the OE SDK host library for SGX platforms, when the SGX quote-ex library is integrated
    - License: BSD
  + [snmalloc:](https://github.com/openenclave/openenclave/tree/master/3rdparty/snmalloc) High performance allocator
    - License: MIT
  + [Symcrypt-engine:](https://github.com/openenclave/openenclave/tree/master/3rdparty/symcrypt_engine) OpenSSL engine to use with the symcrypt library
    - License: MIT
* Release methodology
  + Aside from the release mechanisms listed in original submission, Windows NuGet packages uploaded to <https://www.nuget.org/packages/open-enclave/>

1. In terms of the progress against the growth plan:

* The OE SDK has settled into quarterly release cadence as it stabilizes towards an LTS release, currently on v0.17.
  + Releases are also made when there are CVEs fixed in dependent libraries.
* The OE SDK is close to feature complete for SGX.
* Continues to be actively maintained, averaging ~6 commits weekly.
* The number of contributors from grew from around 90 to 100 over the past year, the project has been starred ~754 times (530 times in the last annual report) and forked 286 times (205 times in the last annual report).
* The committers are making progress towards the completion of [Inclusive Open Source Community Orientation.](https://training.linuxfoundation.org/training/inclusive-open-source-community-orientation-lfc102/) This is currently tracked by an [issue](https://github.com/openenclave/openenclave/issues/4319) on the repo.
* The CGC is actively working on the remaining requirements for graduation:
  + The CGC is the governing body of the OE SDK project. The CGC currently consists of people from 3 different companies. We are therefore progressing towards our goal of getting to the ratio of members in the CGC from a single employer to be equal to or less than 1/3.
  + The project is in the process of encouraging contributors to become full committers and eventually members of the CGC. We feel that we have not achieved a healthy number of committers from at least two organizations.
  + OE SDK has not yet published a public list of adopters (i.e. ADOPTERS.md) or advertised their logos as recommended in the project progression policy.

At this point, the OE SDK is not ready to request a vote from the TAC to move to the Graduation stage, and will continue to iterate on its growth plan to address the remaining requirements as follows:

* + Invite contributors from other organizations to become maintainers and members of CGC as they demonstrate good contributions via PRs and/or Issues filed and/or code/design review feedback.
  + Expand to other TEEs and other OS's by inviting contributions.

1. For budgeting purposes
   * The Zoom account used for public meetings is funded by CCC.
   * The OE SDK DL oesdk@lists.confidentialcomputing.io is hosted via CCC’s "groups.io" site.
   * There was a basic LF license scan done.
   * There only new request for budget at this time is to perform another basic LF license scan on the repo once the problems found in the last scan are mitigated. Please see the following section for more details.
2. [Results of license scan:](https://lfscanning.org/reports/ccc/openenclave-2021-09-16-7e3b9beb-97a5-4f46-867e-81d9e0ad5be0.html) Mitigations in progress

|  |
| --- |
| **Finding #1**  **Files:**  Openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/bin/busybox  Priority: Very High  **This appears to be a compiled binary / object code file that contains GPL-2.0 content without corresponding sources. This file should be removed from the repo.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).        **Finding #2**  **Files**:  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace-log-merge  Priority: High  **This file contains content under LGPL-2.1, a weak copyleft license. This file should likely be removed from the repo.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).      **Finding #3**  **Files**:  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/qemu-system-aarch64  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/lib/libpthread-2.28.so  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/usr/bin/strace  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/ls-ls1012grapeboard/lib/openenclave/enclave/liboelibc.a/iconv.c.o  openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/sdk/optee/vexpress-qemu\_armv8a/lib/openenclave/enclave/liboelibc.a/iconv.c.o  Priority: High  **This appears to be a compiled binary / object code file. We do not recommend including binary files in the source code repo. These files should likely be removed.**  **Mitigation**: Pull devkit out of the repo and place it on a blob store. Pull it during extension’s build process and provide documentation pointing directly to public sources for creating the devkit binary (buildroot/OP-TEE test framework).      **Finding #4**:  **Files:** Doxygen generated docs used on https://openenclave.io  Priority: High  **This file contains a notice that it is distributed under a version of the GPL. This file should likely be removed from the repo, since it is under a strong copyleft license that is not typically viewed as compatible with OpenEnclave's MIT project license.**  487 files (show files)  **Mitigation**: None: Documents produced by Doxygen are derivative works derived from the input used in their production; they are not affected by Doxygen’s license. (From <https://www.doxygen.nl/index.html> )    **Finding #5**:  **Files**:  openenclave/3rdparty/openssl/include/bn\_conf.h openenclave/3rdparty/openssl/include/dso\_conf.h openenclave/3rdparty/openssl/include/opensslconf.h openenclave/devex/vscode-extension/assets/devkit/devdata.tar.gz/devdata.tar/emu/vexpress-qemu\_armv8a/rootfs.cpio.gz/rootfs.cpio/etc/ssl/misc/tsget.pl openenclave/docs/GettingStartedDocs/Contributors/SignUsingEngines.md  Priority: Medium  **This file contains content under the old (pre-3.0.0) OpenSSL license. The old OpenSSL license used to require certain statements to be included in advertising materials and redistributions. Is it possible to omit these files from the repo, or to upgrade them to versions from OpenSSL 3.0.0 or later (which are under Apache-2.0)?**  5 files (show files)  **Mitigation**: Cannot delete all files. Plan to move to OpenSSL 3.0.0 likely next year since developers using Open Enclave SDK need enough lead time to upgrade to OpenSSL 3.0.0 |