Zephyr Project Security WG Meeting

** For Table of Contents / Document outline, select the ☰ button to the upper left

Prior Years: Security Working Group Meeting Minutes

- March 14 - December 31, 2022

Ways to join meeting:

1. Join from PC, Mac, iPad, or Android

https://zoom-lfx.platform.linuxfoundation.org/meeting/91063909291?password=708b7604-fd5c-4458-8247-ca861eb35458

2. Join via audio

One tap mobile:
US: +12532158782,,91063909291# or +13462487799,,91063909291

Or dial:
US: +1 253 215 8782 or +1 346 248 7799 or +1 669 900 6833 or +1 301 715 8592 or +1 312 626 6799 or +1 646 374 8656 or 877 369 0926 (Toll Free) or 855 880 1246 (Toll Free)
Canada: +1 647 374 4685 or +1 647 558 0588 or +1 778 907 2071 or +1 204 272 7920 or +1 438 809 7799 or +1 587 328 1099 or 855 703 8985 (Toll Free)

Meeting ID: 91063909291

Meeting Passcode: 649363

International numbers: https://zoom.us/u/alwnPIaVT

LF Antitrust Policy Notice

Zephyr Project meetings invoice participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, and activities that are prohibited under applicable US state, federal, or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Zephyr Project meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation

Zephyr Project Security WG - Nov 20, 2023

Agenda:

- Static Analysis - Audit group creation
- Software security training (https://ost2.fyi/)
- Crypto drivers enhancements and security subsystem covering:
    - AES Encryption and Decryption (Currently supported by Crypto Subsystem)
- SHA/HMAC Authentication Service (HMAC is still not Implemented)
- ECDSA Signing and Verification Service (Not Implemented)
- User Key Management (Not Implemented)
- Attestation service (Not Implemented)
- Device Provisioning (Not Implemented)

Meeting Recording:
https://zoom.us/rec/share/XanlI3rQkQjg9Iy4IAw4oCTjxM0RjVB6cML3BpHcKmkrYHqChkdXvHanb24bIgIQ.Qm68oLnVv8T3LGgS

Discussions:

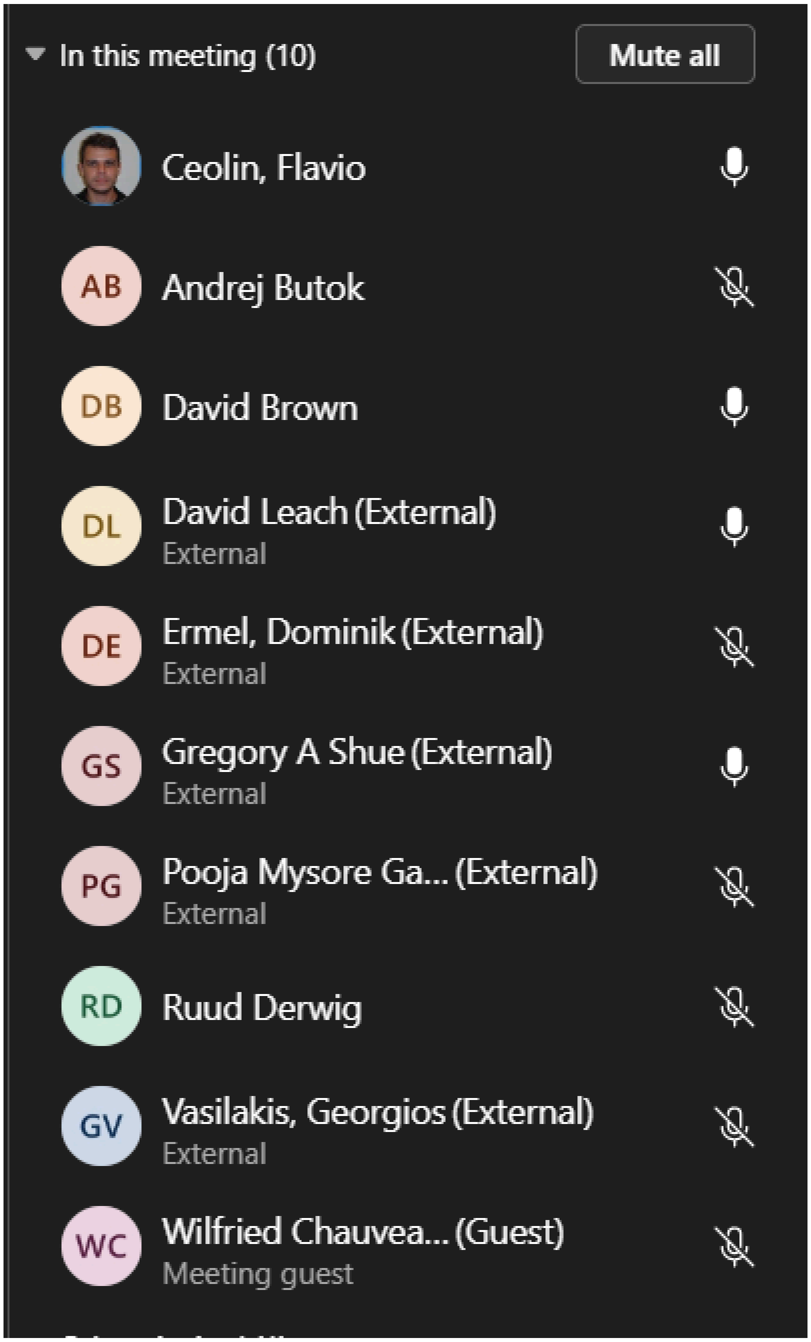
Zephyr Project Security WG - Oct 23, 2023

Agenda:

- Static Analysis (Coverity) process
- Security Standards
- PSA crypto continuation

Discussions:

Zephyr Project Security WG - Sept 25, 2023



Ceolin, Flavio

Andrej Butok

David Brown

David Leach (External)
External

Ermel, Dominik (External)
External

Gregory A Shue (External)
External

Pooja Mysore Ga... (External)
External

Ruud Derwig

Vasilakis, Georgios (External)
External

Wilfried Chauvea... (Guest)
Meeting guest

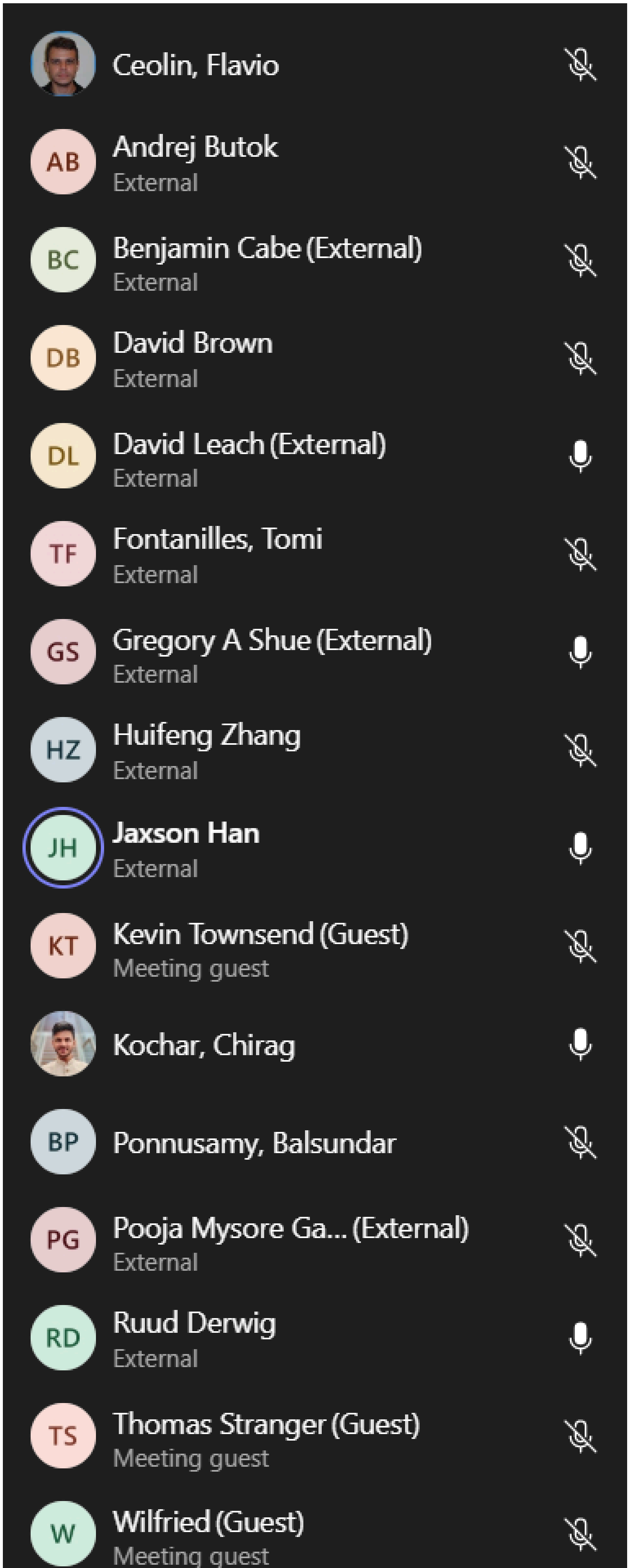
Agenda:

- Security Standards and requirements

Zephyr Project Security WG - Sept 11, 2023

Meeting canceled

Zephyr Project Security WG - July 31, 2023



Ceolin, Flavio

AB Andrej Butok
External

BC Benjamin Cabe (External)
External

DB David Brown
External

DL David Leach (External)
External

TF Fontanilles, Tomi
External

GS Gregory A Shue (External)
External

HZ Huifeng Zhang
External

JH **Jaxson Han**
External

KT Kevin Townsend (Guest)
Meeting guest

Kochar, Chirag

BP Ponnusamy, Balsundar

PG Pooja Mysore Ga... (External)
External

RD Ruud Derwig
External

TS Thomas Stranger (Guest)
Meeting guest

W Wilfried (Guest)
Meeting guest

Agenda:

- [RFC]Introduce Hardware-level Device Isolation Subsystem https://github.com/zephyrproject-rtos/zephyr/issues/60289
- View 1 · Security (github.com)

Discussions:

Zephyr Project Security WG - July 31, 2023

Agenda:

- p256-m (follow up)
- View 1 · Security (github.com)

Discussions:

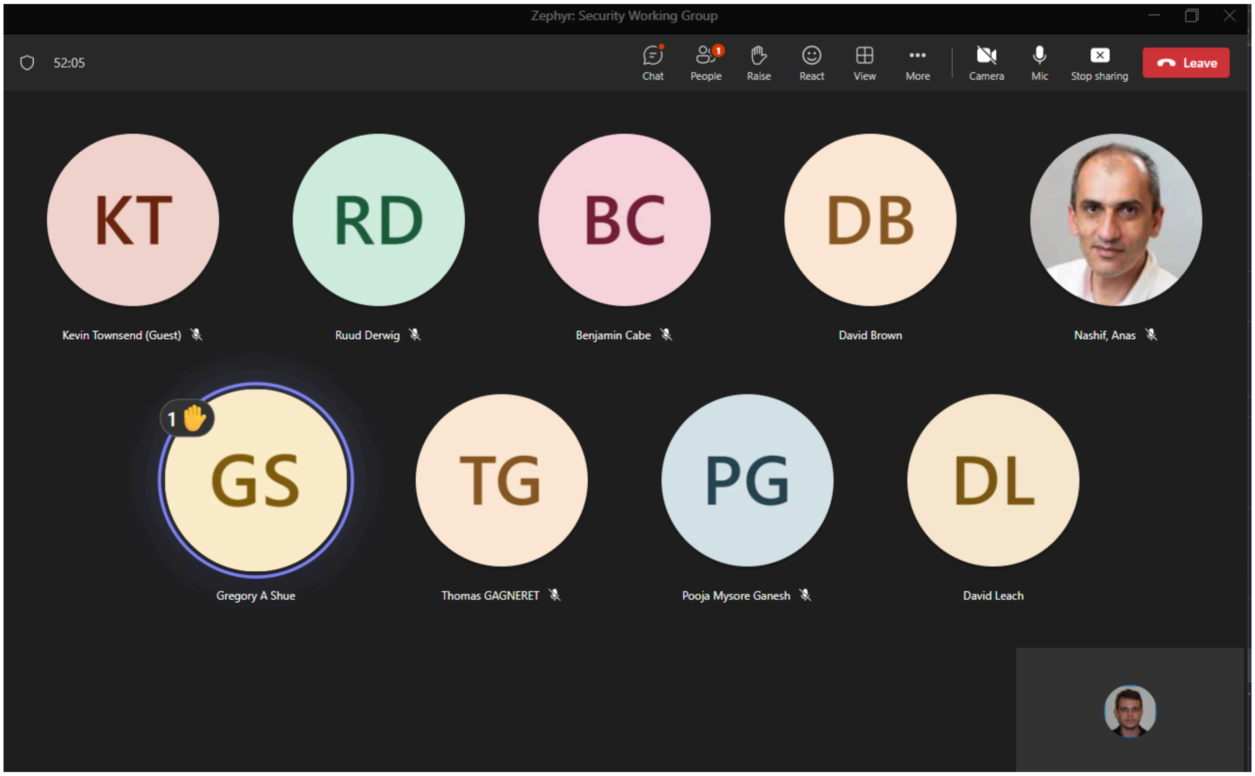
Zephyr Project Security WG - July 17, 2023

Agenda:

- p256-m (possible replacement for TinyCrypt use cases)
- Future plans for mbedTLS / TF-M / Zephyr maintainability (specially on LTS)
- SBOM and third party modules vulnerabilities
- Touch base on PSA Crypto

Discussions:

Zephyr Project Security WG - May 22, 2023



Agenda:

- Clean disable of boot image and hardware before handoff to app image https://github.com/zephyrproject-rtos/zephyr/issues/44564
- [mbedtls/tf-m] PSA API conflicts

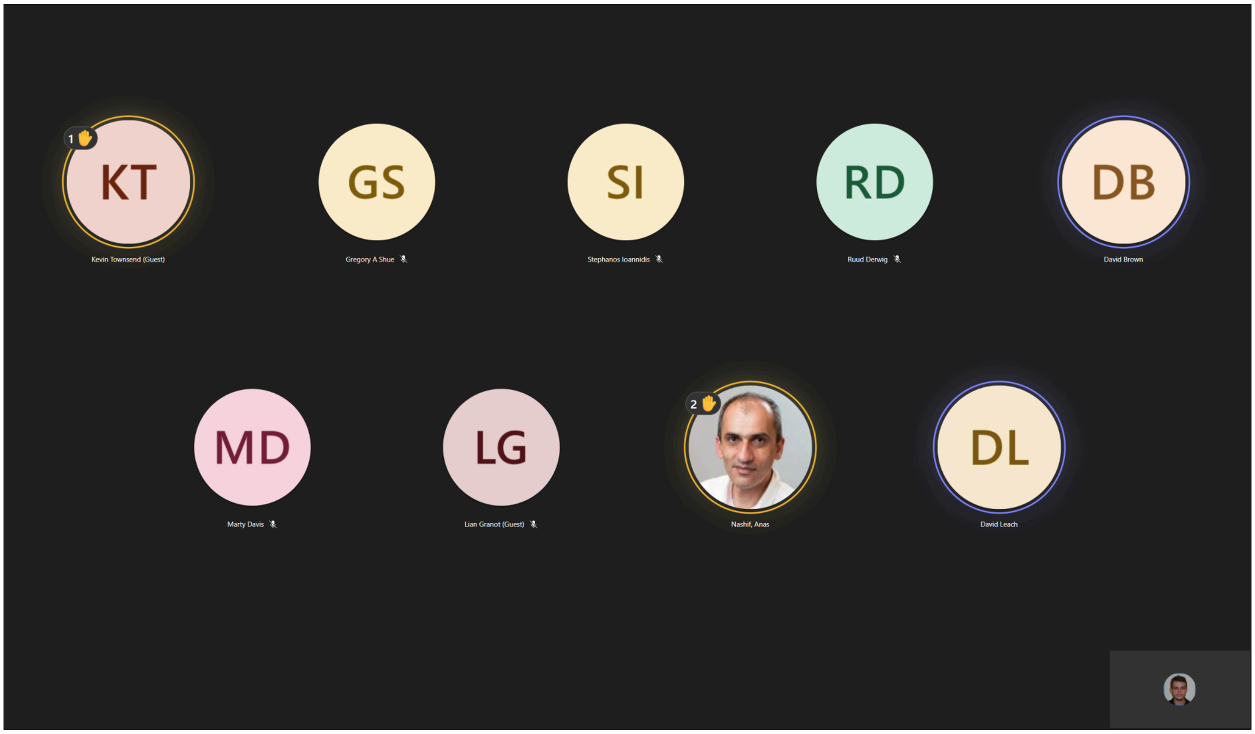
https://github.com/zephyrproject-rtos/zephyr/issues/56995

- Support Uptane as a way to update Zephyr software https://github.com/zephyrproject-rtos/zephyr/issues/52987

Discussions:

Zephyr Project Security WG - May 08, 2023

Attendees:



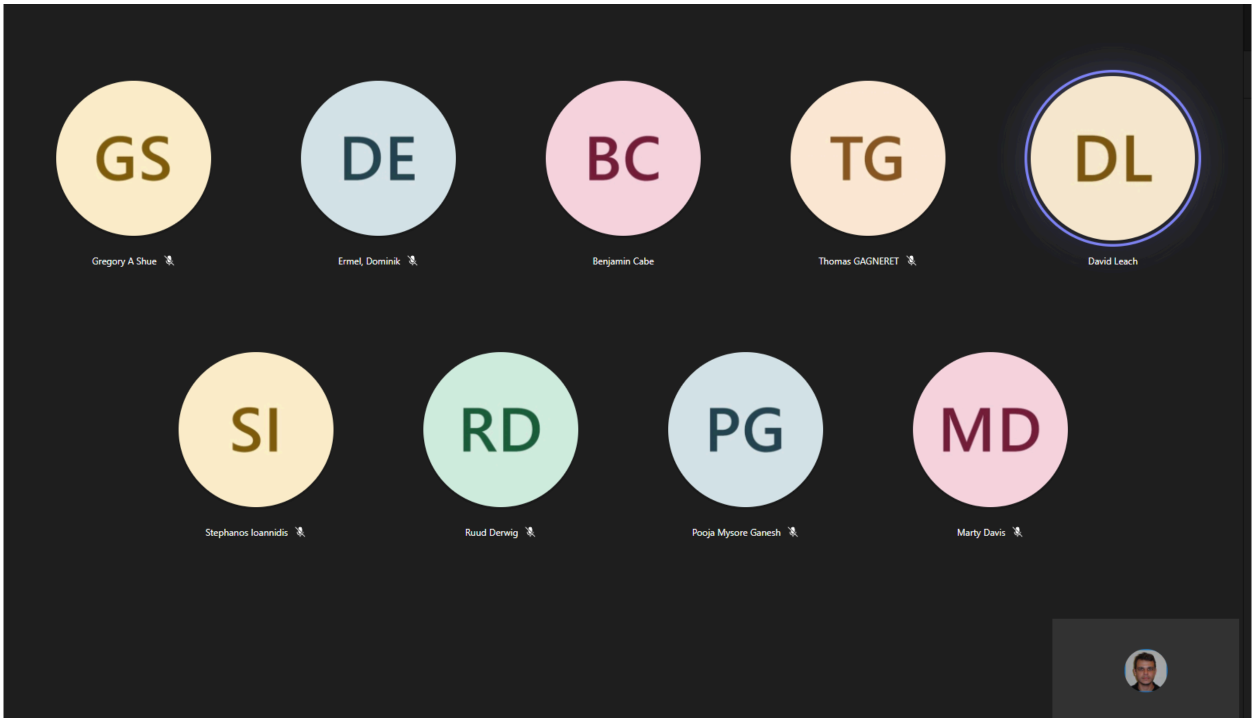
Kevin Townsend (Guest)
Gregory A Shue
Stephanos Ioannidis
Ruud Derwig
David Brown
Marty Davis
Lian Granot (Guest)
Nashif, Anas
David Leach

Agenda:

- mbedTLS vulnerabilities on Zephyr LTS
    - https://github.com/zephyrproject-rtos/zephyr/issues/56071
-

Zephyr Project Security WG - April 24, 2023

Attendees:



Agenda:

- mbedTLS vulnerabilities on Zephyr LTS
  - https://github.com/zephyrproject-rtos/zephyr/issues/56071
- Add OpenSSF Scorecard
  - https://github.com/zephyrproject-rtos/zephyr/issues/50975
- Vulnerabilities in Zephyr modules
  - https://github.com/zephyrproject-rtos/zephyr/issues/53479
- Support for OSV-scanner
  - https://github.com/zephyrproject-rtos/zephyr/issues/56884
- Clean disable of boot image and hardware before handoff to app image
  - https://github.com/zephyrproject-rtos/zephyr/issues/44564

Discussions:

Zephyr Project Security WD - April 10, 2023

Attendees:

Agenda:

        - Request for a new crypto library (https://github.com/zephyrproject-rtos/zephyr/issues/56411)
        - mbedTLS update on Zephyr LTS (https://github.com/zephyrproject-rtos/zephyr/pull/54084)

Zephyr Project Security WG - March 13, 2023

Attendees: Flavio Ceolin, David Leach, David Brown, Gregory Shue. Thomas GAGNERET
Agenda:

-

Zephyr Project Security WG - January 23, 2023

Attendees: Flavio Ceolin, David Leach, David Brown, Kevin Townsend, Greg Shue, Anas Nashif , Thomas S., Marty Davis, Pooja Mysore

Agenda:

- ETSI EN 303 645 (https://docs.google.com/spreadsheets/d/1HZU95peYek_7GCEJJoITI7IKI-rhXxfyG1eRyz9MIiA/edit#gid=0).
- mbedTLS update and TF-M
- Vulnerabilities in Zephyr modules https://github.com/zephyrproject-rtos/zephyr/issues/53479

Discussion:

- Kevin working looking to de-couple mbedTLS from TF-M for next release.
    - There are conflicts between TF-M and mbedTLS projects
- [Kevin] TF-M uses QCBOR and it is pulling from internet we need a fork
    - [David] That is against Zephyr policy
    - [Anas] I rather having an exception than creating a module
        - That is not different from SoF that has other dependencies, like rimage.
- [Anas] Do we need to build TF-M as part of Zephyr's build ?
    - [David Brown] That is probably a "hack"
- [ceolin] Zephyr has to take responsibility on modules vulnerabilities
    - Dependabot does not understand west
    - It seems it is possible to monitor arbitrary repositories
- [ceolin] https://docs.cvesearch.com/#api-details provides an API to query CVEs
- Deadline - 30 days to review https://docs.google.com/spreadsheets/d/1HZU95peYek_7GCEJJoITI7IKI-rhXxfyG1eRyz9MIiA/edit#gid=0
    - [Anas] Zephyr should be generic about standards. Mark in the project documentation which items met a standard requirement

- [ceolin] Ensure everyone in the meeting have access to the document