Companion note for the Public review of document GPT_SPE_153 – SESIP Profile for WPC Qi Secure Storage Subsystem

Purpose: Following the Committee review of the document, a liaison was established with the Wireless Power Consortium, in order to obtain clarifications on the choice of the SESIP2 assurance package.

Question from the GP TEE-MCU Security Working Group:
"We would like to ask the Wireless Power Consortium to confirm the choice of AVA_VAN.2 and share the rationale behind it – including which attacks and types of attackers the chosen level is expected to be a sufficient deterrent against and what the residual accepted risks are, for instance in relation with counterfeiting activities."

Answer from WPC:

- *Rationale for which attacks and types of attackers the chosen level is expected to be a sufficient deterrent against:*
    - *The reason WPC believes the proposal (including AVA_VAN.2) is no less adequate than our existing accepted certifications, is based upon an independent assessment provided to us from SGS Brightsight*
    - *Value to the WPC of a security certification—is confidence that simple compromises or human error during development is minimized*
    - *Manufacturers that did not take simple precautions against counterfeiting (e.g. forget to lock the debug interface in a microcontroller used as a TOE)*
- *Residual accepted risks (for instance in relation with counterfeiting activities):*
    - *Known methods of compromise exist*
    - *PTx (wireless charger products) are typically not field updatable devices, so cannot be protected against future attacks*
    - *Supply chain theft e.g. bribery of a courier driver carrying a Tape & Reel (T&R) of 60,000 pieces of provisioned secure storage subsystems (WPC term describing our Target Of Evaluation, TOE) being delivered between a provisioning site and an end product's final assembly site*
    - *WPC relies upon its Certificate Revocation List (CRL) to mitigate any compromises that do occur*
    - *Certificate Revocation List must keep up with compromises to be effective; this implies WPC actively searches for counterfeit devices—WPC will add this to its existing "Market Surveillance" program*