ioXt
internet of secure things

Frequently Asked Questions

Q: Where can an OEM learn more about the ioXt Pledge and the Android Profile?
A: The pledge is available here and the certification details for the baseline and Android Profile are here.

Q: Does an OEM need to be a member of ioXt to do a self-assessment?
A: Yes, the OEM must be an Implementor or Contributor. Membership is free. See the membership chart.

Q: How does an OEM submit their self-assessment?
A: Three easy steps:

1. Create an account.
2. Enter the device through the online wizard.
3. On payment screen, select invoice, enter the Google PO # and "Google Authorized" in the Comments section to ensure the fee will be waived for the first device. More info here.

Q: How long does it take for the self-assessment to show up on the ioXt Certification Portal?
A: The self-assessment takes about 2-4 business hours to show up.

Q: Who can the OEM reach out to if they have any questions about the specific criteria descriptions or the process?
A: Rebecca Onaitis (rebecca@ioxt.com) is the program's primary point of contact.

Q: How often can the OEM change the data submitted to ioXt?
A: Data can be changed as often as you wish. New software versions are very easy to add and are covered under the single fee per SKU.

Q: How would scoring apply to device variants for different regions?
A: In general, you certify per SKU. The goal being the images and data shown on the website match what a consumer will see in their market. If a single product has multiple SKUs, arrangements can be made to waive the certification fee for each additional SKU only if the product remains functionally identical across each SKU.

Q: Can the score change over time for a specific device model? For example: Automatically Applied Updates is something the OEM may need to keep updating on a periodic basis. Or maybe an OEM decided to undergo NIAP in the 2nd year for Proven Cryptography for a specific model.
A: The core requirements can change over time, but new profiles will contain a version number whenever the core security levels change. Possible reasons the score may change is if a

researcher finds an issue, or a new firmware version changes the security rating of the device (up or down). Therefore, the SmartCert label and API integrations into ecosystems and retail sites are vitally important.

Q: How will the standard evolve over time? Will it be updated every year? Will there be any visual indicators (i.e. version #) to help cover the changes?
A: The core standard will evolve over time and will happen no less than every 12 months. In addition, profiles will also evolve and be merged over time. Yes, there will be visual indicators: the current base profile is ioXt 2020 Base and next year, the base profile will be ioXt 2021 Base.

Q: What happens to devices that were rated against the older version and now the newer version?
A: Each SKU can have multiple firmware versions and ratings. The website allows a user to view each rating for each version.

Q: What is the expectation for recertification? Should a vendor recertify with every major OS release (i.e. going from Android 10 to 11) or if the ioXt base is updated?
A: You must recertify if your product rating has changed. The second trigger to recertification is if the profile you are certifying under has changed. We recommend that you register the new major OS releases in the portal so that the consumers & researchers can see the different versions that are available.

Currently ioXt has no requirement for periodic recertification - when a product becomes known to no longer be compliant, it will be delisted as a compliant product. For example, if a manufacturer or researcher or member of ioXt certification committee notes that a product is no longer receiving security updates, then the product would be delisted.

Q: Is there a visual indicator or notification if a SKU rating changes?
A: The ioXt SmartCert logo is removed if a device drops below the certification minimum. It can get reapplied if the issue is addressed by the manufacturer. Currently, the ioXt product listing shows a snapshot of the latest known security posture.

Q: How does the process work where a researcher can challenge the score for an OEM self-attestation?
A: A third-party researcher may challenge published results at any time by submitting through the ioXt researcher portal. Such claims are reviewed by the ioXt certification committee.

Q: How is the preloads risk score calculated?
A: Preloads risk scores can be determined using open source projects such as Uraniborg. A Uraniborg score of less than 6.25 is considered “Very Low”. A Uraniborg score of 6.25 to 7.5 is considered “Low”. A Uraniborg score of 7.5 is considered “Medium” and all scores greater than 7.5 is a failure.