GLOBAL CERTIFICATION FORUM
Consumer IoT Security Accreditation Program Procedures

Reference:	GCF-Consumer IoT Security
Version:	3.2.0
Date:	4 March 2021
Document Type:	Permanent Reference Document (PRD)

Table of Contents

1 Scope

This document is the top-level description of the process by which Consumer IoT product manufacturers can declare their product compliance to the requirements as specified in GCF Consumer IoT Security Declaration.3.x.x

The GCF Consumer IoT Security Accreditation Program can be used by any Consumer IoT product manufacturer, regardless of their membership status in GCF.

The declaration is only applicable for Consumer IoT end products and is not applicable for IoT modules and IoT chipsets, and constrained devices (as defined in ETSI EN 303 645).

The user shall preserve the confidentiality of this document and shall abide by the procedural guidelines established by GCF concerning its distribution.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this document is available at http://iotsecurity.globalcertificationforum.org

Any errors or feedback to the present document, should be sent to: iotsecurity@globalcertificationforum.org

2 References

The following may be cited or referenced in this document.

ETSI EN 303.645 Cyber Security for Consumer Internet of Things

3 Declaration Process

The following points define the specific steps required by the product manufacturer to complete the declaration:

- Review and sign the User Agreement outlining the terms and conditions for participating in the declaration program
- Complete and sign the declaration as defined in GCF Consumer IoT Security Declaration V3.x.x
- Email the completed documentation to iotsecurity@globalcertificationforum.org
- GCF Office will confirm receipt and review associated documentation
- GCF Office will invoice non-member manufacturers the declaration fee. For GCF member manufacturers, the services is offered as part of existing membership privileges.
- Upon receipt of payment, the product will be listed on the GCF portal indicating (but not limited to) the following information:
    - GCF Reference Number
    - Date of Accreditation
    - Manufacturer Name
    - Product Model Number
    - Product URL
    - Public Point of Contact
    - Compliance Version
    - Date of Last Update

- Compliance Status for
  - No Default Password
  - Reporting of Vulnerabilities, including Vulnerability Disclosure URL, and public contact information for reporting of vulnerabilities
  - Keeping Software Updated, including Support Period and Update Schedule

- A confirmation message will be sent to the product manufacturer informing them of the outcome of their declaration submission

4 Declaration Management

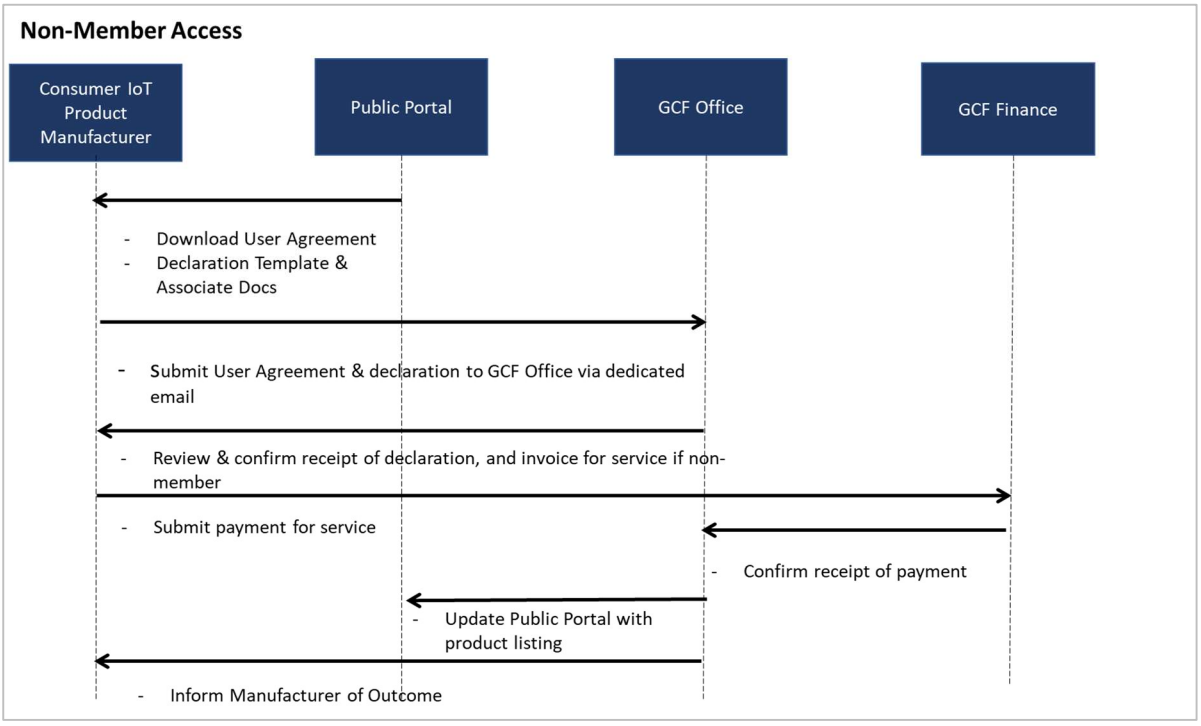
The following points define the specific steps to be followed with regards to access request for declarations from the general public, and ongoing declaration maintenance by the product manufacturer:

- Submitted declarations remain the property of the product manufacturer at all times
- Submitted declarations will be stored by the GCF, but will not be available for download via the GCF portal
- Request for access to declarations from the public shall be directed to the product manufacturer's public point of contact provided in the product listing
- Queries and concerns relating to the declaration shall be made to the product manufacturer directly via the public point of contact provided in the product listing
- Concerns relating to any particular declaration can be brought forward to the GCF for review should those concerns not be addressed by the product manufacturer
- Formal contests to declarations can be brought forward by the public to the GCF Office with supporting evidence of non-compliance
- The GCF Office will review the contest and address any issues directly with the product manufacturer
- If a contest is deemed to be valid, the product listing will be delisted while the product manufacturer addresses any issues
- Should outstanding issue be resolved with corresponding evidence of conformity provided, the product will be relisted on the GCF portal
- The product manufacturer can at any time submit updates to any existing declaration by emailing the latest updates to iotsecurity@globalcertificationforum.org.
- The product manufacturer, at their own discretion, can at any time request the GCF to remove any of their product declaration listings from the GCF portal

5 Process Call Flows

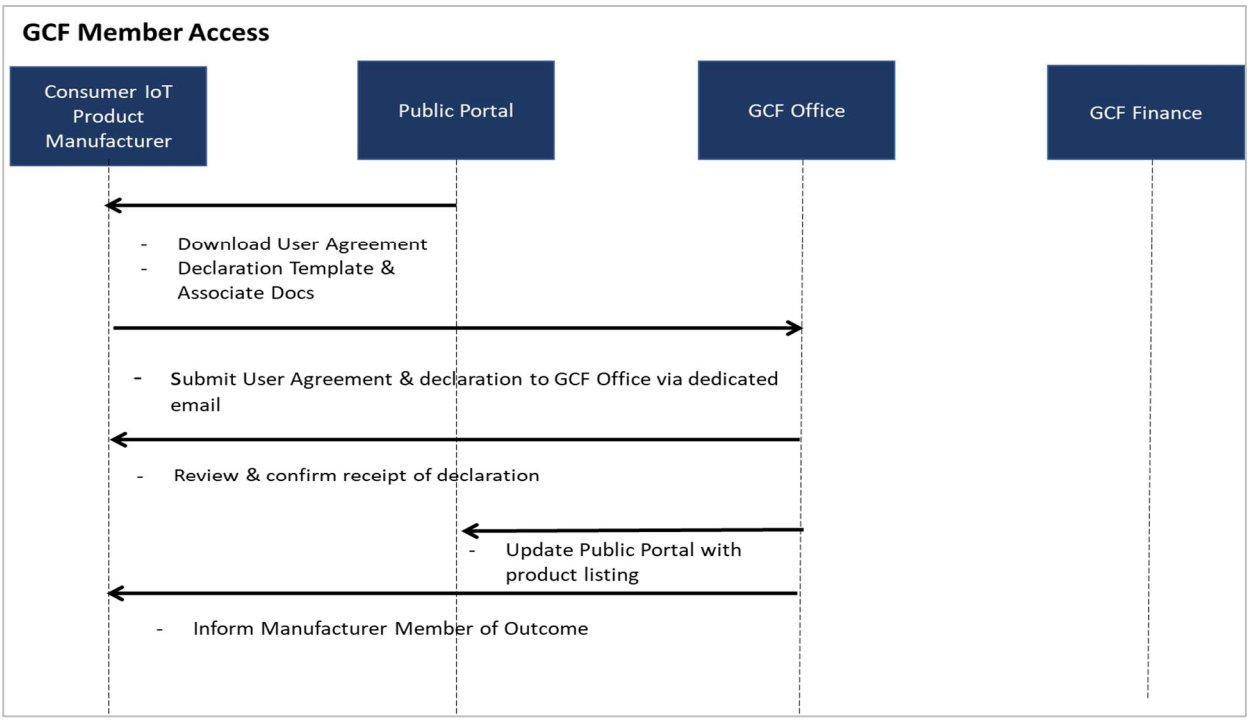
5.1 Non-Member Access

The following call flows depict the process by which GCF non-member product manufacturers access the GCF Consumer IoT Security Accreditation Program:



5.2 GCF Member Access

The following call flows depict the process by which GCF member product manufacturers access the GCF Consumer IoT Security Accreditation Program:



A.1 Declaration Template

GCF Consumer IoT Security Compliance Declaration

This Consumer IoT Security Compliance Declaration is only applicable for Consumer IoT End Products. It is not applicable for IoT Modules and IoT Chipsets, and constrained devices (as defined in ETSI EN 303 645).

Declaration:

Manufacturer's Name: _____

Manufacturer's Business Address: _____

I, _____[Insert Signatory Name]_____, declare that _____[Insert Product Name]_____

as described below and submitted by _____[Insert Manufacturer Name]_____, having its principal place of business as indicated above, has conducted Self-Assessment on the afore-mentioned Product in accordance with the following guidelines as defined in ETSI EN 303 645 Cyber Security for Consumer Internet of Things

I, _____[Insert Signatory Name]_____, also acknowledge that it is my responsibility to maintain this compliance for the above referred device, and have it reviewed as part of my quality assurance programme.

Relevant version of **ETSI EN 303 645** **Version** _____ (state declared published version)

Declared By:

Title	Name
Tel	Email
Date	Signature

1.0 Cyber Security provisions for consumer IoT:

All requirements specified below are mandatory and are required to be met in full in order to achieve GCF Consumer IoT Security Compliance.

1.1 No universal default passwords (Mandatory)

All IoT device passwords, except for the factory default shall be unique per device and shall not be resettable to any universal factory default value.

Additional Information:

1.2 Implement a means to manage reports of vulnerabilities (Mandatory)

Companies that provide internet-connected devices and services have a duty of care to consumers and third parties who can be harmed by their failure to have a CVD (Coordinated Vulnerability Disclosure) programme in place. Therefore, the company shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and other are able to report issues.

Public point of contact:

_____

Vulnerability disclosures can be access via: _____
(Ex: URL)

In addition, the policy shall provide information on timelines for:

1) initial acknowledgement of receipt; and

2) status updates until the resolution of the reported issues

Additional Information:

1.3 Keep software updated (Mandatory)

All software components in the Product shall be securely updateable, and shall maintain the overall security integrity of the product. The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required together with information on the risks mitigated by that update.

Additional Information:

1.4 Defined support period (Mandatory)

A defined support period shall be published in an accessible way that is clear and transparent to the user.

Support Period: _____ (years, months, date, etc.)

Update Schedule:_____(ex: quarterly, annually, etc.)

Additional Information:

1.5 Product URL: _____

Manufacturer Public Contact Info: _____

2.0 Additional information

Additional information of the implementation of the above requirements may be provided in the appendix to this declaration.

For products that are transmitting and storing data in the cloud, an Information Security Policy regarding the usage and management of this data is also being provided to the end user.

Appendix

Cyber Security provisions for consumer IoT:

A1.1 No universal default passwords

Requirement
All IoT device passwords, except for the factory default shall be unique per device and shall not be resettable to any universal factory default value. “Device” here means each individual physical Consumer IoT product, not e.g. the product model.
The password of the Product shall not be resettable to a default value.
In addition, the password shall not be easy to guess or predict. Where pre-installed passwords are used, these shall be produced with a mechanism that reduces the risk of automated attacks against a class or type of device.
When the Product uses password authentication, it shall only use a password that provides sufficient entropy (not easy to guess or attack via brute-force). a) Each password is checked for validity by the Product and/or an associated service (e.g. an online service) before being applied by the Product. b) A password will pass the validation check if and only if it provides sufficient entropy. c) The Product applies a password if and only if it has been successfully validated.
If a password that provides sufficient entropy is not available to the Product, the Product shall initiate a procedure to establish a new password.
The Product should have a mechanism which makes brute-force attacks on authentication mechanisms via network interfaces impractical.

Additional information

A1.2 Implement a means to manage reports of vulnerabilities

Requirement
Disclosed vulnerabilities should be acted on in a timely manner. “Timely” means here the standard practice in the industry, typically that the handling of the disclosed vulnerability on the side of the device manufacturer shall be considered complete within 90 days.
Manufacturer shall continuously monitor, identify and rectify security vulnerabilities in the Product and the related services that the Manufacturer operates during the defined support period.

Additional information

A1.3 Keep software updated

Requirement
All software components in the Product shall be securely updateable. The consumer should be informed by the appropriate entity, such as the manufacturer or service provider, that an update is required together with information on the risks mitigated by that update.
The device shall use best practice cryptography to support secure update mechanisms.
The device shall verify the authenticity and integrity of software updates.
The manufacturer should inform the consumer in a recognisable and apparent manner that a security update is required together with information on the need for that update.
An update shall be easy to apply and automatic update mechanisms should be used.
Application of an update shall be subject to user consent.
The device should check right after its first boot, and then periodically, whether security updates are available.
If the device supports automatic updates and/or update notifications, these should be enabled by default in the initialised state and configurable so that the user can enable, disable, or postpone installation of the security updates and/or update notifications.

Additional information

A1.4 Defined support period

Requirement
When software components are updateable, a defined support period shall be published for the Product that explicitly states the period of time during which software updates shall be provided for the Product and the reasons for the length of the support period. In addition, if different from the support period, the period of time during which security updates shall be provided for the Product shall be explicitly stated and published. If only the support period is explicitly stated and published, it shall be understood and interpreted that security updates for the Product shall be provided during the support period.
Each security update shall identify unambiguously all of the security issues that it resolves.
A policy shall be published in an accessible way that is clear and transparent to the consumer

Additional information

Document Change Record

Ver	Change reference			Record of changes made to previous released version	
	ACRN	Approved Date	Document	Clause	Comment
3.0.0	4017	25-Sept-2020	S-20-119	New	New PRD
3.1.0	4049	5 Nov 2020	1010DCR-CISA-001	3, A.1-1.5	Alignment with website implementation
3.2.0	4072	4 Mar 20021	IAG-21-021r1	Annex A	Several changes and updates