Internet of Things

GSMA IoT Security Assessment Process

CLP.19

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential
Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice
Copyright © 2016 GSM Association

Disclaimer
The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice
The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Overview

1. Document Purpose

This document defines the GSMA IoT Security Assessment Process that accompanies document CLP.17 "GSMA Security IoT Assessment Checklist".

The process will be published on the GSMA Internet of Things "IoT Security Assessment" website at this location: **www.gsma.com/iot/iot-security-assessment/**

2. GSMA IoT Security Assessment Process

The following process should be followed when completing a GSMA IoT Security Assessment:

1. Assess your IoT product, service or component for compliance with the recommendations and controls stated in the GSMA Security IoT Assessment Checklist document (CLP.17).
2. Complete all relevant parts of the GSMA IoT Security Assessment (CLP.17) contained in section 3 of the checklist. Most sections should be self-explanatory. As a guide, we note that following sections within section 3 may be relevant to the following entities:

Example Entity Profiles	CLP.17 Section		
	3.3.1	3.3.2	3.3.3
IoT Service Provider (E.g. A fleet management service provider, smart city service provider etc.)	✓	✓	✓
IoT Service Platform Vendor or Component Vendor (e.g. An IoT service platforms vendor, Cloud Service Vendor or a supplier of an service platform technology component such as operating system vendor, hardware platform provider)	✓	✓	-
IoT Endpoint Vendor or Component Vendor (e.g. An IoT gateway vendor, smart meter manufacturer or a supplier of an endpoint technology component such as a communication module vendor, microprocessor vendor)	✓	-	✓

3. Sign the declaration contained in section 3.4 of the checklist.
4. Submit the completed checklist* to: iots@gsma.com

   NOTE: Regarding step 4: If, for confidentiality reasons, you do not wish to share the content of section 3.3 of your completed checklist with the GSMA, you may just complete sections 3.1, 3.2 and 3.4. The content of sections 3.1, 3.2 and 3.4 shall be known as the 'summary information')
5. Within 14 days the GSMA will perform an administrative check of the summary information contained within the checklist (i.e. sections 3.1, 3.2 and 3.4) and, if completed correctly, the GSMA will assign a unique reference number to the checklist.
6. The GSMA will inform the entity that submitted the checklist of the unique reference number. The entity shall add this unique reference number to section 3 of their completed checklist.
7. The GSMA will publish the summary information contained in section 3.1 and 3.2 of the completed checklist on the public GSMA website, together with the unique reference number.
8. Published checklist summaries can be found here: www.gsma.com/iot/completed-assessments/
9. Once your checklist summary is published on the GSMA website, any entity that wishes to see the completed checklist will be instructed to contact the designated contact person within your organisation; this will be the contact person stated within the checklist summary published by the GSMA. The unique reference number should be quoted for the specific checklist.
10. The exchange of the checklist shall only be completed bilaterally between the entity that submitted the checklist and the entity that requests the checklist. The release of the checklist document may be subject to a NDA between the two respective entities.
11. The process is subject to the terms of use described below.

For help and assistance with this process please email iots@gsma.com or visit the GSMA IoT Security Guidelines website: **www.gsma.com/iot/iot-security-assessment/**

3. Terms of Use

Notwithstanding anything set out herein, the fact that the GSMA makes this document available and performs certain tasks hereunder, does not constitute a service rendered by the GSMA to any third party.

Both this document and the tasks performed by GSMA in association with this document are provided solely on an 'as is' basis without any expressed or implied warranties, undertakings or guarantees attached.

The GSMA disclaims any and all liability for any mistakes, faults, incorrect information/instructions, variations, inconsistencies, actions or omissions; any information provided by a third party; any assessment declaration; or any other activities, associated with this document.

Any user of this document waives, and will fully indemnify and hold the GSMA and its associates harmless against, any claims in relation to this document; the assessment; the declaration described herein; or any associated activities or documentation. The GSMA does not certify any party based on this documentation. The GSMA does neither verify the assessment nor the assessment declaration. The GSMA merely facilitates the assessment of such parties. The GSMA publishes the fact that third parties have completed the assessment and signed the assessment declaration. Such assessment and declaration are at the third party's own risk.

The fact that the third party has requested and/or undertaken the assessment; signed the assessment declaration, and/or has been published in having done both of the above, does not constitute a certification, endorsement or affirmation of a 3rd party's services', devices' or networks' integrity, security or safety and the GSMA disclaims any responsibility for any information provided in relation to the document.

Any warranties, whether expressed, implied or statutory, including without limitation, any implied or other warranties of merchantability, fitness for a particular purpose, non-infringement, quality, accuracy, completeness, title or quite enjoyment with regards to this documentation, any certification, third party products and services and associated activities and documentation are expressly disclaimed and excluded by the GSMA.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	6 Sept 2016	1st Revision of Document	PSMC/CLP	Ian Smith / GSMA
1.3	29 Sept 2017	Addition of CLP13_7.12	IoT Security Group	Rob Childs / GSMA

A.2 Other Information

Type	Description
Document Owner	GSMA Internet of Things Programme
Editor / Company	Rob Childs / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at **prd@gsma.com**

Your comments or suggestions & questions are always welcome.

Floor 2, The Walbrook Building
25 Walbrook, London EC4N 8AF UK
Tel: +44 (0)207 356 0600

iot@gsma.com
www.gsma.com/iot

©GSMA October 2017