

2 PfG CH 0003 - Protected Privacy IoT Service Catalogue of Requirements		Valid from: 10.2019
TÜV Rheinland Greater China	Created: Ivan Deng	Reviewed: Roy Luo

TÜV Rheinland Catalogue of Requirements for Protected Privacy IoT Service

1. Purpose /目的

This document describes evaluation requirements for the certification of Protected Privacy IoT Service as defined in the scope for TÜV Rheinland China Mark approval, for below keywords / 本文介绍了TUV莱茵中国标志认证范围内定义的IoT服务的隐私保护认证的评价要求，适用于以下关键字：

Protected Privacy IoT Service

IoT服务的隐私保护

TÜV Rheinland catalogue of requirement 2 PfG CH 0003 for "Protected Privacy IoT Service" is newly created as there is no GB, GB/T, EN, IEC or ISO standard applicable for the specified products/services. The "Protected Privacy IoT Service" examination is intended to give a service provider the option of obtaining a qualified statement that the personal data of his customers are well protected and transparently processed for the customer. The examination also evaluates to what extent the service provider implemented processes and measures to prevent security incidents and, if necessary, can respond appropriately. The requirements to be met by a service provider are described in more detail in this document.

由于没有GB、GB/T、EN、IEC或ISO标准适用于指定的产品/服务，莱茵公司最新发布的“IoT服务的隐私保护”要求 2 PfG CH 0003。“IoT服务的隐私保护”认证旨在让服务提供商获得一份合格声明，表明其客户的个人数据得到了良好的保护，并且对客户来说，处理过程透明。该目录规定的要求，评估了服务提供商实施预防安全事件的流程和措施，及在必要时是否能够做出适当的响应。


2. References / 引用

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

下列全部或部分文件在本文件中规范性引用，对其应用是必不可少的。凡是标注日期的引用文件，只有引用的版本适用。凡是未注日期的引用文件，其最新版本（包括任何修订）适用。

General Data Protection Regulation

通用数据保护法案

 TÜVRheinland® "China Mark" for Protected Privacy IoT Service™		Page: 2 of 4
2 PIG CH 0003 - Protected Privacy IoT Service Catalogue of Requirements		Valid from: 10.2019

ISO 27001 Information Security Management Systems
信息安全管理体系

3. Scope of application / 范围

The requirements specified in this catalogue of requirement apply to Protected Privacy IoT Service. / 该目录规定的要求适用于IoT服务的隐私保护。

4. Definitions / 定义

End User 终端客户	The end user is a natural person who uses the IoT product along with the service to be certified. 使用经认证的 IoT 产品和服务的自然人
EXT-VP	EXT-VP acts as the person responsible (in accordance with Article 4 (7) of the GDPR) towards the end user and as the principal vis-à-vis the service provider. 按照 GDPR Art.4 (7)的要求, 对终端客户的负责人, 也是服务提供者的代理人
IoT product IoT 产品	The IoT product is the certification-related device that is operated by the end-user and provides data to the service being certified. 由终端客户操作, 并向被认证的服务提供数据, 与认证相关的设备。
Service 服务	Service includes the service provided by the Service Provider to provide end-users with added value by transmitting and processing data to and from systems by the IoT Products. 由服务提供者通过 IoT 产品向系统传输和处理数据, 提供给终端客户的增值服务。
Service Provider 服务提供者	Service Provider is the company that provides the service to be certified. 提供经认证的的服务的公司

5. Required specimens, documents and evidence / 所需的测试样本、文件和证据

The applicant has to provide representative IoT product/ IoT service and corresponding processes available for all tests and evaluation. For certification the exact address of product/service provider must be named / 申请人必须提供适用于测试和评价的IoT 产品/ IoT服务及对应的相关流程。证书上涉及的产品/服务提供者的具体地址必须注明。

The applicant has to provide the following information (if applicable)
申请人必须提供以下信息 (如适用):

- Exact product name and description / 准确的产品/服务名称和描述
- Name and address of product/service provider / 产品/服务提供者的名称和地址



6. TÜV Rheinland Mark (Template) / TÜV 莱茵标志 (模板)



Protected
Privacy
IoT Service



www.tuv.com
ID 0123456789

7. Requirements / 要求

The catalogue outlines the main requirements of the service, underlying processes and necessary hard-ware (IoT product). The data protection requirements are also enumerated. The description focuses solely on the key aspects. The aspects for examination are detailed in GDPR.

该目录概述了服务的主要要求、基础流程和必要的硬件(物联网产品)。还列举了数据保护要求。这一描述只着重于关键方面。具体审核内容详见GDPR。

	Catalogue	Reference
1	Cryptography Requirements	Ref: ISO 27001 Ref: BSI,NIST
2	Requirements of the Service Provider's Network Architecture	Ref: ISO 27001
3	Requirements relating to the Service Provider's Use of IaaS services	Ref: ISO 27001
4	Data Storage and Data Communication Requirements	Ref: ISO 27001
5	Requirements on the Conformity Certificate of IoT Devices	Ref: IoT Certificate
6	Requirements of the Service Provider's Databases	Ref: ISO 27001
7	Configuration Requirements of the Service Provider's Network Components	Ref: ISO 27001
8	Configuration Requirements of the Service Provider's Systems	Ref: ISO 27001
9	Requirements on the Conformity Certificate of the IoT Configuration	Ref: IoT Certificate
10	Identity and Authorization Management Requirements	Ref: ISO 27001
11	Web Application Requirements	Ref: Penetration Test
12	Mobile Applications (Android, iOS) Requirements	Ref: Penetration Test

	Catalogue	Refer to GDPR
13	Requirements of the Service Provider's Physical Security	Ref: ISO 27001
14	Data Centre Availability Requirements	Ref: ISO 27001
15	Service Provider Back-up Requirements	Ref: ISO 27001
16	Patch and Vulnerability Management Requirements	Ref: ISO 27001
17	Monitoring Requirements for the Service Provider's Systems	Ref: ISO 27001
18	Requirements of the Conformity Certificate concerning the Documentation for Consumers	Ref: ISO 27001
19	Requirements in Emergency Management at the Service Provider	Ref: ISO 27001
20	Requirements of Incident Management at the Service Provider	Ref: ISO 27001
21	Requirements of Change Management at the Service Provider	Ref: ISO 27001
22	Requirements of Data Processing by the Service Provider	Ref: Art. 6 para. 1 DSGVO Ref: Art. 6 (1) (b) GDPR Ref: Article 30 sentence (1) GDPR Ref: Article 30 sentence (2) GDPR Ref: Art. 28 GDPR Ref: Art 42 DSGVO
23	Requirements for Order Processing	Ref: ISO 27001
24	Organizational Requirements	Ref: ISO 27001
25	Requirements of the Service Provider's Employees	Ref: ISO 27001
26	Requirements of the Service Provider's Technical and Organizational Security	Ref: ISO 27001

8. Revision history/ 版本历史

Version	Changes	Author	Approval	Revision date	Effective date
Draft 1.0	//	Ivan Deng	Roy Luo	2019-10-24	2019-10-24

2019-11-13

Date

Created by: *Ivan Deng*

Ivan Deng / Expert

Reviewed by:

Roy Luo
Roy Luo / RFM

Rev.: 1.0 / approved: Roy Luo