ISC 35.100.70

201□-□□-□□实施

201□-□□-□□发布

智能家电云云互联互通标准

第2部分： 信息安全

Cloud to cloud interconnection for smart household appliances

Part 2 ：Information security

公开征求意见稿

本稿完成时间2018.10.25

L 79

团 体 标 准

中国家用电器协会 发布

T/ CHEAA 0001.2—201□

目  次

目次 I

前言 II

引言 III

1. 范围 1

2. 规范性引用文件 1

3. 术语和定义及缩略语 1

4. 应用场景…… 3

4.1场景1：A厂商的App远程控制B厂商的家电设备 3

4.2场景2：不同家电厂商的设备通过互联网和云平台进行联动 4

5.接口安全规范 4

5.1通信安全 4

5.1.1通讯两端建立TLS传输通道 4

5.1.2 个人敏感信息加密密钥获取 5

5.1.3 个人敏感信息传输 5

5.1.4 访问源控制 5

5.2 认证和授权 5

5.2.1 用户登录接口 5

5.2.2 访问令牌管理 5

5.3 数据过滤 5

5.4 错误信息处理 6

5.5 业务服务稳定性保护 6

5.5.1 分布式拒绝服务攻击（DDoS）防护 6

5.5.2 应用服务的系统安全 6

5.6 日志审计 6

6 安全事件管理要求 6

6.1 安全事件的分类和分级 6

6.1.1 数据所有权 6

6.1.2 安全事件 6

6.1.3 事件分级 7

6.1.3.1分类要素和级别 7

6.1.3.2 事件分级准则 7

6.2 责任模型 7

6.3 服务条款 7

6.4 明确责任部门和人员 8

6.5 应急响应 8

6.6 事件通告 8

6.7 持续改进 8

A.1导则 9

A.2 我国相关标准系列 9

A.3 国际相关标准及技术法规系列 9

B.1导则 10

B.2 数据生产和收集 10

B.2.1 基本原则 10

8.1.2 用户知情权 10

8.1.3 用户权限 10

B.3 数据传输 10

B.3.1 建立安全的加密传输通道 10

B.3.2 个人敏感信息加密传输 10

B.3.3 访问源控制 10

B.4 数据的使用 11

B.4.1 认证和授权 11

B.4.2 数据展示 11

B.4.3 数据审计 11

B.5 数据保存 11

B.6 数据销毁 11

前  言

本标准提出了智能家电云云互联互通的信息安全要求。

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国家用电器协会提出。

本标准由中国家用电器协会标准化委员会归口。

本标准版权归中国家用电器协会所有，未经中国家用电器协会许可不得随意复制，其他机构采用本标准的技术内容制修订标准须经中国家用电器协会允许，任何单位或个人引用本标准的内容需指明本标准的标准号。

截至本标准正式发布之日，中国家用电器协会未收到任何有关于本标准涉及专利的报告，中国家用电器协会不负责确认本标准的某些内容是否还存在涉及专利的可能性。

本标准起草单位：

本标准主要起草人：

引  言

近年，随着越来越多的智能家用电器与互联网、物联网络连接的普及，众多家电厂商的智能云平台从私有走向开放共享，而安全风险也随着被扩大，所以，互联的厂商达成一致的安全思路就势在必行。

本标准针对智能家电互联互通面临的安全风险，规范了互联企业云平台接口的技术规范，以及出现安全事件的协同管理机制，同时也包含了共享的用户数据的保护建议，旨在帮助互联互通的企业达成一致的信息安全规范，保障双方利益，遏制因共享而产生的安全风险。

智能家电云云互联互通标准

第2部分： 信息安全

1. 范围

本标准规定了不同厂商云平台之间互联互通接口协议的信息安全解决方案。

1. 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/Z 20985-2007 信息技术 安全技术 信息安全事件管理指南

GB/Z 20986-2007 信息安全技术 信息安全分类事件分级指南

1. 术语和定义及缩略语

3.1术语和定义

以下术语和定义适用于本标准部分。

3.1.1

智能家电 smart household appliance

具有网络通信能力的家用电器，可以在家庭或类似场所内实现互操作或通过控制终端实现集中控制，也可以直接或通过网关连接服务平台，实现对家电的网络操控与管理等应用。

3.1.2

智能家电云平台 cloud platform of smart household appliance

是指能够实现智能家电、智能家电应用的接入和管理，为智能家电提供家电管理、操作、控制等应用服务的平台系统。

3.1.3

安全传输层协议 Transport Layer Security

安全传输层协议用于在两个通信应用程序之间提供保密性和数据完整性。

3.1.4

数字证书颁发机构 Certificate Authority

负责发放和管理数字证书的权威机构，并作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

3.1.5

个人信息 Personal Information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生 理信息、交易信息等。关于个人信息的范围和类型详见GB/T 35273-2017。

3.1.6

个人敏感信息 Personal Sensitive Information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 ：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。关于个人敏感信息的范围和类型可详见GB/T 35273-2017。

3.1.7

密钥 Key

在密码学中，密钥是指某个用来完成加密、解密、完整性验证等密码学应用的秘密信息。在对称密码学（或称密钥密码学）中，加密和解密用的是同一个钥匙，因此钥匙需要保密。而在公钥密码学（或称非对称密码学）中，加密和解密用的钥匙不同：通常一个是公开的，称为公钥；另一个保密，称为私钥。

3.1.8

匿名化 Anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别，且处理后的信息不能被复原的过程。

注：个人信息经匿名化处理后所得的信息不属于个人信息。

3.1.9

去标识化 De-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息 主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段 替代对个人信息的标识。

3.2缩略语

以下缩略词适用于本标准部分，详见表3.1。

表3.1 缩略语（首字母组合词）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 缩略语 | 英文含义 | 中文含义 |
| 1 | TLS | Transport Layer Security | 安全传输层协议 |
| 2 | AES | Advanced Encryption Standard | 高级加密标准 |
| 3 | JSON | Java Script Object Notation | 对象标记 |
| 4 | DDoS | Distributed Denial of Service | 分布式拒绝服务攻击 |
| 5 | CDN | Content Delivery Network | 内容分发网络 |
| 6 | API | Application Programming Interface | 应用程序接口 |

1. 应用场景

4.1场景1：A厂商的App远程控制B厂商的家电设备

由于A厂商（可以是家电厂商，也可以时非家电厂商）APP只能连接到A厂商云平台，而A厂商云平台不能直接管理B厂商的家电设备，所以A厂商云平台必须与B厂商云平台互联，才能把App的控制命令传递给B厂商云平台，从而实现A厂商App对智能家电的远程控制。如图4.1所示：

图4.1 互联场景1：A厂商的App远程控制B厂商的家电设备

4.2场景2：不同家电厂商的设备通过互联网和云平台进行联动

A厂商云平台与B厂商云平台互联，设备联动的业务逻辑放置在A厂商云平台内。当A厂商设备状态改变时，A厂商根据设备联动的业务逻辑控制B厂商的设备，如图4.2所示：

图4.2 互联场景2：不同家电厂商的设备通过互联网和云平台进行联动

1. 接口安全规范

5.1通信安全

5.1.1通讯两端建立TLS传输通道

1. 厂商云平台之间的通讯接口都必须采用TLS安全机制，并且使用安全的TLS版本。
2. 厂商云平台需要到数字证书颁发机构申请证书（也可以通过特定组织统一自建证书），并在云平台上部署证书。
3. 厂商云平台互联时通过各自的证书进行双向认证，只有证书校验通过才能完成请求。

5.1.2 个人敏感信息加密密钥获取

1. 厂商云平台之间共享的数据，如果涉及个人敏感信息，需要下发密钥，用来加密传输。
2. 用户认证后，B厂商会下发密钥给A厂商，用来加密隐私数据。
3. 密钥必须不可预测，应结合用户ID等用户信息，以及时间戳和随机数的哈希函数生成128位字符串。
4. 动态密钥，每次用户登录认证后，下发最新密钥，旧密钥废弃。
5. 用户登出操作后，就密钥废弃。

5.1.3 个人敏感信息传输

1. 个人敏感信息必须使用动态获取的加密密钥加密后，才能完成传输。
2. 涉及个人身份信息、个人生物识别信息或者密码和口令的传输需通过安全的哈希方式方式处理。
3. 其他信息的传输需要根据业务场景选择去标签化或匿名化处理。

个人敏感信息举例：

|  |  |
| --- | --- |
| 个人身份信息 | 身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等 |
| 个人生物识别信息 | 个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等 |
| 个人健康生理信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、 手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以 往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康 状况产生的相关信息等 |
| 网络身份标识信息 | 系统账号、邮箱地址及与前述有关的密码、口令、口令保护答案、用户个 人数字证书等 |
| 其他信息 | 个人电话号码、性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记 录和内容、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等 |

关于个人敏感信息的范围和类型可详见GB/T 35273-2017 附录B。

5.1.4 访问源控制

1. 厂商云平台互联接口，应通过对请求的源IP进行白名单控制，实现更加严格的通讯源的访问控制。

5.2 认证和授权

5.2.1 用户登录接口

1. 厂商云平台的唯一标识符PlatID需要保证不可预测性。
2. 厂商云平台的身份令牌AuthToken根据PlatID和时间戳、随机数等计算得出，应通过安全的哈希方式生成，长度不低于16位，使用数字和字母组成。
3. 每对PlatID和AuthToken仅适用于对接的两个平台，比如A平台给B平台发送的的PlatID和AuthToken，仅适用于B平台对A平台的身份验证，其他平台需要重新协商。
4. 严格的双向身份校验，A平台发送验证信息给B平台，B平台再确认A平台身份正确后，也发送自己的验证信息给A平台。

5.2.2 访问令牌管理

1. 完成身份验证后，A平台通过AuthToken提交获取AccessToken的请求，B平台下发给A平台访问令牌AccessToken、更新令牌RefreshToken和AccessToken有效时长，A平台所有的请求都需要在有效时长内包含该AccessToken才能正常请求。
2. AccessToken和RefreshToken，根据PlatID和时间戳、随机数等，通过安全的哈希方式生成，长度不低于32位，使用数字和大小字母和特殊字符组成。
3. AccessToken有效期不超过2小时，过期或登出操作后自动销毁。RefreshToken有效期不超过14天，过期或登出操作后自动销毁。
4. 主动更新AccessToken，需要使用RefreshToken进行请求更新，同时RefreshToken仅可使用一次，更新一次AccessToken后，RefreshToken也会进行更新。

5.3 数据过滤

1. 所有的参数，都需要使用强类型和固定长度的校验。比如PlateID使用Long数字类型，长度为16等。
2. 数据传输，需要使用PUT或POST传输JSON格式的数据，请求头部必须指明类型application/json。
3. 安全过滤，针对数据的进行安全监测后，包括对特殊字符和数据库注入等进行严格检测和过滤，拦截一切不在预期内的数据内容。

5.4 错误信息处理

请求失败的情况下，通过错误编码来表示错误类型，不允许暴露任何平台或用户的敏感信息。

5.5 业务服务稳定性保护

5.5.1 分布式拒绝服务攻击（DDoS）防护

* 1. 流量型和系统资源型的攻击，需要有完善的应急防护手段，建议通过运营商或基于域名的云防护产品实现快速流量迁移和清洗或者通过CDN等方式实现流量的稀释。
  2. 针对应用服务资源消耗类型，可以通过中间件层，或者应用层面对访问频率和访问特征进行限制。

5.5.2 应用服务的系统安全

提供API的平台和对应的服务器，需要执行系统和服务的加固，包括开放端口的白名单严格限制和对外服务的加固，比如使用了Apache，需要使用安全的Apache版本，并进行安全的配置。

5.6 日志审计

* 1. 应该建立具备自动化请求日志收集和审计的系统，监控所有API进出流量。
  2. 审计过程形成的记录应能对安全事件的处置、应急响应和事后调查提供支撑。
  3. 应防止非授权访问、篡改或删除审计记录。
  4. 接口请求日志保存时间至少6个月。
  5. 日志严禁记录用户敏感数据信息。
  6. 针对异常日志，自动告警到相关运维人员，进行对应的分析和处理，具体详见后面一个章节。

1. 安全事件管理要求

6.1 安全事件的分类和分级

6.1.1 数据所有权

个人信息所有权归属信息所标识的自然人，也就是使用物联网服务的实际个人用户。个人信息所有者拥有信息数据的完全访问和控制权限，并且有权利要求互联互通对信息数据进行对应的操作，比如删除其提供的信息数据。

经过匿名化处理后的数据和信息，归属这些信息的提供者，也就是提供信息的云平台主体。数据归属平台有数据的完全访问和控制权限，并且有权利要求互联互通对数据进行对应的操作，比如删除其提供的数据。

6.1.2 安全事件

根据信息安全事件产生的结果表象做分类，分为数据泄露事件和服务不可用事件。

* 1. 数据泄露事件：云互联共享的数据出现泄露。
  2. 服务不可用事件：服务出现不稳定或者不可用情况，并且影响到云互联的其他厂商的事件。
  3. 其他事件，除了上述事件以外的其他事件。

6.1.3 事件分级

根据信息安全事件的分级考虑要素，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

6.1.3.1分类要素和级别

信息系统的重要程度分为：特别重要、重要、一般，对应信息系统等级保护：五级和四级、三级、二级和一级。

系统损失分级为：特别严重、严重、较大、较小。

社会影响分级为：特别重大、重大、较大、一般。

6.1.3.2 事件分级准则

1. 特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：a) 会使特别重要信息系统遭受特别严重的系统损失；b) 产生特别重大的社会影响。

1. 重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况： a) 会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损 失； b) 产生的重大的社会影响。

1. 较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：

a) 会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、 一般信息信息系统遭受特别严重的系统损失；b) 产生较大的社会影响。

1. 一般事件（Ⅳ级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况：a) 会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失， 一般信息系统遭受严重或严重以下级别的系统损失；b) 产生一般的社会影响。

6.2 责任模型

* 1. 针对数据泄露事件，责任归属直接导致数据泄露的云平台或者客户端所属的厂商。
  2. 针对服务不可用事件，根据导致服务不稳定或不可用的节点判断，责任归属该节点所有者平台。
  3. 在责任未明确的时候，需要双方共同协商、承担和调查原因。在双方对于数据泄露事件无法达成一致的情况下，需要由独立的第三方介入调查。如还调查无果，双方需要共同承担责任。

6.3 服务条款

云互联双方必须签订具有法律效应的服务条款，需要包含（不仅限于）如下内容：

* 1. 互联互通企业双方的服务内容。
  2. 互联互通企业双方各自的权利和义务。
  3. 涉及用户数据、用户隐私数据，需要明确数据的所有权，使用权限。
  4. 保密条款，包括用户数据、用户隐私数据不允许主动向第三方披露等。
  5. 服务期限和终止。
  6. 违约责任和免责条款。

6.3.1 数据所有权说明

详见6.1.1。

6.3.2 数据使用权限说明

1. 数据的披露
   * 向第三方披露
     + 未在双方书面允许下，不允许向第三方披露。
     + 只允许为提供或改进产品、服务的目的而与第三方共享。
     + 不允许为第三方的销售目的而与第三方共享数据，更不允许销售共享数据。
2. 数据的删除
   * 用户有权申请删除其在双方平台交互过程中，产生的个人数据。平台双方需要在7天内完成数据删除。
   * 非个人数据，数据归属平台有权利要求共享平台对数据进行删除的操作。
   * 所有数据删除的操作，需要在企业内部有明确的流程和制度保障。

6.4 明确责任部门和人员

对于厂商云平台双方的要求包括：

* 1. 应明确厂商云平台主要负责人对信息安全负全面领导责任，包括为信息安全工作提供人力、财力、物力保障等。
  2. 应明确厂商云平台对接的安全接口人和备用接口人。

6.5 应急响应

* 1. 协同诊断，确认事件的责任方和认定安全事件类型。
  2. 事件责任方需要根据合作服务条款内的明细，在指定时间内抑制受害范围并恢复业务服务。
  3. 事件责任方继续寻找安全问题成因，封堵攻击源。
  4. 业务恢复。

6.6 事件通告

* 1. 云互联任何一方有权利和义务向对方通告详细的安全事件原因。
  2. 如果因特别重大事件、重大事件或较大事件，而导致对业务可用性和稳定性的影响时间超过1个小时，需要按照双方的服务条款进行事件对外的通告。

6.7 持续改进

云云互联双方需要对重大事件和特别重大事件进行持续的跟踪，包括。责任方需要出台相应的改进措施，并通过管理手段或技术手段真实落地。

附 录 A

（规范性附录）

云平台和家电企业信息安全相关标准及技术法规

A.1导则

以下列举当前（2018.8）对于云平台和个人信息保护具有一定代表性的标准及技术法规系列，为了保障互联双方具有能力共同保障互联业务的信息安全，云云互联双方应在满足或参考以下一项或多项标准及技术法规的基础上，实现云云互联互通。

A.2 我国相关标准系列

1. 中国网络安全等级保护（DJCP）
2. 可信云服务认证（TRUCS）
3. 信息技术安全性评估准则（GB/T 18336）

A.3 国际相关标准及技术法规系列

* 1. ISO 27001 信息安全标准
  2. ISO 27017 云服务安全标准
  3. ISO 27018 云服务隐私保护操作规范
  4. CSA Star 云安全保障认证
  5. 欧盟一般数据保护条例（GDPR）

附 录 B

（规范性附录）

数据和隐私保护建议

B.1导则

当前（2018.8）云云对接涉及的场景不共享用户隐私数据，但是随着未来云平台不断开放，可能会涉及个人健康管理方面的小家电或者医疗设备等，需要传递部分用户隐私数据才能提供服务，故针对该部分，应更加严格的进行数据安全建设。

B.2 数据生产和收集

B.2.1 基本原则

* 1. 信息收集主体的所有行为的合法要求，包括信息主体的授权和法律责任的明确。
  2. 收集的数据最小化原则，不收集和提供的服务无关的数据。
  3. 数据分类，区分个人数据和平台信息数据，个人敏感信息在共享前要做匿名化处理。

8.1.2 用户知情权

* 1. 隐私条款必须包含应用收集的所有用户数据及这些数据用来提供的服务。
  2. 隐私条款必须披露提供的第三方云平台服务的基本信息和数据。
  3. 隐私条款必须包含数据删除、迁移、保存、用户权限等信息。

隐私条款模板可参考《GB/T 35273—2017 个人信息安全规范》的附录D。

8.1.3 用户权限

* 1. 用户拥有数据被收集的选择权，如果选择不上传数据，或者不同意隐私条款，则不允许收集用户数据。
  2. 用户对自己的数据拥有访问权和删除权。访问权允许通过电邮或联系客服的方式，获取。删除权，支持用户账号注销机制，注销后删除与之相关的所有数据。同时，云云对接中其他厂商也要支持数据删除。

B.3 数据传输

B.3.1 建立安全的加密传输通道

* 1. 厂商云平台之间的通讯接口都必须采用TLS安全机制，并且使用安全的TLS版本。
  2. 厂商云平台需要到数字证书颁发机构申请证书（也可以通过特定组织统一自建证书），并在云平台上部署证书。
  3. 厂商云平台互联时通过各自的证书进行双向认证，只有证书校验通过才能完成请求。

B.3.2 个人敏感信息加密传输

* 1. 个人敏感信息必须使用安全的动态加密密钥加密后，才能完成传输。
  2. 数据传输需通过数据去标识化或匿名化等方式处理。

B.3.3 访问源控制

1. 厂商云平台互联接口，应通过对请求的源IP进行白名单控制，实现更加严格的通讯源的访问控制。

B.4 数据的使用

B.4.1 认证和授权

1. 严格的双向身份校验，A平台发送验证信息给B平台，B平台再确认A平台身份正确后，也发送自己的验证信息给A平台。
2. 对被授权访问的厂商，采用最小授权的原则，使其只能访问和其平台业务相关的最少够用的服务和信息。

B.4.2 数据展示

涉及通过界面展示个人信息的（如显示屏幕、纸面），个人信息控制者宜对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。

B.4.3 数据审计

1. 完备的自动化数据库操作审计记录
2. 针对可能有风险的操作，比如A厂家要求删除其所有数据，需要进一步沟通和需要一定的审批流程。

B.5 数据保存

1. 数据隔离，对敏感数据进行集中地分布式存储，统一监控管理，通过VPC隔离。
2. 加密存储，数据库加密, 对所有隐私信息进行加密或hash后存储。
3. 数据存储区域限定，如果有国外的用户，需要根据当地的法律限定，如欧洲用户的数据仅能存放在欧洲数据中心，互联的企业的数据中心也必须在欧洲数据中心。
4. 多副本冗余存储，采用分布式架构，所有业务服务器需要同时部署在多个不同的机房，数据同时存放两个以上机房，并实时备份。
5. 共享的用户隐私数据保存时间，根据具体业务内容制定，保存时间不超过1年。

B.6 数据销毁

1. 安全删除，用户有权对自己的数据进行删除操作。
2. 敏感数据清除，对于曾经存储过客户数据的内存和磁盘，一旦释放和回收，其上的残留信息将被自动进行零值覆盖。同时，任何更换和淘汰的存储设备，需要统一执行消磁处理并物理折弯之后，才能运出数据中心。