|  |  |
| --- | --- |
| ICS | 点击此处添加ICS号 |
| CCS | 点击此处添加CCS号 |

|  |
| --- |
| 3502 |

福建省厦门市地方标准

DB XX XXXXX—XXXX

海峡两岸数据和通信安全术语对照

Comparison of terms of electromagnetic compatibility across the Taiwan Strait

(点击此处添加与国际标准一致性程度的标识)

XXXX - XX - XX发布

XXXX - XX - XX实施

厦门市市场监督管理局  发布

1. 前言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由厦门市两岸名词术语标准化技术委员提出并归口。

本文件起草单位：

本文件主要起草人：

1. 引言

近年来，海峡两岸在数据和通信安全领域的交流互动日益频繁，双方通过技术研讨会、学术交流和项目合作等多种形式，共同推动了数据和通信安全技术的进步与应用，为行业的发展带来了积极的影响。大陆和台湾地区在数据和通信安全领域涉及的技术原理、工艺等基本相同,但是由于双方长期形成的用语习惯等原因使得两岸数据和通信安全名词术语存在一定的差异,给海峡两岸技术及人员在数据和通信安全领域交流造成一定的困扰与不便。因此，海峡两岸数据和通信安全名词术语的对照、订正以及统一，将促进两岸数据和通信安全领域的深入交流与合作。

本文件的制定将便于海峡两岸数据和通信安全行业技术人员相互沟通交流时，对于数据和通信安全术语名词能有一个快捷的理解，有助于减少两岸工业数据和通信安全技术人员正常学术交流及经贸往来的障碍，并能够在海峡两岸数据和通信安全领域的融合发展方面发挥重要的推进作用。

海峡两岸数据和通信安全术语对照

* 1. 范围

本文件给出了海峡两岸数据和通信安全相关术语的对照。

本文件适用于大陆与台湾地区工业数据和通信安全的术语及其表达。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19769.1-2022 功能块 第1部分：结构

GB/T 21099.2-2024 企业系统中的设备和集成 过程控制用功能块（FB）和电子设备描述语言（EDDL） 第2部分：FB概念规范

GB/T 21099.5-2024 企业系统中的设备和集成 过程控制用功能块（FB）和电子设备描述语言（EDDL） 第5部分：EDDL内置库

GB/Z 25320.2-2013 电力系统管理及其信息交换 数据和通信安全 第2部分：术语

GB/T 32402-2015 通信名词术语 数据通信 因特网

GB/T 4365-2024 电工术语 数据和通信安全

* 1. 术语和定义

本文件没有需要界定的术语和定义。

* 1. 基本要求
     1. 大陆术语及其译名应符合GB/T 19769.1-2022、GB/T 21099.2-2024、GB/T 21099.5-2024、GB/Z 25320.2-2013、GB/T 32402-2015、GB/T 4365-2024以及数据和通信安全相关规范性、权威性文件的要求。
     2. 台湾地区术语参考台湾地区数据和通信安全词汇标准及相关规范性文件的要求。
  2. 海峡两岸数据和通信安全术语对照原则
     1. 本文件收录大陆与台湾地区数据和通信安全中意义相近而词汇不同或词汇相近而意义不同的术语词汇进行对照。
     2. 海峡两岸数据和通信安全术语对照表见附录 A。

2. （规范性）  
   海峡两岸数据和通信安全术语对照
   1. 海峡两岸数据和通信安全术语对照
      1. 基本概念

海峡两岸数据和通信安全相关基本概念术语对照见表A.1。

* 1. 海峡两岸数据和通信安全相关基本概念术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | 八位元组 | 8 位或 1 字节。在网络中，octet 这个术语通常被使用（而不是字节），因为有些机器架构配置的字节不是 8 位长度。[来源：GB/T 32402-2015，3.1.224] | 八位元组 | 被视为一个单元之 8 个位元之有序序列，等同于 8 个位元之位元组。备考：于 ISO/IEC 19762 及 ASN.1 标准中此词比 “byte” 优选，以避免与硬体相关之混淆情形，例如：7 个位元之位元组、16 个位元之位元组。 | octet |
| 2 | 保护框架 | 对符合特定用户需要的评估对象(TOE)类别，与实现无关的安全需求集合。[来源:GB/Z 25320.2-2013,2.2.151] | 保护剖绘 | 某类评估目标(TOE)之一组实作无关安全要求，其符合特定消费者之需要。 | protection profile |
| 3 | 保证 | 通过系统安全策略的强制实施提供可信性的系统属性。[来源：GB/T 40211-2021，3.2.8] | 保证 | 于安全全景中：交付事项符合其安全目标之信心基础。备考： 安全社群中通常接受此定义。于ISO中更通用之定义如下：对产品、过程或服务满足所规定要求事项之产生信心的活动，该活动结果为一种声明。 | assurance |
| 4 | 标识 | 对系统呈现标识符的行为或过程，从而该系统能识别系统实体并把它与其他实体区分开来。。[来源:GB/Z 25320.2-2013,2.2.106] | 识别 | 行动或过程，对系统出示识别符，使此系统能辨识系统个体并与其他个体之区别。 | identification |
| 5 | 操作 | 完全明确的动作，该动作作用于任何已知实体的允许组合时，产生一个新的实体。[来源：GB/T 21099.2-2024，3.1.55] | 运作 | 程式之可执行映像，于调用时为主体执行某些功能/活动 | operation |
| 6 | 抽象句法 | 一种数据结构的描述，独立于面向机器的结构和编码。[来源：GB/T 32402-2015，3.1.14] | 抽象语法 | 使用记法规则 (notation rule) 之应用协定资料单元的规格，其系与用以表示编码之技术无关。 | abstract syntax |
| 7 | 脆弱性 | 系统设计、实现或操作和管理中存在的缺陷或弱点，可被利用来危害系统的完整性或安全策略。[来源：GB/T 40211-2021，3.2.135] | 脆弱性 | 系统之设计、实作或运作及管理的瑕疵或弱点，可能被用以违反系统之完整性或安全政策。信息系统设计或实作(包括与系统相关之安全程序及安全控制)中之瑕疵或弱点，可能被蓄意或非蓄意利用，透过丧失机密性、完整性或可用性而不利于组织之运作或资产。资产或资产群组之弱点能被1或多个威胁所利用。 | vulnerability |
| 8 | 脆弱性评估 | 信息系统中脆弱性的正式描述和评价。[来源:GB/Z 25320.2-2013,2.2.217] | 脆弱性评鉴 | 信息系统中对脆弱性之正式描述及评估。 | vulnerability assessment |
| 9 | 对象标识符 | 事物的正式且全局唯一的名字，写作一个整数序列（按ASN.1标准的规定，形成和指定该序列）而且在抽象规范中和协议中安全服务协商期间，用以对该事物进行引用。[来源:GB/Z 25320.2-2013,2.2.137] | 物件识別符 | 由国际物件识别符树之根至节点的基元整数值之有序清单，其明确识别该节点。 | object identifier, OID |
| 10 | 分散控制系统/分布式控制系统 | 系统单元被分离但是以耦合方式运行的一种控制系统类型。注 1：分布式控制系统有比那些典型的 SCADA 系统更短的耦合时间常数。注 2：分布式控制系统通常用于连续过程处理，例如发电、石油和天然气提炼、化工、制药和造纸，也用于离散过程处理，例如汽车、其他食品生产、包装和仓储。[来源：GB/T 40211-2021，3.2.44] | 分布式控制系统 | 控制系统中，意指藉由分散有关受控制过程之智慧(而非集中位于单一单元)所达成之控制。 | distributed control system, DCS/distributed control |
| 11 | 服务 | 资源可使用的功能性，可以用服务原语序列来模型化。[来源：GB/T 21099.2-2024，3.1.63] | 服务 | IEC 61850 全景中之许可。 | service |
| 12 | 服务器 | 给客户端设备和应用提供信息或服务的设备或者应用。[来源：GB/T 40211-2021，3.2.119] | 服务器/伺服器 | 接受源自客户端之关联请求的个体。备考：此用语系针对特定关联关系规定个体之角色。该个体可能具另一关联关系之另一角色。 | server |
| 13 | 个人标识码 | 用于证明身份的字母数字代码或口令。[来源:GB/Z 25320.2-2013,2.2.143] | 个人标识号 | 用以鉴别身分之文数字编码或通行码。 | personal identification number, PIN |
| 14 | 功能 | 实体的预期目的或它的特征行为。[来源：GB/T 21099.2-2024，3.1.33] | 功能 | 透过自动化，藉由有或无直接用户互动之计算机系统所履行之任务。功能依赖于可与其他应用交换数据之 1或多个软件应用。 | function |
| 15 | 关键系统资源 | 某个服务或某个系统资源的状况，以致对那资源造成拒绝访问（即可用性缺失）就会危及系统用户执行主要功能的能力，或会导致其他严重后果。 | 关键系统资源 | 服务或其他系统资源之情况，诸如拒绝该资源的存取(亦即，可用性缺乏)将危害系统用户履行主要功能之能力或造成其他严重后果。备考：除拒绝存取外，其他安全威胁诸如信息完整性缺乏亦能使资源归类为关键系统。 | critical system resource |
| 16 | 关联 | 系统实体间的合作关系，通常用于相互传递信息的目的。[来源：GB/T 40211-2021，3.2.7] | 关联 | 应用个体调用间之合作关系，其启用资讯的通讯与供其通讯实例的联合运作之协调。备考:可借由使用下层服务之应用协定控制资讯的传送形成此关系。 | association |
| 17 | 管理信息库 | 包括被管理对象的虚拟数据库，也就是可以通过网络管理规程访问的对象的集合，它包括网络管理系统所管理的全部资源的信息，它通过路由器运行。被管理对象包括网桥、路由器、计算机、服务器、交换机、多路复用器等，它们的名字、属性和特性也可以视为被管理对象。管理系统可以对被管理对象进行查询、修该或删除等操作。[来源：GB/T 32402-2015，3.1.195] | 管理信息库 | MIB 为一种数据库，用以管理通讯网络中之装置。其由(虚拟)数据库中之对象集所组成，用以管理网络中之个体(诸如路由器及交换器)。MIB 中之对象使用抽象语法记法 1(abstract syntax notation one, ASN.1)定义，而履行剖析之软件为 MIB 编译程序。数据库为阶层式(树状结构)，其数据项以对象识别符寻址。讨论 MIB 之因特网标准主要为 RFC 1155，其 2 个相关标准为RFC 1213及 RFC 1157。 | management information base;MIB |
| 18 | 互操作性 | 共享传输数据类型和语义的两个或多个设备，在一个或多个分布式应用中一起工作的能力。[来源：GB/T 21099.2-2024，3.1.48] | 互换性/互运性 | 交换具相同形式、合用及功能、跨平台，且不影响系统功能性之硬件组件的能力。当2或多个品项具备等同之效能及耐久性，并能除调整外，不变更品项本身或联接品项，且不需选择合用及效能，而互换之功能及实体特性时存在之条件。 | interoperability |
| 19 | 互换性 | 按照过程设计的要求，在物理过程和分布式应用中，一个设备可完成另一个设备的角色的能力。[来源：GB/T 21099.2-2024，3.1.44] | 互换性 | 未经同意(且通常不延迟或妨碍传输)，取得原属他人之通讯资产。意图延迟或消除由预期之目的地用户的信号接收，而获取所传输之信号。 | interchangeability |
| 20 | 回拨 | 用于经电话线远程访问计算机的终端的认证技术。主视系统断开呼叫者连接，然后回拨那个终端的先前已审定的电话号码。[来源:GB/Z 25320.2-2013,2.2.35] | 回拨 | 经由电话线路远程访问计算机终端设备之鉴别技术。主机系统解连呼叫者，再以先前该终端设备授权之电话号码回拨。 | call back |
| 21 | 基带 | 与从调制源来的原始信号有关的或包括原始信号的频带。[来源：GB/T 32402-2015，3.1.42] | 基频 | 由 1 个信号或一组多工化信号所佔据且不随调变而改变之频率。 | baseband |
| 22 | 计算机的 | 宽泛地说，是对与计算机或网络化相关的任何事物的前缀。[来源:GB/Z 25320.2-2013,2.2.66] | 网宇 | 任何泛指有关于计算机或网络之非严谨前缀字。 | cyber |
| 23 | 解码 | 通过对先前编码的结果进行还原，对数据进行变换。对代码进行翻译。通过代码方法把编码的文本变换为相应的明文。[来源:GB/Z 25320.2-2013,2.2.77] | 解码 | 藉由反转先前编码之结果，转换数据。对码之解译。藉由使用码将已编码文字转换为等同之明文。备考：译码不包括以密码分析法获得明文。 | decode |
| 24 | 可靠性 | 在规定的时间周期内，在规定的条件下系统执行所要求功能的能力。[来源：GB/T 40211-2021，3.2.82] | 可靠度 | 系统于规定期间内，依所声明条件履行要求功能之能力。 | reliability |
| 25 | 可用性（性能） | 假定提供了其所需的外部资源，在给定的时刻或者给定的时间内，在给定的条件下执行必要功能时的能力。注 1：性能来源于可靠性，可维护性和维护支持。注 2：所需的外部资源，除了维护资源，不影响项目的可用性能力。[来源：GB/T 40211-2021，3.2.16] | 可用性 | 经授权之个体，依需可存取且可使用的性质。依系统效能规格，经授权系统个体，依需可存取且可使用的系统性质或系统资源性质；亦即，若用户请求系统依其系统设计 而提供服务，则其为可用。 | availability（performance） |
| 26 | 控制系统 | 由受控系统、它的控制系统、测量元件和相关的变送元件所组成的系统。使用周密的控制或操纵使变量达到规定值的系统。控制系统包括数据采集和监控系统（SCADA）、分散控制系统（DCS）、可编程逻辑控制器（PLC）和其他类型的工业测量和控制系统。[来源:GB/Z 25320.2-2013,2.2.55] | 控制系统 | 由受控系统、其主控系统、量测组件及结合之传感组件所构成之系统。使用蓄意指引或调处，以达成变量之规定值的系统。控制系统包括监控及数据撷取（SCADA）、分布式控制系统（DCS）、电力线载波（PLC），以及其他型式之工业量测与控制系统。 | control system |
| 27 | 控制系统运行 | 包括生产、维修保养和质量保证运行的集合以及生产机构的其他活动。包括（1）对原料转化为最终产品所涉及的人员、设备和材料进行协调的机构活动；（2）可以由物理设备、人力和信息系统执行的功能；（3）对机构内所有资源（人员、设备和材料）的信息进行管理，这些资源信息是关于机构资源的计划安排、使用、容量、规定、历史记录和当前状况的信息。[来源:GB/Z 25320.2-2013,2.2.56] | 控制系统运作 | 控制系统运作包括生产、维护及质量保证运作之汇集，以及制造设施之其他活动。系统运作包括下列项目：协调原始物料转换为终端产品过程中所涉及之人员、设备及材料的设施活动。藉由实体设备、人力及信息系统执行之功能。设施中关于所有资源(人员、设备及物料)之排程、使用、容量、定义、历史及状态之管理信息。 | control system operation |
| 28 | 时延 | 对于存储转发装置，时延是从输入帧的最后比特达到输入口时开始并且在输出口上看到输出帧的第一个比特时终止的时间间隔。对于位转发装置，时延是从输入帧第一个比特的终止沿达到输入口时开始并且在输出口上看到输出帧的第一个比特的起始沿时终止的时间间隔。[来源:GB/Z 25320.2-2013,2.2.124] | 潜时 | 就存转装置而言：时间间隔始于输入讯框之最后位抵达输入端口时，并止于输出埠上出现输出讯框之第 1 位时。 | latency |
| 29 | 实体 | 特定的事物，如：人、地点、过程、对象、概念、联系或事件。[来源：GB/T 21099.2-2024，3.31] | 个体 | 涵盖人类使用者、自动化系统、软体应用程式、通讯节点、场域装置及其他型式资产之通用用语。 | entity |
| 30 | 使用分析 | 对出自数据流的可观察特征信息进行推断，即使数据是加密的或者并非直接可用的。这些特征包括源端和目的地端的身份和位置以及事件出现、发生次数、频度和持续时间。在通信系统中，对通信传输率、通信量、通信密度、通信容量和通信模式进行分析，尤其为系统性能改善而进行。[来源:GB/Z 25320.2-2013,2.2.205] | 讯务分析 | 由数据流之可观察特征的推论信息，甚至数据经加密或不能以其他方式直接取得时亦然。此等特征包括来源及目的地之身分及位置，以及事件之存在、数量、频率及持续时间。通讯系统中，讯务速率、数量、密度、容量及型样之分析，专用于系统效能改善。 | traffic analysis |
| 31 | 事实上标准 | 广泛接受和使用的标准，但未经公认的标准组织的正式批准。[来源:GB/Z 25320.2-2013,2.2.80] | 业界标准 | 广泛接受及使用之标准，但缺乏公认标准组织之正式核准。备考： 即使广泛使用且通常相当有效，某些安全技术仍专属于某些供应者。无论如何，此等宜认为业界标准，直至其正式标准化。 | de-facto standard |
| 32 | 适度安全 | 与信息的丢失、滥用或者未经授权访问或未经授权修改所导致的风险和危害大小相称的安全防护。这包括通过使用成本－效益管理、运行控制和技术控制，确保组织所使用的信息系统和应用有效地运行并且提供适当的机密性、完整性和可用性。[来源:GB/Z 25320.2-2013,2.2.7] | 合宜安全 | 安全性之说明，相当于因信息流失、误用、未经授权存取或修改所造成后续伤害之风险及大小。此包括透过使用合乎成本效益之管理、操作及技术控制措施，以保证组织有效运作所用信息系统及应用，以及提供适当机密性、完整性及可用性。 | adequate security |
| 33 | 数据采集和监控系统 | SCADA是监管和控制一个地理上分布的过程的系统。SCADA系统也被称为“远动系统”。用作对地理上广泛分布过程进行监视和控制的系统。这包括用于采集、处理、传输和显示必要的过程信息的所有设备和功能。[来源:GB/Z 25320.2-2013,2.2.195] | 监控及资料撷取 | SCADA：监测及控制地理分布式过程之系统。SCADA系统亦称为“远距控制系统”：用作对地理广泛散布之过程进行监视及控制的系统。此包括用以撷取、处理、传输及显示必要过程信息之所有设备及功能。 | supervisory control and data acquisition, SCADA |
| 34 | 数据对象 | 逻辑节点对象的一部分，表示特定信息如状态或量测。从面向对象的观点，数据对象是数据对象类的实例。DO通常用作事务对象，即数据对象都是数据结构。[来源:GB/Z 25320.2-2013,2.2.74] | 数据对象 | 表示特定信息(例如状态或量测)之逻辑节点对象的部件。就面向对象观点，数据对象系数据对象类别之实例。DO通常用作交易对象，亦即，其为数据结构。 | data object, DO |
| 35 | 数字数据 | 与模拟数据不同，由离散数值或状态表示的数据。变量的整数化值的离散表示，例如用数字表示数量，可能带有特殊字符和“空格”字符。[来源:GB/Z 25320.2-2013,2.2.87] | 数字数据 | 以离散值或状态表示之数据，相对于模拟数据。变量量化值之离散表示，例如数目之数字表示，也许含特殊字符及“空格”字符。 | digital data |
| 36 | 通用高层安全 | ISO/IEC 11586的第5部分，用于安全信息的交换和保护应用数据机密性和完整性的安全变换功能。[来源:GB/Z 25320.2-2013,2.2.102] | 通用上层安全 | ISO/IEC 11586系列之 5部标准，用于安全信息及安全转换功能之交换，以保护应用数据之机密性及完整性。 | generic upper layer security, GULS |
| 37 | 吞吐量 | 不丢弃单数据包，设备单位时间能够处理的最大连续通信量。[来源:GB/Z 25320.2-2013,2.2.204] | 通量 | 装置能处置而不丢弃任一封包之最大连续讯务速率。 | throughput |
| 38 | 一致性测试 | 与验收测试不同，一致性测试是由独立团体执行的测试，以确定某个特定设备是否满足规定的控制文件的标准，比如美国联邦标准、美国国家标准、军用标准或军用规范。[来源:GB/Z 25320.2-2013,2.2.53] | 符合性测试 | 由独立单位执行之测试，以判定设备之特定部件是否满足指定控制文件中之准则，该控制文件诸如美国联邦标准、美国国家标准、军用标准或军用规格。附验收测试之契约。 | conformance test |
| 39 | 用户 | 不管是否授权，能够访问系统的个人、组织实体或者自动化过程。[来源：GB/T 40211-2021，3.2.133] | 使用者 | 人类或系统应用程式。 | user |
| 40 | 远动应用服务元素．2 | 正式是IEC 60870-6标准和非正式称为控制中心之间通信协议(ICCP)。。[来源:GB/Z 25320.2-2013,2.2.202] | 远距控制应用服务组件编号 2 | 系 IEC 60870-6之正式用语，而非正式用语为控制中心间通讯协议（ICCP）。 | TASE.2 |

* + 1. 安全管理

两岸安全管理术语对照见表A.2。

* 1. 海峡两岸安全管理术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | BIS机制 | 安全模块对TCP/IPv4模块和网卡驱动模块之间的数据流进行监听并且转换IPv4成IPv6或反之，这些安全模块嵌入主机因而使它们成为自转换器。[来源:GB/Z 25320.2-2013,2.2.33] | 堆栈中阻碍物 | 安全模块插件，其窥探TCP/IPv4模块与网络卡驱动模块间之数据流，且可自行将IPv4转译为IPv6或将 IPv6转译为 IPv4。 | Bump-in-the-Stack |
| 2 | SSH协议/安全壳协议 | 安全壳协议，利用非安全网络提供安全远程登录的协议。SSH是有专利的但在不远将来将成为IETF标准。SSH原是由SSH通信安全公司开发的。[来源:GB/Z 25320.2-2013,2.2.170] | 安全外壳程序 | 使用不安全网络时提供安全远程登录之协议。SSH将成为 IETF标准。SSH 原由 SSH 通讯安全组织所发展。 | secure shell, SSH |
| 3 | 安全 | a）保护系统所采取的措施；b）由建立和维护保护系统的措施而产生的系统状态；c）能够免于非授权访问和非授权或意外的变更、破坏或者损失的系统资源的状态；d）基于计算机系统的能力，能够提供充分的把握使非授权人员和系统既无法修改软件及其数据也无法访问系统功能，却保证授权人员和系统不被阻止；e）防止对工业自动化和控制系统的非法或有害的入侵，或者干扰其正确和计划的操作。注：措施可以是与物理安全（控制物理访问计算机的资产）或者逻辑安全（登录给定系统和应用的能力）相关的控制手段。[来源：GB/T 40211-2021，3.2.99] | 安全 | 由建立及维护保护手段所产生之状况，其确保不受敌对行动或影响侵犯之状态。所有关于定义、达成及维持机密性、完整性、可用性、不可否认性、可归性、鉴别性及可靠度之层面。 | security |
| 4 | 安全边界 | 应用了安全策略和安全体系结构的区域分界线（逻辑的或物理的），即系统资源得到安全服务保护的区域分界线。[来源：GB/T 40211-2021，3.2.110] | 安全周界 | 安全政策或安全架构适用之领域边界；亦即，安全服务保护系统资源空间之边界。 | security perimeter |
| 5 | 安全策略 | 规范或限定系统或组织如何为保护其资产提供安全服务的规则集合。[来源：GB/T 40211-2021，3.2.112] | 安全政策 | 一组规则及实务，其规定或管制系统或组织如何提供安全服务以保护敏感及关键系统资源。组织单位内部之一组规则，于法律及文化全景内，管制此单位如何保护其资产之管理以符合所规定组织目标。安全计划之目标及限制条件。政策以若干等级建立，范围由组织或公司政策至特定运作之限制条件(例：远程访问)。通常，政策提供〝何者〞及〝为何〞等问题之解答时而不处理”如何〞，政策通常以技术独立用语表示。 | security policy |
| 6 | 安全导则 | 安全导则规定安全程序的目标和限制。在若干层面上，范围从公司或团体策略到特定运行限制（例如远程访问），创建各个导则。通常对“做什么”和“为什么做”这些问题，导则提供答案但不涉及“如何做”。导则一般以与技术无关方式陈述。[来源:GB/Z 25320.2-2013,2.2.175] | 安全指导纲要 | 安全指导纲要定义安全计划之目标及限制条件。指导纲要建立若干等级，范围自公司或企业政策至特定运作限制条件(例：远程访问)。指导纲要通常提供“何者(what)”及“为何(why)”问题之解答而不处理“如何(how)”。指导纲要通常以非技术性用语说明。 | security guideline |
| 7 | 安全风险评估 | 对信息系统(IS)的威胁和信息系统脆弱性进行分析，以及对信息或系统能力的丧失将对国家安全（或任何系统安全）所具有潜在影响进行分析的过程。使用组合分析作为确定适当且成本有效的应对措施的基础。[来源:GB/Z 25320.2-2013,2.2.180] | 安全风险评鉴 | 分析对信息系统(IS)威胁及其脆弱性之过程，以及系统之信息或能力损失对国家[或任何系统]安全的潜在冲击。分析结果系作为识别妥适及合乎成本效益之对策的基础。 | security risk assessment |
| 8 | 安全服务 | 用于提供保密性、数据完整性、认证或信息防抵赖的机制。[来源：GB/T 40211-2021，3.2.115] | 安全服务 | 用以提供信息之机密性、数据完整性、鉴别性或不可否认性之机制。 | security services |
| 9 | 安全管理 | 网络管理中，安全管理是一组功能：（1）防护远程通信网和系统，防止未经授权的个人访问、未经授权的行动或影响；（2）包括许多子功能，比如对安全服务和机制进行创建、删除和控制，分发安全有关信息，报告安全有关事件，控制密钥载体的分发以及批准订阅者的访问、权利和权限。[来源:GB/Z 25320.2-2013,2.2.176] | 安全管理 | 于网络管理中，一组功能(a)保护电信网络及系统，防范个人、行动或影响之未经授权存取，以及(b)包括许多子功能，诸如建立、删除及控制安全服务与机制；散布安全相关信息；报告安全相关事件；控制密码建钥材料之配发；以及授权订户存取、权限及特权。 | security management |
| 10 | 安全性能 | 程序的符合性和措施的完整性，确保了安全措施的持续有效性和适用性。包括特定威胁的保护、泄密后分析、业务需求变更、新威胁、脆弱性信息的审核，以及控制系统的周期审计。注：要求用测试、审计、工具、措施或者其他方法来评定实际的安全性能。[来源：GB/T 40211-2021，3.2.111] | 安全效能 | 效能评估，依据程序遵循性、提供特定威胁保护之措施的完整性、后破解分析、变更营运要求事项之审查、新威胁及脆弱性信息，以及控制系统之定期稽核，以确保安全措施保持有效及妥适。测试、稽核、工具、措施或其他方法须评估其安全实务效能。 | security performance |
| 11 | 安全域 | 由安全策略、安全模型或安全体系结构定义的环境或上下文，包括各系统资源和有权访问这些资源的各系统实体。在单一可信机构管控下的系统或子系统。安全局可以是组织化的（如层次的），以形成更大的域。[来源:GB/Z 25320.2-2013,2.2.174] | 安全领域 | 由安全政策、安全模型或安全架构所定义之环境或全景，包括1 组系统资源及1组有权存取资源之系统个体。 | security domain |
| 12 | 安全证明 | 为支持安全合格鉴定，对信息系统的管理、运行和技术的安全控制所作的综合评估，确定在符合系统的安全需求上，正确执行控制、按预期运行和产生期望结果的程度。[来源:GB/Z 25320.2-2013,2.2.39] | 验证 | 信息系统中管理、运作及技术性安全控制措施之综合评鉴，于安全认证之支持中为之，以决定何种程度上正确地实作控制措施、如预期运作，以及产出关于符合系统安全要求事项之预期成果。 | certification |
| 13 | 风险 | 以概率的形式表示特定威胁利用特定脆弱性造成特定后果的预期损失。[来源：GB/T 40211-2021，3.2.87] | 风险 | 给定威胁将利用资产或资产群组之脆弱性，因而导致伤害组织之可能性。其依事件机率及其后果之组合量测。损失之期望值，以特定威胁将利用具特定有害结果之特定脆弱性的机率表示。给定威胁之潜在冲击及该威胁发生之可能性，对机构运作(包括任务、功能、形象或声誉)、机构资产或信息系统运作之个别结果的冲击等级。 | risk |
| 14 | 风险管理 | 基于风险评估来辨识和采用与所保护的资产价值相称的对抗措施的过程。[来源：GB/T 40211-2021，3.2.89] | 风险管理 | 信息系统运作造成对机构运作(包括任务、功能、形象或声誉)、机构资产或个人之管理风险过程。其包括风险评鉴、本益分析、安全控制措施之选择、实作及评鉴，以及对运作系统之正式授权。过程考虑有效性、效率，以及来自法律、指令、政策或法规之限制条件。 | risk management |
| 15 | 风险评估 | 系统地辨识重要系统资源的潜在脆弱性和威胁，基于发生的概率量化损失风险和后果，并（可选地）建议如何对各对抗措施分配资源以使总风险最小的过程。注 1：资源类型包括物理资源、逻辑资源和人力资源。注 2：风险评估常与脆弱性评估相结合，以辨识脆弱性并量化相关风险。周期地执行这些内容是为了反映组织机构的风险裕度、脆弱性、规程、人员和技术上的变化。[来源：GB/T 40211-2021，3.2.88] | 风险评鉴 | 风险评鉴系风险识别、风险分析及风险评估之整个过程。风险评鉴过程之目标系识别及评估对所识别之资产具有负面冲击的风险，以及适当的安全防护及行动之定义，其极小化所识别风险之效应。经由决定发生机率、造成冲击及将减轻此冲击之额外安全控制措施，识别对机构运作(包括任务、功能、形象或声誉)、机构资产或个人之风险的过程。风险管理一部分，与风险分析及连带之威胁及脆弱性分析为同义词。 | risk assessment |
| 16 | 计算机安全/网络安全 | 用于防止关键系统或者信息类资产的非授权使用、拒绝服务、修改、泄露、财政损失和系统损害的行为。注：目标是降低风险，这些风险包括人身伤害、威胁公共健康、丧失公众或者消费者信任度、泄露敏感资产、不能保护商业资产，或者违背法规。这些概念适用于生产过程的任何系统，包括单机的和网络的设备。系统间的通信可以通过内部报文或者通过任何操作员或机器接口，以便认证、操作、控制，或和任意的控制系统交换数据。计算机安全包括标识、认证、问责制、授权、可用性和隐私。[来源：GB/T 40211-2021，3.2.36] | 网宇安全 | 信息安全。不论是意外或蓄意，防止信息未经授权揭露、转送、修改或破坏之保护。 | cyber security/cybersecurity |
| 17 | 计算机紧急响应组织 | 一般认为CERT是作为因特网正式应急组织。[来源:GB/Z 25320.2-2013,2.2.50] | 计算机紧急应变小组 | CERT通常被认定为因特网之正式紧急应变小组。备考：此用语亦可用于公司或其他群组内部，以描述紧急应变小组。 | Computer Emergency Response Team; CERT |
| 18 | 监管链 | 以包括处理证据的每个人、收集或传递证据的日期／时间和传递目的形成文件，通过证据的收集、安全保管程分析生命期，对证据迁移进行追踪的过程。[来源:GB/Z 25320.2-2013,2.2.41] | 监管链 | 藉由登载每个人处置之证据、搜集或转送之日期/时间及转送之目的，透过搜集、保护及生命周期分析以追踪证据移动之过程。 | chain of custody |
| 19 | 审计 | 对记录和活动的独立的审查和检查，来评估系统控制的充分性，以确保与已建立的策略和操作规程一致，并且给出对控制、策略或者程序进行必要改动的建议（见 3.2.100）。注：审计有三种形式：外部审计是由非组织雇员或者承包人实施；内部审计是由组织内专门从事内部审计的独立部门实施；自我评估控制由组织内部的同行实施。[来源：GB/T 40211-2021，3.2.11] | 稽核 | 就遵循性及符合性，针对预期事项作正式询问、正式检查或事实之查证。进行独立审查并检视系统纪录及活动，测试数据安全及数据完整性程序之适切性及有效性，以确保遵循已建立之政策及运作程序，且建议任何必要改变。 | audit |
| 20 | 审计纪录域 | 包含关于一个事务中的所有实体和这些实体所执行的处理类型指示的信息的域。[来源:GB/Z 25320.2-2013,2.2.19] | 稽核纪录字段 | 包含于交易中所有有关个体之信息，以及该等个体所履行处理之型式指针的字段。 | audit record field |
| 21 | 审计日志 | 包含修改记录详情的计算机文件。要求系统恢复时也可以使用该文件。启用该特性通常导致一些系统开销，但它的确使所有系统活动能事后评估。[来源:GB/Z 25320.2-2013,2.2.18] | 稽核存录 | 包含对纪录修订细节之计算机档案，其亦可用于要求系统复原之事件。启用此功能经常引起某些系统额外负担，但其的确有助于所有系统活动之后续审查。备考：于可能安全遭破解后之技术及鉴识分析时，稽核存底至关重要。 | audit log |
| 22 | 审计追踪 | 一个或一系列记录，使得计算机或文秘系统所执行的处理能被精确地识别出来。因包括创建和对修改进行授权的用户的细节，这通常使得能核查修改的真实性。[来源:GB/Z 25320.2-2013,2.2.20] | 稽核存底 | 纪录或一系列纪录，其能准确地识别由计算机或事务系统所执行之处理，亦常能查证修订之正确性，包括建立及授权该等纪录之用户细节。备考：于可能安全遭破解后之技术及鉴识分析时，稽核存底至关重要。 | audit trail |
| 23 | 授权过程 | 同意给予系统实体访问系统资源权限的过程。[来源:GB/Z 25320.2-2013,2.2.24] | 授权过程 | 授权过程系（对系统个体）赋予权利（以存取系统资源）之程序。 | authorization process |
| 24 | 授权用户 | 安全防护中，经授权用户就是根据组织的安全策略，可以执行某种操作的用户。[来源:GB/Z 25320.2-2013,2.2.25] | 授权用户 | 安全上，用户依组织之安全政策可进行操作。 | authorized user |
| 25 | 数据安全 | 防护数据免受未经授权（无意或有意）修改、破坏或泄露。[来源:GB/Z 25320.2-2013,2.2.75] | 数据安全 | 数据之保护，以防止未经授权(意外或故意)之修改、破坏或揭露。 | data security |
| 26 | 特权 | 执行特定功能的授权或一系列授权，尤其是在计算机操作系统环境中。注：使用特权控制的功能包括：确认报警、改变设定点、修改控制算法。[来源：GB/T 40211-2021，3.2.78] | 特殊权限 | 由权责单位指派予主体之属性或性质。 | privilege |
| 27 | 网络管理 | 对网络进行规划、设计、实施、运行、监视和维护的过程。[来源:GB/Z 25320.2-2013,2.2.135] | 网络管理 | 规划、设计、实作、运作、监视及维护网络之过程。 | network management |
| 28 | 问责制/可证实性/可审计性/可追溯性 | 系统属性（包括其系统的所有资源），以确保一个系统实体的行动可追溯到该唯一的实体，并且该实体可为他的行为负责。[来源：GB/T 40211-2021，3.2.3] | 可归责性 | 确保个体之行动可被唯一地追踪至该个体之性质。系统之性质（包括其所有系统资源），其确保系统个体之行动可被唯一地追踪至应对该行动负责之个体。 | accountability |
| 29 | 信任 | 1.信息系统用法：信赖系统的某人对该系统符合其规范能够达到完全相信的程度，即系统做它声称所做的事而不执行不需要的功能。在密码技术和密码系统中：使得一个实体能假定另一个实体的行为完全如第一个实体所期望的那样的特性。[来源:GB/Z 25320.2-2013,2.2.210] | 信任 | 对资讯之可靠度及真实性，或对个体于规定全景下采取适切行动的能力及倾向之坚定信念。 | trust |
| 30 | 信息安全防护 | 为了提供机密性、完整性和可用性，保护信息和信息系统免受未经授权访间、使用、泄露、中断、修改或毁坏。[来源:GB/Z 25320.2-2013,2.2.108] | 信息安全 | 信息及信息系统之保护，防止未经授权之存取、使用、揭露、中断、修改或破坏，以提供机密性、完整性及可用性。 | information security |
| 31 | 嗅探/侦听 | 无源搭线窃听。[来源:GB/Z 25320.2-2013,2.2.189] | 网络封包分析 | 被动搭线 | sniffing |
| 32 | 应对措施/对抗（措施） | 行动、设备、程序或者技术。这些措施能够降低威胁、脆弱性，可预防、消除攻击和最小化攻击所造成的危害，或者可发现和报告这些攻击以便采取正确的行动。注：“控制” 在某些上下文中也用于描述这个概念。本文件中采用 “对抗措施” 这个术语就是为了和文中采用的 “过程控制” 中的控制这个词不相互混淆。[来源：GB/T 40211-2021，3.2.33] | 对策 | 行动、装置、程序或技术，藉由排除或防止、能导致伤害之最小化或发现并陈报而采取之矫正措施，以减少威胁、脆弱性或攻击。行动、装置、程序、技术或其他措施，其减少信息系统脆弱性。与安全控制措施及保全措施同义。 | countermeasure |

* + 1. 攻防视角

两岸攻防视角术语对照见表A.3。

* 1. 海峡两岸攻防视角术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | smurf攻击 | 利用IP广播地址和因特网控制消息协议(ICMP)的ping数据包导致泛洪(flooding)，从而发动拒绝服务攻击(smurfing)的软件。利用 TCP/IP协议内IP协议特性的攻击。[来源:GB/Z 25320.2-2013,2.2.188] | 挂载阻绝服务攻击 | 挂载阻绝服务攻击之软件(“smurfing”)，其利用 IP广播寻址及 ICMP ping封包以导致泛流攻击。利用 TCP/IP 协议中 IP 协议特征之攻击。 | smurf |
| 2 | 安全受损/危害（泄密） | 信息被未授权泄露、修改、替代或者使用（包括密钥和其他关键安全参数）。[来源：GB/T 40211-2021，3.2.26] | 破解 | 对未经授权之人员揭露信息，或系统中违反安全政策之蓄意及非蓄意的未授权之揭露、修改及破坏，或已发生对象之遗失。未经授权之揭露、修改、替代或敏感数据之使用(包括明文、密码密钥及其他关键安全参数)。 | compromise |
| 3 | 病毒/计算机病毒 | 通过将自身副本插入到其他可执行的代码或文件中进行传播的，可自我复制或者自我衍生的程序。[来源：GB/T 40211-2021，3.2.134] | 病毒/计算机病毒 | 隐藏且自我复制之计算机软件区段，通常为恶意逻辑，经感染另一程序传播(亦即将自身复本插入并变成另一程序之一部分)。病毒自身不能运行；其要其求寄宿程序运行使病毒作用。所欲程序，其将自身置入其他程序中，于计算机系统间被分享及自我复制。备考：病毒经常对其感染之可执行程序显露毁灭性或破坏性影响。自我复制之恶意软件区段，将自己附接至应用程序或其他可执行系统组件，且其出现不留下明显记号。 | virus/computer virus |
| 4 | 嘲鸟病毒 | 特洛伊木马型病毒程序，截获用户和主机间通信并且提供如同系统样的响应，而通常为以后（有时恶意）使用还存储用户的响应。[来源:GB/Z 25320.2-2013,2.2.132] | 学舌鸟程序 | 一种特洛伊木马病毒程序，截取用户与主机间之通讯，并提供类似系统之响应，其经常储存使用者响应以供稍后(有时为恶意)使用。 | mockingbird |
| 5 | 篡改 | 1.为确定某些数据（比如保密数据）的特性或监视／记录这些数据，渗透或修改内部操作或者插入有源或无源搭线窃听机制。敏感系统或敏感信息的未经授权修改。[来源:GB/Z 25320.2-2013,2.2.201] | 破坏 | 对内部运作之渗透或修改，或插入主动或被动搭线机制，以决定其本质，或监视或记录，例：秘密数据。未经授权修改敏感系统或敏感信息。 | tampering |
| 6 | 电子欺骗 | 以某种方式故意辐射、再辐射、变更、抑制、吸收、拒收、增强或反射电磁态，试图对敌方或敌方的电子依赖武器传递误导信息和造成拒收有效信息。通过对敌方电子系统所接收的信息进行解析或使用，专用于误导敌方的故意行动。[来源:GB/Z 25320.2-2013,2.2.93] | 电子诈欺 | 精心设计之电磁能放射、再放射、改变、消除、吸收、否认、加强或反射，意图传达误导信息及阻绝有效信息予敌人或敌人之电子相关武器。 备考：电子诈欺之型式有：(1)操控式电子诈欺，以行动消除暴露或传达误导、搅乱可被敌方使用之告示指标；(2)仿真式电子诈欺，表示友善之假象或实际能力以误导敌方；(3)模仿式电子诈欺，将电磁能引入敌方系统以模仿敌方发射。精心设计之活动，以误导敌人对其电子系统所接收信息之解译或使用。 | electronic deception |
| 7 | 钓鱼攻击 | 通过基于计算机的欺骗手段（例如因特网web网站），诱骗个人泄露敏感的个人信息。[来源:GB/Z 25320.2-2013,2.2.144] | 网络钓鱼 | 透过诈欺式计算机工具(例：因特网网站)，诈骗个人使其揭露敏感个人信息。 | phishing |
| 8 | 恶意代码 | 编写的程序或代码，目的是收集有关系统或用户的信息、破坏系统数据，并为进一步侵入系统提供支点、伪造系统数据和报告或者耗费系统操作和维护人员的时间。注 1：恶意代码攻击常以病毒、蠕虫、木马或者其他自动传播的形式出现。注 2：恶意代码也常指 “恶意软件”。[来源：GB/T 40211-2021，3.2.70] | 恶意码 | 程序或部分程序，精心设计编码以造成非预期之非所欲事件。 | malicious code |
| 9 | 恶意软件 | 明确专用于危害或破坏系统的恶意软件，如病毒或特洛伊木马。企业执行未经授权处理的软件或固件，该处理将对信息系统的机密性、完整性或可用性具有负面影响。病毒、蠕虫、特洛伊木马或其他感染主机的基于代码的实体，间谍软件和一些广告软件也都是恶意代码的例子。[来源:GB/Z 25320.2-2013,2.2.127] | 恶意软件 | 恶意软件，诸如病毒或特洛伊木马，特别设计以破坏或扰乱系统。软件或韧体，蓄意履行未经授权过程，对信息系统之机密性、完整性或可用性将有不利冲击。感染主机之病毒、蠕虫、特洛伊木马或其他程序个体。间谍软件及某些形式之广告软件，亦为恶意码(恶意软件)的范例。 | malware |
| 10 | 攻击/计算机攻击 | 来自智能威胁对系统安全的袭击。该智能行动是有意的，企图（特别在方法和技术意义上）规避安全服务和违反系统的安全策略。试图旁路信息系统（IS）的一种或多种安全控制的有意动作。信息系统的安全控制包括不可否认性、认证性、完整性、可用性或机密性。[来源:GB/Z 25320.2-2013,2.2.16] | 攻击/网宇攻击 | 衍生自智能型威胁之系统安全袭击，亦即，精心策划试图(特别是方法或技术)规避安全服务及违反系统安全政策之智能型行动。试图绕过1或多个信息系统(IS)之安全控制措施(不可否认性、鉴别、完整性、可用性或机密性)之故意行动。 | attack/cyber attack |
| 11 | 骇客 | 1.经常随意地闯入或试图闯入或未经授权使用计算机网络或系统的人，出于个人娱乐或高兴因而并不必定具有恶意目的。热衷于对系统、计算机和尤其对计算机网络的内部机理具有实质了解的人。该用语通常并不使用在贬义语境中，而那儿“黑客”似乎是很合适的说法。其目标是击破第三方计算机系统或网络的安全防护的个人。以某种方式使用了计算机资源的人，这并非是故意的或虽然这是有违于容许－使用原则但在动机上并不必定是恶意的（不像是黑客的活动）。[来源:GB/Z 25320.2-2013,2.2.103] | 黑客 | 未经授权即侵入、试图侵入或使用计算机网络或系统之个人，通常系随机，为个人娱乐或满足，且未必具恶意意图。喜好于深入了解系统与计算机，尤其计算机网络等内部运作之个人。此用语常误用于〝刽客〞才是正确用语之恶意情境中。亦参照：刽客。其目标为渗透第 3 方计算机系统或网络安全防护之个人。使用计算机资源之方式系非蓄意或违反可接受使用政策之规定的个人，惟(不像刽客之行为)未必具恶意之意图。 | hacker |
| 12 | 黑客 | 高手(cracker)是黑客行话，表明他是一位突破系统安全防护的黑客。具有恶意意图，获得或试图获得非法访问计算机或计算机程序的个人。[来源:GB/Z 25320.2-2013,2.2.59] | 刽客 | 黑客之行话，泛指称“破解系统安全性者”。备考：“cracker”一词大约于 1985 年由黑客们防止新闻媒体误用“hacker”所创造。具恶意企图之个人，取得或尝试获取对计算机或计算机程序之非法存取。备考：与通行码刽客同义。 | cracker |
| 13 | 后门/陷门 | 一种硬件或软件机制。通过后门而不是用通常的过程，提供对系统和系统资源访问；它是系统设计者或维护者有意保留的，而且通常并不公开让人知道。[来源:GB/Z 25320.2-2013,2.2.27] | 后门/暗门 | 硬件或软件之机制，其（1）以通常程序外之方式，供存取系统及其资源、（2）由系统设计者或维护者故意留置且（3）通常非属众所周知。 备考：类似暗门，但通常并非恶意实作之。 | back door/trap door |
| 14 | 缓冲区溢出 | 接口的一种状况，多于分配容量的输入能被置人缓冲区或数据存储区域而造成对其他信息的覆盖。敌方利用如此状况使系统崩溃或植入特别编成的编码，使其能获得对系统的控制。[来源:GB/Z 25320.2-2013,2.2.32] | 缓冲区溢出 | 输入超出能置入缓冲区或数据保持区所配置容量，因而覆写其他信息之接口的情况。恶意者利用此种情况，使系统当机或插入特别编写之程序代码以允许其取得系统控制。 | buffer pverflow |
| 15 | 间谍软件 | 为了收集个人或组织的信息，在未经他们知道的条件下秘密地或偷偷地安装在信息系统中的软件。间谍软件是一种恶意代码类型。[来源:GB/Z 25320.2-2013,2.2.192] | 间谍软件 | 被秘密或暗中安装至信息系统之软件，于个人或组织不知情之下，搜集其信息；一种恶意码之型式。 | spyware |
| 16 | 肩窥 | 在人们输入他们的口令时，越过他们的肩膀进行窥视。[来源:GB/Z 25320.2-2013,2.2.184] | 肩窥 | 由某人肩膀后面偷窥其输入之通行码。 | shoulder surfing |
| 17 | 键记录器 | 专用于记录计算机键盘上所按压的键位的程序，用于获取口令或加密密钥从而旁路其他安全措施。[来源:GB/Z 25320.2-2013,2.2.121] | 密钥登录器 | 设计以记录计算机键盘键入何密钥用以取得通行码或加密密钥，因而略过其他安全步骤之程序。 | key logger |
| 18 | 拦截 | 未经送信双方同意，企图为他人获得通信的占有并且通常并不延迟或阻断传输。传输信号的截获，具有对由预定的目的用户接收的那个信号进行延迟或消除的企图。[来源:GB/Z 25320.2-2013,2.2.112] | 截取 | 所有结合1或多个处理器之装置，具有由或至外部来源(例：电子多菜单计、数字式电驿或控制器) 接收或发送数据/控制之能力。 | intercept |
| 19 | 欺骗 | 假装是一个授权用户而执行未经授权的活动。[来源:GB/Z 25320.2-2013,2.2.191] | 欺骗 | 伪装成授权之使用者且履行未经授权之动作。 | spoof |
| 20 | 窃取/窃听 | 未授权组织对通信信息的监视或者记录。[来源：GB/T 40211-2021，3.2.46] | 窃听 | 秘密地被动式窃听，亦即，未知通讯之发起者或预期接收者所知悉。 | eavesdropping |

* + 1. 通信

两岸通信术语对照见表A.3。

* 1. 海峡两岸通信术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | [报文] 分组，[信息] 包 | 数据通信网中发送数据的单位。在设备间交换的数据包，可以分为 3 种：数据分组，就是信息或文件的内容；管理分组，就是对通信链路进行管理的分组，如通信出错、重发分组等信息；控制分组，如建立和拆除链路、服务请求等。[来源：GB/T 32402-2015，3.1.229] | 封包 | 按特定格式编排，包含控制资料及可能的使用者资料，且作为整体传输及交换的位元序列。 | packet |
| 2 | Cookie | 与所请求资源一道由web服务器提供给浏览器的一段信息，用于浏览器暂存并在任何随后访问或请求时返网该服务器。[来源:GB/Z 25320.2-2013,2.2.57] | 讯录 | 由信息网服务器提供至浏览器之信息片段，连同所请求之资源，供浏览器暂时储存并于任何后续造访或请求时回传给服务器。 | cookie |
| 3 | IEE 802.lli标准 | 国际电气和电子工程师协会(IEEE)信息技术标准，远程通信和系统—当地和城域网间信息交换—特定要求 第11部分：有线LAN介质接入控制（MAC）和物理层(PHY)规范修正6：介质接入控制（MAC）安全增强。[来源:GB/Z 25320.2-2013,2.2.107] | IEEE 802.11i | 国际电机电子工程师学会（IEEE）标准， 为信息技术与系统间及信息交换－区域及都会局域网络－特定要求事项－第 11 部：无线 LAN 介质访问控制(MAC)及物理层(PHY)规格－补充增修 6：介质访问控制(MAC)安全增强事项(IEEE 802.11i)。 | IEEE 802.11i |
| 4 | 抽象通信服务接口 | 对智能电子设备(IED)的虚拟接口，提供抽象通信服务,例如连接、变量访问、未经请求的数据传输、装置控制和文件传递服务，与所使用的实际通信栈和协议集无关。[来源:GB/Z 25320.2-2013,2.2.1] | 抽象通讯服务接口 | 介接至智能电子装置（IED）之虚拟接口，用以提供抽象通讯服务，例：与使用实际通讯堆栈及剖绘无关之连接、变量存取、非恳求数据传输、装置控制及档案转送服务等。 | Abstract Communication Service Interface：ACSI |
| 5 | 篡改检测 | 对篡改企图已经实现而危及到密码模块安全，由该模块所作出的自动判断。[来源:GB/Z 25320.2-2013,2.2.200] | 破坏侦测 | 密码模块之自动判定已发生危害模块安全性所进行之尝试。 | tamper detection |
| 6 | 存取控制列表 | 告诉计算机的操作系统每个用户拥有哪些访问权限的表格，比如说对一个文件目录或者是单个文件有访问权限。[来源：GB/T 32402-2015，3.1.17] | 访问控制表列 | 藉由列举允许存取资源之系统个体身分，对系统资源实作访问控制之机制。 | Access Control List；ACL |
| 7 | 带宽 | 测量频率的参数，是传输信道的最高和最低频率的差值。有时候，技术人员也常非正式的将带宽称作信道的吞吐量，用 kbit/s 或者 Mbit/s 来表示。[来源：GB/T 32402-2015，3.1.40] | 带宽 | 常意指于给定数量之时间，透过信道传递数据之信道容量。常以每秒位数表示之。 | bandwidth |
| 8 | 点对点协议 | 允许计算机在因特网上使用普通电话线和 Modem 进行 TCP/IP 连接的协议。[来源：GB/T 32402-2015，3.1.234] | 点对点协定 | 经由串接之点对点链路，传输网络层数据报(例：IP 封包)之因特网标准协议。 | point-to-point protocol;PPP |
| 9 | 电路交换 | 在同一电信网用户群中，任意两个或多个用户终端之间建立暂时电路连接的交换方式。当用户发起呼叫时，网络为通信双方建立一条端到端的物理电路，供通信双方专用。本次通信结束时，网络将该物理电路拆除。公用电话网就是采用这种交换方式。[来源：GB/T 32402-2015，3.1.61] | 电路交换 | 一经要求即连接两个或多个资料终端设备，并在连接未解除前，让其专用其间资料电路的过程。 | circuit switching |
| 10 | 访问 | 为了使用系统资源而与系统进行通信，或别的互动的能力和手段。注：访问可能会涉及物理访问（物理上允许在某个区域授权，拥有物理的加密装置，PIN 码或访问卡或允许访问的生物特征）或逻辑访问（通过逻辑和物理方法的结合，获得授权登录到系统和应用）。[来源：GB/T 40211-2021，3.2.1] | 存取 | 为使用系统资源，以处置系统所包含信息或取得其信息之知识，而与系统进行通讯或其他互动之能力及方法。 | access |
| 11 | 访问控制 | 保护系统资源防止未授权的访问；系统资源使用的过程是根据安全策略规定的，并且根据该策略只允许被授权的实体（用户、程序、过程或者其他系统）。[来源：GB/T 40211-2021，3.2.2] | 访问控制 | 防止未经授权使用资源，包括防止以未经授权方式使用资源。保护资源免于未经授权存取，依安全政策监管资源使用之过程，仅允许依该政策所授权之系统个体得以使用资源。规则及部署机制，其控制信息系统之存取及实体进出场所。信息安全所有主题皆以访问控制为基础，若无此基础则所定义之信息安全无法存在。 | access control |
| 12 | 分组交换 | 数据传输的一种方式。采用分组交换，数据被分成许多段，每一段放入一个分组中，每个分组都包含有控制信息，每个分组通过用户共享的电路发送。当每个分组通过网络传输时，占用信道的时间很短，多个用户可以共享信道。[来源：GB/T 32402-2015，3.1.232] | 分封交换 | 资料网络中选路及传输 \* 资料的过程，通过附地址封包，使两个节点间的各传输通道能动态配置给不同位址的封包。 | packet switching |
| 13 | 广播 | 多播分组的一种特别的形式，网络上的所有节点都等待着接收广播报文。[来源：GB/T 32402-2015，3.1.54] | 广播 | 将某些资料传输到所有目的地 。 | broadcast |
| 14 | 基于角色访问控制 | 基于身份的访问控制的形式，其中所识别和控制的系统实体在机构或过程中处于功能性位置。[来源：GB/T 40211-2021，3.2.92] | 角色式访问控制 | 一种身分式访问控制形式，其中所识别及控制之系统个体系于组织或过程中具有功能位置。 | role based access control, RBAC |
| 15 | 接口 | 两个功能单元之间的共享边界，由功能特性、信号特性或其他合适的特性定义。[来源：GB/T 21099.2-2024，3.1.46] | 界面/介面 | 2 个功能单元间之共享边界（shared boundary），由事关功能、实体互连（physical interconnection）、信号交换之特性（characteristic），以及该单元视情况而定之其他特性所定义。 | interface |
| 16 | 控制方向 | 由控制站向被控站传送数据。[来源：GB/T 21099.5-2024，3.3] | 控制方向 | 由主控站至受控站之传输方向。[来源：IEC 60870-5-101:2003 之 3.3。] | control direction |
| 17 | 口令 | 一个秘密数据值，通常是用作认证信息的字符串。用于实体认证的秘密字、短语、数字或字符序列。口令是依靠记忆的弱秘密。用于证明身份或验证访问授权的字符串（字母、数字和其他符号）。[来源:GB/Z 25320.2-2013,2.2.142] | 通行码 | 秘密数据值，常作为鉴别信息用之字符串。供个体鉴别用之秘密字组、词组、数字或字符序列，其为被记忆之弱度秘密。字符(字母、数字及其他符号)串，用以鉴别身分或查证存取授权。 | password |
| 18 | 强认证 | 通过密码技术产生的凭证的认证。认证过程。该认证使用密码技术，特别是公钥证书，以验证实体所声称的身份。[来源:GB/Z 25320.2-2013,2.2.193] | 强鉴别 | 藉由密码衍生信符之手段鉴别。此鉴别过程使用密码学，尤其是公钥凭证，以查证个体所宣称之身分。备考：多因子鉴别可能比任何单一鉴别方法更强。 | strong authentication |
| 19 | 认证/鉴别 | 旨在建立传输、信息或发起方有效性的安全方法，核实接收特定信息类别的个人授权的方法的有效性。[来源：GB/T 40211-2021，3.2.13] | 鉴别 | 为建立传输、讯息或发起者之有效性而设计的安全措施，或对接收特定种类信息查证个人授权之方法。查证用户、过程或装置之身分，常作为允许存取信息系统资源之先决条件。经适当签章或弥封之证据，证明该文件系真实且正式。确认信息来源，或确定个体身分之过程。对个体所宣称身分提供之保证。 | authentication |
| 20 | 软件狗 | 一种可移动的物理电子装置，要求加装到计算机上才使得某特殊软件程序能运行。[来源:GB/Z 25320.2-2013,2.2.91] | 插接物 | 可携式实体电子装置，须附接至计算机以使特定软件程序得以执行。 | dongle |
| 21 | 生物特征 | 人类的身体或行为特征。可测定的身体特征或个人行为特性，用于确认申请者身份或证实其声称的身体。面部影像、指纹和笔迹样本都是生物特征例子。[来源:GB/Z 25320.2-2013,2.2.29] | 生物量测 | 人类之身体或行为特征。可量测之身体特征或个人行为 特质，用以辨识申请者身分，或查证其宣称之身分。脸部影像、指纹及笔迹样本皆为生物量测之例。 | biometric |
| 22 | 授权 | 授予系统实体访问系统资源的权力或权限。[来源：GB/T 40211-2021，3.2.14] | 授权 | 赋予系统个体存取系统资源之权利或许可。 | authorization |
| 23 | 数据报 | 一个独立自主的数据实体，它从源地向目的地传送充分的信息而不依赖于在源和目的计算机之间的初期交换和传送网络。[来源：GB/T 32402-2015，3.1.78] | 数据报/资料包 | 分封交换中，从发送端资料终端设备（DTE）到目的地 DTE，具备充分路由资讯，无需依赖该 DTE 与网络间先前交换，且与其他封包无关的封包。 | datagram |
| 24 | 隧道 | 数据通信系统中的一种封装技术，它在一个分组中封装进去一个高层协议，并通过系统传输。[来源：GB/T 32402-2015，3.1.297] | 隧道 | 计算机网络中所建立之信道，将通讯协议之数据封包囊装(载送、分层)于第2个协定中(于其上)，其通常被载送于第 1层之上层或同层。备考：VPN为隧协定之例。 | tunnel/tunneling |
| 25 | 挑战握手认证协议 | 用于PPP的对等实体认证方法，使用随机产生的挑战并且要求与取决于挑战和秘密密钥的密码哈希的响应进行匹配。[来源:GB/Z 25320.2-2013,2.2.42] | 诘问交握鉴别协定 | 使用取决于诘问及秘密密钥之密码哈希，随机产生之诘问及匹配响应之要求的PPP同层个体鉴别法。 | Challenge Handshake Authentication Protocol;CHAP |
| 26 | 挑战-响应 | 一个认证过程，要求在挑战的响应中所提供的正确认证信息对身份进行验证。在计算机系统中，不可预知的挑战值的响应中认证信息通常是一个要求计算所得的数值。[来源:GB/Z 25320.2-2013,2.2.43] | 凭证请求/诘问－回应 | 当要求新公开金钥凭证或公开金钥凭证之更新时发出的请求。 | certification request |
| 27 | 通道 | 在通信管道（见 3.2.27）内建立的特定的通信链接。[来源：GB/T 40211-2021，3.2.20] | 通道 | 数据传输通道（data transmission channel），数据传输的一种方法。注：通道可由例如频率或分时多工法提供。 | channel |
| 28 | 异步传输模式 | 一种高速的、面向连接的交换和多路复用技术，它使用长度为 53 字节的信元，可以同时传送不同类型的业务，如话音、图像和数据。[来源：GB/T 32402-2015，3.1.36] | 非同步传输 | 每字元或字元块在开始的发生时间是任意的数据传输；但一启动以后，代表字元或区块内位元的每一信号发生时间对固定时间基准之有效瞬间具有同样关系；发送一字元时，先送出一个起始位元，送完后又送出一个停止位元的传输方法。 | asynchronous transfer mode;ATM/asynchronous transmission |
| 29 | 智能电子设备 | 由一个或多个处理器组成的装置，具有从外部源接收或向外部源发送数据／控制的能力（例如电子多菜单、数字继电器或控制器）。[来源:GB/Z 25320.2-2013,2.2.111] | 智能电子装置 |  | intelligent electronic device, IED |
| 30 | 智能卡 | 包含一个或多个集成电路芯片的信用卡大小的设备，这些芯片执行计算机的中央处理器、内存和输入／输出接口的功能。。[来源:GB/Z 25320.2-2013,2.2.187] | 智能卡 | 信用卡大小之装置，包含 1 或多个集成电路芯片，其履行计算机中央处理器、内存及输入/输出接口之功能。 | smart card |
| 31 | 组播 | 允许一个分组的多个拷贝发送到选定的所有可能的目的站点的技术。[来源：GB/T 32402-2015，3.1.203] | 多播 | 将某些资料传输到经选择的目的群组 。 | multicast |

* + 1. 网络

两岸术语网络对照见表A.5。

* 1. 海峡两岸网络术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | SYN泛洪 | 一种拒绝服务攻击，向主机发送超过该协议实现所能处理的TCP的SYN数据包（用于打开一个连接时，请求同步序列号）。[来源:GB/Z 25320.2-2013,2.2.199] | SYN泛流 | 阻绝服务攻击，其发送超过协议实作能处置之大量 TCP SYN 封包(请求同步序号，用于开启连接)给主机。 | SYN flood |
| 2 | WiFi | WiFi Alliance供货的产品商标，支持使用基于IEEE 802. 11标准的无线局域网设备。[来源:GB/Z 25320.2-2013,2.2.219] | WiFi | WiFi联盟所提供之商标，藉以推广使用依据IEEE 802.11标准之无线 LAN设备。 | WiFi |
| 3 | 代理 | 在客户端计算机系统和服务器计算机系统之间中继协议的计算机进程，在客户端看来是服务器，而在服务器看来是客户端。[来源：GB/T 21099.2-2024，3.1.60] | 代理器 | 1.代理器系“分隔”客户端及服务器间连接之应用程序。代理器接受进入或离开网络之某些型式讯务，并将其处理及转送。此有效地关闭内部与外部网络间之直通路径，使攻击者更难获得内部地址及组织内部网络之其他细节。常用因特网服务皆可用代理服务器；例：超文本转送协议(HTTP)代理器供网页存取使用，简易邮件转送协议(SMTP)代理器供电子邮件使用。计算机过程－通常作为防火墙或其一部分－于客户端及服务器计算机系统间转送协议，以客户端对待服务器，并以服务器对待客户端。 | proxy |
| 4 | 端口 | 端口在网络中意味这几种事物：（1）在一个网络设备中是电缆的硬件连接点。集线器和交换机典型地提供用于连接以太网设备的多个端口。这些硬件端口有不同的物理形状，例如，雄、雌、圆形、矩形、正方形等。（2）一个网络端口在用 TCP 或 UDP 传输的数据报中是一个应用程序的鉴定。[来源：GB/T 32402-2015，3.1.235] | 埠 | 信号能进出网络的端点 。 | port |
| 5 | 端口扫描 | 使用程序远方确定系统哪些端口是开放的（即是否系统允许通过那些端口连接）。[来源:GB/Z 25320.2-2013,2.2.148] | 端口扫描 | 使用程序以远程决定系统上哪些端口开放(例如系统是否允许透过该等埠连接)。 | port scanning |
| 6 | 泛洪 | 企图以向实体提供超出其能够适当处理的输入，导致计算机系统故障（特别是计算机系统安全方面故障）或另一个数据处理实体故障的攻击。[来源:GB/Z 25320.2-2013,2.2.98] | 泛流 | 藉由提供比个体能正确处理更多之输入，试图导致计算机系统或其他数据处理个体(特别是安全)失效之攻击。 | flooding |
| 7 | 非军事化区 | 逻辑上介于内部和外部的网络段。注 1：非军事化区的目的是为外部信息交换提供内部网络策略，实现外部非信任源的受限访问，同时屏蔽内部网络免于外部攻击。注 2：工业自动化和控制系统的上下文中，术语 “内部网络” 典型地应用于主要需点保护的网络或网段。例如，当其连接到 “外部的” 商业网络时，控制网络被指 “内部的” 网络。[来源：GB/T 40211-2021，3.2.41] | 非军事区 | LAN 区段，其用以于 2 个不同区段间，分层存取应用程式 / UI / 档案。 | demilitarized zone、de-militarized zone, DMZ |
| 8 | 广域网 | 用于连接远距离（例如国内或跨国）的计算机、网络和其他设备的通信网络。[来源：GB/T 40211-2021，3.2.136] | 广域网路 | WAN (缩写) ，为比区域网路或都会区网路服务范围更大的地理区域提供通讯服务的网路。 | wide area network, WAN |
| 9 | 局域网 | 在有限的地理区域（通常少于 10 km），用于连接计算机和其他智能设备的通信网络。[来源：GB/T 40211-2021，3.2.69] | 区域网路 | LAN (缩写) ，位于有限地理区域内使用者场所（premise）的电脑网路。区域网路内通讯一般不受外部法规限制，但跨越 LAN 边界的通讯可能受法规约束。 | local area network |
| 10 | 拒绝服务 | 对授权访问系统资源的阻止或者中断，或者系统操作和功能的延缓。注：工业自动化和控制系统的环境中，拒绝服务是指过程功能的损失，而不仅仅是数据通信的损失。[来源：GB/T 40211-2021，3.2.42] | 阻绝服务 | 阻止授权存取系统资源或延迟时间敏感运作及功能。阻止授权存取资源或延迟时间敏感运作。(时间敏感依所提供服务而定，可为毫秒或小时。) | denial of service, DoS |
| 11 | 控制网络 | 用于连接控制物理过程设备的实时网络（见 3.2.97）。注：控制网络可划分为若干区域，并且在一个公司或者场所内可以有多个独立的控制网络。[来源：GB/T 40211-2021，3.2.31] | 控制网络 | 通常连接控制实体过程且是时间或安全至关重要之设备的企业网络。控制网络能细分为区域，且可在企业及场域中，有多个单独的控制网络。 | control network |
| 12 | 宽带 | 通信信道的带宽。宽带通信信道具有的带宽远远超过话音的业务。在模拟通信中，通常使用频分复用技术将多个用户业务融合到一条电缆中传输，并不会在各个用户业务之间造成干扰，如商业无线电系统。在数据通信系统中，多个低速用户线路汇合到一起，形成一条高速数据线路，从而实现宽带传输。[来源：GB/T 32402-2015，3.1.53] | 宽频 | 用于要求大范围频率之应用的频带。备考:宽频能分割为数个窄频，各窄频能用于不同用途，或为不同使用者可用。 | broad band/broadband |
| 13 | 流控制 | 为确保在系统内信息传递不会从一个安全层向另一安全层，且特别不会从高层向低层进行的过程或技术。[来源:GB/Z 25320.2-2013,2.2.99] | 流量控制 | 资料通讯中，实际转送率（transfer rate）之控制。 | flow control |
| 14 | 网关 | 连接功能相近但实现不同的两个（或多个）计算机网络的中继装置，且该装置能够使一个网络的主机与另一网络的主机进行通信。注：也被描述为两个计算机网络转换接口上的中间系统。[来源：GB/T 40211-2021，3.2.53] | 网关 | 中继机制，其附接至具类似功能惟不同实作之 2 (或多)个计算机网络，且使一网络上之主计算机能与另一网络上之主机通讯；作为 2 个计算机网络间接口之中间系统。 | gateway |
| 15 | 网络 | 用各种软件和硬件将各种计算机连接起来，使这些计算机能在互联系统中进行高速的电子通信。在网络环境中，允许计算机用户共享信息，访问一些不是直接连接在本地计算机上的设备，如打印机和文件服务器。网络还为同一组织内的计算机用户提供资源共享。[来源：GB/T 32402-2015，3.1.215] | 网络 | 未明确完整解释，结合前文推测是用各种软件和硬件将各种计算机连接起来，实现电子通信、资源共享等功能的系统 。 | network |
| 16 | 无线局域网 | 使用无线电频率的网络。使用中的最常用标准是IF EF 802. llb和IEEF 802. IIg，应用2.4 GHz频带具有54 Mbit/s传输率、各自最高II Mbit/s带宽。[来源:GB/Z 25320.2-2013,2.2.222] | 无线 LAN | 使用无线射频之网络。最常用之标准为 IEEE 802.11b及 IEEE 802.11g，其使用 2.4 GHz 频带，分别具有高达11Mbps及54Mbps传输速率。 | wireless LAN, WLAN |
| 17 | 虚拟专网 (VPN) | 一个受限使用的逻辑（即人为的或模仿的）计算机网络；用相对公开的物理（即真实的）网络（例如因特网）的系统资源，通常通过使用加密（位于主机或网关处）和经常通过虚拟网的隧道链路穿越真实网，构造VPN。由物理网络的系统资源构造的受限使用的逻辑计算机网络,即在真实网络上使用加密和/或虚拟网的隧道链路穿越真实网。虚拟专用网络是一个建立在开放系统互连(OSI)模型应用层的逻辑网络，该网络建立在已存在的物理网络之上然而通常并不包括该物理网络现有的每一个节点。[来源:GB/Z 25320.2-2013,2.2.214] | 虚拟私用网络 | 有限制使用之逻辑(亦即人造或仿真)计算机网络，其系建构自相对公开之实体(亦即，真实)网络(诸如因特网)，通常使用加密(位于主机或网关)，且常使用虚拟网络之穿隧链路穿越真实网络。有限制使用之逻辑计算机网络，其系建构自实体网络之系统资源，例：使用加密及/或使用虚拟网络之穿隧链路穿越真实网络。虚拟专用网络系建立于开放系统互连(OSI)模型应用层之逻辑网络，其经由既有实体网络，但通常不包括出现于实体网络上之所有节点。 | virtual private network, VPN |

* + 1. 协议体系

两岸协议体系术语对照见表A.5。

* 1. 海峡两岸协议体系术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | Diffie-Hellman密钥交换 | 密码协议，使得先前彼此毫不认识的双方能够通过不安全的通信信道共同确定共享的秘密密钥。[来源:GB/Z 25320.2-2013,2.2.85] | Diffie-Hellman密钥交换 | 允许事前彼此不认识之双方，于不安全信道上联合建立分享秘密密钥之密码协议。 | Diffie-Hellman key exchang |
| 2 | IP层安全构架 | IPsec的体系结构和整套协议的集合名。实现IPsec协议，对于IPv4是可选的而对于IPv6是强制的。[来源:GB/Z 25320.2-2013,2.2.115] | 因特网安全协定 |  | Internet protocol security, IPsec |
| 3 | PGP加密软件 | 公开可用的基于公钥密码技术的加密软件程序。[来源:GB/Z 25320.2-2013,2.2.149] | 妥善隐私 | 基于公钥密码学之公开可用加密软件程序。讯息格式规定于 RFC 1991及RFC 2440。 | pretty good privacy, PGP |
| 4 | RSA 密码算法 | 基于因数分解问题的公钥密码系统。RSA来自RSA公钥密码系统的开发者Rivest、Shamir和Adleman。[在Rivest、Shamir及 Adleman的著作中定义][来源:GB/Z 25320.2-2013,2.2.164] | RSA公钥密码系统 | 以分解因子问题为基础之公钥密码系统。RSA 代表 RSA公钥密码系统之发展者 Rivest、Shamir及 Adleman。 | Rivest, Shamir and Adleman, RSA |
| 5 | S/MIME协议/安全/多用途因特网邮件扩展协议 | 安全/多用途因特网邮件扩展协议 Secure/Multipurpose Internet Mail Extensions; S/MIME提供发送和接收安全MIME数据的一致方法。基于通用因特网MIME标准，S/MIME为电子消息化应用提供以下密码的安全服务：认证、原件的消息完整性和不可抵赖性（使用数字签名）以及保密和数据安全（使用加密）。[来源:GB/Z 25320.2-2013,2.2.172] | 安全/多用途因特网邮件延伸 | 提供一致性方法以发送及接收安全 MIME 数据之方法。依普及之因特网MIME标准，S/MIME提供下列电子传讯应用之密码安全服务：鉴别、讯息完整性及来源不可否认性(使用数字签名)，以及隐私及数据安全性(使用加密)。 | secure/multipurpose Internet mail extensions,S/MIME |
| 6 | SHA算法 | 安全哈希算法。[来源:GB/Z 25320.2-2013,2.2.169] | 安全哈希算法 | 安全哈希算法。 | secure hash algorithm, SHA |
| 7 | SSL协议/安全套接层协议 | 1.一个因特网协议（起初由Netscape通信公司开发）。该协议使用面向连接的端对端加密，为客户（通常是web浏览器）和服务器之间通信流，提供了数据机密性服务和数据完整性服务并且能够可选地提供客户和服务器之间的对等实体认证。是由Netscape为通过因特网传输私有文件而开发的协议。SSL是使用公钥对在该SSL连接上传输的数据进行加密。大多数web浏览器都支持SSL，因而许多web站点使用该协议去获得机密的用户信息，比如信用卡号。按约定，要求SSL连接的URL“https:”而不是“http:”开头。TLS是基于SSL3.0版本的因特网标准。在SSL和TLS之间只存在非常微小的差别。[来源:GB/Z 25320.2-2013,2.2.171] | 安全接套层 | 因特网协议(原由 Netscape 通讯公司开发)，其使用连接导向式端对端加密，以提供客户端(通常为网页浏览器)与服务器间讯务之数据机密性服务及数据完整性服务，其能于客户端与服务器间选项提供同层个体鉴别。安全接套层系由 Netscape 公司所开发经由因特网传输私用文件之协议。SSL 之运作经由使用公钥加密数据，其被经由 SSL 连接转送。多数网页浏览器支持 SSL，许多网站使用此协议以获得机密之用户信息，诸如信用卡号码。依常规，要求 SSL 连接之 URL 以“https:”而非“http:”开始。TLS 系依 SSL 版本 3.0 之因特网标准。SSL与 TLS 间仅些微差异。 | secure socket layer, SSL |
| 8 | X.509建议 | X.509是一个国际通信联盟ITU-T建议。X.509定义了提供和支持数据源认证服务和对等实体认证服务的框架，包括X.509公钥证书、X.509属性证书和X.509证书撤销列表(CRL)的格式。[来源:GB/Z 25320.2-2013,2.2.224] | X.509 | ITU-T 标准[X.509]定义框架以提供及支持数据源鉴别及同层个体鉴别服务，包括 X.509公钥凭证、X.509属性凭证及X.509 CRL等之格式。 | X.509 |
| 9 | 不可否认性/不可抵赖性 | 证实动作或事件已经发生的能力，因此事后这事件或动作就不可能被否认。防止对通信中所涉及情况进行错误否认而提供保护的安全服务。[来源:GB/Z 25320.2-2013,2.2.136] | 不可否认性 | 证明已发生之动作或事件的能力，以致无法于事后否认此事件或动作。提供，以防参与通讯之不诚实否认的安全服务。 | non-repudiation |
| 10 | 不可伪造的 | 密码数据结构（即规定使用一个或多个密码函数的数据结构）的特性，使得只要多个密钥中一个密钥不知道，以计算机方式构造（即计算）出该结构的一个虽毫无根据但正确的值是不可行的。[来源:GB/Z 25320.2-2013,2.2.212] | 不可变造 | 密码式数据结构(亦即，使用1或多个密码函数定义之数据结构)之性质，使得于不知道 1或多个密钥时，建构(即计算)结构之未经授权但正确的值，于计算上不可行。 | unforgeable |
| 11 | 传输层安全协议 | 基于而且非常类似于SSL 3.0版本的因特网协议。[来源:GB/Z 25320.2-2013,2.2.206] | 传送层安全 | 依据且极类似 SSL3.0版 SSL之因特网协议 | transport level security, TLS |
| 12 | 抵赖 | 参与通信的某一实体拒绝承认参与了全部通信或部分通信。[来源：GB/T 40211-2021，3.2.85] | 否认 | 涉及关联(尤其是转送信息之关联)之系统个体否认其已参与关系。 | repudiation |
| 13 | 对称密码学/秘密密钥加密 | 密码学的一个分支。包括对算法的两个不同阶段（例如加密和解密或签名创建和签名验证）都使用相同密钥的算法。加密变换和解密变换都使用相同秘密密钥的密码技术。[来源:GB/Z 25320.2-2013,2.2.196] | 对称式密码学/秘密密钥加密 | 密码学之分支，所涉及算法就 2个不同步骤(诸如加密及解密或签章建立及签章验证)使用相同密钥。就加密及解密2种转换使用相同秘密密钥之密码学技术。 | symmetric cryptography |
| 14 | 对称密钥 | 在对称密码算法中使用的密钥。[来源:GB/Z 25320.2-2013,2.2.197] | 对称式金钥 | 密码金钥，用以执行密码运算及其逆运算(例:加密及解密)，或用以建立讯息鉴别码及查证该码。 | symmetric key |
| 15 | 访问授权机构 | 负责对其他授权实体的访问权限进行监视和授予的实体。[来源:GB/Z 25320.2-2013,2.2.3] | 存取权责机构 | 负责监视及赋予其他被授权个体存取特权之个体。 | access authority |
| 16 | 非对称密码 | 基于非对称密码技术的密钥加解密，密钥的公开变换用于加密而密钥的私有变换用于解密。[来源:GB/Z 25320.2-2013,2.2.13] | 非对称式加密 | 基于非对称式密码技术之加密法，其公开式转换用于加密，而其私密式转换则用于解密。 | asymmetric cipher |
| 17 | 非对称密码学 | 一种现代密码学分支（一般以“公钥密码学”为人所知），算法使用一密钥对（公钥和私钥）而且为算法的不同步骤使用该密钥对的不同组成成分。[来源:GB/Z 25320.2-2013,2.2.14] | 非对称式密码学 | 现代密码学之分支(众所周知之“公钥密码学”)，其算法引用1对密钥(公钥及私钥)，以及就算法之不同步骤使用该配对密钥对之不同组件。 | asymmetric cryptography |
| 18 | 非对称密钥对 | 一对相关的密钥，其中私有密规定私有变换，公开密钥规定公开变换。[来源:GB/Z 25320.2-2013,2.2.15] | 非对称式配对密钥 | 1对相关密钥，其私钥定义私密式转换，而其公钥则定义公开式转换。 | asymmetric key pair |
| 19 | 分组加密 | 对明文分组（即规定长度的位串）进行运算而产生密文分组，具有这样一种特性的对称加密算法。[来源:GB/Z 25320.2-2013,2.2.30] | 区块加密法 | 对称式加密算法所具之性质，其加密算法于明文区块(亦即已定义长度之位串)上运作，以产生密文区块。 | block cipher |
| 20 | 高级加密标准/先进加密标准 | 一种对称加密机制，提供可变密钥长度并使得能高效实现。规定了能够用于防护电子数据的美国政府批准的密码算法。AES算法是对称分组密码，能够加密（加密器）和解密（解密器）信息。该标准规定Rijndael算法，使用128、192和256位长度密钥，能处理128位数据分组的对称分组密码。[来源:GB/Z 25320.2-2013,2.2.8] | 进阶加密标准 | 提供可变密钥长度且遵循高效率实作规范之对称式加密机制。进阶加密标准规定美国政府核可之密码算法，其能用以保护电子数据。AES算法为对称式区块加密法，其能对信息加密（加密器）及解密（解密器）。此标准规定之Rijndael算法为对称式区块加密法，其能对128位之数据区块，使用加密密钥长度可以为128位、192位及256位。 | Advanced Encryption Standard；AES |
| 21 | 更新密钥 | 每一财密钥对都需要定期更新（即用新密钥对来代替），因而需要颁发新证书。当密钥对是由于到期而过期，相关的端实体可以请求密钥更新，即端实体可以请求CA(证书机构)为新密钥对颁发新证书。使用密钥更新请求(KUR)消息作出此请求。[来源:GB/Z 25320.2-2013,2.2.213] | 更新密钥 | 每组密钥对需定期更新(亦即，以新密钥对取代之)，且需签发新凭证。当 1组密钥对到期时，相关终端个体〝可〞请求密钥更新，亦即，其〝可〞请求CA签发新密钥对用之新凭证。此请求系使用密钥更新请求(KUR)讯息。备考：对称式更新密钥可能不涉及新凭证，而只是新密钥。 | update key |
| 22 | 公钥 | 用于非对称密码技术的一对密钥，其能向公众暴露的部分。实体非对称密码对的那个能够被公开的密钥。非对称密码对的公开部分，通常用于检验签名或加密数据。与一个实体唯一相关的且可使之公开的，公钥密码算法使用的密钥。在非对称（公钥）密码系统中，公钥是与私钥相关的。任何人都可知道公钥，因而决定于算法，公钥可用作：（1）验证数字签名，该签名是用相应的私钥所签；（2）加密数据，该加密数据能用相应的私租解密；（3）计算共享的数据块。[来源:GB/Z 25320.2-2013,2.2.154] | 公钥 | 非对称式密码学所使用密码式密钥对之可公开揭露组件。个体之非对称式密钥对中能公开者。非对称式密钥对之公开部分，通常用以查证签章或加密数据。与公钥密码式算法一起使用之密码式密钥。公钥系唯一地与个体关联，并可被公开。于非对称式(公开)密码系统中，公钥与私钥相关联。公钥可被所有人知道，且取决于算法，可用于下列用途：(1)查证以对应私钥签署之数字签名。(2)加密数据，其能以对应私钥解密。(3)计算共享数据之片段。 | public key |
| 23 | 公钥非对称密码算法 | 便用两个相关密钥（公钥和私钥）的密码算法。两个密钥都具有一个特性，即以计算方法从公钥推导出私钥是不可行的。[来源:GB/Z 25320.2-2013,2.2.155] | 公钥非对称密码式算法 | 密码式算法，其使用2个相关密钥(公钥及私钥)。2个密钥具有由公钥推衍出私钥为计算上不可行之性质。 | public key asymmetric cryptographicalgorithm |
| 24 | 公钥基础设施 | 证书机构(CA)的系统，或者包括证书机构(CA)、（可选）注册机构(RA)以及其他支持服务机构和代理机构的系统。为应用非对称密码技术的用户团体，该系统执行证书管理、档案管理、密钥管理和令牌管理功能的某种组合。[来源:GB/Z 25320.2-2013,2.2.158] | 公钥基础建设 | CA之系统(及选项之 RA及其他支持服务器及代理器)，其履行非对称密码学应用之用户社群所使用之某组凭证管理、存盘管理、密钥管理及符记管理功能。备考：凭证亦可由其他受信赖群组所管理，诸如 PGP 信赖网。 | public key infrastructure, PKI |
| 25 | 公钥密码学 | 一种密码技术类型，加密过程是公开可用且不被保护的，但解密密钥的一部分是被保护的，这样仅仅对解密过程的两部分都了解的一方才能够解密密文。用双密钥对的加密系统。一对密钥用于加密，其他一对密钥用于解密。[来源:GB/Z 25320.2-2013,2.2.157] | 公钥密码学 | 一种型式之密码学，其中加密过程系公开可取得且未受保护，但其中解密密钥部分系受保护，故仅有知悉双方解密过程者能解密密文。 备考：于专业密码学界，通常称为非秘密加密。FIREFLY 系公钥密码学之应用。加密系统使用相链结之密钥对。一对密钥之加密，以另一对解密。 | Public key cryptography |
| 26 | 公钥证书 | 唯一标识实体、包含实体的公钥并且是经可信方数字签名，从而绑定公钥于该实体的一组数据。[来源:GB/Z 25320.2-2013,2.2.156] | 公开金钥凭证 | 个体之公开金钥连同某些其他资讯，借由以核发该凭证的CA之私密金钥进行数位签章变得不可伪造。备考:公开金钥凭证通常称为X.509凭证或数位凭证。然而，此等用语并不明确因其可能亦指由ISO/IEC9594-8:2020|Rec.ITU-TX.509(2019所定义之属性凭证。 | public key certificate |
| 27 | 哈希函数 | 一种算法，基于一个数据对象（比如消息或文件，通常可变长度，可能非常大）计算出一个值，因此把该数据对象映射为一个通常是固定长度数值的较小数据对象（“哈希结果”）。映射位串为固定长度位串的函数，满足以下两个性质：（1）给定输出，用计算方式求得映像为这输出的输入是不可行的。（2）给定输入，用计算方式求得映像为相同输出的第二个输入是不可行的。[来源:GB/Z 25320.2-2013,2.2.104] | 杂凑函数 | 将任意长度之资料对映至称为摘要(digest)的固定长度资料之(数学)函数。 | hash function |
| 28 | 会话密钥 | 在对称加密过程中，会话密钥是临时的或在相对短的时间段中使用的密钥。[来源:GB/Z 25320.2-2013,2.2.183] | 会期金钥 | 于对称加密全景中，暂时或使用期间相对短之密钥。 | session key |
| 29 | 机密性/保密性 | 保证信息不被泄露给未授权的个人、过程或者设备。[来源：GB/T 40211-2021，3.2.28] | 机密性 | 信息存取及揭露之保留授权限制，包括保护个人隐私及专属信息之手段。属保密或敏感数据，系指数据未遭破解/违反之程度；亦即，不对未经授权之个人、过程或其他个体成为可用或揭露。保证信息未揭露予未经授权之个人、过程或装置。个体或团体之相关信息不对未经授权之个人、个体或过程成为可用或揭露的性质。信息不对未经授权之个人、个体或过程成为可用或揭露的性质。 | confidentiality |
| 30 | 基本编码规则 | ISO 制定的对数据元素进行编码的 OSI 规则和网络转移语法。它在 ISO 8825 中说明。[来源：GB/T 32402-2015，3.1.43] | 基本编码规则 | 数种 ASN.1 编码规则方法中之一种。 | basic encoding rules;BER |
| 31 | 加密（动词） | 包括加密和编码的通用术语。通过密码系统将明文变换为难以理解的形式。[来源:GB/Z 25320.2-2013,2.2.95] | 加密（动词） | 包括加密及编码之通用用语。藉由密码系统将明文转换为无法理解之形式。备考：用语加密涵盖加密及编码之意。 | encrypt |
| 32 | 加密（名词） | 明文转换成密文的密码变换，隐藏了数据的原始意义以阻止该数据被知道或者使用（见 3.2.39）。注：如果进行反向转换，相反的逆向过程被称为 “解密”，解密是将储存的加密数据转换成它的原始状态。[来源：GB/T 40211-2021，3.2.47] | 加密（名词） | 藉由密码算法(可逆)转换数据以产生密文，亦即，隐藏数据之信息内容。数据(称为“明文”)加密转换 为隐藏数据原始意义之另一形式(称为“密文”)，以防止被知悉或使用。若为可逆转换，则对应之反转过程称为“解密”，其为回复加密数据至其原始状态之转换。 | encryption |
| 33 | 简单网络管理协议 | 网络管理中使用的一个标准协议，它最初是为美国国防部的网络而设计的。后来广泛地用于支持各类网络产品和功能管理。它工作在 UDP 上，用于监视和管理主机、路由器及各种智能网络设备，它也是网络上的设备收集管理信息的公用通信协议。[来源：GB/T 32402-2015，3.1.266] | 简易网络管理协议 | 基于UDP之应用层因特网标准协议，用以载送管理者与代理者间之管理信息。网络管理之标准 TCP/IP 协议。网络管理者使用 SNMP 监视并对映网络可用性、效能及错误率。为与 SNMP 运作，网络装置使用分布式数据储存，称为管理信息库(MIB)。所有遵循SNMP 之装置皆包含MIB，其提供装置之特定属性。某些属性于MIB 中为固定或“硬编码”，其他属性则为运行于装置上之代理者软件所计算之动态值。 | simple network management protocol;SNMP |
| 34 | 解密（动词） | 包括解码和解密的通用术语。通过密码系统把加密文本变换为其相当的明文。（这并不包括用密码分析方案）。[来源:GB/Z 25320.2-2013,2.2.78] | 解密（动词） | 包含解碼及解密法之通用用语。藉由密码系统，转换加密文字成为等同明文。(此不包括密码分析法之解决方案。)备考： 用语“解密”涵盖“解密法”及“解碼”之意。 | Decrypt |
| 35 | 解密（名词） | 使用密码算法和密钥，把密文转换成明文的过程（见 3.2.47）。[来源：GB/T 40211-2021，3.2.39] | 解密（名词） | 对应于加密之反转。使用密码式算法及密钥，变更密文为明文之过程。 | decryption |
| 36 | 开放系统 | 具有以下特性的系统：系统遵循明确规定、公开维护且迅速可用的各种标准，并因而系统能够连接到遵循同样这些标准的其他系统。[来源:GB/Z 25320.2-2013,2.2.139] | 开放系统 | 其堆栈若非标准化即是公开可用之协议。 | open system |
| 37 | 开放系统互联的参考模型 | 开放系统互联信息技术一基本参考模型一规定OSI服务的约定，第1层～第7层。[来源:GB/Z 25320.2-2013,2.2.141] | 开放系统互连参考模型 | 通讯或分布式数据处理系统之分层式层阶结构、组态或模型。(1) 使系统描述、设计、开发、装设、运作、改进及维护于阶层式结构中之给定 1 或多层履行。(2) 允许各层提供 1 组存取功能，该层可由其上层中之功能控制及使用。(3) 使被实作之各层不致影响其他层之实作。(4) 允许藉 1 或多层之修改，于不改变其余各层之既有设备、程序及协议，已变更系统效能。备考 1. 独立变更之范例包括下列各项：(1) 物理层由缆线转换为光纤，除提供更多讯务容量外，不影响数据链路层或网络层。(2) 变更网络层级之运作协议，但不变更物理层。备考 2. 开放系统架构，当设计系统以符合效能要求时，可使用开放系统互连参考模型(OSI-RM)作为实作指导纲要。非专属之系统架构。信息技术－开放系统互连－基本参考模型－OSI服务(1-7层)定义规约。 | open system interconnection-reference model,OSI-RM |
| 38 | 开放系统体系结构 | 通信或分布数据处理系统的分层的层次结构、配置或模型。该体系结构：（1）使得系统的描述、设计、开发、安装、运行、改进和维护能在层次结构中指定的层或指定的几层上实行；（2）使得每一层都能提供一组可访问功能，该层的上一层中功能能够控制和使用这组功能；（3）使得每一层能实现而并不影响其他层的实现；（4）使得对一层或几层进行修改就能改变系统性能而并不要改变其余层的已有设备、过程和协议。非专用的系统体系结构。[来源:GB/Z 25320.2-2013,2.2.140] | 开放系统架构 | 具有符合已规定、公开维护、备妥可用标准等特性之系统，并因此能连接至符合此等标准之其他系统。 | open system architecture |
| 39 | 开放协议 | 协议栈是标准化的或是公众可用的协议。[来源:GB/Z 25320.2-2013,2.2.138] | 开放协议 | 事物之官方全球唯一名称，以(依 ASN.1标准定义形成及指派)整数序列书写，用于抽象规格中及于协议中之安全服务协商期间用以参引事物。 | open protocol |
| 40 | 可信凭证 | 为确定自称身份或审定系统实体，被传递或表示的数据。[来源:GB/Z 25320.2-2013,2.2.60] | 信符 | 转送或展现以建立所宣称身分或系统个体授权之数据。 | credential |
| 41 | 可信签名 | 能够信赖的签名（特别是数字签名），因为能对该签名进行核查。[来源:GB/Z 25320.2-2013,2.2.21] | 鉴别签章 | 签章(特别是数字签名)因其能被查证，故能被信赖。 | authentic signature |
| 42 | 秘密密钥 | 1.对称密码技术所使用的并且仅由一组特定实体才能使用的密钥。唯一地与一个或多个实体相关且不应使之公开的，秘密密钥密码算法使用的密钥。[来源:GB/Z 25320.2-2013,2.2.166] | 秘密密钥 | 与对称式密码技术一起使用之密钥，且仅有一组所规定之个体可用。与秘密密钥密码算法一起使用之密码密钥，其与 1 或多个个体唯一地关联，且不宜公开。 | secret key |
| 43 | 密码 | 1.用于保护数据机密性的密码技术，并且它由三部分处理组成：加密算法，解密算法和生成密钥方法。任何一个密码系统，在该密码系统中根据某些预定规则，硬性确定的符号或符号组表达规则长度的单位明文（通常为单个字母），或重新排列单位明文，或者两种方法一起使用。[来源:GB/Z 25320.2-2013,2.2.45] | 加密法 | 用以保护数据机密性之密码技术，由加密算法、解密算法及密钥产生方法等3个组件过程所组成。加密法为任何密码系统，其依据某些预定规则，以任意符号或号群组表示规律长度之明文单元，通常为单一字母组或其明文单元经重新安排，或两者。 | cipher |
| 44 | 密码哈希 | 把任意长度的8位位串映射为固定长度的8位位串的函数，以致于用计算方式求得输入和输出之间的相关性是不可行的，而且如给定输出的一部分而不给输入，用计算方式推测任何一点剩余输出也是不可行的。精确的安全防护要求取决于应用。哈希函数是从大值域（甚至非常大值域）的数值映射入较小数值范围的数学函数，并且哈希函数是单向（即要以计算方式去求得映像为预先指定输出的输入是不可行的）而且无冲突（即要以计算方式去求得映像为相同输出的任何两个不同输入是不可行的。[来源:GB/Z 25320.2-2013,2.2.63] | 密码式哈希 | 将任何长度之 8 字节串映像至固定长度 8字节串之函式，使得找出输入与输出间之相互关系于计算上不可行，且使得给予一部分输出，而非输入，预测剩余输出之任何位于计算上亦不可行。精确安全要求事项取决于应用。从大(甚或非常大)定义域中之值映射至较小值域之数学函式具有下列特性。(1) 找到单向映射至预先规定输出值之任何输入，于计算上不可行。(2) 找到无碰撞映射至相同输出 值之任何2个不同输入值，于计算上不可行。 | cryptographic hash |
| 45 | 密码技术 | 关注于把明晰的信息表示为难以理解的信息和把加密信息恢复为可理解形式信息的原理、手段和方法的科学或技术。密码学的分支，涉及设计和使用密码系统的原理、手段和方法。为了隐藏信息内容、防止信息未经检测的修改和/或防止信息未经授权的使用，包含数据变换的原理、手段和方法的学科。[来源:GB/Z 25320.2-2013,2.2.65] | 密码学 | 关于将明文信息以无法理解之形式呈现，以及将加密信息回复为可理解形式之原理、手段及方法的艺术或科学。论及设计及使用密码系统之原理、手段及方法的密码学分支。为隐藏信息内容，以避免其遭受未察觉之修改及/或避免其遭受未经授权使用，包含将数据转换之原理、手段及方法的学科。 | cryptography |
| 46 | 密码算法 | 基于密码科学的算法，包括加密算法、加密哈希算法、数字签名算法和密钥协商算法。[来源：GB/T 40211-2021，3.2.34] | 密码算法 | 完善定义之程序、一连串的规则或步骤，或是一系列数学方程式，用以描述诸如加密/解密、密钥产生、鉴别、签章等密码过程。 | crypto-algorithm |
| 47 | 密文 | 通过加密后传输的数据，这样其语义信息内容（它的含义）不再是可理解的或者直接能用的。[来源：GB/T 40211-2021，3.2.21] | 密文 | 已转换以隐藏其信息内容之数据。 | ciphertext |
| 48 | 密钥 | 通过加密算法执行变换的输入参数。[来源：GB/T 40211-2021，3.2.35] | 密钥/密码式密钥 | 用以控制密码运作，诸如解密、加密、签章产生或签章查证之数值。 | cryptographic key/key |
| 49 | 密钥对 | 两个数学上相关的密钥，具有以下特性：能够使用一个密钥对报文加密而仅能够使用另一密钥解密该报文，而且即使已知一个密钥，以计算方式发现另一个密钥也是不可行的。公钥算法使用的公开密钥（公钥）和它的相应私有密钥（私钥）。[来源:GB/Z 25320.2-2013,2.2.122] | 配对密钥 | 2个数学上相关之密钥，具性质：(1)使用一密钥加密之讯息，仅能使用另一密钥解密，以及(2)即使知道一密钥，探索另一密钥于计算上为不可行。与公钥算法一起使用之公钥及其对应私钥。 | key pair |
| 50 | 密钥对称密码算法/对称密钥算法 | 加密和解密都使用单一秘密密钥的密码算法。[来源:GB/Z 25320.2-2013,2.2.168] | 秘密密钥对称式密码算法/对称式密钥算法 | 使用单一秘密密钥供加密及解密两者使用之密码算法。 | secret key symmetric cryptographic lgorithm/symmetric key algorithm |
| 51 | 密钥分发 | 从拥有密钥或生成密钥的实体尚想要使用该密钥的另一个实体，传送密钥和其他密钥载体。[来源:GB/Z 25320.2-2013,2.2.120] | 密钥派送 | 由拥有密钥或产生密钥之个体，传送密钥及其他建钥材料至另一预期使用密钥之个体。 | key distribution |
| 52 | 密钥更新 | 从已有密钥导出新密钥。[来源:GB/Z 25320.2-2013,2.2.123] | 密钥更新 | 由既存密钥推导出新密钥。 | key update |
| 53 | 明文 | 没加密的信息。[来源:GB/Z 25320.2-2013,2.2.47] | 明文 | 未加密之信息。 | cleartext；plaintext |
| 54 | 签名证书 | 包含一个公开密钥的公钥证书。该公钥将用于验证数字签名，而并不是用于加密数据或执行其他密码功能。[来源:GB/Z 25320.2-2013,2.2.185] | 签名证书 | 公钥凭证，包含预期用于查证数字签名，而非用于加密数据或履行其他密码学功能之公钥。 | signature certificate |
| 55 | 强秘密值 | 具有足够大熵阶的秘密值，这样的熵阶导致穷举搜索该秘密值是不可行的，即使给出使得秘密值的正确推测能与不正确推测区分的知识。[来源:GB/Z 25320.2-2013,2.2.194] | 强秘密 | 具足够级数熵值之秘密，即使针对该秘密所给定之知识使其能区分正确与不正确的猜测，实施穷举搜寻该秘密仍是不可行。备考：例：此知识或许可由具备均匀机率分布之足够大集合的可能值中随机选择秘密达成之。 | strong secret |
| 56 | 确认 [消息] | 一种消息类型，说明一个数据块无错的到达它的目的地。[来源：GB/T 32402-2015，3.1.18] | 确认 | 接收者对发送者以指示传输之资料已收受之肯定反应。 | acknowledgment;ACK |
| 57 | 三重DES/三次DES | 基于DES(数据加密标准)的分组密码，三重DFS算法使用有效密钥长度为112位或l68位的两个或三个不同密钥，采用数据加密算法连续三次对每64位的明文组进行变换。[来源:GB/Z 25320.2-2013,2.2.208] | 三重数据加密标准 | 依 DES之区块加密法，使用 2或 3个不同密钥，藉由连续 3次应用数据加密算法，转换各64位原文区块，有效密钥长度为 112位或 168位。 | triple DES |
| 58 | 数据加密标准 | IBM 开发的加密系统。1976 年由美国国家标准学会建议用作政府和公共数据的加密标准，它是 SNMPv2 安全性的一部分。它利用一种数据加密算法，将数据加密后，形成一个长 64 bit 的数据块。[来源：GB/T 32402-2015，3.1.77] | 数据加密标准 | 保护未保密之计算机数据的密码式算法。备考：DES 未被核准用于保护国家安全机密信息。使用 56 位密钥之习知对称式加密机制。由于短密钥长度，DES 已被 AES取代，但仍用于多重加密模式，例如3DES或三重DES(FIPS 46-3)。 | data encryption standard, DES |
| 59 | 数据鉴别 | 确认数据真实性。鉴别技术通常形成所有形式对系统或数据的访问控制的基础。[来源:GB/Z 25320.2-2013,2.2.70] | 资料鉴别 | 资料鉴别性之查证。鉴别技术通常构成对系统或数据所有访问控制形式之基础。 | data authentication |
| 60 | 数据完整性 | 数据在未授权或者意外情况下，不被修改，破坏，或者丢失的属性。注：该术语描述的是数据值的持续性和保密性，不涉及数据值代表的信息或者值的来源的可靠性。[来源：GB/T 40211-2021，3.2.38] | 数据完整性 | 数据未遭未经授权或意外之方式变更、破坏或遗失之性质。当数据未从其来源变更，且未经意外或恶意修改、改变或破坏，其所存在之状况。任何运作(诸如转送、储存及检索)期间，数据维持相同之状况。 | data integrity |
| 61 | 数字签名 | 数据密码变换的结果，正确完成时，提供数据源认证，数据完整性和签名者非抵赖服务。[来源：GB/T 40211-2021，3.2.43] | 数位签章 | 资料之密码式转换结果，当正确实作时，提供用以查证来源鉴别性、资料完整性，以及签署者(signatory)不可否认性的机制。 | digital signature |
| 62 | 数字签名标准 | 包括数字签名算法的遂行数字签名的标准。由NIST批准，由美国商务部1994年5月发布“数字签名标准”发布。[来源:GB/Z 25320.2-2013,2.2.89] | 数字签名标准 | 包括数字签名算法之数字式签署的标准，系由美国国家标准及技术研究院核准，于 1994年由美国商务部发布。 | digital signature standard, DSS |
| 63 | 数字证书 | 数字数据对象（由计算机使用的数据对象）形式的证书文件，根据这数据对象计算所得数字签名值被附加于该数据对象。[来源:GB/Z 25320.2-2013,2.2.86] | 数字证书 | 数字数据对象(计算机使用之数据对象)形式之凭证文件，该数据对象中附加依该数据对象而计算之数字签名值。 | digital certificate |
| 64 | 私钥 | 1.用于非对称密码技术的一对密钥，其秘密部分。实体非对称密码对的那个仅应该由该实体使用的密钥。非对称密码对的秘密部分，通常用于数字签名或解密数据。与一个实体唯一相关的而且不使之公开的，公钥密码算法使用的密钥。在非对称（公开）密码系统中，私钥是与公钥相关的。取决于算法，私钥可用于：（1）计算相应的公钥；（2）计算可由相应公钥验证的数字签名；（3）解密由相应公钥加密的数据；（4）与其他信息一起，计算一个公共共享数据。[来源:GB/Z 25320.2-2013,2.2.150] | 私密金钥 | (于公开金钥密码系统中)仅由该个体知悉之个体金钥对中的金钥。 | private key |
| 65 | 椭圆曲线密码技术 | 一种基于定义予曲线上点的群数学的非对称密码技术类型。[来源:GB/Z 25320.2-2013,2.2.94] | 椭圆曲线密码学 | 非对称密码学之型式，系基于由曲线上之多点所定义的群数学。 | elliptic curve/cryptography |
| 66 | 完整性 | 防止不适当的信息修改或毁坏,而且包括确保信息的不可否认性和真实性。敏感数据不被以未经授权和未被检测方式修改或删除的特性。敏感数据不被以未经授权和未被检测方式修改或删除的特性。[来源:GB/Z 25320.2-2013,2.2.110] | 完整性 | 保护以防止不适当之信息修改或破坏，包括确保信息不可否认性及鉴别性。敏感数据未被以未经授权及未经侦测方式修改或删除之性质。敏感数据未被以未经授权及未经侦测方式修改或删除之性质。 | integrity |
| 67 | 网络层协议 | 用于报文路由通过复杂网络的协议，OSI参考模型第3层（网络层）。[来源:GB/Z 25320.2-2013,2.2.134] | 网络层协议 | 经过复杂网络之讯息选路协议。OSI参考模型之第 3层。 | network layer protocol |
| 68 | 伪随机数发生器 | 产生比特序列的算法，该比特序列唯一由称为种子的初始值所决定。伪随机数发生器(PRNG)的输出“似乎是”随机的，即该输出统计上与随机值是无法区别的。密码的PRNG具有另外特性即假设不知道种子，输出是不可预知的。[来源:GB/Z 25320.2-2013,2.2.153] | 拟随机数产生器 | 产出位序列之算法，序列系由称为种子数之初始值所唯一决定。PRNG之输出为〝似乎〞随机，亦即输出与随机值于统计上无法区别。密码式 PRNG，具有假设未知种子数，无法预测输出之额外性质。 | pseudo random number generator, PRNG |
| 69 | 无线应用协议 | 为蜂窝电话、寻呼机和其他手持装置，提供对E-mail和基予文本的web网页安全访问的标准。[来源:GB/Z 25320.2-2013,2.2.221] | 无线应用协议 | 提供手机、呼叫器及其他手持装置可安全存取电子邮件及文字式网页之标准。 | wireless application protocol, WAP |
| 70 | 物理层协议 | 在通信信道上传输原始电信号的协议。物理层协议涉及传输物理，如布线、调制和传输率。属于OSI参考模型第1层。[来源:GB/Z 25320.2-2013,2.2.145] | 物理层协定 | 经由信道传输原始电子信号之协议。处理传输实体，诸如布缆、调变及传输率。OSI参考模型第 1层。 | physical layer protocol |
| 71 | 校验和 | 在数据处理和数据通信领域中，用于校验目的的一组数据项的和。[来源：GB/T 32402-2015，3.1.60] | 核对和 | 数据项群组之和，该和系用于核对目的以侦测错误或传输期间之调处。 | checksum |
| 72 | 协议，规程 | 两个系统间执行和控制某些关联类型（例如通信）的规则集（例如格式和规程）。[来源：GB/T 40211-2021，3.2.80] | 协定 | 决定用以实现通讯之功能单元之行为的一组规则。 | protocol |
| 73 | 协议数据单元 | 按指定协议组成的信息单元，它包括净荷以及协议所要求的控制信息，一般都包含有信头。PDU 通过现有的协议层之间的协议接口传递。每一层附加到 PDU 中信息，应由另一系统的相同层接收。[来源：GB/T 32402-2015，3.1.241] | 协定资料单元 | 由给定层内之协定机 (个体) 所交换的资料物件，其由协定控制资讯 (protocol control information, PCI) 及使用者资料组成。备考：此系 OSI “封包 (packet)” 之用语。 | protocol data unit, PDU |
| 74 | 循环冗余校验 | 为了保证数据内容能得到正确传送而使用的一种差错检验算法，用来检查传输过程中可能产生的错误。一般来说在数据发送时，由发送端计算出一个 CRC 校验码，并将它加到分组的后面发送出去；在接收端，重新对收到的数据计算出一个 CRC 校验码，并与收到的 CRC 进行比较，以确定收到的分组是否出错。[来源：GB/T 32402-2015，3.1.75] | 循环冗余检验 | 确保数据透过信道发送之后未被改变的方法。 | cyclic redundancy check, CRC |
| 75 | 应用层 | 网络协议栈的最高层，它关心信息（例如：格式化电子邮件消息）的语义。[来源：GB/T 32402-2015，3.1.32] | 应用层 | 参照开放系统互连(OSI)参考模型第7层。 | application layer |
| 76 | 有线等效保密协议 | 提供128位密钥长度的流密码加密的密码协议。该协议在IEEE 802. 11无线局域网规范中定义。无线局域网（WLAN）的安全协议，定义在IEEE 802.11b标准中。WEP试图提供与有线局域网同等的安全。[来源:GB/Z 25320.2-2013,2.2.220] | 有线等效隐私 | 一种密码协议提供，以密钥长度 128位加密之串流加密；其定义于 IEEE802.11无线LAN标准。无线局域网络(WLAN)安全协议，定义于 IEEE 802.11b 标准之WEP 旨在提供与有线 LAN 相同之安全等级。 | wired equivalent privacy, WEP |
| 77 | 证书 | 在密码技术中，证书是公共密钥积实体身份并且带有以发放证书机构的私钥对全信息进行数字签名而造成不可能伪造的其他信息。信息的数字表达，这些信息至少应包括确定发放证书的证书机构，命名或确定证书的签署者，包含签署者的公钥，确定它的有效期以及是已由发放证书的证书机构经过数字签名。[来源:GB/Z 25320.2-2013,2.2.36] | 凭证 | 密码学中，个体之公钥、身分及其他信息，藉由凭证签发机构之私钥数，以数字式签署所有的信息，呈现其未遭假造(无法被假造)。信息之数字化表示，至少做到下列项目:识别签发凭证之凭证机构、命名或识别其签署人(subscriber)、包含签署人之公钥、识别其运作期限及系由签发凭证的凭证机构以数位式签署之。 | certificate |
| 78 | 证书撤销列表 | 已撤销的公钥证书列表，该证书是由证书机构(CA)创建和数字签名。已撤销但未过期的CA发放的证书表。[来源:GB/Z 25320.2-2013,2.2.38] | 凭证注销表列 | 凭证机构(CA)所建立且数字式签署之已注销公钥凭证表列。CA 所签发之已注销但未到期的凭证表列。 | Certificate Revocation List；CRL |
| 79 | 证书管理 | 证书被生成、存储、防护、传递、装载、使用和注销的过程。[来源:GB/Z 25320.2-2013,2.2.37] | 凭证管理 | 制作、储存、保护、传输或寄送、加载、使用及废止或销毁凭证之过程。 | anagement |
| 80 | 证书机构 | 为创建和分配证书，由一个或多个用户所信任的机构。证书机构也可以创建用户密钥，这是可选的。可信的第三方（类似“证券交易机构”），发放数字签名和数字证书。发放数字证书（特别是X.509数字证书）并对证书中数据项间绑定关系进行担保的实体。[来源:GB/Z 25320.2-2013,2.2.40] | 凭证机构 | 1或多个使用者所信赖之机构，其制作并签发凭证。凭证机构可选项地建立用户密钥。签发数字签名及数字证书之受信赖第三方“清算机构”。签发数字证书(特别是X.509凭证)，并担保凭证中数据项间之系结的个体。 | Certification Authority；CA |
| 81 | 指定批准机构 | 以可接受风险级别，为运行一个系统正式承担责任的权威官方机构。[来源:GB/Z 25320.2-2013,2.2.83] | 指定核可机构 | 具授权之官方，正式承担可接受风险等级运作系统之责任。同义词：认证机构、指派认证机构、指定认证机构。 | designated approving authority, DAA |
| 82 | 制造报文规范 | 1.ISO 9506是与OSI通信模型一致的应用层通信规范。对自动化设备和查询或控制通信的系统间通信，它提供一套适合于此通信的服务。它的相互作用描述遵循客户/服务器模型。它适宜于在任何支持全双工可靠通信的网络上使用，比如因特网。对在此类自动化系统中发现的信息对象，ISO 9506－1：2003提供了一套信息对象的抽象模型并且提供了一套运行在这些模型上的抽象服务的规范。ISO 9506-2提供客户和服务器之间交换消息的协议，实现对第1部分中规定的抽象服务的支持。MMS是一个通信协议，映射IEC 61850到MMS。[来源:GB/Z 25320.2-2013,2.2.130] | 制造讯息规格 | ISO 9506系与 OSI通讯模型一致之应用层通讯规格。其提供一组服务，适合于自动设备与系统间诘问或控制之通讯。其互动之描述遵循客户端服务器模型。其适合用于支持全双工且可靠通讯之任何网络，诸如因特网。ISO 9506-1:2003 提供一组可出现于此等自动化系统之信息对象的抽象模型，以及一组于此等模型中运作之抽象服务的规格。ISO 9506-2 提供客户端及服务器间交换讯息之协议，以实现对定义于第1部(ISO 9506-1)中抽象服务的支持。MMS 系 IEC 61850 所对映通讯协议之一。 | manufacturing message specification, MMS |

* + 1. 硬件

两岸硬件术语对照见表A.5。

* 1. 海峡两岸硬件术语对照

| 序号 | 大陆术语 | 大陆释义 | 台湾地区术语 | 台湾地区释义 | 英文词汇 |
| --- | --- | --- | --- | --- | --- |
| 1 | BTW技术/链路端加密装置 | 安全防护中在通信链路的每一端，在与装置或系统的连接后增加的加密盒。一个加密盒从一个装置取得明文报文且对它们进行加密，而另一个盒接收这加密报文且把它们解密回明文，以及反之。这种方法提供外部加密从而避免需要在装置内嵌入加密功能。[来源:GB/Z 25320.2-2013,2.2.34] | 线路中阻碍物 | 安全上，装置/系统连接后，于通讯链路任一端附加保密盒。1 个保密盒从 1 个装置取得明文讯息后，将其加密，而另 1 个保密盒接收该加密讯息后，将其解密回明文，反之亦然。此作法提供外部加密以避免需于装置中嵌入加密功能（习惯用法）。 | Bump-in-the-Wire |
| 2 | 被控站 | 将现场收集数据传送到控制站的远方设备。在一些协议规范中一般称作 “子站” 或 “从站”。[来源：GB/T 21099.5-2024，3.2] | 受控站 | 由主控站所监视或命令及监视之站所。备考：于某些规格中通常称为 “外站” 或 “从属站”。 | controlled station |
| 3 | 边界防护 | 完全在组织的管理和控制之下的信息系统和非完全在组织的管理和控制之下的信息系统之间外部边界处和完全在组织的管理和控制之下的信息系统之间关键内部边界处，为防护和探测恶意的和其他未经授权通信，使用受控接口（例如：代理、网关、路由器、防火墙、加密隧道），对通信进行监视和控制。[来源:GB/Z 25320.2-2013,2.2.31] | 边界保护 | 通讯之监视及控制，于组织完全管理及控制之信息系统与组织不完全管理及控制之信息系统间的外部边界处为之，以及于组织完全管理及控制下之信息系统间的关键内部边界处为之，使用受控制接口(例：代理服务器、网关、路由器、防火墙及加密隧道)，以防止及侦测恶意及其他未经授权之通讯。 | boundary protection |
| 4 | 防火墙 | 两个互连网络间限制数据传输的网际连接设备。注：防火墙可以是安装在通用计算机上的应用软件或者是专有平台（设备），用于转发或者拒绝 / 丢弃网络上的包。典型的防火墙用于定义区域边界。防火墙通过定义规则来限制端口开放。[来源：GB/T 40211-2021，3.2.52] | 防火墙 | 因特网网关，其限制数据通讯讯务进出连接网络之一(称为防火墙“内侧”者)，因而保护网络之系统资源免遭受来自其他网络(称为防火墙“外侧”者)的威胁。备考：防火墙非恒为网关，其可被视为分隔安全领域或多重网络之机制。 | firewall/fire wall |
| 5 | 告警 | 以产生可听或可视断续变化或者两者同时变化，通告异常情况存在的装置或功能，以起对那种情况的注意。[来源:GB/Z 25320.2-2013,2.2.9] | 告警 | 装置或功能，其藉由发出声音或(同时)闪烁改变可见光之方式对存在之异常状况发出讯号，以吸引注意该情况。 | alarm |
| 6 | 节点 | 网络上功能单元的连接点，它通常指网络用于数据传输的物理设备。例如，在互联网络环境中的一台计算机终端、客户机、工作站、服务器、打印机或其他的连网设备，都能提供网上数据传输服务。[来源：GB/T 32402-2015，3.1.223] | 节点 | 在数据网络中，一个以上之功能单元将通道或数据电路相互连接之一点。 | node |
| 7 | 客户端 | 接收或请求来自服务器端的服务或信息的设备或应用。[来源：GB/T 40211-2021，3.2.22] | 客户端/用户端 | 启动与伺服器建立关联关系之应用个体。备考 1. 此用语规定特定关联关系之个体的角色。该个体对另一关联关系，可具另一角色。备考 2. XMPP 具稍微不同之客户端 / 伺服器概念。 | client |
| 8 | 控制站 | 启动大部分通信和发布命令的设备或应用。在一些协议规范中一般称作 “主站”。[来源：GB/T 21099.5-2024，3.1] | 主控站/控制站 | 执行受控站之遥控的站所。备考：于某些标准中通常称为 “主站 (master station)”。 | controlling station/control station |
| 9 | 蜜罐 | 专用于吸引潜在的黑客和入侵者的系统（如web服务器）或系统资源（如服务器上文件），就好像蜂蜜吸引熊一样。诱骗系统的通用说法。用于欺骗、分散或转移注意力并且激发攻击者花费时间在似乎是非常有价值的，而实际上是伪造且对合法用户不会感兴趣的信息上。[来源:GB/Z 25320.2-2013,2.2.105] | 诱捕蜜罐 | 一系统(例：网页服务器)或系统资源(例：服务器上之档案)，系设计以吸引潜在刽客及入侵者，如同蜂蜜吸引熊。诱捕系统之通用用语，该系统用于欺骗、岔开、转移及鼓励攻击者耗费时间于看似很有价值但实际上系假造，且合法用户不感兴趣之数据。 | honey pot |
| 10 | 入侵检测系统 | 监视和分析网络事件或系统事件的安全服务，为了发现未经授权访问系统资源的企图并且提供实时或接近实时的警告。用于确定试图入侵、正发生入侵或已发生入侵从而对信息系统的网络中入侵可能作出反应的信息系统。[来源:GB/Z 25320.2-2013,2.2.118] | 入侵检测系统 | 安全服务，为寻找以未经授权方式存取系统资源之企图，并提供实时或接近实时告警之目的，而监视及分析网络或系统事件。信息系统，用以识别已发生之试图入侵、正发生或已发生之入侵，且可能响应信息系统及网络中之入侵。 | intrusion detection system, IDS |
| 11 | 装置/设备 | 适用于某种用途或执行某个功能的一个机械装置或装备。[来源:GB/Z 25320.2-2013,2.2.84] | 装置 | 实作特定功能之组件，其可扮演客户端(例:TLS客户端)或服务器(例:GDOI之金钥配送中心)。 | Device |

参考文献

[1]CNS 9359-9:2011 信息技术-词汇-第9部:数据通讯

[2]CNS 11404:1985 数据处理词汇（第9部:数据通信）

[3]CNS 15275-3:2009 信息技术—自动识别与数据撷取技术—调和词汇—第3部:无线射频识别

[4]CNS 62351-4:2022 电力系统管理及关联信息交换－数据及通讯安全－第4部：包括MMS及衍生之剖绘 [5]CNS 62351-5:2023 电力系统管理及关联信息交换－数据及通讯安全－第5部：IEC 60870-5及其衍生协定之安全

[6]CNS 62351-7:2023 电力系统管理及关联信息交换－数据及通讯安全－第7部：网络及系统管理(NSM)数据对象模型

[7]CNS 62351-8:2023 电力系统管理及关联信息交换－数据及通讯安全－第8部：用于电力系统管理之角色式访问控制

[8]CNS 62351-9:2024 电力系统管理及关联信息交换－数据及通讯安全－第9部：电力系统设备之网宇安全密钥管理 [9]CNS 62351-10:2018 电力系统管理及关联信息交换-数据及通讯安全-第10部:安全架构指导纲要

