电子政务系统商密应用安全性评估中数据安全测评规范

1 范围

本文件规定了电子政务系统商用密码应用安全性评估中数据安全的检测要求与评估方法。

本文件适用于规范监管部门、第三方评估机构在电子政务系统商用密码应用安全性评估中数据安全监督、管理与测评，为电子政务数据安全保护工作提供支撑与参考。

2 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 39786-2021信息安全技术 信息系统密码应用基本要求

GB/T 信息安全技术 网络数据分类分级要求（征求意见稿）

GM/Z 4001 密码术语

GM/T 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

GM/T 0115-2021 信息系统密码应用测评要求

GM/T 0116-2021 信息系统密码应用测评过程指南

3 术语和定义

GB/T 25069 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40692-2021 政务信息系统

GM/Z 4001 密码术语

上述标准定义和范围界定的以及下列术语和定义适用于本文件。

3.1

电子政务系统 e-governance system

电子政务系统是由政务部门建设、运行或使用的,用于直接支持政务部门工作或履行其职能的各类信息系统。

3.2

密码测评 cryptographic evaluation

按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

3.3

电子政务数据 e-governance data

由政务部门或为政务部门采集、存储、加工、使用、处理等的信息资源。

注: 政务信息资源包括:政务部门依法采集的信息资源 ;政务部门在履行职能过程中产生和生成的信息资源 ;政务部门投资建设和外购服务获取的信息资源;政务部门依法授权管理的信息资源。

3.4

收集 acquisition

通过电子政务系统采集、人工填写、交易购买、共享交换等方式获取数据的行为。

3.5

存储 storage

电子政务数据以某种格式记录在计算机内部或外部存储介质上的行为。

3.6

使用加工 processing

通过对电子政务数据进行数据挖掘、分析、加工等活动，获取目的结果的行为。

3.7

传输 transmission

电子政务数据从一个系统、设备、平台、企业传送到另一个系统、设备、平台、企业的通信过程。

3.8

提供 provide

电子政务数据处理者向其他数据处理者提供数据，或将电子政务数据处理权由一个处理者向另一个处理者转移，且双方分别对数据拥有独立处理权的过程。

3.9

公开 public disclosure

将电子政务数据向社会或不特定人群公开发布的行为。

3.10

销毁 destruction

将电子政务数据进行彻底删除，使其无法复原的过程。

3.11

数据全生命周期 data life cycle

数据收集、存储、使用加工、传输、提供、公开等各环节数据处理活动。

3.12

数据处理者 data processor

对电子政务数据进行收集、存储、使用加工、传输、提供、公开等数据处理活动的组织。

4 缩略语

下列缩略语适用于本文件。

a) IP：互联网协议（Internet Protocol）。

b) MAC：媒体访问控制（Medium Access Control）。

c) IMSI：国际移动用户识别码（International Mobile Subscriber Identification Number）。

d) IMSI： 国际移动设备识别码（International Mobile Equipment Identity）。

5 电子政务系统商密应用安全性评估中数据安全总体框架

5.1 概述

电子政务系统通过密码技术保障数据的机密性、完整性、真实性和敏感性，建立建全分类分级、组织保障、人员管理和安全评估，提升数据采集、数据传输、数据存储、数据处理、数据交换、数据清除等数据生命周期中的安全保障能力。电子政务系统商密应用安全性评估中数据安全总体框架如图 1 所示。

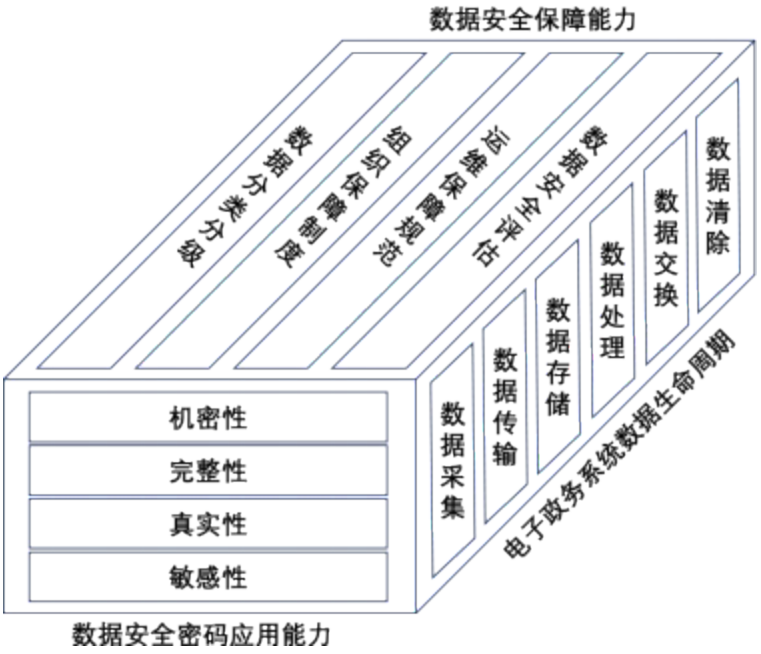

图1 电子政务系统商密应用安全性评估中数据安全总体框架

5.2 数据安全保障能力

5.2.1 概述

实施电子政务系统的数据分类分级管理，建立组织保障制度和运维保障规范，通过数据安全评估提升数据安全的保障能力。

5.2.2 电子政务系统数据分类

参照系统运行场景和商用密码应用性安全评估规则，将电子政务数据分为四种类型，包括鉴别类数据、主体类数据、业务类数据、系统类数据。电子政务系统数据分类说明如表 1 所示。

表 1 电子政务系统数据分类说明

数据分类	参考说明
鉴别类数据	用于电子政务系统用户鉴别身份的数据，一旦遭到未经授权的查看或未经授权的变更，会对电子政务系统的使用主体的数据造成危害。包括但不限于： 1）电子政务系统常规使用的身份鉴别数据，如：账号、卡号、USBKEY、口令等数据。 2）电子政务系统使用生物特征的身份鉴别数据，如：弱隐私（如人脸、声纹、步态、耳纹、眼纹、笔迹等。）、强隐私（指纹、虹膜等）的个人生物特征样本数据与特征值数据。 3）电子政务系统辅助用于身份鉴别的数据，如动态口令、短信验证码、口令提示问题等。

主体类数据	用于电子政务系统可识别特定个人、组织的主体身份数据，一旦遭到未经授权的查看或未经授权的变更，会对个人、组织主体造成危害。包括但不限于： 1）基本数据 指个人基本情况数据，如个人姓名、性别、国籍、民族、婚姻状况、证件类型、证件号码、证件生效日期、证件到期日期、家庭住址等。 组织基础概况数据，如法定代表人姓名、企业名称、

	统一社会信用代码、经营许可证、经营范围、行业分类、经济类型、人员规模、注册资本、企业地址等。 2）通讯数据 指个人、组织各类通信联系方式数据，如手机、固定电话、电子邮箱地址、微信号、联系人、通讯地址等。 3）关系数据 指个人、组织各类关系的记录数据，如个人与个人的关系数据（子或女、父母、兄弟姐妹、配偶等）个人与组织的关系数据（法定代表人、财务负责人、业务经办人、一般雇员、高管等）。组织与组织的关系数据（如集团关系、家族企业、互持股情况等）。 4）位置数据 指能用于标记个人地理空间或网络空间位置的数据，如定位信息、IMEI/IMSI、IP地址、MAC地址、地理位置等。 5）政治面貌数据 指个人政治、宗教信仰等数据，如党员、团员、党派、宗教信仰等。
业务类数据	电子政务系统业务过程种生成的数据，一旦遭到未经授权的查看或未经授权的变更，会对个人、组织主体造成危害。包括但不限于：教育、财产、卫生、司法、交通、招投标等。
系统类数据	电子政务系统运行过程种生成的数据，一旦遭到未经授权的查看或未经授权的变更，会对电子政务系统运行造成危害。包括但不限于：系统规划数据、软件程序数据、运行日志数据、安全管理数据等。

5.2.3 电子政务系统数据分级

依据国家相关法律法规，电子政务系统数据安全遭受破坏，对国家安全、公众权益、个人权益、组织权益等影响，主要考虑以下情况：

a) 影响对象为国家安全的情况，一般指数据的安全性遭到破坏后，可能对国家政权稳固、领土主权、民族团结、社会经济、市场稳定等造成影响。

b) 影响对象为公众权益的情况，一般指数据的安全性遭到破坏后，可能对生产经营、教学科研、医疗卫生、公共交通等社会秩序和公众的政治权利、人身自由、经济活动等造成影响。

c) 影响对象为个人权益的情况，一般指数据的安全性遭到破坏后，可能对敏感个人信息和其他受法律保护的个人权益造成影响。

d) 影响对象为组织合法权益的情况，一般指数据的安全性遭到破坏后，可能对某单位或企业的生产运营、声誉形象、公信力等造成影响。

影响程度包括严重损害、一般损害、轻微损害和无损害，影响程度说明如表2所示。

表 2 影响程度说明

影响程度	参考说明

严重损害	1）可能导致危及国家安全的重大事件，发生危害国家利益或造成重大损失的情况。 2）可能导致严重危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致市场秩序遭到严重破坏等情况。 3）可能导致监管部门重要/关键业务无法正常开展的情况。 4）可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。 5）可能导致电子政务系统各项业务对外无法正常开展的情况。
一般损害	1）可能导致危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致市场秩序遭到严重破坏

	等情况。 2）可能导致监管部门业务无法正常开展的情况。 3）可能导致个人信息安全风险、侵犯个人隐私等危害个人权益的事件。 4）可能导致电子政务系统各项业务对外无法正常开展的情况。
轻微损害	1）可能导致监管部门部分业务临时性中断等情况。 2）可能导致个别的组织、个人在电子政务或其他领域中的业务中断等情况。 3）可能导致电子政务系统内部业务临时性中断等情况。 4)可能导致超出个人客户授权加工、处理、使用数据等情况，对个人权益造成部分或潜在影响。
无损害	对组织权益和个人隐私等不造成影响，或仅造成微弱影响但不会影响国家安全、公众权益、市场秩序或者电子政务系统各项业务正常开展。

电子政务系统数据安全分级规则如表3所示。

表 3 电子政务系统数据安全分级规则

参考安全级别	影响范围		数据特征
	对象	程度	
5	国家安全	严重损害/一般损害/轻微损害	• 数据通常主要用于国家监管机构、大型或特大型机构，电子政务系统中重要核心节点类关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。
	公众权益	严重损害	
4	公众权益	一般损害	• 数据主要用于电子政务系统中重要核心节点的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人权益或组织权益造成严重影响，但不影响国家安全。
	个人权益	严重损害	
	组织权益	严重损害	
3	公众权益	轻微损害	• 数据用于电子政务系统关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人权益或组织权益造成一般影响，但不影响国家安全。
	个人权益	一般损害	
	组织权益	一般损害	
2	个人权益	轻微损害	• 数据用于电子政务系统一般业务使用，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据。 • 数据的安全性遭到破坏后，对个人权益或组织造成轻微影响，但不影响国家安全、公众权益。
	组织权益	轻微损害	
	国家安全	无损害	• 数据一般可被公开或可被公众获知、使用。

1			• 个人或组织主体主动公开的信息数据。 • 数据的安全性遭到破坏后，可能对个人权益或组织权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。
	公众权益	无损害	
	个人权益	无损害	
	组织权益	无损害	

5.2.4 电子政务系统数据安全的组织保障

组织保障，是电子政务系统数据安全保障能力的重要组成部分，明确数据安全的组织管理、制度管理、人员管理、第三方机构管理，保障电子政务系统数据安全的实施。

5.2.5 电子政务系统数据安全的运维保障

运维保障，是电子政务系统数据安全的运营支撑部分，明确访问控制、安全监测、安全审计、应急处置等过程中的密码应用要求，保障电子政务系统数据安全的运行。

5.2.6 电子政务系统数据安全的安全评估

安全评估，是电子政务系统数据安全的检查评估部分，明确数据采集、数据传输、数据存储、数据处理、数据交换和数据清除的密码应用的评估流程与评估原则，保障电子政务系统数据安全的可靠性。

5.3 数据安全密码应用能力

5.3.1 概述

商用密码技术是电子政务数据安全的重要技术能力，重点实现数据的机密性、完整性、真实性、敏感性，降低数据破坏、泄露的风险。

5.3.2 机密性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算、非对称算法的加解密，实现数据的机密性。

5.3.3 完整性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算法或密码杂凑算法的消息鉴别码机制，公钥密码算法的数字签名机制，实现数据的完整性。

5.3.4 真实性

使用商用密码技术，对电子政务系统中安全级别三级以上的数据，可采用基于对称密码算法或密码杂凑算法的消息鉴别码机制，公钥密码算法的数字签名机制，实现数据的真实性。

5.3.5 敏感性

使用商用密码技术，对电子政务系统中安全级别二级以上的数据，可采用格式保留加密或差分隐私算法等脱敏技术，有效降低数据的敏感性。

6 电子政务系统商密应用安全性评估中数据生命周期安全防护要求

6.1 数据采集密码应用安全要求

数据采集，指电子政务系统内部新产生数据，以及外部收集数据的阶段。数据采集存在数据源伪造、特权账户滥用、数据泄露、数据篡改、恶意数据注入等安全风险，应基于商用密码技术保障数据来源的真实性，保障采集安全级别3级以上数据的机密性与完整性。

基于商用密码技术的数据采集安全要求如下：

a) 应使用商用密码的电子签名技术，对数据采集的来源的真实性实施保护。

b) 应采用商用密码技术对鉴别类数据的采集时，实施机密性和完整性保护。如口令、生物特征数据等。

c) 应采用商用密码技术对安全级别3级以上的主体类数据采集时，实施机密性和完整性保护。如证件号、手机、定位等数据。

d） 应采用商用密码技术对安全级别3级以上的业务类数据采集时，实施机密性和完整性保护。如电子单证、标书等数据。

e） 应采用商用密码技术对采集数据的应用软件程序，实施完整性保护。

f） 应采用商用密码技术对采集数据过程产生的日志数据，实施完整性保护。