ICS
CCS

团　体　标　准

T/CGCC XX—20XX

大宗商品电子交易
敏感信息脱敏和加密　规范

Electronic trading of bulk commodities—

Desensitization and encryption of sensitive information—Specification

（征求意见稿）

（本稿完成日期：2021 年 6 月 21 日）

20XX－XX－XX 发布　　20XX－XX－XX 实施

中国商业联合会　　发布

目　　次

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 1
4 总体原则 2
4.1 敏感信息脱敏的原则 2
4.2 敏感信息加密的原则 2
5 敏感信息的分类和内容 2
5.1 敏感信息的分类 2
5.2 敏感信息的内容 3
6 脱敏和加密要求 6
6.1 敏感信息的脱敏要求 6
6.2 敏感信息的加密要求 7
7 证实方法 8
7.1 敏感信息脱敏的证实方法 8
7.2 敏感信息加密的证实方法 8
附录A（资料性） 字段型敏感信息脱敏前后展示形式对照示例 9
参考文献 11

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。

本文件由北京金网安泰信息技术有限公司提出。

本文件由中国商业联合会归口。

本文件起草单位：北京金网安泰信息技术有限公司、商业科技质量中心、江西省联交运登记结算中心有限公司、包头稀土产品交易所有限公司、国能互通内蒙古网络科技有限公司、牡丹国际商品交易中心有限公司、临沂国际商品交易中心有限公司、南方小麦交易市场有限公司。

本文件主要起草人：关键、肖燕林、唐泽宇、刘晓东、薛计涛、祁永星、刘祖国、李汉武、陈秀昆、刘月廷、谢永军、付元虎、王兰军、宋宪余、包银锋、王立荣、王轲菲。

引　　言

大宗商品交易平台的数据涉及到交易参与各方的身份信息和业务数据等重要信息，这些信息具有非常高的敏感性，一旦泄露会给交易参与各方和交易平台带来较大风险。

随着互联网技术和大宗商品电子交易行业的快速发展，基于大宗商品交易平台的行业应用呈现出需求日益增长、服务范围扩大、个性化需求突出的趋势。这些应用在服务过程中需要读取和使用交易平台数据，为确保交易平台敏感信息的安全，一个行之有效的方法就是对所涉及的交易平台敏感信息进行脱敏或加密。

本文件针对交易平台敏感信息安全问题，规范在涉及交易平台敏感信息的行业应用项目中对敏感信息的脱敏和加密工作，旨在加强交易平台信息安全，防止交易平台敏感信息泄露，最大程度地保障交易参与各方和交易平台合法权益。

大宗商品电子交易　敏感信息脱敏和加密　规范

1　范围

本文件确立了大宗商品交易平台敏感信息脱敏和加密的原则，给出了敏感信息的分类和内容，规定了敏感信息脱敏和加密的要求，描述了对应的证实方法。

本文件适用于在涉及大宗商品交易平台敏感信息的行业应用项目中对敏感信息的脱敏和加密。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

交易平台　trading platform

为企业及个人提供交易、资金结算以及交收等相关服务的电子商务平台。

注：在本文件中专指大宗商品交易平台。

3.2

交易用户　customer

在交易平台（3.1）参与交易或其他相关业务，并接受相关服务的企业用户或个人用户。

3.3

交易帐号　customer ID

由交易平台（3.1）为交易用户（3.2）分配，作为关联该交易用户（3.2）在交易平台（3.1）内所有相关信息的交易用户（3.2）唯一标识。

3.4

信息主体　information subject

信息所标识的交易用户（3.2）。

3.5

敏感信息　sensitive information

能够单独或者与其他信息结合识别信息主体（3.4）身份，一旦泄露、非法提供或滥用可能危害信息主体（3.4）安全，泄露信息主体（3.4）隐私或商业机密的交易用户（3.2）信息。

3.6

脱敏　desensitization

为实现敏感信息（3.5）的可靠保护而对敏感信息（3.5）按照一定规则进行的信息变形处理。

3.7

原始信息标识　original information identification

为保证内容一致的原始敏感信息（3.5）在脱敏（3.6）后其一致性仍能被识别，而为脱敏（3.6）后信息分配的一个标识性编码。

4 总体原则

4.1 敏感信息脱敏的原则

4.1.1 前置性原则

从交易平台获取业务数据的应用程序，在非保密场景中进行处理、使用、存储之前，需要对敏感信息数据进行识别，并对其中的敏感信息进行脱敏。

4.1.2 安全性原则

使用脱敏后的信息无法单独或者与其他信息结合识别出信息主体身份。

4.1.3 可用性原则

脱敏后的信息数据之间的关联关系与脱敏前的关联关系保持一致，以保证数据的可用性。

4.1.4 一致性原则

同类的原始敏感信息采用相同的脱敏规则。在同类型的字段型敏感信息中，为相同内容的原始信息分配同样的原始信息标识，不同的敏感信息分配不同的原始信息标识。

4.1.5 展示性原则

脱敏后的敏感信息，需要保留原有信息的部分特征，以保证具有一定的展示效果。

4.2 敏感信息加密的原则

4.2.1 前置性原则

从交易平台获取业务数据的应用程序，在非保密场景中进行处理、使用、存储之前，需要对敏感信息数据进行识别，并对其中的文件型敏感信息进行加密。

4.2.2 安全性原则

宜采用业内广泛认可的主流加密算法，以保证在没有密钥的情况下无法对加密文件进行解密。

4.2.3 效率原则

在保证安全性的同时，敏感信息的加密需要兼顾应用程序加密和解密的处理效率。

5 敏感信息的分类和内容

5.1 敏感信息的分类

交易平台涉及的敏感信息较多，识别敏感信息的类别有利于脱敏工作的顺利进行。按照不同的属性可以将敏感信息划分为不同的类别。

a) 按照信息主体可以将敏感信息划分为以下类别：
   - 企业敏感信息：交易平台的企业用户敏感信息；
   - 个人敏感信息：交易平台的个人用户敏感信息。

b) 按照原始信息数据类型可以将敏感信息划分为以下类别：
   - 字段型敏感信息：单一字段的敏感信息数据；

- 文件型敏感信息：以文件形式存储的敏感信息数据。

5.2 敏感信息的内容

5.2.1 企业敏感信息

交易平台涉及的企业敏感信息包含以下几个方面的内容。

a) 企业基本信息：
   1) 企业名称，
   2) 统一社会信用代码，
   3) 联系地址。
b) 联系人信息：
   1) 姓名，
   2) 手机号码。
c) 法定代表人信息：
   1) 姓名，
   2) 手机号码，
   3) 身份证号码，
   4) 军官证号码，
   5) 警官证号码，
   6) 护照号码，
   7) 其他有效证件号码。
d) 银行账户信息：
   1) 银行账号，
   2) 银行账户余额。
e) 交易信息：
   1) 交易帐号，
   2) 资金账户余额，
   3) 委托记录，
   4) 成交记录，
   5) 订货记录，
   6) 入金记录，
   7) 出金记录，
   8) 交收记录，
   9) 仓储记录。
f) 融资信息。
g) 电子存档文件：
   1) 包含以上敏感信息的电子存档文件，
   2) 包含交易用户生物特征信息的电子存档文件。

5.2.2 个人敏感信息

交易平台涉及的个人敏感信息包含以下几个方面的内容。

a) 个人基本信息：
   1) 姓名，

2) 手机号码，
3) 电子邮箱，
4) 出生日期，
5) 联系地址，
6) 身份证号码，
7) 军官证号码，
8) 警官证号码，
9) 护照号码，
10) 其他有效证件号码。

b) 银行账户信息：
1) 银行账号，
2) 银行账户余额。

c) 交易信息：
1) 交易帐号，
2) 资金账户余额，
3) 委托记录，
4) 成交记录，
5) 订货记录，
6) 入金记录，
7) 出金记录，
8) 交收记录，
9) 仓储记录。

d) 融资信息。

e) 电子存档文件：
1) 包含以上敏感信息的电子存档文件，
2) 包含交易用户生物特征信息的电子存档文件。

5.2.3 字段型敏感信息

5.2.3.1 企业字段型敏感信息

交易平台涉及的企业字段型敏感信息包含以下几个方面的内容。

a) 企业基本信息：
1) 企业名称，
2) 统一社会信用代码，
3) 联系地址。

b) 联系人信息：
1) 姓名，
2) 手机号码。

c) 法定代表人信息：
1) 姓名，
2) 手机号码，
3) 身份证号码，
4) 军官证号码，

5) 警官证号码，
6) 护照号码，
7) 其他有效证件号码。

d) 银行账号。
e) 交易帐号。

5.2.3.2 个人字段型敏感信息

交易平台涉及的个人字段型敏感信息包含以下几个方面的内容。

a) 个人基本信息：
1) 姓名，
2) 手机号码，
3) 电子邮箱，
4) 出生日期，
5) 联系地址，
6) 身份证号码，
7) 军官证号码，
8) 警官证号码，
9) 护照号码，
10) 其他有效证件号码。

b) 银行账号。
c) 交易帐号。

5.2.3.3 其他敏感信息

以下的企业或个人敏感信息中，可能包含上述字段型敏感信息中的“交易帐号”等多个敏感信息字段：

a) 银行账户余额，
b) 资金账户余额，
c) 委托记录，
d) 成交记录，
e) 订货记录，
f) 入金记录，
g) 出金记录，
h) 交收记录，
i) 仓储记录，
j) 融资信息。

5.2.4 文件型敏感信息

交易平台涉及的文件型敏感信息包含以下两个方面的内容：

a) 企业文件型敏感信息：指企业的各类电子存档文件；
b) 个人文件型敏感信息：指个人的各类电子存档文件。

6 脱敏和加密要求

6.1 敏感信息的脱敏要求

6.1.1 原始信息标识

为了识别脱敏后信息与原始敏感信息的对应关系，在对每一个字段型原始敏感信息脱敏的同时应为其分配一个原始信息标识。标识的长度固定为16位，前2位为敏感信息名称标识代码，使用大写字母编码；后14位为纯数字编码，采取顺序累加的方式分配。

在同类型的字段型敏感信息中，应为相同内容的原始信息分配同样的原始信息标识，不同的敏感信息应分配不同的原始信息标识。

不同敏感信息名称的标识代码不可重复，各字段型敏感信息名称标识代码见表1。

表1 敏感信息名称标识代码

敏感信息名称	标识代码
企业名称	QY
统一社会信用代码	XY
联系地址	DZ
姓名	XM
手机号码	SJ
电子邮箱	YX
出生日期	CS
身份证号码	SF
军官证号码	JG
警官证号码	JC
护照号码	HZ
其他有效证件号码	QT
银行账号	YH
交易帐号	JY

每一个字段型敏感信息脱敏后应在数据库中与为其分配的原始信息标识建立对应关系。

6.1.2 脱敏规则

在脱敏方式上，根据不同字段型敏感信息的特点，一些字段采用隐匿部分信息、替换部分信息的处理方式，还有一些字段采用以原始信息标识替换原始信息的处理方式。

各种字段型敏感信息应按照表2给出的脱敏规则进行脱敏。

表2 字段型敏感信息脱敏规则

敏感信息名称	脱敏规则[a]
企业名称	更改为“公司”后边跟随该企业名称的原始信息标识
统一社会信用代码	只保留前 8 位，其余各位均以半角星号（*）替换

表2　字段型敏感信息脱敏规则（续）

敏感信息名称	脱敏规则[a]
联系地址	对能识别出省、市、区（县）全部或部分信息的地址，最多只保留省、市、区（县）三级信息；否则，最多只保留前 4 位字符
姓名	对于汉字姓名，将第 1 位汉字随机替换为其它常见 1 位汉字姓氏，后边跟 2 位半角星号（*）；对于非汉字姓名，只保留第 1 位字符，后边跟 2 位半角星号（*）
手机号码	保留前 2 位和最后 1 位，中间各位均以半角星号（*）替换
电子邮箱	@左边保留第 1 位字符，后边跟 4 位半角星号（*）；@右边保留原样
出生日期	只保留年份，月份和日期的各位均以半角星号（*）替换
身份证号码	保留前 10 位，其余各位均以半角星号（*）替换
军官证号码	数字编号前面全部保留，数字编号部分只保留首尾各 1 位，中间各位均以半角星号（*）替换
警官证号码	
护照号码	
其他有效证件号码	
银行账号	只保留首尾各 2 位，中间各位均以半角星号（*）替换
交易帐号	使用该交易帐号的原始信息标识替换该交易帐号
后台管理员、仓库管理员、会员等的敏感信息可参照本表脱敏规则脱敏	
[a] 4.2.3.3 列出的其他敏感信息应按照本表给出的脱敏规则对其中包含的所有字段型敏感信息进行脱敏。	

字段型敏感信息脱敏前后展示形式的对照示例见附录A。

6.2　敏感信息的加密要求

6.2.1　文件的加密

6.2.1.1　加密算法

针对文件型敏感信息，应采用公开的对称加密算法对文件进行加密，如GB/T 32907—2016定义的国密SM4分组加密算法、ISO/IEC 18033-3:2010定义的高级加密标准AES等。

6.2.1.2　密钥长度

加密使用的密钥长度应大于等于128Bit，宜使用256Bit。

6.2.2　密钥的保管和使用

6.2.2.1　密钥的保管

密钥用于对文件型敏感信息的加密和解密，应由交易平台与密钥使用者协商保管方式并妥善保管。

6.2.2.2　密钥的启用

初次使用密钥前应由密钥保管者授权。

6.2.2.3　密钥的使用

在密钥启用后，密钥使用者方可以使用密钥。

6.2.3 文件名的处理

对于从交易平台获取的交易用户文件型敏感信息，在加密后存储到本地时，应采用通用唯一识别码（UUID）命名文件，确保文件不重名，并保留原始文件扩展名。

7 证实方法

7.1 敏感信息脱敏的证实方法

对敏感信息的脱敏，采取以下步骤进行证实：

——检查展示界面所展示的字段型敏感信息，确认展示内容符合 6.1 的脱敏要求；

——检查数据库里存储的字段型敏感信息，确认已按照 6.1 的脱敏要求进行脱敏。

7.2 敏感信息加密的证实方法

对文件型敏感信息的加密，采取以下步骤进行证实：

——检查文件是否未加密：使用与文件类型匹配的文件查看器，检查是否能够成功读取文件，如果能成功读取，则说明文件未加密；

——检查加密算法和密钥长度：检查用于加密文件的加密算法和密钥长度，确认符合 6.2.1 的要求；

——检查密钥的保管和使用：确认密钥的保管和使用符合 6.2.2 的要求；

——检查文件名命名：确认文件名的处理符合 6.2.3 的要求。

附　录　A
（资料性）
字段型敏感信息脱敏前后展示形式对照示例

表A.1给出了字段型敏感信息脱敏前后展示形式对照示例。

表 A.1　字段型敏感信息脱敏前后展示形式对照示例

敏感信息名称	脱敏前	脱敏后
企业名称	北京 xxx 贸易有限公司	公司 QY12341234123412
统一社会信用代码	91110108666610000K	91110108*********
联系地址	北京市东城区东四街道 xx 小区 xx 号楼 x 单元 101	北京市东城区
	河北省保定市涿州市第一大街	河北省保定市涿州市
	广西南宁市	广西南宁市
	美国洛杉矶	美国洛杉
姓名	张三	朱**
	诸葛亮	王**
	Jack Lee	J**
手机号码	13812341234	13********4
电子邮箱	98765432@qq.com	9****@qq.com
	cn@qq.com	c****@qq.com
出生日期	1990-12-01	1990-**-**
	1990/12/01	1990/**/**
	19901201	1990****
	1990 年 12 月 01 日	1990 年**月**日
身份证号码	110101199012011234	1101011990********
军官证号码	军 1234567	军 1*****7
警官证号码	123456	1****6
护照号码	E12345678	E1******8
银行账号	6200123412341234	62**********34
	6200123456789000123	62**********23
交易帐号	1000110001	JY12345678901234
注：表中所列举的示例并非真实信息，与真实数据或许存在一定差异。		

表A.2给出了部分其他敏感信息脱敏前后展示形式对照示例。

表 A.2　部分其他敏感信息脱敏前后展示形式对照示例

敏感信息名称	字段名	是否需要脱敏	脱敏前	脱敏后
成交记录	成交编号	否	10000001	10000001
	交易帐号	是	1000110001	JY12345678901234
	撮合成交号	否	10000	10000
	对手撮合成交号		10001	10001
	商品编号		M2103	M2103
	买卖方向		买入	买入
	转让标志		订立	订立
	成交价格		1000.00	1000.00
	成交数量		100	100
	成交时间		2020-12-01 09:30:10	2020-12-01 09:30:10
	对手交易帐号	是	1000110002	JY12345678901235
入金记录	内部流水号	否	20678	20678
	交易帐号	是	1000110001	JY12345678901234
	银行编号	否	10	10
	银行账号	是	6200123412341234	62**********34
	入金金额	否	2000.00	2000.00
	入金时间		2020-09-01 10:25:38	2020-09-01 10:25:38

注1：表中所列举的示例并非真实信息，与真实数据或许存在一定差异。

注2：银行账户余额、资金账户余额、委托记录、订货记录、出金记录、交收记录、仓储记录、融资信息等其他敏感信息脱敏前后展示形式与本表中示例类似，不再一一举例。

参 考 文 献

[1] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人信息保护指南
[2] GB/T 32907—2016 信息安全技术 SM4分组密码算法
[3] GB/T 35273—2020 信息安全技术 个人信息安全规范
[4] GB/T 37964—2019 信息安全技术 个人信息去标识化指南
[5] ISO/IEC 18033-3:2010 Information technology—Security techniques—Encryption algorithms—Part 3: Block ciphers