ICS 71
CCS G 07

中华人民共和国国家标准

GB/T 40640.2—2021

化学品管理信息化　第2部分:信息安全

Informationalized management of chemicals—Part 2:Information security

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

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。

本文件是GB/T 40640《化学品管理信息化》的第2部分。GB/T 40640《化学品管理信息化》已经发布了以下部分：

——第1部分：数据交换；

——第2部分：信息安全；

——第3部分：电子标签应用；

——第4部分：化学品定位系统通用规范；

——第5部分：化学品数据中心。

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。

本文件由全国危险化学品管理标准化技术委员会(SAC/TC 251)提出并归口。

本文件起草单位：中国化工经济技术发展中心、中华人民共和国合肥海关、安徽省征信股份有限公司、合肥诚益信息科技有限公司、重庆知行数联智能科技有限责任公司、中国石油化工股份有限公司青岛安全工程研究院、青岛卫戈斯供应链管理有限公司、上海化工院检测有限公司、广东宏川智慧物流股份有限公司、中山市利达斯供应链管理有限公司、佛山小林智慧科技发展有限公司、江门市泽信润业科技有限公司、华峰集团有限公司、江阴澄星实业集团有限公司、国化低碳技术工程中心、生态环境部固体废物与化学品管理技术中心。

本文件主要起草人：刘振、盛旋、周典兵、郑平、俞阳国、商照聪、温涛、张蕾、孙昊、刘建围、杨杰群、傅强、包剑、施红勋、冷啟源、周荃、曹梦然、林海川、赖博、雷初泽、黄贤业、王波。

引　言

信息化是实现化学品管理现代化的重要手段。随着物联网及大数据应用技术的发展，现代信息技术的应用为提升管理效率、促进信息共享、消除管理盲区、有效遏制化学品事故发生提供了技术支撑。在这方面，我国已经建立了化学品管理信息化的国家标准体系。

在该标准体系中，GB/T 40640《化学品管理信息化》是规范我国相关机构从事化学品管理信息化系统建设开发活动时的方法和依据，拟由五部分构成，目的在于确立实施化学品管理信息数据交换、维护信息安全、电子标签应用、定位系统应用以及化学品数据中心建设时的方法和依据。

——第1部分：数据交换；

——第2部分：信息安全；

——第3部分：电子标签应用；

——第4部分：化学品定位系统通用规范；

——第5部分：化学品数据中心。

本文件是GB/T 40640《化学品管理信息化》的第2部分。信息安全是实现管理信息化的基础，有效的信息安全管理可以提高信息化管理系统的隐私性、真实性、完整性、可用性，避免对系统服务连续性产生不利影响。本次制定对化学品管理信息化有关的信息安全要求进行了详细的规定，以更好的规范和促进化学品管理信息化系统相关建设。

化学品管理信息化　第2部分:信息安全

1　范围

本文件规定了化学品管理信息化信息安全的基本要求和技术要求。

本文件适用于化学品管理信息化的信息安全管理。

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 2887　计算机场地通用规范

GB/T 5271.8　信息技术　词汇　第8部分:安全

GB 17859　计算机信息系统　安全保护等级划分准则

GB/T 20269　信息安全技术　信息系统安全管理要求

GB/T 20270　信息安全技术　网络基础安全技术要求

GB/T 21052　信息安全技术　信息系统物理安全技术要求

GB/T 22080　信息技术　安全技术　信息安全管理体系　要求

GB/T 22240　信息安全技术　网络安全等级保护定级指南

GB/T 30283　信息安全技术　信息安全服务　分类

3　术语和定义

GB/T 5271.8、GB 17859 界定的以及下列术语和定义适用于本文件。

3.1

访问控制　access control

按确定的规则,对实体之间的访问活动进行控制、防止未授权使用资源的安全机制。

3.2

令牌　tokens

由系统创建的包含登录进程返回的安全标识符和由本地安全策略分配给用户和用户的安全组的特权列表。

4　基本要求

4.1　安全目标

4.1.1　应通过整体安全体系规划,综合运用各种安全技术和手段,从侵害程度、侵害对象两个方面划分化学品信息管理系统的信息安全等级,其安全要求应不低于对应安全等级应符合 GB 17859 和 GB/T 22240的规定。

4.1.2　在化学品信息采集、信息存储、信息加工、信息交换、信息应用、信息消亡过程中应研究目标化学

品的信息安全特征，确定相对应的安全目标，分为静态安全目标和动态安全目标。

4.1.3 静态安全目标保证系统实体平台安全，应包括整个系统的物理环境、系统软硬件结构和可用的信息资源。

4.1.4 动态安全目标保障系统的软环境安全，应包括安全管理、安全服务、安全意识和人员的安全专业素质。

4.2 安全体系

信息安全体系应包括：

a) 安全管理：建立信息安全管理相关的制度和规定，实现管理上的安全；
b) 安全服务：建立信息安全体系不仅应依靠现有的安全机制和设备，还应全方位地提供各类安全服务；
c) 数据安全：保证数据库的安全和数据本身及网络传输安全；
d) 应用系统安全：系统内部的应用安全，是系统实现时最被关注的部分；
e) 软件平台安全：保证软件平台系统（如操作系统和应用系统基础服务软件等）安全；
f) 网络安全：把被保护的网络从自由开放、无边界的环境中独立出来，使网络成为可控制、可管理的内部系统；
g) 物理安全：从物理上保证系统设备的安全。

4.3 安全管理

4.3.1 化学品信息管理系统和监管平台应建立一套完善的安全管理方案，并贯穿信息安全的各层次，包括安全制度管理和安全目标管理。

4.3.2 应从建立完善机房管理、网络管理、数据管理、设备管理、应急处理、人员管理、技术资料管理等方面加强安全制度管理。

4.3.3 应按照资源管理目标，对信息系统涉及的物理资源、网络资源、信息资源实施统一的资源分配，并根据资源重要程度确定安全等级和安全管理范围。

4.3.4 应按照 GB/T 20269 和 GB/T 22080 的要求，安排专门人员负责以保证安全管理制度实施。

4.3.5 应展开对最新安全技术的跟踪研究，加强安全技术进行交流、探讨，优化安全管理策略。

4.3.6 应加强与已有的防火墙、防病毒、数据备份等安全设施的紧密配合。

4.4 安全服务

4.4.1 安全服务应包括安全咨询、安全工程实施、安全技术培训和安全维护，应符合 GB/T 30283 的要求。

4.4.2 信息安全不是安全产品的简单集合，而是一项系统工程并有其专业体系，应采用先进科学的知识结构进行全面细致地把握。

4.4.3 信息安全系统存在固有弱点，即使最微小的安全漏洞都可能引发整个网络系统的崩溃。且系统安全只是暂时的、静态的，应通过持续全面的安全服务进行加强。

5 技术要求

5.1 物理安全

5.1.1 根据不同的目标对象，物理安全包括：

a) 环境安全，对系统所在环境的安全保护，如区域保护和灾难保护；
b) 设备安全，主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电

源保护；

c) 媒介安全，包括媒介本身的安全及媒介数据的安全。

5.1.2 环境安全应符合 GB/T 2887 的要求，物理安全应符合 GB/T 21052 的要求。

5.2 网络安全

5.2.1 一般要求

网络安全应符合 GB/T 20270 的要求。

5.2.2 网络冗余

5.2.2.1 应采用网络冗余、系统隔离、访问控制、加密、安全监测、网络扫描等技术手段来保障化学品信息系统的网络安全。

5.2.2.2 应通过网络冗余解决网络系统单点故障，对关键性的网络线路、设备采用双备份或多备份的方式。网络运行时，应对运营状态相互实时监控并自动调整，当网络的一段或一点发生故障，或者网络信息流量突变时应能在有效时间内进行切换分配。

5.2.3 系统隔离

应划分物理隔离和逻辑隔离，应结合信息安全等级划分合理的网络安全边界，实现不同安全级别的网络或信息媒介不能相互访问。应针对应用系统特点和化学品信息的特征采取相应的隔离措施。

5.2.4 访问控制

5.2.4.1 对于网络不同信任域，应根据双向控制或有限访问的原则加强访问控制，有效控制受控的子网或主机访问权限和信息流向。

5.2.4.2 对网络对象，应解决网络的边界控制和网络内部的控制，根据有限访问的原则对网络资源进行合理配置，对信息流向应根据安全需求实现单向或双向控制。

5.2.4.3 访问控制最重要的设备是防火墙，宜安置在不同安全域出入口处，对进出网络的信息包进行过滤并按安全策略进行信息流控制，同时实现网络地址转换、实时信息告警等功能，高级防火墙还应实现基于用户的细粒度的访问控制。

5.2.5 加密

应采用加密手段防止网络上的窃听、泄漏、篡改和破坏。加密应从三个层次来实现：

a) 链路层加密应侧重通信链路而不考虑信源和信宿，对网络高层主体透明；

b) 网络层加密应采用网络安全协议，具备加密、认证双重功能，并应在系统的服务器间通信采取此协议；

c) 应用层加密应根据实际业务的应对处理、传输和存储的数据采取多种加密算法进行加密保护。

5.2.6 安全监测

应采用安全监测寻找未授权的网络访问尝试和违规行为，包括但不限于网络系统的扫描、预警、阻断、记录、跟踪。网络扫描监测系统应具有实时、自适应、主动识别和响应等特征。

5.2.7 网络扫描

应采用网络扫描对网络设备的安全漏洞进行检测和分析，包括但不限于网络通信服务、路由器、防火墙、邮件、WEB 服务器，从而识别能被入侵者利用非法进入的网络漏洞。网络扫描系统应对检测到的

漏洞信息形成详细报告，包括位置、详细描述和建议的改进方案，有效检测和管理安全风险信息。

5.3 软件平台安全

5.3.1 影响软件平台安全性的因素主要包含操作系统安全漏洞和病毒。

5.3.2 在操作系统安装的时候应使用平台软件厂商提供的安全漏洞扫描工具进行漏洞扫描；在新漏洞信息发布的时候，应利用软件平台厂商提供的更新服务安装相应的漏洞补丁，即时保障系统安全。

5.3.3 应采取专业的防病毒解决方案，实现从网络、服务器、客户机三个方面的立体防范。对于重大的安全漏洞和病毒，应及时向统管理员发出安全警告信并提供相应应对措施。

5.4 应用系统安全

5.4.1 应用系统安全设计原则

5.4.1.1 有限授权

系统设计应实现基于角色的权限控制，用户只能进行与当前身份角色相应的操作和访问权限范围内的数据。对于没有授权的操作和数据，用户无法执行和访问。

5.4.1.2 全面确认

对于用户进行的每一个操作，系统应对用户当前身份和权限进行确认，并对用户每次提交的数据进行完整性和合法性校验。

5.4.1.3 功能分级控制

5.4.1.3.1 应实现管理工作的分级管理，系统管理员负责所管理系统的整体系统管理、版本管理等工作；实际业务管理员负责其他业务系统的管理。

5.4.1.3.2 应实现对涉及实际业务的系统功能的分级控制，普通用户具有普通的操作权限；高级用户在普通用户所有操作权限的基础上，具有其他高级操作功能权限。

5.4.1.4 安全跟踪

5.4.1.4.1 系统应具有安全跟踪和告警框架，保证与安全相关事件的跟踪。

5.4.1.4.2 在安全事件发生时，对于符合一定策略的事件应能够自动预警，以系统预定的方式提示相应人员，并采取措施实现系统资源的自我保护。

5.4.1.4.3 应能够记录发生的安全事件，宜对记录的安全事件提供审计和分析功能。

5.4.2 组织结构与角色管理

5.4.2.1 系统权限宜依据角色进行分级划分，保证适当的用户访问到适当的资源和操作。用户只能进行和当前身份角色相应的操作和访问权限范围内的数据。对于没有授权的操作和数据，用户无法执行和访问。

5.4.2.2 基于角色的权限管理应做到完整的独立于应用、基于实际组织结构的管理功能以及具有灵活的管理方式和高可维护性。系统应支持集中式管理或分级管理。

注：集中式管理，即由一个管理员负责所有组织结构、角色管理。分级管理，即仅由系统管理员管理部门创建和其他应集中管理的功能，其他部分则由具体部门管理员进行管理。

5.4.2.3 统一的组织和角色管理应与组织结构形成直接对应关系，其主要功能包括：

a) 单位部门管理；

b) 统一添加删除维护单位信息；

c) 设置部门间的上下级关系和同级部门间排序；
d) 职能管理；
e) 设置单位和部门职能相关信息，主要包括部门介绍、部门主要职能、部门主要职能；
f) 角色与岗位管理；
g) 设置各单位的角色(岗位)；
h) 设置角色(岗位)与用户的关联关系；
i) 设置角色(岗位)相关工作职能范围介绍。

5.4.3 统一认证与授权服务

5.4.3.1 设计目标

设计目标应包括以下内容：
a) 登录账户管理及个人信息管理；
b) 账户的添加维护、登录认证以及多个应用系统间访问的一次登录；
c) 完整的独立于应用、基于业务逻辑的授权管理功能；
d) 灵活的管理方式和高可维护性。

5.4.3.2 设计结构

图 1 给出了统一认证与授权服务管理结构，包括以下内容：
a) 验证管理服务，负责用户账户、密码等的维护和登录认证，以及为一次登录提供支持；
b) 个性化服务，负责用户相关个性化数据的存储和提供查询、维护接口；
c) 组织结构服务，为应用程序提供下属部门的树形组织架构服务，提供组织结构的统一管理和维护接口；
d) 授权服务，如前面设计目标中所述，建立用户功能管理、授权机制，并提供给应用系统相应开发接口，系统授权支持基于角色的授权模型、存取控制列表(ACL)方式以及自定义授权模型多等安全模型；
e) 资源服务，对系统中的功能和应经过验证才能访问的事物提供统一的注册登记服务。未经过资源服务登记，不应在授权服务中设置资源与角色的访问关联，也不应使应用系统获得相应的资源授权访问验证服务；
f) 审计服务，对系统中与用户操作相关的事件进行记录和跟踪，并提供相关的查询统计服务。

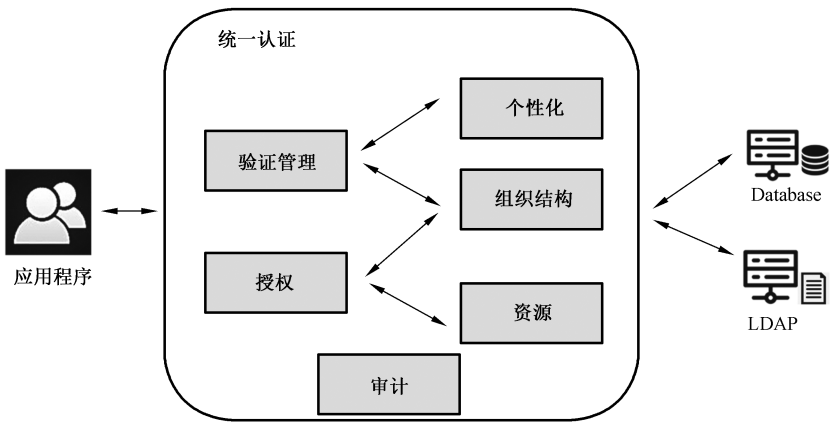
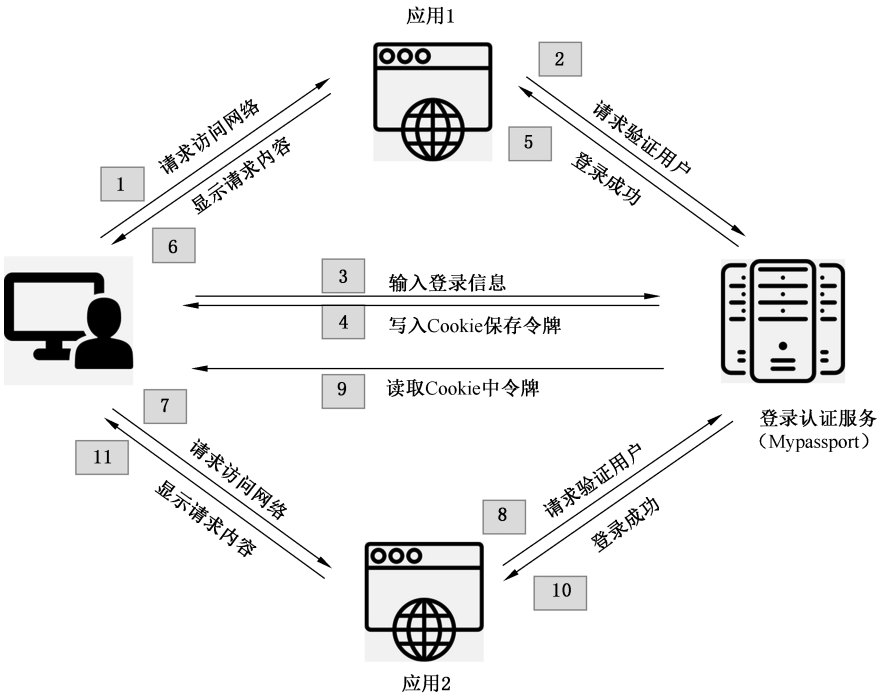


图 1 认证管理服务结构图

5.4.4 一次登录

应采用统一的认证授权模块，以支持一点登录多个子系统访问的功能。多个应用系统间一次登录指用户访问不同域名（虚拟目录）应用，只应登录一次。图 2 给出了一次登录实现原理。



标引序号说明：

1 ——用户请求访问应用 1 的内容；

2 ——应用 1 无法验证用户，应向登录认证服务请求验证用户；

3 ——用户输入登录信息；

4 ——登录认证服务读取数据库中的信息，验证用户。如果验证成功，应向用户本地浏览器写入辨别用户身份的缓存数据（Cookie），保存登录成功后的唯一、有时间期限、代表用户身份的访问令牌；

5 ——登录认证服务向应用 1 传递用户登录成功的信息，并应在信息中包含用户登录后的身份；

6 ——应用 1 向用户输出用户要访问的信息；

7 ——用户请求访问应用 2 的内容；

8 ——应用 2 无法辨别用户身份，应向登录认证服务请求验证用户；

9 ——登录认证服务读取用户本地的 Cookie，获取用户身份令牌；

10——登录认证服务向应用 2 传递用户登录成功的信息，并应在信息中包含用户登录后的身份；

11——应用 2 向用户输入用户要访问的信息。

图 2 一次登录实现原理图

5.4.5 日志与报警

5.4.5.1 应根据化学品信息安全管理的需要，记录用户每一次或重要操作形成日志，并提供相应的分析功能。

5.4.5.2 系统宜具有自动预警功能。对于非法操作，系统根据设定的操作级别采用设定的形式自动报警（如给系统管理员发送电子邮件、短消息、在线消息），并根据定制的策略实现资源的自我保护功能（如锁定账户、锁定要访问的资源、锁定访问 IP）。

5.5 数据安全

5.5.1 应采用可信赖的数据库系统，确保数据库系统的运行安全，并通过对数据库账户和访问权限范围设置实现安全访问策略。

5.5.2 应确保存储在数据库的数据和服务器文件数据本身的安全，采取的保护措施包括但不限于安装反病毒软件、建立可靠的数据备份与灾难恢复系统以及对重要数据采取加密保护。