ICS 35.020
CCS L 70

团　　体　　标　　准

T/GDCSA 019-2024

企业级安全浏览器技术规范

Technical specifications for enterprise security browser

2024-12-20 发布　　2025-01-20 实施

广东省网络空间安全协会　　发布

目　次

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。

本文件由广东电网有限责任公司广州供电局提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：广东电网有限责任公司广州供电局、奇安信科技集团股份有限公司、广东省网络空间安全协会、中国交通信息科技集团有限公司、北京升明科技有限公司、数字广东网络建设有限公司、广州市白云区城市管理和综合执法局、广州大学、华南师范大学、广州华南信息安全测评中心、网安联认证中心有限公司。

本文件主要起草人：张智泉、毛叶凡、杨杰、林海、林志达、赵静、陈凌剑、罗朗、黄士超、胡璇、李倩蕴、林傲宇、池燕清、梁景生、方力、王楹、徐兵、王占鳌、杨佳、彭欣、赵玥麟、田亮、刘晓健、华鹏、李少阳、蔡佩宸、范宇航、郝明、曹望、林蒽蒽、崔健文、郑志彬、郑伟平、丁慧洁、邓志超、朱剑、李峰、王伟彬、郝瑞、成珍苑、黄珊珊、黎韵婷。

企业级安全浏览器技术规范

1 范围

本文件规定了企业级安全浏览器的技术要求，包括浏览器客户端、管理平台、应用要求、Web 应用访问质量数据管理的技术要求。

本文件适用于企业级安全浏览器的选型和设计等。

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 18792-2002 信息技术 文件描述和处理语言 超文本置标语言（HTML）

GB/T 38636-2020 信息安全技术 传输层密码协议（TLCP）

GM/T 0024-2023 SSL VPN技术规范

IETF RFC 1945 超文本传输协议HTTP/1.0 （Hypertext transfer protocol(HTTP/1.0)）

IETF RFC 2109 HTTP状态管理机制 （HTTP state management mechanism）

IETF RFC 2616 超文本传输协议HTTP/1.1 （Hypertext transfer protocol(HTTP/1.1)）

IETF RFC 2818 TLS之上的HTTP （HTTP over TLS）

IETF RFC 5246 运输层安全协议版本1.2 （The transport layer security(TLS) protocol version 1.2）

IETF RFC 7540 超文本传输协议HTTP/2 （Hypertext transfer protocol(HTTP/2)）

IETF RFC 8446 TLS1.3 (The Transport Layer Security (TLS) Protocol Version 1.3)

3 术语和定义

本文件没有需要界定的术语和定义。

4 缩略语

下列缩略语适用于本文件。

CSS：层叠样式表（Cascading Style Sheets）

ECMA262：ECMAScript语言规范 （ECMAScript language specification）

HTML：超文本置标语言（HyperText Markup Language）

HTML5：超文本置标语言 （HyperText Markup Language 5）

NPAPI：网景插件应用程序接口（Netscape Plugin Application Programming Interface）

PPAPI：Google开发的运行于沙箱环境的应用程序插件接口（Pepper Plugin API）

SSL：安全套接层（Secure Sockets Layer）

TLS：传输层安全（Transport Layer Security）

WebGL：Web图形库

WebRTC：Web实时通信（Web Real-Time Communications）

XHTML：可扩展超文本置标语言（eXtensible HyperText Markup Language）

XML：可扩展置标语言（eXtensible Markup Language）

5 浏览器客户端

5.1 基本功能要求

企业级浏览器基本功能应符合以下要求：

a) 应提供符合计算机架构与操作系统版本的安装程序，安装过程无错误，可正常运行浏览器显示示页面无异常；

b) 应提供卸载程序，卸载程序可以完全清除安装与使用过程中配置的各项内容且卸载后无残留数据；

c) 显示功能：应支持屏幕适应、多窗口浏览显示、全屏模式、网页链接显示、文字显示、多媒体内容显示等功能；

d) 适老化：应支持调整页面比例与字体大小，并支持适老化、屏幕朗读相关的第三方插件、扩展；

e) 地址栏：应支持输入网址、地址栏自动补全、地址栏搜索、地址栏输入推荐、网站安全状态显示等功能；

f) 调整标签页位置，固定标签页，关闭标签页；

g) 书签功能：添加、编辑、移动、显示/隐藏书签栏、导入/导出书签、本地备份书签；

h) 下载管理：下载路径设置、多任务下载、删除下载项、下载显示及提示、下载文件，检查结果、查看下载项；

i) 上网痕迹清理：应按内容清除上网痕迹、按时间段清除、自动清除；

j) 打印支持：打印预览、浏览器支持打印为 PDF、支持连接至物理打印机并打印、支持快捷键调用打印；

k) 证书管理：应支持数字证书（RSA、国密）导入、导出、删除等常用功能；

l) 常用功能：浏览器启动关闭、窗口新建、窗口关闭、打开网页、网页保存、页面查找、页面导航、前进、后退操作、刷新操作、复制和粘贴；

m) 历史记录：查看用户访问历史记录，记录访问 URL 的时间与域名；

n) 查看网页源代码，查看 Web 前端代码内容，可以代码形式呈现；

o) 设置：主页管理、自定义启动页、代理管理、自动保存密码及填充；

p) 开发者工具，帮助开发者调试网页、查看源代码、检查网络请求等，具体内容包括但不限于：元素面板、控制台面板、源代码面板、网络请求面板、性能面板、内存面板等；

q) 插件管理：主流插件应支持-NPAPI 插件/PPAPI 插件、插件的独立启用/停用；

r) 流版签支持：可支持主流流版签插件，如 WPS、OFD 格式插件；

s) 旧技术兼容：均可支持 Java Applet 等插件；

t) 扩展支持：应支持扩展安装、删除、启用、禁用；

u) 代理服务器支持：应支持设置代理服务器，包括 http、https、Socks5 代理协议的支持，支持通过指定网址获取 PAC 规则。

5.2 兼容性要求

5.2.1 软件兼容性要求

企业级浏览器应兼容主流 web 相关技术，包括但不限于以下内容：

a) Web 标准兼容性：支持 W3C 发布的 Web 标准；
b) 传输协议标准：支持 HTTP/1.0、HTTP/1.1、HTTP/2、HTTPS、WebRTC 等，满足：IETF RFC 1945、IETF RFC 2616、IETF RFC 2109、IETF RFC 7540 等技术要求；
c) HTML 兼容性：支持 HTML 4.0.1 Strict、HTML 5、XHTML Basic 1.1，符合 GB/T 18792-2002 的要求；
d) CSS 兼容性：支持 CSS 2.1，CSS 3 层叠样式表支持度 60%以上；
e) JavaScript 兼容性：支持 ECMA-262、ECMAScript 5、ECMAScript 2015、ECMAScript 2016、ECMAScript 2017；
f) XML 兼容性：支持 XML 1.0 与 XML Namespaces；
g) 字体：支持调用系统字体库并可设置生效字体。

5.2.2 芯片兼容性要求

企业级浏览器应支持主流芯片的指令集，包括但不限于：ARM、MIPS、Loongarch、X86、SW64 等。

5.2.3 操作系统兼容性要求

企业级浏览器应支持主流操作系统，包括但不限于银河麒麟、统信、麒麟信安、Windows系列等。

5.3 安全可控要求

5.3.1 运行稳定性要求

企业级浏览器应具备硬件加速能力，提供运行态性能监测能力，包括但不限于：浏览器内核综合性能、浏览器图形综合性能、浏览器 WebGL 综合性能、浏览器页签性能、检测浏览器页签性能、浏览器启动时间等。

浏览器应无故障地执行网页渲染能力，呈现 Web 应用系统前端页面，在访问单一页签及同时启动多页签时应稳定渲染 web 前端网页，具备异常自动恢复能力。

5.3.2 安全性要求

企业级浏览器应通过密码技术保障敏感数据输入、本地数据存储和数据通信的安全性,包括信息的保密性、完整性和真实性。浏览器客户端安全能力包括但不限于：

a) 密码管理，用户访问 web 应用可保存登录的账号密码，并可通过管理平台配置是否允许保存；
b) DNS 安全，使用 DoH（https DNS）协议，在进行 DNS 查询时通过加密方式传送数据包，避免 DNS 解析中间人攻击；
c) 网址云安全，开启网址云安全检测功能，对用户访问 URL 进行安全检测，防止访问恶意网址；
d) 抗攻击能力，包括但不限于 XSS 跨站点脚本攻击、CSRF 跨站请求伪造攻击、中间人攻击；
e) 防调试，反跟踪，反编译能力；
f) 证书服务能力，包括但不限于打开有效的证书网站，页面正常显示；打开异常（过期、吊销）的证书网站，发出警告提示；应支持通过 OCSP 协议查询证书状态；
g) 浏览器通过危险下载链接进行下载时，弹出警告提示；
h) 网络协议安全，符合 IETF RFC 2818 、IETF RFC 5246、IETF RFC 8446、GM/T 0024-2023、GB/T 38636-2020 等技术要求；
i) 支持修复已公布的 CVE 漏洞；

j) 兼容商用密码算法和 RSA 算法，并支持配置网站优先使用商用密码算法；
k) 内置商用密码算法根证书和 RSA 算法根证书；
l) 本地数据加密，加密的数据范围包括但不限于浏览器客户端缓存、cookie、保存的密码。

5.3.3 可维护性要求

要求包括：

a) 企业级浏览器应支持在线升级和离线升级两种方式；支持全量升级和增量升级两种模式。升级后保持原用户设置和个人数据不变，应支持书签同步功能。
b) 应支持故障信息收集、上报功能，可支持本地导出，也可支持指定设备自动上报故障信息，并将上报的故障信息导出，便于问题快速定位解决。

6 浏览器管理平台

6.1 基本功能配置

6.1.1 基本配置

浏览器客户端基本配置应符合以下要求：

a) 内核兼容管理：按 URL 配置内核自动切换策略，支持配置针对子域名生效、禁止手动切换内核、禁止智能切核；URL 可支持有 path 路径的域名；
b) 弹出窗口管理：浏览器管理后台可阻止指定网站弹出窗口；
c) 资源替换：浏览器管理后台可上传文件对指定网站进行资源替换，快速修复网页中影响浏览的错误资源；
d) 内部专用域名管理：浏览器管理后台支持填写内部专用域名，客户端输入域名将直接访问，不调用搜索引擎进行搜索；
e) 代理服务器管理：浏览器管理后台支持添加代理服务器配置；
f) 扩展脚本接口管理：浏览器管理后台支持对第三方应用开放脚本接口，以实现获取浏览器 cookie、终端信息（终端名称、CPU 平台、CPU 名称、操作系统名称、MAC 地址、ip 地址）等数据；
g) 网站 UA 管理：浏览器管理后台支持对指定网站配置浏览器 UA；
h) 下载管理：浏览器管理后台支持对指定网站选择下载器；
i) 数据回调：支持多窗口间数据回调，如 showmodaldialog 回调函数。

6.1.2 组织架构及用户管理

企业组织管理方式支持按 IP 分组、用户分组和企业 LDAP/AD 域分组。

选择按 IP 分组管理，根据 IP 分组信息自动判断终端所属分组，浏览器客户端无需登录。

选择按用户分组管理，根据创建用户及分组来进行组织管理，浏览器客户端需要进行用户登录。

选择按 LDAP/AD 组织信息管理，根据 LDAP/AD 域组织信息来控制分组，浏览器客户端需要使用 LDAP/AD 域账号登录。

6.1.3 终端管理

按分组信息查看终端设备详细信息，按相关条件进行查询，包括但不限于：设备名、IP 地址、MAC 地址、登录用户、设备状态、客户端版本、所属组织等。

在设备列表中按设备在线离线、启用禁用或显示全部快速过滤终端设备，支持批量禁用启用，支持查看设备的具体信息如：操作系统、系统架构、CPU 品牌、客户端版本和最近活跃时间；应支持设

备列表导入导出功能。

6.1.4 消息管理

支持按分组推送消息通知，支持自定义消息有效期，消息内容支持包含网址链接。消息发至客户端后，客户端可查看消息状态，包含送达状态及阅读状态，支持查看历史消息记录，支持基于时间查询消息，支持消息删除。

6.1.5 安装升级管理

企业级浏览器管理平台提供安装包下载页面，支持管理员统一上传并发布浏览器客户端安装包。下载页面无需登录认证即可访问下载页面。通过下载页面获取的安装包，在安装后浏览器可自动连接管控中心。

多种架构浏览器客户端支持增量和全量升级两种模式，设置签名校验，限制最大并发数和限速，客户端下载页面自定义，升级指定客户端版本，查看客户端版本使用情况。

6.1.6 日志管理

企业级浏览器管理平台应支持留存管理员操作和系统运行日志，并支持日志自动清理，支持设定日志存储时长，支持日志转发。

6.1.7 可视化检测

应支持浏览器终端设备的运行状态查看，统计在线设备情况和版本分布情况，进行可视化管理。

6.2 安全可控配置

6.2.1 环境监测

企业级浏览器管理平台应支持监测、采集浏览器客户端环境信息与性能数据。客户端环境信息包括但不限于芯片信息、操作系统信息、网络连接信息、环境风险信息等。浏览器性能数据包括但不限于网络性能、页签打开性能等。

6.2.2 安全配置

企业级浏览器管理平台具备客户端访问应用权限控制，应符合以下要求：

a) 个性化水印：对选定范围的用户下发自定义格式与内容的水印；
b) 禁止打印：禁止指定范围用户在浏览器内进行打印操作；
c) 禁止复制：禁止指定范围用户在浏览器内进行复制操作；
d) 禁止鼠标右键：禁止指定范围用户在浏览器内通过在页面单击鼠标右键打开选项；
e) 禁止截屏：在操作系统支持的前提下，禁止指定范围用户截取浏览器屏幕所显示的内容；
f) 禁止保存网页：禁止指定范围用户下载或保存网页内容；
g) 禁用开发者工具：禁止指定范围用户使用开发者工具；
h) 禁止查看源文件：禁止指定范围用户查看网页源文件；
i) 禁用地址栏：禁止指定范围用户通过浏览器上方的地址栏访问其他网页；
j) 禁止下载：禁止指定范围用户在浏览器内下载来自页面的文件；
k) 禁止上传：禁止指定范围用户通过浏览器上传文件至页面；
l) 禁止截屏：在操作系统支持的前提下，禁止指定范围用户对所浏览页面进行截屏；
m) 传访问历史记录：浏览器客户端将用户访问历史记录上传至浏览器管理平台进行统一管理，支持对访问历史记录的查询导出；

n) 上网痕迹清除：浏览器管理平台可配置客户端的上网痕迹清除策略，可配置其清理内容、清理时间等；
o) 开启 URL 访问控制：浏览器管理平台可限制终端用户可访问的 URL，支持黑白名单两种模式；
p) 上传文件查毒：浏览器管理平台可开启浏览器客户端上传文件查毒功能；
q) 信任网站管理：浏览器管理平台应支持将指定网站设置为信任网站，在客户端访问时将默认此网站安全；
r) 国密优先管理：浏览器管理平台支持将指定网站设置为国密优先网站，在客户端进行访问时优先建立国密 SSL 连接；
s) 非国密优先管理：浏览器管理平台支持将指定网站设置为非国密网站；在客户端进行访问时不采用国密 SSL 连接；
t) 插件扩展部署及管理：浏览器管理平台支持对插件和扩展统一下发至客户端；支持对终端用户所使用的插件和扩展进行限制；支持按组织架构下发插件与扩展，并支持设定访问指定网站时自动安装扩展；
u) 可信外链管理：浏览器管理平台支持将指定外链协议设置为可信外链。若某协议处于可信外链列表，浏览器客户端将允许此协议直接调用本地应用程序，无需获取用户许可；
v) 证书管理：浏览器管理平台支持手动添加国密和 RSA 类型的证书，并进行统一下发，实现证书信任。

7 应用要求

7.1 应用场景

企业级浏览器应对企业单位典型应用场景提供定制化能力，典型场景包括：企业级办公、生产调度业务、工控平台、IM 工作台集成等。

7.2 通用要求

应符合以下要求：

a) 第三方组件：企业级浏览器可支持按需集成第三方组件，如流版签插件、公文加密插件、外设调用插件等；
b) 配置管理要求：企业级浏览器管理平台应具备应用服务访问地址配置管理能力，包括但不限于 web 应用访问地址、浏览器下载地址、第三方组件下载地址、隐私政策访问地址等。配置管理项和配置策略应支持实时添加、修改和删除以及生效时间。

7.3 场景要求

应符合以下要求：

a) IM 工作台集成：支持定制浏览器 WebAPP 模式，与 IM 工作台集成，工作台调用浏览器窗口，显示工作台中应用系统数据；
b) 工控平台集成：支持跨平台框架能力支持，定制为应用系统的专属客户端；
c) 桌面应用集成：支持定制浏览器，与桌面应用集成，提供相关API接口进行位置、窗口大小、内容自定义等功能。

8 Web 应用访问质量数据管理

8.1 概述

企业单位基于企业级浏览器对业务应用服务质量进行实时监测与分析，直观呈现从终端到 web 应用完整访问数据的质量，实现应用性能和异常状态的高效可视化管理，采集与分析数据应支持以下内容。

8.2 基础数据：

企业级浏览器采集并上报的基础数据包含：操作系统版本号、浏览器版本号、 终端架构、mac 地址、计算机名、用户名等基础数据；管理平台将数据数据与各维度数据结合，并交叉分析，呈现 Web 应用系统访问质量情况。

8.3 访问性能数据

企业级浏览器采集并上报的数据应包含: 采集的 PV 数，页面完全加载时间、首字节时间，记录 DNS、TCP、SSL、请求响应、内容传输、DOM 解析、DOM Ready、资源加载、首屏绘制、首屏内容绘制、可交互时间、最大内容绘制、首次有效绘制、总下载字节数、下载 header 大小、请求大小、上传大小、上传速度、传输耗时、重定向时间、总下载时间、下载速度、文件大小、完全载入的性能平均值等性能数据；管理平台进行用户访问性能数据分析，呈现访问性能态势。

8.4 报错数据

企业级浏览器采集并上报的数据应包含：在用户访问该应用时获取 HTTP 响应状态码，状态码为 4xx、5xx 时视为应用报错，并采集上报具体脚本报错数据内容；管理平台针对报错数据实时统计与分析，并针对报错提供告警能力。

8.5 实用化数据

企业级浏览器采集并上报的数据应包含：页面访问的流量、内容访问的点击量和点击率、操作次数、ajax 回调时间、慢网络次数、慢事务次数、慢请求次数、请求次数、传输数据大小、服务端响应时间、响应时间、文档类型、认证结果等实用性数据；管理平台及时对实用数据处理，按照模型分析。

8.6 健壮性数据

企业级浏览器采集并上报的数据应包含：前端错误数、前端告警数、前端日志数、前端错误率、ajax错误次数、最近一次响应码、最近新建连接数、重定向次数、重定向URL等健壮性数据；管理平台及时对健壮性数据整理，按照模型分析。

参 考 文 献

[1] GB/T 13000-2010 信息技术 通用多八位编码字符集（UCS）
[2] GB 18030-2022 信息技术 中文编码字符集
[3] GB/T 25069-2023 信息安全技术 术语