ICS 35.020
L 70

团　　体　　标　　准

X/XXXXX XXX-XXXX

国产化浏览器技术规范

Technical specifications for localized browsers

（征求意见稿）

2024-XX-XX 发布　　2024-XX-XX 实施

XXXXXXXXX　　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。

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管理。

本文件起草单位：XXXX…。

本文件主要起草人：XXXX。

国产化浏览器技术规范

1 范围

本文件规定了国产化浏览器在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域场景下功能、性能、兼容性、易用性、可靠性、安全性、可维护性、可移植性等方面要求。

本文件适用于国产化浏览器技术规范。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 25069 信息安全技术 术语

GB/T 13000-2010 信息技术 通用多八位编码字符集（UCS）

GB 18030-2005 信息技术 中文编码字符集

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）

CSS 2.1/3.0（W3C） 层叠样式表 （Cascading style sheets）

XHTML（W3C） 可扩展超文本置标语言 (eXtensible hypertext markup language)

HTML 5（W3C） 超文本置标语言 （Hypertext markup language）

ECMA 262 ECMAScript 语言规范 （ECMAScript language specification）

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 4287 原子整合格式 （The atom syndication format）

IETFRFC 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

下列术语和定义适用于本文件。

3.1

浏览器 browser

能够显示网页服务器文档和资源的内容，并可以让用户与这些文档和资源进行交互的一种软件。

3.2

缓存 cache

用于保存用户访问过的网页，以便在用户再次访问该网页时，可以直接从终端的本地存储器中读取该网页。

4 基本要求

4.1 浏览器客户端

4.1.1 概述

为满足电力行业国产化浏览器使用要求，国产化浏览器应满足以下基本功能。

4.1.2 基本功能要求

国产化浏览器基本功能包括浏览器一些常用功能如浏览器启动与关闭、窗口的新建、关闭、打开网页等功能。

a) 应提供符合所用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页面无异常；
b) 浏览器应提供卸载程序，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：桌面端浏览器应支持屏幕适应、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：针对适老化，浏览器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：桌面端浏览器应支持输入网址、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；
g) 固定标签页；
h) 关闭标签页；
i) 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；
j) 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；
k) 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；
l) 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；
m) 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；
n) 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；
o) 历史记录；
p) 查看网页源代码；
q) 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；
r) 开发者工具支持；
s) 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；
t) 流版签支持：可支持主流流版签插件，如 WPS、OFD 格式插件；

u) 旧技术兼容：均可支持 Java Applet 等插件；
v) 扩展支持：应支持扩展安装、删除、启用、禁用；
w) 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。

4.1.3 软件兼容性要求

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

4.1.4 芯片兼容性要求

国产化浏览器应支持主流芯片的主流指令集，包括但不限于 ARM、MIPS、Loongarch、X86。

4.1.5 运行稳定性要求

国产化浏览器应具备硬件加速能力，并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指定功能，在访问单一页签及同时启动多页签时应具备稳定性，且具备异常自动恢复能力。

4.1.6 安全可靠性要求

国产化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；
b) 恶意网页拦截；
c) DNS 安全；
d) 网址云安全；
e) 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；
f) 防调试，反跟踪，反编译能力；
g) 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；
h) 浏览器通过危险下载链接进行下载时，弹出警告提示；
i) 网络协议安全，支持 IETF RFC 2660 HTTPS、IETF RFC 5246 TLS 1.2、IETF RFC 8446 TLS1.3、GM/T 0024-2014 SSL VPN、GB/T 38636-2020 信息安全技术 传输层密码协议（TLCP）等安全协议；
j) 支持修复已公布的 CVE 漏洞；
k) 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；
l) 内置商用密码算法根证书和 RSA 算法根证书；
m) 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。

4.1.7 可维护性要求

a) 国产化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。升级后的浏览器应保持原用户设置和个人数据不变。
b) 国产化浏览器应支持书签同步功能。
c) 国产化浏览器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。

4.2 浏览器服务端功能

4.2.1 客户端环境监测

国产化浏览器管理后台应支持监测、采集浏览器客户端环境信息、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。

4.2.2 客户端安全配置

国产化浏览器管理后台应具备对网址设置使用权限，设置项包括但不限于：

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) 上传访问历史记录：浏览器客户端将终端用户的访问历史记录上传至浏览器管理后台进行统一管理，支持对访问历史记录的查询导出；
n) 上网痕迹清除：浏览器管理后台可配置终端用户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：浏览器管理后台可限制终端用户通过浏览器可访问的 URL；
p) 上传文件查毒：浏览器管理后台可开启对浏览器客户端上传文件的查毒功能；
q) 信任网站管理：浏览器管理后台支持将指定网站设置为信任网站，在客户端进行访问时将默认此网站安全；
r) 国密优先及非国密网站管理：浏览器管理后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；浏览器管理后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；
s) 插件扩展部署及管理：浏览器管理后台支持对插件和扩展统一下发至客户端；浏览器管理后台支持对终端用户所使用的插件和扩展进行限制；浏览器管理后台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；
t) 可信外链管理：浏览器管理后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；

u) 证书管理：浏览器管理后台支持手动添加国密和 RSA 类型的证书。

4.2.3 客户端其他配置

国产化浏览器管理后台应具备根据网址配置兼容性、客户体验等策略，包括但不限于：

a) 弹出窗口管理：浏览器管理后台可阻止指定网站弹出窗口；
b) 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；
c) 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；
d) 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；
e) 扩展 JS 接口管理：浏览器管理后台支持对第三方应用开放 JS 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；
f) 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；
g) 下载管理：浏览器管理后台支持对指定网站选择下载器；
h) 数据回调：支持多窗口间数据回调，如 showmodaldialog 回调函数。

4.2.4 企业级配置管理

国产化浏览器管理后台在企业级应用场景应具备终端、人员及网址的身份认证和访问控制能力，包括但不限于：

4.2.4.1 组织架构及用户管理

a) 新建用户；
b) 移动用户分组；
c) 用户筛选；
d) 禁用用户；
e) 导入用户；
f) 导出用户；
g) 编辑用户；
h) 删除用户；
i) 从 LDAP 同步分组与用户；
j) 从 AD 同步分组与用户；
k) 接入 LDAP 用户认证；
l) 接入 AD 用户认证。

4.2.4.2 终端管理

a) 新建分组；
b) 编辑分组名称；
c) 删除分组；
d) 导入分组；
e) 手动添加设备；
f) 移动设备；
g) 禁用设备；
h) 查看设备详情；
i) 设备筛选；

j) 设备查询；
k) 设备删除；
l) 导出设备。

4.2.4.3 消息管理

a) 支持消息内容设置，如消息标题、内容；
b) 按分组下发消息；
c) 支持设定消息发布起始时间；
d) 终端支持消息查看；
e) 支持查看消息终端送达率。

4.2.4.4 安装升级管理

a) 多平台多操作系统安装包管理；
b) 指定范围升级；
c) 最大并发数控制；
d) 最大速度控制；
e) 安装包验签；
f) 全量升级；
g) 增量升级；
h) 升级完成率监控；
i) 升级完成终端数监控；
j) 未完成升级终端查询及导出；
k) 升级策略启停；
l) 多策略升级；
m) 指定原版本与目标版本升级。

4.2.4.5 后台日志管理

国产化浏览器管理后台应支持留存管理员操作日志和系统运行日志。并支持日志自动清理，支持设定日志存储时长。

4.2.4.6 可视化

实时检测浏览器终端设备的运行状态，并进行可视化管理。

5 应用要求

国产化浏览器应对电力行业典型应用场景提供良好支持，典型场景包括：柜面运营、企业级办公。国产化浏览器应满足应用场景所需通用要求与场景要求。

通用要求具体如下：

a) 第三方组件：国产化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：国产化浏览器管理后台应具备应用服务访问地址配置管理能力，包括但不限于业务系统访问地址、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。