ICS 35.240.99
L 67

ZWFW

国家政务服务平台标准

C 0112-2018

国家政务服务平台
统一身份认证系统信任传递要求

2018-10-09 发布　　2018-10-09 实施

国务院办公厅电子政务办公室 发布

目　次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由国务院办公厅电子政务办公室提出并归口。

本标准起草单位：国务院办公厅电子政务办公室、浙江省人民政府办公厅、广东省人民政府办公厅、江西省人民政府办公厅、四川省人民政府办公厅、南京市政务服务管理办公室、中国电子技术标准化研究院。

本标准主要起草人：卢向东、尹智刚、马运领、王齐春、陈治佳、魏春江、徐云、李景曦、王赟萃、李松渊、孙杨、张军、钱学文、李恒训、王立建、陈亚军。

国家政务服务平台统一身份认证系统信任传递要求

1 范围

本标准规定了国家政务服务平台统一身份认证系统信任传递、跨节点认证与信任传递流程、安全要求。

本标准适用于国家政务服务平台统一身份认证系统国家节点、地方和部门节点。

2 规范性引用文件

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

C 0110-2018 国家政务服务平台统一身份认证系统接入要求

C 0111-2018 国家政务服务平台统一身份认证系统身份认证技术要求

3 统一身份认证系统信任传递

统一身份认证系统，包括国家节点、地方和部门节点，地方和部门节点统一接入国家统一身份认证系统，实现跨节点访问。

以国家节点作为信任传递枢纽，通过传递统一令牌，地方和部门节点本地令牌、统一令牌映射，统一规范化用户实名等级和认证编码，规范同一用户的识别标准，规范信息传递通道，使用成熟的单点登录方法、协议、流程，实现同一账号的“一地登录，各地互认”。

采用统一令牌作为信任传递的公共令牌，地方和部门节点只信任统一令牌，相互信任通过统一令牌完成。地方和部门节点维护本地令牌、统一令牌的映射关系，国家节点维护统一令牌以及地方和部门节点请求统一令牌的记录等，国家节点不维护保存地方和部门节点的令牌以及映射关系。为了安全传递令牌，采用票据令牌方式传递，即下发一次性票据，在票据有效时间内（如 15s），用票据申请获得令牌。票据可作为数据参数传递。主要流程见第 4 章。

令牌的数据模型和信息内容约定见计划中的《国家政务服务平台统一信任服务平台接口要求》。

4 跨节点认证与信任传递流程

4.1 用户信息查询和推送

4.1.1 用户信息查询

用户信息查询见图1。

图 1 用户信息查询流程示意图

用户在地方和部门节点登录时，地方和部门没有该用户信息，使用国家节点提供的用户信息查询接口 UserResult getUserInfo(UserRequest request)，获取用户信息。

4.1.2 地方和部门节点推送用户信息

地方和部门节点推送用户信息见图 2。

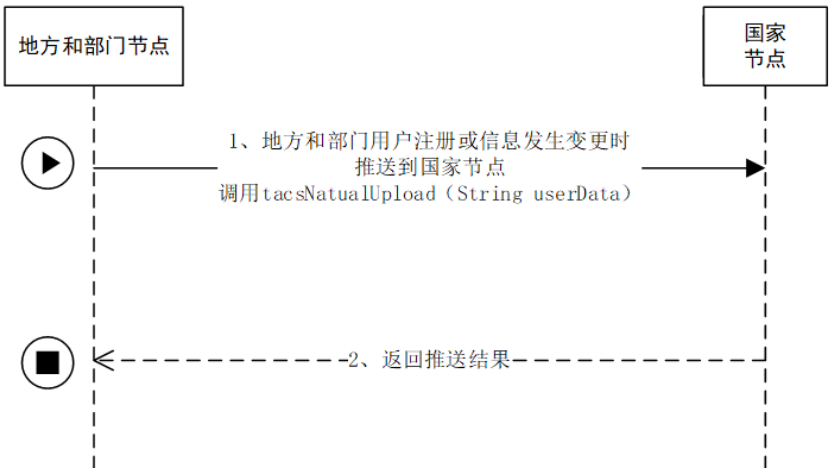

图 2 地方和部门节点推送用户信息流程示意图

地方和部门节点注册或用户信息变更后，调用 tacsNatualUpload 将地方和部门注册的自然人用户信息同步到国家节点。国家节点按冲突处理原则处理用户数据。

4.2 登录并建立统一令牌

4.2.1 使用国家节点账号登录

使用国家节点账号登录过程如下：

a) 在节点 A 用国家节点账号入口登录；
b) 国家节点登录成功，创建统一令牌。

4.2.2 使用地方和部门节点账号登录并隐性登录

使用地方和部门节点账号登录流程见图 3。

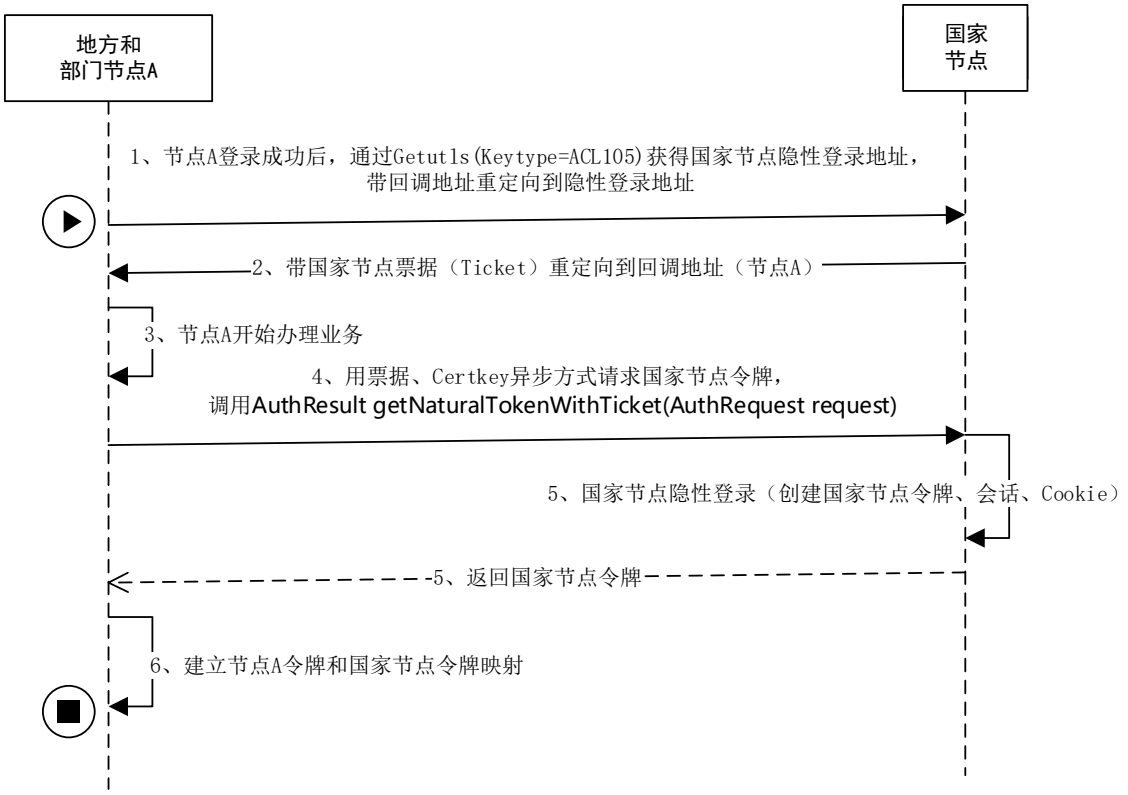

图 3 使用地方和部门节点账号登录流程示意图

上述流程如下：

a) 在地方和部门节点 A 用节点 A 的账号登录；
b) 登录成功，节点 A 通过 GetUrls(keyt)获得国家节点隐性登录地址，带回调地址和 Certkey（用户标识的散列值）重定向到国家节点进行隐性登录；
c) 在国家节点进行隐性登录，节点 A 开始办理业务，生成国家节点统一令牌；
d) 带国家节点票据重定向到节点 A,节点 A 使用票据获取统一令牌(调用 AuthResult)，建立映射，节点 A 登录。

4.3 跨节点访问

跨节点认证时，采用星型连接结构。按国家节点为枢纽传递令牌，地方和部门节点使用国家节点的令牌进行跨节点身份互认。

按 C0110-2018 第 6 章要求，地方和部门节点登录界面要有地方和部门账号登录入口和国家节点账号登录入口。

4.3.1 使用国家节点账号登录进行跨节点访问

使用国家节点账号进行跨节点登录流程见图 4。

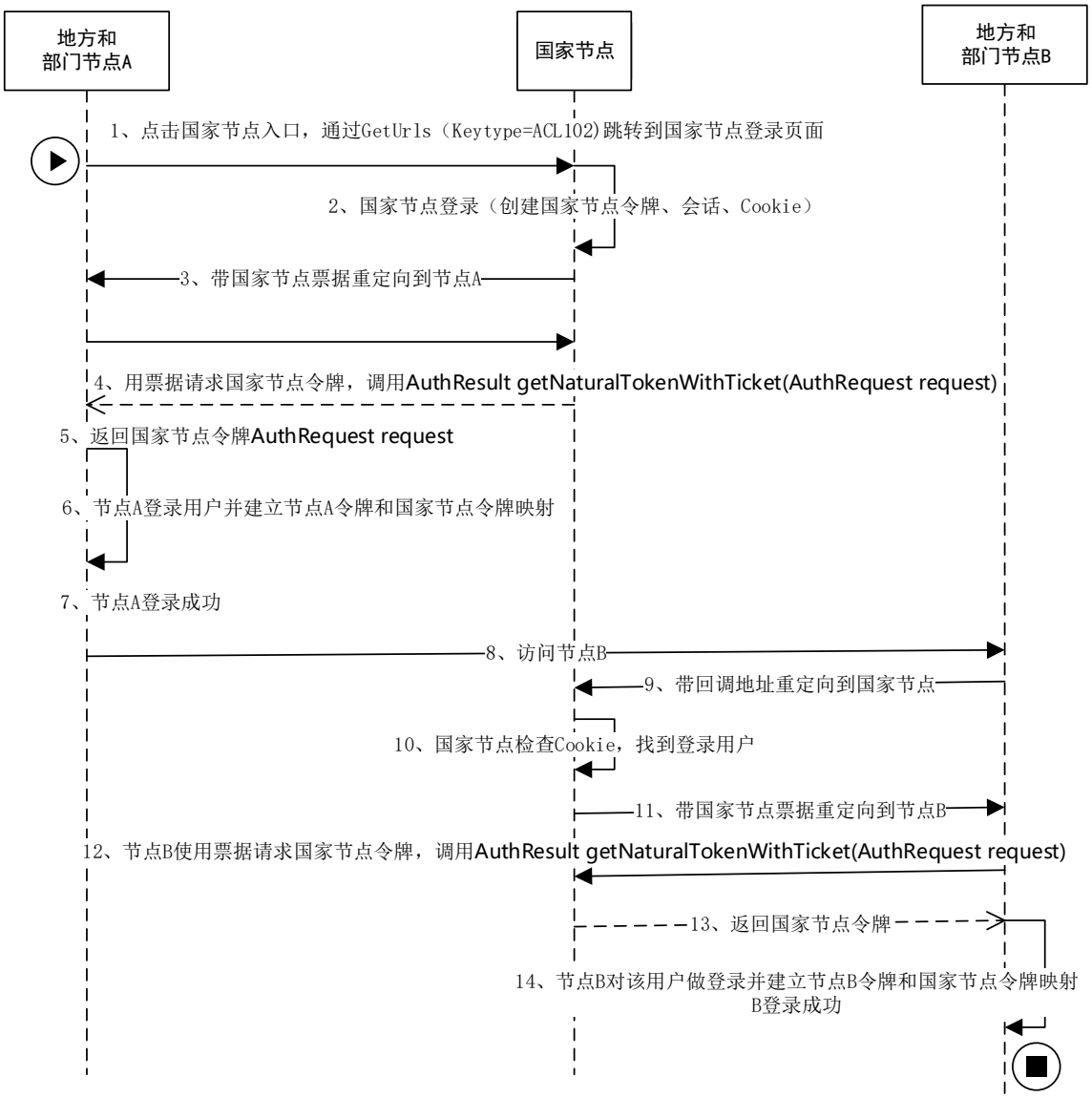

图 4 使用国家节点账号进行跨节点登录流程示意图

上述流程如下：

a) 在节点 A 国家节点账号入口用国家节点账号登录；

b) 登录成功，国家节点创建统一令牌，带一次性票据重定向到节点 A，节点 A 使用票据获取国家节点令牌（调用 AuthResult），建立令牌映射，自动登录该用户，节点 A 登录成功；

c) 同一浏览器访问节点 B，节点 B 带回调地址重定向到国家节点；

d) 国家节点检查已经有用户会话和 Cookie，带票据重定向到节点 B；

e) 节点 B 用票据获取统一令牌（调用 AuthResult），自动在本地登录用户，建立映射，跨节点登录 B 成功。

4.3.2 使用地方和部门节点账号跨节点访问

使用地方和部门节点账号跨节点访问流程见图 5。

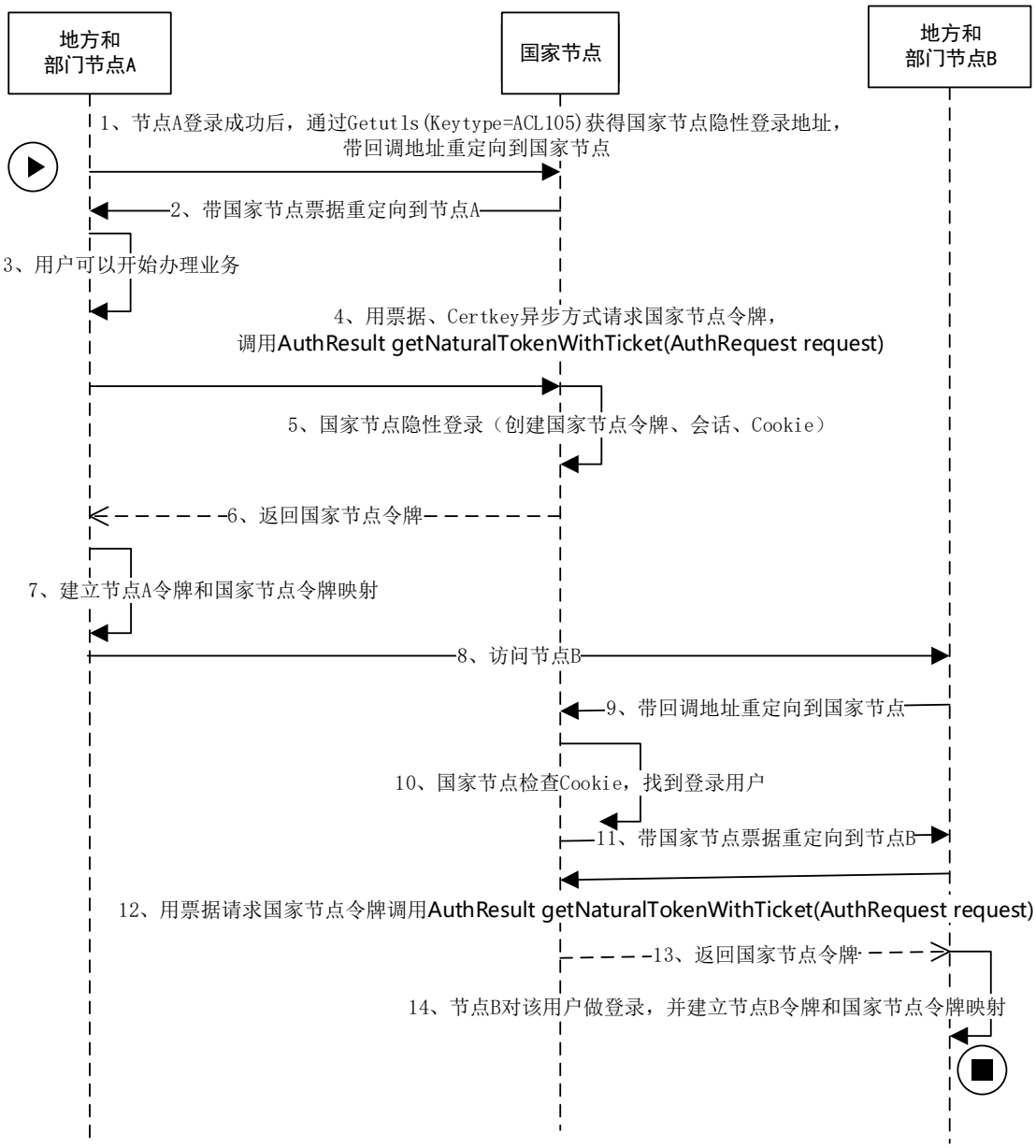

图 5 使用地方和部门节点账号跨节点登录流程示意图

上述流程如下：

a) 在节点 A 用地方和部门账号登录；

b) 登录成功，节点 A 通过 GetUrls 获得国家节点隐性登录地址，带回调地址和 Certkey（用户标识的散列值）重定向到国家节点进行隐性登录；

c) 在国家节点进行隐性登录，生成国家节点令牌；

d) 带国家节点票据重定向到节点 A,节点 A 使用票据获取统一令牌(调用 AuthResult)，建立映射，节点 A 登录；访问节点 B，B 带回调地址重定向到国家节点；

e) 国家节点检查已经有用户会话和 Cookie，带票据重定向到节点 B；

f) 节点 B 用票据获取令牌，自动登录用户，建立映射，节点 B 登录成功。

4.4 登出

4.4.1 地方和部门节点登出

地方和部门节点登出流程见图 6。

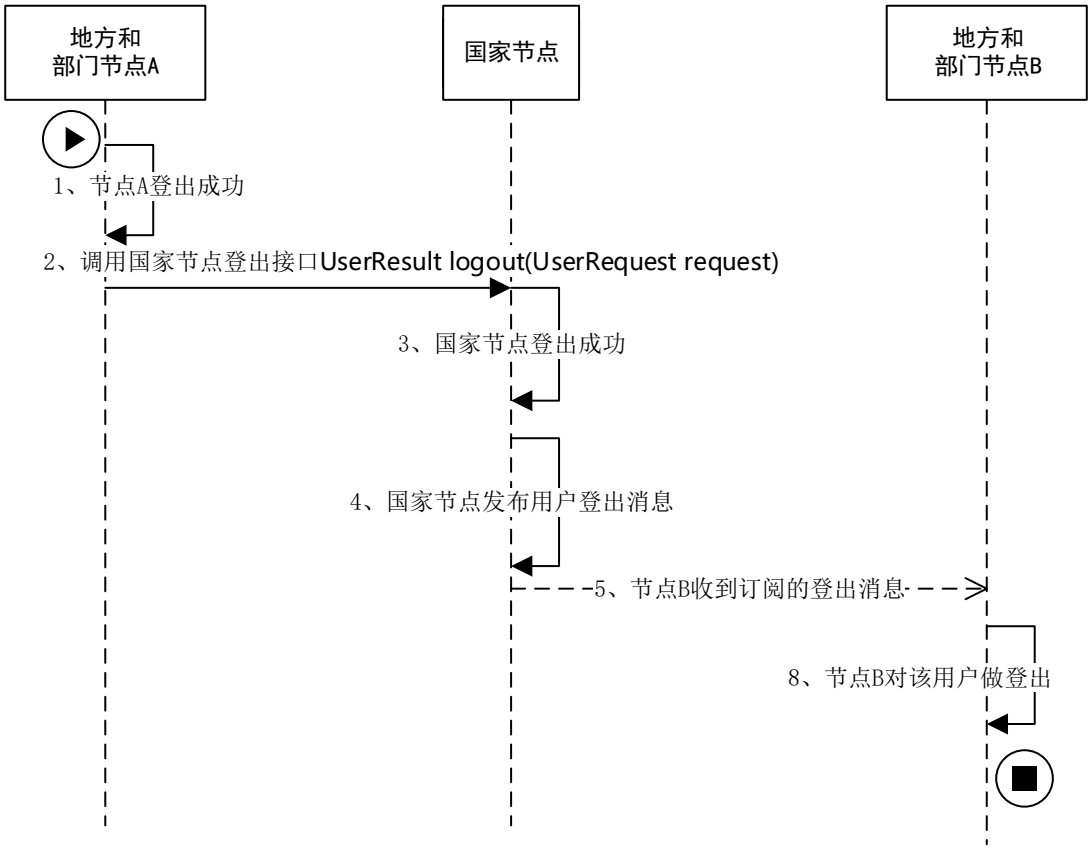

图 6 地方和部门节点登出流程示意图

上述流程如下：

a) 本流程只适用于跨节点访问的用户，未跨节点访问的用户在地方和部门原节点登出即可。用户在节点 A 进行登出操作，节点 A 注销会话，登出用户；

b) 节点 A 请求国家节点登出服务，由国家节点注销当前登录会话，并发布该用户登出消息；

c) 跨节点访问节点 B，节点 B 会收到国家节点登出消息，节点 B 对该用户做登出。

4.4.2 国家节点登出

国家节点登出流程见图 7。

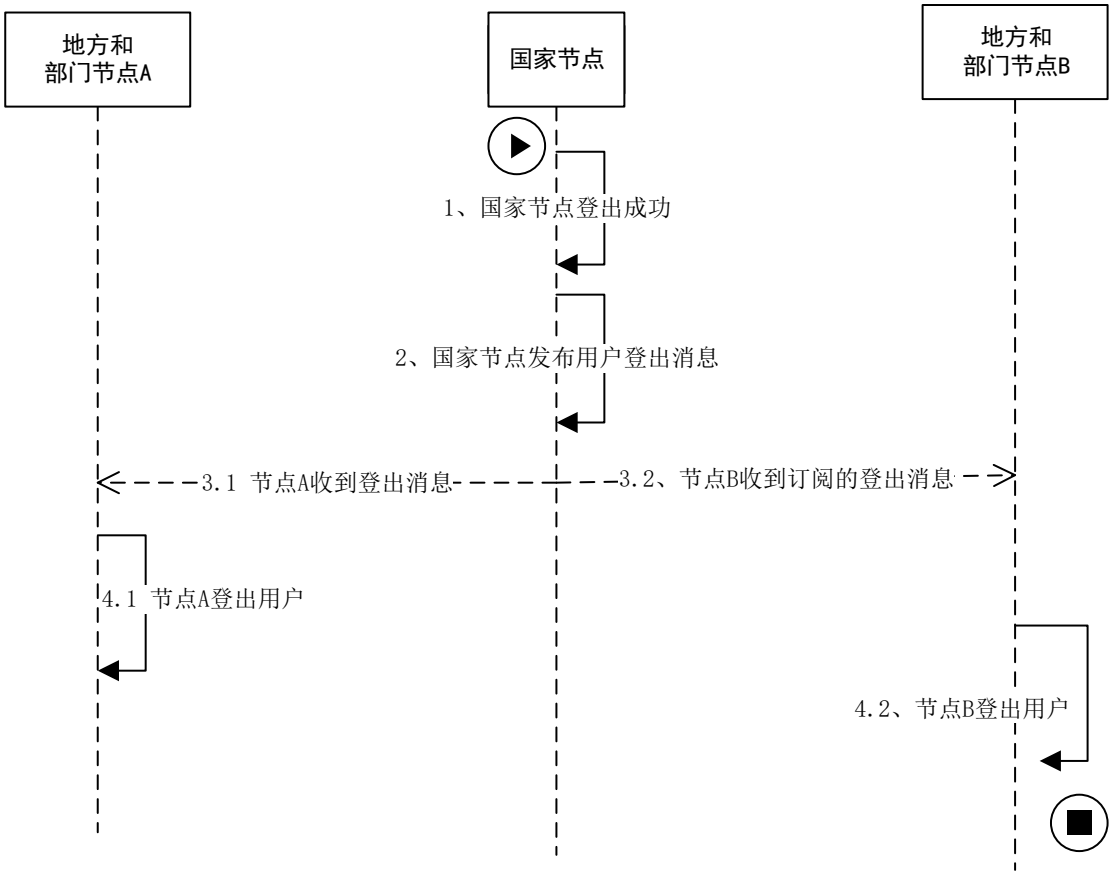

图 7 国家节点登出流程示意图

上述流程如下：

a) 用户请求国家节点登出，国家节点登出，并发布该用户登出消息；

b) 订阅消息的地方和部门节点 A、节点 B 接收到该用户登出消息，在本节点登出；

c) 登出接口见计划中的《国家政务服务平台统一信任服务平台接口要求》。

4.5 令牌延期

令牌延期流程见图 8。

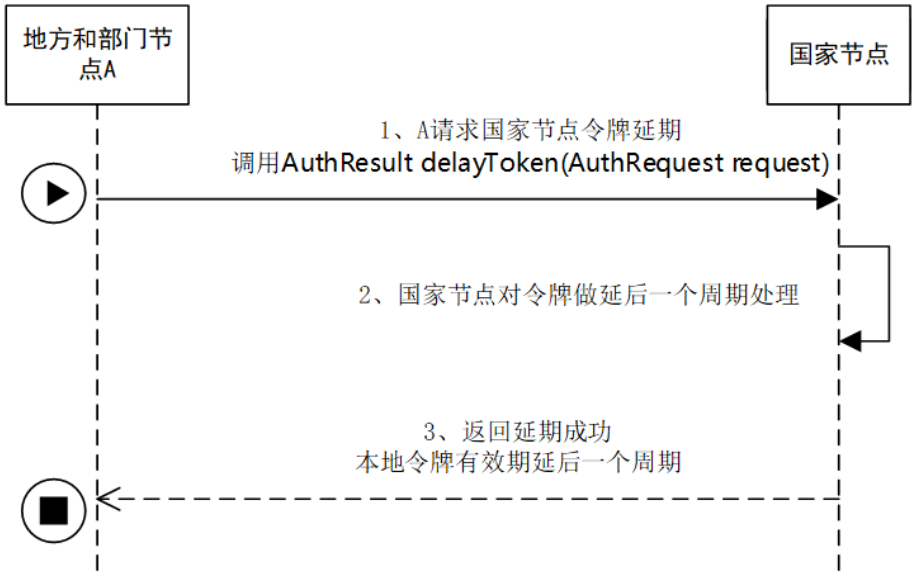

图 8 令牌延期流程示意图

节点 A 向国家节点请求统一令牌延期（调用 AuthResult delayToken，国家节点检查令牌有效，对令牌延后一个周期，返回节点 A 延期成功，节点 A 进行本地令牌延期。

5 安全要求

地方和部门节点应按 C0111-2018 第 8 章、计划中的《国家政务服务平台统一身份认证隐私保护要求》安全要求，完成系统安全防护和数据安全保护。

地方和部门节点应按 C0111-2018 第 8 章、计划中的《国家政务服务平台统一信任服务平台接口要求》安全要求进行通讯。