关于第三方认证与管理对接技术方案

会议时间：2024 年 1 月 10 日 10:50
参与人员：中心领导：竺欣平、刘志勇　　架构部：志福、超人、国锋、喻秀

需求背景

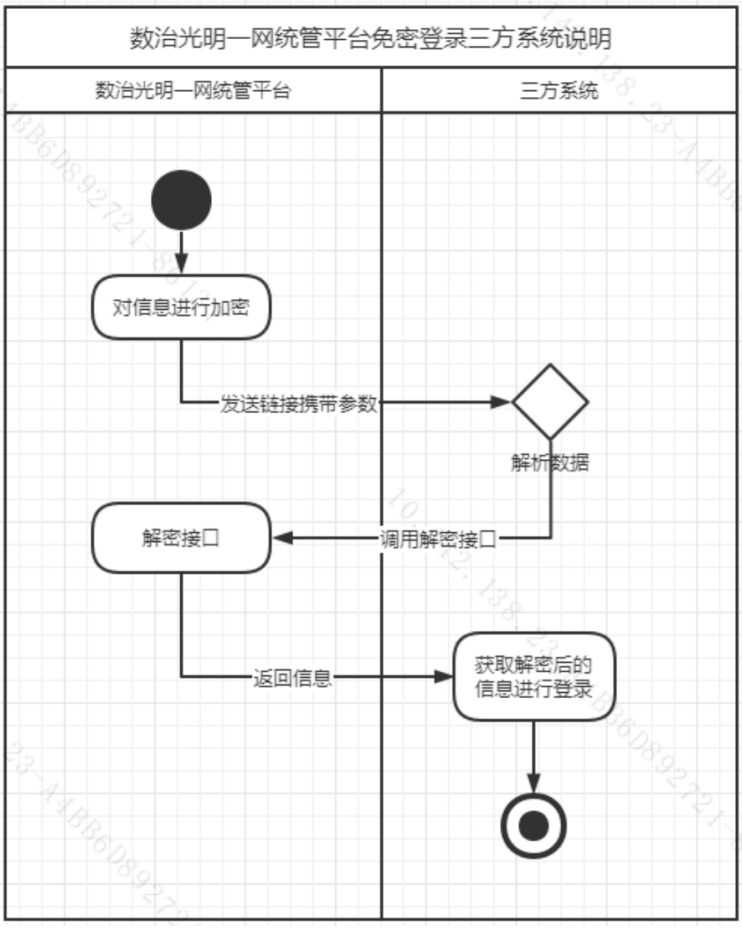
为了满足第三方（不限于光明一网通免密登录、云南数字体育统一认证）等等第三方管理平台来授权登录我方应用系统。

需求说明

我们先来对比一下上述第三方的接口要求与认证流程，以便提取公共点与业务设计。

1. 光明一网通接入要求

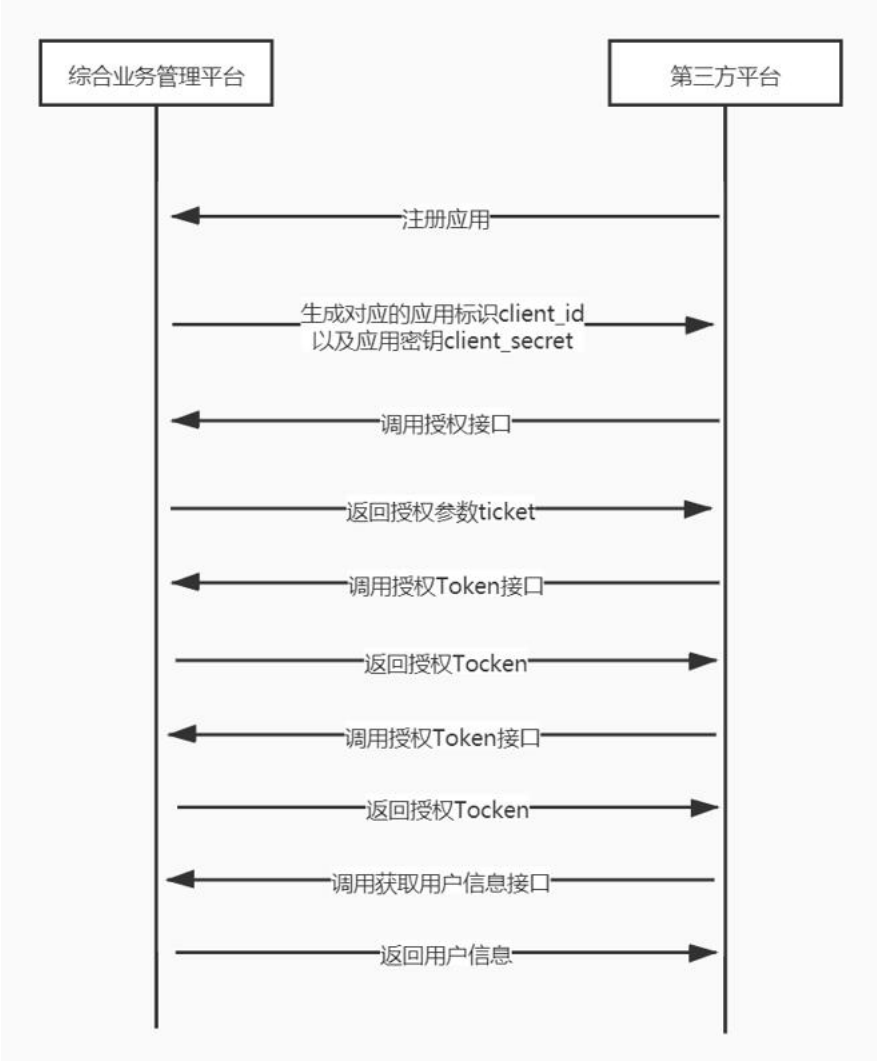
ps：携带链接的参数为第三方提供，我方在该链接的基础上传递三个参数，比如：
http://ip+端口/xxx?digest=${digest}&Authorization=${Authorization}&data=${data}



2. 云南数字体育认证接入要求

ps：第三方提交业务系统 URL 地址，在云南数字体育统一身份认证平台进行注册操作，注册后会生成对应的应用标识 client_id 以及应用密钥 client_secret 进行配置。

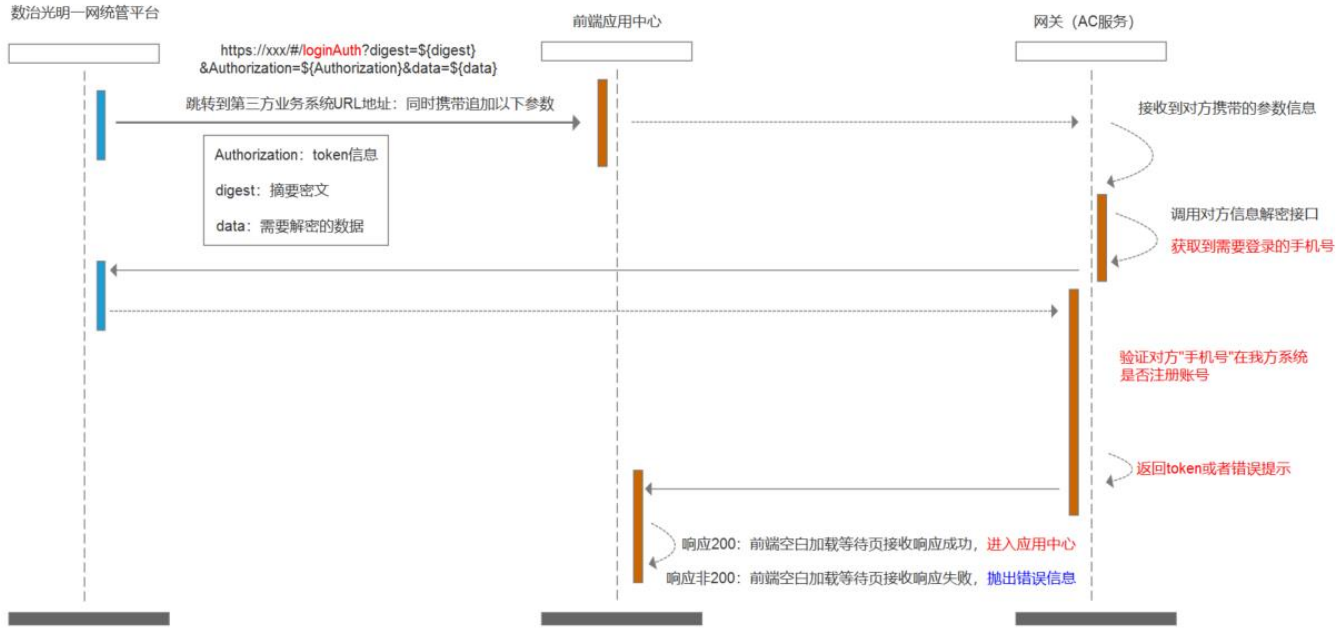
- 请求用户授权接口返回值：重定向到业务系统 URL 地址的页面，并携带认证参数 ticket
- 通过认证参数 tocket 与业务系统 url 地址获取授权 token
- 通过 token 获取用户信息



业务设计

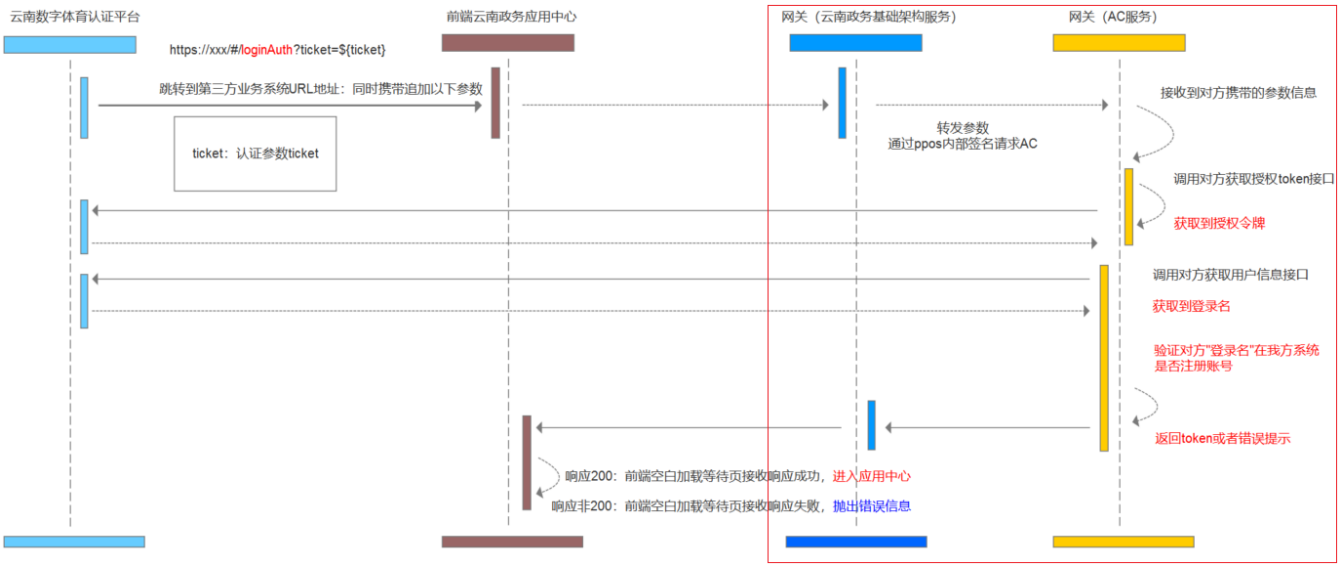
通过上述的概括表达应该大体清楚了第三方的授权调用方式，都是采取跳转到业务域名之后再做响应的授权操作，我们只要对接不同的授权规则即可。

1. 光明一网通接入时序图



“光明数字标识平台”免密登录三方系统

2. 云南数字体育接入时序图



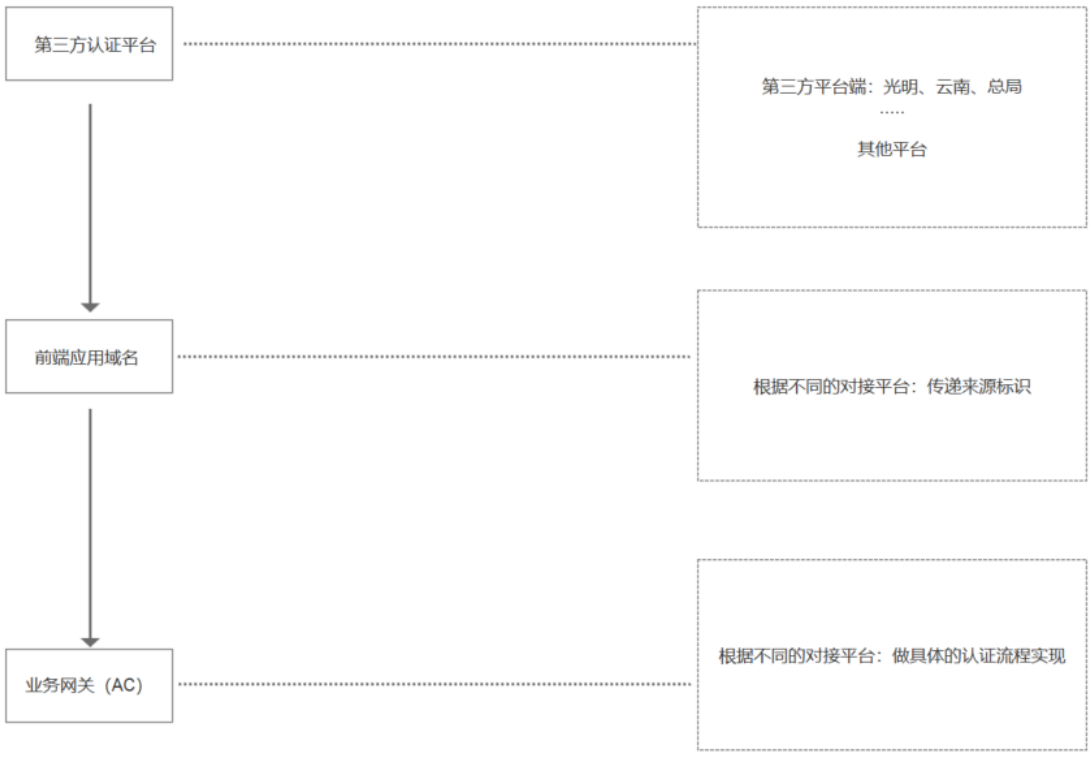
云南数字体育一期统一身份认证平台

综合上述：

不论是对接现在的光明、还是云南的登录认证流程，还是未来的总局对接等等第三方授权，我们可以就以下几点来实现：

1. 提供我方应用的前端域名给第三方，用于第三方跳转登录使用。
2. 前端将具体的应用授权情况(追加 get 参数)告知后端接口，例如参数：type=gm、yn 等标识。
3. 核心认证流程在 AC 服务中，用于对接第三方的授权（获取手机号、登录名），验证该账号是否存在等等。
4. 如果存在则返回我方应用的 token。
5. 我方其他业务系统根据具体情况再对该 token 做相应的调整即可。

业务流程图



其他

对请求方的日志记录、获得免密令牌标记、系统安全防护等措施。