

eduroam@CERNET 承诺书

我单位_____自愿申请通过中国教育科研网加入全球 eduroam 网络，并承诺遵守以下规定。

1. eduroam IdP 的管理和技术承诺

- 1.1. Eduroam 身份提供者 (Eduroam Identity Provider, IdP) 负责管理用户身份、运行认证服务器，也称之为“身份所在学校”(Home Institutions);
- 1.2. eduroam IdP 承诺实现 RADIUS 接口来连接 eduroam 路由框架;
- 1.3. eduroam IdP 承诺对所有的本地用户实现同一种 EAP 方法;
- 1.4. 当收到认证请求的时候，eduroam IdP 对于认证为有效的本地用户必须发送 RADIUS 通过消息 (accept message); 对于本地认证不通过的用户 eduroam IdP 一定不能发送 RADIUS 通过消息 (accept message);
- 1.5. eduroam IdP 承诺提供用户管理和用户支持;
- 1.6. eduroam IdP 承诺记录所有的认证请求，至少要记录以下信息：认证请求和相应应答的时间戳、认证请求中的 outer EAP id (用户名属性 User-Name attribute)、Inner EAP id (实际用户 id, actual user identifier)、客户端 MAC 地址 (Calling-Station-Id 属性)、认证应答的类型 (通过或拒绝, accept or reject)。日志最少保留 6 个月。

2. eduroam SP 的管理和技术承诺

- 2.1. eduroam 服务提供者 (eduroam Service Provider, SP) 运行可支持 eduroam 用户访问的接入网络，一旦用户在他们自己的 IdP 认证通过，即可以通过 SP 接入 Internet。也称之为“被访学校”(Visited Institutions);
- 2.2. eduroam SP 网络必须实现 802.1X 和 RADIUS 接口来接入 eduroam 框架，承诺转发过程不修改 EAP 包;
- 2.3. eduroam SP IEEE802.11 无线网必须广播 SSID “eduroam”;
- 2.4. eduroam SP IEEE802.11 无线网必须支持 WPA2+AES，也可以支持 WPA/TKIP 以支持建设较早硬件;
- 2.5. eduroam SP 网络必须为用户提供 IP 地址和 DNS 解析的自动配置;
- 2.6. eduroam SP 网络应该为用户提供可访问互联网的 IP 地址;
- 2.7. 在不改动 eduroam 框架的情况下，eduroam SP 可以转发发往不同 eduroam 目标的所有 EAP 消息;
- 2.8. eduroam SP 支持所有 eduroam 用户的使用，承诺不向用户或者他们的 IdP 收费;
- 2.9. eduroam SP 应该保存足够的日志信息，并可识别出为用户提供认证的 IdP，至少要记录以下信息：认证请求和应答的时间戳、认证请求中 User-Name 属性、客户端 MAC 地址、认证应答类型 (通过或拒绝, Accept or Reject)、客户端 MAC 地址和 IP 地址的对应关系；日志最少保留 6 个月。

承诺单位 (网络中心公章):

承诺单位代表 (签名): _____ 日期: _____