eduroam CN 接入承诺书

我机构自愿申请加入全球 eduroam 网络，并承诺遵守以下规定：

1.eduroam IdP 的管理和技术条款

1.1 eduroam IdP 需要实现 RADIUS 接口来连接 eduroam 路由架构。

1.2 eduroam IdP 需要对所有的本地用户使用同一种 EAP 认证方式，并且支持双向认证和端到端的证书加密。

1.3 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）。

1.4 对于本地认证不通过的用户，eduroam IdP，不能发送 RADIUS 通过消息（accept message）。

1.5 eduroam IdP 需要提供用户管理和用户支持。

1.6 eduroam IdP 需要确保提供的账号为实名制账号。

1.7 eduroam IdP 需要记录所有的认证请求，至少包含以下信息：

- 认证请求和相应应答的时间戳
- 认证请求中的外部 EAP id（用户名属性 User-Name attribute）
- 内部 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）

日志最短保留时间为 6 个月。

2.eduroam SP 的管理和技术条款

2.1 eduroam SP 网络必须实现 802.1X 和 RADIUS 接口来接入 eduroam 架构。

2.2 eduroam SP IEEE802.11 无线网必须广播 SSID “eduroam”。

2.3 eduroam SP IEEE802.11 无线网必须支持 WPA2+AES，如果是建设较早的设备需要支持 WPA/TKIP。

2.4 eduroam SP 网络必须为用户提供 IP 地址和 DNS 解析的自动分配服务。

2.5 eduroam SP 网络必需为用户提供可访问互联网的 IP 地址。

2.6 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。

2.7 eduroam SP 支持所有 eduroam 用户的使用，不能向用户或者他们的 IdP 收费。

2.8 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
- 认证请求中外部 EAP id(User-Name attribute)
- 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

日志最短保留时间为 6 个月。

附 1.名词术语

1、 eduroam 身份提供者（eduroam IdP）

eduroam 身份提供者负责管理用户身份、运行接入 eduroam 的认证服务器，也被称为“身份所在机构”。

2、eduroam 服务提供者（eduroam Service Provider，SP）

eduroam 服务提供者是运行可支持 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 接入网络，也被称为“被访机构”。

承诺单位（单位公章）：

承诺单位代表（签名）：_____日期：_____