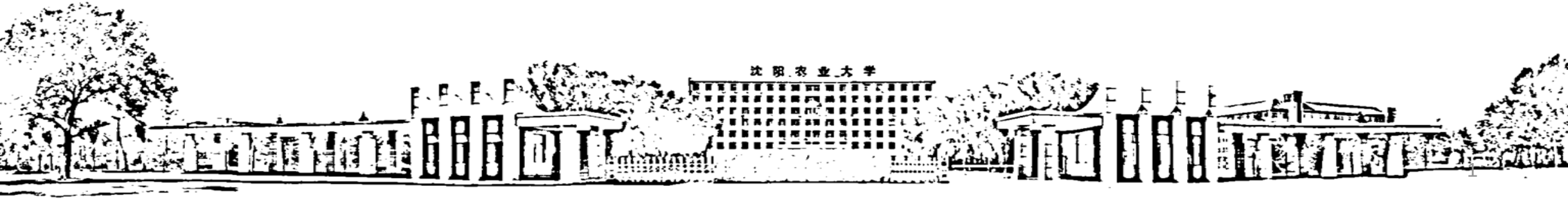
沈阳农业大学
Shenyang Agricultural University

基于CARSI构建灵活安全的认证共享体系

刘占文

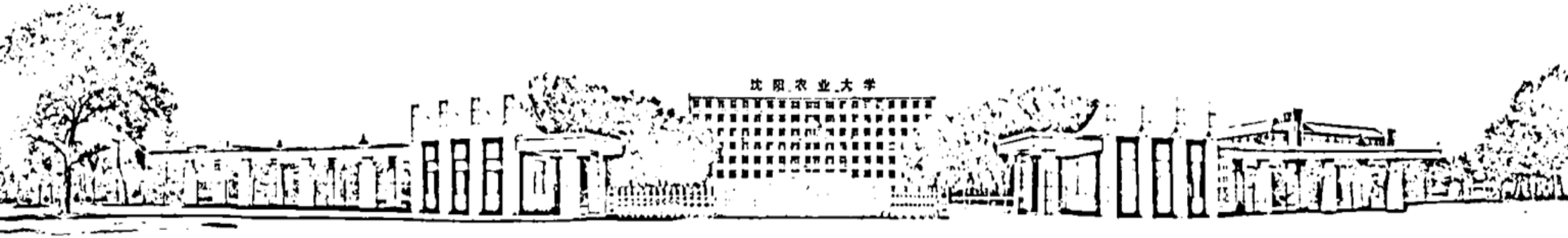
2019年11月



汇报提纲

身份认证现状	• 身份认证的方法与使用局限性 • 以电子图书数据库为例
加入CARSI意义	• 为什么加入CARSI • 以电子图书数据库为例
IDP部署难点	• 系统对接 • 安全防护
融合与应用	• 认证源的选择 • 企业微信的融合
未来与思考	• 数据隐私保护 • 未来发展，规模发展

一、学校身份认证现状



校园身份认证的方法

常规身份认证方式

用户名/密码认证

智能卡认证

动态口令认证

USB Key认证

生物特征认证

校园身份认证

基于统一认证系统的LDAP、SQL、CAS等

基于学校校园网络IP地址/电子邮箱地址等

基于学校微信/QQ、公众平台、微博等

基于生物特征的指纹识别/人脸识别等

基于人工的数据传递等

以电子图书数据库为例

1. 必须使用学校IP地址才能访问，变更地址，通知厂商；

2. 校园网出口采用**NAT**技术，经常被厂商认为非法下载，封地址；

3. VPN主要用于图书访问，账号借用、滥用导致**信息安全问题**；终端多样化，造成VPN兼容性差；

4. **缺少统计和分析**，不能为学校提供采购建议。

以某服务商学生用户审核为例

提交时间	QQ号	来源	认证信息	照片	当前状态	操作
2019-09-19 19:39	4353445657	申请	姓名：张三 类别：学生 入学年份：2019 学院：工学院 学号：20199910393		待审核	通过 驳回
2019-09-29 09:19	8956456854	申请	姓名：李四 类别：学生 入学年份：2019 学院：经管学院 学号：2019109208		待审核	通过 驳回
2019-09-19 09:19	8945895689	申请	姓名：王二 类别：学生 入学年份：2019 学院：文学院 学号：201999089		待审核	通过 驳回

众多校外服务商要求提供师生证件照片和信息进行身份鉴别和审核；
各类证件、个人信息有严重的泄露风险和隐患。

认证情况分析

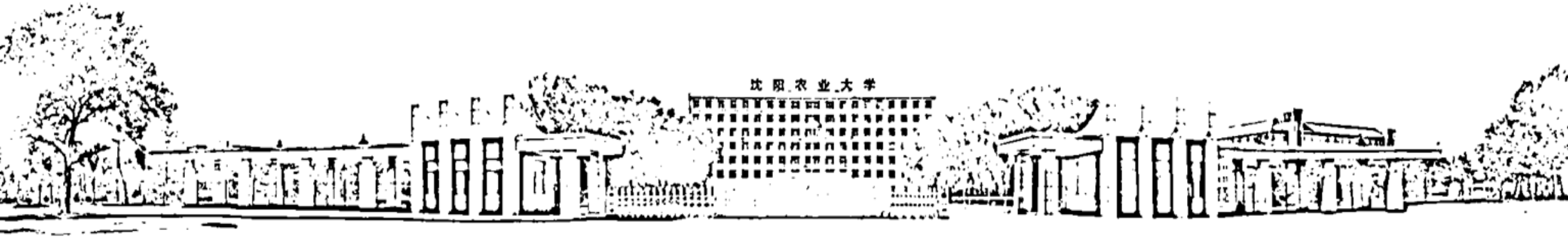
1. 学校的统一身份认证多数仅限应用于学校自有的信息系统；

2. 对于校外的服务，多数采取粗放形式的认证，不能精细化的管理；

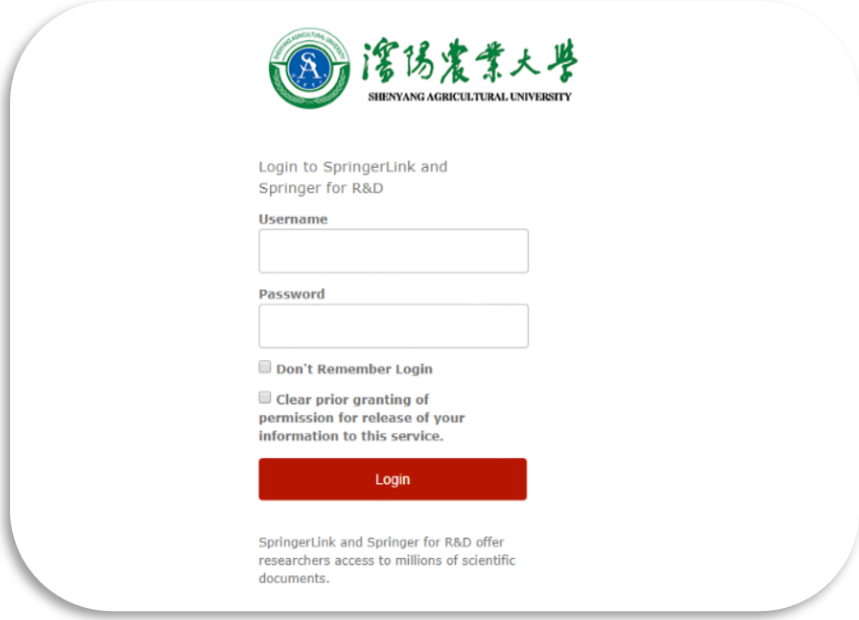
3. 对于校外的服务，认证手段往往体验不佳；

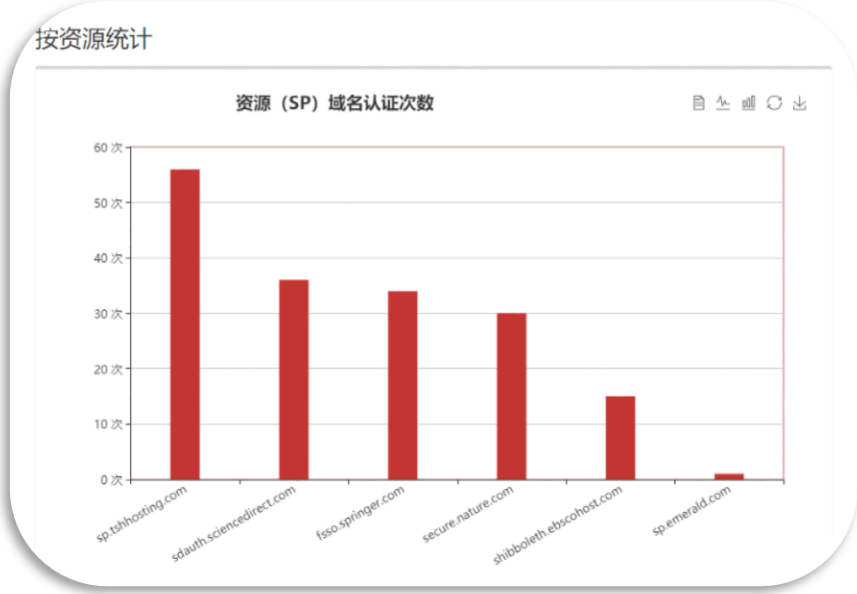
4. 手工交换数据的方式存在信息安全风险。

二、加入CARSI意义



以电子图书数据库为例





1. 全程浏览器操作，比VPN便捷，不需要插件和软件，不关注浏览器版本；大大降低使用门槛，提升用户体验。

2. 用户实名制，能溯源可查；少数用户行为不当，一般也不影响其他用户。

3. 系统提供各类应用服务的访问分析，自己也可以根据日志做个性的详细的分析统计；

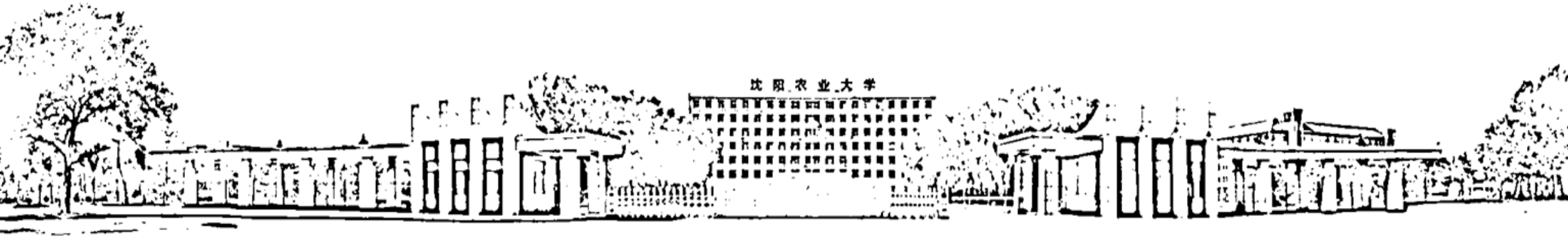
加入CARSI意义

1. 基于CARSI平台提供的标准接口，为跨域、跨国、跨校**身份认证**和**资源共享**服务提供了平台基础；

2. 基于CARSI平台，身份认证**更安全**，提供服务**更便捷**，开发时间**更短**，维护成本**更低**；

3. CARSI & eduroam，即将成为高校**国际化办学水平**的标志之一。

三、IDP部署难点



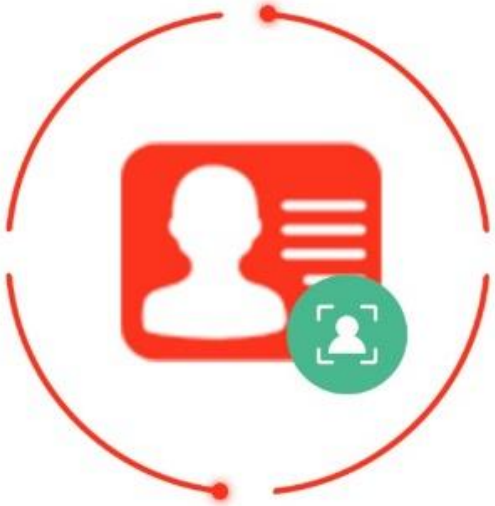
认证系统的对接

1. IDP是学校现有认证系统的延展，IDP一般应基于学校的认证系统构建。

2. IDP支持多种认证数据的对接，查看相关文档；

3. 多数高校认证系统是支持LDAP的；LDAP文档较多，较容易配置。相对复杂配置需咨询厂商协助；

4. 认证数据同步至LDAP，支撑IDP。



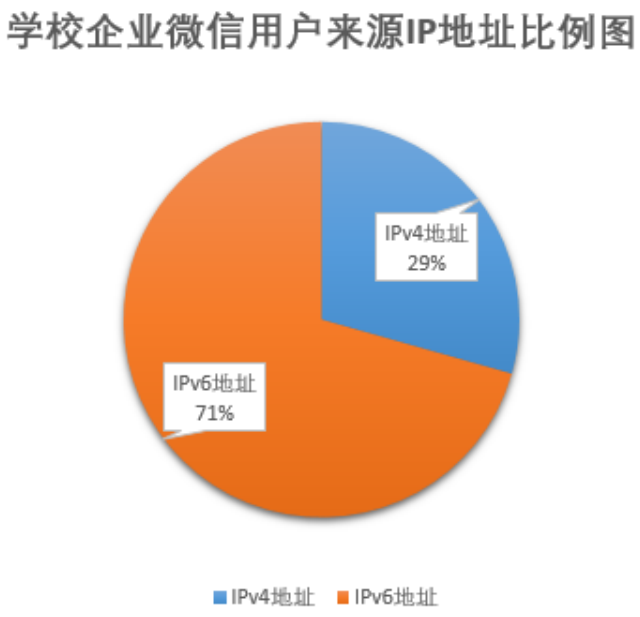
数据传输的安全

SSL数字证书：实现网站HTTPS化，加密用户与网站间的交互访问，防劫持、防篡改、防监听。

通配符SSL证书：可以保护同一主域名下同一级所有的子域名，不限个数。性价比较高。

SSL证书获取渠道：赛尔网络等；

IPv4/IPv6协议



1. IPv6使用率：移动终端迅速攀升，固定终端稳步提升；

2. IPv4/IPv6网络互作备份，浏览器一般优先使用IPv6；

3. IPv4/IPv6双栈：中间件完全支持，日志分析系统需要调整开发，**IPv4/IPv6地址格式不同。**

信息系统安全

1. 由于采用了https，WAF设备分析拦截功能有限；

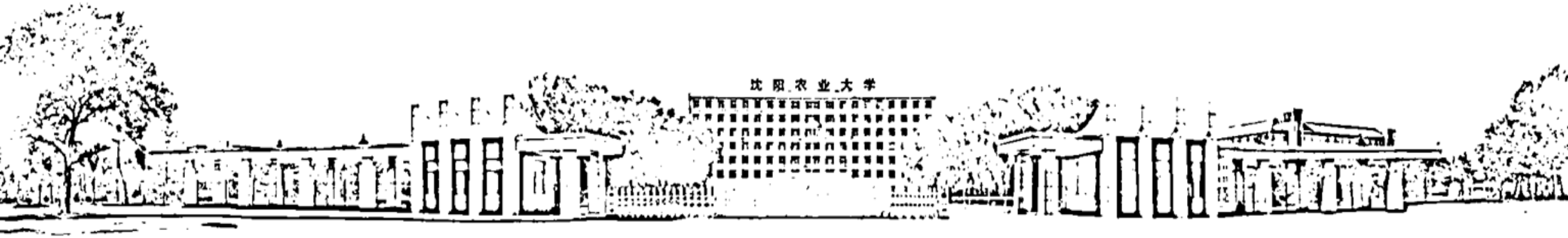
2. 利用好校园网或数据中心出口防火墙等安全设备；

3. 做好Linux自身iptables的安全策略；

4. 仅保留必要的端口和服务，及时修复操作系统与应用软件的漏洞；

5. 基于访问日志的分析统计，动态调整iptables策略，拦截频繁扫描与攻击行为；

四、企业微信的融合与应用



为什么要融合学校企业微信

IDP与学校企业微信对接的原因：

1. 基于企业微信的校园移动应用初见规模。

2. 学校用户认证体系还不是完全的统一。

3. 做一个让用户看得见，用的好的应用。

4. 认证系统的权限与安全问题。

基于企业微信的校园移动应用

2016年
学校微信企业号申请注册

2017年
实现与学校统一认证系统关联

2018年
实现协同办公、邮箱、通知等

2019年
实现查工资、查课表、查成绩等

学校企业微信已经经成为学校师生员工教学、科研、管理的主流移动应用APP，具有固定的用户群体和较高的使用粘性。

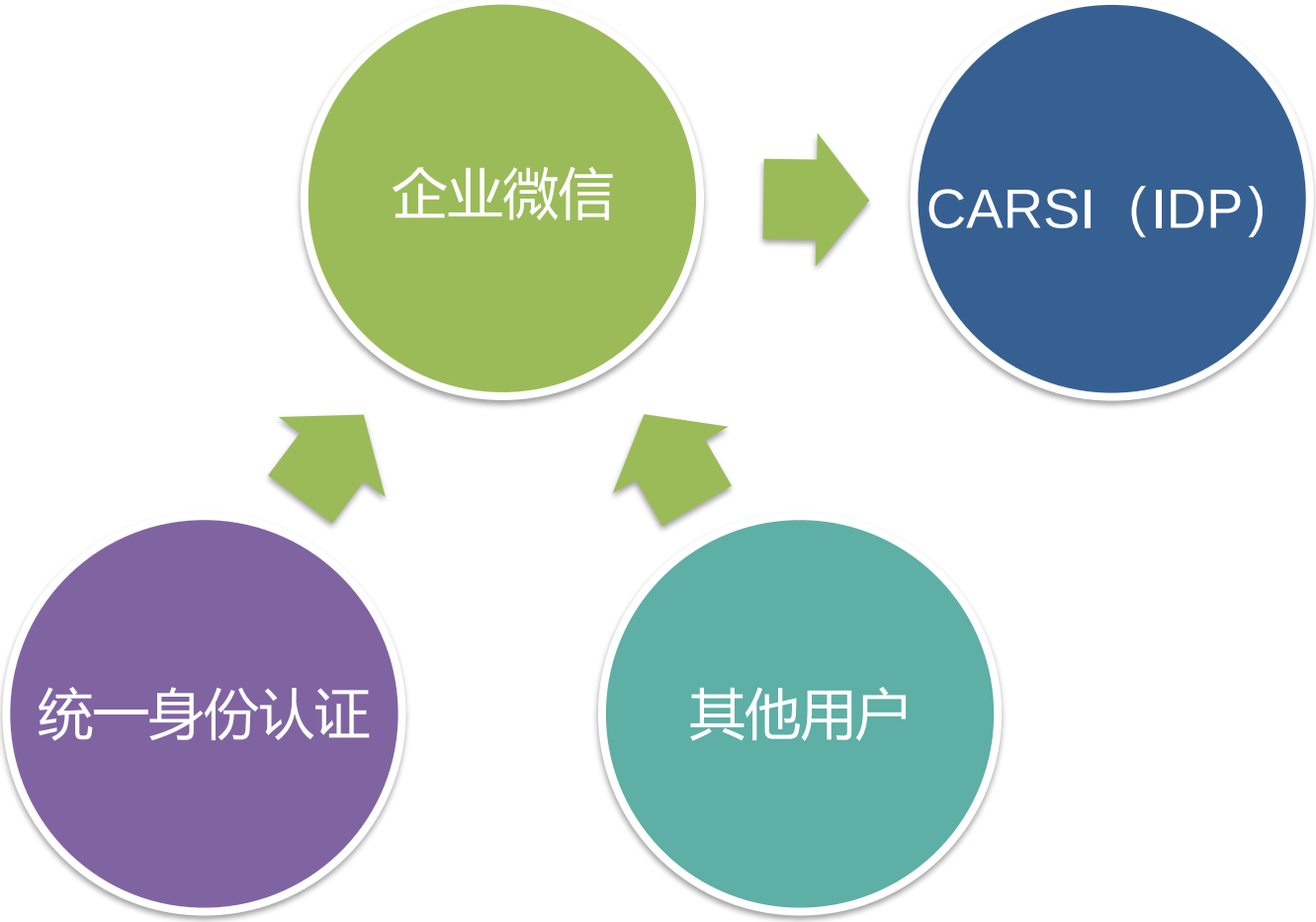
80%
覆盖学生

90%
覆盖教师

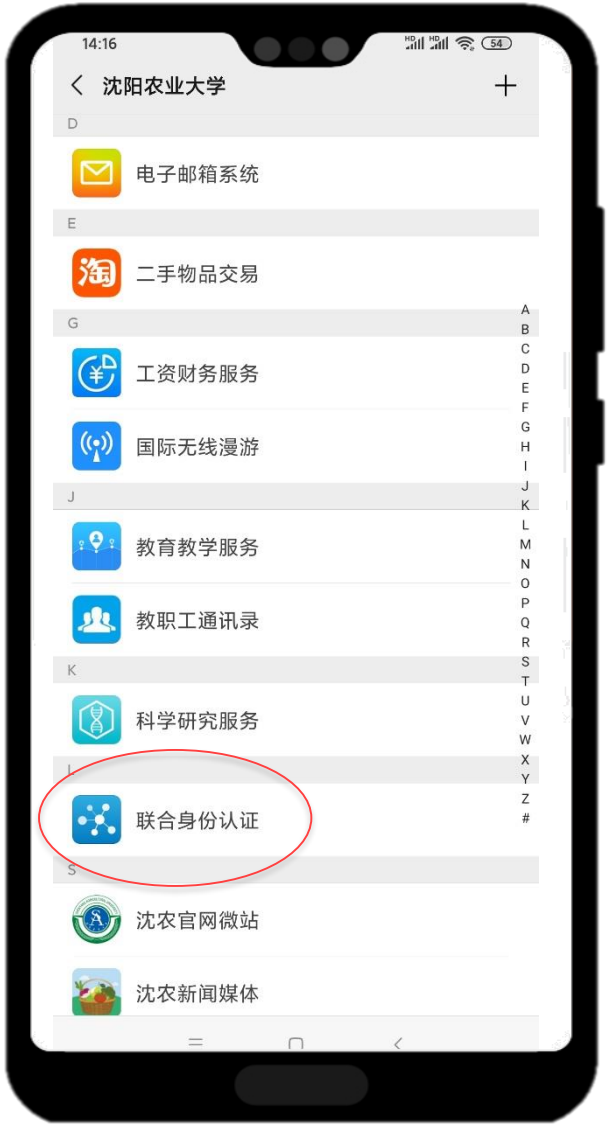
20+
应用程序

学校企业微信认证数据源

企业微信用户 = 统一身份认证用户 + 其他用户



IDP在学校企业微信中的呈现



学校微信企业号
&
学校企业微信

利弊分析

1. 用户名、密码、使用向导、帮助文档全部在企业微信内一站式呈现，**降低了使用门槛**，尤其是初期的用户，手机在手，使用无忧。

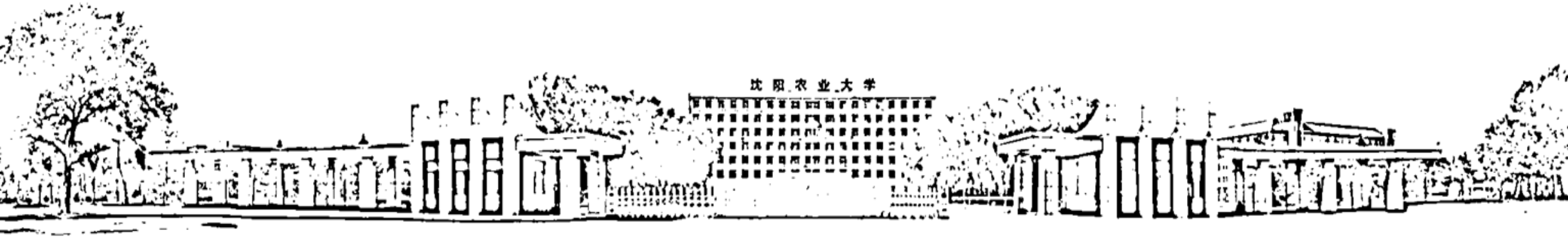
2. 通过消息群发，能够使师生及时了解新应用的动态和进展。

3. **拓展**了移动终端APP的功能，**宣传**了CARSI联合认证的应用。

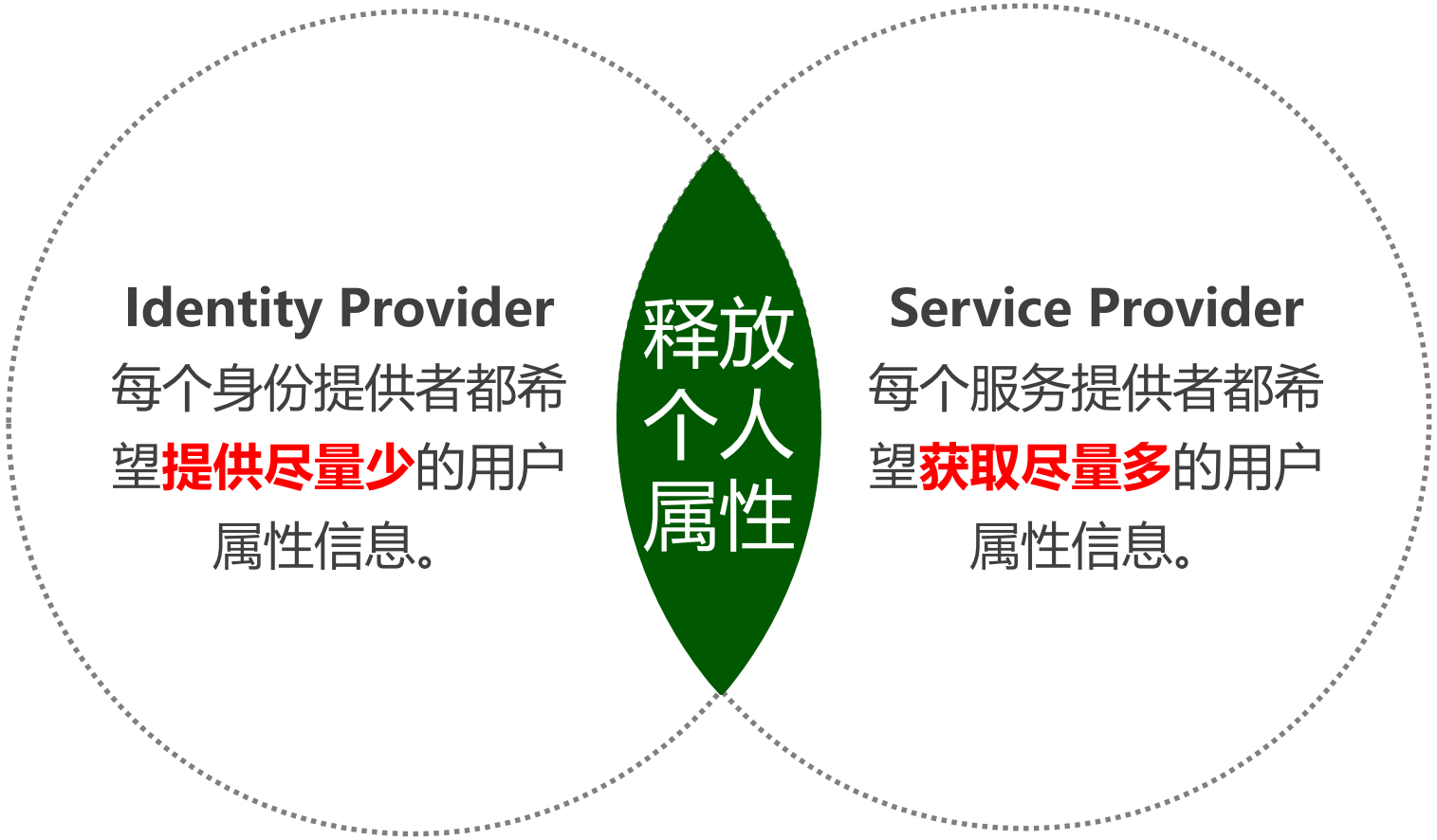
4. 用户实名；用户权限控制灵活，校外账户信息安全可控；用户日志分析可靠。

5. 但是产生了新密码，今后逐步融合统一，直至取消。

五、关于CARSI的一些思考



信息安全保护

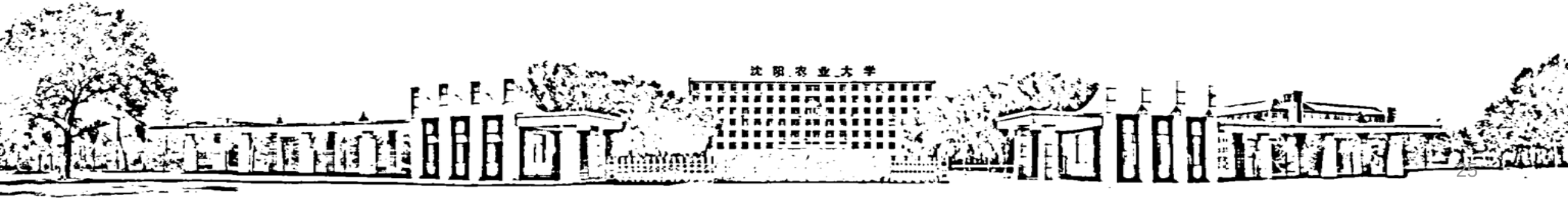

Identity Provider
每个身份提供者都希望提供尽量少的用户属性信息。
释放个人属性
Service Provider
每个服务提供者都希望获取尽量多的用户属性信息。

未来...

1. 充分考虑各类学校发展水平的不同，引入或吸引更多服务加入。

2. 加大宣传和推广，吸引更多的高校参与，构建完整的网络生态；

3. 形成行业标准和行业规范；

4. 建立良好的沟通协作机制。

谢谢！