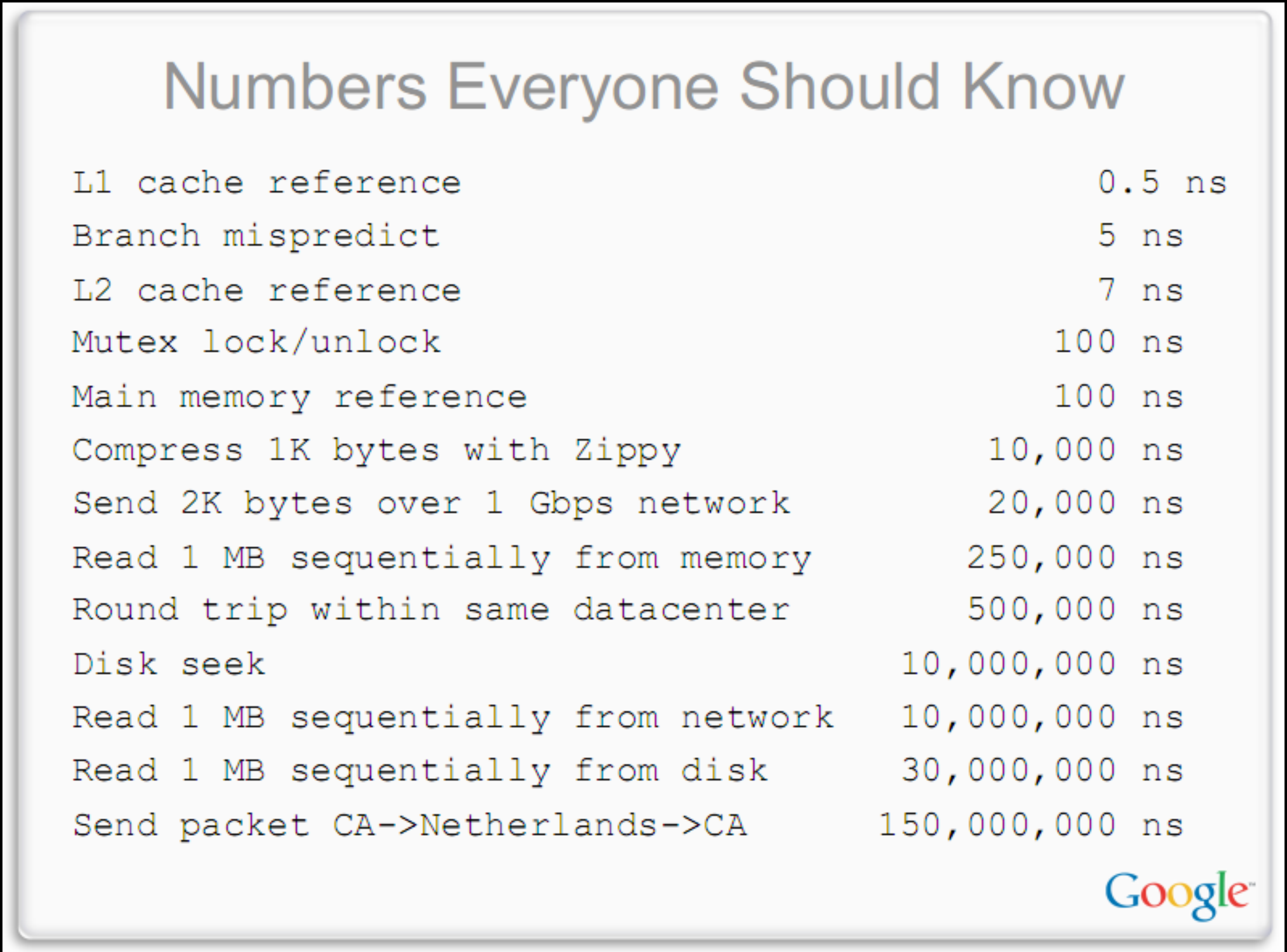
Induction training of Dev Team

Au & Az, SSO

By PuGong



Numbers Everyone Should Know

L1 cache reference	0.5 ns
Branch mispredict	5 ns
L2 cache reference	7 ns
Mutex lock/unlock	100 ns
Main memory reference	100 ns
Compress 1K bytes with Zippy	10,000 ns
Send 2K bytes over 1 Gbps network	20,000 ns
Read 1 MB sequentially from memory	250,000 ns
Round trip within same datacenter	500,000 ns
Disk seek	10,000,000 ns
Read 1 MB sequentially from network	10,000,000 ns
Read 1 MB sequentially from disk	30,000,000 ns
Send packet CA->Netherlands->CA	150,000,000 ns

List

- Product / Develop / Operation
- Software lifecycle
- ITIL
- Source Control
- Evolution of A Website’s Architecture
- ***AuAz & SSO***
- Cache
- Message Queue
- Storage
- Database and SQL
- NoSQL & New SQL
- TOGAF & 4+1 Arch View
- 测试
- 发布
- 监控

Authentication

- A process of verifying that "you are who you say you are”.
- Parts:
  - Query for credentials
  - Verify Credentials
- Method：
  - Form Authentication
  - AD / LDAP Authentication
  - Sign, Fingerprint
  - Factual verification
  - Two Factor Authentication
  - SSO: OAuth, OpenID, SAML etc
- Security, Security, Security

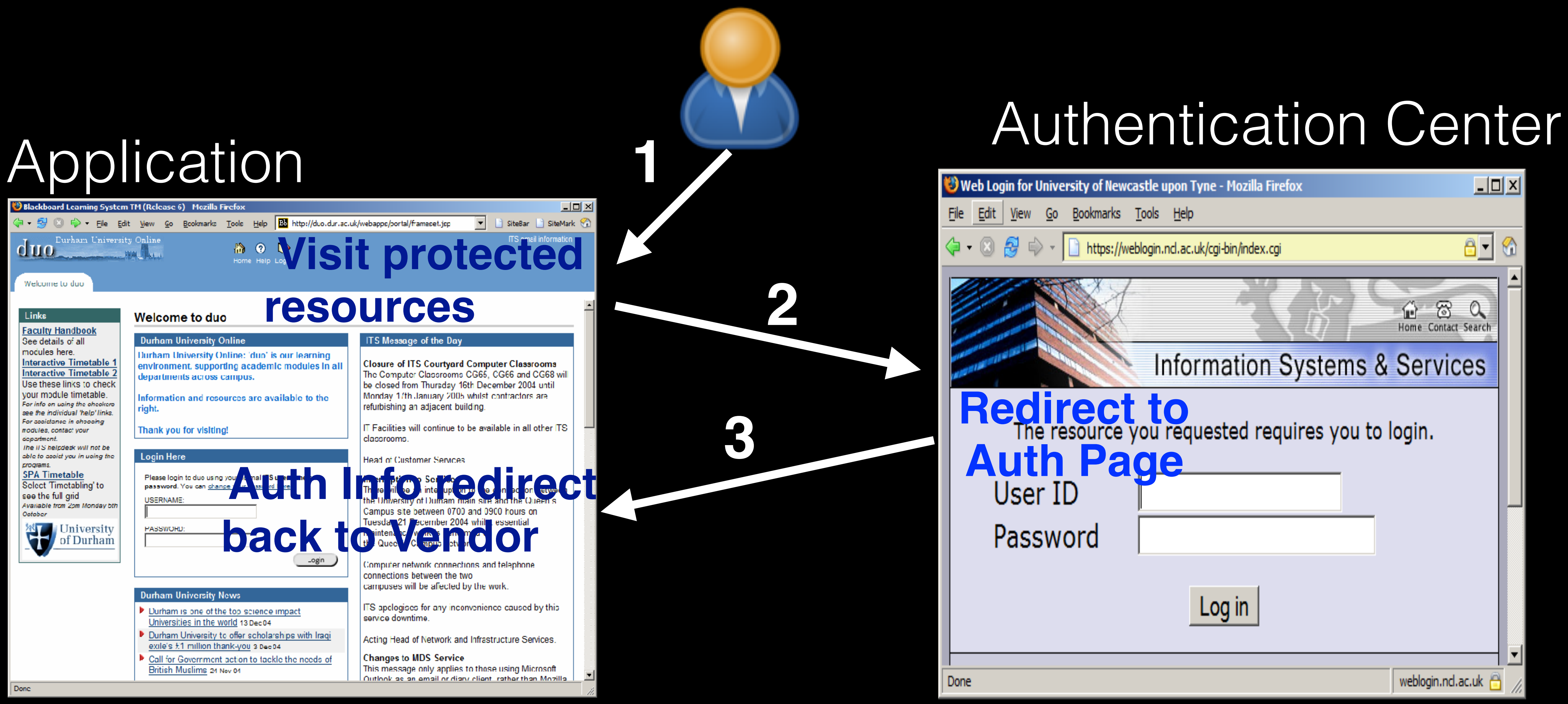
Authorization

- A process of verifying that "you are permitted to do what you are trying to do”
- Method:
  - RBAC
  - ACL: most file system: Read, Write, eXecute
- Principle of least privilege

SSO

- Single sign-on is a user/session authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

- Web SSO



Application

1 Visit protected resources

2 Redirect to Auth Page

3 Auth Info redirect back to Vendor

Authentication Center

Blackboard Learning System TM (Release 6) Mozilla Firefox

http://duo.dur.ac.uk/webapps/portal/frameset.jsp

duo Durham University Online

ITS email information

Welcome to duo

Links

Faculty Handbook
See details of all modules here.

Interactive Timetable 1
Interactive Timetable 2
Use these links to check your module timetable.
For info on using the checkers see the individual 'help' links. For assistance in choosing modules, contact your department. The ITS helpdesk will not be able to assist you in using the programs.

SPA Timetable
Select 'Timetabling' to see the full grid
Available from 2pm Monday 5th October

University of Durham

Welcome to duo

Durham University Online

Durham University Online: 'duo' is our learning environment, supporting academic modules in all departments across campus.

Information and resources are available to the right.

Thank you for visiting!

Login Here

Please login to duo using your [illegible] password. You can change [illegible]

USERNAME:

PASSWORD:

Login

Durham University News

- Durham is one of the top science impact Universities in the world 13 Dec 04
- Durham University to offer scholarships with Iraqi exile's £1 million thank-you 3 Dec 04
- Call for Government action to tackle the needs of British Muslims 24 Nov 04

ITS Message of the Day

Closure of ITS Courtyard Computer Classrooms
The Computer Classrooms CG65, CG66 and CG68 will be closed from Thursday 16th December 2004 until Monday 17th January 2005 whilst contractors are refurbishing an adjacent building.

IT Facilities will continue to be available in all other ITS classrooms.

Head of Customer Services

[illegible] Service
There will be an interruption to the connection between the University of Durham main site and the Queen's Campus site between 0700 and 0900 hours on Tuesday 21 December 2004 whilst essential maintenance [illegible] the Queen's Campus [illegible]

Computer network connections and telephone connections between the two campuses will be affected by the work.

ITS apologises for any inconvenience caused by this service downtime.

Acting Head of Network and Infrastructure Services.

Changes to MDS Service
This message only applies to those using Microsoft Outlook as an email or diary client, rather than Mozilla

Done

Web Login for University of Newcastle upon Tyne - Mozilla Firefox

https://weblogin.ncl.ac.uk/cgi-bin/index.cgi

Information Systems & Services

The resource you requested requires you to login.

User ID

Password

Log in

Done

weblogin.ncl.ac.uk

Advantages

- 用户(角色)统一管理
- 降低运营和管理成本
- 提升用户体验
- 减轻开发人员的复杂
- 增强系统安全性

- 多种认证方式
- Smartcards
- Security token
- 记录登录信息
- 满足安全审计要求 (SOX, HIPAA)

Criticisms

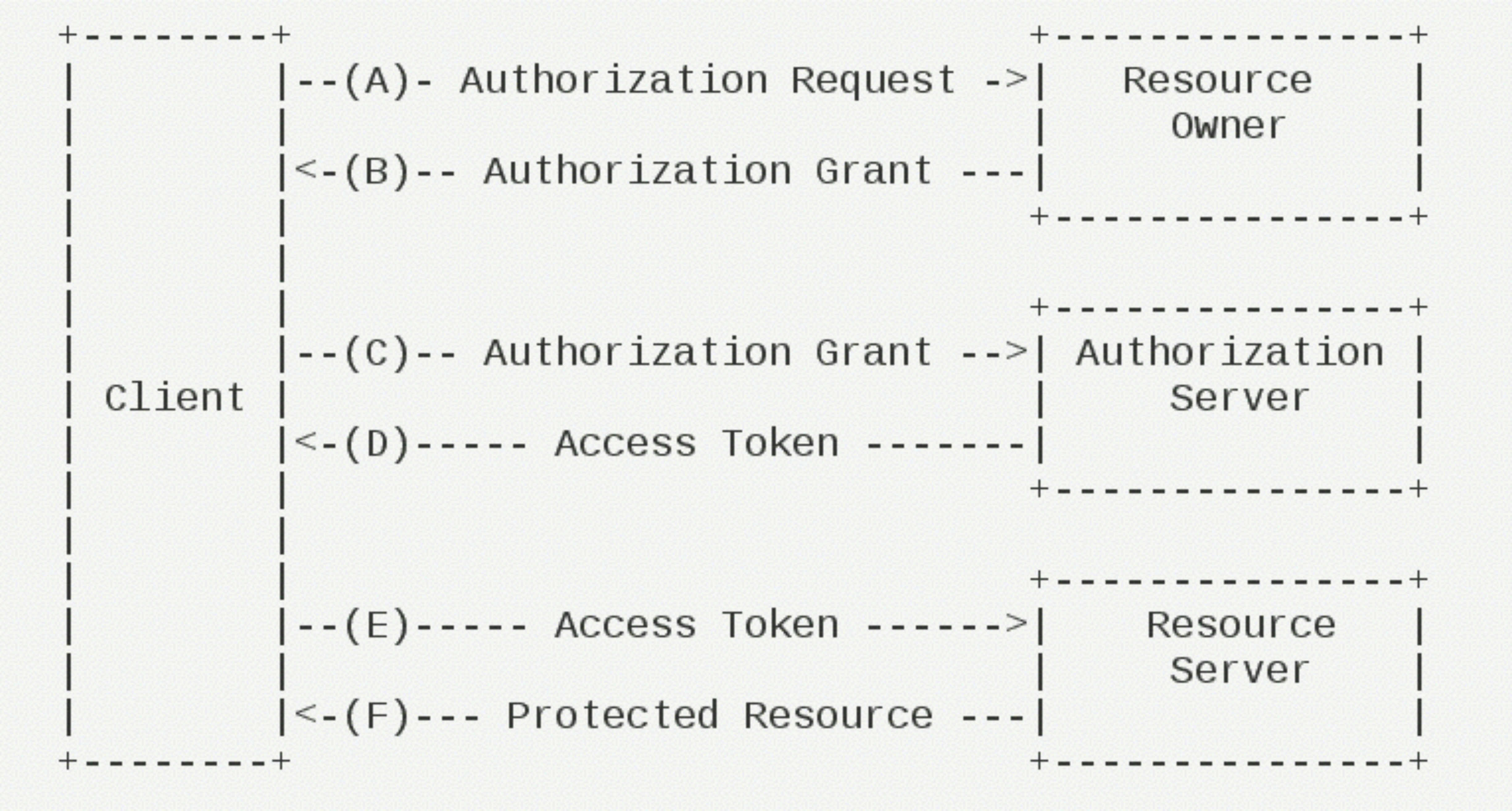
- 成为企业关键应用，存在单点故障风险
- 系统被攻破或者系统不严谨导致SSO下所有应用都被暴露
- SSO安全报告 by Rui Wang, Shuo Chen和XiaoFeng Wang，研究googleId, paypal Access, facebook等，找到数个严重逻辑错误

Implementations

- Mechanism
  - Cookie
  - Token/Ticket
  - SAML 安全断言
  - Kerberos 代理人
  - Gateway

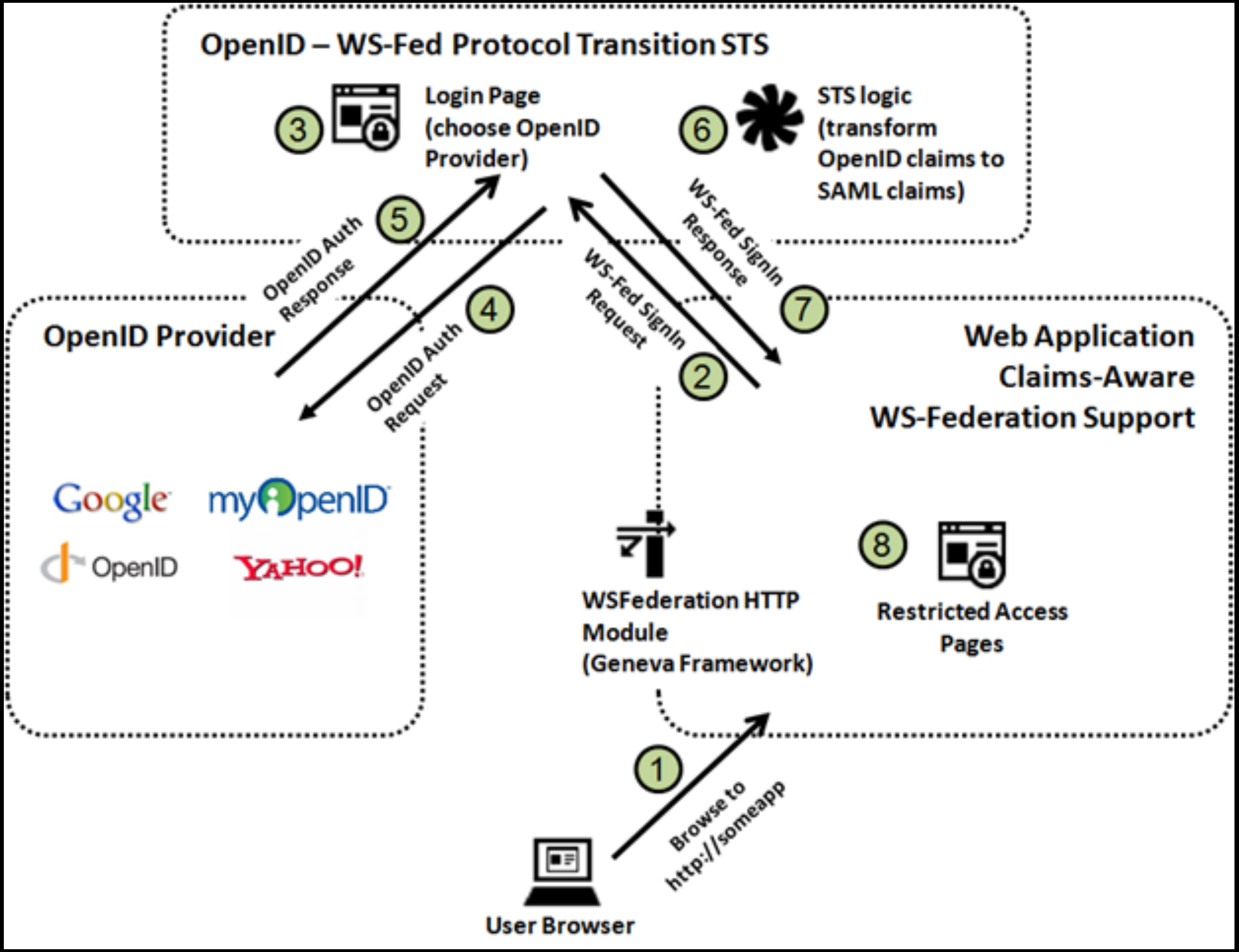
- Products
  - CAS
  - SAML
  - Facebook connect
  - IBM TAM ／Windows Live Id
  - OAuth
  - Open Id (Google ID, Paypal Access)
  - CA SiteMinder

OAuth



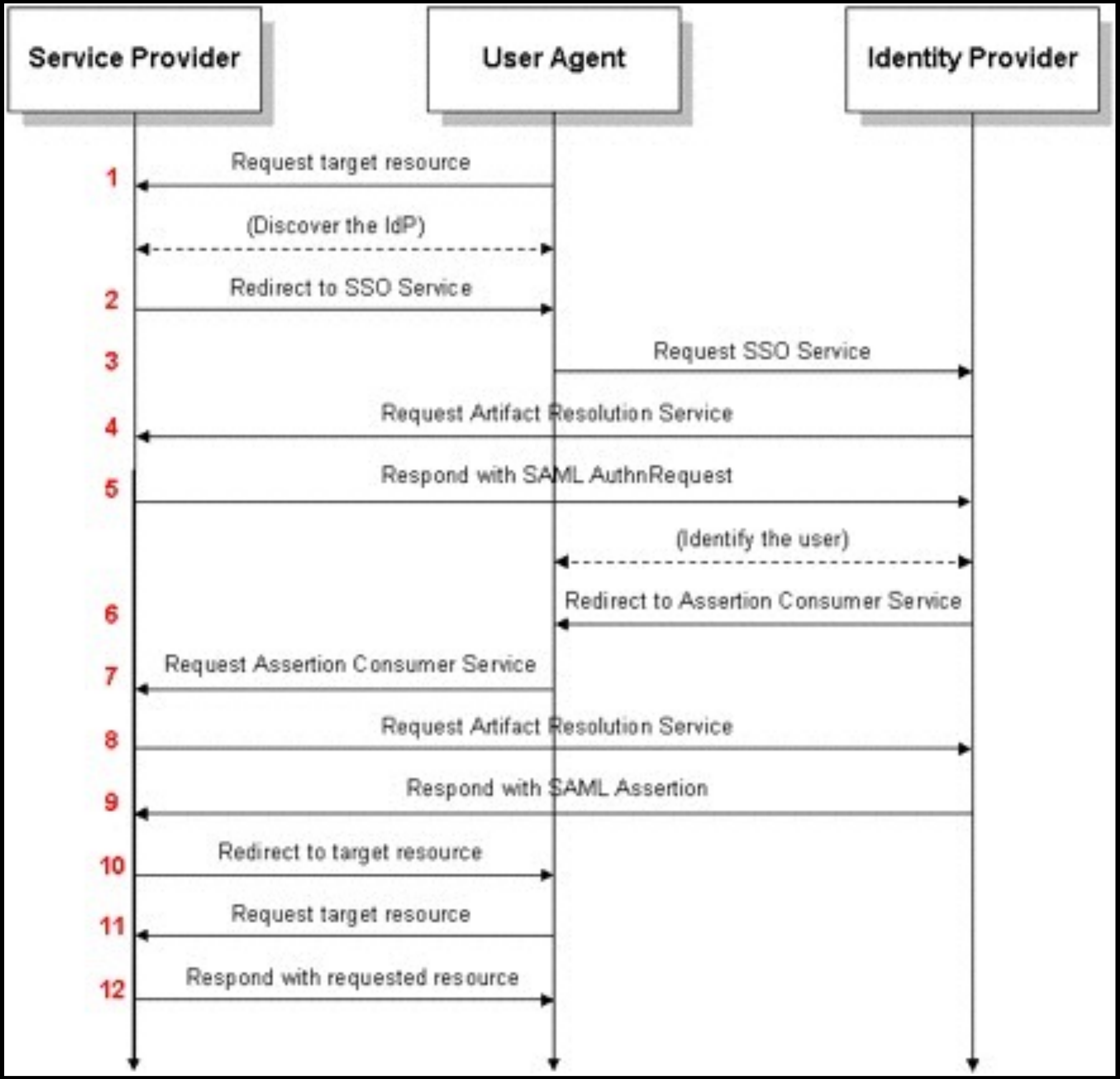
```
+--------+                               +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(C)-- Authorization Grant -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

Open Id



- 以用户为中心的数字身份识别框架

SAML


Service Provider
User Agent
Identity Provider
1
Request target resource
(Discover the IdP)
2
Redirect to SSO Service
3
Request SSO Service
4
Request Artifact Resolution Service
5
Respond with SAML AuthnRequest
(Identify the user)
6
Redirect to Assertion Consumer Service
7
Request Assertion Consumer Service
8
Request Artifact Resolution Service
9
Respond with SAML Assertion
10
Redirect to target resource
11
Request target resource
12
Respond with requested resource

- Security Assertion Markup Language
- Standard of OASIS (SOAP, UDDI)
- 实现：Shibboleth

References

- OAuth: http://oauth.net/2/
- Open Id: http://openid.net/
- http://en.wikipedia.org/wiki/Single_sign-on
- http://en.wikipedia.org/wiki/List_of_single_sign-on_implementations
- http://en.wikipedia.org/wiki/Central_Authentication_Service
- http://en.wikipedia.org/wiki/SAML_2.0
- http://sso-analysis.org/