Web Authentication

Thierry Sans

Several Methods

- **Basic Authentication**
  Stateless authentication
- **Local Authentication**
  Stateful authentication
- **OAuth 2**
  Third-party authentication

Basic Authentication

Standard : RFC 2617

➡ Passwords are sent in **clear** (Base64 encoding) in **the headers** `"authorization"`

```
$ curl -u login:password http://url
$ curl http://admin:password@url
```

Local Authentication

The simple recipe for user authentication

1. **Ask the user for a login and password** and send it to the server (HTTP POST request)
2. **Verify the login/password** based on information stored on the server (usually in the database)
3. **Start a session** if the login password matches i.e. once the user has been successfully authenticated
4. **Grant access to resources** according to the session

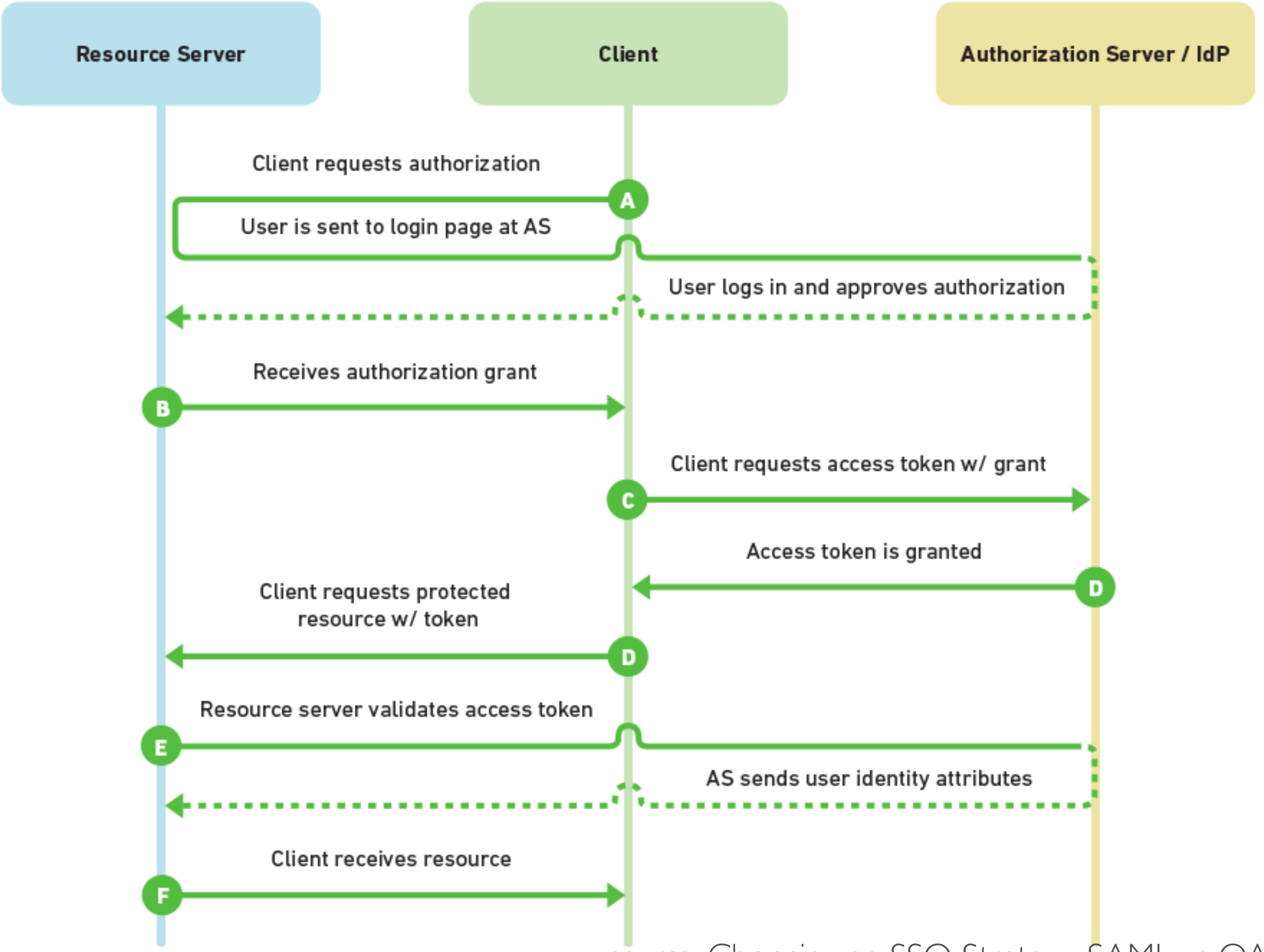
Third-party Authentication

Single-Sign-On (SSO)

• **Pubcookie** (a.k.a webiso)	1998
• **OpenID**	2005
• **SAML** (Security Assertion Markup Language)	2005
• **OAuth**	2010
• **Mozilla Persona**	2011

among others …

OAuth 2.0 Flow


Resource Server
Client
Authorization Server / IdP
Client requests authorization
A
User is sent to login page at AS
User logs in and approves authorization
Receives authorization grant
B
Client requests access token w/ grant
C
Access token is granted
D
Client requests protected resource w/ token
D
Resource server validates access token
E
AS sends user identity attributes
Client receives resource
F

source: Choosing an SSO Strategy: SAML vs OAuth2