Introduction to Single Sign-On: **OAuth and OpenID Connect**

HACKMANIT

Dr. Christian Mainka | @CheariX

The Password Dilemma

Username / Password1

Username / Password2

Username / Password3

Username / Password4

Username / Password5

Slashdot
News for Nerds. Stuff that matters.

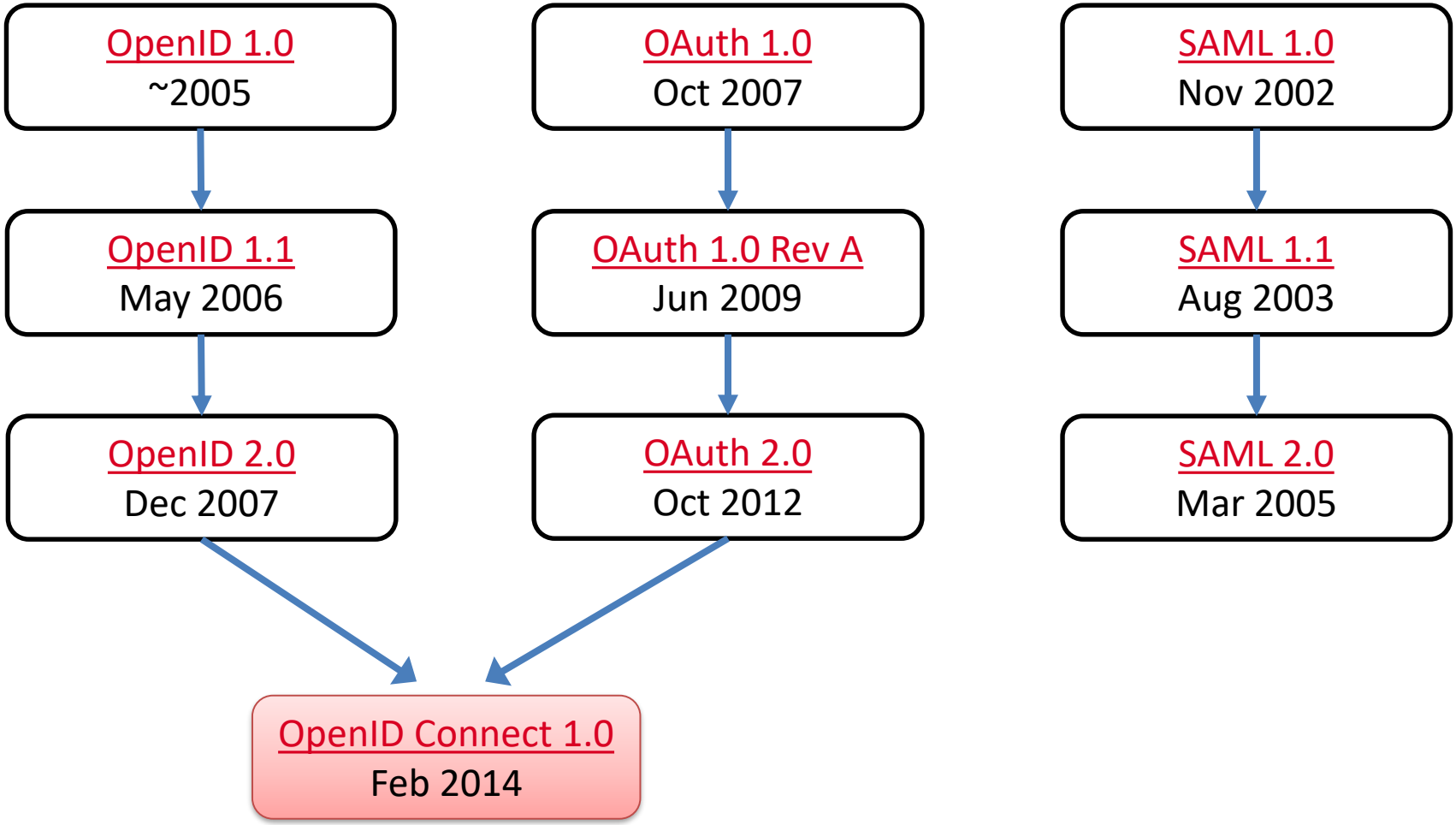
salesforce
SOFTWARE

stackoverflow

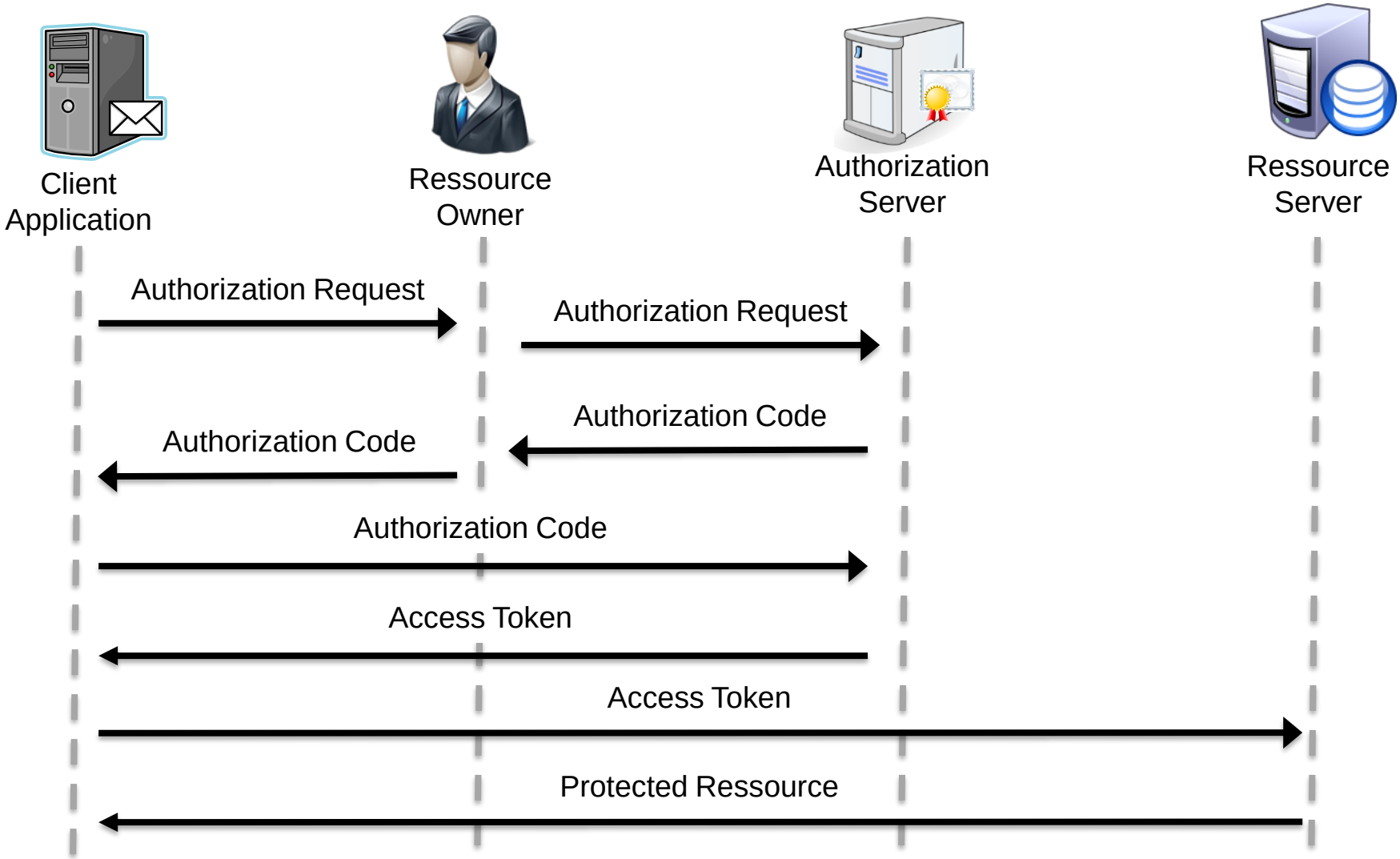
NETFLIX

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

History of Single Sign-On



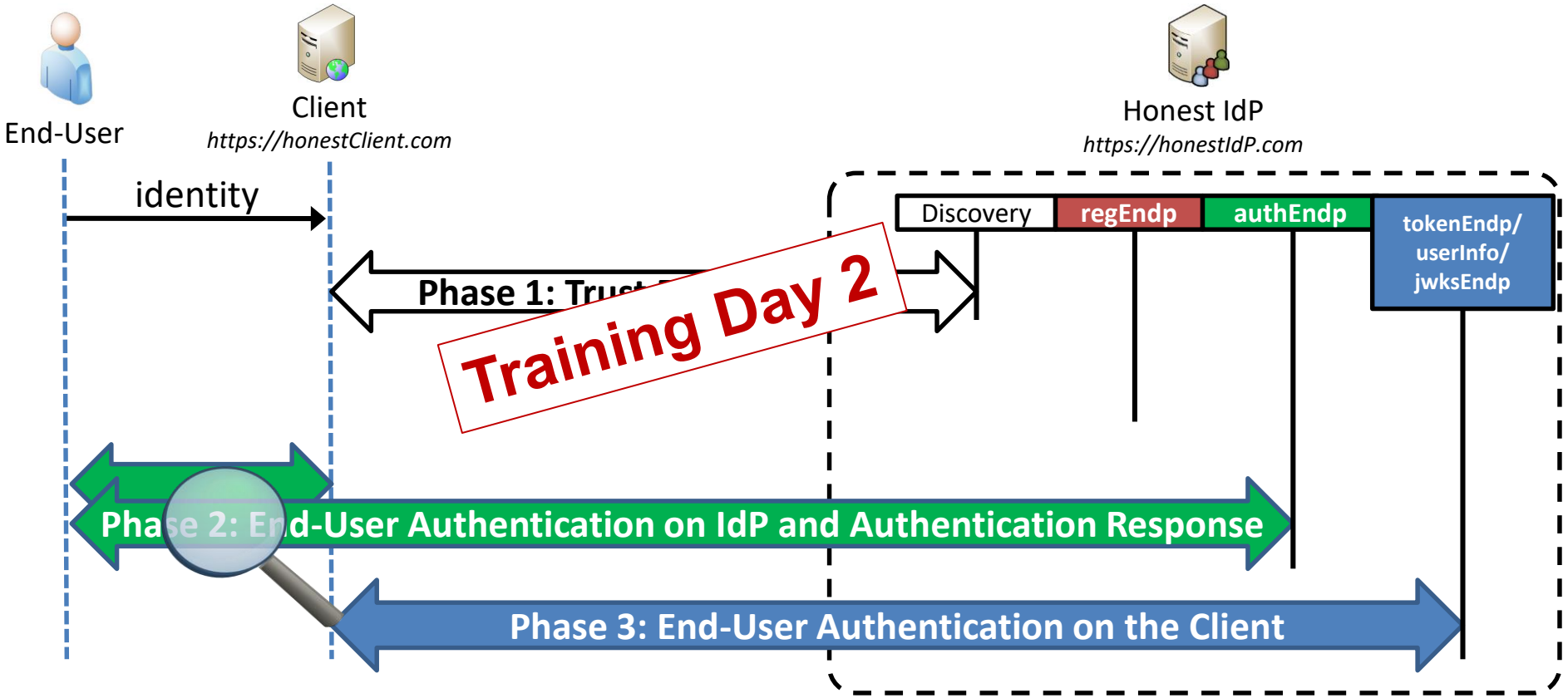
OAuth 2.0 Overview and Terminology



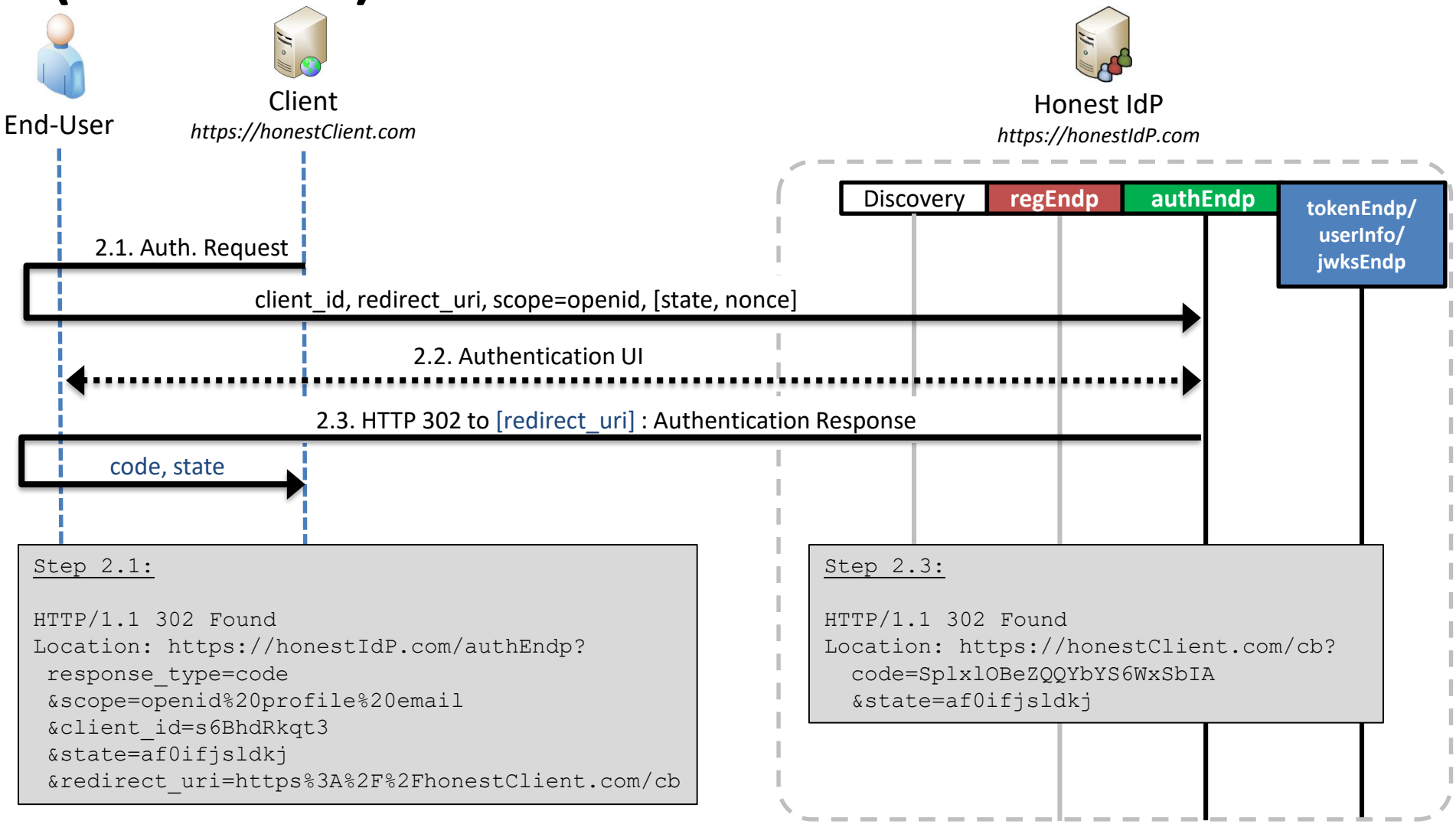
Agenda: OAuth

- OAuth vs. OpenID Connect
- Flows
    - Code Flow: OAuth + OpenID Connect
    - Implicit Flow: OAuth + OpenID Connect
    - Hybrid Flow: OpenID Connect
- Flow Recognition Cheat-Sheet
- Additional OAuth Grants
    - OAuth: Refresh Token
    - OAuth: Token Revocation
    - OAuth: Token Introspection

OpenID Connect in Three Phases



OpenID Connect: End-User Authentication on IdP (Code Flow)



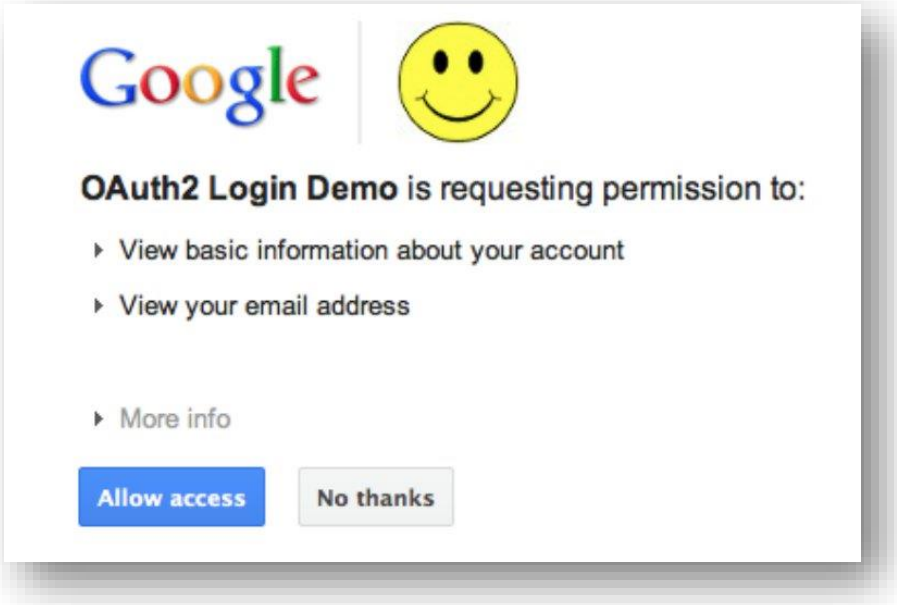
Flow Recognition Cheat-Sheet

- OpenID Connect has `scope=openid`
  - OAuth does not define a scope value
- Flow distinguished by `response_type`

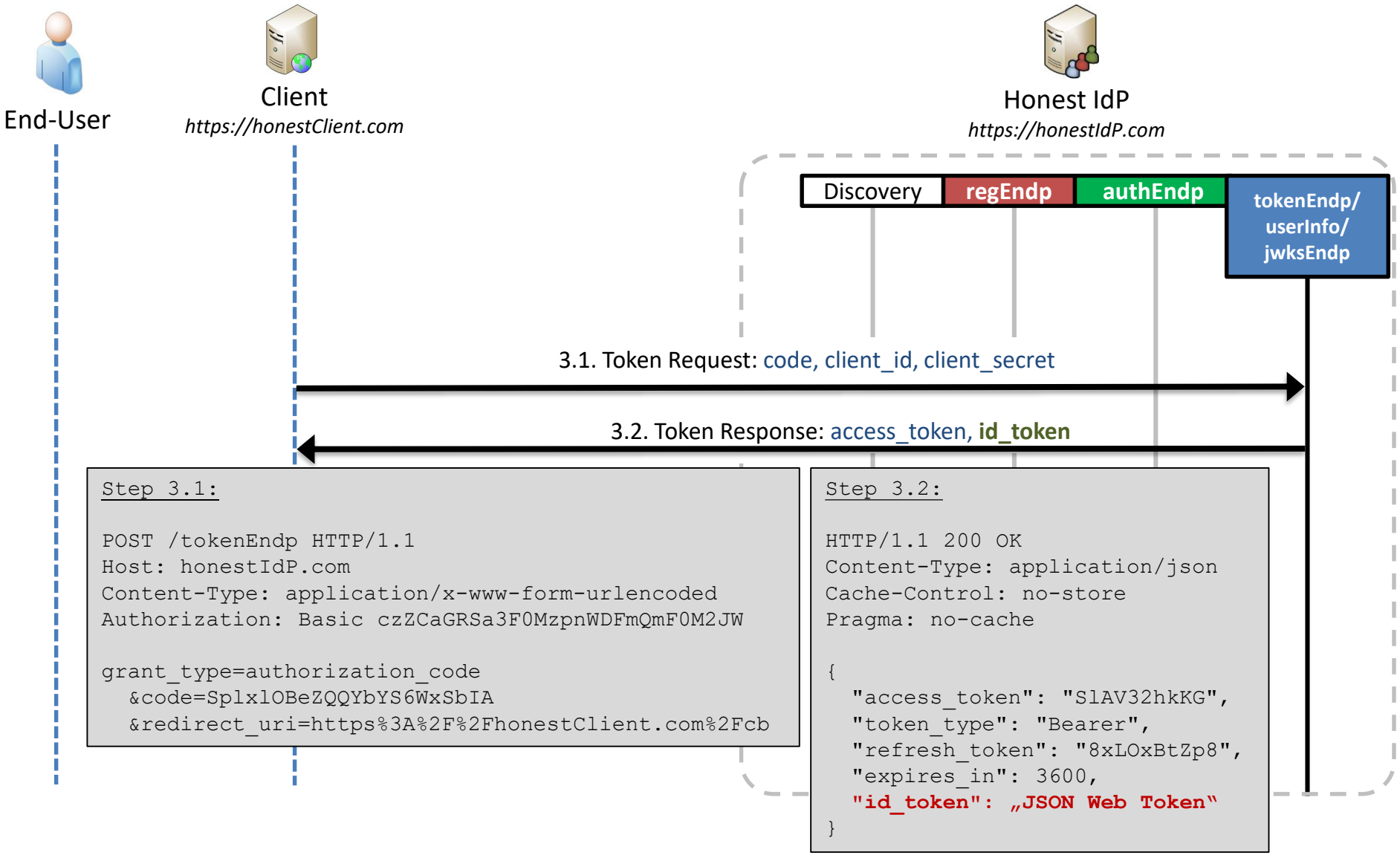
	OAuth	OpenID Connect
Code Flow	• `code`	• `code`
Implicit Flow	• `token`	• `id_token` • `id_token token` (token means access_token)
Hybrid Flow	(not existing)	• `code token` • `code id_token` • `code token id_token`

The Consent-Page

- Why should you use it?
- Which information to show?
- What can go wrong?



OIDC: id_token in Code Flow



SSO Token in OpenID Connect

Identity

= iss sub

Freshness

= iat exp nonce

Recipient

= aud

Security

= sig alg

JWT Header

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

JWT Body

```
{
  "iss": "https://idp.com/",
  "sub": "user1",
  "iat": 1442673964,
  "exp": 1444148308,
  "nonce": "40c6b33b9a2e",
  "aud": "client_id"
}
```

JWT Signature

```
[0x02, 0xF1, …, 0xDA]
```

HACKMANIT

THREAT ANALYSIS | TRAINING | PENETRATION TESTS

Dr. Christian Mainka: christian.mainka@hackmanit.de

www.hackmanit.de | @hackmanit