

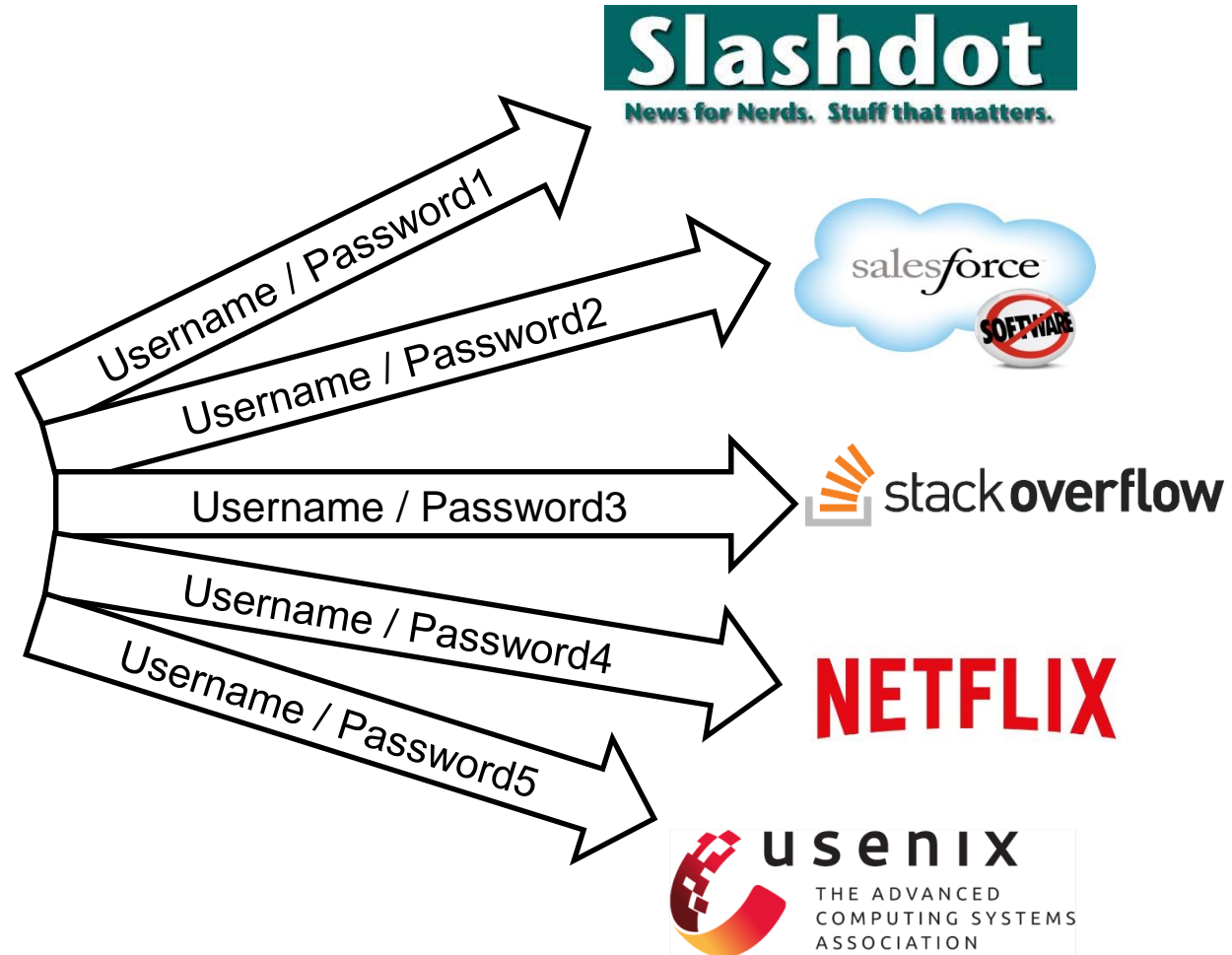
# Introduction to Single Sign-On: OAuth and OpenID Connect



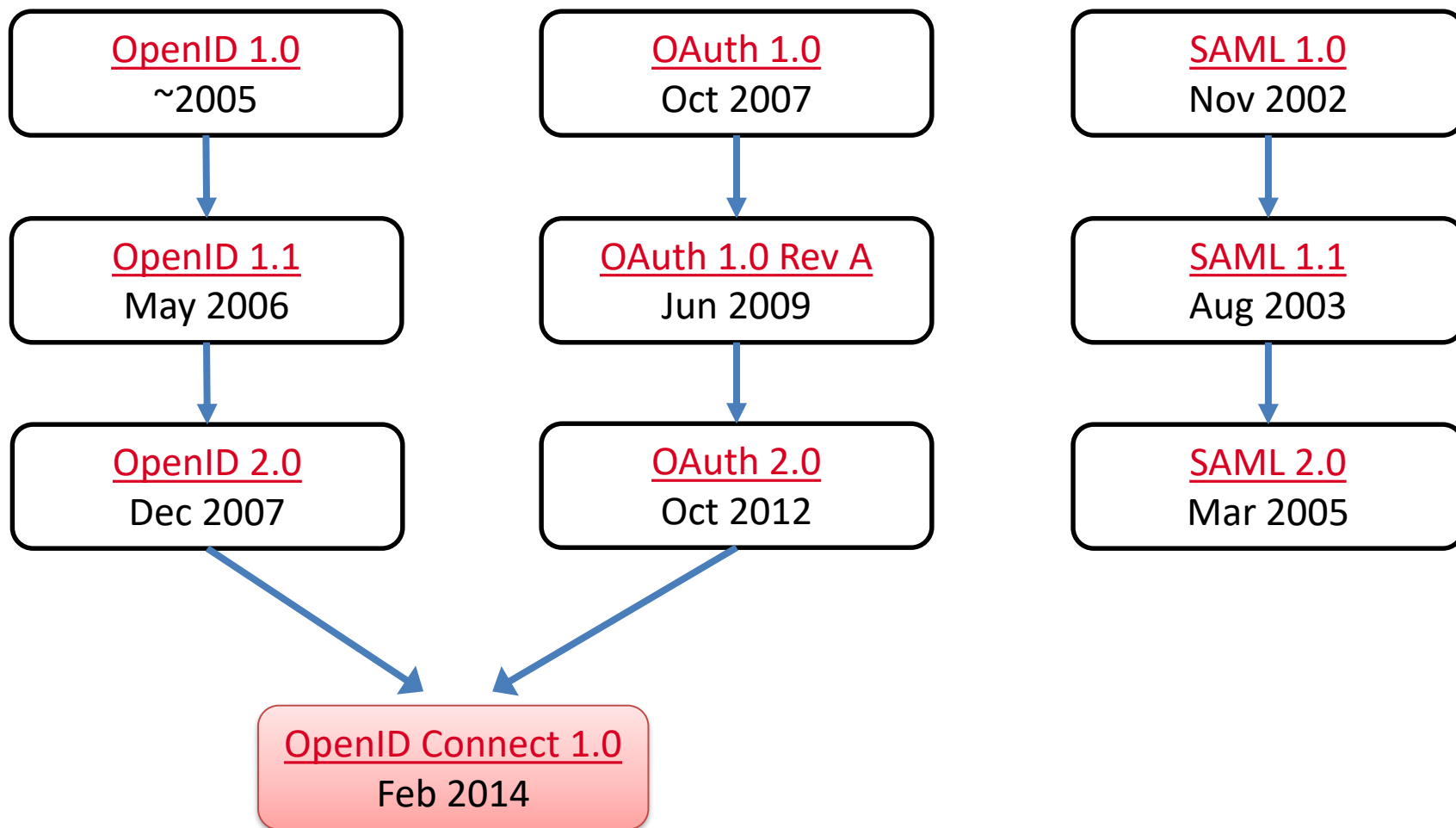
HACKMANIT

Dr. Christian Mainka | @CheriX

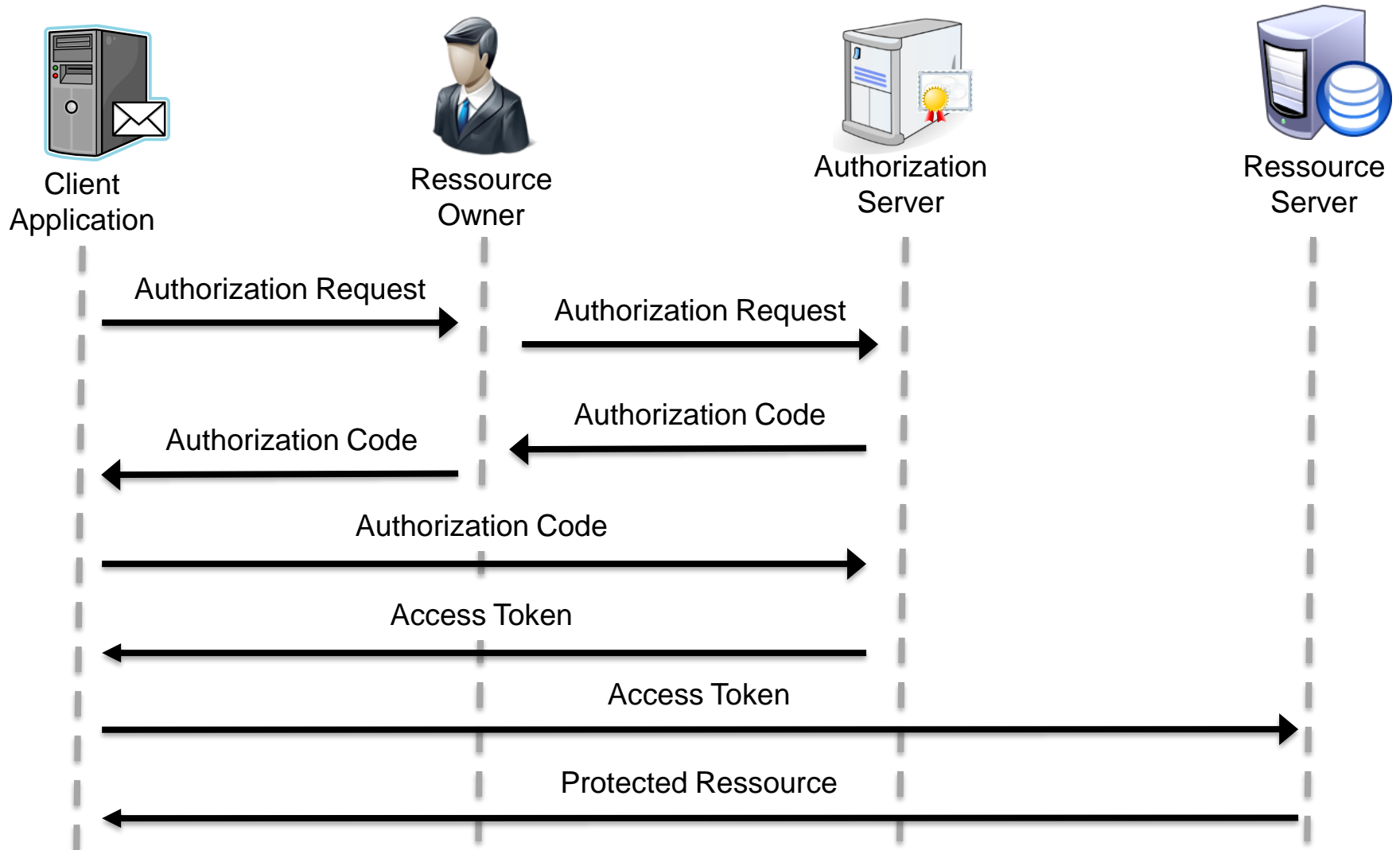
# The Password Dilemma



# History of Single Sign-On



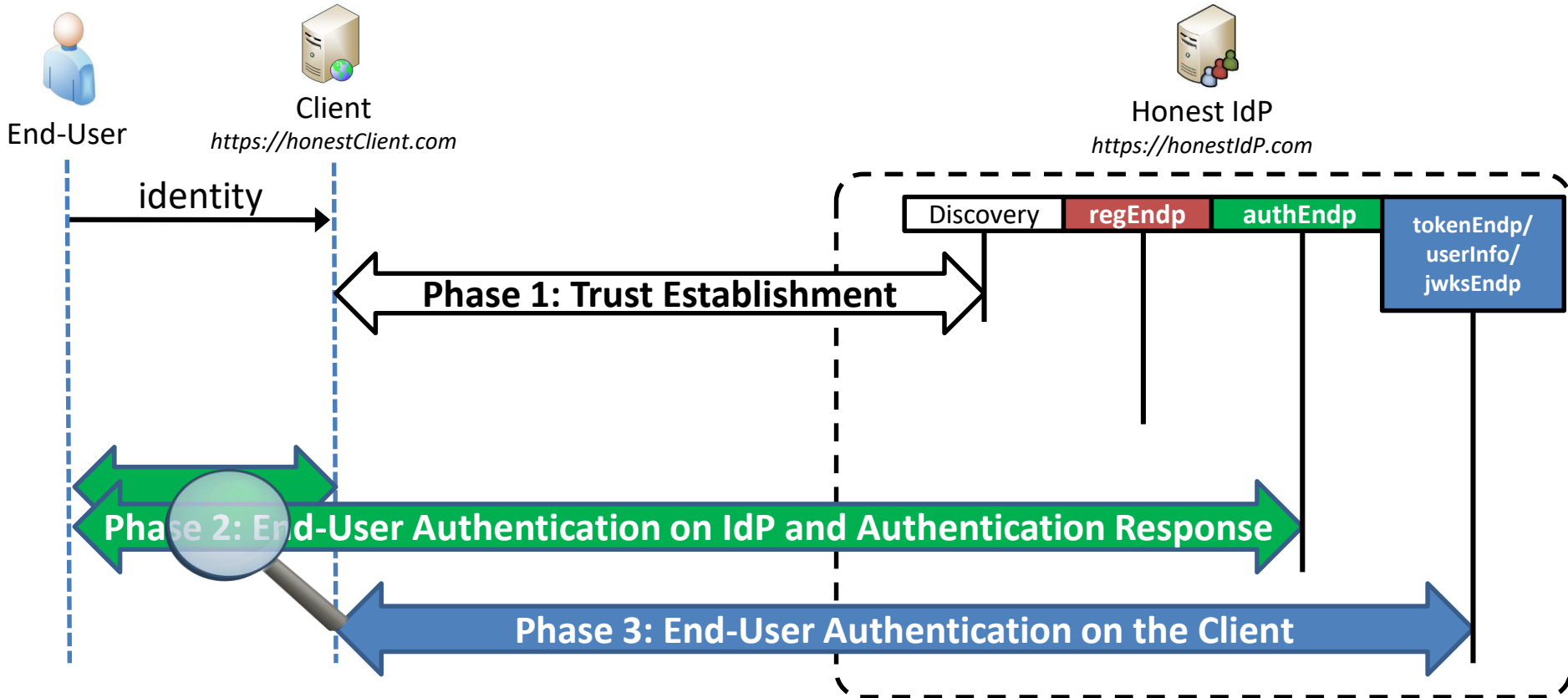
# OAuth 2.0 Overview and Terminology



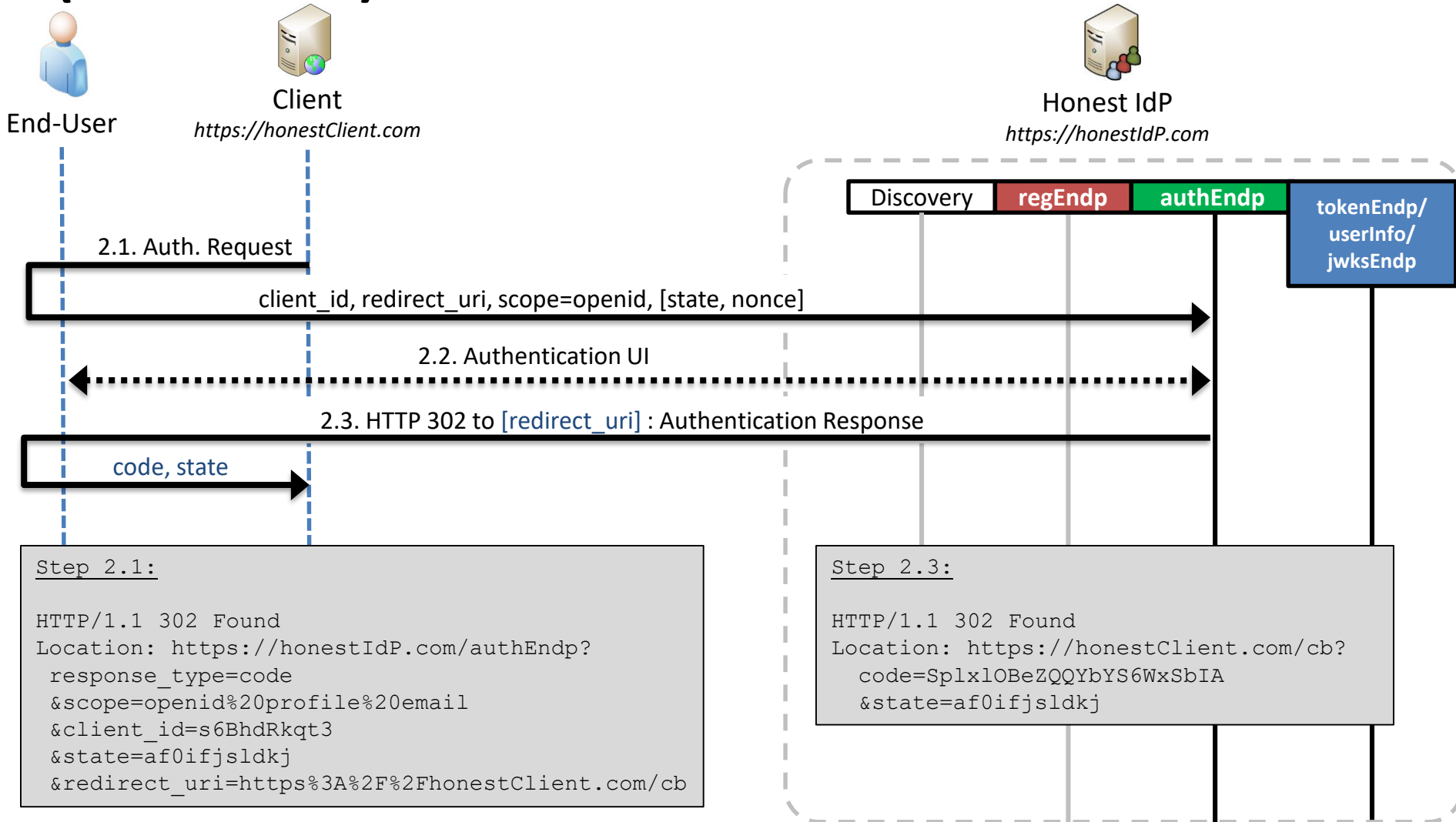
# Agenda: OAuth

- 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

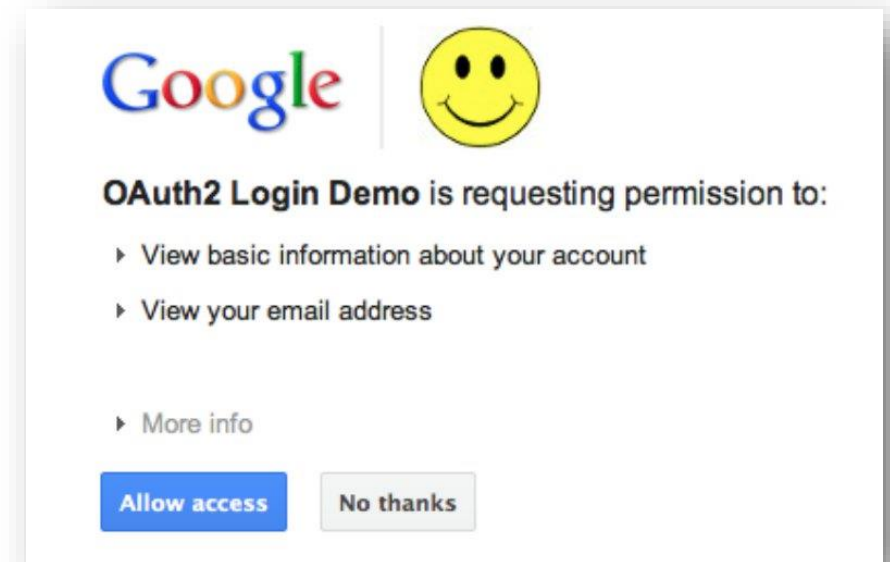
- OpenID Connect has `scope=openid`
  - OAuth does not define a scope value
- Flow distinguished by `response_type`

	OAuth	OpenID Connect
Code Flow	<ul style="list-style-type: none"><li>• <code>code</code></li></ul>	<ul style="list-style-type: none"><li>• <code>code</code></li></ul>
Implicit Flow	<ul style="list-style-type: none"><li>• <code>token</code></li></ul>	<ul style="list-style-type: none"><li>• <code>id_token</code></li><li>• <code>id_token token</code> (token means <code>access_token</code>)</li></ul>
Hybrid Flow	(not existing)	<ul style="list-style-type: none"><li>• <code>code token</code></li><li>• <code>code id_token</code></li><li>• <code>code token id_token</code></li></ul>

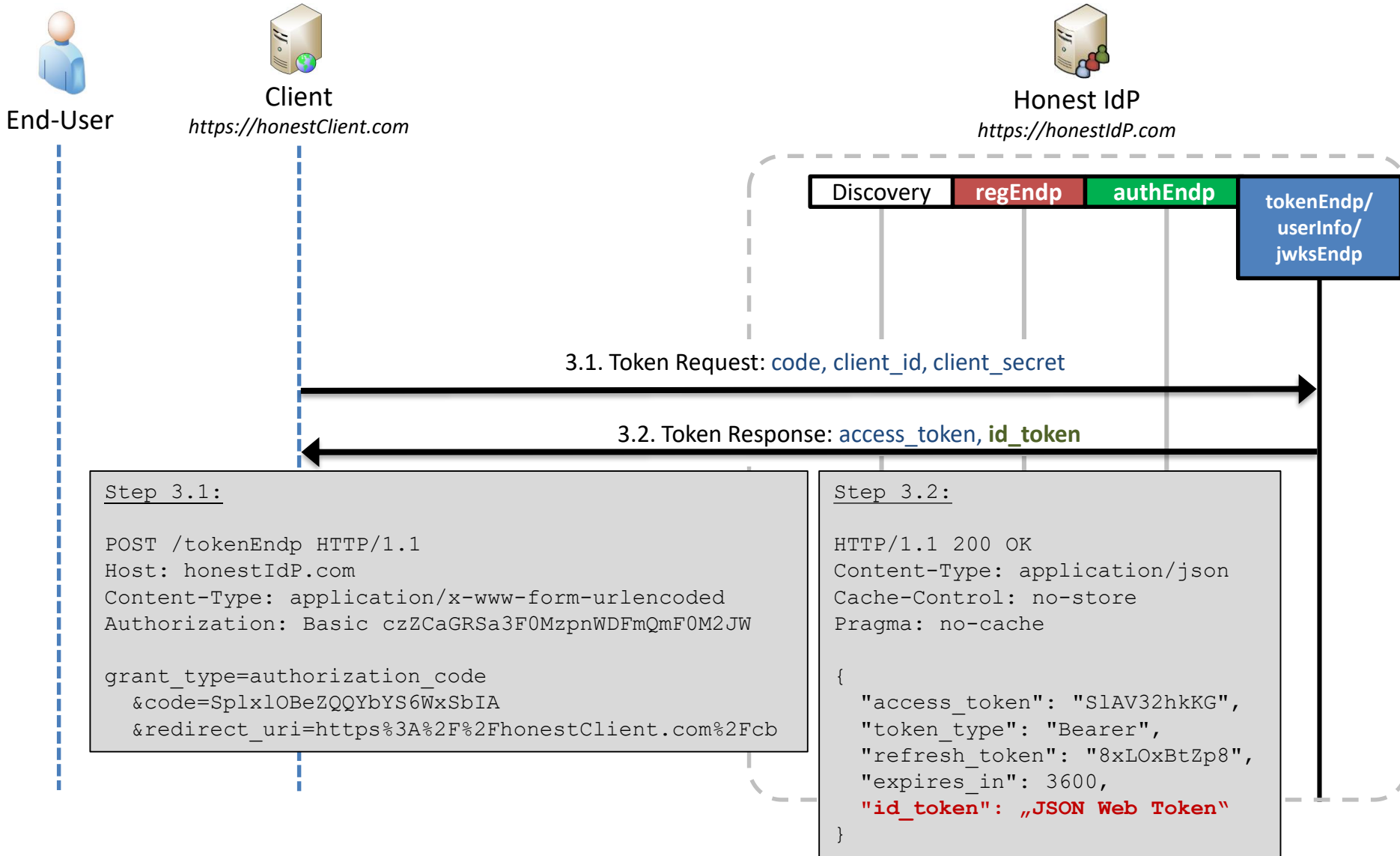


# The Consent-Page

- 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

## JWT Header

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

## Freshness



=

iat

exp

nonce

## JWT Body

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

## Recipient



=

aud

## JWT Signature

```
[0x02, 0xF1, ..., 0xDA]
```

## Security



=

sig

alg



# HACKMANIT

THREAT ANALYSIS | TRAINING | PENETRATION TESTS

Dr. Christian Mainka: [christian.mainka@hackmanit.de](mailto:christian.mainka@hackmanit.de)  
[www.hackmanit.de](http://www.hackmanit.de) | @hackmanit