JÖNKÖPING UNIVERSITY

School of Engineering
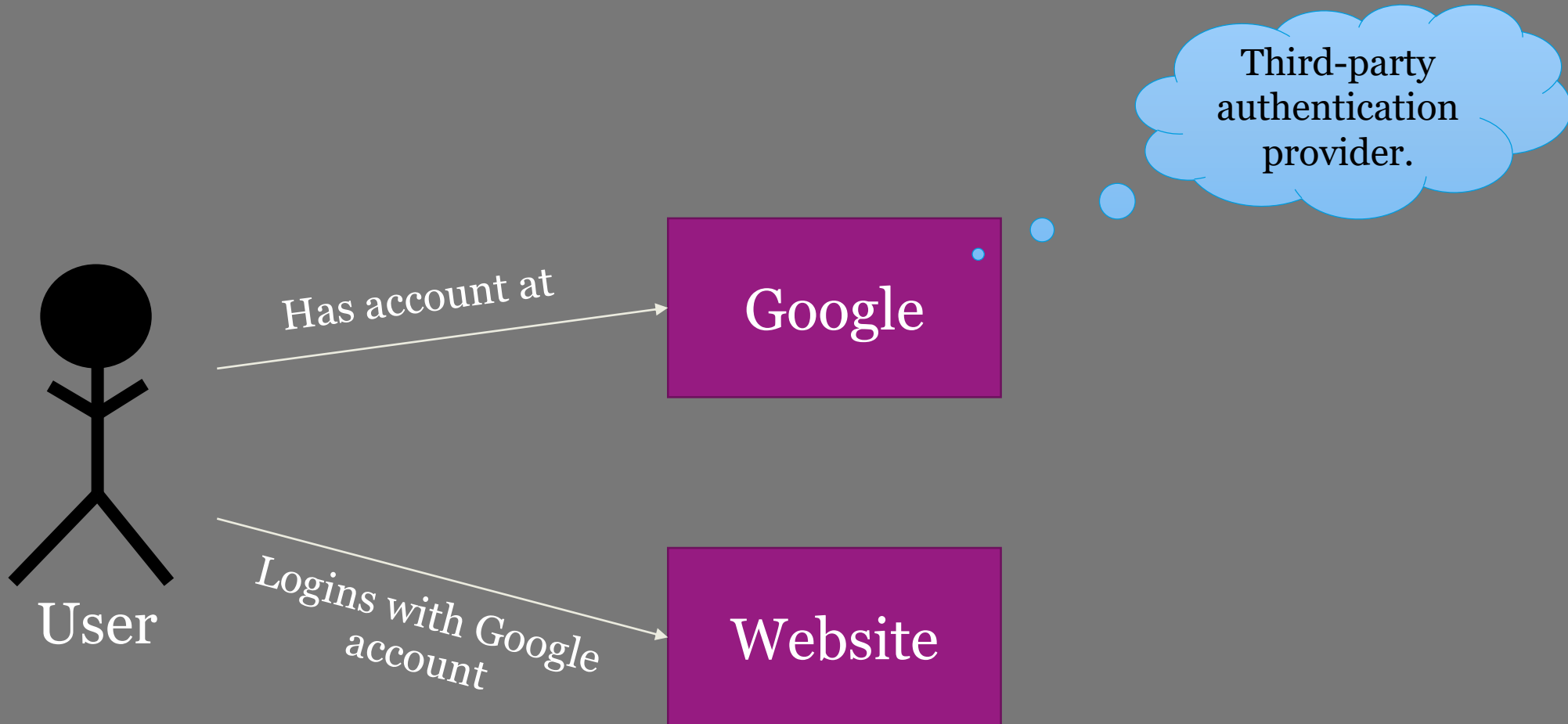
THIRD-PARTY AUTHENTICATION

Peter Larsson-Green

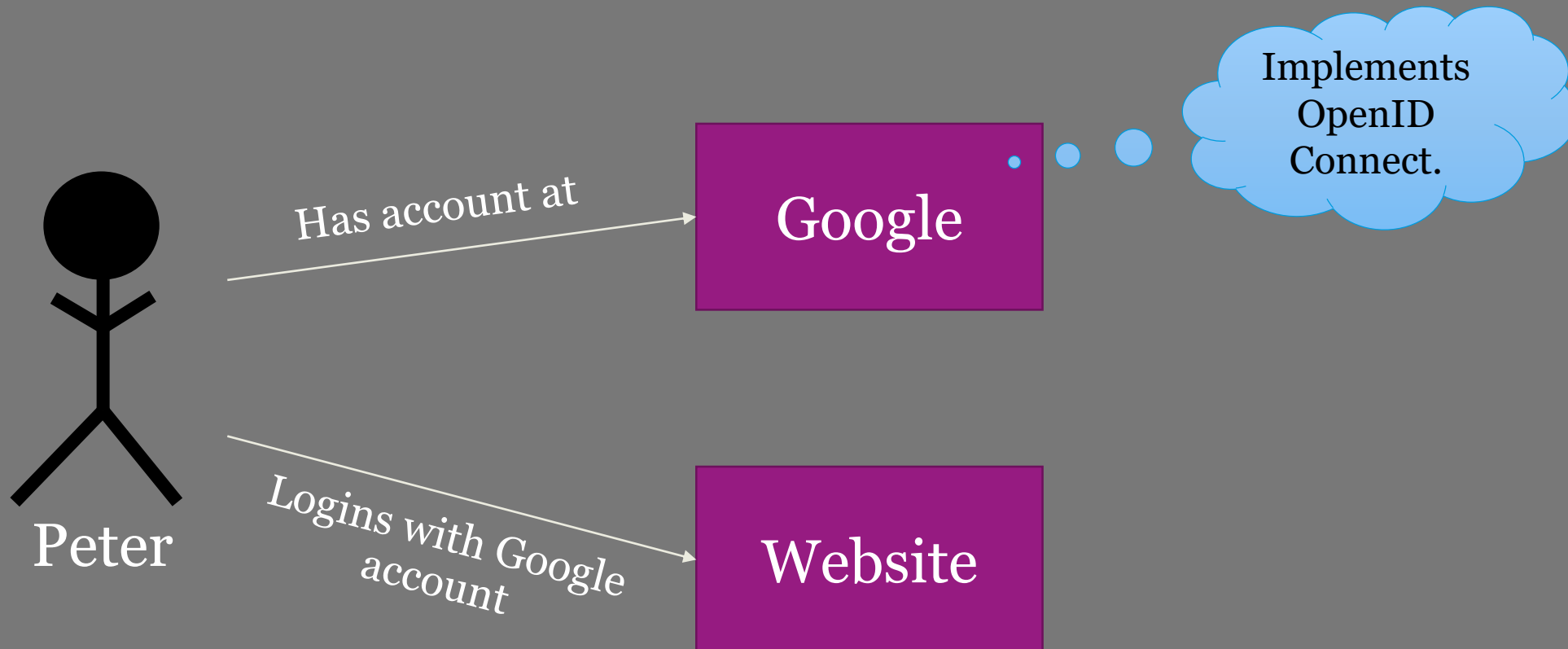Jönköping University

Autumn 2018

OPENID CONNECT - WHAT IS IT?

An authentication layer built on top of OAuth 2.0.

Implements OpenID Connect.

Has account at

Google

Logins with Google account

Website

Peter

OPENID CONNECT - HOW DOES IT WORK?

Pretty much as OAuth 2.0, but:

- You receive an *ID Token*, not an *Access Token*.
  - (you can receive both)
- The ID Token is a JSON Web Token.
- Some of the claims supported by the ID Token:
  - `sub` - A unique identifier.
  - `name` - The user's entire name.
  - `preferred_username` - The user's preferred username.
  - `email` - The user's email.
  - `gender` - `"female"` or `"male"`, or something else.

EXAMPLE

Let a user login with its Google account on your application.

1. Register your application as a client at Google API Console:
    1. Login at: https://console.developers.google.com
    2. Create a new project.
    3. Obtain `client_id` and `client_secret`.

EXAMPLE

Let a user login with its Google account on your application.

1. Register your application as a client at Google API Console.
2. Ask a user to login with its Google account:
   1. Redirect user to:
      ```
      https://accounts.google.com/o/oauth2/v2/auth?
      client_id=YOUR_CLIENT_ID&
      redirect_uri=http://YOUR_SITE.COM/GOOGLE_RESPONSE&
      response_type=code&
      scope=openid
      ```
   2. User accepts and is redirected back to:
      ```
      http://YOUR_SITE.COM/GOOGLE_RESPONSE?code=YOUR_CODE
      ```

EXAMPLE

Let a user login with its Google account on your application.

1. Register your application as a client at Google API Console.

2. Ask a user to login with its Google account.

3. On the server, exchange authorization code for ID Token:

    1. Send a POST request to:
       `https://www.googleapis.com/oauth2/v4/token`
       with the following body:
       `code=`**`YOUR_CODE`**`&`
       `client_id=`**`YOUR_CLIENT_ID`**`&`
       `client_secret=`**`YOUR_CLIENT_SECRET`**`&`
       `redirect_uri=`**`http://YOUR_SITE.COM/GOOGLE_RESPONSE`**`&`
       `grant_type=authorization_code`

    2. Read ID token from the body of the response.