OPENID CONNECT @ DEUTSCHE TELEKOM

Dr. Torsten Lodderstedt, Deutsche Telekom AG
SERVICE ECOSYSTEM AND TELEKOM LOGIN
We rely on open standards whenever they are secure, easy to understand, and to implement.

Therefore, we
- follow the standardization processes
- implement emerging standards
- involve in standardization bodies

Dr. Torsten Lodderstedt / OpenID Workshop @ IIW #18 2014-05-05
WHY OPENID CONNECT?
IT’S SIMPLE AND SECURE

- Simple Identity Layer on top of OAuth 2.0
- REST and JSON instead of SOAP and XML
- No signatures (for lower levels of assurance)
- Protocol Complexity, e.g. Message Format

- Authentication request in OpenID Connect

- Authentication request in OpenID 2.0
THE ONE PROTOCOL

- OpenID Connect allows us to use the same protocol for all use cases since it adds OpenID features to OAuth
  - no need to understand different protocols
  - no need for proprietary hybrid protocol: OpenID 2.0 with OAuth 2.0 token handling

Features

- User Authentication/ User ID
  - OpenID Connect
  - Yes
  - 2.0
  - Yes

- Resource Authorization (Token)
  - OpenID Connect
  - Yes
  - 2.0
  - Yes
  - Yes

- Provides User Attributes
  - OpenID Connect
  - No
  - 2.0
  - Yes
  - Yes

- Web Flow
  - OpenID Connect
  - Yes
  - 2.0
  - Yes
  - Yes

- App Support
  - OpenID Connect
  - Yes
  - 2.0
  - Yes
  - Yes

Dr. Torsten Lodderstedt / OpenID Workshop @ IIW #18

2014-05-05
IT WORKS GREAT FOR MOBILE APPS
OPENID CONNECT INTEGRATION PATTERNS

- Supports the typical OAuth 2.0 integration patterns for Web Flows: web-based for login and REST calls for token exchange and user data access

Alternative 1: In-App Browser

Alternative 2: External Browser

Login URL

http://localhost/myapp/callback?code=3741057699

myapp://openid-connect/callback?code=3741057699

- No hassle with RP Discovery, form-encoded Login Response, ...
- And it’s getting even better with the upcoming results of the Native Applications Working Group
IT WORKS GREAT FOR MOBILE APPS
STAY LOGGED IN

- Long-term access to ID data can be requested using a scope value of “offline_access”
- OpenID Provider issues a Refresh Token
- App stores Refresh Token permanently and uses it for subsequent “login” requests
- Simplifies flow by eliminating user interactions
- Works for any grant type, e.g. authorization code
OUR IMPLEMENTATION
HOW?

- Another interface of our IDM service
- Extension of existing OAuth 2.0 implementation/interface
  - Same client_id can use both OAuth and OpenID Connect
- Core logic is shared among OpenID 2.0 and Connect implementation
  - Authentication methods
  - User interfaces
  - User consent management
  - Session management and single logout
WHAT?

- Starting with basic feature set and extending it demand-driven
  - Grant types: code, refresh token, resource owner password, and JWT bearer
  - ID token signing algorithms: none, hmac, rsa
  - Control of authentication process: prompt, max_age, login_hint, acr_values
  - UI optimized for Web and mobile (display parameter)
  - offline_access
  - claim requests by scope values and claims parameter
  - combined authentication & authorization requests
  - discovery document
- DT-specific session management & single logout
- Telco-specific functions
- 3rd party login and attribute providing
- All kinds of security measures
**AUTHENTICATION**

- App may specify requirements regarding the authentication process
- Authentication process itself (methods, user interaction, etc.) is at the discretion of the OP
- Deutsche Telekom uses
  - username and password
  - stay logged in
  - SIM authentication
- In some scenarios, we also use PIN and/or mobile TAN/OTP
Handling of MSISDN

- Customers may associate their MSISDN(s) to their user account.
- Network authentication based on associated MSISDN
- Applications may retrieve associated MSISDN’s in login response and in access token content
- e.g. OpenID Connect

Authorization Request

```
http://accounts.login.idm.telekom.com/oauth/auth
?response_type=code
&[...]
&scope=openid+phone
&[...]
```

UserInfo Response

```
{
  "sub":"120049010000000046553883",
  "name":"Dr. Torsten Lodderstedt",
  "phone_number":"+491711234567",
  "phone_number_verified":true
}
```
3RD PARTY APPS

- Our customers shall use their Telekom Login
  - for any Telekom application/service
  - for web-based and mobile applications
  - for 3rd party apps and portals

- Benefits for our
  - customers: simple access to additional services
  - partners: simple access to a large user base

- User has to consent to data transfer to a 3rd party application (at least once per partner)

- Partner-specific user IDs to prohibit tracking across applications
OpenID Connect

- Secure, easy to understand and implement
- Versatile in its usage
- Covers all our use-cases or may be easily extended to do so

Deutsche Telekom Timeline

- Mid of 2013: first adoption of OpenID Connect
- Today: standard API for partner integrations is OpenID Connect
- Mid of 2014: switch of our largest service to OpenID Connect

This is also our contribution to the ongoing GSMA efforts on cross-operator identity providing (Mobile Connect).
ANY QUESTIONS?