Mittwoch, 17. Juni 2015 13:49

oAuth & openID

Wir haben für leute die unterwegs sind WS (=Webservies) oder Webservices die über XML kommunizieren.

Die standart smartphones haben kein SOAP, kein SAML, kein WS .

Wir bekommen wir das zusammen ?

Ich habe mein unternehmen da kann ich ein zertifikat auf mein mobilephone drauf machen. Aber nicht alle bekommen ein zertifikat -> wie kommt man nun rein ?

Wie spreche ich den aus der welt draußen wie drinen an? Wie binde ich api's sicher einbinden? - Und as ist jetzt der zweite stchritt, wie komme ich aus all diesen diensten wie java, android, mac, windows phone, php, html5 an web.api's hat z..b von amazon, bahn etc. und wie kann ich das absichern und wie kann ich appls deployen ?

Wie kann ich mit einer cross-plattform mein ziel erreichen? -Und es muss ja auch icher sein.

oAuth & open ID soll dies ermöglichen und eine ischerheit ermöglihcen.

oAuth: nicht ich mache selber mit irgenwem oAuth , sondern mit einer API schnittstelle mache ich oAuth. Der entwickler einer anwendung will zugriff auf die daten eines anderen programms haben.

Z.B. flikr fotodienst und sie mögchten bei DM die fotos drucken. Dann müsste ich eigentlich ja mein passwort und username an DM geben -> also ist das ziel dass ich der anwendung (von DM z.b.) meine daten bzw. bilder geben ohne dass ich ihm meine zugangsdaten gebe.

openID : mit dezentraler Authetifizierung für webbasierte Dienste.

Ich habe eine nacc bei fb, einen bei dm, einen bei google -> wie mrke ich mir die passwörter?
Wäre es nicht geschickter ich hole mir einen account der verwaltet mein passwort -> wenn ich zu amazon gehe kann ich für die authorisierung meinen FB-account nehmen.

Der open id provider sagt dann "habe ich mich richtig authentifiziert?".

Also oAuth -> wie kann ich die anwendung sichern.
openId singelSignOn -> openId. (hier werden applikationen nicht betrachtet)

oAuth

Mittwoch, 17. Juni 2015 14:00

1. Dreibeiniges oauth: wir haben drei rollen, den endbenutzer (z.B. studenten), eine nesrvideprovider ist z.b. facebook, wo man info gespeicher hat. Und der neue der dritte ist der "Konsument" -> die anwendung zu der man geht z.b. bilder drucken (druckdienst von DM) . Der konsumer holt dann vom service-provider die bilder.

DM möchte z.b. die daten konsumieren die biem service provider liegt .

2. das zweite ist eine simplikation davon , ohne endnutzeranwendung -> der konsument und der service provider unterhalten sich unternander z..b für eine wetter prognose -> kann diese information an eine ndritten ausgebn der ishc nicht zu erkennen geben muss.

Alice möchte fotos mit freunde teilen, diese packt sie in eine dienst z..b faji, flikr (foto sharing dienst) und frag den freunden das ist meine id. Diese fotos makiert sie als privat.

Sie nimmt dann z.b. beppa und sagt ich möchte fotos drucken. Und die fotos liegen auf einem foto server (z.b. faji) .

Der bepper server schickt ein request an den faji server , ein "anfrage token" , damit eine sitzung etabliert wird und diese sitzungskennung benötigt.

Ich muss diese nfvogang authentifizieren - der request von bepper an faji wird übergeben, hier muss ich dan meine daten eingeben , hier wird ich jetzt gefragt -> bepper will darauf zugreifen, willst du das erlauben, ja / nein. Wenn ich es nicht erlaube geht nachricht zurück nicht authentifiziert, wenn ich es erlaube holt es die bilder: die freigebenen bilder werden an den konsumenten beppa ausgetausch und kann da auf print drucken . (das wars grob).

Damit das geht, muss der programierer der konsumenten-anwendung (bepper) muss vorab mit service provider auseinadner gesetzt haben und sagt ich möchte von dir bilder holen für meine kunden und damit das möglich ist und man von sicheren bilderholen sprechen, müssen gewisse dinge ausgetauscht werden.
Der serviceprovider sagt ich eb doch nicht alles heraus -> sag mir name, autor und sagt mir url von der du kommst.

Was ist ds ws akzeptiert wird?

- Ei nkonsumentenschlüssel also der schlüssel mit denen alle date ndie zum service anwender schickt . Diesen schlüssel wird in die anwendung hart reinprogrammiert.
- Ein geheimnis bzw. ein public key wird noch zur authentifizierung bzw. signierung verwendet ("challange-response" , dass der ander das nachrechnen kann sagt "ja kommt von dem passt".

Folie 19:

Entwikler geht zum service-provider sagt ich möchte schlüssel haben, service provider bekommt schlüsse und packt diesen in seine anwendung hinein.

Wie sieht nun das dreibeinige oAuth aus: (folie 20)

Der edanwender wendet sich an den konsumenten (z.b. bepper oder dm) und sagt möchte fotos austauschen Und sagt meine fotos liegen bei z.b. facebook oder faji. (man kann keinen beliebigen wählen die anwendungen müssen sich kennen).

Dann schickt der konsument eine nicht bestätigte anfrage bzw. anfragetoken mit einer nummer(token) , was sagt ich möchte mit dir daten austauschen.
Dann schickt der service provider einen token zurück und sagt ja lass uns kommunizieren spielen (beide sind ja verschlüsselt.).
ACHTUNG BILD STIMMT NICHT

Der consument leitet den endannutzer nun zum serviceprovider (re-direct zum serviceprovider) beim servie provider logt der endannutzer sich nun ein, bekommt vom service provider die daten zurück geschickt .
Wenn der endnutzer nun zustimmt wird der endannutzer nun an den konsument zurückgescchikt punkt 7

Bekomme redirect zurück zum konsumenten . (hier kam ich nimmer so gut mit) Das ist schritt . 8. 9. 10. 11

Web ist ja ein zustandsloses protokoll: also müsste ich mit jeder neuen anfrage mich neu authentifizieren und alles neu machen, wenn nicht etwas zwishcengespeichert wird.

Sinn und zweck ist: ich möchte ienem konsumenten den zugriff auf service-provider anbieten.
Da den in der mitte (konsument) meine zugangsdaten nichts angeht, authentifiziere ich mich beim serviceprovider und der stell teine autoamtische anfrage an den konsumenten.

Man bekommt der konsument und der serivce-prvodier ein sitzungs-token und der Endbenutzer und der serivce-provider ein sitzungs-token.

Es werden nur die nummern ausgetauscht und wird nur geguckt ob das passt - bei oauth.
(wikipedia zu oAuth ist scheisse, gut ist heisse.de , hueniverse ist gut.

oAuth 2. hat den großen nachteil gibt nicht viele fertige bibliotheken.

OpenID

Mittwoch, 17. Juni 2015 14:25

Ich möchte mich einmalig irgendwo anwenden und dann nicht mehr (z.b. bei einen applicatin rovider).

z.b. google, facebook -> und unter dieser url bin ich eindeutig greifbar. Und wenn ich nun zu einer webseite gehe wo ich mic hauuthentifizieren soll.

Damit das geht benöitge ich die open id, eine url da stehckt mein name drin .
Alle gorße sind open-id provider , jeder kann ein open id provider sein. Die frage ist - wem vertraue ich meine identität an.

OpenID open source , gibt's in c, c# , php, python, ruby & java - nur wer traut ihnen?

(etwas älter als oAuth… . Ab 2007 gabs dannn eine foundation die ein standart daraus vereinbart haben.

2014 2 mio webseiten sind die webseiten bei denen man open id eingeben kann und nachsehen kann beim open-id provider. Und sogar über 1.3 milliarden nutzer.

----- ACHJTUNG utnerscheidung openId-anbieter und "dienst-anbieter"

Pro
Singel sign on
Alle daten einmal hinterlegt super
Man kann bei unterschiedlichen open id providern konten machen
Da man nicht bei allen ein passwort eingeben muss und ich nicht weiss wie die mit meinem passwort umgehen macht das mein opnid provider von mir.

Kontra.

-jemand könnte versuchen meine id mitzulesen (phishing) und wenn ich dann den anwender dazu bringen auf eineer gefakten seite meine daten einzugeben bin ich drin.
- man ist abhänging vom open id provider
- Der open id provider weiss dann ziemlich genau was ich so tue , z.b. google kann gute benutzer-profile von mir zu erstellen und diese benutzer-profile können verkauft werden. Bin ich aber biem kleine nanwender gibt's den morgen vielleicht nicht mehr.
- Weiss ich den ob ich dort wo ich bin ein gesichertes protokoll habe?
- F

Weiss ich ob der open id provider und applikation anbeiter ob die die daten gesichert austauschen das ist hier die gefahr - früher war das manchmal nicht der fall ist heute igentlich erledigt wegen https .

Pro für anbeiter
Ipro kontra von anbiter
- Ich kann tolle surfprofile erstellen (als openid-anbbieter))
- Für den dienstanbieter (=ist z.b. ein webschopbetrieber , der dienstanbieter hat von mir nix , das kommt vom open id-anbeiter bei dem findet die authentifizierung statt).

Kontra:
Der open id anbieter muss erhöhte sicherheitsvorkerhrungen treffen wie ler das ziel gern ist.
- Der dienstanbieter
- Open id-anbeiter und dienstanbieter sind von einander abhänging

Folie 27 wie funktioniert das

(youtube dienstanbieter) ,
1. youtube schickt mir eine autehtitfizierungsanfrage an nutzer, dann schickt der nutzer:

2. die open id zurück (die url , eingabefehl)
Aus dieser url kann der idenstleister, welcher open id provider z.b. google, hs mannheim etc. herausfinden wer der username ist und der open id anbieter.
3. applikation wird also biem open id provider gucken ob es den nutzer gibt.
4. wenn der open id server sagt ja den gibt es, bitte kommuniziere mit diesem und jenem server. (adresse)

5. applikation fordert nun für den nutzer die authentifizierung an . Durch die rückgabe des open id providers
Schick 6. open id provider an den nutzer die anfrage gib mir dein login name und passowr 7.

8. open ip provider schickt an die applikation

9. erlaubt zugriff auf die gesicherte verwaltung.

Besonderheit ist iher in der mitte der identitäts verwalter oder bei oaut der verwlter der zugriffsrechte.

"openid-connect" wir ind 2-3 jahren wahrscheinlich das mittel der whal werden.

Was sie auf jedenfall mitnehmen sollten klausur:

Was ist openID:
Open id ist nur dezentrale authentifzierung - ich gehe zu irgend einer applikation will daten da haben und will aber kein login und passwort geben -dass z.b ich wo anders . Aber ich bleibe in der einen applikation.

Was ist oauth
-eine sichere api-authorisierung frü eine applikation, dass wenn eine applikation auf daten einer andere napplikation zugriefen will - wie ich die identität credentials durchreiche ohne dass ich die passwörter geben muss.
Ich mache dich zu meinem stellvertreter dass du an eine andere applikation gehst und dort die daten holst.

Unterschied paypal, sparkasse, bei der sparkasse meldet man sich nur ab, während man paypal die abwiklung der bezahlung abwikelt.

klausur

Mittwoch, 17. Juni 2015 15:23

Zusatz

Er lässt weg wep .
openid und openAuth wie passen die zusammen ?