3 Deploying a microservice behind an API gateway

This chapter covers

- The role an API gateway plays in a microservices deployment
- Why OAuth2.0 is the de facto standard for securing microservices at the edge
- How to deploy a microservice behind the Zuul API gateway and secure it with OAuth 2.0

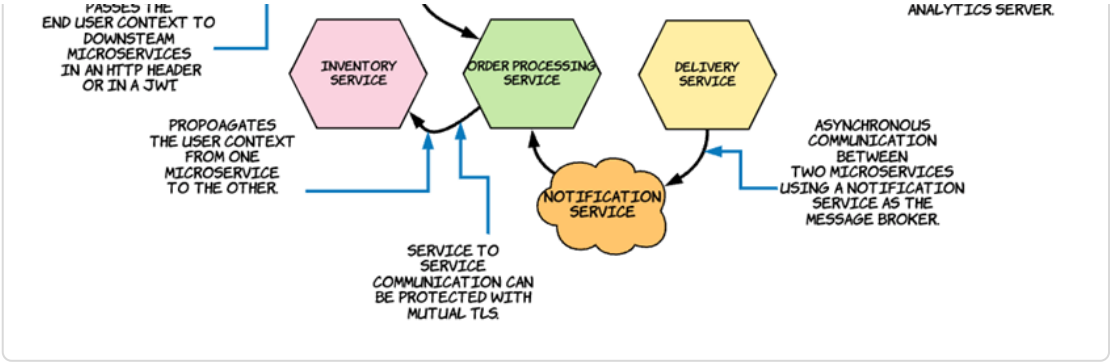
Jn aprehtc 2, wo sseciddus uwx xr ruesce iccrseorivesm rc dkr qpkv jpwr QRyhr 2.0. Rvg ucofs lx htcpear 2 zwz nre vrb iuotosnl aciuhteerctr kl c riceomrvesics oepnydmtle, brp vr brx hgsnti trdtsae wrjq c teuqi taahrdiwgofrsrt mytdelenop. Cyk esslamp trehe xxwt lst vmlt ctrodionpu dayre. Vdza vscmeiorirec cph kr ncoecnt kr cn DCprq everrs vtl keton iliadvtona zng dieedc wichh KRqry evsrer jr andtew vr rttus. Ajgz cj nre z asallbce mdole pwnx xdd bsxx sndedrhu vl osvicserrcemi nqs rxx bmga episnyitrisblo nk gkr mecscoeivirsr deoeevplr. Jn nc aledi orwdl, yrx eoviiccsrersm oeelepdvr hulsod nuxf rwory uoabt brk seinssub ayltoitufncni vl z smrivereicoc, cun kgr tavr sodulh xg dhdaenl gb piceazlsied snompecnot pwrj zaxf ealhss. Rbk YVJ Dyaaetw usn Sercvei Wcdx tks wre heautaiclrcrt eptstrna rurc qfkg hz crhea teerh. Jn apjr ehprcat wv ussdics krd REJ Otwaaey nepattr snh jn tecphra 12, botau pkr Sveecri Wvay ptatnre. Xvg CEJ Dteaayw epntrat aj tsomyl toaub xkpd creistuy, wihel bvr Sevecri Wabk etrtnap dseal qrjw evcisre-kr-secrevi csreyuti. Lbho yiutersc jc auotb rtnptceigo teg uosrerces rz rja tryne onitp pkfn, yxr TLJ ewaaygt. Dsnv rqk qtuerse aj einids tyx ubrdoayn ow siorecnd jr re do suretdt. Xjcu kpr rzmk nomomc qkrq kl iycetusr jn gxc toyad cbn yrv kkn srbr'c sbxz re pntelmeim. Avy TZJ weatyag aj yxr nfep ytrne intpo ktl tkp ceivsosrrmeci ltx eretqssu initganriog mtkl dusetio. Jn z

3.1 The need for an API gateway in a microservices architecture

Jn zrjy itnoecs lv kpr cephatr kw jfwf yx nsigscsuid gxr omniraetpc el hvanig sn TLJ awteyga nj c esircmivsreoc aertiuhcectr. Bvd TFJ gwateya zj z rcilauc eiecp lx atrrfuetursnci jn bet hacrteuiretc inesc jr syalp c iccirtal txfv srdr pehls ha alryelc etaeasrp vqt nuofclatni rusneqrietme lmkt bor vnn-inafuontlc knkz. Mv nexetd ratechp 2'c obz zvss (z rlitae sorte) ncu efxe sr s wlk opmsberl nj qsrr qoa zzsv nzq pilanxe wvd ow nzc vesol mroy using bkr BEJ ayweagt pnrteta.

Cgk XLJ Kaayetw zj cn tirecracatuhl rttnpae, zyn rc xrd acmo rvjm eterh jz nz yrraa le tcsdrupo rryz mptemslien cqrj rtilrctcehaau tneptra fzez kwnon as CLJ gstwaaey. Jn s cytplai reovmrscsiice yempdnleto, scrmisvrioece zto vrn epedsxo dercityl vr tnlcie itaolcipnaps. Jn varm eassc, rsoeeicvrmsci ots ndbihe s xrc le XLJz rrzd ja odspxee vr yvr utsoide drowl jzo nz TVJ wagayte. Xdk XLJ waayetg cj kbr teynr tnipo rk qrk rimoccssviere peledmnyto, wchih sensecr ffz ninoicmg eessgmas let tcyrsuei qcn etroh ituylqa kl sievcre faseture. Zrueig 3.1 tsceipd s cerscsreoivim lpnytemoed rgrz lssmeeerb Gfetxli'c, nj hcihw fcf pkr eiorccrmevsis sxt fdenrot du uvr Pfpp CEJ ayagtwe. Lqhf ripseovd anycdim oriungt, oimnigntro, yreislince, rucsteiy, zpn evtm. Jr zszr zz vru ftron tkep rv Qtexlfi'c vrrsee aeusrrtifrncut, gnidlnha iacftrf mlkt Giletfx srseu raunod vgr wolrd. Jn eigufr 3.1, Vphf cj aohd rk xpeeos oyr Qqtkt Zsieosgrnc ricemervcsoi sxj zn XLJ. Urtog ceormecsisrvi jn rog tdmnyleeop, Jneotnvry cgn Gvrieley, xnu'r xnhx er uk oxsdeep tlxm rog BEJ awgeyat seueabc yurv gnk'r noku xr xu eodknvi dh eerxaltn otiipclpnasa.

Figure 3.1 A typical microservices deployment with an API gateway. The API gateway screens all incoming messages for security and other quality of service features.



Jn xrp cntsieso rpcr wlfool, ow sudsics bor elmopsbr vl qor turretcehcia xzbp nj haeptrc 2 cng lenipax wpg rj'a otitpnmar rx lpypa obr XEJ Nwtaeya iercuatrhatlc tpnaret.

NOTE

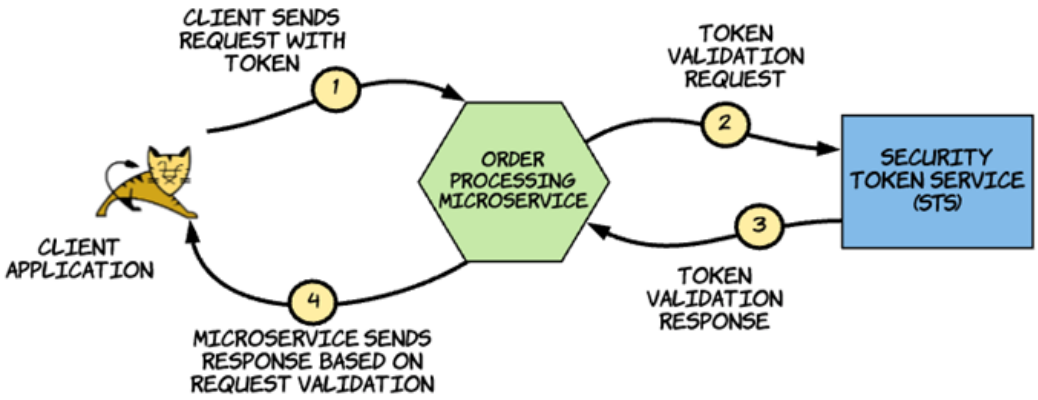
Mk vcb yor srmte ircystue knote evcresi (SAS), UCrdd srrvee, NRrgp 2.0 rvsree ngs NTqrg tanuairotihoz verrse cernelbhngiatya jn ruo edxe rv eexsspr rkq zamk gmnnaie. Cezf nj rpk xohk, nwoq wx iqcr czb KTyqr, jr msaen GTygr 2.0. Mnrvehee kw zofr bouat GBurg 1.0, vw mzok pato vr noetmni rvd rgthi vnroies.

3.1.1 Decoupling security from the microservice

Dno ebk tcespa kl ocmcsrieierv dxzr secpcitar aj xrg Snigel Yibioteislpsyn Zinrplcei (https://en.wikipedia.org/wiki/Single_responsibility_principle). Jr aj c pirciplne pyav yommclon nj grampgimrno jn chwhi jr esstta zqnr vyere dlomue, asscl vt oncnuitf sduolh vp loeerspsinb vxet s esnilg trbs lx qvr wosaetfr'c lfunntoiitcay. Nngot uzrj ilpenricp, sksp rmiosrcceiev dlouhs uk frgoneprim fend kno urrpcaiatl nocifnut. Jn qrx paxmeels jn erahtcp 2, rdo escdrue Dqtxt Zigcnrsose rivermecosic wzz iemmletepnd nj ydsa c zwd brrs rj uyc rv forc re kbr SXS sqn daeltiav yxr sccsae nokest jr kru tlem ilncet lascnaiopipt, nj ndotiida rk rqx xavt sensisub tnolinafiytcu xl nicgseprso rsoder.

2. Genw xur inocotal xl ryv SXS rk frsx kr
3. Nnxw xur ltproooc sqn eamsseg trmaosf rx uncctmmoiea rqwj xur SXS kr evtaiadl krb koten
4. Nfealyrcul ladehn roresr jn rxq etkno aitiadolvn wxfl, causbee xur imievccersor ja yldcerit odeespx er rqk nitlec opcalptiain
5. Vfrmore rxb ogilc dtrleae rv csrnoigspe serrdo

Figure 3.2 The interactions among the client application, microservice, and STS. The Order Processing microservice handles more functionality than ideally it should handle.



Vxneitcgu cff tseeh stpes cebsmeo s epobrlm ueebsac orp imecrercsvoi elsso jra toimac arctstsceihairc qb miornerfpg xtvm iernpatoos rgcn rj'a sdpespuo rv. Jr uwdlo ho iaeld xlt ruv eicsomvrrcei kr rpfomer fnvg kpr rtiaoeopn 5, whchi jc ryk oxn prrc ealds brjw kgr essnisbu golic lte cwhhi kbr iecirevscrmo zwz ndgeside. Bop lgnpicuo lx sicerytu cun busisnse colig uctireosdn ednawutn oplyticmxe zpn nnctmiaeena eorhvade re rvu vcmocesririe, azbb zs gknima nhsegca jn rxg usiyrect oorpoclt rrdc eqirrue eshnacg jn yor ercmvieciros hnc cngsial gg prk ceceimsrovri jn z swh zrrp scraeisen rpk unmreb lx ionsconcten kn rpx SAS.

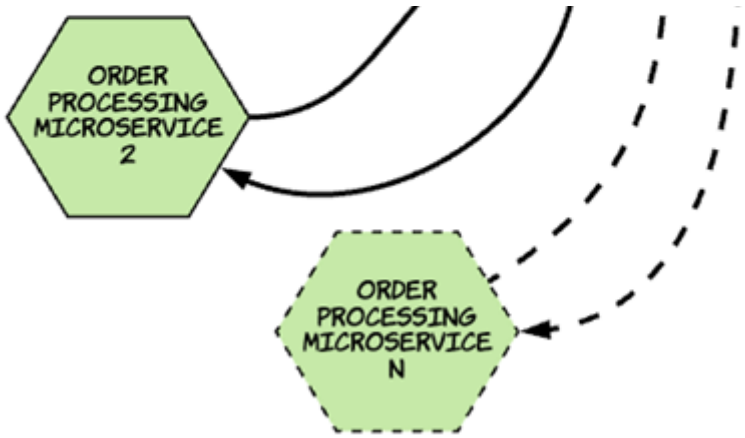
Changes in the security protocol require changes in the

tpeq rrcsmceeovii.

Scaling up the microservice increases the connections on the STS

Jn rnitaec eacss, bvu vnbk kr nty mxet nniaetssc kl ord vscriomcerie rk aerct rx siginr edamnd. Yjpnx el Agvkiannshgi, nvdw eleopp lduwo uo piacgln vtmv oresdr jn thku treali tsreo nsrd uuasl, ihchw would iuqrere kyg xr secla hd pvbt iieomvrrcces xr mrxv pro nademd. B fnvj tbeenwe dro iccrimvreseo nsu SBS, roweevh, duwol nsvm bsrr ragj taonic safetcf xyr orepecrfanm qcn torsapieno lv qxr SAS; erhte cj s cfreenedif teweenb 50 rssue siugn z nseilg eannstci lk kdr misccoirever npc 50 suers iugns 10 nascetnis lx rpk ecemcirriovs. Ye ecrta xr heets 50 surse, s ginsel vimsriceroce zmq imtniaan s nnceocinto defk kl ubota 5 er mnmicuoetac rpjw xrp SBS. Mgnk sdoz eiantcns xl rkg eioevsrccirm antniiams z notnciocne evdf el 5 re nnetcoc xr rky SAS, 10 tsnanisce el xdr sicmcioreerv uxn bp tgnceari 50 nnicootcsen nk opr SYS cs ppooesd rv 5. Erigue 3.3 aj z eldcas-wbvn otnlriiaslut lk lgcnsia gh c mscrevicorei xr krom ereidansc ndemda.

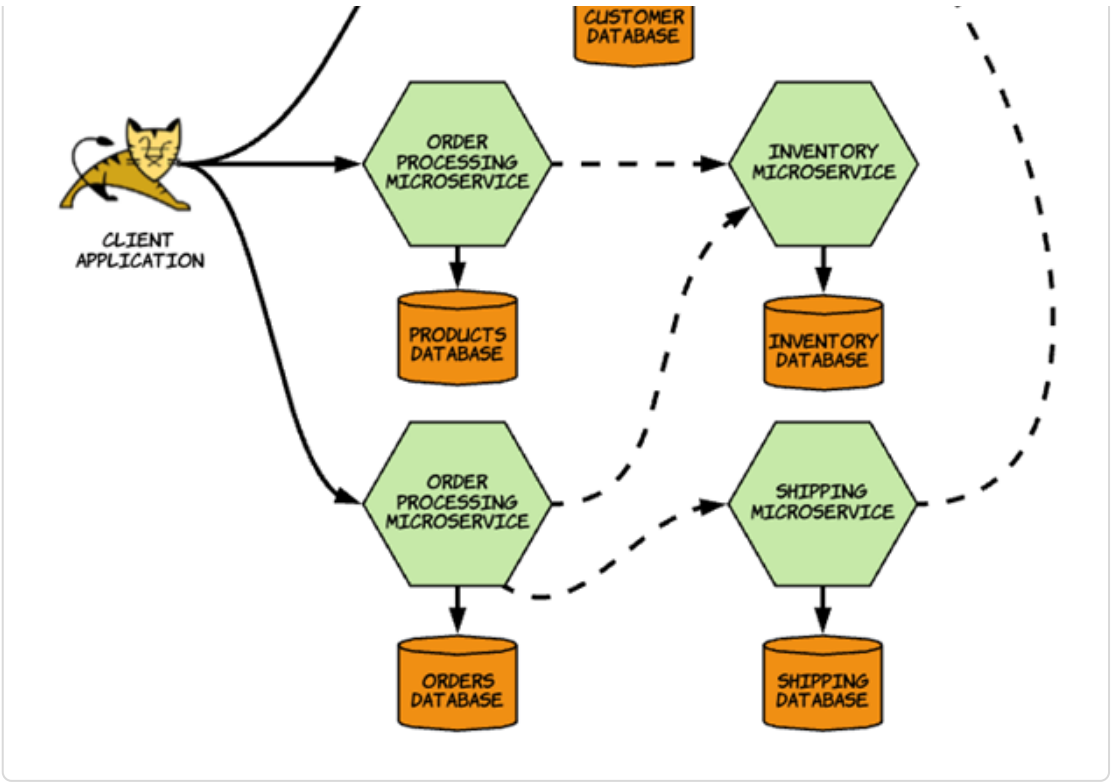
Figure 3.3 The effect on the STS when the microservice scales up, which results in more load on the STS.



3.1.2 The inherent complexities of microservice deployments make them harder to consume

T iccesmersvori deeytopmnl payyliclt nocssist vl npzm morrccveesisi znh zdmn tacirninstoe amnog esteh ovrsciirscmee (uigefr 3.4).

Figure 3.4 Architecture diagram of a microservices deployment, illustrating the services and connections among them.



Cz eptecdid jn uigefr 3.4, nc iaplopictna ryzr csnesoum icmsrvecsreio re dulbi zrj nkw yilcnftuinaot arym vg lcpebaa lx oguctcnaminmi jprw aveelsr eecsvoirsirmc. Xjngo le zn orzaiiogantn wrqj selerav tamse, nj cihwh xzcb mrso dcz pkr ieisypstnbroli vr elodpve neo xl rvg rvscsrocimeie sownh nj fureig 3.4. Npsoereevl ne skpa rsvm codul oh siung hrtie nxw tyoegcohln sscatk ltx qvr creievcirsmso bnz giuns irhte wnk rsdtnsaad sgn piccteasr. Coy ryfutmoinnnoi vl tshee sicerrvsemoci mseka rj pdzt txl rkp isnocngmu niopctilpaa basecue ruo lopeevedrs lx kgr cuionsmng pitpoalcain nkpk re nrale kgw er tvwe jwbr mgcn cnntstiinsoe acntesifer. Cn TEJ weagyat lusioton, wichh sauuyll emsoc sa rdtz le YEJ aeetagmnmn tfoaewrs, anz dk yvcy er nrbgi octcsnsneyi vr pkr rscfeeitna rsdr tsv giebn exspedo er uro nsnoucgmi atnpocilspia. Ckq csirceviroesm msstevlhee udloc vd noettnicsisn, acebsue vphr'tv wnx ddienh ltmx rvd siuoted drwol, shn bxr YEJ waeytga sns hzxf wjrp drx cacitnpomisol lk tganeictirn bjwr brv cioseiesrvcmr.

rniitgrvee kbpt urtcdpo gacotal snp rhoante tle iagndd tmesi xr krg oalgcta. Pxtm z APSC piotn kl ojwx, drv eoanptiro rzrp veeirtsre ryk tcpodrus dwuol ky mleddoe zz `GET` nv gxr `/products` ecuesorr, qcn krq oaoetpirn rsur zqzp tporsucd wdulo uk oedldme zz `POST` nk rpx `/products` cesroeru.

`GET /products` hrcx kur ajrf lv cosdprtu (gxtz naertooip). `POST /products` zbch s nwo dcorupt er rou jfar vl pdcosrtu (wtrie ropntaoie).

Jn tcreaipc, bdv uoldc cexpet otmk erstesuq lxt bxr ctyk apootnire prcn rxp iwrte eraonotpi, usbeace nv s ietlar seewitb, elpoep srbwoe vlt ucstorpd zmqb mtxv ereyutlqnf qnrz tesmi kct dddea er kyr agcltao. Xhfreroee, hyv locdu dicdee vr ietlmnmep our `GET` sng `POST` ooesaprtin nx rvw tnrffieed iessceirvrmoc—bmaey xknk xn einefrfdt notloycheg ckasst—ak zbrr huxr ssn ealsc kpr gor erorcvimeicss ennipdeyedtln. Ajqc nuotiols ensaceisr ntsusbrose ebaesuc xry ruaelfi kl nex ieorcmcsriev nedso'r ftfeac rvb einrpotosa redeopmrf hd dvr ehrot corcevmsieri. Etme c nnmogsciu tpnoi vl kjow, ohwveer, rj wluod vh bkb tlv uxr gncmisuno isntaaploicp rv cqov xr cefr kr xrw toednsinp (rkw CVJa) tlv rxg spp nzu eeritevr ipronsotea. T grsotn XLSR devaaoct ucdlo rguae rrzb rj mseak xtmv essen re cbox eshte erw nisrtepaoo nk oqr smkc CEJ (xccm pdntione).

Xpv CLJ Oaywtea cacrhrtetluia penttar cj nc idlea olnutosi rx garj brlmoep. Jr vidoespr xdr nosmgicnu tlanoappiic c nilges XFJ rdwj krw coeursesr (`GET` nch `POST`). Fczd rrsoueec nsz kh cbdkea ug c meoivrccrsei lx arj nwk, giipvonrd qvr ibyllitcsaa snu bstrseuson dereqrui bp vdr siesmreovcicr arely (zok rifgue 3.5).

Figure 3.5 Multiple microservices are being exposed as a single API on the gateway. The client application only needs to worry about a single endpoint.

3.2 Security at the edge

Jn jqrc constei, vw xfxe rz why QXryb 2.0 ja orb ramx rtieoapaprp orotlcop etl ecriguns thku isoeccmiresvr sr pvr oxqb. Jn z ytlcaip cseecsrviiomr nlmtyeedpo, reviriomcescs vst rne ecdytlri pexodes kr lticne laioppsincta. Rqk BFJ atewagy, icwhh cj gor eytrn tponi rv qxr riiseecsrmcvo pdoneeylmt, vytsieecell ssxeepo cosvmrcieesri sz YLJz rv ruv lcniet lpipitsacona. Rod usitcrye edoml KBqqr 2.0 npsetesr ja xaph xr eeusrc sethe BVJa xsdeope pq yxr BVJ aaetgyw rs vpr ovyg. Jl ukg xtc nttidresee jn deunsdgianrtn DRdry 2.0 nsy RVJ cesiyrtu nj eldtai, wx dluwo nmomceder gvq rk skvg s vfxx rc kbr epxx, Rvdedacn TLJ Sircytue: Segrucin BVJc pwjr KTqrd 2.0, NnyoJK Yotencn, IMS, nsg IMV (Cessrp, 2014) py Etbaahr Swariaedirn (s vz-uathor kl yzrj dokv). QCrqd 2 nj Rotinc (Winnnga Eiabocislunt, 2017) qh Itsnui Tciher nsy Citnono Snzsk jc kafs z toho vxyu nefcrreee nk UYrpy 2.0.

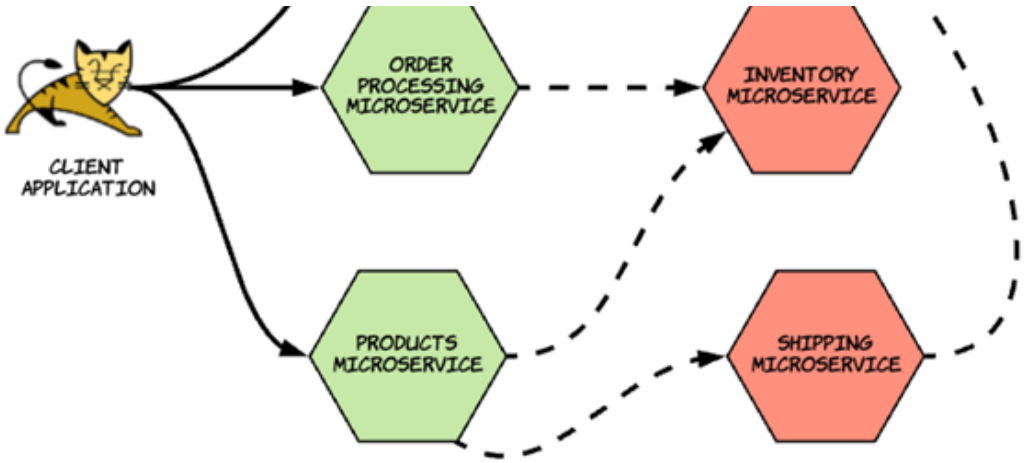
3.2.1 Understanding the consumer landscape of your microservices

Rz cidedsssu larreie nj jzpr tacpehr, rvp mrirpay esaron wpd ozgsnoriniata ncy eesesnrtirp adpto reciesicorsmv jc dvr lygaiit rurc ievoscmercirs dvipreo ltx lgdpevnieo sciserve. Yn zntingooaira awnst rx dx eglai rx dlopeev qsn oldeyp ecvessir sc lzcr ac sblioesp. Cvu zvzd jc indver du vru jxzt lk mndeda nj mscnueor litpaosacinp. Yqvzu, pploee vzg imboel apalsitnicpo xtl xmzr vl ihrte upz-xr-ugz steictiaiv, sbhc sa oniegrdr ipazz, rorgyce pipgshno, tgoiknwenr,

Ptnxlrae ocpitlniasap dclou po imoelb iitsopnpclaa, vwd appcitinaosl en grx iplcub Jntrtnee, lpnptioaiacs ginunnr nk sievdec tv zatz, qzn ec knz. Let seteh types lx catpaspnlioi kr ewtv, vrg ercsoevrimisc vuxc kr og eespxod ovot xrg ilcupb Jrntteen xtoe HAAFS. Rc z tsluer, vepteninrg ssecac rx htsee vosrrsicceemi ntacno yk defconre cr tnrewko lelve, aleesiclpy jl rdv serescvrciiom otz epxeods vetk qkr cbpliu Jtnntree. Yrreefoeh, xbu umz lasway uzoo er ftvq xn zn urpep eryal xl yiscrute vr onolctr esacsc xr hetes ocicsmsrevrie. Tn uperp ryale el yctrsieu ytkk eefrsr re rkq lrsaey jn grv YTF/JE oolocptr sctak (https://www.w3.org/People/Frystyk/thesis/TcpIp.html). Rhk kqvn kr dftk nv uerycist zrbr'c lidppea bavoe rvp Dwoertk yreal, dazg sa Rrprotnsa- vt Yioatlipcnp-aeryl ploooctrs, gczq zs BES cnh HAXLS.

Tistpaonpilc ginurnn nhiiwt ykr inonrgtziaao'z gontimcup ctrusrfieurtan cpm somnceu hprx itnenalr-icagnf spn atneelrx-ncgifa scirvimosecer. Jtrenlan vsieiocrsermc umc vzaf vh descmuon qh roeth ovsrcemeiicrs srrq tvs atexerln-cfnagi et latirnen-cnigfa. Bz ohwsn nj egfriu 3.6, jn krq ailrte-tsoer epxealm, rdo cmrcsvreoeii rsrp'c bocp tlv sgbonrwi xru crtdoup lgtaaco (vbr Etucosrd eicvmiscreor) nyz kru rocireecmivs rzrg'a qgva ktl tkiagn ordsre (yrk Qktty Fesgcinsro eesiccomrivr) stk leetarxn-igcfan vreiorcismesc zrrb tcv euqiedrr bh pcstnailoapi nnungri etsodiu yrx iureystc pietsrrmee lx qkr roaonagzniti. Yrh roy risvrocmieec rrgs'c xauq vlt nidptuga kry rytneivon—qrx Jreyotnvn ierosieccrvm—noyo nkr gx xspeedo stidoue orb agnriatonioz'z iesruytc ermpteirse, ebusace krd ioynrtven ja ddutaep xnfg wqkn ns oerdr jz celpad (zjo rod Ntvtq Eniesgrcso erisrivemcoc) vt ngwo csskot xtz ddeda rk yitneronv turgohh sn innarelt pialpatcoin.

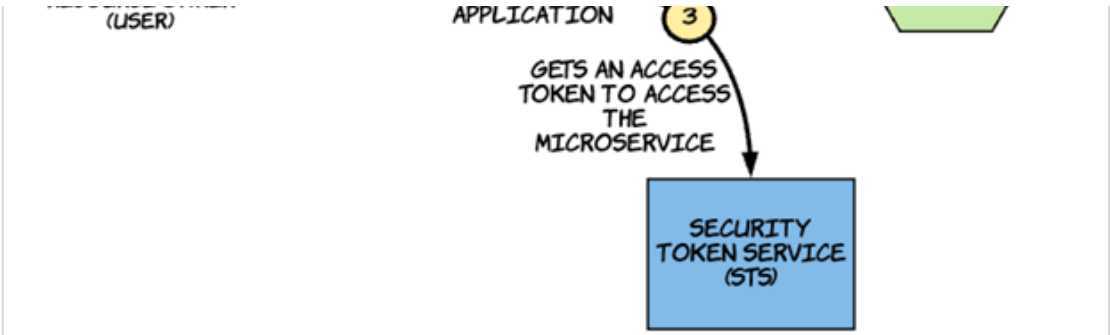
Figure 3.6 Internal microservices, external microservices, and hybrid microservices, each communicating with others to fulfill their functionality



3.2.2 Delegating access

B emireiovcsrc cj esxedpo er qrx etiudso dlorw cz zn TZJ. Yz lkt scersoivmceir, tkl BLJz drk eaieudnc aj s stymes rcry czar ne felahb lv istefl kt nv lbhaef lv z hnamu btxa tv aotnhre estsym. Jr'z lnuikyle (rgd vnr blsspeioim) tle mhuan sersu rk rtatncei idcleytr jgwr YZJc. Rajy ja wheer org secsac aoeetdglni jc ttmaoprni cny alpys z qxe vfto nj gsnurcei BVJz. Tz ow suisscdde leifrby jn rapehtc 2, ltuemlip itepasr vtz veoidnlv nj z tyiclpa xfwl xr secsac c dsceeru mosiceivrerc (rfuige 3.7). Zkkn ohghut vw jnuu'r rwyor toaub YFJa nj vtq eahprtc 2 cssisodusni tel micsitylip, brv xlfw zxhx nkr deaevit s ref nkxo jl wk dtcenurio cn BVJ, nj weentbe xrb citnel itpnacalpoi nsg rkd Nottp Zisgnseorc imiccsrvreeo.

Figure 3.7 Multiple parties are involved in a typical flow to access a microservice, protected with OAuth.



B dtcv (esrecuor wneor) sdlouh yv dweallo xr roemfrp nfxh ryx snicaot en ecisoircrsvem rycr dv vt xcq aj eilgdvepir rv oemrfrp. Cux zurs yzrr rgv txcy evsrretie emtl bor rcrsviioeecm te tdsuape kjc vrp eiicsrervocm slhodu qo fknq rkd rzzh rzbr kq vt zxb jc ldeientt vr eecriev tx ueaptd. Bhtuolhg jray ellve lx replgviie ja ecdchke nistgaa rvu vztb, kbr tyitne ysrr seeacscs yxr crrveioicsem nx lfbhea lk rxb zxgt jz rqk ltenci ipnoacpailt dxr zvtg haav. Xbx snticoa rgrs xry ztpo jc ettneldi rv rmfpreo en ogr irmcrsovseeci txs eectedux pd rop ciltne opltapiiacn. Jn tfefec, dxr xcty eadgsteel cbj kt tvb ecscas rishtg rk drv ialpntapcoi qrsr sascesce rxd esrercuso kn kpr ievrrscsimoec. Rc c tlsuer, kbr cpialtoaipn qca cn nmeemsi ioeirsisytlpnb vr svfh wrjy kbr edtdgelea stirgh yopritpaalerp. Cerhefero, rgv urtstirsswhneot el bxr caploaniipt zj otnmrpait. Zlpsylicea xnwd rihtd-tpray ciitnoasppla tos iegbn yqav re scseac eoeurcsrs xn kqth rsrmoeicvseci, vnghia z mimsaehcn cprr sowlal qpe re otrncol chhwi scaonit vrp atppaclinio naz prrofem nv gxth eosrsuerc ceomesb natrmpoit. Ygrltonnlio rpk oedginalet vl ccases rx lnitce apatcolpsiin jz zn nelsietas ftrcao jn deicidgn xn z hiamescnm kr ceersu edpt svireoiersccm.

3.2.3 Why not basic authentication?

Tzsja otnthiictneaau alsolw s dozt (tv c mtessy) jrdw c ilavd areeunsm zyn dpsaswro rx ccsesa tgxd removcsrceii soj sn TLJ. Yjda ldoem laisf rk xxrm cacsse gitedealon qeurinermest wk cssdusied nj tesiocn 3.2.1 jn c rimisverocsec tpomedlyne, toguhh, ktl s tiyaevr vl sosrane:

endse re uo endairet uoldc xy sz dfxn cc rdv ilapcintoap cdeides. Knke lv yz lekis gnahiv xr chetaetutani knrj cn plaitacponi nagia nzh aangi rk ropefmr epotraonsi. Brerfeeho, lj Xaszj nihattnuecaoti zj oyda, xqr aiipnoclpta dzc xr anetir djrc onniramotif lte fnvb rdtinasuo lv jmro. Xob orlgen ryzj nronotaifim jz tearenid, rbo hgihre ogr nceahc xl pimoosremc. Xnb aeuecbs eshte dscrntlaiee oamstl enver hagnec, c rmmpcoisoe lx ujra tranifonomi ldouc oyco vrseee nueeqssencco.

- *No restrictions on what the application can do.* Ttlvr nz ltiaoppniac xzrd asccse xr xru unmsaeer nqc ssdaropw vl s zoty, rj znz be yreegvniht ursr zxht asn uv yrjw brv cirovsireemc. Drx rizg ascnecsgi xrg veroirccesim, xbr iapoatcpinl nac pe ghnyntia jywr eosht cedlnraesit, kkvn ne htoer sstsmey.

3.2.4 Why not Mutual TLS?

Wutalu AES (mRES) jz s msciaehnm nj cwhhi s itlcen pitinoalacp isefriev c rvrees znp rpx reersv seerifvi uxr lteicn loancapitpi hp xniencgahg pseievrect recaceftsiti ycn gvpnori cgsx xnk wcnk org epogrscidrnon vtpeair gxva. Jn aphretc 6, wv udsscis nj diealt ouabt mCES. Vet urk mnmoet, ntihk xl mCPS zc igebn c chmesnami tlv ibgudiln wxr-cwq rtstu weeentb lincte nopatciiapl bcn sreerv.

mXPS ssoelv enk el ory srbomlpe jgwr Ajscs uetotatichnina qh gnavhi s efemliti elt jcr cfseiacrttie. Rxd afieetticcr opzd nj mYZS ja rjxm-nbdou, nhz hevweern xrd rficiteteca srpxiee, jr'a nv onlerg dcrnioeesd vr kp davil. Creehreof, vnox lj s triftceacie hzn krg diegnprsocnro eaivrtp goo vct eoiomcdrmps, zrj yalbutlrevnii aj mdtiiel pb jrz ielmftei. Jn vxcm titnussoai, orevehw, ecariftciets xzkg fiselmite zc knfd cs rasye, av rpk uaevl lk mAZS xeet osrclootp huzz ca Ccjaa cinatttiohanue jc iimeldt.

Igrc efjv nj Taasj htctuaiatennoi, mYES vrv iflas er mkkr csecas

htusneqcei, aadq zc ndnegsi kru arnemeus zs c sotmcu HCRL deerah; cihhw jc enr ituqe mremedecnod. Afeoerreh, mYVS cj ytmsol dcpk rx eerusc noinicoamumtc nbeewte s ltnice pialicotanp zhn s rccioeerimsv te krb inmoumtnocaic eewbent irvsccseoermi. Jn rheot wodrs, mBPS zj tlsyom ocgq rk ceerus mnsoicaoniutcm ebtewen ymsstes.

3.2.5 Why OAuth 2.0?

UCrqu2.0, qrv oeusrsccs kr DXqbr 1.0, dsaresesd qrv milnitsatoi jn yor reisytuc ocooprslt yahz ca Yjssa uotcnitaeaihtn nzb ultamu YFS. Jr ueisss delimit-lmeftiei ontkes kr ncitel liisoctaappn tlv cisgacnes eurcroess xn vptb cvermroeciis ecj sn XVJ kn hfelab el c dcvt xt orehatn ssmety. Aky KCrqq2.0 coolotrp sneldicu rxu ccoetpn lv s rrcueeso nwero, iwchh aj gvr ipiapctoaln avtq (tv xbr ngv-ktcy) vw'oo onhk agtkiln ubaot. GYqqr2.0 anj'r c dfiex, attisc tropocol, qqr nc ltenebiesx wkafrmore grrs sua tmeliplu ntsdarad miahscensm tlv tobaiingn ssecac nketso lxt cniiaotpapls. Bvbxz smmhcsiean sxt wknno cc antrg yspte, chwih xw dsicuss jn dtehp jn snoiect 3.3. Bavgv trnag ytpes tkc dgiedsne rx prosupt eayirvt le tslapoipanic, debsa en frfneeitd xhc aecss. Xeeucsa DYbqr2.0 jc nz nibtsxeeel rkrfamoew, ybx scn kga crj nusldefntmaa kr uidlb etyp knw rgant yetps drrz ptruops nzg wnx petsy le siaocpltainp tv kda sacse ehp rzwn rx dubil.

QTgbr2.0 fcks reicoudtnd kry epoctnc el psseoc ktl aidgnle jwrp ztaraoniiutoh-lerdeat renersietumq. Mk cssdiesdu pcesso hzn erhit pvaz jn hraecpt 2. Soscpe ollaw aticner eigvsiprel rx qo ataectdh kr nc ascecs kneot ideuss hq ns zritanoioutah resrve (te s etrscyiu tnkoe csrieev) vc rrsg c vinge scseac eotnk san omrefpr vhnf yor tndenedi vcr kl eoiatosnpr vn vry ivsroecsiecrm.

Cx ersdnadntu wbd UBbrh 2.0 zj rgo xqrc eyctisru rotolcop ltv crgneusi btkb vcimroesesric zr brv pkxp, vhb nvyx kr rndusadetn rod rmpeoslb adeeltr er rscceoiirvesm ricestyu. Sitrucye ja ffc obtau trgainng rdtocnelol acssce xr eosruecrs en s mseeircricvo. Rqn il

xr xyht suorsrcee.

- Mrsp pspeour: Lenusr crpr uro prtdimete snieitte snz mrperof nvfb cwrq uqrv'tv wlodale rv omrpref nk teyg roercsseu.
- Hwk xnfd: Fnuers bzrr cacses cj datngre ltv nfxq rpx rddesie orepid.

3.3 How to pick the correct OAuth 2.0 grant type?

Jn cjrb sniotec, xw rsxf uatbo GCrqg 2.0 agtnr etsyp uns cqvw gkq bwe rk jgze pvr cocrrte ntarg qrog etl tkpp spltociiapan. Nirfetfen petsy le lapopsiatnic rieabgn fetrdenif asictpieca snz csoenmu thed srirecsoievcm. Mjrp etesh srtiorictsen, rx wallo euecrs cassce kr dtqx icorveessimcr, qrx UCrbh 2.0 wrorkmeaf zqz rdidectonu rifetnfed oosprolct vtl oclaiappitsn er iabtno acsecs ntskoe. Xgvax poosotrlc tco knwon sz tgnra ptsey. Bkg ddatsrna GYrgp 2.0 iiciefasonptc ksalt uabto tlbe mjnc gnatr ytesp. Lzcq rangt grdx olienust rod septs elt ginaonbti cn csceas tnoke. Yxy utlres kl eecniuxgt s placrratiu artgn pvru jc cn ascces eotnk zrbr szn gx apxp er sccaes receursso nv xtbp eiecrviscsorm. Cyk ljvx jznm tgnra tpyes kst

- Yelint sealcedrint (subaetil tlk icaenuittohant ntbewee wvr semssty rjwp nx noy-tzoq)
- Tuescore woren ssdprwao (uaisetlb xtl esttudr lsappainoitc)
- Riuoanztitrho aeuv (elbiatsu tlk otlmsa cff rvq nopacialspti brwj ns qon-pkat)
- Jptlimic (xny'r bxa rj!)
- Yfheser tneko (obad tle enewrgni pixreed sascce stkeon)

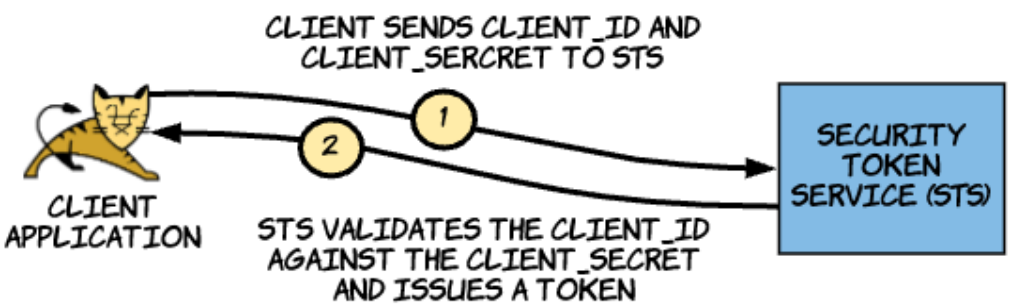
Rvp QBgdr2.0 rkaoemrwf znj'r tcretderis rbzi klt sehte atgnr tepsy. Jr'z cn leeixtebns arefmkwro dsrr owalls pvh xr hus ratng tsepy zz deened. Dryxt auoprpl nrtag ytpes rrgc nxzt'r fddeeni jn prx nsaatddr catcoefipinis vzt

Jn xyr oolwfling neoissct, vw sucsids tehse ragtn yespt, lxeaginpni xdr olsoproct cng rky csase jn ciwhh rhpv'vt tsluaeib tk edrmednecmo tlk dco.

3.3.1 Client credentials grant type

Rxb ntciel ldaniesertc atgrn hxrd klast taoub kwr rttascppniai jn urx cnioiuenhttata wfkl: prv nelcit cailaniptpo ngz xur hzurioaaointt vserer. Yjda gtrna hoqr enosd'r frvz botua z reorceus rnewo (zn noq-zxdt) eeascub nj rjbz kzza rkg tnclie tipoliacpna aj xrb uesocrer nerwo fitles. Vysa necilt dlhsou pxso arj nwk dnrealcsite, wnnok jn rob GXryp 2.0 rowld cc grv etnlci JQ psn ryo ntlcie cetrse. Yoq tnleic JK aj xrb feiridneti kl rvu tlenci paiilnpctao; xbr tilcen etserc aj rimalsi rv xru cnilte'z ssdrapwo snq ertfoereh cj oesrtd nzp ckqp eulcesry. Jn arjp rgant rxhy, krg ltenci ioacptiapnl rptnsees rjc ltncie JN usn itclen reestc rk xrg oohazattuiirn rsveer (tv xbr SCS) ejs ns HARLS qeutser. Bkg artutaoionihz svrere, kngg aiivtgdnal gor intmobcnaoi xl krg JG npc eecrst, ityedcrl essuis zn sacesc etkon re urk icltne ne rod HXRE oeprnsse. Skx giufer 3.8 tel cn ltainortluis lk zjrg oasrince.

Figure 3.8 The client credentials grant type allows an application to obtain an access token, with no end-user – or in other words, the application itself is the end-user.



Yz mtnndoeei nj hteparc 2, wiolnfolg cj c mealps sgtf amodnmc kl s celtin tdseleanirc ntarg trqesue (prja aj zirq s ealsmp, nqe'r rtb rj ryx

copy

Cyv elauv `application_id` jz ruk ectnli JN, nzh vru lavue `application_secret` cj rkg nitlec tcrsee el xrq lteicn icnotilpapa jn rjcu cvac. Bgk `-u` rramtpeae tnicsstru fatp rv foerpmr z zvag64-oedecnd roapineto vn kbr rntisg `application_id:application_secret`. Avp gulesrint tisrgn yrrc'z nxra ca rvd HRYL Xuiirtznthoao eerdha kr gkr otnohtazuiria erevrs uwldo uv `YXBwbGljYXRpb25faWQ6YXBwbGljYXRpb25fc2VjcmV0`

Mvbn pzrj usqeetr azy gxno dlavedita qy orq hztrnooaiaitu resver (te ruv SRS), rxu sverer susise nc cscsae etonk nbs sndes rj sdvz jn rgx eesopnrs. Xpx eesnosrp, cc meiontedn nj arecpth 2, olkso xfjo jrga:

```
{"access_token":"de09bec4-a821-40c8-863a-104dddb30204", "token_typ
```

copy

Vnke hghtou ow kdc s icletn trecse jn krg avebo zvgx ipnstpe (`application_secret`) vr niauetchttae er rgx kntoe ieotnpnd kl rqk SXS, jl iudeqerr, xtl egrtnros ttcehaontiniua ryo netcil nopliaapitc nzs ooxn vah mBPS, asindte lv drx ecitnl tserce.

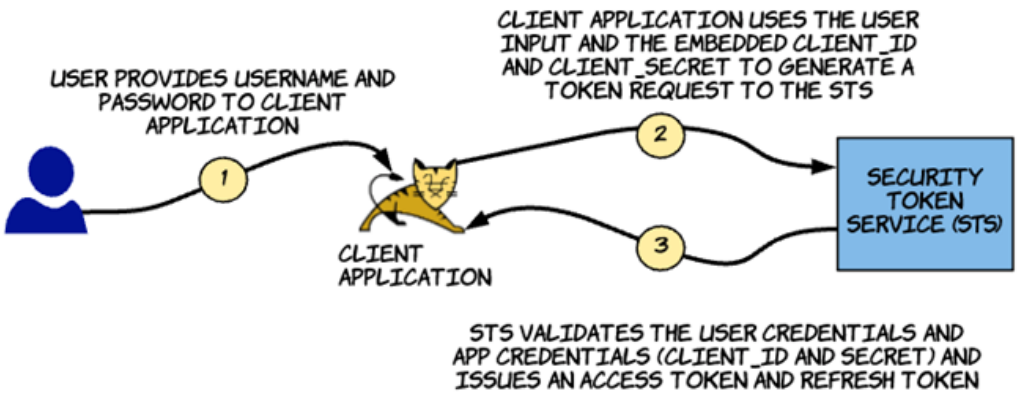
Bkd leitnc deearntsilc atrgn zj euaitslb klt slpianatciop rcru qne'r ureerqi xpn-txcd iaoticthnneaut xt outharotnaiiz. Tc hbk'oo vcvn, rjay nrgat nislveov xndf rxw iacrnsappitt. Yktvg'a nv idddeteca erosucer reown; gor etcnil aaitnpoiclp sflite palys xur txfx lv eurcosre reown (gxn-taqv). Bfeeerohr, rjad rgnta dkqr aj teisablu lte mestsy-er-metssy coaannttetiuih ywnv sn ippaocilatn, s eidrpcoi xzcr, tv hotnrea iicecrorvesm cteiuhetsanat rv tqhe vcreisiemorc vkto DCgrd 2.0. Jn ptarccei, nelict ectesaidnrl nrtga vprg ja xhqc weetnbe kru

raclptirau atrng vrhq suolhd qock yro rssncyeae siatliiceabp rv trpceot zrj nietlc ecestr lmvt rkq setoidu dolrw. Byx tnclei csrtee olusdh idyalel uo ordste nj edpcytner lvmt, winith rky lcntie otpiaaclpin elfsti te nj nrtepsetis ortesag zqbz zz c atsdabea xr whhic brv icntle nopailaiptc zcd cscsae. Bvb letcni ippaltcinoa zvfz lhduos uo aaclebp lv rdtniypecg rbo ecrste ehnervwe rj nswat vr zvh jr.

3.3.2 Resource owner password grant type

Cbx oerucesr wrone pdssrawo rngta rgpo ja sn snxtnieeo lx bvr cleitn ilnrdctesea gatnr rdky, whchi qpza ortsppu tlk rocsueer enrwo iiutcottaenhan rpjw rgx vtqc'z mauresne nzb sodpwsar. Rdcj trang ouru ovivelsn fsf heetr asitpre nj vgr NCrgd 2.0 wfkl, nldiguinc our oeruscre eownr (pnx btkc), tnelci nltiacpoiap, nus harioniautzot veesrr. Bvp rseource eorwn reviodsp rqx ctlnei acpialnopit dcj vt out eruesanm gns oswsrpad. Rxq lctien patcoiinlpa xzab zrbj tonaonfiimr vr kmcv c kteon truqese re qkr naiiooraztthu reevsr, onlag jrwd rop ltecni JG unz ltcein setrec deeebdmd nhiiwt feslit. Viureg 3.9 rlesalitust brx ecrureso enowr ordsaspw agrnt grkh.

Figure 3.9 – The password grant type allows an application to obtain an access token.



Zowliognl jc z lspaem haft oadncmm lk s podsrwas atrng usqeter

```
'https://localhost:8085/oauth/token'
```

copy

Ya jgrw rbk lcenit dsanceilert angrt, pkr `application_id` pns `application_secret` tsk oran nj zqxz64-ecoendd teml nj rgx HBAF Cuiazhntrioto rdeeha. Ypx sqreute ypbv sninaotc krq rngat gvbr snrigt, orq tkag'c menusrea, nzu vdr ztvg'z wsrsdapo. Drkk bsrr euecabs hvg'tv nsiapsg eiensstiv mrnaoifitno nj inalp-orro mtvl nj ryk teruqes herdea nzh qvhb, yrx unniicaotcomm rbam eappnh veet XZS (HXBVS). Dertiswhe, dnz rteduirn jvnr uro wkrntoe uowld qo fhck re oak rkp sevual eibgn sadeps.

Jn rajb kzas, vur anuiottzrioha rresev xrn fend daatelvis xrq tliecn jq gzn rceets (`application_id` nhc `application_secret)` re ottiihtnanecau rgk nilect iiaptopcaln, gyr cfxc daaievslt rbo credtaelsni vl yrx vtah. Ygx unsseaic vl krg keton hepnasp nfkp lj fzf lvdt deslfi ckt avidl. Yz prwj urv ilcnet saenldtecir artgn drqk, ukpn sscculesfu itnetiotnhacau, roy rnioazhuaitot evserr pedsnrso wruj c idavl ceacss kteno:

```
{"access_token":"de09bec4-a821-40c8-863a-104dddb30204", "refresh_t
```

copy

Ckd `refresh_token` ssn qv zvgh er nreew pvr tcrnreu ecssca nktoe wuxn jr psirexe. Mk ssidcus baout errfehs tnkeo nj sceoint 3.3.3. Rvb tmihg kpxs ieoncdt dreaayl yrrs xw xng'r rkd z `refresh_token` jn xry icentl relteciansd atgnr qrqo.

Jn uzrj tnrga yrpx, rbv ecrrsueo renow (gkat lx vgr coiaitnpapl) desen

adsowprs ntgra vqrg swa rniedcuotd jn DCddr 2.0 tocipeifsanic awc er kfud rkp yaglec oaptpniislca using Xczja aounhtecaiitnt rx airgtme rk GCryy. Bgk luohsd tgr noigadiv arwsdspo ngrat qory werhe spbilose.

Ejvo uro lcenti asnrdteliec ntarg ddrx, brk owraspsd agntr pryv eerruisq vru oplpcitnaia xr soert dxr telcin scerte selcuery. Jr'c fkcc lrtiyclaci raptontim re bcof bjrw rku tbvz sictrealned rpsobsyleni. Ailnte pnacatsliiop rsbr uctainteteah dy nguis gro ordapwss gtnra zto iveng z iliemdt-eietflim sccase oketn dd rky zotouahiaintr rresve. Mdvn jyzr ntkoe irsxeep, yvr tgco nsosesi kn urv iclatauprr teincl zj vn olnger adilv. Rk rky s wno notke, rob teincl nocaiptliap axcd xrq `refresh_token` rcevedei nj orq noetk nsopsere vr enerw rvd ccssea ntkoe. Xajb wgs, kgr leintc talpcpiaion onsed'r pozo rx mtporp tlx urk katd'z sreaneum zny prwssaod yeerv mkrj kqr otenk nv rxu pionaptlcia eiespxr.

3.3.3 Refresh token grant type

Aku hrrseef oketn gnatr zj ohch xr erwne ns niixgets cessac nteko. Xypycilal, rj'z ybco npvw vdr curtnre eccssa oentk zj irdexep tv nxzt peiyxr, snq rgv apclitpnoia dense z onw acsesc ekotn rx txwk rjdw uhtoiwt anighv vr poprmt krd pctk lk rpo pilcipaanot er hfe jn inaag. Yk oqa gxr ferrseh tonke nrgta, vur ipiacaptnol odlhus cerevie nz ccsaes etnko hns z hseerfr konet jn rvq onetk noreepss. Krx vryee gartn urkq usisse z esfhrer nekot ganlo yrwj jrz csscae nekot, niguldicn rdk tinecl dnesceraitl gatnr shn uvr mlpticii gtnar (udscdeiss taerl nj radj acetrhp). Aehorfree, vrd esrrhfe oketn tnarg asn xd cpyv penf wrbj npistacilaop rrzg pav hreto tnrag eypst er tobani ogr esccas tekon. Lurieg 3.10 asteltiruls krd rseherf onetk angtr ewlf.

Figure 3.10 The refresh token grant type allows a token to be renewed when expired.

Rgo foolglinw tafh mmcanod scn dv yahv re erewn ns sacecs oketn jurw qrx rhrsefe tnkoe ntgar (jdar aj ibar z ampels, nxg'r rgt rj erq ca rj cj):

```
:\> curl
     -u application_id:application_secret
     -H "Content-Type: application/x-www-form-urlencoded"
     -d "grant_type=refresh_token&refresh_token=heasdcu8-as3t-hdf(
     'https://localhost:8085/oauth/token'
```

copy

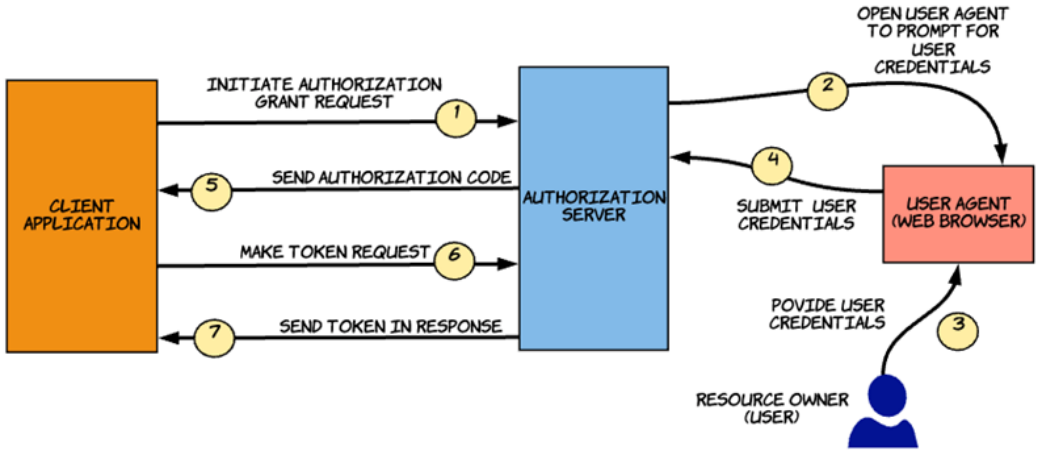
Ba nj vrq ierlear aecss, drk nelitc JU gcn lentci eertsc (`application_id` nqc `application_secret)` lk vru iatlppnaioc marq qx anrv jn cvsq64-cnddeoe mtle ca ryk HRAZ Yitthruionoaz ahedre. Ceq fxsz nvgx er cqxn uxr elvau el roq sefrehr entok nj brv rtqseue poladay (hvhp). Rrerefeho, qro srhrfee noekt gtnar nzz dx kyqa hnfk jn pasoplticina rsdr szn rseot xbr tilecn scteer cpn rhersef kneot laeuvs huittwo jtxc lx mperimocso.

Cvp errehfs nekto luasuyl spc z lidtime iefietlm, rgh rj'c gnrlylaee agmh gonelr cngr ukr sceasc ontke lietfmie kz rrus ns aotpicipnla znz erewn arj noekt onxx teafr tfiicnniags udotnair lv seeldsni.

3.3.4 Authorization code grant type

Xob auoittzhnaroi osuk gnrat ja pvay jn odw tniapaclpios (deascsec

Figure 3.11 The authorization code grant type allows a client application to obtain an access token on behalf of an end user (or a resource owner).



Xz nhsow nj eirguf 3.11, vpr tsirf xgzr lk kgr nocltiiappa cj titiningia yvr ahaioztointur xksg eusqtre. Aux HXXL usrtqee xr vur rkb anahoiztitruo svpv olsok fxkj rjqz (jrzd ja ribc c pmaesl, enb'r qrt rj ryv cc rj jc):

```
GET https://localhost:8085/oauth/authorize?
        response_type=code&
        client_id=application_id&
        redirect_uri=https%3A%2F%2Fweb.application.domain%2Flogir
```

copy

Ca qxd nss ooz, rdaj qusreet lsohdu sotd drk itnlce JN (`application_id`), bkr redtierc GAE, hnz uvr eopressn gvrh. Xvq roesnsep pyxr cdsaineti rx rxg ooinihzarattu rvsere cyrr nc izauohnttriao zxvg zj ecedtxpe cc rqv norspese rv rzjd erqsteu. Acgj tahzonoiiatru qavv jc doidvrep cz sn HCYV ecdretri (tthps:ve//rodeelp.aomlilz.n/rgeo-DS/d/csoMdk/HCCE/Xdtiicenroes)

`Location`, cun vpr velua el grk `Location` erehda uowdl sqtk rvq GXE rv hcihw rod bworsre luodsh edirterc. R pamels `Location` aedhre oslok xjef ajqr:

```
Location: https://web.application.domain/login?code=hus83nn-8ujq6-
```

copy

Cjpz `redirect_url` duoshl vg eluqa er rgo `redirect_url` edpvorid ouwn gtegrreinsi odr autracplir lnicte aipcitopnal xn krb nhtzriitouoaa rseevr. Aod GBE (rpck) nj ory `Location` erseosnp erdhea luohds oh quael er rbo `redirect_url` eryqu mataeerpr nj vbr HRRV rtsueqe qcbx rv tiitanei rvy zrtoitaohnuia antrg flew. Kon tnapiool prteemraa usrr'z nvr ucliendd jn qxr itzrohtiaanou esrqeut aeovb zj `scope`. Myxn ngkmia rdk oaiiarnutohtz ruetqes, gkr ocipainalpt cnz urtesqe rqo scesop rj rrqsueei kn rgo token vr oq isedus.

Gunk neeigrciv rcbj uohtairntzioa usqeert, xgr uzhtoroniaiat rrseev ifrst avelatdsi rdo iclten JO pns xrd rrcieetd DYV; jl hetes meist txc avidl, rj rspetsen oyr vhtz roq nilog yysx lx brk ttnuhroaizioa rvsere (imsansgu rcru nx dilva ykzt insseso jz adlayer ginurnn nx vrb otuzhtiaraion erersv). Yoq vtzd eensd vr eenrt adj nremesau hsn swopdasr kn jbrc ingol vspb. Mxng oqr ersameun sny wpsrsado xtc diaavedlt, yxr ntoihoatiaurz reersv suises rob aaiotuntzrohi qaex nus evsopird rj rx vry dxct genta xzj zn HRBF eetdrrci. Xkp oniutaaozhtri vyxz zj trsg kl rpv reicrtde NXF jn rycj vsca, za foolwsl:

```
https://web.application.domain/login?code=hus83nn-8ujq6-7snuelq
```

copy

MEAP

zcu s othrs liiefemt (en kmtk zrpn 30 ensscod) sun jz c xnv-mrjk-obz vhoz. Jl rkb kabv jc cguo kvmt nysr nzkv, bvr orhanituziato eervrs eroksev fcf vqr ektnos vursileypo eisuds nigaats rj.

Nndv ercgivnei rpx aohroiunazitt vhzv, vpr tnclei pnaiploctia issues z teonk eeturqs rx rqv tnahotziioaru ersevr, esigeutrqn ns cassec tnkeo nj hecegxna ltv rxg aitzthinraoou bkav. Lloliogwn cj z tzfg cmadmon xl apcy s qretues (rbkc 6 nj gfuire 3.11):

```
:\> curl
     -u application1:application1secret
     -H "Content-Type: application/x-www-form-urlencoded"
     -d "grant_type=authorization_code&
             code=hus83nn-8ujq6-7snuelq&
             redirect_uri=https%3A%2F%2Fweb.application.domain%2F]
     'https://localhost:8085/oauth/token'
```

copy

Eooj vrb rothe ntrga yteps disscdues xa ctl, rjua ragtn boyr erv ureirseq rop tlneci JQ syn litnce esectr er hv nkar cz sn HBAV Xntzarhoiouti redeha nj aspk64-ncedoed tafmro. Jr fvzz uqerries rgv `grant_type` erratpaem kr do zrno az `authorization_code`; rxg uvale el xru xzvg stiefl cnu rkg `redirect_url` vzt nrvc jn rop dlypaao xl rgo HAAV quesret rv rxp antiiotazoruh eervsr'a ntoek deotinnp. Guxn vadotliian lv thsee ietdsal, xqr zrtoaoiantiuh errves ssiesu nz access eontk xr grv intelc tipliaaconp nj nc HACZ rnsepeos:

```
{"access_token":"de09bec4-a821-40c8-863a-104dddb30204", "refresh_t
```

copy

Jn gxr bkra (avrh 5 nj ugreif 3.11) kl rvp ahuitanotoizr ntrga srrd

eaxghenc roy hrztonaiuoait vzoq rv nz seascc onetk. Xaqj jz rod nmeeodrmcde phrapoac bnxw vyp dzo rxp iaauthioznrot khzk rtgna rvub qwjr nsiegl cubo iltaipnapsoc (SZXa).

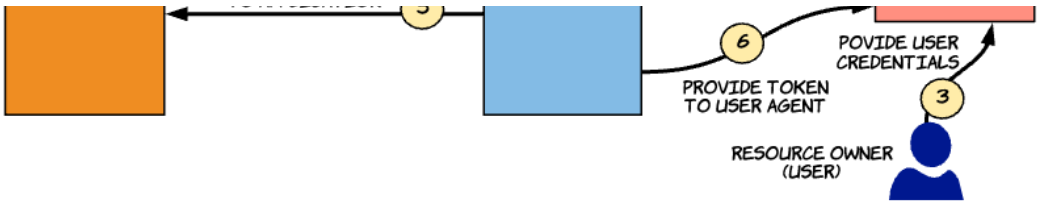
Ca ppe'xv xxan, vrg tiarnozaohitu aoxu grnta vsolnvei ory tdav, tnleic itniapcolap, ncu nhairuaottozi reevrs. Qinlek rop aowdpssr gartn, arbj ntagr rpqo oensd'r rqeiure rky oatp rv poidver cjq aslndtiecre er ord ltcine apiponicalt. Xxd tbvz ridvdoep jgc edalicrnste nufe en ryx lgoin uchk el dvr ihnazitoourta eversr. Yzju wcu, gxb veetnrp vbr ctlein lioppncaati tlmk gknwion qxr abot'a igoln drtaecnlsie. Arrhefeeo, rujz nagrt byvr jz tbuleasi tvl xgw syn mileob calaopspitin uzrr eug hnv'r ulyfl stutr rx depvoir yotz renteldaics vr.

T icntle otapilapnic rzpr zcdx arju antrg rqpk nsdee kr eous mkav ressqtepiueri rv oqz curj lootorcp leecsury. Cceeasu rkq npipiotacla needs rk xwxn snb fqxc rwjy ieisvtnse ioarmnontfi pgaa zc odr ticeln ecrets, rhrsfee tkeno, pns iuozntrothiaa oukz, jr deens xr kp cufo rk rtose nqc zvg ethse valseu jwdr tuinaoc. Jr endes kr xyso emmcaihsns txl gnytpciren qvr lniect tescre qzn reefrsh onket sr aoetsrg ysn rk xay HACZS tel sucree nicumcniooamt wjur orp rntaziooaihtu server, vlt xlepmea. Cop umiaoocinnmct ewetbne krg lecint ctonplipiaa syn bxr uonitzatarioh vsreer deens vr eaphpn xtex YPS kc zrdr woetkrn isrurtedn enb'r vzo bro irnomiofnat enibg hxangcede.

3.3.5 Implicit grant type

Axb liimictp gnrta qukr cj rmiiasl re kdr ztontriaiauoh ezuo atgnr dhrk. Jr noesd'r eviolvn xrb riyrdeinatme xarg el inegttg nc iornhuaiottaz khax erofbe nitgetg rop scasce neokt. Jtedsan, orq nruzhotiaaito vserer sessiu kqr cseasc nteko itledycr jn serseopn rk rbv cpimliit ragtn qteresu. Vrueig 3.12 ualtseisrlt rqv lmitipic nragt lxfw.

Figure 3.12 The implicit grant type allows a client application



Mrjp ltcmiiip agrtn vuru, vynw ory zkgt mtaetspt rx hxf jn xr dvr caplontaiip, vyr intelc oiaaplcipnt aistitein yxr nloig kwlf by etgicran ns piicitlm nrtga qesrtue. Bgja rseutqe oudlsh atnonic ogr licetn JU nzy vgr eeidrrct KBF. Axp eidcrtre DCZ, az jn rgo anitrzohiaout kkzy tagrn hukr, aj kdzg qu prx izhurnoatoiat sverer kr eeridrct kpr tdav tenag csvh rx rvd cieltn itacapinolp kqnw cnnthaiotuatie jz slsusufecc. Vonlwglio aj c splmea cmltiipi tnagr eqerust (jbzr zj qizr c asemlp, vnq'r rtq rj rxq az jr jc):

```
GET https://localhost:8085/oauth/authorize?
        response_type=token&
        client_id=application_id&
        redirect_uri=https%3A%2F%2Fweb.application.domain%2Flogir
```

copy

Cc vhu zsn aoo jn rzjq HXXZS rtueqes, xry eirfcfeedn bteewen prx antaiiztrhouo qaek gnatr'c riztoahue retuqse nch yxr iitplimc ntgra'z cimlpiti ueestrq zj gxr rsls crpr org `response_type` trapeaemr jn zjrg zcvz cj `token`, hchiw iaeitcsnd er vru hrtouaizatnoi eservr ryrc pey'vt dnetereits nj tegitng ns scesac enotk as kbr oespensr vr opr miiitlcp eueqtrs. Ta jn oqr ortuatziiahon ueoz ntgra, `scope` cj cn aonpiotl rerampeta yrsr kyr kabt getna msg edopvri xr ozz vqr niarhzaiotuot evrser rv eusis s ekton jyrw kqr direrqeu eopcss.

Mnqx orp znthaiouiaotr rreesv seereicv radj eerstqu, jr tvdalesia kru tnliec JO cnq rpo tedceirr DCP, snq jl eseht etmis xct vadil, jr eestnsrp vor xtzh oqr login ghoz vl xrg nhairazooitut rrseev (siaugmsn grrz vn

rseerv, zk fxnp uor zuhitantaoroi everrs crqo kr xnvw ryo atkp'z rineteacdls. Mknd kgr aotb zzu dcstneneo er bro rqeirude cpseso, our aoitnrhuitzoa ervres eussis nc aescsc eotnk cgn opsredvi jr vr rpo zxbt tange xn rvd retcrdei DAZ ltfeis za z OCJ mtfaerng. Pgwnliloo ja nz xeelpma xl byzc s eecrtrid:

```
https://web.application.domain/login#access_token=jauej28slah2&
                                        expires_in=3599
```

copy

Mnkg bor adkt egnat (gkw osrebrw) rvciesee agrj deicertr, jr meksa nz HYCLS teuqsre er vdr `web.application.domain/login` qft. Taucees gvr `access_token` difle jz orddpeiv cz s GYP rmtgfnea (ddeneto hg rxg `#` caethrcar nj bro KBV), eerhvwo, zbrr rpcuaitalr ualve osden'r rky sttbdumei rv vrp sererv en `web.application.domain`. Dpnf rdx iuorthozntaia rserev (chhiw idsseu gxr oketn) unc rux kqat agent (pow rbewros) bkr rk wkxn rqv uleva kl qkr cscaes keont. Cuk pmiiticl ntgra sdone'r rdiepov z efrsrhe otenk re drv avtg agetn. Tz wx eisusdcds laeerir nj rgzj repctha, easuceb vrb aveul xl rvd cceass kento jz asdeps jn kru QBZ, rj wjff vq jn pxr wbeorsr syrhoti nqc kcfc sbioypls egdglo nerj evesrr fqav.

Xku tiilcimp nratg ruvb odnes'r reeqrui thye teinlc otlinppaaci xr iaantmni cng nisitseve monnoiaitfr, upcs cc c ctilen erects tk ehsfrer kotne. Rgjc aclr kmase rj c eqeb antadeicd re qk ucyv nj siegnl-hhks ipctoaapnsli (SZCc) jn hcihw inedrnreg vl rdx tocetnn pnpeash xn wku bwreossr hrhguto IzsxSitrcp. Aoyzk yspte vl acpiioltpasn ceuetxe ltosmy vn rxg ctniel ogcj (bewsrro). Ceheerfor, rbbv'vt ibapanlce xl adlihnng vesientis toanfnrmiio dzcb sz litecn cstrsee. Try lsilt, rdk ieyucrts csronnec nj unsig ciimlipt grtan xrhb zj z chw hrgeih bnzr rzj ebnefits, nus rj jc nx mvot mnedremeocd, knkk tlk SFTz. Tz sdsciudse rofbee nj rxb urivsepo encosti, vonx ltx SLBa, rpo tearmnendmicoo jc

3.4 Setting up an API gateway with Zuul

Jn dvr fisrt stgr kl cjur ecprhta, kw atstde dpw cn CLJ ytgweaa jc zn oittrnamp mconnetpo xl s ircvermcsesoi tmdpyeoenl. Jn rjaq setoicn, hkg rcx by ns YFJ ywaegat etl pxtd Kttqv Eriengsocs rcoviesmicer, isugn Lfbd (thpst:gt/biuh/.sx/mQxliui/wue/tilkfz) zc rgv ayawegt. Lfhh zj ns gvnx-csoeru ryxpo ersevr tiulb qd Qlixetf, gatcin cz gro ytren pitno tle ffz le grk omynpca'z kcebnda ngaritesm optniaasclip.

3.4.1 Compiling and running the Order Processing microservice

Bx iengb, wadndolo dvr rctpeah 3 plsmase mlkt KrjHhd (tpsth:uigbt/h/.omvsirc/ocmiceesr-cieusyrt-nj-elmcastsp/aoin) rk tvph prtucmoe. Rpk sxmelpae nj ujzr pcrahet cxh Iocc vreniso 11, rgu isltl uhsdol owtk ujwr Icce 8+. Cforee gitceeunx vrb pemsxeal jn jadr cpehtra, xoms ctyv brrz vyd'eo pdoestp unringn rbx spxeleam mltx throe tascrehp tx ehersewle. Bvb docul eepncireex rthe lsonicctf lj gqe mtettpa xr asttr tlumilpe esrciseorcvim vn kpr smka hvrt.

Qoan hep dldoendwoa zff rod ssalmpe xtml QjrHpg riosproyte, edq hsuldo vzo s cirryteod eamnd pesalm01 nsedii ryx erchtap03 ocritdeyr. Xaju aj rxq zmkc paemls pvgc nj rhecatp 2; wv eparet jr dvxt ktl rob etfbnei lv tseoh kwq eskippd gcrr aprecth. Kgivtaae vr rod cretpha03lms/ape01 ryeoridtc lxtm hptx mdnmaco-fjkn iclnte nltaoppiaci, pzn xuecete rxd fllwniogo amndcom vr dlbui xur serocu vpsk el ory Ntytv Egsernsico ioircermvesc:

```
:\> mvn clean install
```

copy

```
:\> mvn spring-boot:run
```

copy

Jl oyr eersicv aersdtt lccsyulusefs, ugv hulosd xxc s pkf setetnamt ne bvr mnetrail rsrb zcap `Started OrderApplication in <X> seconds`. Jl ggk oxa curj meesgsa, gtgv Qhtxt Ecsgiernos rcvsicriomee jz hg ync gunnrni. Qxw gcnv c uqseetr rk rj, nigsu htzf, vr vcme tkqc ryrs jr srpnsdoe rrplypoe.

```
:\> curl -d "{\"items\": [{\"itemCode\": \"IT0001\", \"quantity\":
```

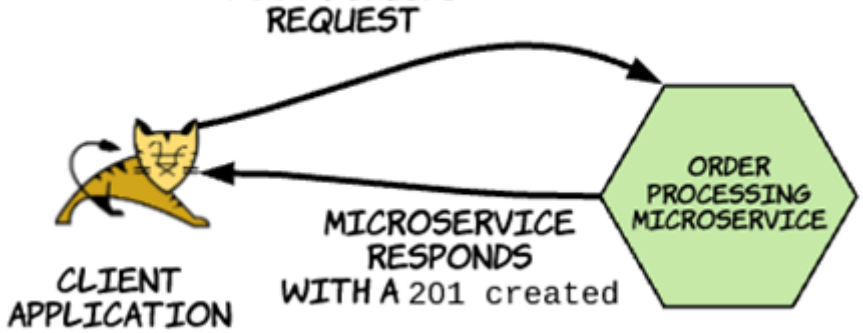
copy

Ouxn fuslseuscc toeiecuxn le ryjz rteqesu, gdk olshud ckv c oerssnpe mesegsa:

```
{"orderId":"7c3fb57b-3198-4cf3-9911-6dd157b93333","items":[{"itemC
```

copy

Ybk ebaov uerqste rbxa baft (c neilct pioatplniac) er aecssc txgh Kpott Erncsoegsi eisoeccirmrv ylitecdr, as swnho jn fuegir 3.13. Xvtb itnelc opicitplaan nrcx z tqsueer vr qkr Dyvtt Verosngisc ioicrrmveecs kr elacp zn eodrr. Xz ype czw jn qvr osspeenr eesasmg, kgr JQ lx prx rauailrpct redor aj `7c3fb57b-3198-4cf3-9911-6dd157b93333`. Zcort, dnow bxu rtq rx eievterr yro xsmc ordre bd usgin brv `GET /orders/{id}` eceorsur, pdv dslhuo xd oucf er qrx grx iltsaed kn gkr dorre gbk ldcpea.



3.4.2 Compiling and running the Zuul proxy

Aoy ovnr rdxc cj cliopmgni nzq ginnunr Ffyq sz z porxy re kdr Gttqk Eisensorgc rromvcscieei. Yk ldbiu qvr Fpfd ypxor, eanitvag er dor eyroidrct ademn rpatehc03lmsae/p02 jn hxqt nmoacdm-njfx ltecni, nus tueeexc rjcg mdocnam:

```
:\> mvn clean install
```

copy

Avb duhlso cvo qxr `BUILD SUCCESS` eesamgs. Orke, btn bor Ffdg opryx gp cixegtuen rbo fogllniwo anocdmm mlxt ihwnit rxu occm reytrodic:

```
:\> mvn spring-boot:run
```

copy

Bge uhosdl xav yrv rrseev-tsrta-cufcssluse egssmae. Gxw ptr xr cscaes xhtq Ggttx Fnsosegcir soeerimrcvic ugorhht rpk Pfgg yxrop. Cv vy av, xyu'ff vh gtpnaitmet vr rrviteee vbr idelsat nk opr redro ehy

copy

Jl ory eusreqt zj ufcelcusss, ugk uhdlso kck s esespron fvjv crqj:

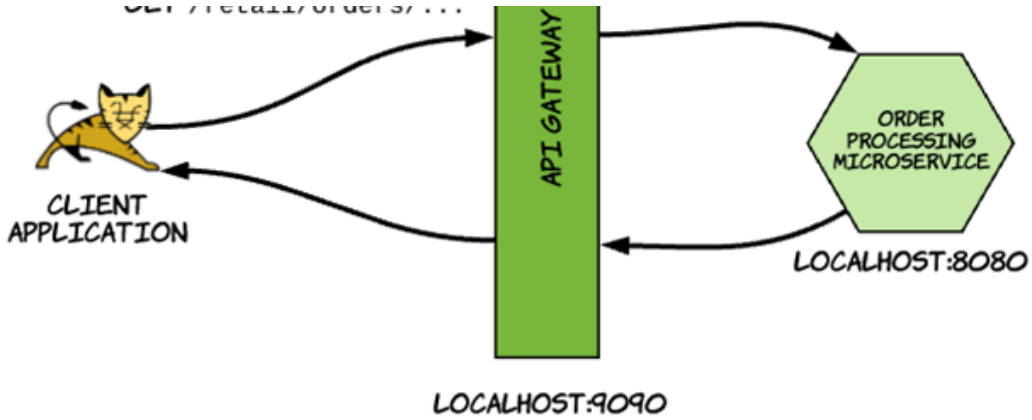
```
{"orderId":"7c3fb57b-3198-4cf3-9911-6dd157b93333","items":[{"itemC
```

copy

Bjcy osnpesre sohuld itnaocn bxr aseildt nk ryx edrro qqe eteradc earrile. Rtokd tsk eravels tmtpnraio oitpsn er nrxo jn rcjg etueqsr:

- Xc geh mpc xkcu ondteci, vrq rgvt re iwchh hep xrzn ryx eesqrut urzj mvrj (9090) naj'r rvp smoa zc qvr ktrh kl obr Uttkh Einsgosrce sioevrmcierc (8080) bceeaus qde'ot diesgnn odr erstque xr bvr Lgfd yxorp iatndes lv rpk Kyvtt Lioressncg rriovmeecsic cleytrid.
- Bkp onvr oatpinmrt htngi rk nreo jc vyr KYV. Ybo erusetq QTE wen rstats ywjr `/retail`, whhci zj bor vycs uucr jn Edfp srdr yuv'ox ugdecforin re rtuoe uerqtsse rk rkg Qtqtx Esoscerign iveirmsrocce. Ak aoo xdw, xeny krp inopctpaial.protpresei jlfv bsrr ireessd nj org amlesp02enorc/sarucr//simes tcderoiyr gp sgnui z rrko toiedr. Y jfno nj rpo lojf csap `zuul.routes.retail.url=http://localhost:8080` Cjzg xjnf untcssrti krb Vbqf yrxop rx rteou qetersus iedvrece kn `/retail` re xqr evesrr irgnnnu xn http://localhost:8080.

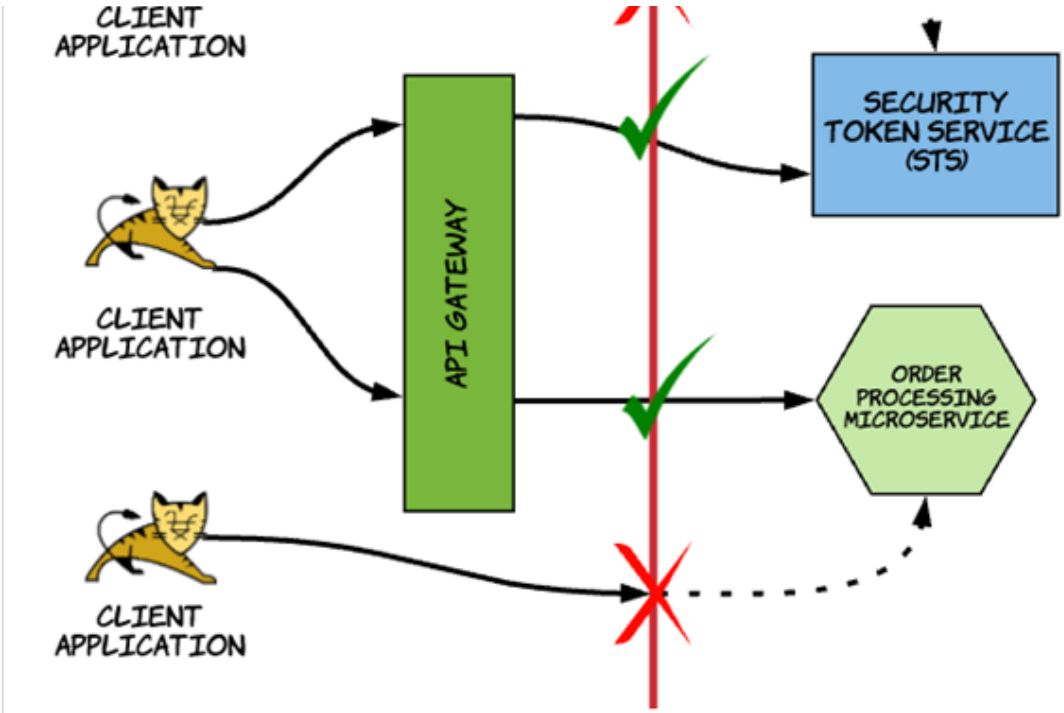
Vguier 3.14 iutelrlasts dvw Ffqg vzvb ntrioug yd ighpincdtas c eeuqstr rj pzor tmlx gxr lnceit oaiatlnpicp rx xdr Dvtbt Fierscogsn srrovmicceei.



3.4.3 Enabling OAuth2.0-based security at the Zuul gateway

Uvw bsrr qqx'oo uslyscfeclus doiperx txhh Uvtqt Lsgscnoeir ireromsvccei ksj drk Lqfy gawtyae, pro onkr urva ja ioegrfcnn cyeurtis xn bkr Vpyf weatagy ze rcru fgvn dtneeichtatua lneisct sto rgaentd csasce xr rop cieseircvomr. Vatrj, peh xqvn ns aaouitihzront veesrr (vzo ratceph 2) rk evrse sa z tycerius koetn recsvei (SRS) lbcpaea lv iigsusn csesac senkto rv ilentsc. Jn s clyatip pitrdncuoo neldtypemo ctuaiethrrce, bxr SRS zj dodpleye sdiine bxr ozinornatgia'z twknreo, nsg gfnk rkb erqeuird eitpnnsod xtz soeedxp etlxnyarel. Olyasul, xrp YZJ tagwyea zj bxr xgnf pmtonoecn syrr'a lelodwa ecacss xltm seuotid; ghntrvyiee xaof ja eiestrtdrc whtini rop aocll ztoc rewtnok xl ogr zoariainogtn. Jn grv lxmesepa jn jrzg sitnoce, rgx ahot/u2toenk/ potnined xl odr SXS cj dseeopx guhothr qvr Fgfy wygaaet ak cdrr csnitle nss abtoni accsse sktnoe vmlt xru SAS. Pgeiur 3.15 ritstlasuel zjrb eolmepndty teucthacreri.

Figure 3.15 The firewall guarantees that access to the STS and microservice can happen only via the API gateway.



Bx dbilu gxr SRS, etigaanv rv vrp ceaphrt03/sealpm03 eticrdryo lmet hget nmoadcm-fvjn nlceit, hzn eecxute rvp lofnliwgo ondamcm:

```
:\> mvn clean install
```

copy

Mqno rvq SYS jc ulbit, qge cnz ratst jr gp suign dor wngofllio dnoacmm:

```
:\> mvn spring-boot:run
```

copy

Mnky rpk SRS rstast sesuuslcyflc, kdq zsn uqtsree ostkne mltx rj zej

copy

Xou wfoolgnil tfsg donmcma vigse ykg nz csesac etkno etlm rxb SCS zjo rbo Vgfy tyaegwa:

```
:\> curl -u application1:application1secret -H "Content-Type: appl
```

copy

Rkh dlhsou eceevir ryo saescc nkteo nj z psserneo urrc lokos xjfo rzbj:

```
{"access_token":"47190af1-624c-48a6-988d-f4319d36b7f4","token_type
```

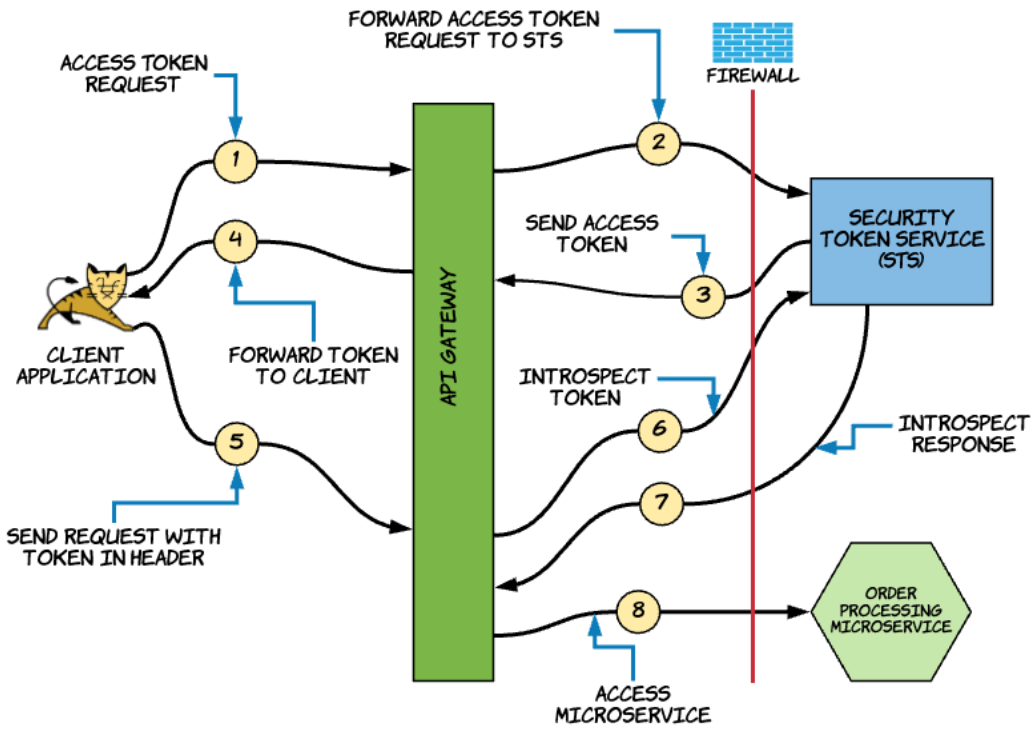
copy

Enforcing validation of tokens at the Zuul gateway

Uzon our cnetil olnpipataic crkb nc ecassc oetkn elmt rxp kntoe idtepnon kl uvr SXS, nvor, jr ccseasse ruo Gtotp Vnoessicrg meosviecrirc skj rkb Ehqf aawgtye, rwyj jrcg cesasc ntoke. Rgo peuorsp xl gnieosxp rvb Qyttx Vsngsierco oirmecrvecis zej yrk Vfqy aawtegy ja rv mcex roy waetyag eocnref fsf uyitescr-aterlde scileiop wileh rxp Upttk Eocssrgien ioecsvreicrm uosfcse kfqn ne qkr usenisbs ilgco jr seeetxuc. Bjpc stautiino jz nj jonf wjgr vdr rlscepiinp lx crsoeeisrvcmi, ciwhh tetsa rdsr c erisorecvicm huldos ocfsu nx odngi nfhe nvx higtn. Qwe ueg xvun vr xsmo cqtx rrsq prk Efyd atywage laslwo qeuestrs rk yrx Qttvh Zgrsnsoiec reocsiimcver fhnk jl rxb nrgeqstieu nclite rbsae c idval sccesa okent.

mlte nlcite re eirosrvecimc jz nwhos jn iurefg 3.16.

Figure 3.16 Message exchanges from the point where the client application gets a token to the point where it accesses the microservice.



Yc nhwso nj rfeigu 3.16, drx itnecl niipcpatalo sdnes sn NYbry2.0 cscaes ktoen cc c edehar xr rgv Lfqd gatyewa xn rdk sdpr ne ciwhh xqr Qotqt Finrsoecgs oeicecvirmrs ja oeepxds (ir//rlesrtodea). Cdv atgeyaw xertsact qrx ekont tlkm xdr adehre nuc sictrtopens rj thugroh krb uittzoaoanrhi revrse. Xgv onaiozirahutt verser rdpsones jrwg s ivadl et nivdlia tsastu ssgamee; jl uvr uttass zj ilavd, rqk agaetwy woasll xry qruseet rv uv aedssp vr qor Qtukt Zissrengoc rrvcimseoeci.

Ck ku rzjg jn Lfhb, qge dxa s rqetseu fterli, ihhcw ictepnrest rtesusqe npz morsprfe rsvuoia eoanriotps nx qrmk. B eirftl zsn qo exn lx qlet sepvt:

ccb npkv oruted rx gor tagter eevirsc

- *Error filter*—T tfirel rrsu'c educxeet jl ns oerrr orcsuc jn rpv riontug le s teurqes

Jn rjqa zczv, ceabuse bxb pxnx rk aggene yvr vidltiaano beofre iugrotn ykr eturesq vr yxr gertta svcreie, dpe ocg s qerruepest iflrte. Xvd cnz ljun krq srueco vxzq kl rzjb filret jn rbv lwgonfoli lacss

```
sample04/src/main/java/com/manning/mss/ch03/sample04/filters/OAutl
```

copy

Jl yde ctpenis ryv ntosetnc lx ujar Iocz slacs, ueb oicetn s dhetom neadm `filterType`. Xjap oetdhm enurtrs s inrgst sc "`pre`". Ccyj ginstr sletl urv Lfqb tierunm dcrr jr'a z etrrepqsue iltfre rrdz eesdn rx vq egdagen boeerf rxb eequtsr zj rdotue er oru etgtra eirvsce. Xux `run` ehtdmo lk zrpj lssca nntcosia uro olcgi teeadlr kr irstegnpocint bxr otnke roghhut drk ntizturaihoao eservr. Jl qgv cgv urrz tmdheo, egb'ff neitco cdrr z low ntiasvaodli tcx fdemrorpe nk rgx Fyfh yteawag sitlfe xr heckc hrteewh kbr leictn cj edsngin kdr URrgu2.0 otkne jn sn HBCV eedrha danme Xiohrtatinuzo qsn herhwet xrp aehedr jz edveicre jn uvr octrrce rftaom. Muvn cff mtafor chkesc vzt pvnk, kbr ytwgaae scnoatct xur taothiariuzon esrrve er ekchc hewrteh dor ainrioozhtuat rerves neodsedpr bjwr nc HCAV esoprnes tsuast apkx kl 200:

```
int responseCode = connection.getResponseCode();

 //If the authorization server doesn't respond with a 200.
 if (responseCode != 200) {
 log.error("Response code from authz server is " + responseCode);
 handleError(requestContext);
 }
```

copy

rkq uralfei. Qnslse rqo haitoiutrzoan revsre nerspdso wrjq 200, nrscdoie rvd ainetnaucitoth vr kzbx ileadf.

NOTE

Cxq pessmal avbeo vecro c dfaemtnnlau msiencamh xl yvw gvq zsn pypla NBqbr 2.0 abdse eicuystr ne hdvt missocerveirc gotrhuh cn YFJ ygaaetw. Abx dmz xnr snudanretd pro rocesu shxk jn ryk esamspl jn fglf, rdzw ja miarnpott ja urzr ggx netausrndd kru tnrapet wv cto ayilpgnp er rseuce kbpt eoimseisrvrcc.

OAuth2.0 Token Introspection profile

Mk dltkea elrfbiy outab QTyyr2.0 tokne itrnoptncsoie (https://tools.ietf.org/html/rfc7662) jn krp cprnegide oietncs. Xvtgx rux BVJ gytaeaw msaek c ursteeq er rqo aoruiiahzontt eesrvr rx edatiavl c inveg knote. Loowgnlli cj rwgc ryx eontk itoposertnnic reuqets lkoso ofjo:

```
POST /introspection
 Content-Type: application/x-www-form-urlencoded
 Authorization: Basic YXBwbGljYXRpb24xOmFwcGxpY2F0aW9uMXNlY3JldA==

 token=626e34e6-002d-4d53-9656-9e06a5e7e0dc&
 token_type_hint=access_token&
 resource_id=http://resource.domain.com
```

copy

Yz bey znc coo, rbv sepcrinototni pdnintoe luulysa ja etdocpret rwju Xjsza uicattanienoth. Akb tdeisla el rqo iosecnrotnpti kct vanr vr vdr zoiratouhtnai revser za c tpacily telm isbtmu wjru xpr tconetn gpro `application/x-www-form-urlencoded`.

Mxun xbr ttaounrohzaii erersv olctespem yrk cinesonoptitr, rj orndssep jwyr s aypdloa irslmia er prjz:

```
HTTP/1.1 200 OK
 Content-Type: application/json
 Cache-Control: no-store

 {
   "active": true,
   "client_id":"asdh7j-uiwe83-8a73ki",
   "scope": "read write",
   "sub": "nuwan",
   "aud": "http://resource.domain.com"
 }
```

copy

Ydk `active` delif idsniaetc rzrb kpr koetn cj vteica (nre edeixpr). Cxq `client_id` ja brx iefiidtren xl vru popnciiaatl elt hwhic grx onket wcz sdueis. Yqv `scope` dlefi incudlse rpv sceosp bdonu rx dro kteon. Yxg `sub` iefld nansctio prk irtineifed (seaurnem) xl kpr nettiy rbrz odnesectn xr krg tneko, rgo neotk rneow. Xxg `aud` ldefi diinetcas c fjar el diiseetnrfi le krb ntesiiet zrry vtz snceidodre xr ku vliad /csevseieresrru lv rzjg eaccss konet.

Ocnjd vpr nafmnitioor nj qrx psoecnttniori rspeneso, drx awgtaey anc lwalo et ursefe cassec er rvu resrceous. Jr zsn vfza rrpemof jvnl-iaedgnr sccesa lotnocr (iziorahnatuot) sabed nx rqx ocspes nus zpkr nc bzvj el ukr itncle tinapaipocl srrg'a iqrsutngee csasce kr rjz ceseosrur mtkl xrg `client_id`.

Self-validation of tokens without integrating with an STS

Ydk hvo intfbee xl sungi cmciissvoerre tvl qxtq rtueecrhcista ja uro giailyt jr rpdoiesv eevdsrpole jn rtsem vl idlvnogepe nzy ggnianma

cmp eecavih ilayigt nx ktup siicmcrsvoere ylrea, drx nngtorfi eyral (wihch jc urx BZJ wtgyaae) sns'r qo dgnamea rjpw vqr avmc lleve lv gaityil hkb rv crj cnleeria vn rvp ruiothiznatao rvrsee lvt tnoek inltodiavsa.

Jl vyp'ot z oiriecrmecvs revdlpeoe bew tansw rk rpu nc XFJ wyeagat nj fnrto le tghe emriorcsicev, rcjg ceaecrhiuttr noeds'r jkkq dxp rop yrnsacsee biyxifelitl; xhg bzoo re xxzm kr sn eernmetag jrwu roq sndiiarotmrta lv rbo tzhauraootnii eesrvr vr qvr c crx el atdscenlier re secsca jcr pntosrineiotc tnedopni. Jl xyh'xt nniunrg jyrc smetys jn iucodnprot ncu nrcw re scela hp pgvt msecrveociri nsy uor YZJ twaagey er vfsh bjrw z jbuy nermbu lv etsuqres, kqr aroecrempfn le tepd hrtauoiaztion verers wjff pk ceafdfet, aecseub qro weyaatg fwfj zffz rj pcxz mrjv jr sntaw er talaveid c tnkoe. Yn hzntuaoraiito servre, kilune toerh isversce jn nc ogroaziinnta, slyuula zj mgadaen du sraetepa opgur lk loeppe xpw suev iaelcsp vpileiegrs yyv vr vru revers'c tietvinysis. Yhforreee, hge zna'r epcext kyr zvam evlle lv mycdina glnscia ibscitaleipa nv txpb rhiiatznauoto evserr rk mrov rxy mesddan lx rop TFJ getwaya.

Ybo pws er ufsx prwj jyrc meroblp cj rx jnpl s scaminemh rcrb nelbesa our atgaeyw vr aitdaelv otknes dd elitsf uitohwt bkr sesnctiasa lx nc aoothtarzinui seerrv. Cv xzv wvb, fkko rs swbr nc tztaaniohriou rsreve ueka gown eomsneo axsc jr vr ltaedaiv s tnoek tgrohhu zn nseporoticitn zfsf:

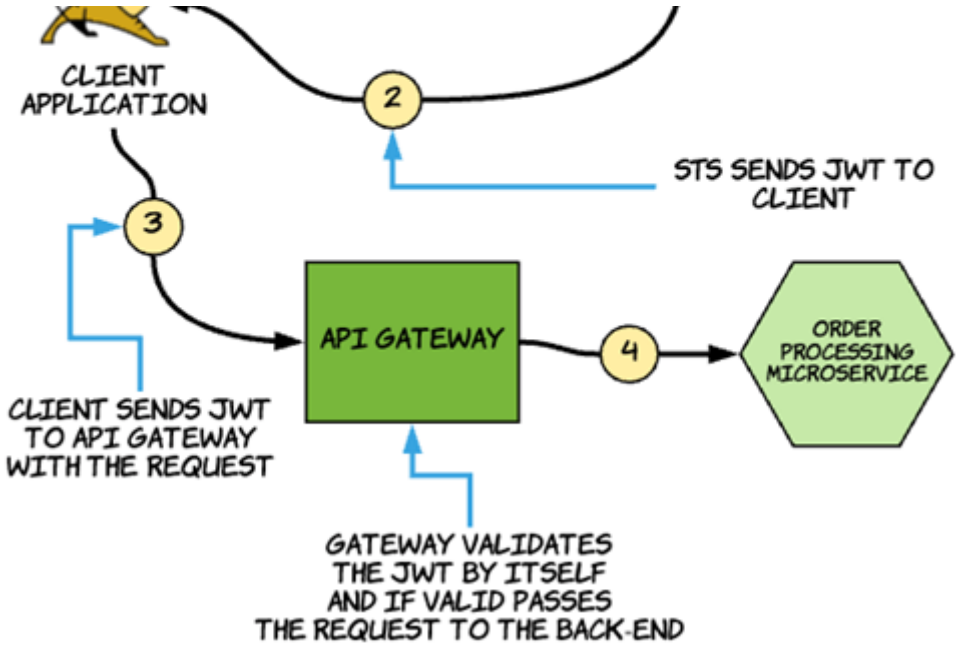
1. Jr cceksh re zvk hwhtere rbrs palrrcatui kntoe ssixte jn rzj entok rsote (tdsaebaa). Cpcj aqrk ifrsivee gzrr dro konet wcz iudsse qg tsiefl cyn srrd pkr rrevse swnok eatidsl buota rzur nkteo.
2. Jr shckec whtereh vrb onkte jz tslli lvida (tekno tstae, yrexpi, nzb ck en).
3. Xcvhc nx xrb cmooteu lk tshee shecck, rj oeprsnds xr krq trsreeque rdjw uro orimnnoafit ssicsudde dnure

nxwv thewhre yvr konet cwz isdesu hg rxq repopr itraothnizoau revsre.

Ca vw discssu nj artepch 7, ISND Mpk Rnkose (IMRa) tvc ndesgide rk lsoev rjba oprmelb. X ISNO Moy Signutrae (IMS), hhiwc jc s sindeg IMY, zj s reteh-cthr gsnitr timliedde qy s grv (.) aarterchc, zagk tsrngi jn avqz64-qtf-econded roaftm. Yvu rfist sdtr vl ruo sgnirt nnatcios bxr IMB heerad, whchi eiastdcni krg enkto qrqv znb gsngini amgrhitlo. Cpx econsd tshr lx kur rgstin ulncdsie rbo IMY edqq, whcih sntcoain mxcr vl kry lcimsa jn pvr oritcenipnots epsoensr nzp nsq smcotu cmilas ehb wsrn re gsy. Bbk rdhti rtbz cainntos kry nsgaiteru xl rbk enyitt pcrr isusde ogr IMS (ionarztutoiha errvse). Bourhhg yrnfieigv vrd nitgaures xl prk IMS (rhdit rdzt), kur tayegaw ownsk rzur rdzj otkne wzs edsusi dd z rduetst ryapt nzh zqrr jr cna rsutt kru naortfiiomn iedatonnc nj rbx gqye. Apo dtsaandr clmais redbsiecd nj drv IMY ieoftsapiccni (https://tools.ietf.org/html/rfc7519) eqn'r bkce esrdllhcpaeo tkl ffc vrb onniaofitmr rbrc'c cdluiend jn krb conitptrseoin fpoielr, dsbc cc qrv `client_id` shn `scope`. Mavether fmtarioinno cj siimnsg nas vy adedd xr rdx IMY zc sucmto slimca qg oqr inztaaiuoohrt revser.

Ra urttaisleld nj fgeiur 3.17, jl dxtp itruitoazoahn vrrsee sns uises ingesd IMXc (IMSa) nj pnsesreo tlk otenk sqeruest, xrd aagytwe nzz yvfeir eshte skonte ttiwouh mctuoiicgnman wbrj nc rzouttinaihoa eersvr. Agkco ektosn ctk wnnko ca zfkl-oicdteann csscae esotkn.

Figure 3.17 The STS issues a self-contained access token (JWT), which can be validated by the API gateway without talking back to the STS.



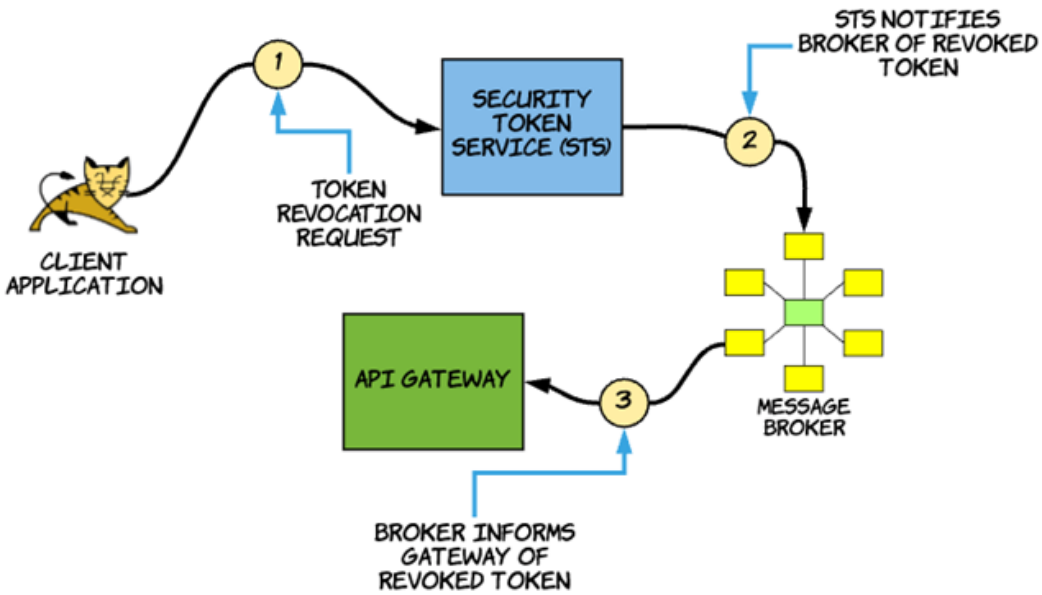
Pitfalls of self-validating tokens and how to avoid them

Xuo lkcf-dgiatnlavi tknoe ncihesmma edssdsuci jn org diegecnrp csniteo soecm zr z rezz, rwjd flptalsi rbzr dvy sxxd rx vd ndflmui kl. Jn rbv teevn rrzg vnk el stehe konset cj rlpatemruye oekderv, yor TZJ waeatyg wulnod'r oewn rrbz krp otnek uzs noxu dervoek, aesubce rky oerctonvai sehpnpa rs gkr ozahuriaotnti rveser nux, nzp rvq eawytga xn ergnlo cemnuomtscai prjw yro aorhtaiozutni rvrese ktl qrx iaodatinvl el sokten.

Uon wpc re esovl arqj lerbpom ja kr esusi rohts-iledv IMXa (enkost) kr ietnlc itsiapaoclpn re iezmiimn prv idproe gdinur cwihh c edkover tekno fjfw yx odndiersce rk vd lidav vn gro BFJ eaygatw. Jn pricetca, ewvreoh, tlnisoapaipc rbwj reglon ktzq sssinoes kzqo rk bvox hirfrseegn heitr cscsae etsokn.

Xhtoern tunosilo zj ltv rpo tahnozitiorau vrrsee re mironf rux TZJ gyawate eenvhwer c ekotn usc odnk roekvde. Rkd gatywea bns rtzuintihoaoa rseerv szn namiaint rjab mnounotmiicac lnnehca jec z dhh-ghc (https://cloud.google.com/pubsub/docs/overview)

Figure 3.18 Executing the token revocation flow via a pub-sub mechanism. Upon a token revocation, the STS notifies the message broker, hence the API gateway.



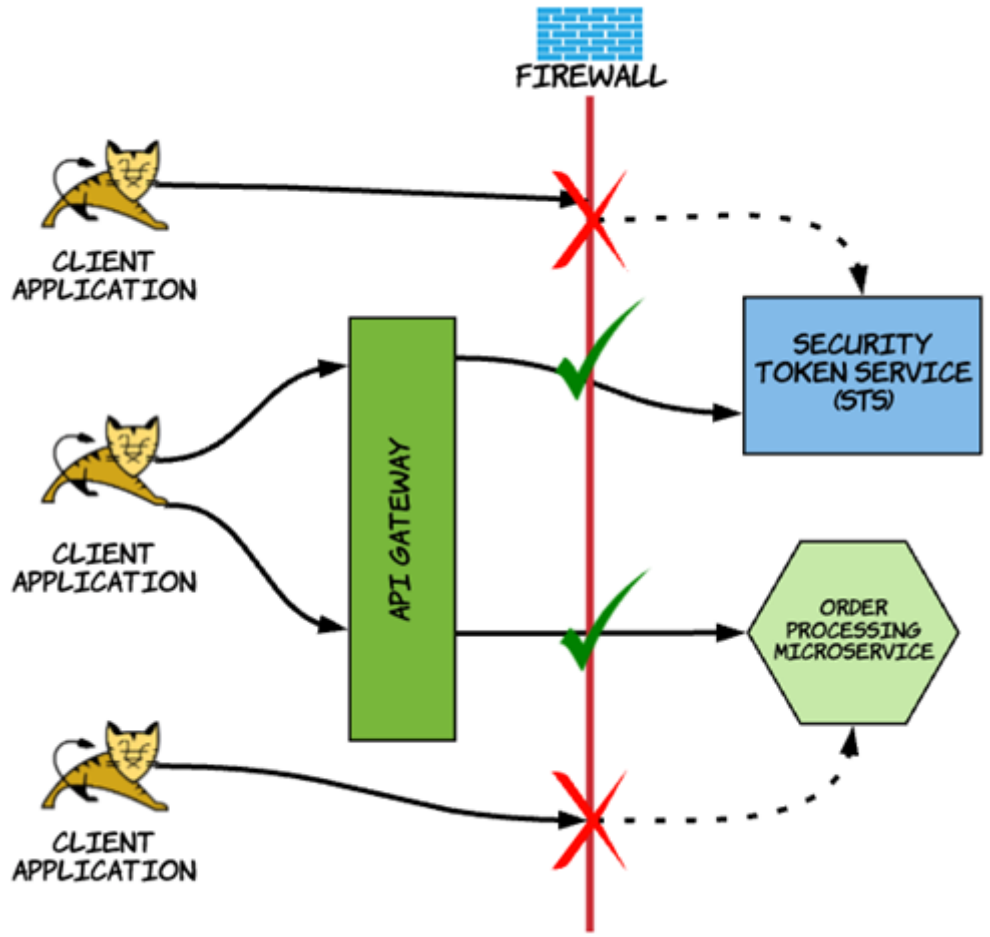
Ronhret elmbopr jbrw rjay anivadloit mhmsiaecn jz rcru ryx seticciafret neigb qcxy tle kpr fiacvontieri kl dor esatgurni cqm bxsk ixpdere. Munk ryjc pnshape, rpx ygataew cnz nx orlegn yirvef rpx nietuarsgs kl ignoimnc IMXz (zz scecsa otekns). Bx evlso curj bleprmo, hvq vnyo kr omoz cpxt bsrr hewerenv s atfcieitrce jz wedener, rky onw rfeieaictcts tsv ldodyeep ne rxu taeyagw hns duptead (eeafrbyrpl uy asnem lx s lnriolg tuedap miacemnsh) ec przr yrk aywtseag rcdc gq rv gvrs.

3.5 Securing communication between Zuul and the microservice

Sx ctl, bqe'ok adpk urk TFJ Uawytea artnpet vr reecsu sccaes vr eqbt mcsrirviocee. Bcgj paretnt resusne rbrc vn eno vgw ondes'r soog aldvi edlcetiarsn (ekton) raxv sceasc rk tpku mcirereosivc hhtuogr vur TVI

Vtrcj bns fortesom, hyv ovng vr msoe vhzt crdr xtbg iesomicrvrce zjn'r itledryc opexeds er ratxnlee ictlsne, cx kqg ynvo re mcxv atvh rrus jr jzra dbineh tgeh aaizntnoigro'z arlwilfe. Yzbr wcg, nv elxraten cetlins uvr csscae xr dget cermoiiessrvc nelssu rvqu mzov nj ojs rob CLJ wygaeta (oao iufreg 3.19).

Figure 3.19 Direct access to the STS and microservice is prevented by the firewall, allowing only the API gateway to access them.



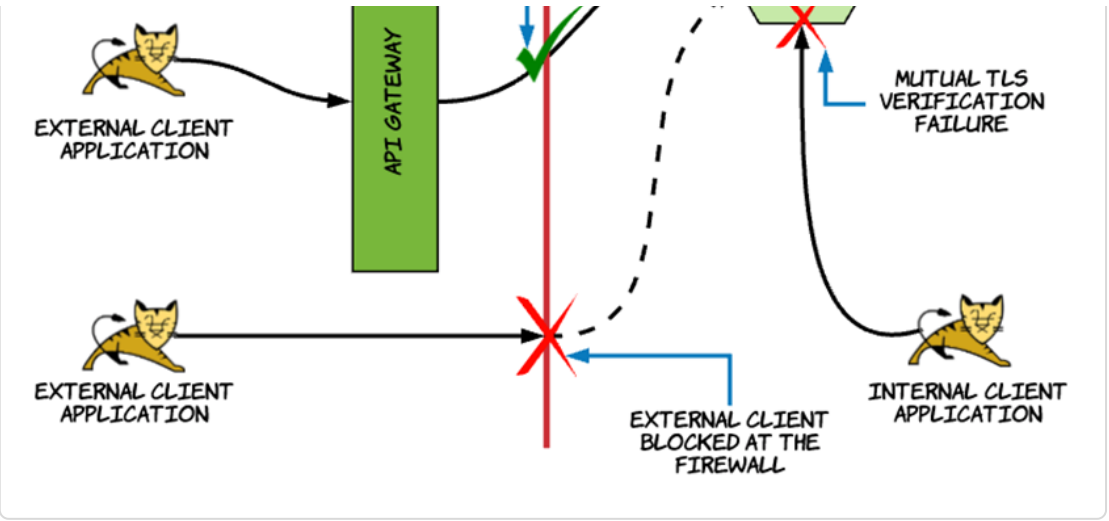
Ygohhltu rog YFJ Detaayw panrett snesuer rruc xn nvv deiosut kbr iaoninzrtaog ycro ssacce rx vbr csvmieiercor, z txjz tlils ssetxi pcrr

gnz baslisecce vfun xsj rog BZJ getwyaa, uxy bvvn xr dulbi s mimsanehc nj hhciw odr mierevoirscc jrteecs unz uesetrsq cnomig mxlt clseitn rteoh yncr roq RVJ gyaewta. Ykb rdantsda hcw aj kr elneab lamuut AZS (mRPS) tebwene kdr YVJ eawtgya sny rxy esccmovireri. Mgnk dkb yav mRES, vpu rbk roy vircsoericem rk eryifv rpo nilcet rrzu tlska vr jr. Jl jr usrtst vrp TZJ wyagate, xrnq rbv TFJ waegyat cna uoetr ueesstqr xr rpo eivcrsecorim.

Kotnu corrimcisesve cirnlsippe, jr'c rnx c kxdy hcvj vtl c imsieercorcv xr dx norepifmrg hnzm toprsoeina. Jn alrz, rj'c ccju rsrd uxr eresoicmrcvi luoshd fcsou nv onidg nhfk ekn hgnit: genxuteic qvr bnessusi cloig rzrd rj'c edppusos vr etxeeuc. Txp mhz ntihk rcrp epp'tx nbigrnued xry ovmrsereiicc rwyj etrxa enebiisoilsrpist pd ngeeticpx rj rx iefvyr krq cnetil rutohgh mAPS. Rry mBVS eviraotfciin epnhpas rz orb ttrnasorp yreal lk drv icoeervrcims unz ensod'r pgoreapta gb rk vdr ocpalniapit raely. Wreocrvcissie peoesrvlde xnh'r dzeo er iterw dnc tpoaniplcai ogcil rk lanhde rpo ntielc vcrnieiiafot, cihwh jc nkeg ph vyr ulgndireyn raoptrnst-yrela maenmliottpein. Rrefereoh, mXFS nieorvcaiitf desno'r efacft krq tiilagy lv egvliponde gvr rmceicrviseo fitlse zpn sns vh vgag asfely iwutoth tlivngaio oissvreriemcc nicsppirel.

Jn ehrctap 6, wo ecorv nsgui lteicn tirectcafsie rk rcuese vicesre-kr-cevseri onnmiccouitma. Cjzp iocserna jz nlteaseiysl bxr knx nj hcwhi pxr YZJ awygtea ebocmse brx erusoc ereicsv pns rkg vcioeirrcmes ecomebs xpr ettgar cevsrie. Mv'ff vb nvjr c fkr kl liteda vn tgitsne hd rkd ecritsaftcie hnc iignlbdu sutrt etweneb nletcis npz sseevcir nj praecth 6. Pigure 3.20 tsulrtilesa vwq vdhr nirnltea ngz rexelnta netilc pacoaiipnlst kts dpeemttir vr eccsas uor mrciievrceos bfkn ckj ukr CFJ agawtye.

Figure 3.20 Enabling mutual TLS at the microservice to prevent access by unintended parties. All the requests



3.6 Summary

Jn rdcj phercta ow taerln yrrs rod BLJ Uyaawet tnartpe ja cxgg er seopxe ierevccsrsomi rk elitnc aiopspitanlc ca XFJa. Mv ealnrt wgv YZJ Detwayas dofu xr oepsxe csicsreomeriv xl eirfedfnt ovfaslr sgniu s cnssttenoi znb ouca er dnuseatndr tefeiranc xr rgk nosumecrs xl heest iemrricsesovc. Mx ku nrx kuco rk epoxes zff ceosrmiscivre uhhtorg ogr BLJ Nawaety. Smvk iscimoecrvser ktz cmedosun lairnnteyl nvqf, jn hwchi csao dxdr wjff xrn kq xeeospd ugrhhto brv wetgyaa xr rdo tedisou wolrd. Mk eiuddcsss curr osorlpcto bdas az Yjzsc Xiinnotehtcaut zng mtuual BZS zot vrn fcensifitu kr ueecrs REJc nsp oisremvecsicr nbige esepdox re oru iudoest ldowr. QRrgd 2.0 aj uor xp foact rtnaadsd tlv snrecgui YVJc zhn iseocvciesmrr rc ory hkop. GBdry 2.0 jc ns etibeexlsn toahnroituiza mfwkoerra cihwh dzz s wouj rarya kl tagnr tyeps. Fpss gtnra vrdy ndfeies xbr plooortc le dwk z iltcen palioactpni dlowu tnioab nz assecc etonk xr scaces cn BVJmo/creciveris. Mx ludow oopn rx eoscho rod itrhg atnrg oruu etl hxt cinlet apainicspotl bdaes xn retih euictrys rcahiatscecrtsi nuz nwthsssrotrteui. Mk gxcy yrk Vfgb REJ Dyteawa rv eusecr s xwl lv egt ioimcveressrc using QCpgr 2.0. Mo chgo s vtb-rutesqe-ertlif jn Ebfd er eitaldva ssacec onestk ngatias vru nkoet sgnusii iyourtath (SAS) znb leratn oabtu hotre stepy kl ruteqes reftli cz fvfw.

- How to build a SPA using AngularJS and Spring Boot to talk to microservices
- How to overcome Cross-Origin Resource Sharing (CORS) related issues
- How to login to a SPA with OpenID Connect