

Insecure Transit

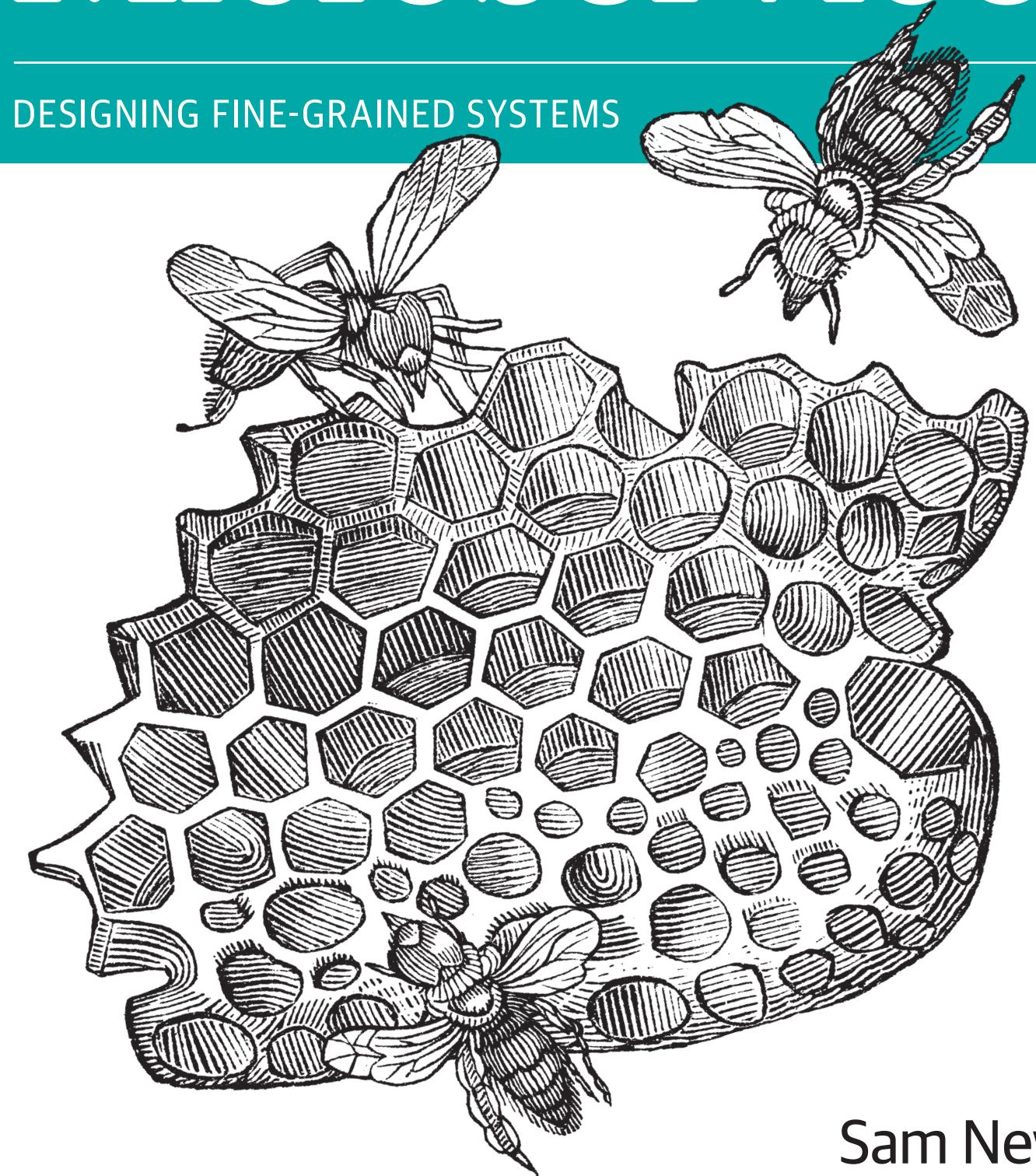
Microservice Security

Sam Newman - QCON London 2018

O'REILLY®

Building Microservices

DESIGNING FINE-GRAINED SYSTEMS



Sam Newman

Sam Newman &
Associates

Massive Equifax data breach - what you need to know



By Cullen Mawer, Money Saving Expert
10 Sep 2017 | 0 comments



Credit report heavyweight Equifax has warned that up to 400,000 UK consumers may have had their personal details stolen as part of a massive global data breach. Info on exactly who's been affected and what you can do about it is still somewhat sketchy, but here's what we know.

Equifax revealed on 8 September that 143 million consumers in the US could have been affected by the incident, which saw Equifax's access data such as names, address and dates of birth, as well as credit card numbers in a smaller number of cases.

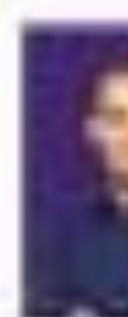
Although its UK business – Equifax UK – runs fairly systems in this country are not affected, it admits a file which was stored in the US and contained more limited personal information on up to 400,000 UK consumers may have been accessed.

Related MSE Guides

[Credit Scores](#)
Find myths & mistakes your bank

[10+ Ways to Drop Scores](#)
As banks get clever, learn to be too

[Check your credit report for free](#)
Get your file and check your score, or even get FICO to do it



Get Our Free Money Tip Email!
For all the latest deals, guides and
inspiration, join the 12m who get it.
Don't miss out!

Enter your email

www.moneysavingexpert.com

What is Equifax and what data does it have?

Equifax is the second largest credit reference agency in the UK, after Experian.

Security

Meltdown, Spectre: The password theft bugs at the heart of Intel CPUs

AMD, Arm also affected by data-leak design blunders, Chipzilla hit hardest

By Chris Williams, 12:00 p.m. CDT 4 Jan 2018 in ST.29

202 24 SHARE ▾



Spectre The severe design flaw in most microprocessors that allows sensitive data, such as passwords and crypto-keys, to be stolen from memory in secret – and its details have been finalized.

On Tuesday, we learned that a decade-old bug in Intel's CPU could allow applications, hardware, and JavaScript running in web browsers, to obtain information they should not be allowed to receive: the contents of the operating system's private memory areas. These zones often contain files cached from disk, a view onto the machine's entire physical memory, and other secrets. This should be invisible to normal programs.



GDPR Portal: Site Overview

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR).

After five years of preparation and delay, the GDPR was finally adopted by the EU Parliament on 14 April 2016. Enforcement date: 25 May 2018 - at which time these organizations will not conform via their home laws.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe. It protects individuals' personal data privacy and to regulate the way organizations handle the region's personal data. While the key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

Quick Links

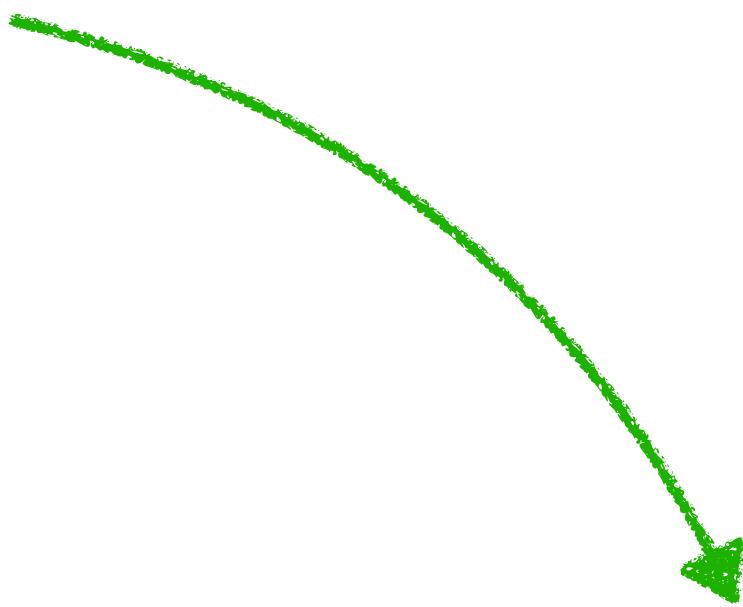
[GDPR Key Changes](#)
[Summary of key changes](#)

[Timeline](#)
[How to prepare](#)
[Is my organization affected?](#)
[What does Brexit mean for GDPR?](#)

<https://www.eugdpr.org>

Design

Design



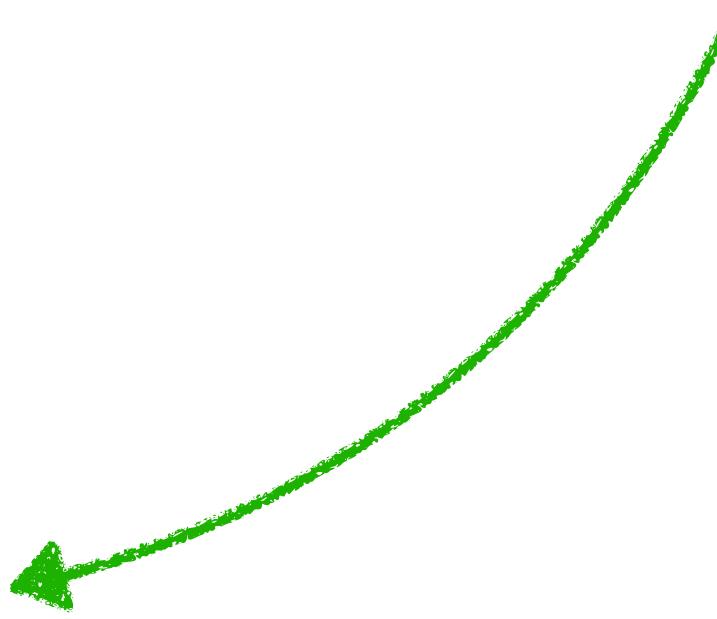
Develop

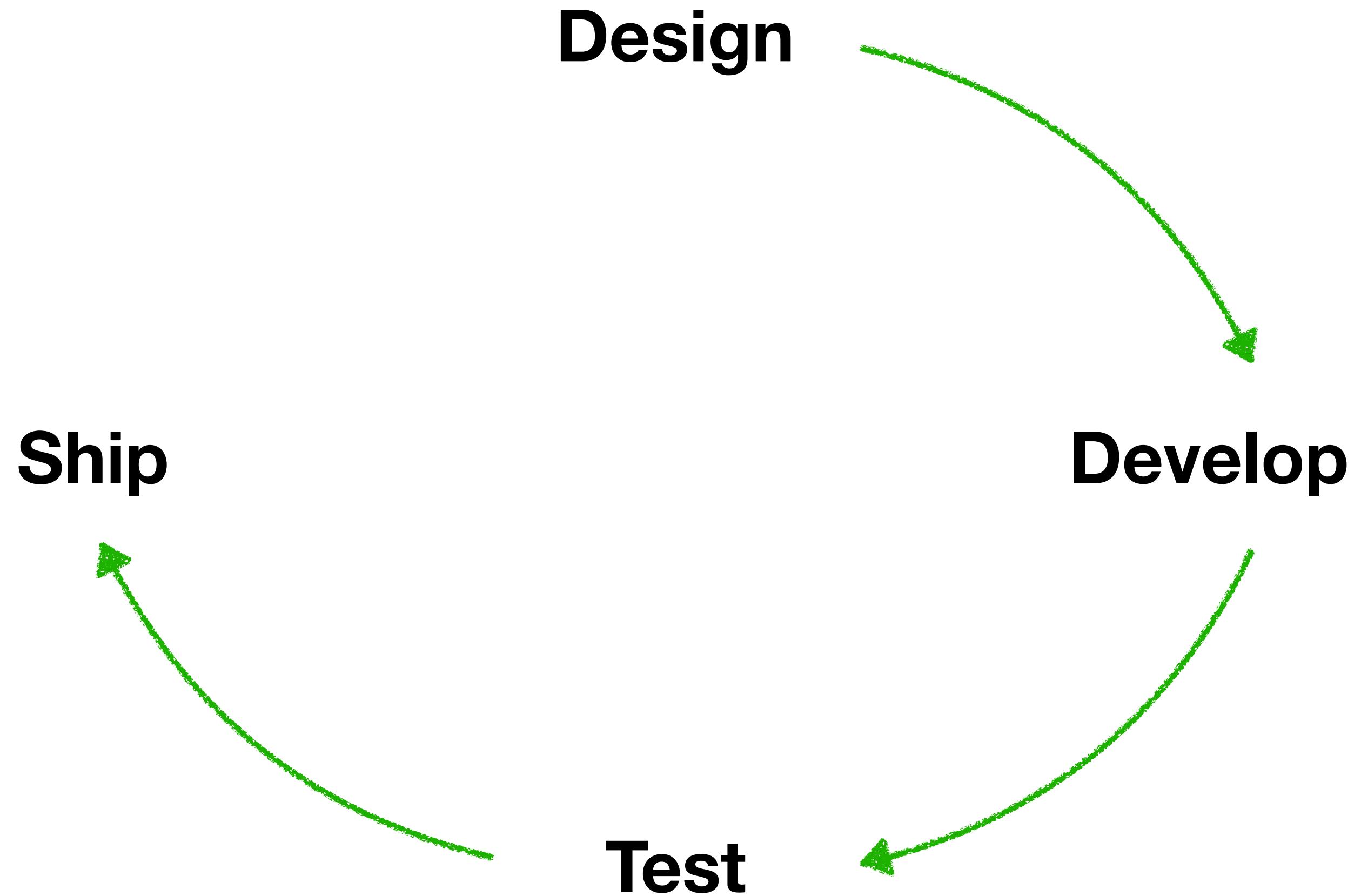
Design

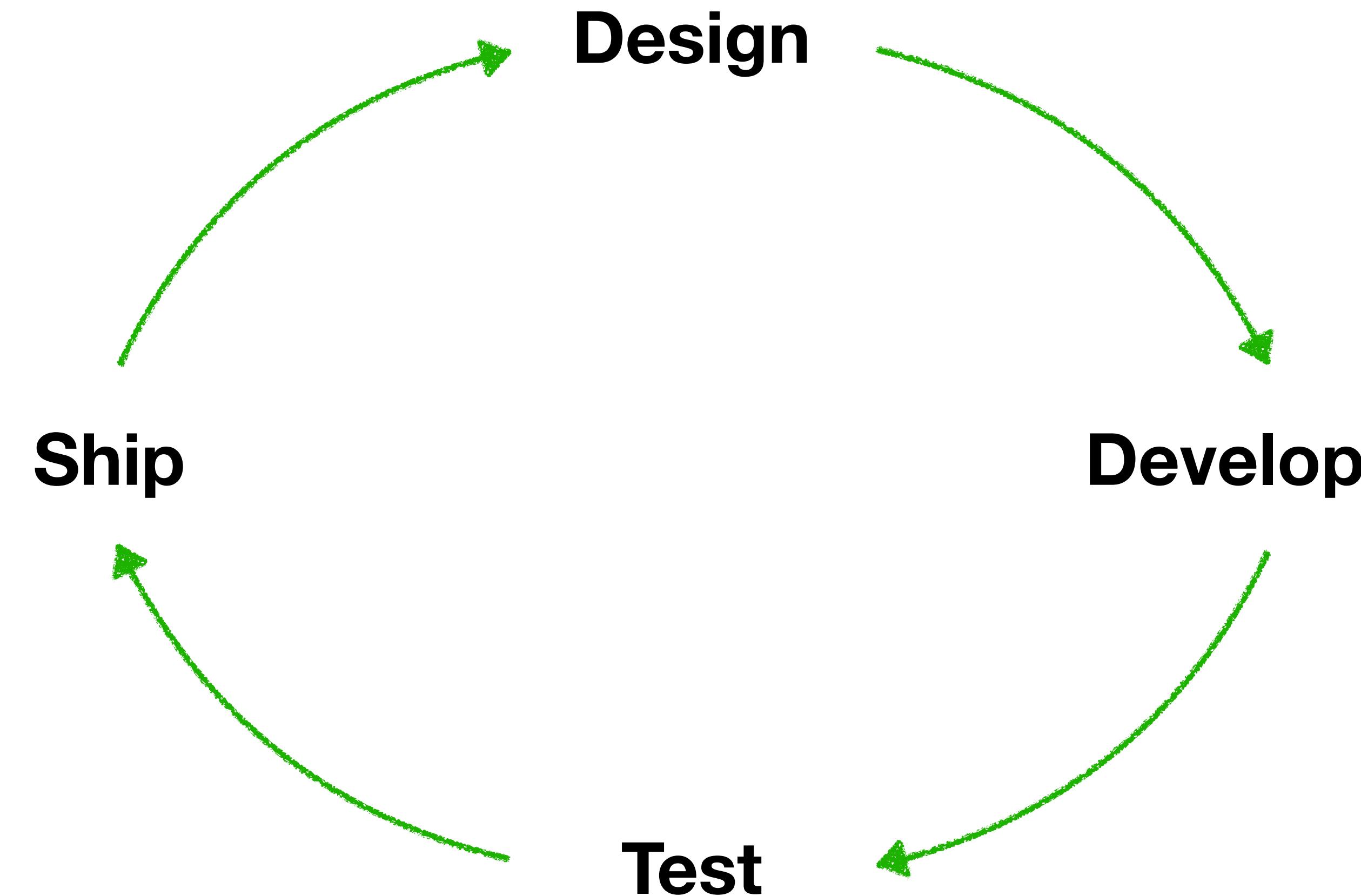


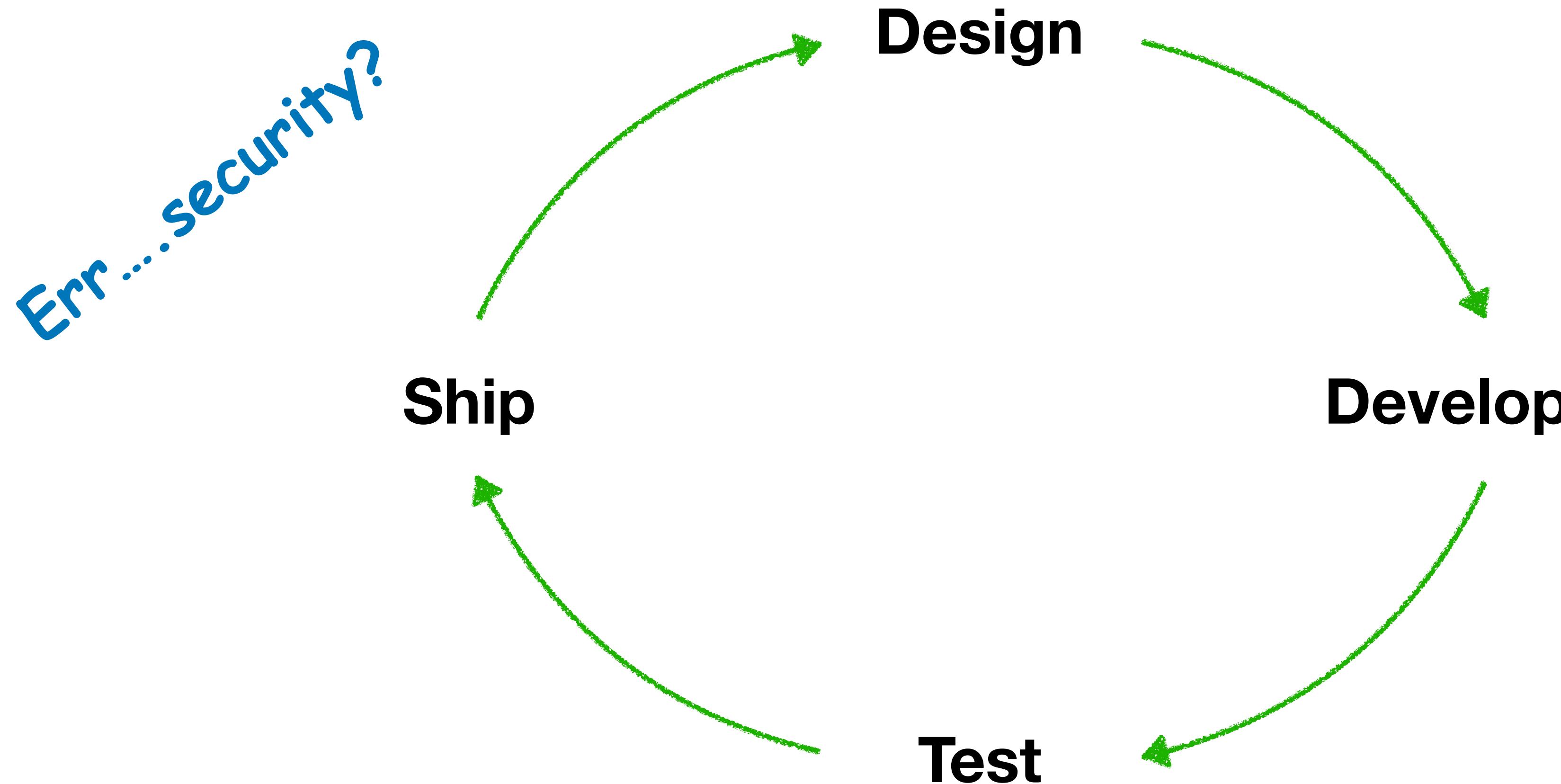
Develop

Test











<https://www.flickr.com/photos/labyrinthx/195473339/>





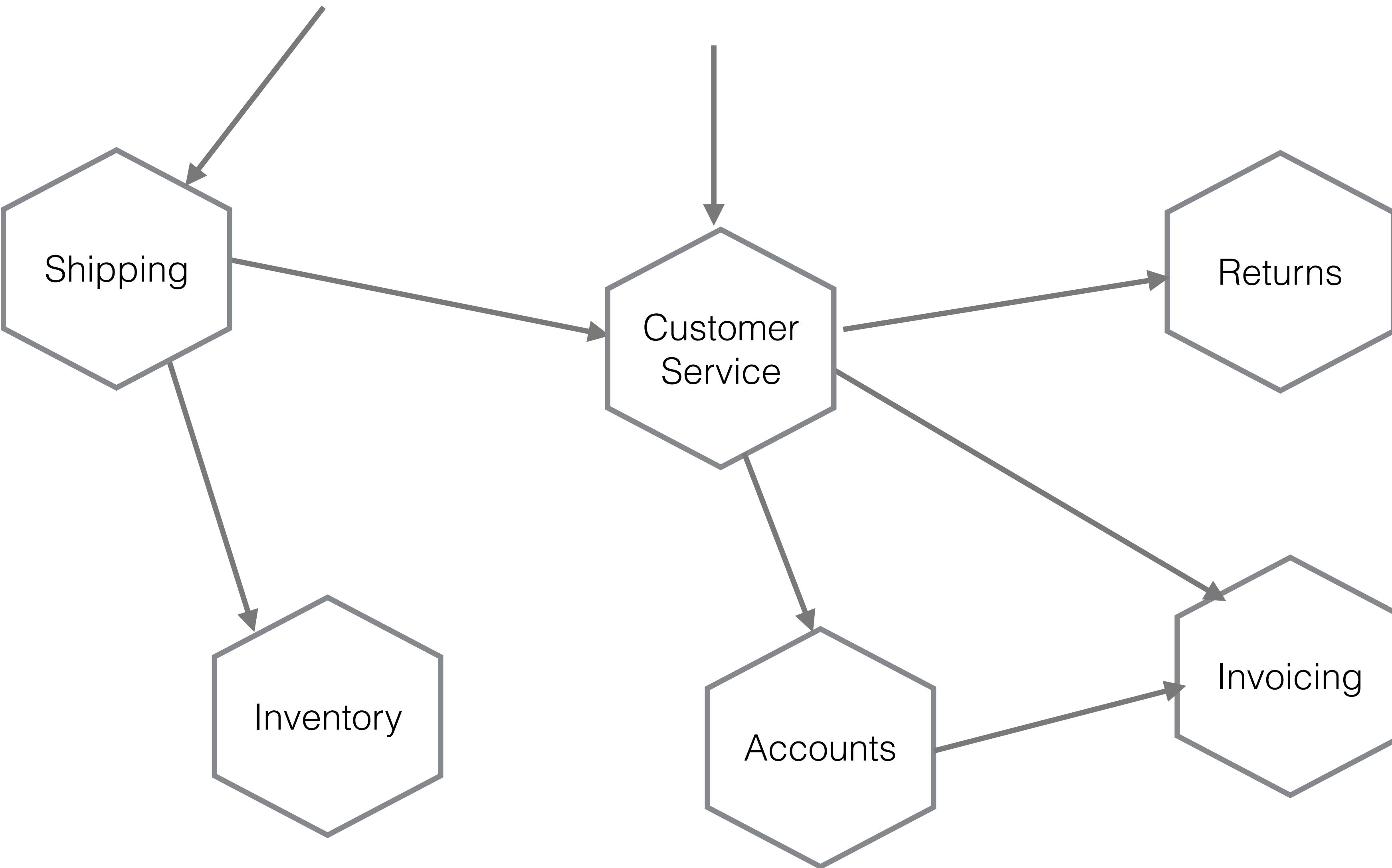
<https://www.flickr.com/photos/seattlemunicipalarchives/4058808950>

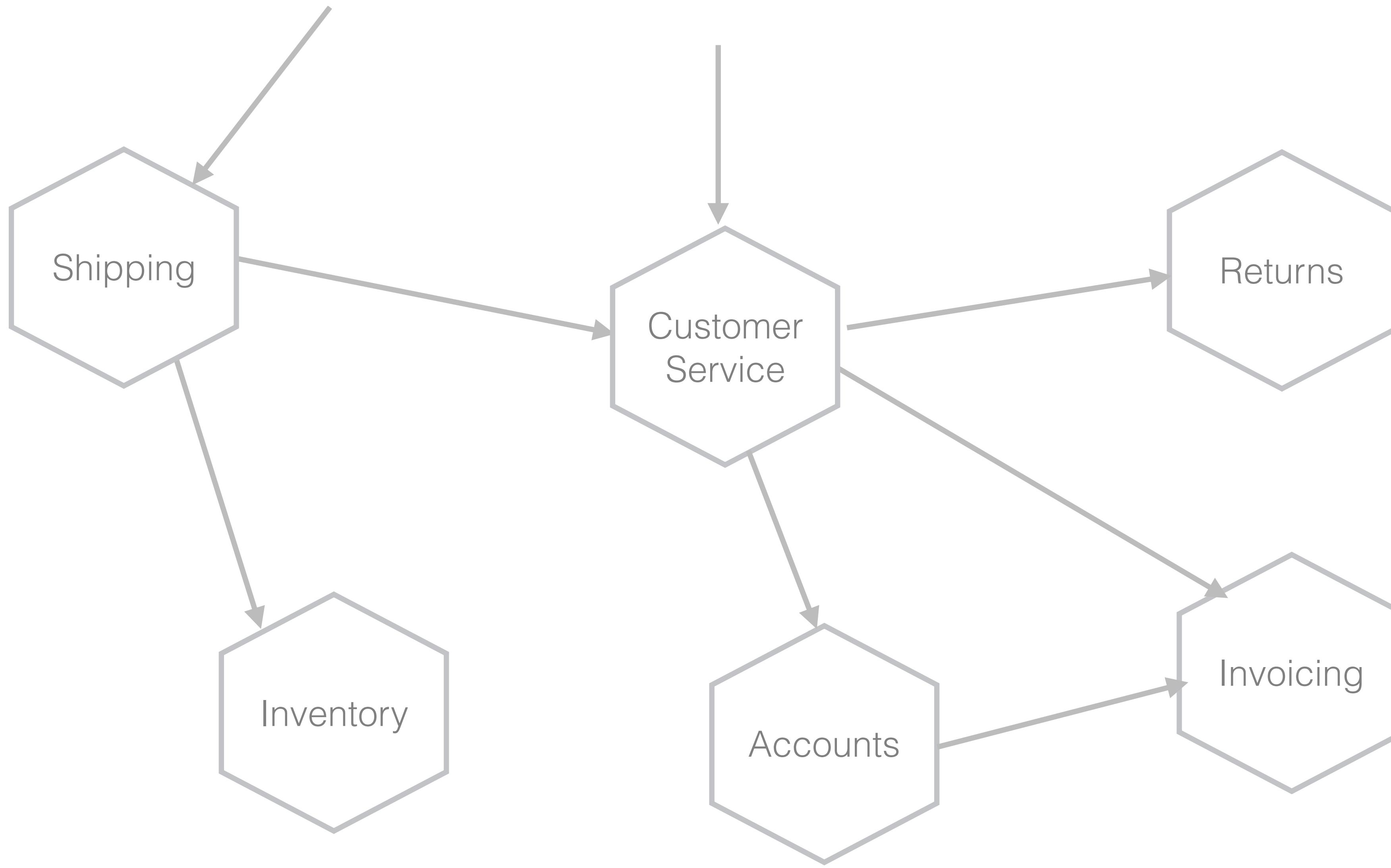
amnewman

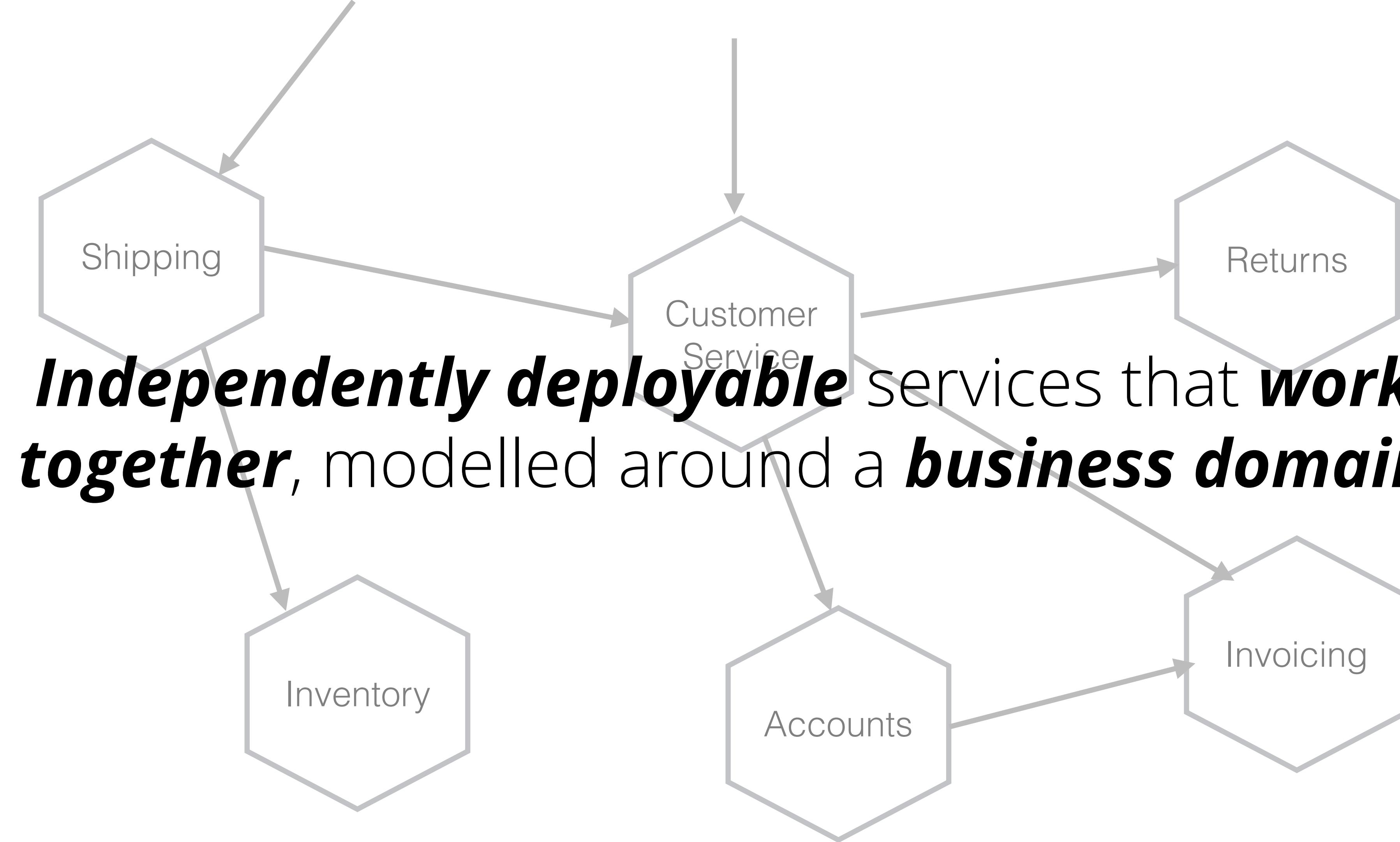


<https://www.flickr.com/photos/theseanster93/485390997/>

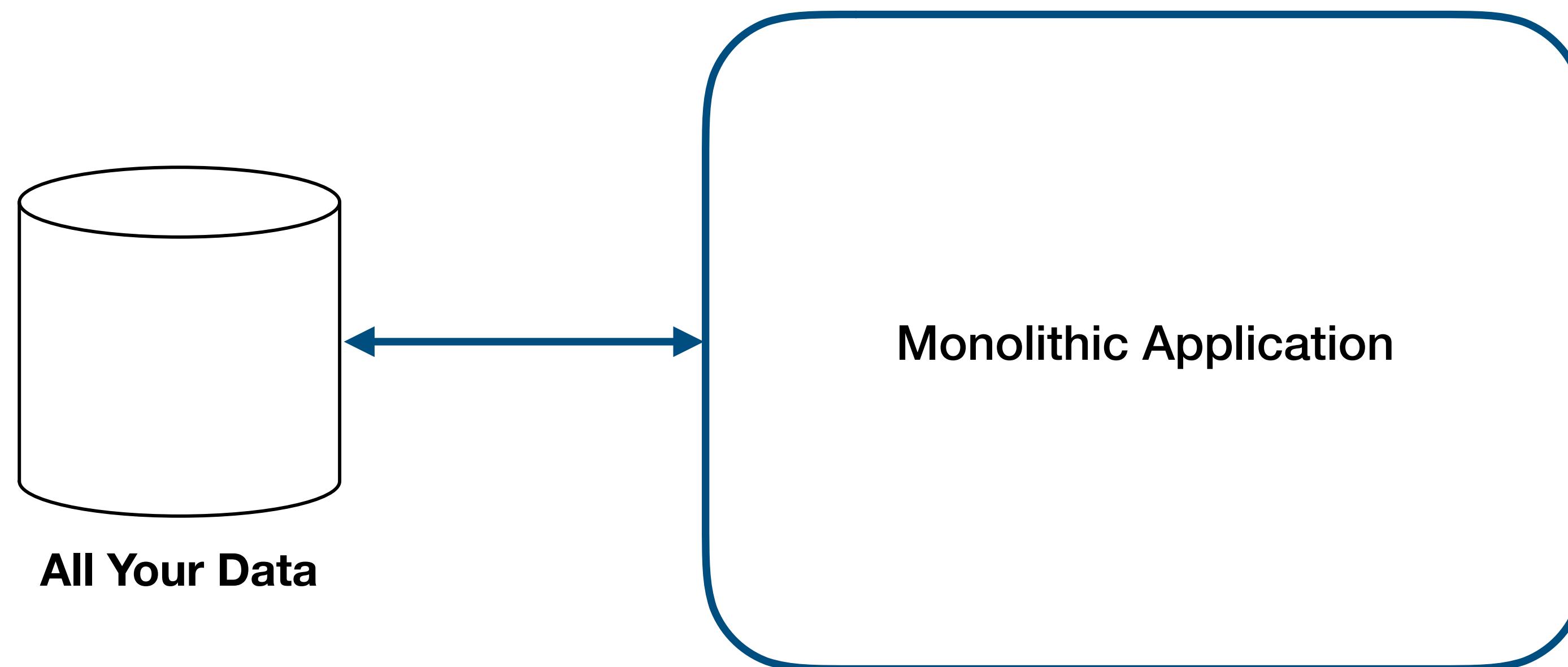
Just Enough Security







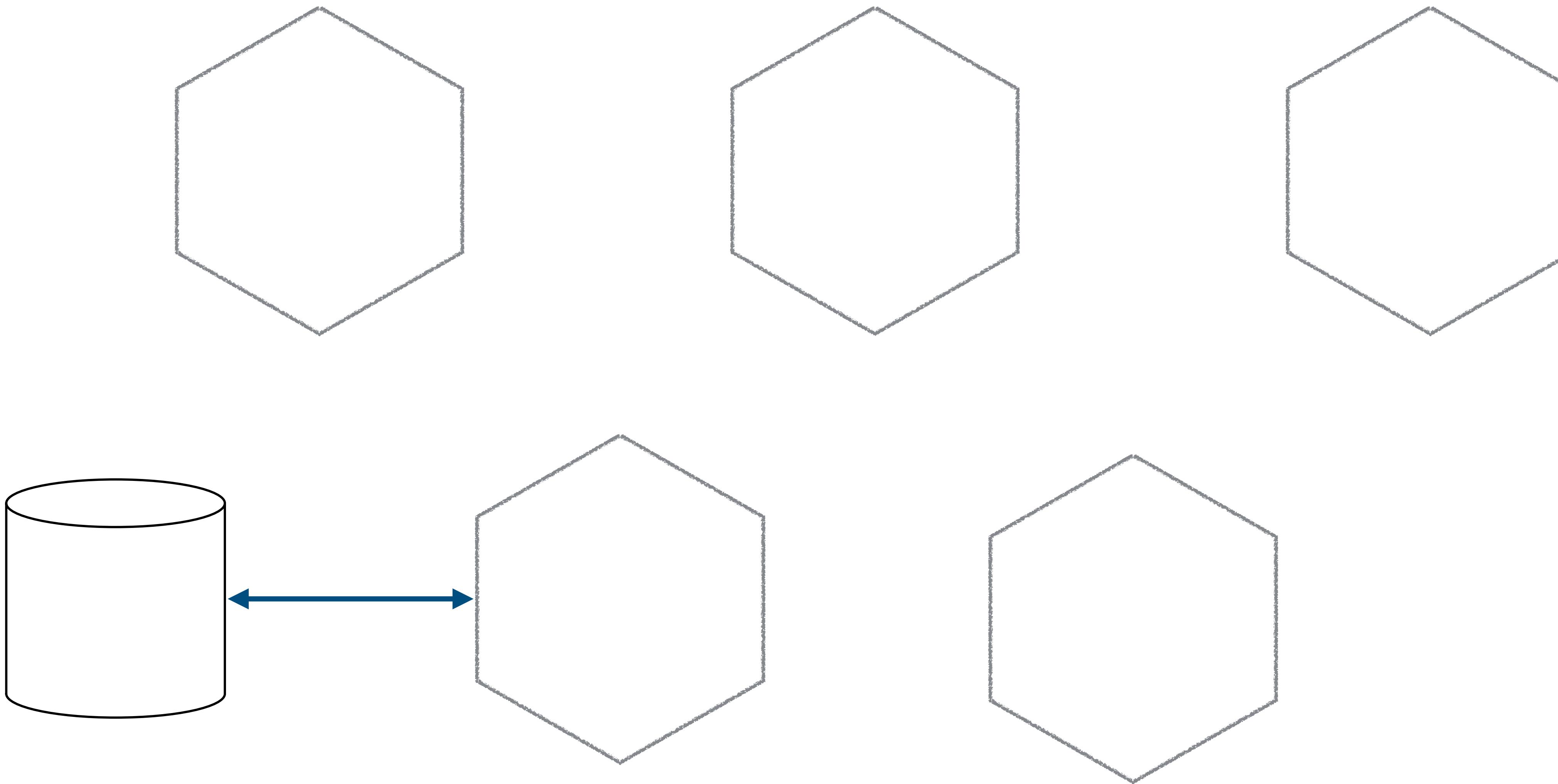


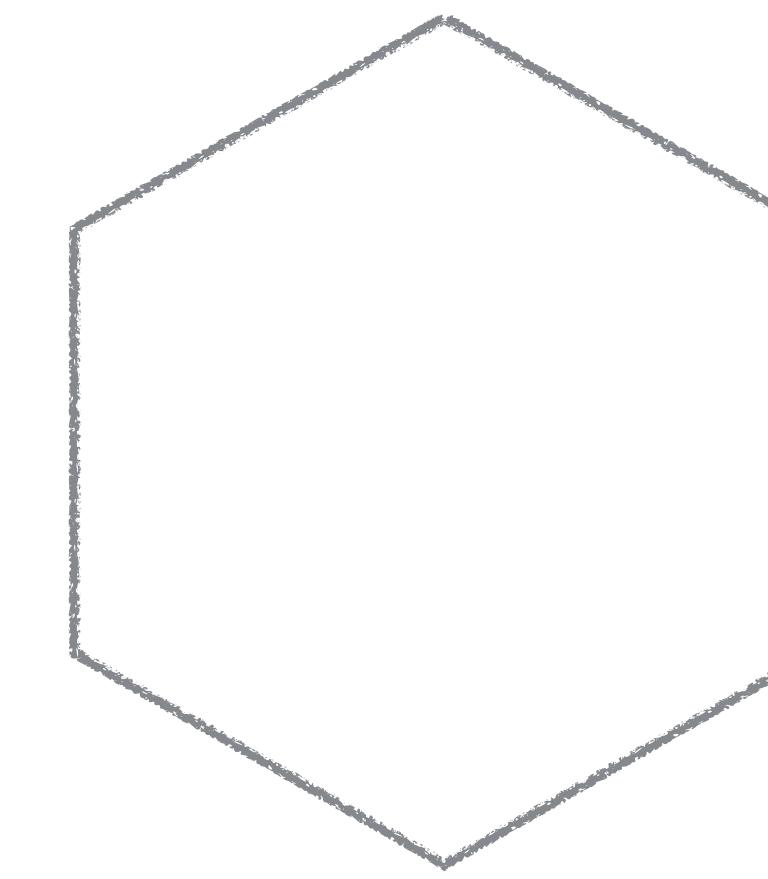
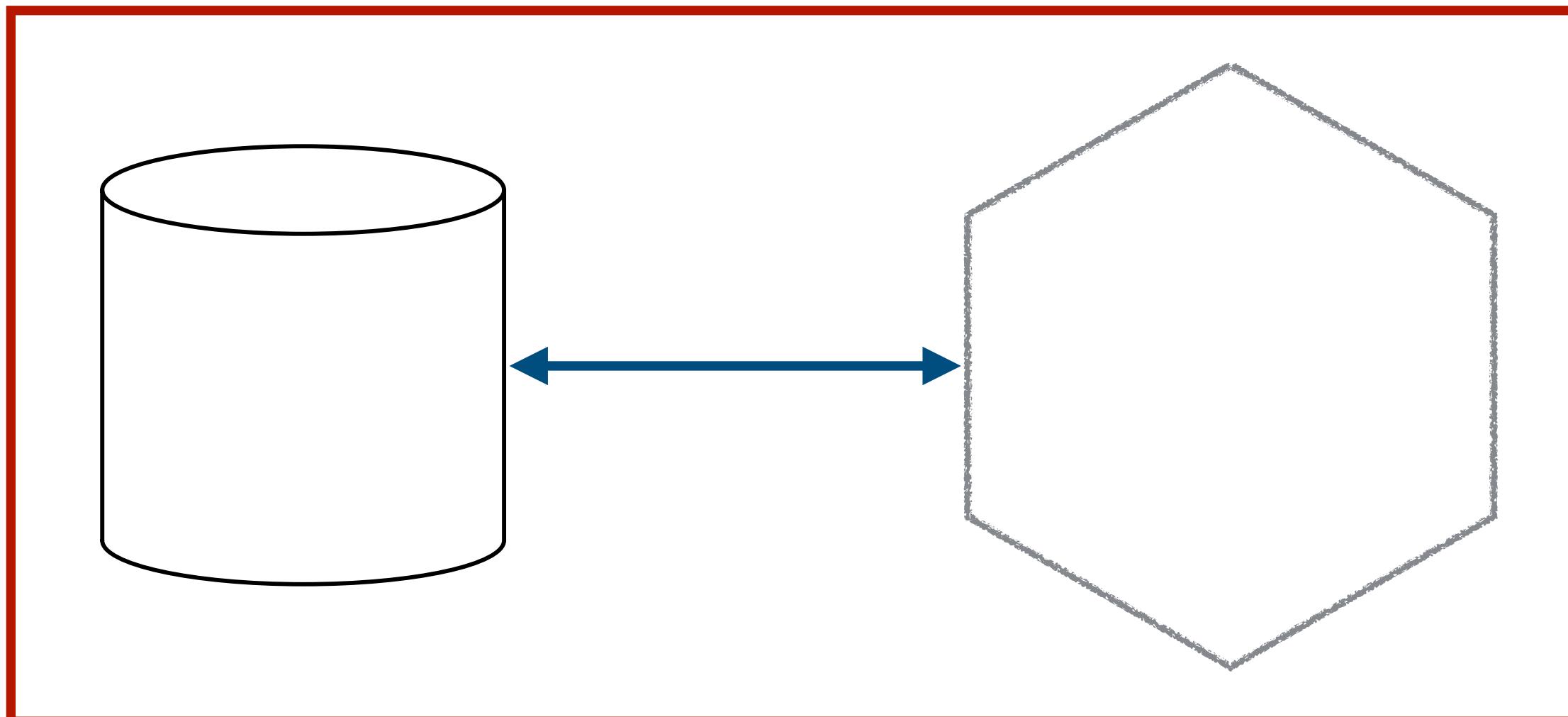
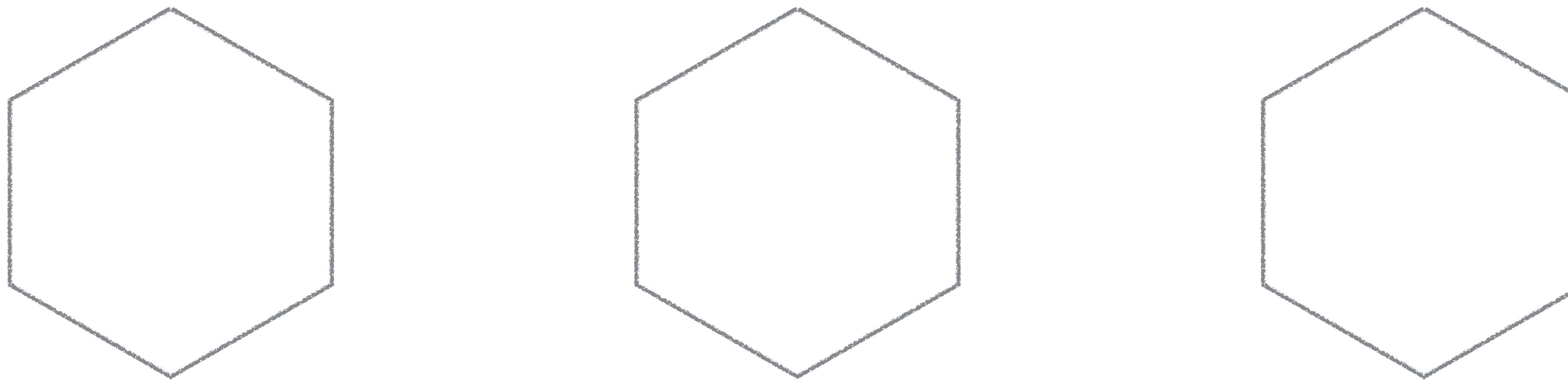




<https://www.flickr.com/photos/lkowen/15803718243/>

@samnewman





Guide to the General Data Protection Regulation (GDPR)

Home  Download options 

Search this document



Introduction

What's new

Key definitions

Principles

Lawful basis for processing

Consent

Legitimate interests

Sensitive category data

Official offence data

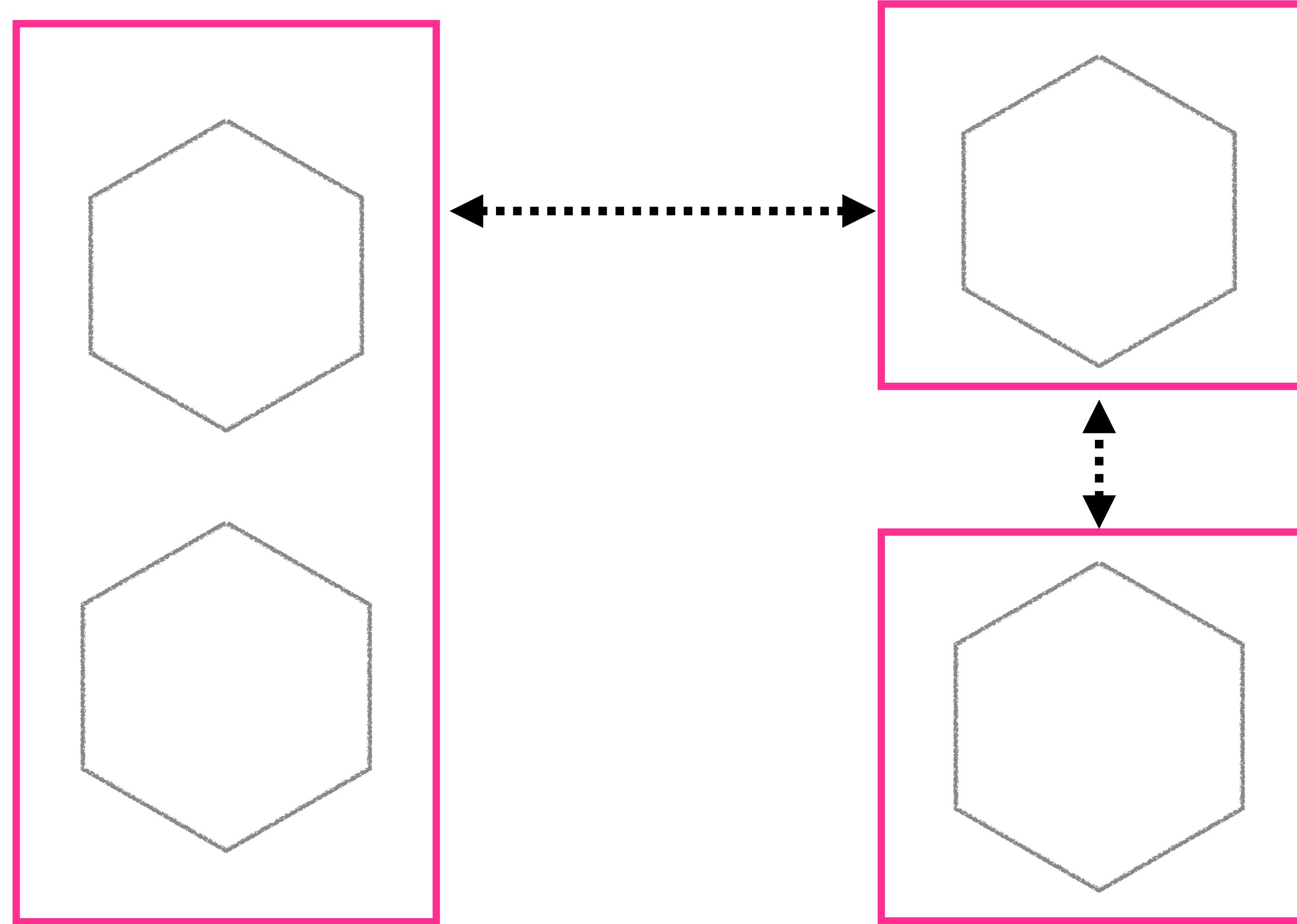
Introduction

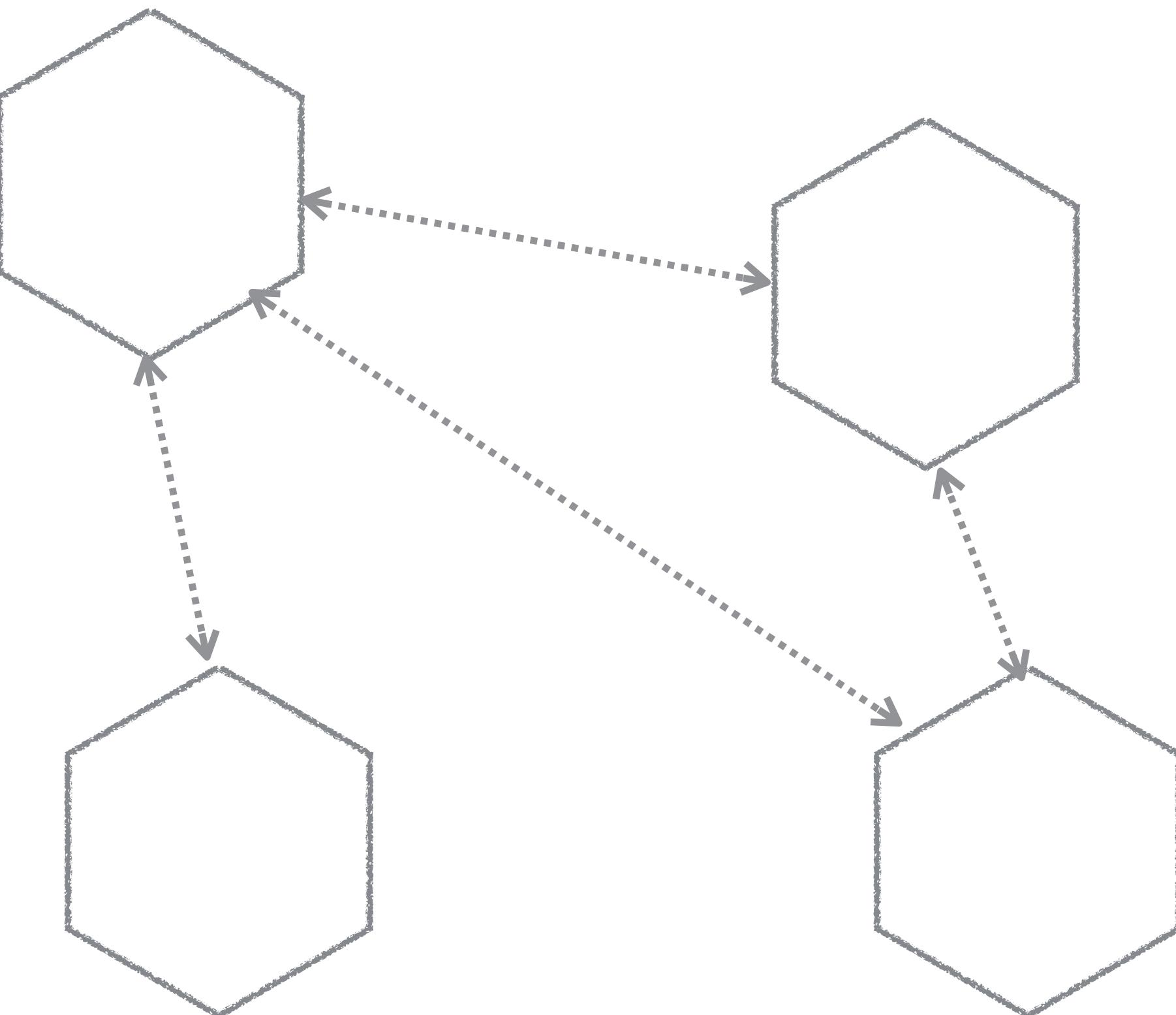
The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

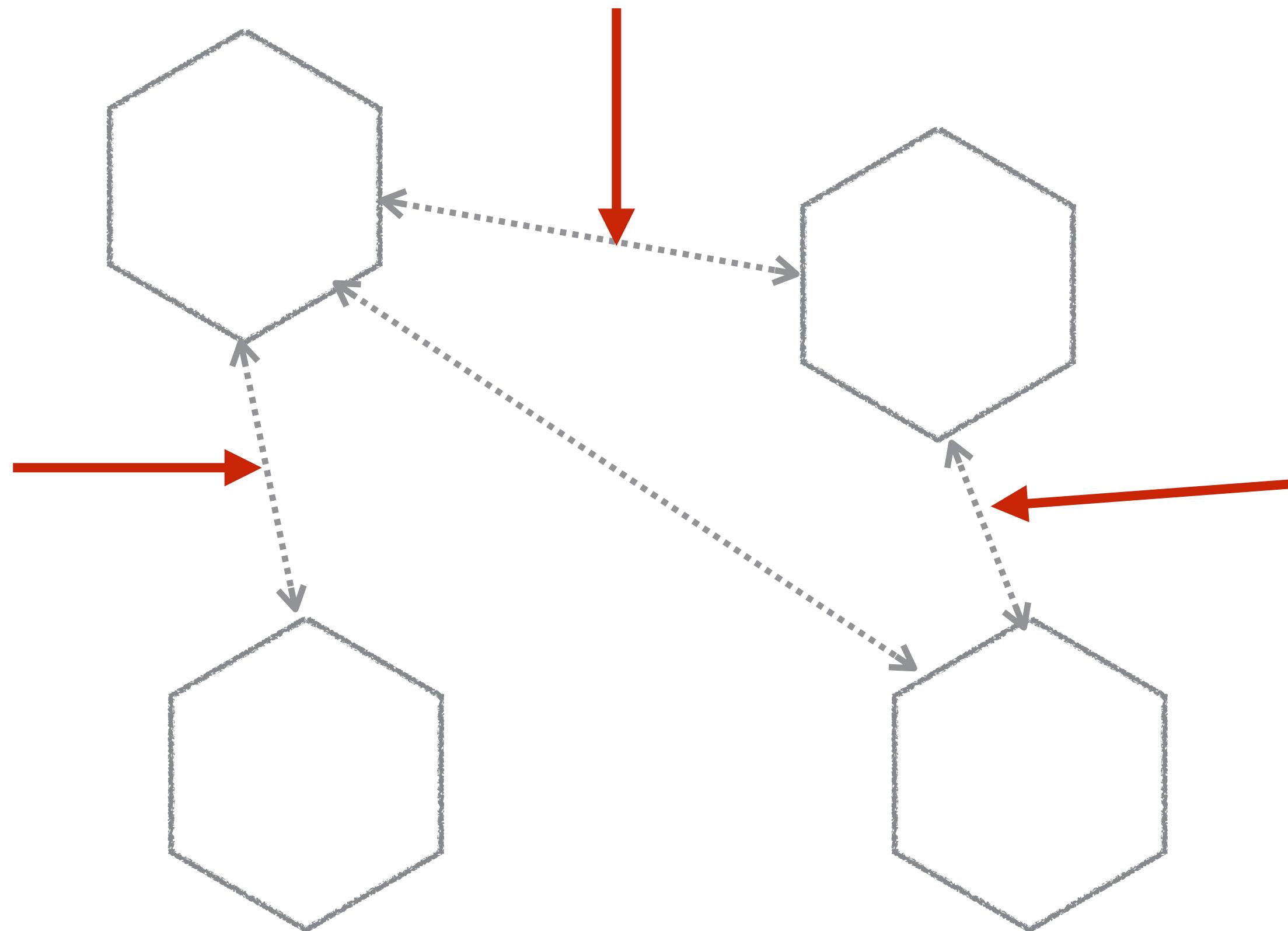
This is a living document and we are working to expand it in key areas. It includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party. The Working Party includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative.

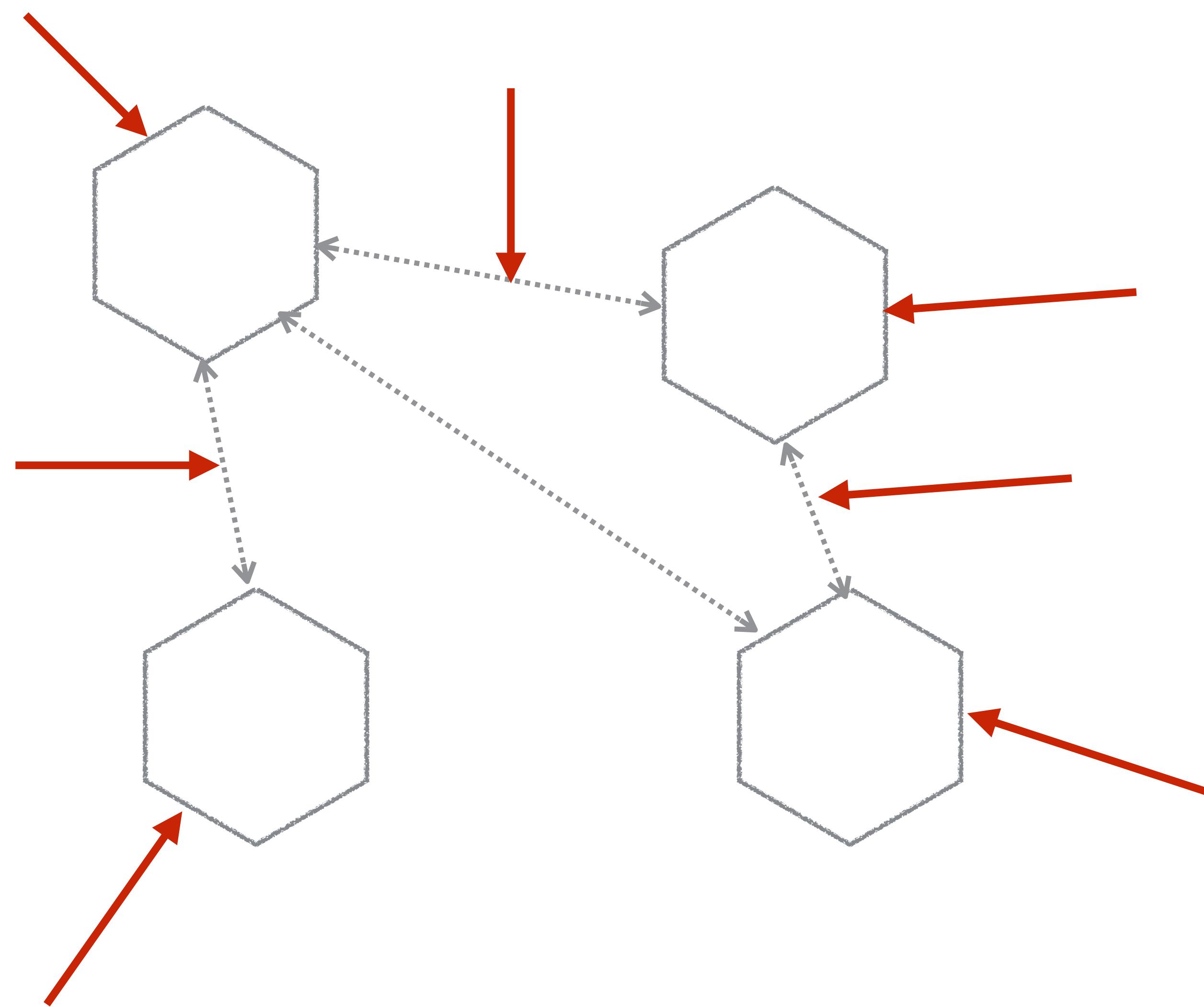
Alongside the Guide to the GDPR, we have produced a number of tools to help organisations to prepare for the GDPR:

 GDPR: 12 steps to take now









The Basics

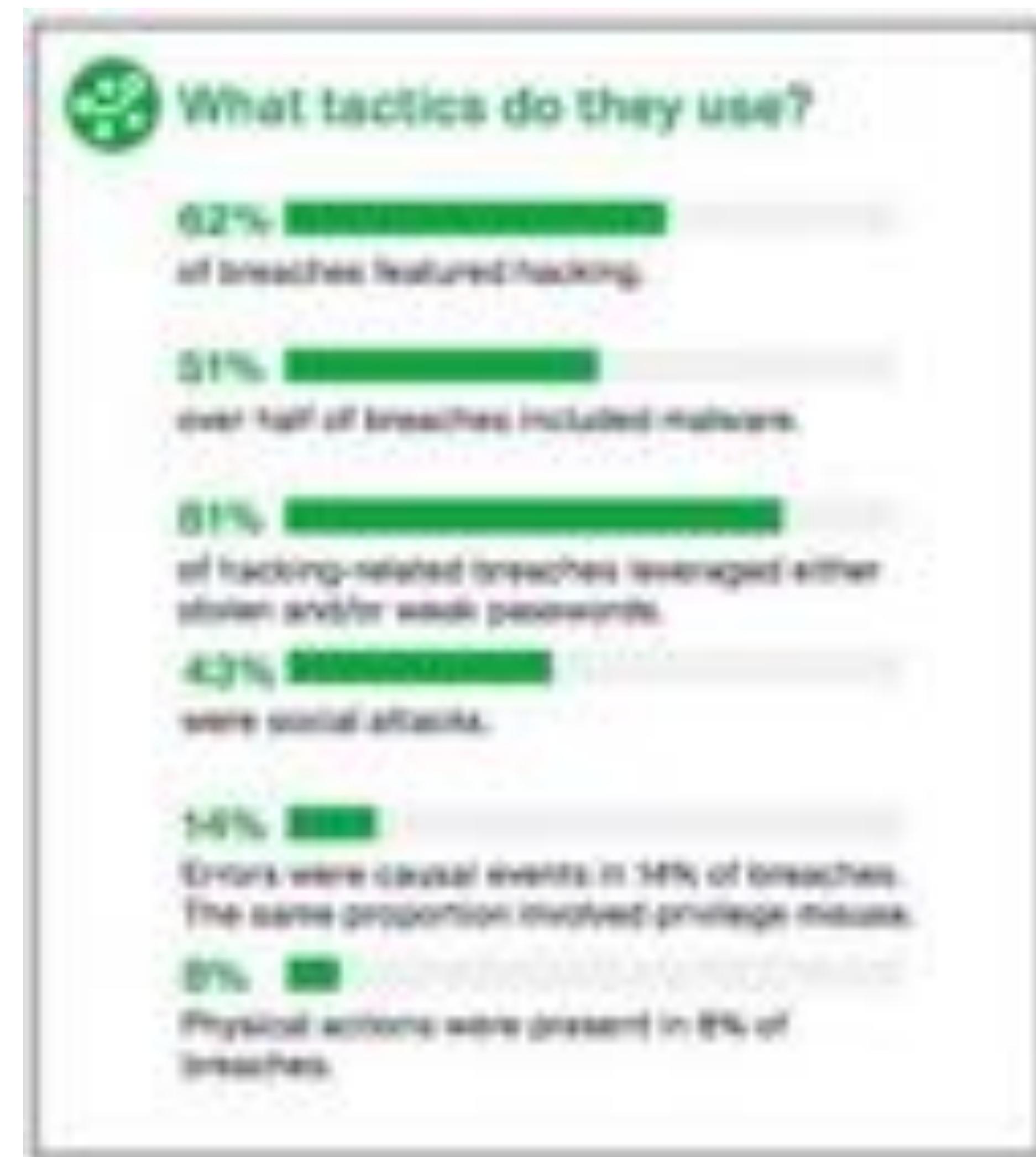
Who here thinks they can assess risks?



http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

@samnewman

HOW DO BREACHES OCCUR?



<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

HOW DO BREACHES OCCUR?



<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

BETTER PASSWORD RULES?

The screenshot shows a presentation slide with the following details:

- Title:** Passwords Evolved: Authentication Guidance for the Modern Era
- Author:** Troy Hunt
- Date:** 2018-01-10
- Content Summary:** In the beginning, things were simple: you had two strong (a password and a pincode) and if someone knew both of them, they could log in. But the ecosystems on which they were used were simple too, for example in 1971. The Xerox Alto was considered to be the first computer system to use passwords.

<https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/>

BETTER PASSWORD RULES?

Passwords Evolved: Authentication Guidance for the Modern Era

In the beginning, things were simple: you had two strong (a password and a passphrase) and if someone knew both of them, they could log in. Easy.

But the ecosystems on which they were used was simple too, for example in 1971. The Xerox Alto was considered to be the first computer system to use passwords.

Summarises ideas from NIST and the UK's National Cyber Security Centre

<https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/>

BETTER PASSWORD RULES?



Summarises ideas from NIST and the UK's National Cyber Security Centre

Packed with great tips, like...

<https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/>

PASSWORDS EVOLVED

<https://www.troyhunt.com/passwords-evolved-authentication-guidance-for-the-modern-era/>

@samnewman

PASSWORDS EVOLVED

Longer is stronger

PASSWORDS EVOLVED

Longer is stronger

Eliminate complex character composition rules

"Sorry that password won't work, you must include: a symbol, a number, a hiero-glyph, a gang sign, an inspiring quote, a poem that you just wrote, a picture of your favorite animal made using only characters on your keyboard, and an uppercase letter."



Load this
http://tinyurl.com/longpassword

Visit

<https://www.pinterest.dk/pin/566679565591724157/>

PASSWORDS EVOLVED

Longer is stronger

Eliminate complex character composition rules

PASSWORDS EVOLVED

Longer is stronger

Eliminate complex character composition rules

Embrace password managers

PASSWORDS EVOLVED

Longer is stronger

Eliminate complex character composition rules

Embrace password managers

Do not mandate password changes

PASSWORDS EVOLVED

Longer is stronger

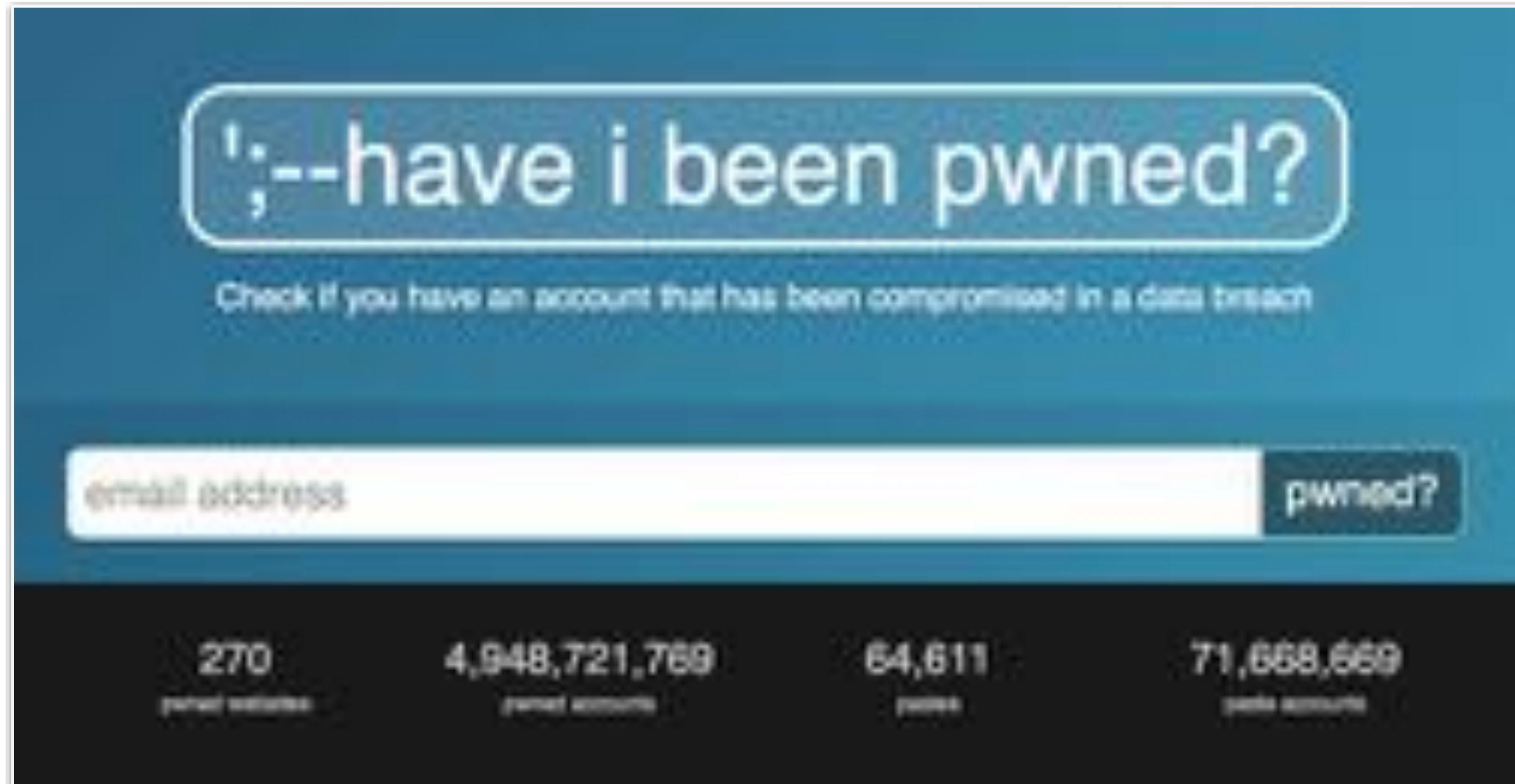
Eliminate complex character composition rules

Embrace password managers

Do not mandate password changes

Block previously breached passwords

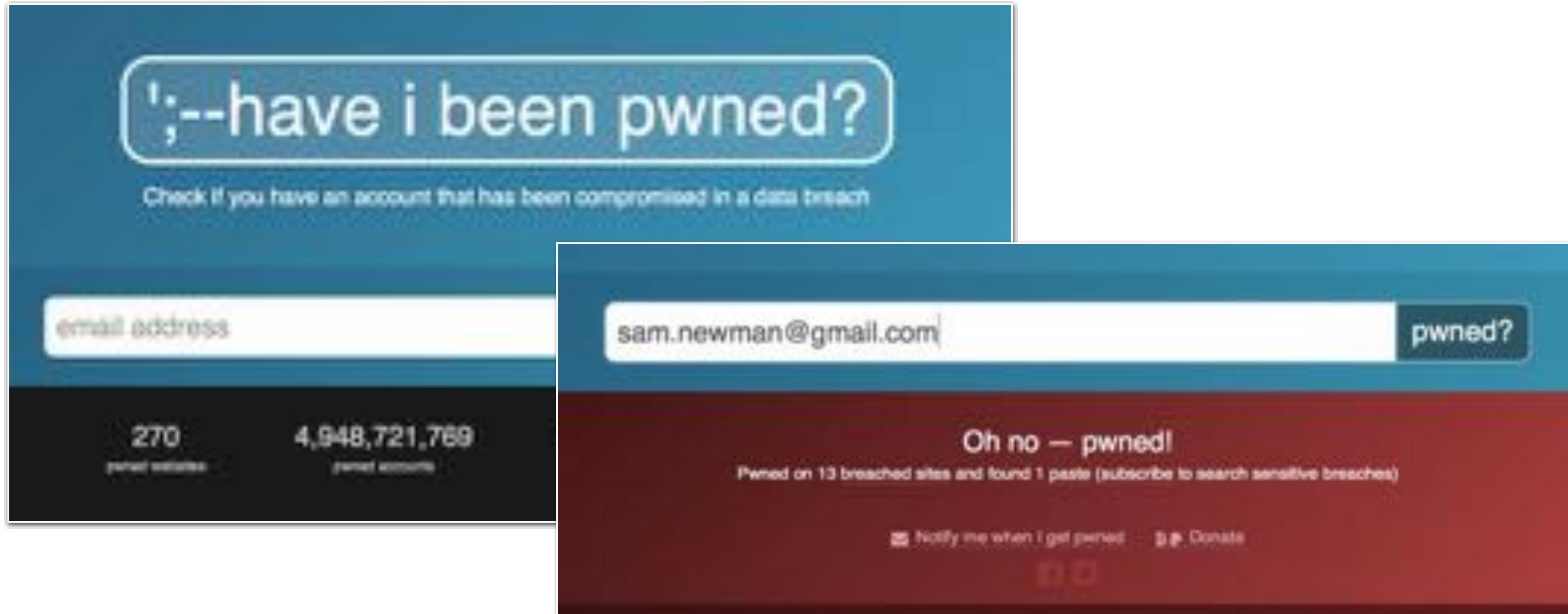
HAVE I BEEN PWNED?



<https://haveibeenpwned.com>

@samnewman

HAVE I BEEN PWNED?



<https://haveibeenpwned.com>

@samnewman

CHECK FOR BREACHED PASSWORDS!

Downloading the Pwned Passwords list

The entire list of password(s) is downloadable for free (along with each password being represented as a SHA-1 hash to protect the original value (some passwords contain personally identifiable information)) followed by a count of how many times that password had been used in the various data breaches. The list may be integrated into other systems and used to verify whether a password has previously appeared in a data breach prior which a system may warn the user or even block the password outright. For suggestions on integration practices, read the Pwned Passwords launch blog post for more information.

Please download the data via the "Normal" link if possible! If you can't access links (for example, they're blocked by a corporate firewall), use the "CloudFlare" link and they'll kindly cover the bandwidth cost.

File	Date	Size	Description	SHA-1 hash of 7-Digit File
Normal CloudFlare	20-Feb-2018	8.00GB	Version 2 (sorted by prevalence)	02B1743244F020A0D90A9D4C77E8A1400007d000

<https://haveibeenpwned.com>

@samnewman

CHECK FOR BREACHED PASSWORDS!

Finding Pwned Passwords with 1Password

February 22, 2018 | 08:45am by [Sam Newman](#) | 0 comments

Yesterday, Troy Hunt announced [Pwned Passwords](#), a new service that allows you to check if your passwords have been leaked on the Internet. His database now has more than 500 million passwords collected from various breaches. Checking your own passwords against this list is extremely valuable.

We loved Troy's free service so much that we decided to try it out ourselves & decided that integrating it with 1Password. Here's how it looks:



<https://blog.agilebits.com/2018/02/22/finding-pwned-passwords-with-1password/>

THE THREE R'S

A screenshot of a Medium article card. At the top left is a circular profile picture of a man in a suit. To the right of the picture, the author's name "Justin Smith" is displayed in black text, followed by a blue "Follow" button with white text. Below the author's name is the title "Identity and Security Geek". Underneath that is the date "Apr 19" and the text "7 min read". The main title of the article, "The Three R's of Enterprise Security: Rotate, Repave, and Repair", is centered below the author information in a large, bold, black font.

<https://medium.com/built-to-adapt/the-three-r-s-of-enterprise-security-rotate-repave-and-repair-f64f6d6ba29d>

THE ADVANCED PERSISTENT THREAT

“At or near the top of security concerns in the datacenter is something called an Advanced Persistent Threat (APT). An APT gains unauthorized access to a network and can stay hidden for a long period of time. Its goal is usually to steal, corrupt, or ransom data.”

- Justin Smith, Pivotal



TARGET



In the summer of 2015, Dutch intelligence services were the first to alert their American counterparts about the cyberattack of the Democratic National Committee by 'Cozy Bear', a hacking group believed to be tied to the Russian government. Intelligence hackers from Dutch AIVD (General Intelligence and Security Service) had penetrated the Cozy Bear computer servers as well as a security camera at the entrance of their working space, located in a university building adjacent to the Red Square in Moscow.

Over the course of a few months, they saw how the Russians penetrated several U.S. institutions, including the State Department, the White House, and the DNC. On all these occasions, the Dutch alerted the U.S. intelligence services, Dutch *ti programe Maatschappij en de volkstaat*, a prominent newspaper in The Netherlands, partly report on Thursday. This account is based on interviews with a dozen political, diplomatic and intelligence sources in The Netherlands and the U.S., with direct knowledge of the matter. None of them wanted to speak on the record, given the classified details of the matter.

<https://nos.nl/nieuwsuur/artikel/2213767-dutch-intelligence-first-to-alert-u-s-about-russian-hack-of-democratic-party.html>

@samnewman

Rotate: Short-lived Credentials

Rotate: Short-lived Credentials

Repair: Patch Your Stuff

Rotate: Short-lived Credentials

Repair: Patch Your Stuff

Repave: Burn It Down!

Rotate: Short-lived Credentials

Repair: Patch Your Stuff

Repave: Burn It Down!

CODESPACES R.I.P.

Data Center > Cloud

Code Spaces goes titsup FOREVER after attacker NUKES its Amazon-hosted data

Source-sharing site to close following total cloudpocalypse



18 Jun 2014 at 20:54. Neil McAllister

54T

http://www.theregister.co.uk/2014/06/18/code_spaces_destroyed/

CHECK FOR LEAKED CREDENTIALS

10| README.md

Gitrob: Putting the Open Source in OSINT

Gitrob is a command line tool which can help organizations and security professionals find sensitive information lingering in publicly available files on GitHub. The tool will iterate over all public organization and member repositories and match filenames against a range of patterns for files that typically contain sensitive or dangerous information.

Looking for sensitive information in GitHub repositories is not a new thing, it has been known for a while that things such as private keys and credentials can be found with GitHub's search functionality, however Gitrob makes it easier to focus the effort on a specific organization.

<https://github.com/michenriksen/gitrob>

@samnewman

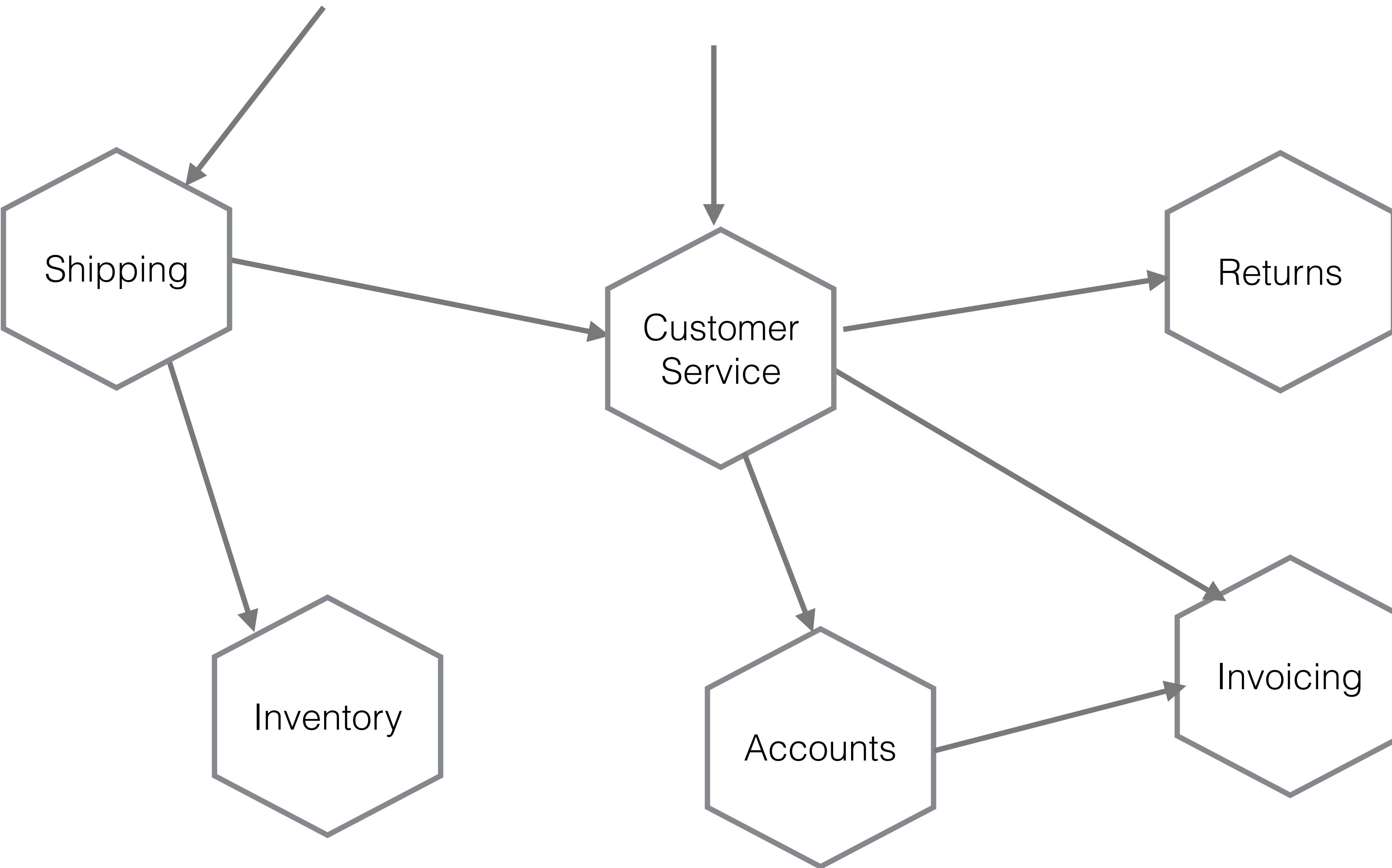
Revocation & Rotation Of Credentials

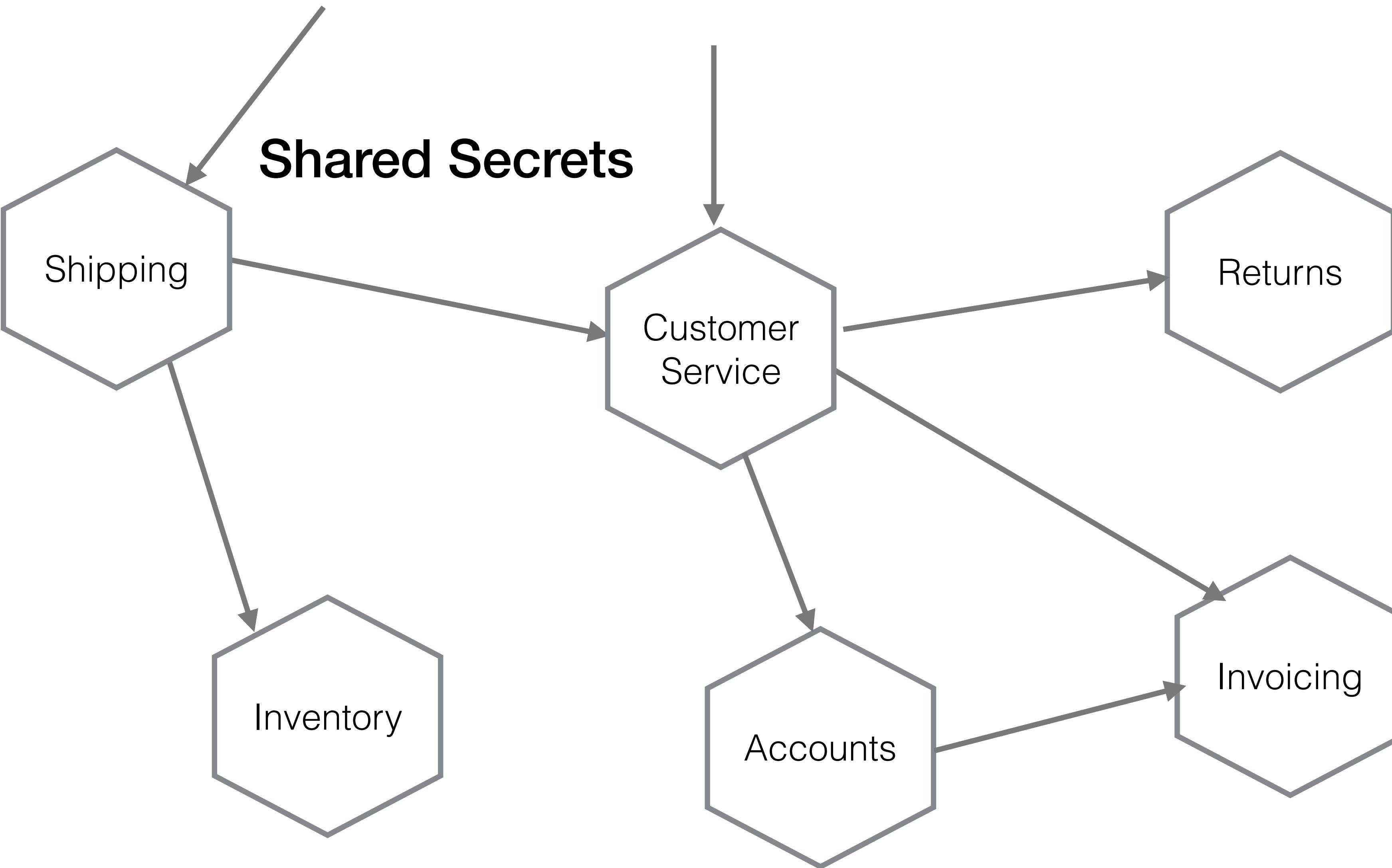
+

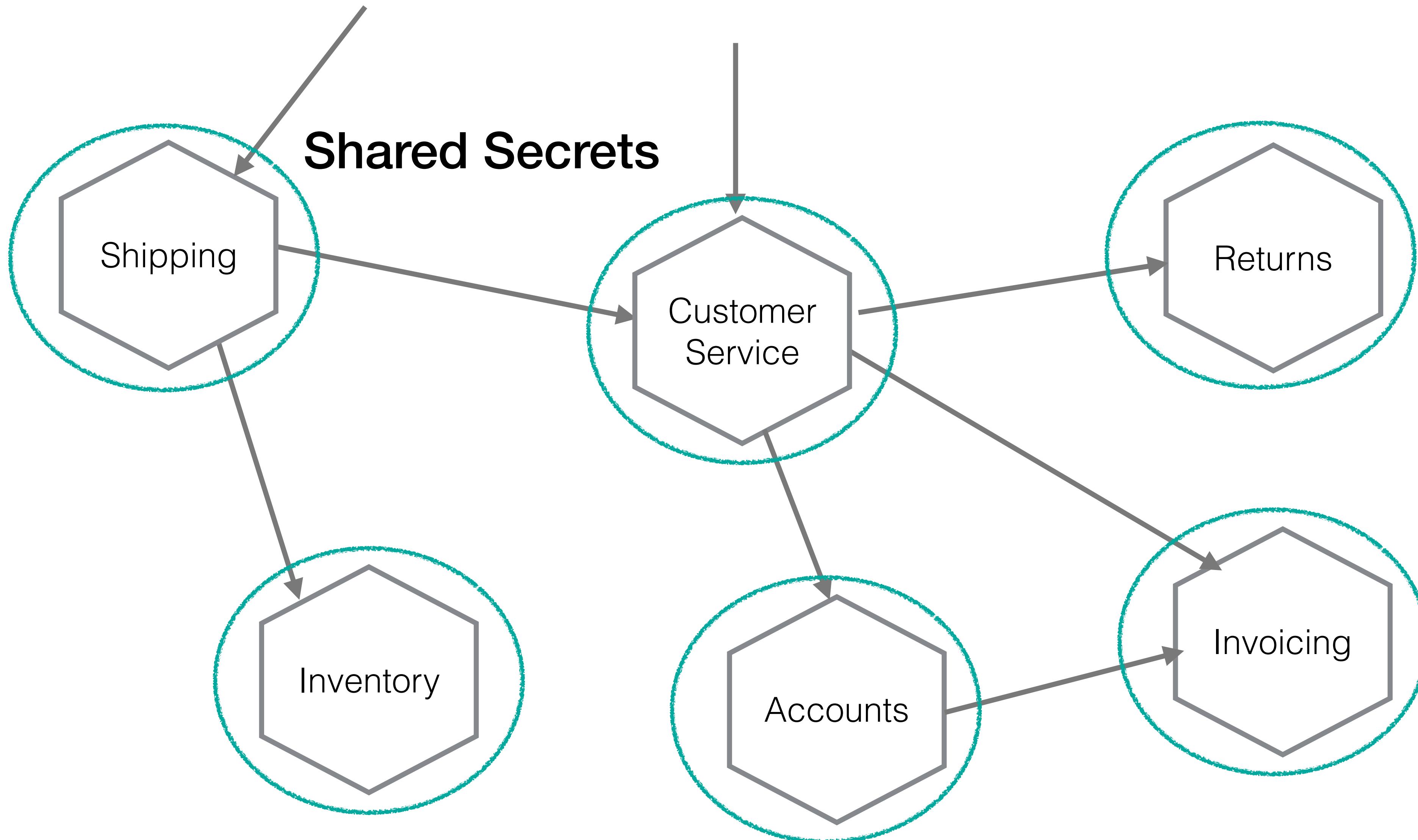
Microservices

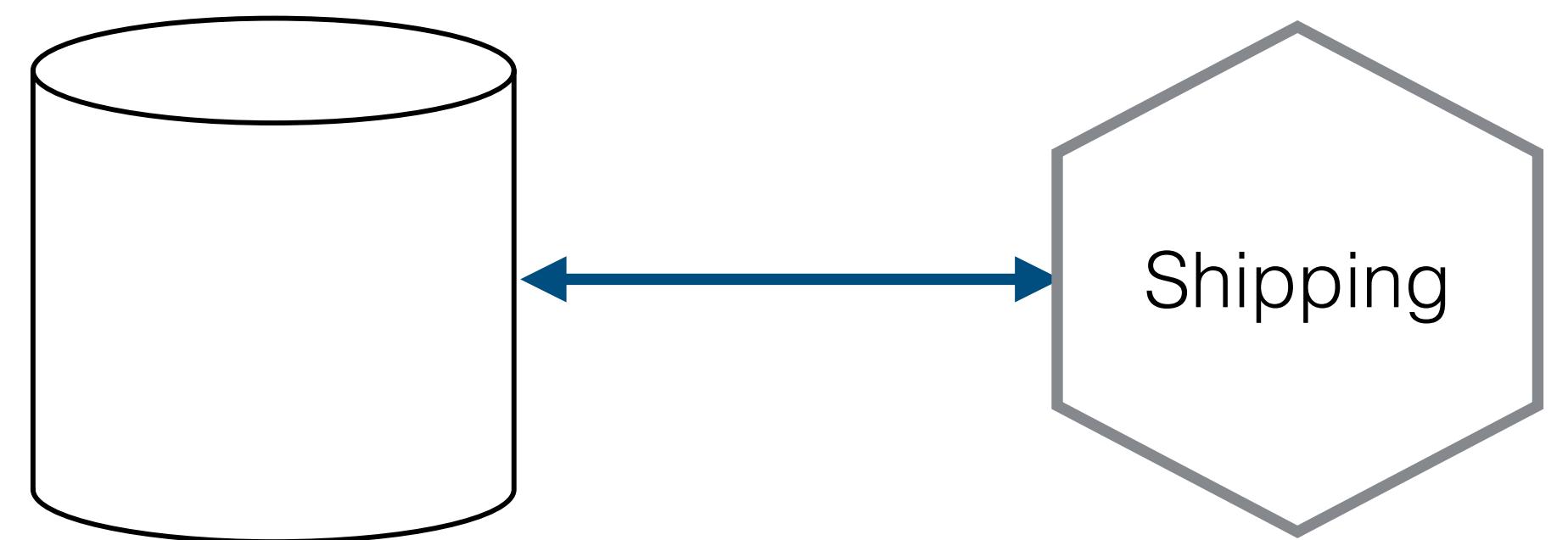
=

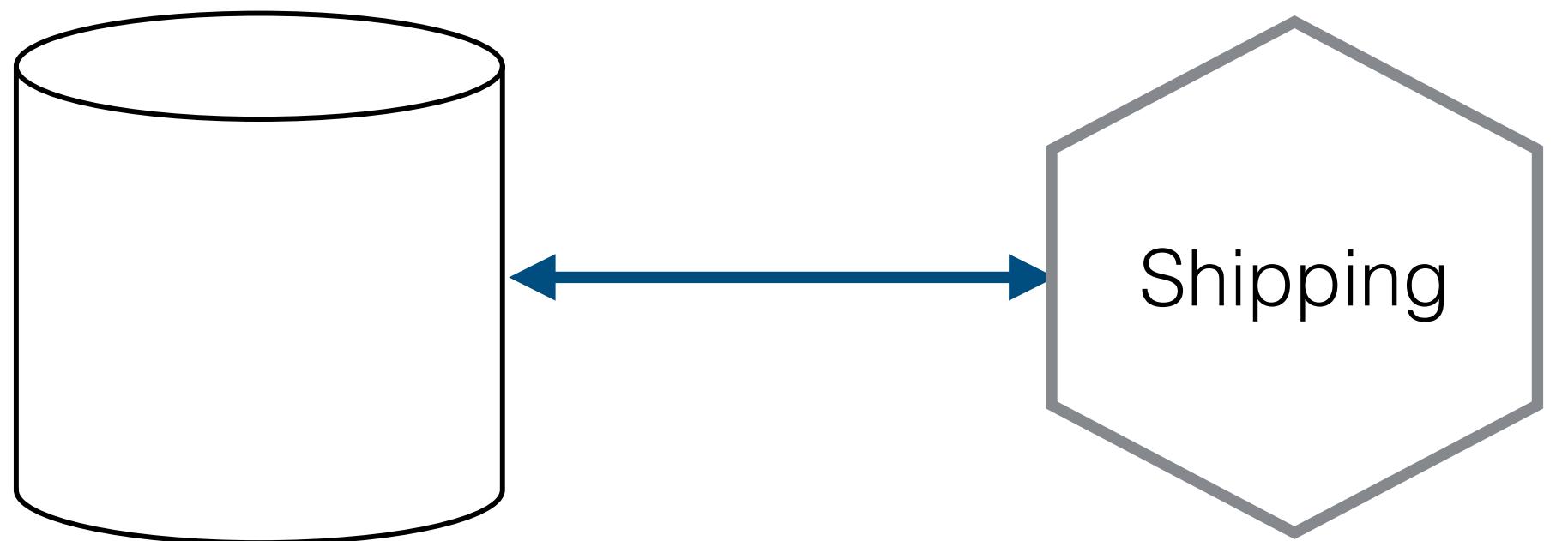
Pain???



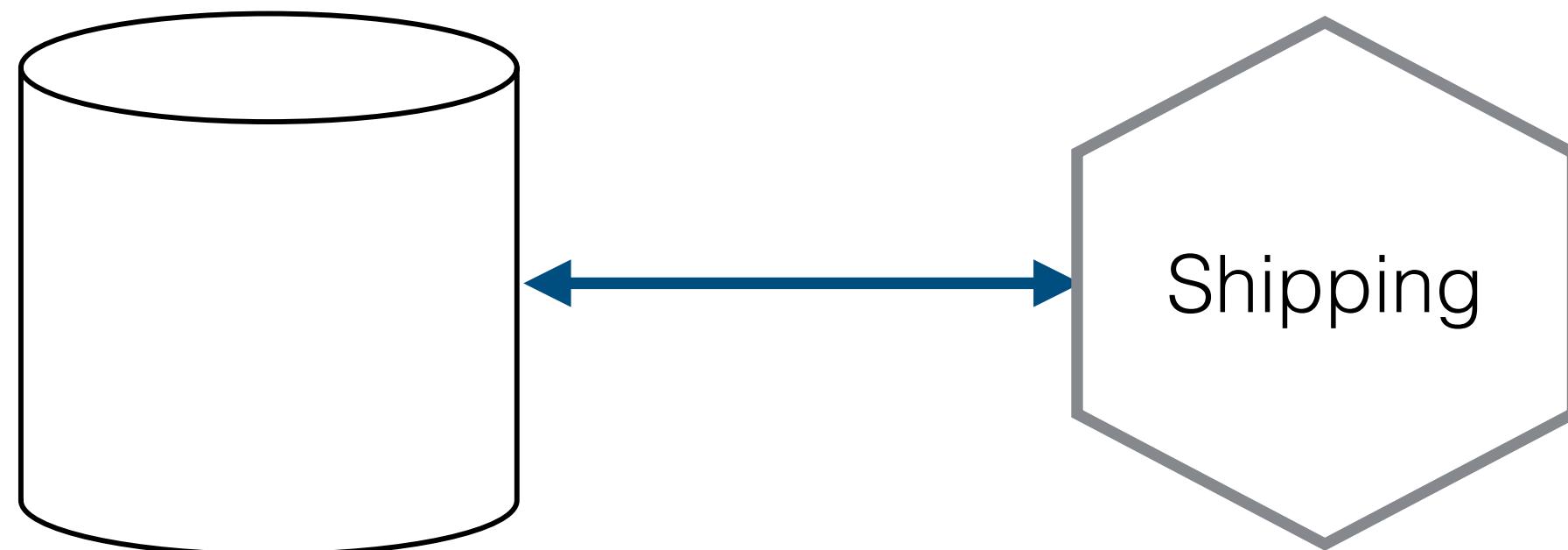






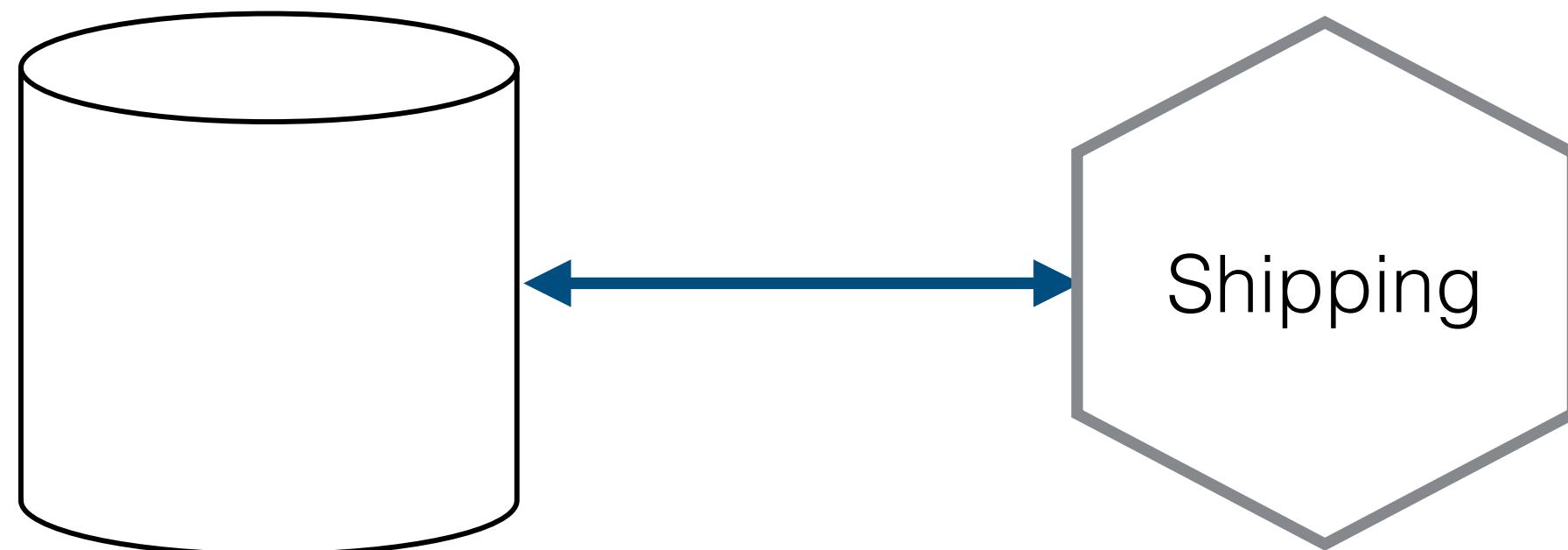


Auth Credentials



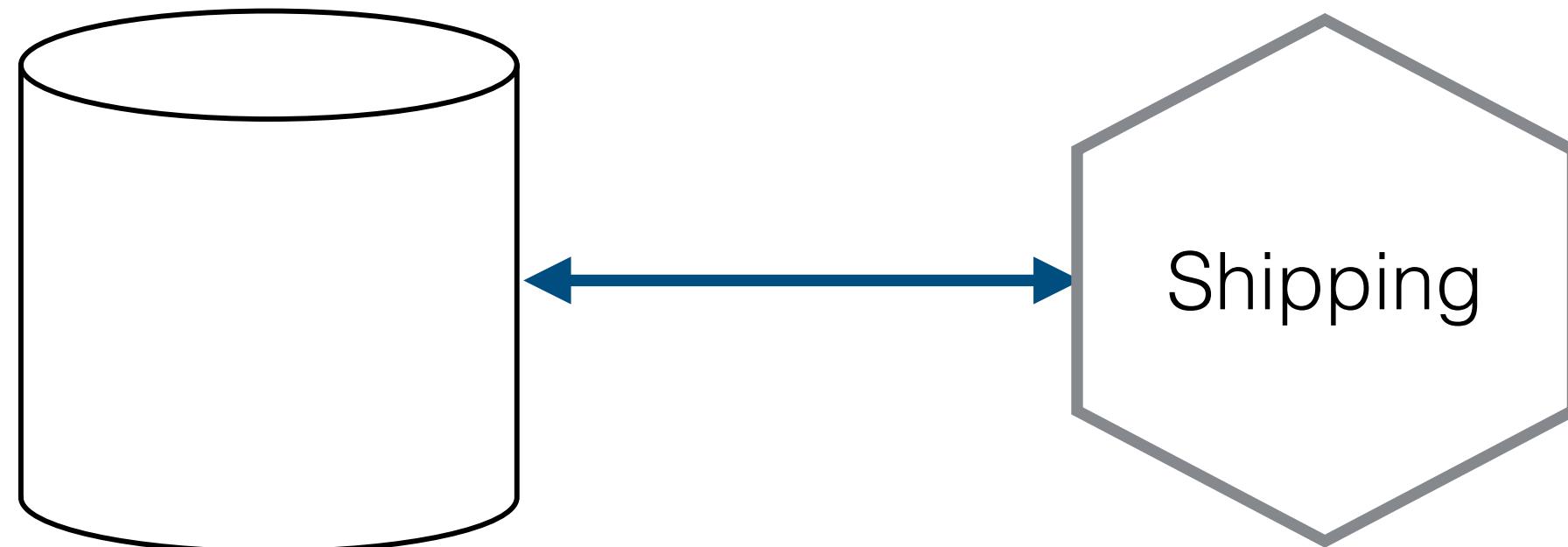
Auth Credentials

```
DB_USERNAME = admin  
DB_PASSWORD = 123ask48321
```



Auth Credentials

```
DB_USERNAME = admin  
DB_PASSWORD = 123ask48321
```

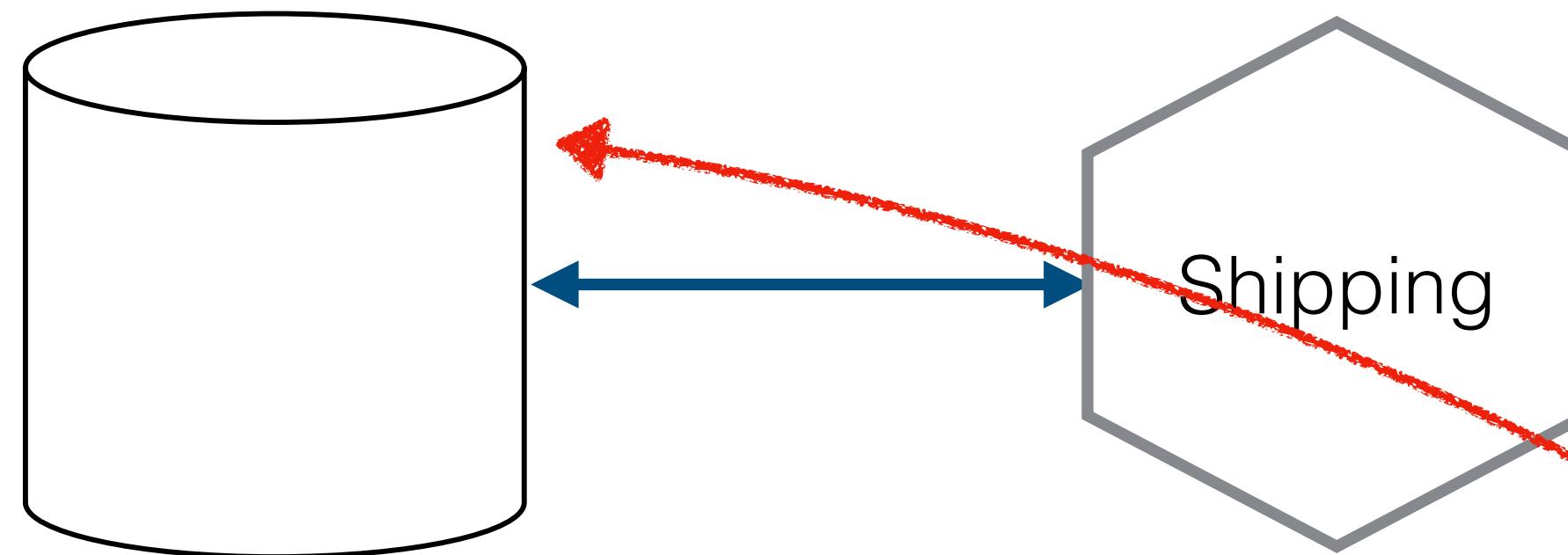


Shipping

Auth Credentials

```
DB_USERNAME = admin  
DB_PASSWORD = 123ask48321
```

Leaving credentials in the open can be bad...



Auth Credentials

```
DB_USERNAME = admin  
DB_PASSWORD = 123ask48321
```

Leaving credentials in the open can be bad...

Secret stores!

V AULT

A tool for managing secrets.

Get Started

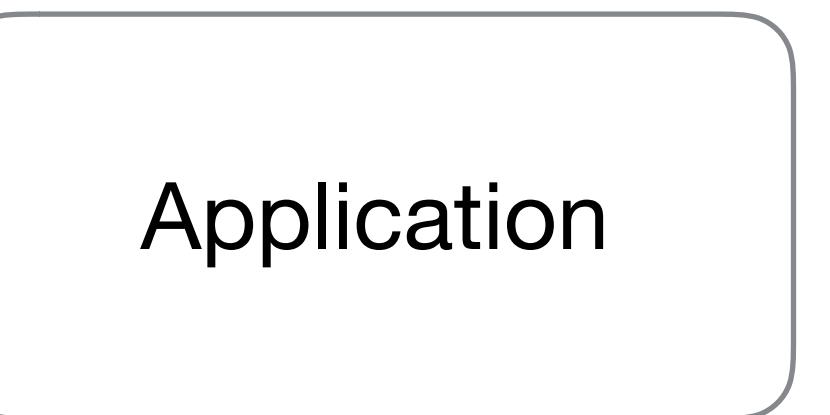
Launch Interactive Tutorial



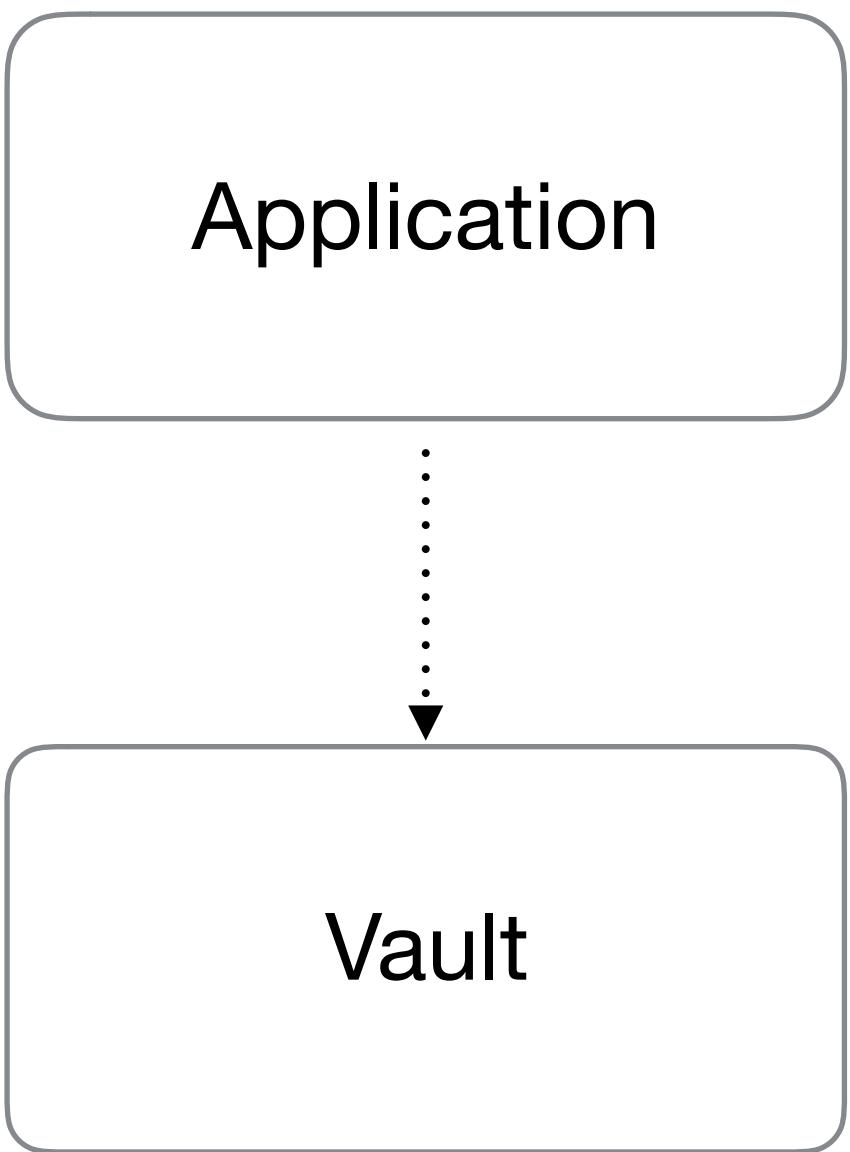


AWS Key Management Service
(KMS)

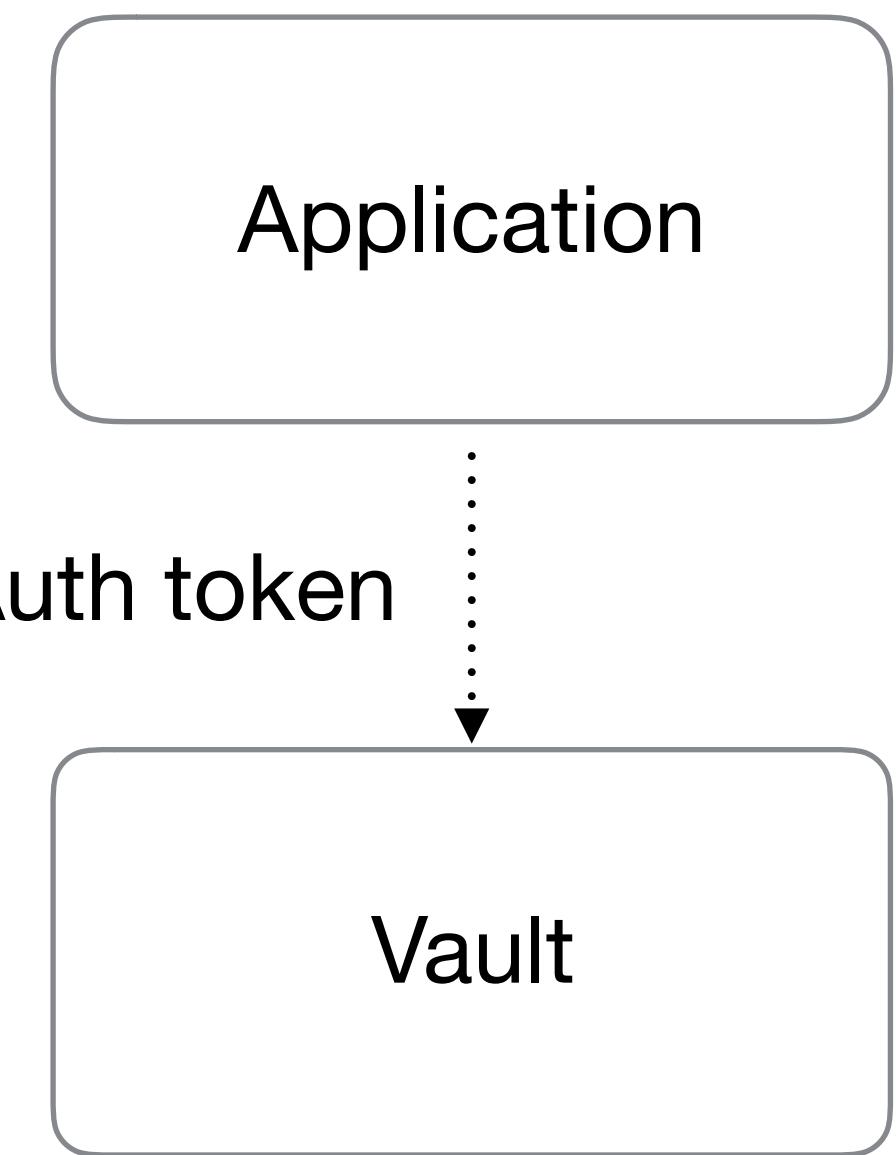
VAULT HIGH LEVEL OVERVIEW



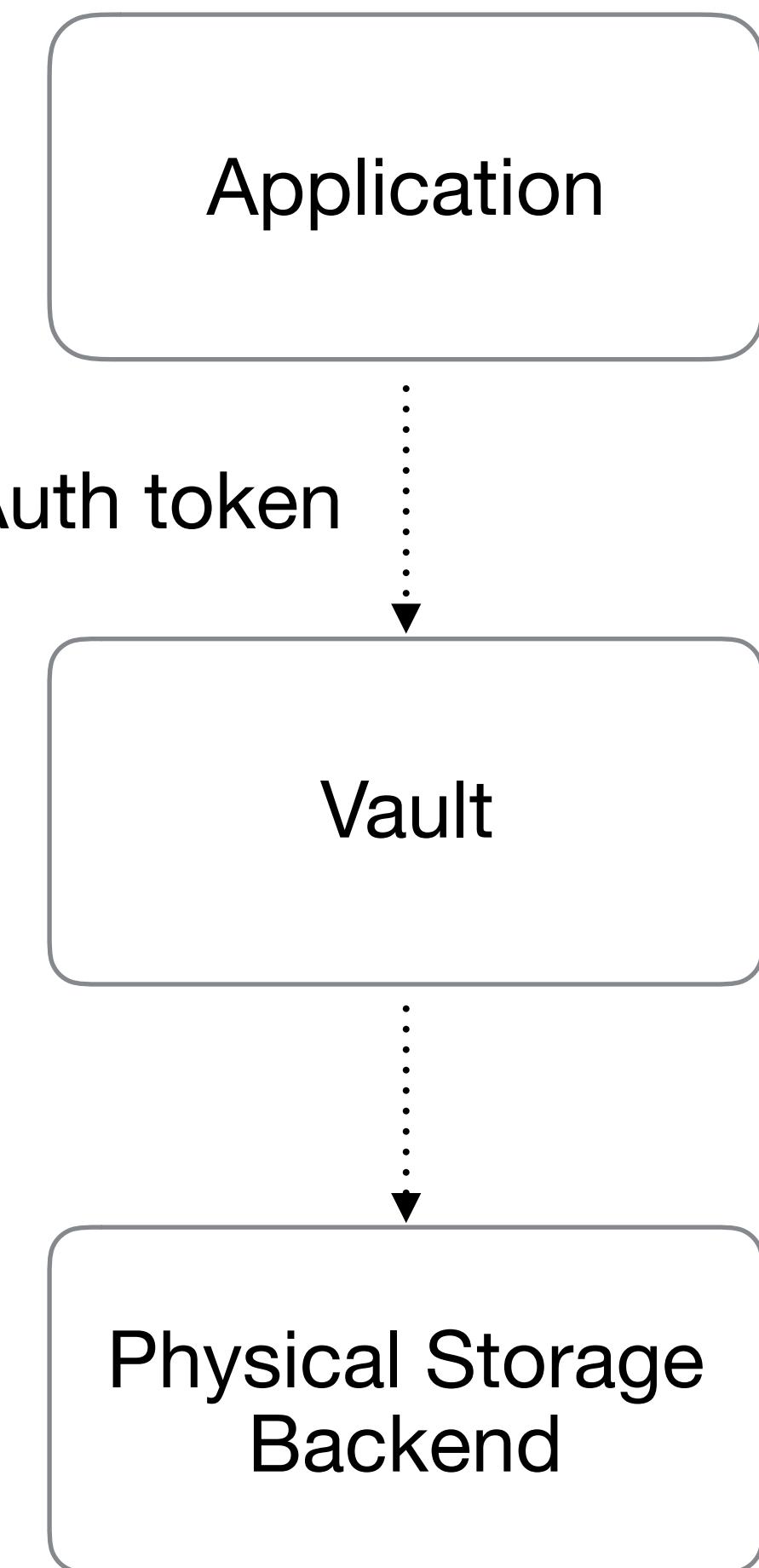
VAULT HIGH LEVEL OVERVIEW



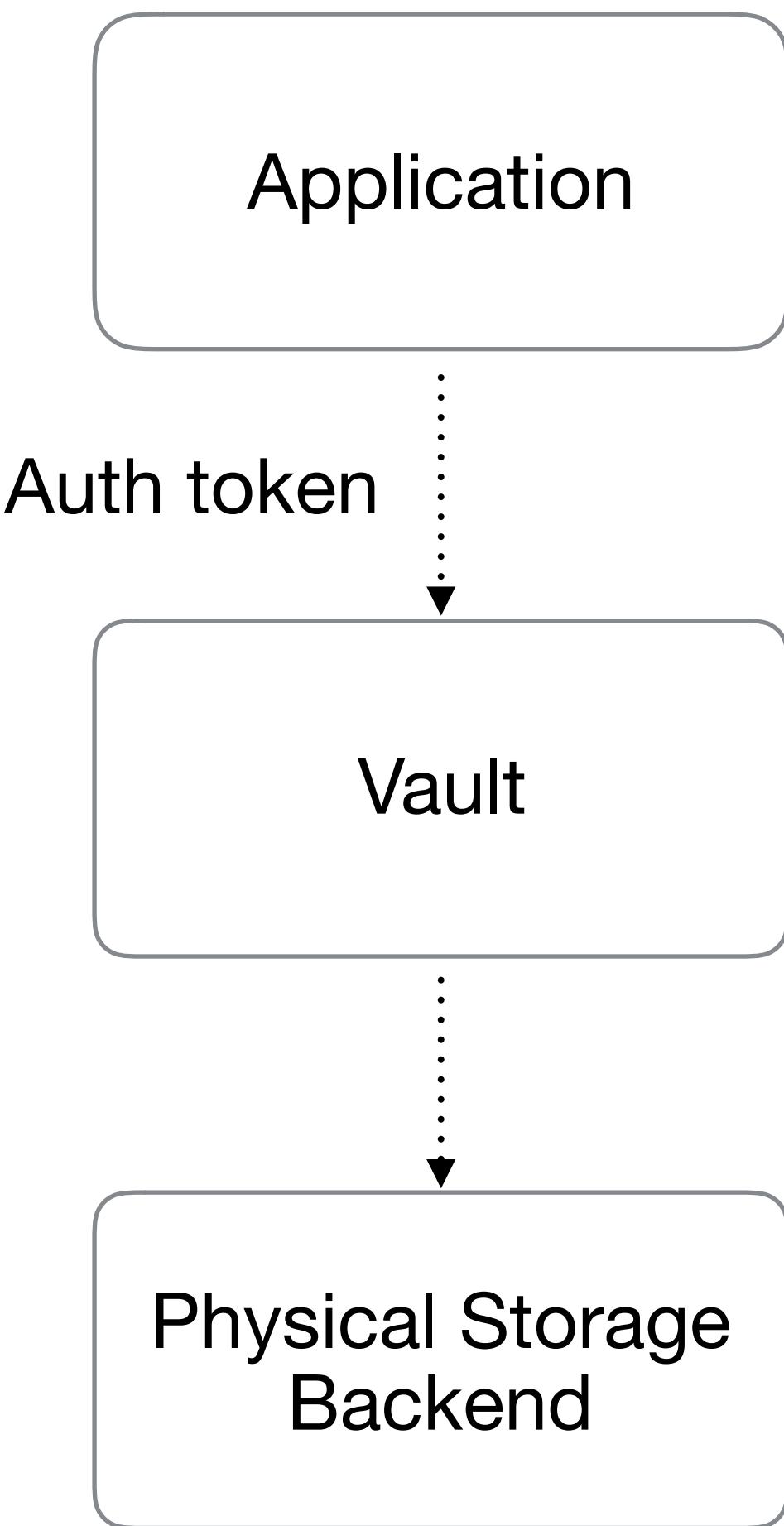
VAULT HIGH LEVEL OVERVIEW



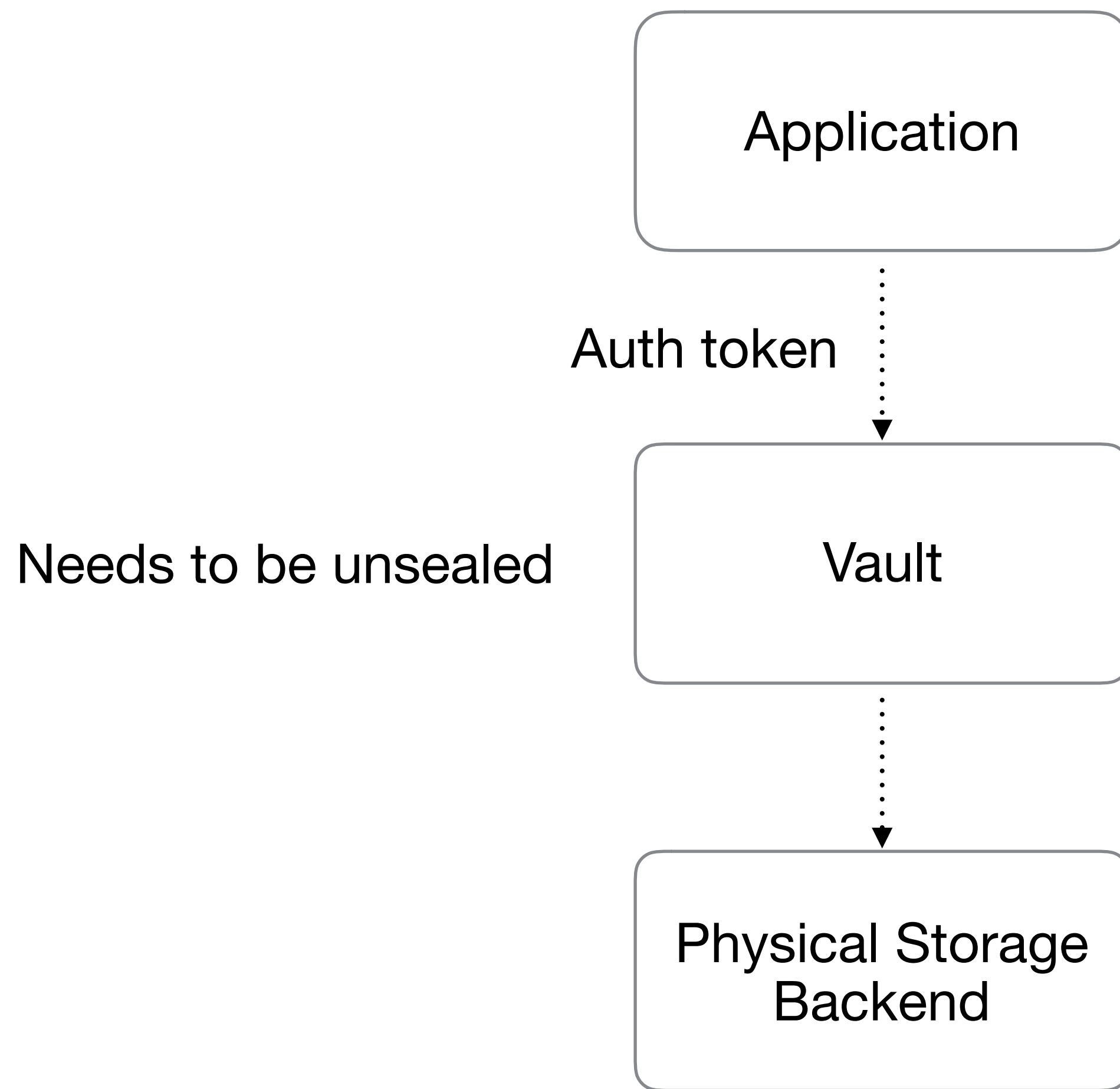
VAULT HIGH LEVEL OVERVIEW



VAULT HIGH LEVEL OVERVIEW



VAULT HIGH LEVEL OVERVIEW



WHO HAS THE KEY?



<https://www.flickr.com/photos/quinnanya/2585541255/>

DON'T HAVE ONE KEY!



Vault



<https://www.flickr.com/photos/quinnanya/2585541255/>

@samnewman

DON'T HAVE ONE KEY!



Vault



Shamir's Secret Sharing

From Wikipedia, the free encyclopedia



This article may be too technical for most readers to understand.
Please help improve it to make it understandable to non-experts,
without removing the technical details. (March 2014) (Learn how and
when to remove this template message)

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

<https://www.flickr.com/photos/quinnanya/2585541255/>

@samnewman

DON'T HAVE ONE KEY!



Vault

Shamir's Secret Sharing

From Wikipedia, the free encyclopedia



This article may be too technical for most readers to understand.
Please help improve it to make it understandable to non-experts,
without removing the technical details. (March 2014) (Learn how and
when to remove this template message)

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

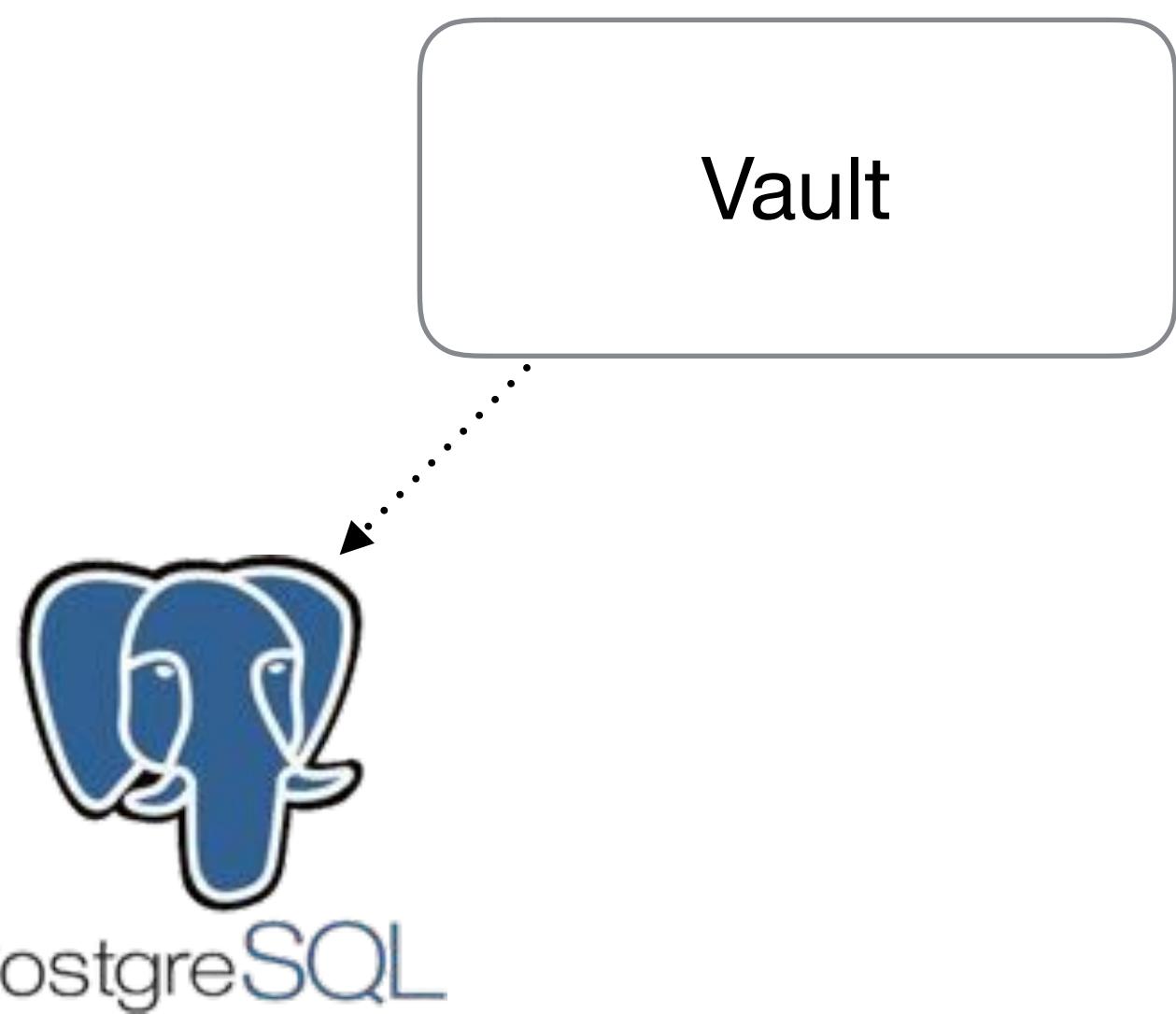
<https://www.flickr.com/photos/quinnanya/2585541255/>

@samnewman

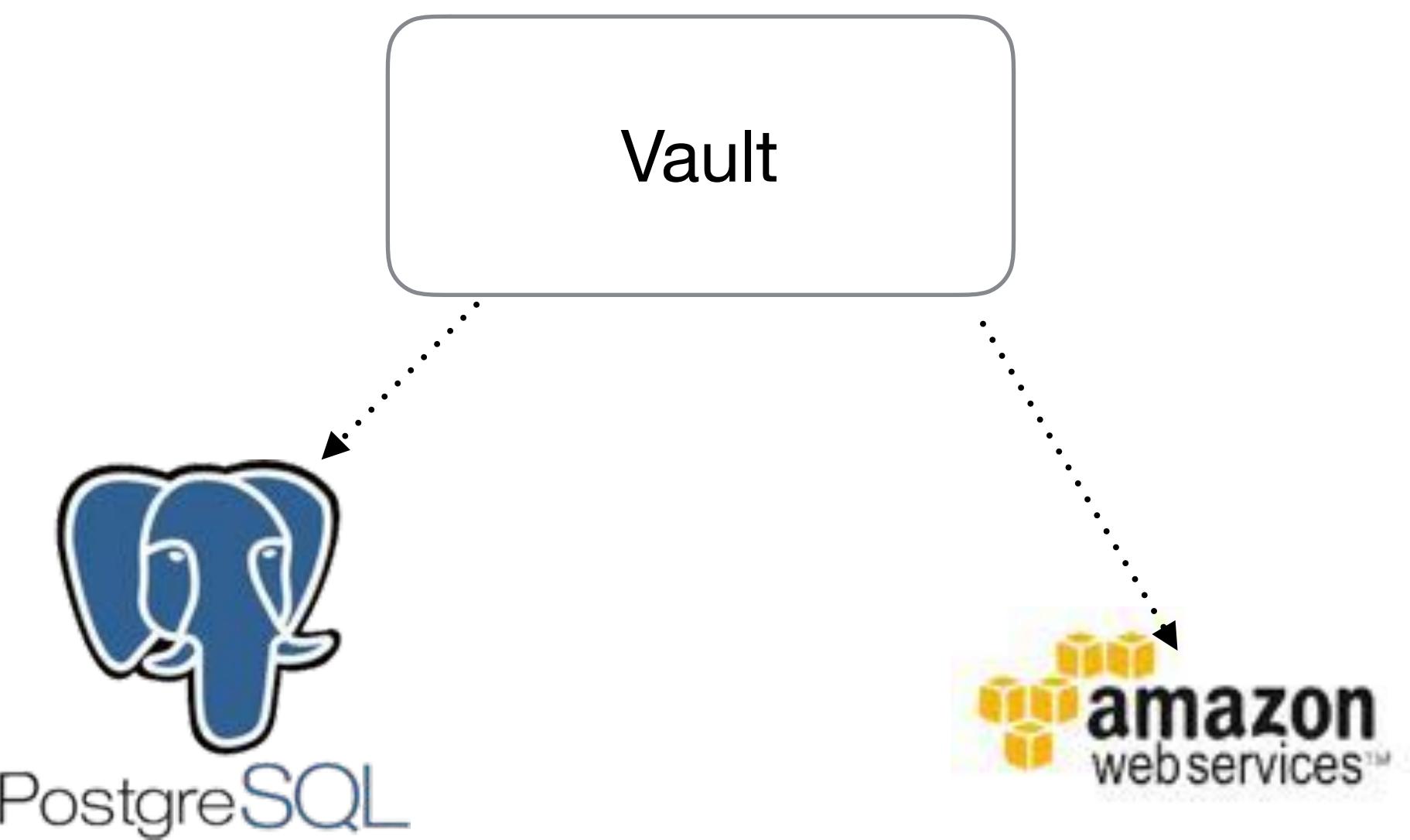
TIME-LIMITED CREDENTIALS

Vault

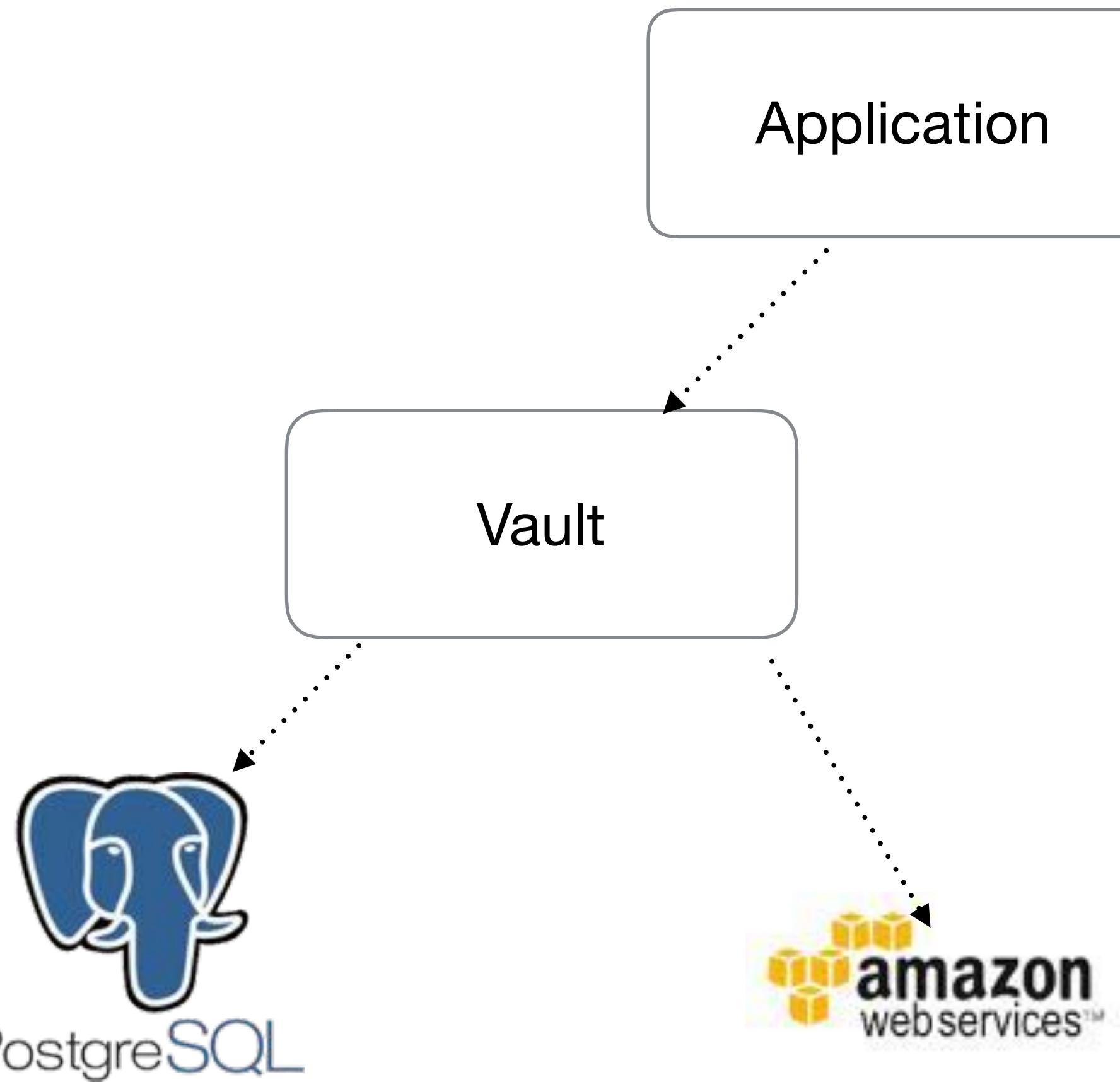
TIME-LIMITED CREDENTIALS



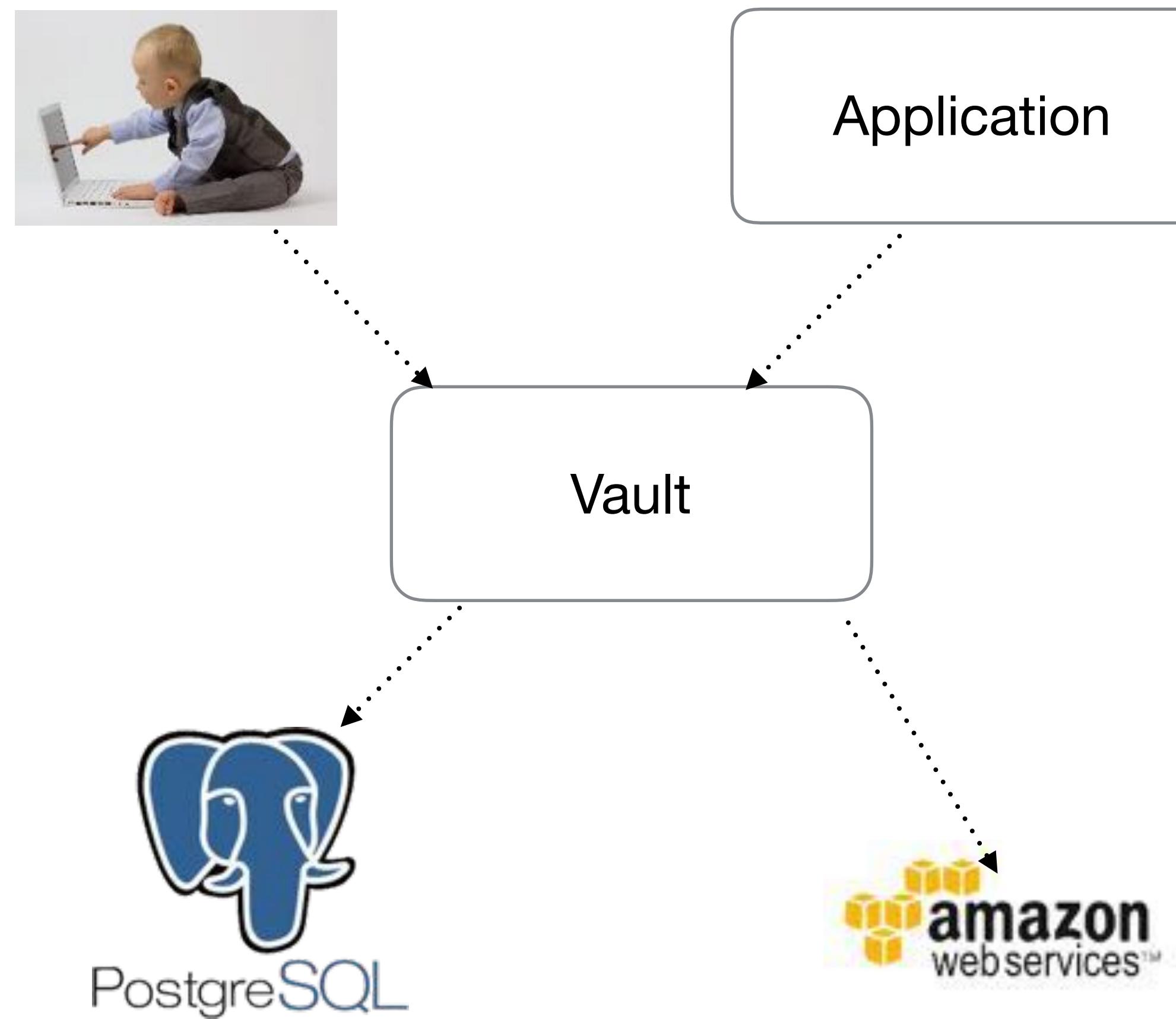
TIME-LIMITED CREDENTIALS



TIME-LIMITED CREDENTIALS



TIME-LIMITED CREDENTIALS



AWESOMENESS



CONSUL
TEMPLATE

<https://github.com/hashicorp/consul-template>

AWESOMENESS



CONSUL
TEMPLATE

<https://github.com/hashicorp/consul-template>

```
adapter: postgresql
host: {{key "my-app/production/host"}}
username: {{$secret.Data.username}}
password: {{$secret.Data.password}}
{{end}}
```

From: <https://www.hashicorp.com/blog/using-vault-with-consul-template>

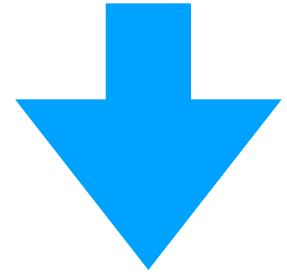
AWESOMENESS



CONSUL
TEMPLATE

<https://github.com/hashicorp/consul-template>

```
adapter: postgresql
host: {{key "my-app/production/host"}}
username: {{$secret.Data.username}}
password: {{$secret.Data.password}}
{{end}}
```



From: <https://www.hashicorp.com/blog/using-vault-with-consul-template>

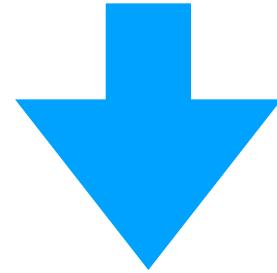
AWESOMENESS



CONSUL
TEMPLATE

<https://github.com/hashicorp/consul-template>

```
adapter: postgresql
host: {{key "my-app/production/host"}}
username: {{$secret.Data.username}}
password: {{$secret.Data.password}}
{{end}}
```



```
adapter: postgresql
host: db-service-183.corp.com
username: as15593kd235423
password: fklk11492309482
{{end}}
```

From: <https://www.hashicorp.com/blog/using-vault-with-consul-template>

WHAT ELSE CAUSES BREACHES?

“44 percent of security breaches occur after vulnerabilities and solutions have been identified. In other words, the problems could have been avoided if found vulnerabilities had been addressed sooner.”

- Forbes/BMC, 2016

Massive Equifax data breach - what you need to know



By Cullen Moore, Money Reporter
10 Sep 2017, 10:00 AM | Updated 10 Sep 2017



Credit report heavyweight Equifax has warned that up to 400,000 UK consumers may have had their personal details stolen as part of a massive global data breach. Info on exactly who's been affected and what you can do about it is still somewhat sketchy, but here's what we know.

Equifax revealed on 8 September that 143 million consumers in the US could have been affected by the incident, which saw Equifax's access data such as names, address and dates of birth, as well as credit card numbers in a smaller number of cases.

Although its UK business – Equifax UK – runs fairly systems in this country are not affected, it admits a file which was stored in the US and contained more limited personal information on up to 400,000 UK consumers may have been accessed.

MSE Guides

[Credit Scores](#)
Find myths & mistakes your bank

[10+ Ways to Stop Scams](#)
As scammers get clever, we've got to be

[Check your credit report for free](#)
Get your free and check your score, or even get Equifax to fix it



Get Our Free Money Tip Email!
For all the latest deals, guides and
inspiration, join the 12m who get it.
Don't miss out!

Enter your email

Get it

www.moneysavingexpert.com

What is Equifax and what data does it have?

Equifax is the second largest credit reference agency in the UK, after Experian.

PATCH MUCH?

Equifax confirms march struts vulnerability behind breach

By Chris Brook for Threat Post|Equifax said the culprit

September 14, 2017, 4:00 pm

behind this summer's massive breach of 143 million Americans was indeed CVE-2017-5638, an Apache Struts vulnerability patched back in March.

The bug was widely assumed by experts to be the "U.S. website application vulnerability" implicated by the company last Thursday, especially after an Apache spokeswoman told Reuters on Friday that it appeared the consumer credit reporting agency hadn't applied patches for flaws discovered earlier this year.

On Wednesday company specified the flaw in a statement posted to its site and stressed it was continuing to work alongside law enforcement to investigate the incident.

<https://www.pinkconnect.com/equifax-confirms-march-struts-vulnerability-behind-breach/>

@samnewman

PATCH MUCH?

Equifax confirms march struts vulnerability behind breach

By Chris Brook for Threat Post|Equifax said the culprit

September 14, 2017, 4:00 pm

behind this summer's massive breach of 143 million Americans was indeed CVE-2017-5638, an Apache Struts vulnerability patched back in March.

The bug was widely assumed by experts to have been the cause of the breach, but Equifax had not yet confirmed it. The company first

implicated the company last Thursday, then confirmed on Friday that it appeared the company had been exploited. The company has since issued patches for flaws discovered earlier this year.

On Wednesday company specified the bug was CVE-2017-5638, an Apache Struts vulnerability that was continuing to work alongside less critical ones.

"Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement."

<https://www.pinkconnect.com/equifax-confirms-march-struts-vulnerability-behind-breach/>

@samnewman

PATCH MUCH?

Equifax confirms march struts vulnerability behind breach

By Chris Brook for Threat Post Equifax said the culprit

September 14, 2017, 4:00 pm

behind this summer's massive breach of 143 million Americans was indeed CVE-2017-5638, an Apache Struts vulnerability patched back in March.

The bug was widely assumed by experts to have been the cause of the breach, but it was only last week that Equifax confirmed the bug was indeed the culprit. The company had previously implicated a "third party" in the breach, but now says that the bug was exploited by criminals.

On Wednesday company specified the bug was Apache Struts CVE-2017-5638. We

CVE-2017-5638

"Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement."

<https://www.pinkconnect.com/equifax-confirms-march-struts-vulnerability-behind-breach/>

@samnewman

CVE-2017-5638

Current Description

The Jakarta Mycat parser in Apache Struts 2 2.3.x (before 2.3.32) and 2.5.x (before 2.5.18.1) has incorrect exception handling and error message generation during file upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a %0d%0a string.

Source: MITRE | Last Modified: 09/21/2017 | [View Access Description](#)

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 (CRITICAL)

Vectors: OSGI-LAUNCHER/PEN/WEB/CC/PRIVILEGE-escalation

Impact Score: 6.3

Exploitability Score: 3.9

CVE-2017-5638

Current Description

The Jakarta Multispart parser in Apache Struts 2 2.3.x (before 2.3.32) and 2.5.x (before 2.5.18.1) has incorrect exception handling and error message generation during file upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a %0d%0a string.

Source: MITRE | Last Modified: 09/21/2017 | [More Details](#) | [Report a Problem](#)

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Vector: [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/C:C/I:C/A:C](#) [Legend]

Impact Score: 6.3

Exploitability Score: 3.9

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

CVE-2017-5638

Current Description

The Jakarta Multispart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.18.1 has incorrect exception handling and error message generation during file upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a %0d%0a string.

Source: NIST | Last Modified: 09/21/2017 | [More Information](#)

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Vector: OSGI-LAUNCHER/PERF/WEB/SCALAR/FILE

Impact Score: 6.3

Exploitability Score: 3.9

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

CVE-2017-5638

Current Description

The Jakarta MyFaces parser in Apache Struts 2 2.3.x (before 2.3.32) and 2.5.x (before 2.5.18.1) has incorrect exception handling and error message generation during file upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a %0d%0a string.

Source: NIST | Last Modified: 09/21/2017 | [More Information](#)

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Vectors: OSGI-LAUNCHER/PERMISSION/OSGI-INF/Launcher Legend

Impact Score: 6.3

Exploitability Score: 3.9

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Reported March 2017

CVE-2017-5638

Current Description

The Jakarta MyFaces parser in Apache Struts 2 2.3.x (before 2.3.32) and 2.5.x (before 2.5.10.1) has incorrect exception handling and error message generation during file upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a %0d%0a string.

Source: NIST | Last Modified: 09/22/2017 | [More Details](#) | [Report a Correction](#)

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/C:H/I:H/A:H [Legend]

Impact Score: 6.3

Exploitability Score: 3.9

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score: 10.0 Critical

Reported March 2017

Patched in struts 2.3.32 / 2.5.10.1 on 7th March

EQUIFAX TIMELINE

sources: <https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/>
<https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

@samnewman

EQUIFAX TIMELINE

Equifax breach happened between mid-May and July

sources: <https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/>
<https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

@samnewman

EQUIFAX TIMELINE

Equifax breach happened between mid-May and July

Equifax spotted it on July 29th

sources: <https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/>
<https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

@samnewman

EQUIFAX TIMELINE

Equifax breach happened between mid-May and July

Equifax spotted it on July 29th

Reported on September 7th

sources: <https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/>
<https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

@samnewman

EQUIFAX TIMELINE

Equifax breach happened between mid-May and July

Equifax spotted it on July 29th

Reported on September 7th

At the time the breach was discovered, the patch had been out for at least 2 months, and perhaps as long as 4 months

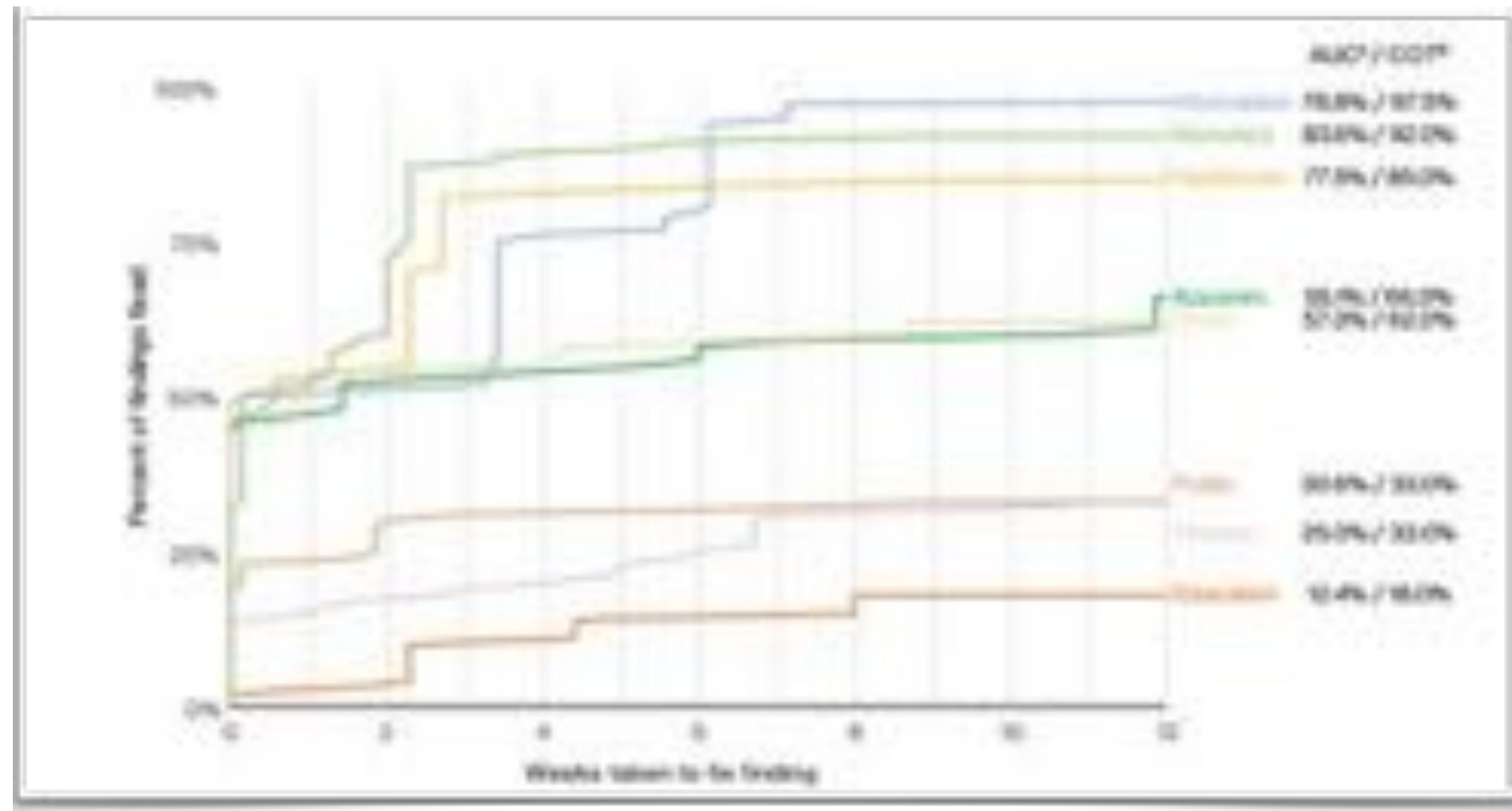
sources: <https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/>
<https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/>

@samnewman

2 to 4 months

**Hands up if you *know* you update your
3rd party libraries for all your code every
2-4 months?**

PATCHING HYGIENE





PATCHING MADNESS!

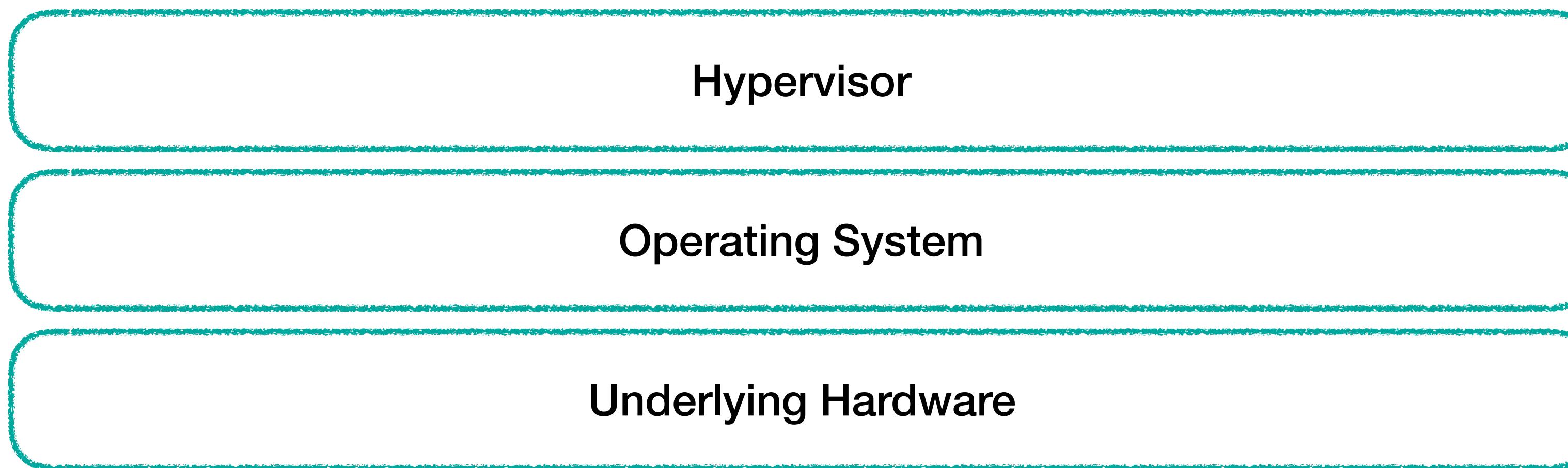
Underlying Hardware

PATCHING MADNESS!

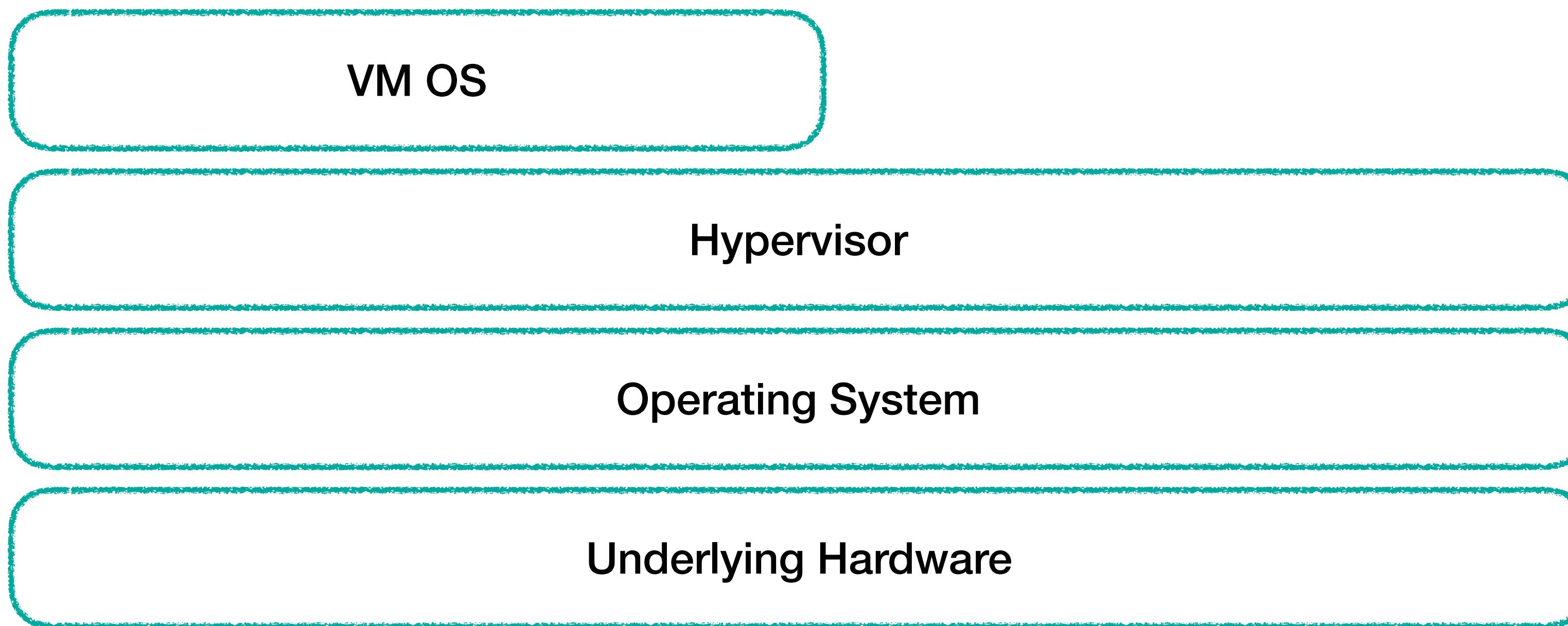
Operating System

Underlying Hardware

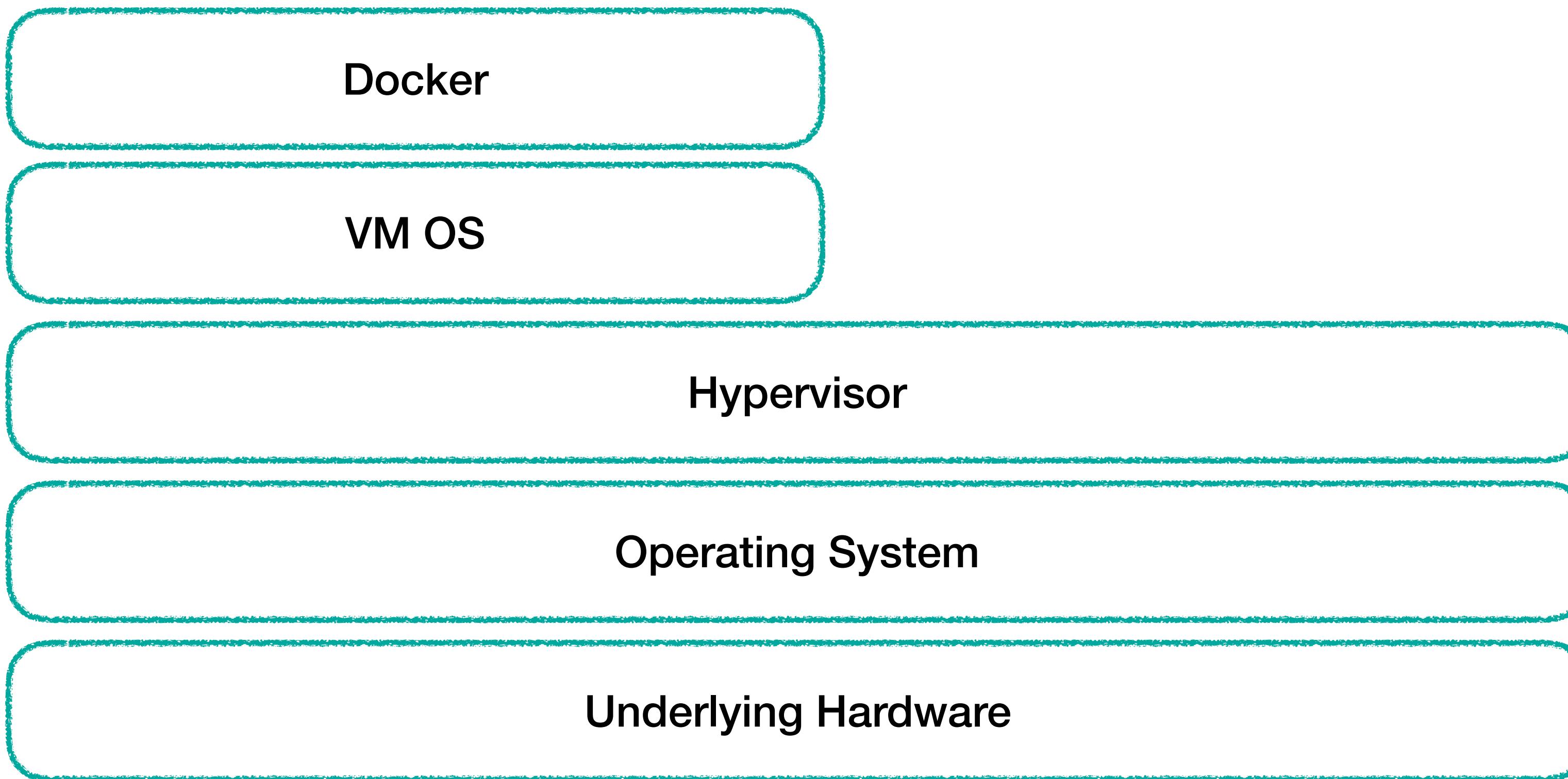
PATCHING MADNESS!



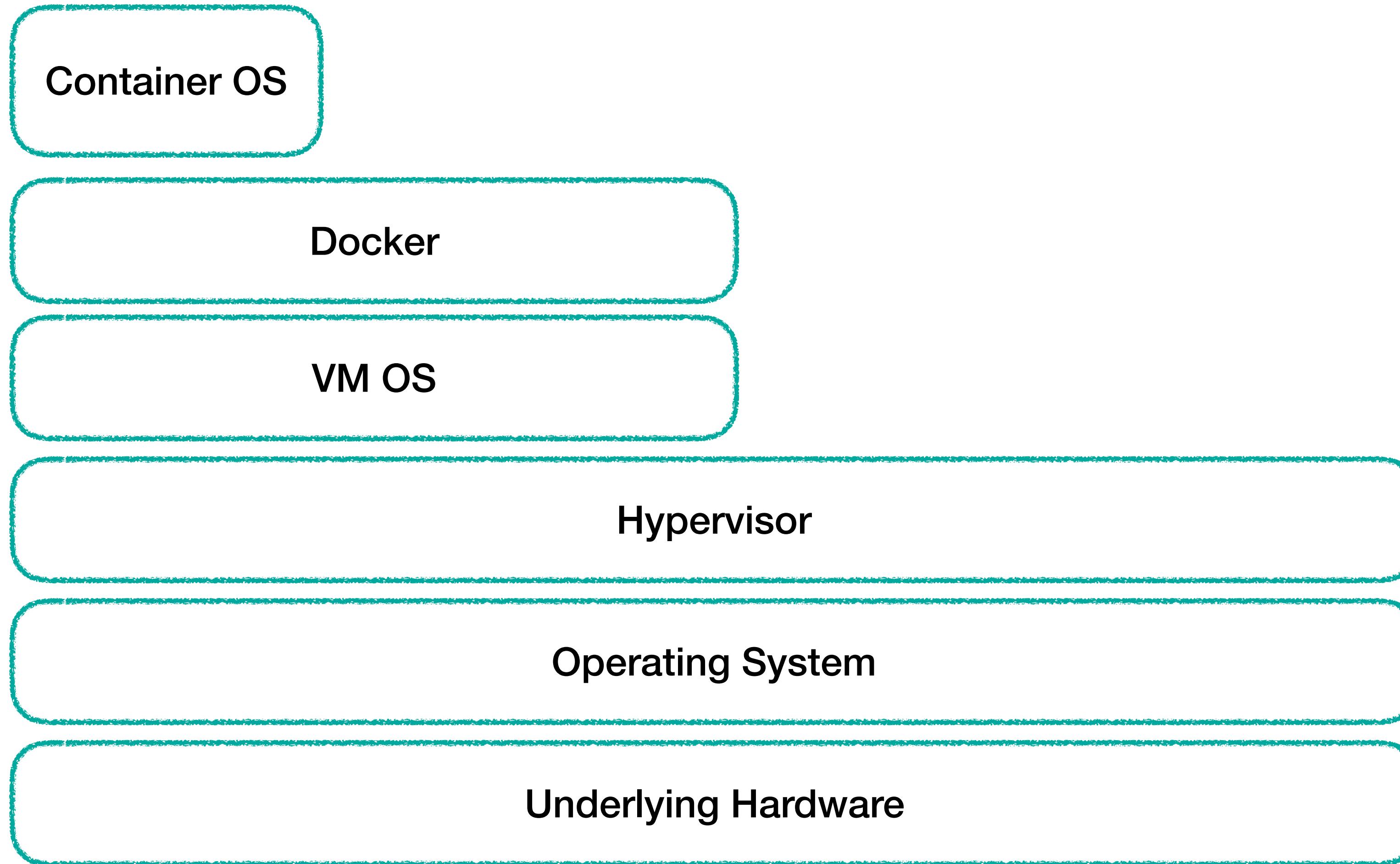
PATCHING MADNESS!



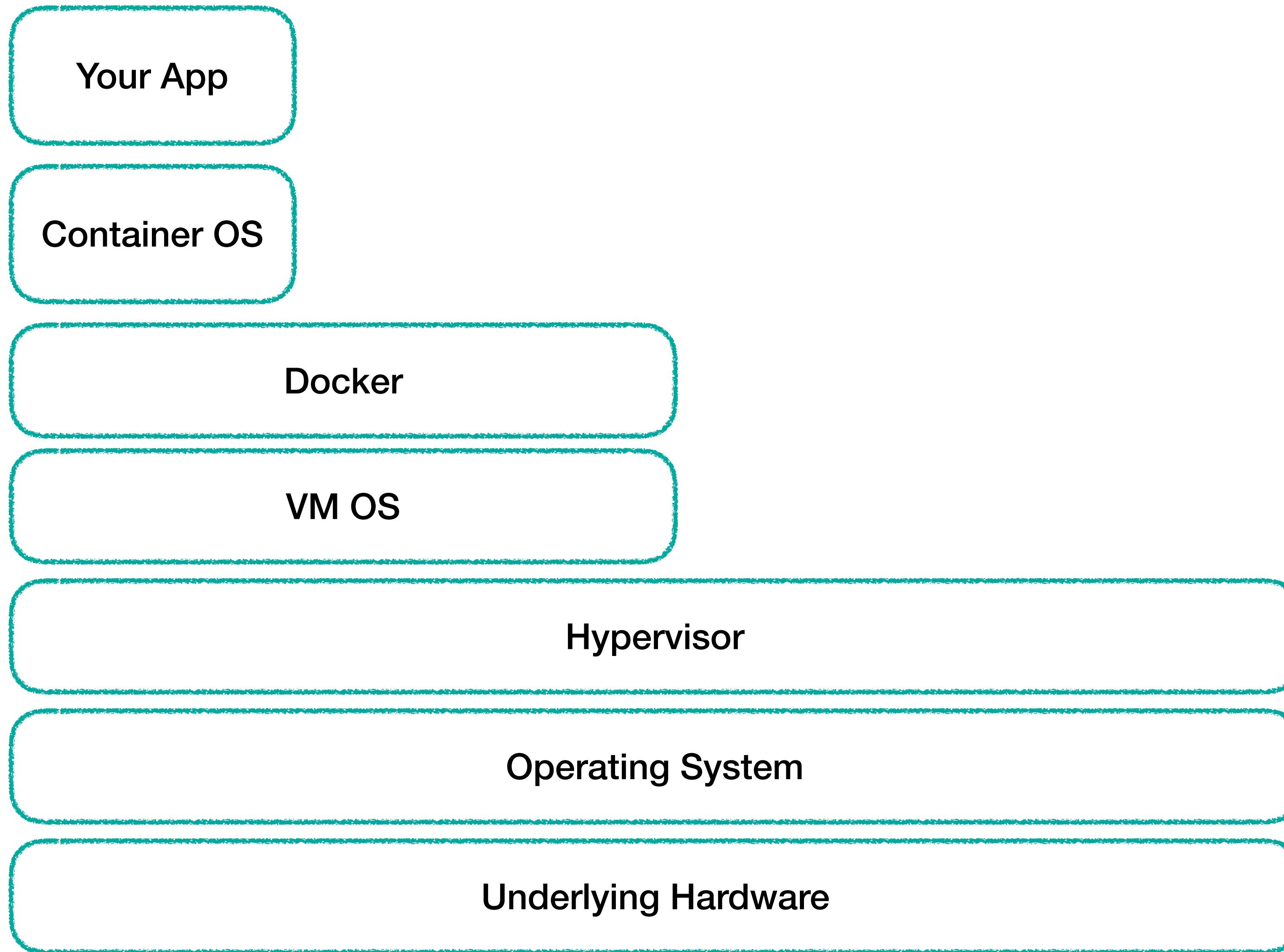
PATCHING MADNESS!



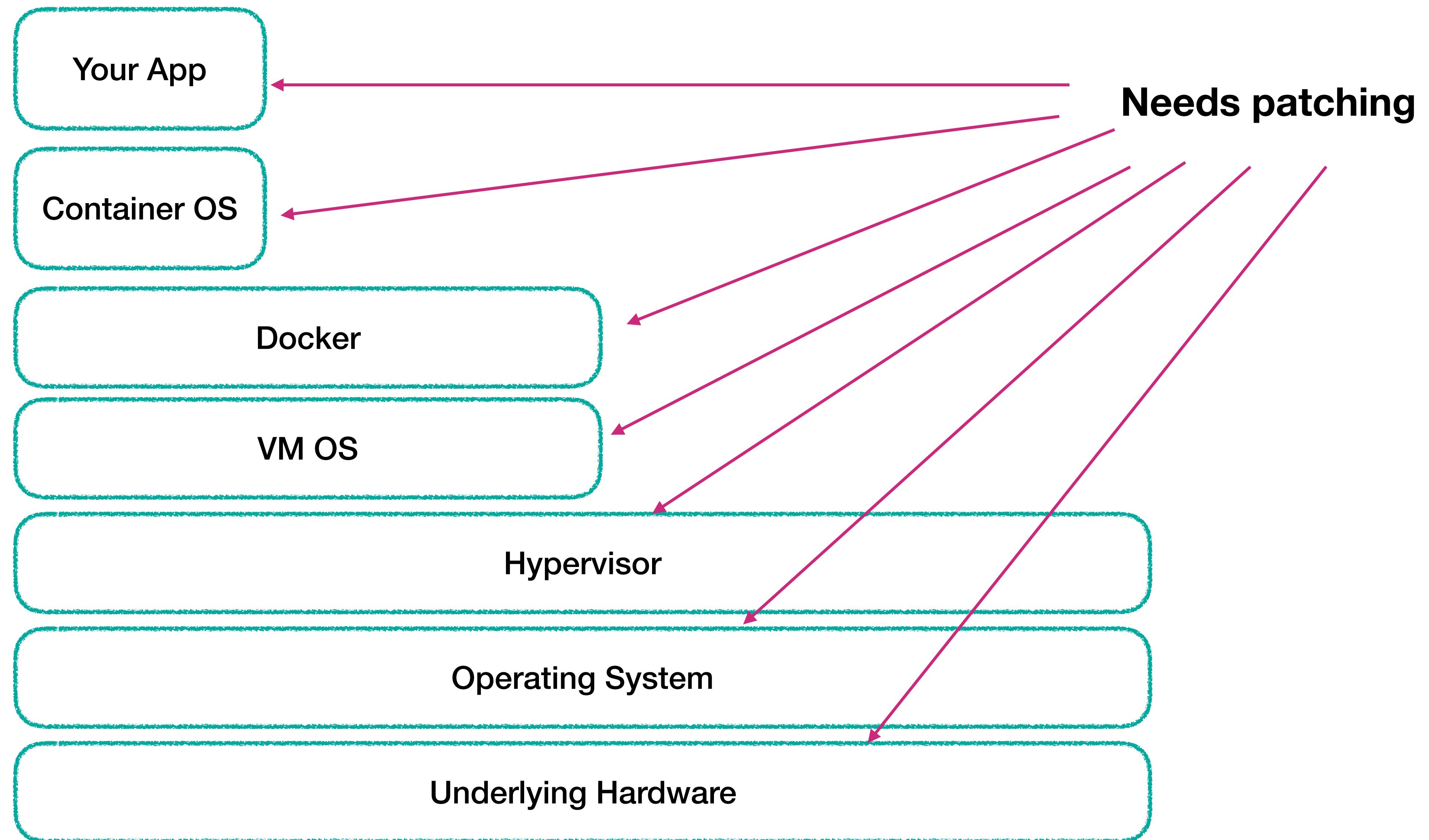
PATCHING MADNESS!



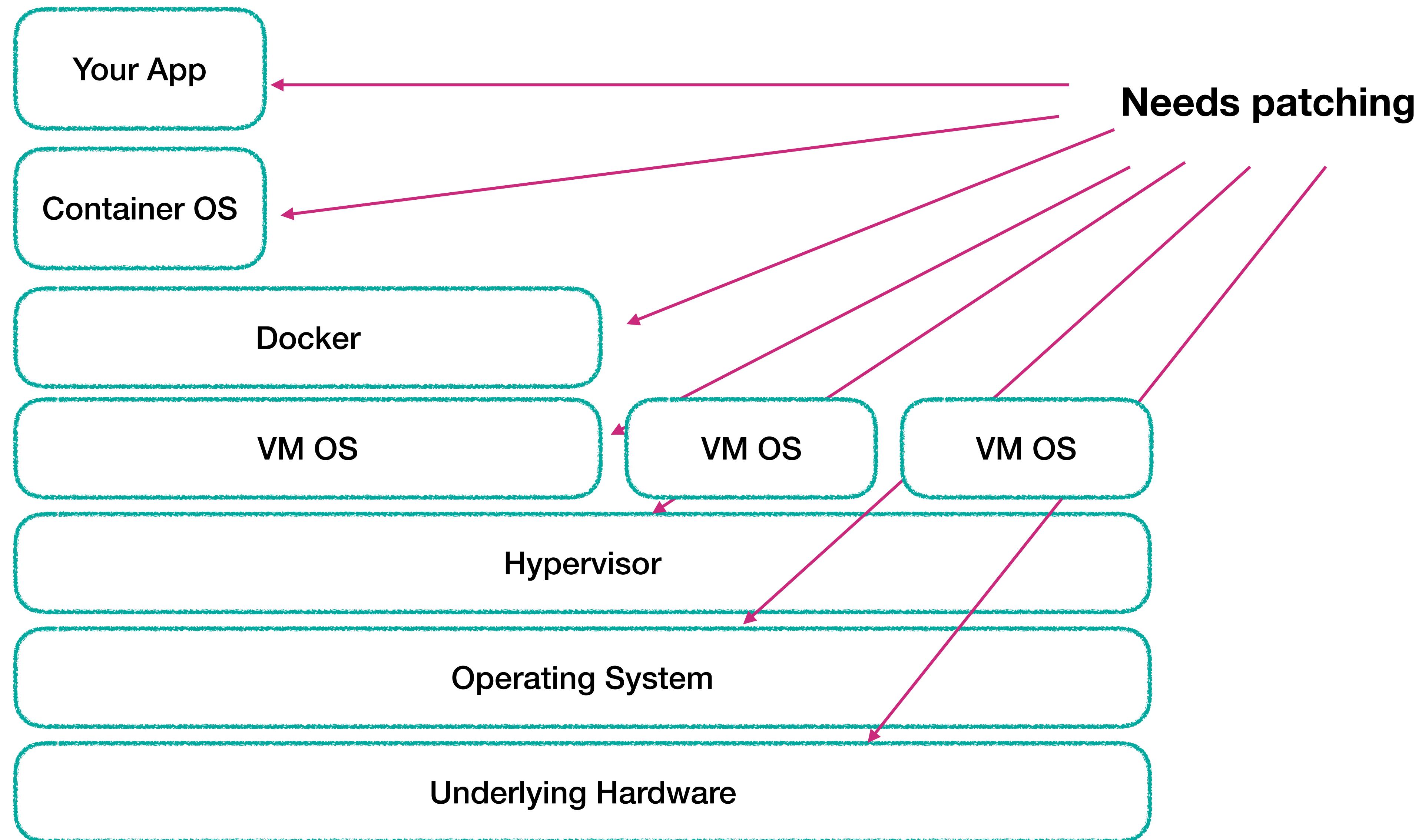
PATCHING MADNESS!



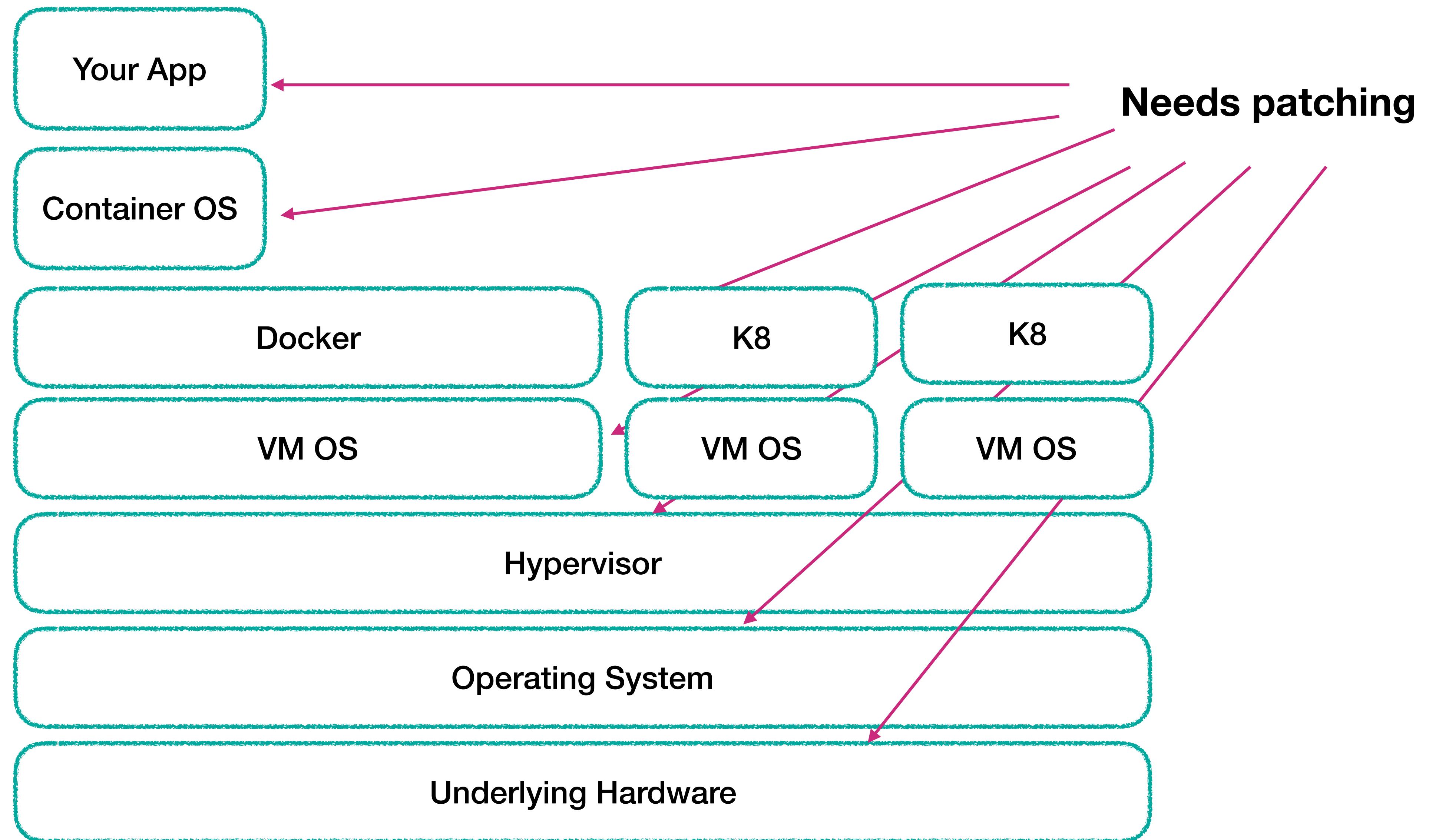
PATCHING MADNESS!



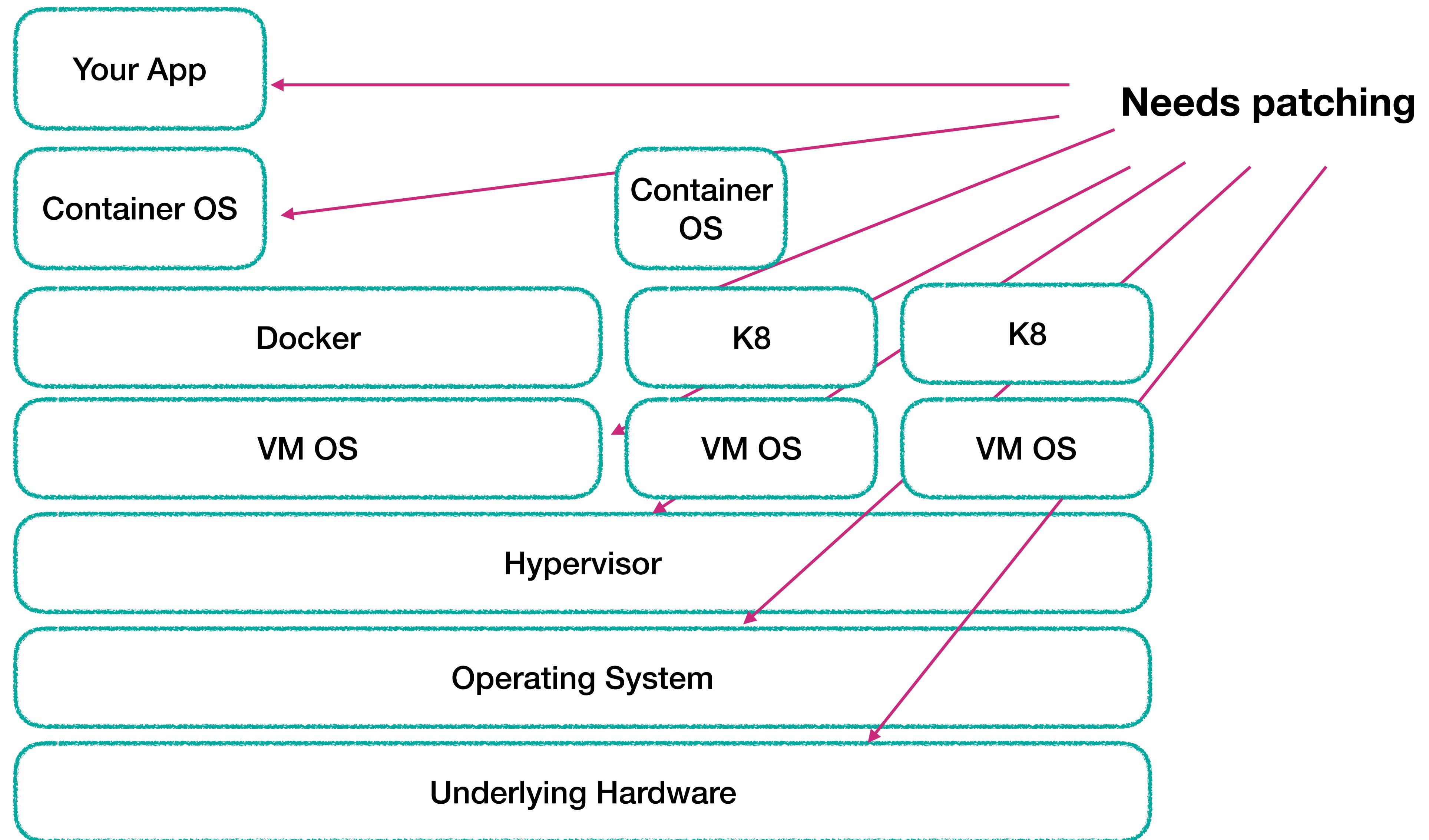
PATCHING MADNESS!



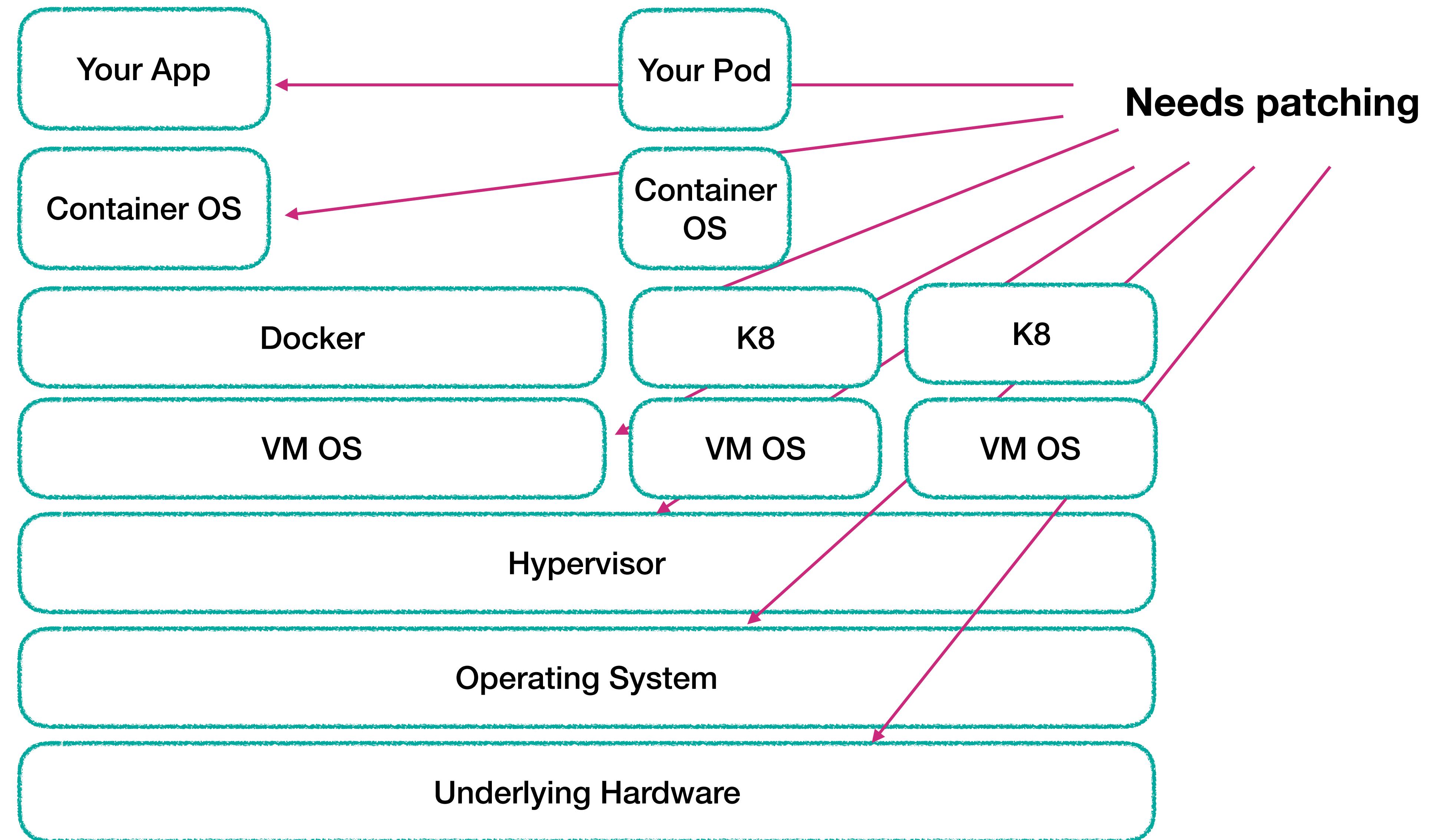
PATCHING MADNESS!



PATCHING MADNESS!



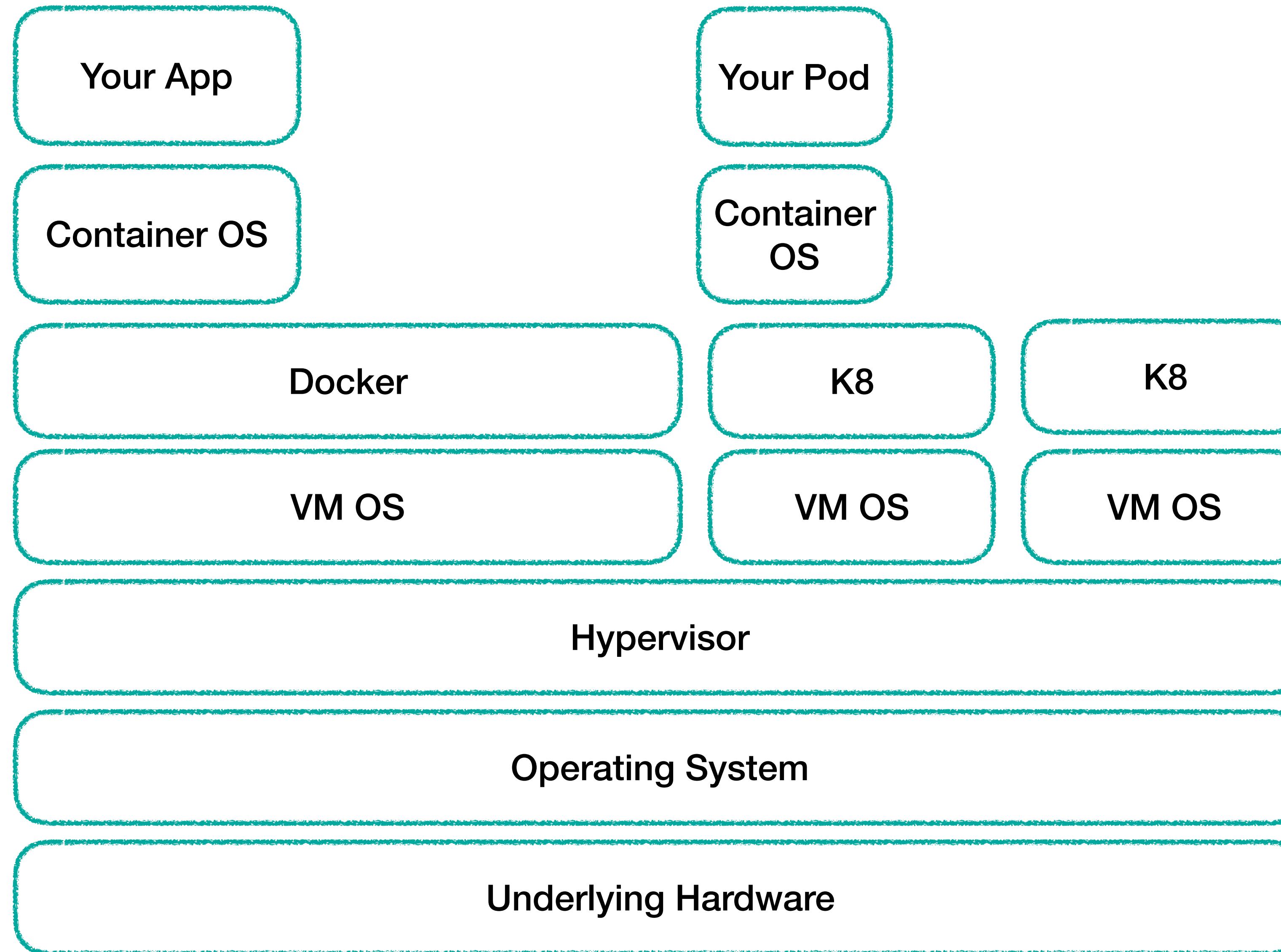
PATCHING MADNESS!



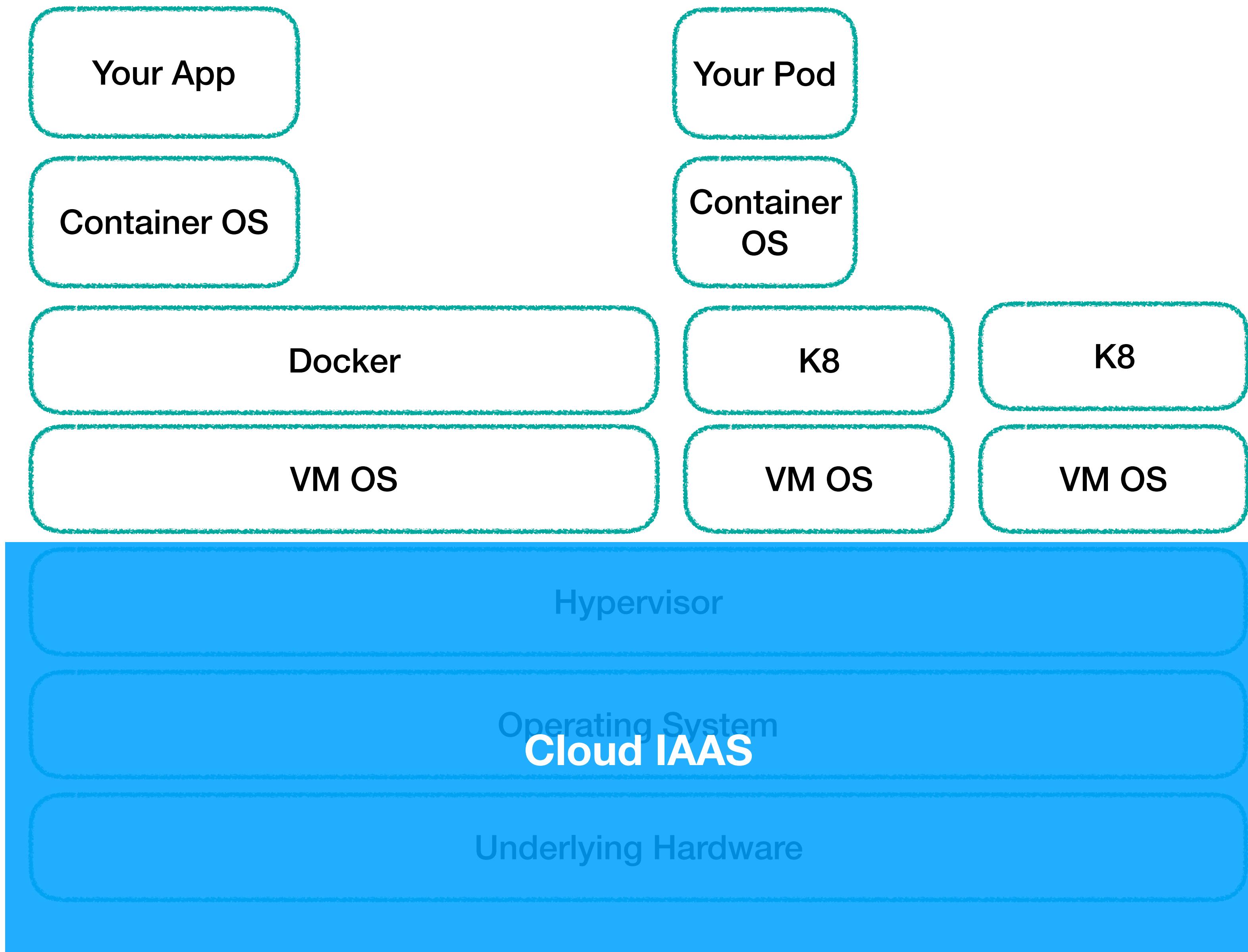
So, how many of you are still sure you apply every patch within 2-4 months of them being found?

So what can you do about this?

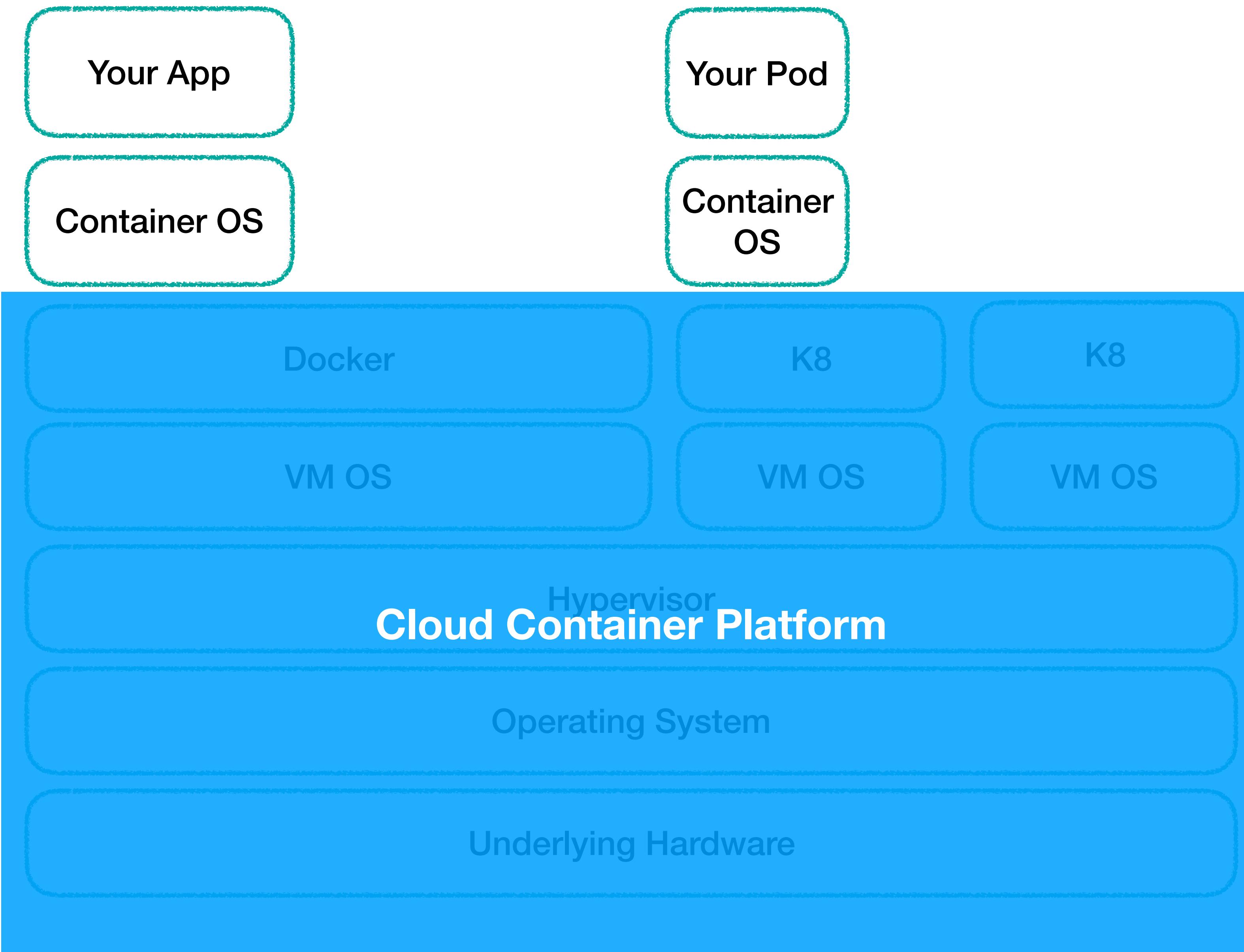
BETTER ON THE CLOUD?



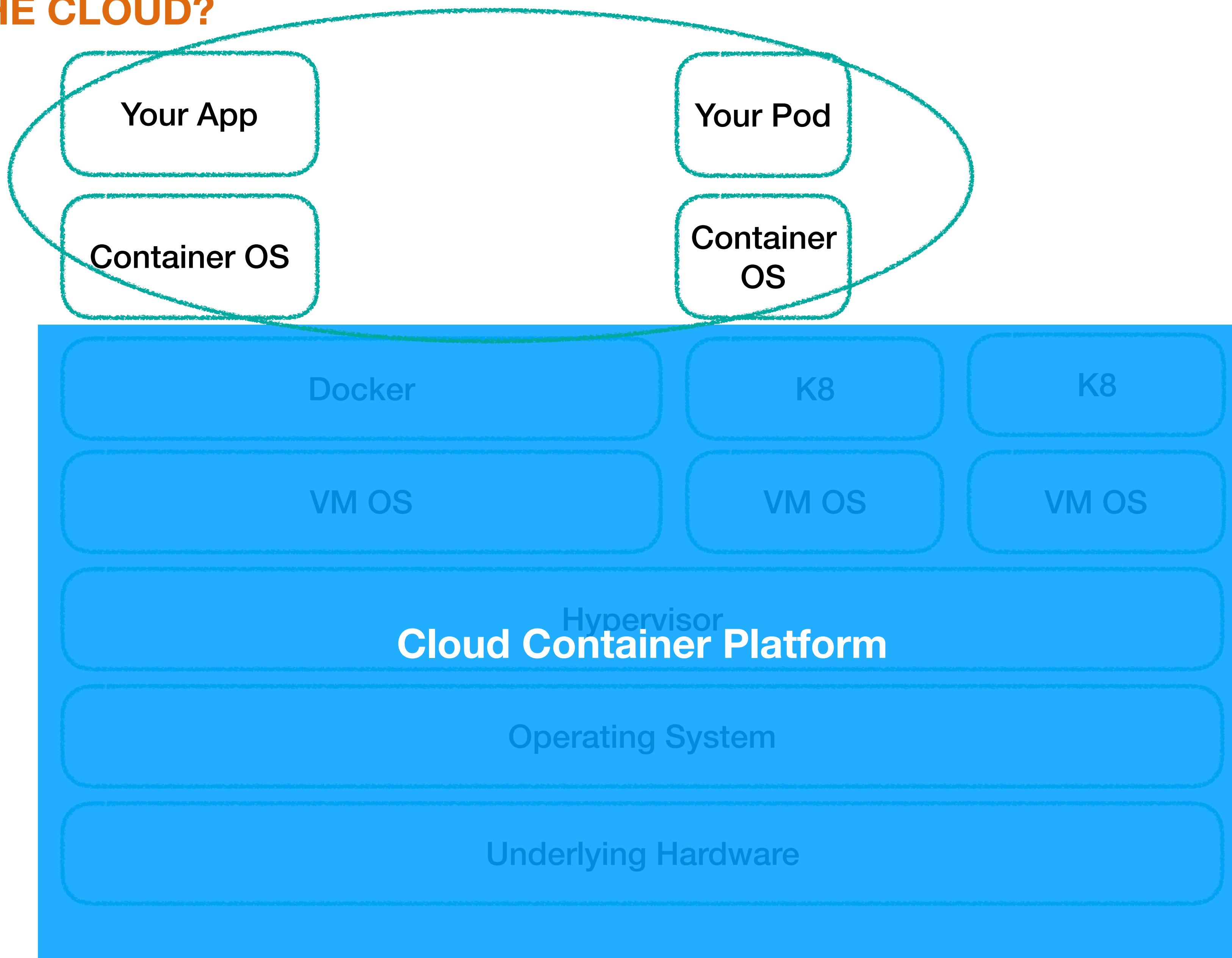
BETTER ON THE CLOUD?



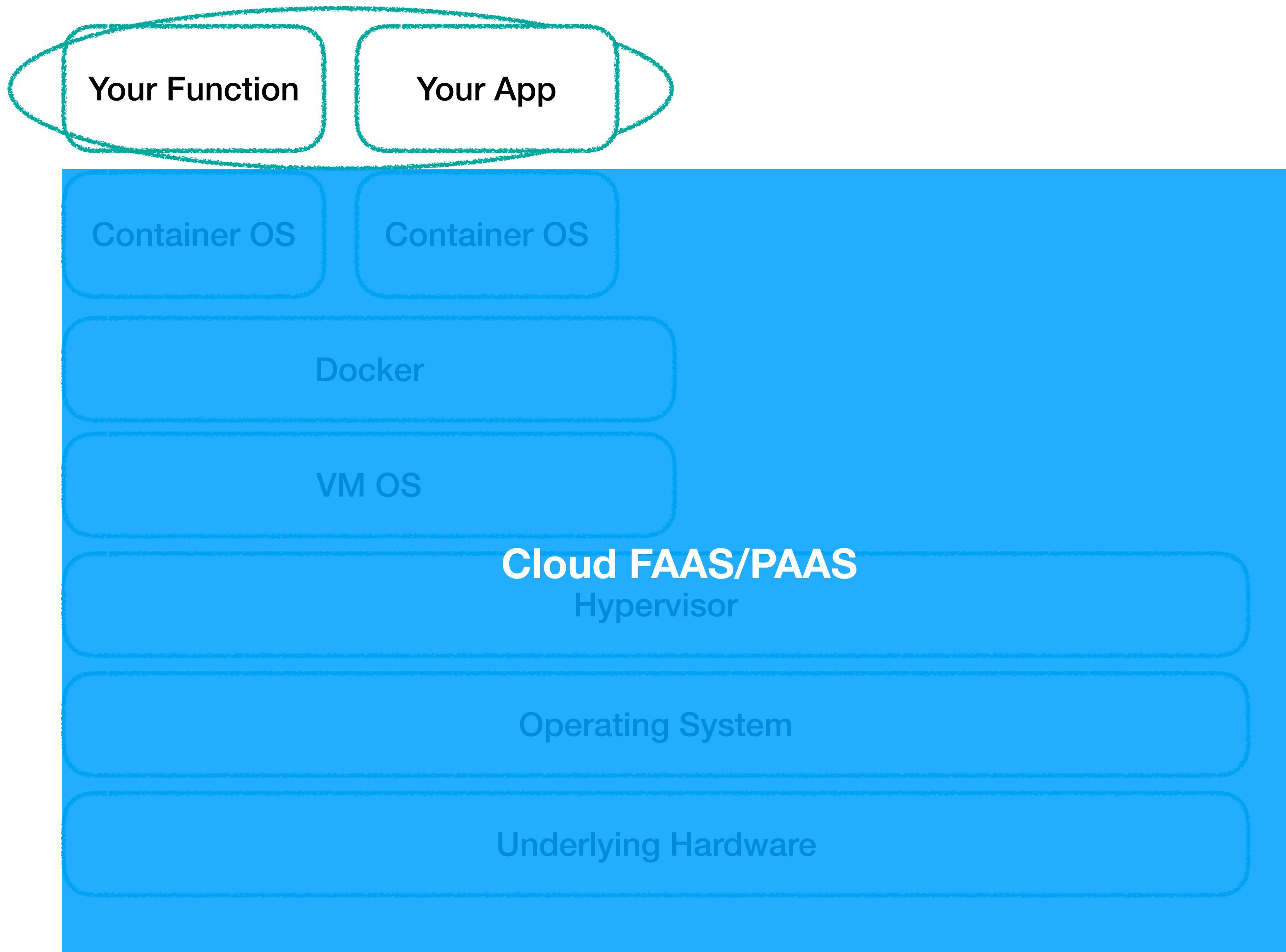
BETTER ON THE CLOUD?



BETTER ON THE CLOUD?



BETTER WITH FAAS?



CONTAINER SCANNING

HEADERS

Clair

Container Image Vulnerability Analysis and Reporting System

Build Status Coverage License Issues Pull Requests Documentation

Note: The master branch may be in an unstable or even broken state during development. Please use releases instead of the master branch in order to get stable binaries.



clair

Clair is an open source project for the static analysis of vulnerabilities in application containers (currently including `oci` and `docker`).

1. In regular intervals, Clair ingests vulnerability metadata from a configured set of sources and stores it in the database.
2. Clients use the Clair API to index their container images. This creates a list of features present in the image and stores them in the database.
3. Clients use the Clair API to query the database for vulnerabilities of a particular image; combining vulnerabilities and features is done for each request, avoiding the need to reparse images.
4. When updates to vulnerability metadata occur, a notification can be sent to alert systems that a change has occurred.

Our goal is to enable a more transparent view of the security of container-based infrastructure. Thus, the project was named **Clair**, after the French term which translates to clear, bright, transparent.

<https://github.com/coreos/clair>

@samnewman

CONTAINER SCANNING (CONT)

The screenshot shows the Aquasec interface for container scanning. On the left, there's a dark sidebar with navigation links: Home, Container, Docker, Kubernetes, Applications, and Help. The main area is titled "Dependencies & Images: untagged latest". It displays a list of dependencies and their status. At the top of the list is "nodejs@v12.13.0", which is marked as "Up-to-date". Below it are "curl@7.61.1" (Up-to-date), "openssl@1.1.1" (Up-to-date), and "python@3.7.3" (Up-to-date). Further down, there are sections for "Dependencies" (with "nodejs@v12.13.0" listed again) and "Images" (with "curl@7.61.1" and "openssl@1.1.1" listed). Each item has a status indicator (green for up-to-date, red for vulnerable) and a "View Details" button.

<https://www.aquasec.com>

MONITOR OUTDATED DEPENDENCIES

The screenshot shows the Snyk homepage with a dark blue header bar containing the Snyk logo and navigation links: New, Vulnerability DB, News, Help, Support, Pricing, Log In, and Sign Up. Below the header is a large banner with the text "Snyk continuously finds and fixes vulnerabilities in your dependencies." and a subtext "Protect and monitor your JavaScript, Ruby and Java apps". To the left, there's a section titled "Secure code protection" with a sub-section "Dependency protection" which includes a link to "Get started". To the right, there's a section titled "New! Dependency & Pull Request Monitoring" with a sub-section "Automatically detect and fix security issues in your dependencies" which includes a link to "Get started". At the bottom left, there's a section titled "80% of Snyk users found security issues in their dependencies" with a sub-section "How can Snyk help?". On the right side, there's a screenshot of the Snyk interface showing a dependency tree with various package names and their versions.

<https://snyk.io/>

AUTOMATICALLY PATCH APP DEPENDENCIES

[Snyk Update] New fixes for 25 vulnerable dependency paths [#1](#)

[Open](#) snyk-bot wants to merge 1 commit into master from upstream

[Conversation](#) 0 [Comments](#) 0 [File changes](#) 0

 snyk-bot commented an hour ago

This project has vulnerabilities that could not be fixed, or were patched when no upgrade was available. Good news, new upgrades or patches have now been published! This pull request fixes vulnerable dependencies you couldn't previously address.

The PR includes:

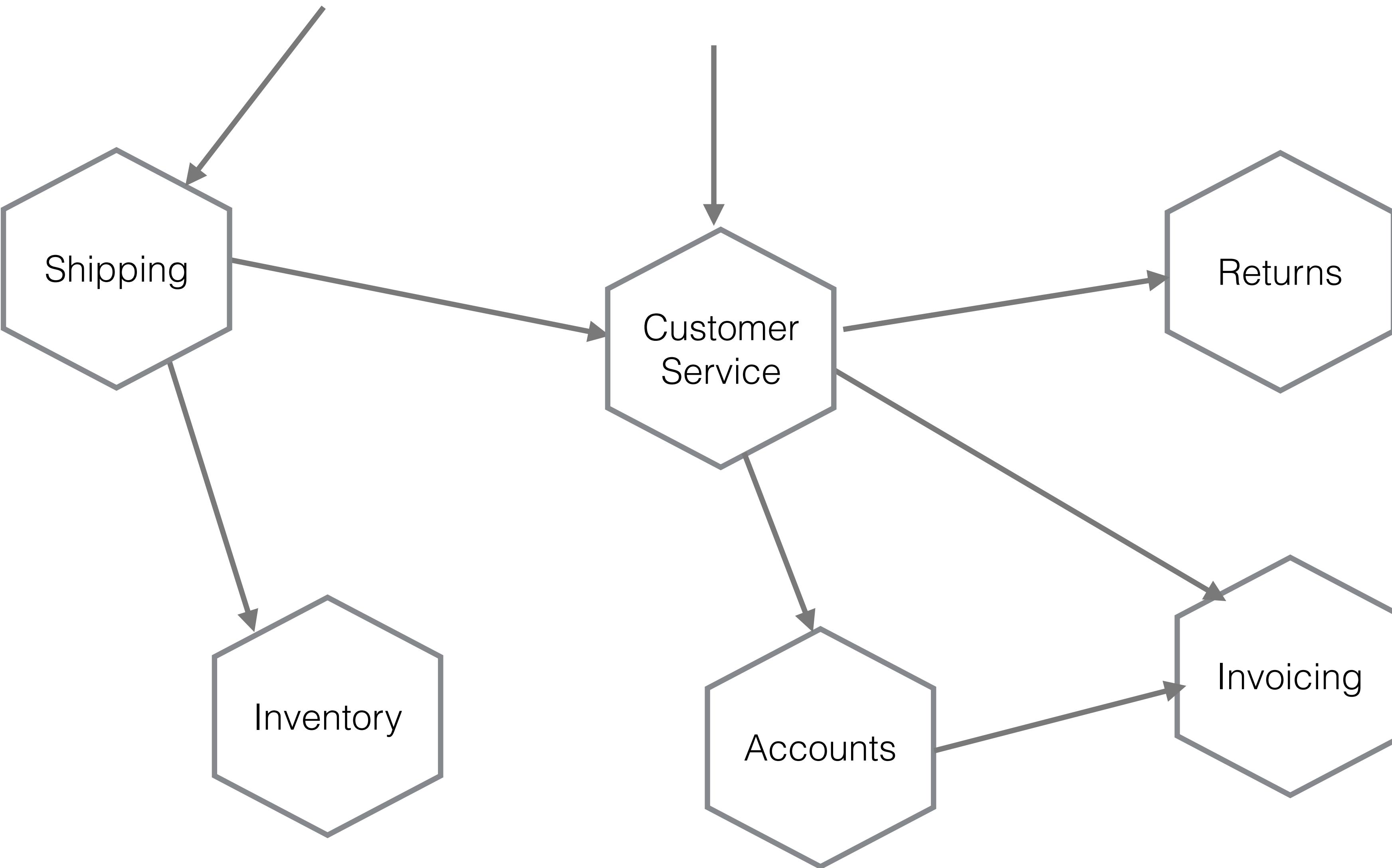
- Changes to package.json to upgrade the vulnerable dependencies to a fixed version.

<https://snyk.io/>

DO SOME THREAT MODELLING

The screenshot shows the Microsoft Security Development Lifecycle (SDL) website. At the top, there's a banner with three people and the text "Life in the Digital Crosshairs" and "Experience the Untold Story". Below this, there's a section titled "What is the Security Development Lifecycle?" featuring a green shield icon and a brief description of the SDL as a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost. A horizontal timeline diagram shows the SDL phases: Planning, Requirements, Design, Implementation, Verification, Release, and Maintenance. The "Design" phase is highlighted in green. Below the timeline, there's a link to "Get to code a phase". Under the "Design Phase" heading, there's a sub-section titled "SDL Practice #5: Establish Design Requirements" with a brief description. To the right, there are sections for "Assess your security" (with links to "Assessment tools" and "Get started"), "Tools" (listing several tools like "SDL Source Analyzer", "SDL Threat Modeling Toolkit", "SDL Code Review Toolkit", "SDL Test Plan Template", and "SDL Security Testing Guide"), and a "Get started" button.

<https://www.microsoft.com/en-us/sdl/>

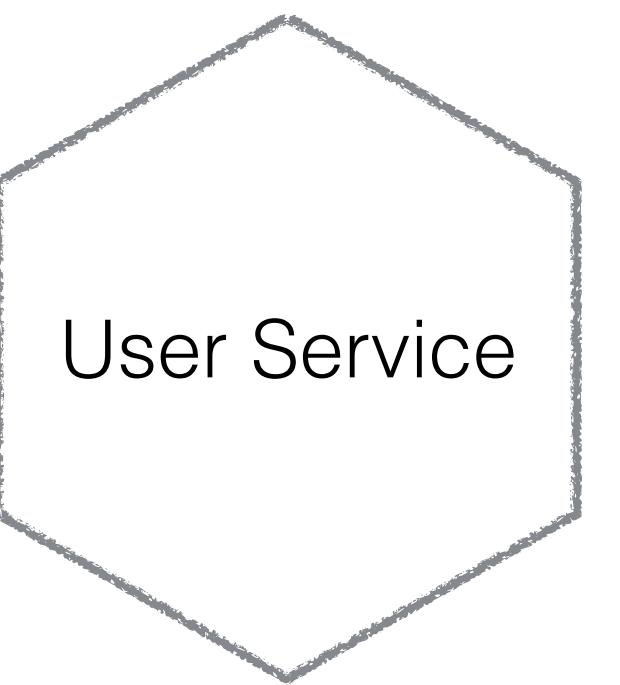


J A S O N C R A T H M A N

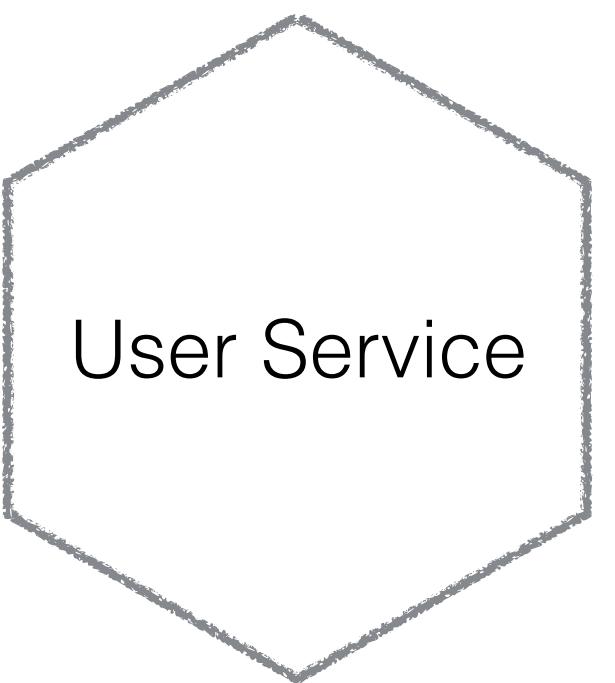


MUSIC CORP 2018

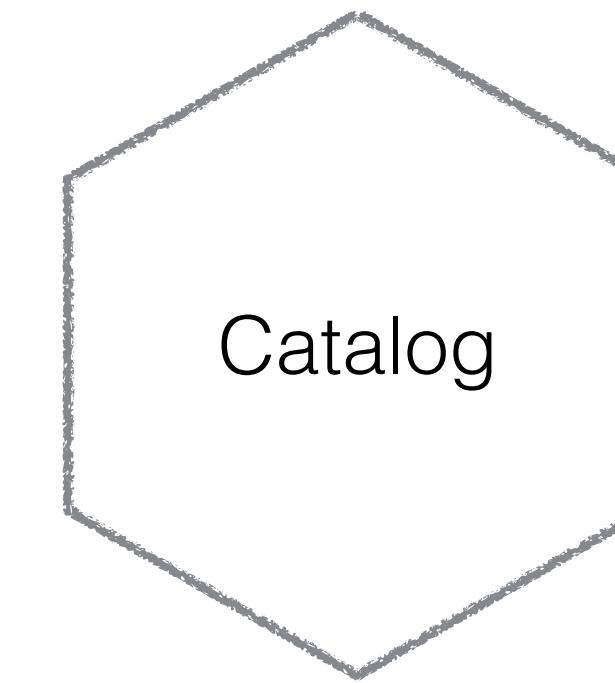
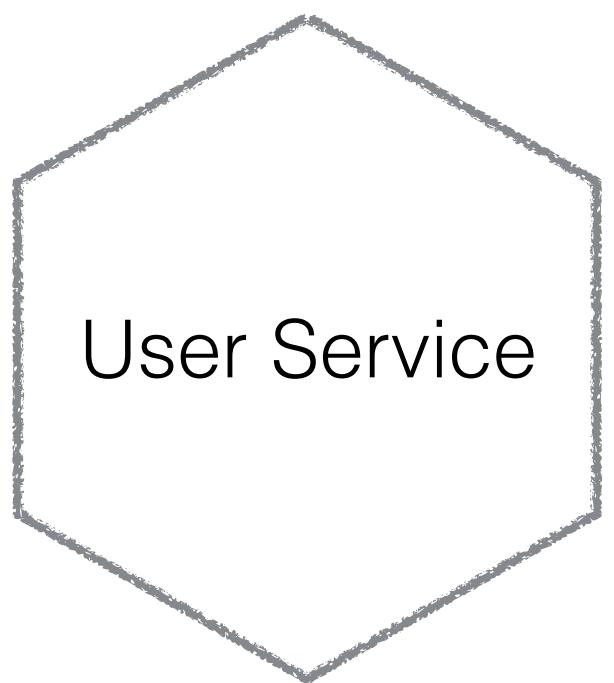
MUSIC CORP 2018



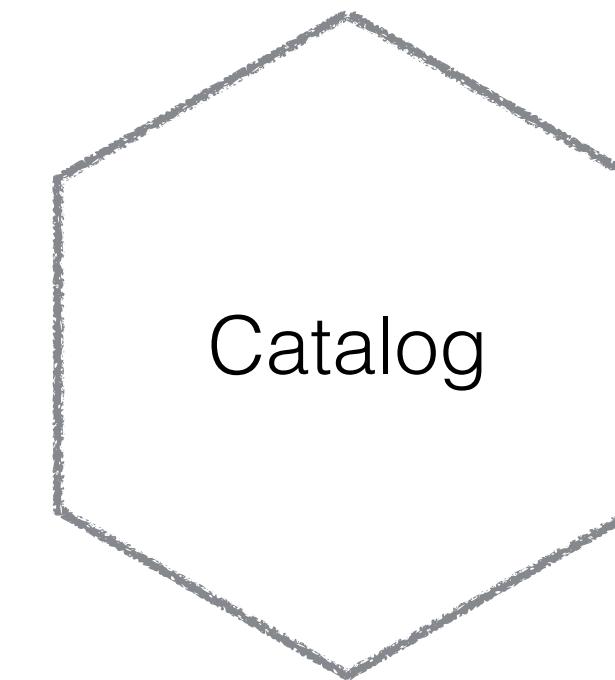
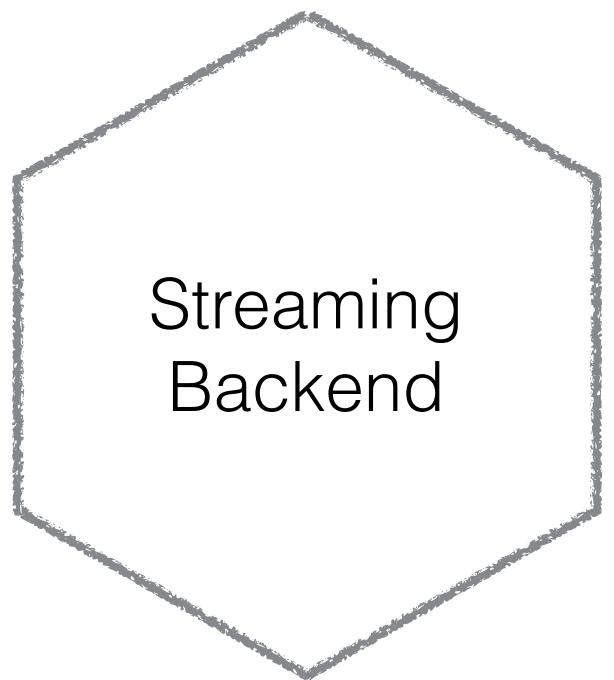
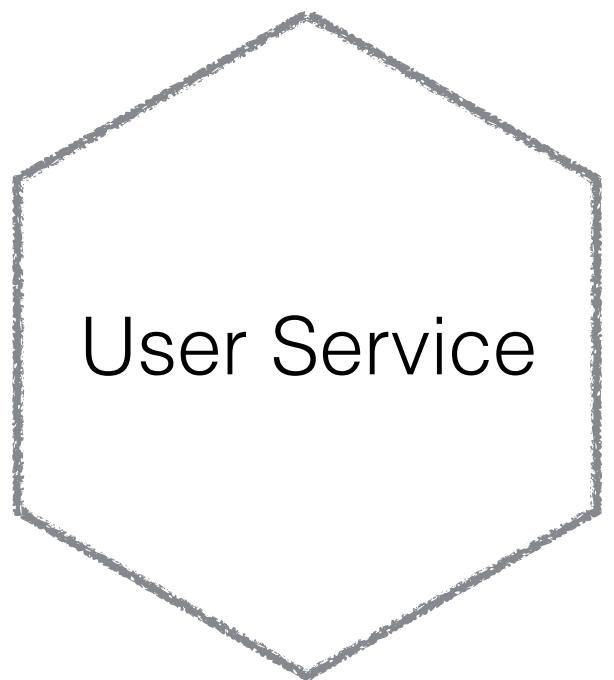
MUSIC CORP 2018



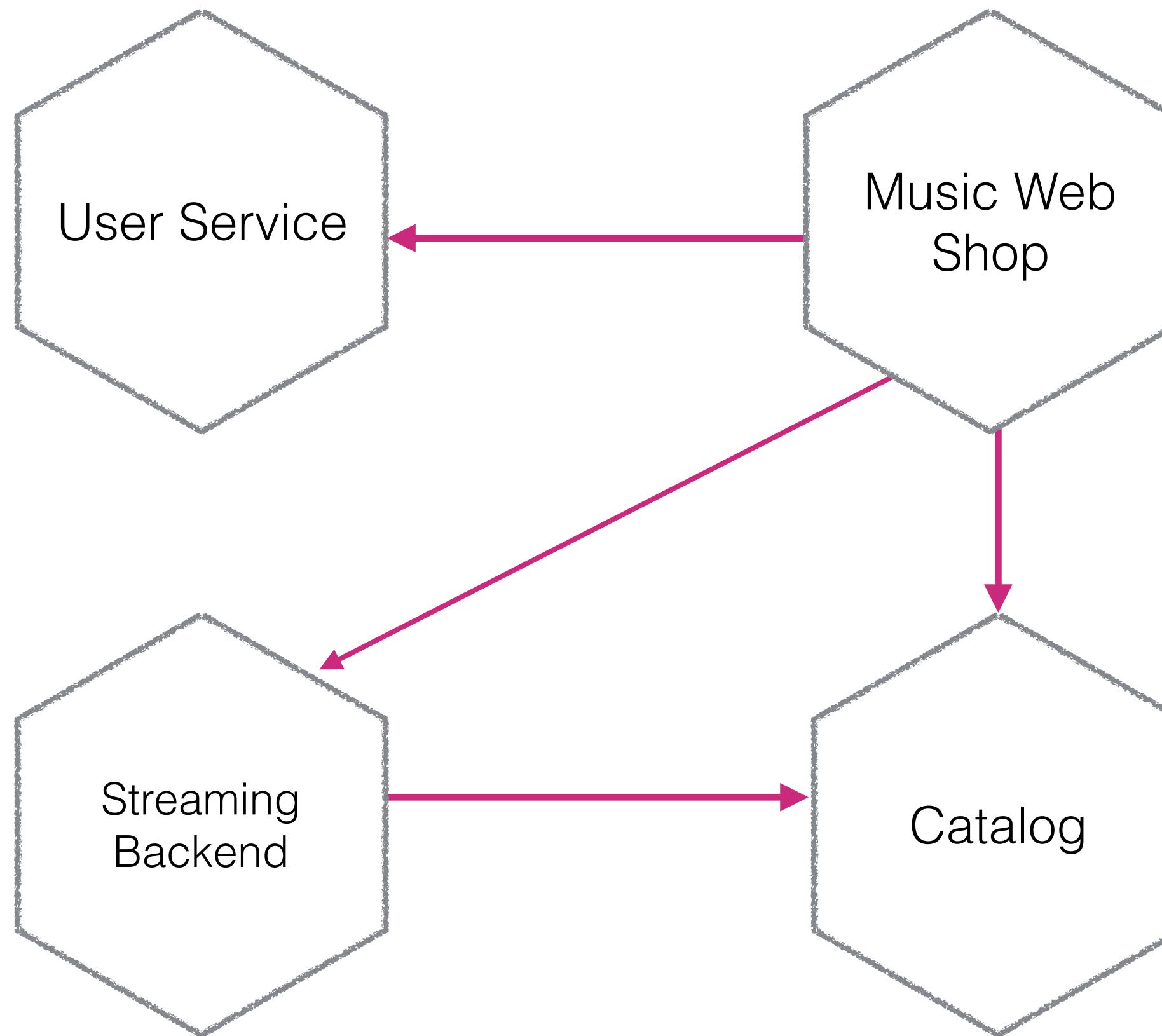
MUSIC CORP 2018



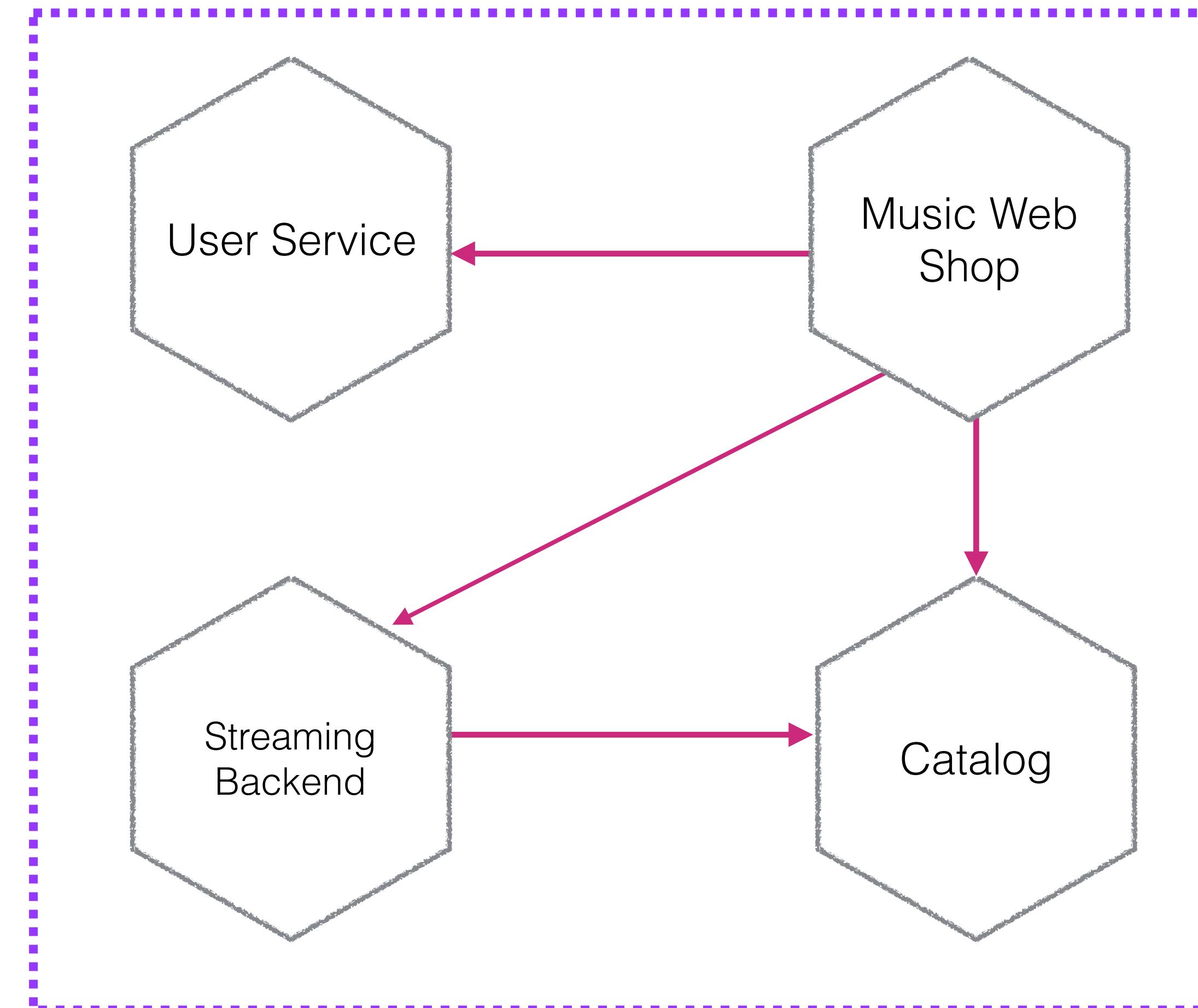
MUSIC CORP 2018



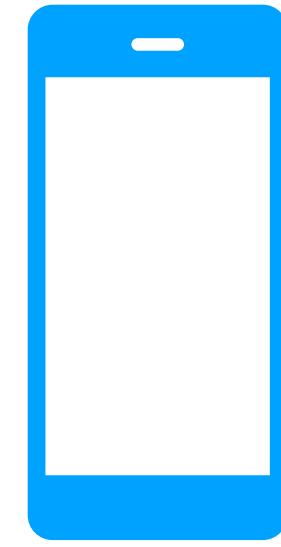
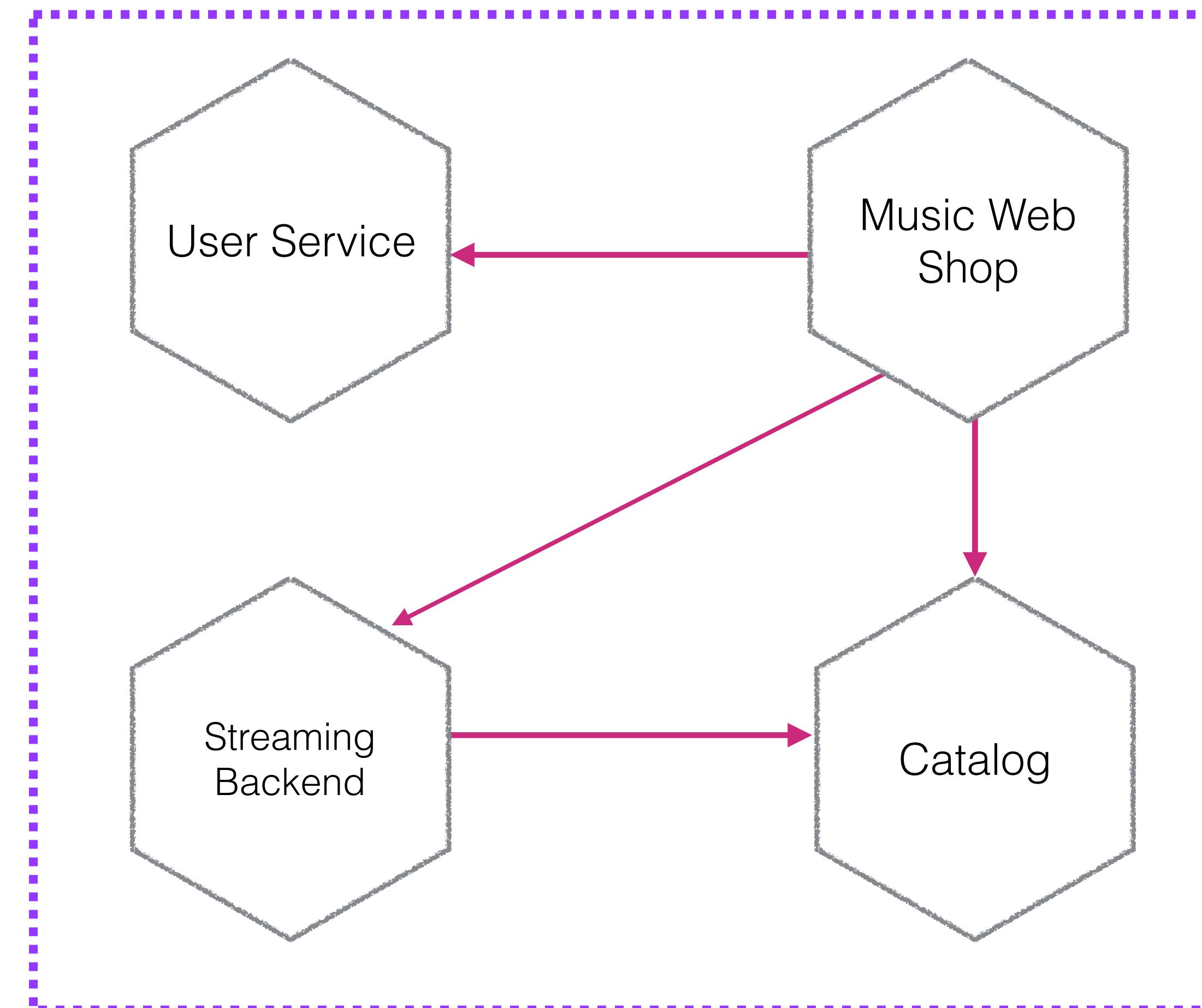
MUSIC CORP 2018



MUSIC CORP 2018

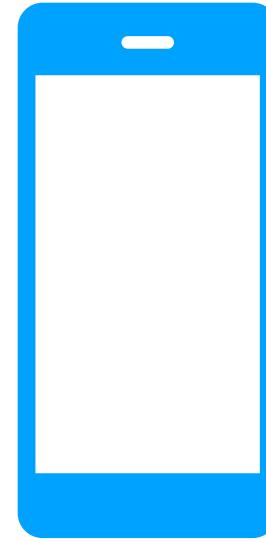
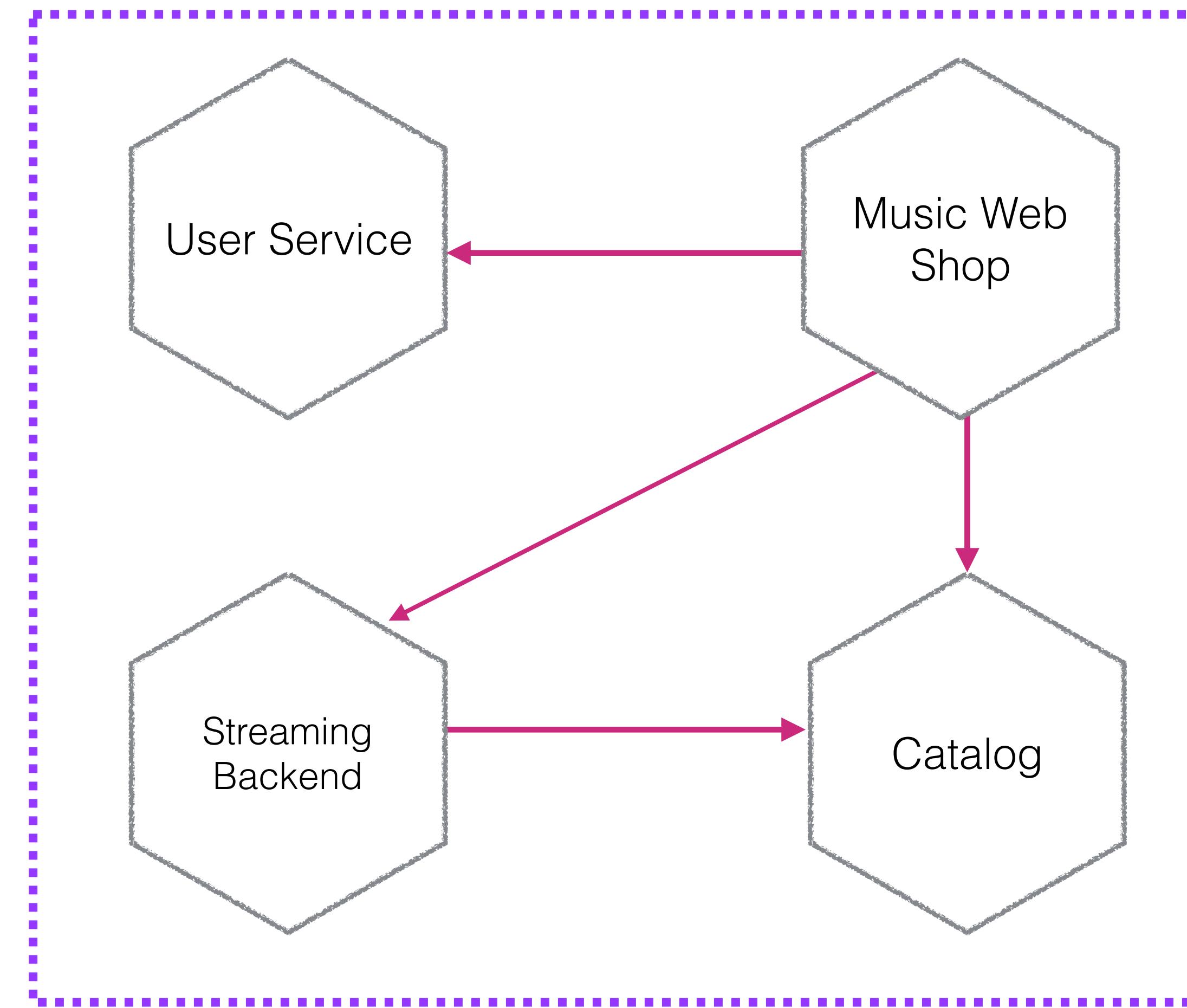


MUSIC CORP 2018



Native Mobile

MUSIC CORP 2018

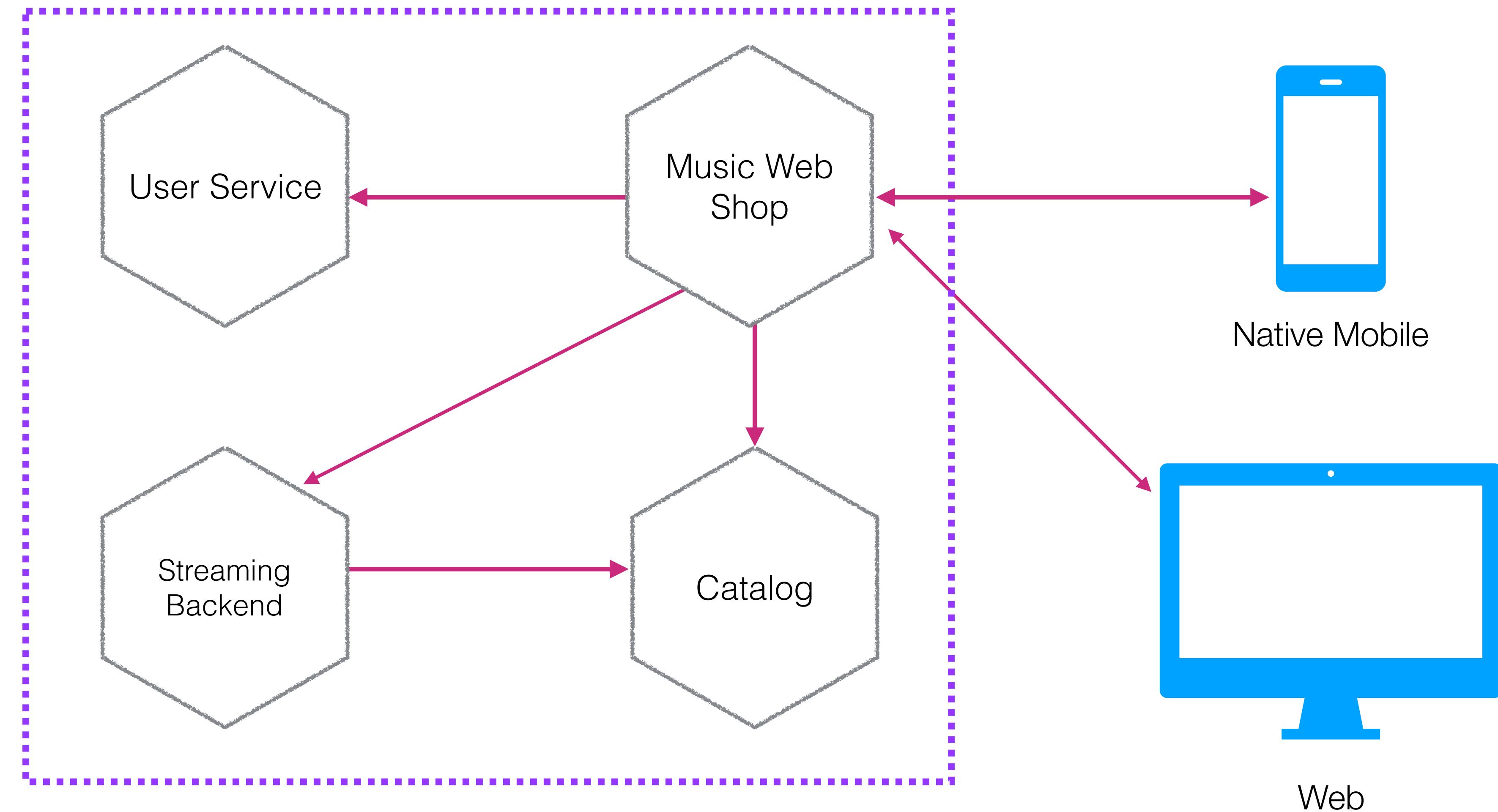


Native Mobile

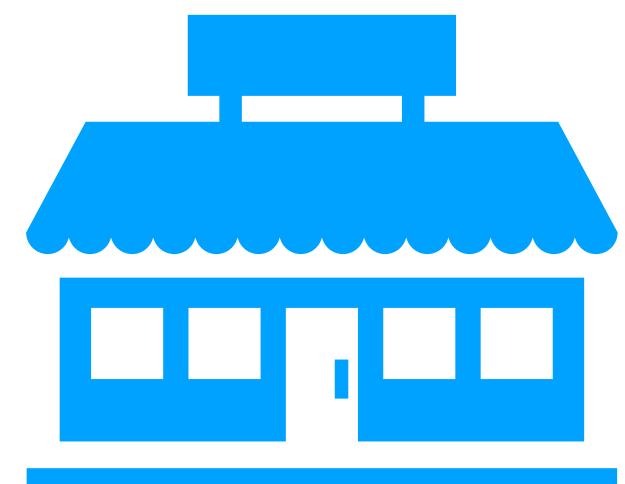


Web

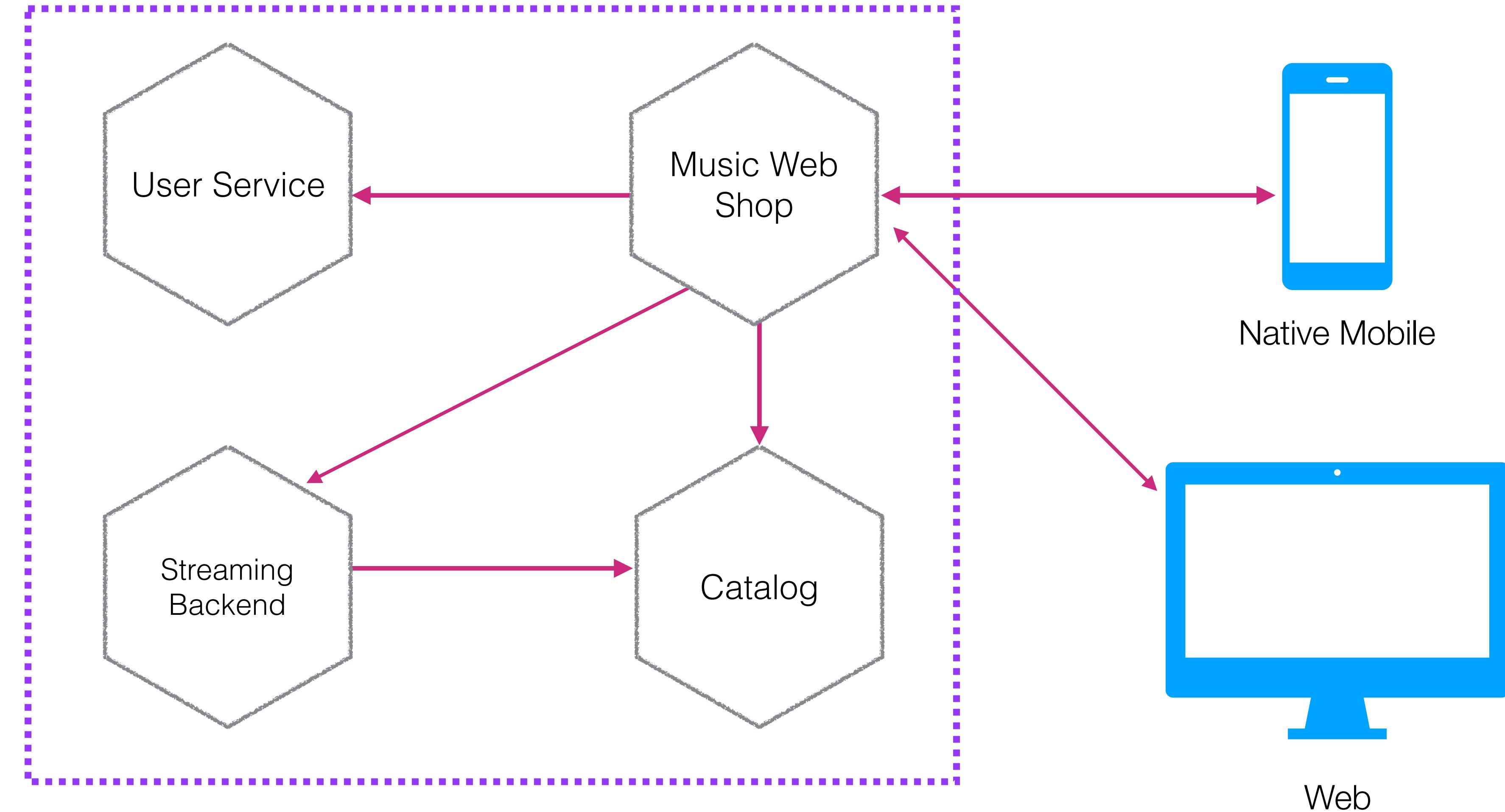
MUSIC CORP 2018



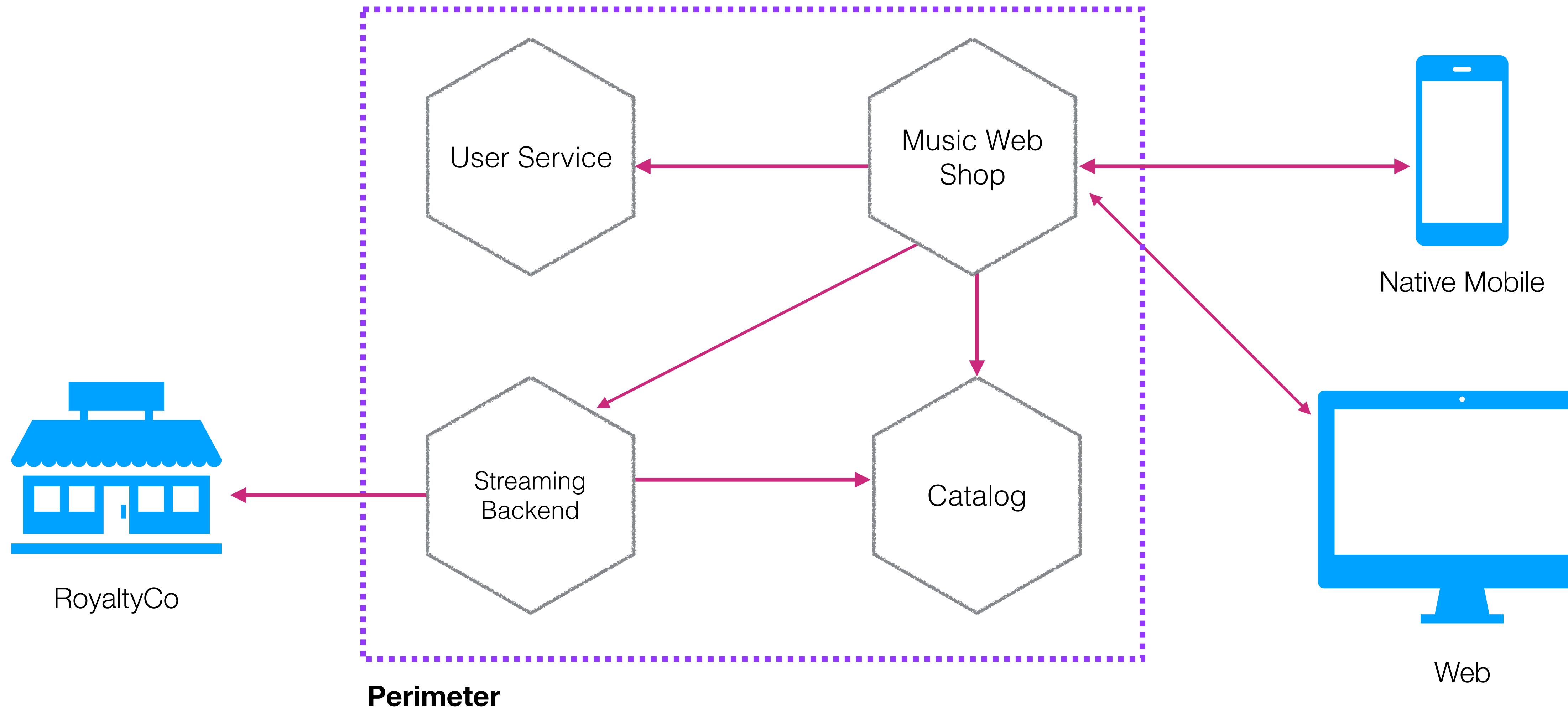
MUSIC CORP 2018



RoyaltyCo



MUSIC CORP 2018



KEY CONCERNS OF TRANSPORT SECURITY

KEY CONCERNS OF TRANSPORT SECURITY

Observation of data

KEY CONCERNS OF TRANSPORT SECURITY

Observation of data

Manipulation of data

KEY CONCERNS OF TRANSPORT SECURITY

Observation of data

Manipulation of data

Restricting access to endpoints

KEY CONCERNS OF TRANSPORT SECURITY

Observation of data

Manipulation of data

Restricting access to endpoints

Impersonation of endpoints

HTTPS Everywhere!

HTTP + TLS

Server guarantees!

Server guarantees!

Payload not manipulated

Server guarantees!

Payload not manipulated

Client guarantees?

Server guarantees!

Payload not manipulated

Client guarantees?

Certificate management can be painful

LET'S ENCRYPT



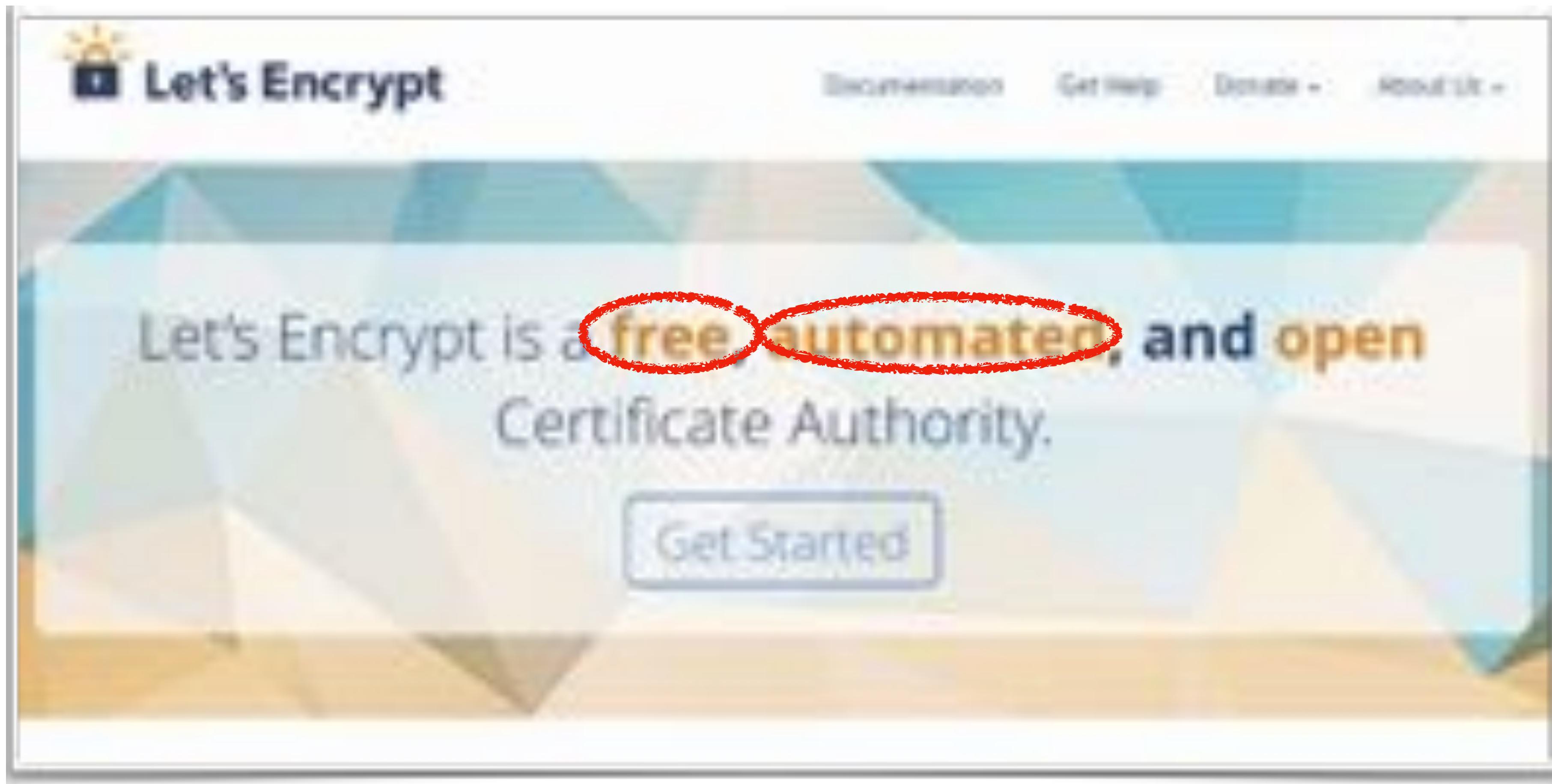
<https://letsencrypt.org/>

LET'S ENCRYPT



<https://letsencrypt.org/>

LET'S ENCRYPT



<https://letsencrypt.org/>

AWS CERTIFICATE MANAGER

The screenshot shows the AWS Certificate Manager landing page. At the top, it says "AWS Certificate Manager". Below that, a large text block explains what AWS Certificate Manager is and how it works. To the right, there are two buttons: "Manage Your AWS Resources" and "Get Started".

AWS Certificate Manager

AWS Certificate Manager is a service that lets you easily provision, manage, and deploy Secure Sockets Layer/TLS Transport Layer Security (SSL/TLS) certificates for use with AWS services. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates. With AWS Certificate Manager, you can quickly request a certificate, deploy it on AWS resources such as Elastic Load Balancers, Amazon CloudFront distributions, and APIs on API Gateway, and let AWS Certificate Manager handle certificate renewal. SSL/TLS certificates originated through AWS Certificate Manager are free. You pay only for the AWS resources you create to run your application.

Manage Your AWS Resources

Get Started

<https://aws.amazon.com/certificate-manager/>

HOW DOES THIS STACK UP?

Server guarantees!

Payload not manipulated

Client guarantees?

Certificate management can be
painful

HOW DOES THIS STACK UP?

Server guarantees!

Payload not manipulated

Client guarantees?

Certificate management can be
painful

Observation of data

Manipulation of data

Restricting access to endpoints

Impersonation of endpoints

HOW DOES THIS STACK UP?

Server guarantees!



Observation of data

Payload not manipulated

Manipulation of data

Client guarantees?

Restricting access to endpoints

Certificate management can be
painful

Impersonation of endpoints

HOW DOES THIS STACK UP?

Server guarantees!

✓ Observation of data

Payload not manipulated

✓ Manipulation of data

Client guarantees?

Restricting access to endpoints

Certificate management can be
painful

Impersonation of endpoints

HOW DOES THIS STACK UP?

Server guarantees!

✓ Observation of data

Payload not manipulated

✓ Manipulation of data

Client guarantees?

? Restricting access to endpoints

Certificate management can be
painful

Impersonation of endpoints

HOW DOES THIS STACK UP?

Server guarantees!

✓ Observation of data

Payload not manipulated

✓ Manipulation of data

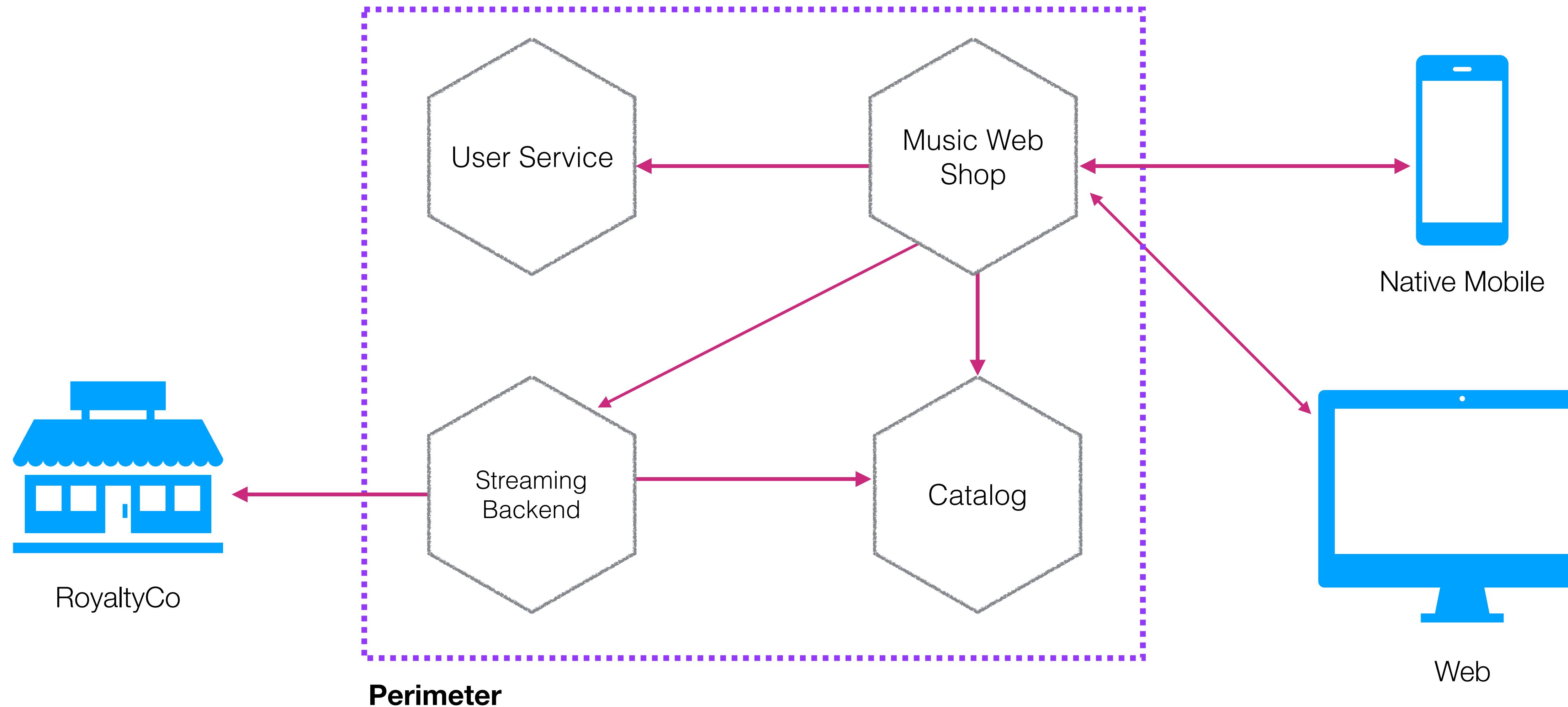
Client guarantees?

? Restricting access to endpoints

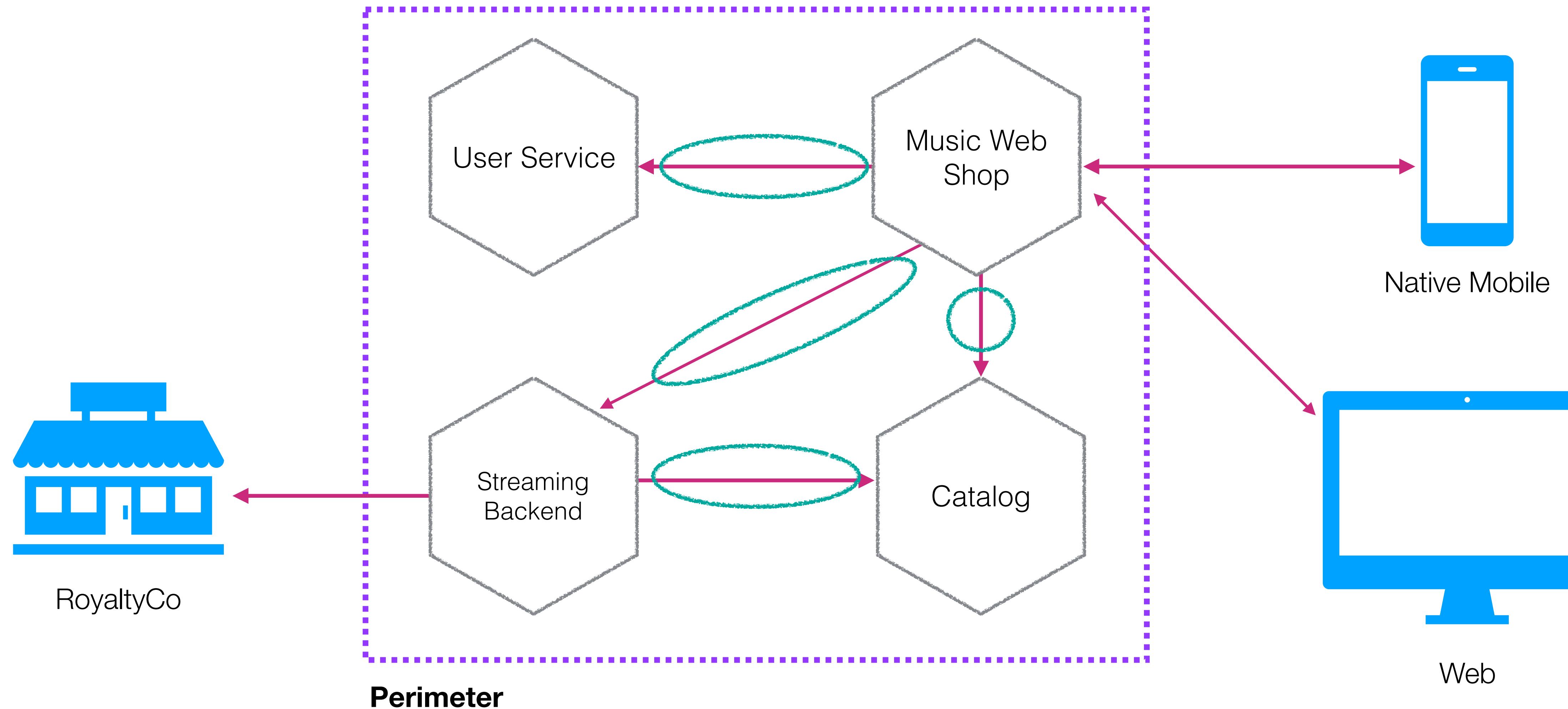
Certificate management can be
painful

✓ Impersonation of endpoints

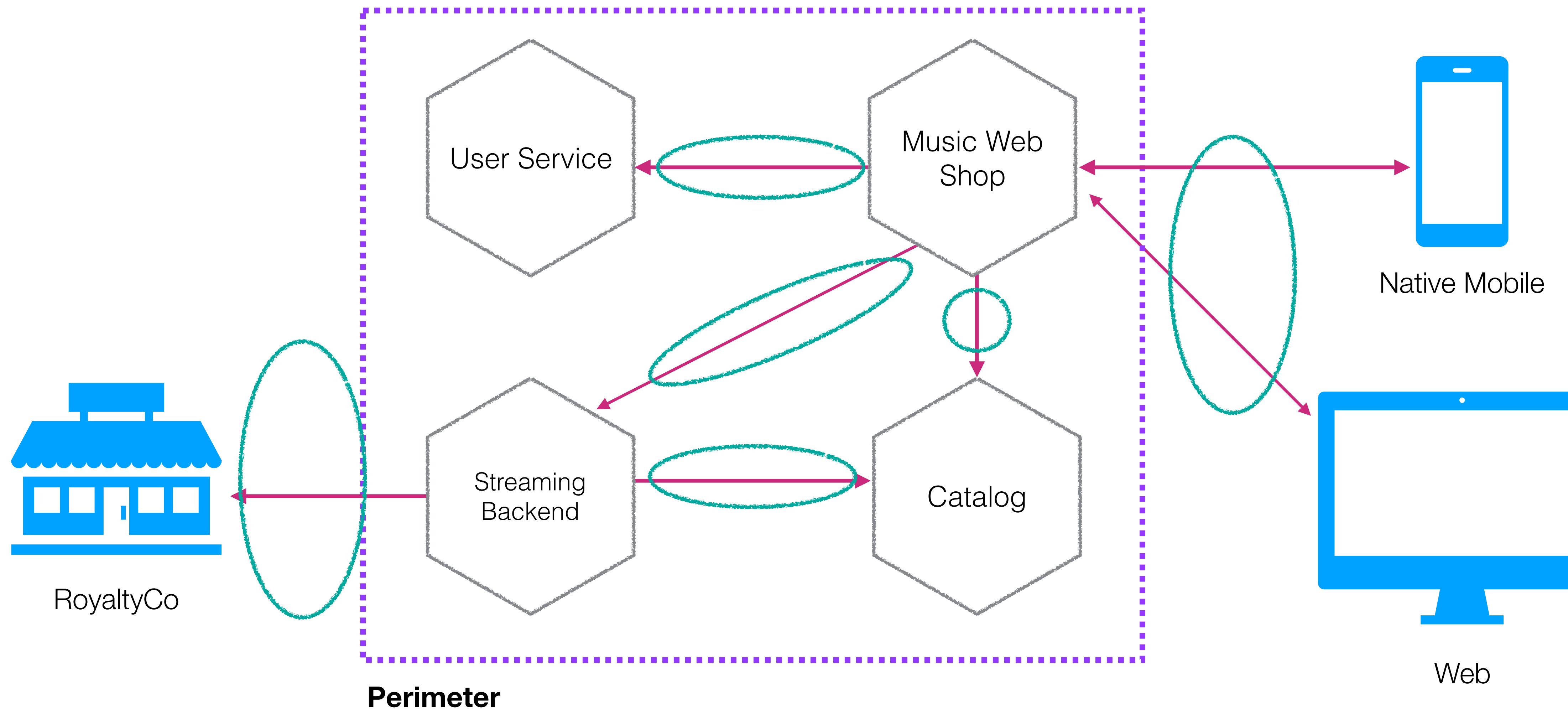
HTTPS EVERYWHERE!



HTTPS EVERYWHERE!

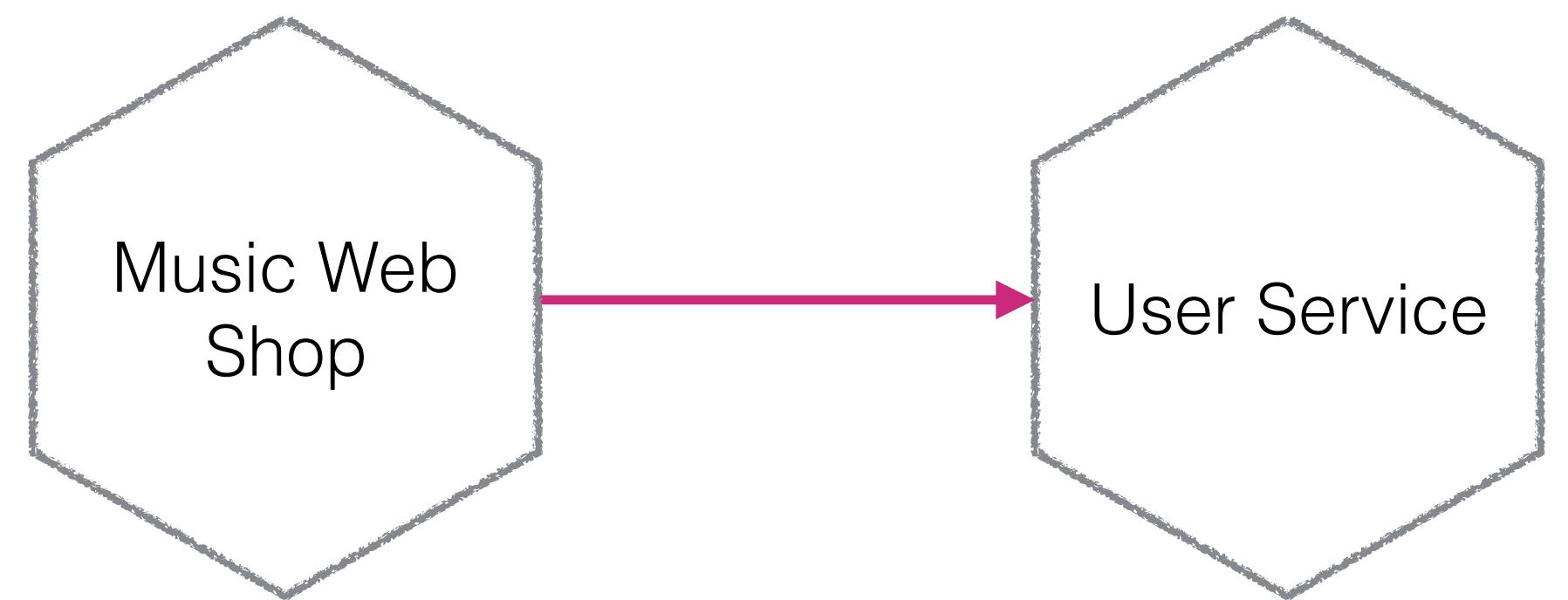


HTTPS EVERYWHERE!

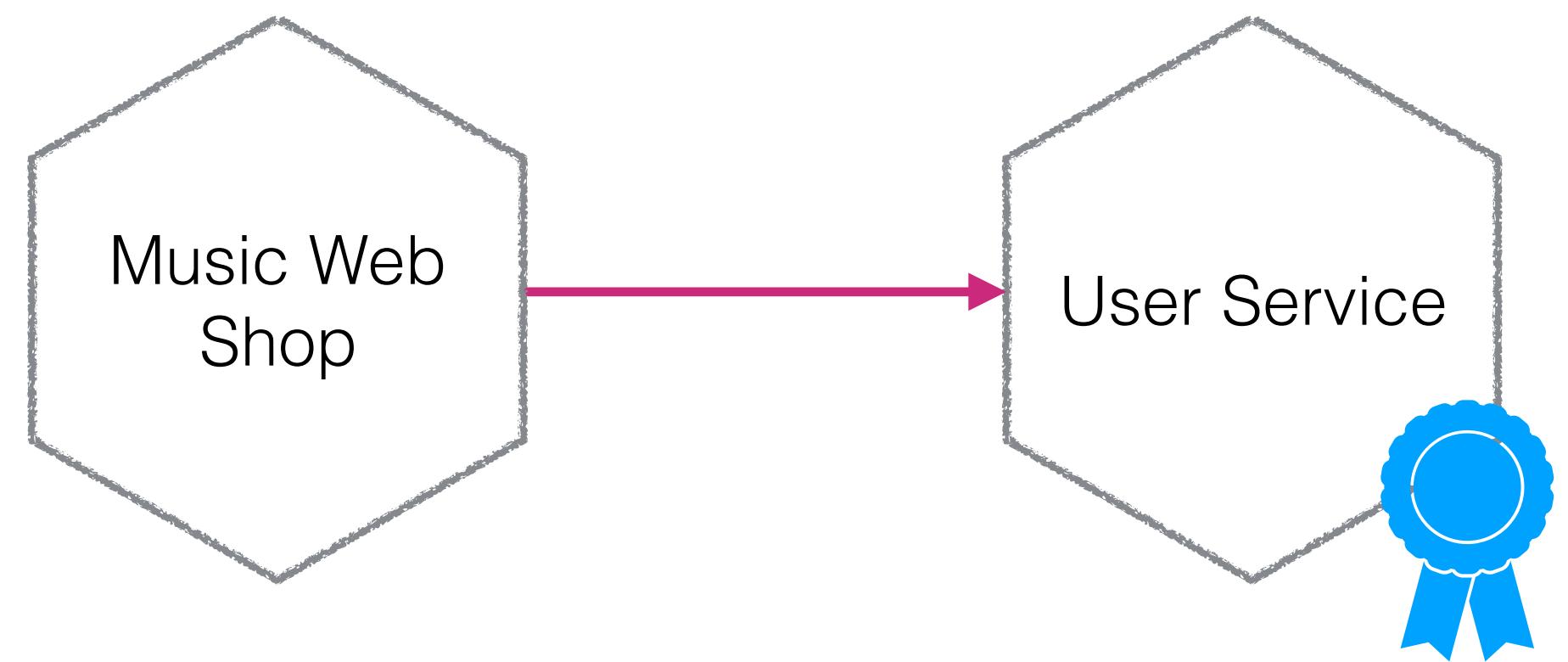


Mutual TLS

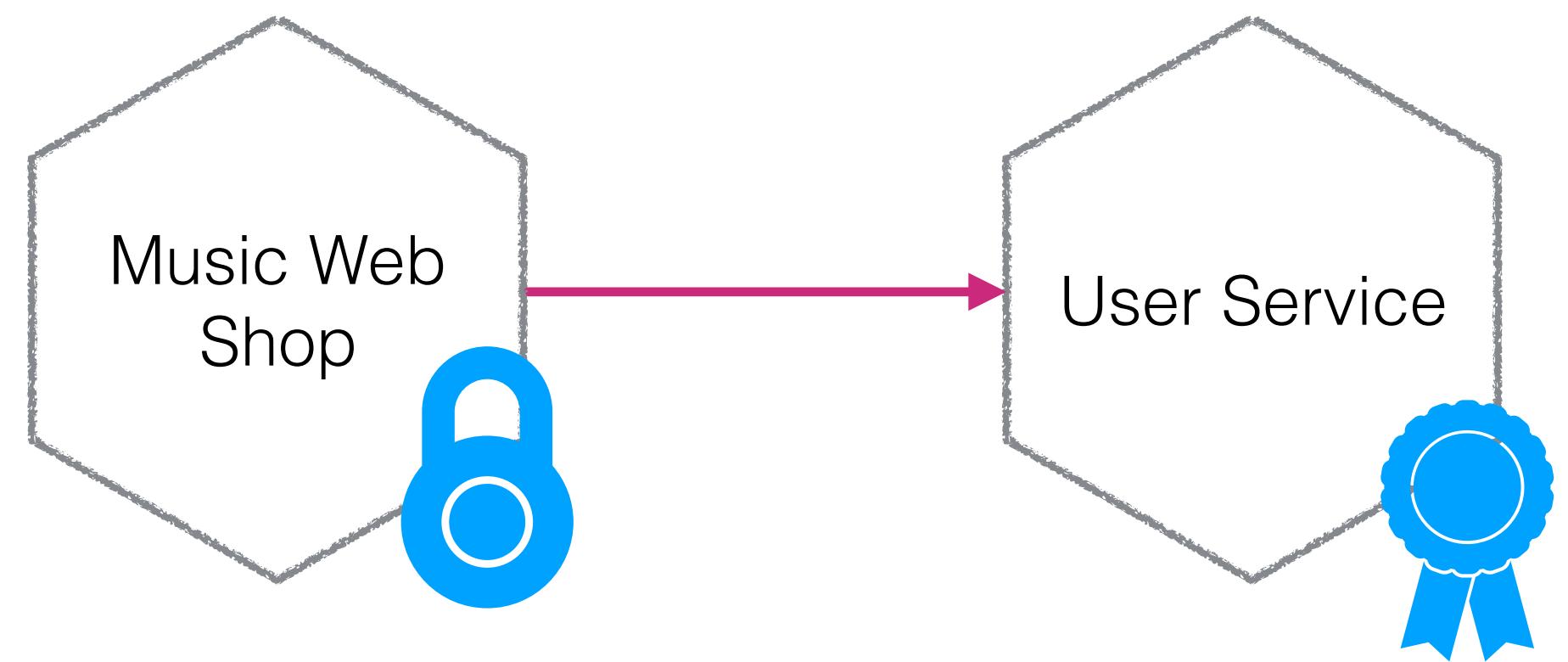
MUTUAL TLS



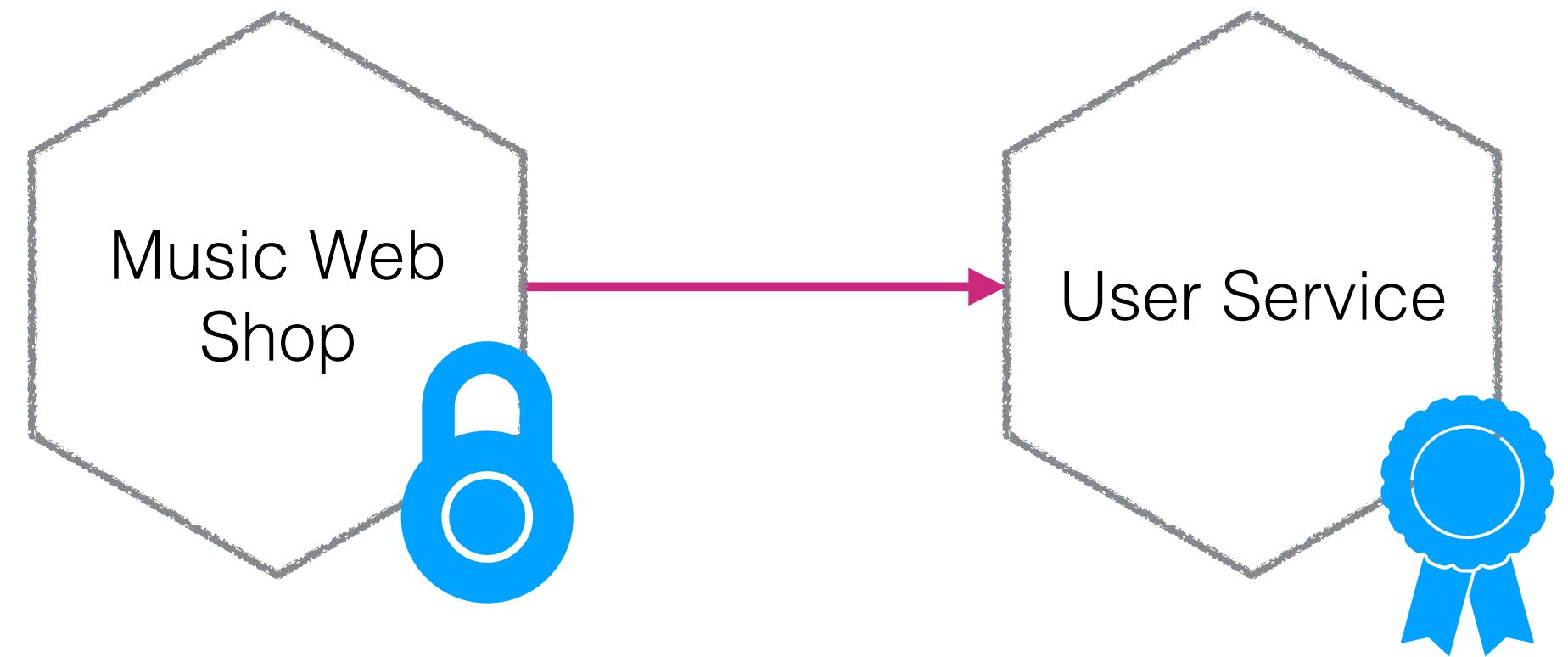
MUTUAL TLS



MUTUAL TLS

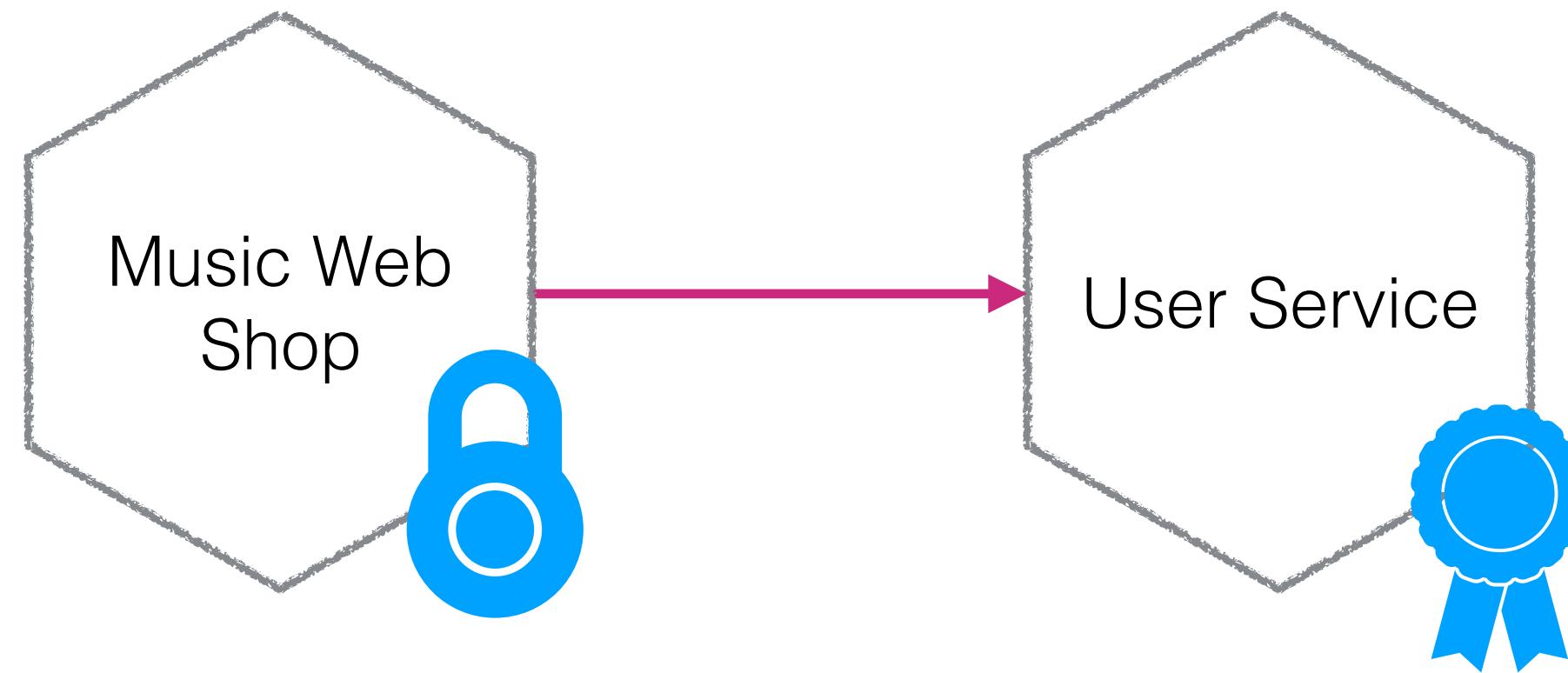


MUTUAL TLS



Client and server guarantees!

MUTUAL TLS



Client and server guarantees!

Certificate management is REALLY painful

AZURE - CLIENT-SIDE CERTIFICATE MANAGEMENT

How to secure back-end services using client certificate authentication in Azure API Management

By [Microsoft](#) • 4 minutes to read • Contributions

In this article

Prerequisites

Upload a client certificate

Delete a client certificate

Configure an API to use a client certificate for gateway authentication

Self-signed certificates

Next steps

API Management provides the capability to secure access to the back-end service of an API using client certificates. This guide shows how to manage certificates in the API publisher portal, and how to configure an API to use a certificate to access its back-end service.

For information about managing certificates using the API Management REST API, see [Azure API Management REST API Certificate API](#).

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-mutual-certificates>

AWS - CLIENT-SIDE CERTIFICATE MANAGEMENT

API Gateway & AWS API Gateway DevTools > Creating APIs > API Policies > Client-Side SSL Certificates for Authentication by the Backend

Use Client-Side SSL Certificates for Authentication by the Backend

You can use API Gateway to generate an SSL certificate and use its public key in the Backend to verify that all HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the endpoint is publicly accessible.

Note

Some backend servers may not support SSL client authentication as API Gateway does and could return an SSL certificate error. For a list of incompatible backend servers, see Known Issues.

The SSL certificates that are generated by API Gateway are self-signed and only the public key of a certificate is visible in the API Gateway console or through the API.

Topics

- Generate a Client Certificate Using the API Gateway Console
- Configure an API to Use SSL Certificates
- Topics
- Configure Backend to Authenticate API

<https://docs.aws.amazon.com/apigateway/latest/developerguide/getting-started-client-side-ssl-authentication.html>

MUTUAL TLS

Observation of data

Manipulation of data

Restricting access to endpoints

Impersonation of endpoints

MUTUAL TLS

✓ Observation of data

Manipulation of data

Restricting access to endpoints

Impersonation of endpoints

MUTUAL TLS

- ✓ Observation of data
- ✓ Manipulation of data

Restricting access to endpoints

Impersonation of endpoints

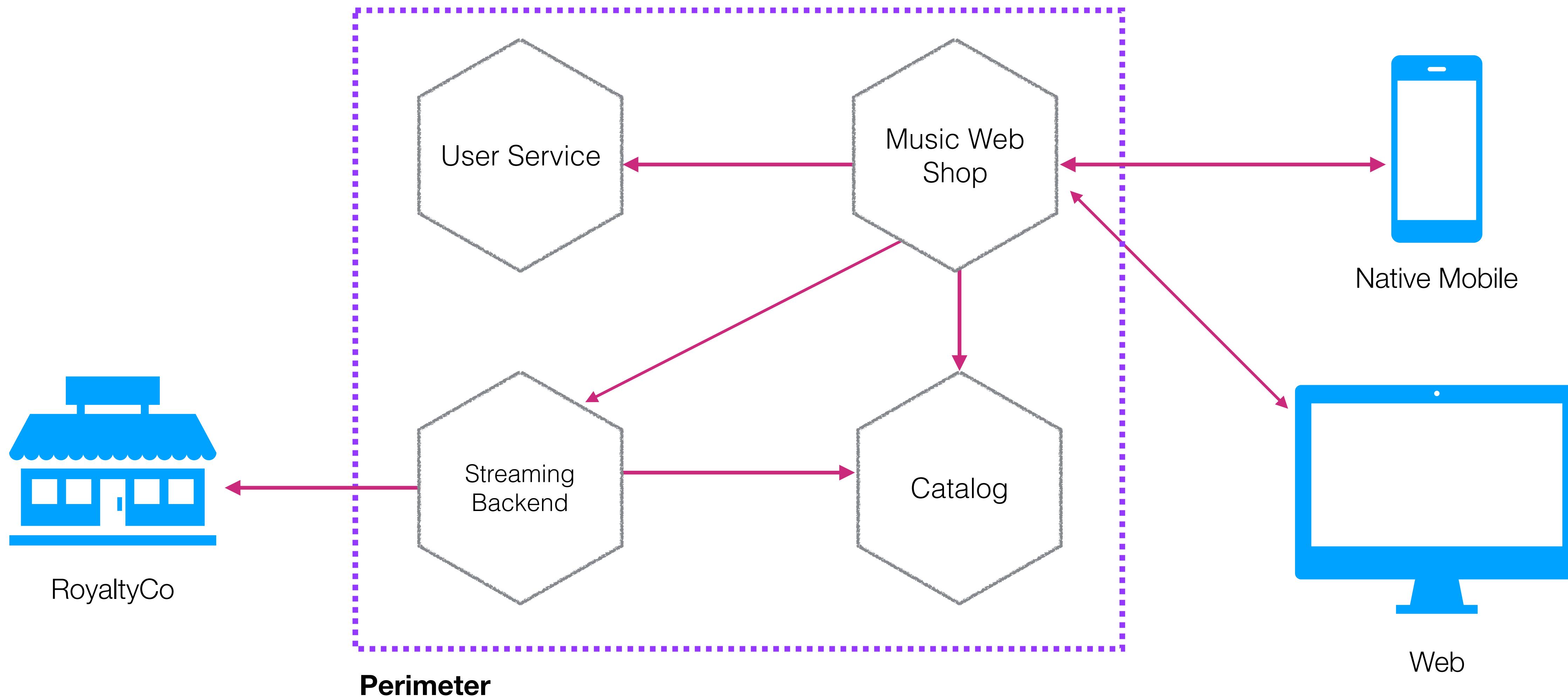
MUTUAL TLS

- ✓ Observation of data
 - ✓ Manipulation of data
 - ✓ Restricting access to endpoints
- Impersonation of endpoints

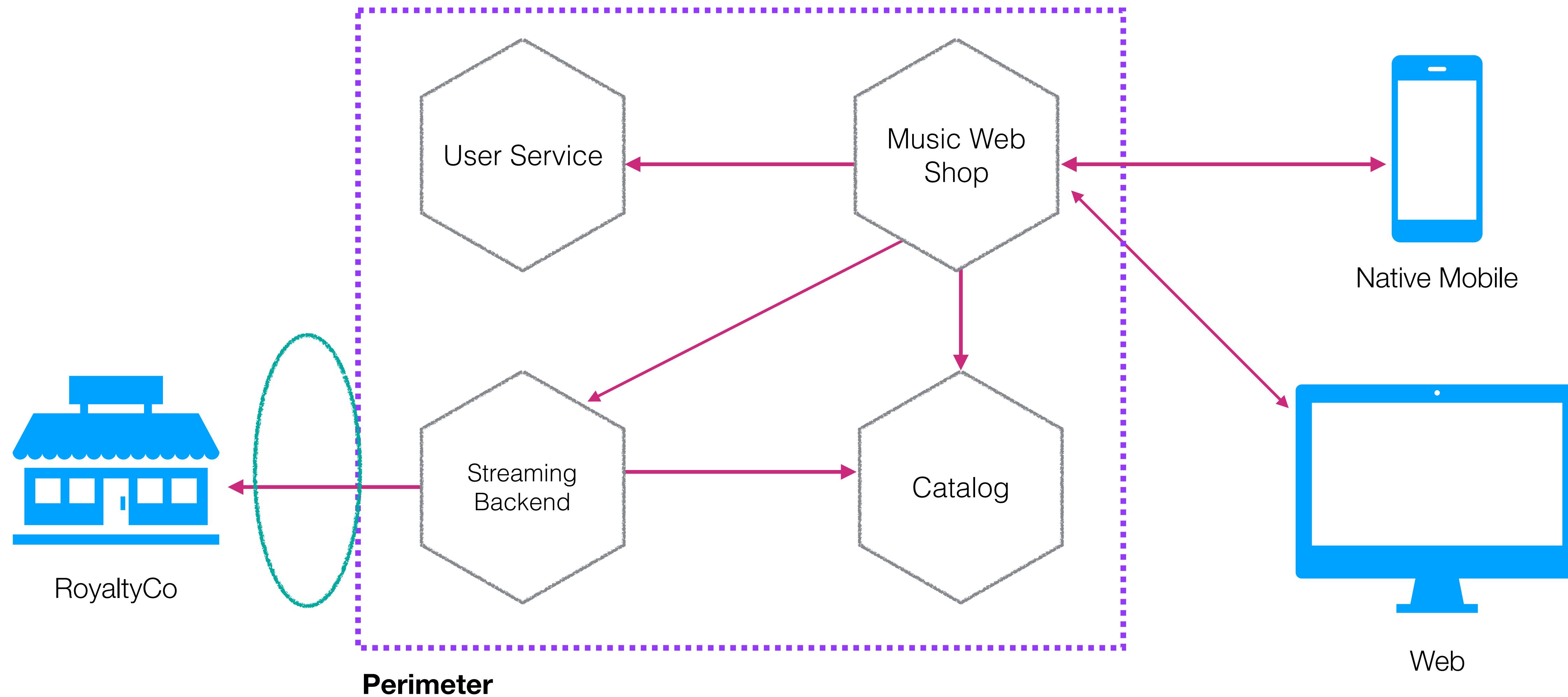
MUTUAL TLS

- ✓ Observation of data
- ✓ Manipulation of data
- ✓ Restricting access to endpoints
- ✓ Impersonation of endpoints

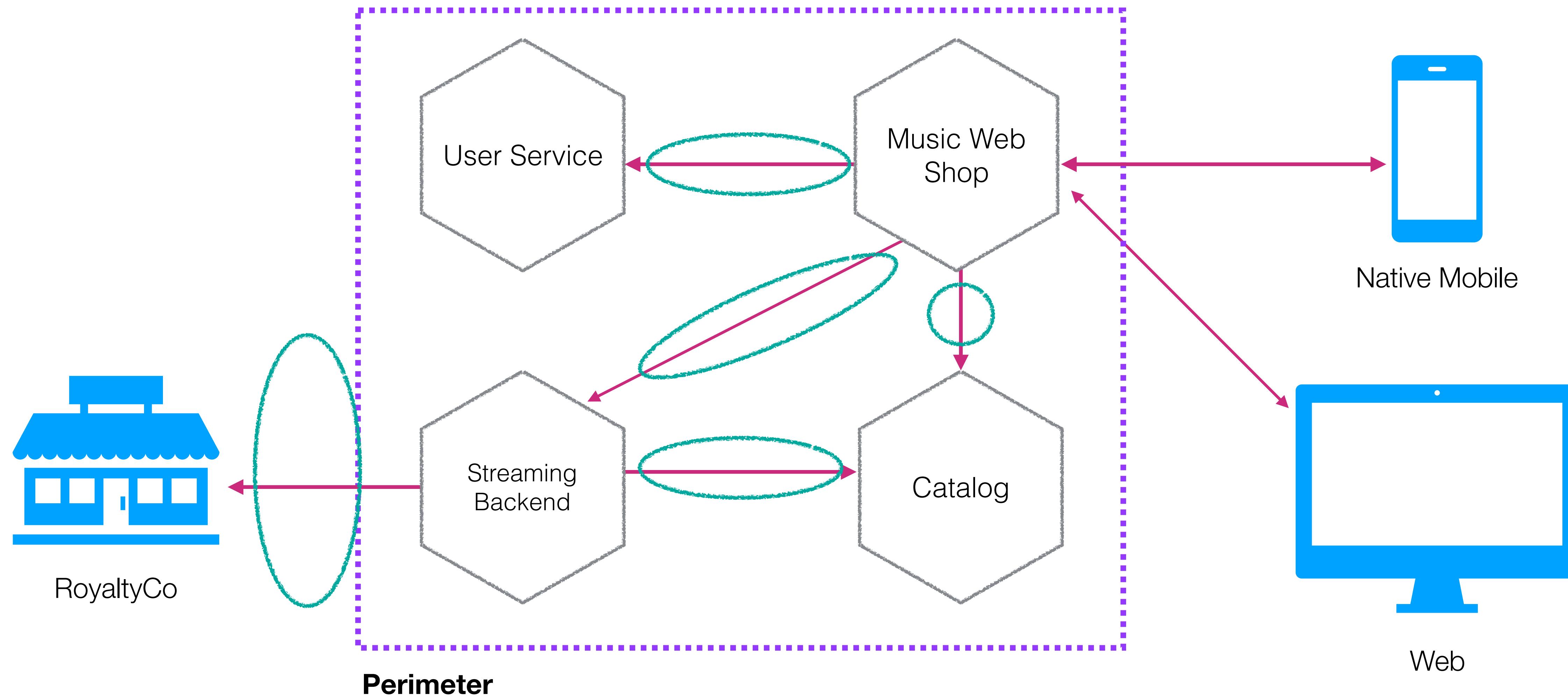
MUTUAL TLS



MUTUAL TLS



MUTUAL TLS



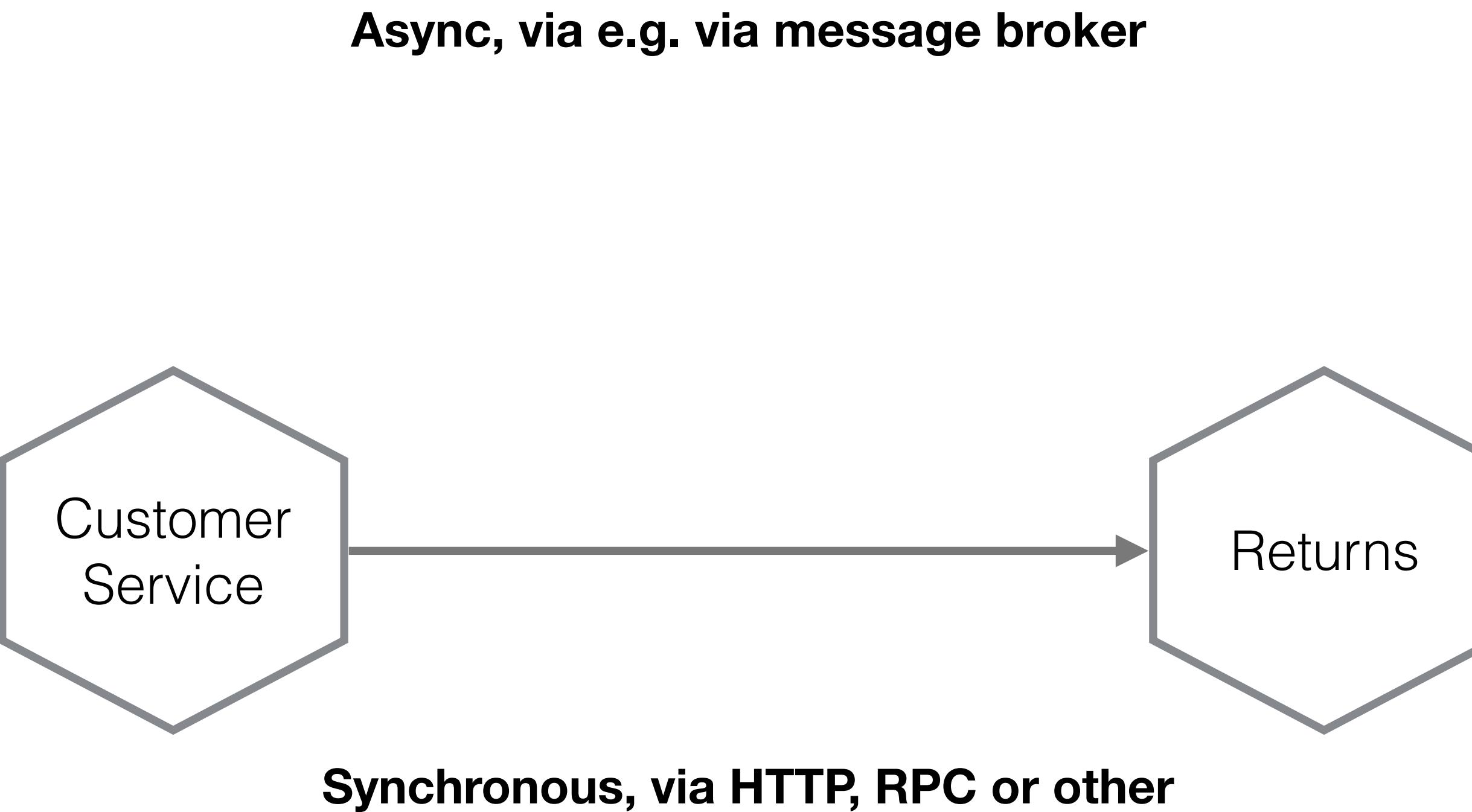
OTHER PROTOCOLS?



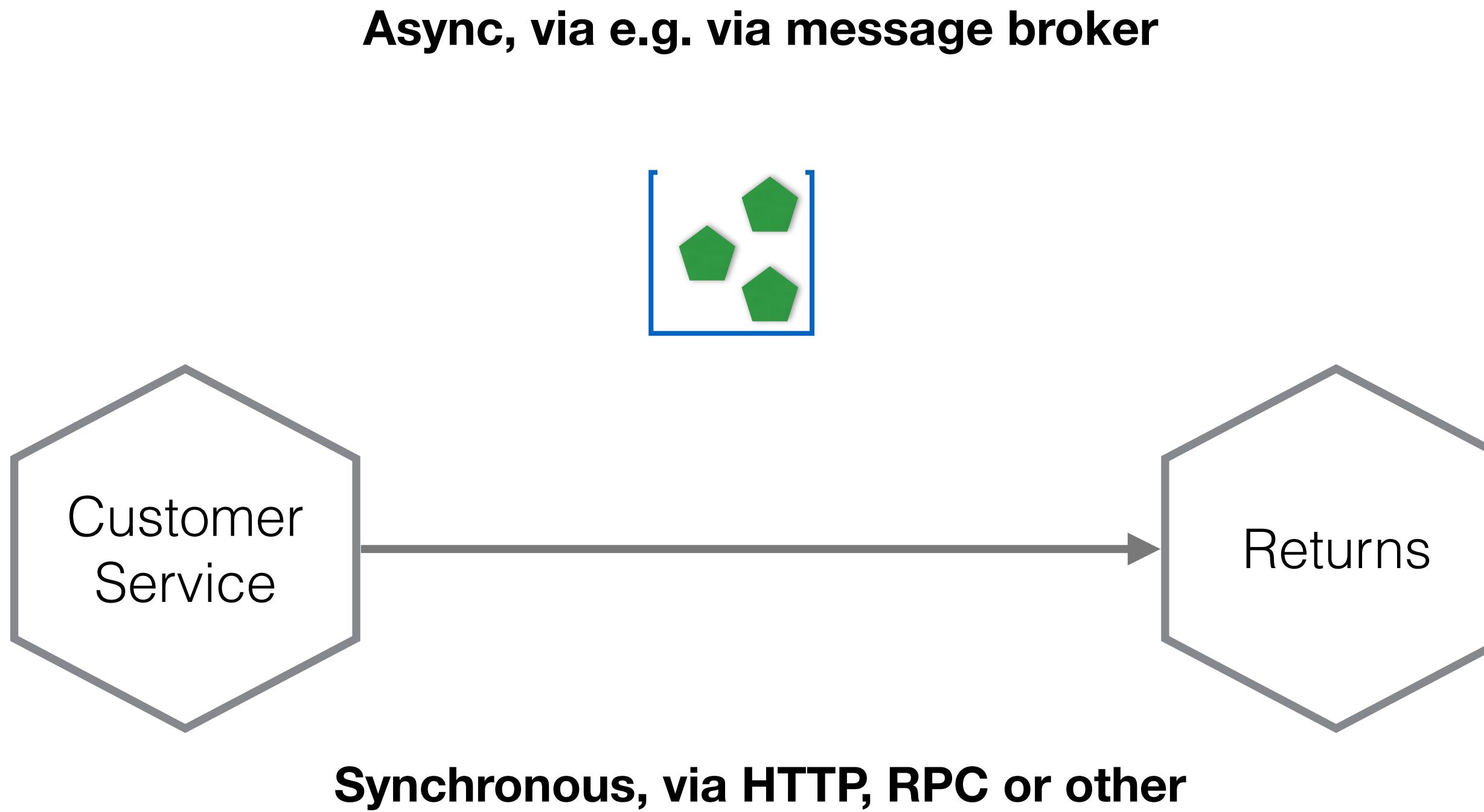
OTHER PROTOCOLS?



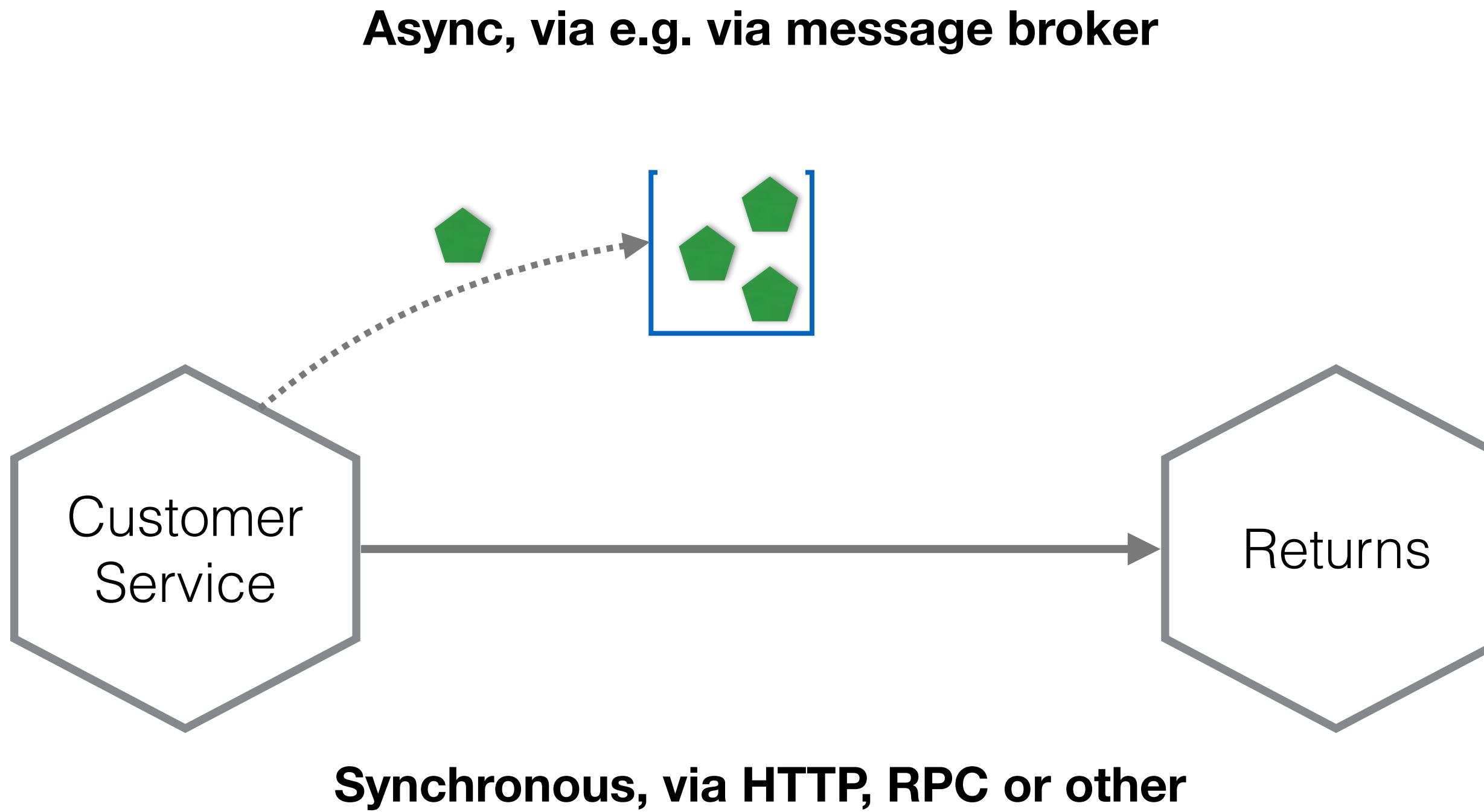
OTHER PROTOCOLS?



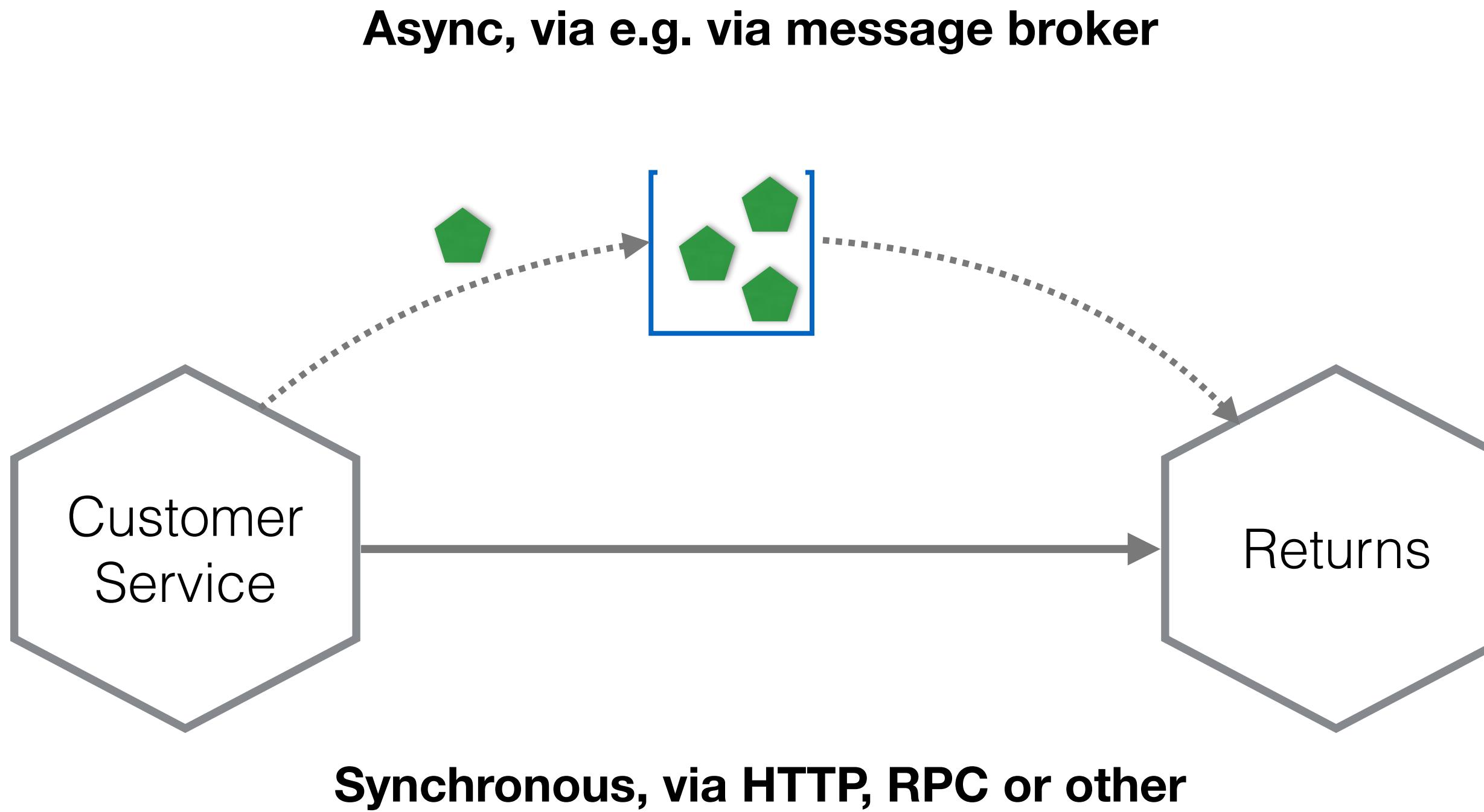
OTHER PROTOCOLS?



OTHER PROTOCOLS?



OTHER PROTOCOLS?



TLS Support

Introd.

RabbitMQ has built support for TLS. This includes client connections and popular plugins, where applicable, such as [Brokerage](#). It is also possible to use TLS to encrypt inter-node connections in clusters.

This guide covers various topics related to PLS in Rainbird M3.

Enabling TLS Interactions in BobbiNG

How to generate self-signed certificates for development and QA environments

TLS configuration in Java and MQTT clients

Börsenamt und Materialberichterstattung

TLS version and cipher suite configuration

Certificate chain validation depth

Topics that can be used to evaluate a TTS system

and phone. It is held, predominantly, as grants-in-aid by local authorities. Public sector information and related legislation, such as contracts, are contained very briefly. A number of long-term-oriented grants, with available elsewhere on the Web: www.oasb.org.

TLS Support

Intro

RabbitMQ has built support for TLS. This includes client connections and popular plugins, where applicable, such as [Brokerage](#). It is also possible to use TLS to [encrypt inter-node connections](#).

This guide covers various topics related to F1.S in Rainbird 4.0.

Enabling TLS Endpoints in RabbitMQ

How to generate self-signed certificates for development and QA environments

TLS configuration in Java and .NET clients

Börsenwerte und Materialien für den Betrieb eines Betriebswirtschaftlers

TLS version and cipher suite configuration

Certificate chain validation depth

Topic 3 Erlang/OTP Requirements for TLS Support

and micro-
biology. 1.
synthesis

In order to support TLS connections, RabbitMQ needs TLS and crypto-related modules to be available in the Erlang/OTP installation. The recommended Erlang/OTP version to use with TLS is the most recent [supported Erlang release](#). Earlier versions, even if they are supported, may work for most certificates but have known limitations (see below).

TLS Support

Intro

RabbitMQ has built support for TLS. This includes client connections and popular plugins, where applicable, such as [Federation Broker](#). It is also possible to use TLS-to-[SSL/TLS inter-node connections in clusters](#).

This guide covers various topics related to TLS in RabbitMQ:

Enabling TLS listeners in RabbitMQ

How to generate self-signed certificates for development and QA environments

TLS configuration in Java and .NET clients

Known vulnerabilities and their mitigation

TLS version and cipher suite configuration

Certificate chain validation depth

Topics

Erlang/OTP Requirements for TLS Support

and more
topics, see
available

In order to support TLS connections, RabbitMQ needs TLS and crypto-related modules to be available in the Erlang/OTP installation. The recommended Erlang/OTP version to use with TLS is the most recent [supported Erlang release](#). Earlier versions, even if they are supported, may work for most certificates but have known limitations (see below).

Access Control (Authentication, Authorisation) in RabbitMQ

This document describes authentication and authorisation machinery that implements access control. Authentication mechanisms should not be confused with [authorization mechanisms](#) in AMQP 0-9-1.

A separate guide covers multiple topics around [access controls](#). It is only applicable to the internal authorisation feature.

Terminology and Definitions

Authentication and authorization are often conflated or used interchangeably. That's wrong and in RabbitMQ, the two are separated. For the sake of simplicity, we'll define authentication as "identifying who the user is" and authorization as "determining what the user is and isn't allowed to do".

Default Virtual Host and User

When the server first starts running, and detects that its database is uninitialised or has been renamed, it initializes a fresh database with the following resources:

TLS, Kerberos, SASL, and Authorizer in Apache Kafka 0.9 – Enabling New Encryption, Authorization, and Authentication Features

[Apache Kafka](#) is frequently used to store on-the-fly data making it one of the most important components of a company's data infrastructure. Our goal is to make it possible to run Kafka as a central platform for streaming data, supporting anything from a single user to a whole company. Multi-tenancy is an essential requirement in achieving this vision and, in turn, security features are crucial for multi-tenancy.

Previous to 0.9, Kafka had no built-in security features. One could lock down access at the network level but this is not viable for a big shared multi-tenant cluster being used across a large company. Consequently securing Kafka has been one of the most requested features. Security is of particular importance in today's world where cyber-attacks are a common occurrence and the threat of data breaches is a reality for businesses of all sizes, and at all levels from individual users to whole government entities.

Four key security features were added in [Apache Kafka 0.9](#), which is included in the [Confluent Platform 2.0](#):

TLS, Kerberos, SASL, and Authorizer in Apache Kafka 0.9 – Enabling New Encryption, Authorization, and Authentication Features

Apache Kafka is frequently used to store a company's data infrastructure. Our goal is supporting anything from a single node to this vision and, in turn, security features are

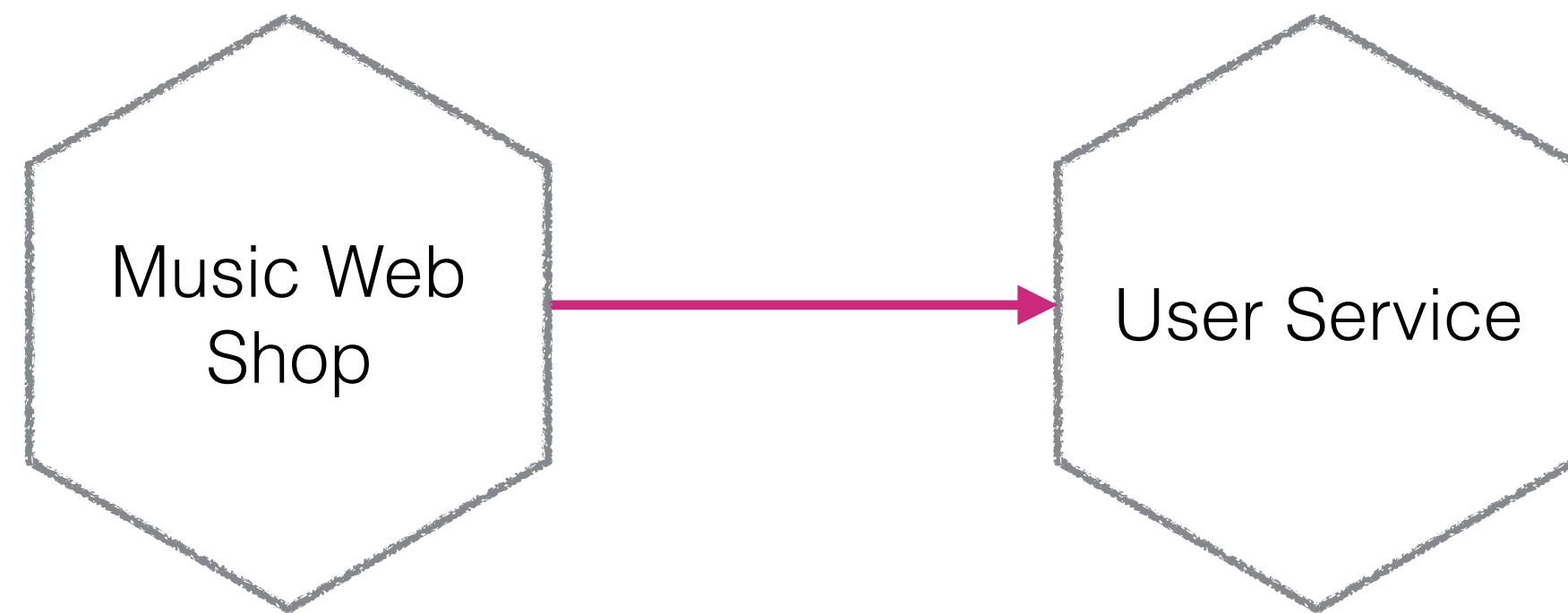
Previous to 0.9, Kafka had no built-in security visible for a big shared multi-tenant cluster. This has been one of the most requested features; attacks are a common occurrence and the levels from individual users to whole organization.

Four key security features were added in [Apache Kafka 0.9](#), which is included in the [Confluent Platform 2.0](#):

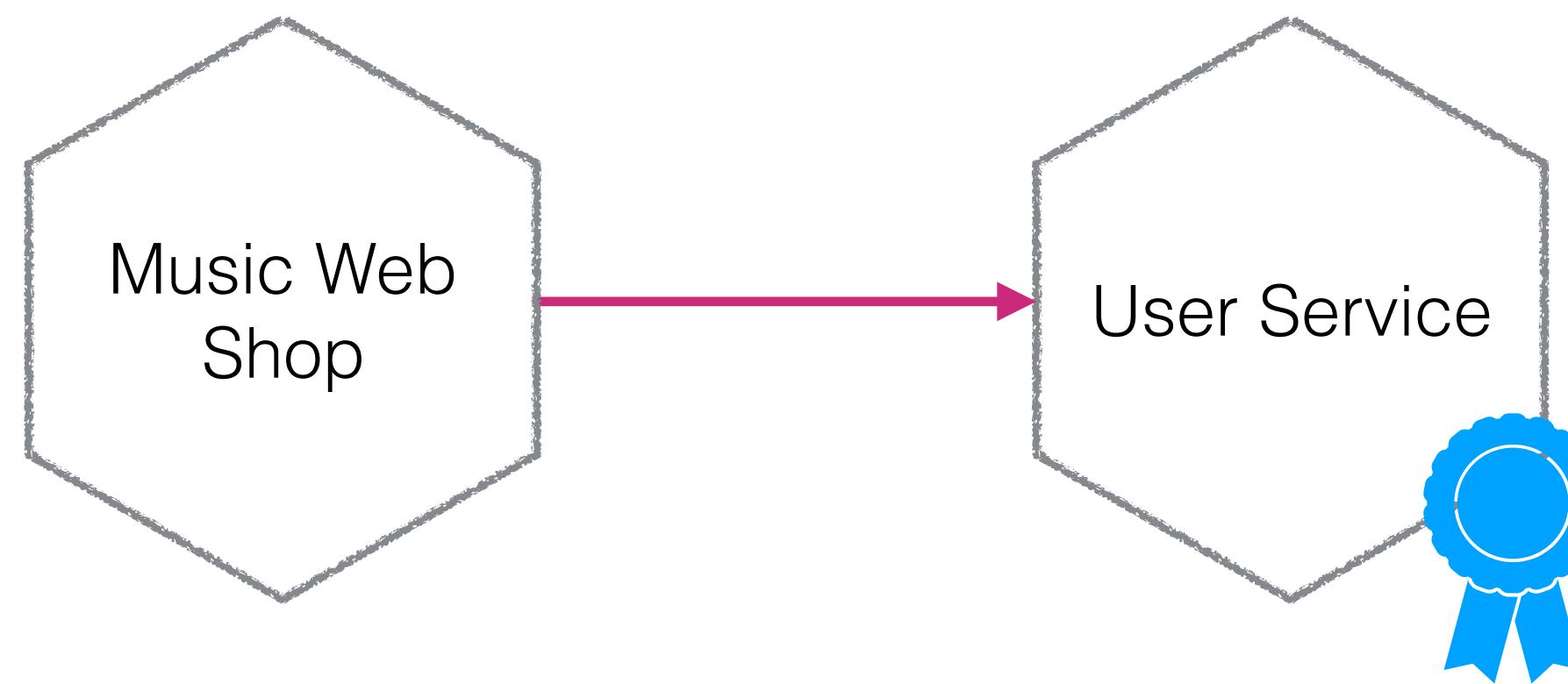
1. Administrators can require client authentication using either Kerberos or Transport Layer Security (TLS) client certificates, so that Kafka brokers know who is making each request.
2. A Unix-like permissions system can be used to control which users can access which data.
3. Network communication can be encrypted, allowing messages to be securely sent across untrusted networks.
4. Administrators can require authentication for communication between Kafka brokers and ZooKeeper.

Four key security features were added in [Apache Kafka 0.9](#), which is included in the [Confluent Platform 2.0](#):

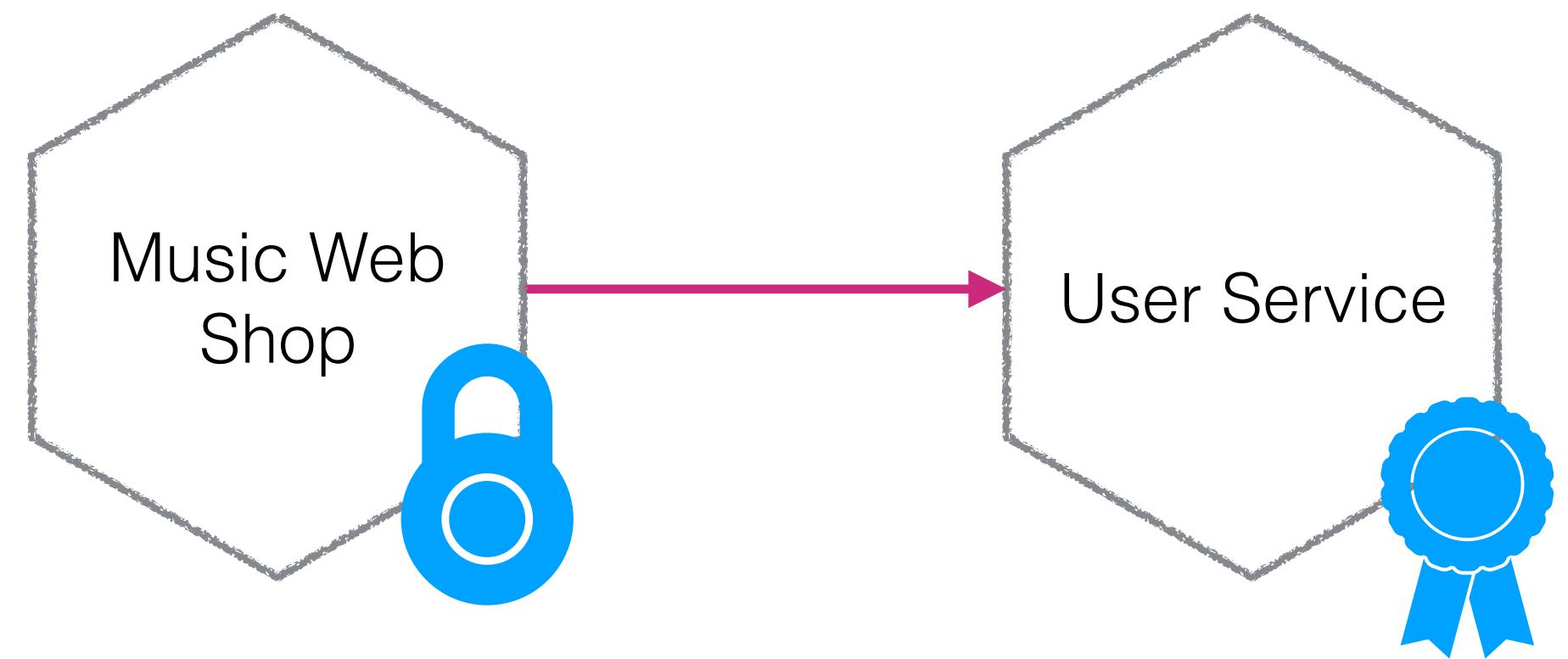
TRANSPORT AUTHENTICATION



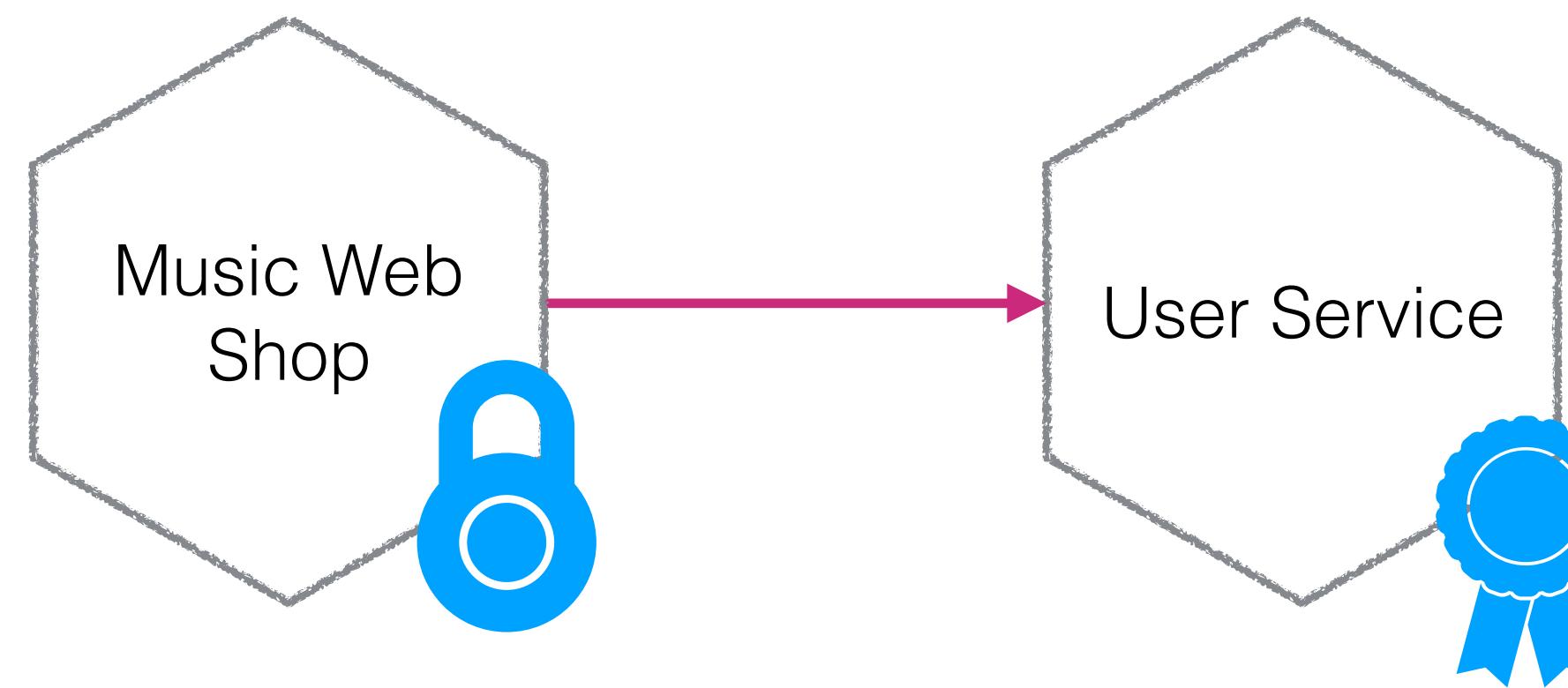
TRANSPORT AUTHENTICATION



TRANSPORT AUTHENTICATION

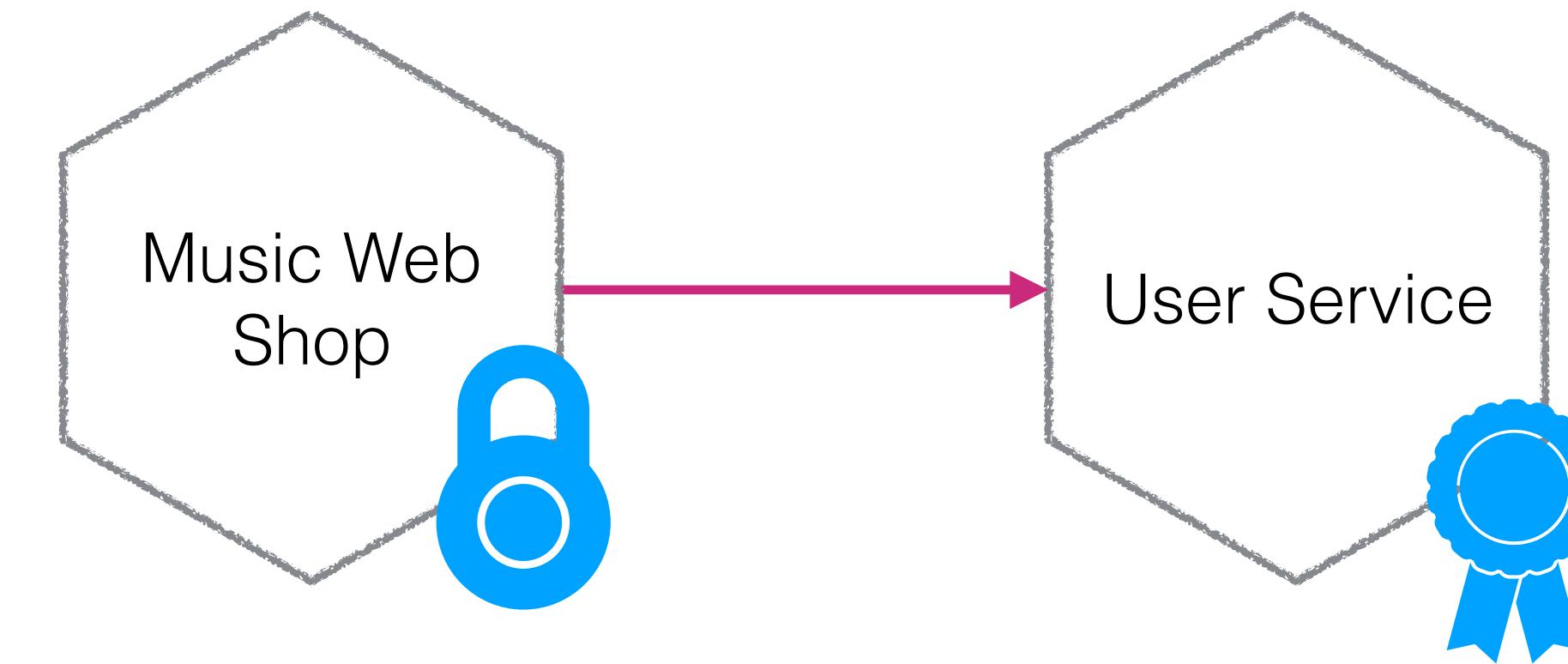


TRANSPORT AUTHENTICATION



Server-side identity

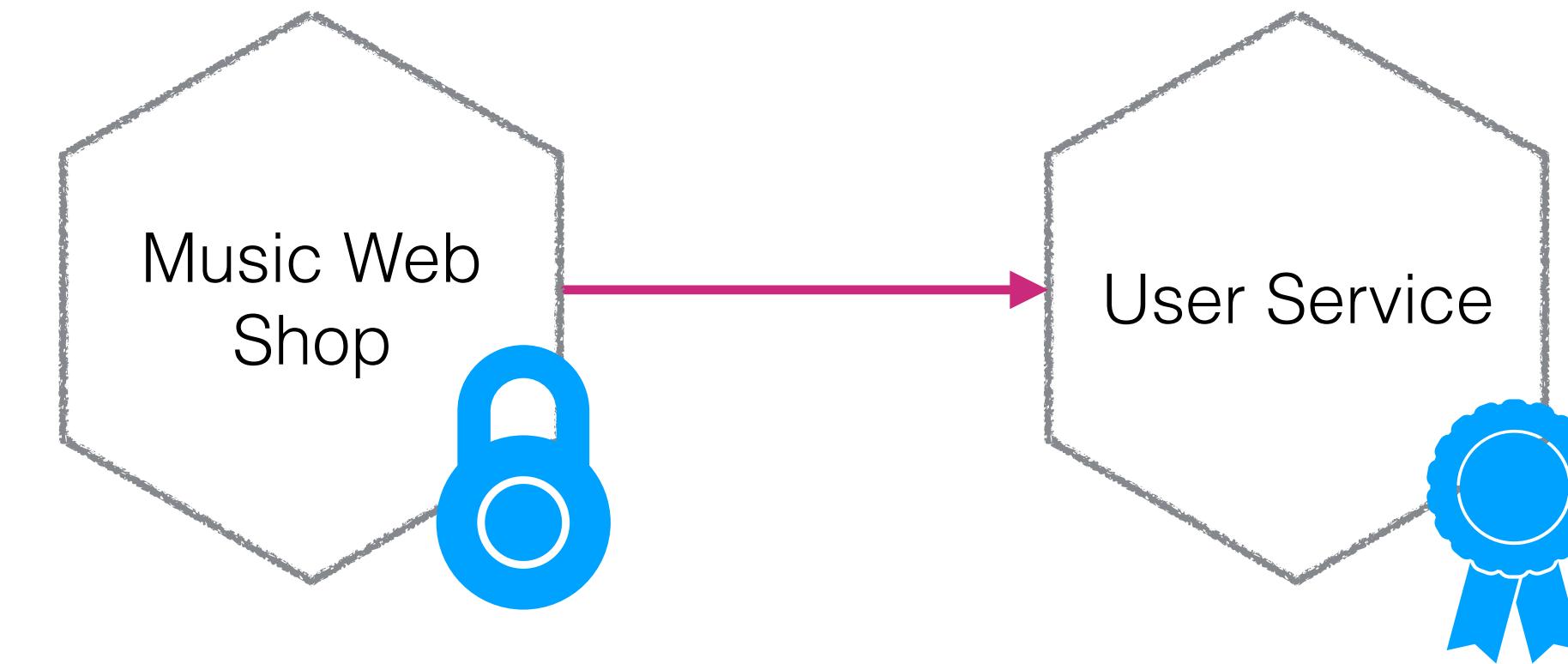
TRANSPORT AUTHENTICATION



Client-side identity

Server-side identity

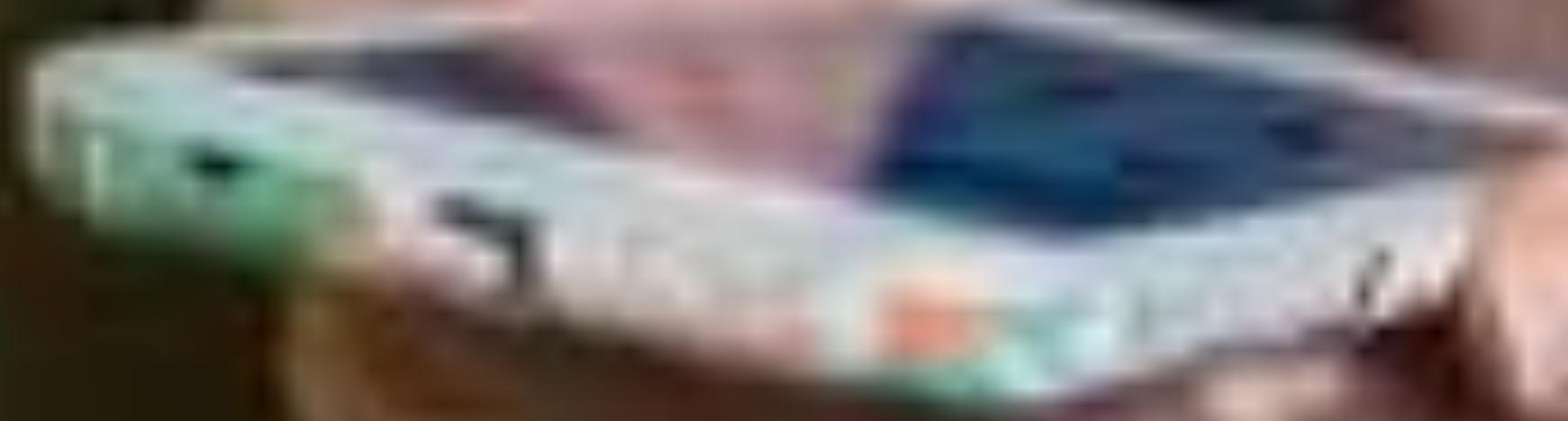
TRANSPORT AUTHENTICATION



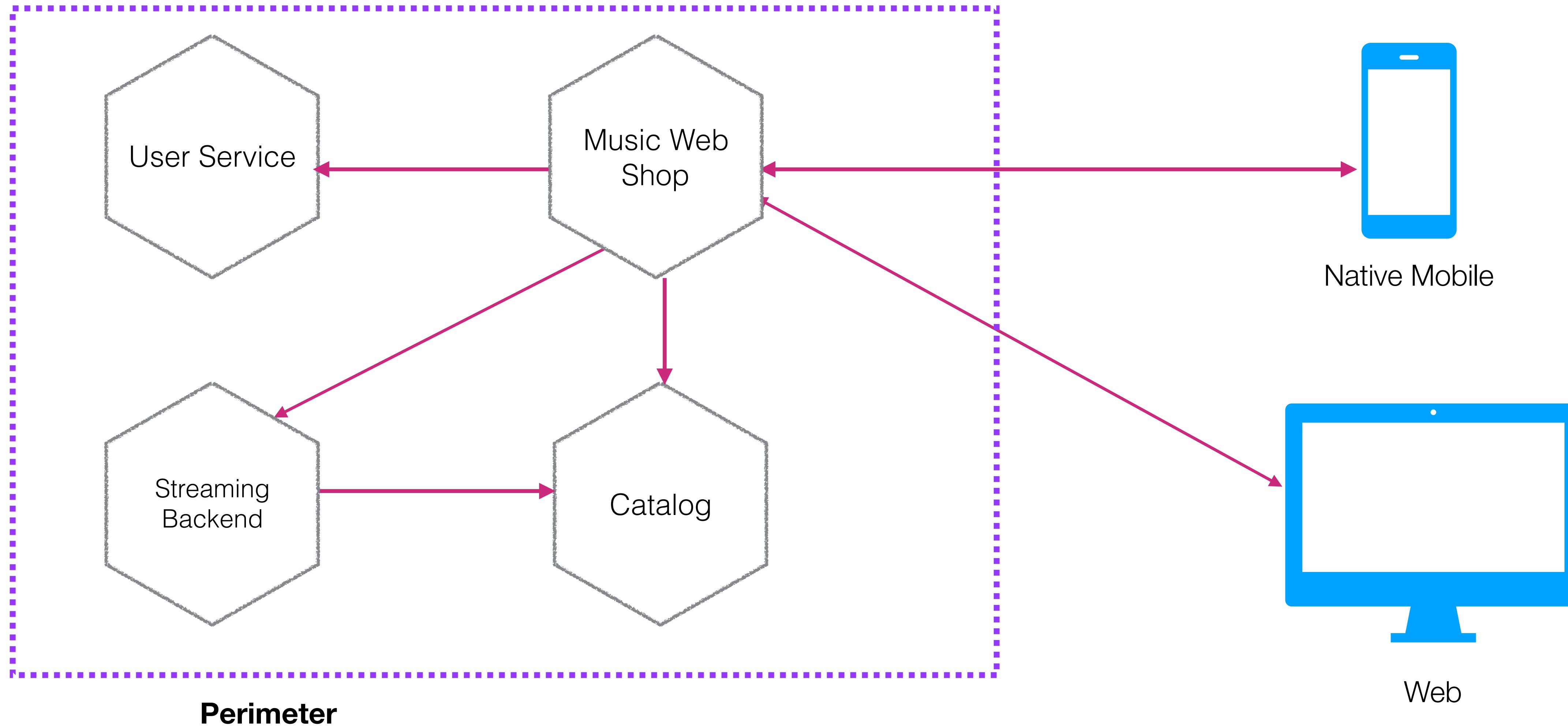
Client-side identity

Server-side identity

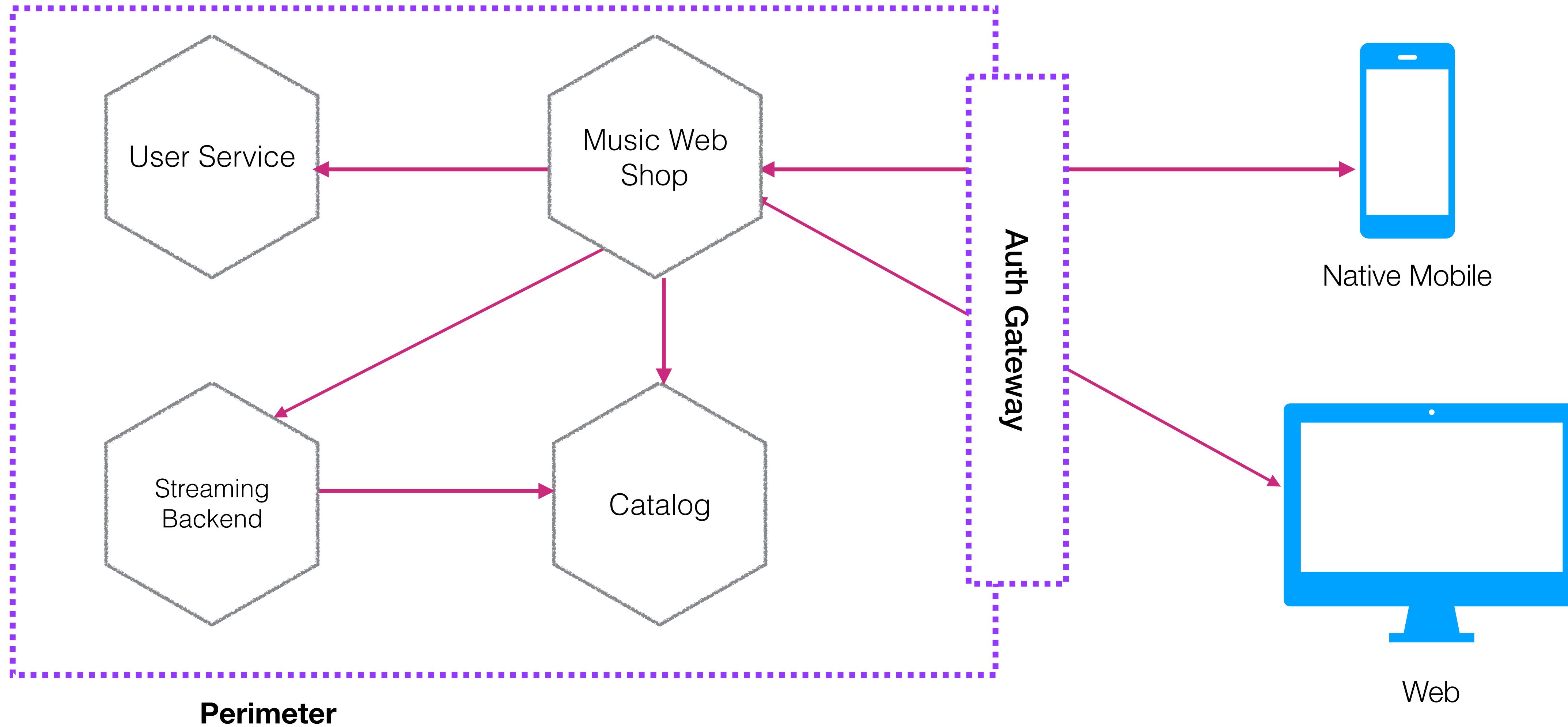
= service-to-service authentication



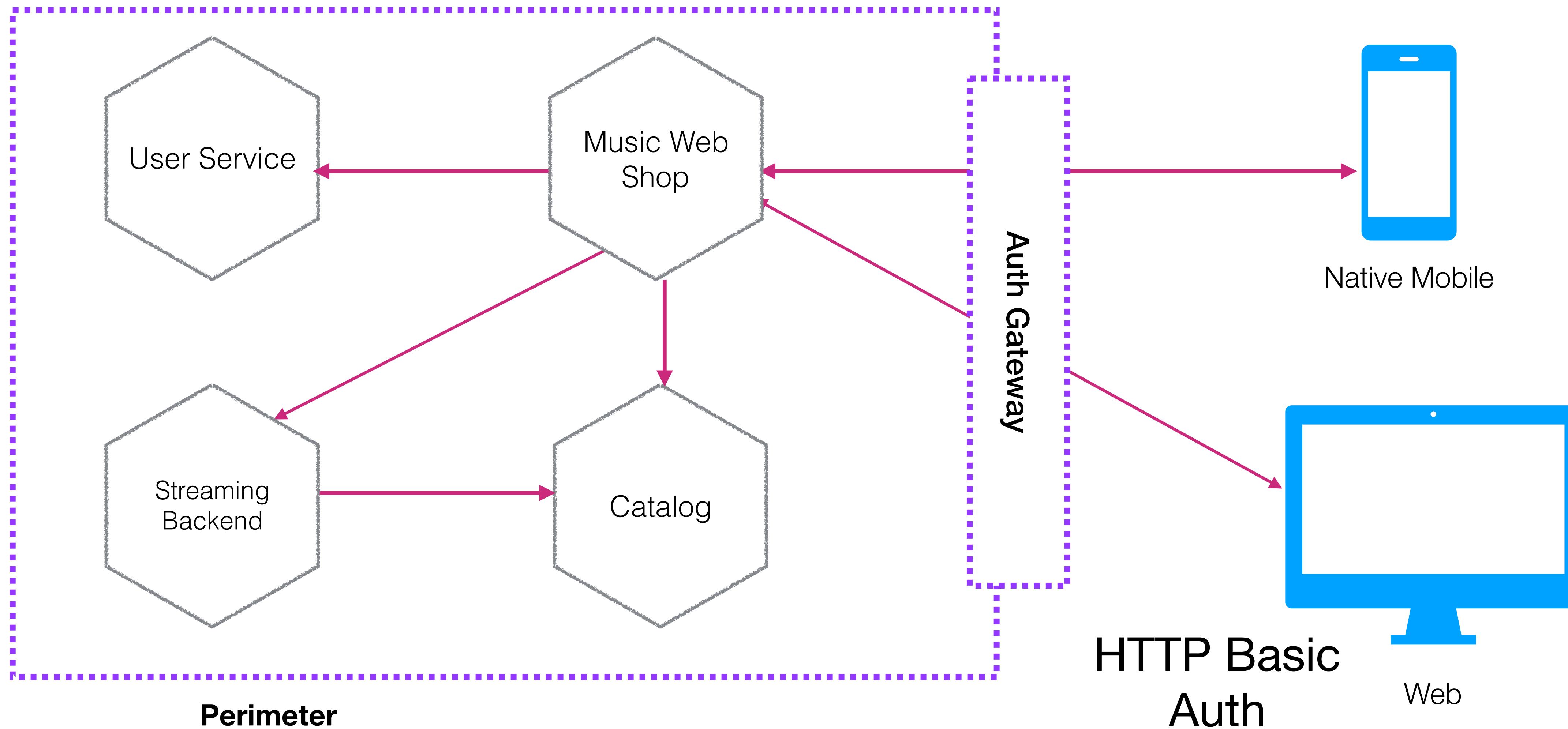
USER AUTHENTICATION - PROXY-BASED



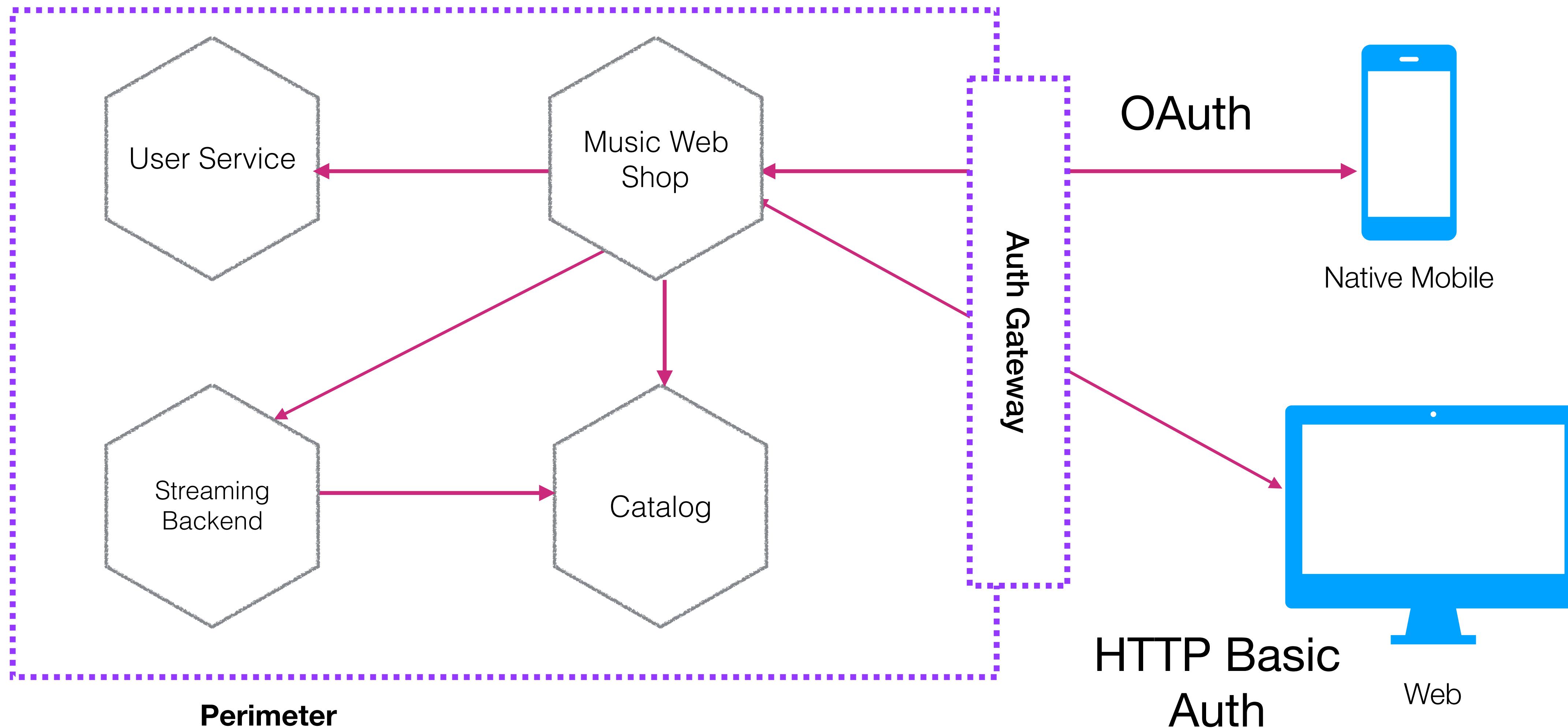
USER AUTHENTICATION - PROXY-BASED



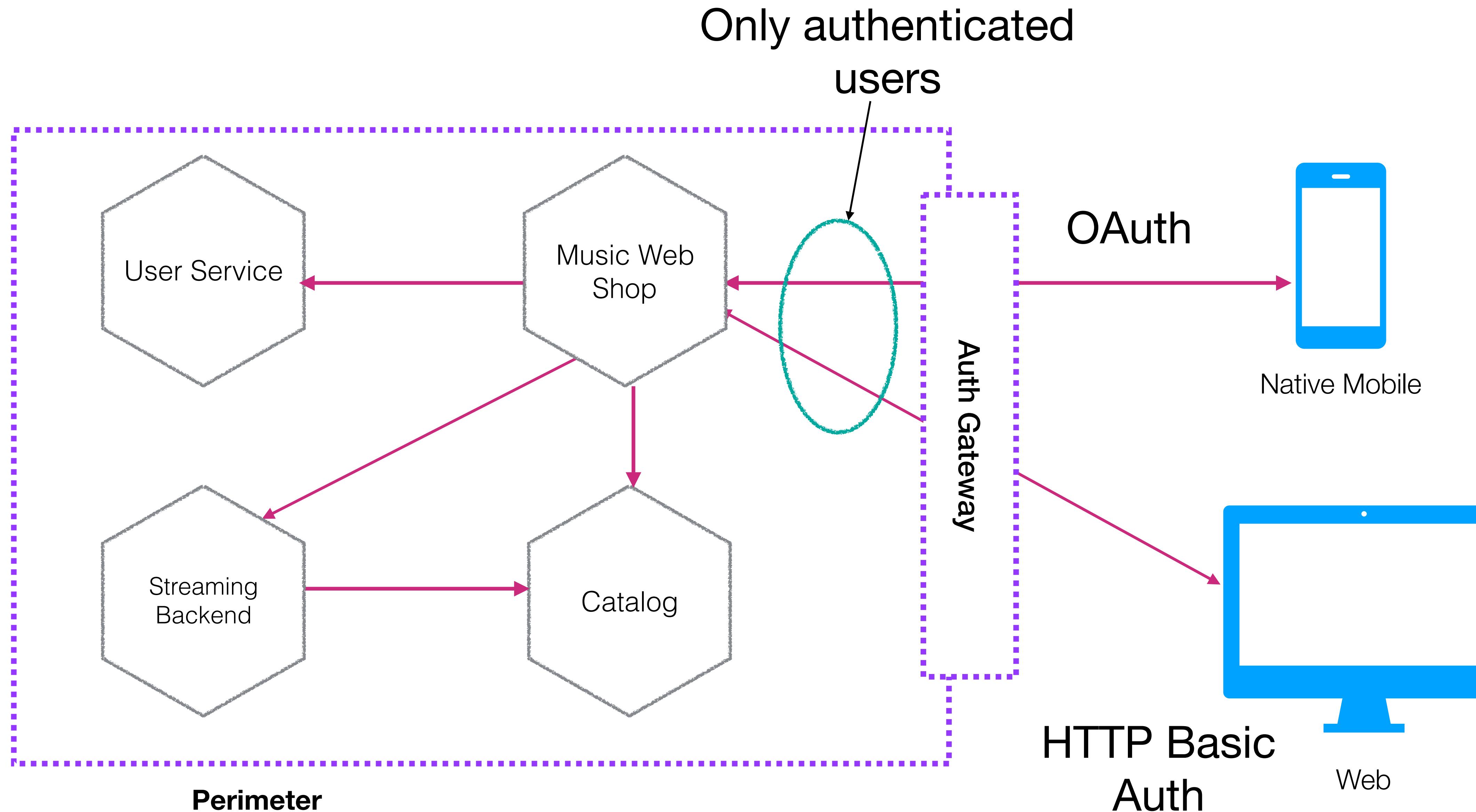
USER AUTHENTICATION - PROXY-BASED



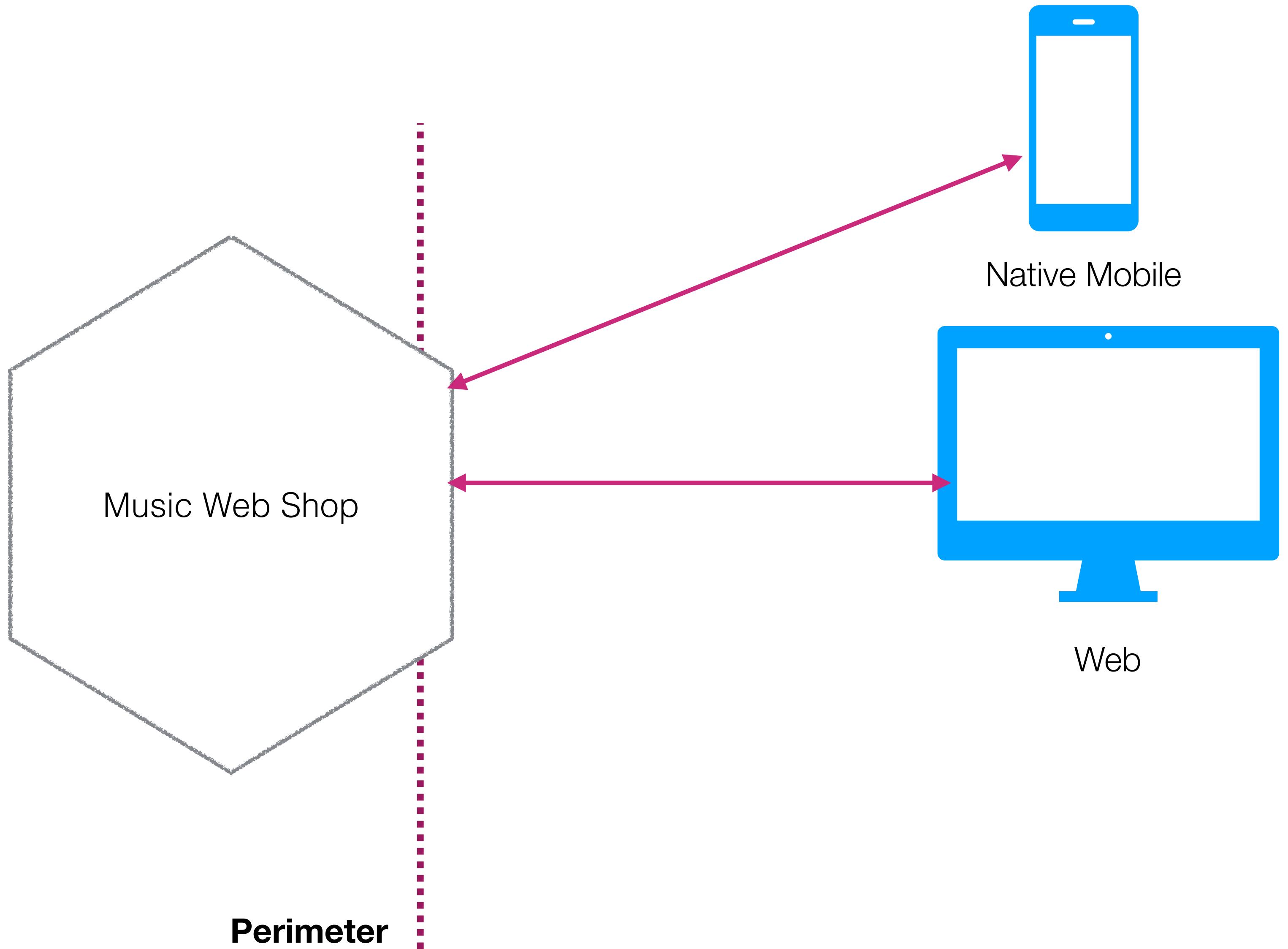
USER AUTHENTICATION - PROXY-BASED



USER AUTHENTICATION - PROXY-BASED

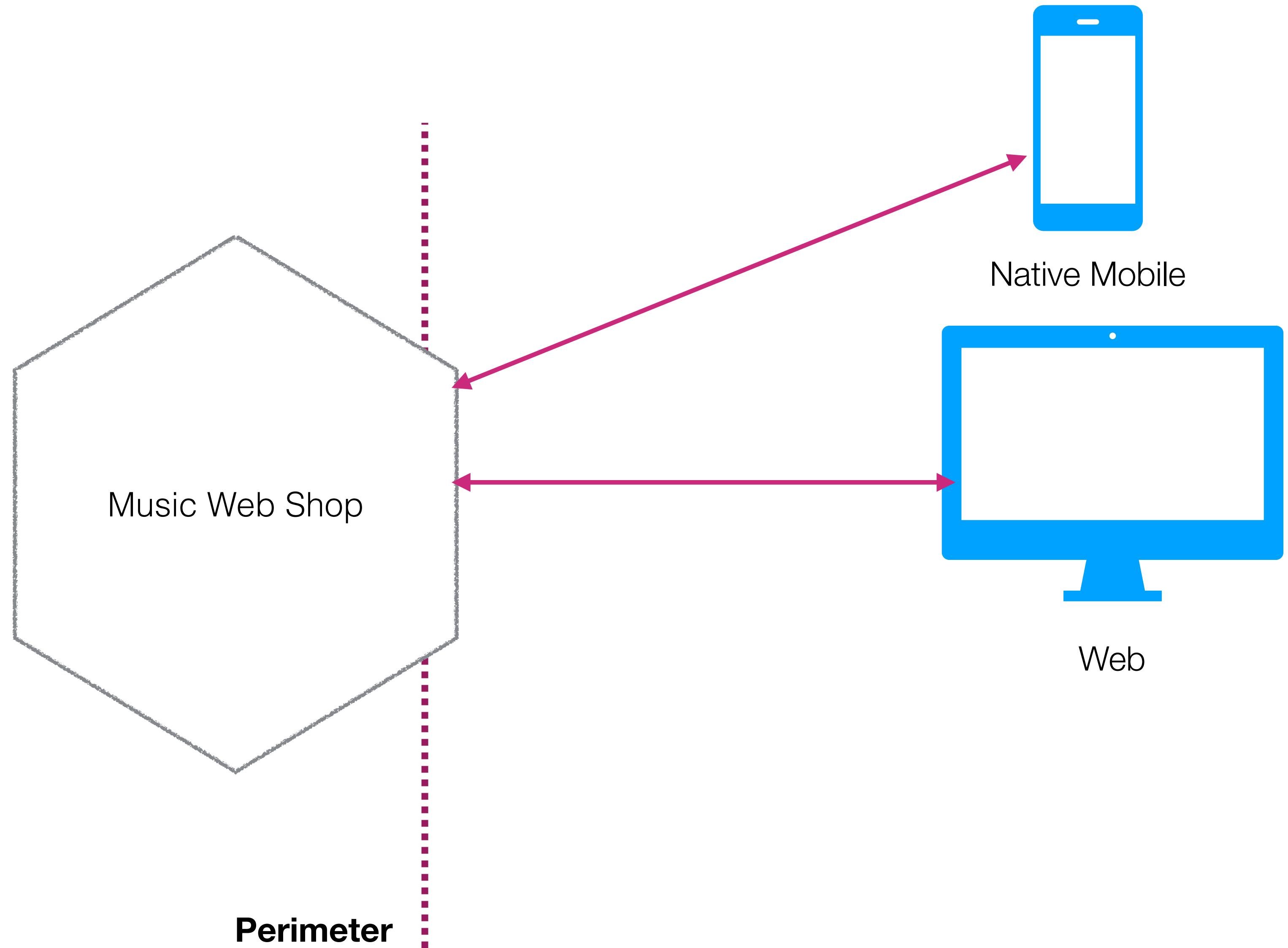


USER AUTHENTICATION - HANDLED IN SERVICE



USER AUTHENTICATION - HANDLED IN SERVICE

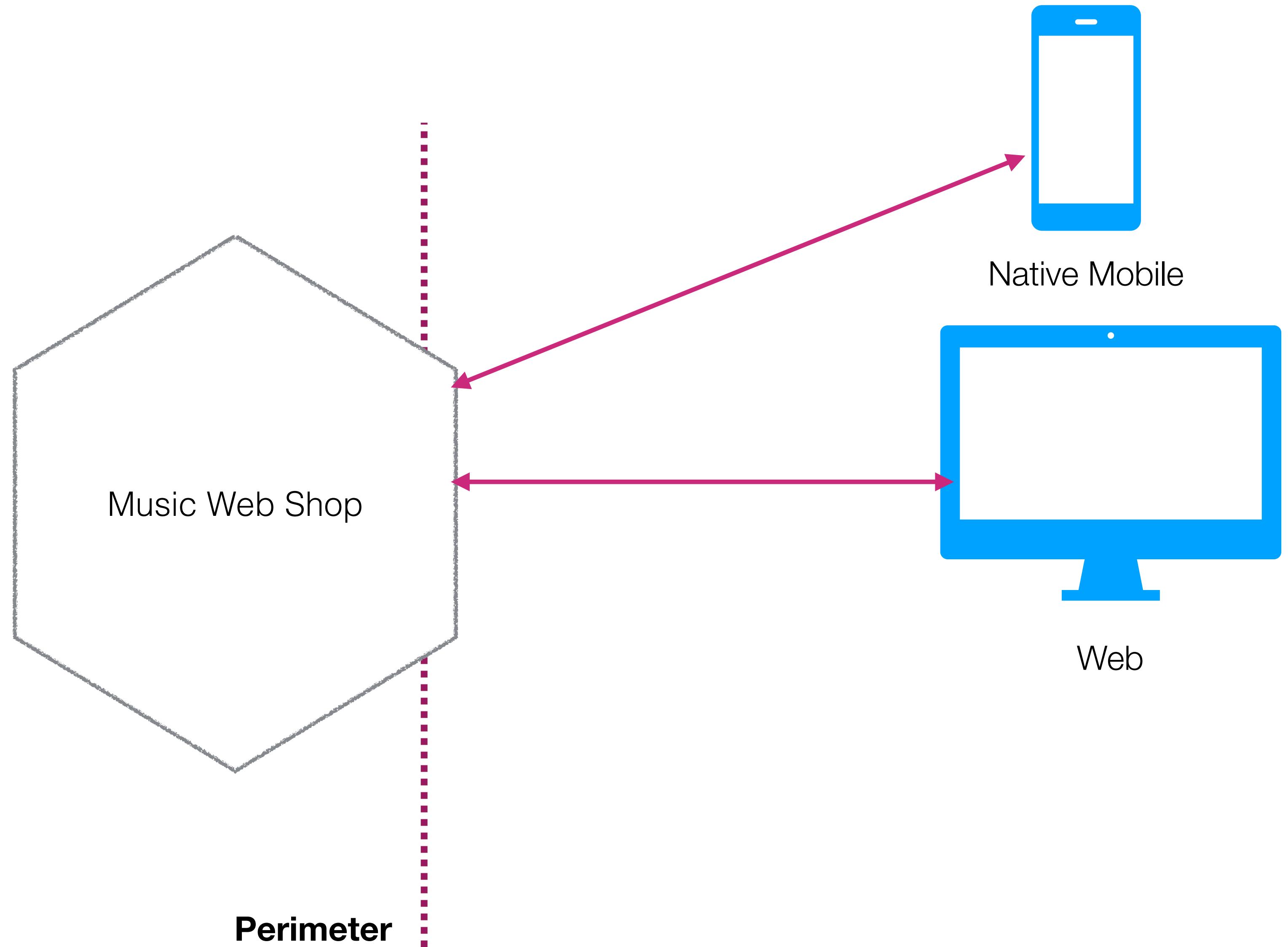
Can reduce latency



USER AUTHENTICATION - HANDLED IN SERVICE

Can reduce latency

Service potentially exposed to public internet

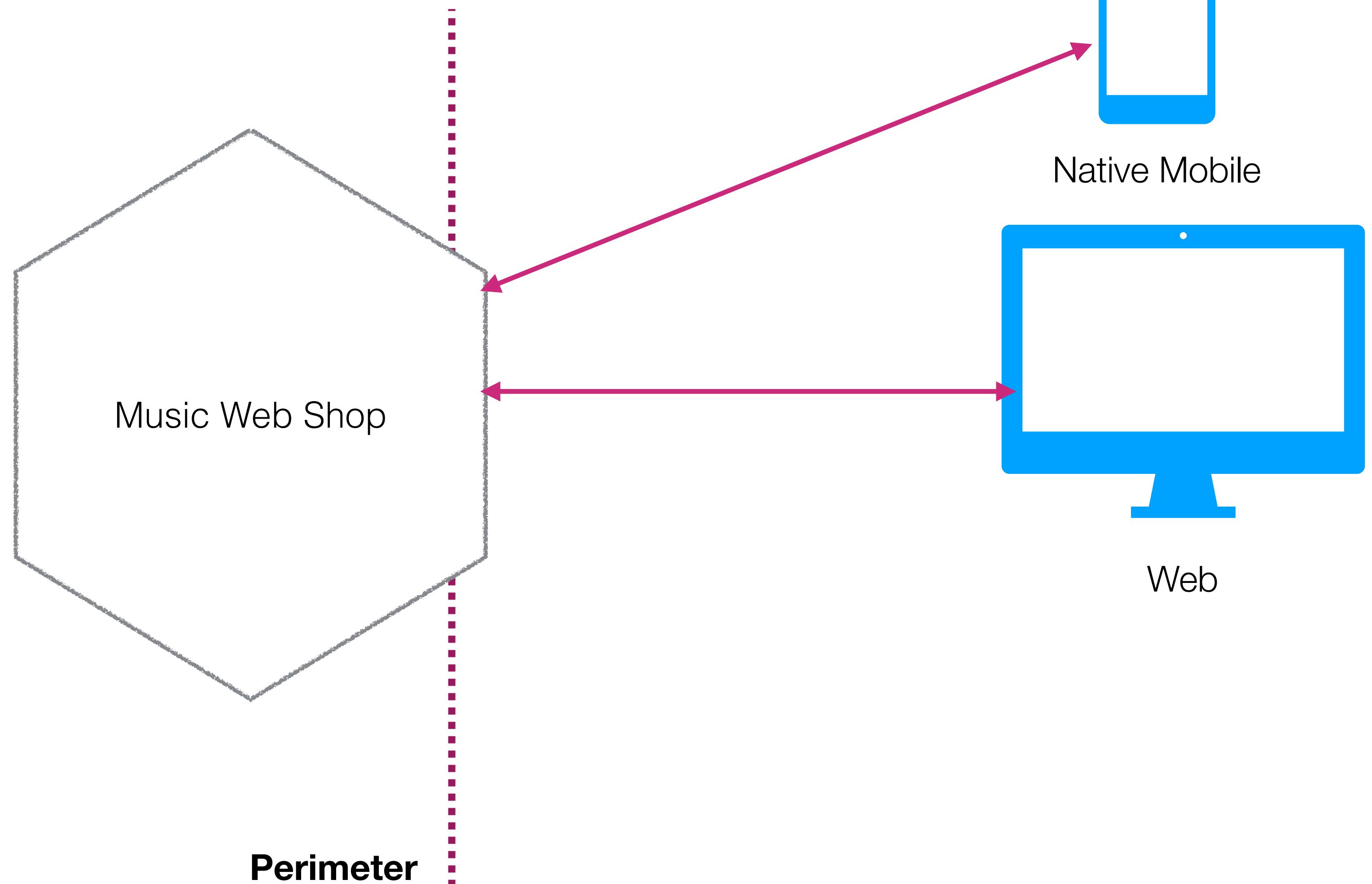


USER AUTHENTICATION - HANDLED IN SERVICE

Can reduce latency

Service potentially exposed to public internet

Self-contained



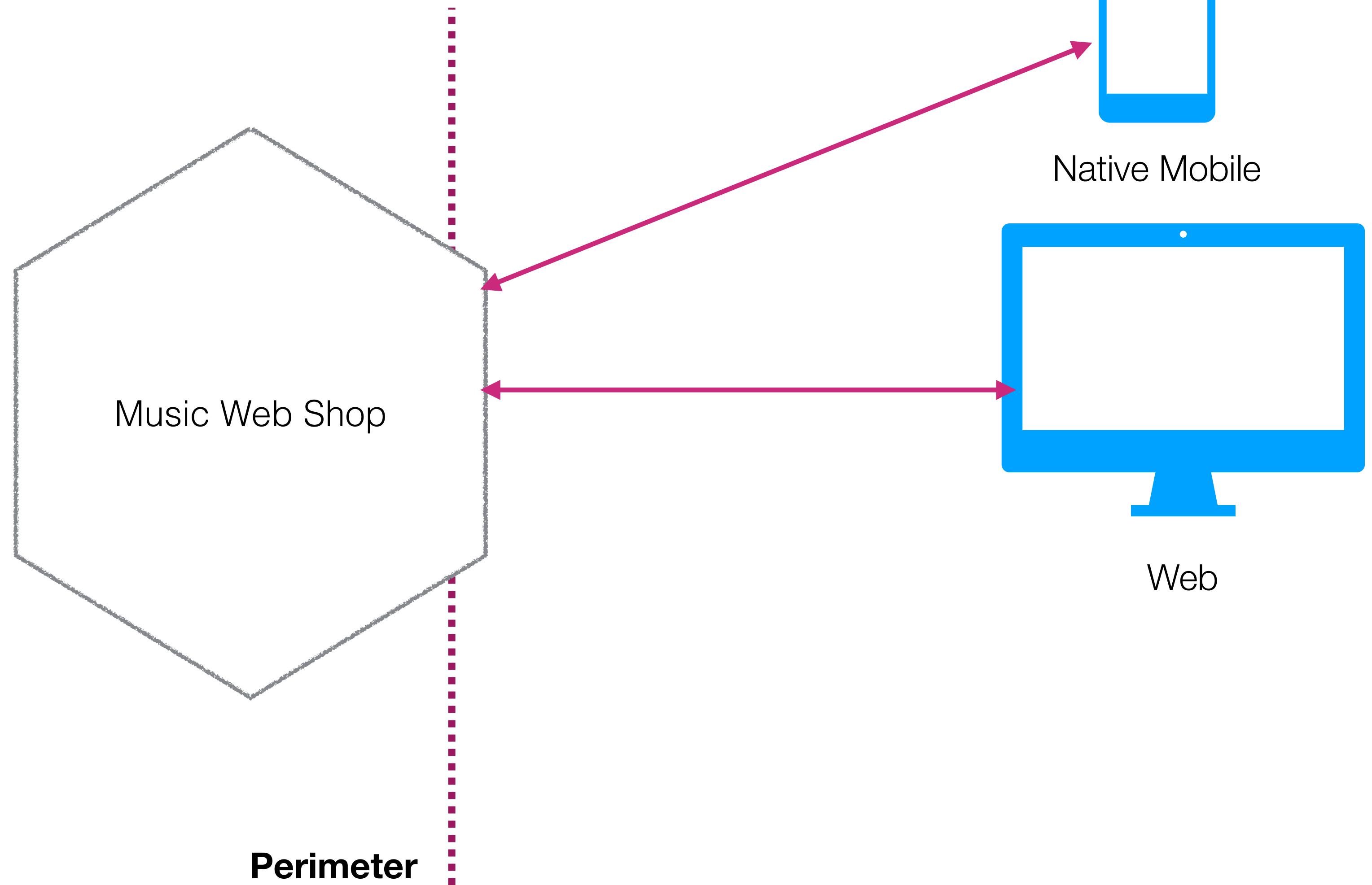
USER AUTHENTICATION - HANDLED IN SERVICE

Can reduce latency

Service potentially exposed to public internet

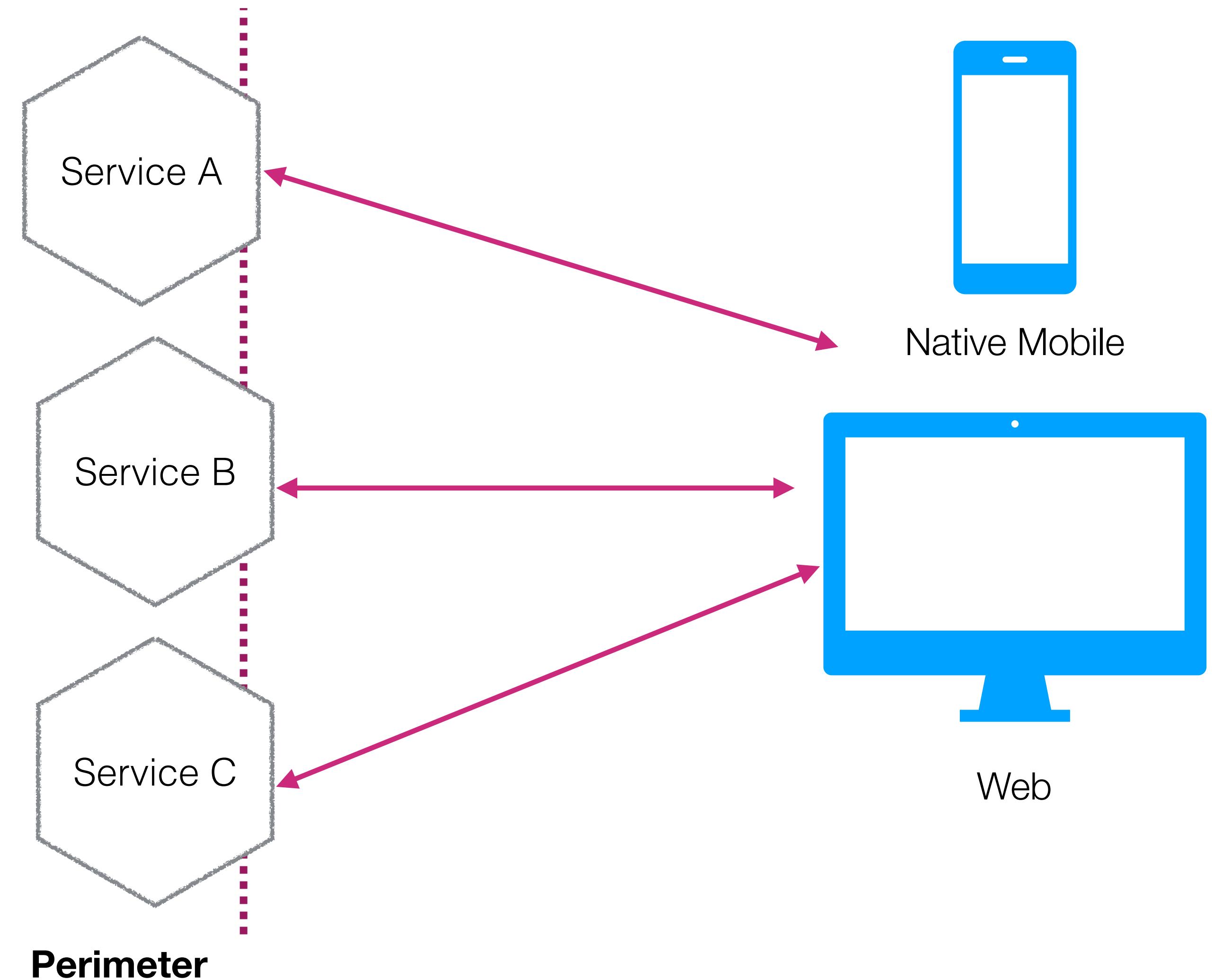
Self-contained

Code reuse?



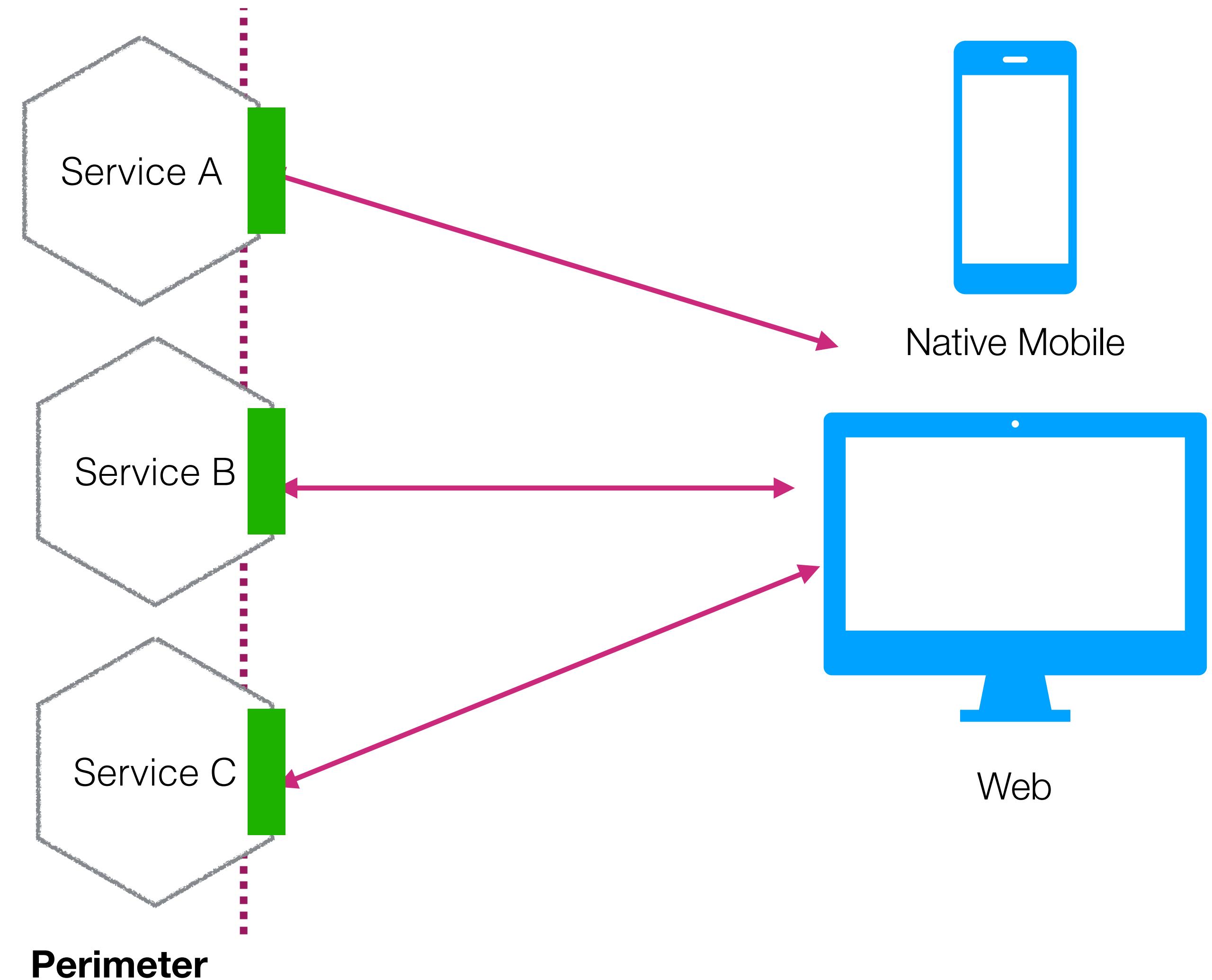
USER AUTHENTICATION - LIBRARY-BASED

Re-use authentication
flow code via library



USER AUTHENTICATION - LIBRARY-BASED

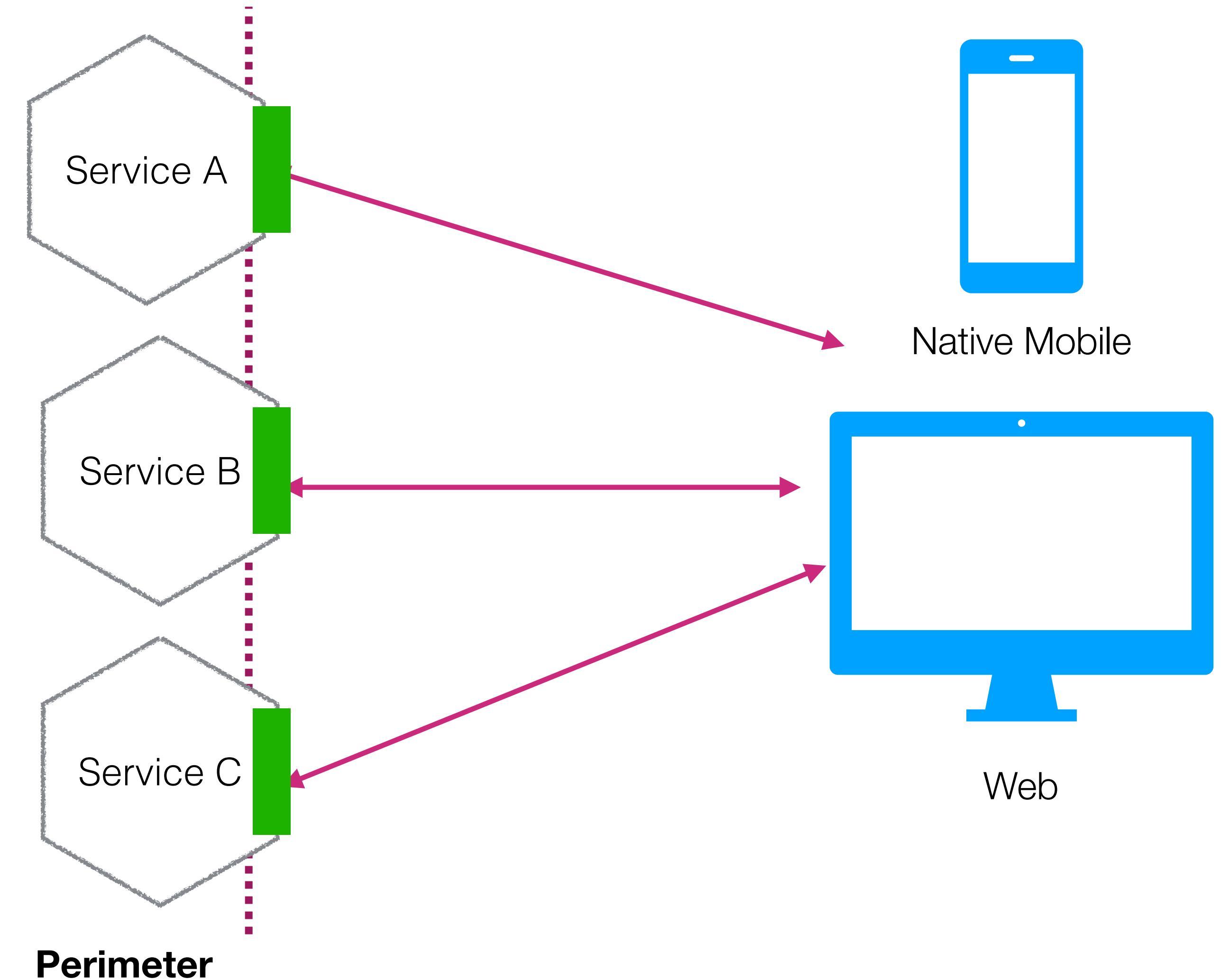
Re-use authentication
flow code via library



USER AUTHENTICATION - LIBRARY-BASED

Re-use authentication
flow code via library

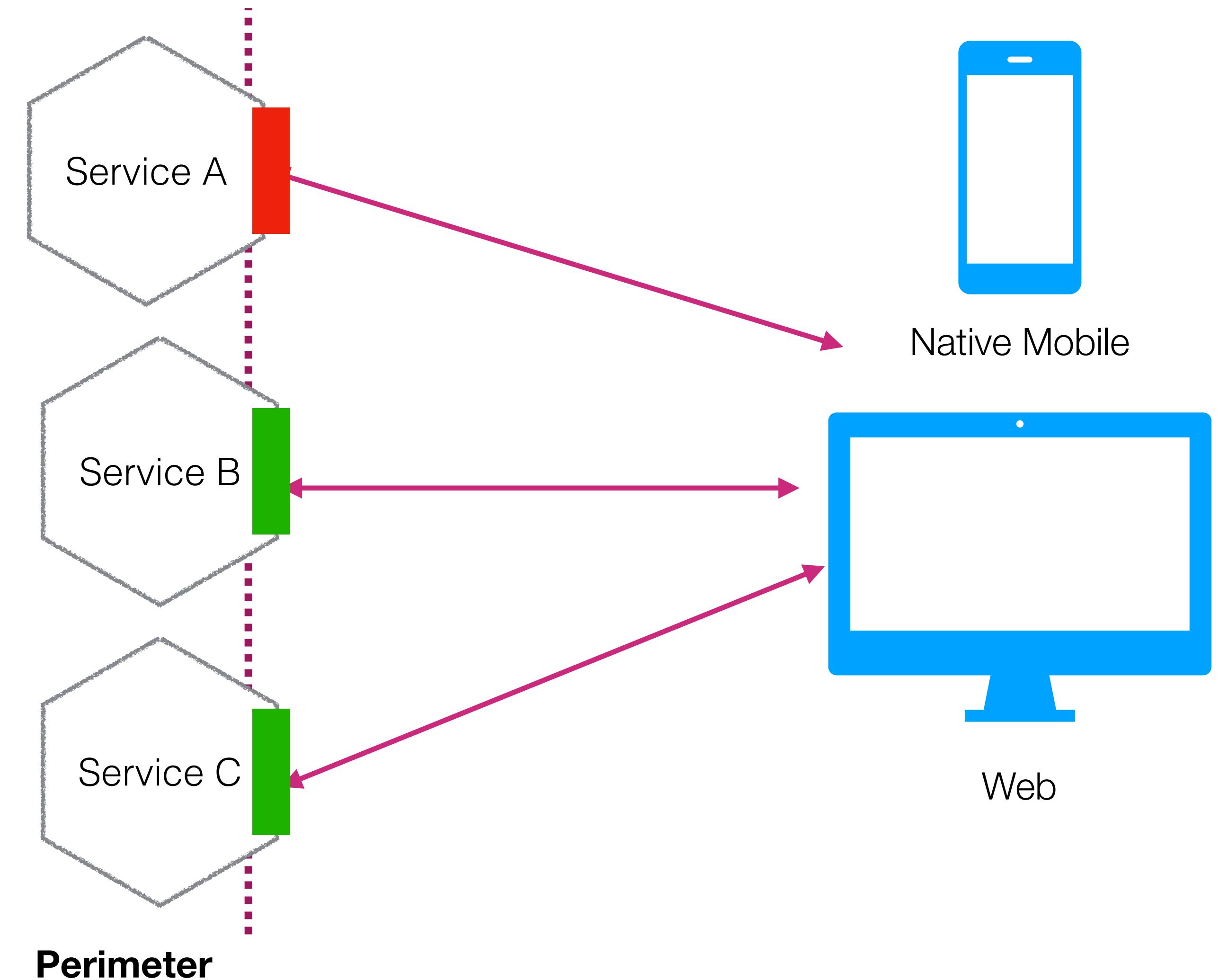
Version drift?



USER AUTHENTICATION - LIBRARY-BASED

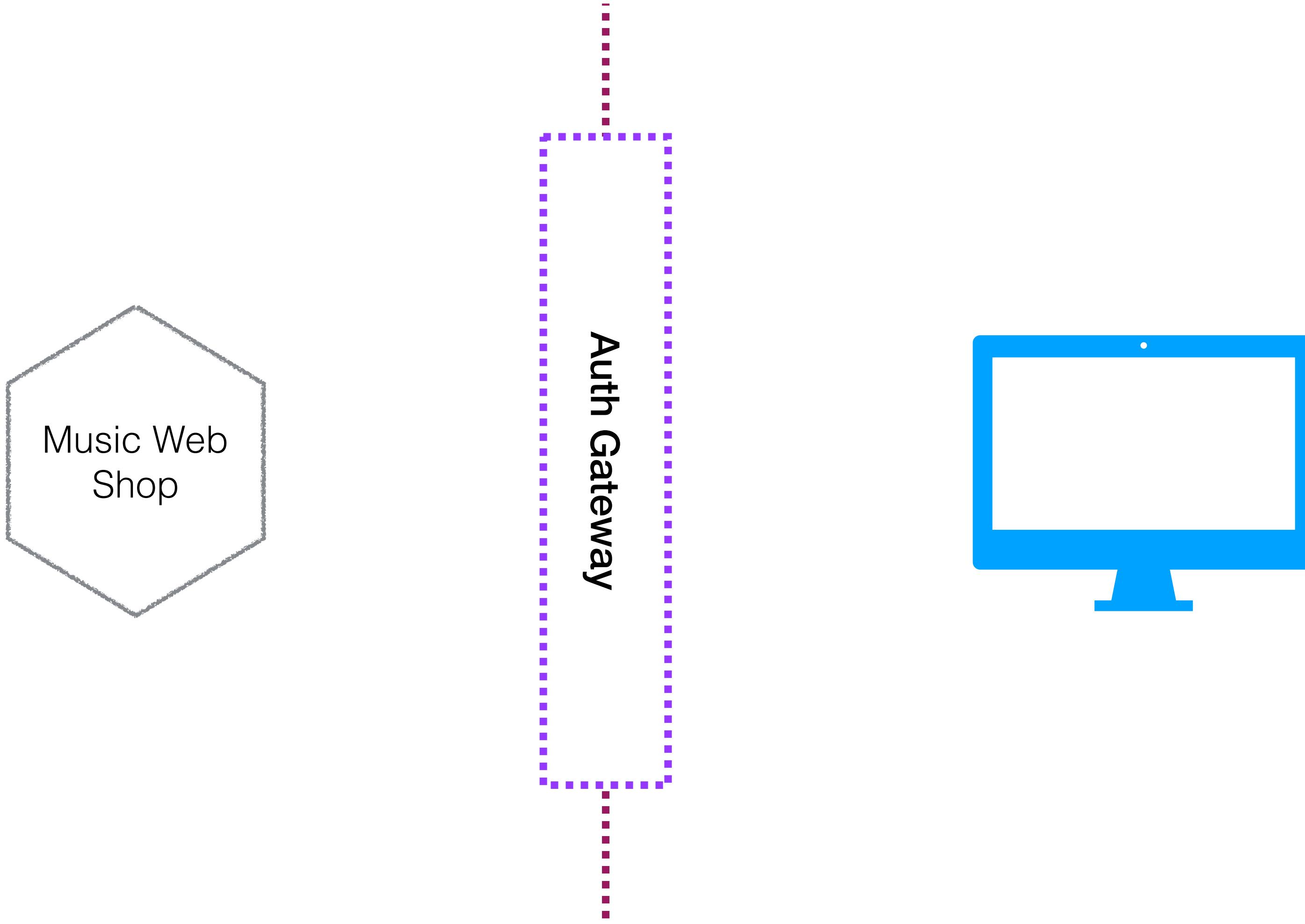
Re-use authentication
flow code via library

Version drift?

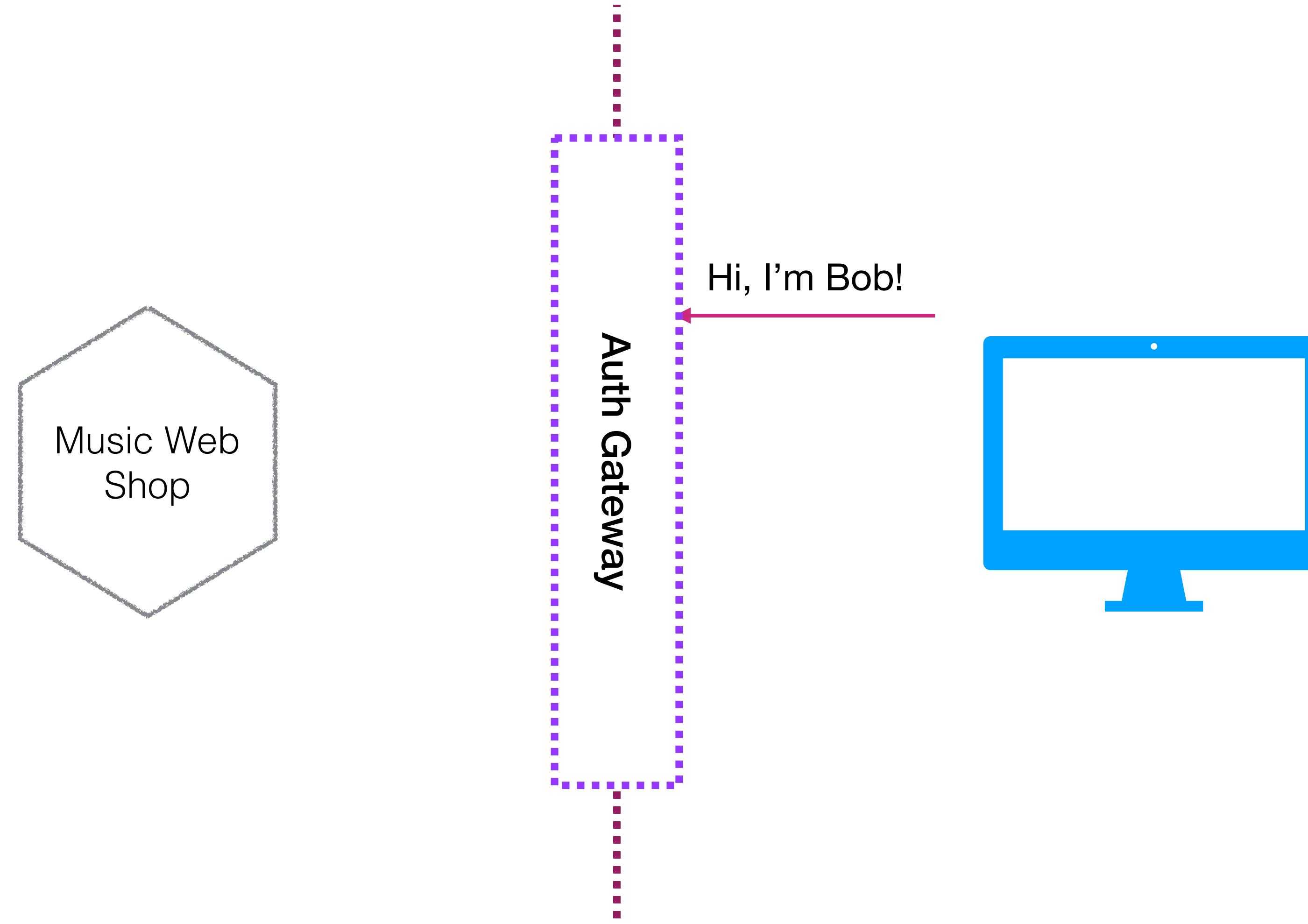


What about authorisation?

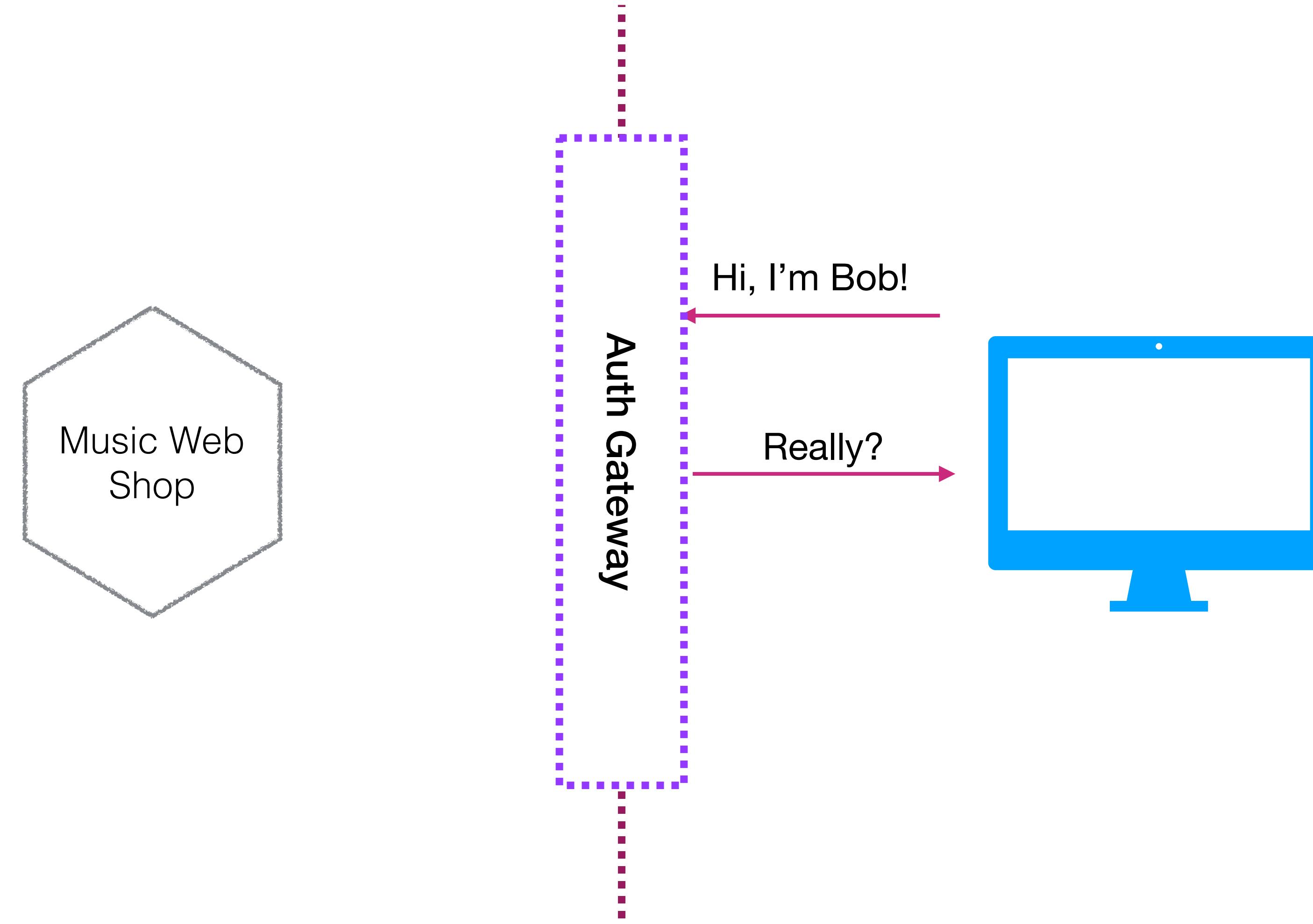
DO YOU EVEN AUTH?



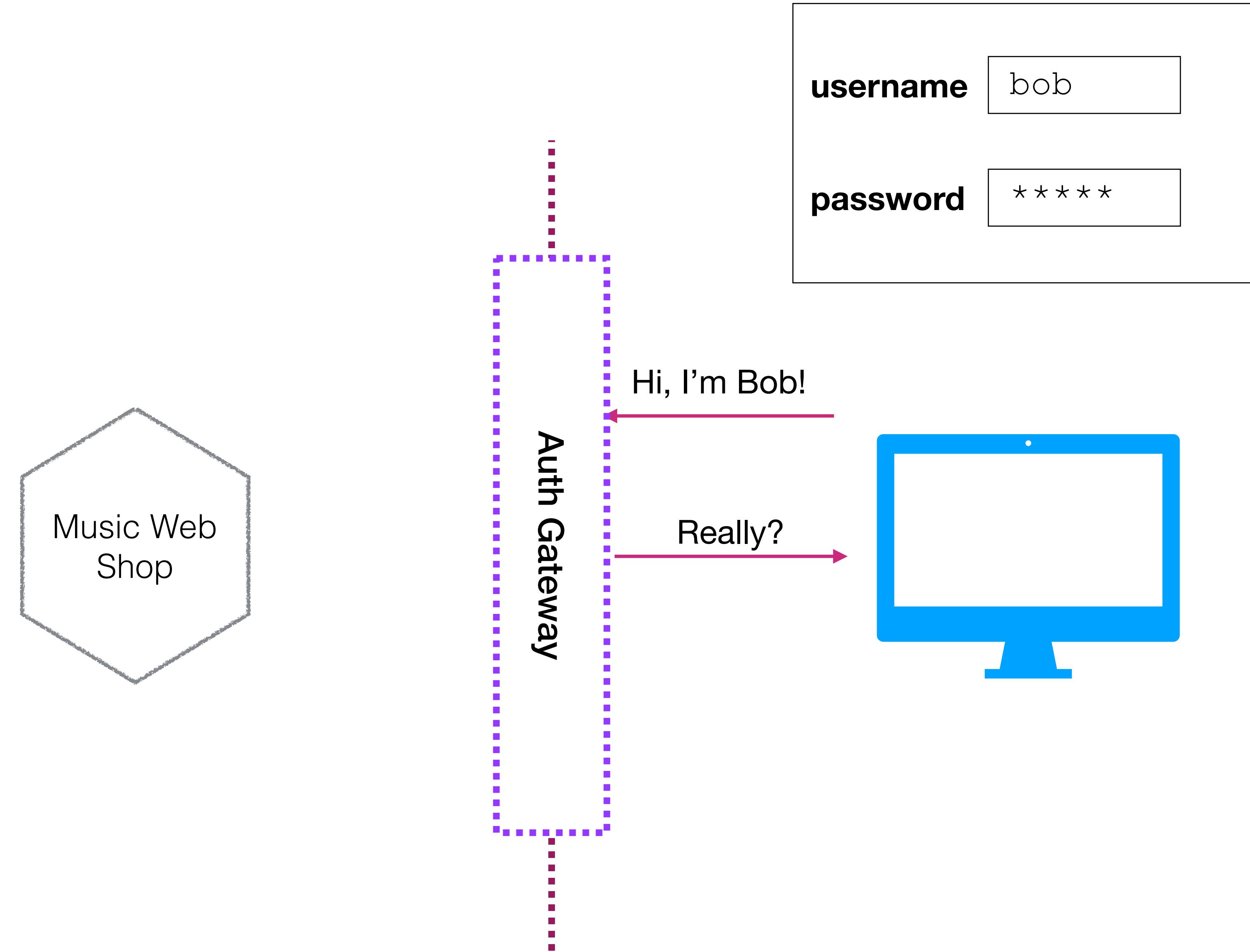
DO YOU EVEN AUTH?



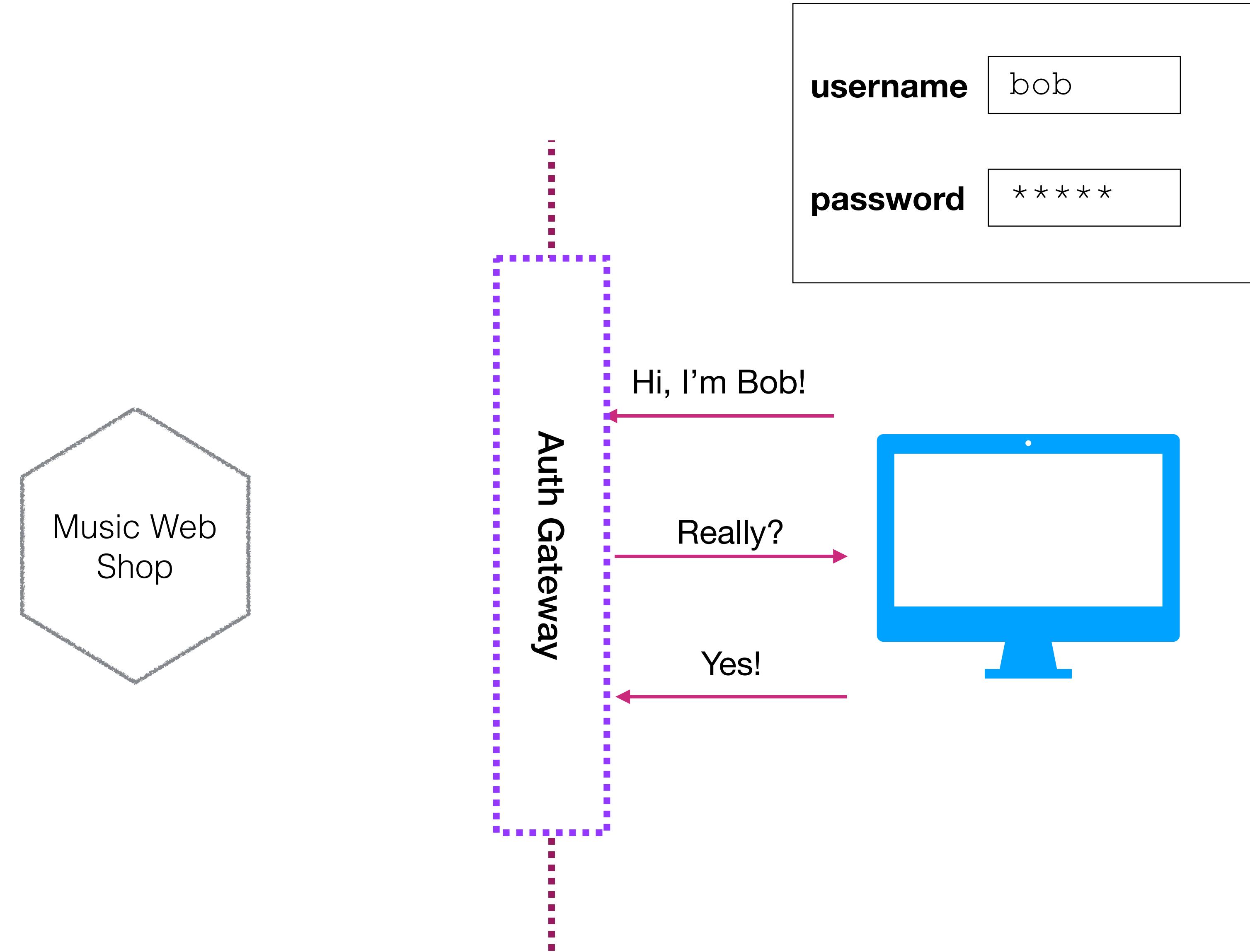
DO YOU EVEN AUTH?



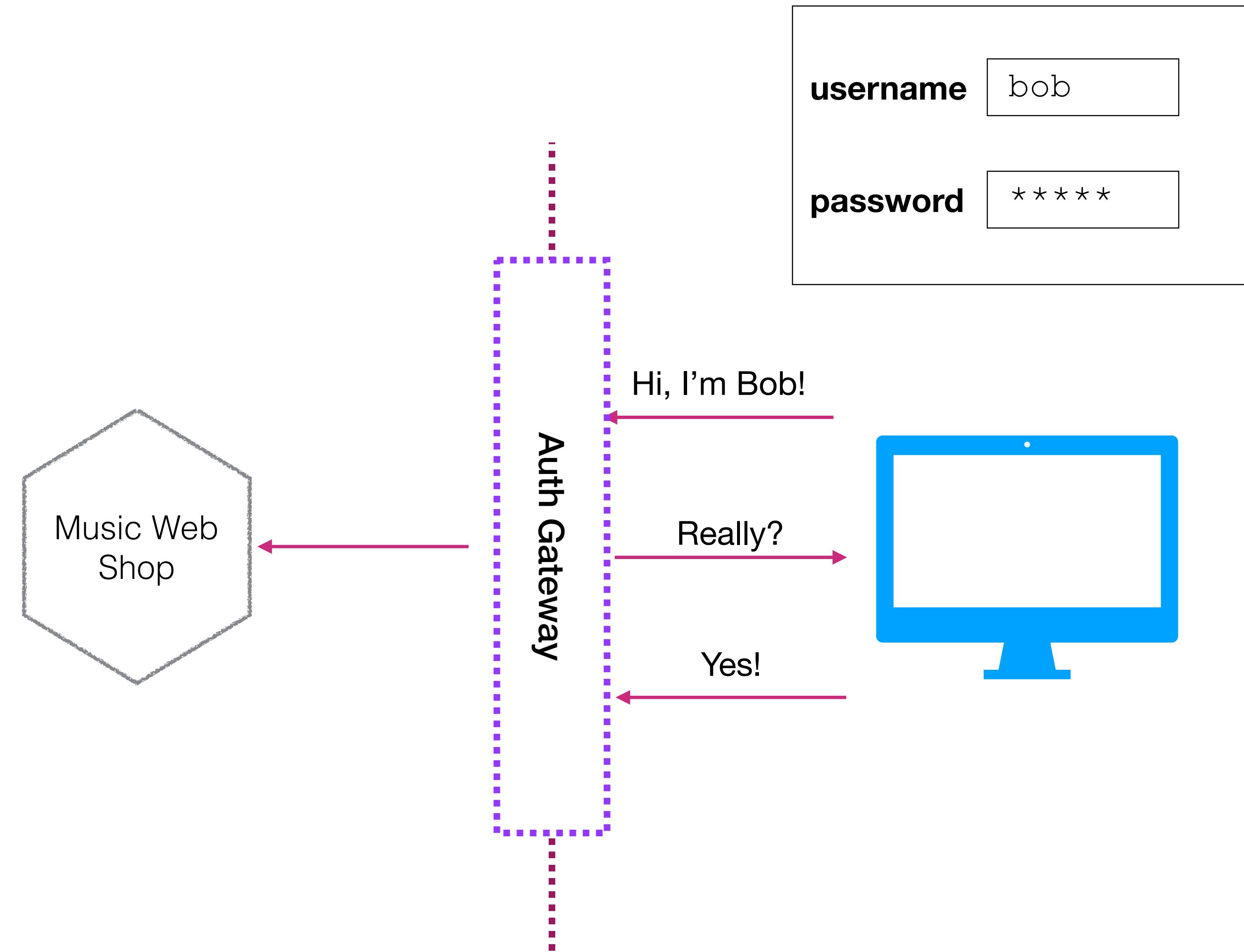
DO YOU EVEN AUTH?



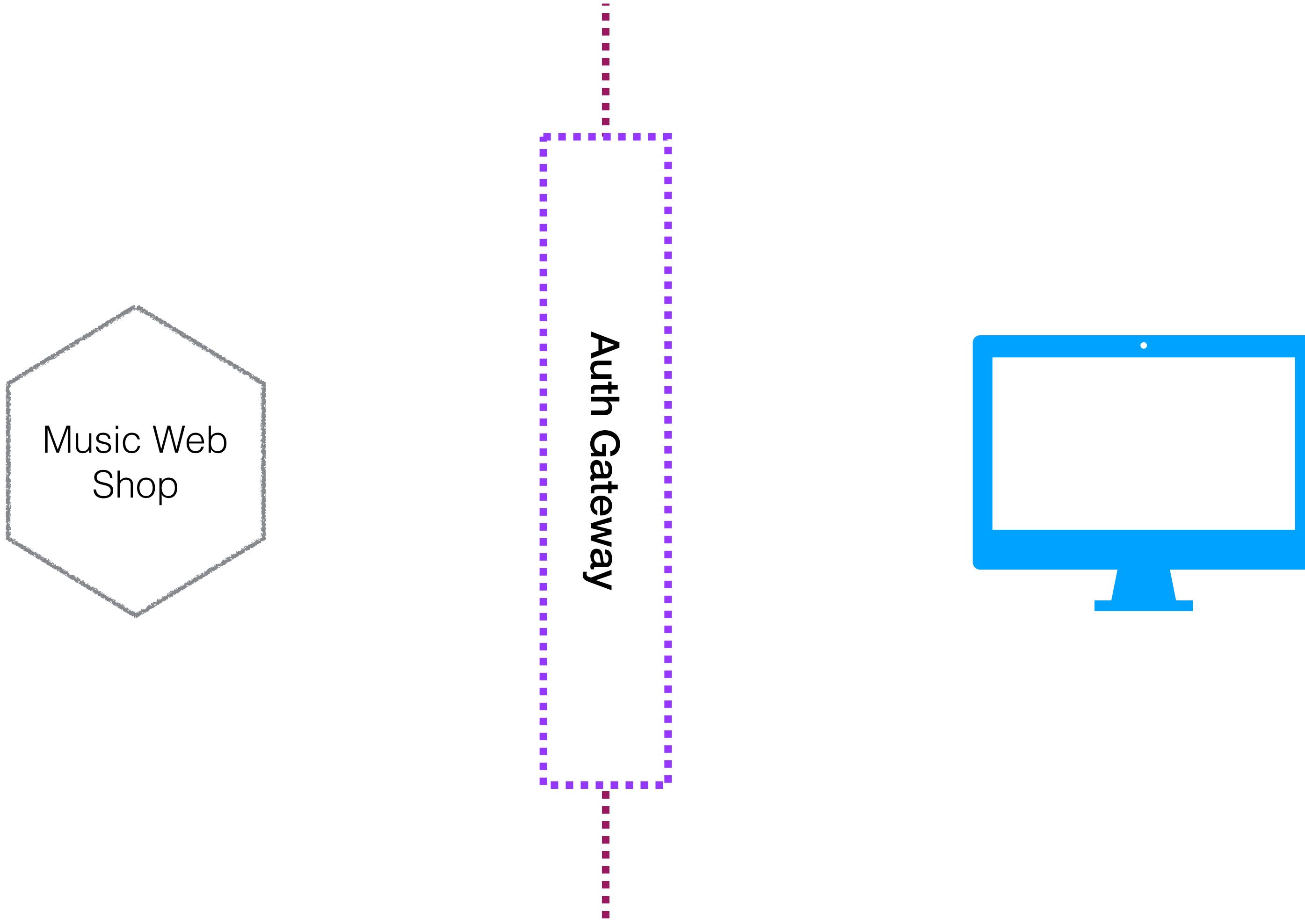
DO YOU EVEN AUTH?



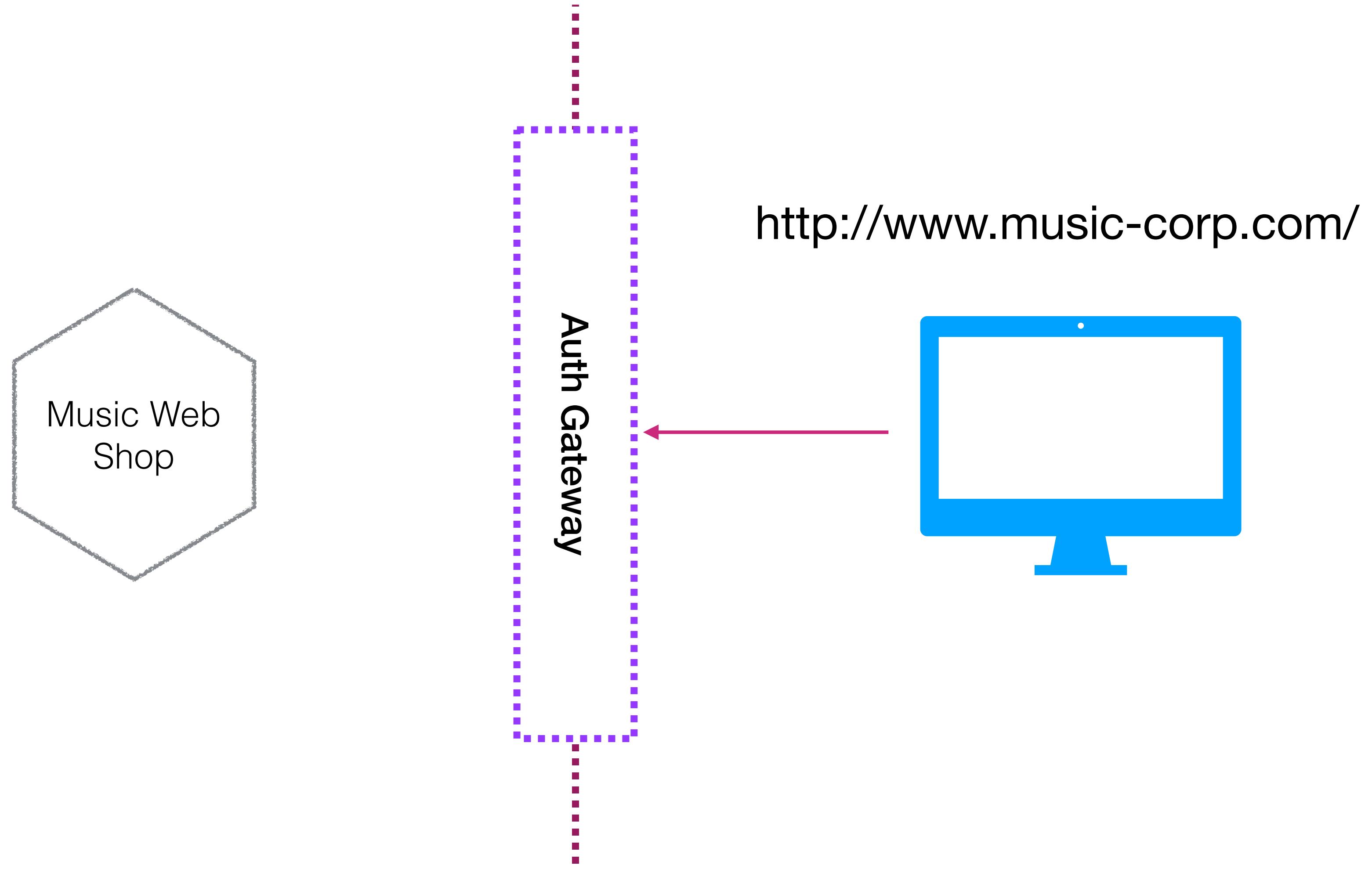
DO YOU EVEN AUTH?



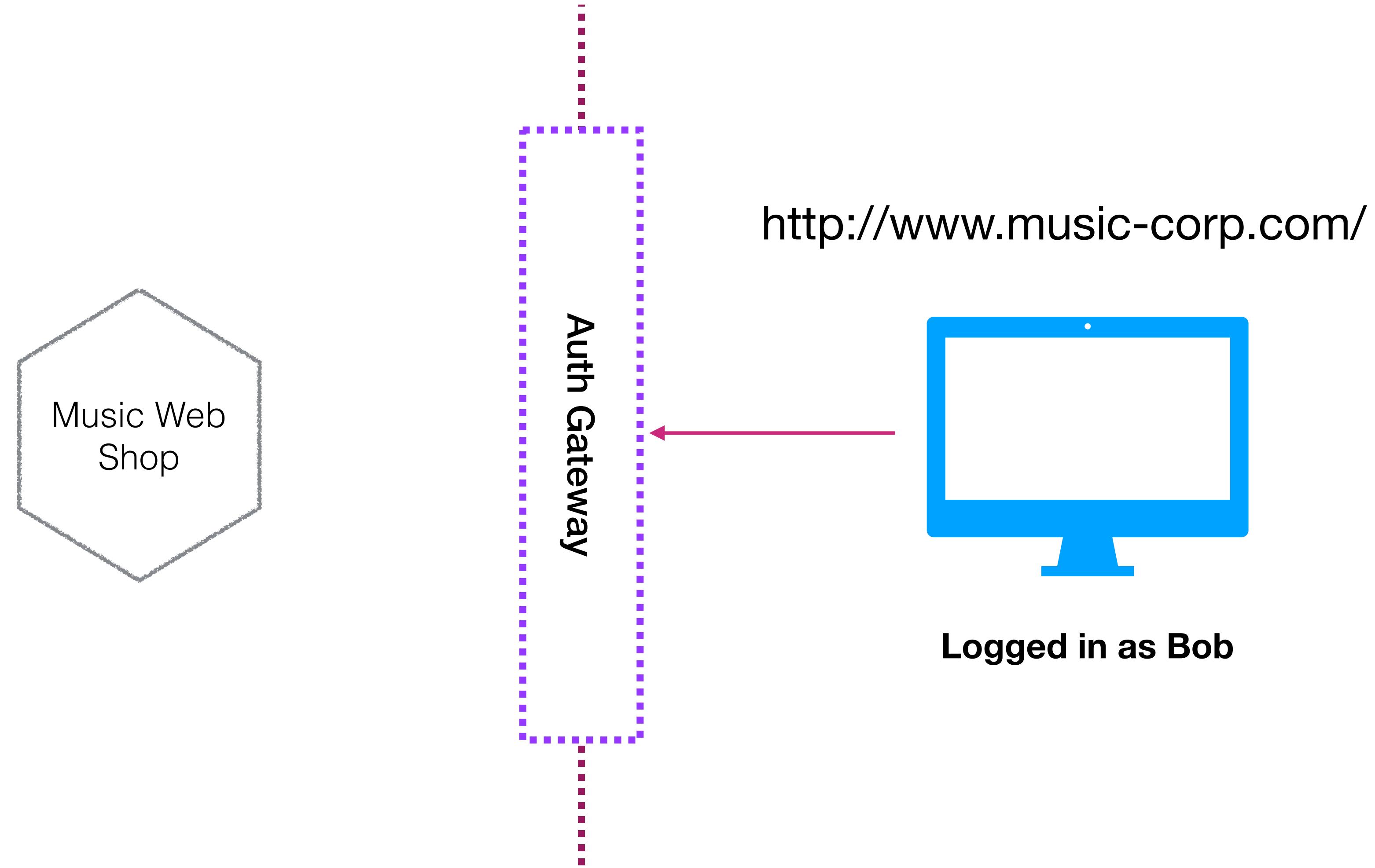
DO YOU EVEN AUTH?



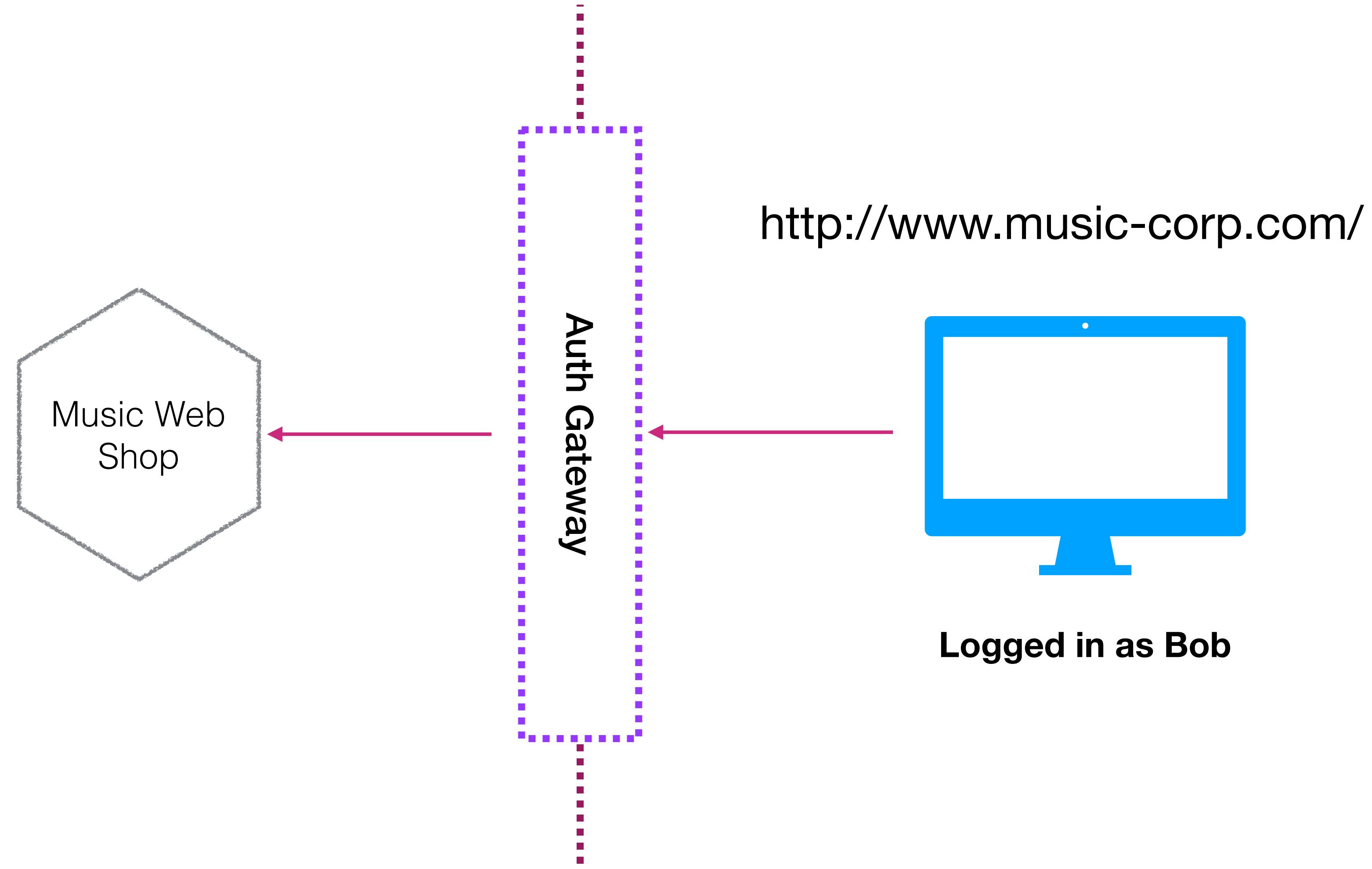
DO YOU EVEN AUTH?



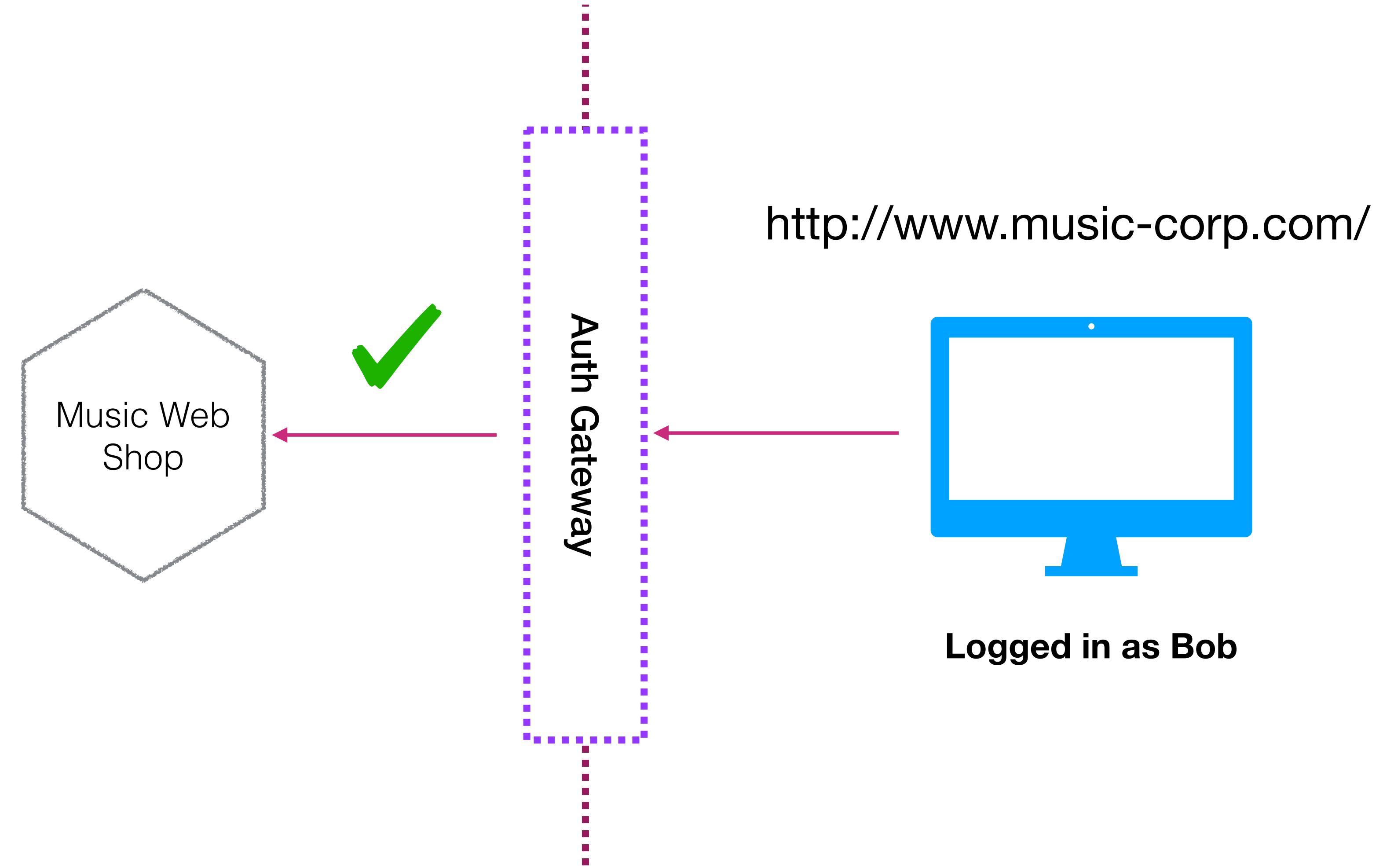
DO YOU EVEN AUTH?



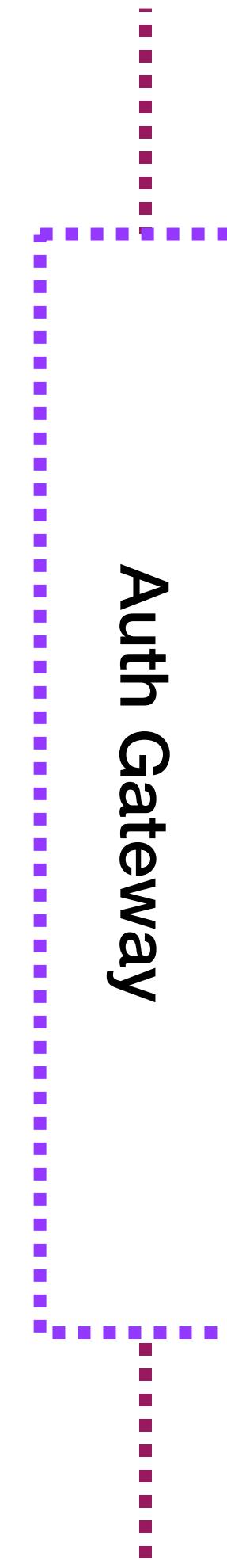
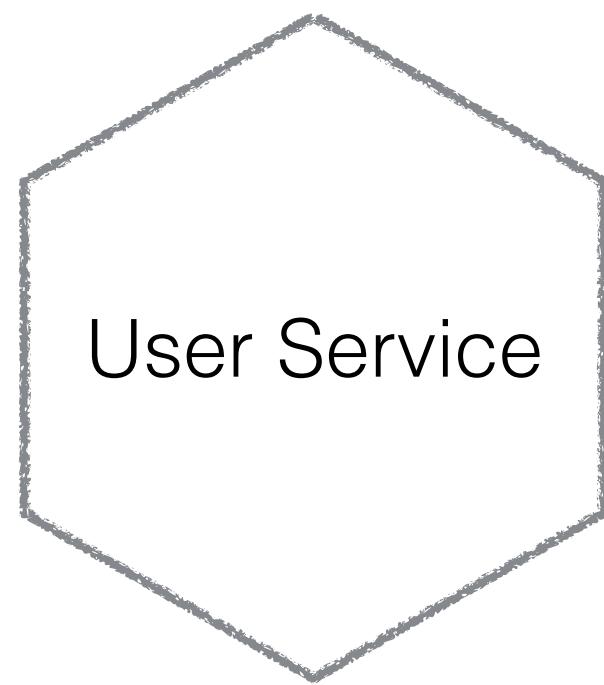
DO YOU EVEN AUTH?



DO YOU EVEN AUTH?

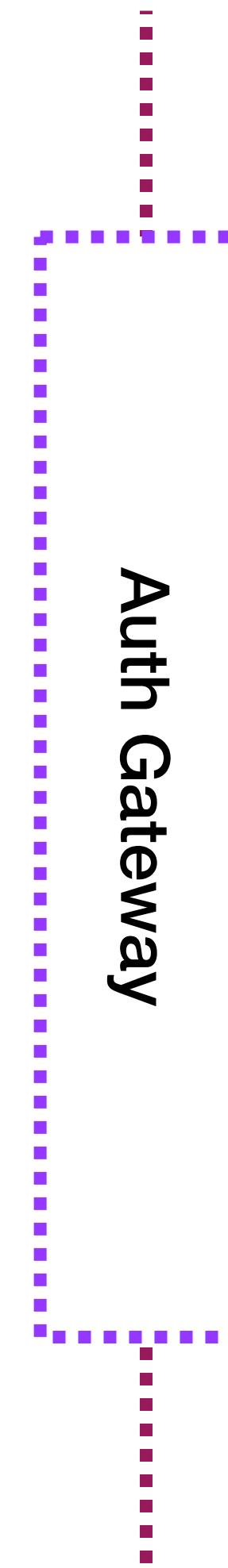
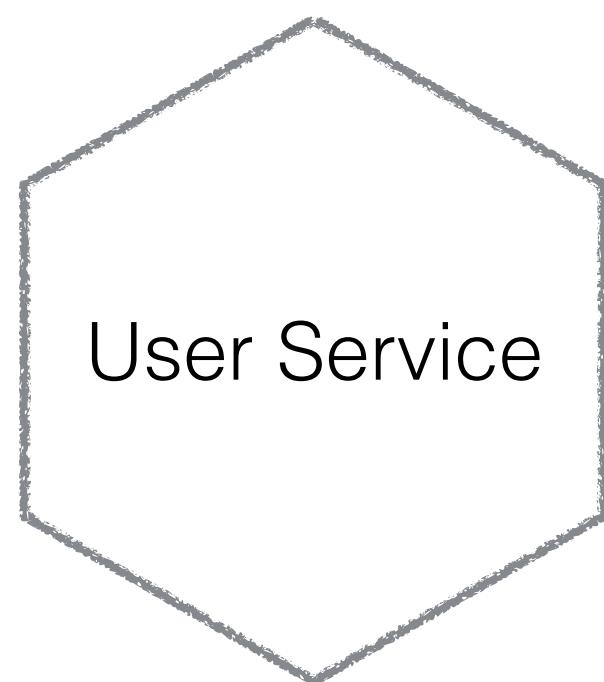


DOWNSTREAM AUTH - IMPLICIT TRUST?



Logged in as Bob

DOWNSTREAM AUTH - IMPLICIT TRUST?

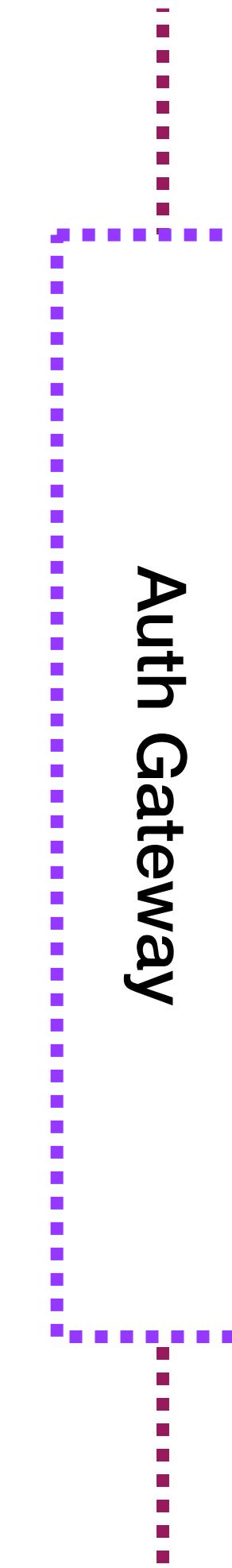
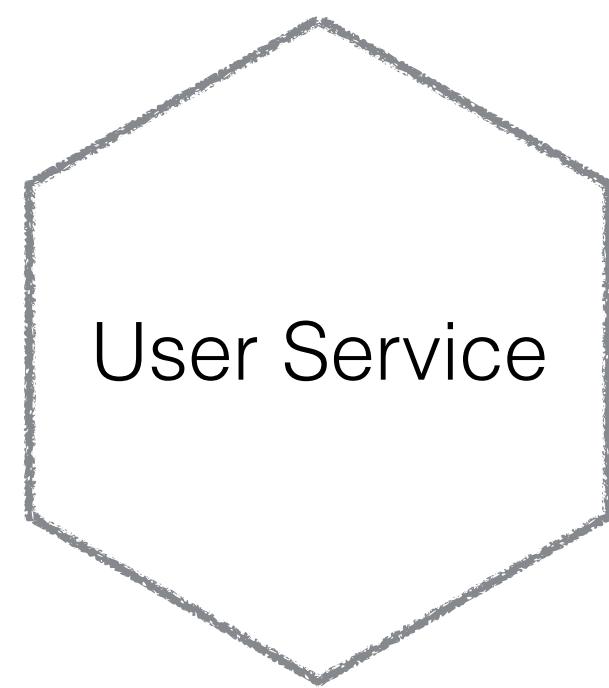


`http://www.music-corp.com/user/bob`



Logged in as Bob

DOWNSTREAM AUTH - IMPLICIT TRUST?

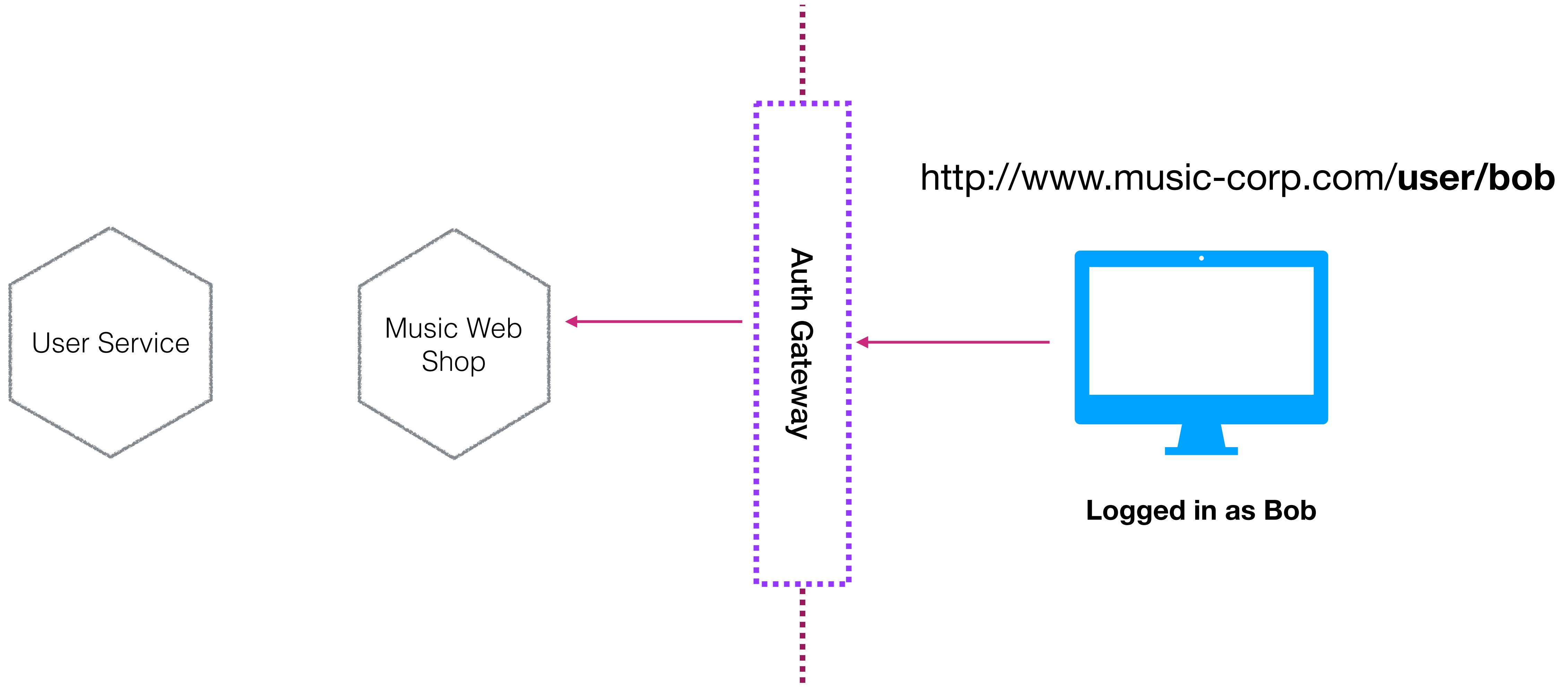


`http://www.music-corp.com/user/bob`

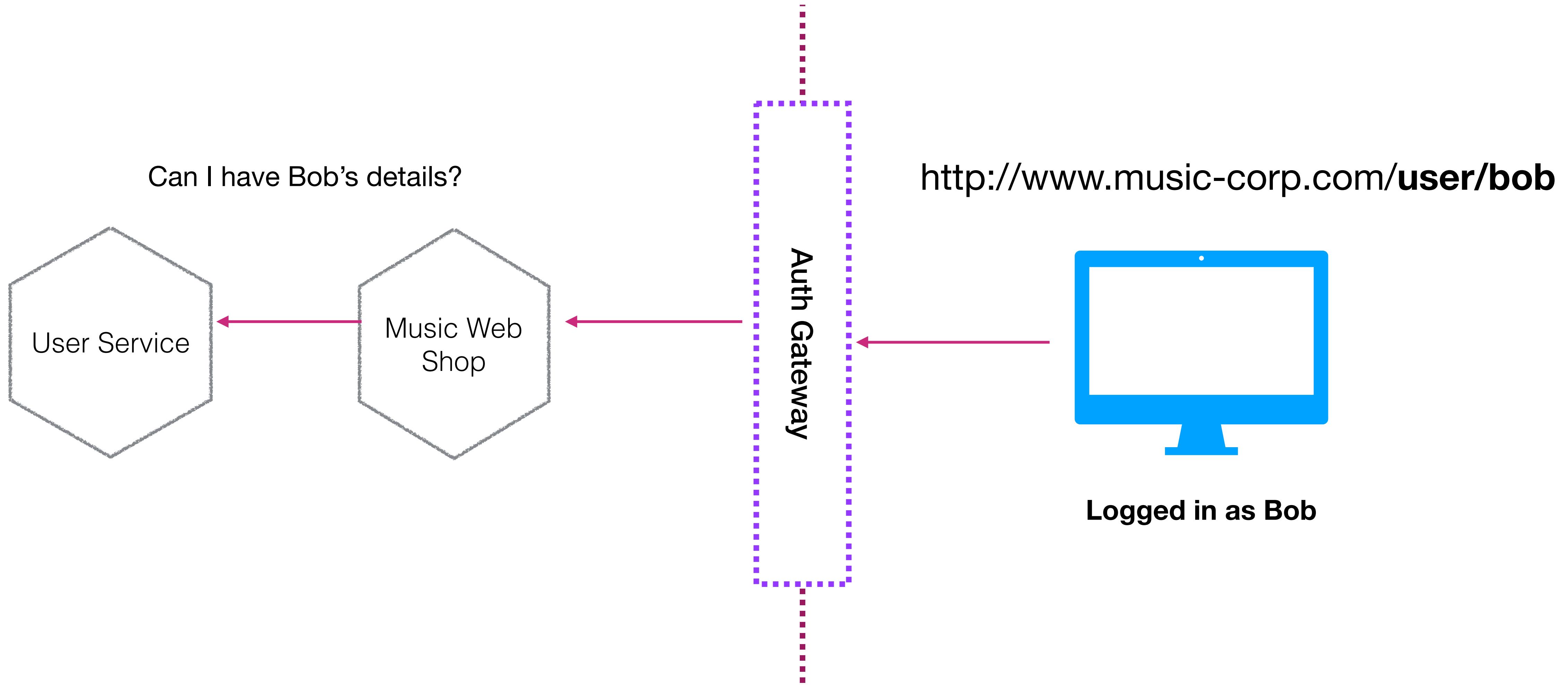


Logged in as Bob

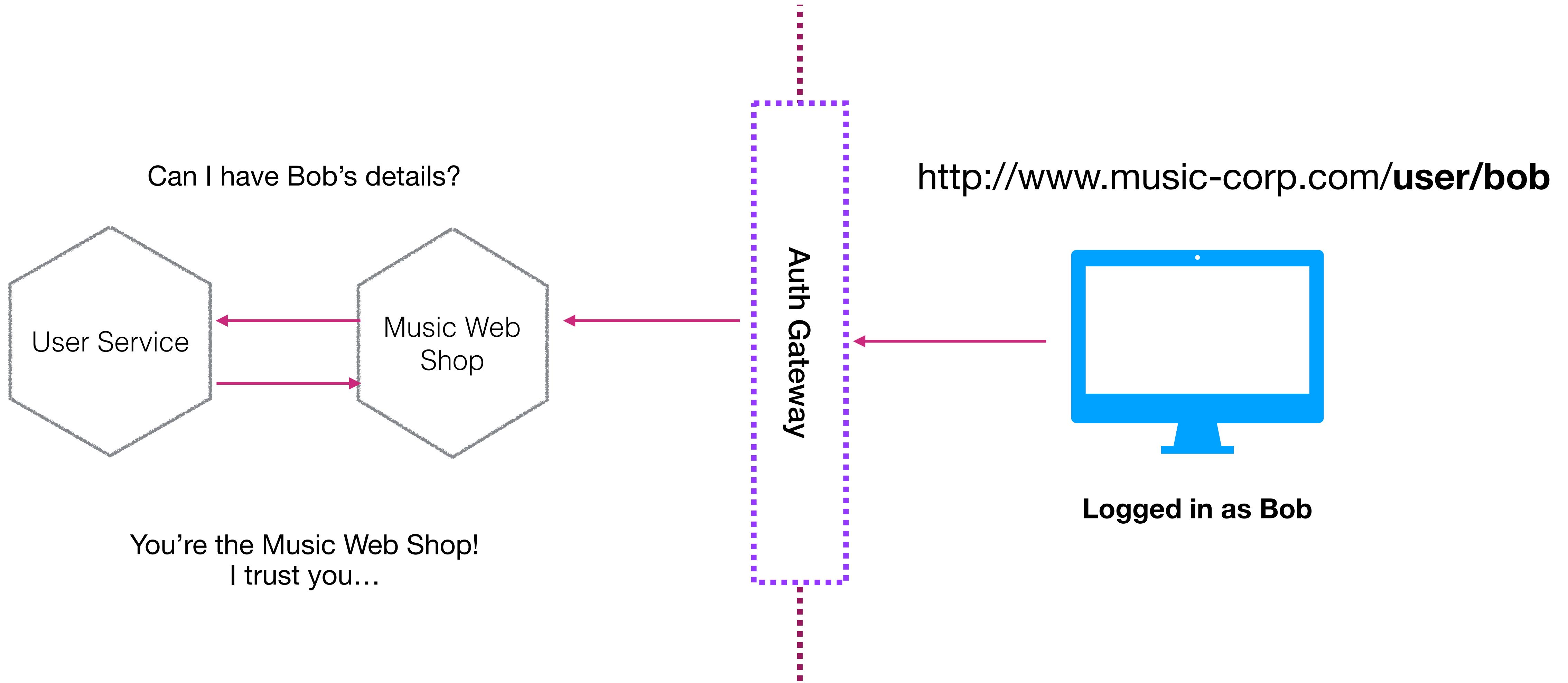
DOWNSTREAM AUTH - IMPLICIT TRUST?



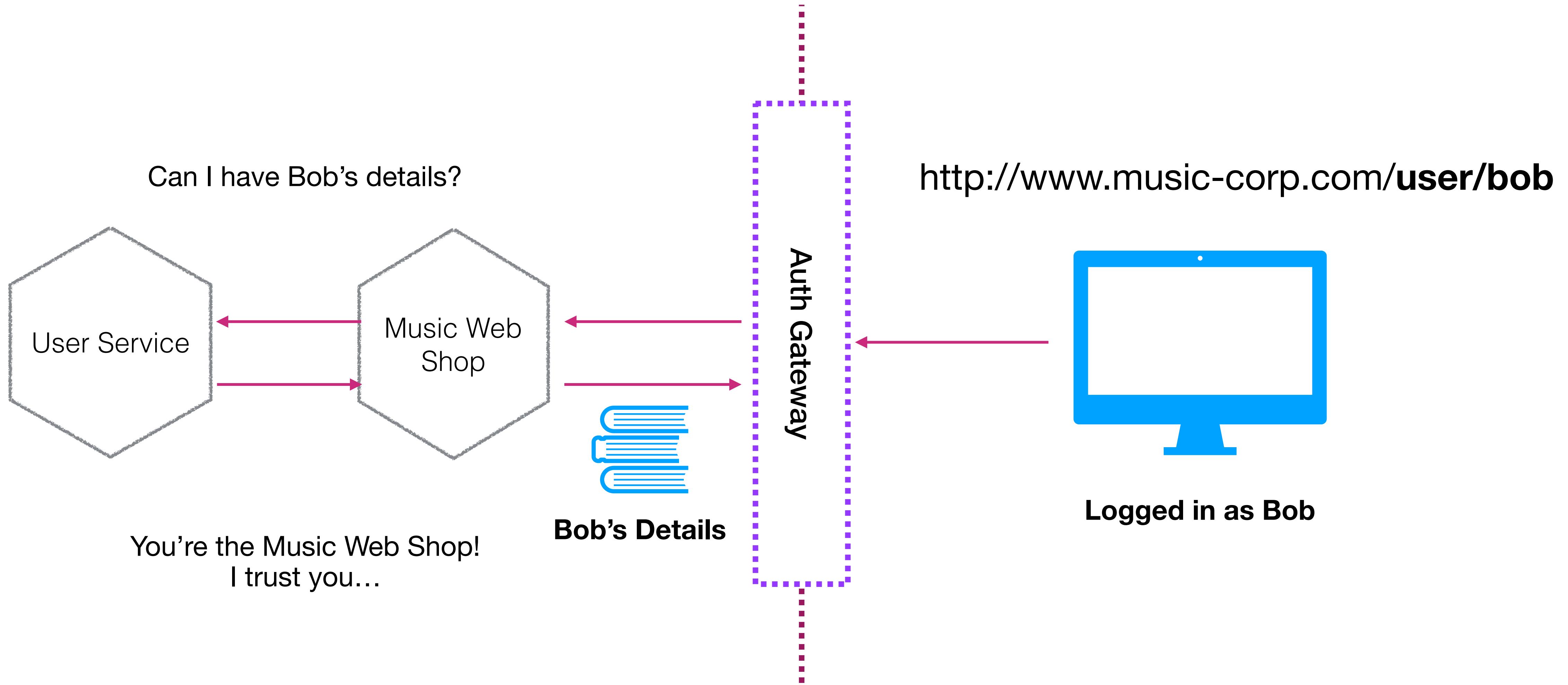
DOWNSTREAM AUTH - IMPLICIT TRUST?



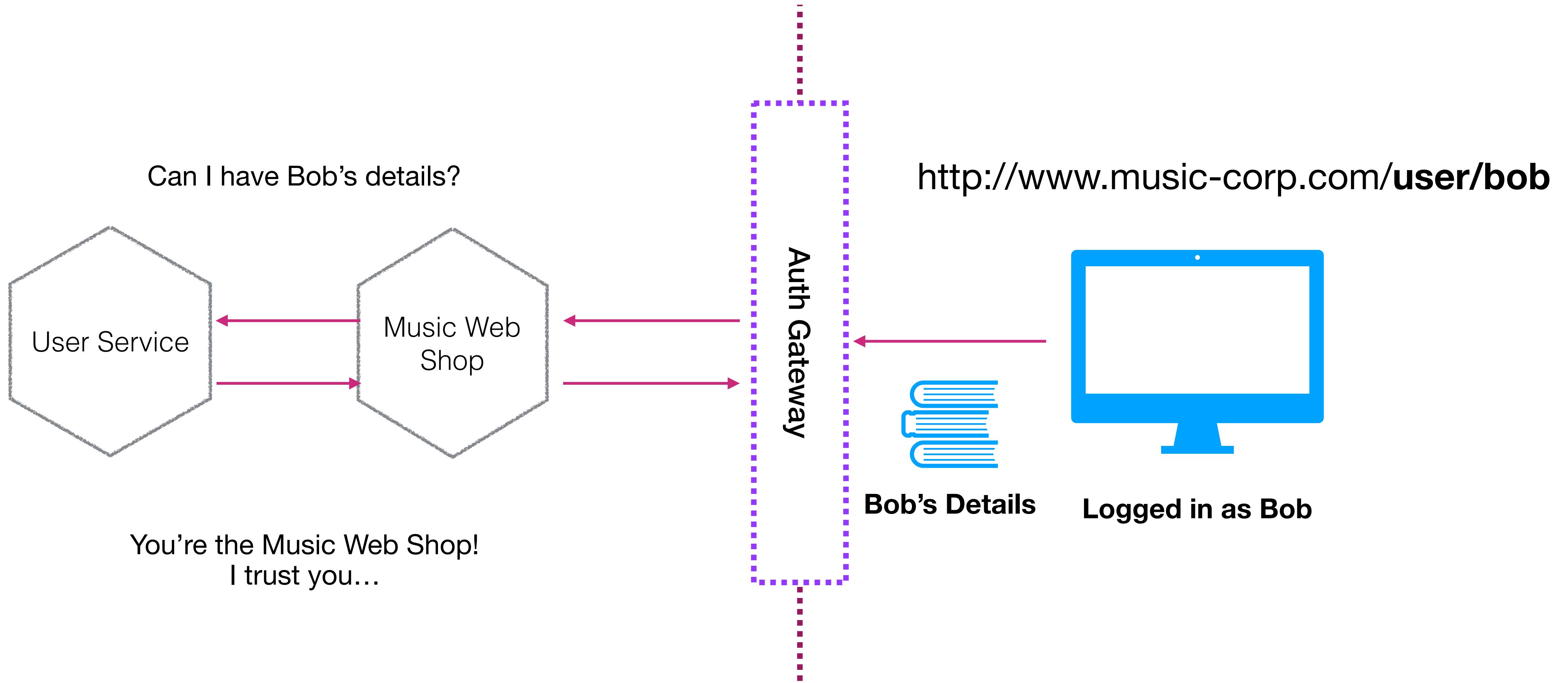
DOWNSTREAM AUTH - IMPLICIT TRUST?



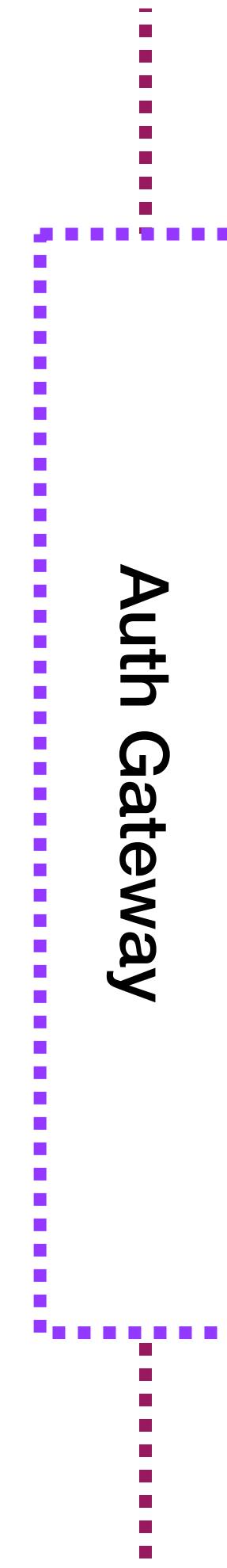
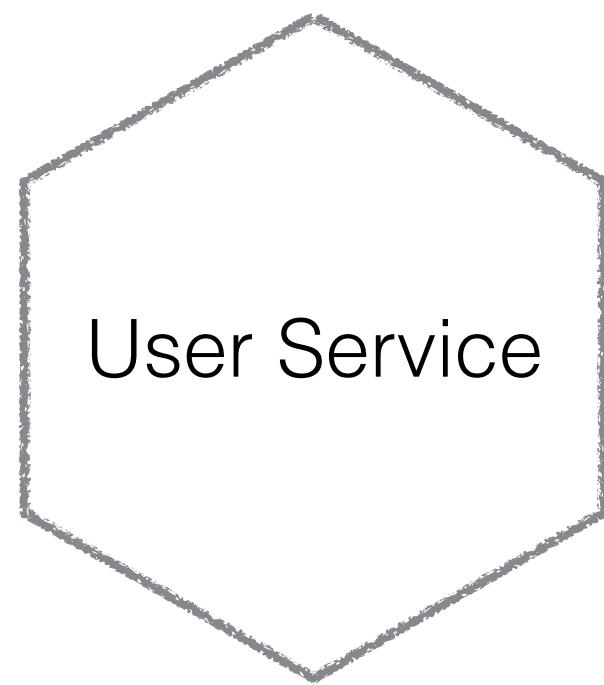
DOWNSTREAM AUTH - IMPLICIT TRUST?



DOWNSTREAM AUTH - IMPLICIT TRUST?

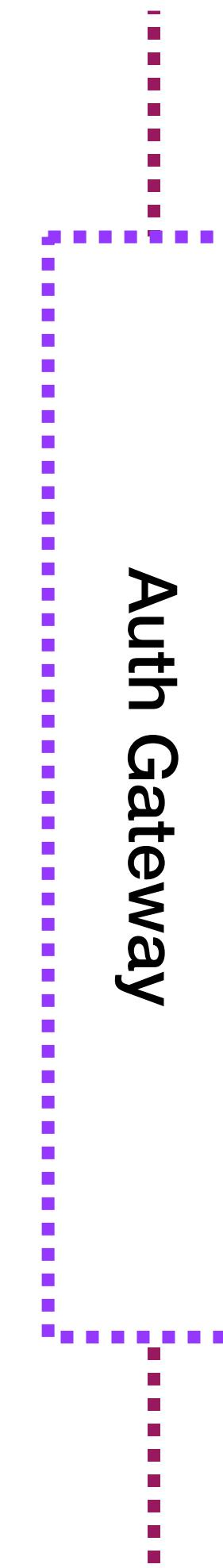
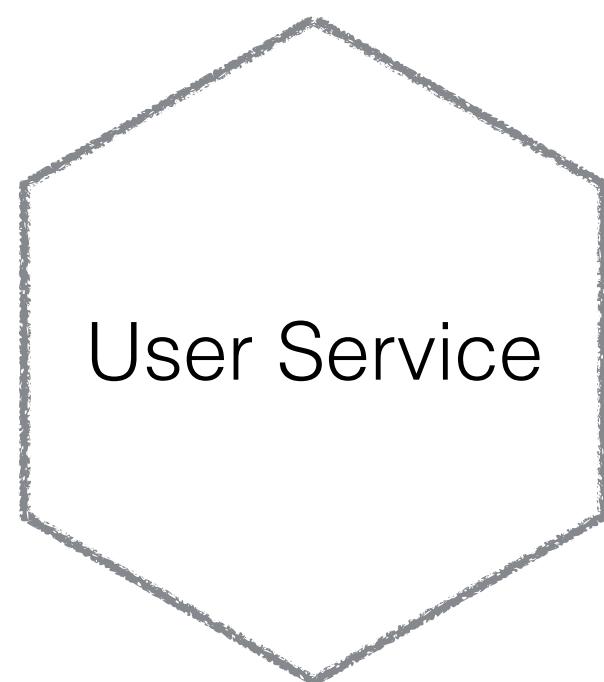


DOWNSTREAM AUTH - IMPLICIT TRUST?

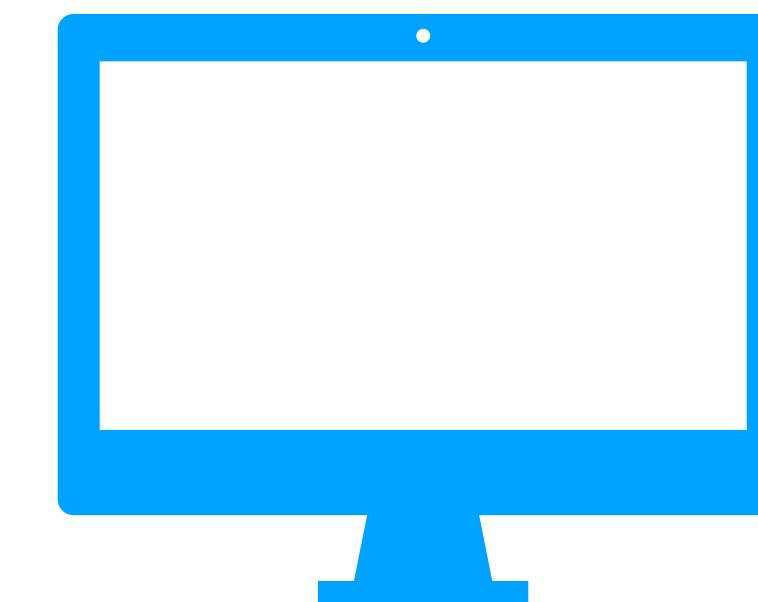


Logged in as Bob

DOWNSTREAM AUTH - IMPLICIT TRUST?

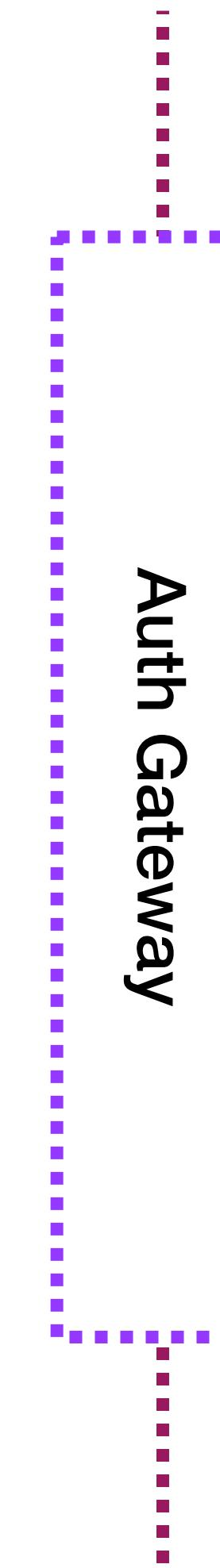
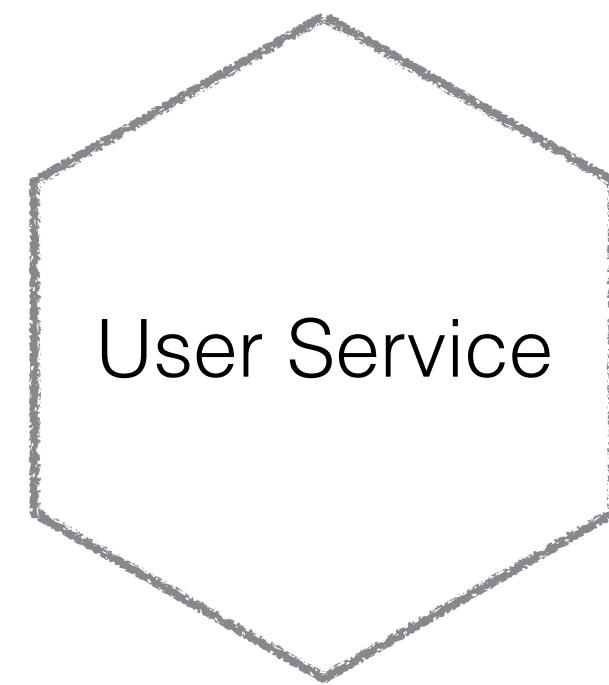


<http://www.music-corp.com/user/alice>



Logged in as Bob

DOWNSTREAM AUTH - IMPLICIT TRUST?

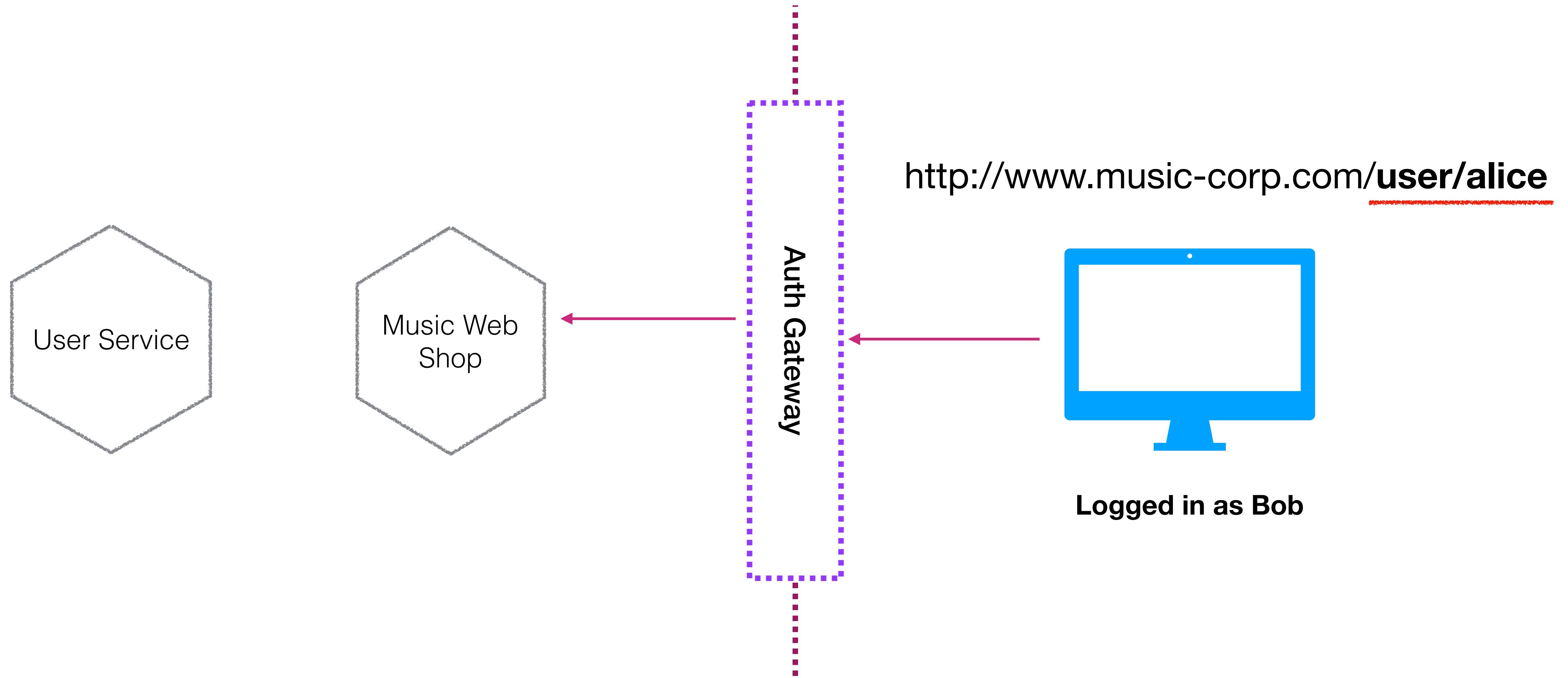


<http://www.music-corp.com/user/alice>

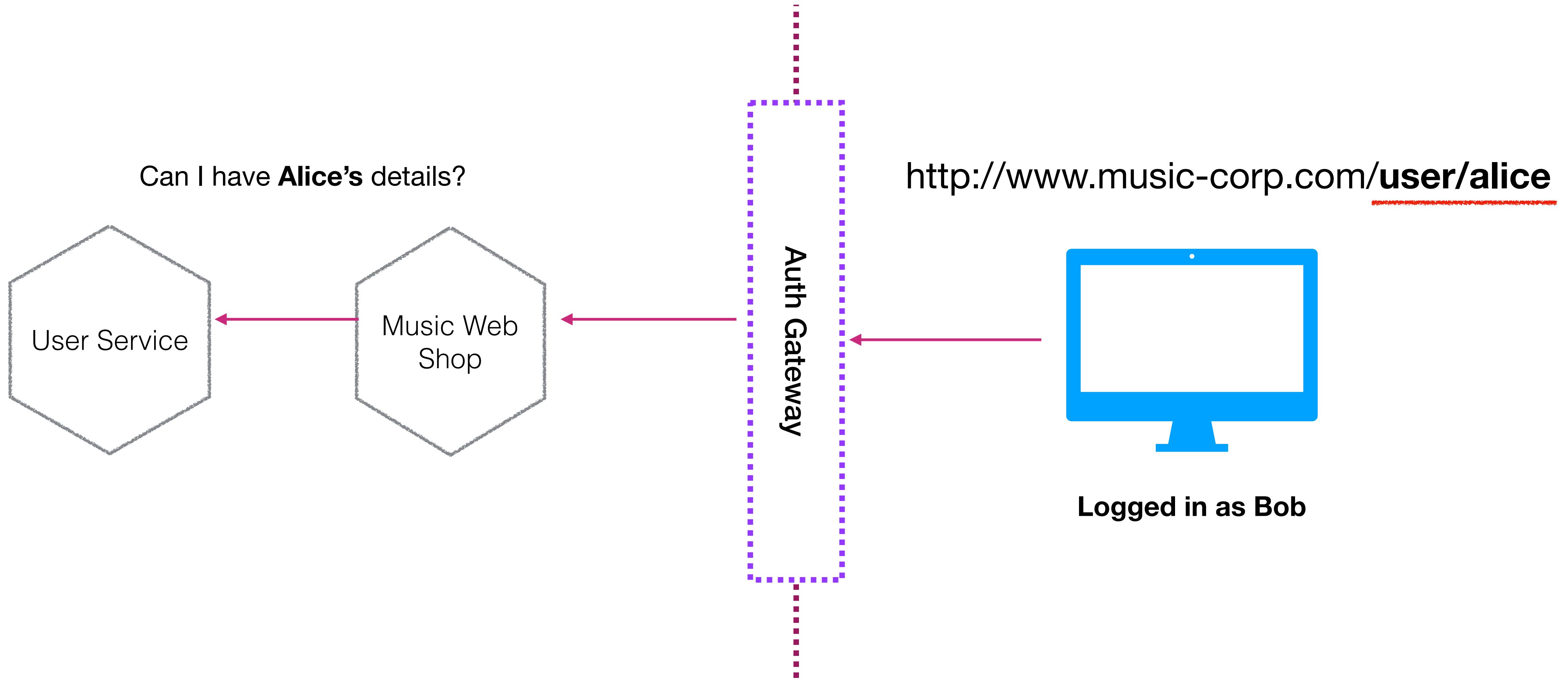


Logged in as Bob

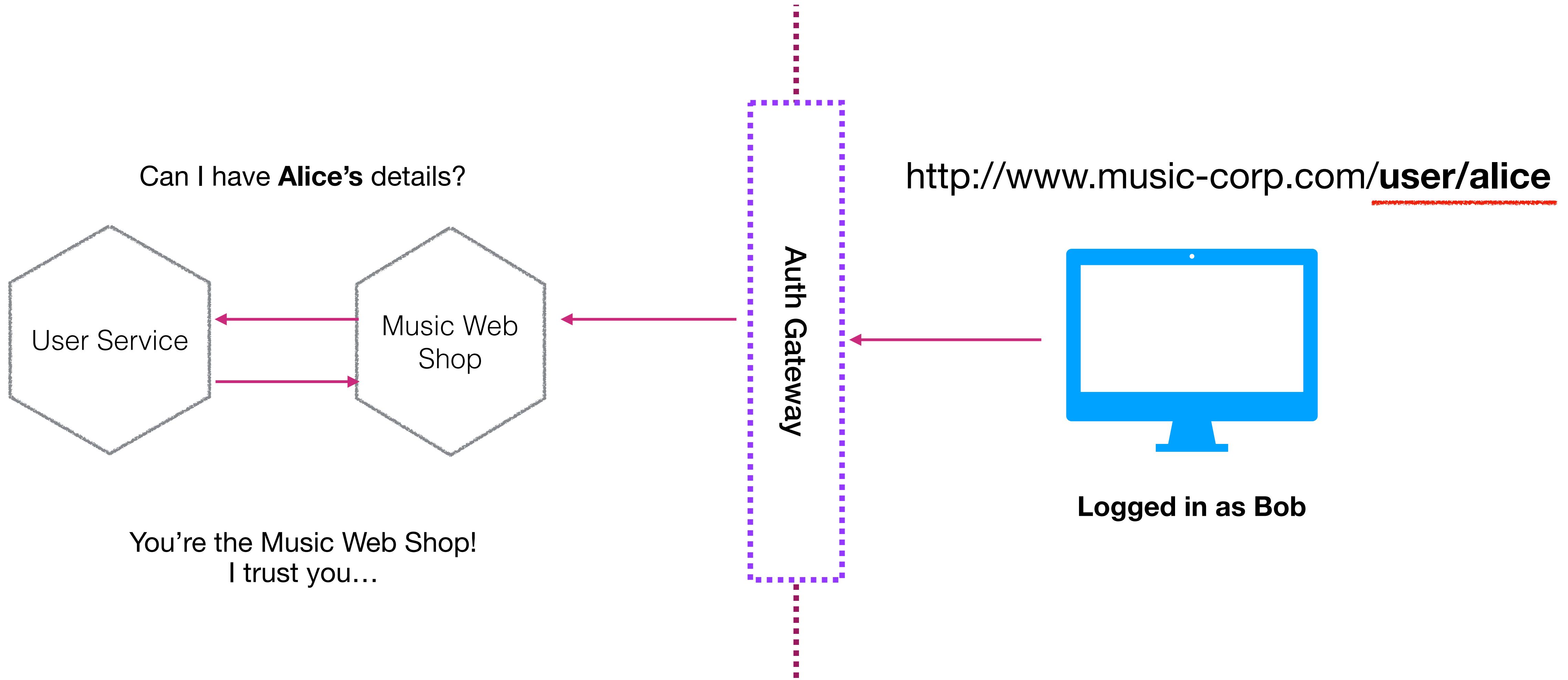
DOWNSTREAM AUTH - IMPLICIT TRUST?



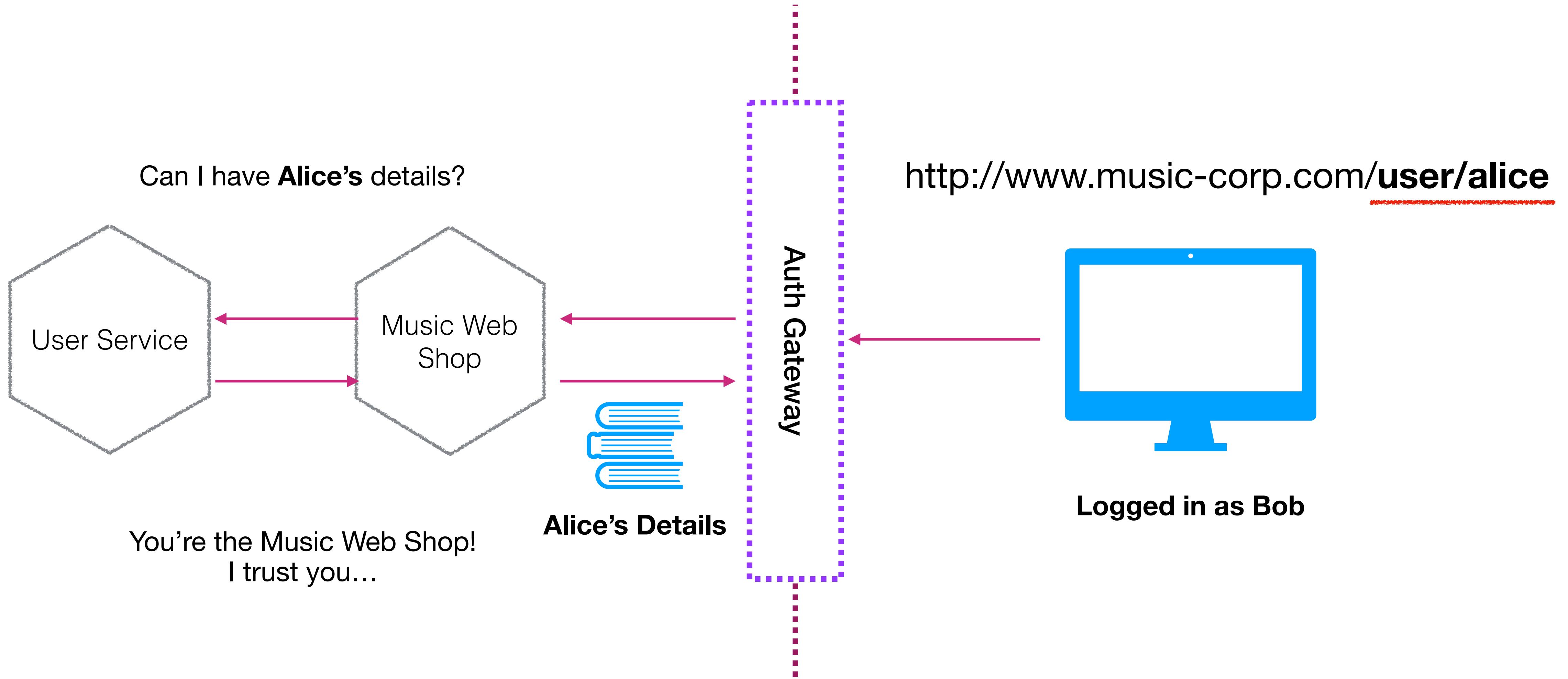
DOWNSTREAM AUTH - IMPLICIT TRUST?



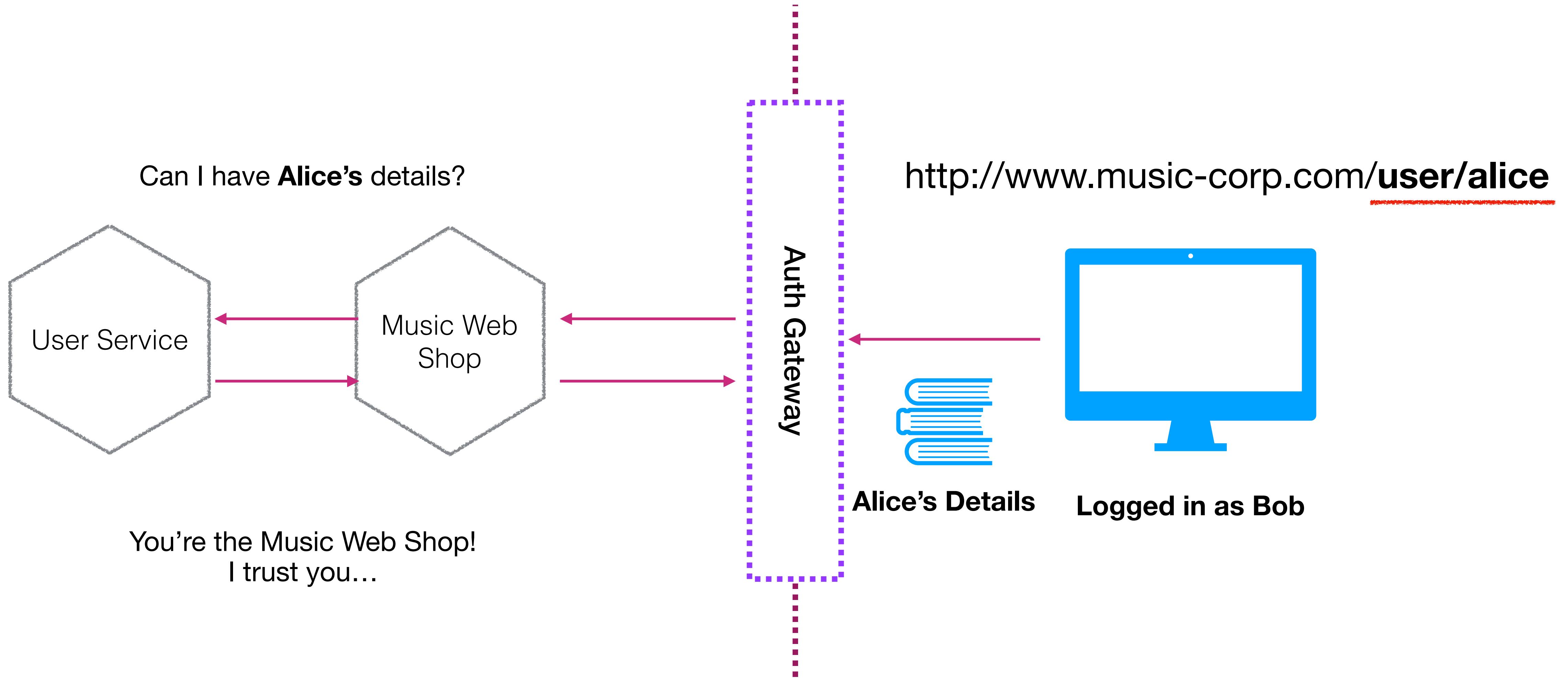
DOWNSTREAM AUTH - IMPLICIT TRUST?



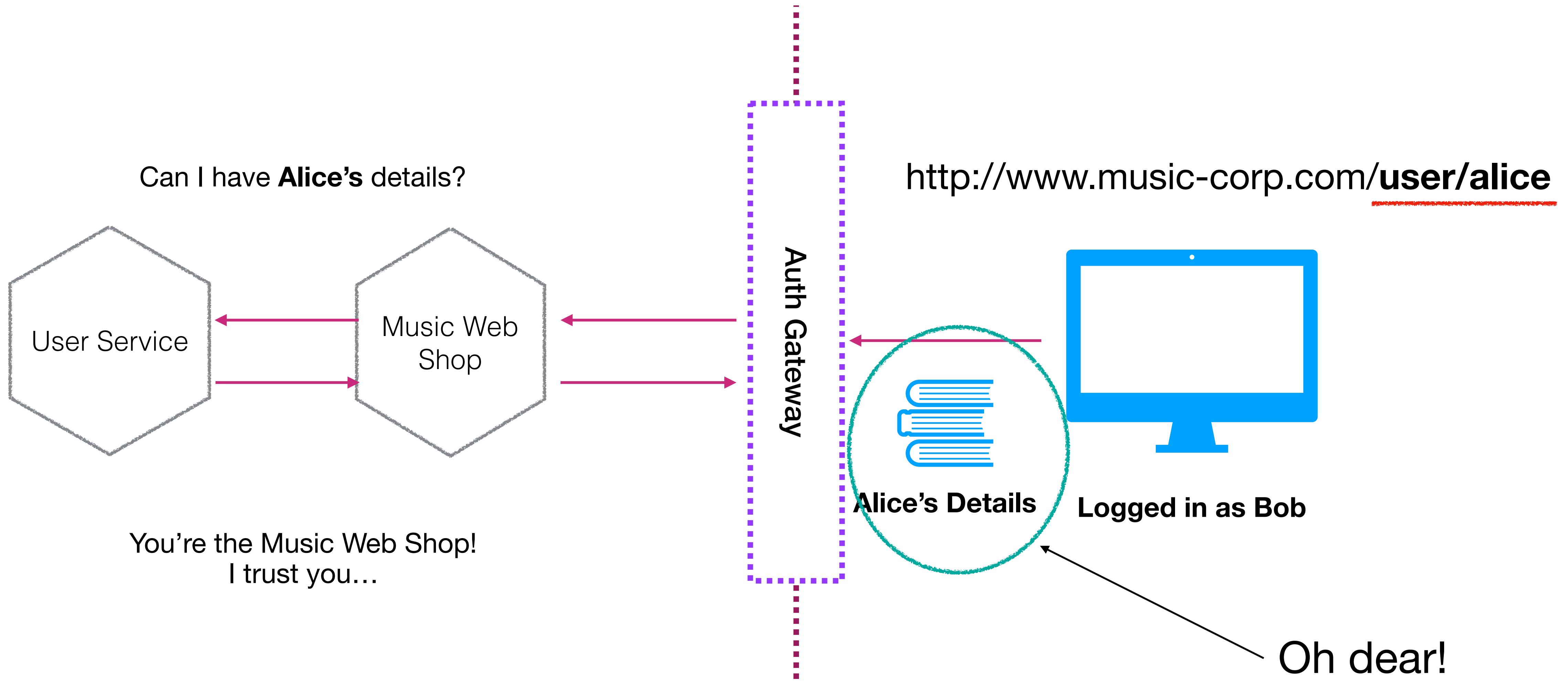
DOWNSTREAM AUTH - IMPLICIT TRUST?



DOWNSTREAM AUTH - IMPLICIT TRUST?



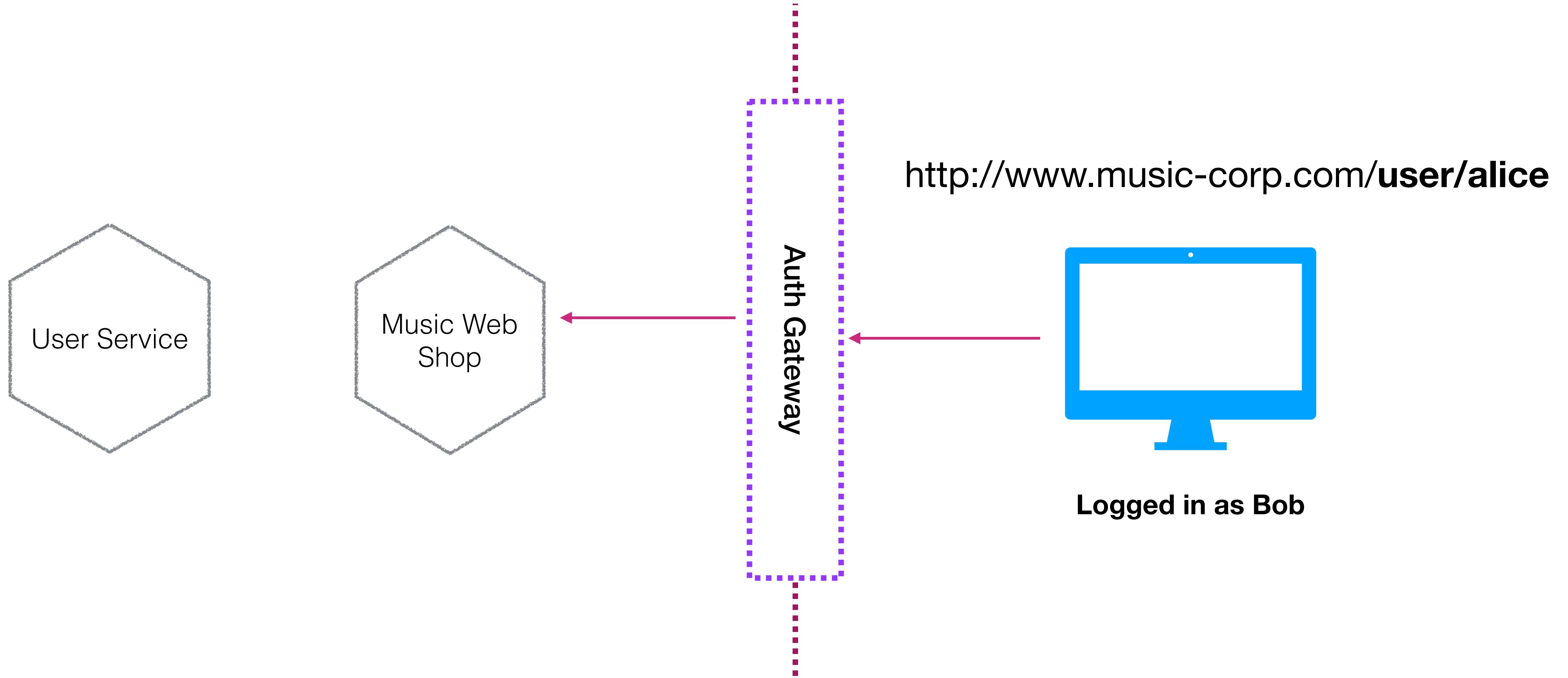
DOWNSTREAM AUTH - IMPLICIT TRUST?



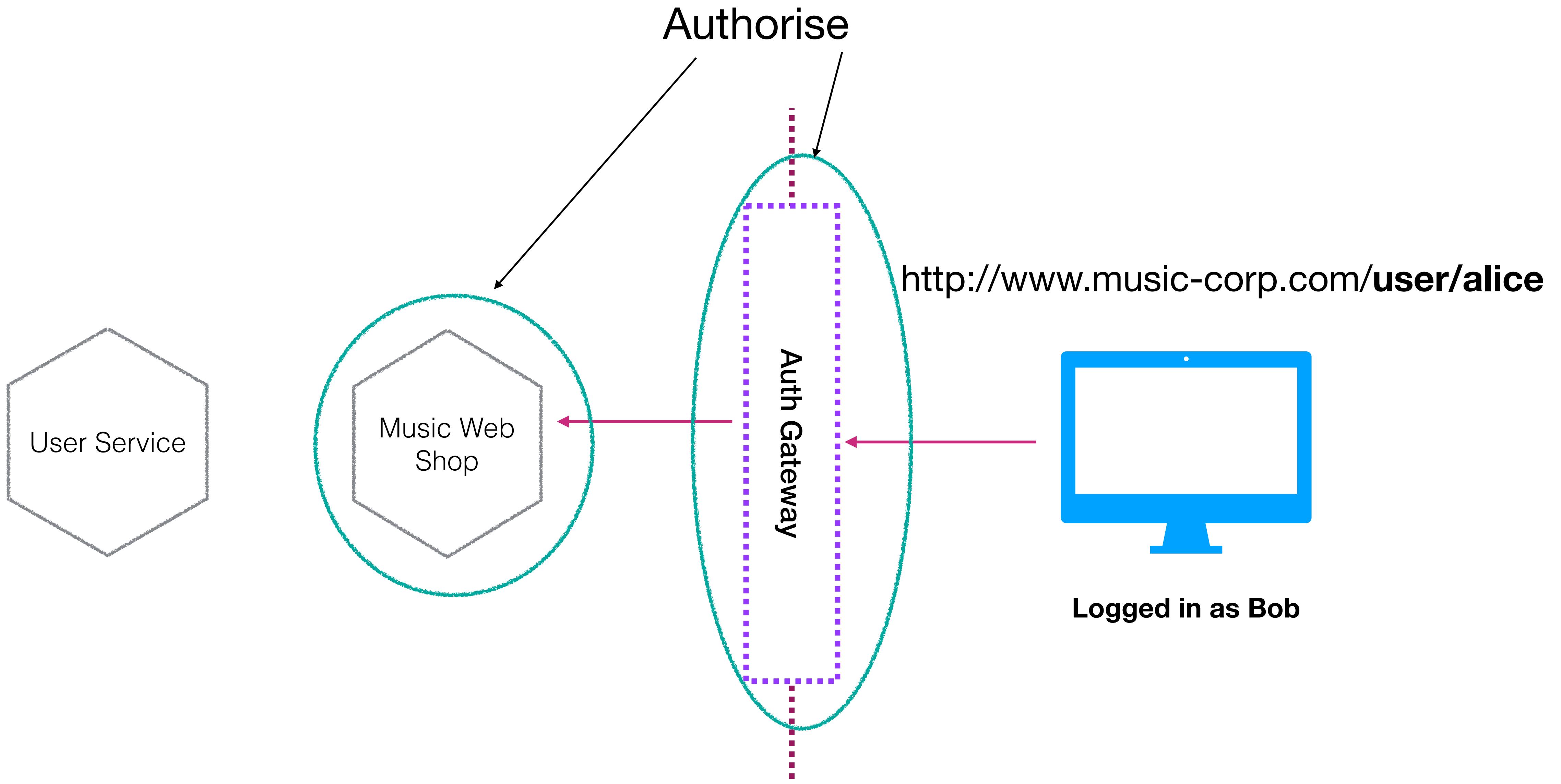
Confused
Deputy
Problem!



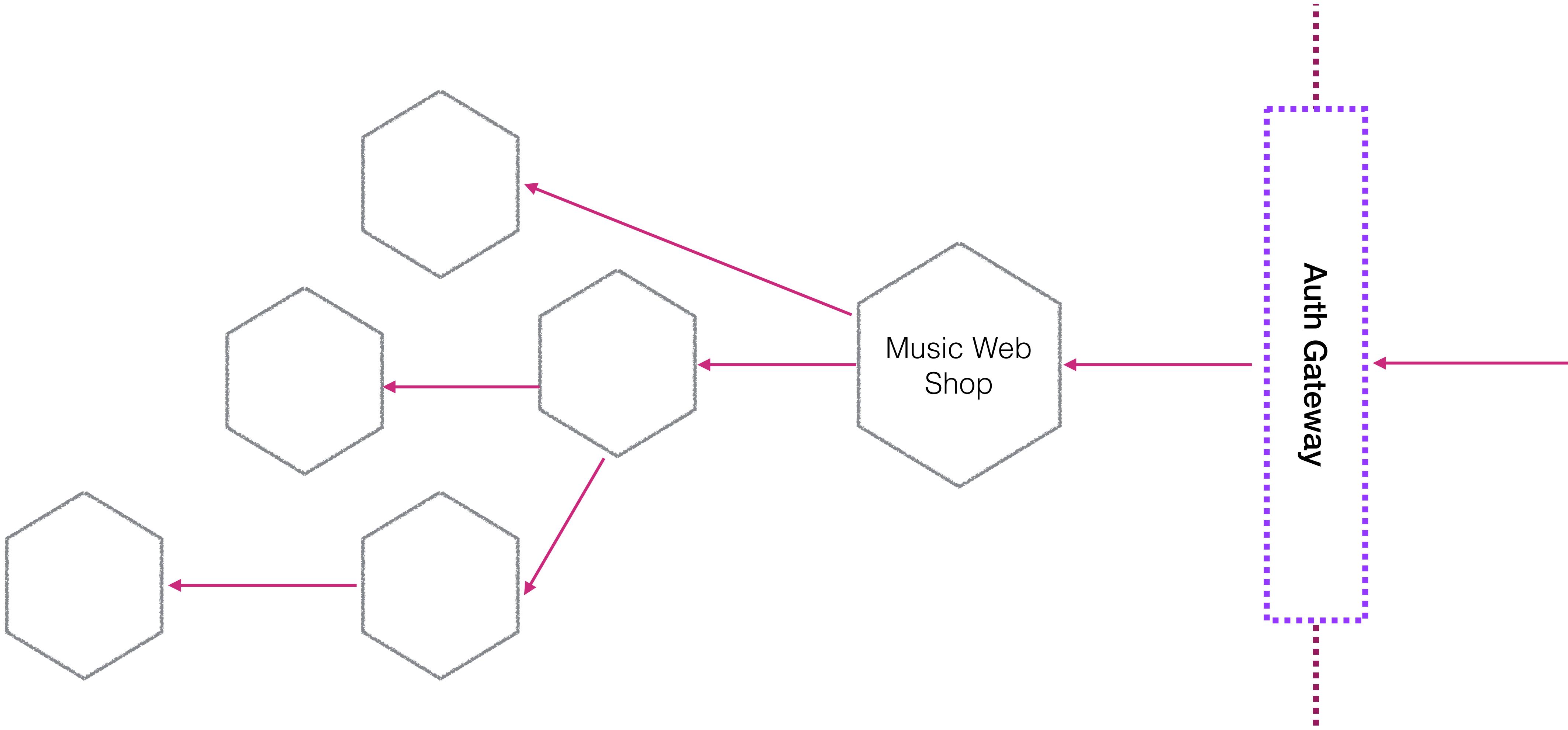
AUTHORISE UPSTREAM?



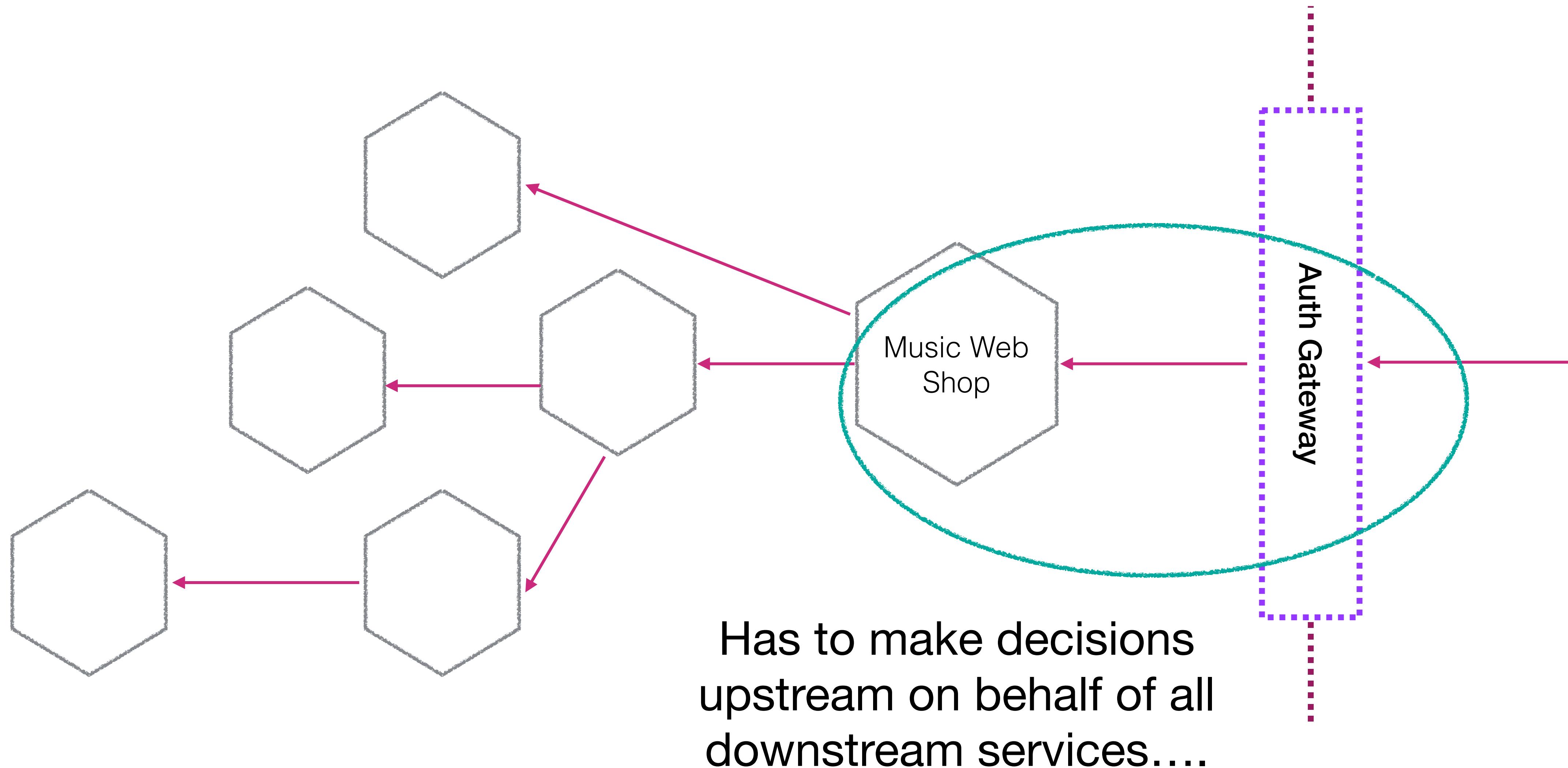
AUTHORISE UPSTREAM?



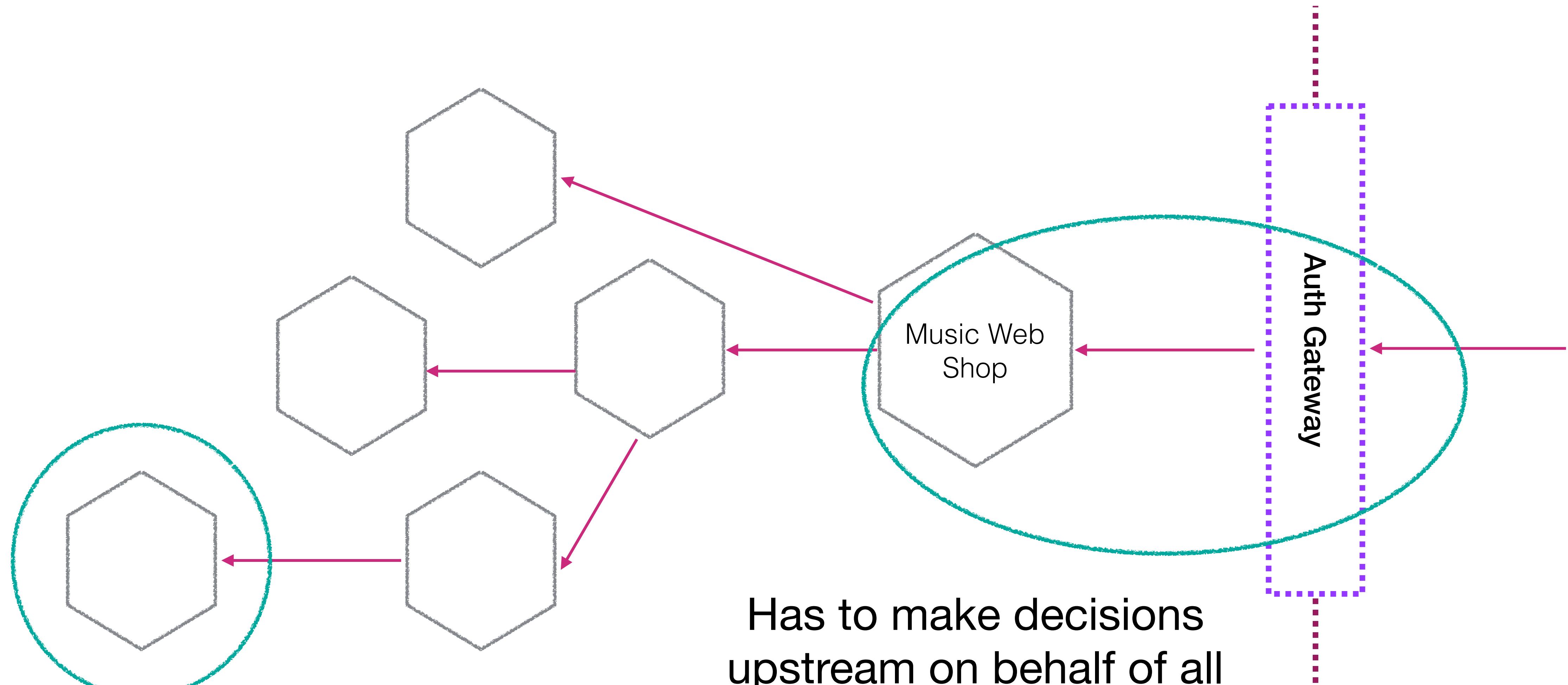
WHERE DO THE SMARTS LIVE?



WHERE DO THE SMARTS LIVE?



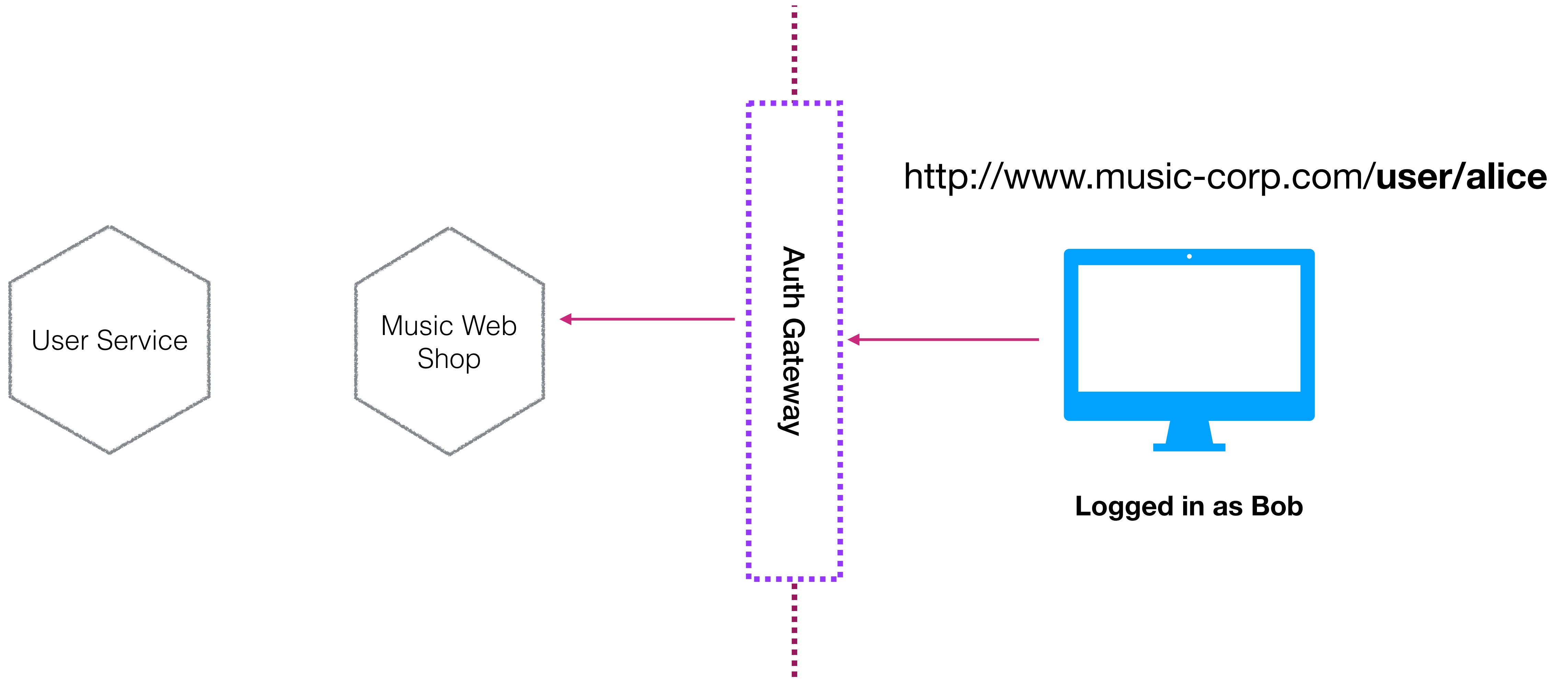
WHERE DO THE SMARTS LIVE?



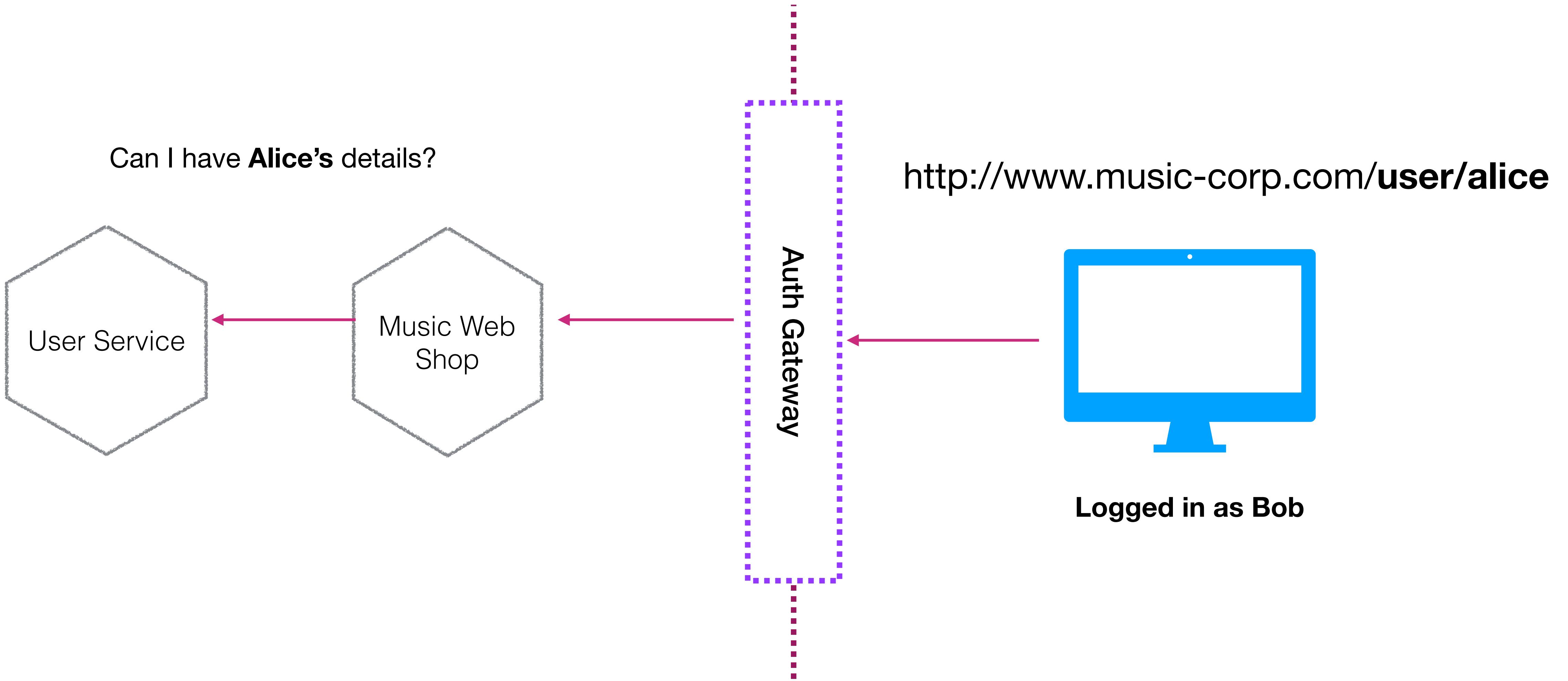
But it can be preferable to push this logic to the service itself

Has to make decisions upstream on behalf of all downstream services....

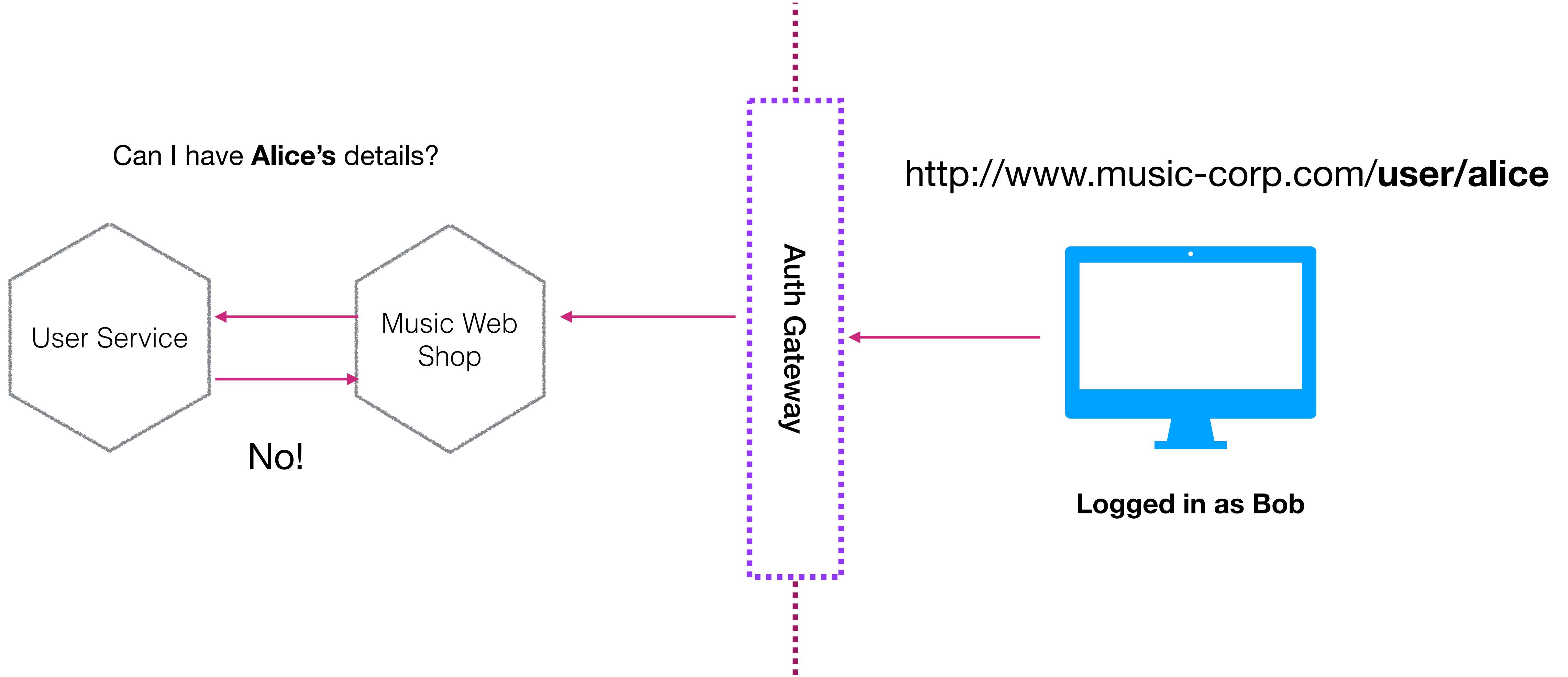
AUTHORISE DOWNSTREAM



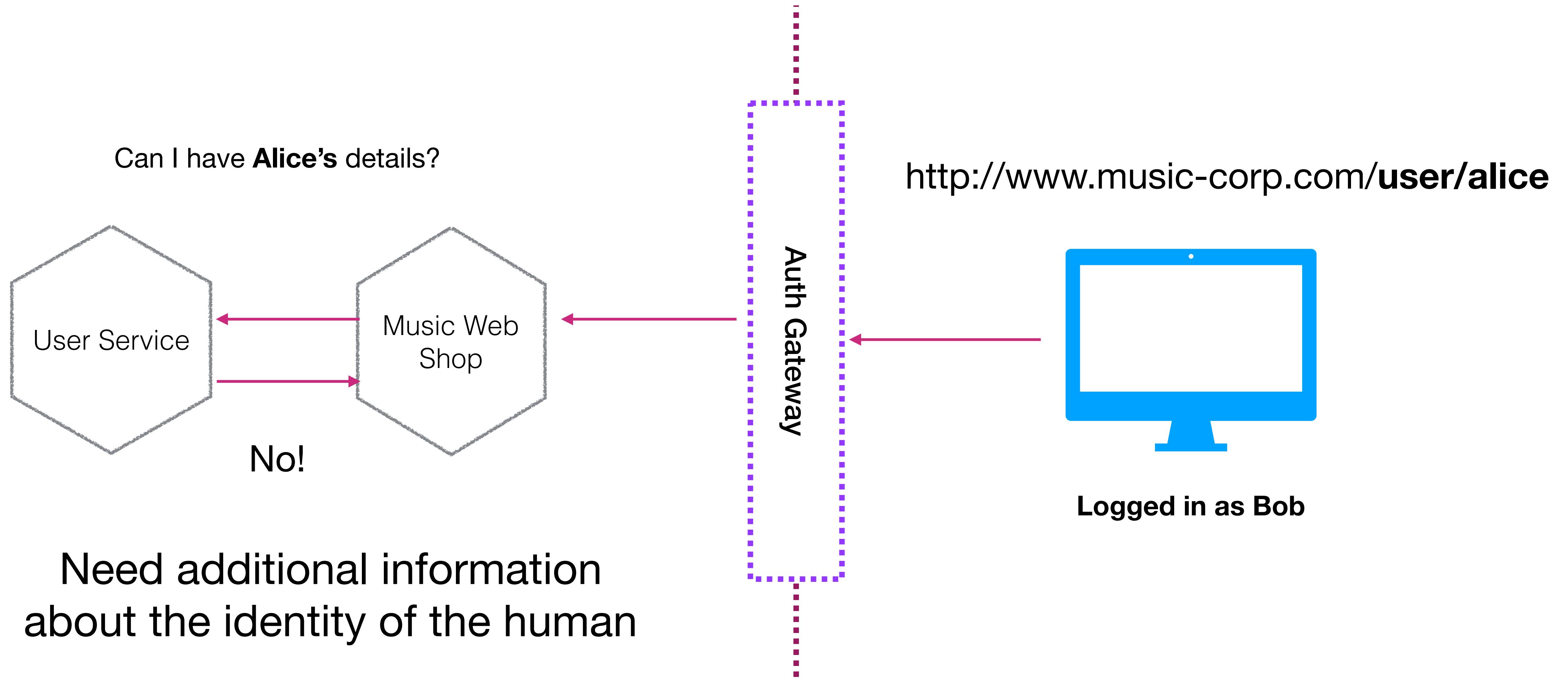
AUTHORISE DOWNSTREAM



AUTHORISE DOWNSTREAM



AUTHORISE DOWNSTREAM





Decoder Encoder Validator API Try it out!

GitHub Audit



JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.

JWT.IO allows you to decode, verify and generate JWT.

<https://jwt.io/>

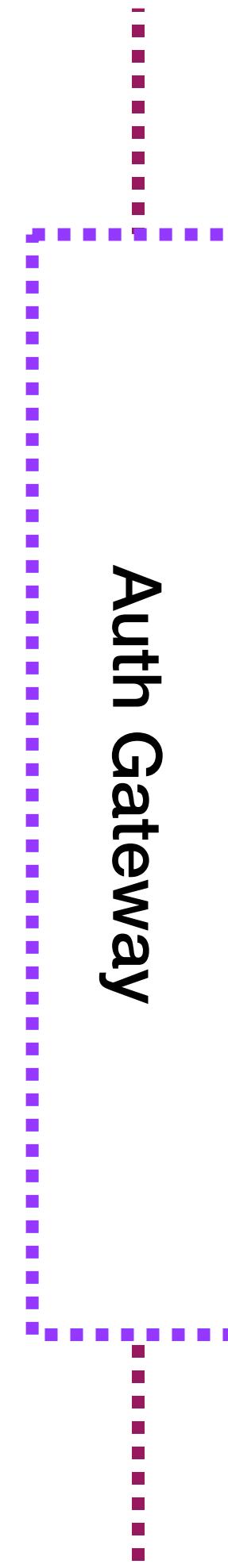
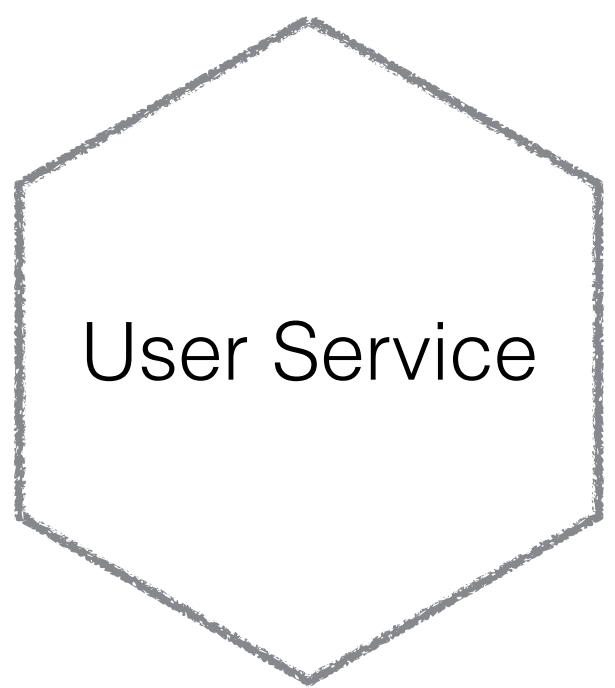
<https://jwt.io/>

```
{  
  "id": "402ndj39",  
  "name": "Alice Alison"  
}
```

```
{  
  "id": "402ndj39",  
  "name": "Alice Alison"  
}
```

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaXNTb2NpYWwiOnRydWV9.
4pcPyMD09o1PSyXnrXCjTwXyr4BsezdI1AVTmud2fU4

USING JWT TOKENS

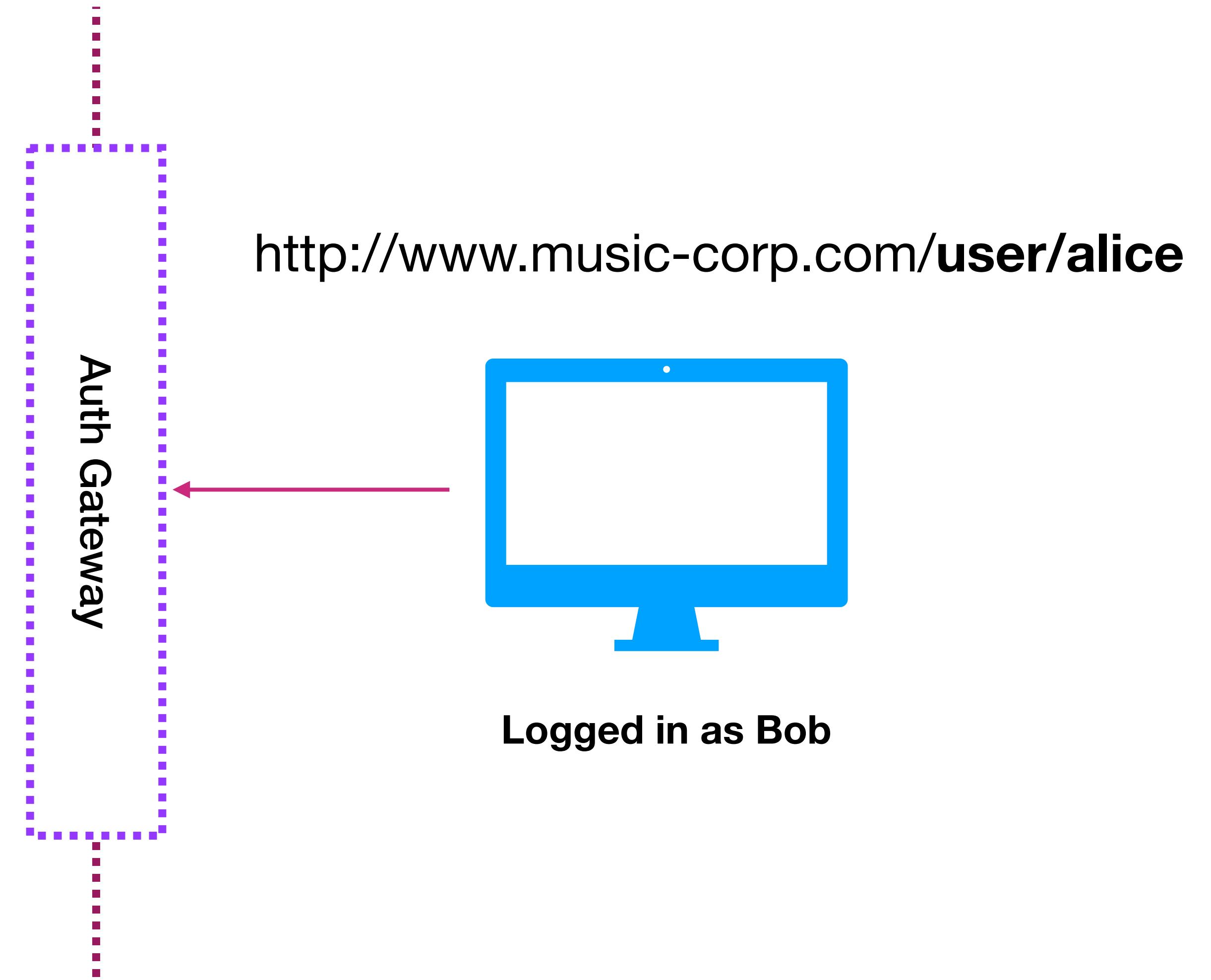
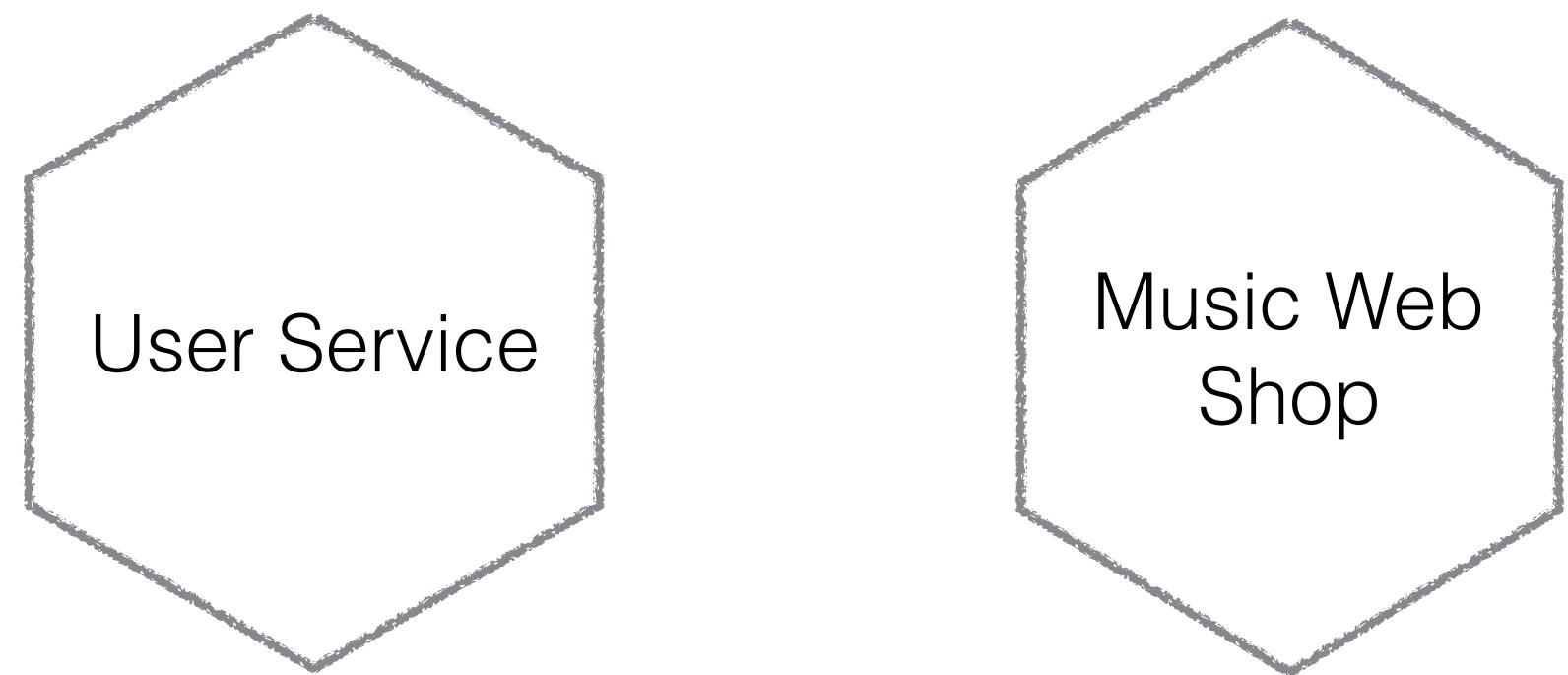


`http://www.music-corp.com/user/alice`

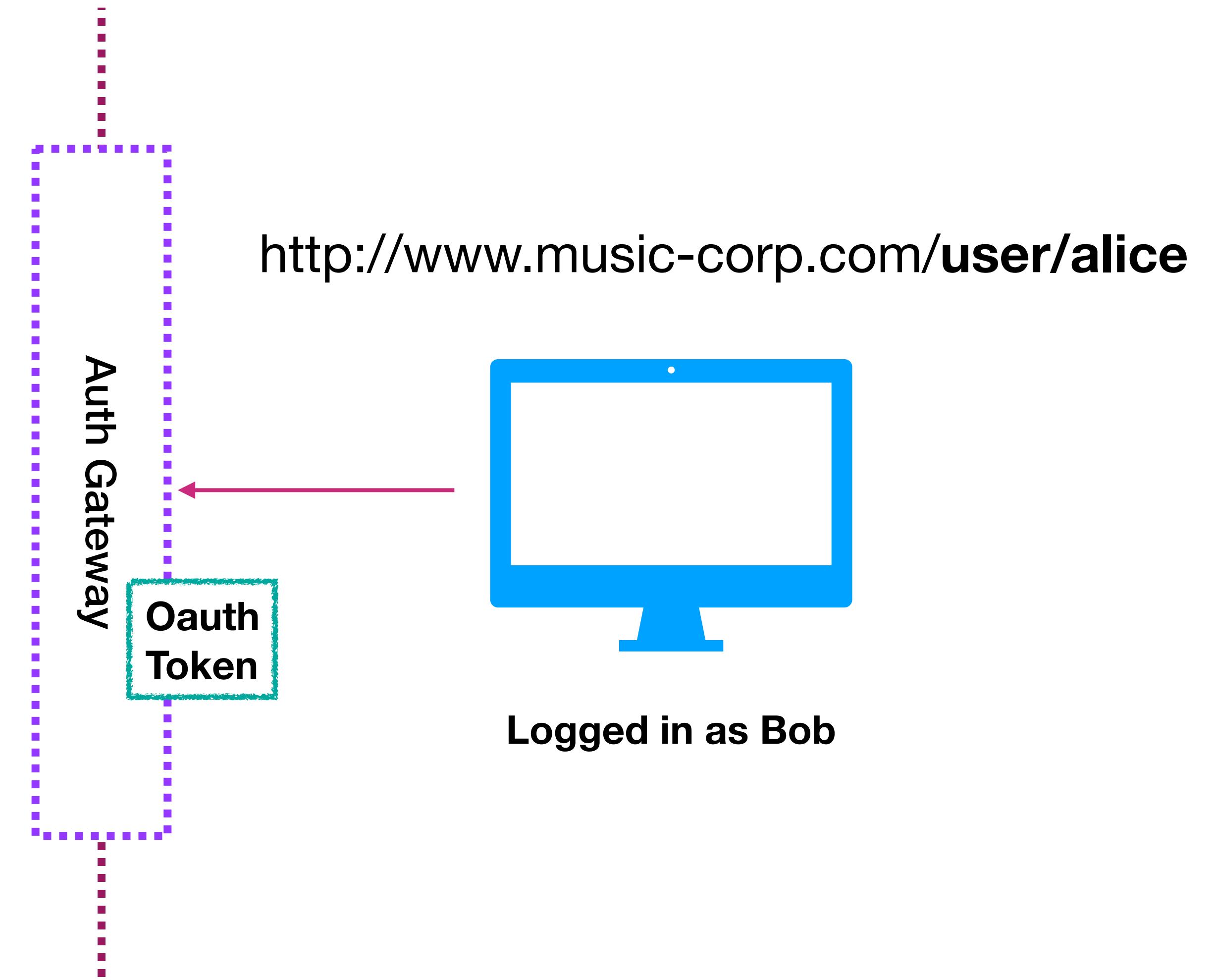
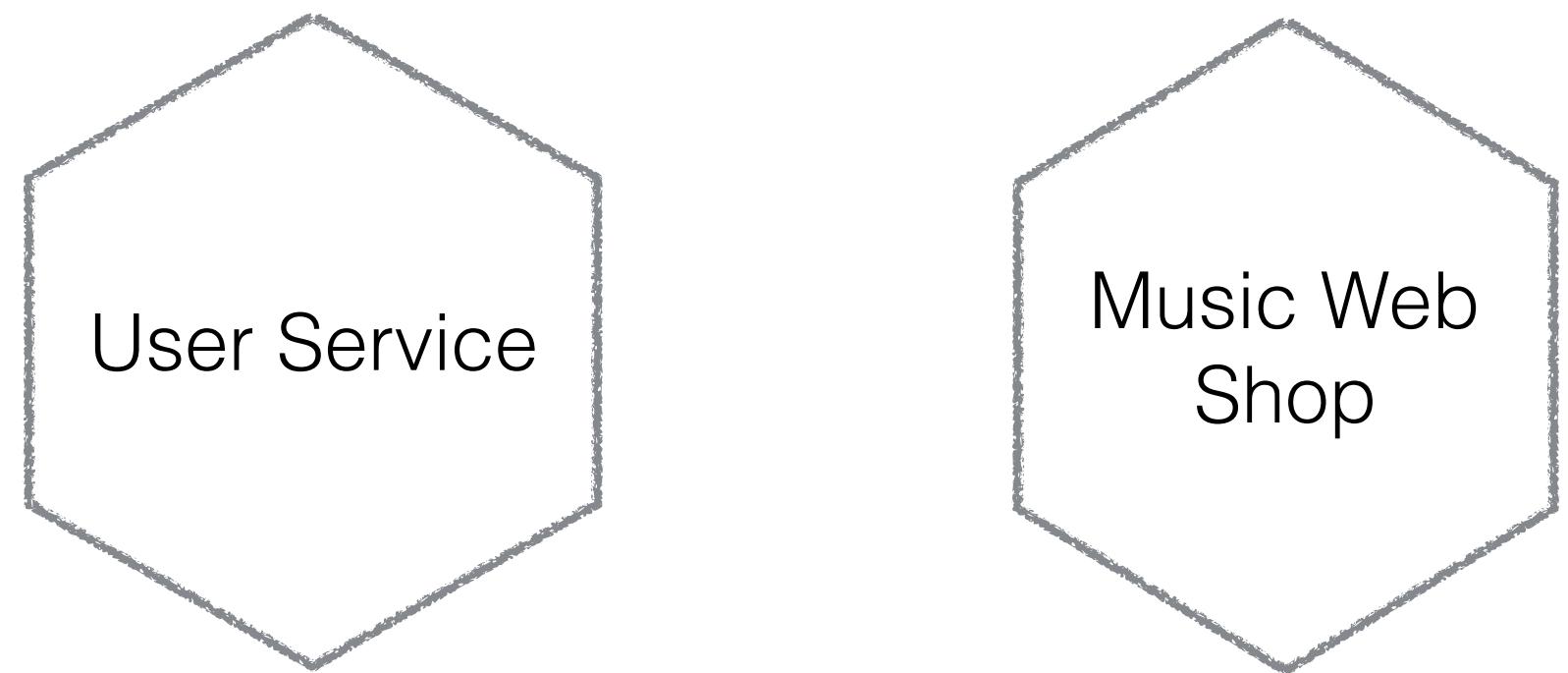


Logged in as Bob

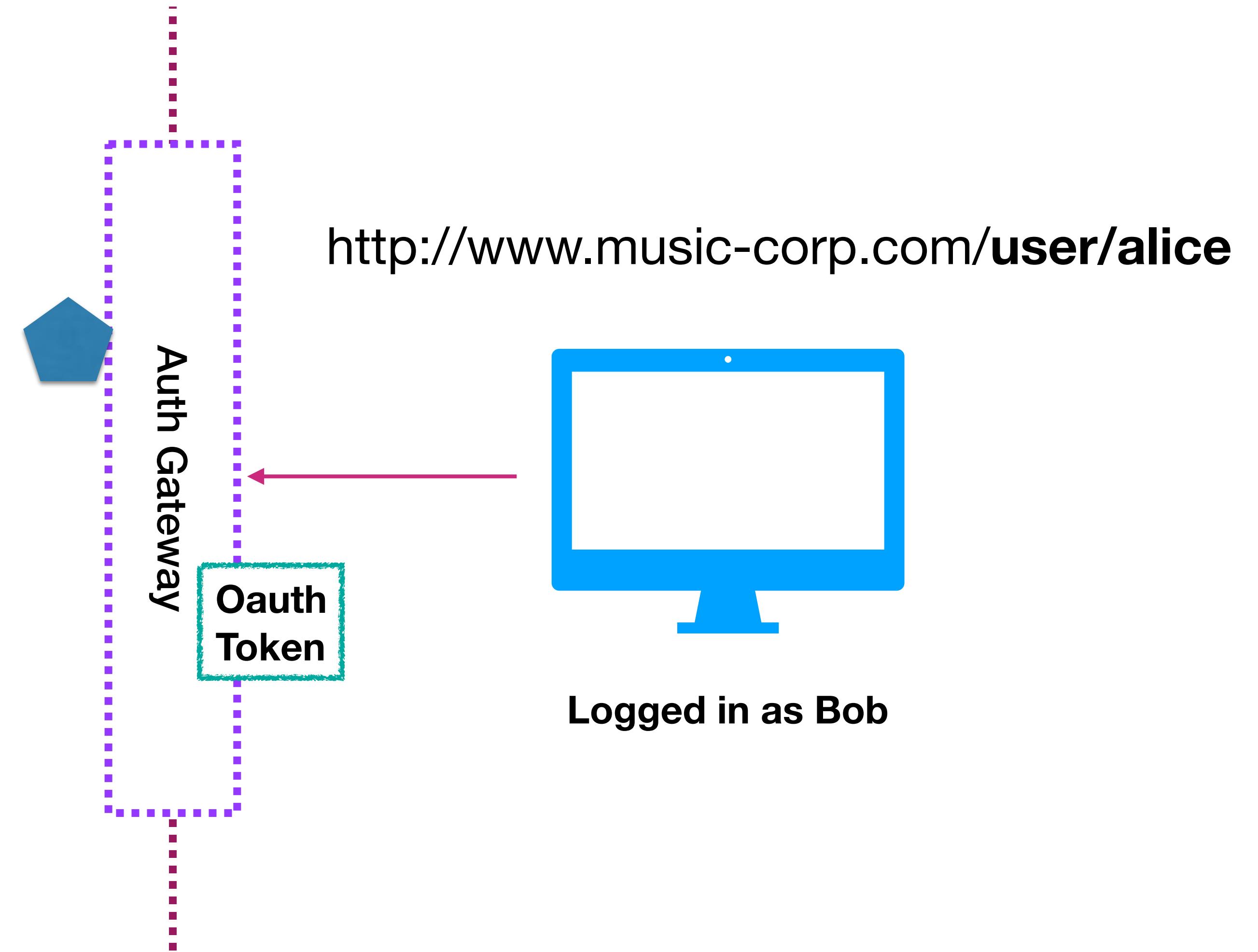
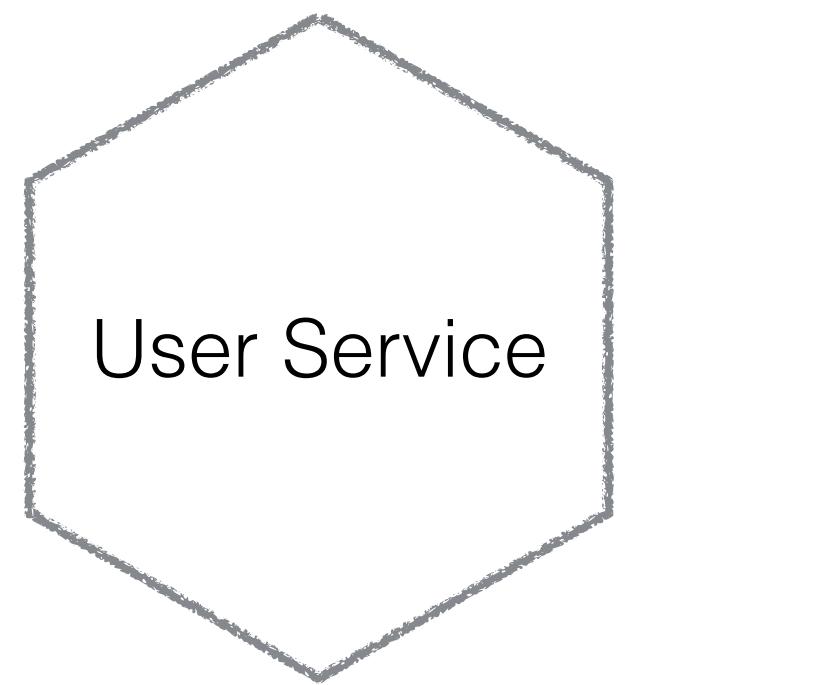
USING JWT TOKENS



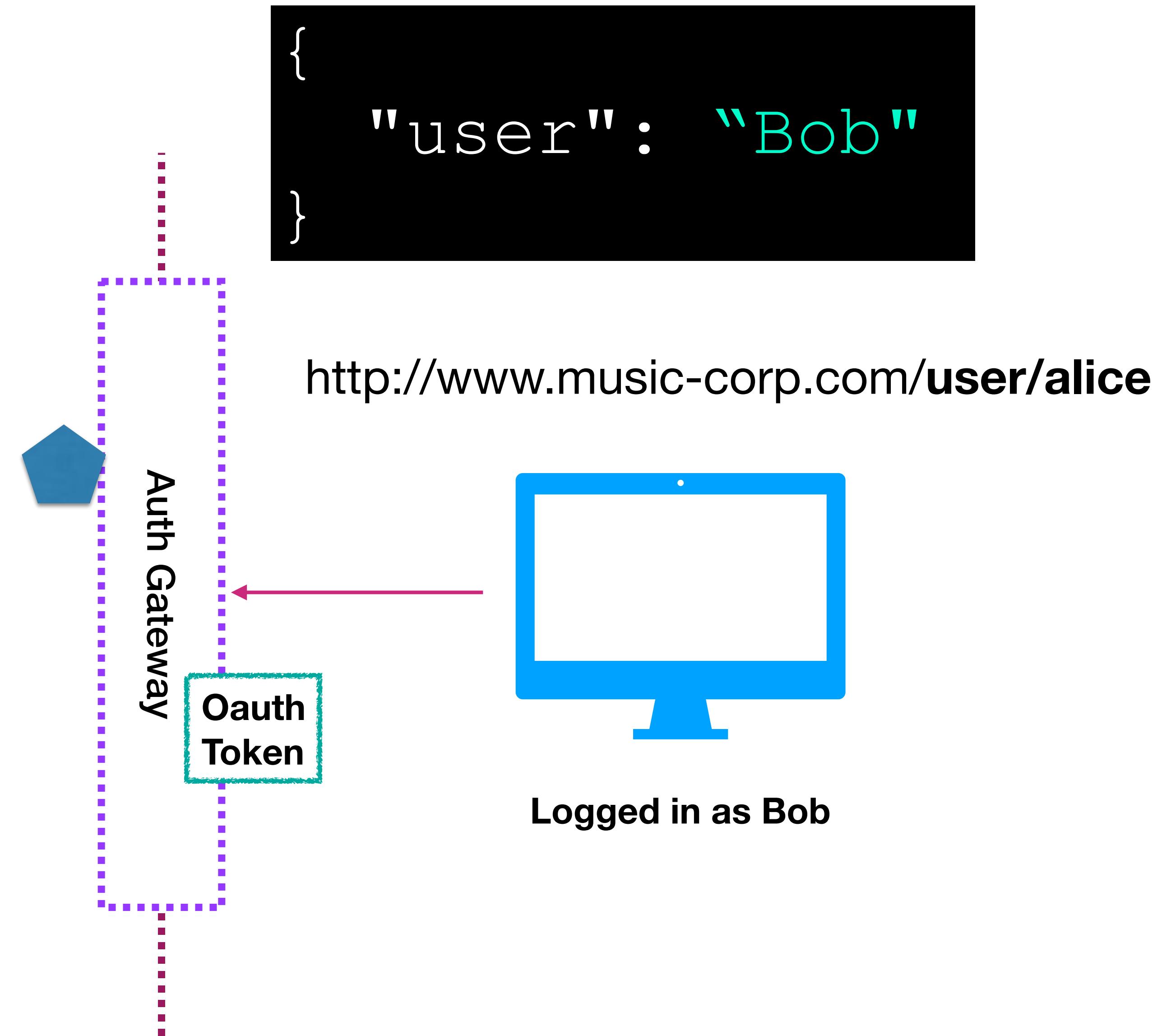
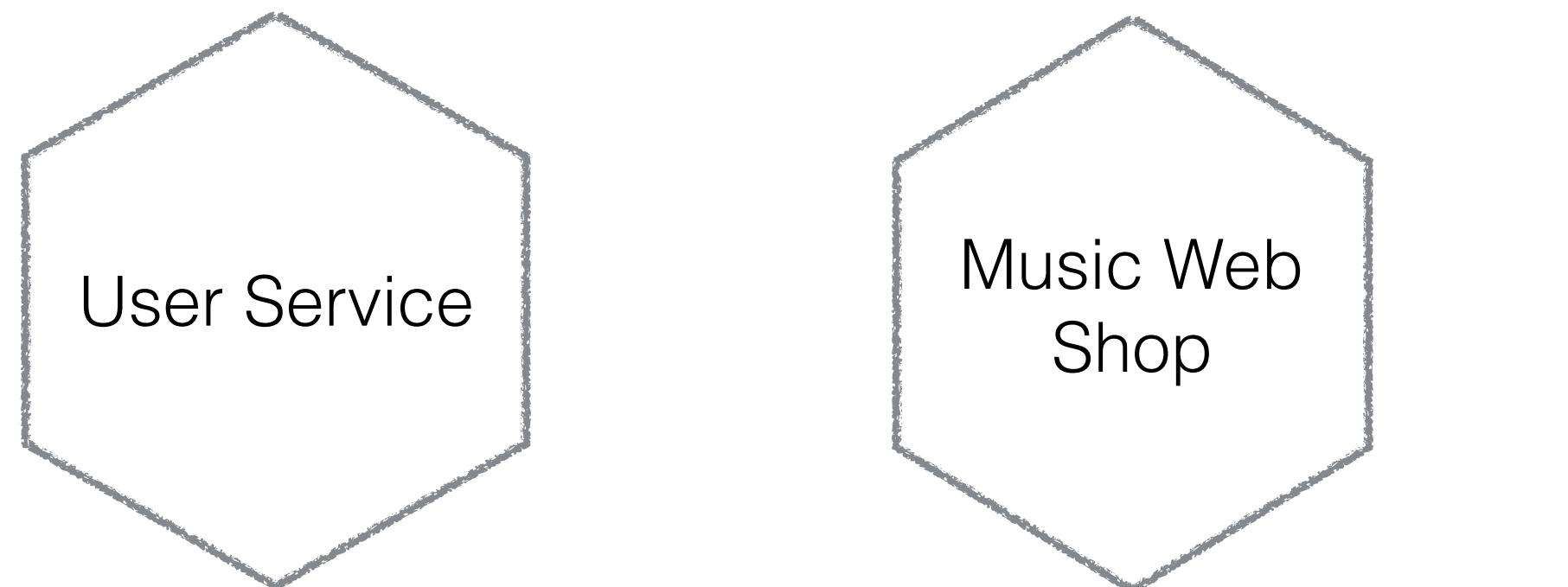
USING JWT TOKENS



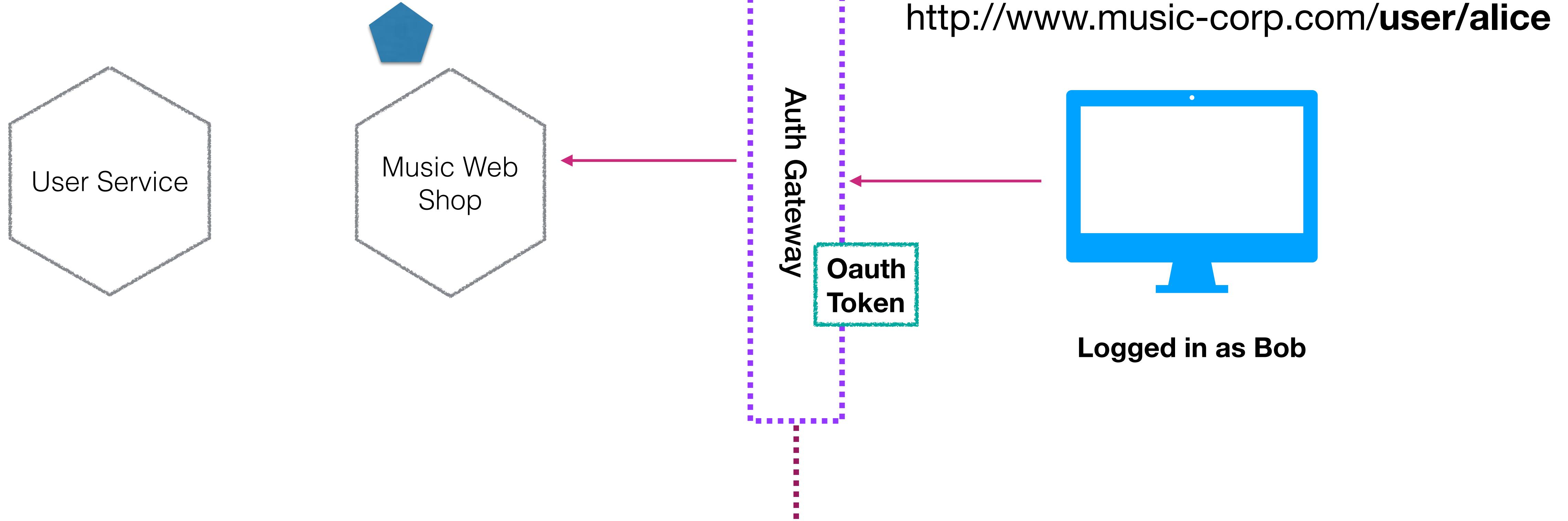
USING JWT TOKENS



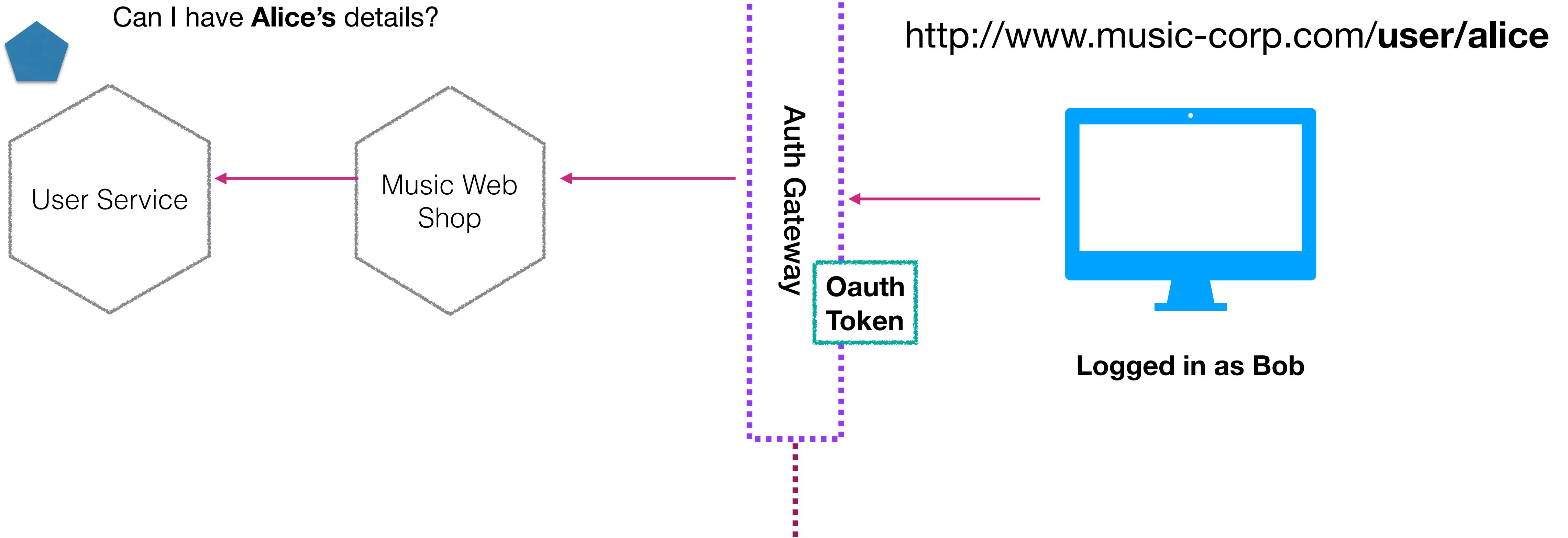
USING JWT TOKENS



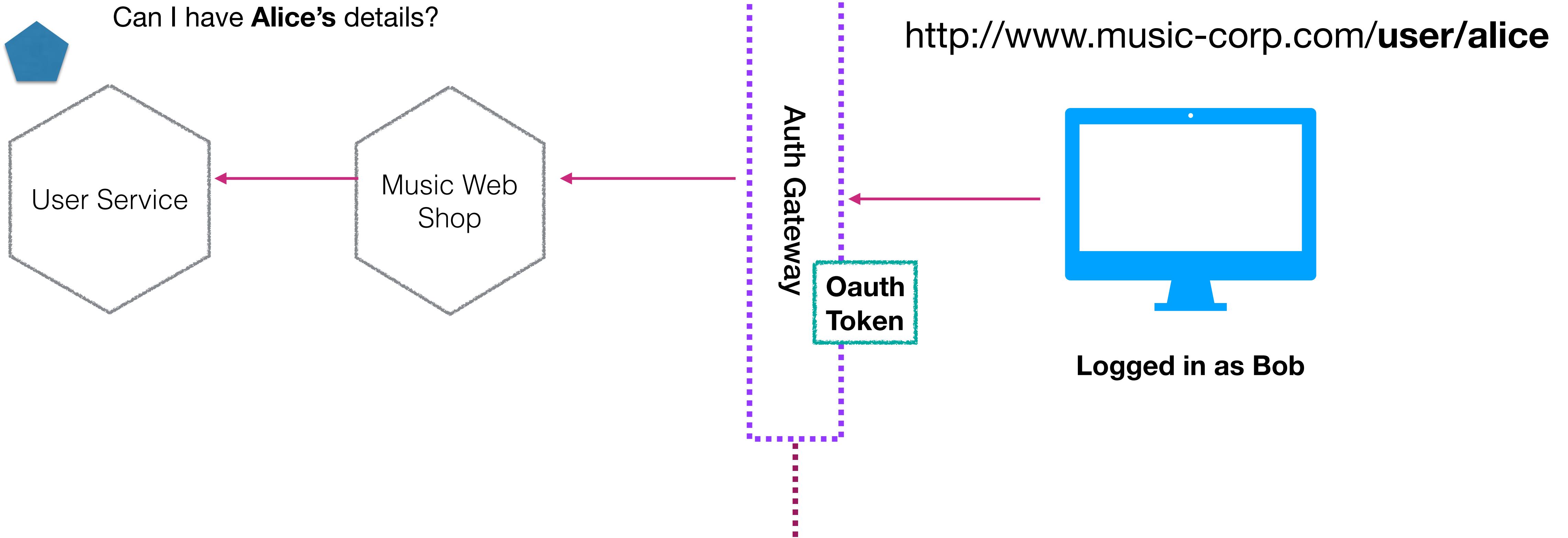
USING JWT TOKENS



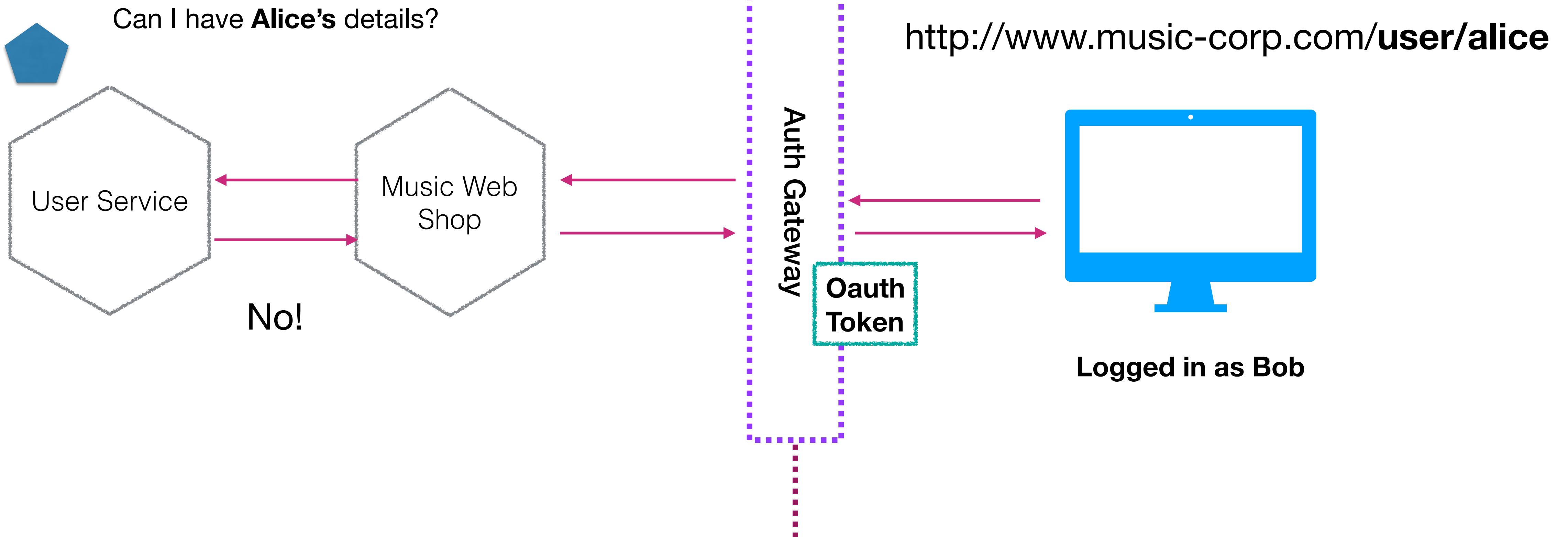
USING JWT TOKENS



USING JWT TOKENS



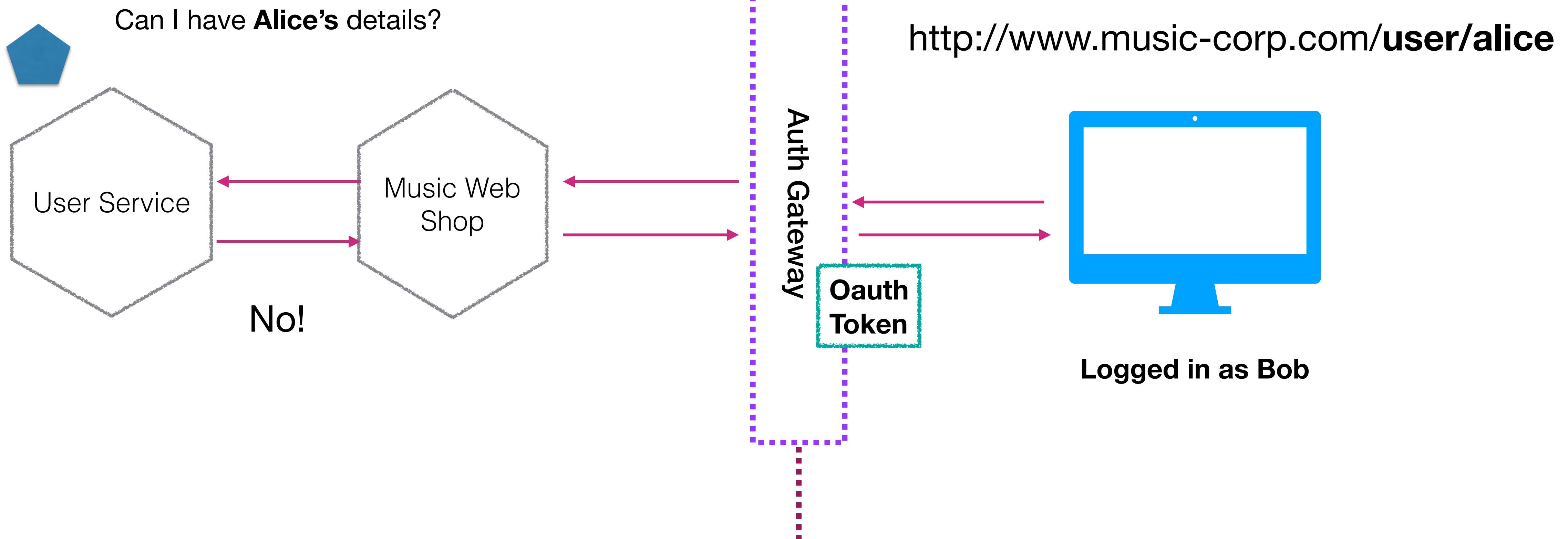
USING JWT TOKENS



USING JWT TOKENS

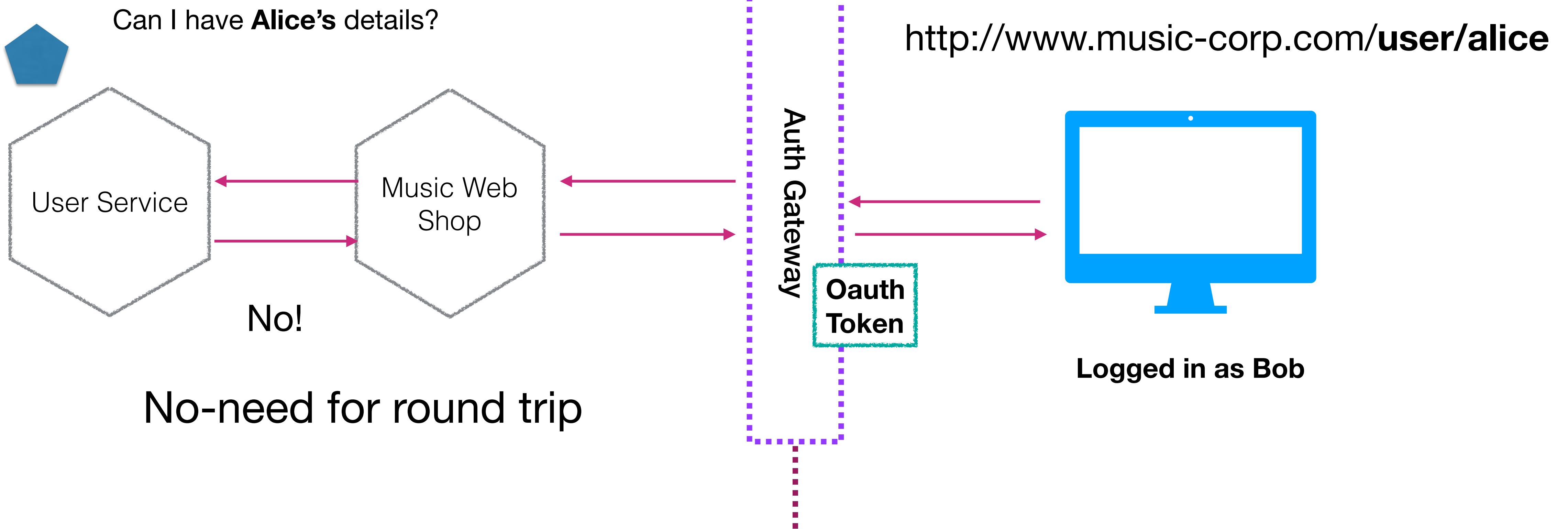
Token can be validated in the user service

```
{  
  "user": "Bob"  
}
```



USING JWT TOKENS

Token can be validated in the user service



SERVICE MESHES



Linkerd

<https://linkerd.io>

SERVICE MESHES



Linkerd

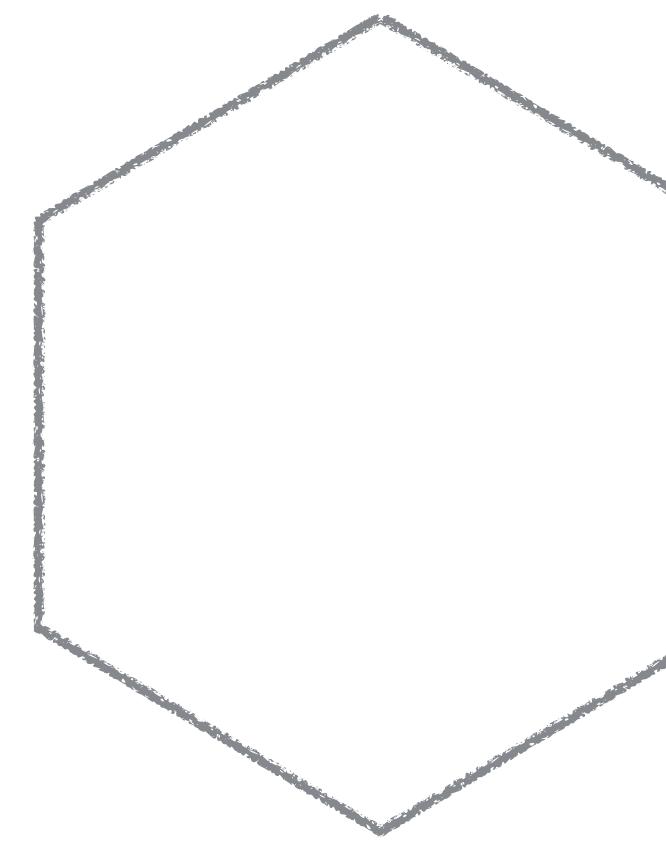
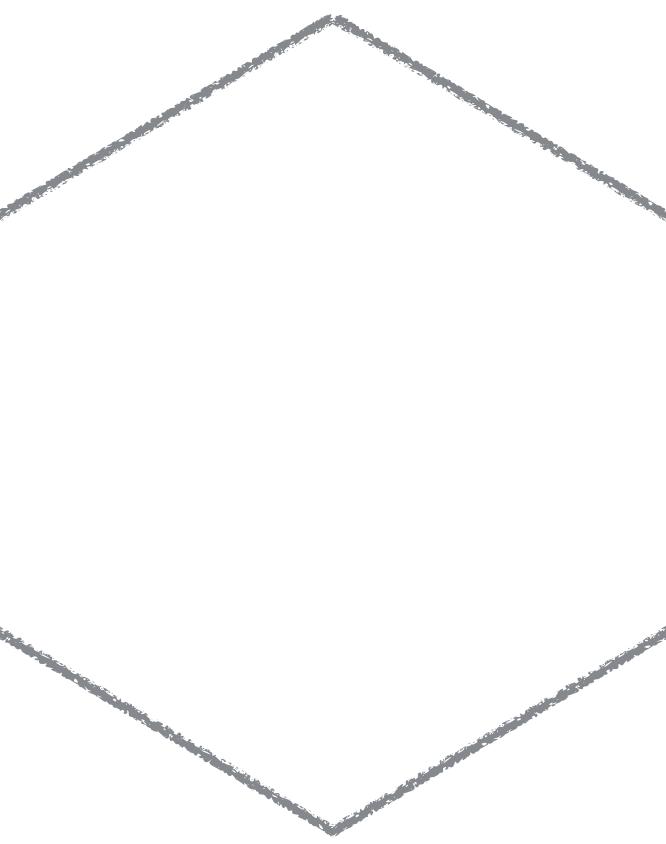
<https://linkerd.io>



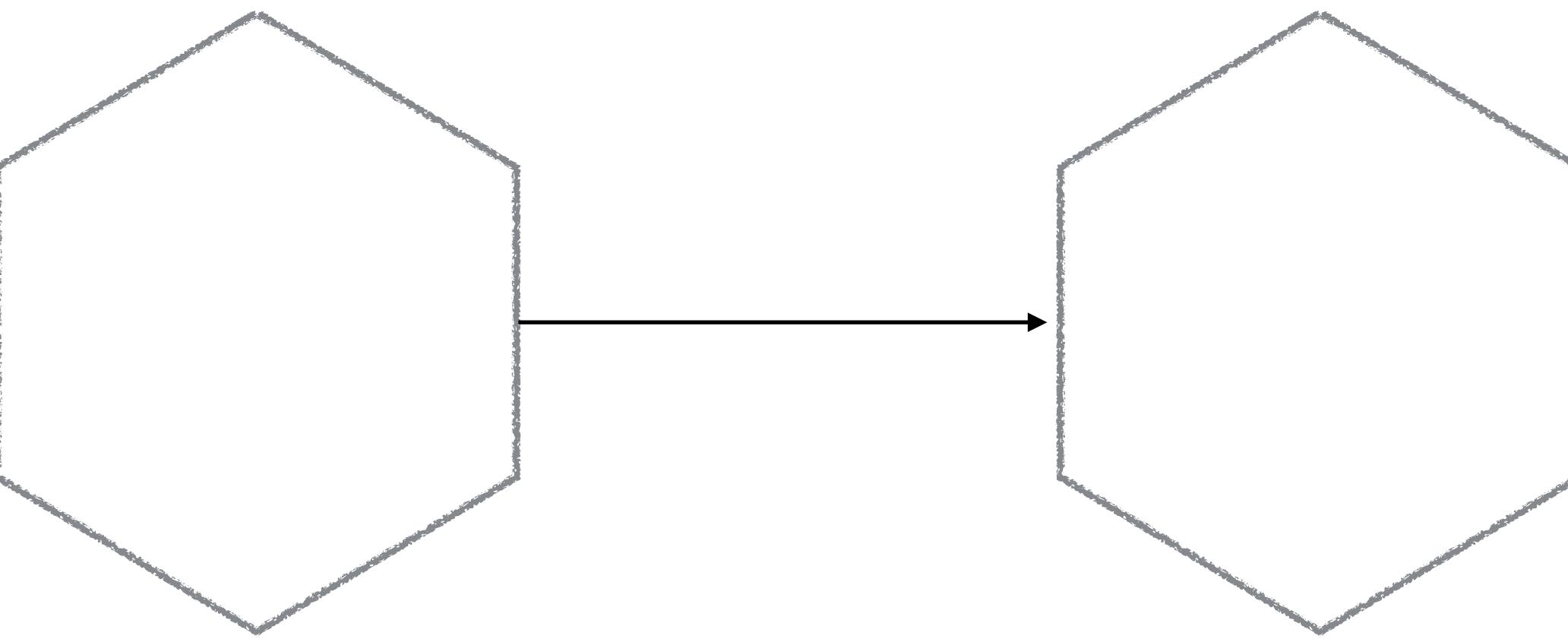
Istio

<https://istio.io>

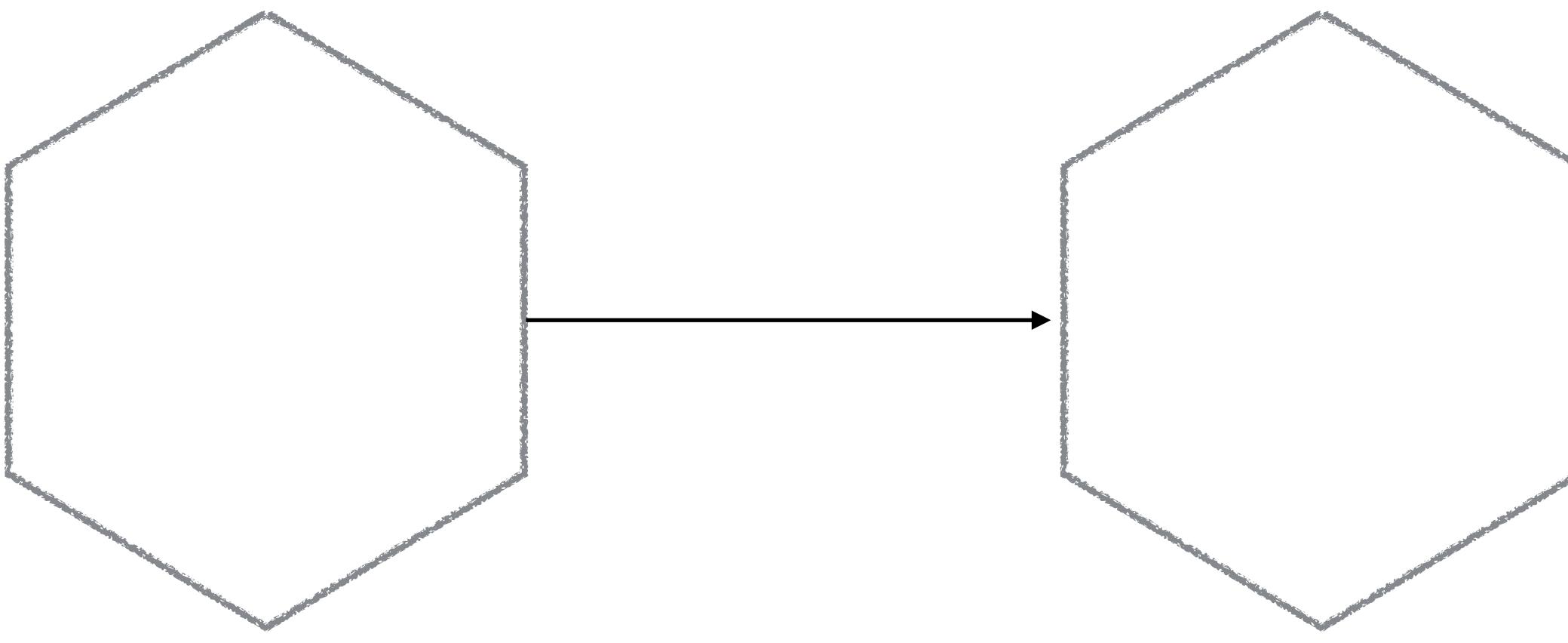
COMMON CONNECTION CONCERNS



COMMON CONNECTION CONCERNS

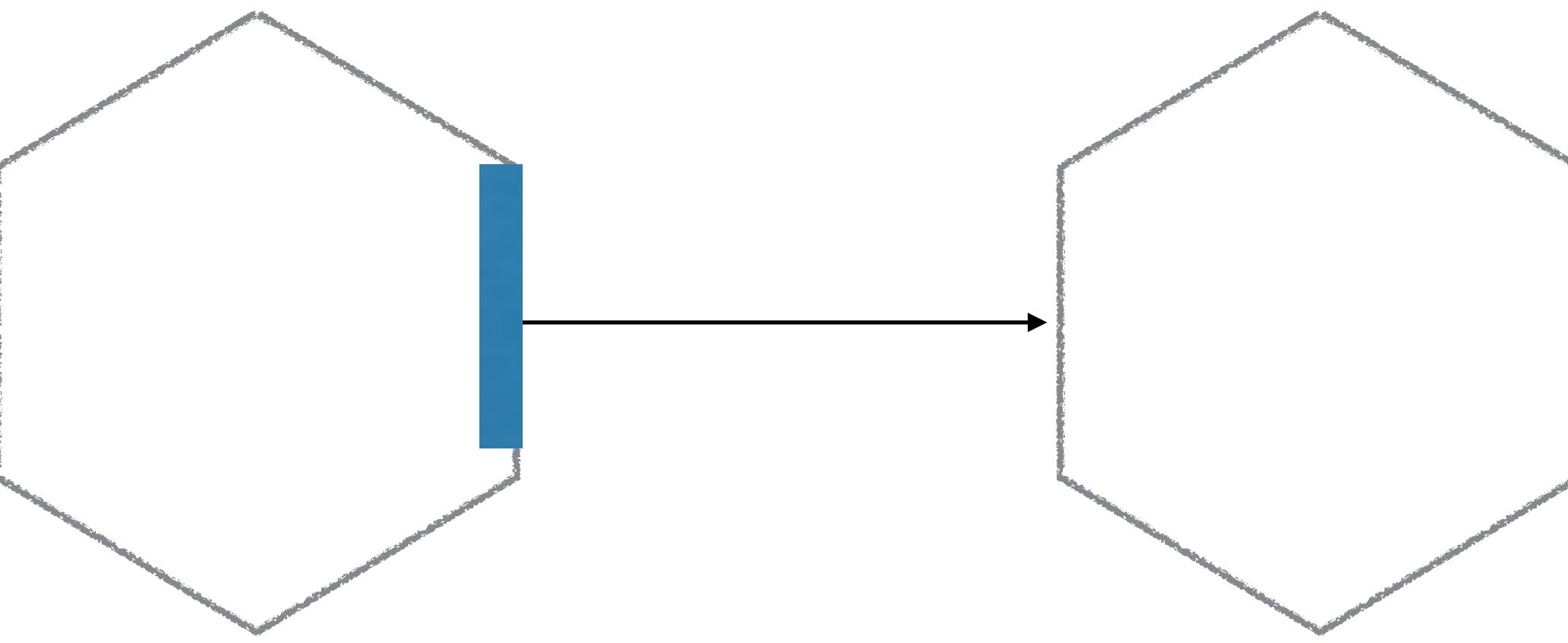


COMMON CONNECTION CONCERNS



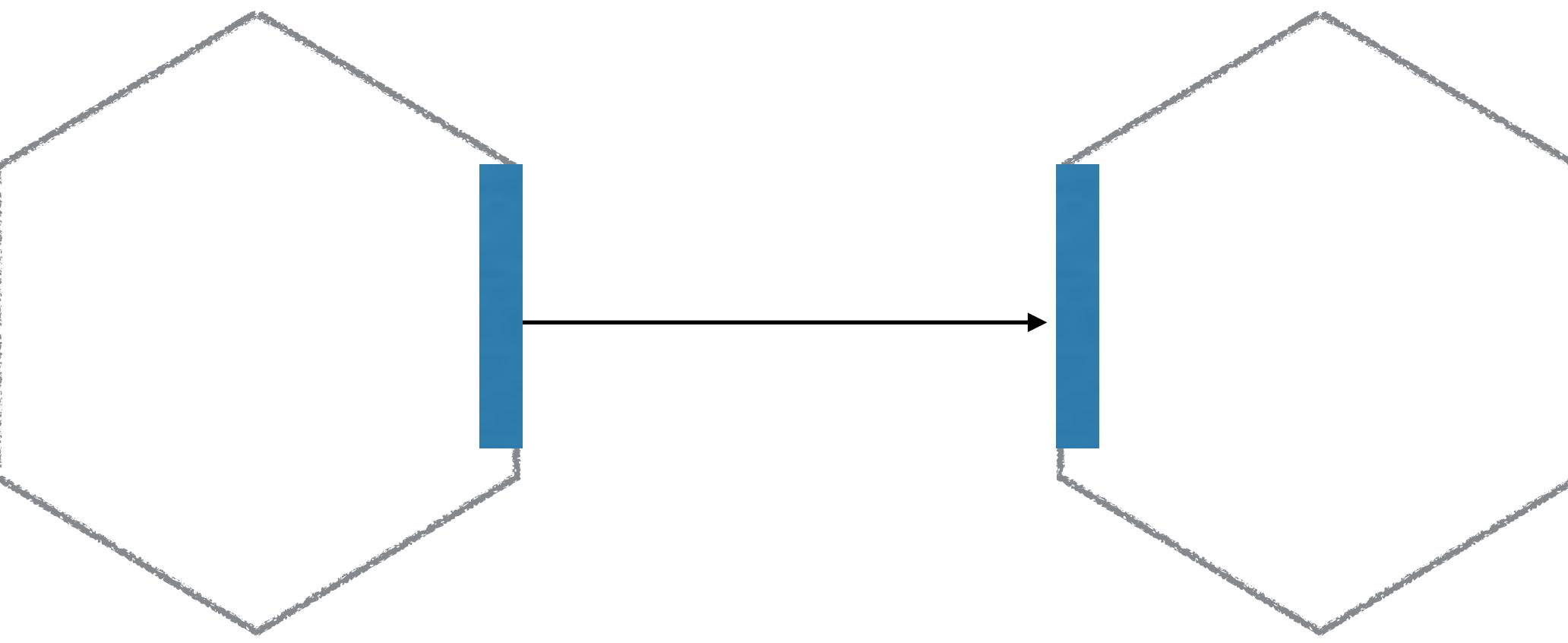
Tracing

COMMON CONNECTION CONCERNS



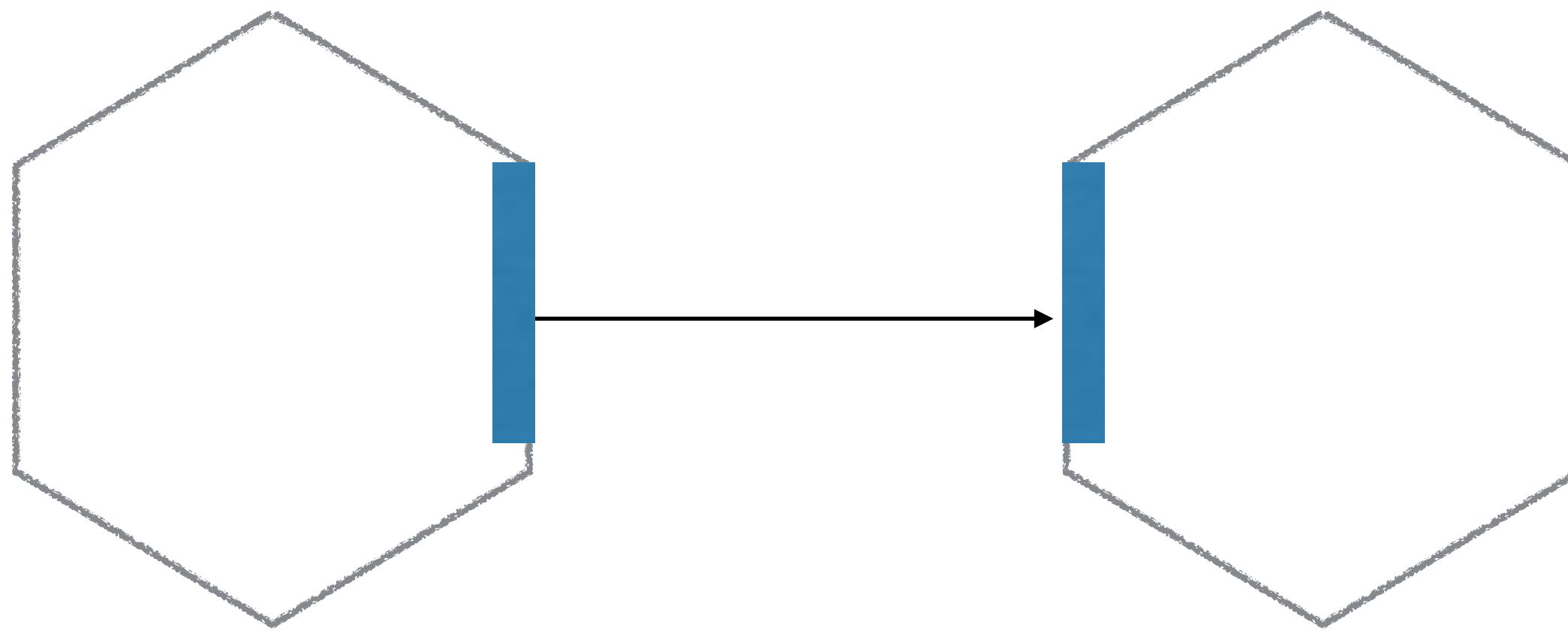
Tracing

COMMON CONNECTION CONCERNS



Tracing

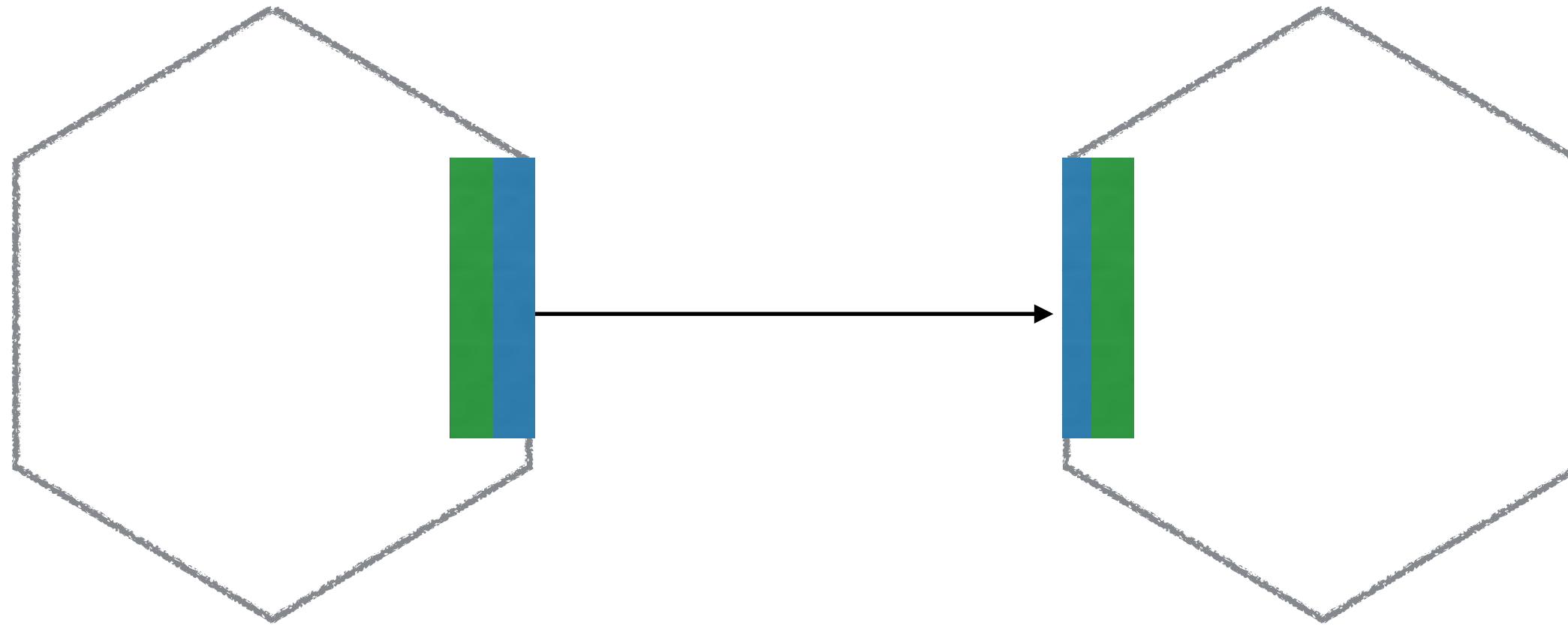
COMMON CONNECTION CONCERNS



Tracing

Load Balancing & Service Discovery

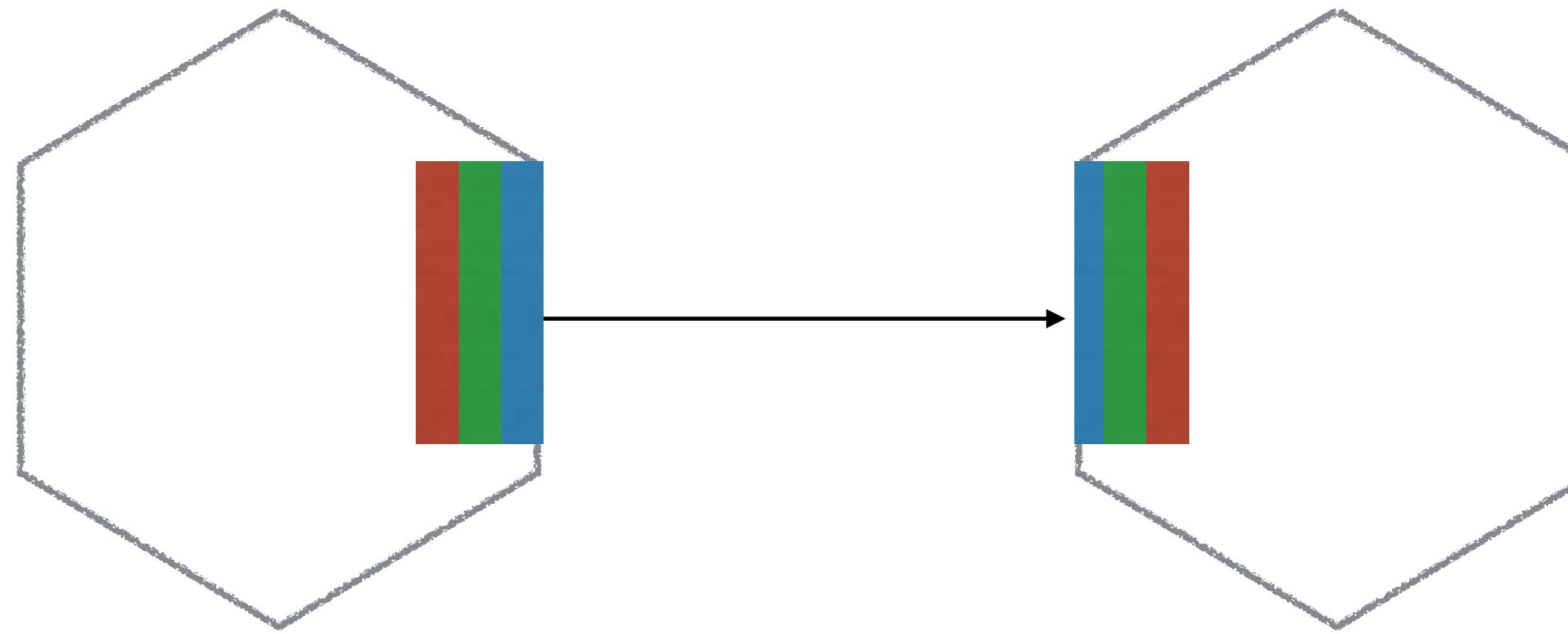
COMMON CONNECTION CONCERNS



Tracing

Load Balancing & Service Discovery

COMMON CONNECTION CONCERNS

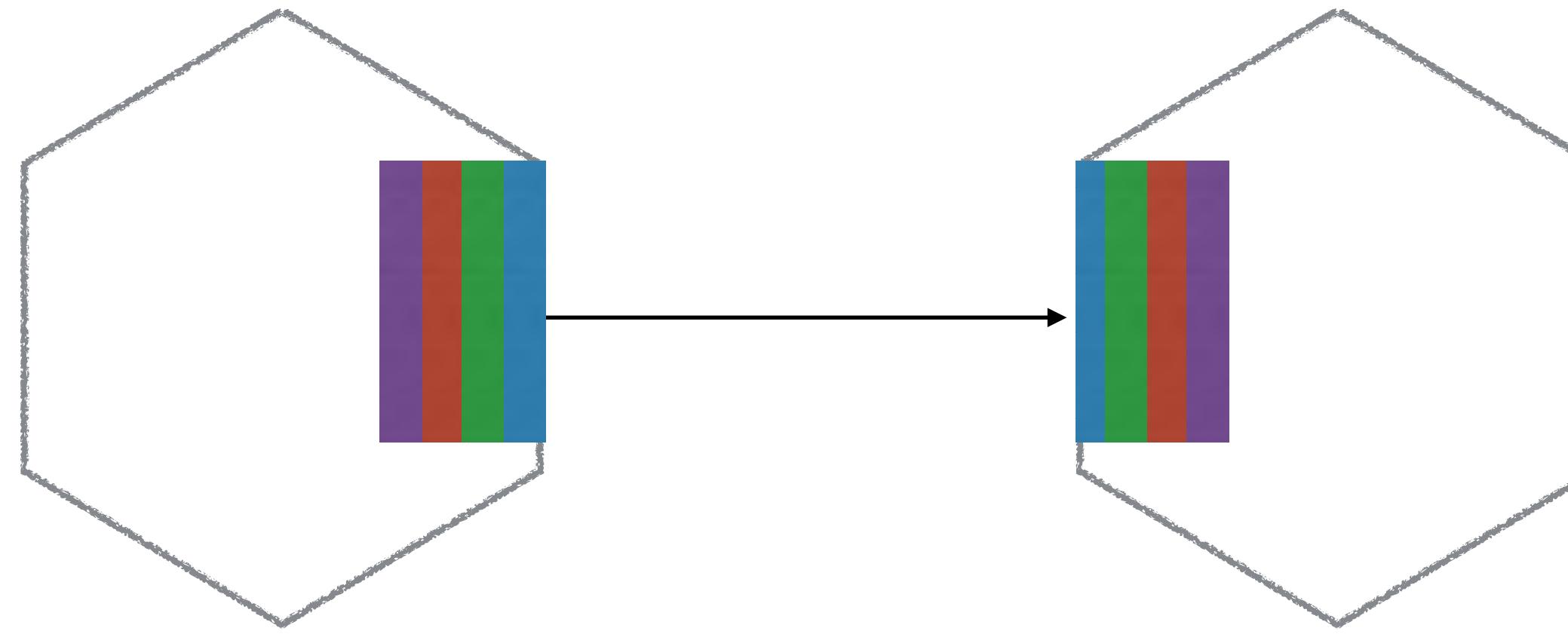


Tracing

Load Balancing & Service Discovery

Authorisation & Authentication

COMMON CONNECTION CONCERNS



Tracing

Load Balancing & Service Discovery

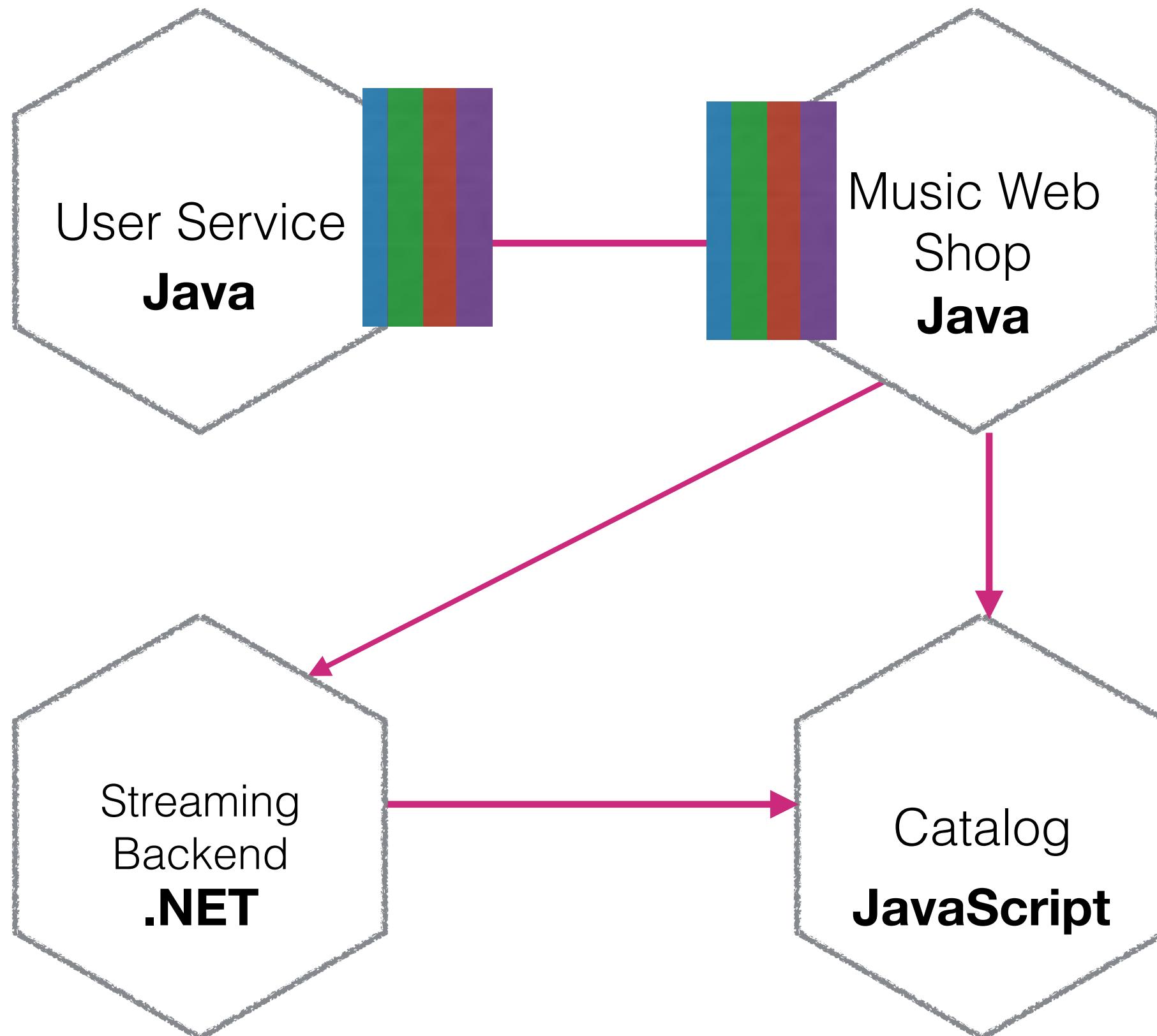
Authorisation & Authentication

Connection Resilience & Retry

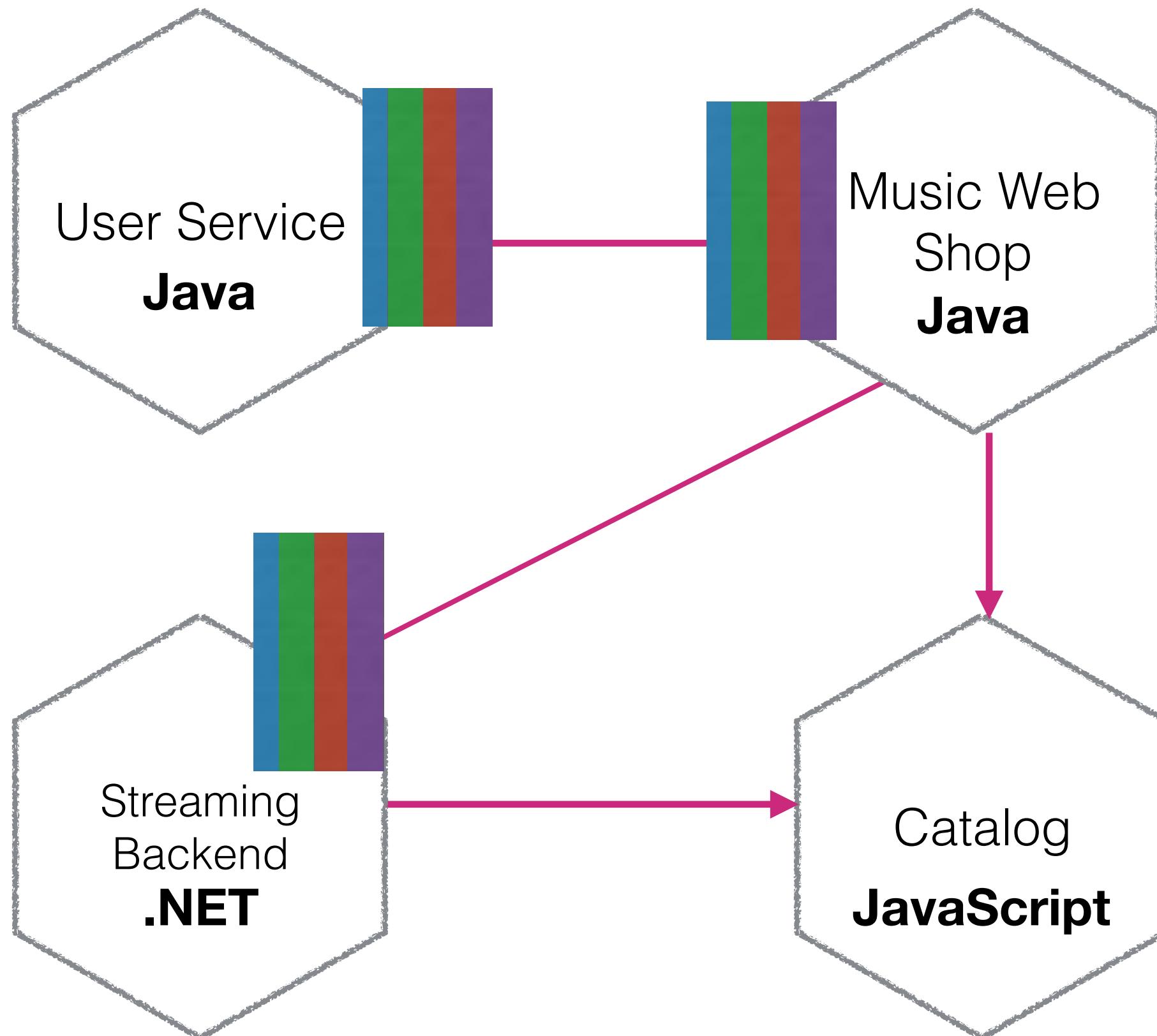
COMMON MICROSERVICE FRAMEWORKS



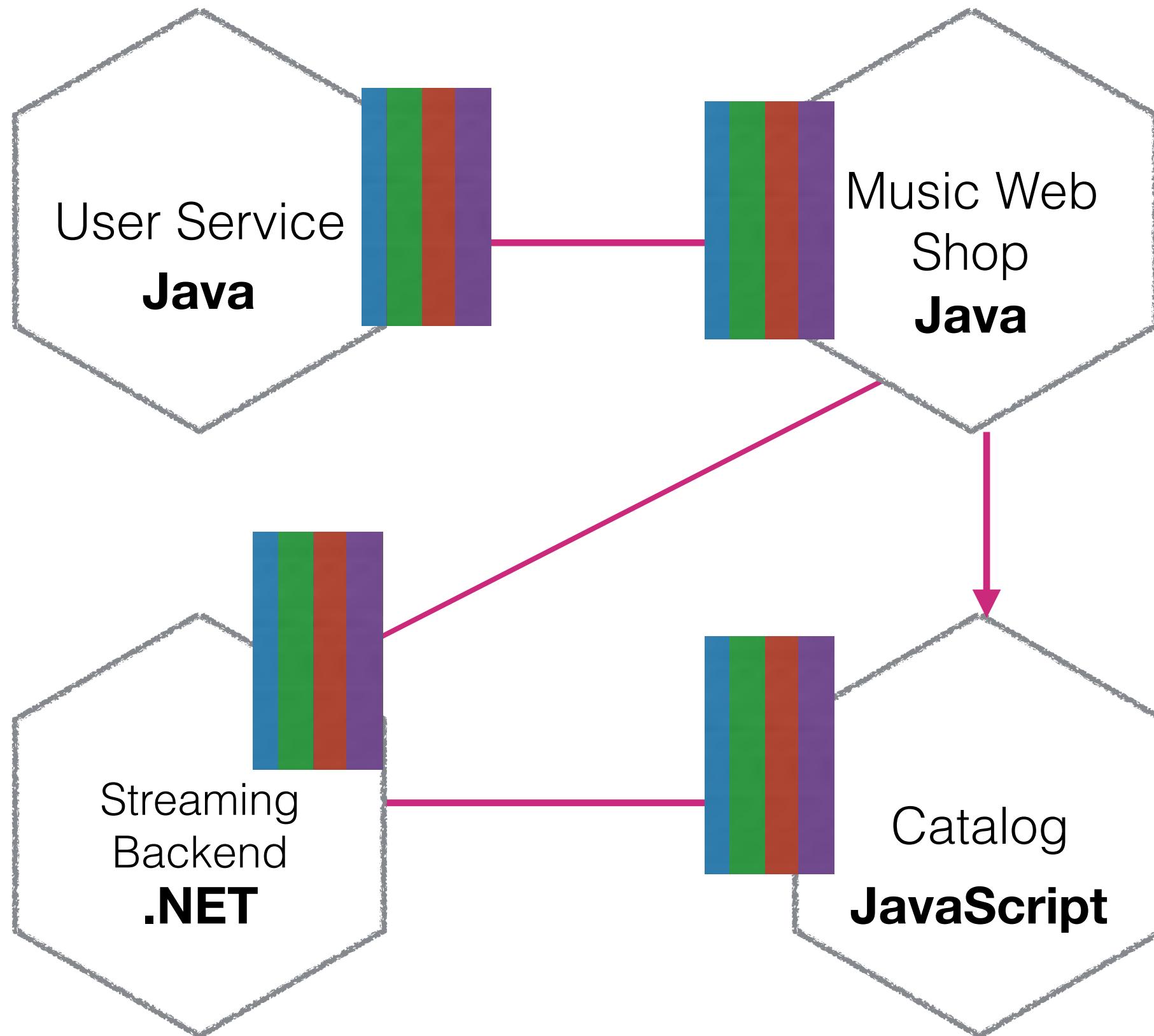
POLYGLOT?



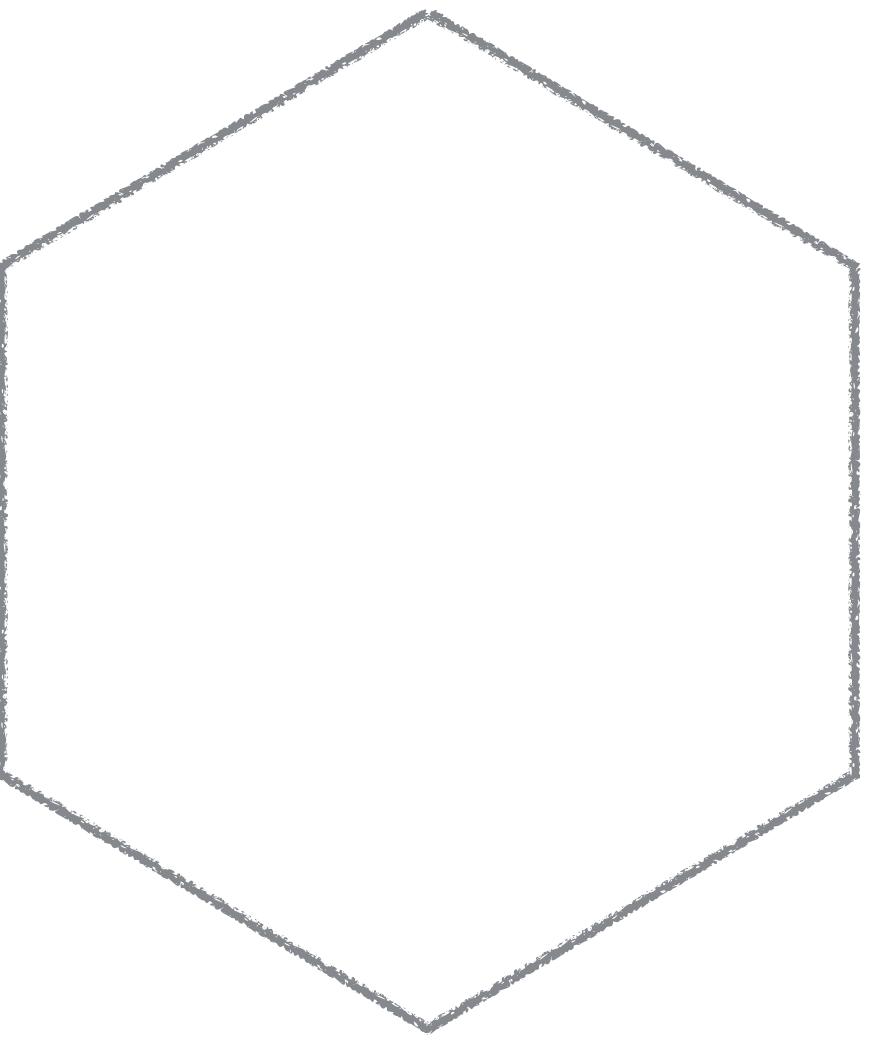
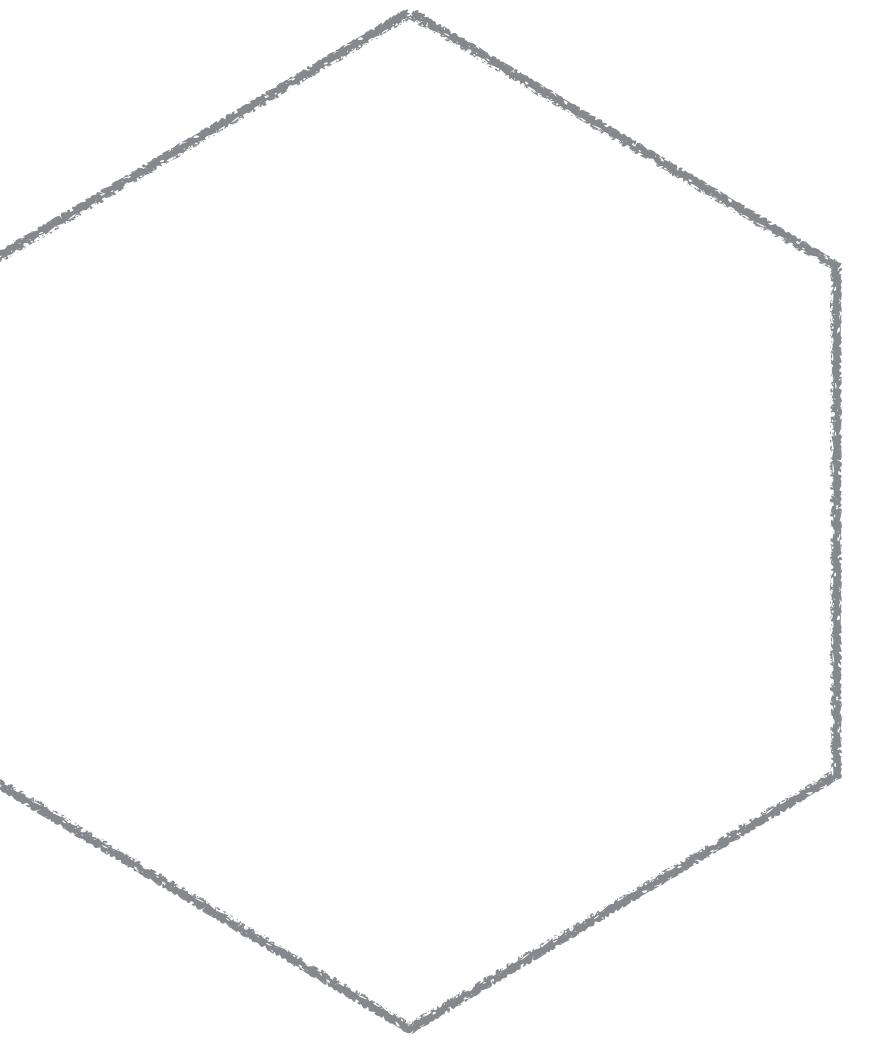
POLYGLOT?



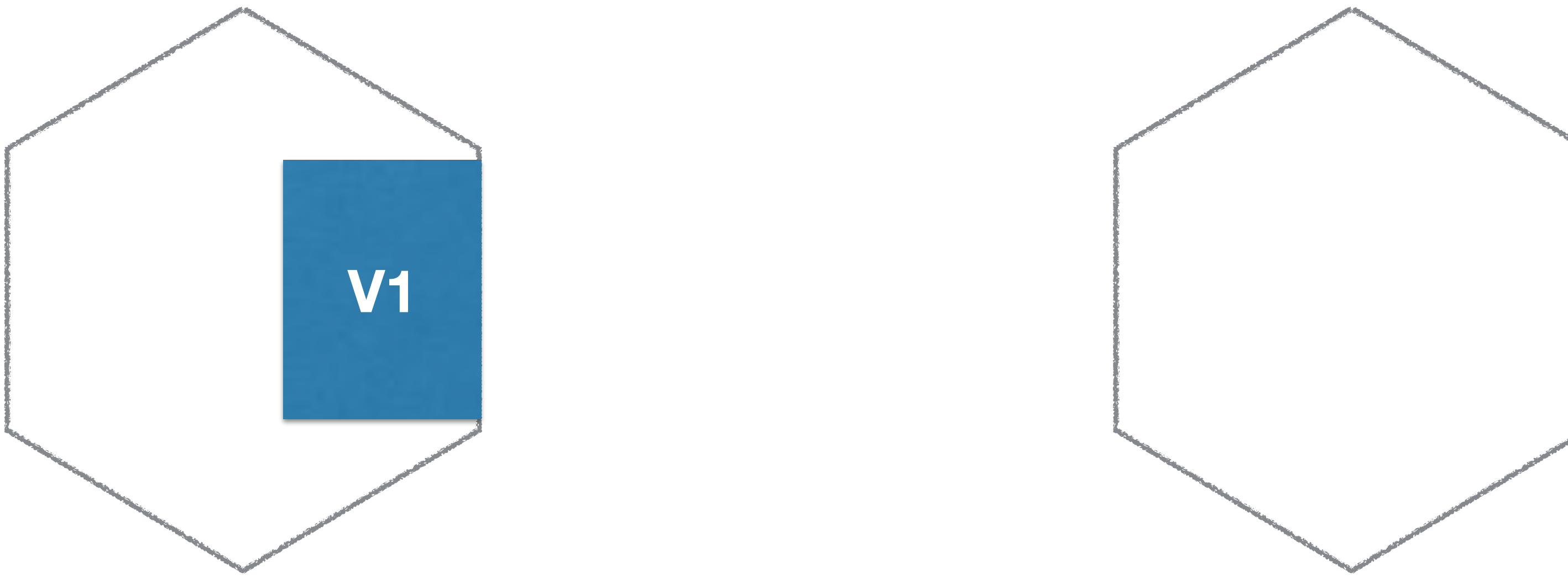
POLYGLOT?



VERSION DRIFT



VERSION DRIFT



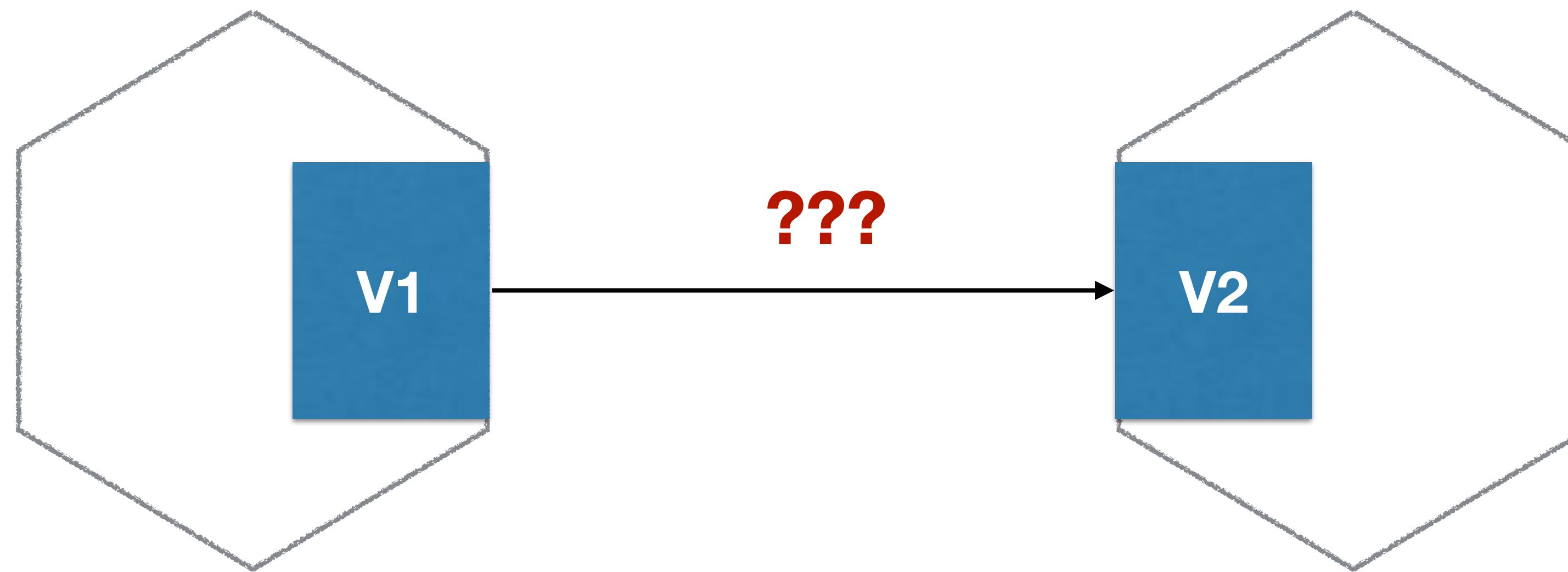
VERSION DRIFT



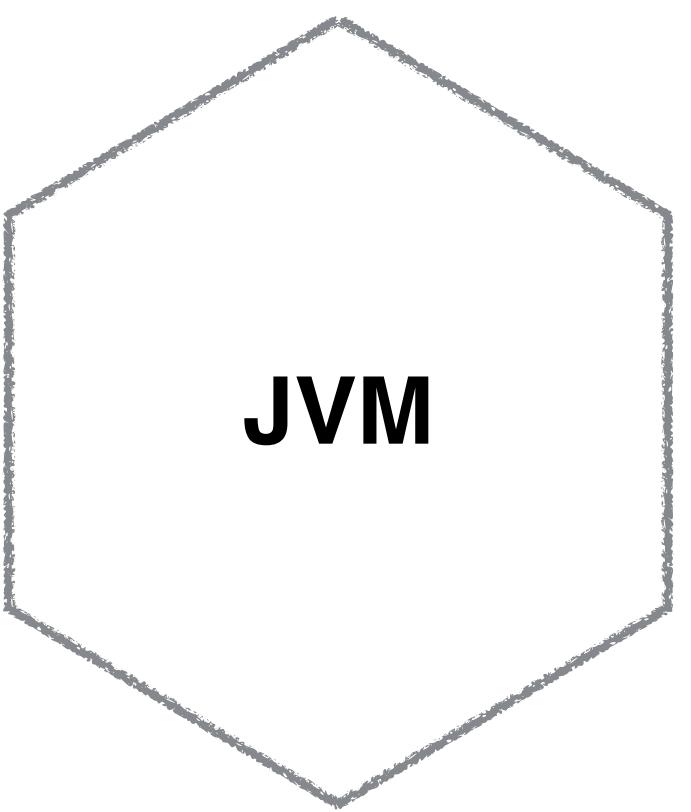
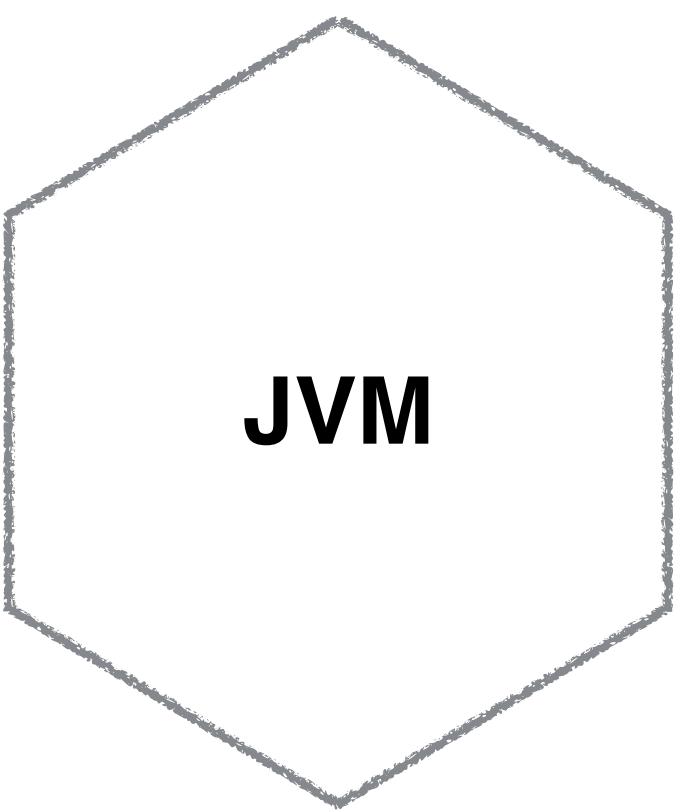
VERSION DRIFT



VERSION DRIFT

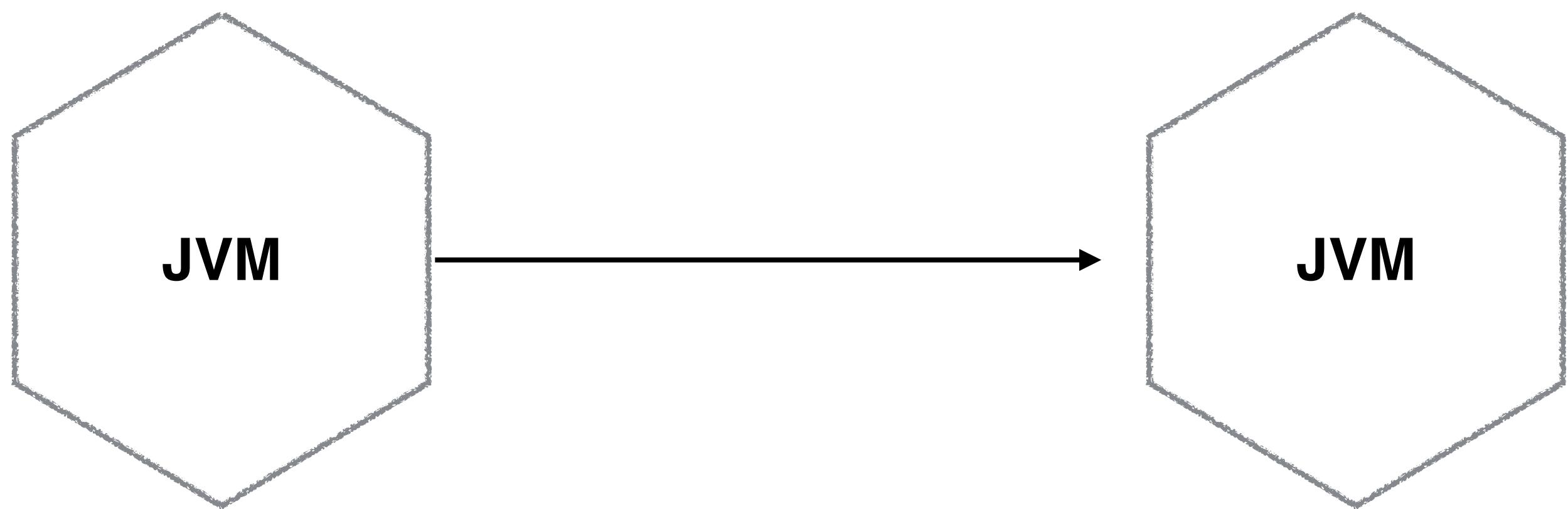


NETFLIX - ENFORCEMENT OF REUSE



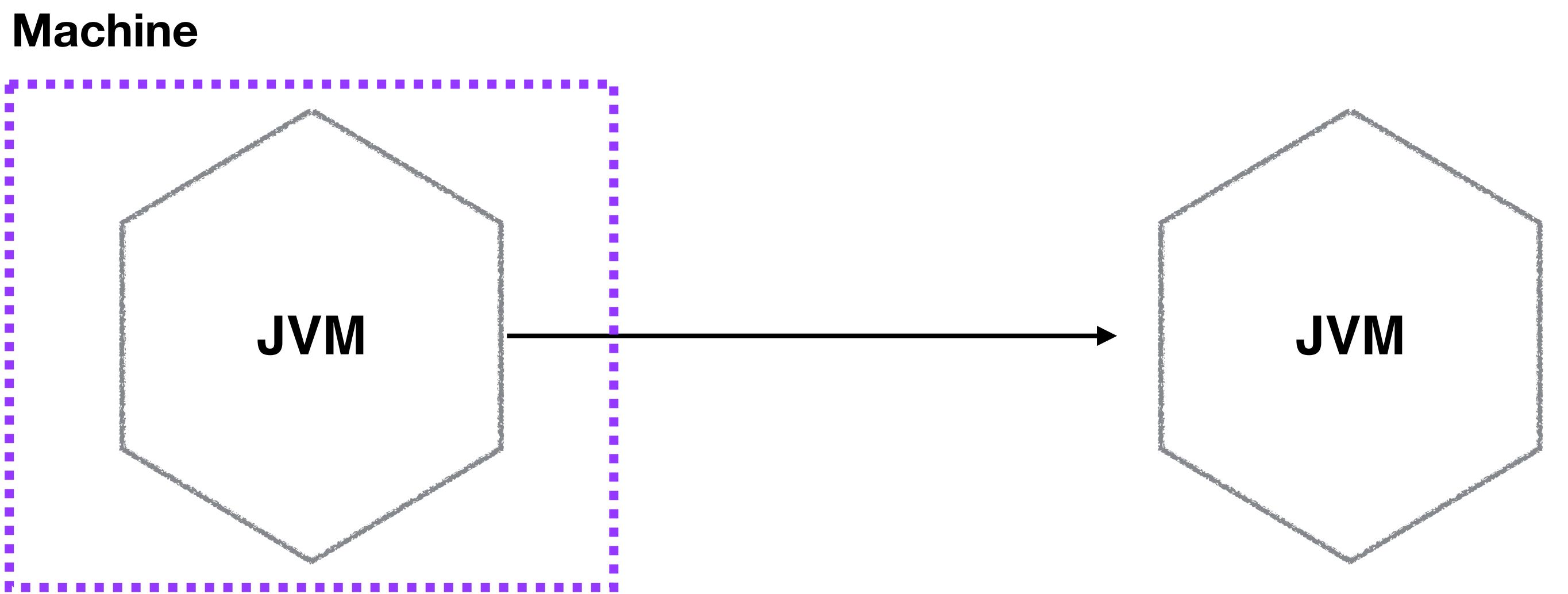
NETFLIX

NETFLIX - ENFORCEMENT OF REUSE



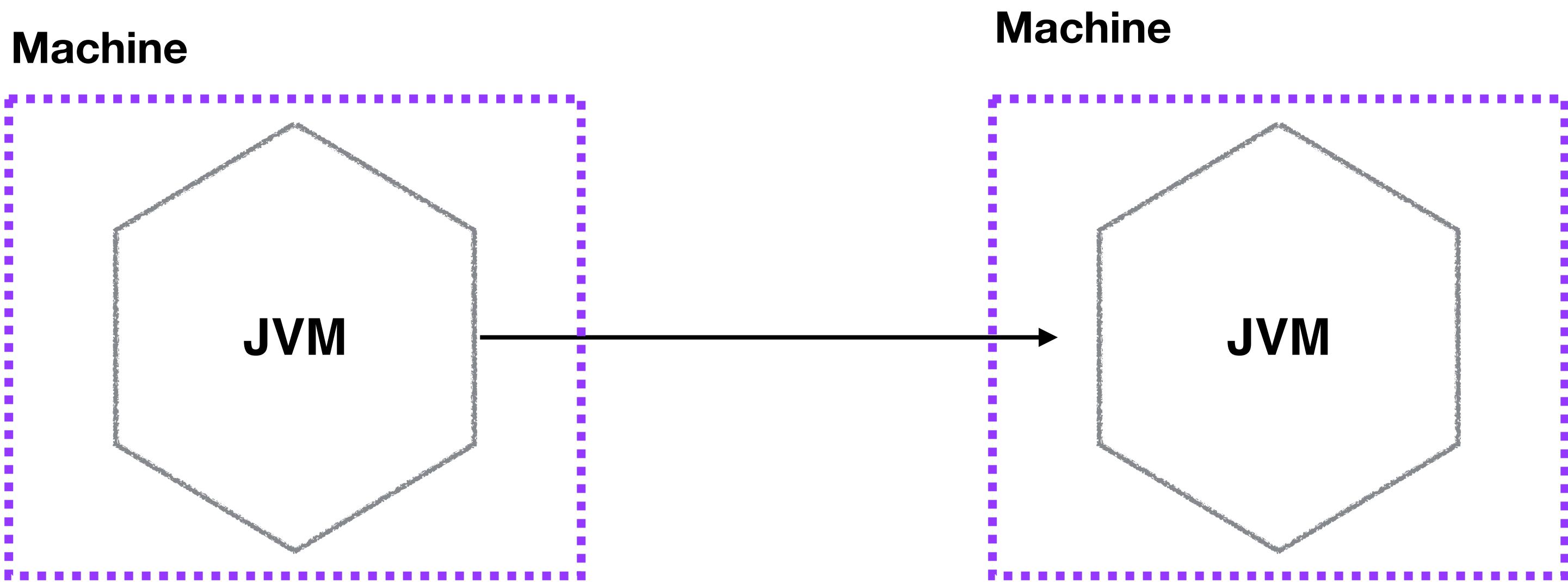
NETFLIX

NETFLIX - ENFORCEMENT OF REUSE



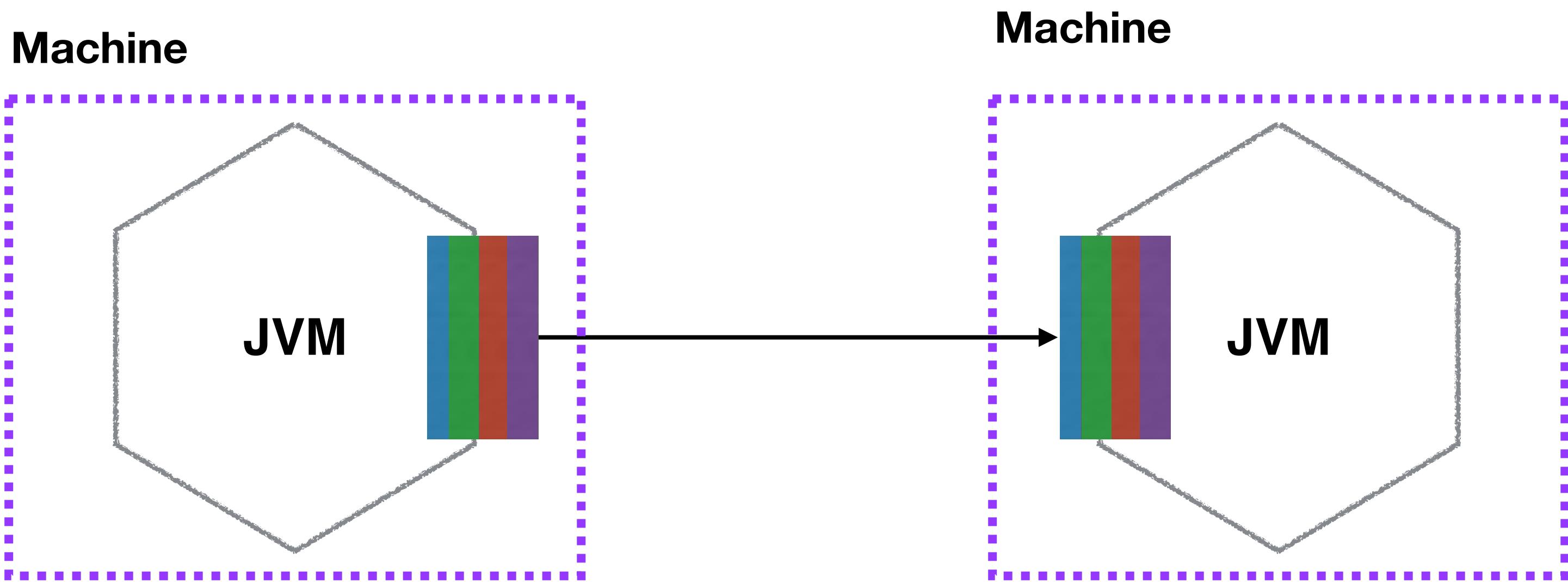
NETFLIX

NETFLIX - ENFORCEMENT OF REUSE



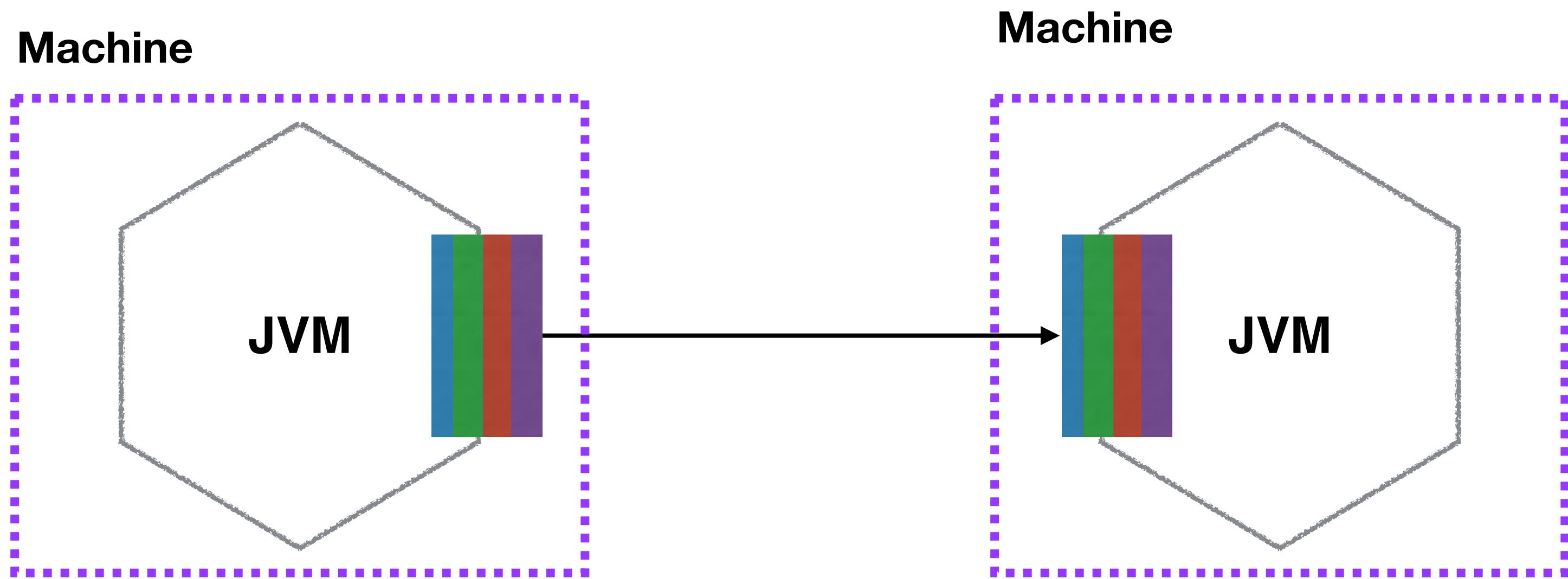
NETFLIX

NETFLIX - ENFORCEMENT OF REUSE



NETFLIX

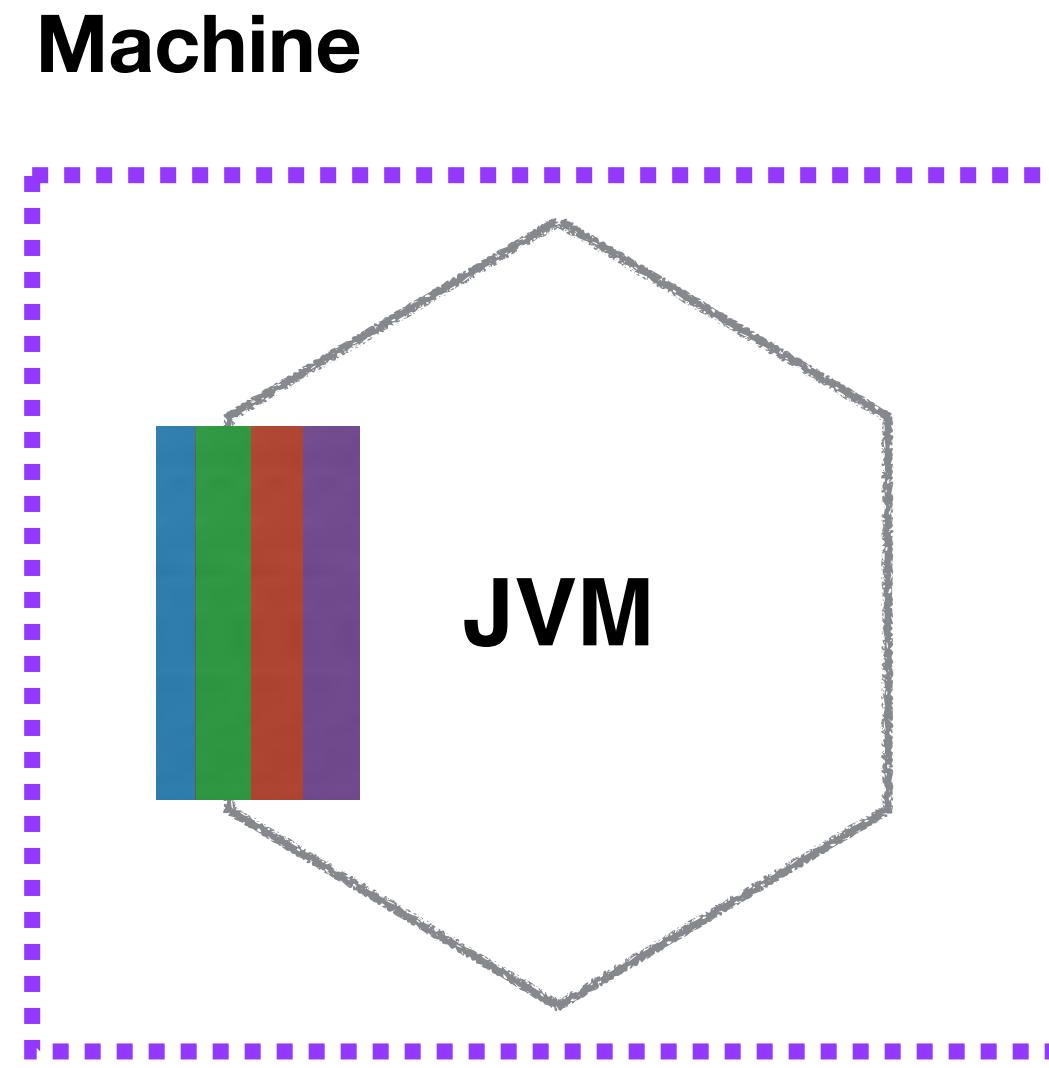
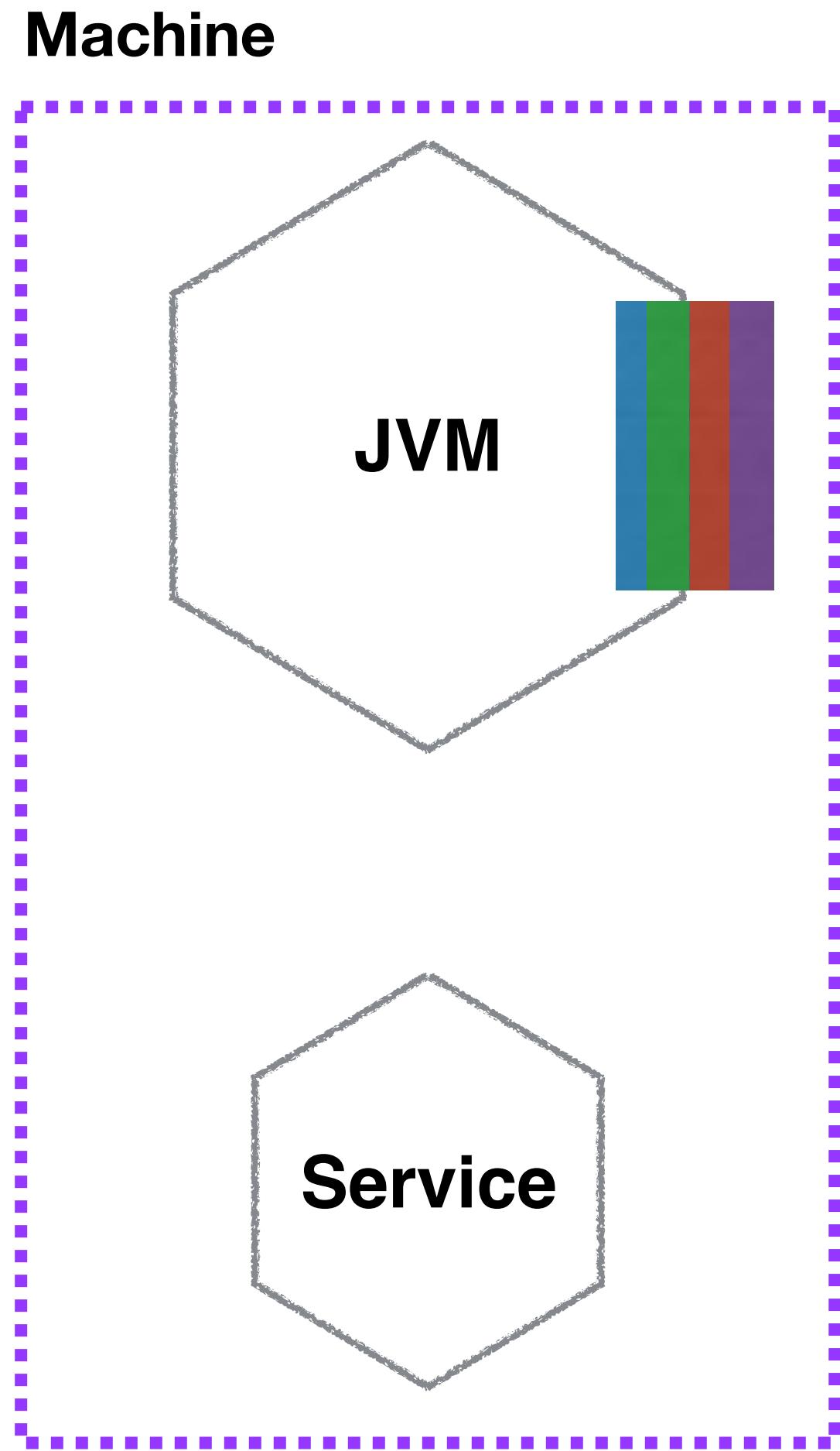
NETFLIX - ENFORCEMENT OF REUSE



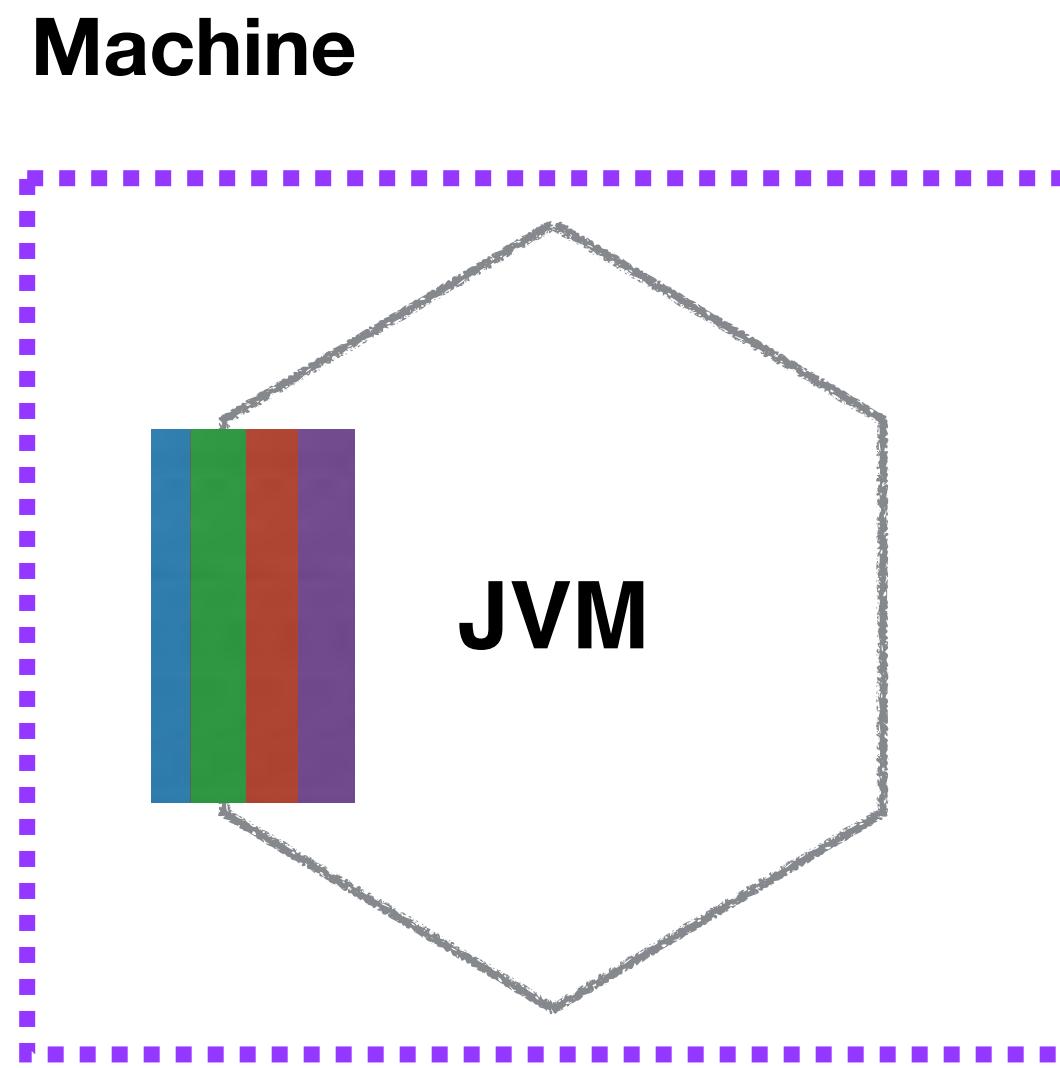
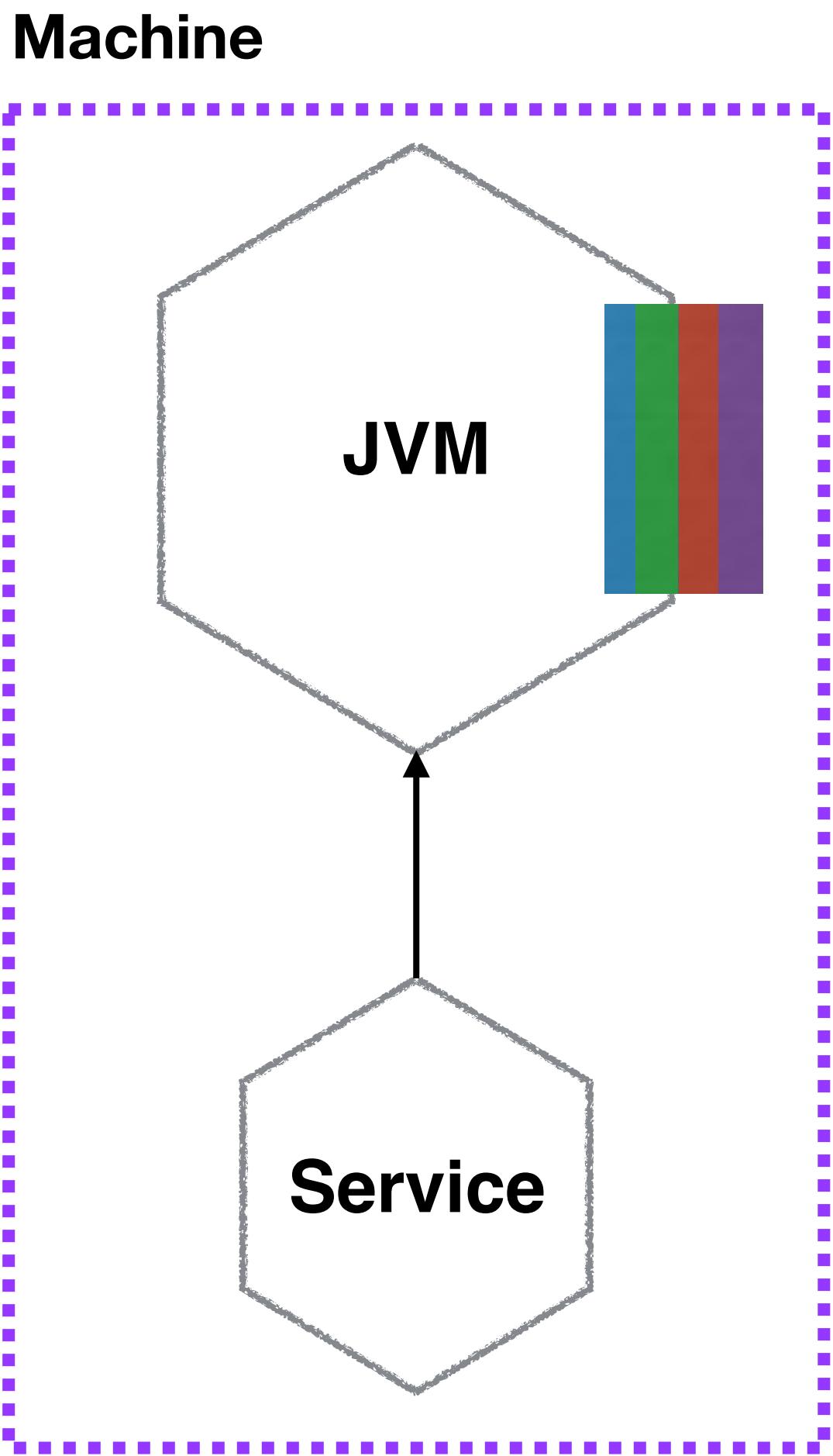
NETFLIX

What about non-JVM
languages?

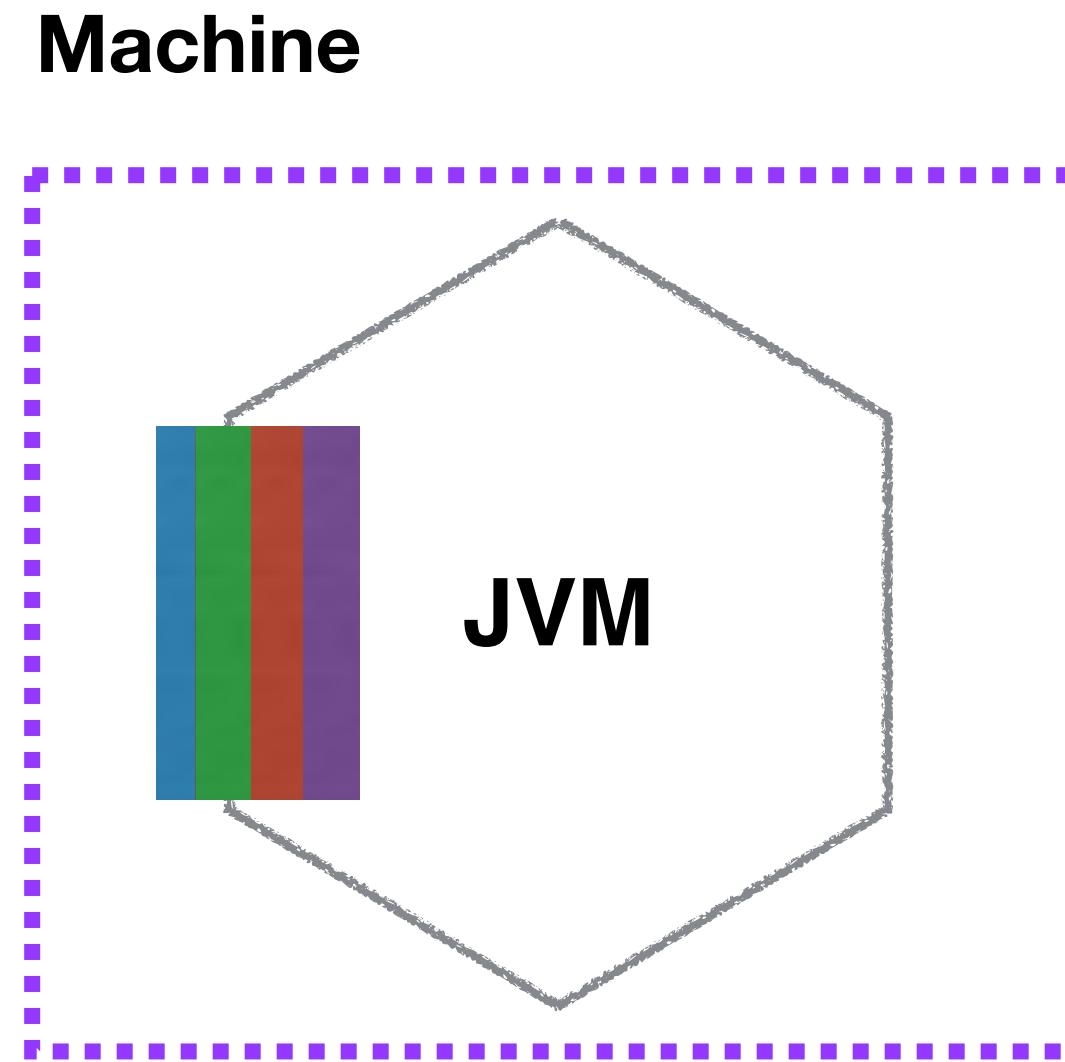
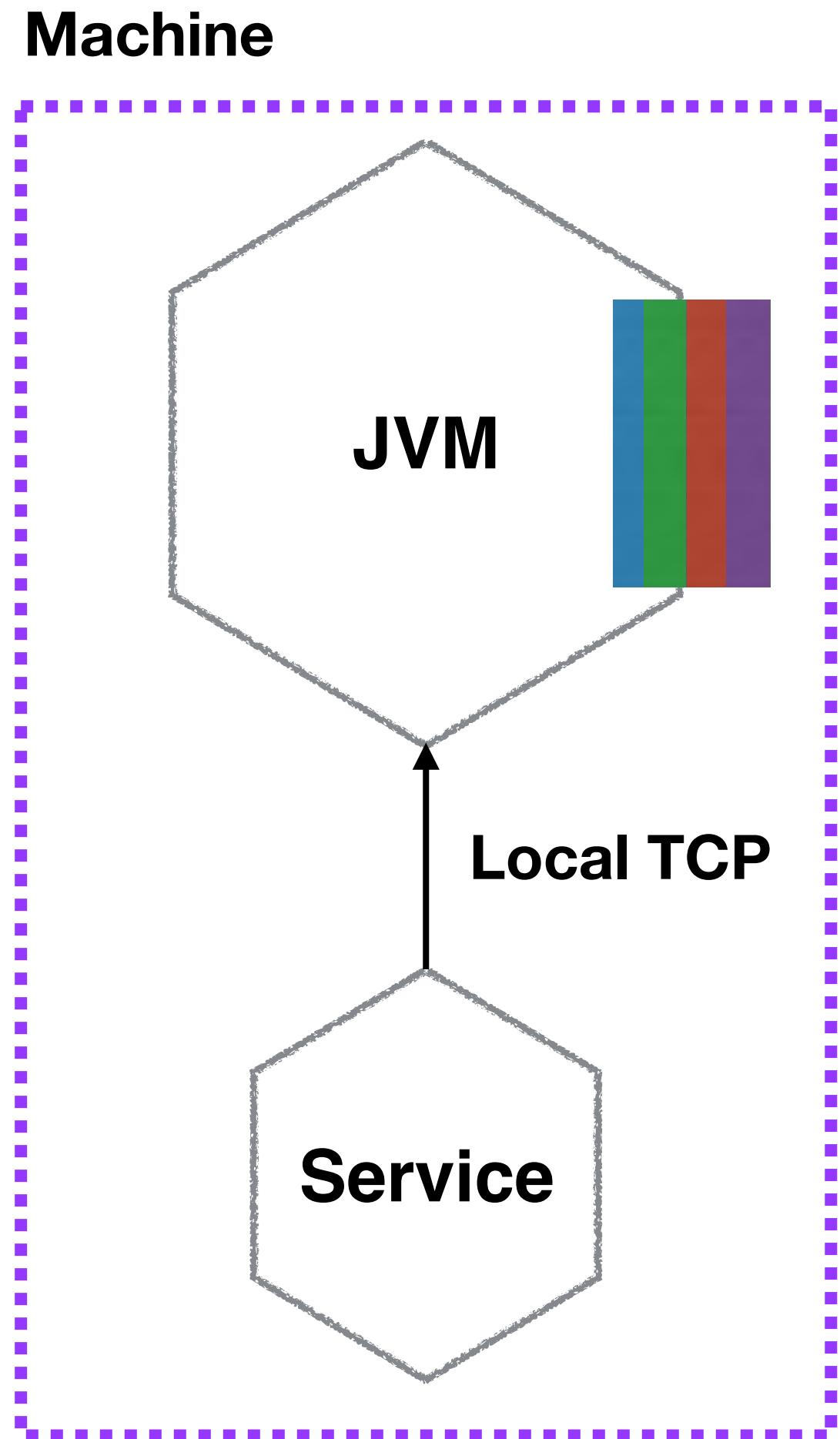
NETFLIX - SIDECAR PATTERN



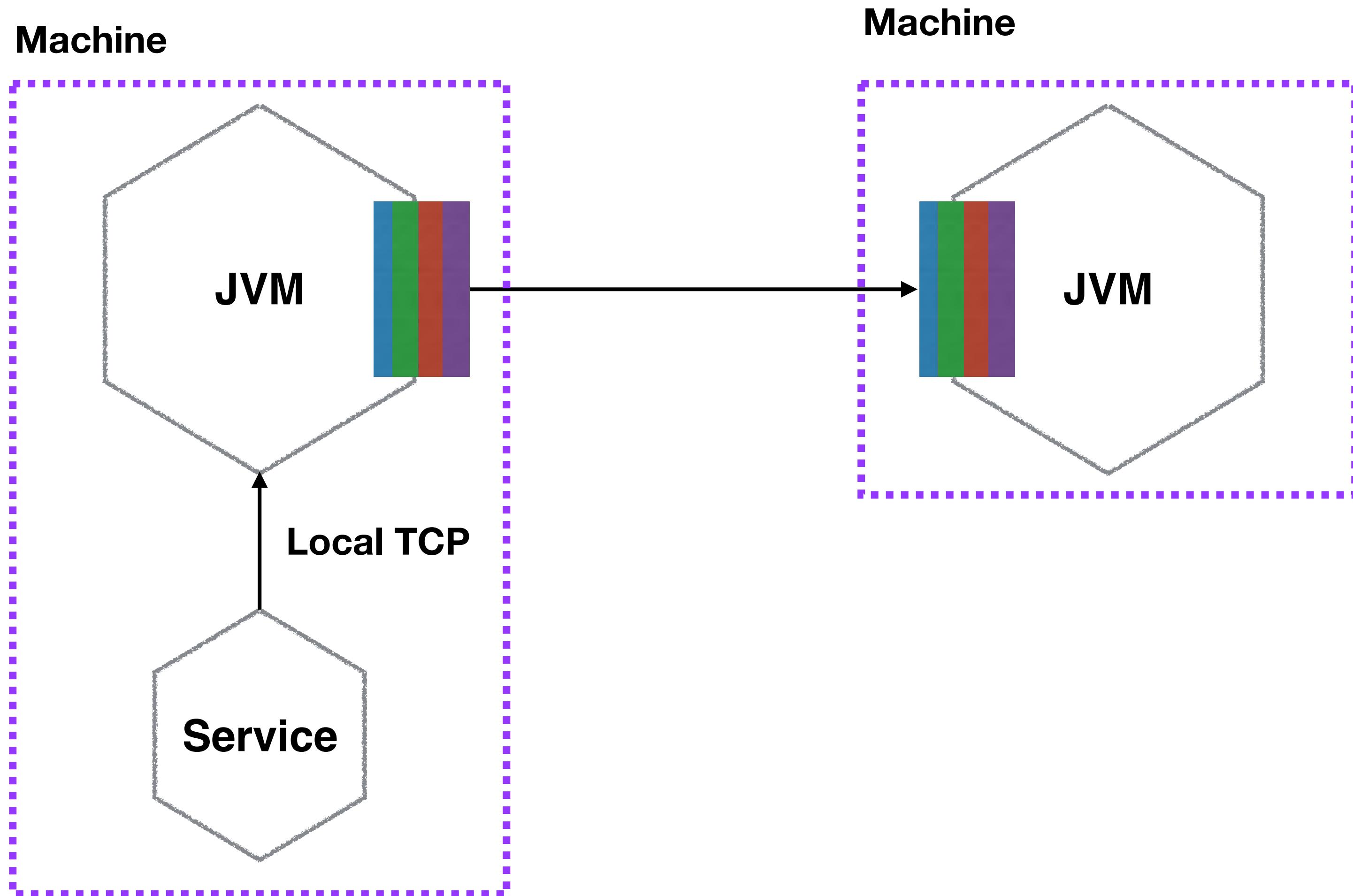
NETFLIX - SIDECAR PATTERN



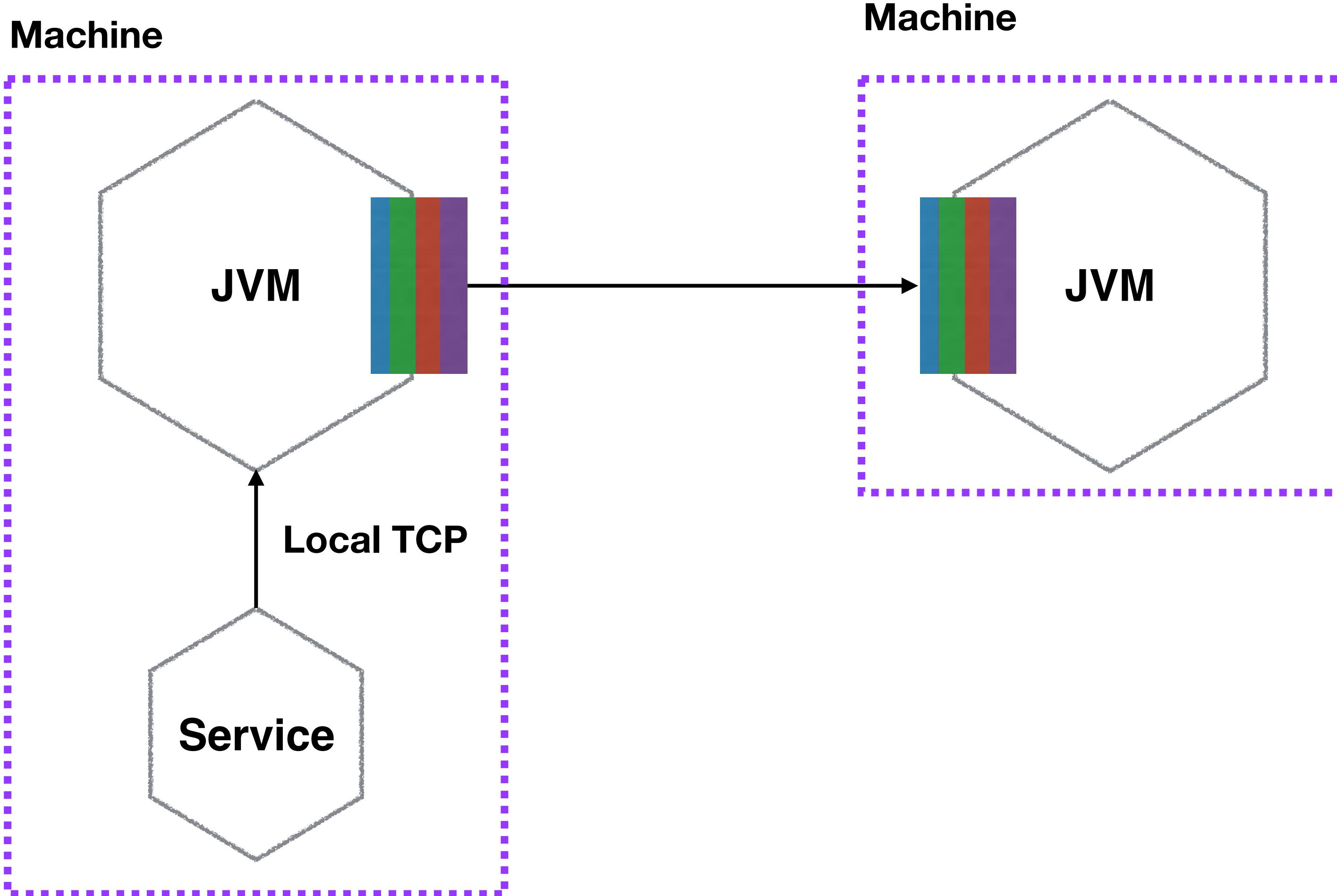
NETFLIX - SIDECAR PATTERN



NETFLIX - SIDECAR PATTERN

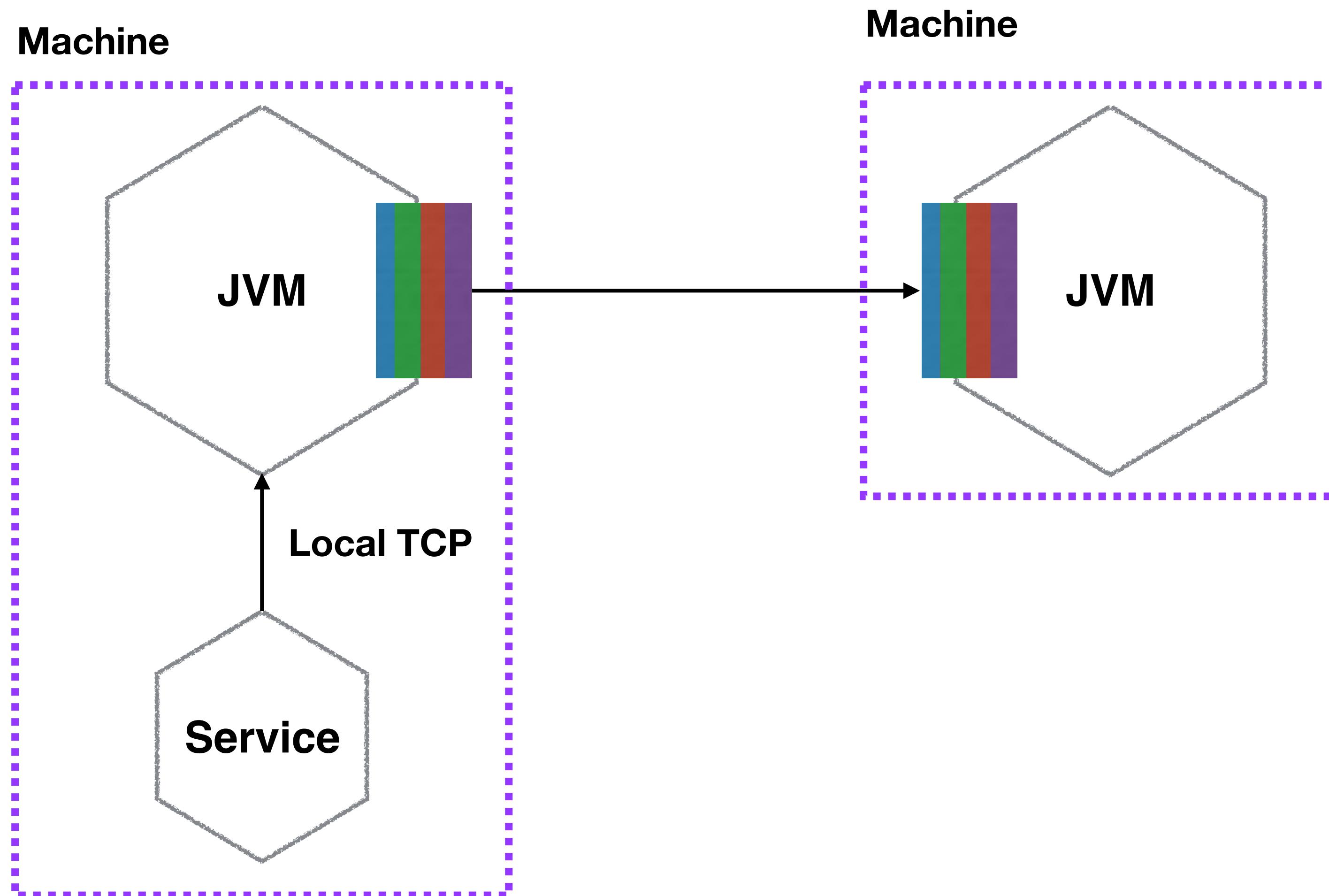


NETFLIX - SIDECAR PATTERN



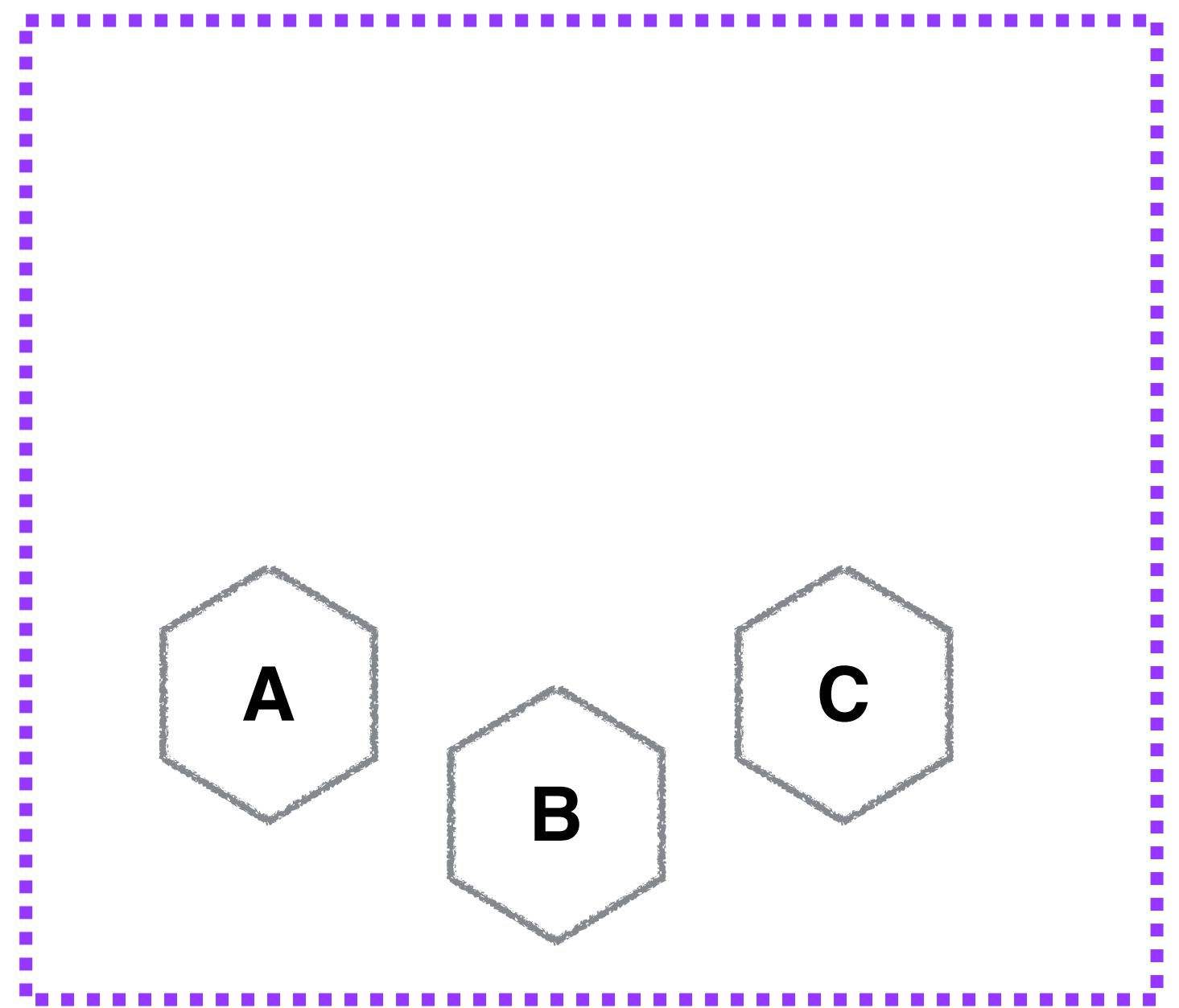
Re-use code across tech stacks

NETFLIX - SIDECAR PATTERN



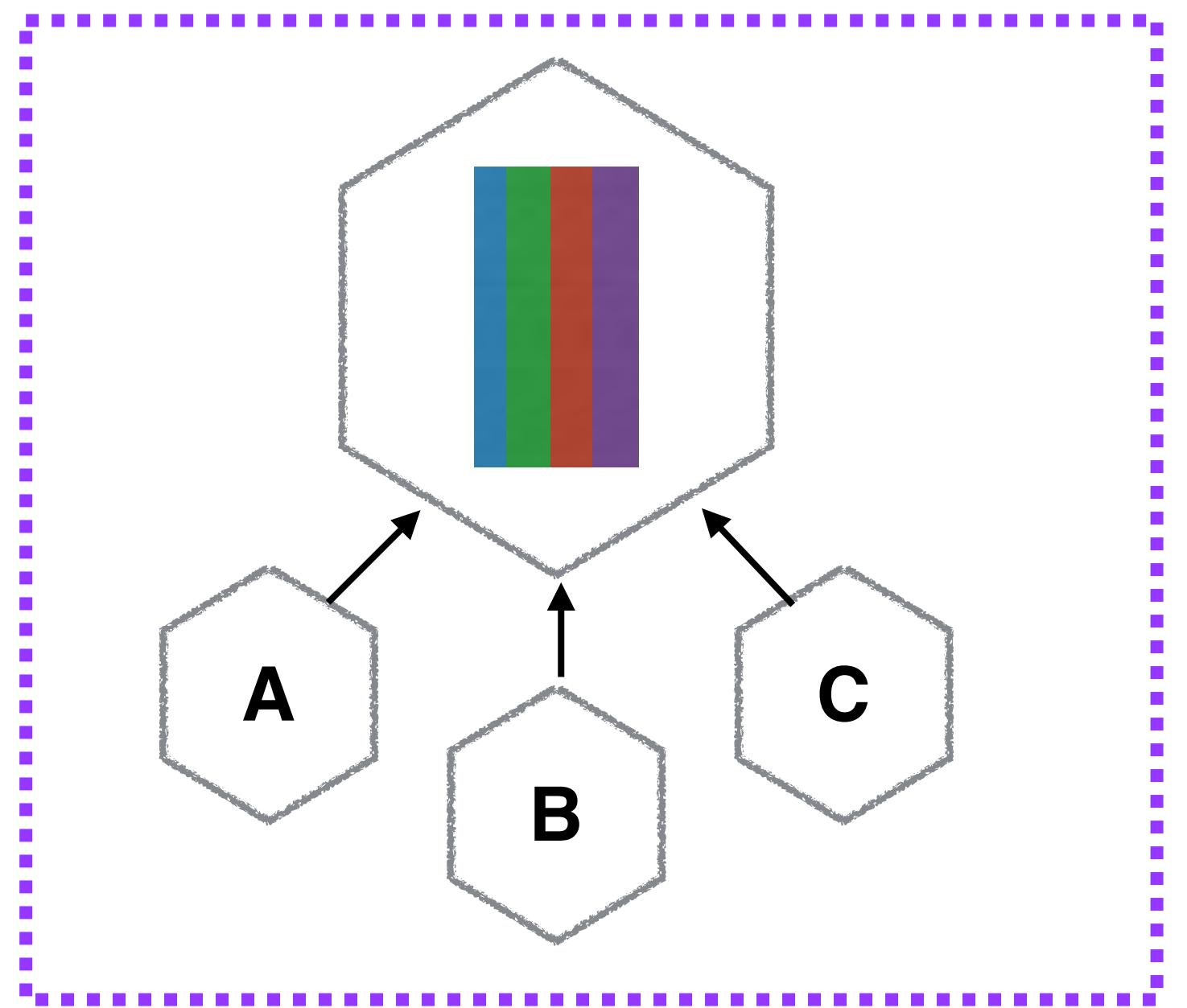
Re-use code across tech stacks
Reduce impact of version drift

FROM PROXIES TO SERVICE MESHS



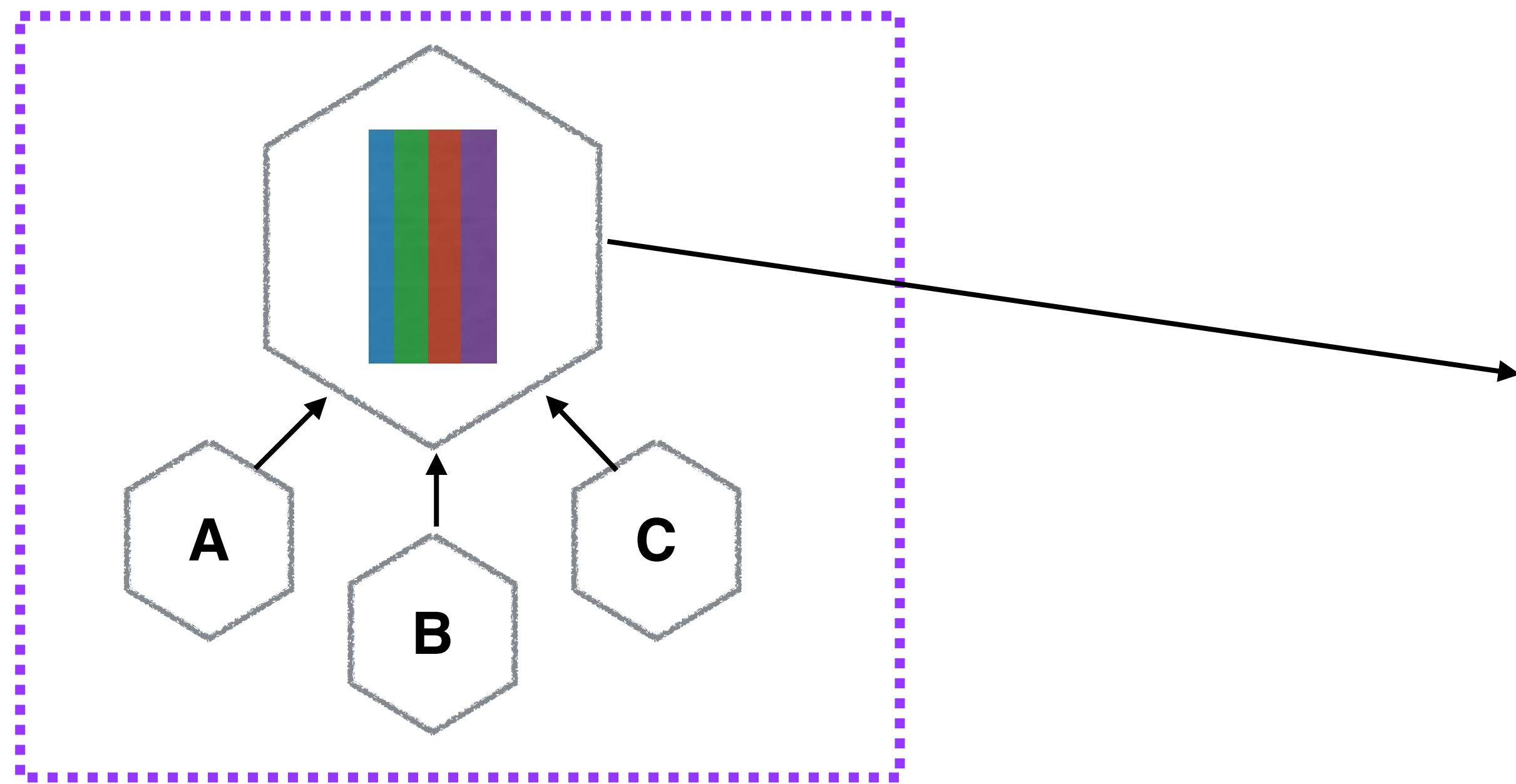
Machine

FROM PROXIES TO SERVICE MESHS



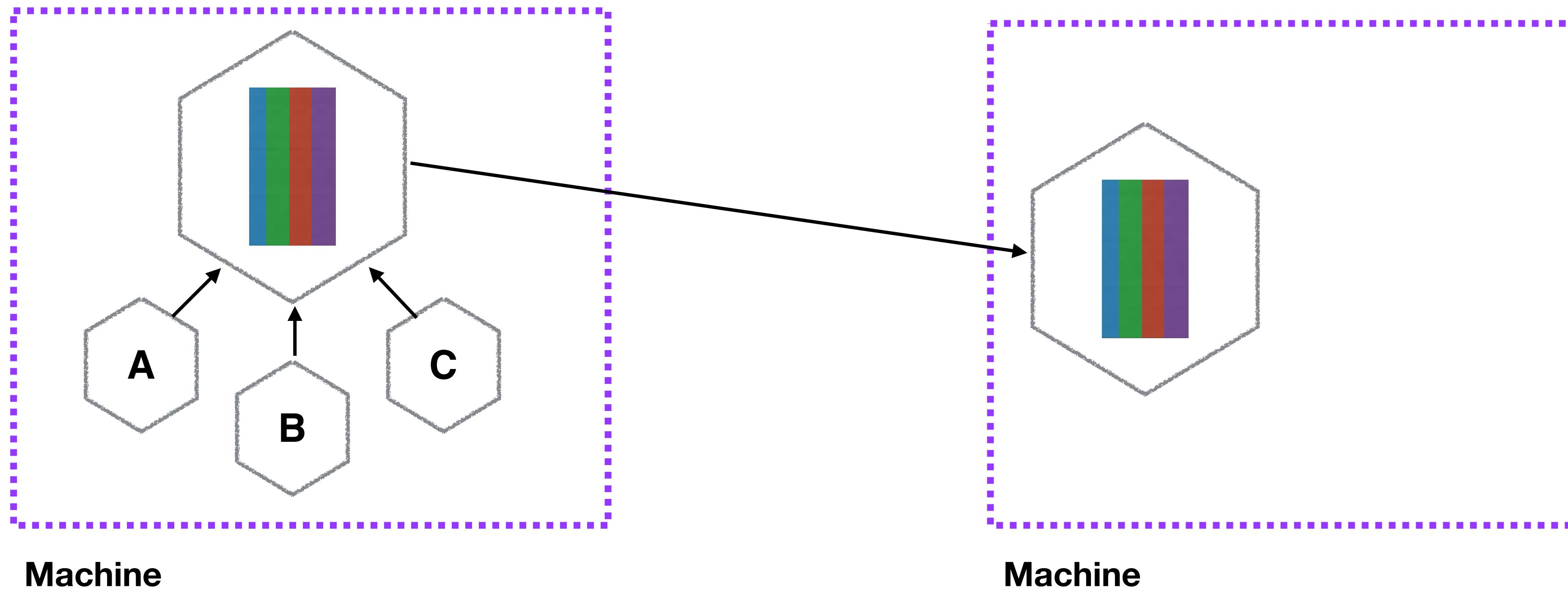
Machine

FROM PROXIES TO SERVICE MESHS

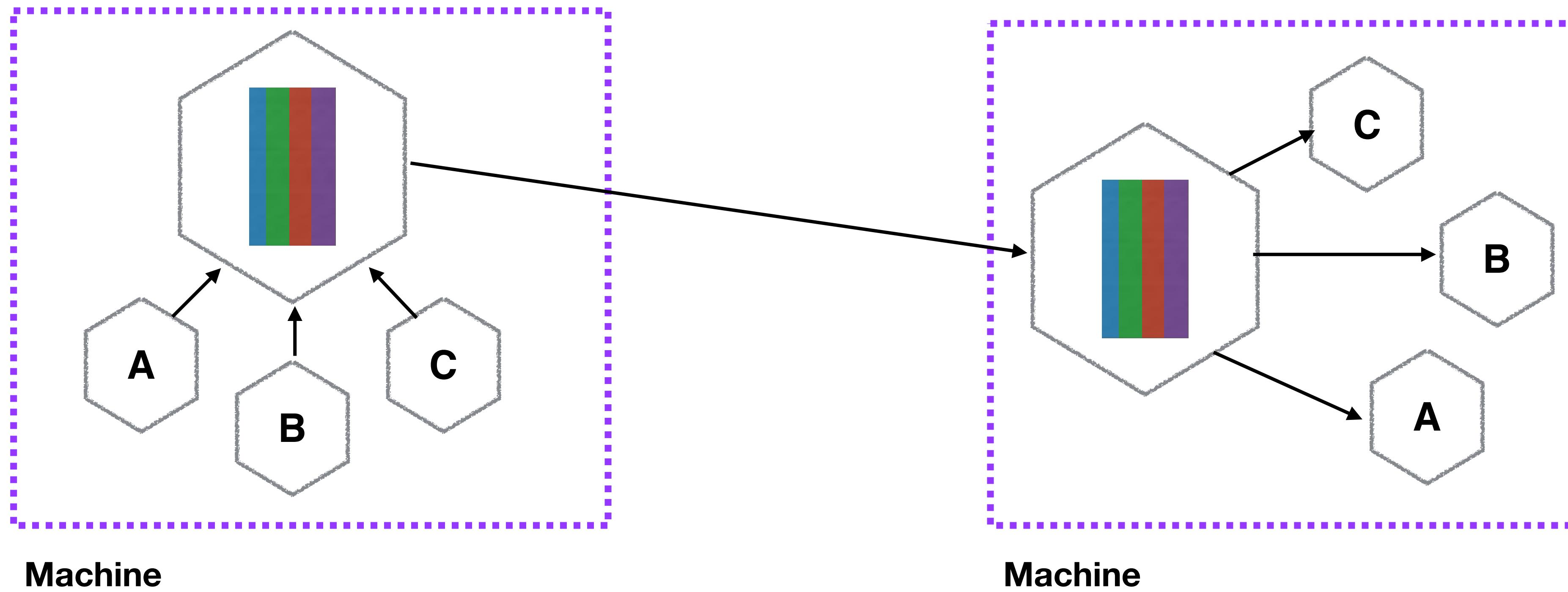


Machine

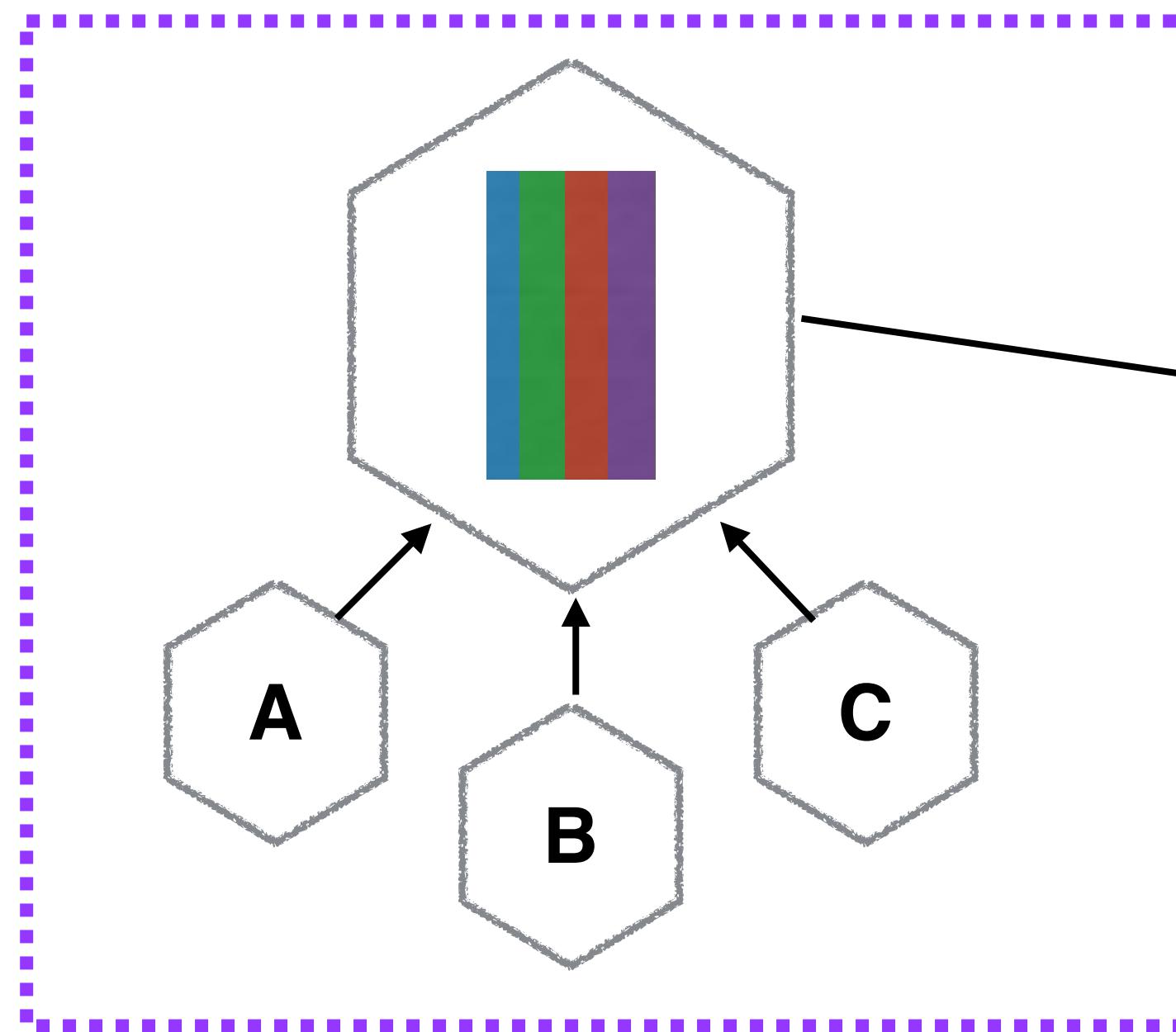
FROM PROXIES TO SERVICE MESHS



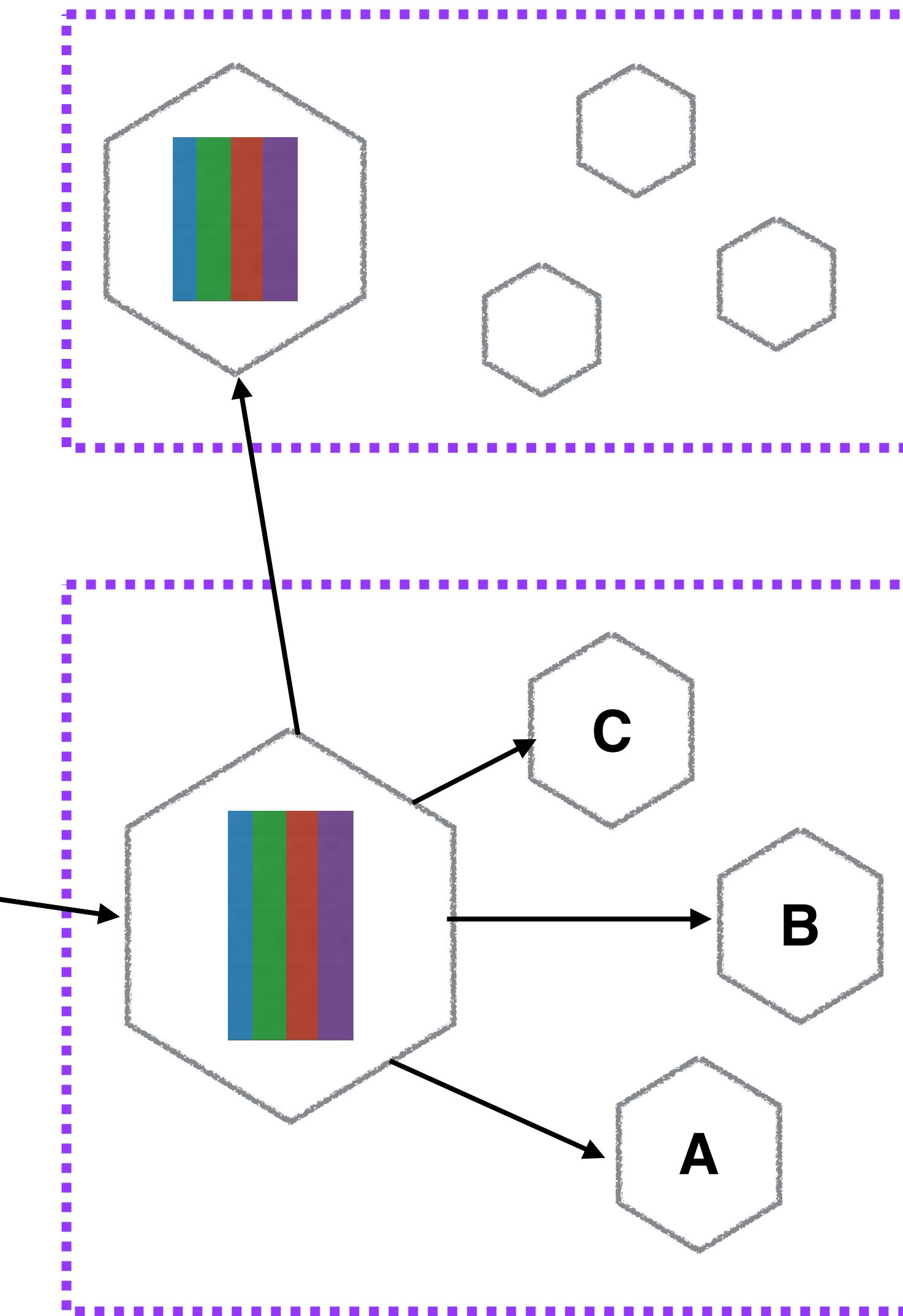
FROM PROXIES TO SERVICE MESHS



FROM PROXIES TO SERVICE MESHS

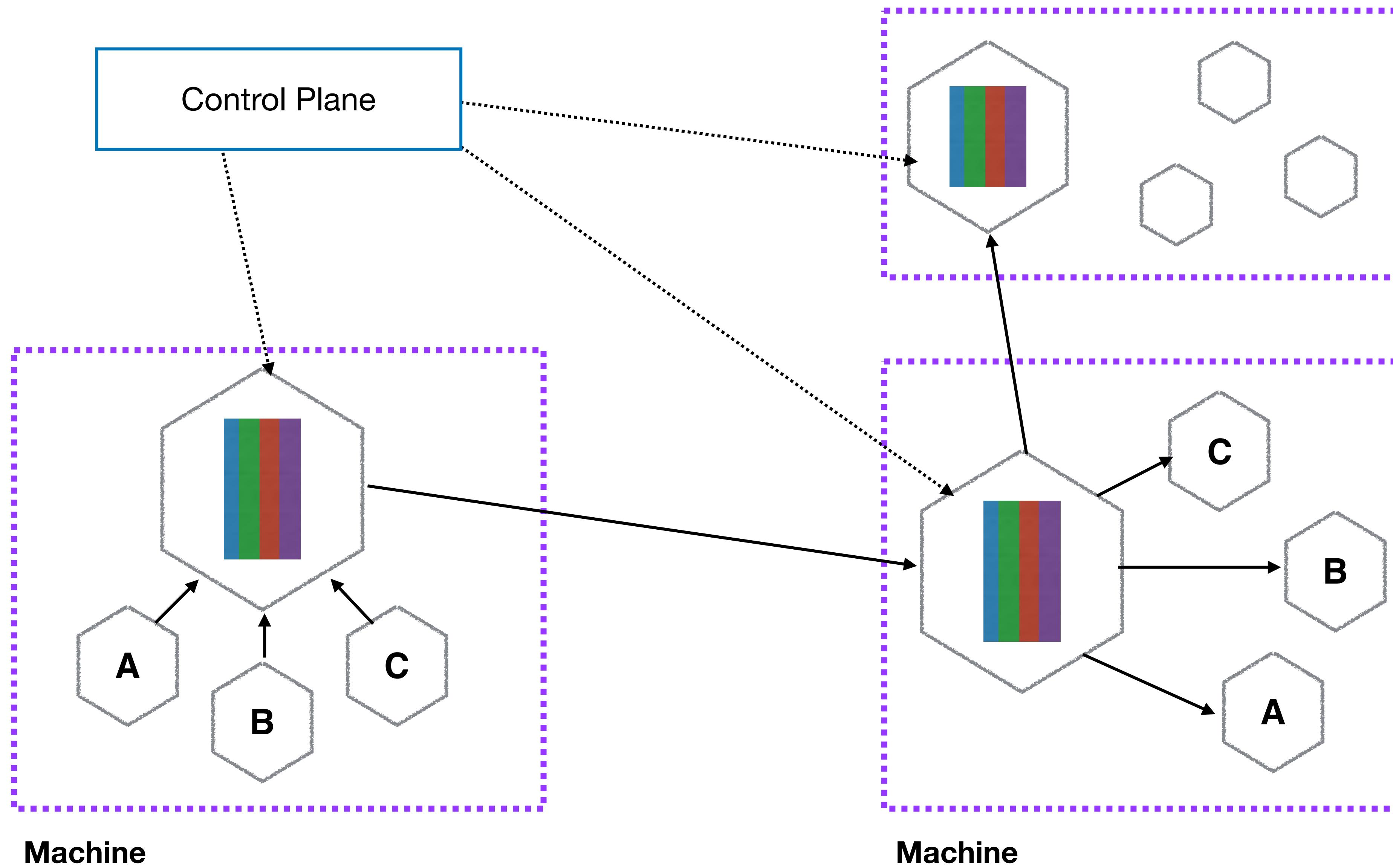


Machine



Machine

FROM PROXIES TO SERVICE MESHS



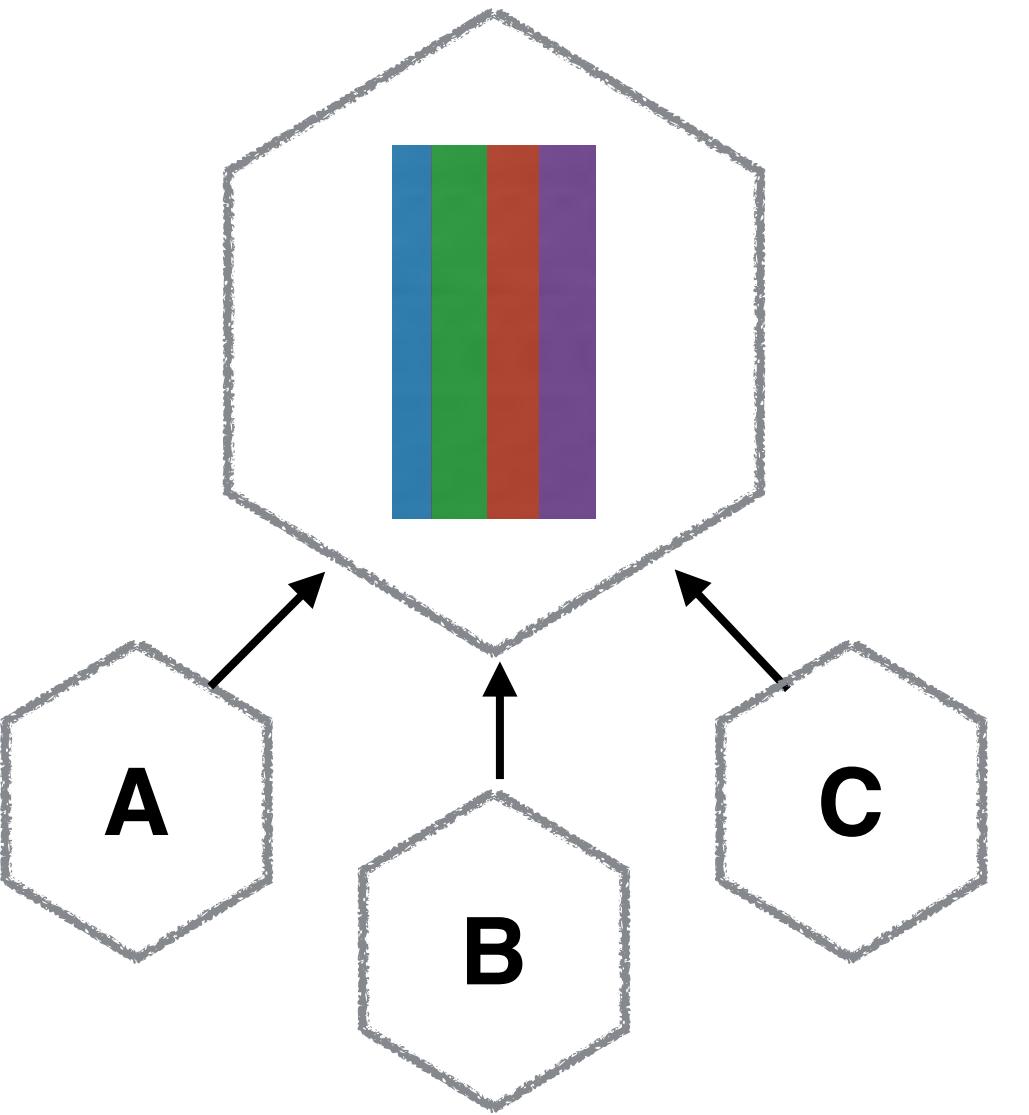
SIDECARS VS PROXIES

Local Proxy

Sidecar

SIDECAR VS PROXIES

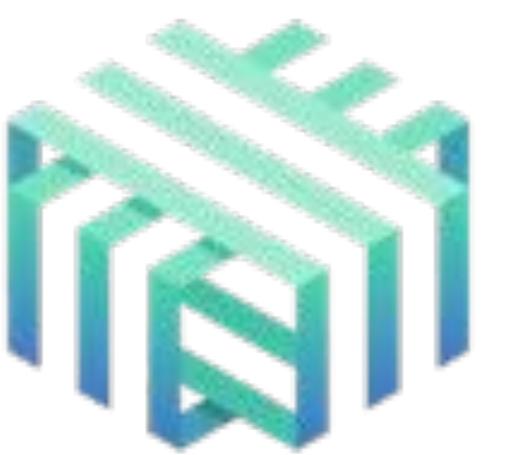
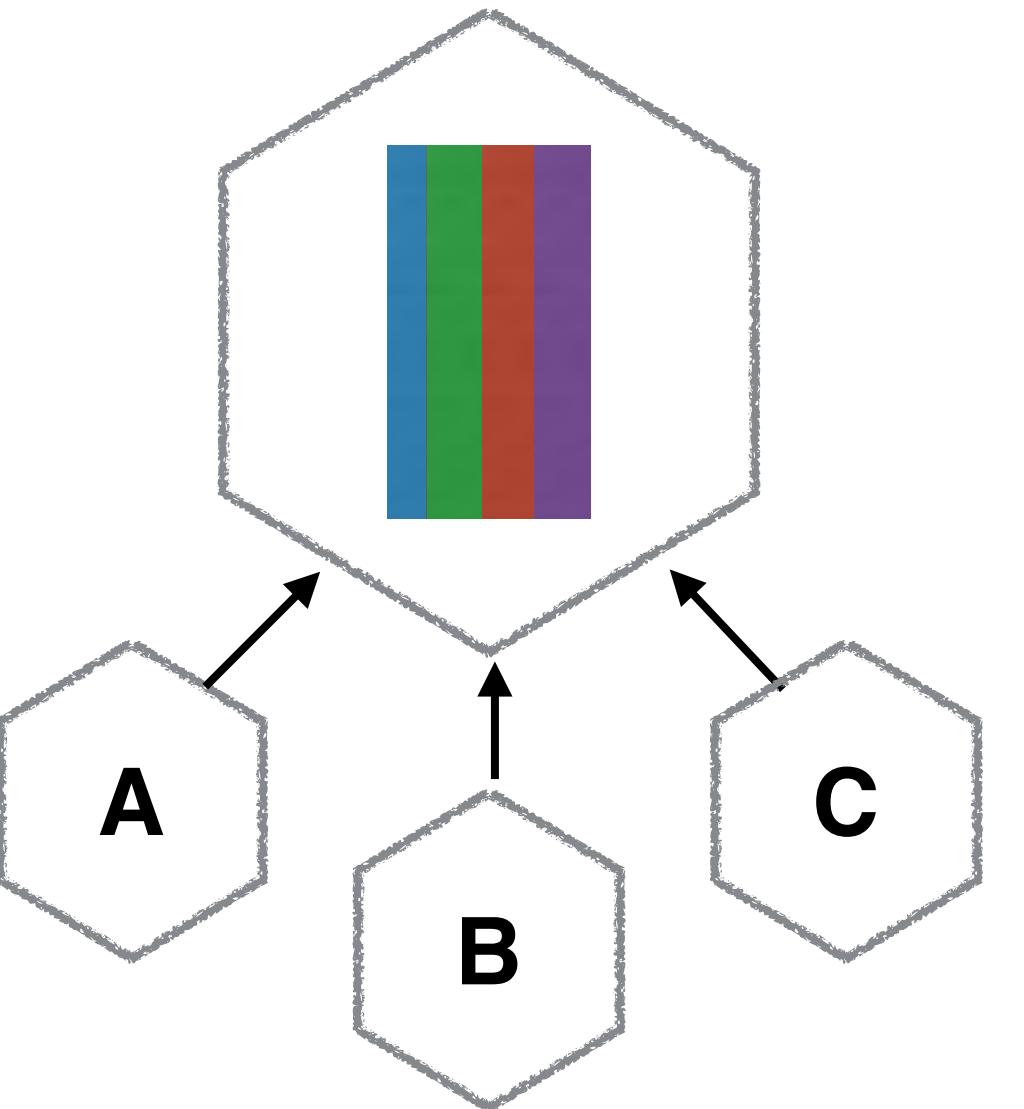
Local Proxy



Sidecar

SIDECAR VS PROXIES

Local Proxy



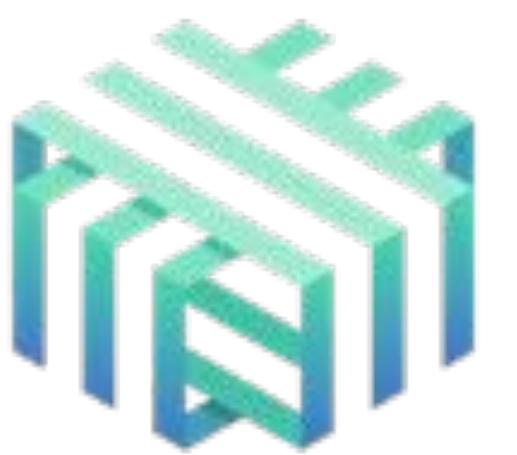
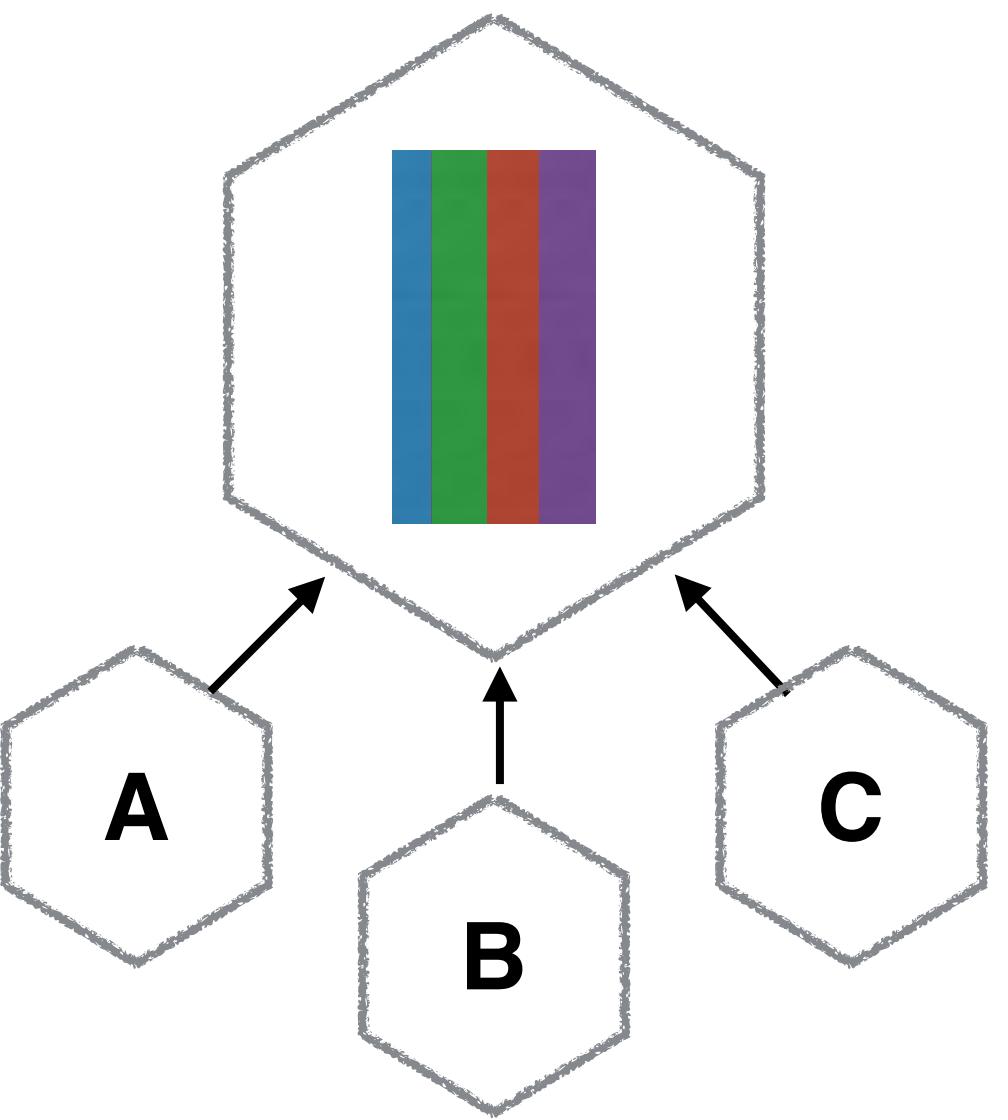
Linkerd

Sidecar



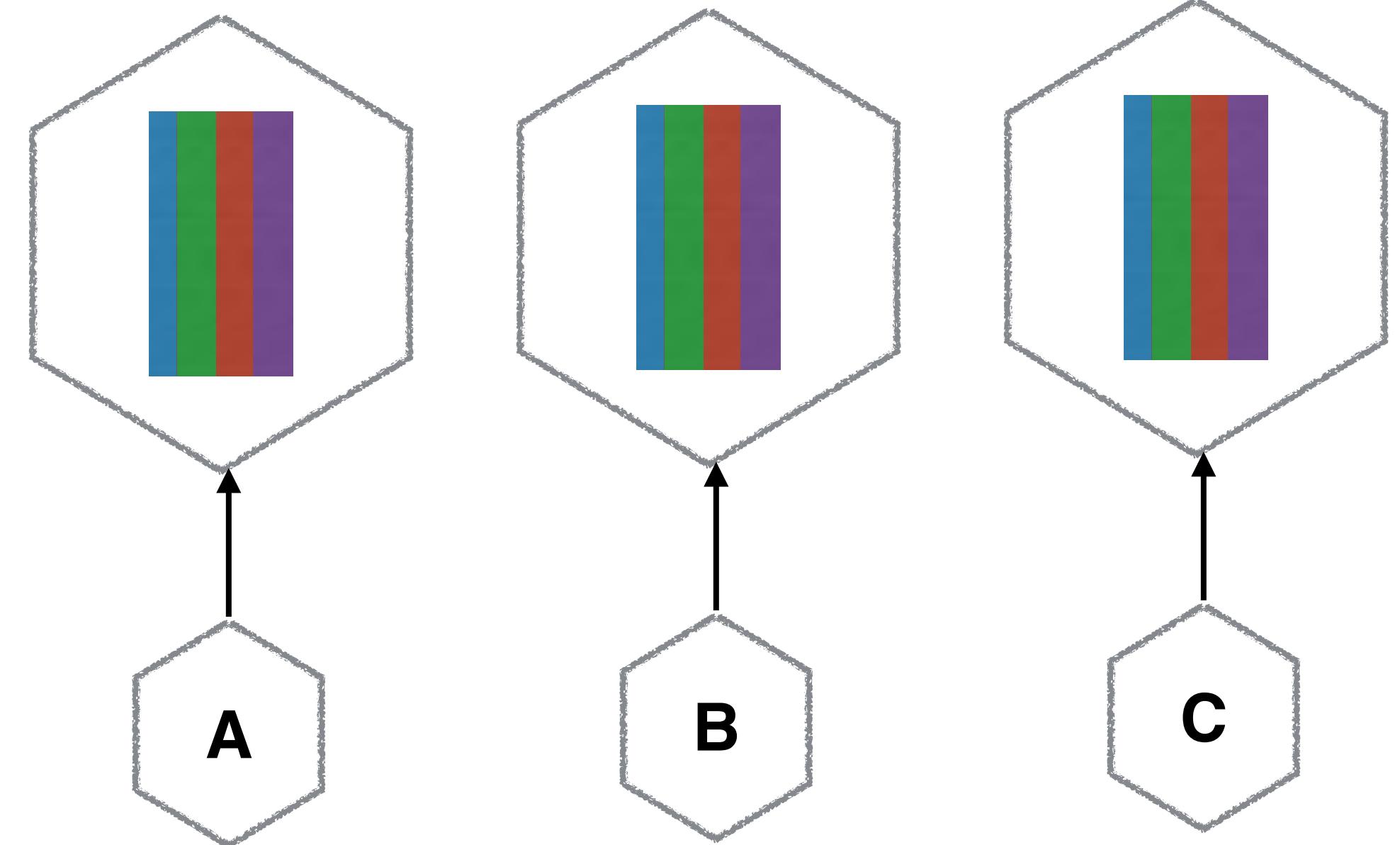
SIDECAR VS PROXIES

Local Proxy



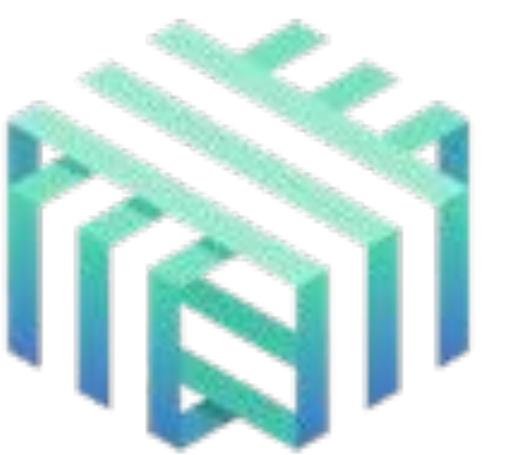
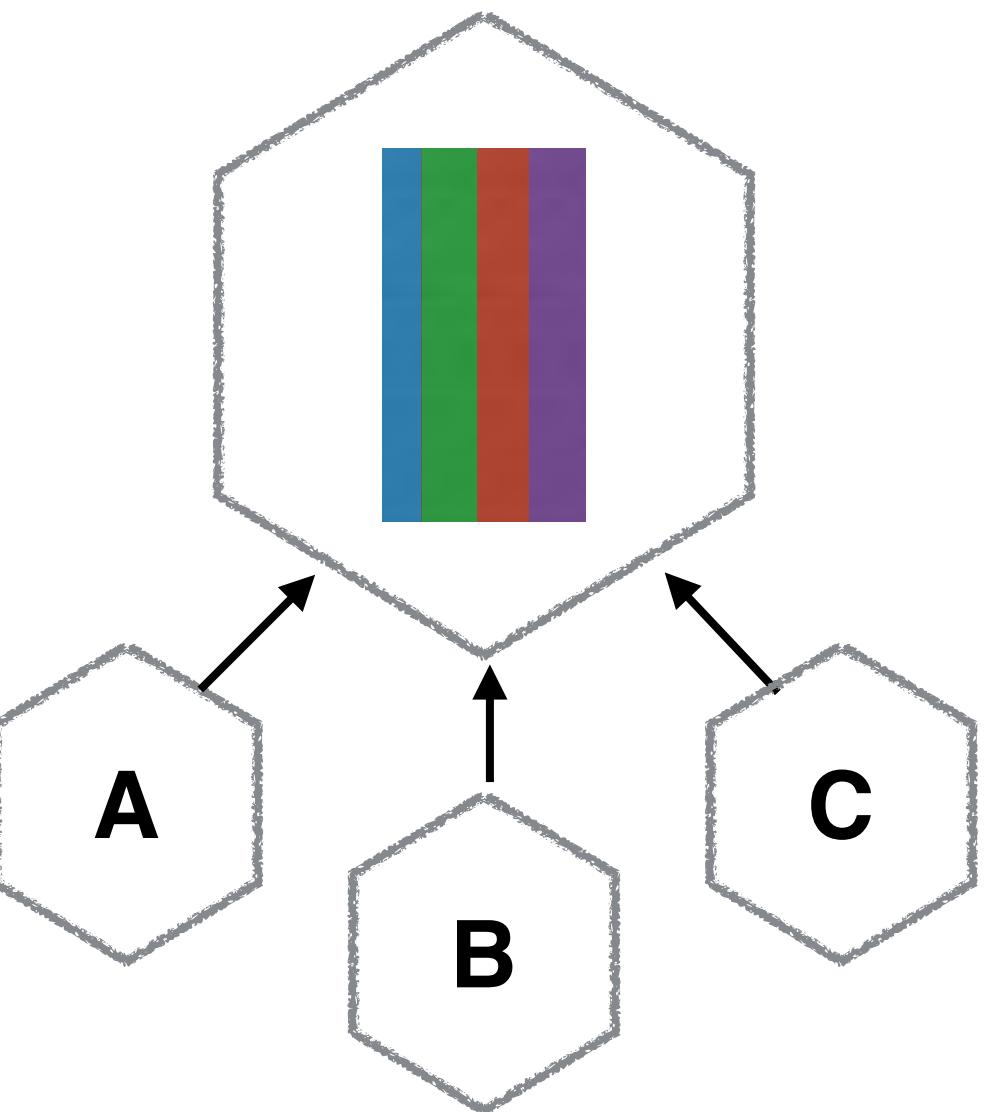
Linkerd

Sidecar



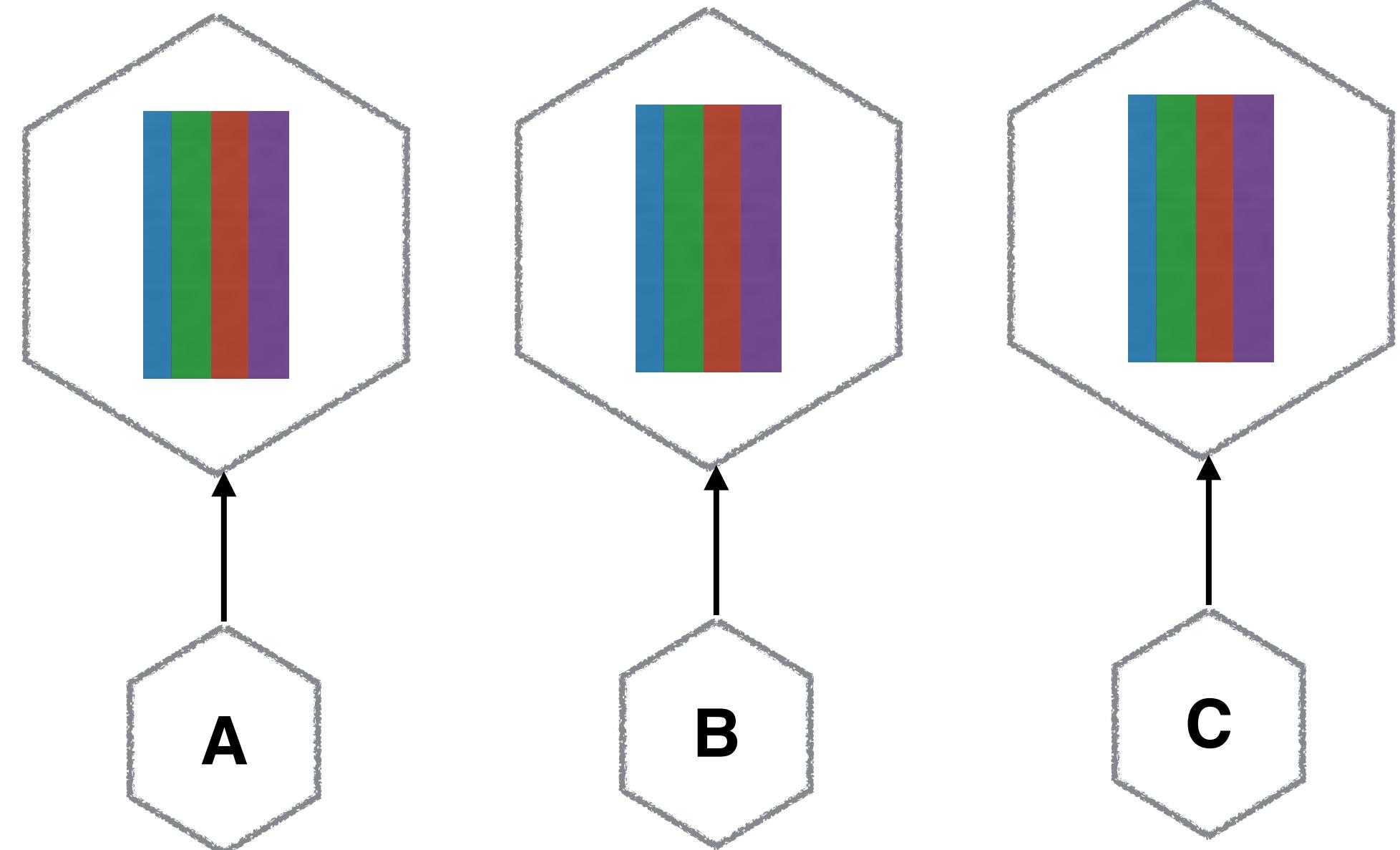
SIDECAR VS PROXIES

Local Proxy



Linkerd

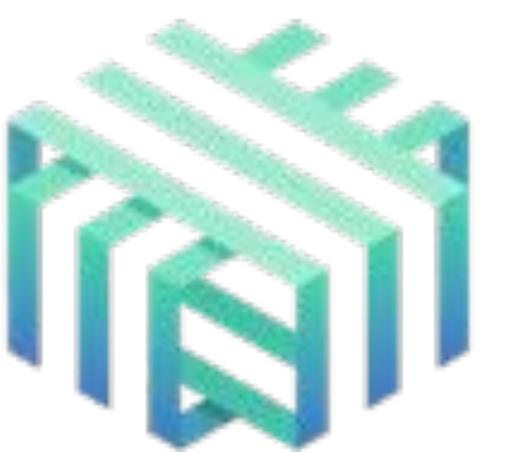
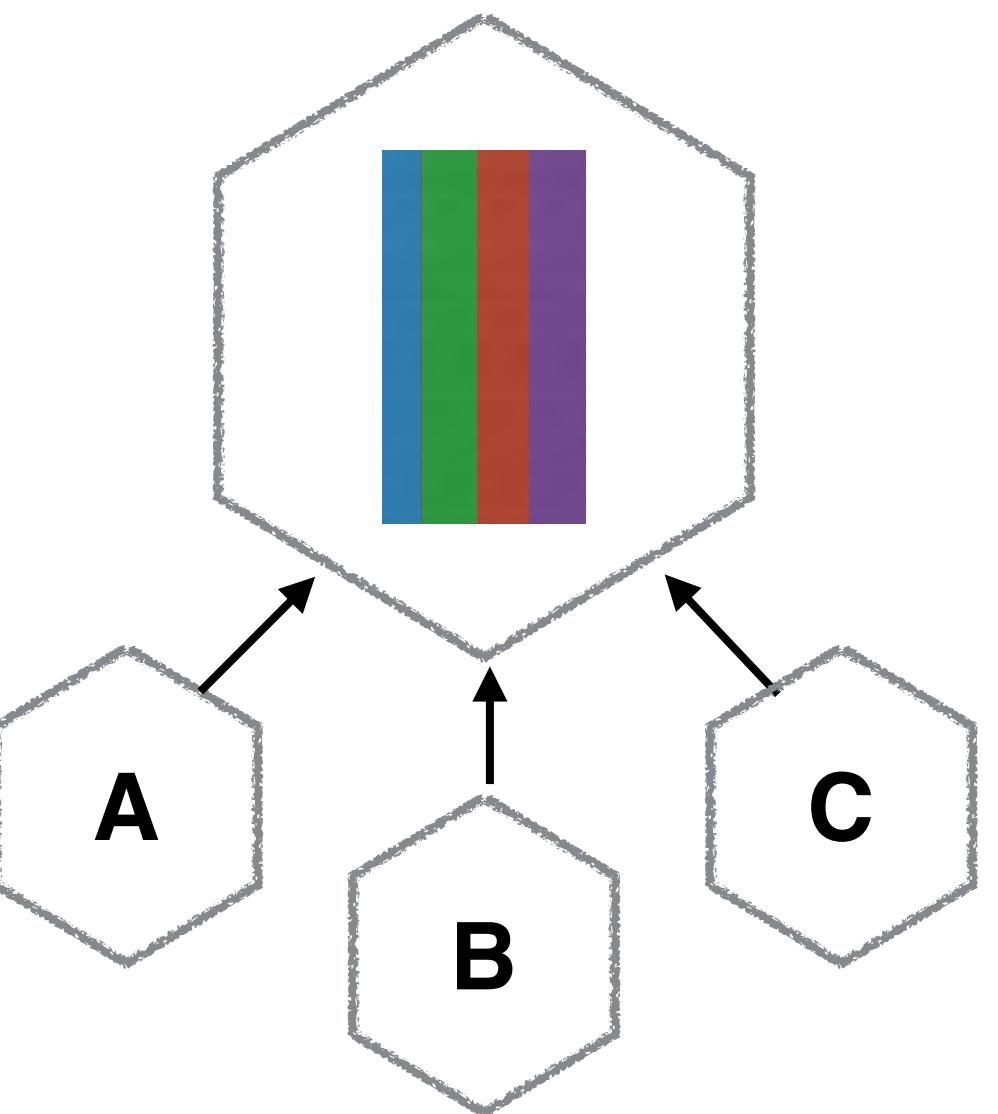
Sidecar



Istio

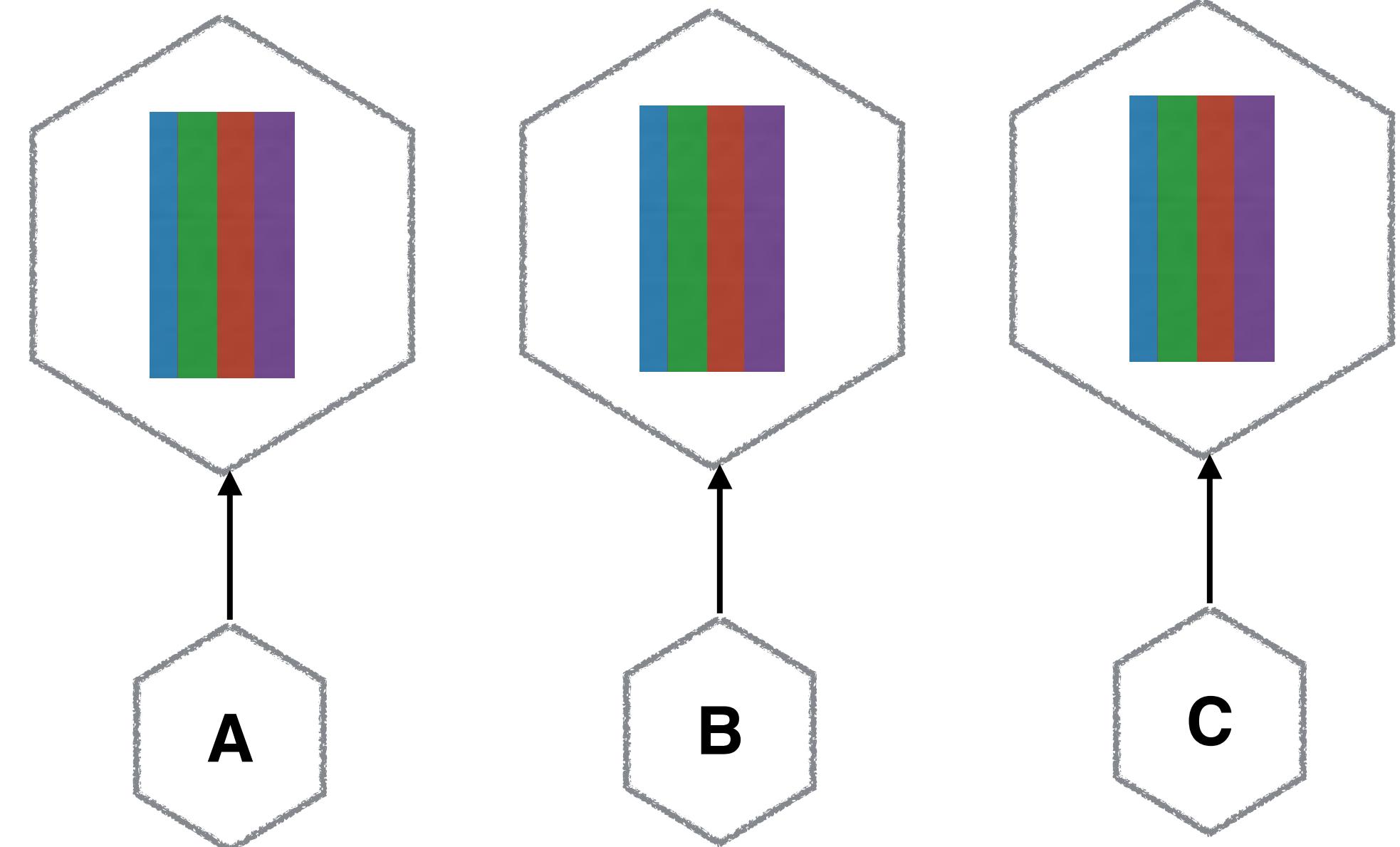
SIDECAR VS PROXIES

Local Proxy



Linkerd

Sidecar



Istio



SERVICE MESH CAPABILITIES

SERVICE MESH CAPABILITIES

Load balancing

SERVICE MESH CAPABILITIES

Load balancing

Traffic Routing (blue/green deploys, canaries)

SERVICE MESH CAPABILITIES

Load balancing

Traffic Routing (blue/green deploys, canaries)

Service discovery

SERVICE MESH CAPABILITIES

Load balancing

Traffic Routing (blue/green deploys, canaries)

Service discovery

Tracing

SERVICE MESH CAPABILITIES

Load balancing

Traffic Routing (blue/green deploys, canaries)

Service discovery

Tracing

Security!

MUTUAL TLS

Mutual TLS Authentication

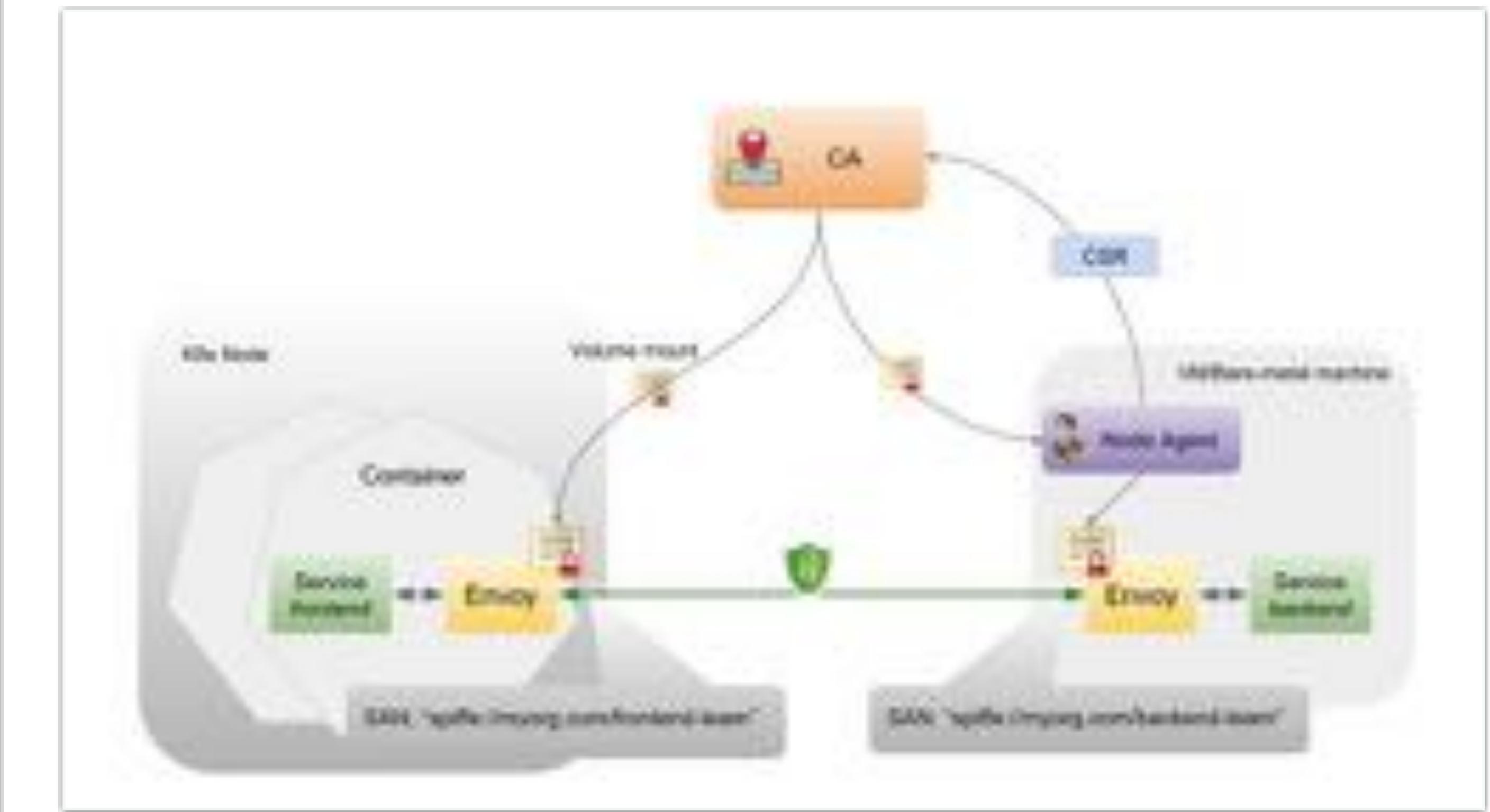
Overview

Istio Auth's aim is to enhance the security of microservices and their communication without requiring service code changes. It is made possible for:

- Providing each service with a strong identity that represents its role to enable interoperability across clusters and clouds.
- Securing service-to-service communication and end user-to-service communication.
- Providing a key management system to automate key and certificate generation, distribution, rotation, and revocation.

Architecture

The diagram below shows Istio Auth's architecture, which includes three primary components: identity, key management, and communication security. This diagram describes how Istio Auth is used to secure the service-to-service communication between service 'Frontend' running as the service account 'FrontendTeam' and service 'Backend' running as the service account 'BackendTeam'. Istio supports services running in both Kubernetes containers and VM bare metal machines.



<https://istio.io/docs/concepts/security/mutual-tls.html>

Caution warranted?

SUMMARY

SUMMARY

Patching & Passwords

SUMMARY

Patching & Passwords

Storing Secrets

SUMMARY

Patching & Passwords

Storing Secrets

Transport Security

SUMMARY

Patching & Passwords

Storing Secrets

Transport Security

Authorisation

SUMMARY

Patching & Passwords

Storing Secrets

Transport Security

Authorisation

Service Meshes

THANKS!

Sam Newman

Home News **Books** Events Writing Contact

Insecure Transit - Microservice Security

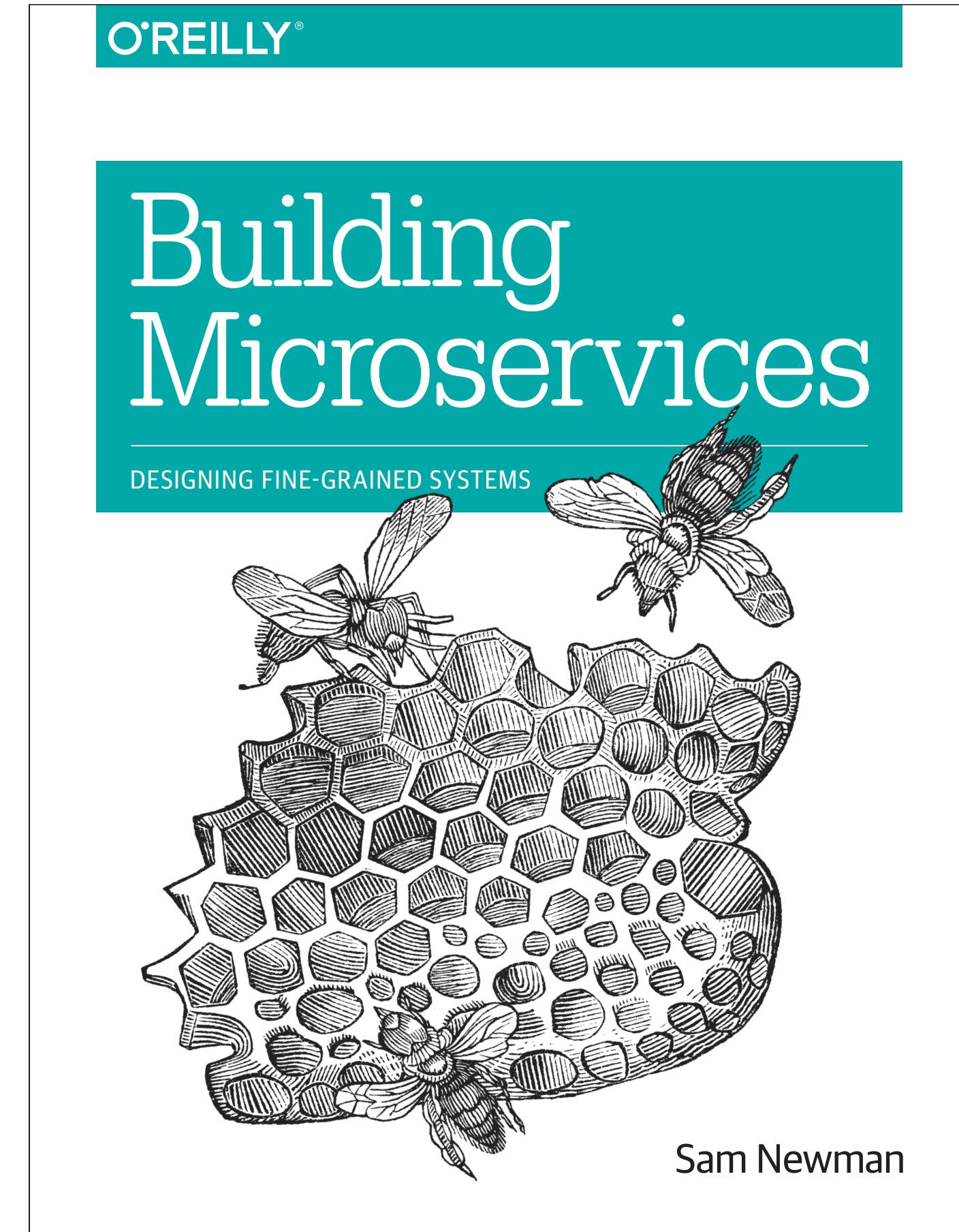
WATCH THIS ARTICLE

Book!

Building Microservices

DESIGNING FINE-GRAINED SYSTEMS

Video!



<http://samnewman.io/>

@samnewman