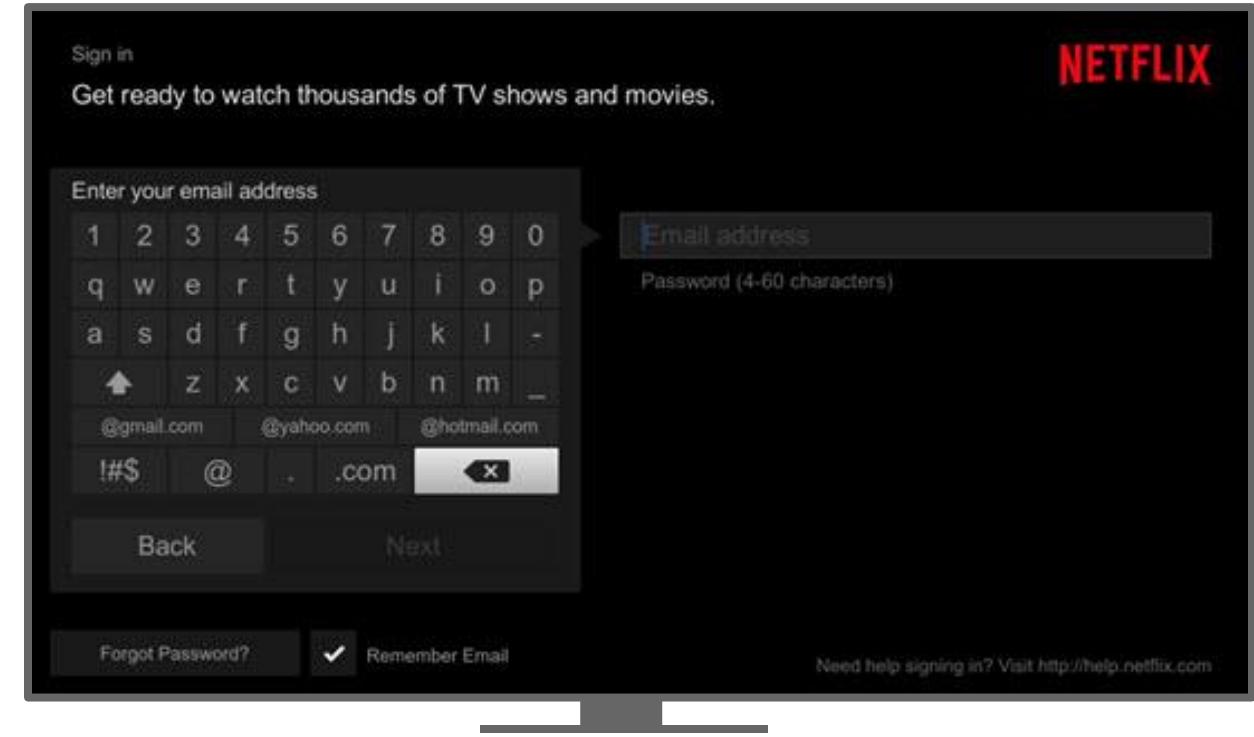
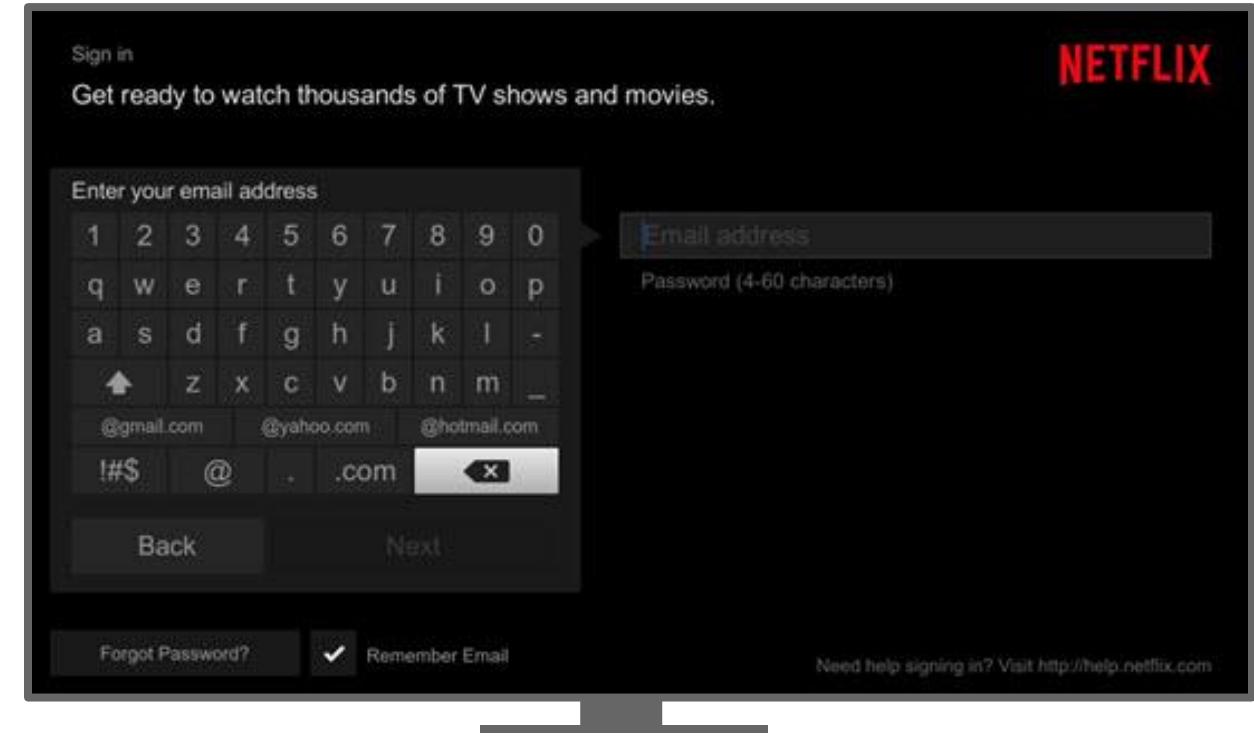


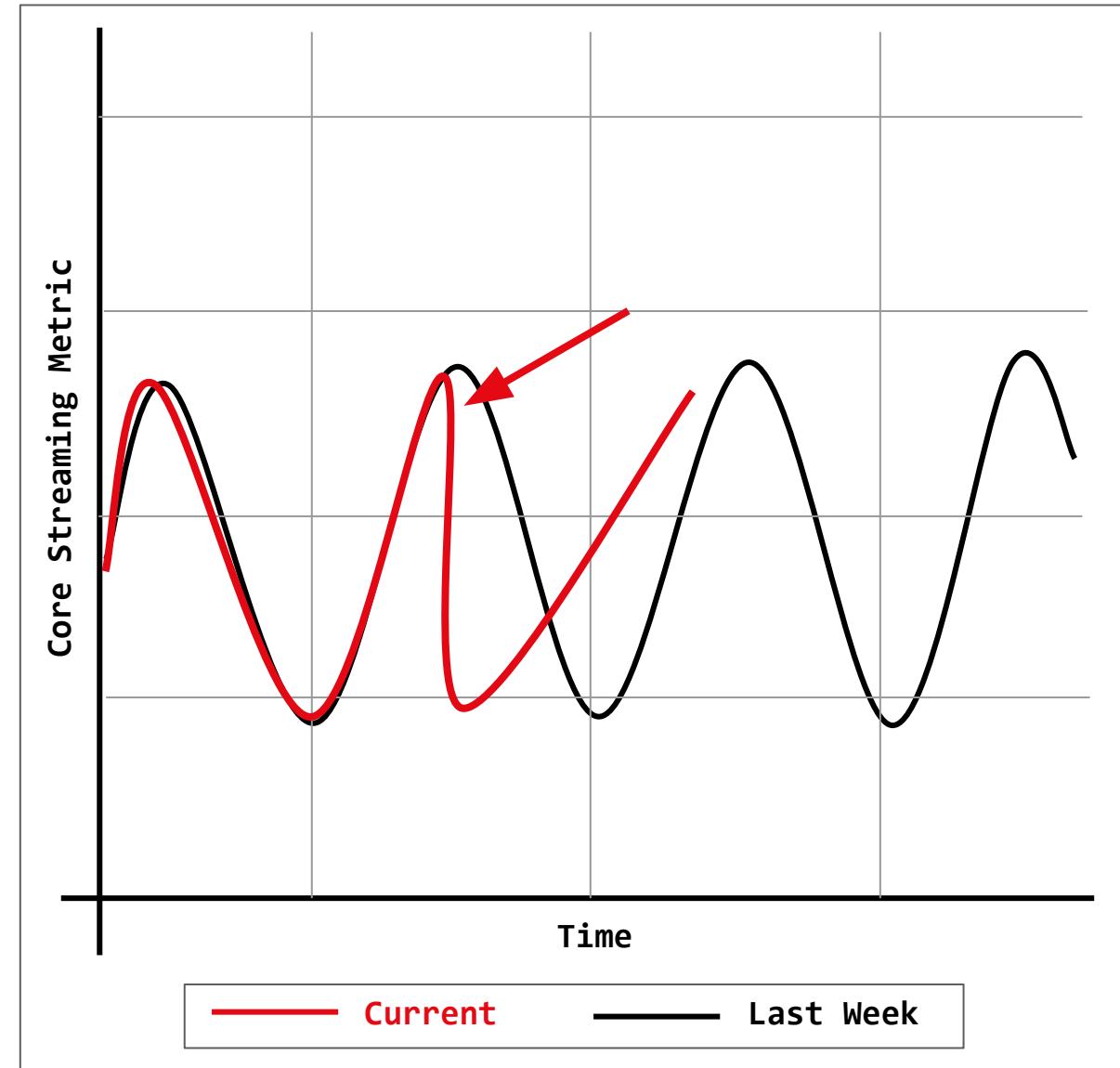
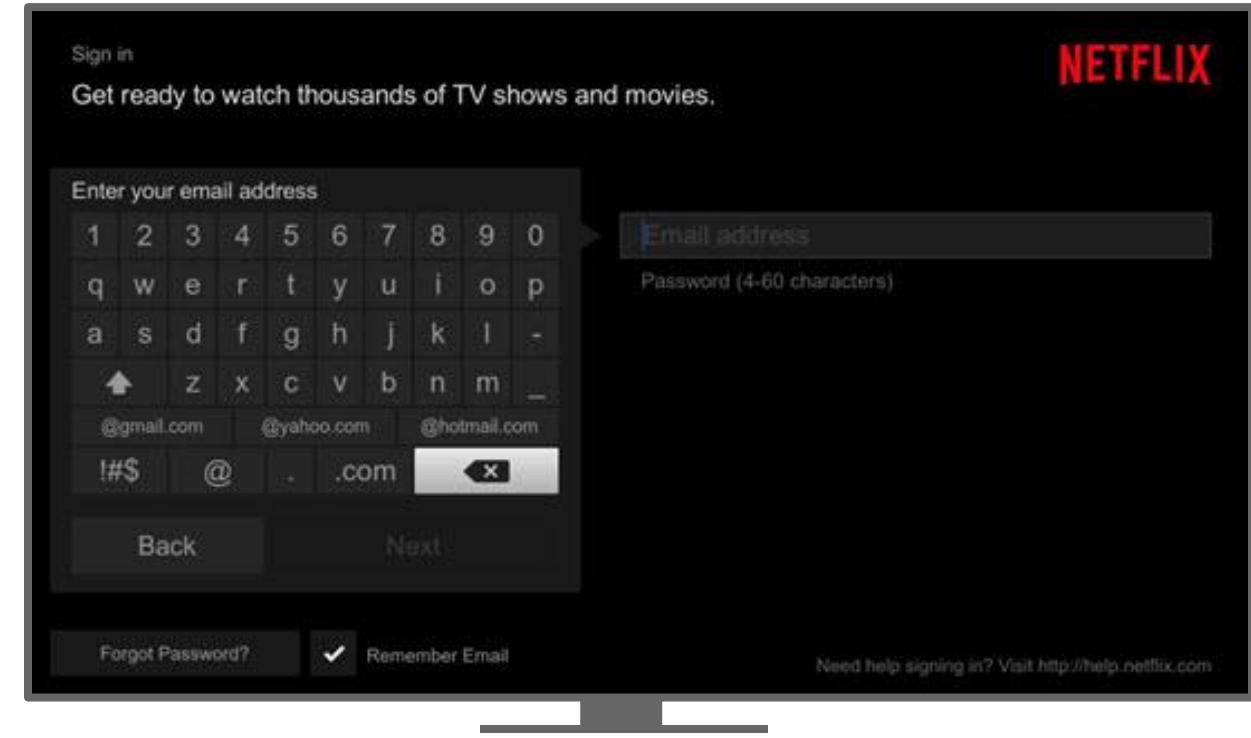
# User & Device Identity For Microservices @ Netflix Scale

**Satyajit Thadeshwari**  
**QCon San Francisco 2019**









# Satyajit Thadesswar

## Product Edge Access Systems

sthadesswar@netflix.com



solved parade of  
suspects, includin  
Allen, the man  
tests have now 1  
assault.

Two years earli  
exposed himself  
grab a woman o  
beach where the  
woman was ass  
Tom Kocourek,  
tired Manitowoc  
iff, said last week  
vestigators neve  
the Two Rivers P  
which hand  
while it

Steven

DNA evidence  
to clear local n  
of 1985 convic

# Complicated



**NETFLIX** Dashboards ▾ Projects ▾ Issues ▾ Capture ▾ Boards ▾ AIO Tableau ▾ Create Search    

 Prod Alert

 Edit  Comment  Assign  More ▾ Resolved Stable Active   Export ▾

**Details**

Type:  Incident Status:  (View Workflow)  
Resolution: Resolved

Labels: None   
Severity: Major  
Cause of Incident: Unknown  
AWS Region: US-East-1, US-West-2, EU-West-1  
Affected Devices: Not Applicable  
Notify Partner(s): No

**People**

Assignee:   
Reporter:   
Votes: 0 Vote for this issue  
Watchers: **57** Stop watching this issue

**Description**

**Involved Parties:**

- CORE -
- API -
- Zuul -
- Website/Shakti -
- Website/Browser Player -
- Playback Access -
- Client Security -
- GPE -
- Subscriber/Auth -
- CS - Tier 3 +

**9 TEAMS**

**57 WATCHERS**

**Dates**

Created: 06/13/2016 11:59 AM  
Updated: 06/28/2016 09:36 AM  
Resolved: 06/22/2016 04:41 PM

**Issue Reminders**

Add New Reminder 

**Development**

7 commits  
5 pull requests 

Create branch



# **Netflix subscribers and the devices that they use**

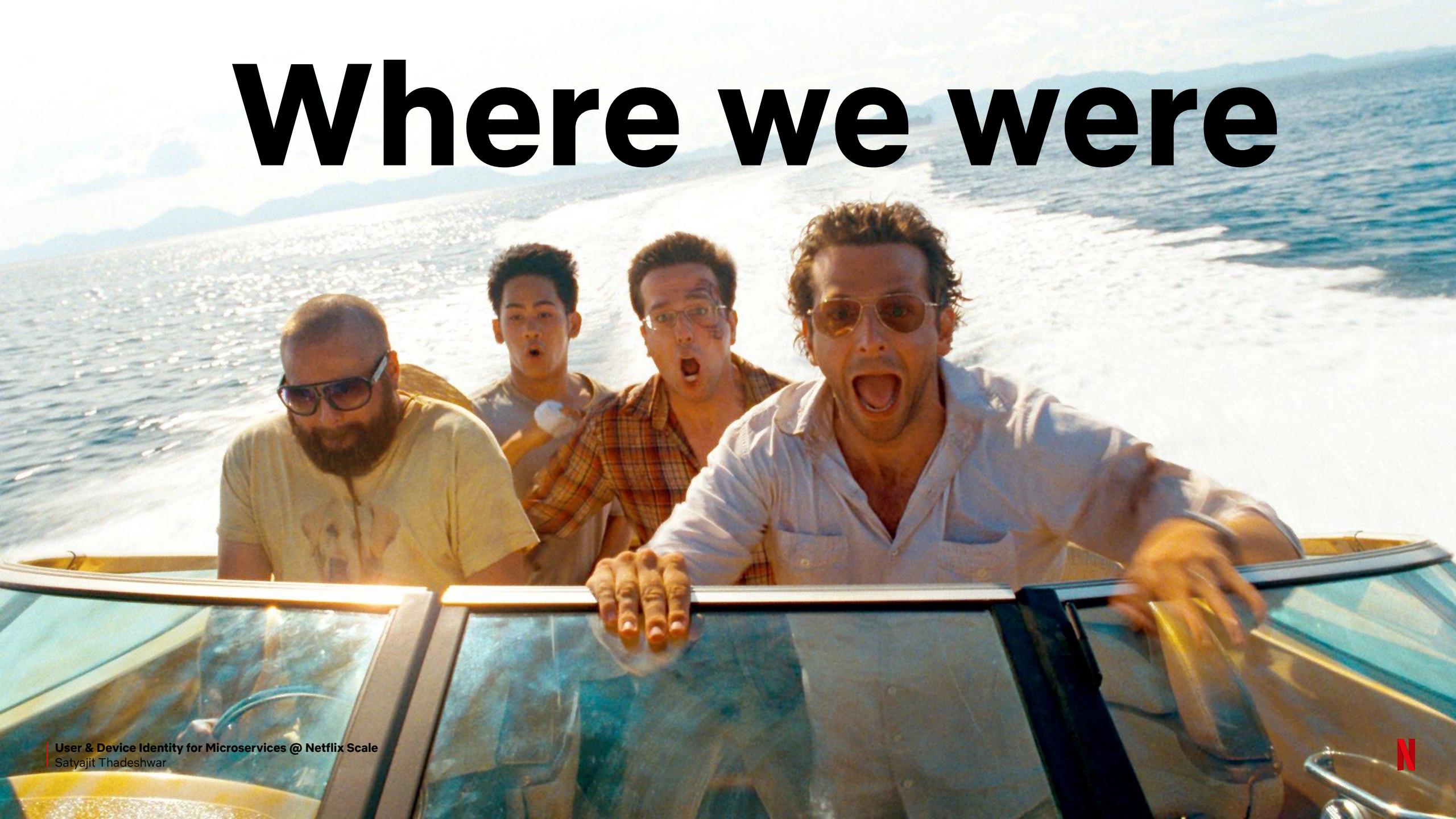


# Where we were

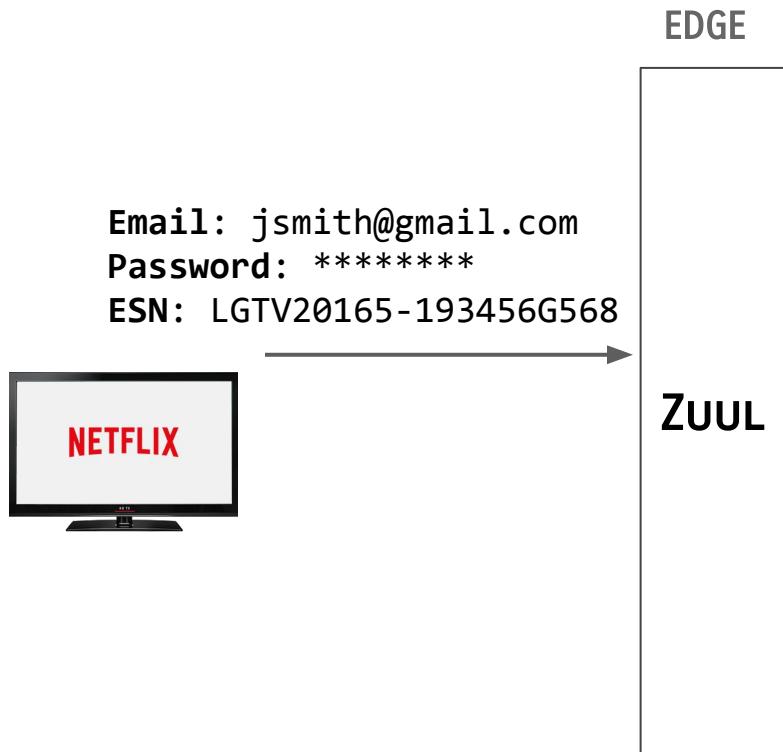
# What we did

# Wins

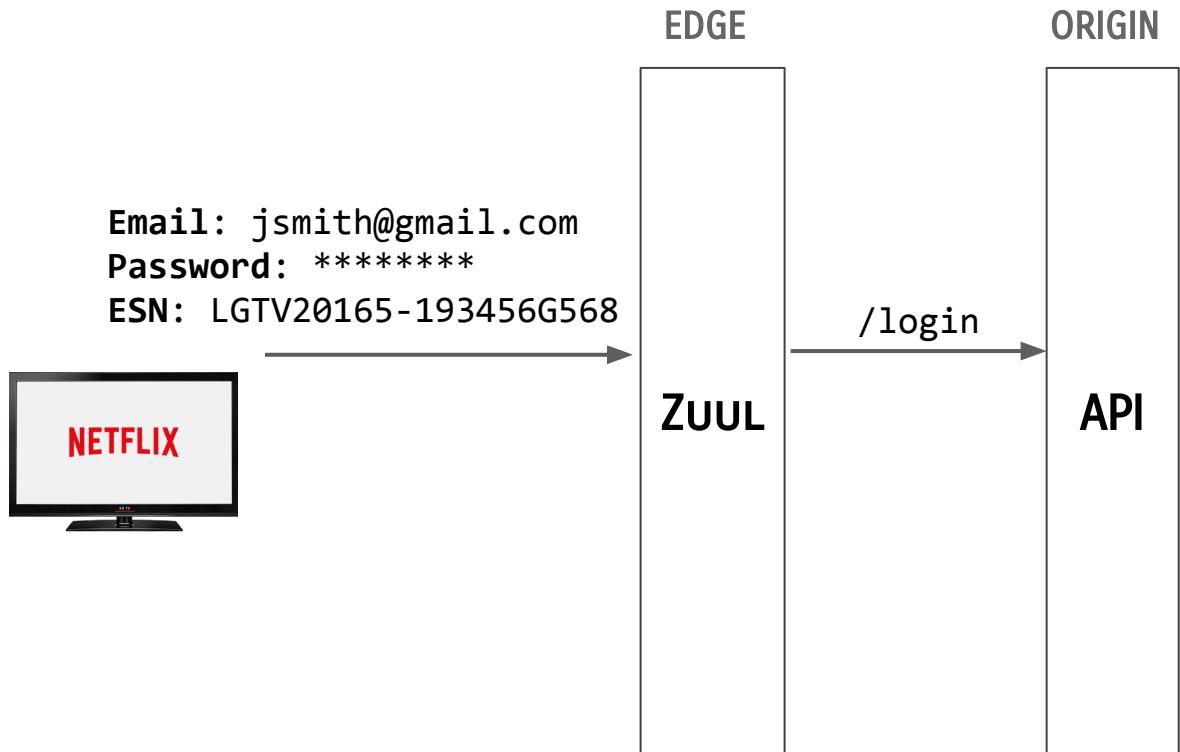
# Where we were

A photograph from the movie Ocean's Thirteen showing four men in a boat. From left to right: Matt Damon (as Rusty), Benicio del Toro (as Gordo), Michael Stuhlbarg (as Danny), and Brad Pitt (as Lincoln). They are all looking forward with expressions of surprise or shock. The boat is moving through the water, creating a wake. The background shows a bright sky and distant mountains.

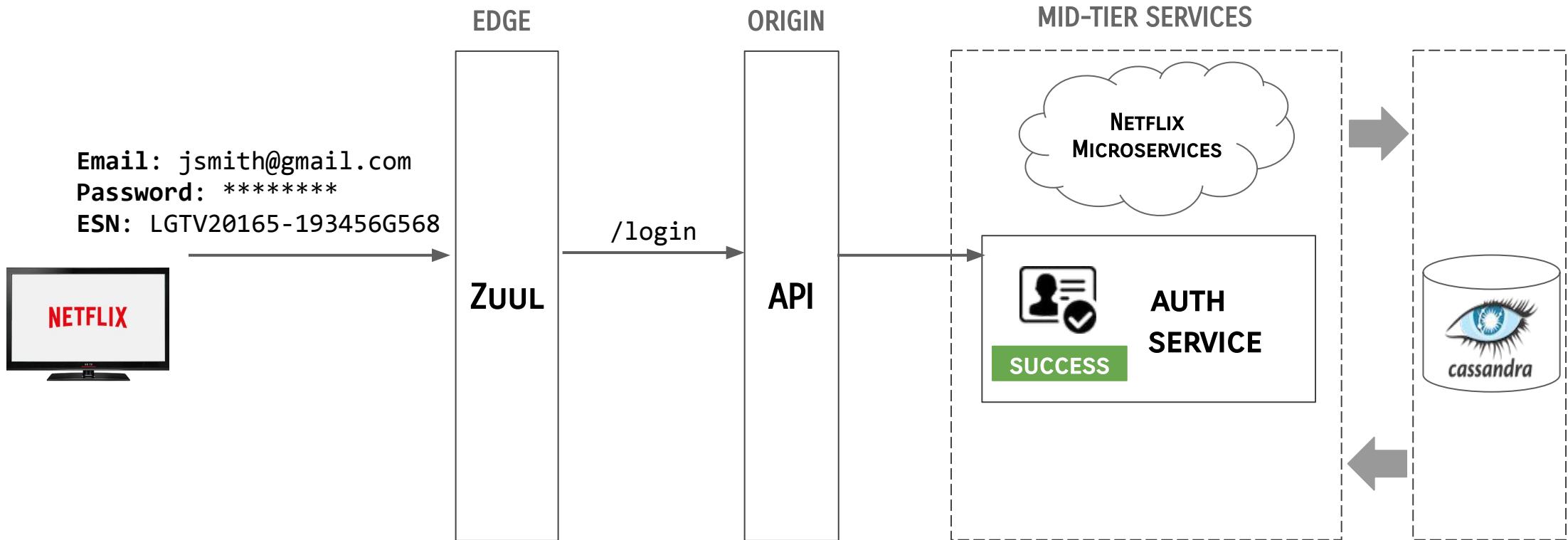
# User Login



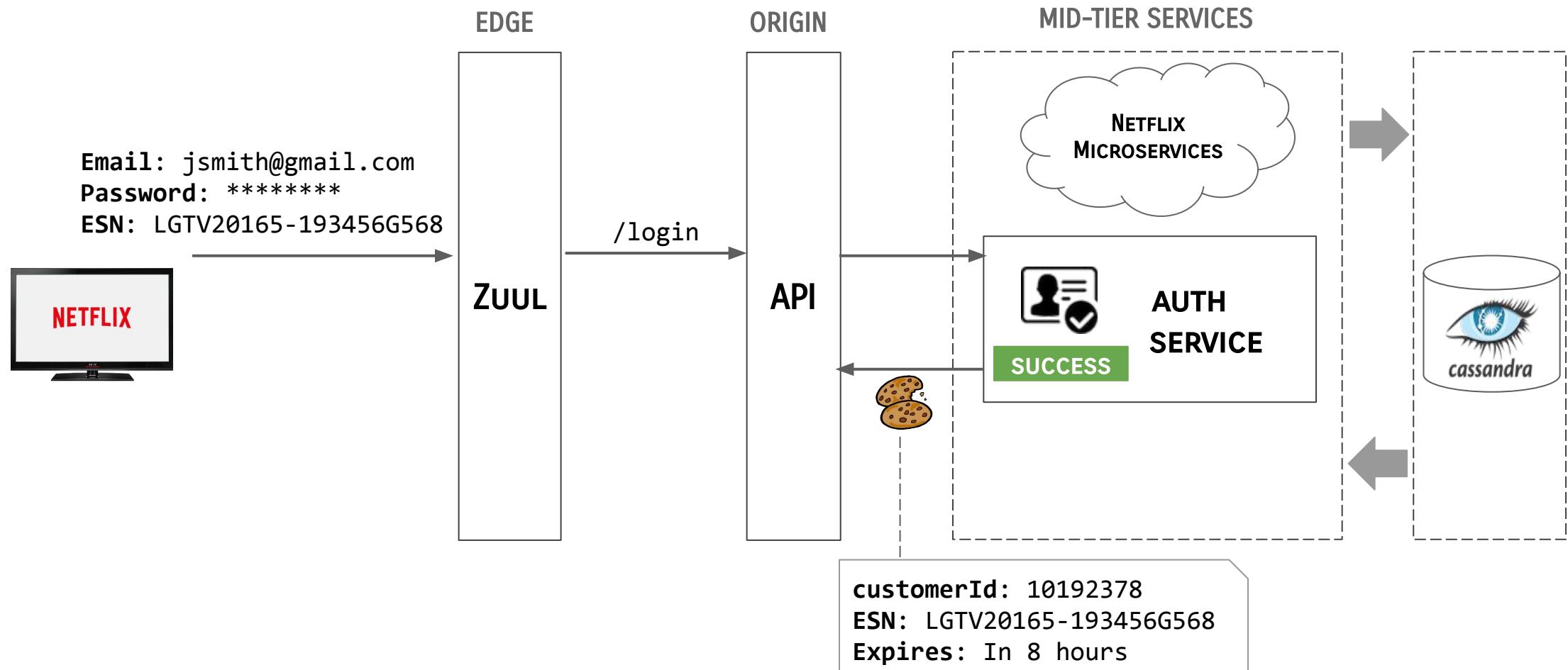
# User Login



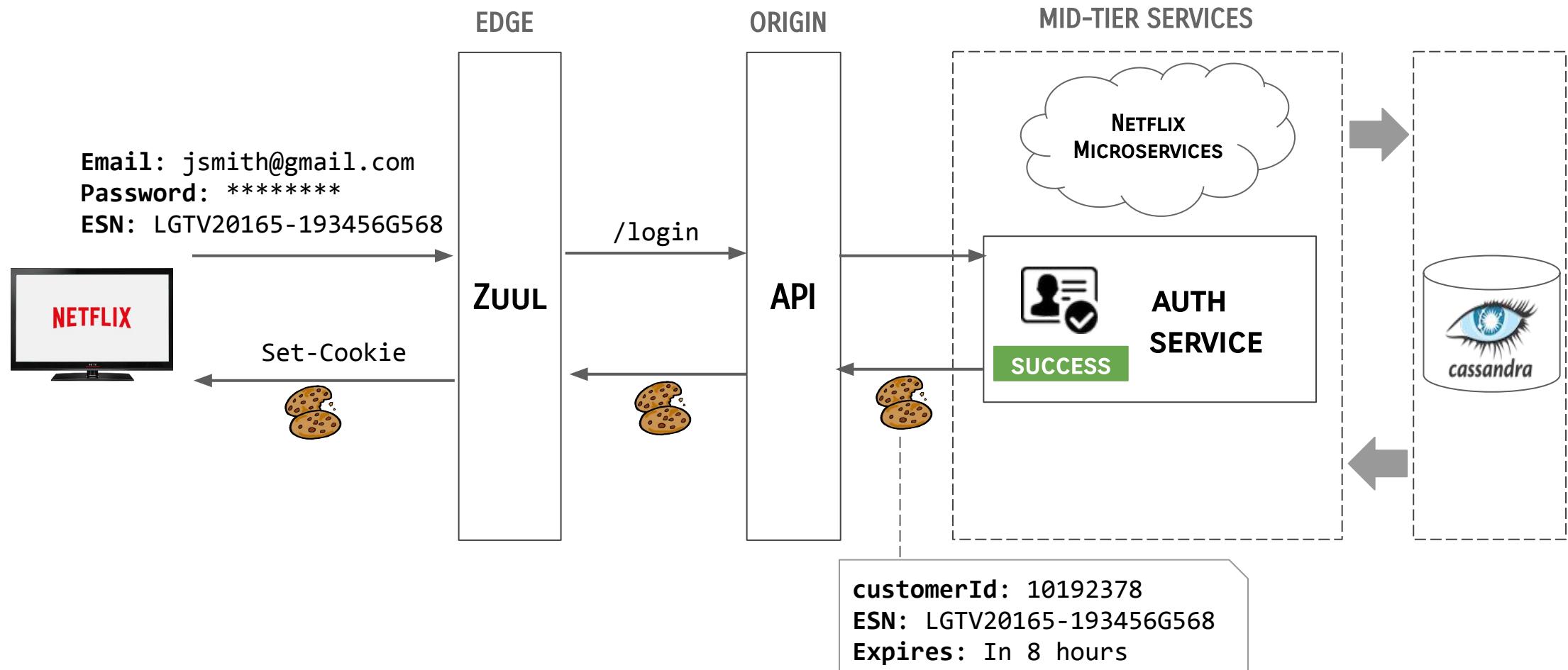
# User Login



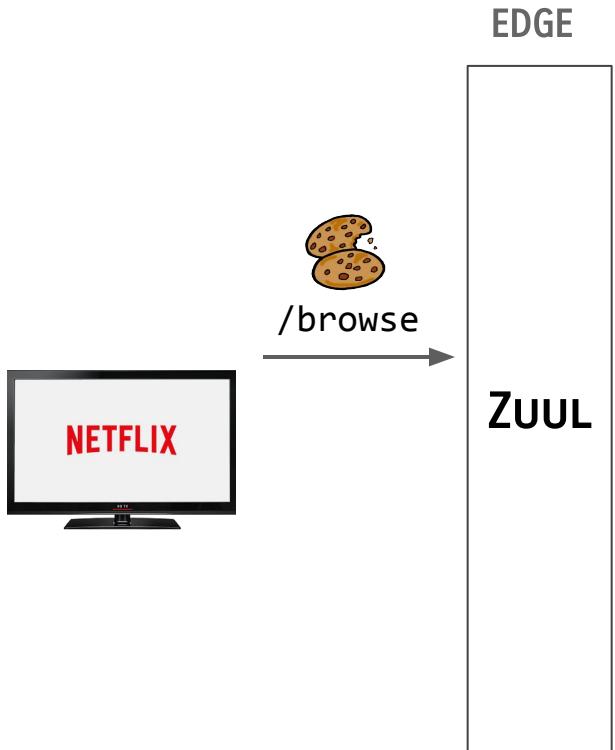
# User Login



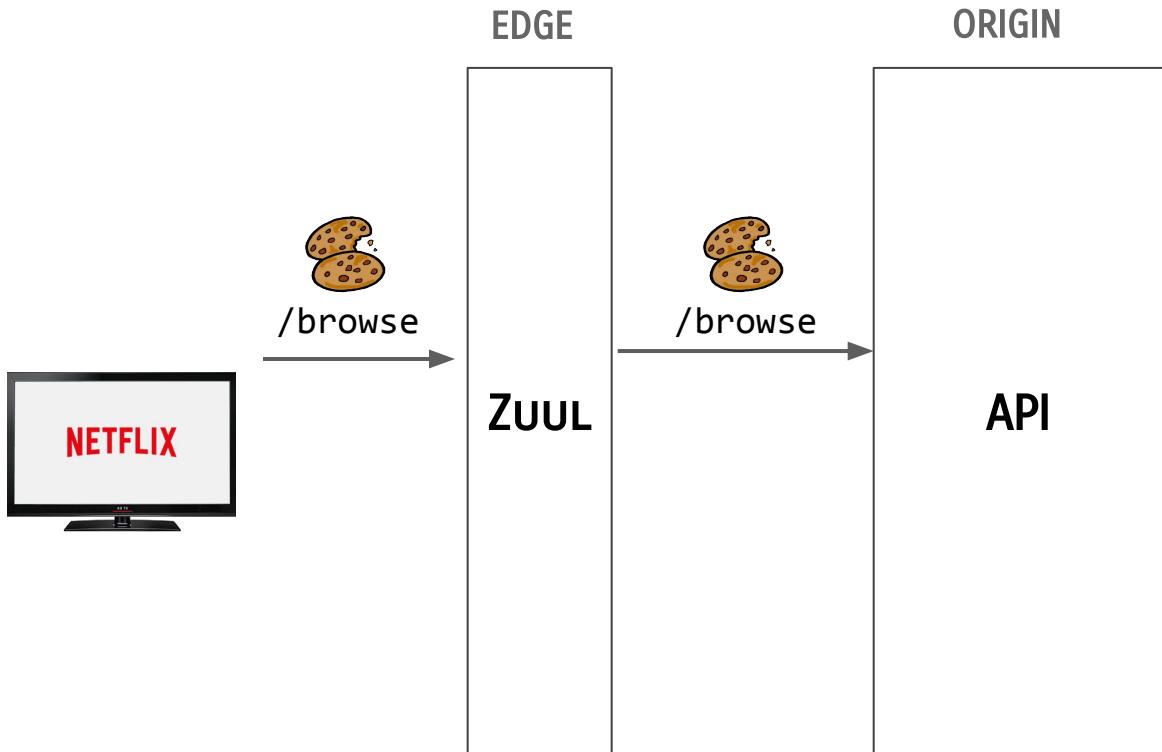
# User Login



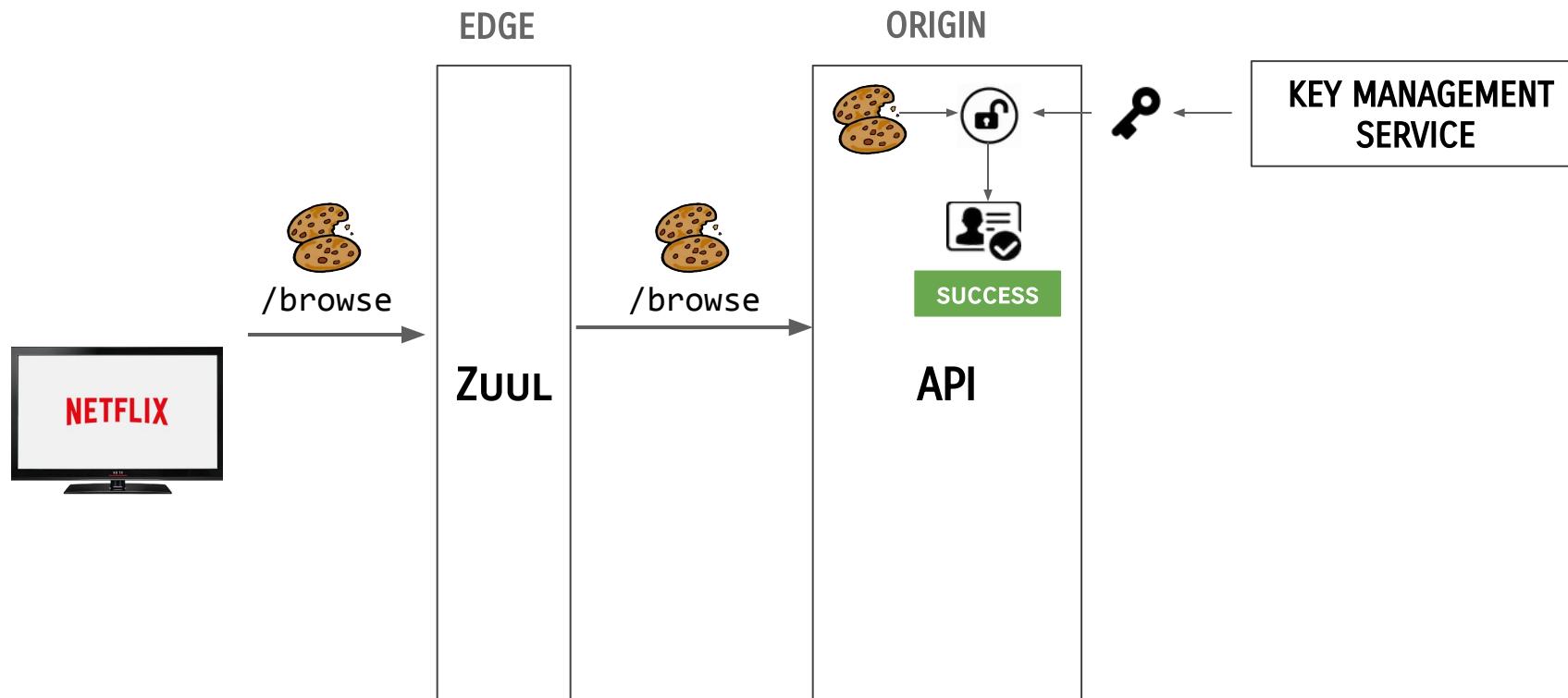
# Authenticate Request



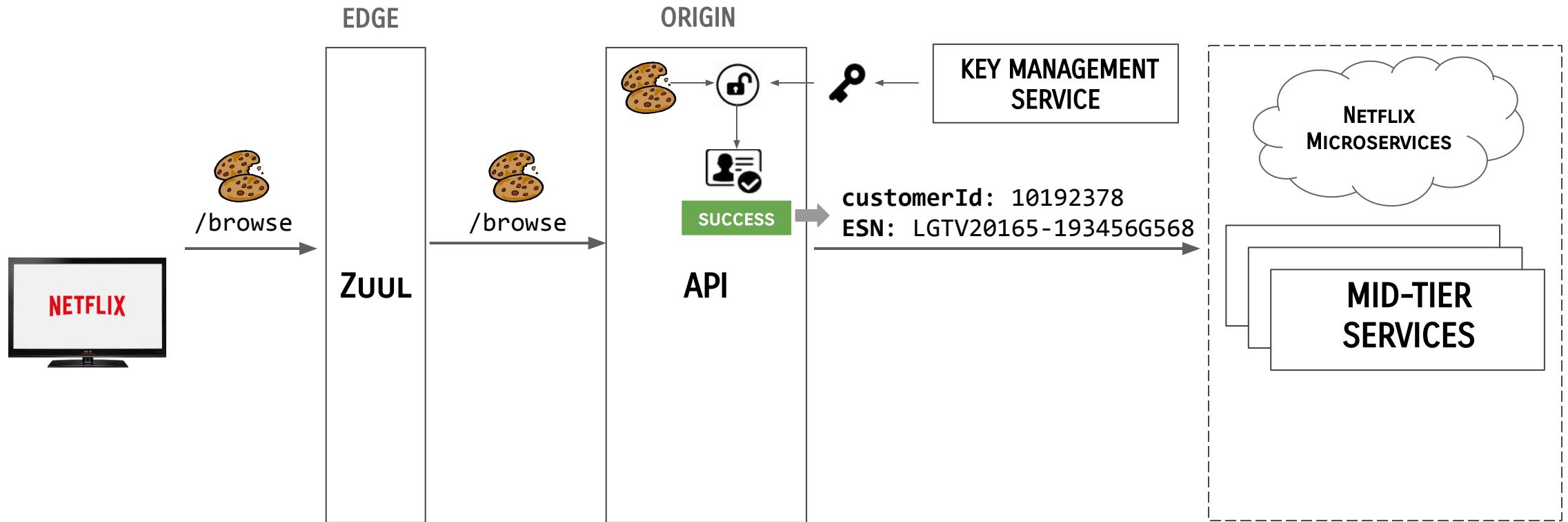
# Authenticate Request



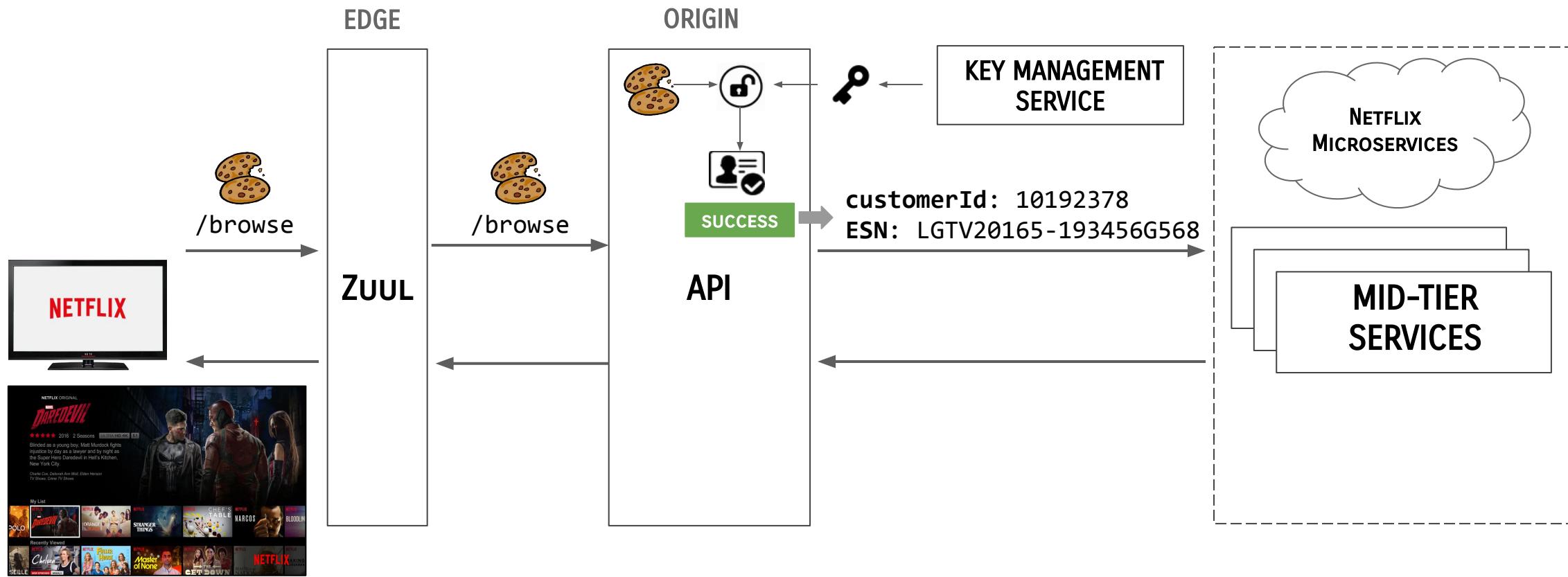
# Authenticate Request



# Authenticate Request

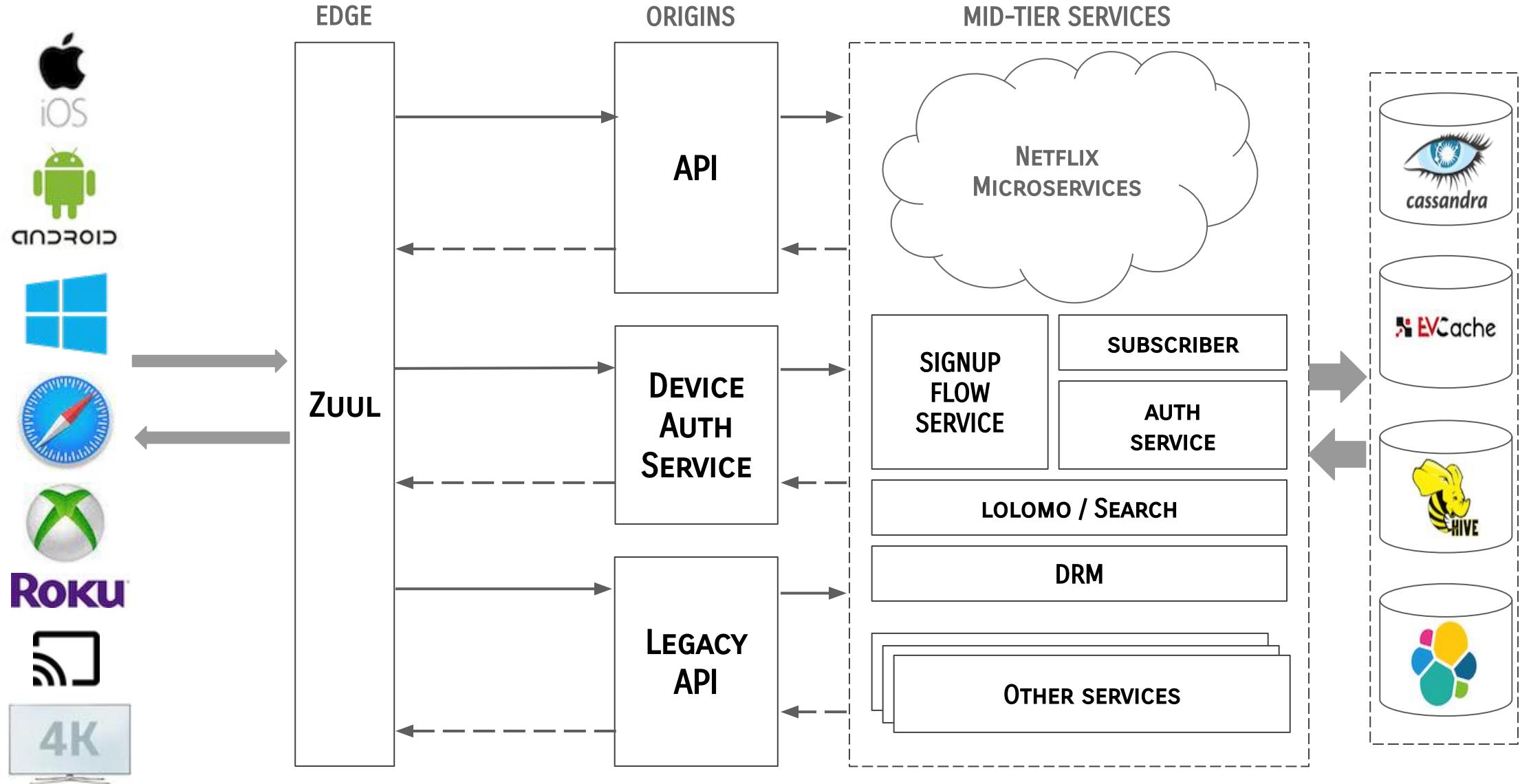


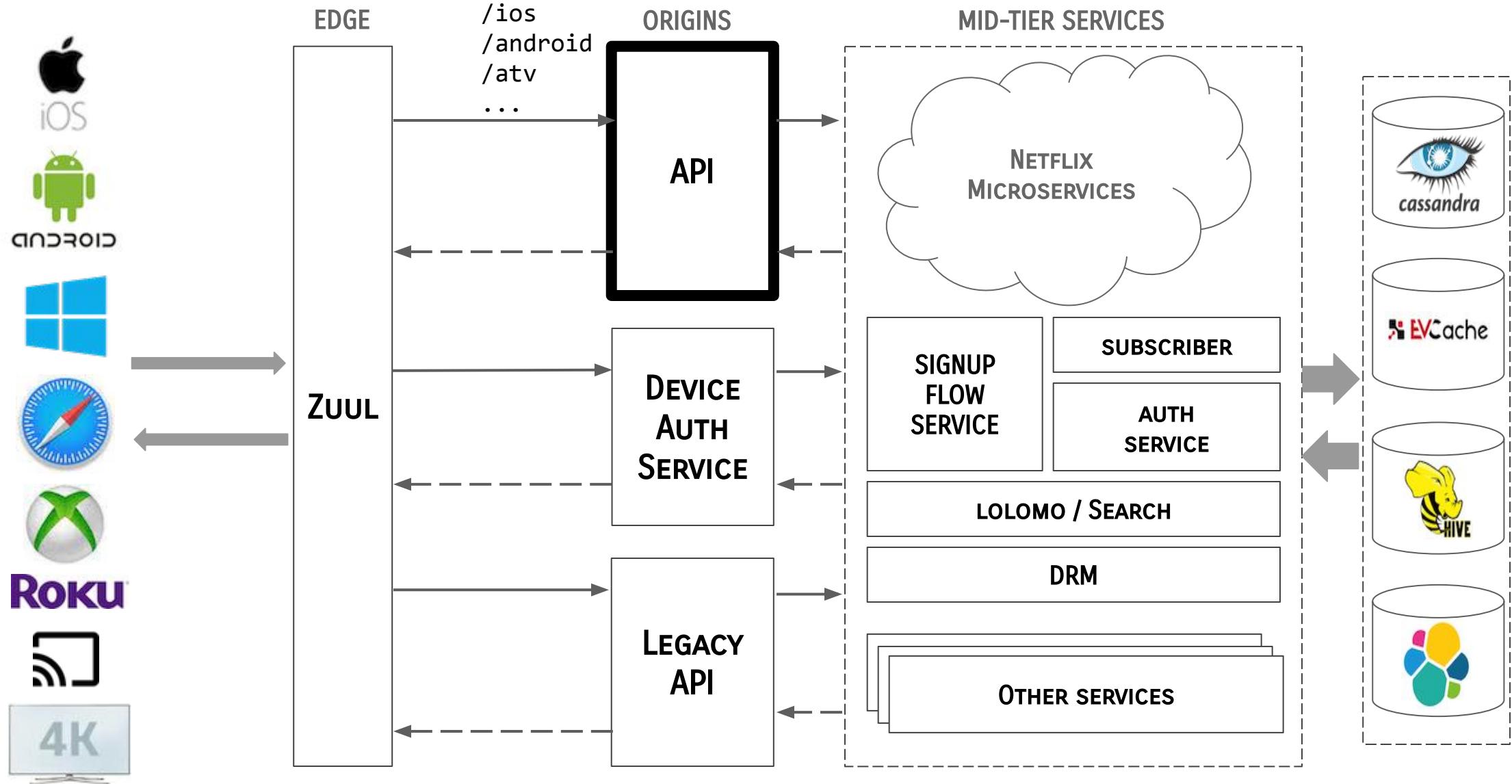
# Authenticate Request

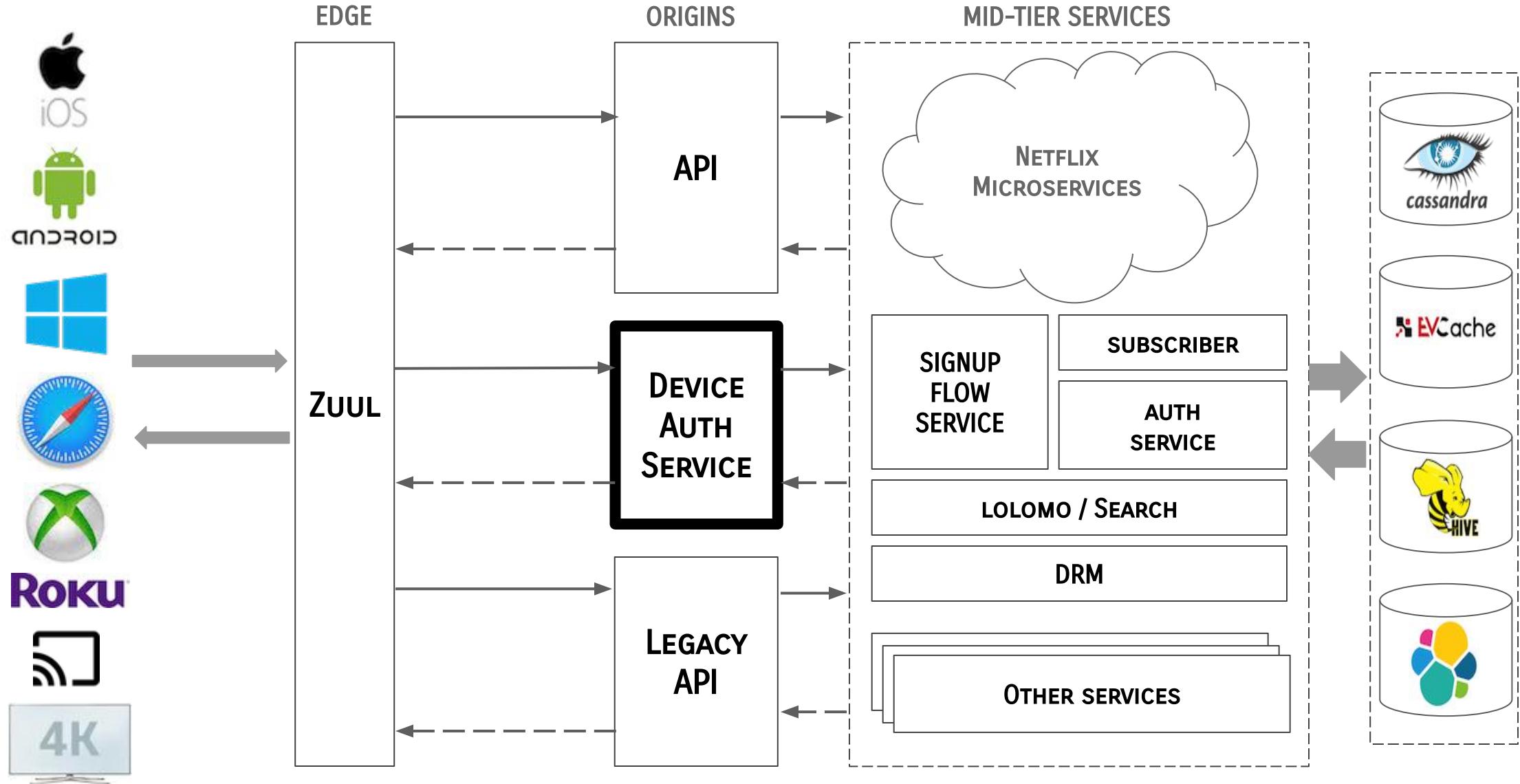


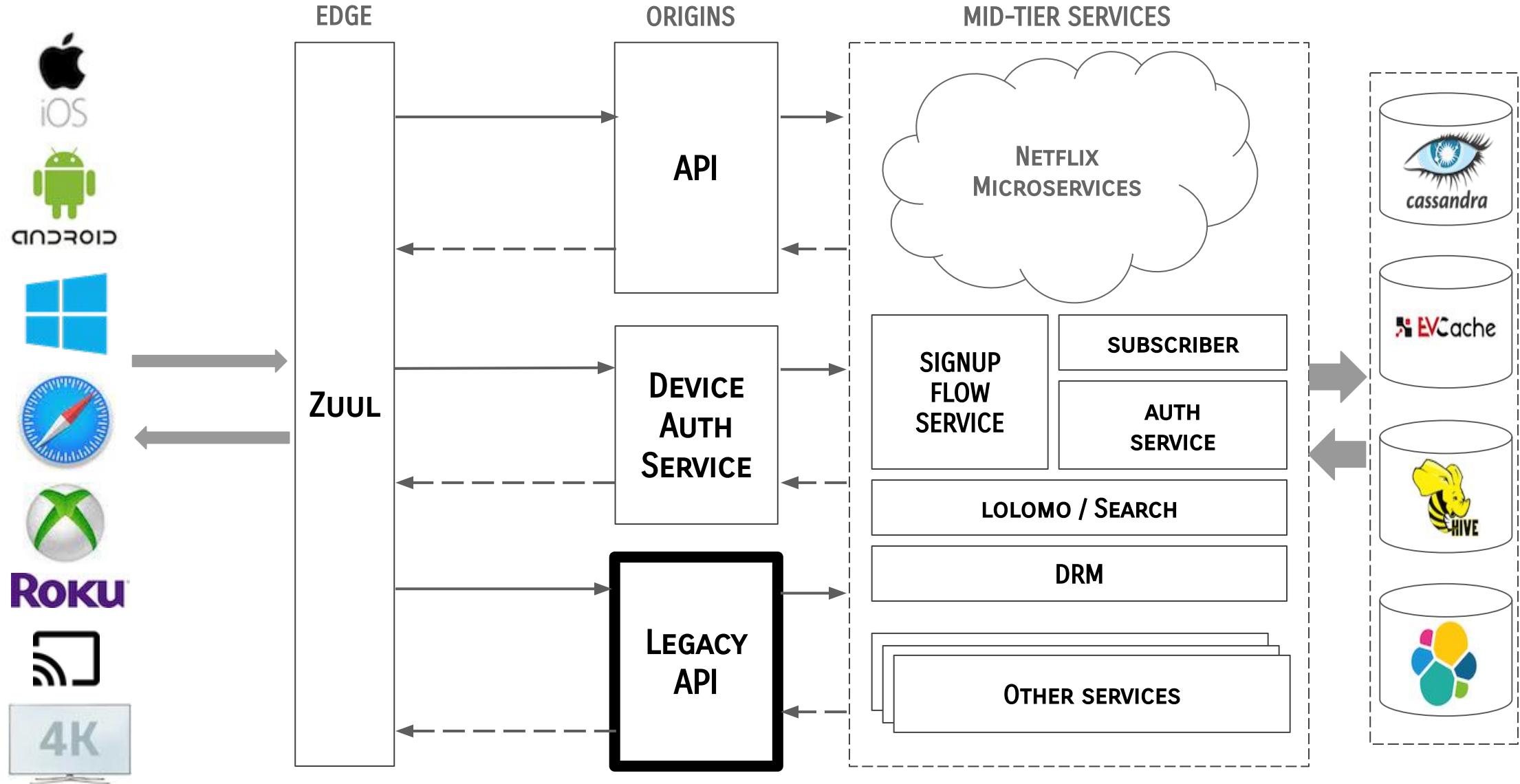
# **More than one service consuming cookies**

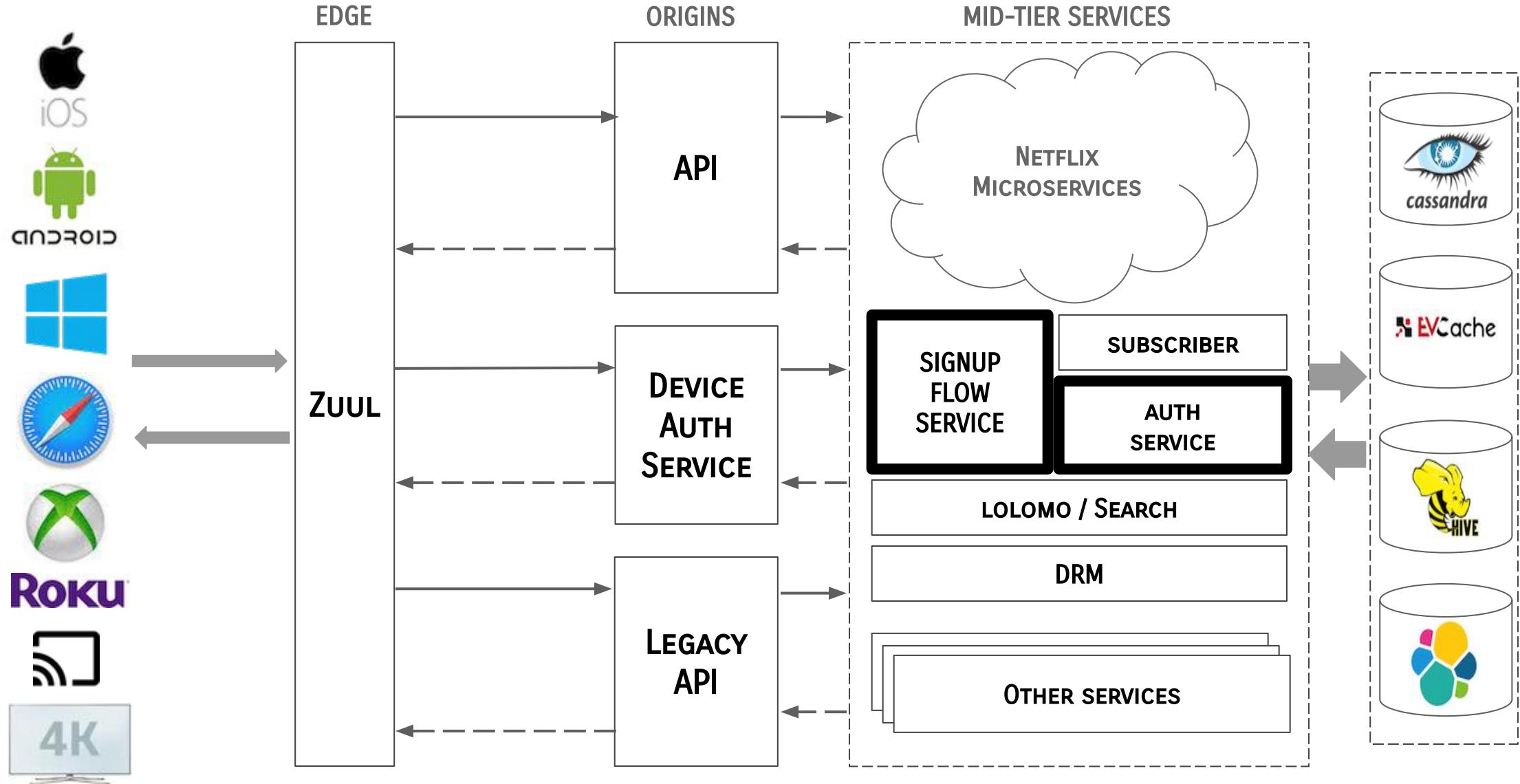


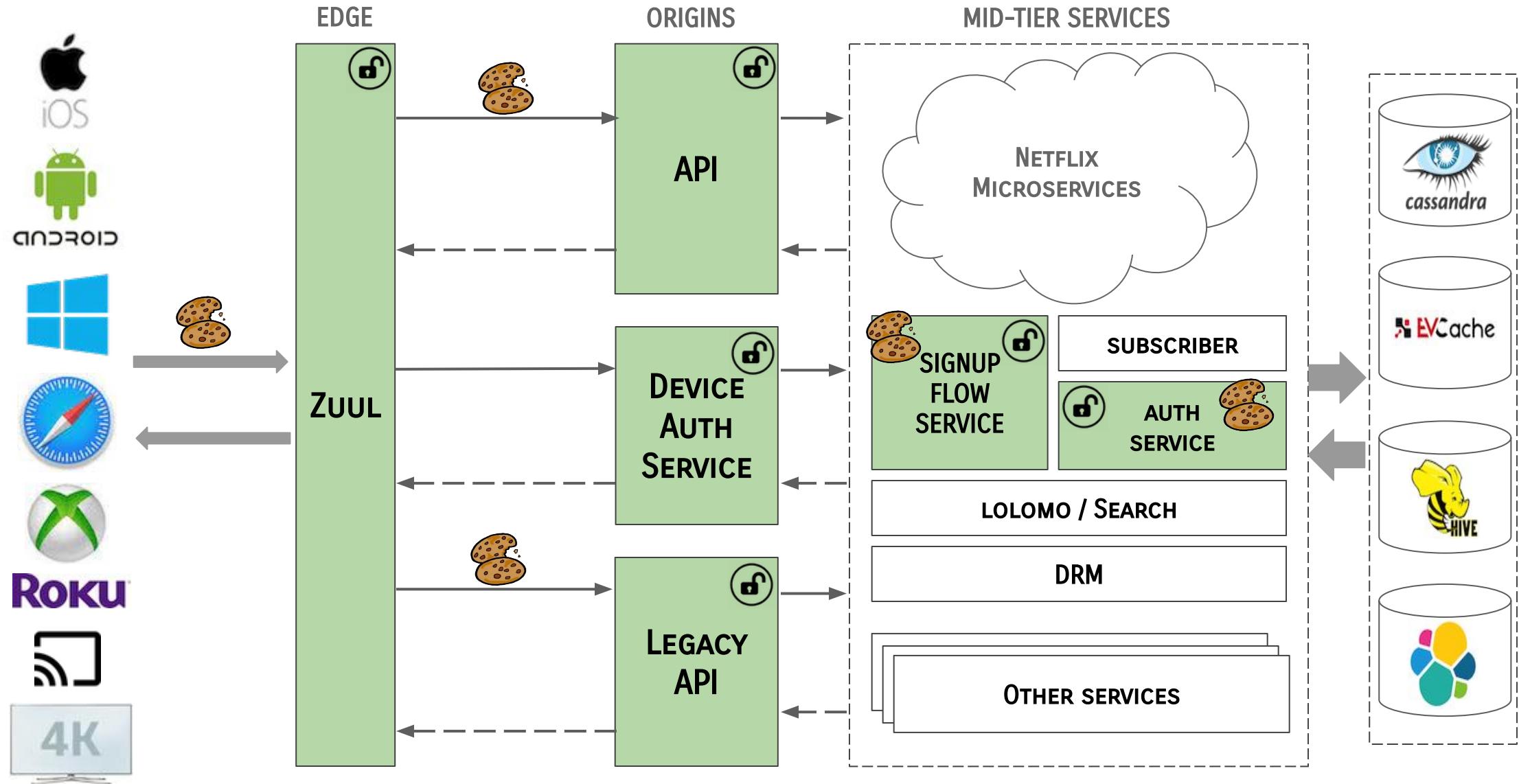










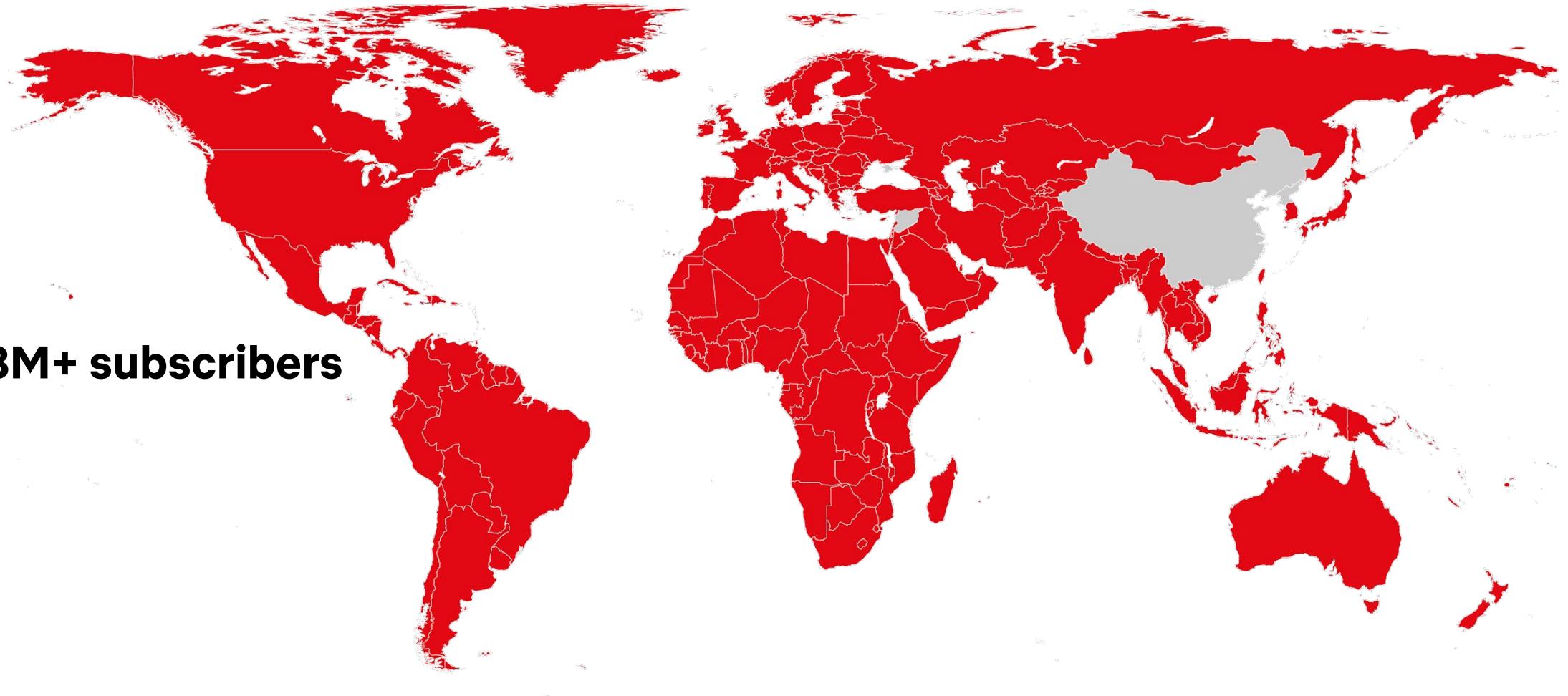


# **At massive scale**



# Netflix

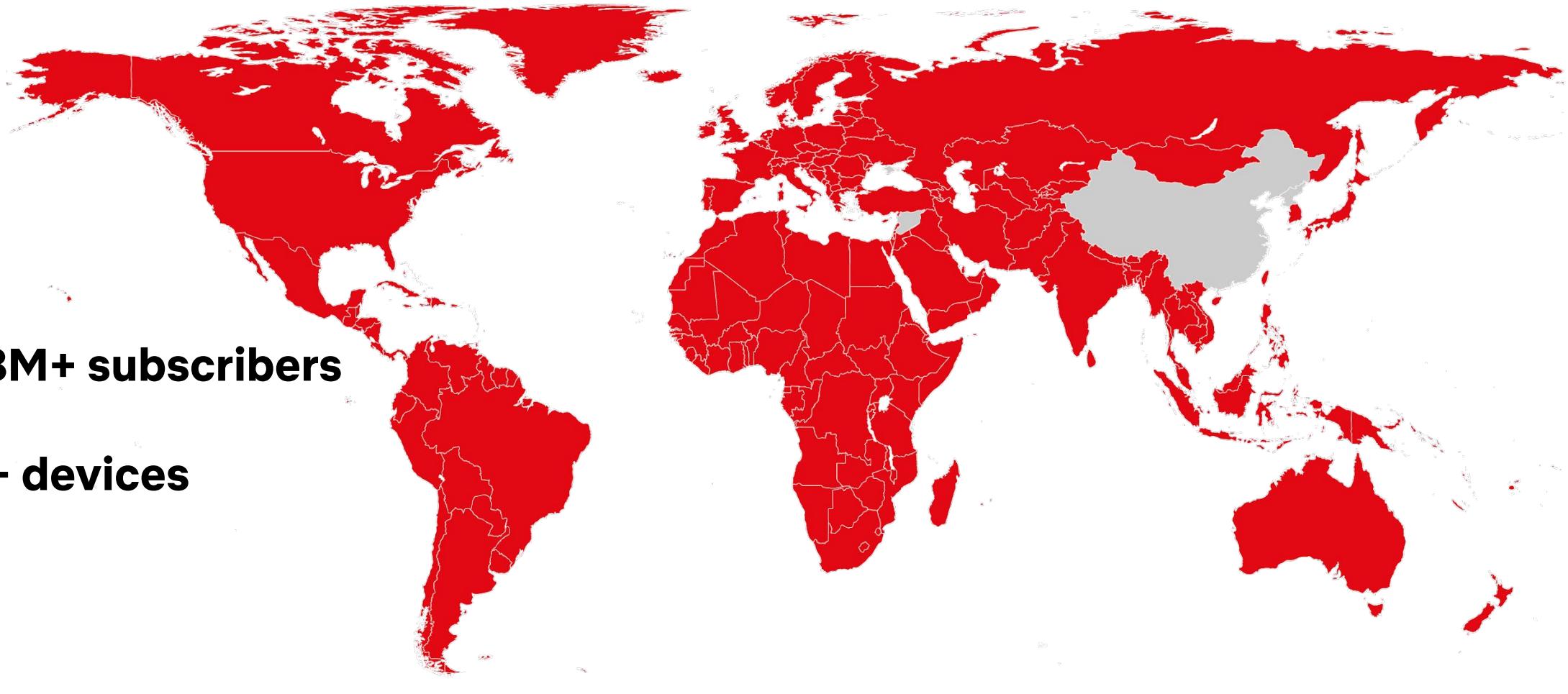
158M+ subscribers



# Netflix

**158M+ subscribers**

**1B+ devices**

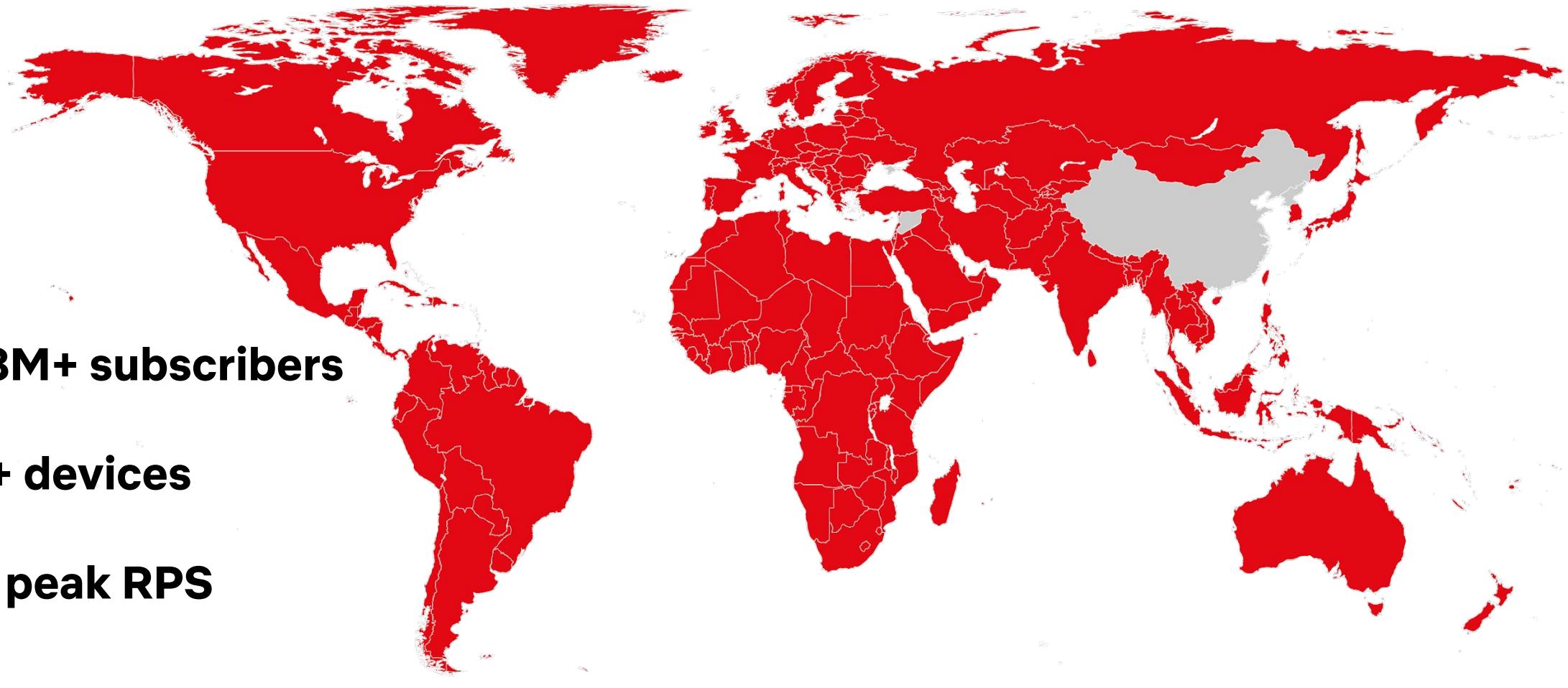


# Netflix

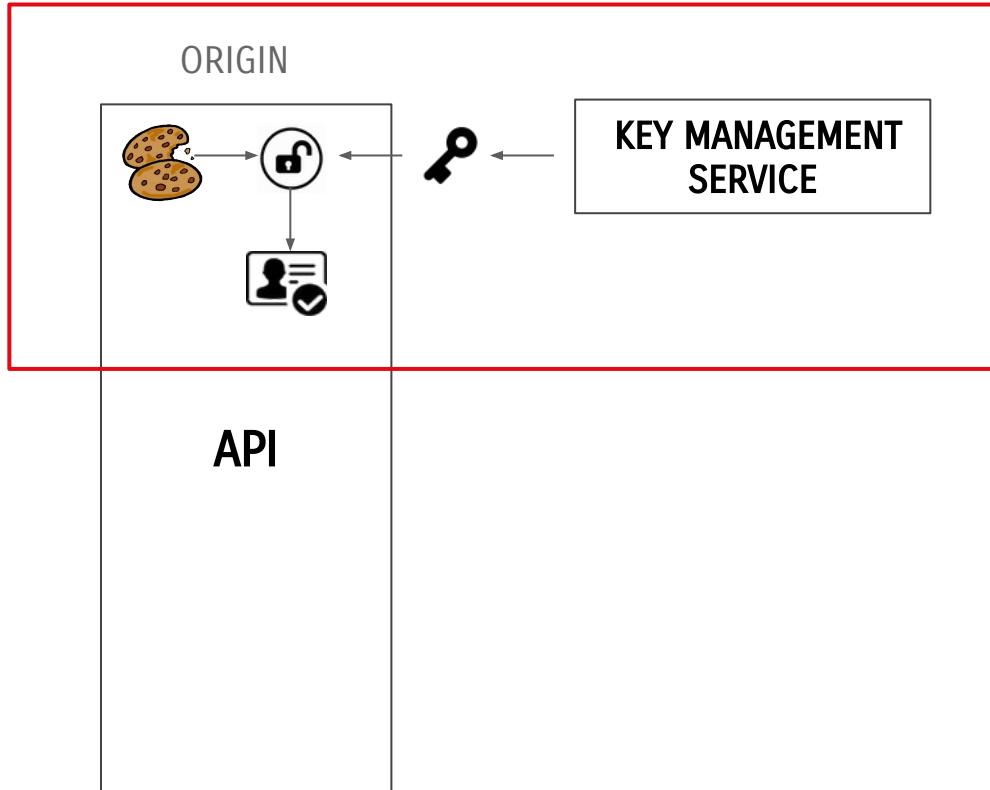
**158M+ subscribers**

**1B+ devices**

**2M peak RPS**



# Authenticate Request / Extract Identity



= 2 million Requests Per Second

# **More than one token type**



# Cookies



# Cookies



## - Signup

STEP 1 OF 3 <b>Choose a plan that's right for you.</b> Downgrade or upgrade at any time			
	Basic	Standard	Premium
Monthly price after free month ends on 2/14/19	\$8.99	\$12.99	\$15.99
HD available	✗	✓	✓
Ultra HD available	✗	✗	✓
Screens you can watch on at the same time	1	2	4
Watch on your laptop, TV, phone and tablet	✓	✓	✓
Unlimited movies and TV shows	✓	✓	✓
Cancel anytime	✓	✓	✓
First month free	✓	✓	✓

# Cookies



- Signup
- Login

Sign in  
Get ready to watch thousands of TV shows and movies.

NETFLIX

Enter your email address

1 2 3 4 5 6 7 8 9 0  
q w e r t y u i o p  
a s d f g h j k l -  
↑ z x c v b n m \_  
@gmail.com @yahoo.com @hotmail.com  
!#\$ @ .com  x

Email address  
Password (4-60 characters)

Back Next

Forgot Password?  Remember Email

Need help signing in? Visit <http://help.netflix.com>

STEP 1 OF 3			
Choose a plan that's right for you.			
Downgrade or upgrade at any time			
Basic	\$8.99	\$12.99	\$15.99
HD available	✗	✓	✓
Ultra HD available	✗	✗	✓
Screens you can watch on at the same time	1	2	4
Watch on your laptop, TV, phone and tablet	✓	✓	✓
Unlimited movies and TV shows	✓	✓	✓
Cancel anytime	✓	✓	✓
First month free	✓	✓	✓

# Cookies



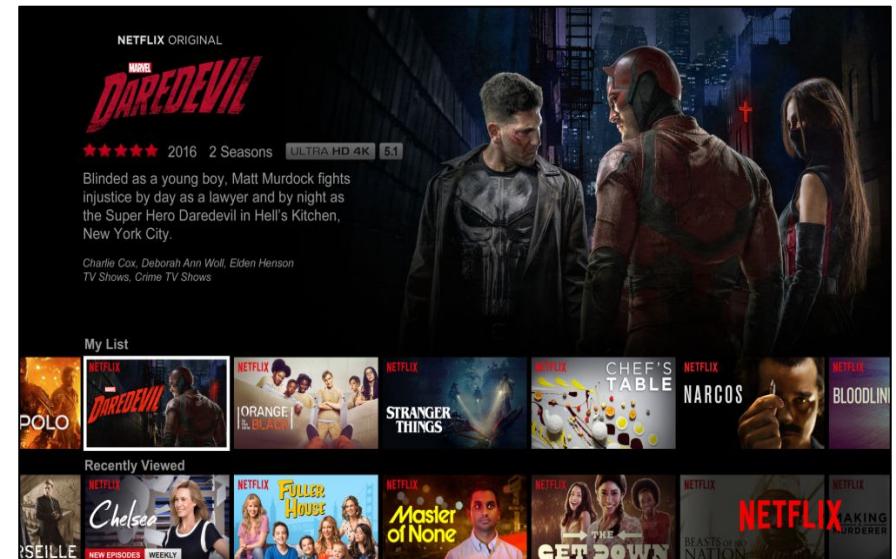
- Signup

The image shows the Netflix sign-in page. It has a dark header with the word "Sign in" and a "NETFLIX" logo. Below it, a message says "Get ready to watch thousands of TV shows and movies." There are two input fields: "Email address" and "Password (4-60 characters)". To the left of the email field is a numeric keypad and a dropdown menu showing "@gmail.com", "@yahoo.com", and "@hotmail.com". Below the password field is a "Forgot Password?" link and a "Remember Email" checkbox. At the bottom are "Back" and "Next" buttons. A note at the bottom right says "Need help signing in? Visit <http://help.netflix.com>".

- Login

STEP 1 OF 3 Choose a plan that's right for you. <small>Downgrade or upgrade at any time</small>			
	Basic	Standard	Premium
Monthly price after free month ends on 2/14/19	\$8.99	\$12.99	\$15.99
HD available	✗	✓	✓
Ultra HD available	✗	✗	✓
Screens you can watch on at the same time	1	2	4
Watch on your laptop, TV, phone and tablet	✓	✓	✓
Unlimited movies and TV shows	✓	✓	✓
Cancel anytime	✓	✓	✓
First month free	✓	✓	✓

- Discovery



# MSL Tokens



- Device authentication
- Encryption

## **Message Security Layer (MSL)**

<https://www.infoq.com/news/2014/11/netflix-msl/>

# MSL Tokens



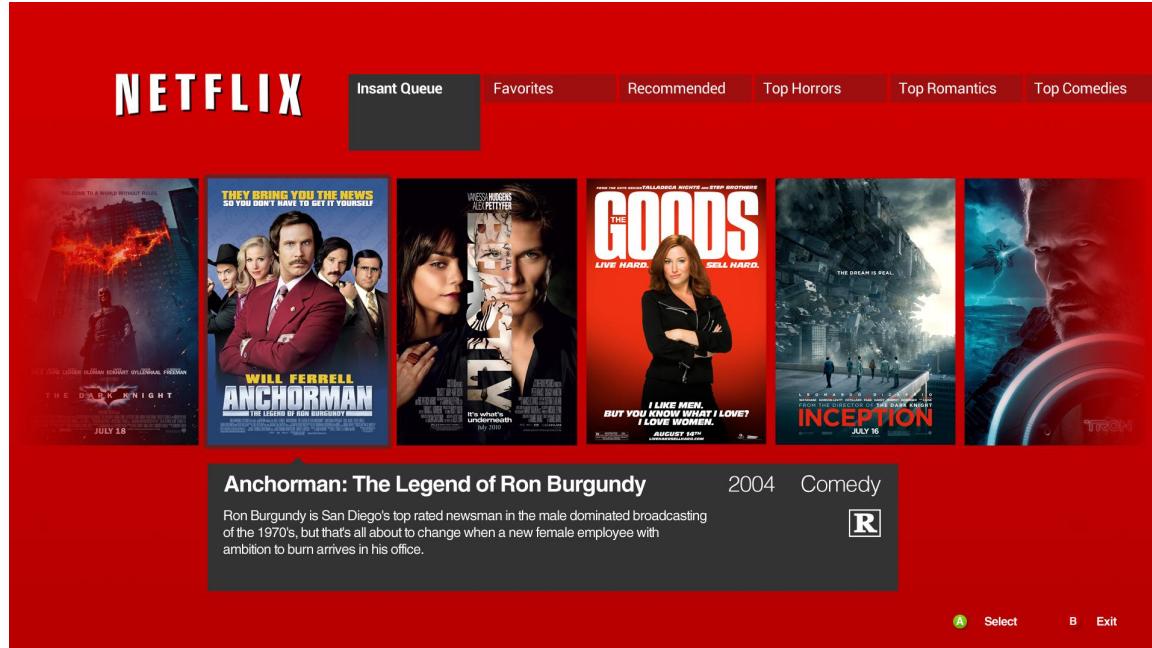
- License
- Playback



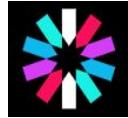
# CTicket



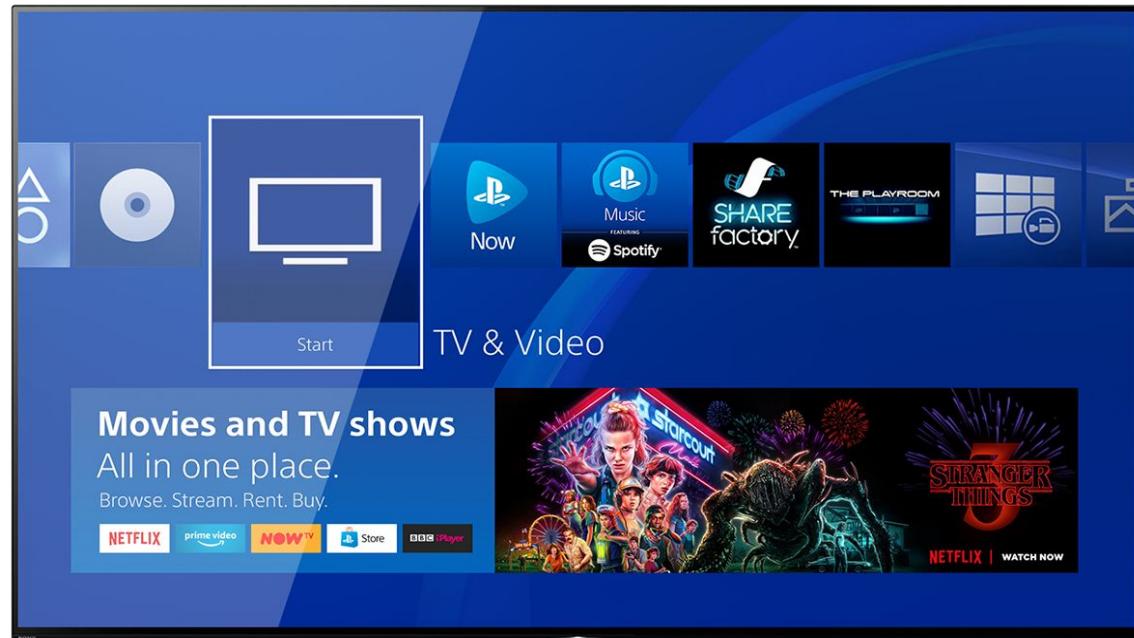
- Legacy devices



# Partner Tokens



- **JWS, JWE**
- **Non-member experiences**



# Cookies



- Signup
- Sign-in
- Discovery

STEP 4 OF 5 Choose a plan that's right for you. Downgrade or upgrade at any time.		
	Basic	Standard
Monthly price after free month ends on 2/14/19	\$8.99	\$12.99
HD available	✗	✓
Ultra HD available	✗	✗
Screens you can watch on at the same time	1	2
Watch on your laptop, TV, phone and tablet	✓	✓
Unlimited movies and TV shows	✓	✓
Cancel anytime	✓	✓
First month free	✓	✓

Sign in  
Get ready to watch thousands of TV shows and movies.

Email address  
Password (4-60 characters)

Back Next

Forgot Password? Remember Email



# MSL Tokens



- License
- Playback

# CTicket



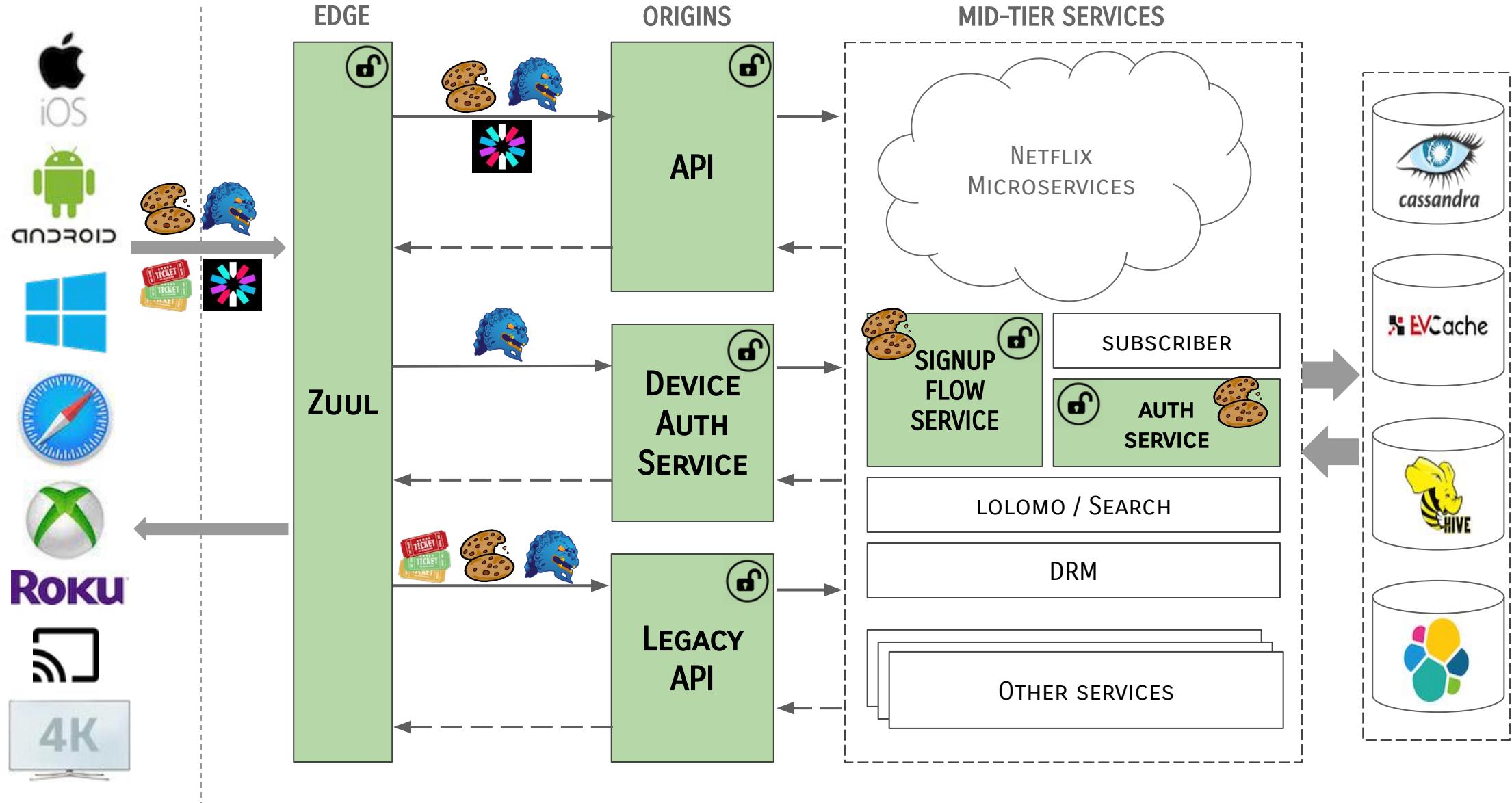
- Legacy devices

# Partner Tokens



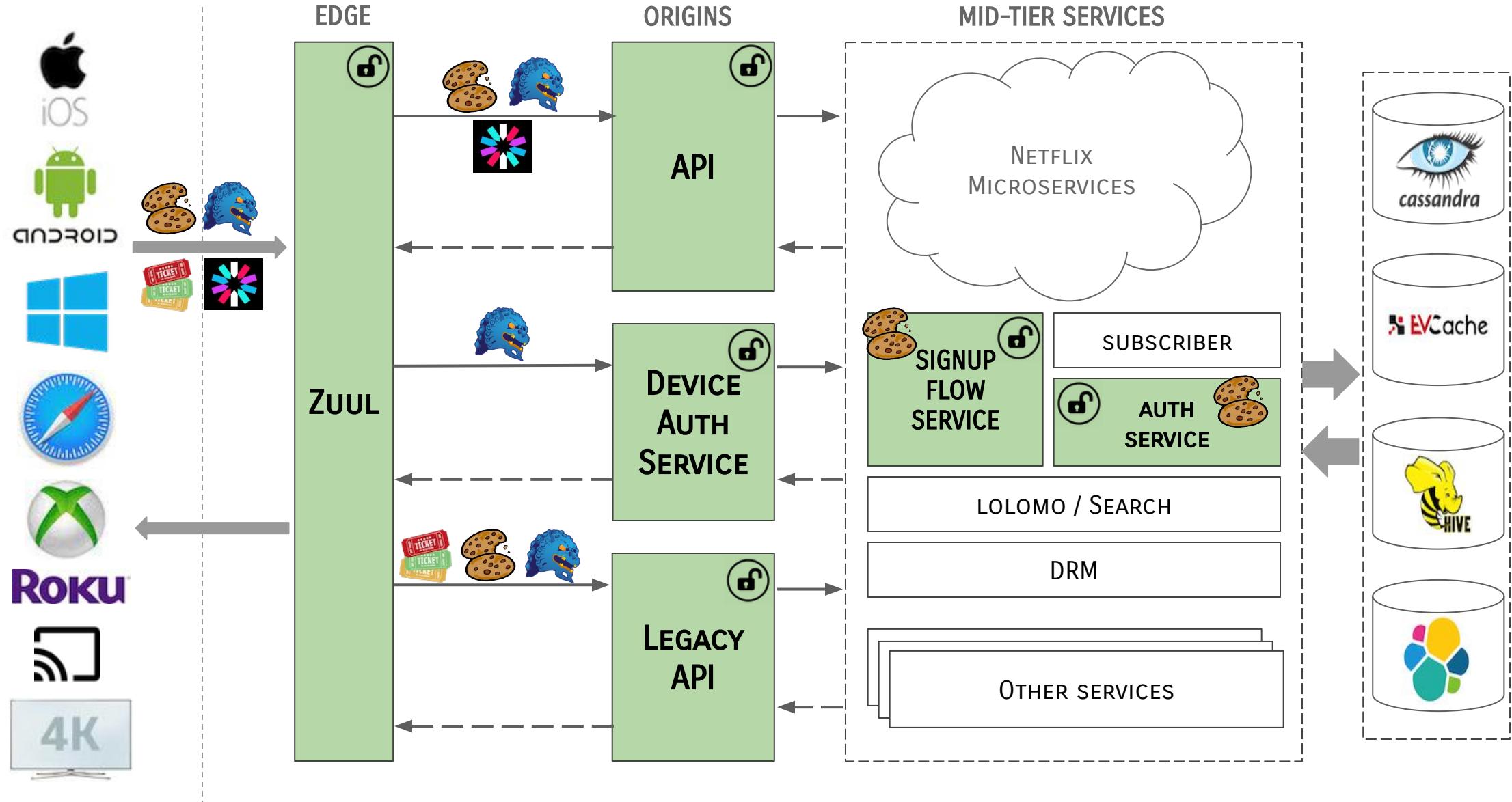
(JWS, JWE)

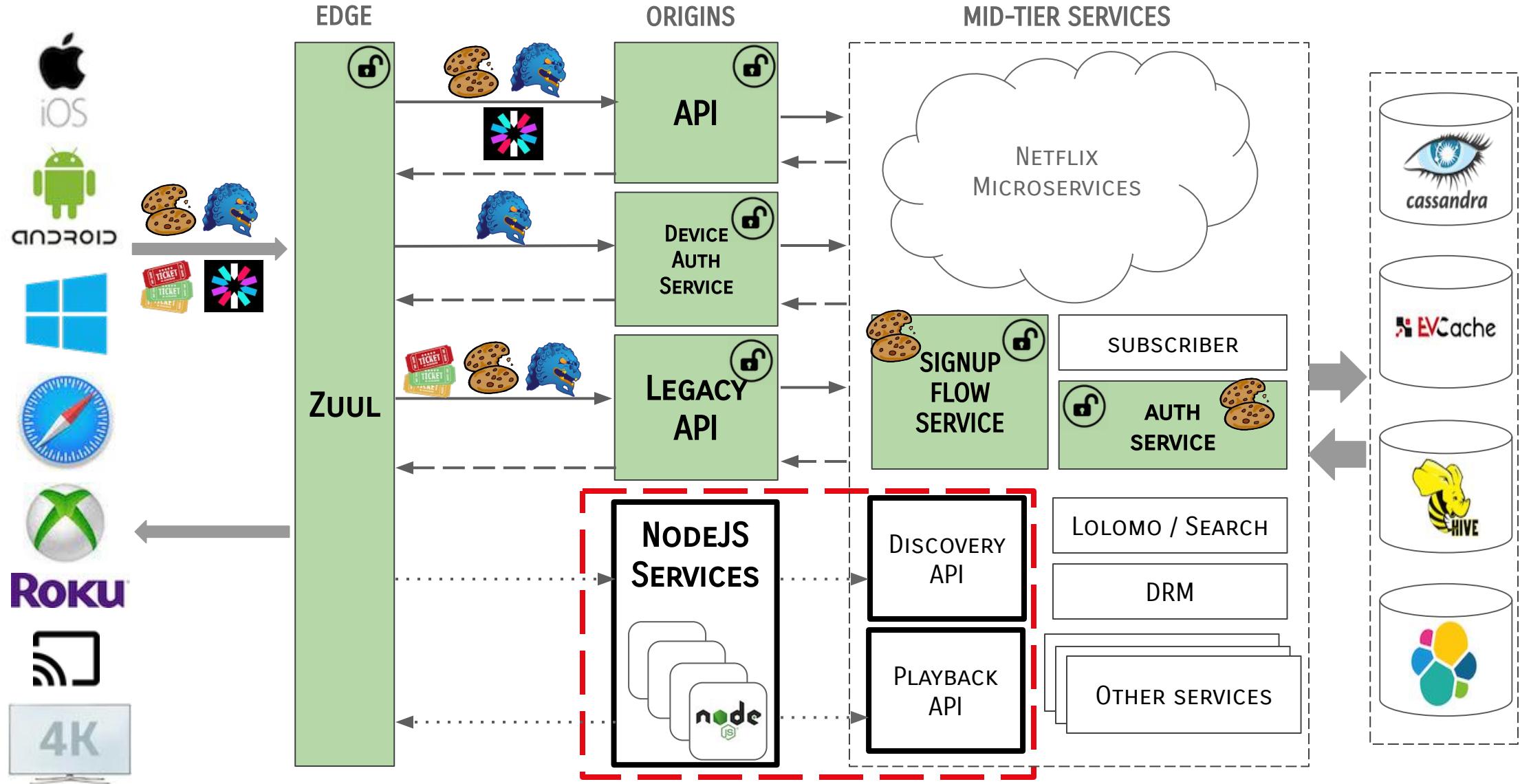
- Non-member experience



# Where we were

- **Multiple services consuming auth tokens**
- **Multiple types of auth tokens**
- **Massive scale**
- **Inefficient, insecure & complicated**



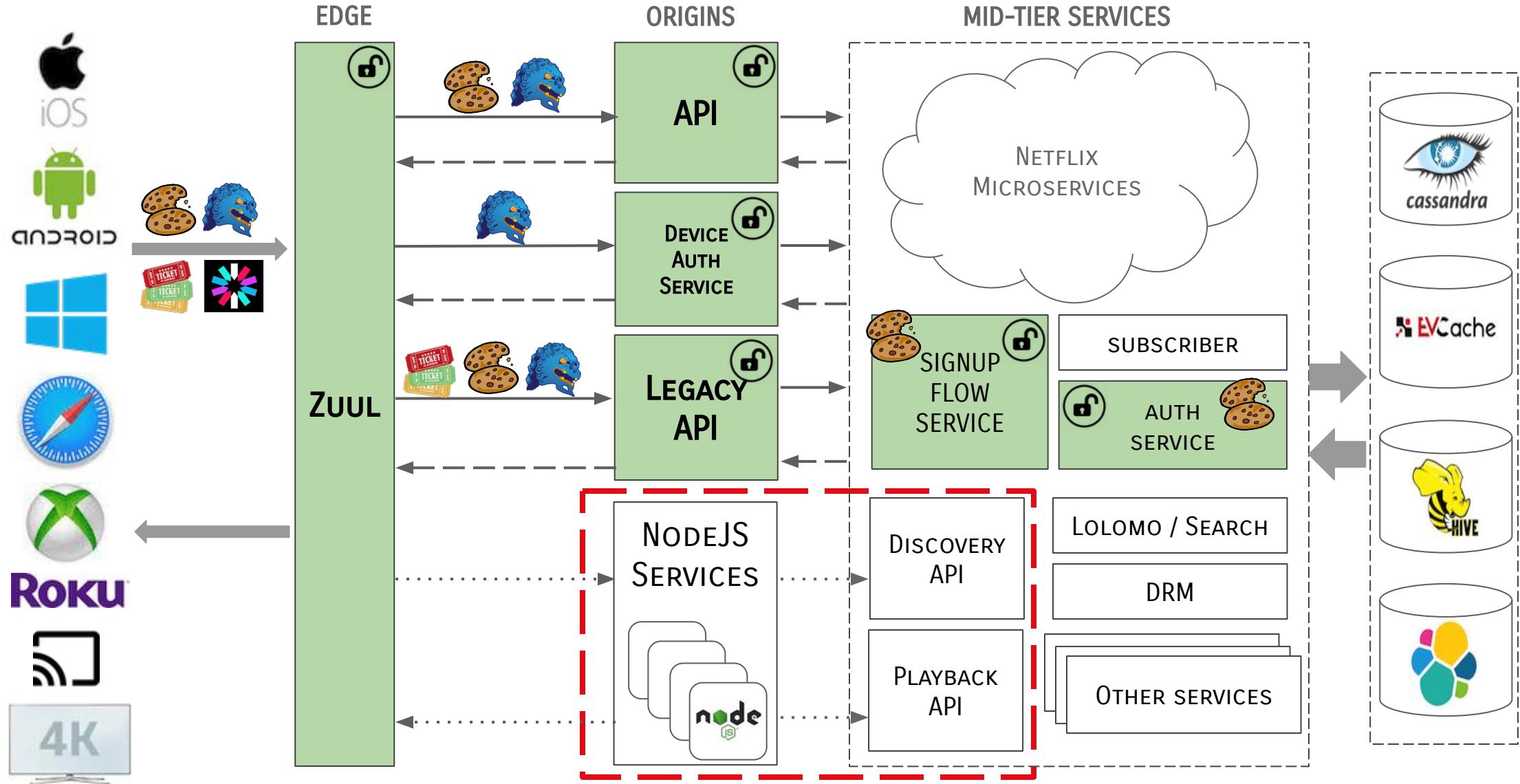


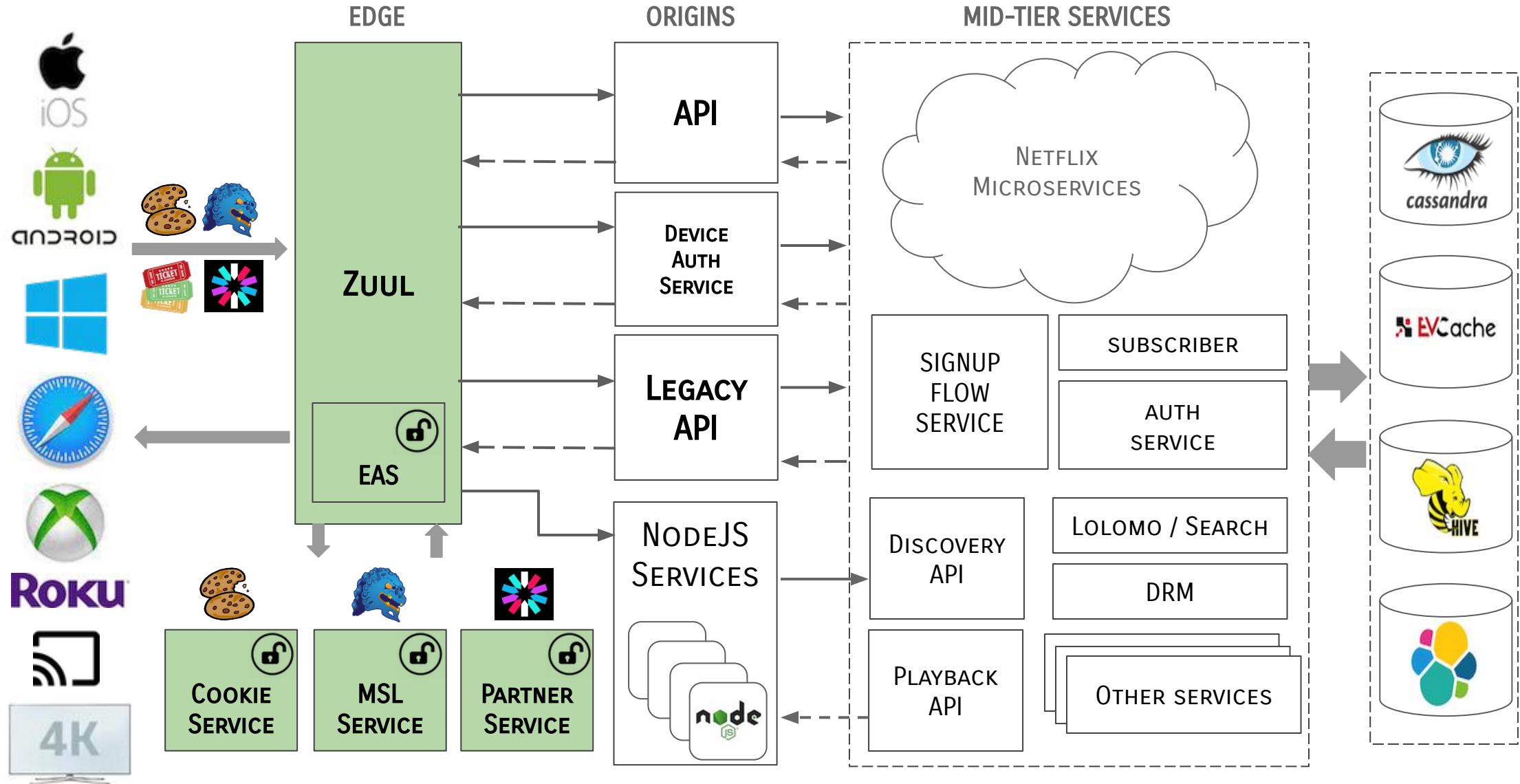


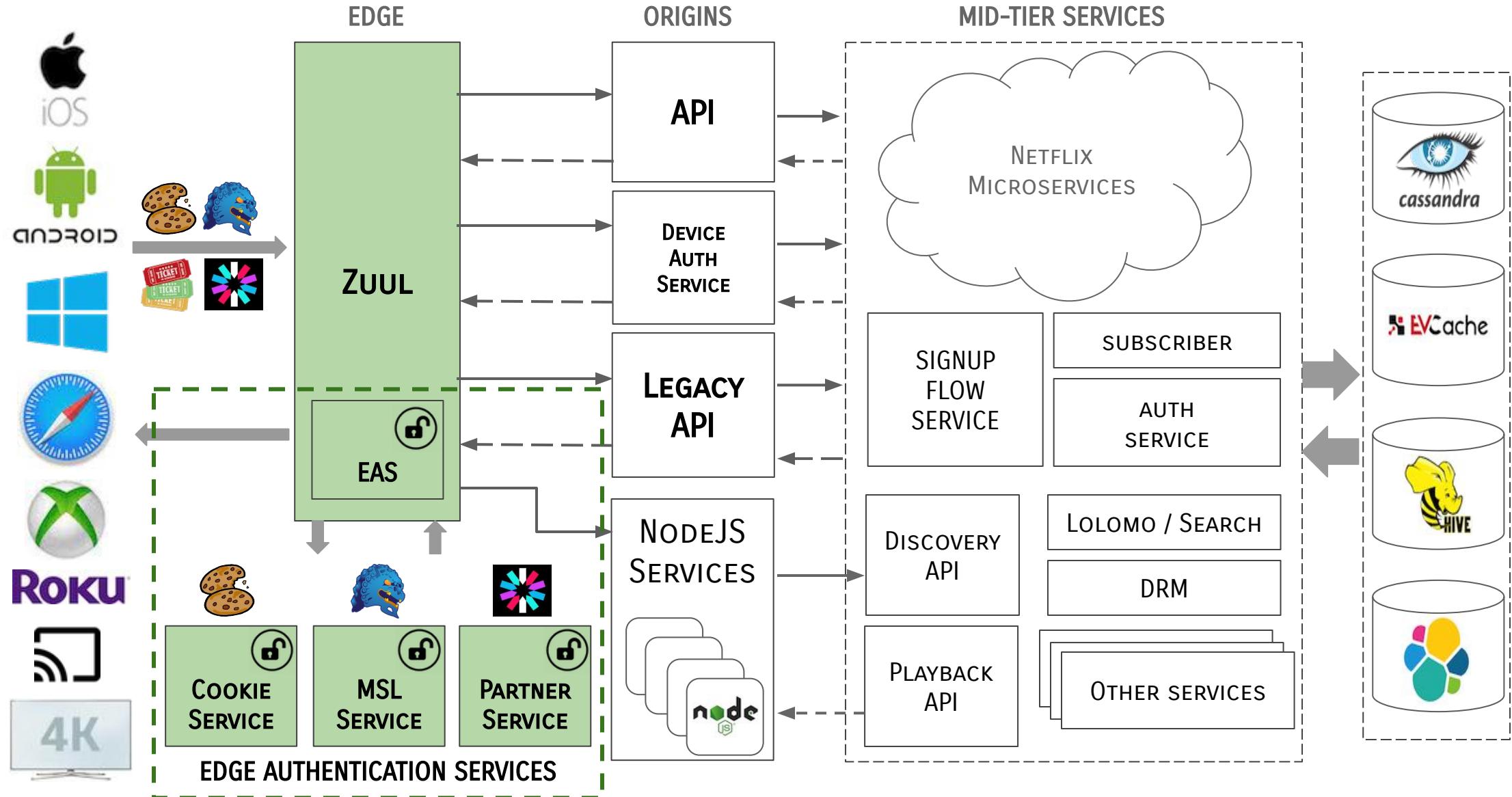
# What we did

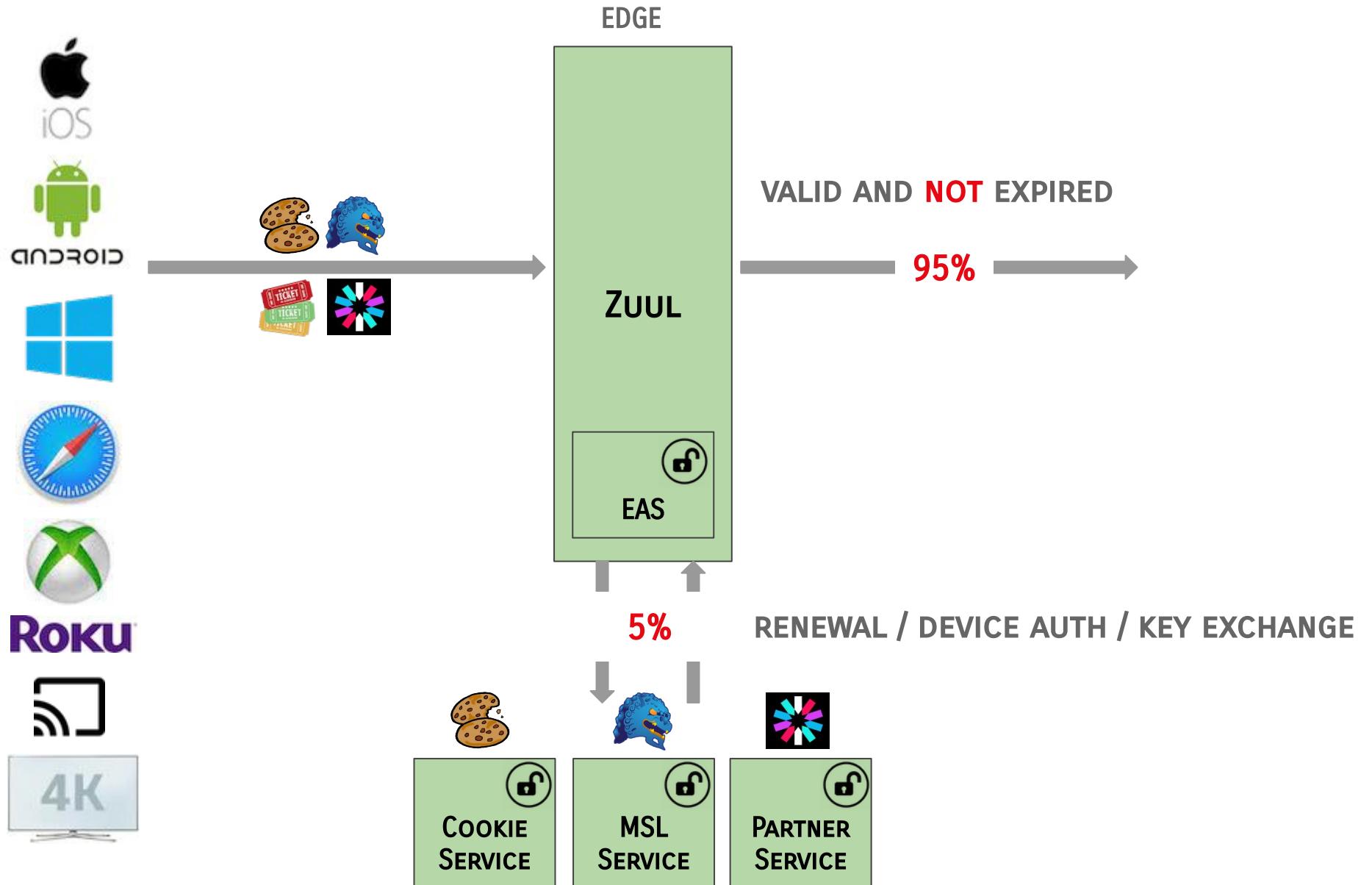
# Moved authentication to the edge

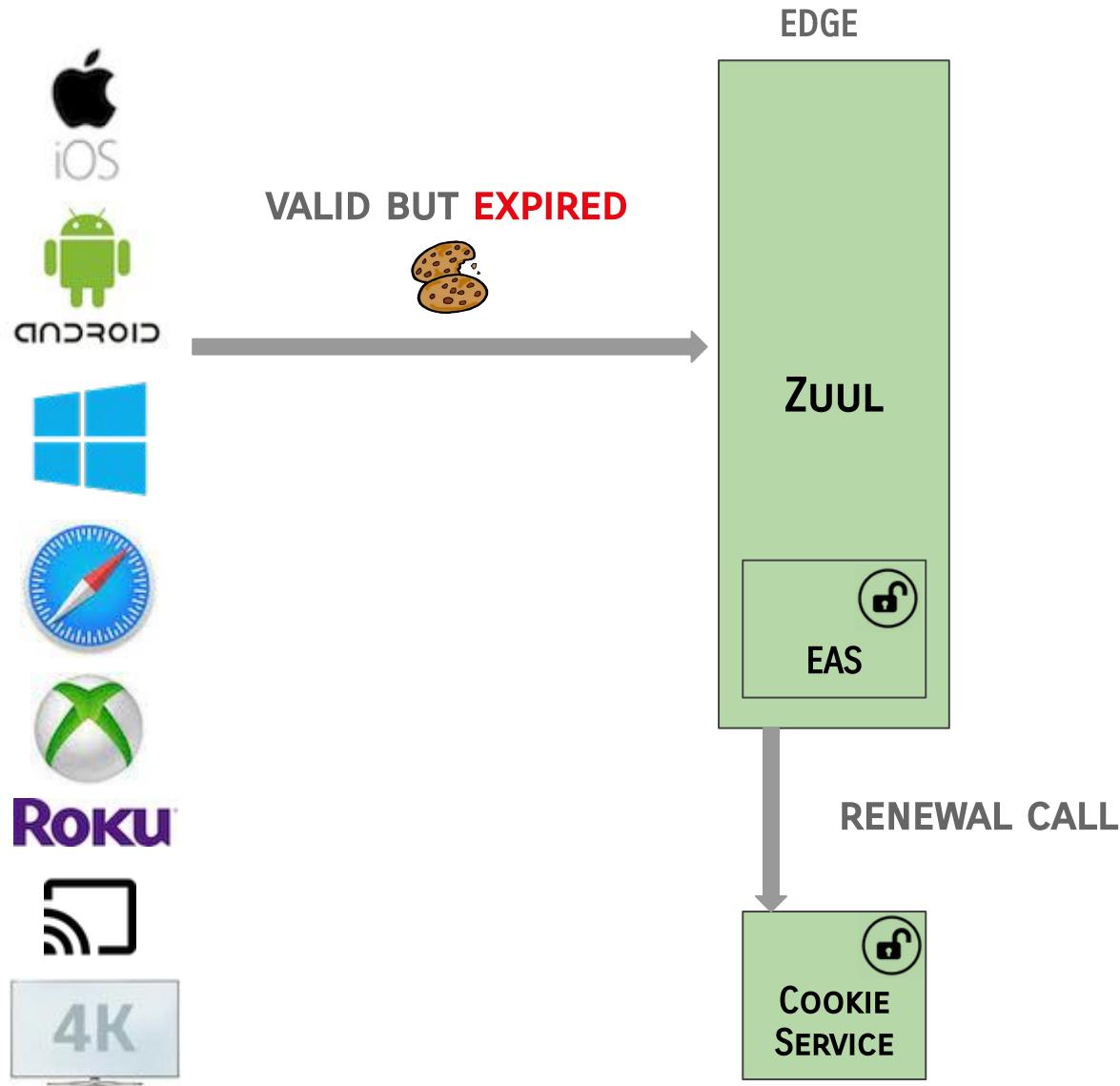


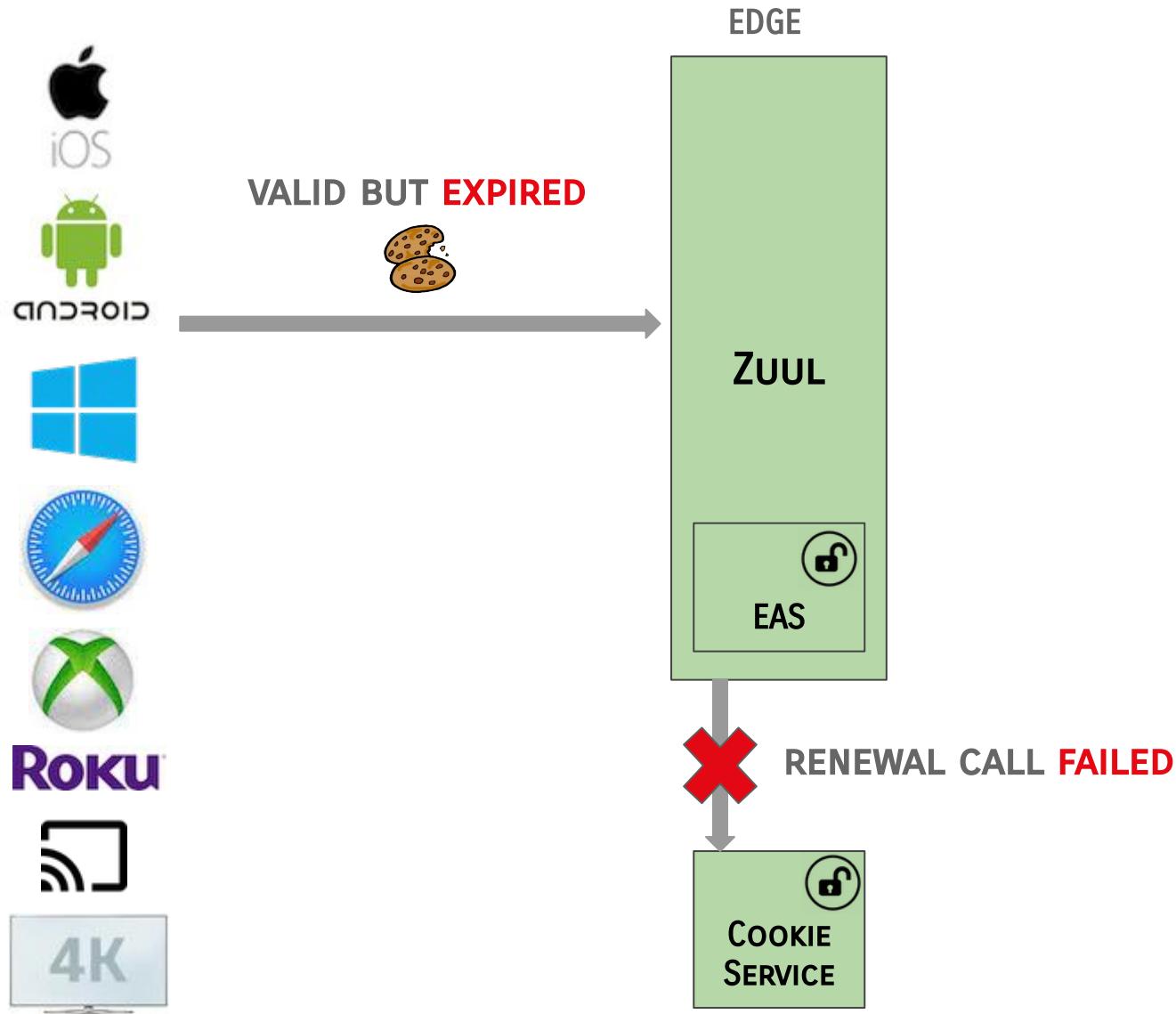


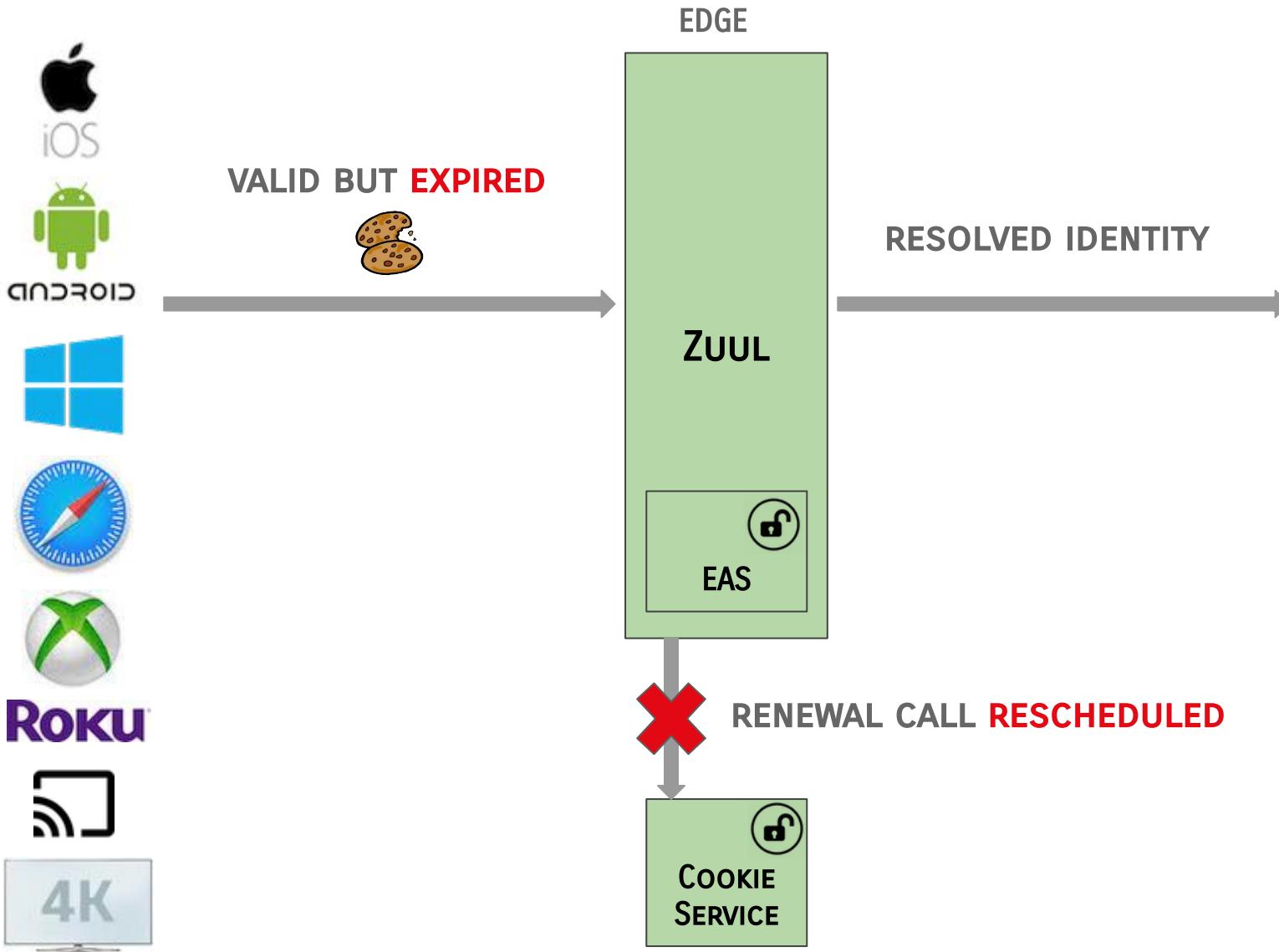


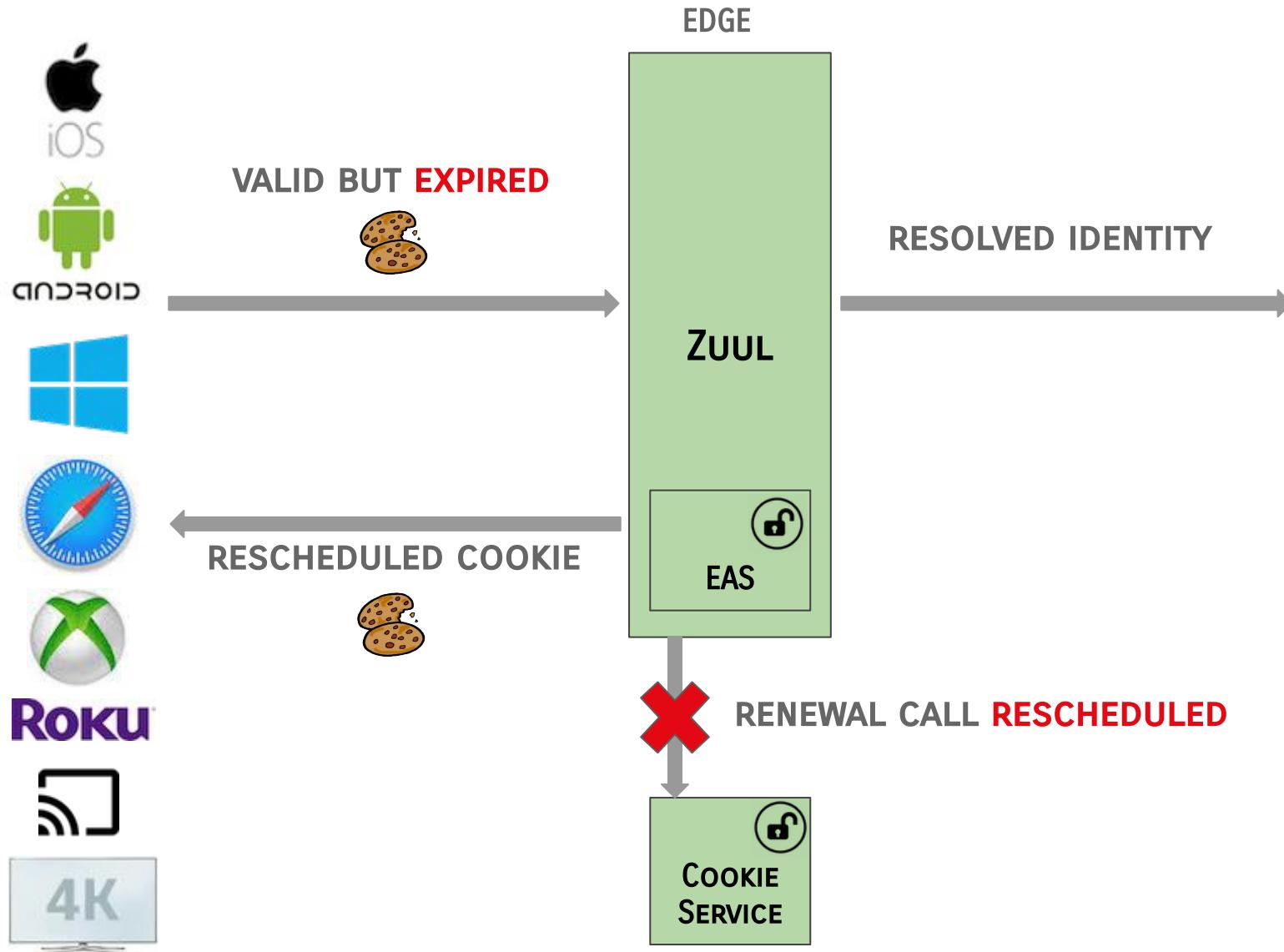


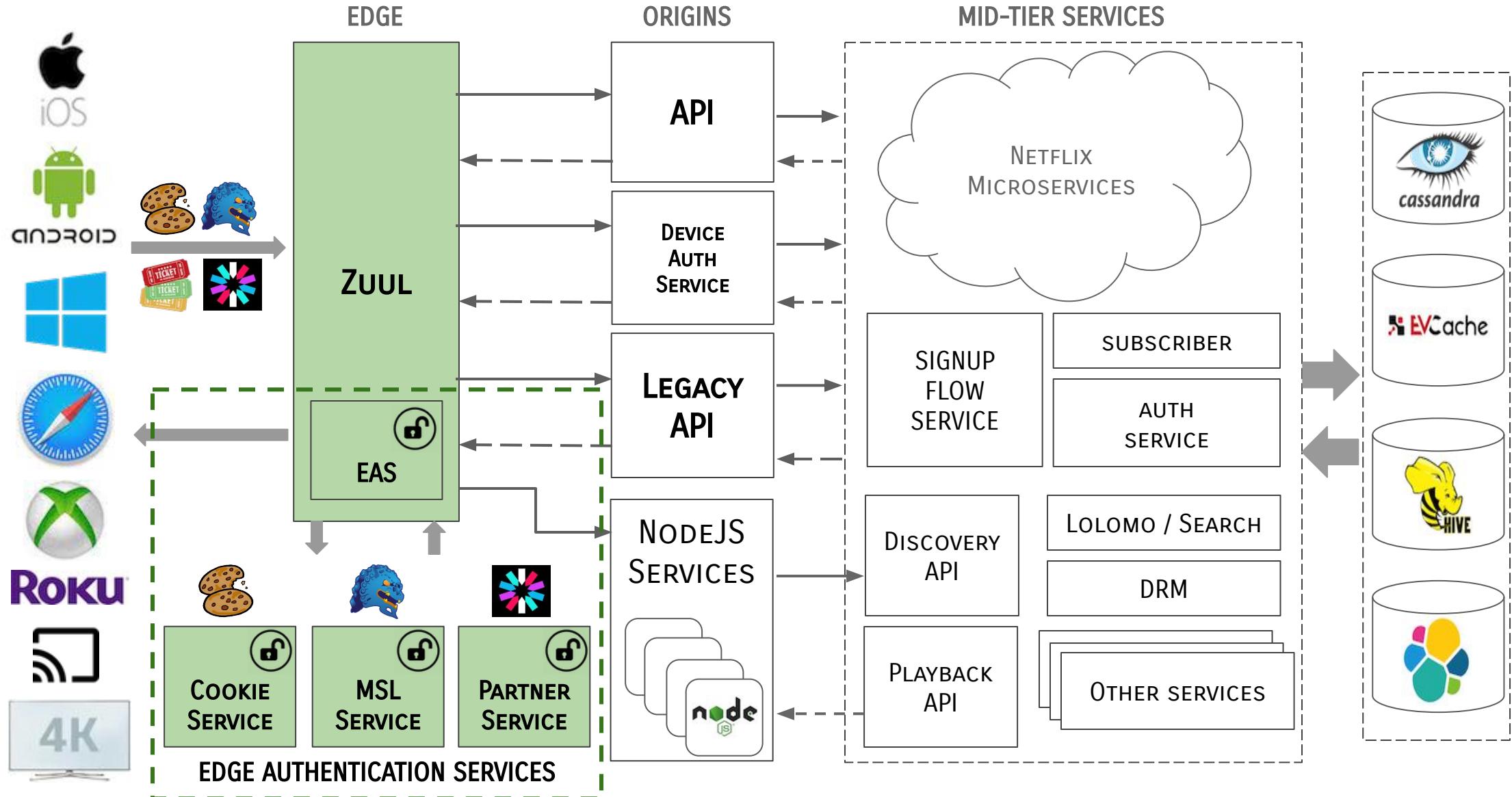


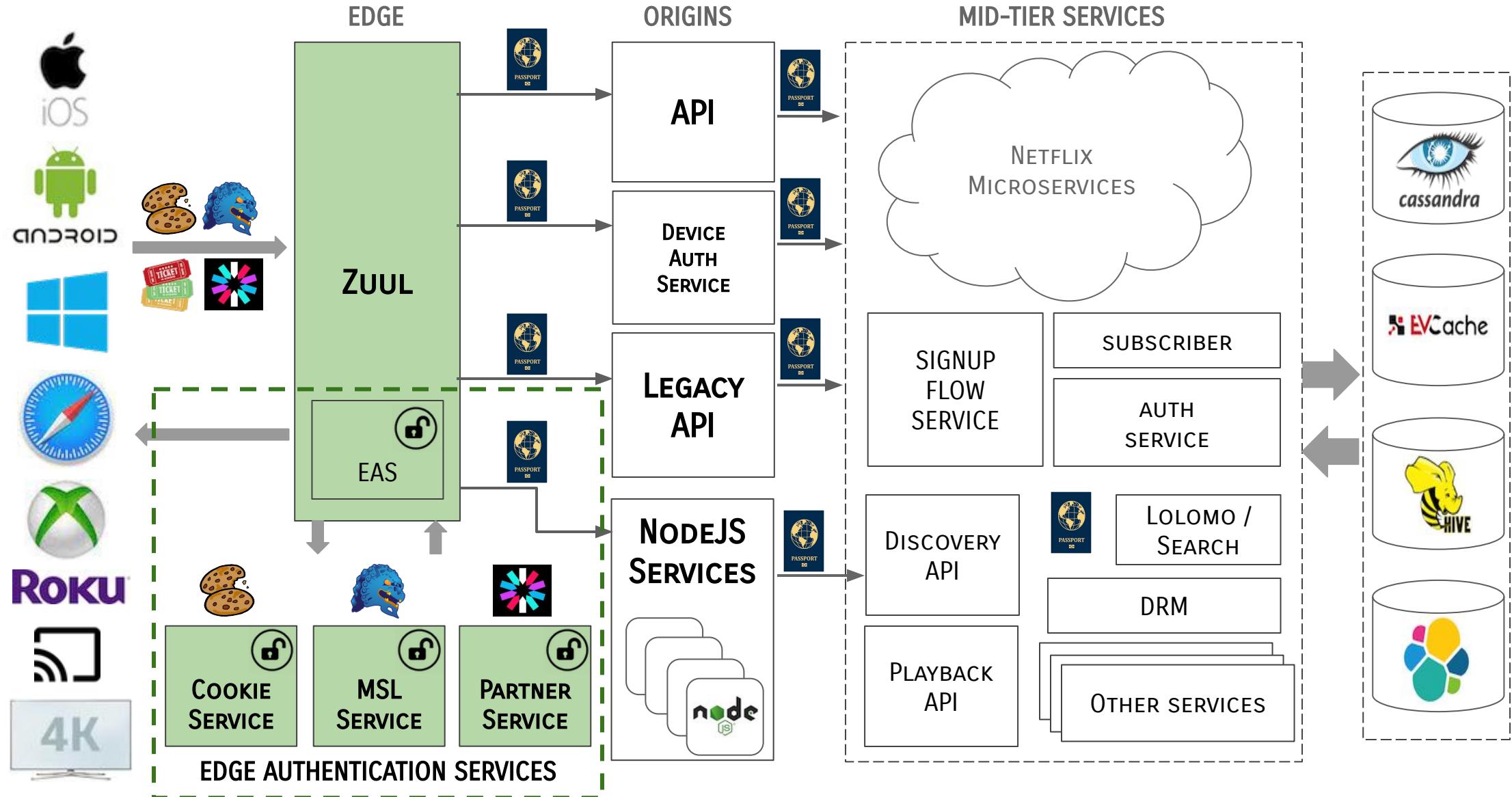












# Passport



# Passport



- Identity structure created at the edge **for each request**

# Passport



- Identity structure created at the edge **for each request**
- Contains **user & device identity**

# Passport



- Identity structure created at the edge **for each request**
- Contains **user & device identity**
- **Internal to Netflix ecosystem**

# Passport



- Identity structure created at the edge **for each request**
- Contains **user & device identity**
- Internal to Netflix ecosystem
- Integrity protected by HMAC

# Passport



- Identity structure created at the edge **for each request**
- Contains **user & device identity**
- Internal to Netflix ecosystem
- Integrity protected by HMAC
- Protobuf format

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}
```

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}  
  
message Header {  
    string originator = 1;  
}
```

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}
```

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}  
  
message UserInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
    { Int64Wrapper customer_id = 3;  
    Int64Wrapper account_owner_id = 4; }  
    repeated UserAction actions = ;  
}
```

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}  
  
message DeviceInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
    {  
        StringValue esn = 3;  
        Int32Value device_type = 4;  
    }  
    repeated DeviceAction actions = 5;  
}
```

# Passport



```
message UserInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

```
message DeviceInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

# Passport



```
message UserInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

```
message DeviceInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

```
enum Source {  
    COOKIE = 1;  
    MSL = 2;  
    PARTNER_TOKEN = 3;  
    CTICKET = 4;  
}
```

# Passport



```
message UserInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

```
message DeviceInfo {  
    Source source = 1;  
    AuthenticationLevel auth_level = 2;  
}
```

```
enum AuthenticationLevel {  
    LOW = 1;          // untrusted transport  
    HIGH = 2;         // secure tokens over TLS  
    HIGHEST = 3;     // MSL or user credentials  
}
```

# Passport



```
message Passport {  
    Header header = 1;  
    UserInfo user_info = 2;  
    DeviceInfo device_info = 3;  
    Integrity user_integrity = 4;  
    Integrity device_integrity = 5;  
}
```

```
message Integrity {  
    string key_name = 1;  
    bytes hmac = 2;  
}
```

# Passport Introspector



- Wrapper over passport binary data

# Passport Introspector



- Wrapper over passport binary data

```
public interface PassportIntrospector {  
    Long getCustomerId();  
    Long getAccountOwnerId();  
    String getEsn();  
    String getPassportAsString();  
    ...  
}
```

# Passport Introspector



- Wrapper over passport binary data
- Consumers create **passportIntrospector** from binary passport data

```
public interface PassportIntrospector {  
    Long getCustomerId();  
    Long getAccountOwnerId();  
    String getEsn();  
    String getPassportAsString();  
    ...  
}  
  
factory.createIntrospector(passport);
```

# Tooling

Self-service tool for  
*teams* to decrypt  
*passport*

TEST PROD

Decrypt Passport

```
CrUfCgUxLjAuMBKrHwoKCghhcGlwcm94eRJCCAESFBBU1NQT1JUX01BQ19LRVkaLAEBA_cAAQEgEg6mzMut89pl6kgehilpPh22504eQzo4jfhYBlwd9yAn7dv1GjkIAxDw56So3y0iJgokU0xXMsItRIU3NFRYOEFRUDRRMzFLSFBNWUcyOVi1VzU4SksSkglIDEADSGaIQggBEhBQQVNTUE9SVF9NQUNfSOVZGiwbAQP3AAEBIBQuWp1Hu1Q51JfKQuRvh2fvBUIBUS2QhIDBXHXNGIfSWy_o6yrZHQgDEMPopKjfLSIKCMq998Cdu62AAyocChpLNEI0U1hQVVhGQ1hGQVJPRVJPVzYzRU1BVTIKCMq998Cdu62AAzocChpLNEI0U1hQVVhGQ1hGQVJmwKCwgDGgcI9uekqN8tGgAiWAoKCMq998Cdu62AAxIKCMq998Cdu62AAxoQUEFTU1BPUIRfUFDX0tFWSIsAQED9wABASDSKMWBPop3rtxZaLN5Fnj02Eo57BtS8d0jNqS-w==
```

Decrypt

User Info

customerId	216372729
acctOwnerId	216372729
customerGuid	K4B4SXPUXFCXFAROE
acctOwnerGuid	K4B4SXPUXFCXFAROE
source	MSL
authenticationLevel	HIGHEST
created	10/22/2019 12:54:44 PDT

Device Info

esn	SLW32-FU74TX8AQP4Q31KHPPYC
deviceTypeId	12
activationDeferred	false
source	MSL
authenticationLevel	HIGHEST
created	10/22/2019 12:54:44 PDT

# Passport Actions

```
message UserInfo {  
    repeated UserAction actions = 6;  
    ...  
}  
  
message DeviceInfo {  
    repeated DeviceAction actions = 5;  
    ...  
}
```



# Passport Actions

```
message UserInfo {  
    repeated UserAction actions = 6;  
    ...  
}
```

```
message DeviceInfo {  
    repeated DeviceAction actions = 5;  
    ...  
}
```

- **Explicit signal** sent by the downstream services, when an **update** to user or device identity has been performed

# Passport Actions

```
message UserInfo {  
    repeated UserAction actions = 6;  
    ...  
}
```

```
message DeviceInfo {  
    repeated DeviceAction actions = 5;  
    ...  
}
```

- **Explicit signal** sent by the downstream services, when an **update** to user or device identity has been performed
- This "signal" is used by EAS to either **create** or **update** the corresponding type of **token**

# Passport Action

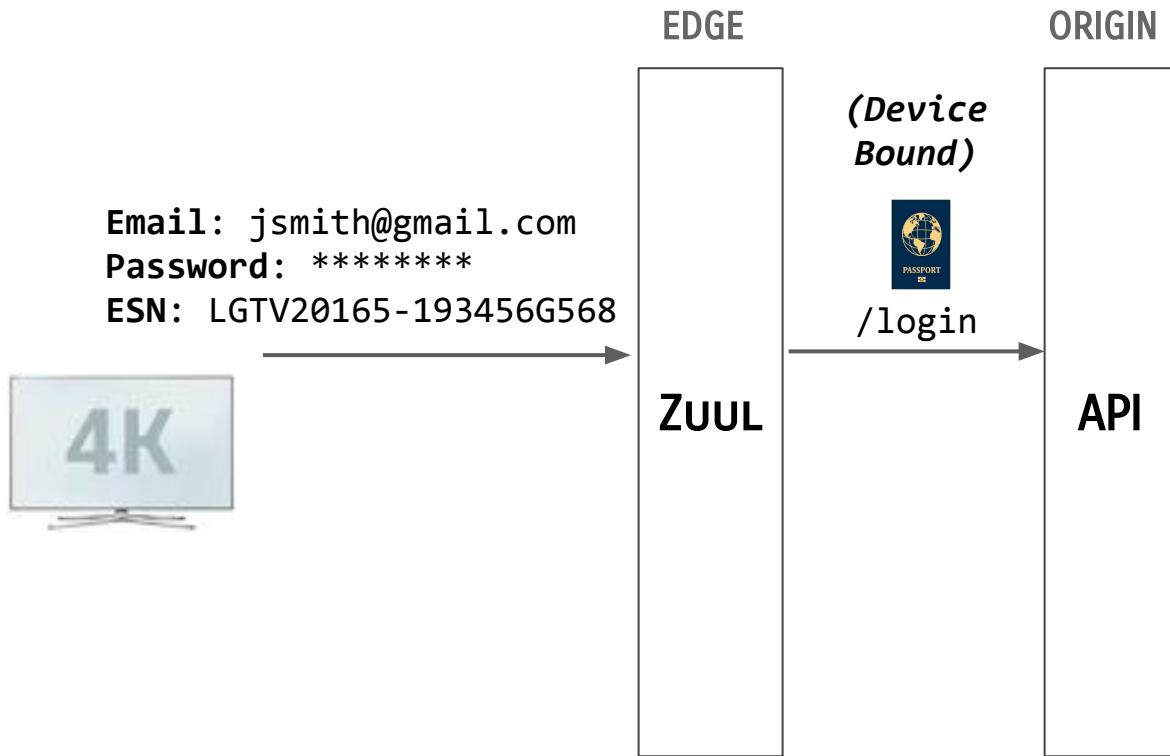


# Passport Action: User Login

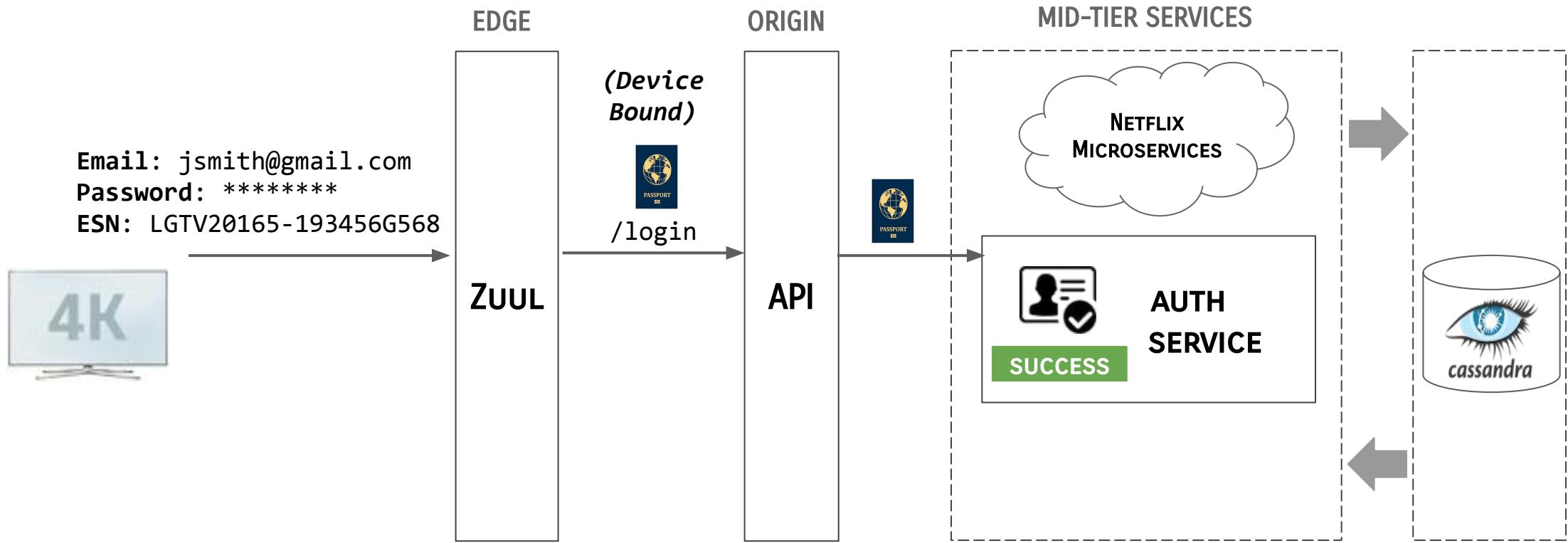
# Passport Action: User Login



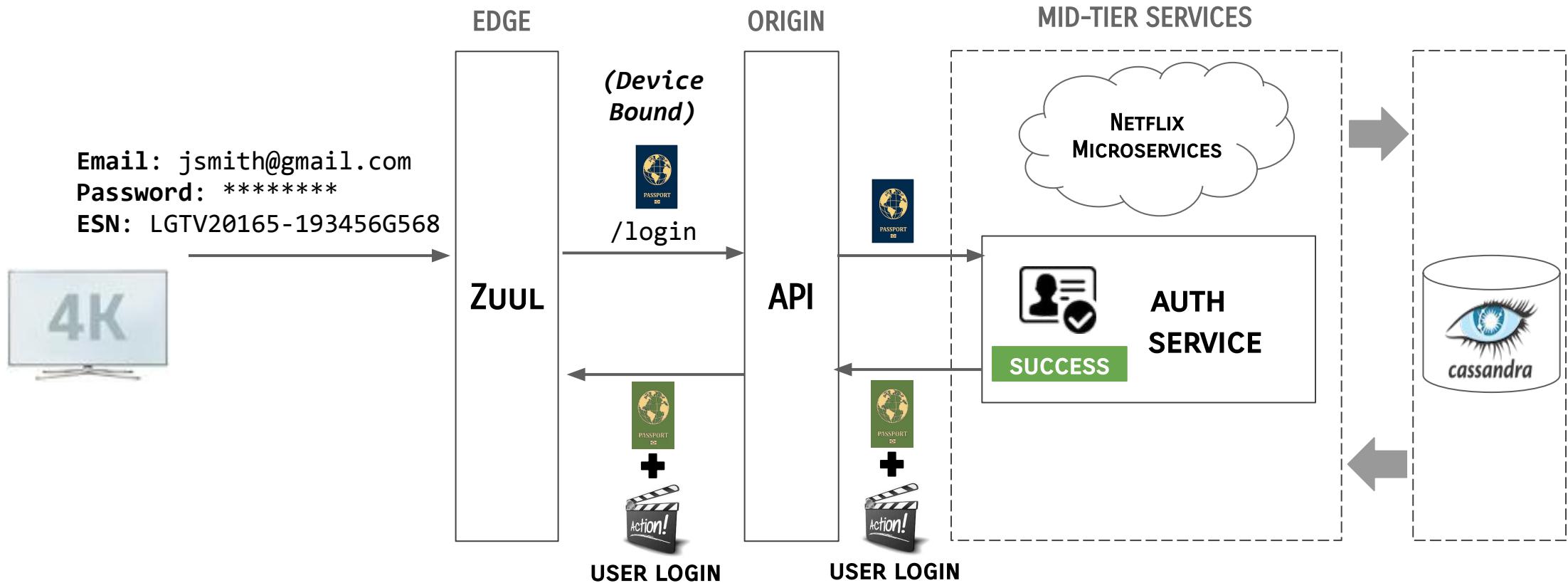
# Passport Action: User Login



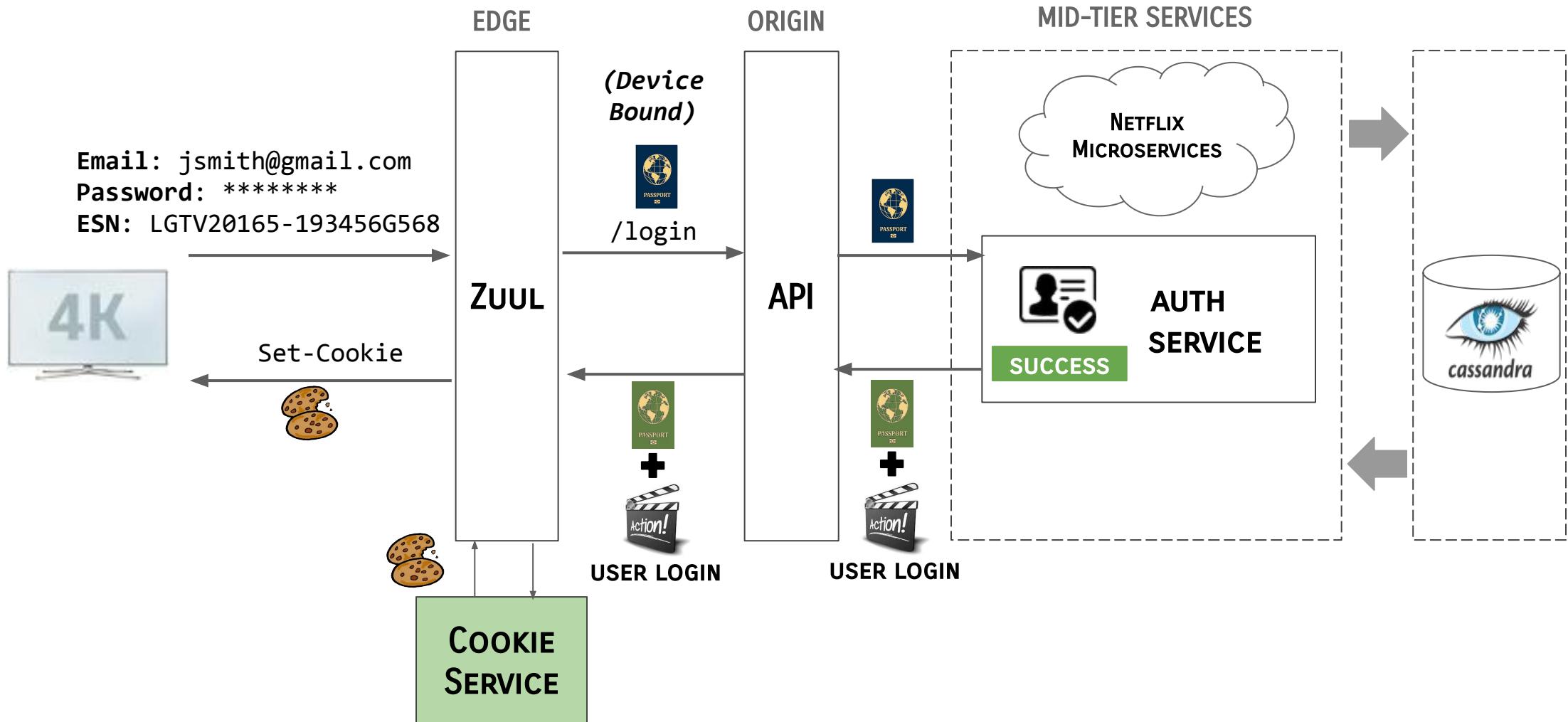
# Passport Action: User Login



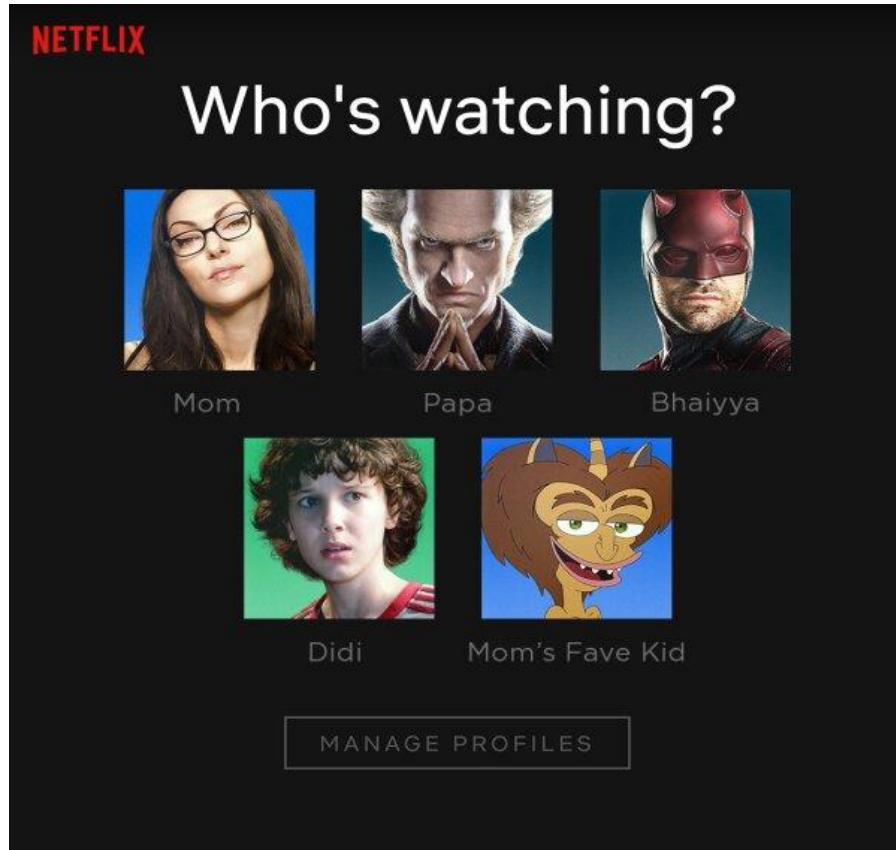
# Passport Action: User Login



# Passport Action: User Login

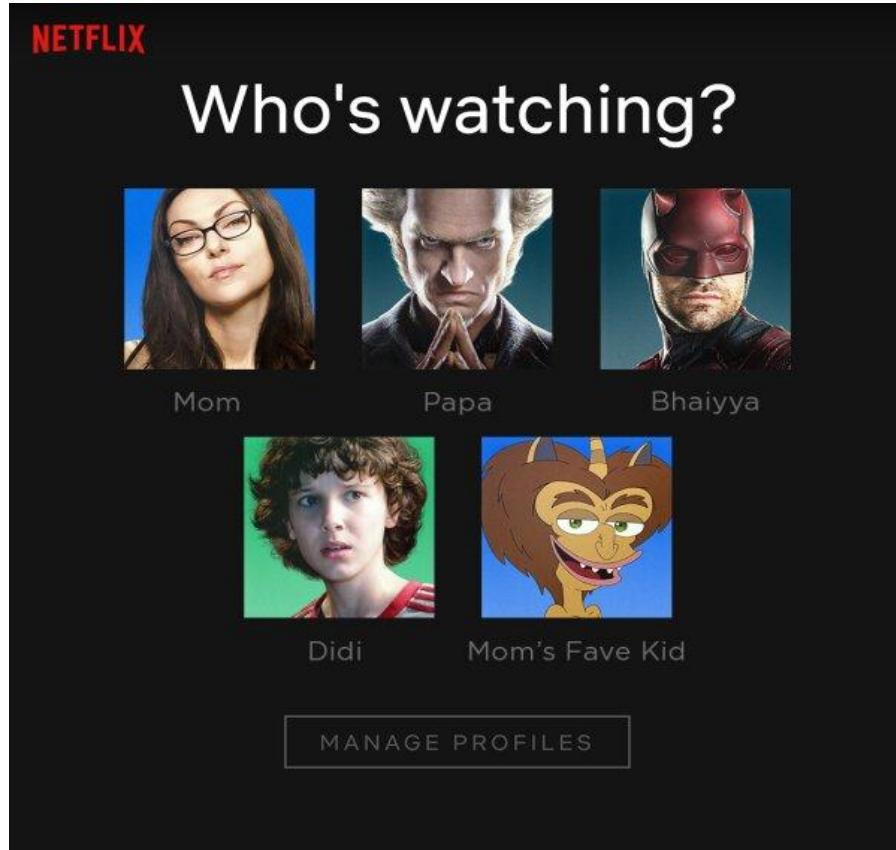


# Passport Action: Profile Switch



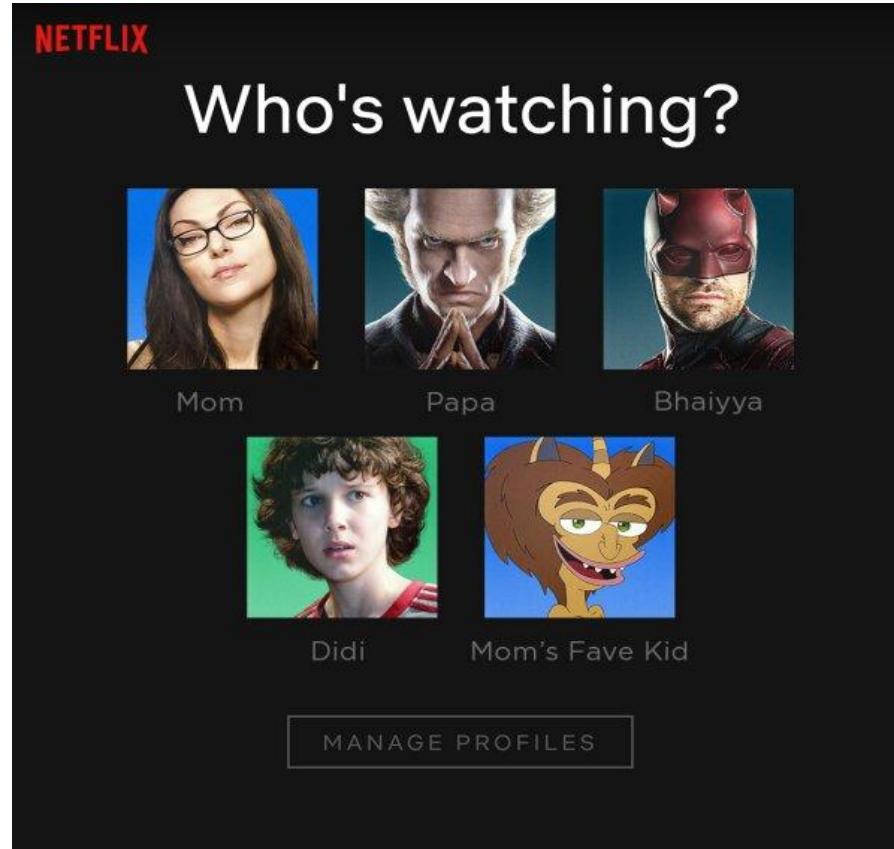
# Passport Action: Profile Switch

- Each profile has its own identity



# Passport Action: Profile Switch

- Each profile has its own identity
- Switched profile tokens sent back to the device





# Passport Actions

Separation Of  
Concerns



# Increased Visibility

# What we did

- Moved authentication to the edge
- Streamlined the identity resolution and mutation path
- Making consumption of user & device identity
- Efficient, secure & simple

# Wins

# Token Agnostic Identity

Downstream systems **don't have to worry about authentication concerns**

# Simplified Authorization

Downstream services use  
**authentication level** for  
authorization decisions

# Simplified Authorization

**Before:**

```
long customerId = 2123125603L;  
String ESN = "NFXBOX-235F...";
```

# Extensible Identity Model

**New attributes about user or device can be added**

# Local cache for up to date subscriber data

```
message UserInfo {  
    BytesValue subscriber_account  
    ...  
}
```

Placeholder for **local cache** of  
subscriber data

# Offloaded & Fine Tuned

Offloaded token processing which resulted into significant gains for

- CPU
- Request Latency
- GC
- Cluster Footprint

# Offloaded & Fine Tuned

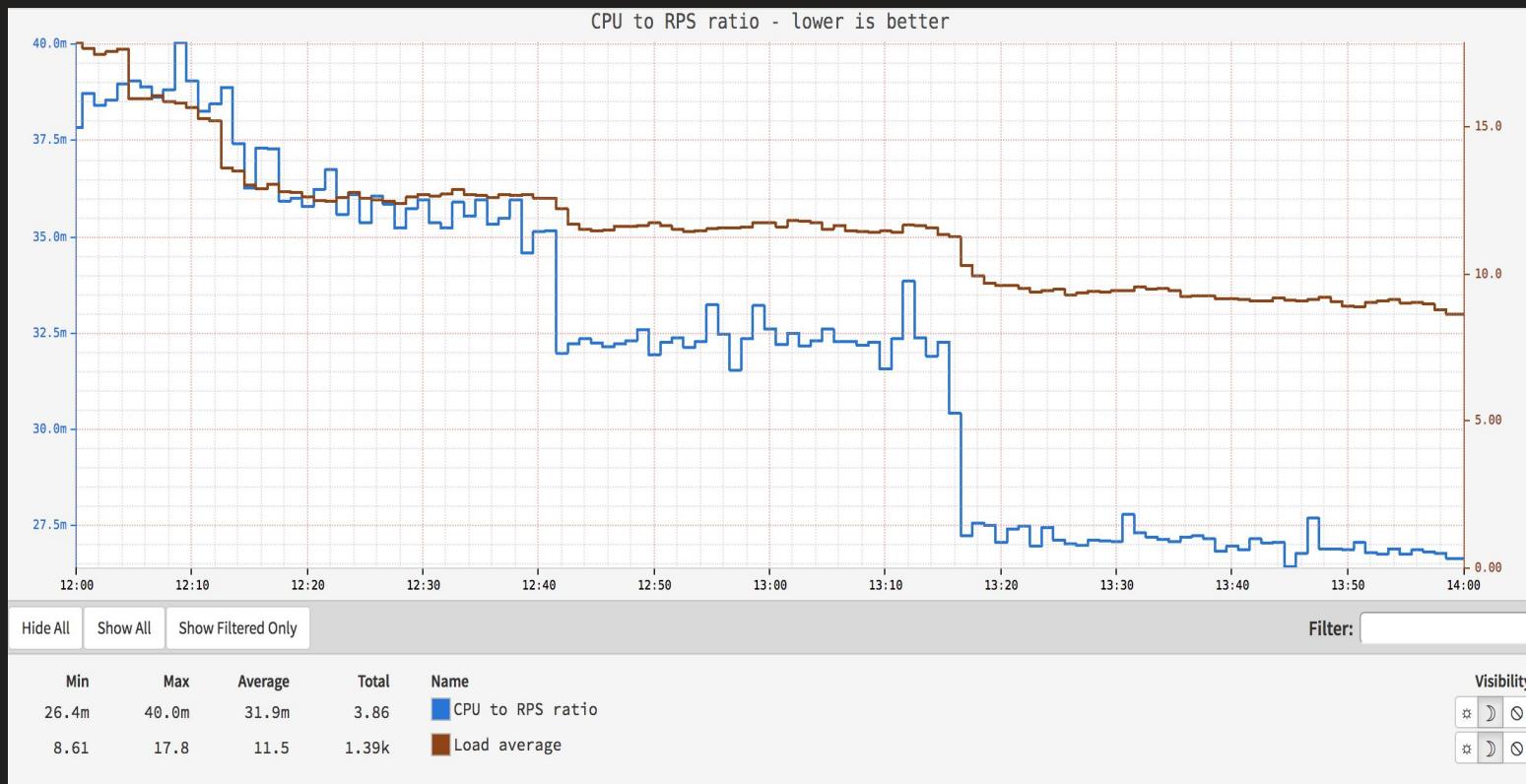
Offloaded token processing which resulted into significant gains for

- CPU
- Request Latency
- GC
- Cluster Footprint

We were able to fine tune EAS systems based on the token processing profile

# Offloaded & Fine Tuned

- 30% reduction in CPU cost per request
- 40% reduction in load average



## CPU to RPS ratio for API instance

# Offloaded & Fine Tuned

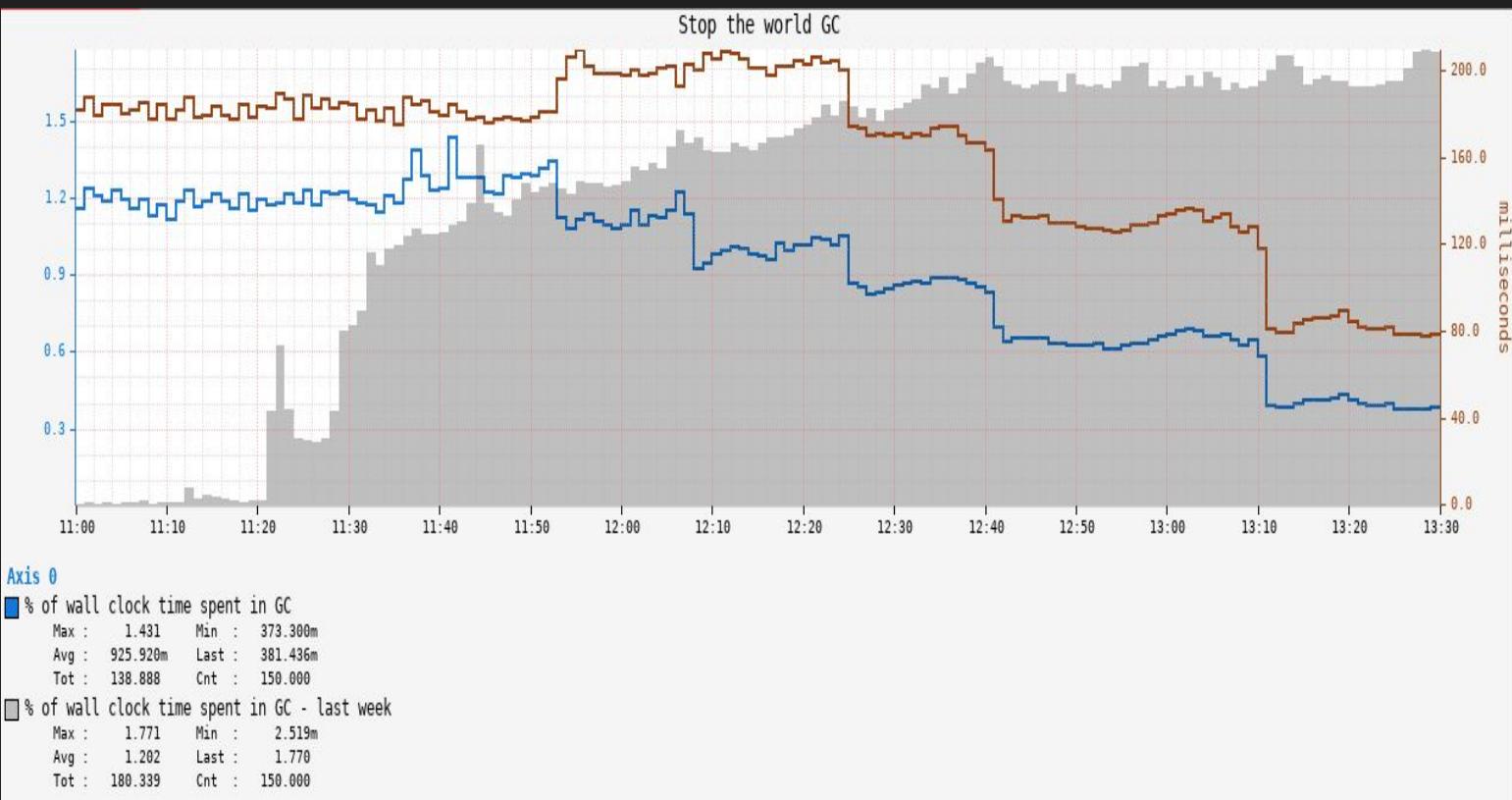
- 30% reduction in average latency
- 99<sup>th</sup> percentile latency dropping by 20%



## Response time for API instance

# Offloaded & Fine Tuned

- Significant reduction in GC pressure and GC pause times



Stop the world GC for API cluster

# Increased Visibility

**Increased visibility into identities  
flowing in and out of Netflix  
ecosystem**

**...and into the identity mutations  
happening in a request**

# Developer Velocity

Greatly increased developer velocity for authentication related changes

# **Team focused on security**

**Separation of concerns among the teams**

# Key Takeaways

- **Token agnostic identity model**
- **Simplified authorization**
- **Extensible identity model**
- **Offloaded all the token processing from many systems**
- **Fine tuned individual microservices to suit the token processing profile**
- **Increased visibility into identities flowing and corresponding mutations**
- **Increased developer velocity for authentication & identity related changes**
- **Team focused on security**

# Thank You.

**Satyajit Thadeshwari**  
[sthadeshwari@netflix.com](mailto:sthadeshwari@netflix.com)  
<https://www.linkedin.com/in/satyajit-thadeshwari>

