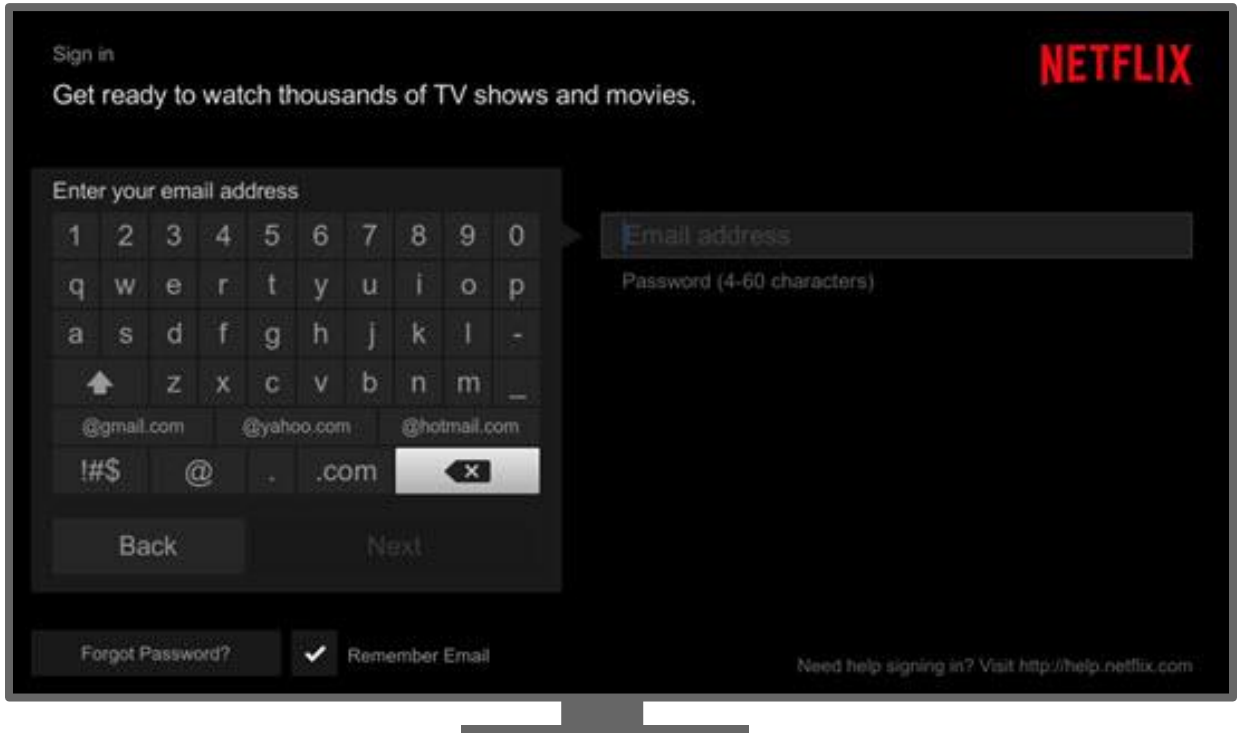
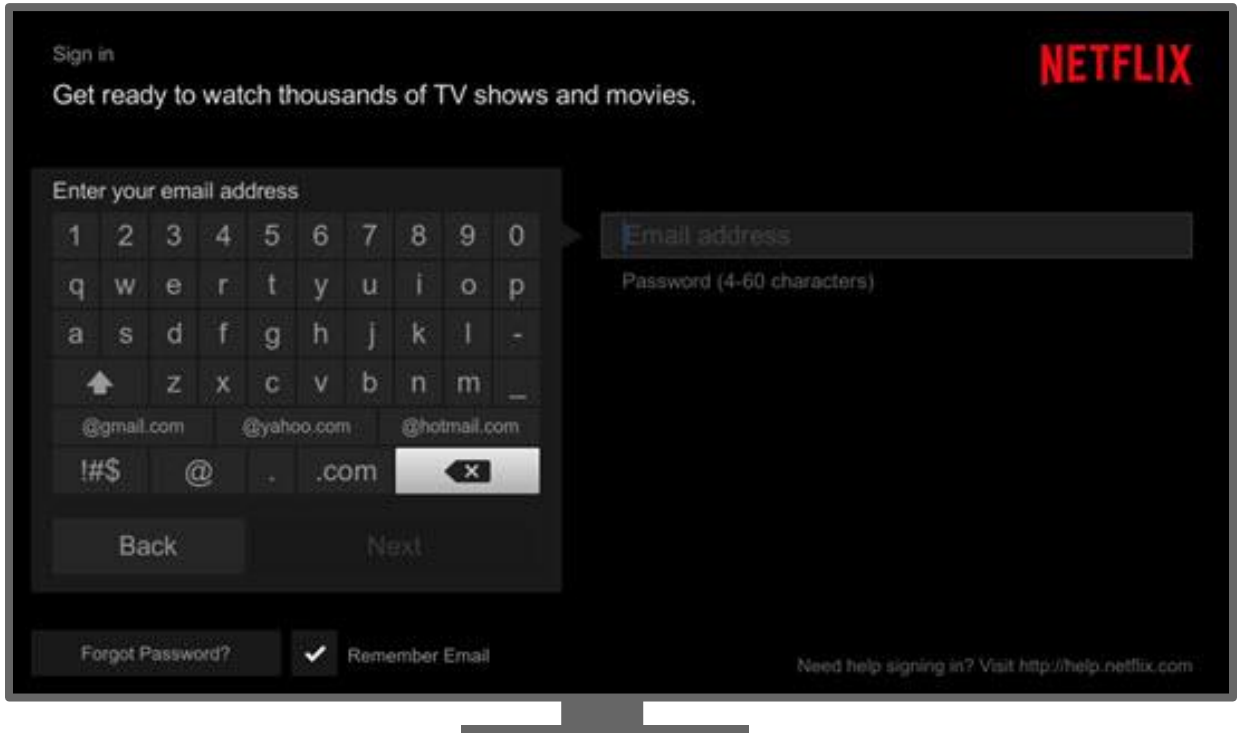
User & Device Identity For Microservices @ Netflix Scale

Satyajit Thadeshwar

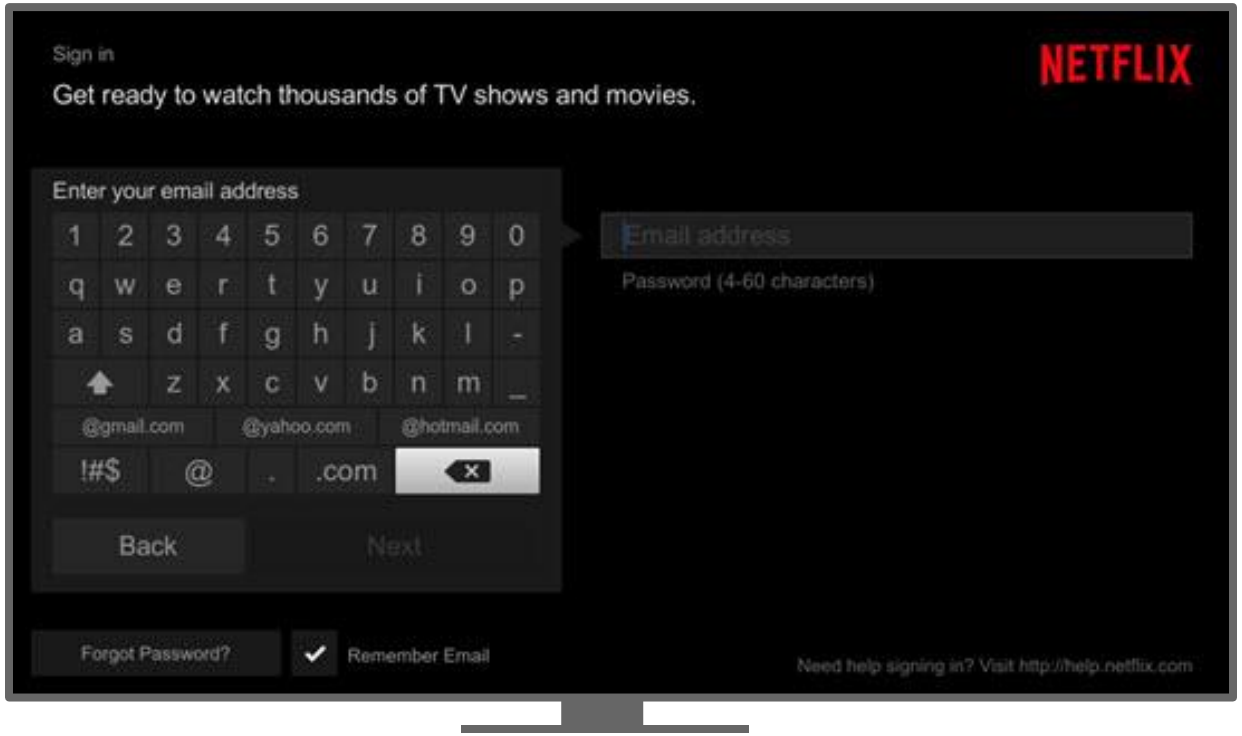
QCon San Francisco 2019

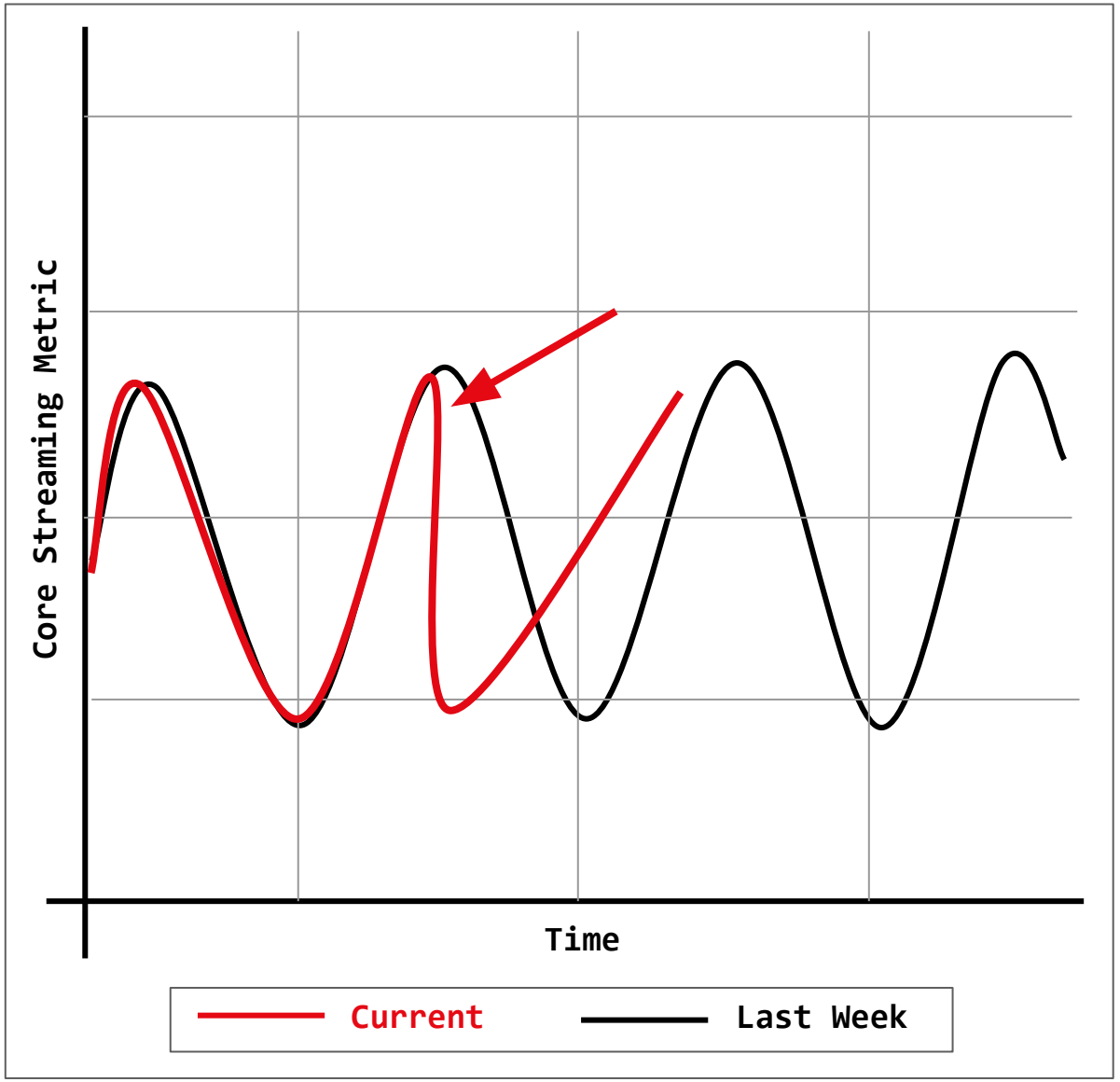

Sign in
NETFLIX
Get ready to watch thousands of TV shows and movies.
Enter your email address
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l -
z x c v b n m _
@gmail.com
@yahoo.com
@hotmail.com
!#$
@
.
.com
Back
Next
Email address
Password (4-60 characters)
Forgot Password?
Remember Email
Need help signing in? Visit http://help.netflix.com


Logged out?
#$%&!


Sign in
NETFLIX
Get ready to watch thousands of TV shows and movies.
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
Back
Next
Email address
Password (4-60 characters)
Forgot Password?
Remember Email
Need help signing in? Visit http://help.netflix.com


Logged out?
#$%&!


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
Back
Next
Email address
Password (4-60 characters)
Forgot Password?
Remember Email
Need help signing in? Visit http://help.netflix.com


Core Streaming Metric
Time
Current
Last Week

Satyajit Thadeshwar

Product Edge Access Systems

sthadeshwar@netflix.com


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:	CLOSED (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		

Description

Involved Parties:

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

People

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

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 MERGED

Create branch

NETFLIX Dashboards Projects Issues Capture Boards AIO Tableau Create Search

Prod Alert

Edit Comment Assign More Resolved Stable Active Export

Details

Type: Incident
Status: CLOSED (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

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 MERGED

Create branch

9 TEAMS

Description

Involved Parties:

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

Netflix subscribers and the devices that they use

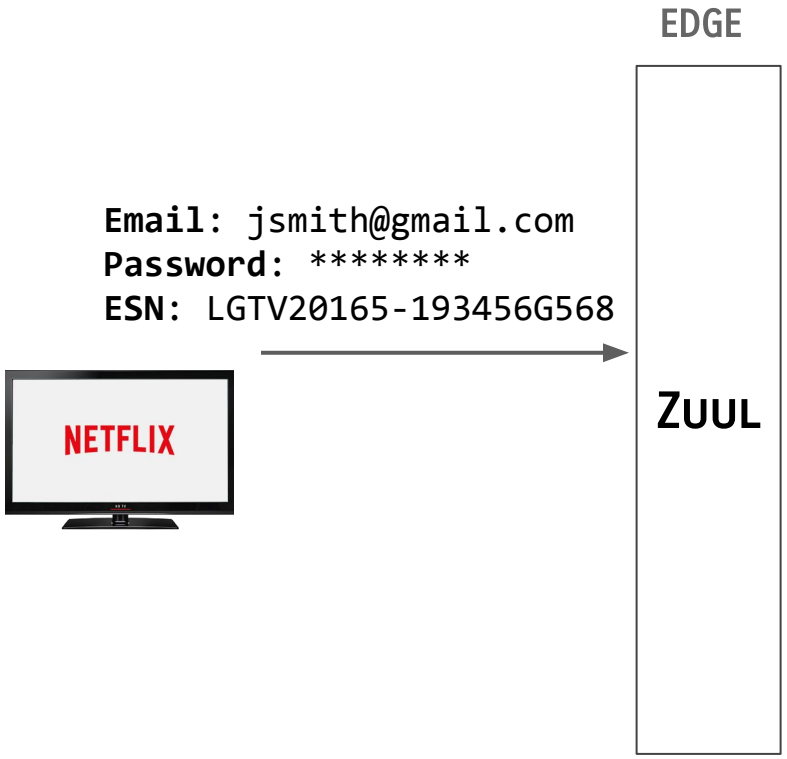
Where we were

What we did

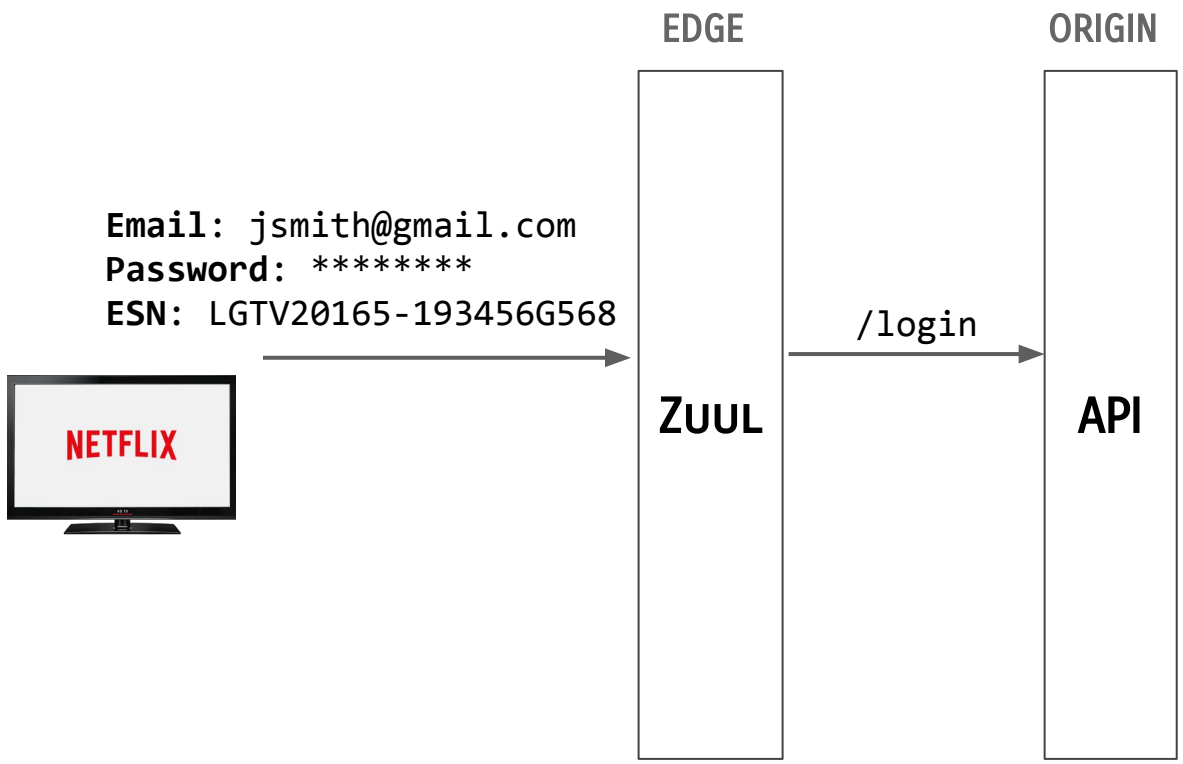
Wins

Where we were

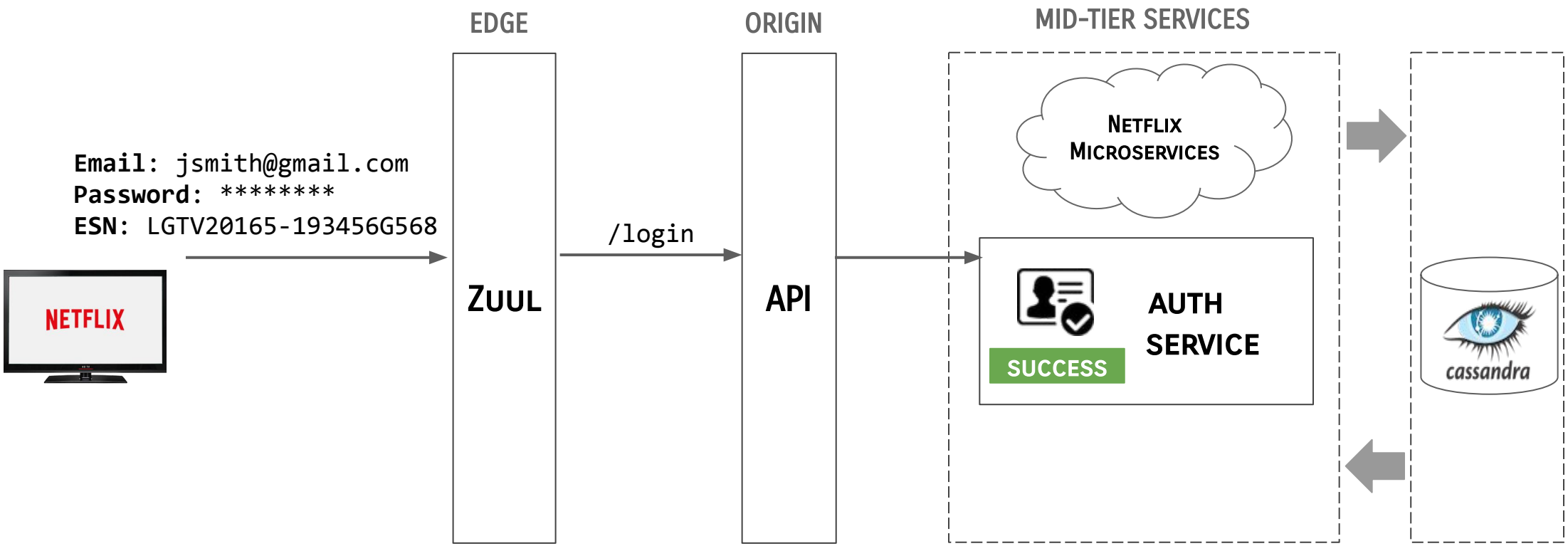
User Login


EDGE
Email: jsmith@gmail.com
Password: ********
ESN: LGTV20165-193456G568
NETFLIX
ZUUL

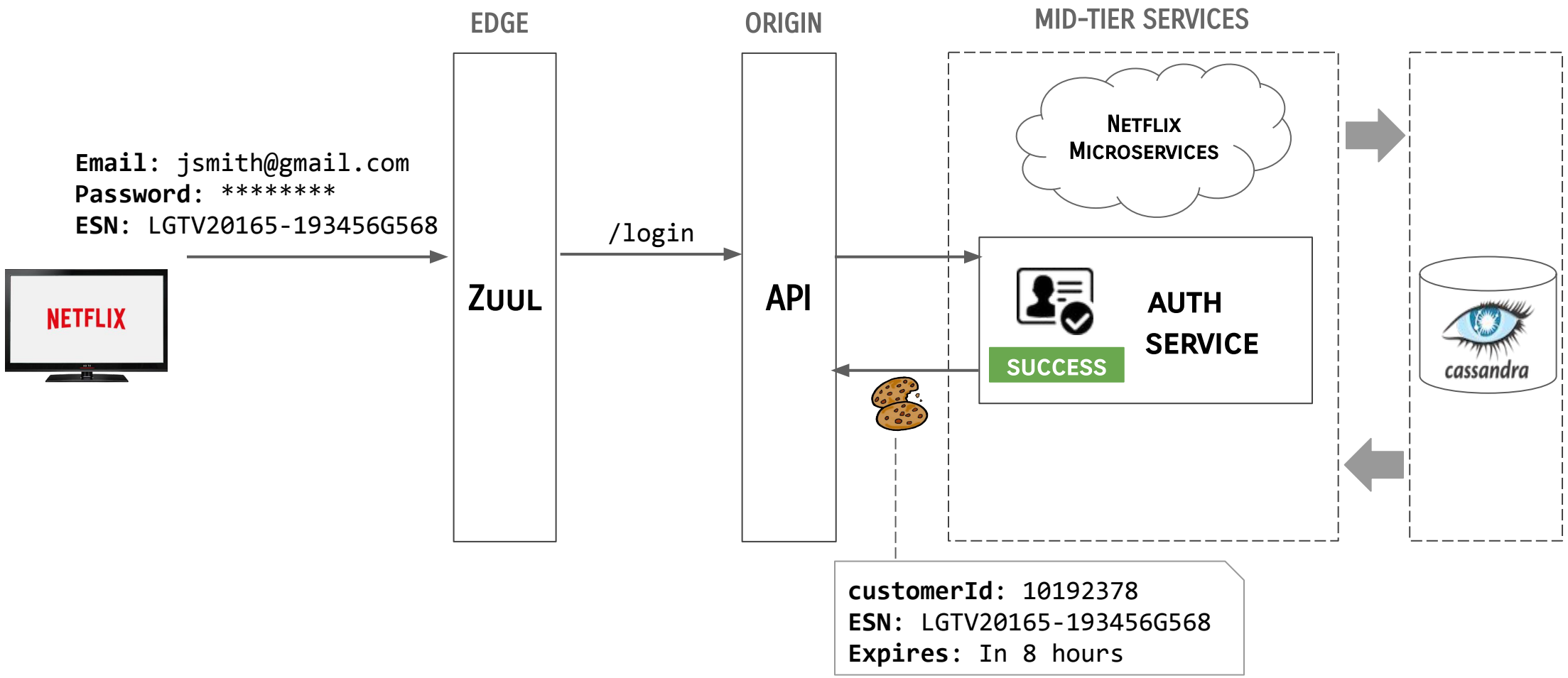
User Login


EDGE
ORIGIN
Email: jsmith@gmail.com
Password: ********
ESN: LGTV20165-193456G568
/login
NETFLIX
ZUUL
API

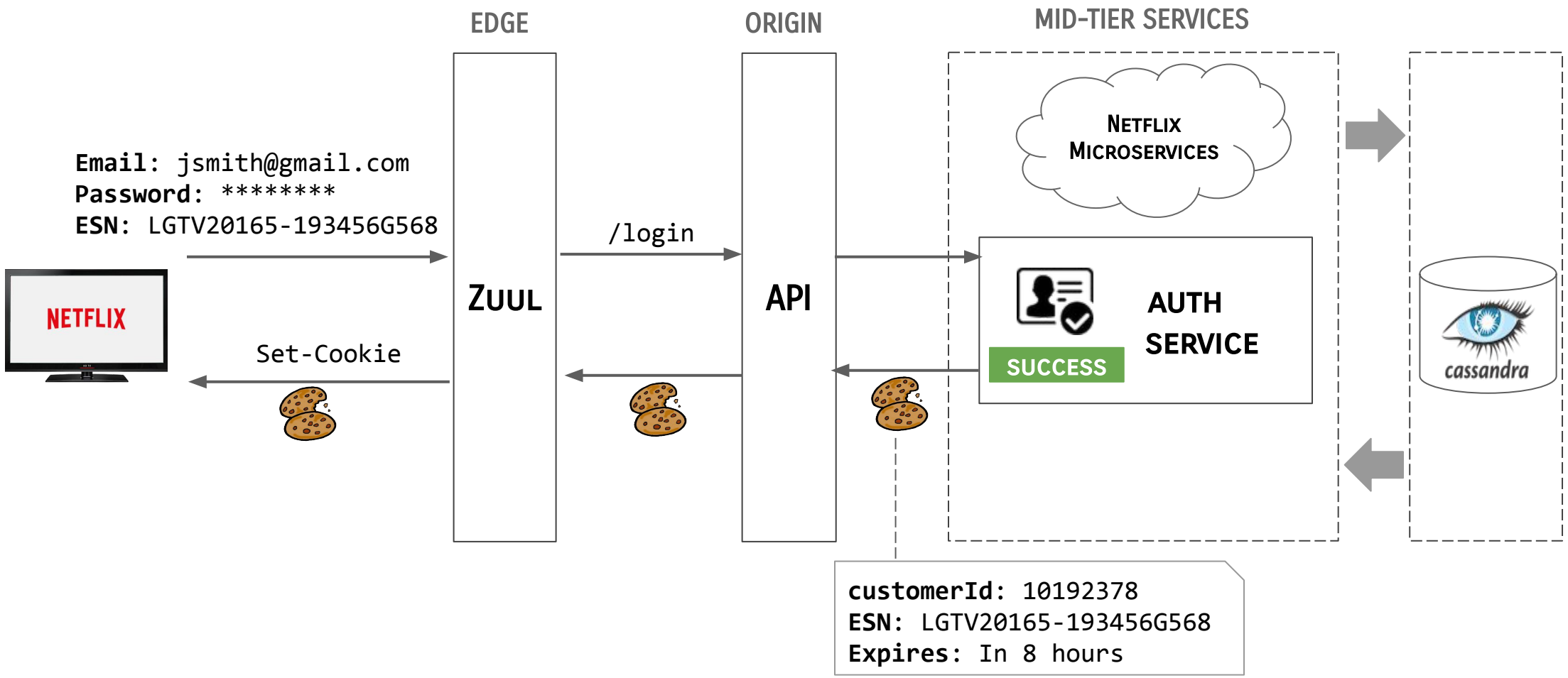
User Login


EDGE
ORIGIN
MID-TIER SERVICES
Email: jsmith@gmail.com
Password: ********
ESN: LGTV20165-193456G568
NETFLIX
ZUUL
/login
API
NETFLIX MICROSERVICES
SUCCESS
AUTH SERVICE
cassandra

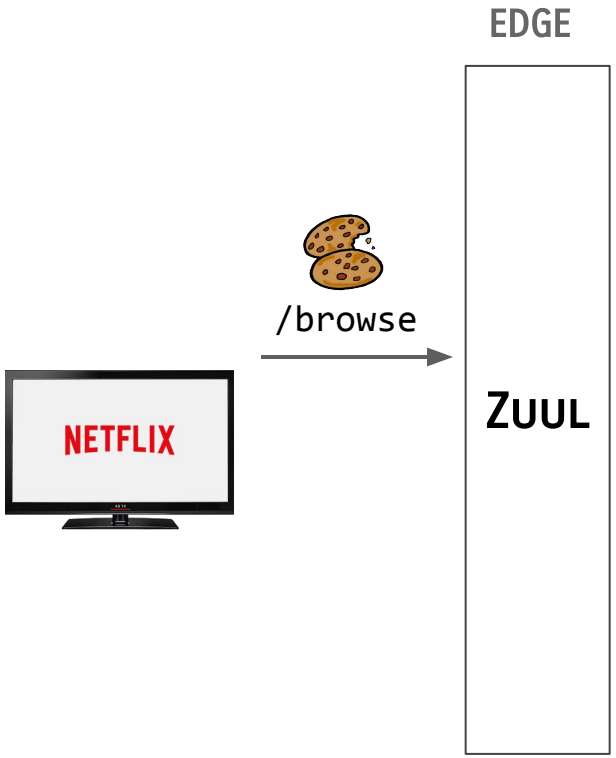
User Login


EDGE
ORIGIN
MID-TIER SERVICES
Email: jsmith@gmail.com
Password: ********
ESN: LGTV20165-193456G568
NETFLIX
ZUUL
/login
API
NETFLIX MICROSERVICES
AUTH SERVICE
SUCCESS
cassandra
customerId: 10192378
ESN: LGTV20165-193456G568
Expires: In 8 hours

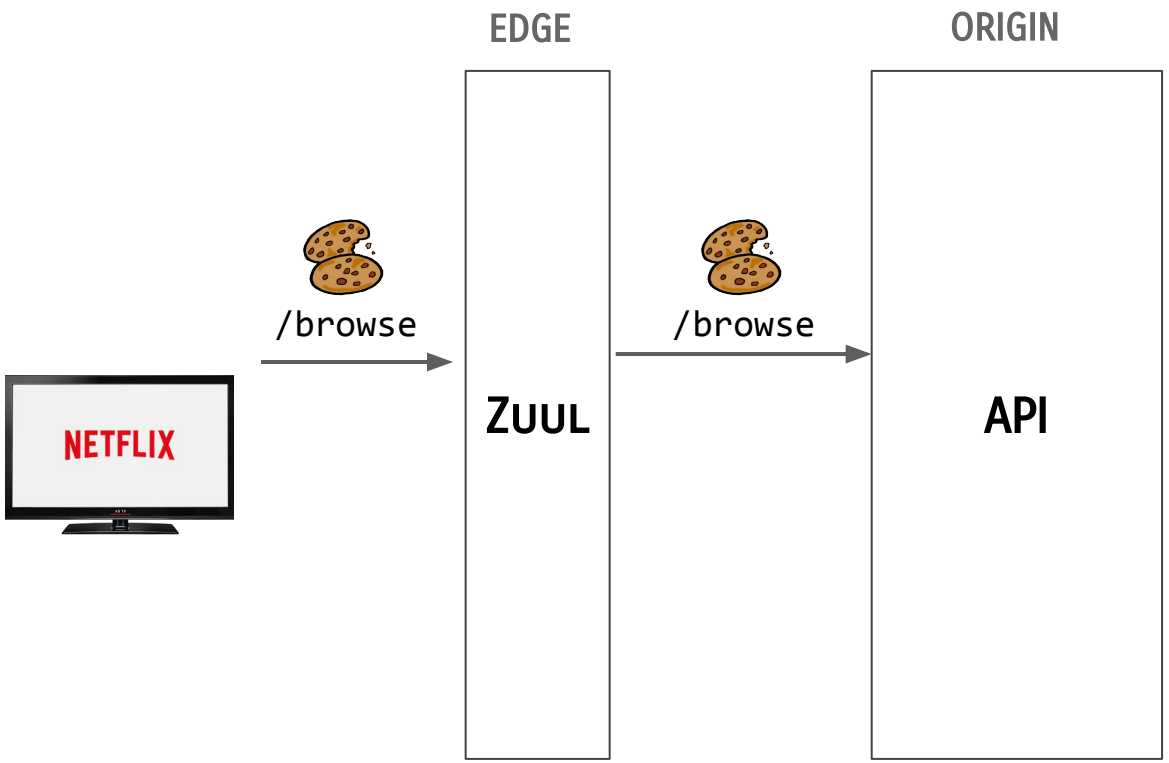
User Login


EDGE
ORIGIN
MID-TIER SERVICES
Email: jsmith@gmail.com
Password: ********
ESN: LGTV20165-193456G568
NETFLIX
ZUUL
/login
API
NETFLIX MICROSERVICES
AUTH SERVICE
SUCCESS
cassandra
Set-Cookie
customerId: 10192378
ESN: LGTV20165-193456G568
Expires: In 8 hours

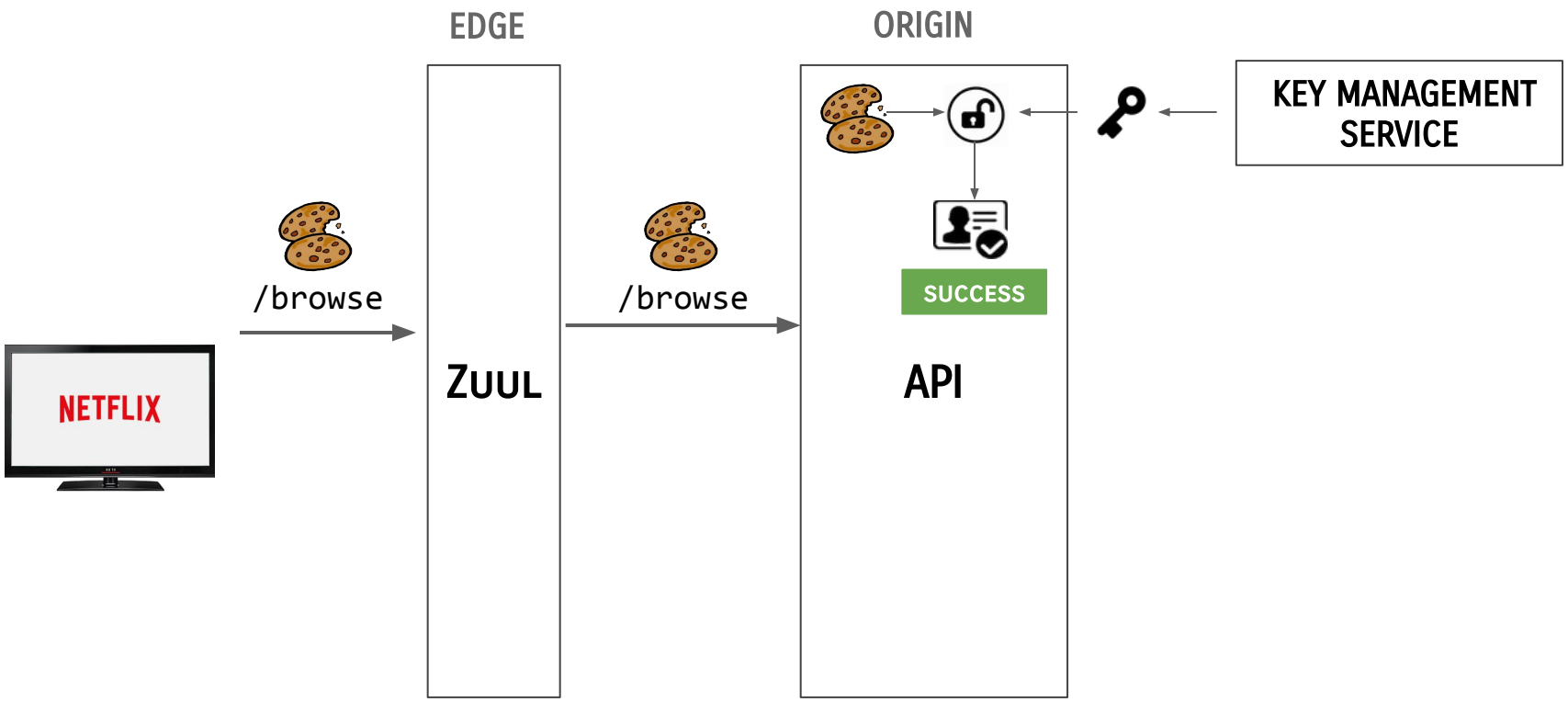
Authenticate Request



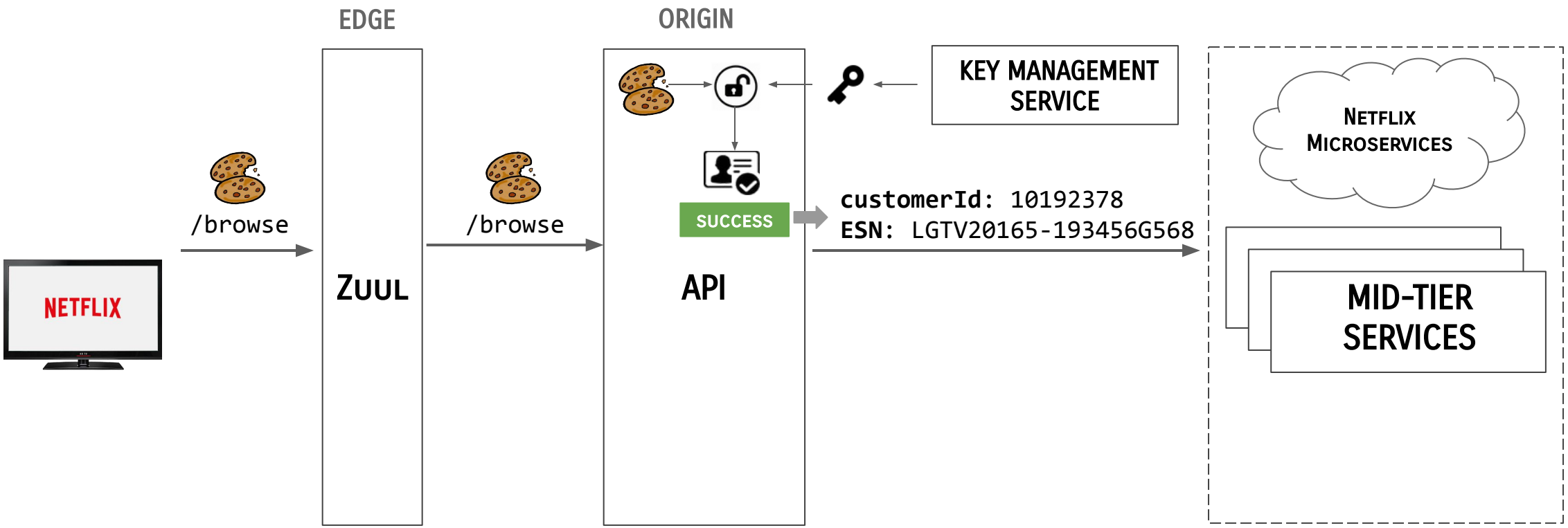
Authenticate Request



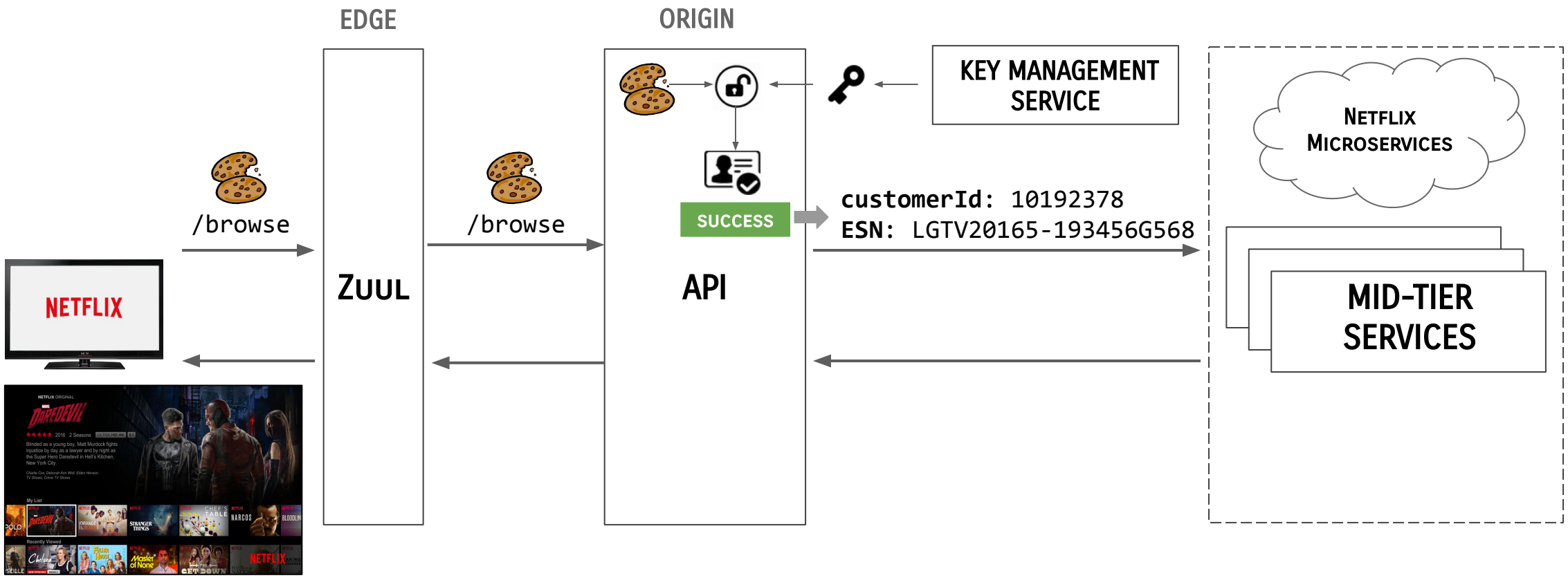
Authenticate Request



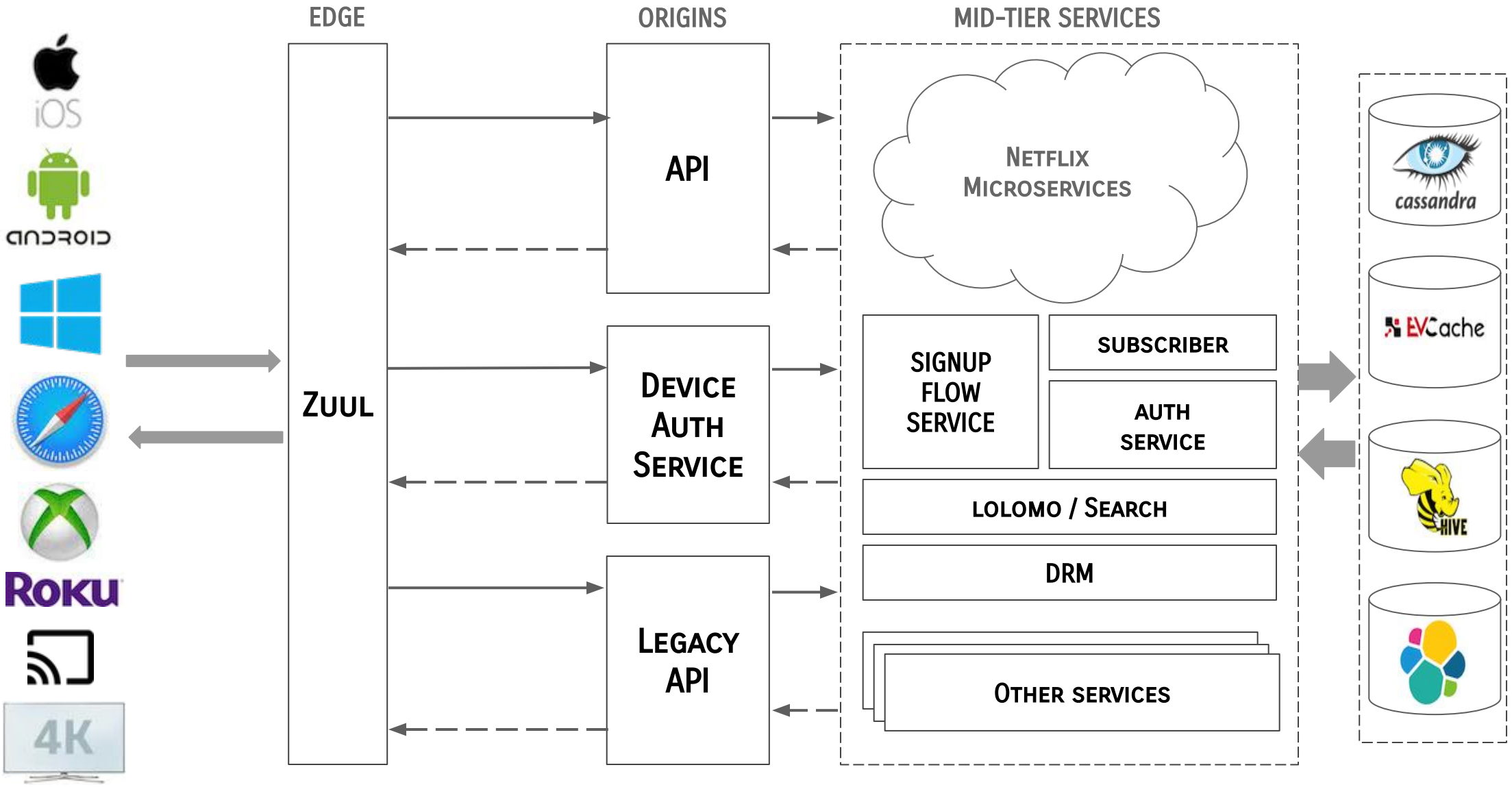
Authenticate Request

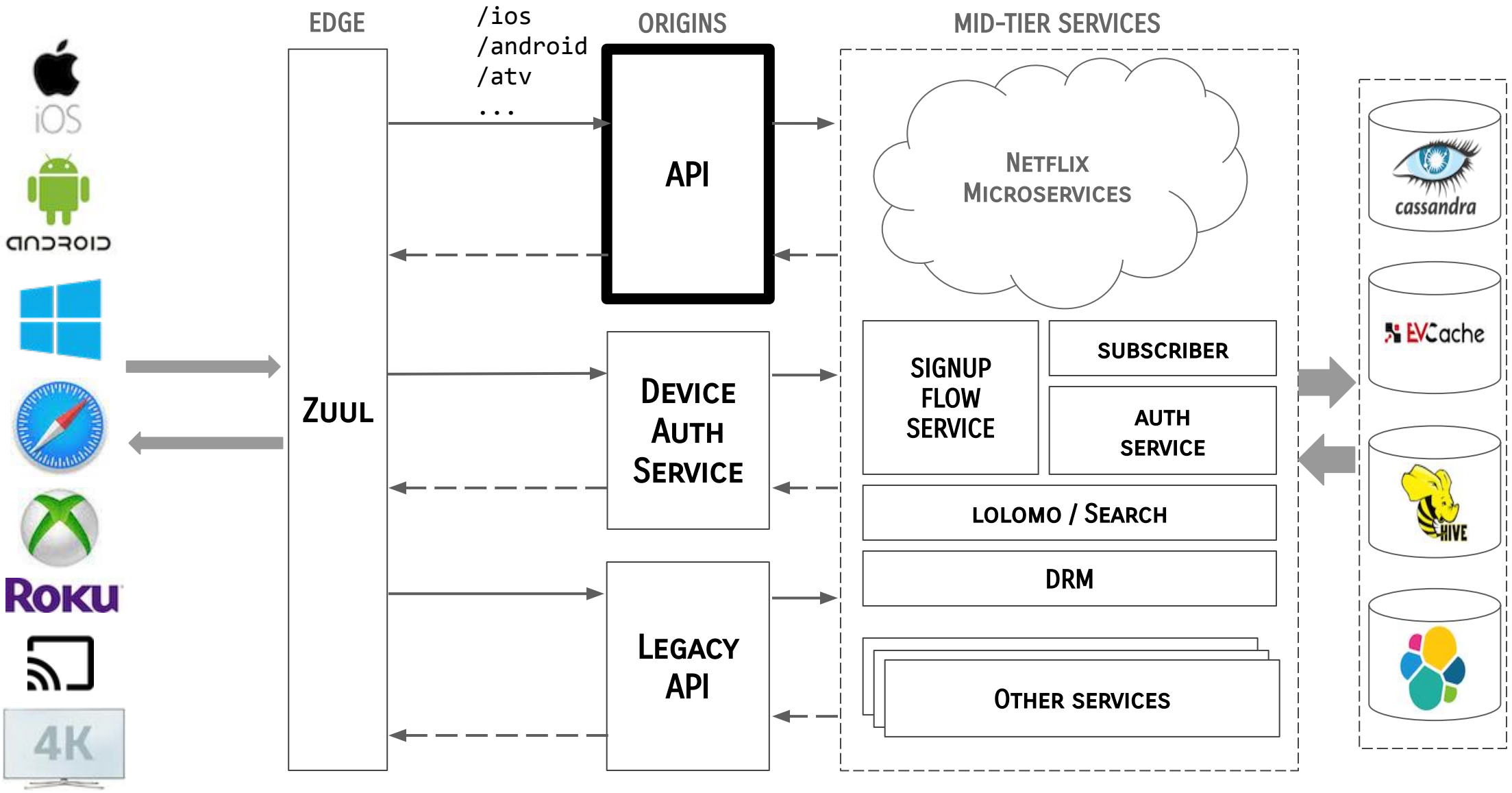


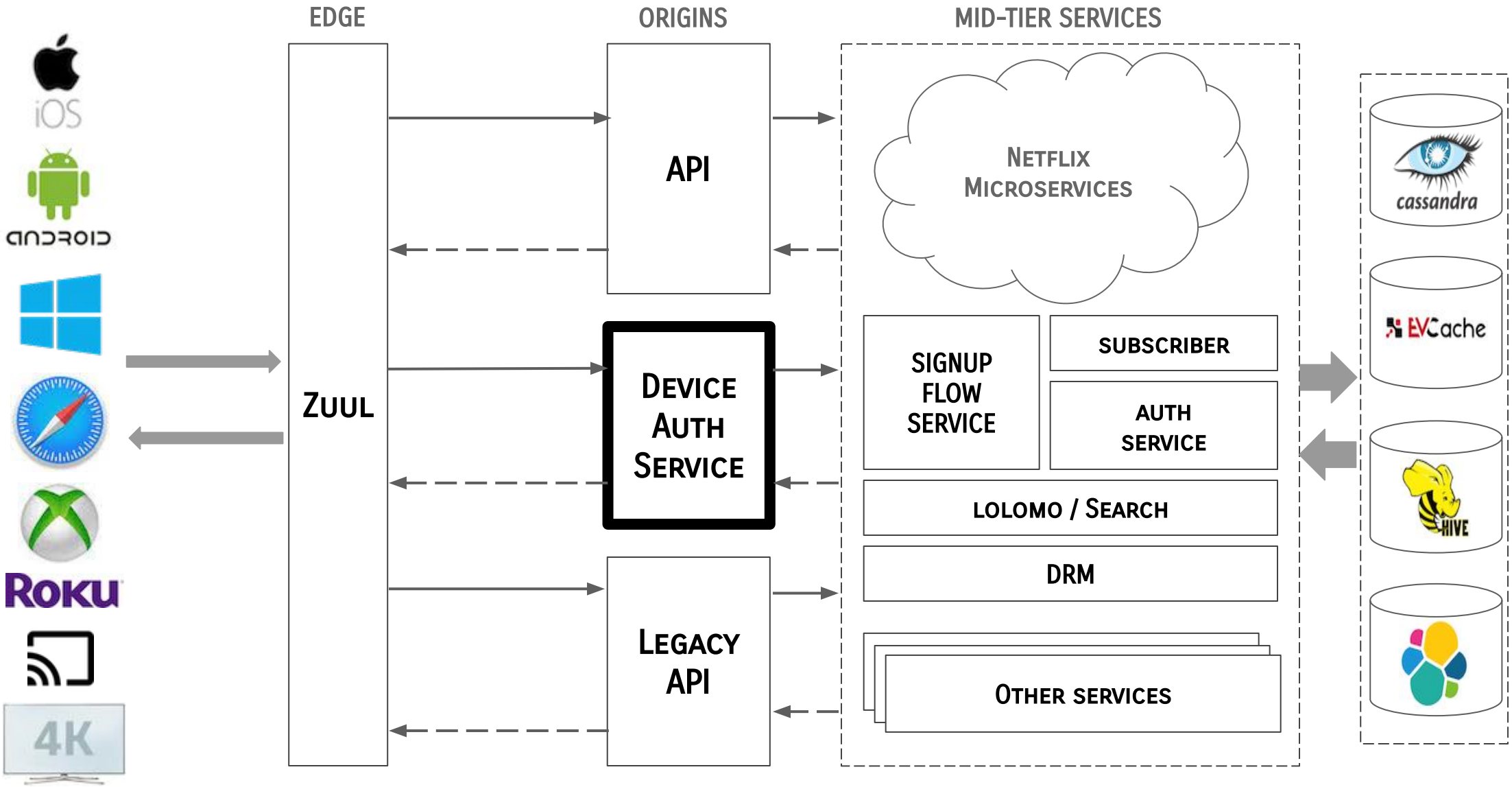
Authenticate Request

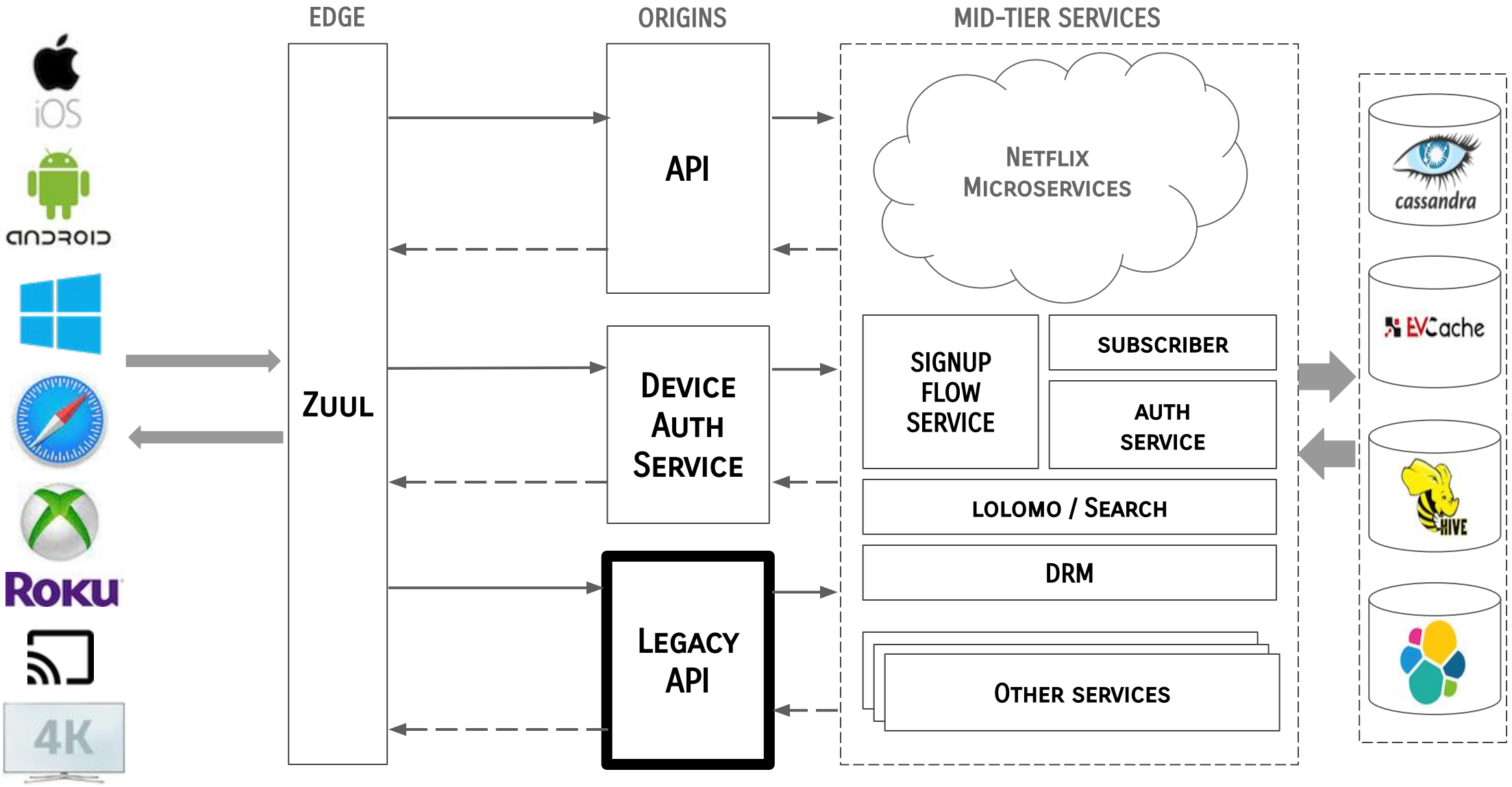


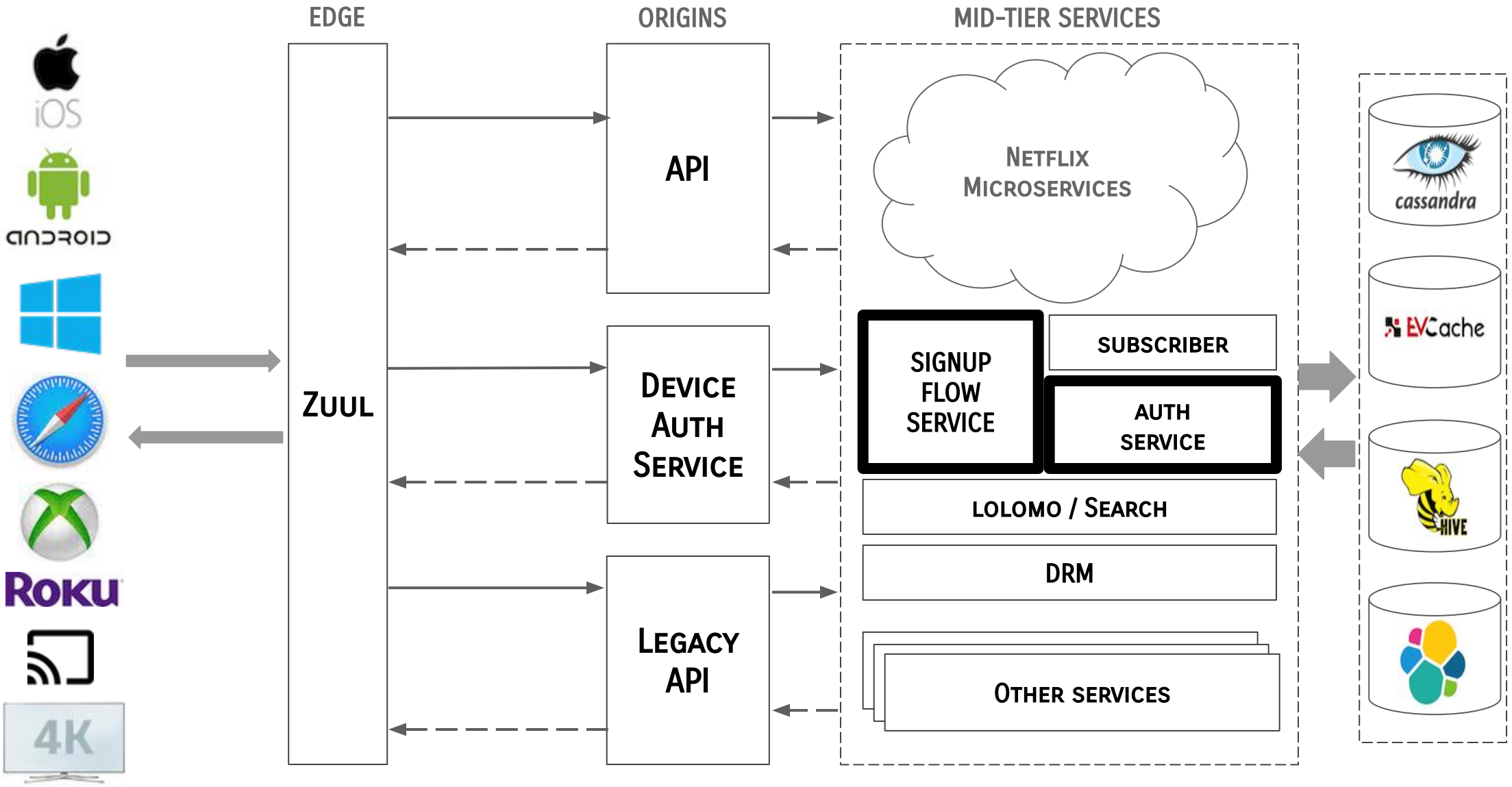
More than one service consuming cookies

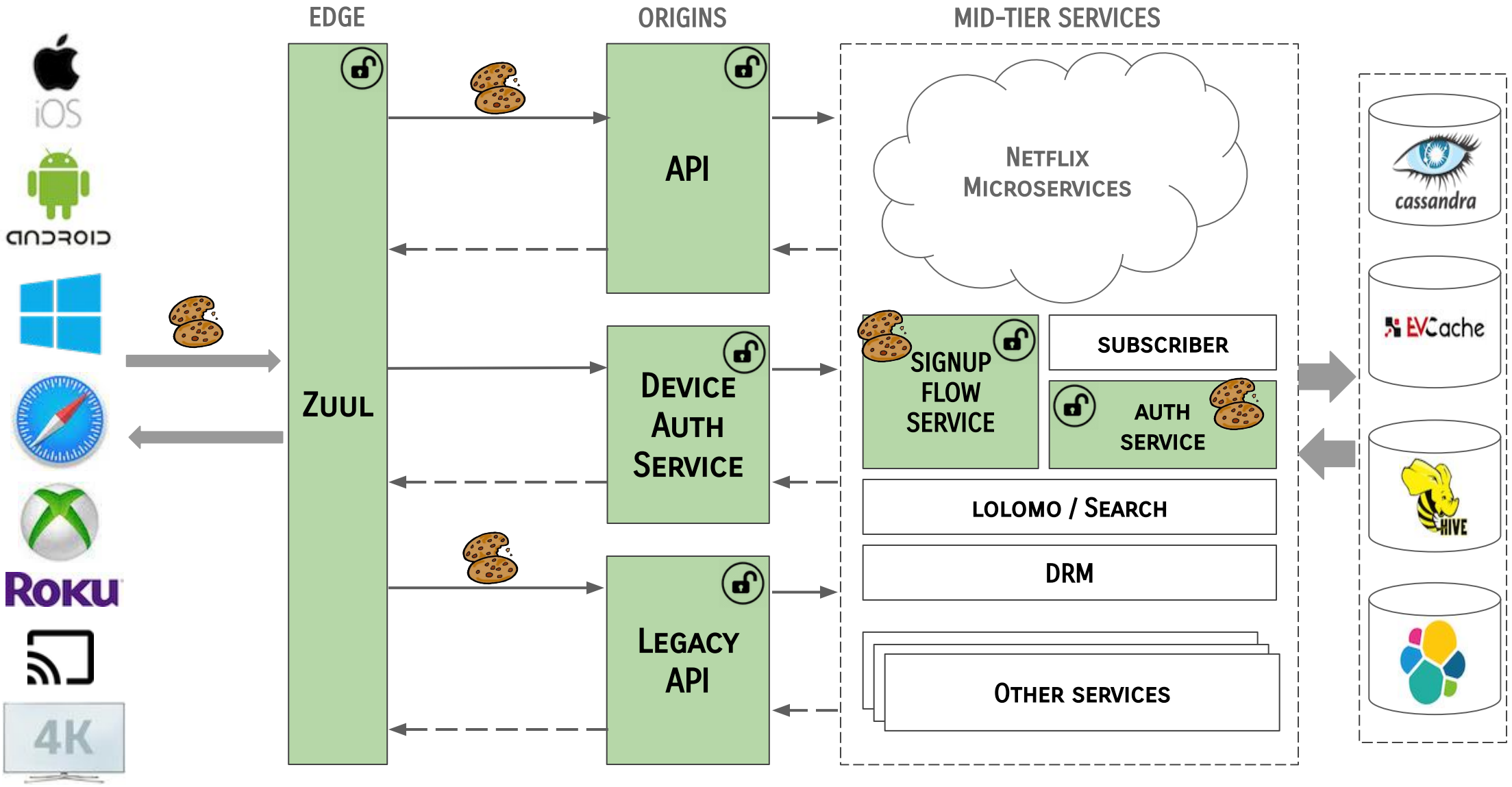

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
Zuul
API
Device Auth Service
Legacy API
Netflix Microservices
Signup Flow Service
Subscriber
Auth Service
Lolomo / Search
DRM
Other services
cassandra
EVCache
HIVE


EDGE
/ios
/android
/atv
...
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
Zuul
API
Device Auth Service
Legacy API
Netflix Microservices
Signup Flow Service
Subscriber
Auth Service
Lolomo / Search
DRM
Other services
cassandra
EVCache
HIVE

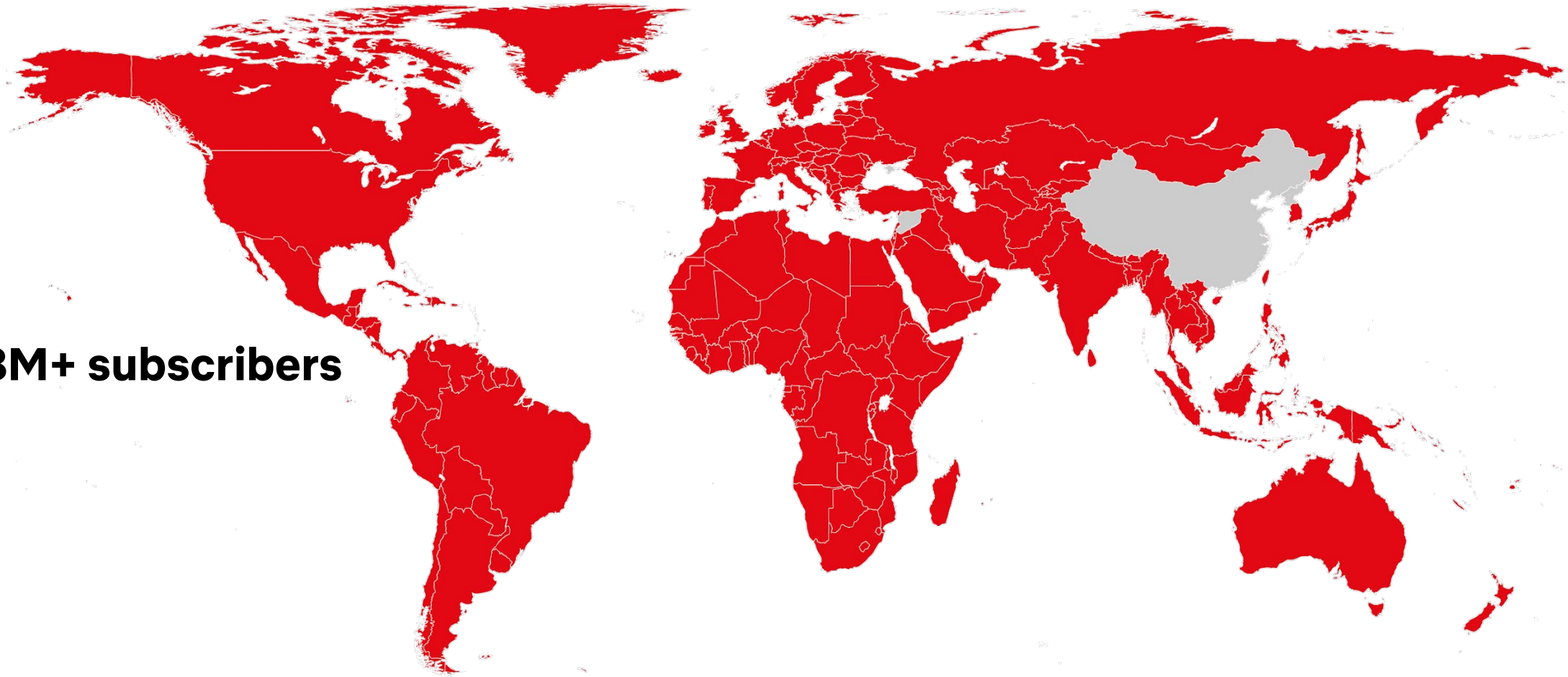

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
Zuul
API
Device Auth Service
Legacy API
Netflix Microservices
Signup Flow Service
Subscriber
Auth Service
Lolomo / Search
DRM
Other services
cassandra
EVCache
HIVE


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
Zuul
API
Device Auth Service
Legacy API
Netflix Microservices
Signup Flow Service
Subscriber
Auth Service
Lolomo / Search
DRM
Other services
cassandra
EVCache
HIVE


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE

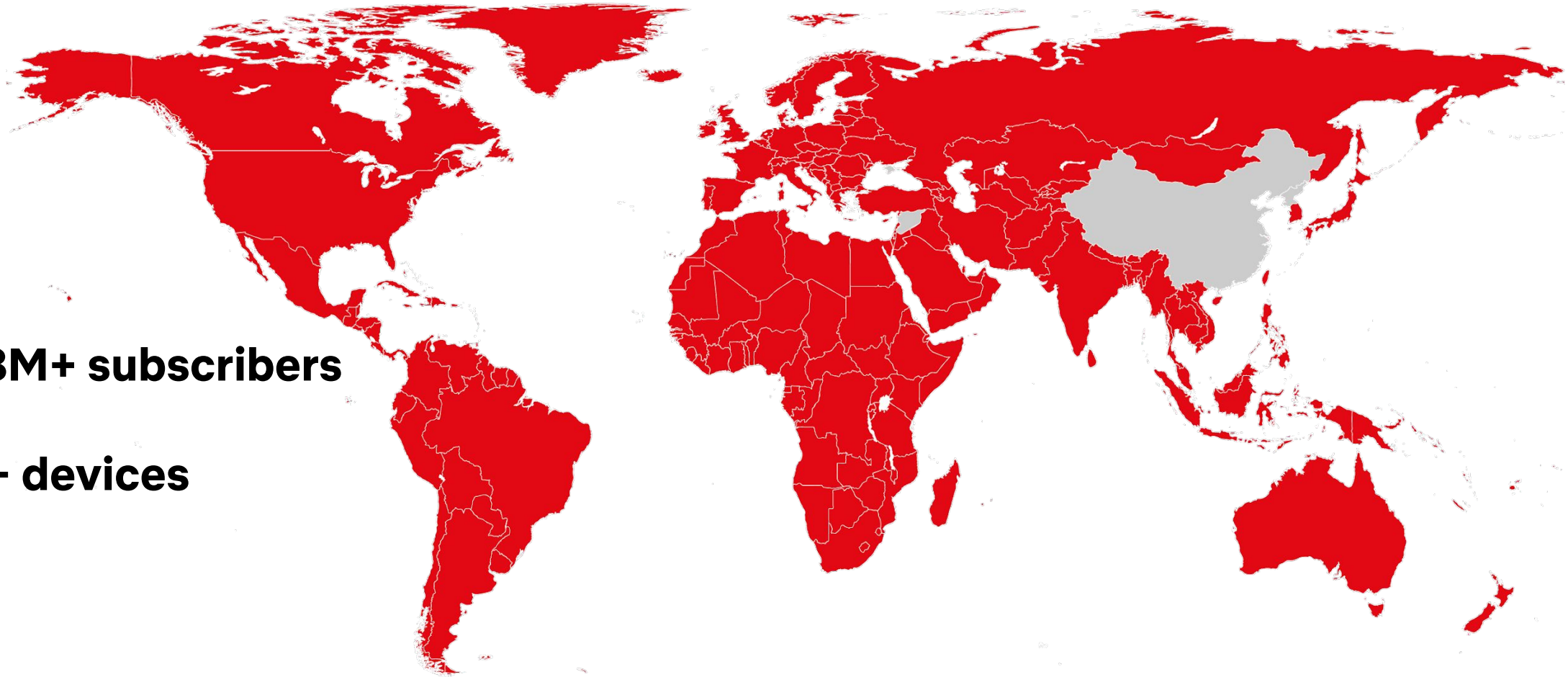
At massive scale

Netflix



158M+ subscribers

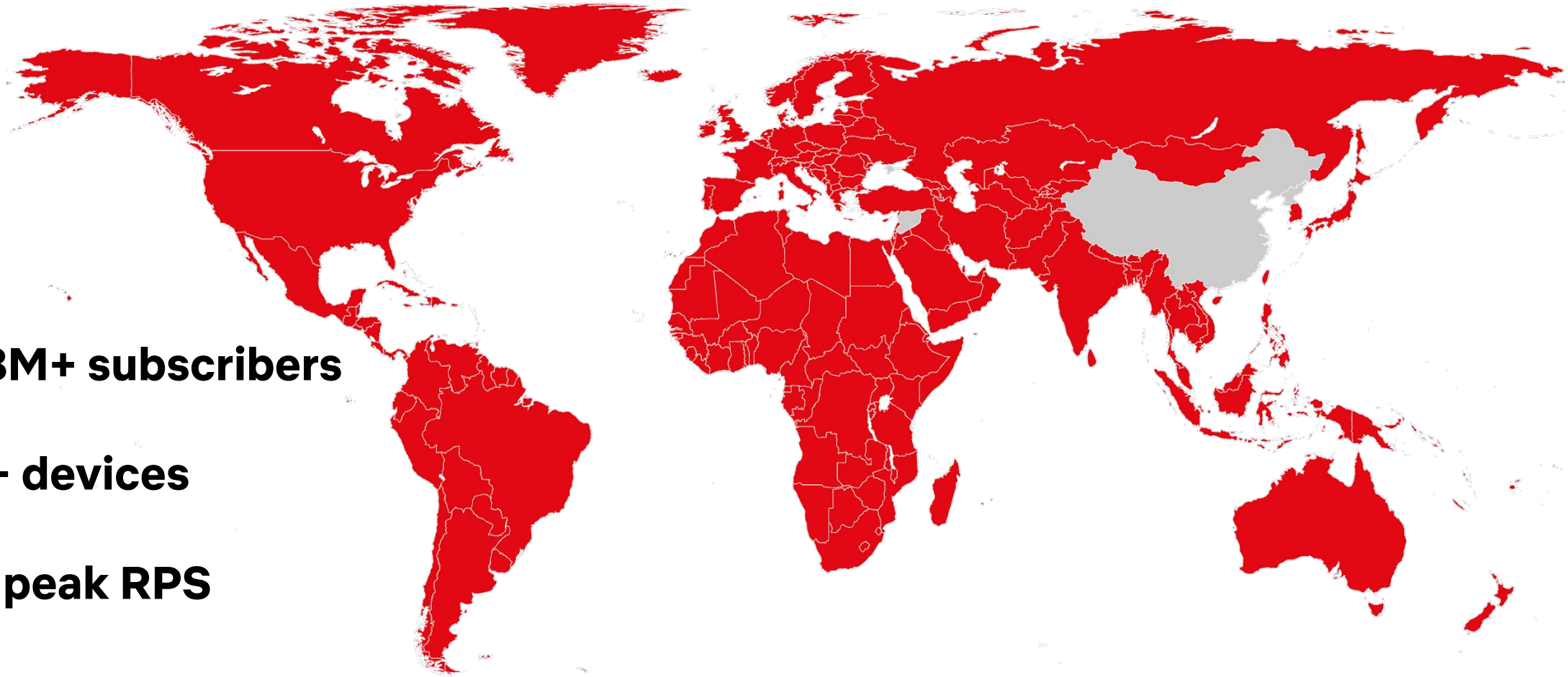
Netflix



158M+ subscribers

1B+ devices

Netflix

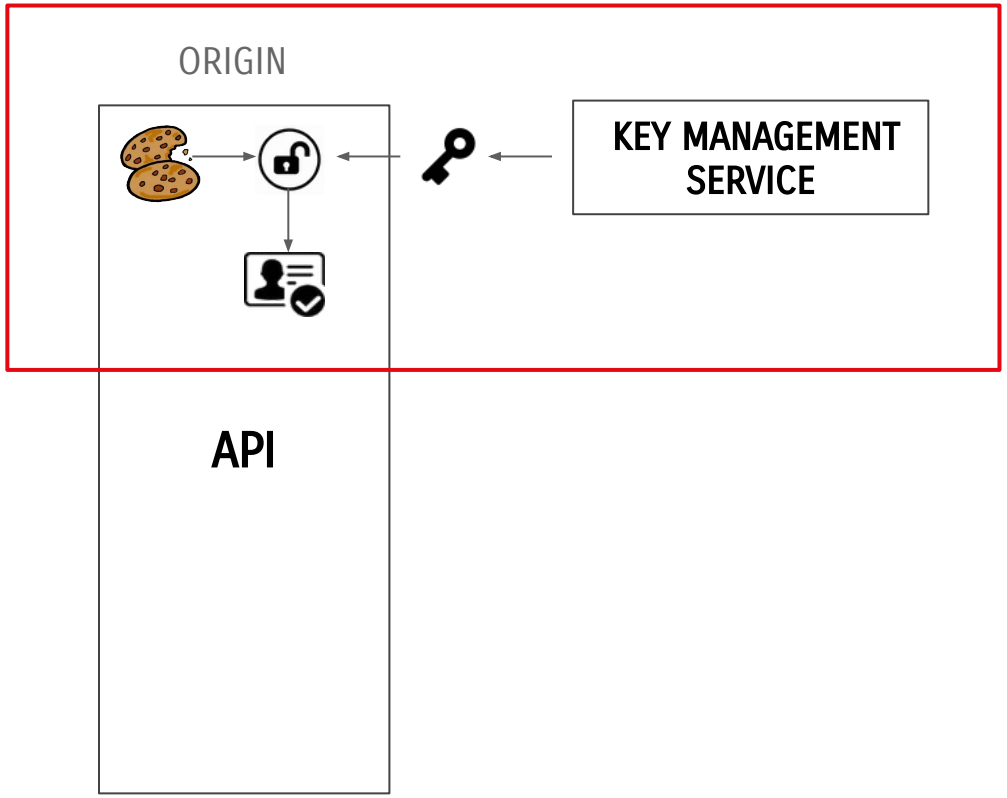


158M+ subscribers

1B+ devices

2M peak RPS

Authenticate Request / Extract Identity



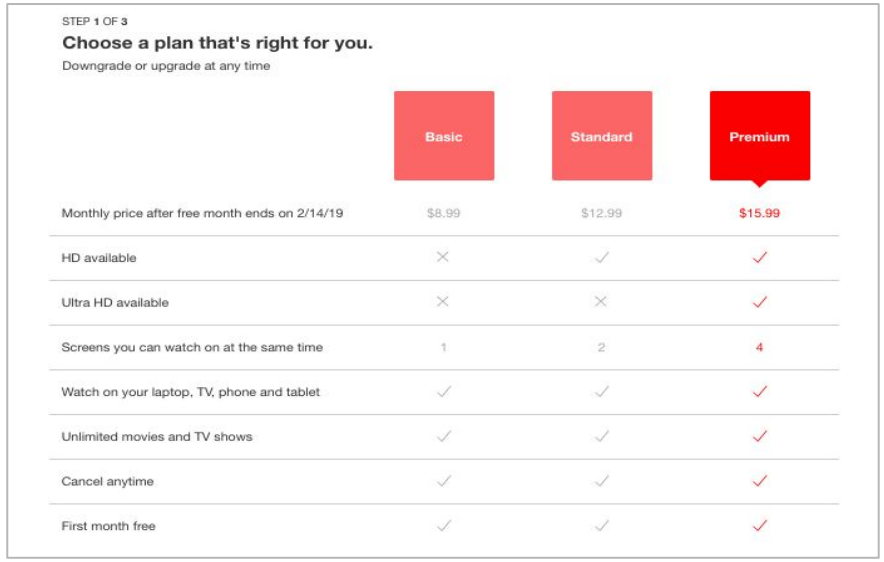
= 2 million Requests Per Second

More than one token type

Cookies 

Cookies 

- **Signup**



STEP 1 OF 3

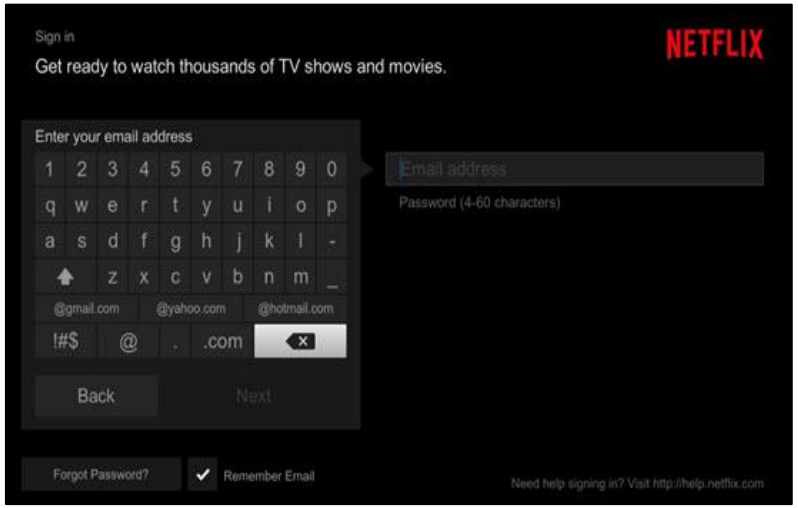
Choose a plan that's right for you.

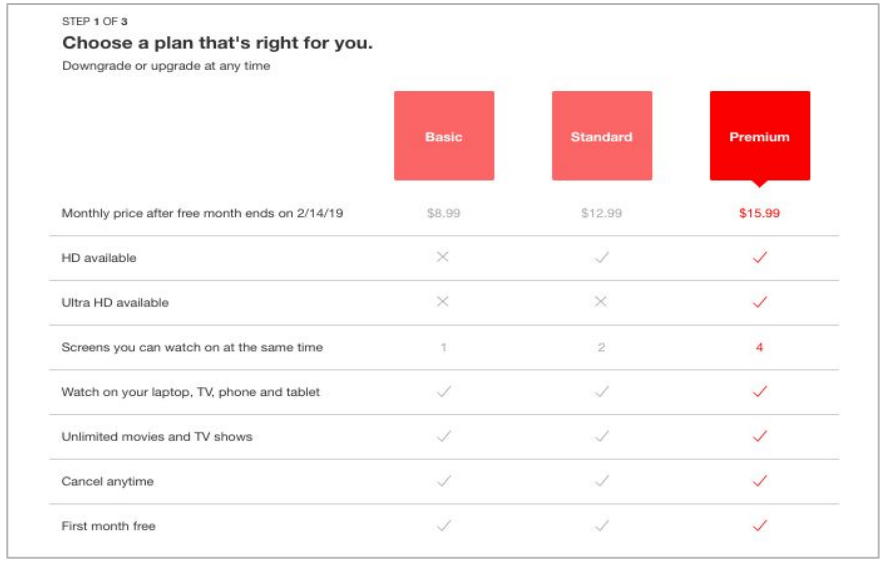
Downgrade or upgrade at any time

	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 

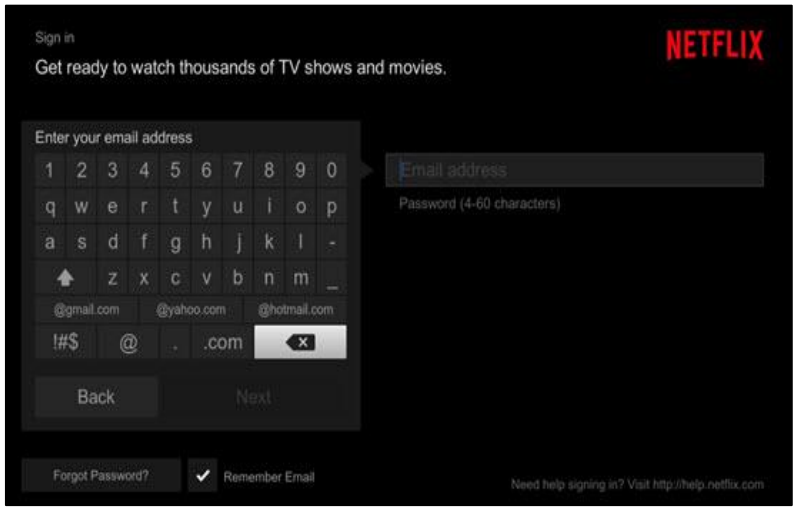
- **Signup**
- **Login**

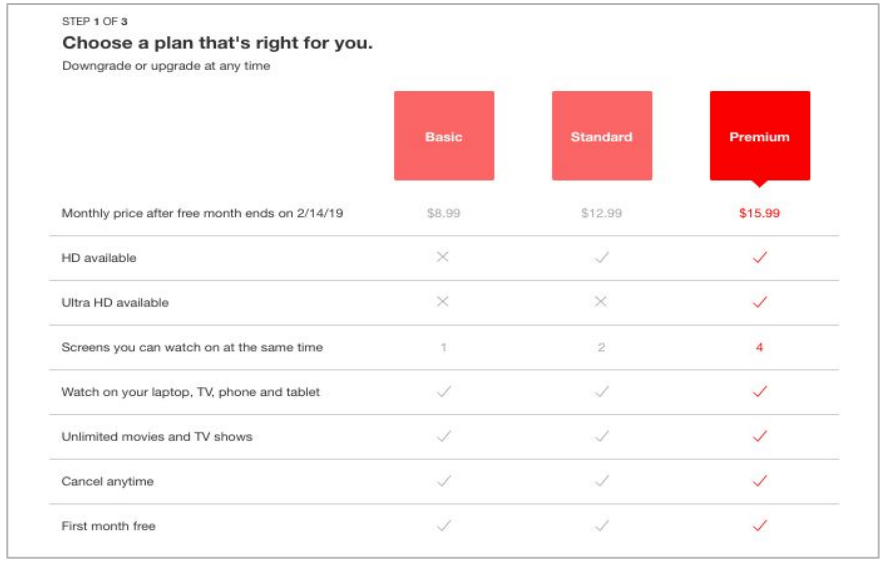


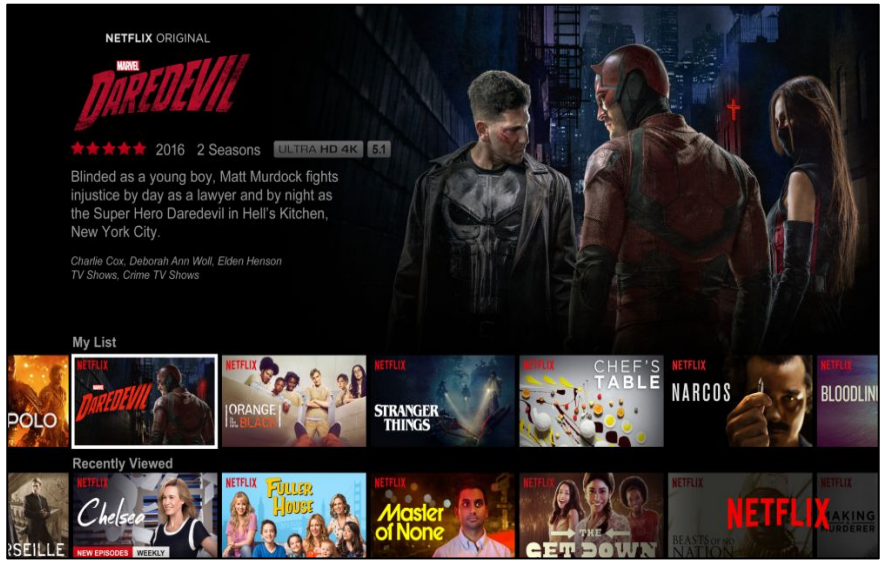


Cookies 

- Signup
- Login
- Discovery







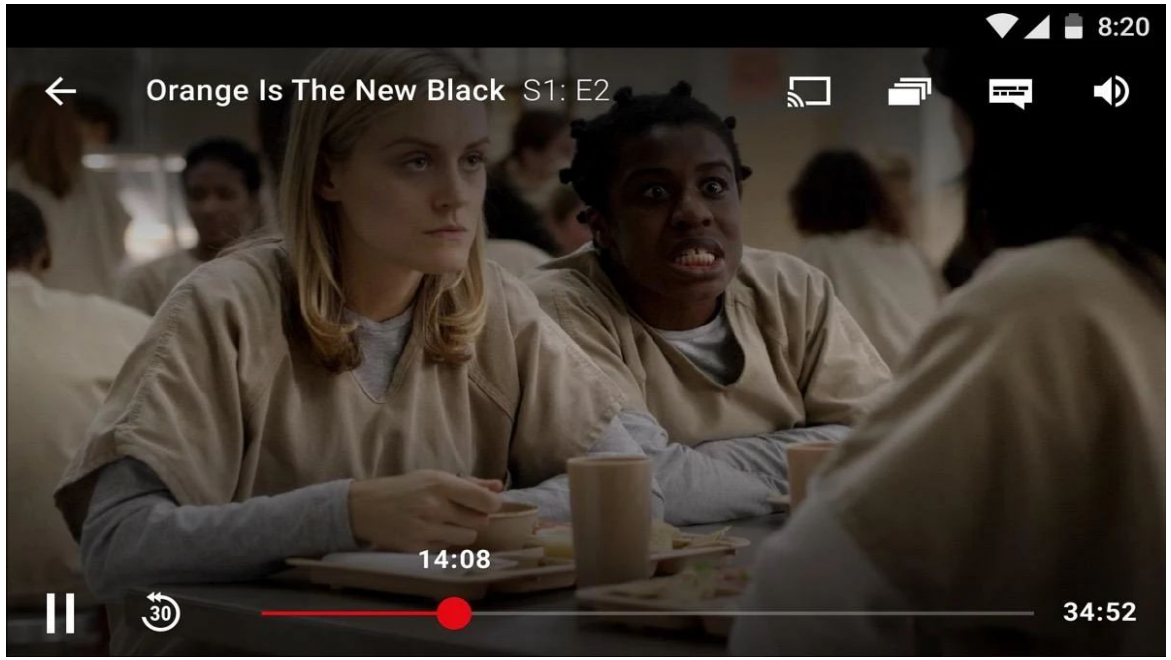
MSL Tokens 

- **Device authentication**
- **Encryption**

Message Security Layer (MSL)
https://www.infoq.com/news/2014/11/netflix-msl/

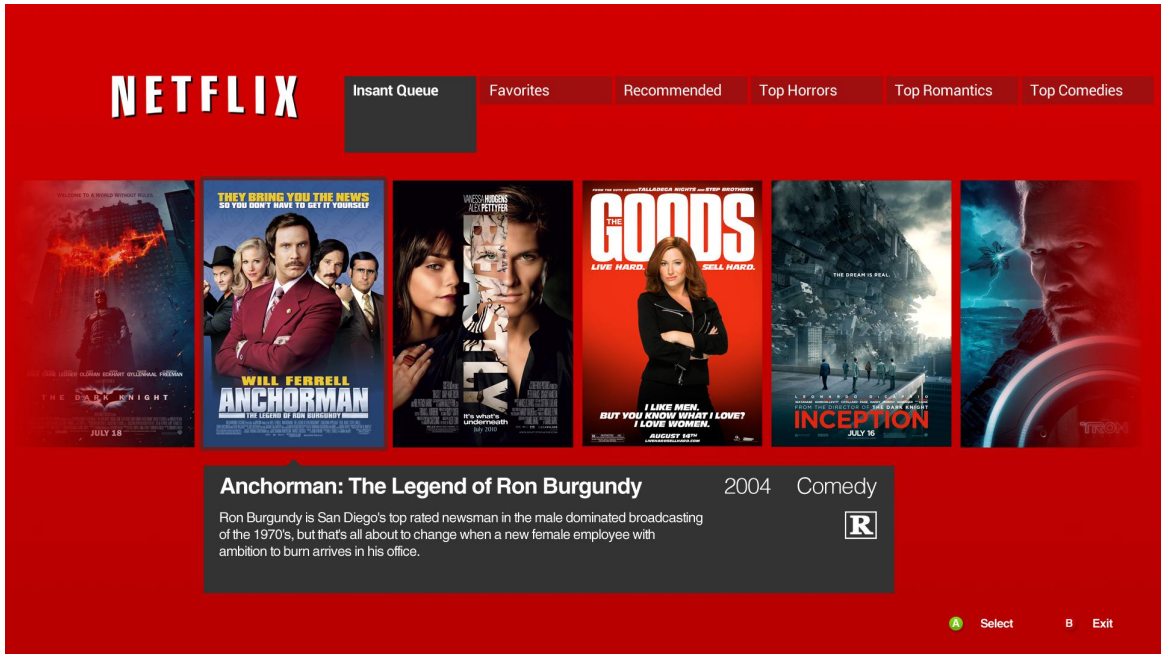
MSL Tokens

- License
- Playback



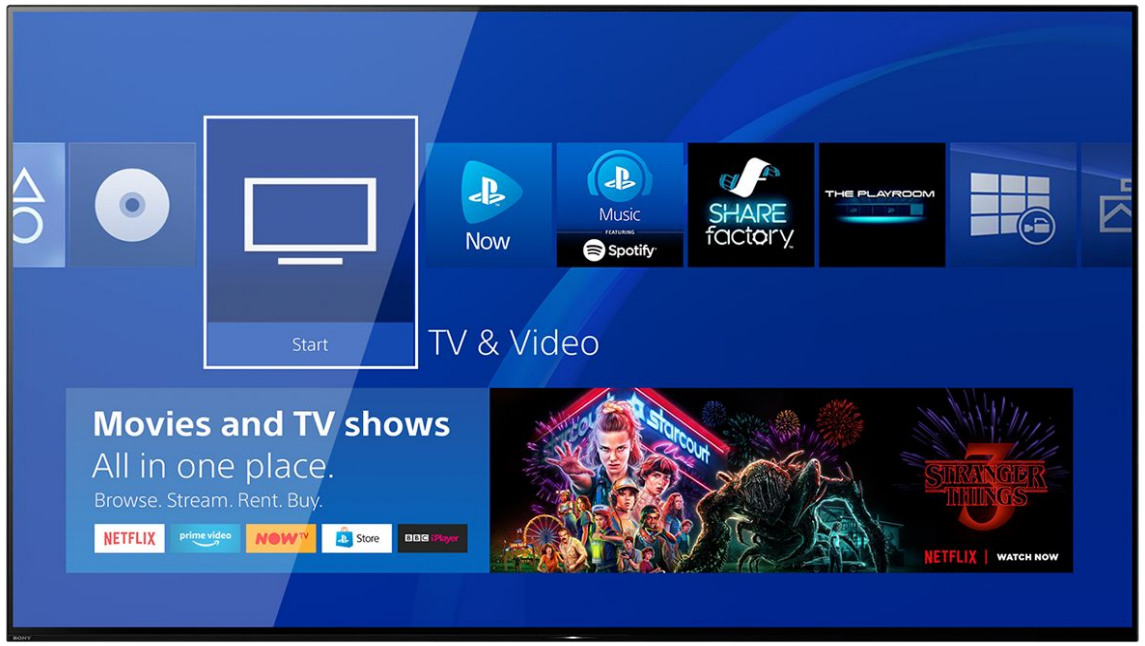
CTicket

- **Legacy devices**



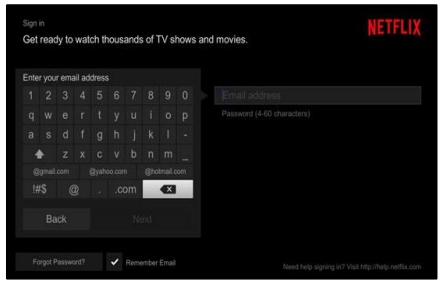
Partner Tokens

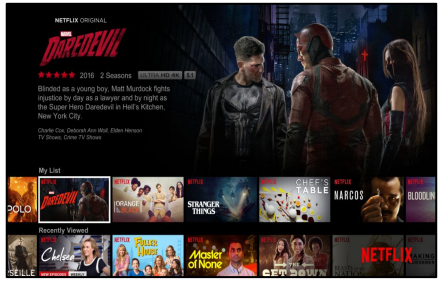
- JWS, JWE
- Non-member experiences



Cookies

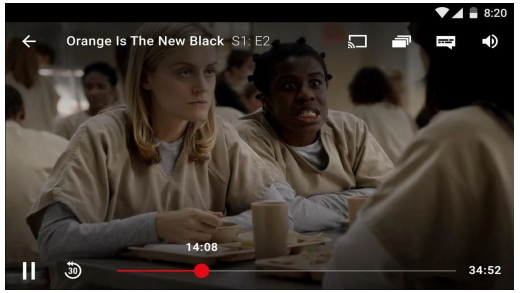
- Signup
- Sign-in
- Discovery





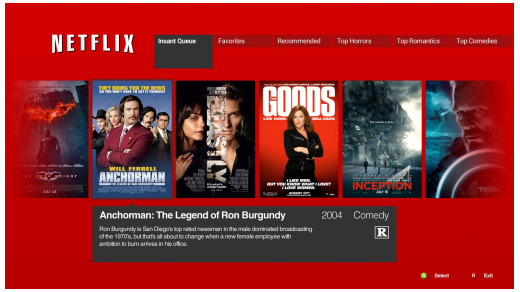
MSL Tokens

- License
- Playback



CTicket

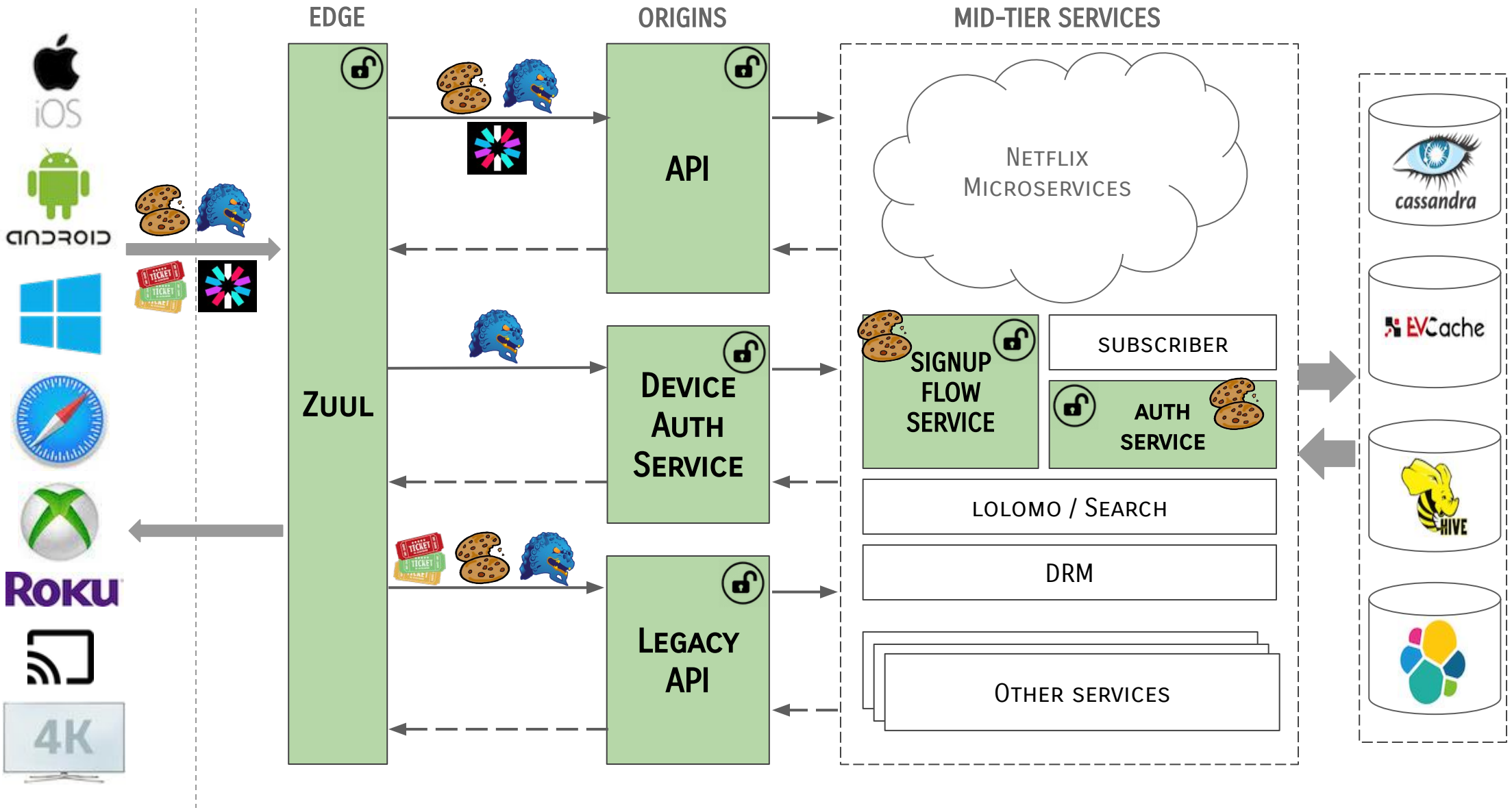
- Legacy devices



Partner Tokens

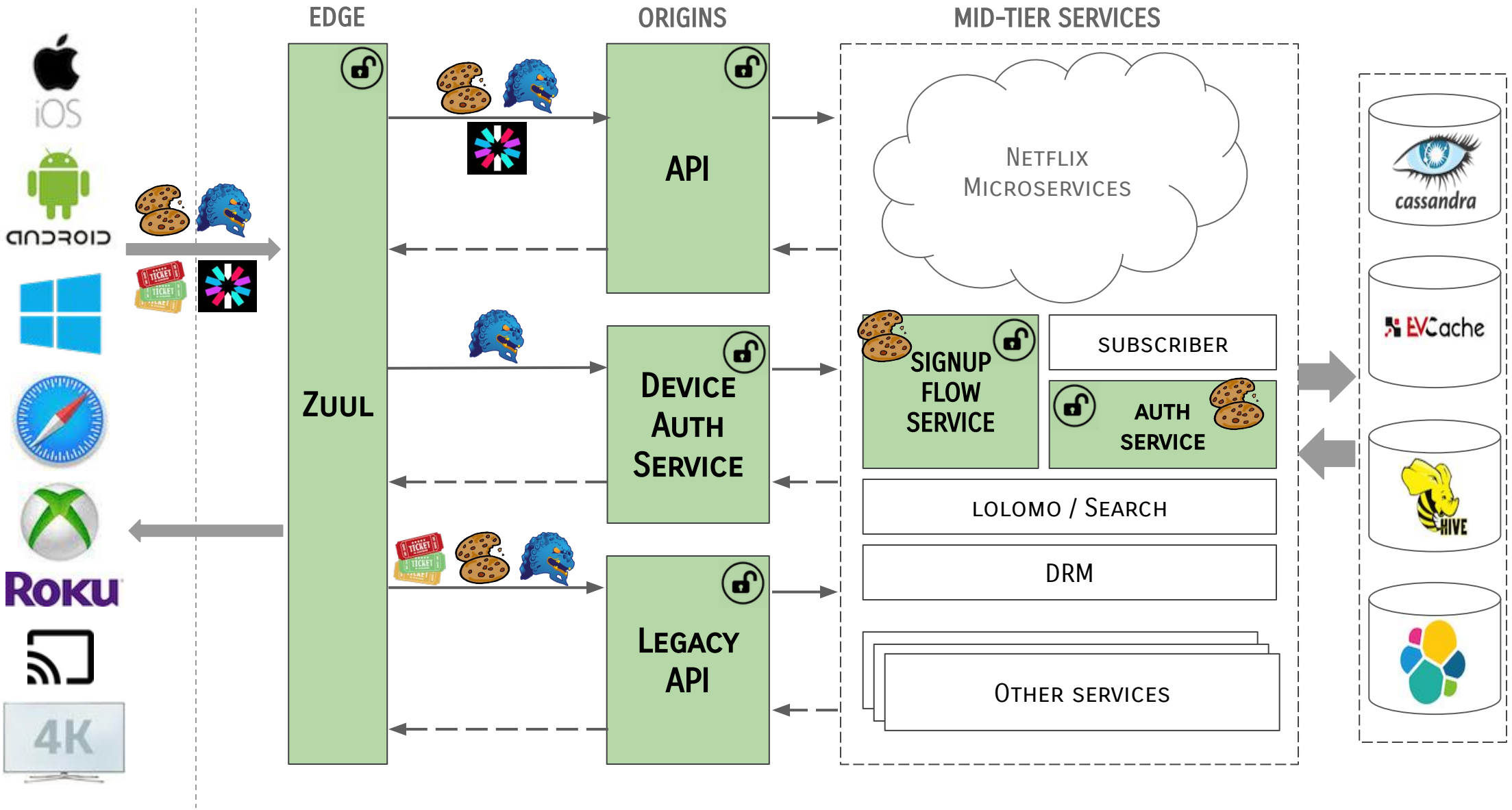
(JWS, JWE)

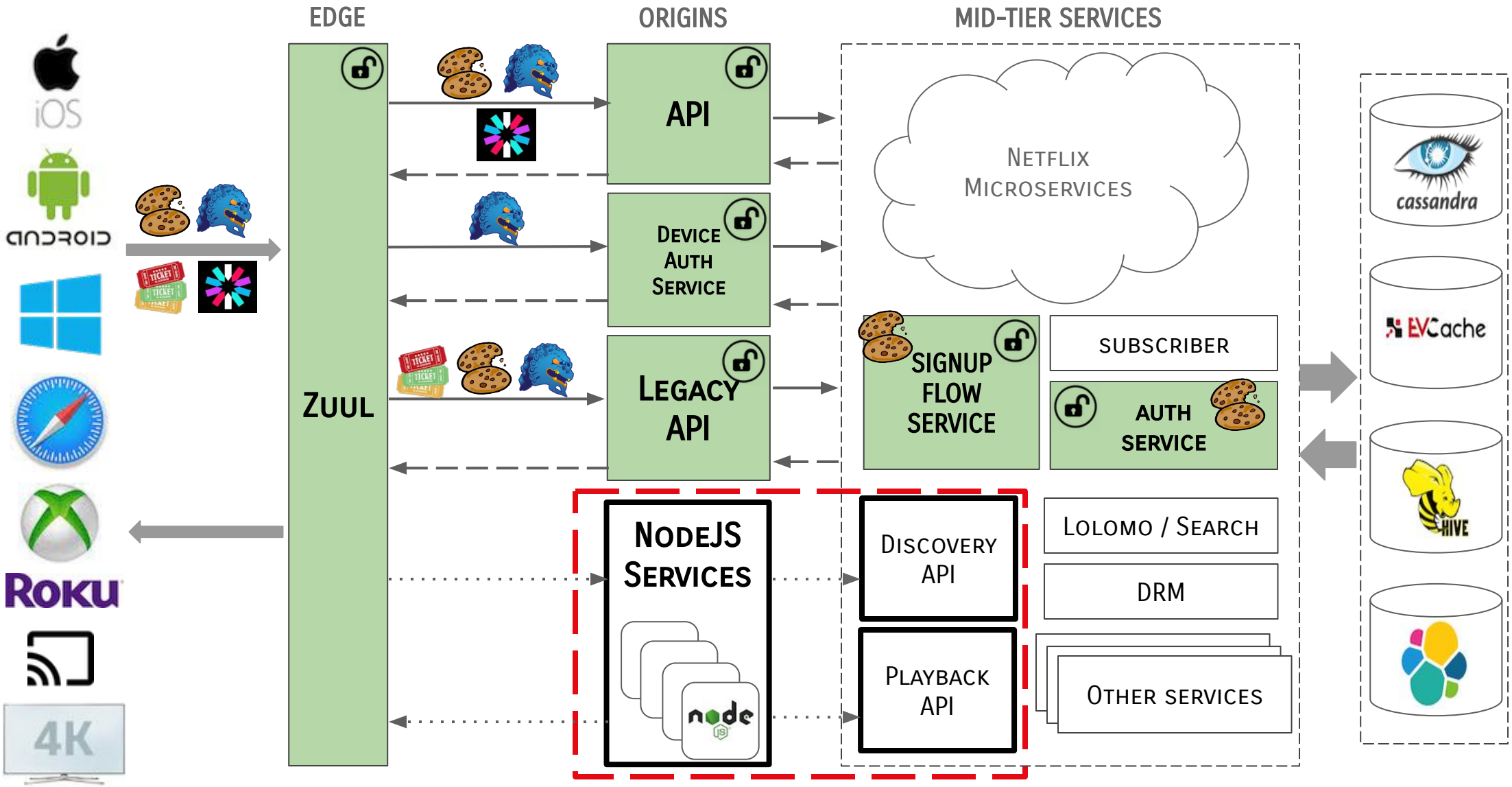
- Non-member experience


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE

Where we were

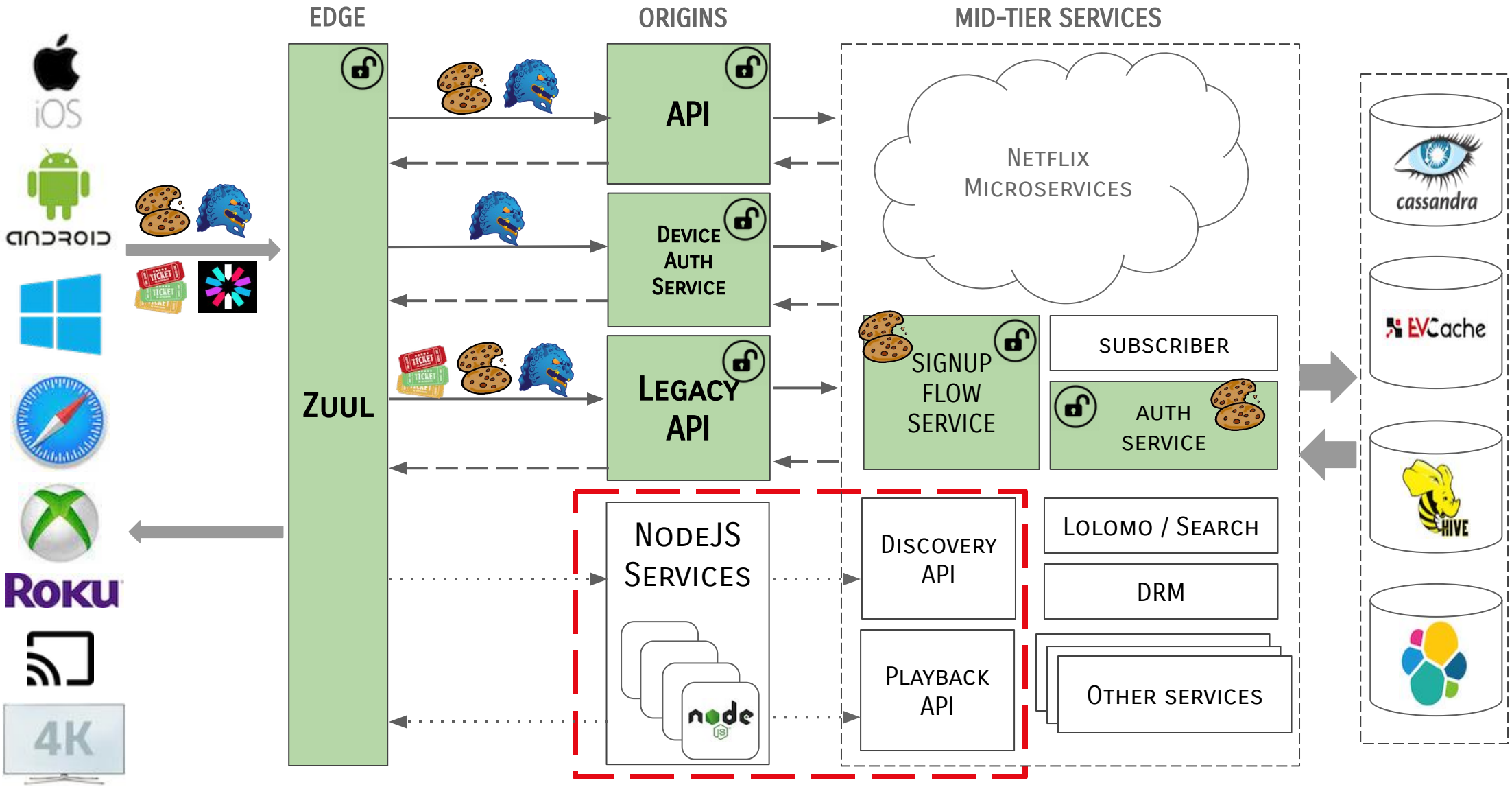
- Multiple services consuming auth tokens
- Multiple types of auth tokens
- Massive scale
- Inefficient, insecure & complicated

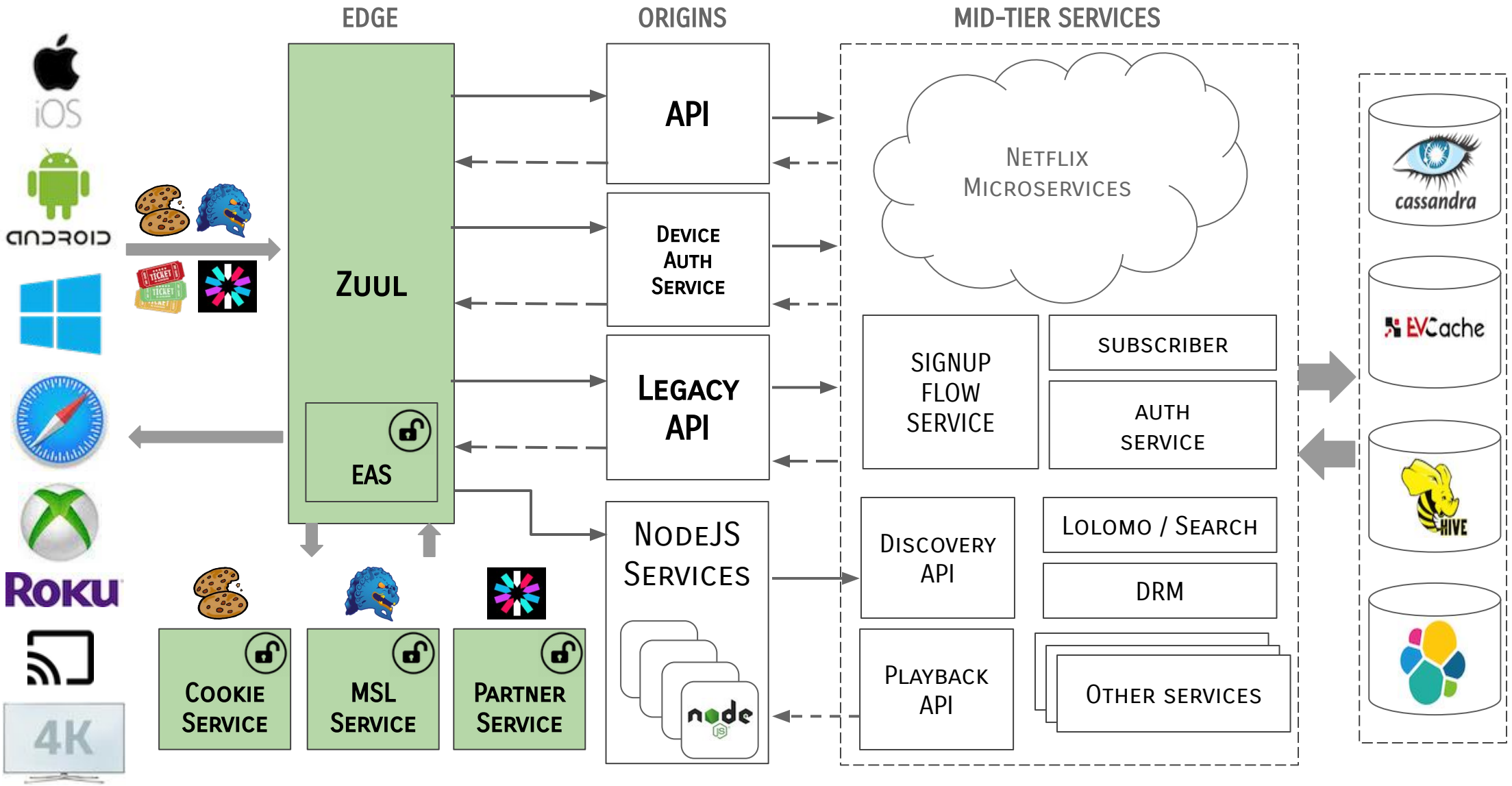

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE

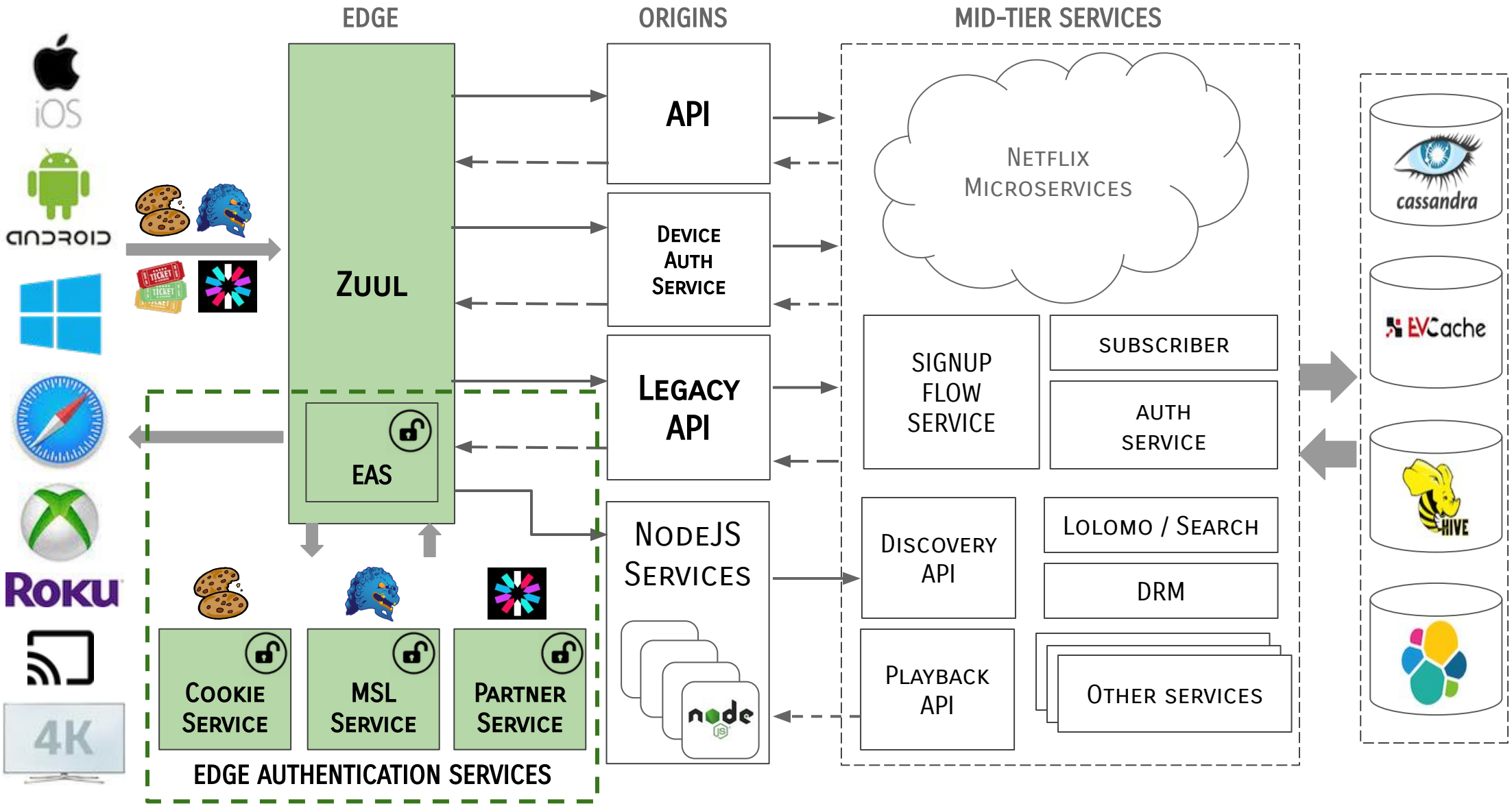

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
NODEJS SERVICES
DISCOVERY API
PLAYBACK API
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE

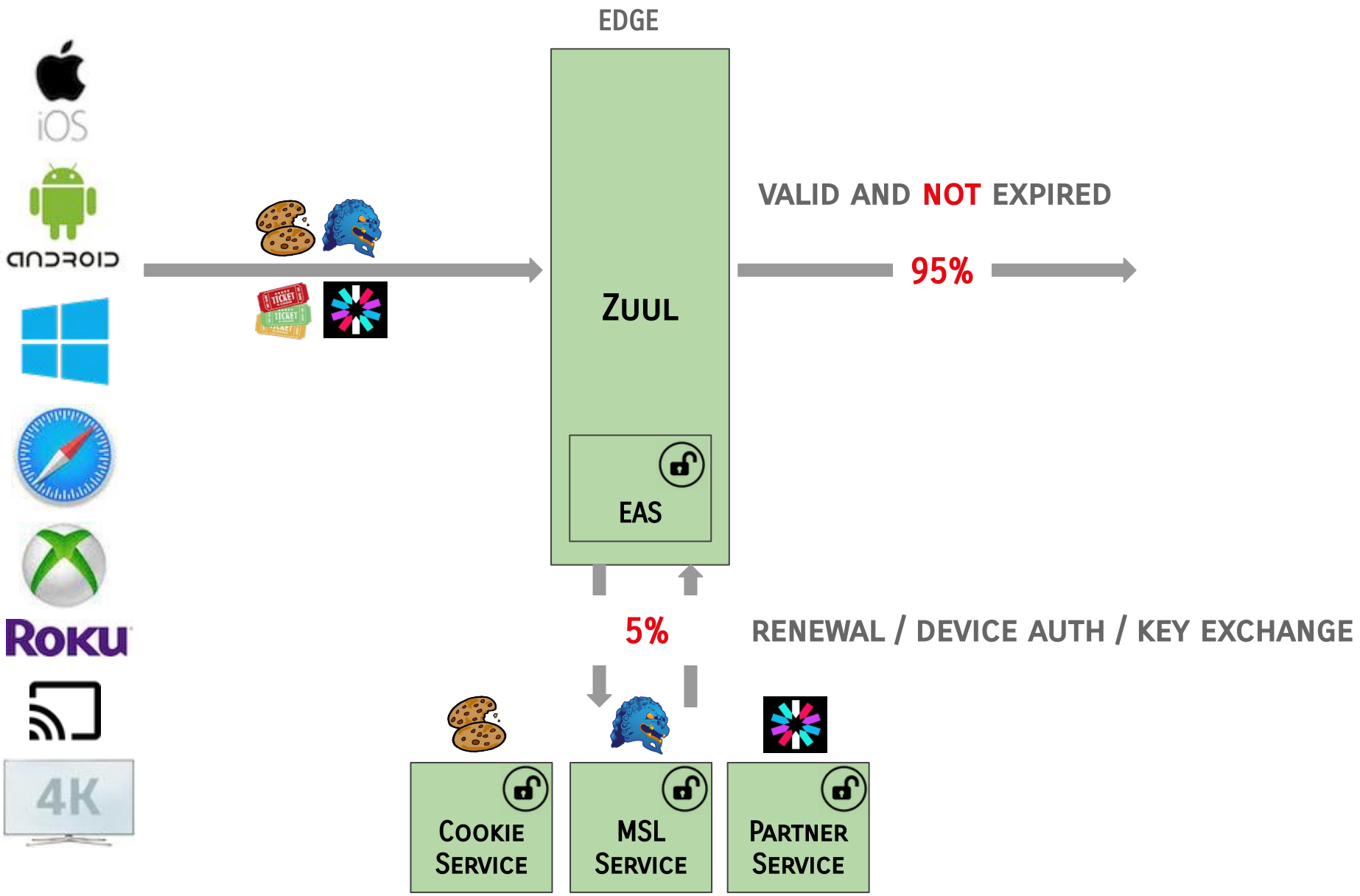
What we did

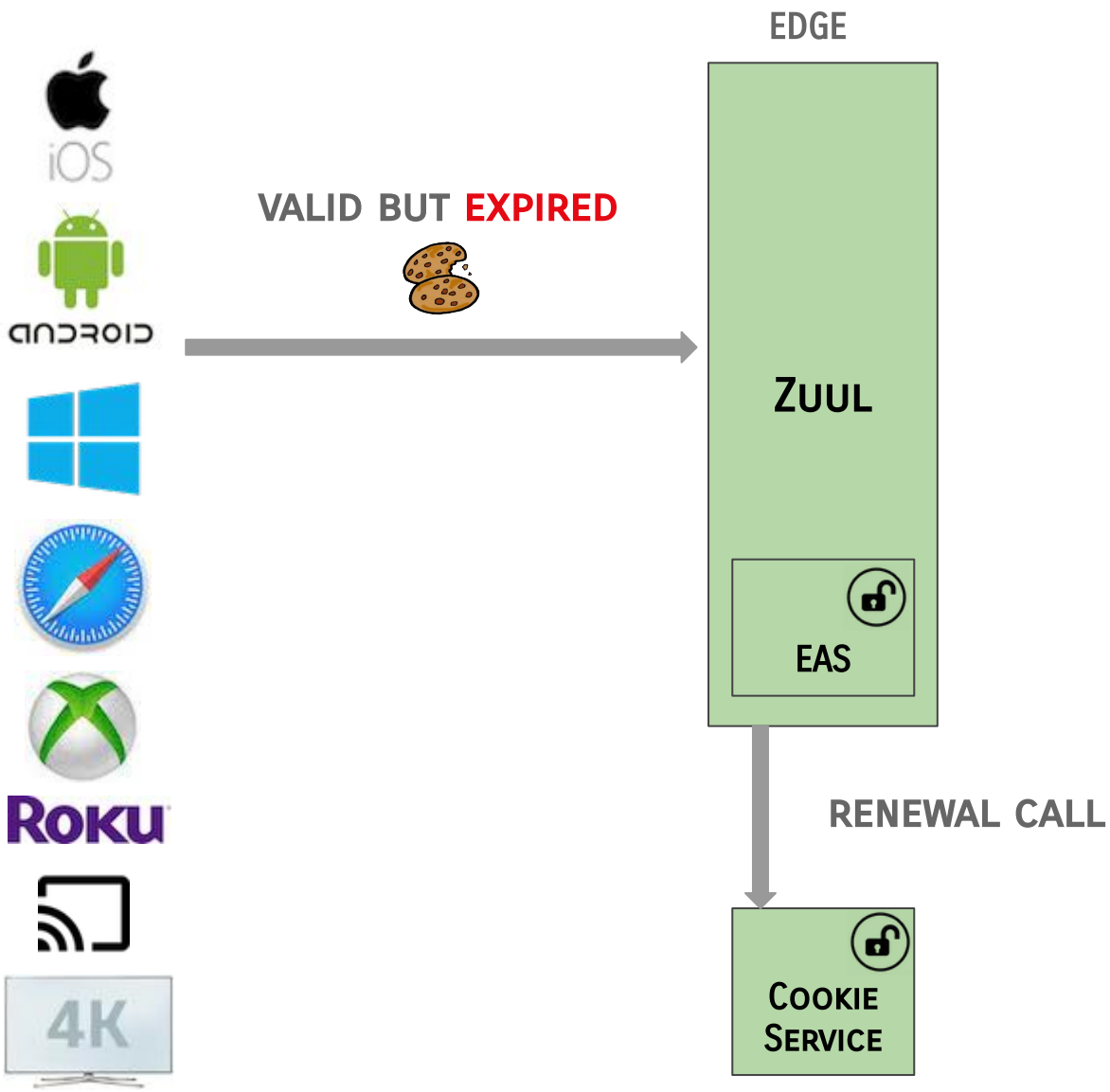
Moved authentication to the edge

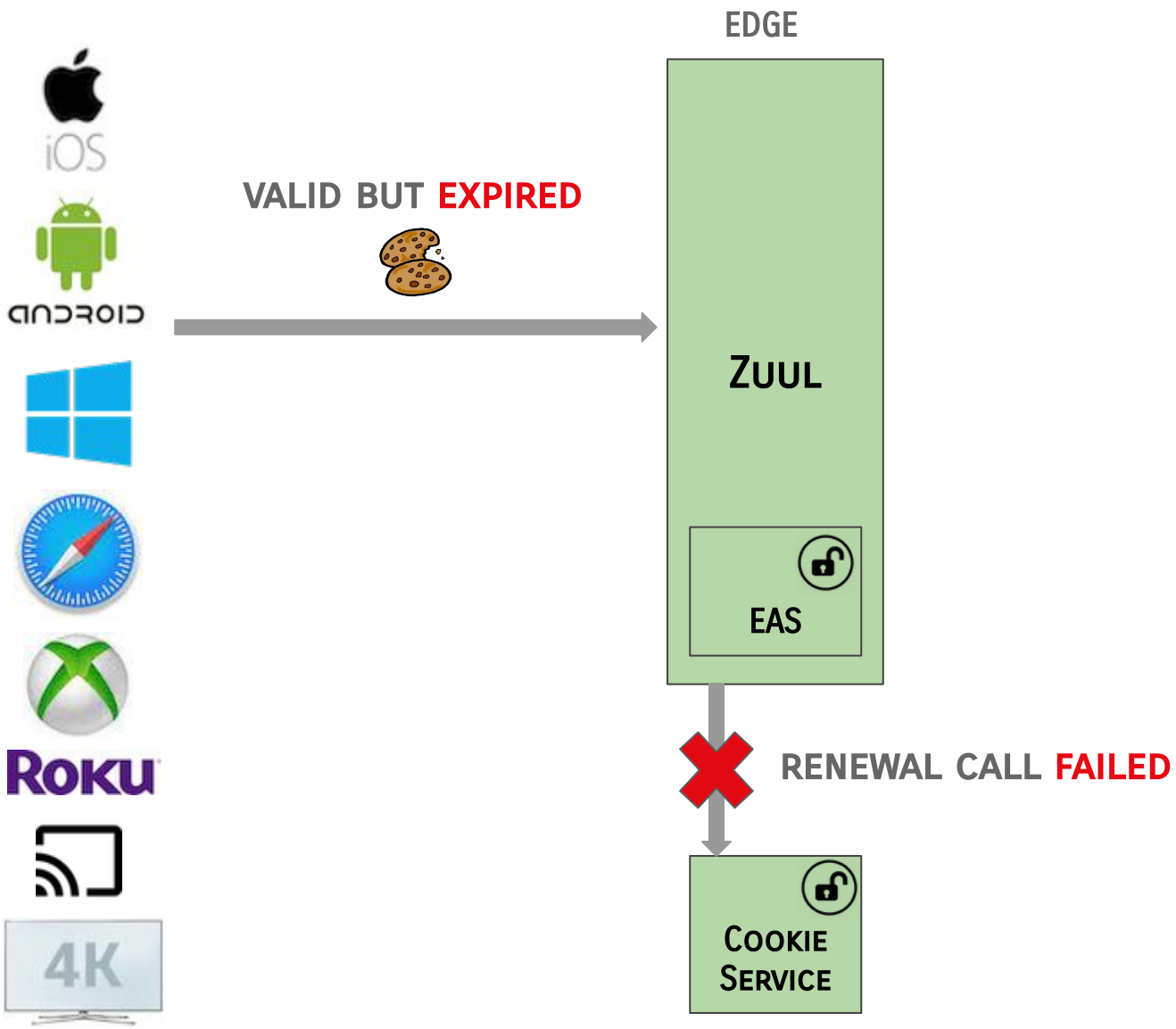

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
API
DEVICE AUTH SERVICE
LEGACY API
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
NODEJS SERVICES
DISCOVERY API
PLAYBACK API
LOLOMO / SEARCH
DRM
OTHER SERVICES
cassandra
EVCache
HIVE

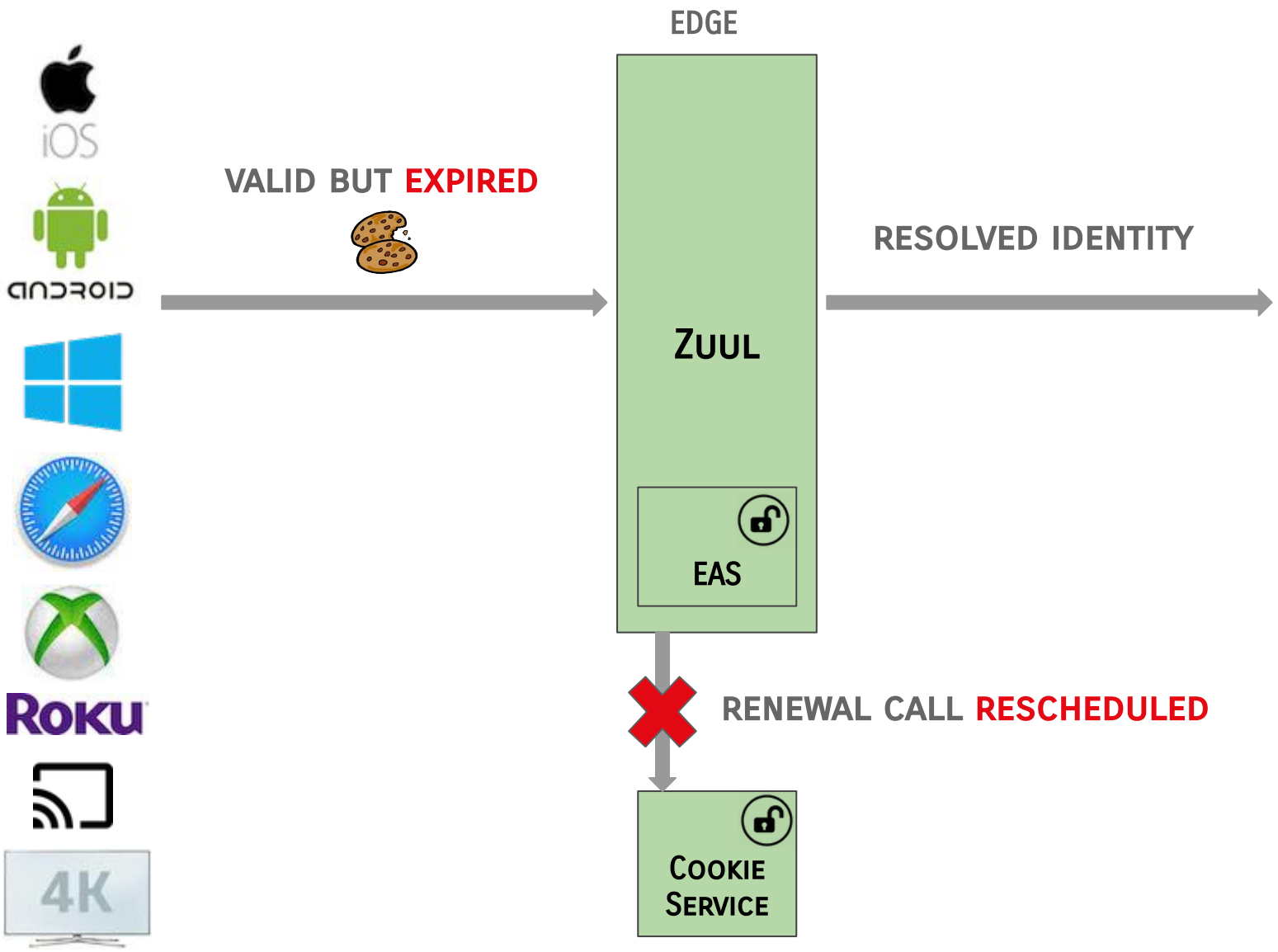

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
EAS
API
DEVICE AUTH SERVICE
LEGACY API
NODEJS SERVICES
node
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
DISCOVERY API
LOLOMO / SEARCH
DRM
PLAYBACK API
OTHER SERVICES
cassandra
EVCache
HIVE
COOKIE SERVICE
MSL SERVICE
PARTNER SERVICE

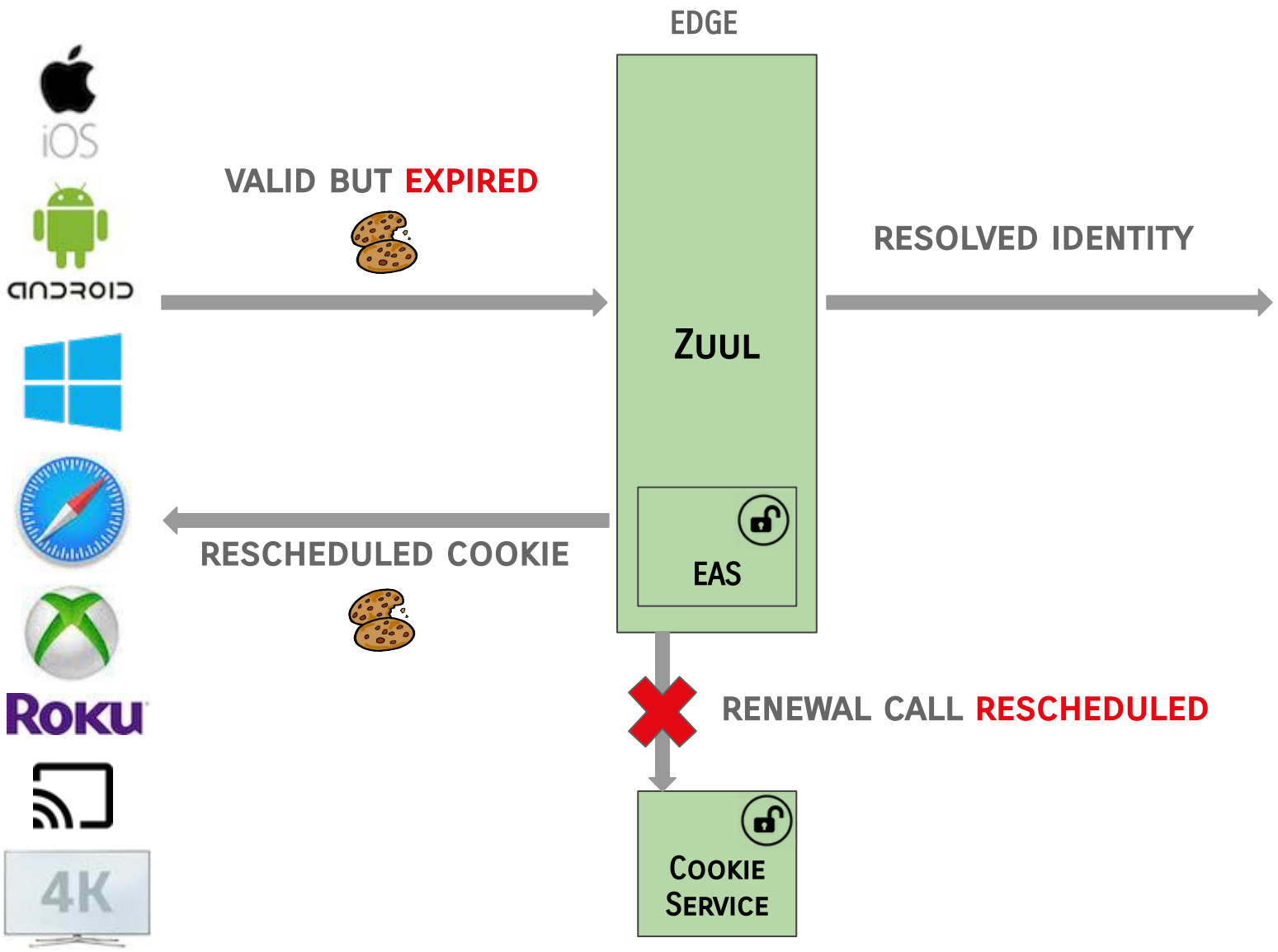

EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
EAS
API
DEVICE AUTH SERVICE
LEGACY API
NODEJS SERVICES
node
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
DISCOVERY API
LOLOMO / SEARCH
DRM
PLAYBACK API
OTHER SERVICES
cassandra
EVCache
HIVE
COOKIE SERVICE
MSL SERVICE
PARTNER SERVICE
EDGE AUTHENTICATION SERVICES

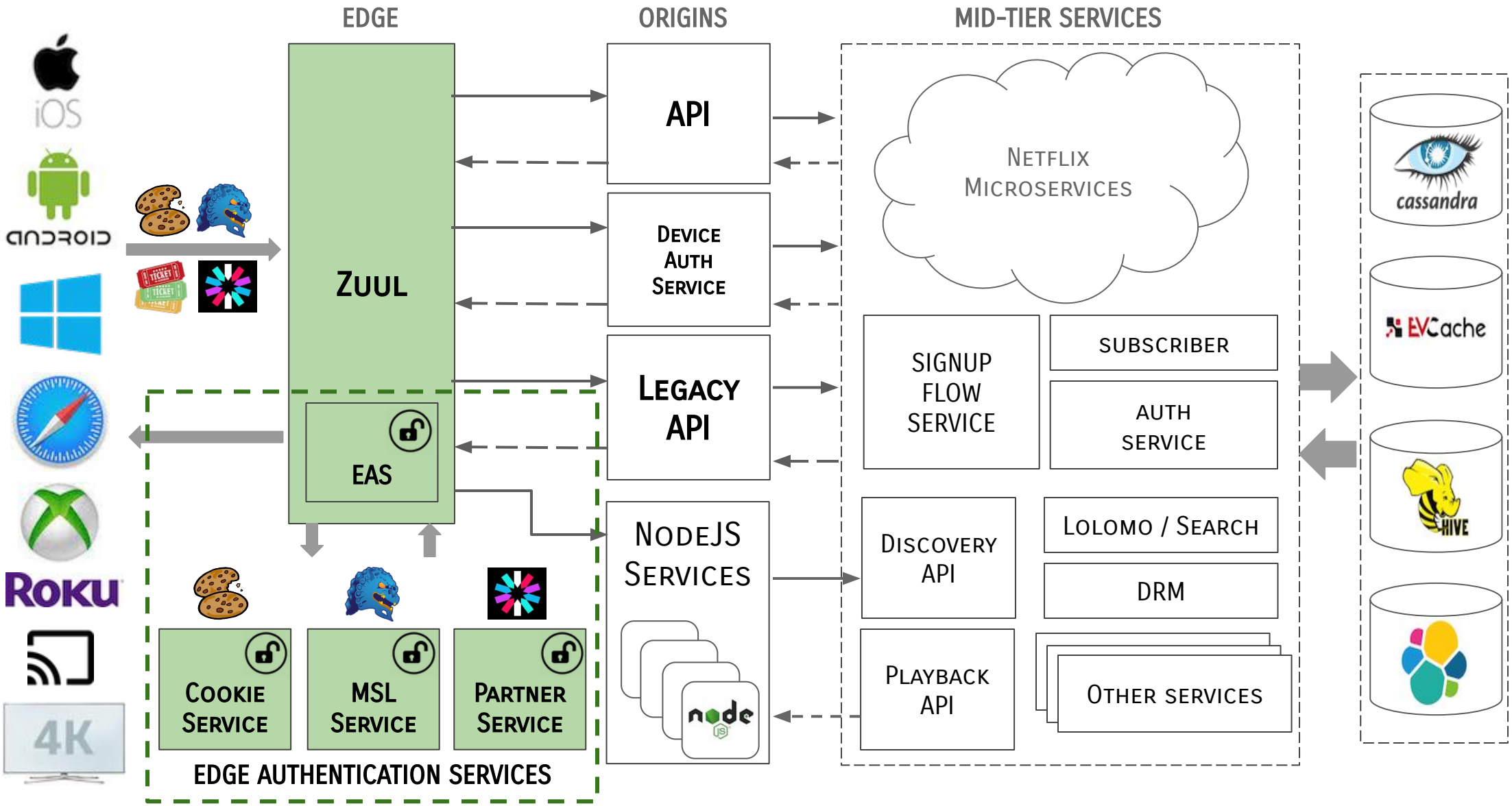

EDGE
iOS
ANDROID
ROKU
4K
ZUUL
EAS
VALID AND NOT EXPIRED
95%
5%
RENEWAL / DEVICE AUTH / KEY EXCHANGE
COOKIE SERVICE
MSL SERVICE
PARTNER SERVICE

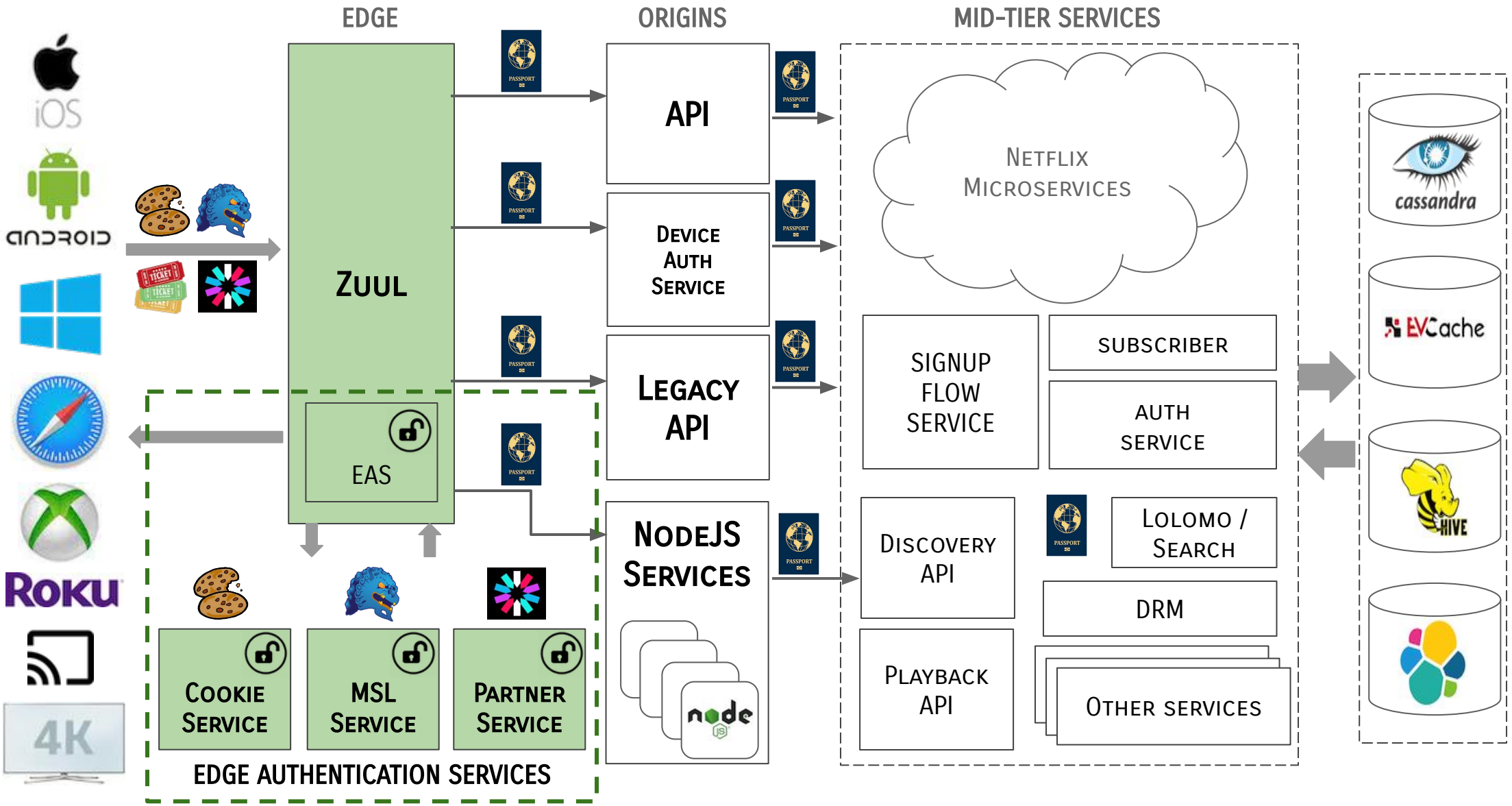

EDGE
iOS
ANDROID
VALID BUT EXPIRED
ZUUL
EAS
ROKU
RENEWAL CALL
4K
COOKIE SERVICE


EDGE
iOS
ANDROID
VALID BUT EXPIRED
ZUUL
EAS
ROKU
RENEWAL CALL FAILED
4K
COOKIE SERVICE


EDGE
iOS
ANDROID
ROKU
4K
VALID BUT EXPIRED
ZUUL
EAS
RESOLVED IDENTITY
RENEWAL CALL RESCHEDULED
COOKIE SERVICE


EDGE
iOS
ANDROID
ROKU
4K
VALID BUT EXPIRED
RESOLVED IDENTITY
ZUUL
EAS
RESCHEDULED COOKIE
RENEWAL CALL RESCHEDULED
COOKIE SERVICE


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
EAS
API
DEVICE AUTH SERVICE
LEGACY API
NODEJS SERVICES
node
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
DISCOVERY API
LOLOMO / SEARCH
DRM
PLAYBACK API
OTHER SERVICES
cassandra
EVCache
HIVE
COOKIE SERVICE
MSL SERVICE
PARTNER SERVICE
EDGE AUTHENTICATION SERVICES


EDGE
ORIGINS
MID-TIER SERVICES
iOS
android
Roku
4K
ZUUL
EAS
API
DEVICE AUTH SERVICE
LEGACY API
NODEJS SERVICES
node
NETFLIX MICROSERVICES
SIGNUP FLOW SERVICE
SUBSCRIBER
AUTH SERVICE
DISCOVERY API
LOLOMO / SEARCH
DRM
PLAYBACK API
OTHER SERVICES
cassandra
EVCache
HIVE
COOKIE SERVICE
MSL SERVICE
PARTNER SERVICE
EDGE AUTHENTICATION SERVICES

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

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

- Consumers create **`passportIntrospector`** from binary passport data

```
factory.createIntrospector(passport);
```

Tooling

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

TEST PROD

Decrypt Passport

CrUfCgUxLjAuMBKrHwoKCghhcGlwcm94eRJCCAESEFBBU1NQT1JUX01BQ19LRVkaLAEBA_cAAQEgEg6mzMut89pl6kgehiIpPh22504eQzo4jfhYBIwd9yAn7dv1GjkIAxDw56So3y0iJgokU0xXMzItRIU3NFRYOEFRUDRRMzFLSFBQWUcyOVI1VzU4SkxSKgIIDEADSgAiQggBEhBQQVNTUE9SVF9NQUNfS0VZGiwBAQP3AAEBIBQuWplHu1Q51JfKQuRvh2fvBUiBUS2QhIDBXHXNGIfSWy_o6yrZHQgDEMPopKjfLSIKCMq998Cdu62AAyocChpLNEI0U1hQVVhGQ1hGQVJPRVJPVzYzRU1BVTIKCMq998Cdu62AAzocChpLNEI0U1hQVVhGQ1hGQVJmwKCwgDGgcI9uekqN8tGgAiWAoKCMq998Cdu62AAxIKCMq998Cdu62AAxoQUEFTU1BPUlRfTUFDX0tFWSIsAQED9wABASDSKMWBLPop3rtxZaLN5Fnj02Eo57BtS8d0jNqS-w==

Decrypt

User Info

customerId	2163727293
acctOwnerId	2163727293
customerGuid	K4B4SXPUXFCXFAROE
acctOwnerGuid	K4B4SXPUXFCXFAROE
source	MSL
authenticationLevel	HIGHEST
created	10/22/2019 12:54:44 PDT

Device Info

esn	SLW32-FU74TX8AQP4Q31KHPPYG
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;
    ...
}
```

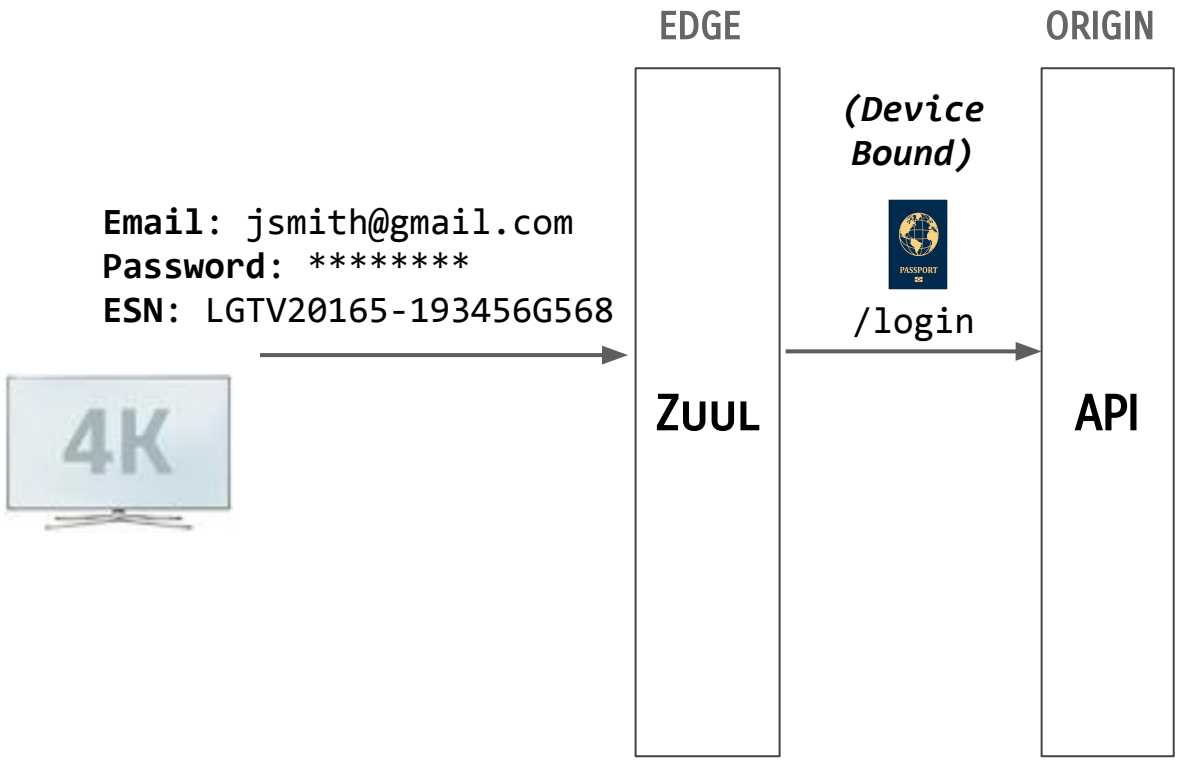
- **Explicit signal** sent by the downstream services, when an **update** to user or device identity has been performed
- This "signal" is used by EAS to either **create** or **update** the corresponding type of **token**

Passport Action

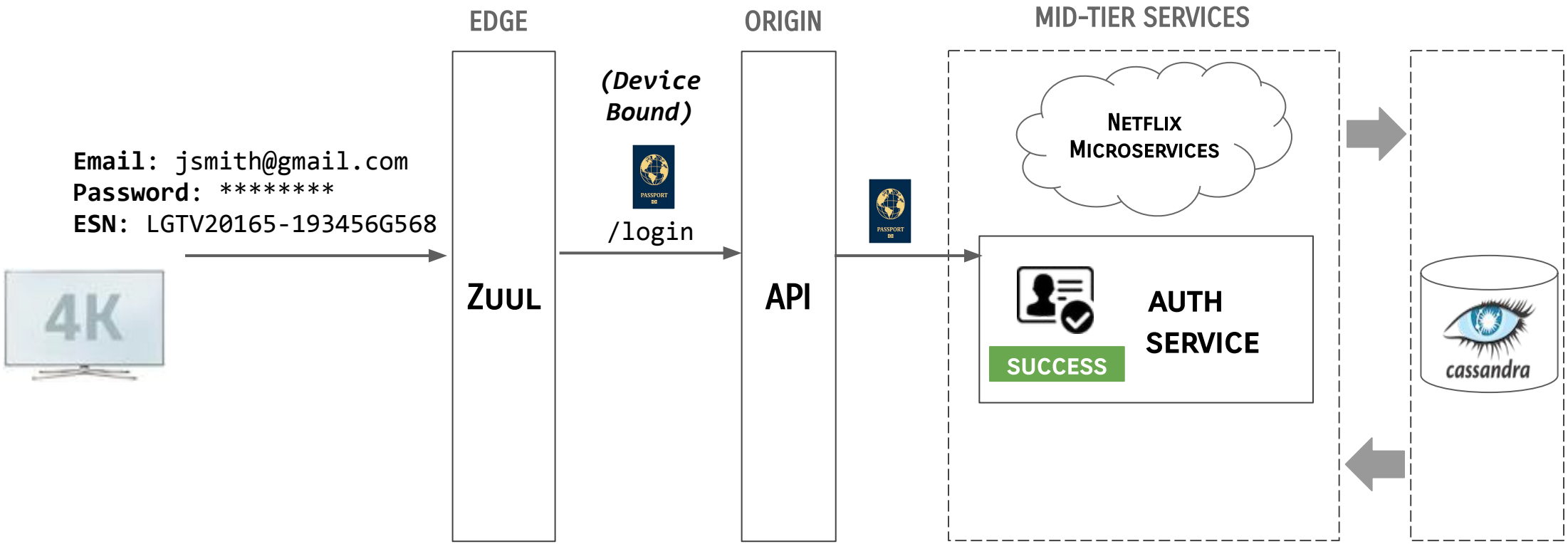
Passport Action: User Login

Passport Action: User Login

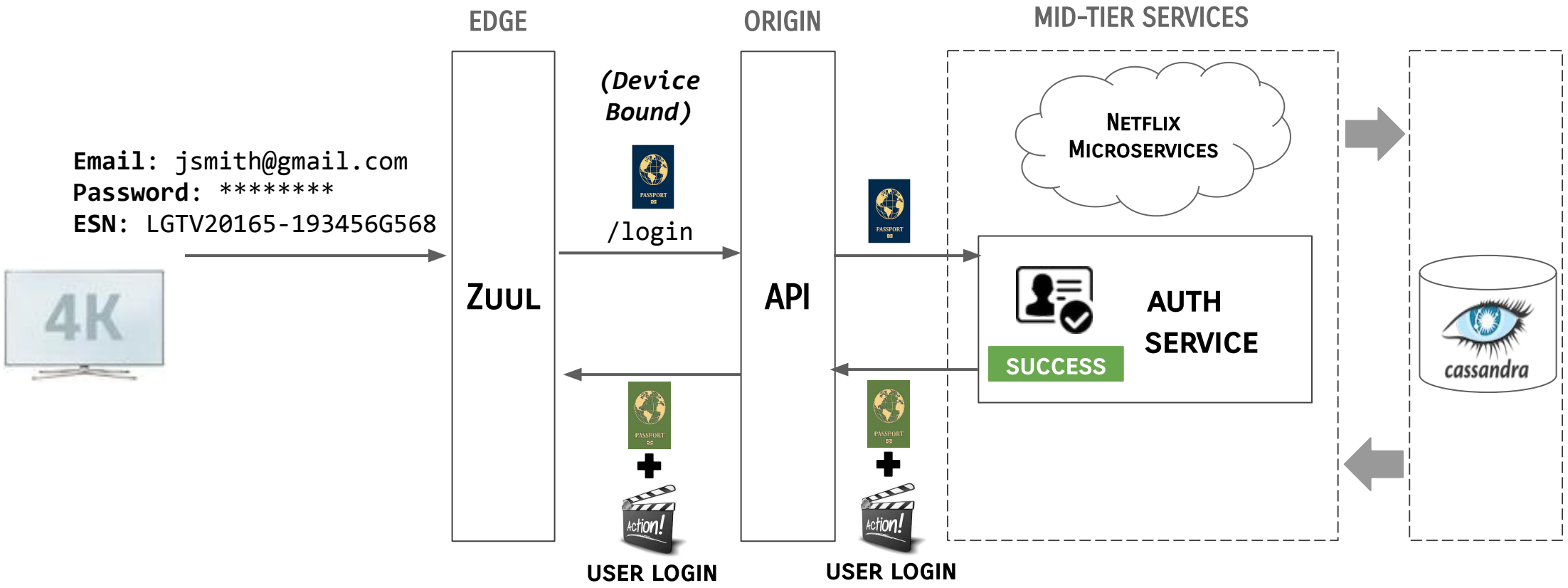
Passport Action: User Login



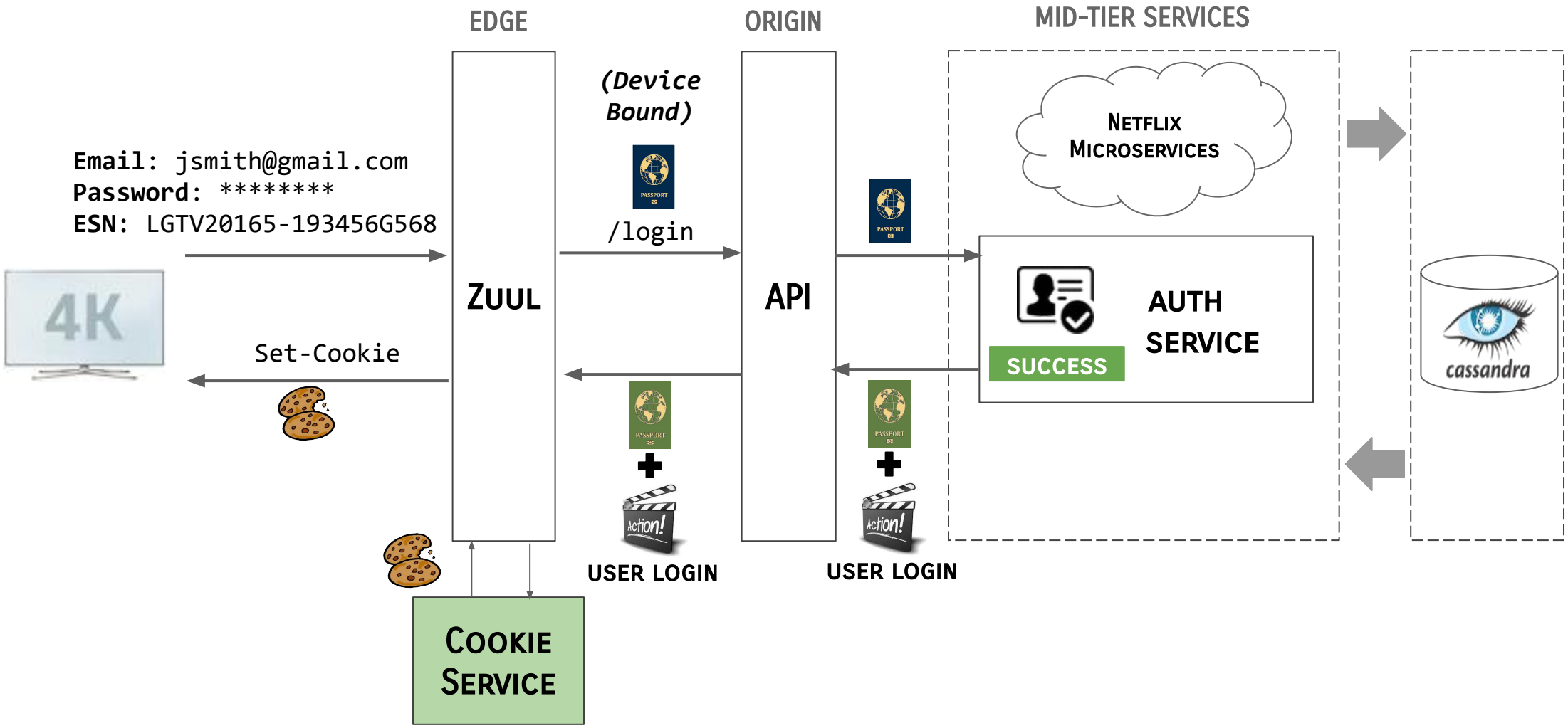
Passport Action: User Login



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

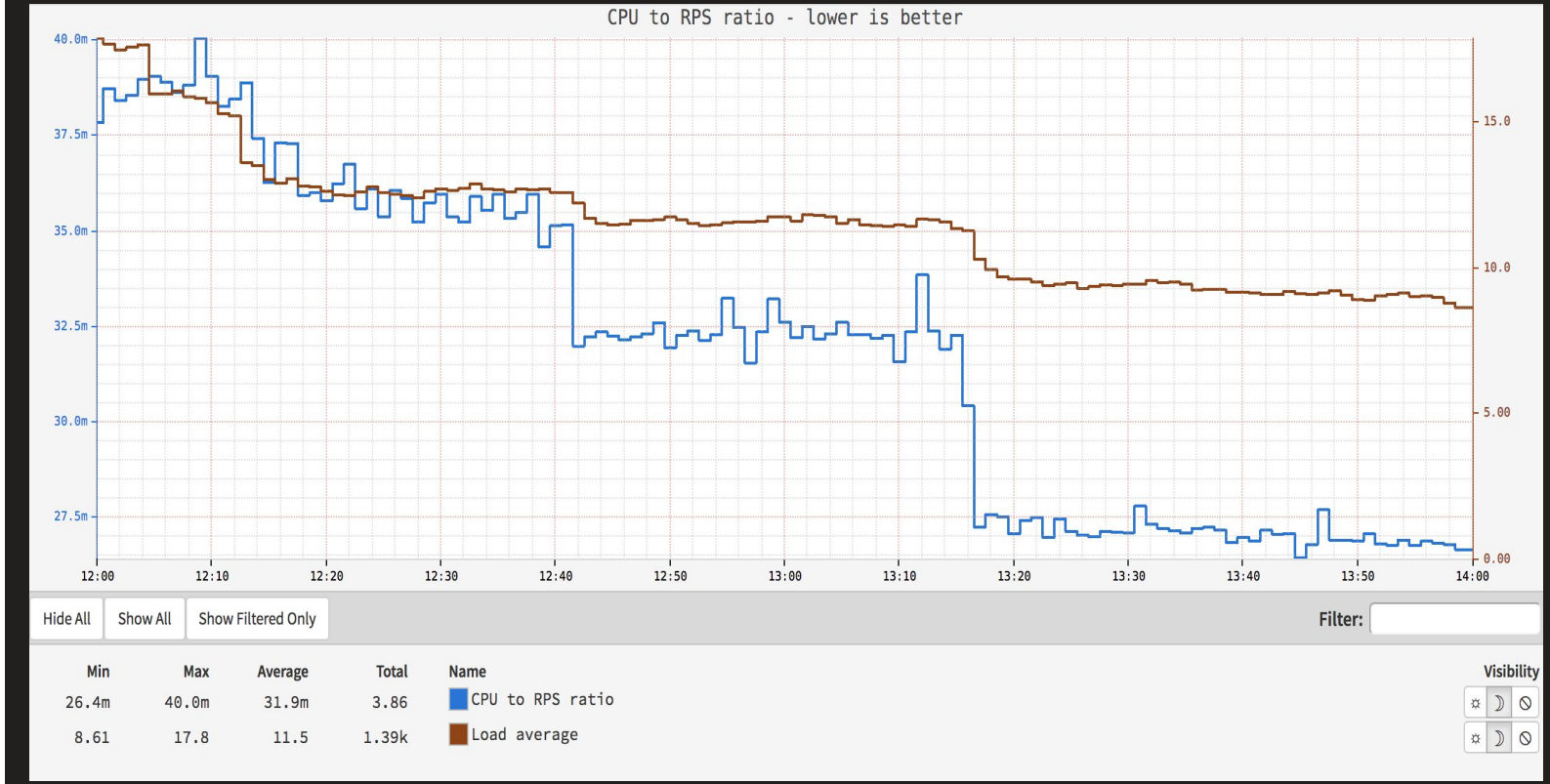
Offloaded token processing which resulted into significant gains for

- CPU
- Request Latency
- GC
- Cluster Footprint

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

Offloaded & Fine Tuned

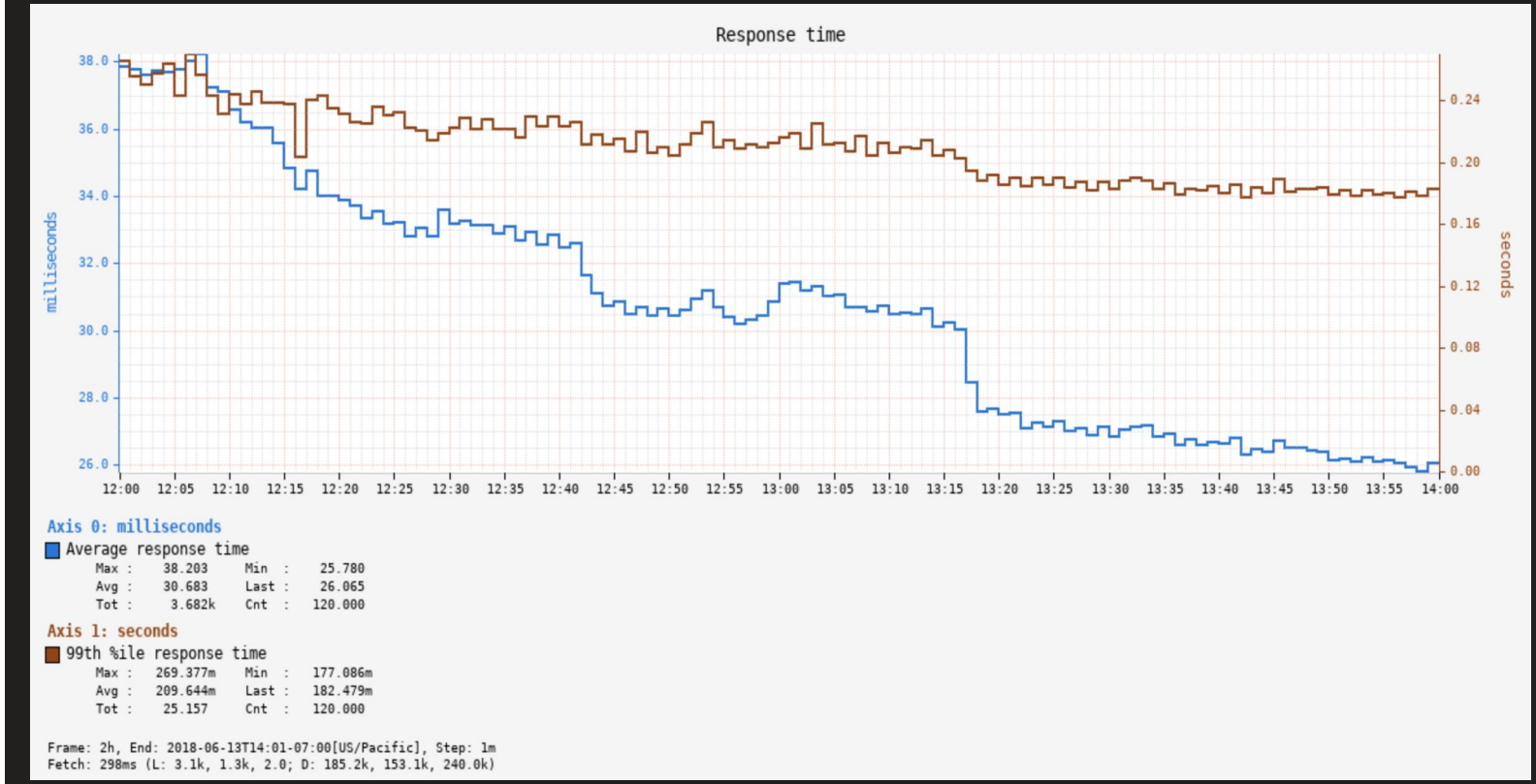
- 30% reduction in CPU cost per request
- 40% reduction in load average



CPU to RPS ratio for API instance

Offloaded & Fine Tuned

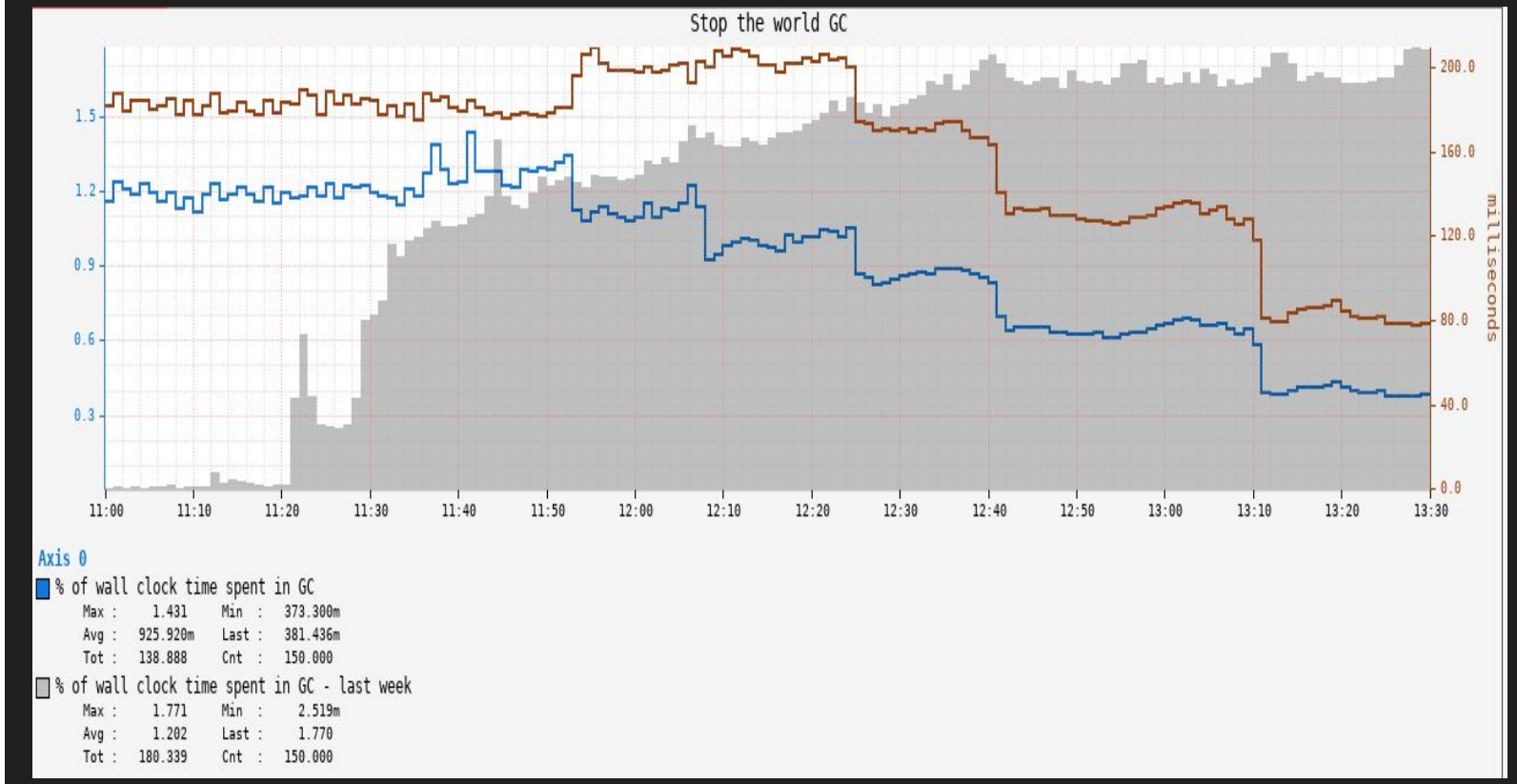
- 30% reduction in average latency
- 99th percentile latency dropping by 20%



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 Thadeshwar
sthadeshwar@netflix.com
https://www.linkedin.com/in/satyajit-thadeshwar