# BNL activities on federated access and SSO.

Tejas Rao

Spring HEPIX, San Diego, CA

March 26th 2019.

In collaboration with : Jamal Irving, Mizuki Karasawa.

BROOKHAVEN NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

# Motivation

- Individual experiments were having individual Kerberos realms. – RHIC, ATLAS, SDCC.
- Management of individual realms was getting difficult.
- Some users had multiple accounts and passwords.
- Shibboleth configuration and management is complex.
- There was a desire for SSO and Federated access for applications like Invenio, Indico, Jupyter, BNLbox and various other web services.

Needs –

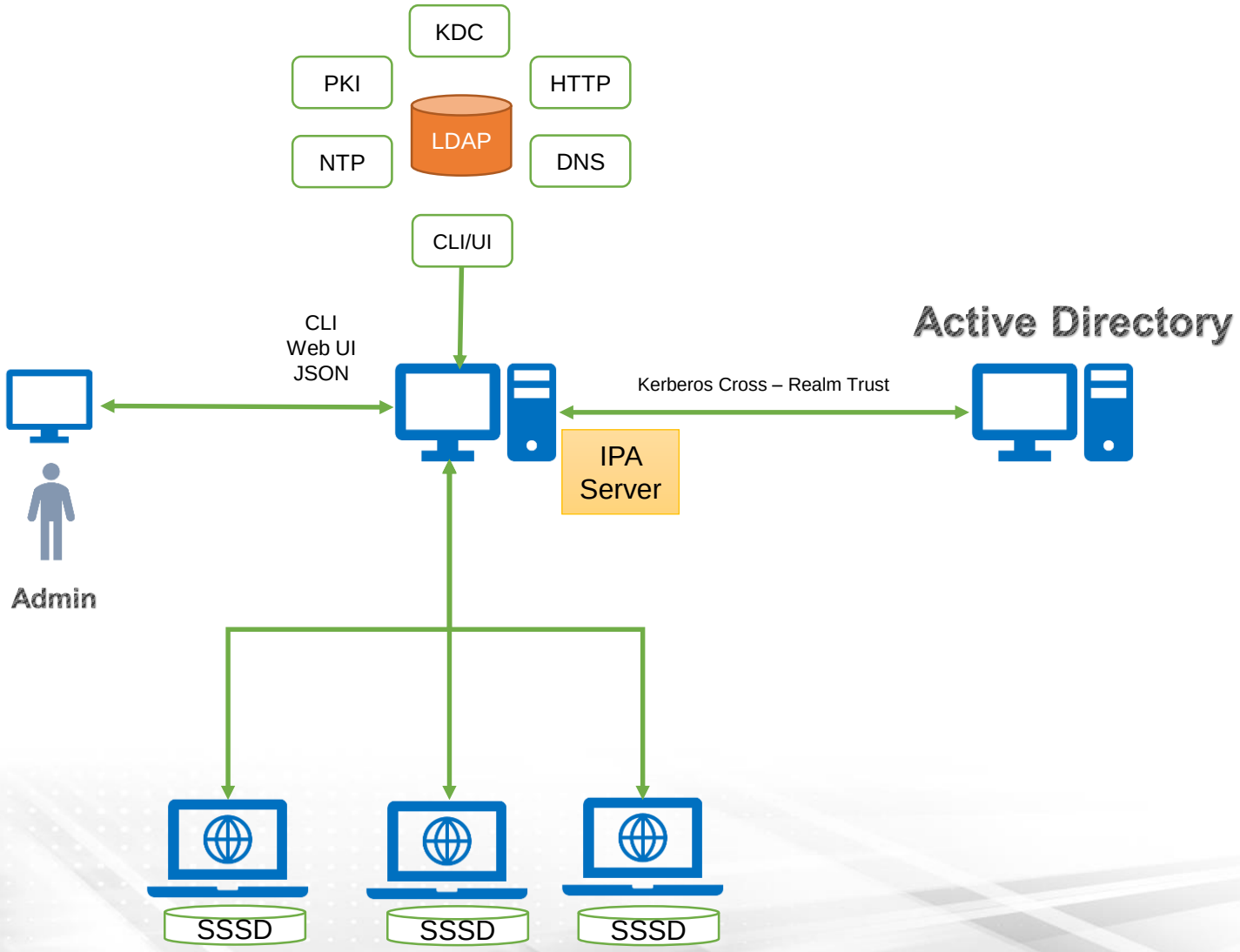
- Single source of Identities. (duplication = confusion)
- Single point of management (comprehensive view)
- Single –Sign on /Single password.
- No single point of failure.
- Automated synchronization and integration.
- Integrated management interfaces.
- Easy distribution of data and credentials.

- We decided to migrate to RedHat Identity management solution (IPA) and completed migration in late 2018.
- For SSO, we will likely switch to Keycloak from Shibolleth.

# RedHat - Identity Management (IPA)

- Integrated into Red Hat Enterprise Linux for versions 6.2 and later.
- Easy installation and setup ipa-{server,replica,client}-install commands.
- Redundancy - multi-master replication, read-only replicas.
- Manages users/user groups, hosts/host groups, services in a central location.
- Defines Policies, HBAC (host-based access control) rules.
- Rich CLI & Web UI for the ease of identity management.
- MFA (Multi-Factor-Authentication) enabled.
- Utilizes SSSD as client-side tool for federation including cross-realm trust with Active Directory (AD), identity operations, rule enforcement, caching, offline support etc.
- Cross-realm trust with Active Directory (AD).

# IPA architecture



# USER MIGRATION FROM OpenLDAP TO IPA

- Merged multiple Kerberos domains (ex, RHIC, ATLAS etc) into one single domain:

SDCC.BNL.GOV.

- Converted users/groups accounts from OpenLDAP into IPA based under new domain tree:dc=sdcc,dc=bnl,dc=gov.
- Modified user creation programs & user auditing programs to be IPA compliant.
- Reconfigured ldap client (nslcd & nscd) at the machine level (ex, Linux Farm nodes etc).
- Reconfigured existing Web authentication mechanism with Shibboleth to be IPA compliant.
- Created migration websites for user Kerberos password changing & enabled the same functions on SSH gateways.
- Ensured HPSS for data archival and retrieval continued to work.

# IPA in Production

- Currently we have 12 IDM servers supporting about 5200 linux clients.
- IPA master,replicas, clients fully puppetized (PuppetForge).

- Tunning -
  - “/etc/dirsrv/slapd-SDCC-BNL-GOV/dse.ldif” - nsslapd-maxdescriptors=32768
  - “/etc/sysconfig/dirsrv.system” - LimitNOFILE=32768

# Keycloak

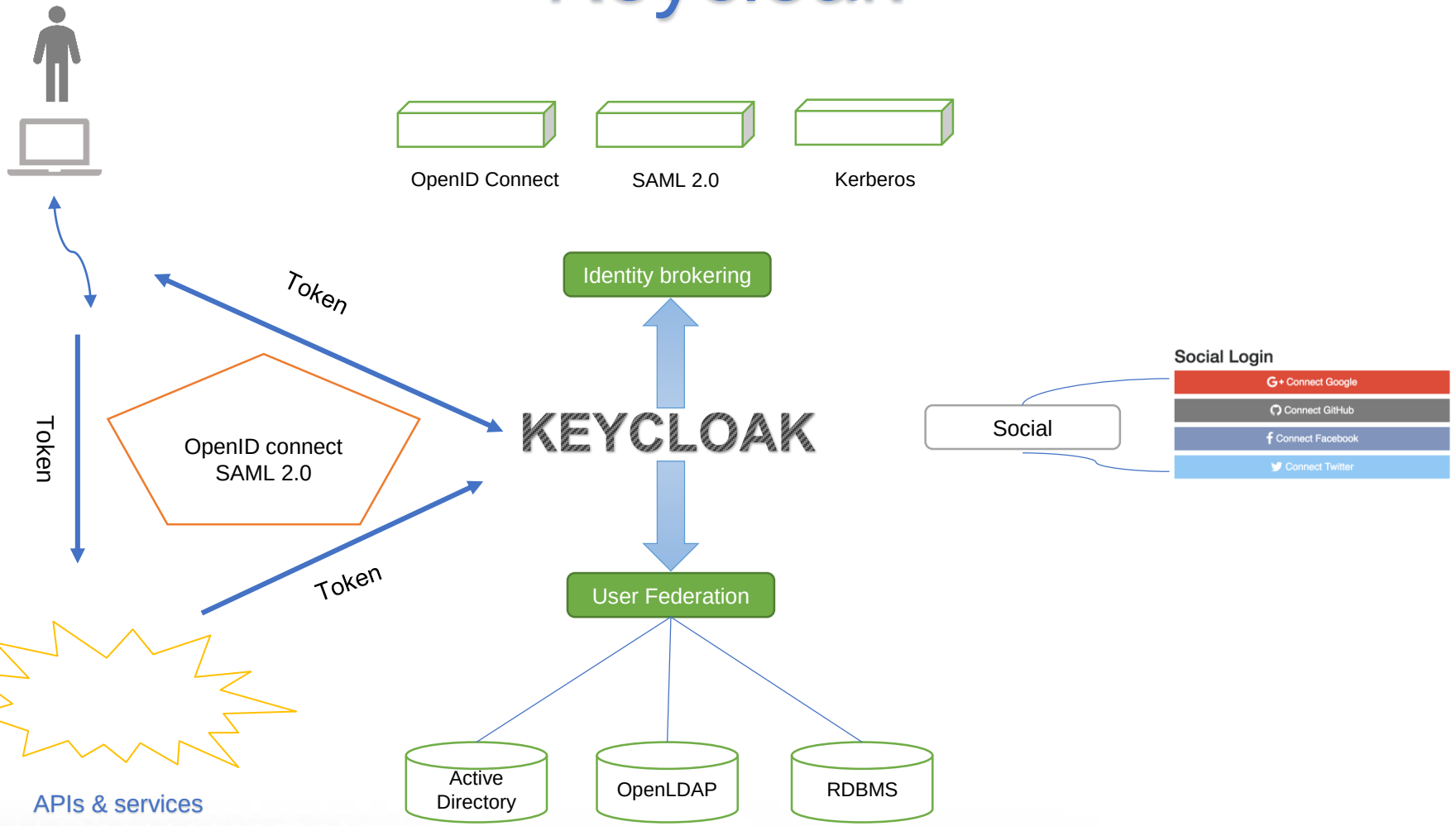
- Keycloak deals with authentication.
- Two factor authentication is very simple to setup.
- Single Sign On.

- Protocols
  - OpenID connect
  - SAML 2.0.

- Keycloak aims to be a out of the box service.
- Clustering.
- Scalability.
- High Availability.

- Theming of the authentication page.
- Identity brokering.

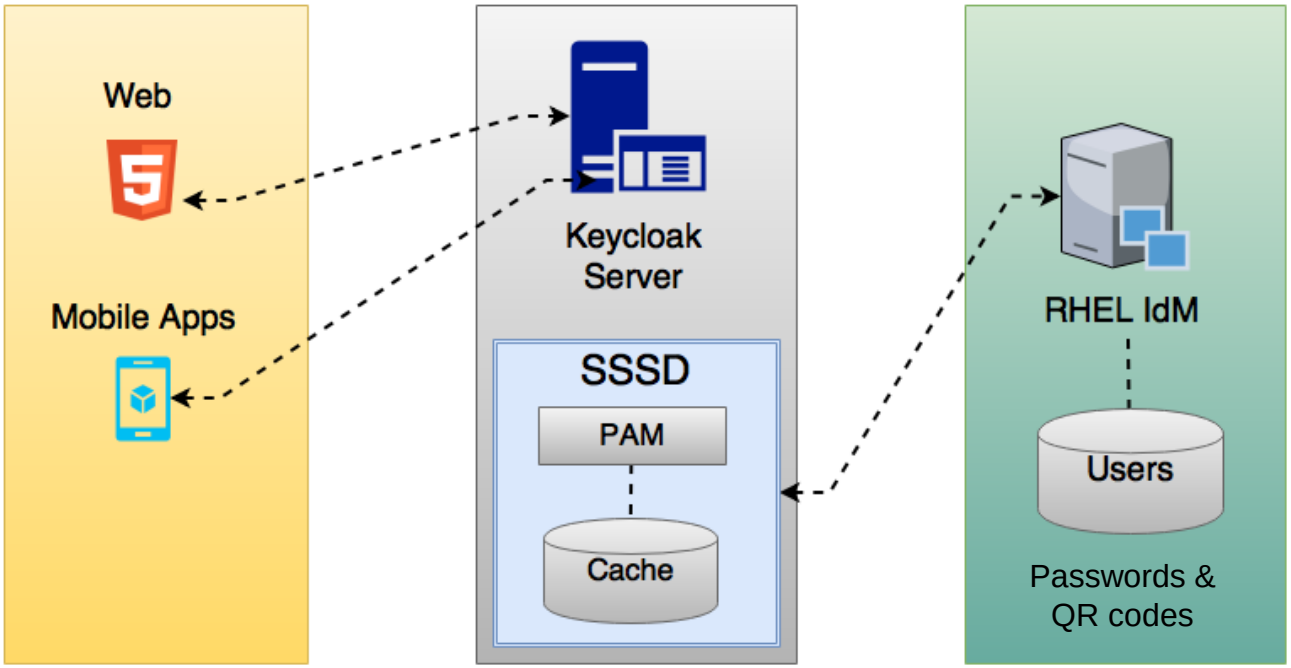
# Keycloak


OpenID Connect
SAML 2.0
Kerberos
Identity brokering
Token
Token
OpenID connect
SAML 2.0
KEYCLOAK
Social
Social Login
Connect Google
Connect GitHub
Connect Facebook
Connect Twitter
Token
User Federation
APIs & services
Active Directory
OpenLDAP
RDBMS

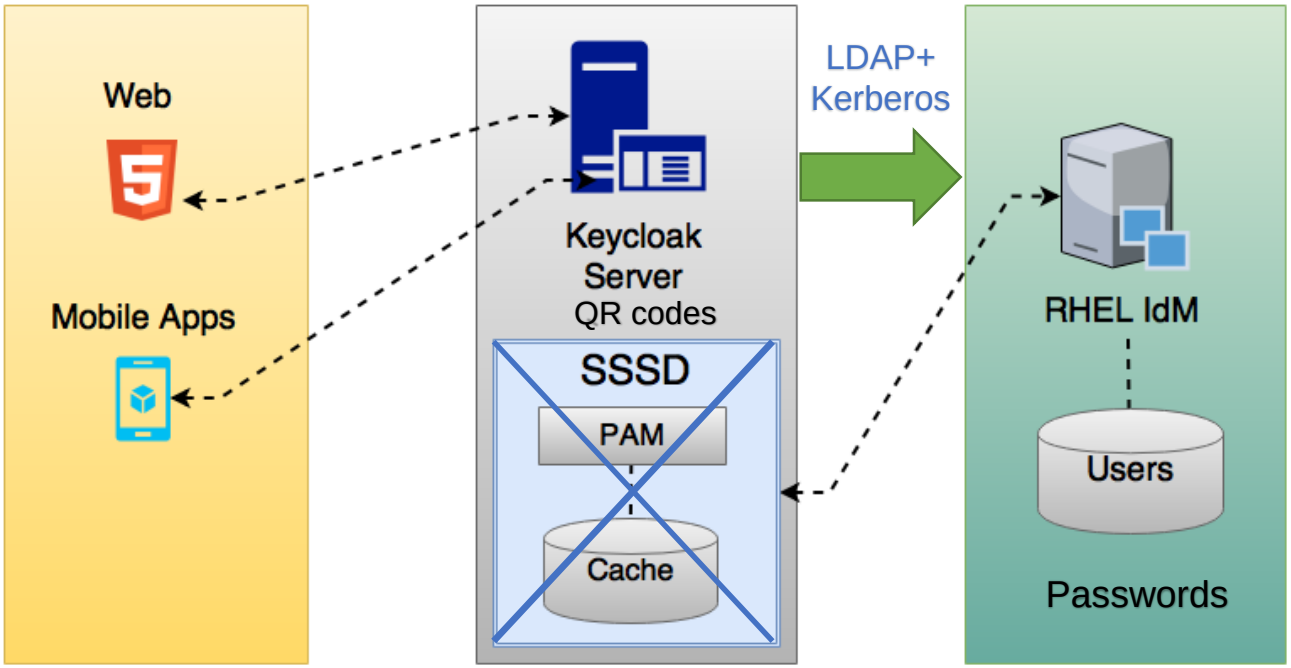
# SHIBBOLETH VS KEYCLOAK

- Shibboleth is SAML based, Keycloak support both SAML 2.0 & OpenID Connect protocols for authentication.
- KeyCloak provides social network logins, acts as identify brokering authenticating with existing identity providers via SAML or OIDC
- Simple and agile application configuration management with KeyCloak.
- KeyCloak provides authorization services aside from AuthZ with Apache
- Identity management is required for Keycloak.

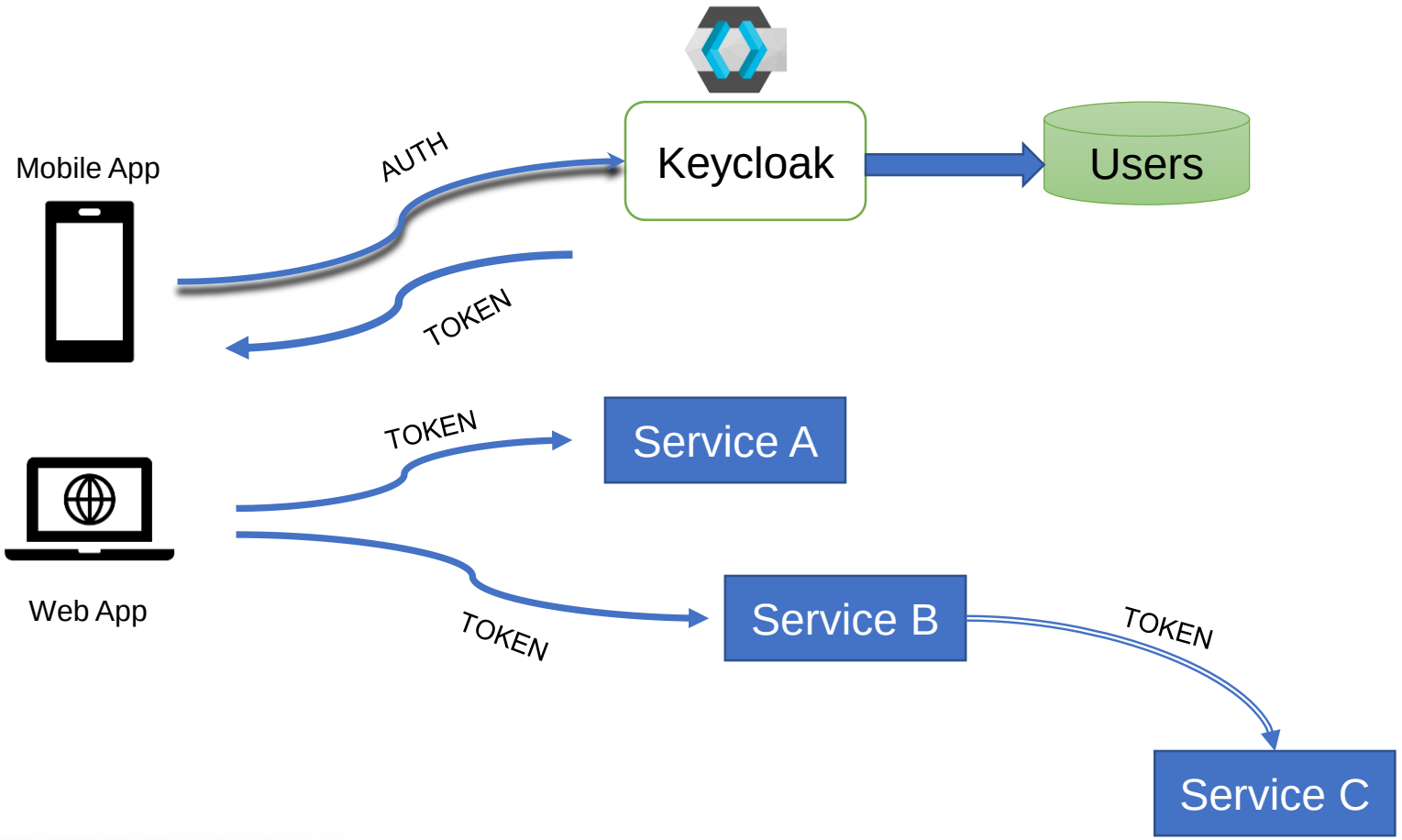
# ENABLING MFA OPTION A: (USING IPA OTP)



# ENABLING MFA OPTION B: (USING KEYCLOAK OPT)



# Keycloak Workflow



# Status

- Invenio test prototype now has federated access setup with CILogon and Keycloak.
- SDCC GPFS Globus endpoint has federated access setup with CILogon.
- Jupyter test instance has MFA access enabled using Keycloak QR codes.

- Will be implemented soon.
  - Production instance of Keycloak server.
  - BNLbox needs SSO and federated access enabled.
  - Indico needs federated access enabled.

- Contact –

  Mizuki Karasawa.
  mizuki@bnl.gov

# Thank You