AWS Foundation

Security – IAM Part II

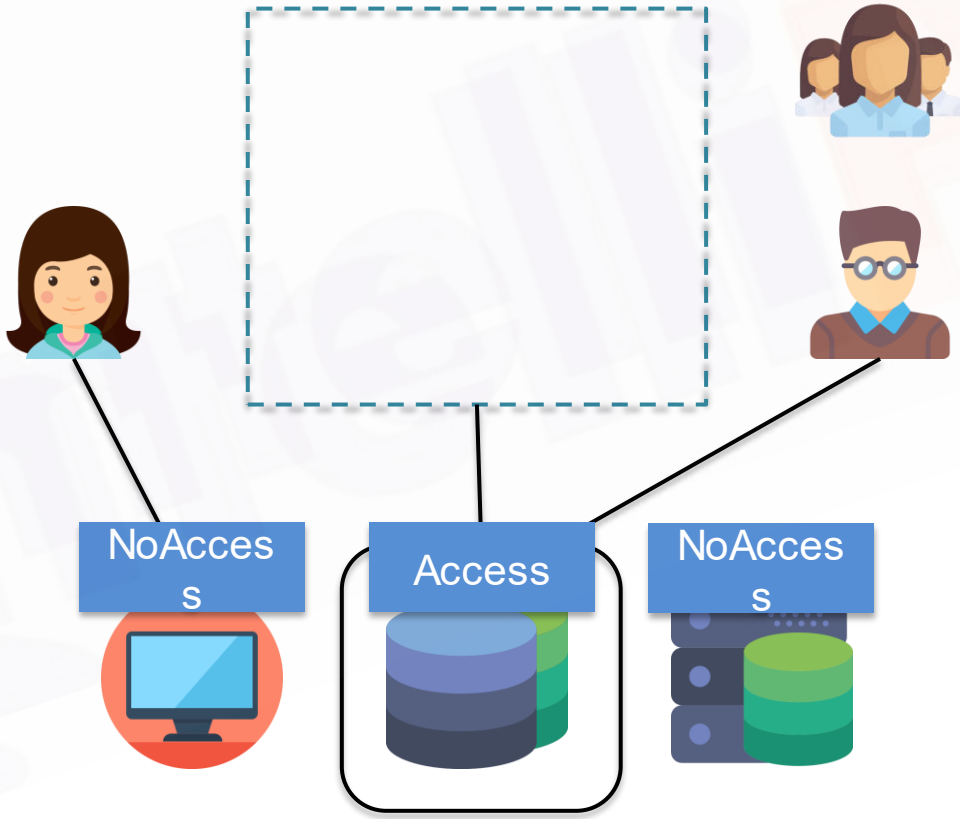
Agenda

1. Permissions
2. Roles
3. Demo
4. Identity Federation
5. STS
6. Pricing

Pre-IAM

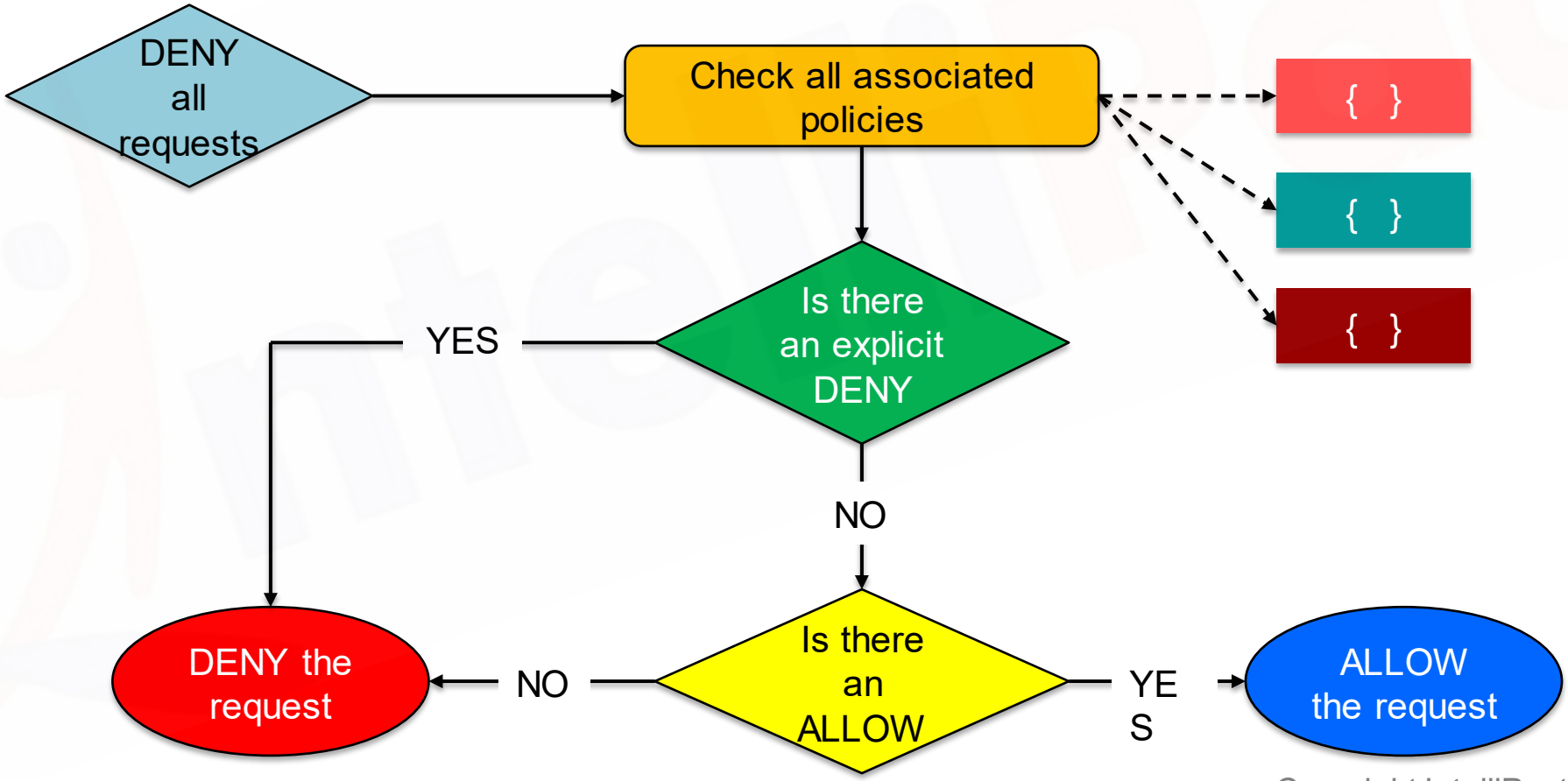
Users, Groups

- Authentication and Authorization
- Users
- Groups
- Permissions



IAM Concept

Policy Evaluation Logic



IAM Concept

IAM Permissions

- Permissions are given by attaching policies to users or groups.
- No permission by default for all IAM users.
- AWS account “root” credential.
- Use the policies defined earlier to provide access to users and groups.

IAM Concept

IAM Roles

- Role is similar to an user/group which has permissions/policies attached to it.
- Roles are temporary access given to anyone who needs to perform the specific task mentioned in the Role.

- Permissions attached to the users are taken away till the time role is getting used.

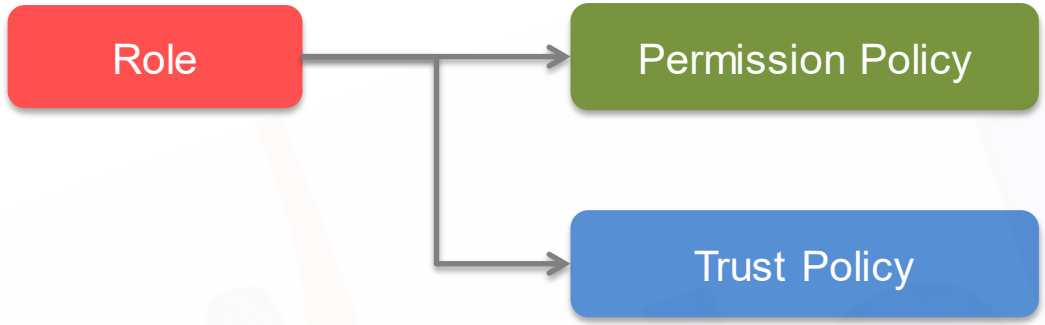
Role: Can access EC2

Role: Can access RDS

IAM Concept

IAM Roles

- Policies and Permissions with Roles:



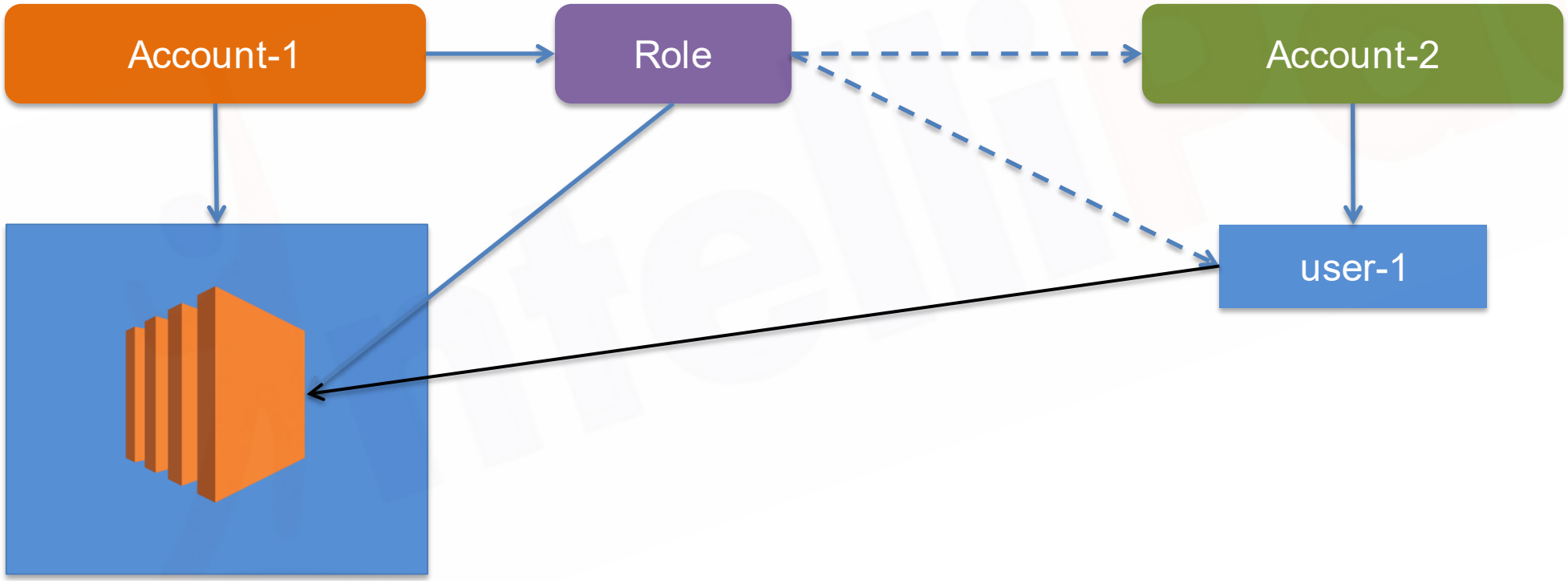

```
{
        “Effect” : “Allow”,
        “Action” : “sts:AssumeRole”,
        “Principal” : “ec2.amazonaws.com”
}
```

- IAM user in the same account
- IAM user in different account
- Another AWS service
- An external user

IAM Concept

Cross-Account Roles

- Cross-Account Role:



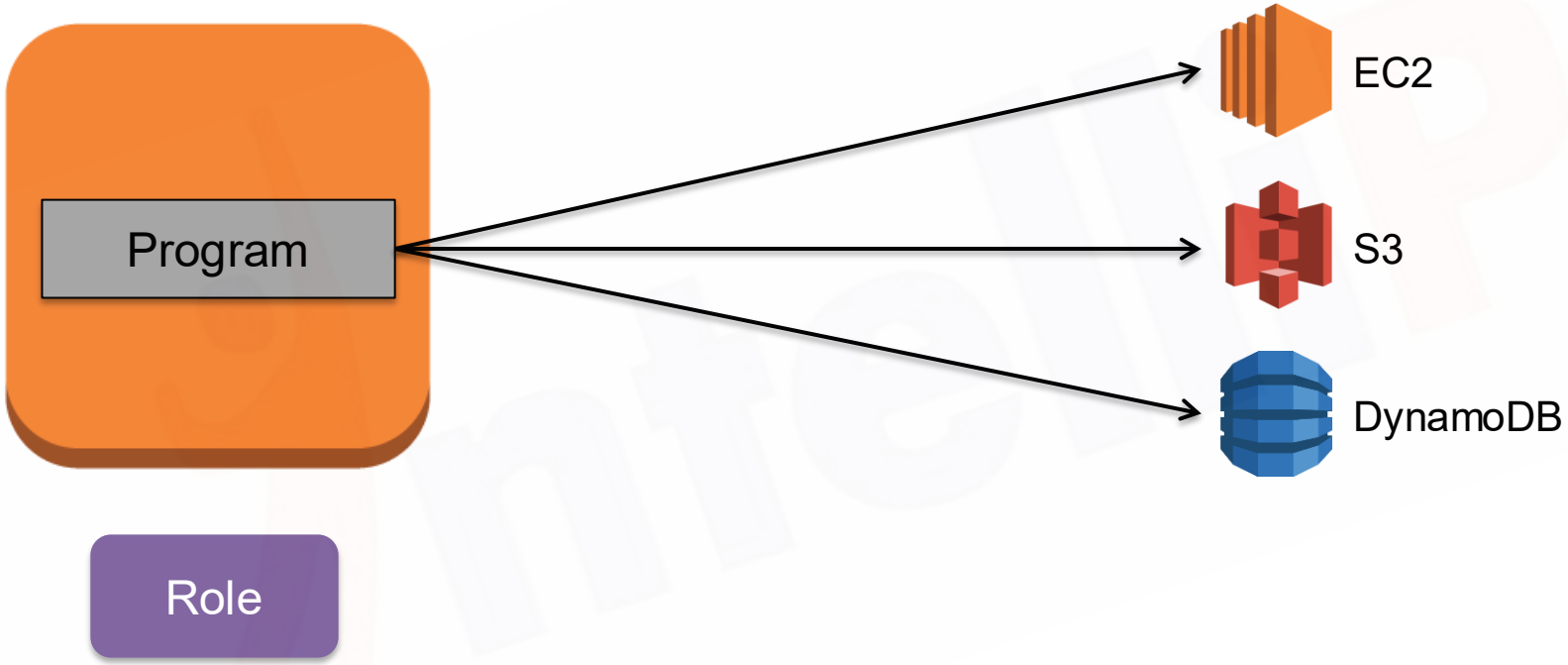
Demo 3: Roles

- Create 2 users – s3-user and ec2-user.
- S3-user should not have any EC2 access.
- ec2-user should have all access on ec2 instances.
- Create 2 roles – s3-role & ec2-role.
- ec2-role should have access to launch EC2 instances and list them.
- s3-role should have access to the S3 buckets.
- Make s3-user to assume ec2-role and ec2-user to assume s3-role.

IAM Concept

Cross-Account Roles

- Instance Profile:



IAM Concept

Cross-Account Roles

- Identity Federation: AWS resources can be accessed by third party Identity Providers (IdP)
  - Web: Facebook, Google, Amazon or any OIDC
  - SAML2.0: LDAP or Microsoft AD

- Steps (Web Identity Federation)
  - Sign up as developer in Facebook or Google or Amazon account.
  - Create an Identity Provider in IAM.
  - Create Role with Trust and Permission Policy
  - In Trust Policy Principal should be the Web IdP
  - Cognito can be used as Identity Broker.

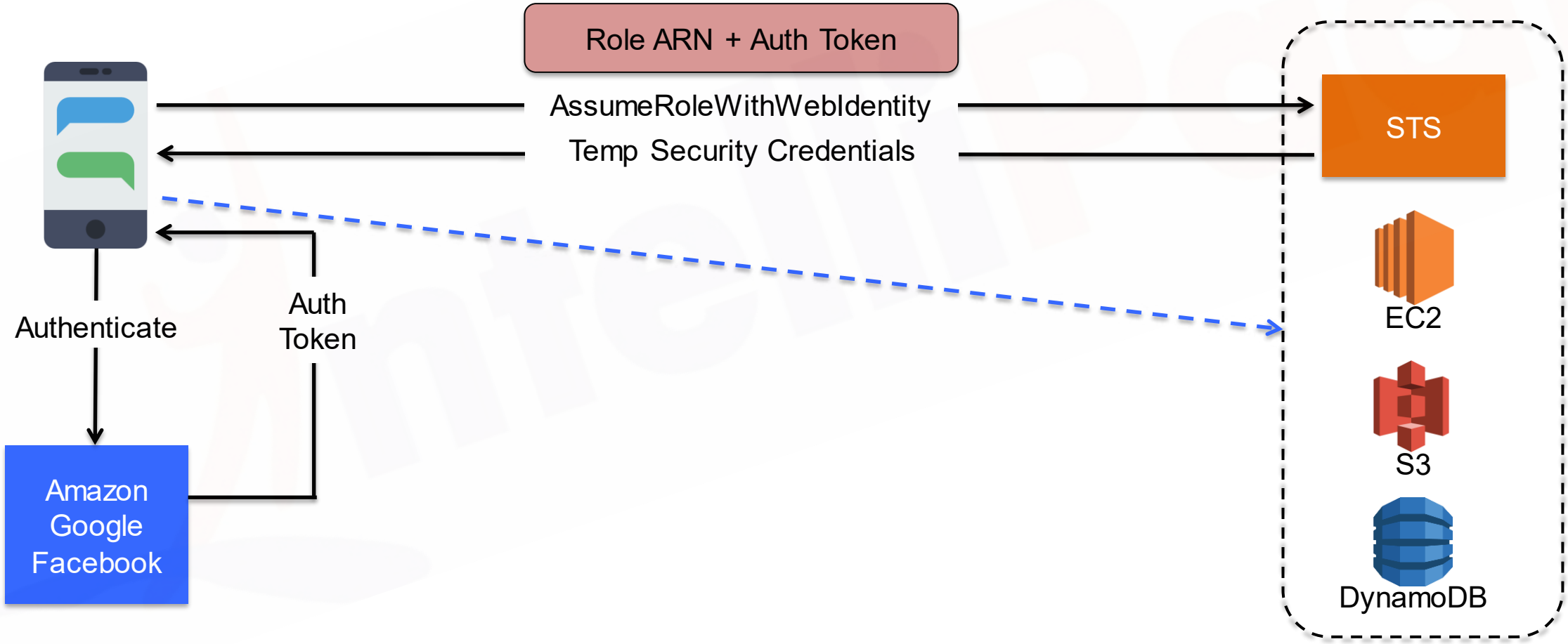
```
"Principal" : { "Federated" : "www.amazon.com" }
"Principal" : { "Federated" : "graph.facebook.com" }
"Principal" : { "Federated" : "accounts.google.com" }
```

```
"Action" : "sts:AssumeRoleWithWebIdentity"
```

IAM Concept

Web Identity Federation

- How does it work?



IAM Concept

SAML Identity Federation

- Steps (SAML Federation)
  - Register AWS with Corporate IdP (LDAP).
  - That will generate a Metadata XML.
  - Create a SAML identity provider with the SAML metadata.
  - Create Roles.
  - These roles should be mapped with Organization's assertions.

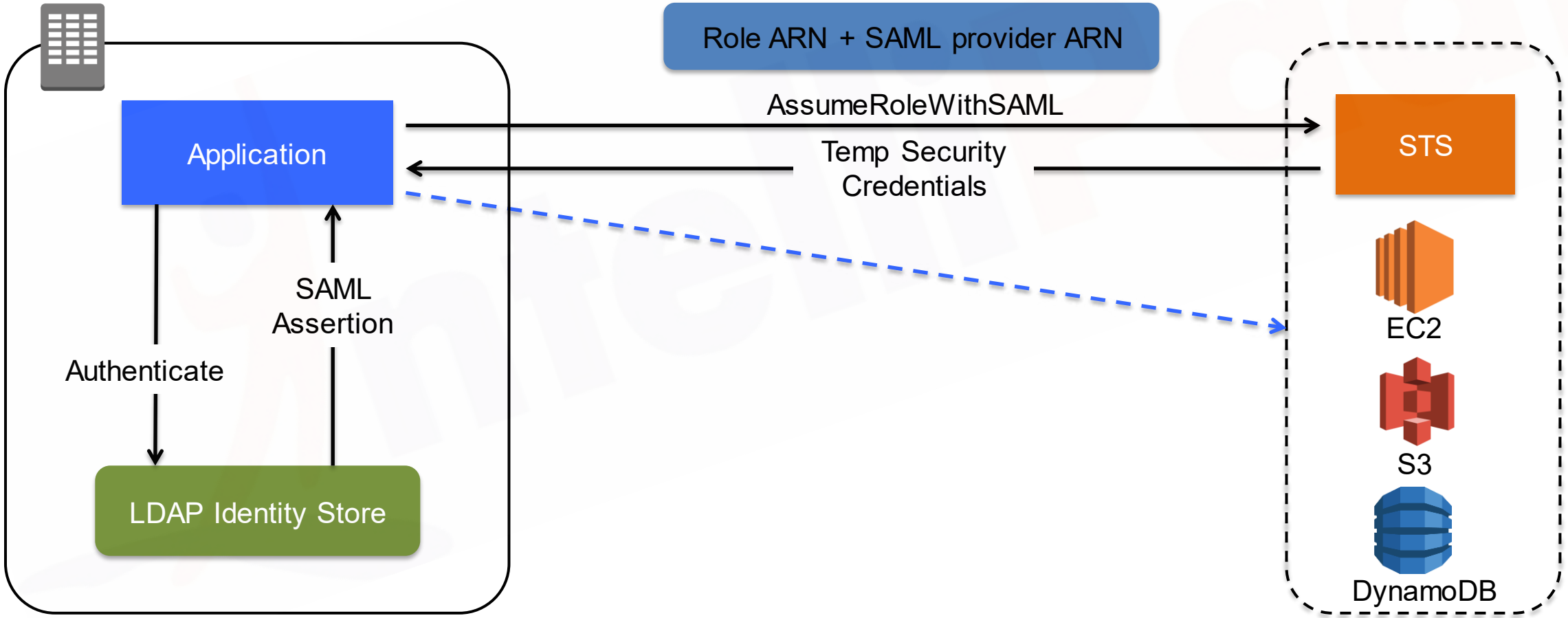
"Principal" : { "AWS" : "ARN of the SAML provider" }

"Action" : "sts:AssumeRoleWithSAML"

IAM Concept

SAML Identity Federation

- How does it work?



IAM Concept

Temporary Security Credentials & STS

- STS can be used to get temporary security credentials.
  - Temporary Access Key ID, Secret Access Key and Security Token

- STS Calls.
  - "AssumeRole": ARN of the Role, Duration (15 mins to 1 hour (Default))
  - "AssumeRoleWithWebIdentity": ARN of the Role, Auth Token, Duration (15 mins to 1 hour (Default))
  - "AssumeRoleWithSAML" : ARN of the Role, ARN of the SAML provider created in IAM, SAML assertion, Duration (15 min to 1 hour (Default)
  - "GetFederationToken"
  - "GetSessionToken"

Summary

- Authorization & Authentication.
- Amazon Resource Name (ARN), IAM Hierarchy.
- IAM Users, Groups and Roles.
- Multi-Factor Authentication.
- Policy Evaluation.
- IAM Roles
  - Roles in the same account
  - Cross-account Roles
- Instance Profile
- Identity Federation – Web (OIDC) and SAML.

Pricing

Entirely Free!!

India : +91-7847955955

US : 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24X7 Chat with our Course Advisor