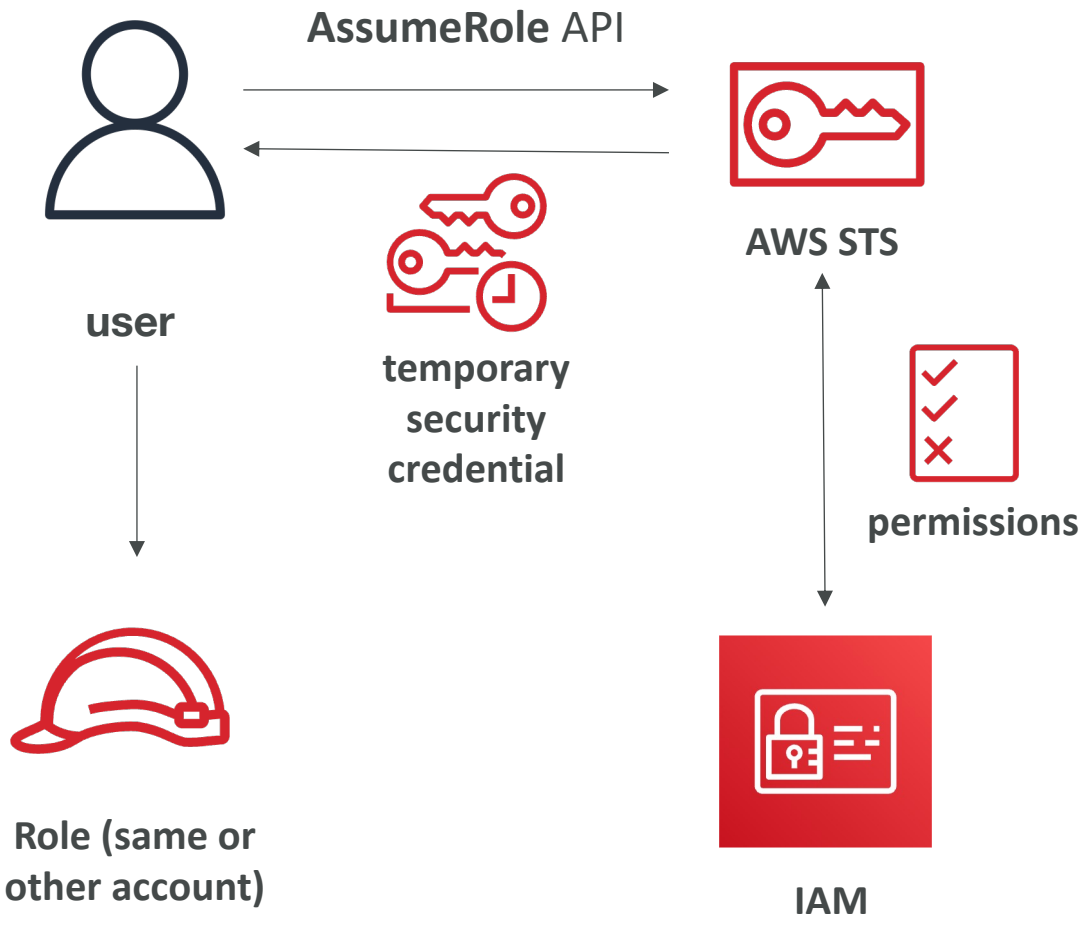
# Using STS to Assume a Role

- Define an IAM Role within your account or cross-account
- Define which principals can access this IAM Role
- Use AWS STS (Security Token Service) to retrieve credentials and impersonate the IAM Role you have access to (**AssumeRole API**)
- Temporary credentials can be valid between 15 minutes to 12 hour



# Assuming a Role with STS

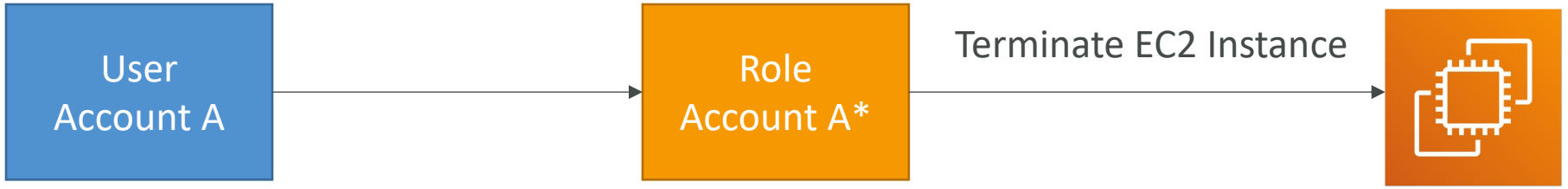
- Provide access for an IAM user in one AWS account that you own to access resources in another account that you own
- Provide access to IAM users in AWS accounts owned by third parties
- Provide access for services offered by AWS to AWS resources
- Provide access for externally authenticated users (identity federation)

- Ability to revoke active sessions and credentials for a role (by adding a policy using a time statement – AWSRevokeOlderSessions)

When you assume a role (user, application or service), you give up your original permissions and take the permissions assigned to the role

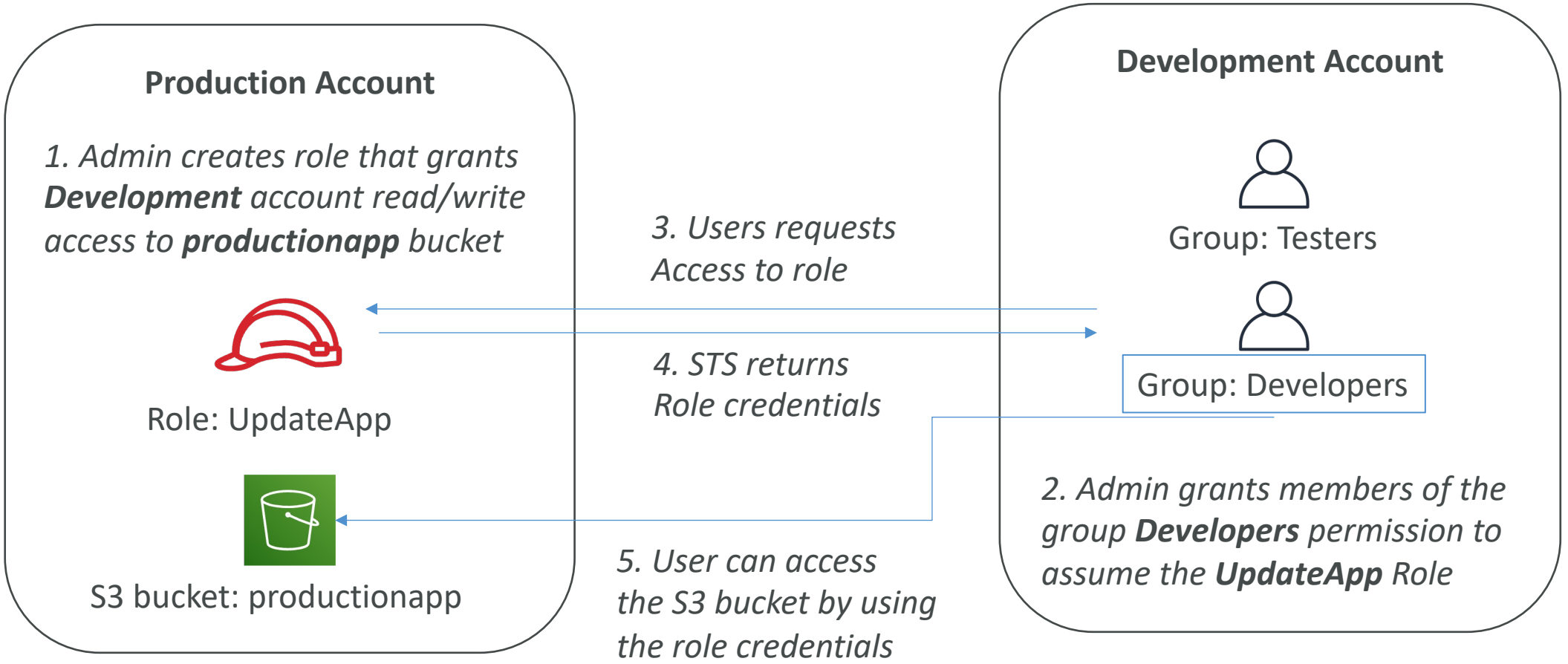
# Providing Access to an IAM User in Your or Another AWS Account That You Own

- You can grant your IAM users permission to switch to roles within your AWS account or to roles defined in other AWS accounts **that you own**.




- Benefits:
  - You must explicitly grant your users permission to assume the role.
  - Your users must actively switch to the role using the AWS Management Console or assume the role using the AWS CLI or AWS API
  - **You can add multi-factor authentication (MFA) protection to the role** so that only users who sign in with an MFA device can assume the role
  - Least privilege + auditing using CloudTrail

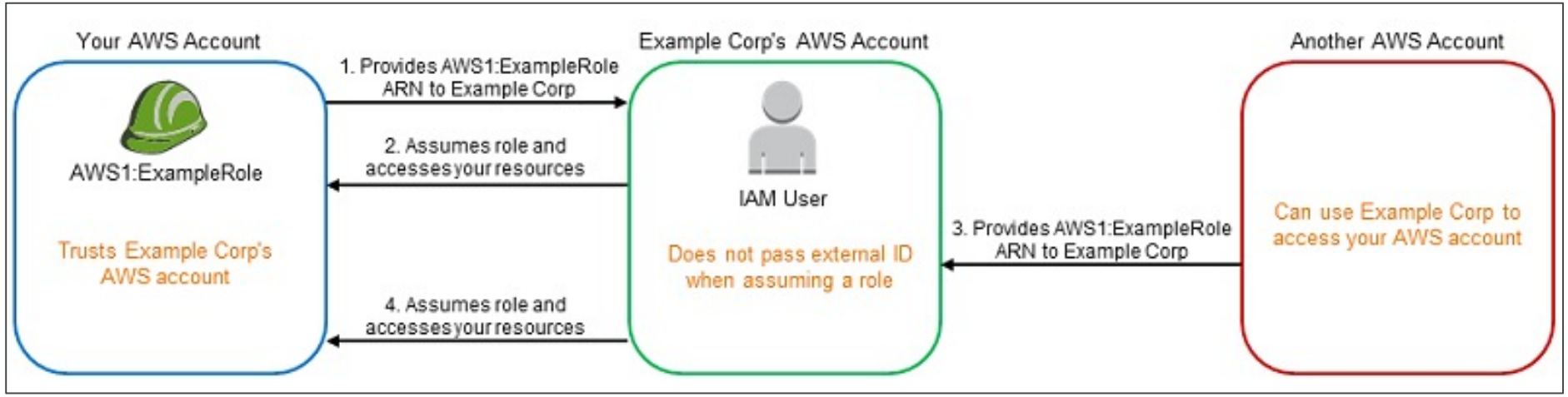
# Cross account access with STS

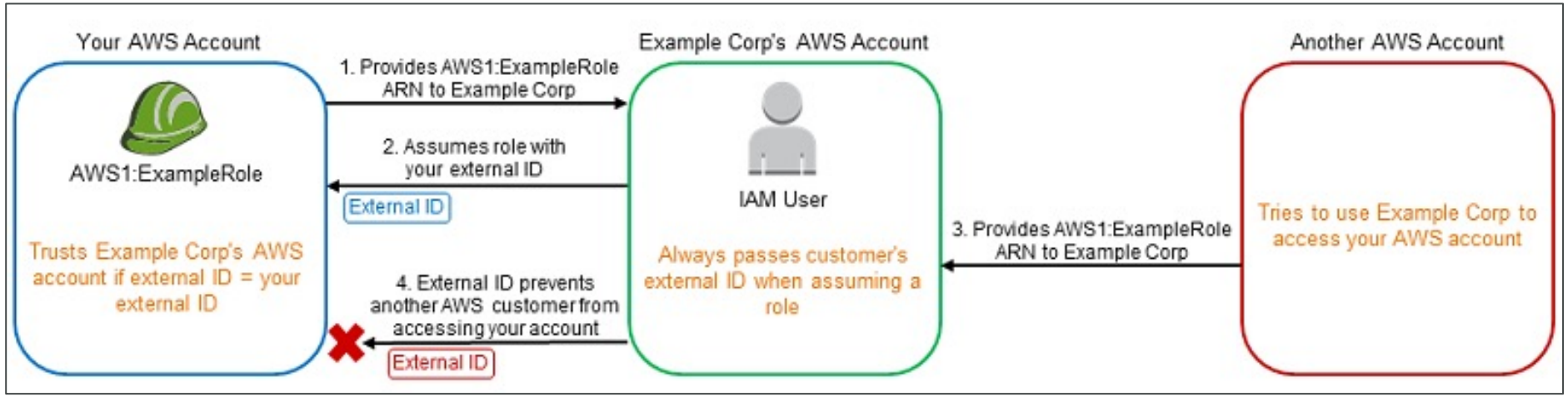


# Providing Access to AWS Accounts Owned by Third Parties

- Zone of trust = accounts, organizations that you own
- Outside Zone of Trust = 3rd parties
- Use IAM Access Analyzer to find out which resources are exposed
- For granting access to a 3rd party:
  - The 3rd party AWS account ID
  - **An External ID** (secret between you and the 3rd party)
    - To uniquely associate with the role between you and 3rd party
    - Must be provided when defining the trust and when assuming the role
    - Must be chosen by the 3rd party
  - Define permissions in the IAM policy

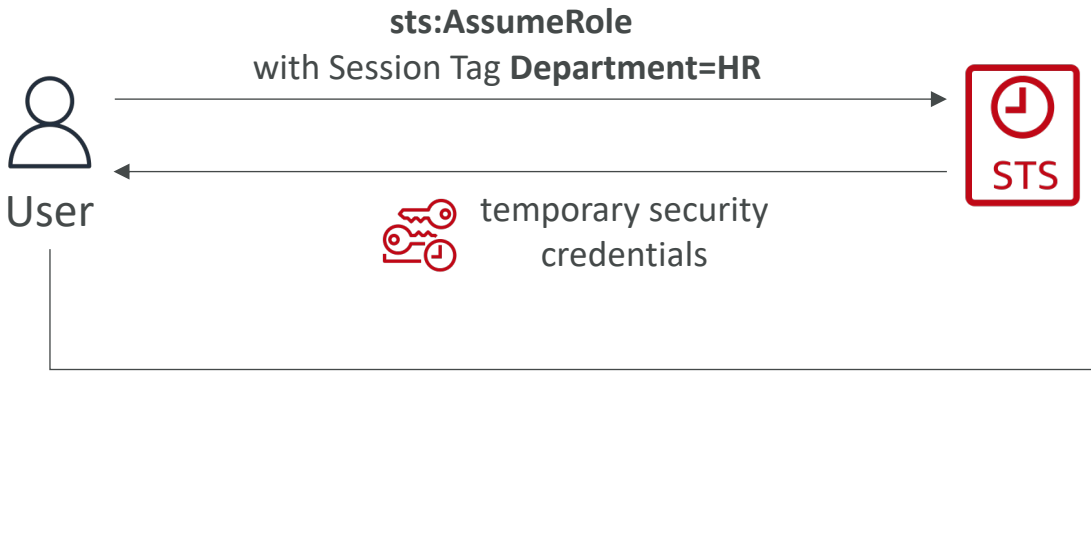
# The confused deputy



# Session Tags in STS

- Tags that you pass when you assume an IAM Role or federate user in STS
- aws:PrincipalTag Condition
  - Compares the tags attached to the principal making the request with the tag you specified in the policy
  - Example: allow a principal to pass session tags only if the principal making the request has the specified tags




```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::hr-docs/*",
        "Condition": {
          "StringEquals": {
            "aws:PrincipalTag/Department": "HR"
          }
        }
      }
    ]
}
```

# STS Important APIs

- AssumeRole: access a role within your account or cross-account
- AssumeRoleWithSAML: return credentials for users logged with SAML
- AssumeRoleWithWebIdentity: return creds for users logged with an IdP
  - Example providers include Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider
  - AWS recommends using Cognito instead
- GetSessionToken: for MFA, from a user or AWS account root user
- GetFederationToken: obtain temporary creds for a federated user, usually a proxy app that will give the creds to a distributed app inside a corporate network

# Identity Federation in AWS

- Give users outside of AWS permissions to access AWS resources in your account
- **You don't need to create IAM Users (user management is outside AWS)**
- Use cases:
  - A corporate has its own identity system (e.g., Active Directory)
  - Web/Mobile application that needs access to AWS resources
- Identity Federation can have many flavors:
  - SAML 2.0
  - Custom Identity Broker
  - Web Identity Federation With(out) Amazon Cognito
  - Single Sign-On (SSO)