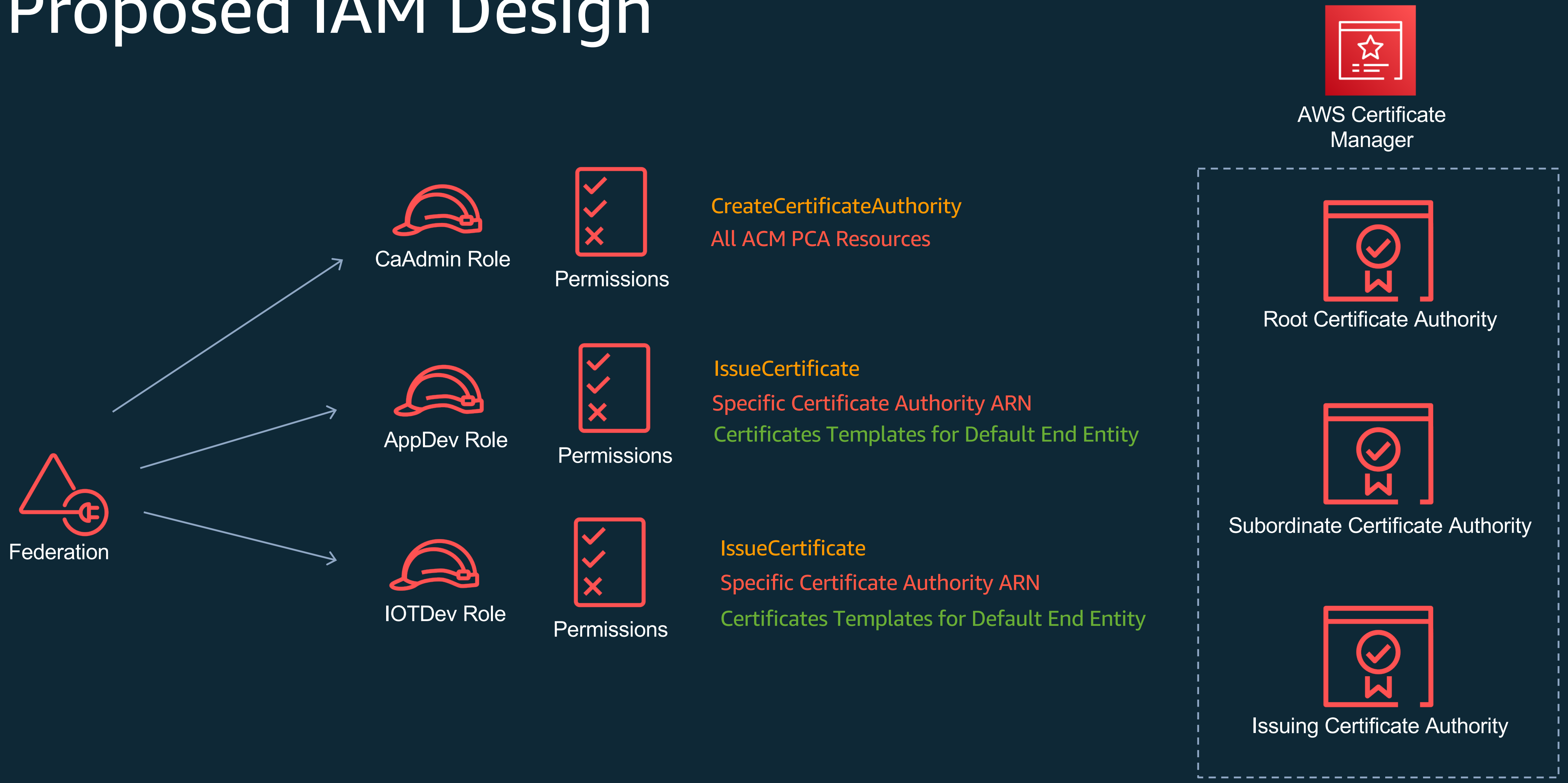
Least Privilege Concepts

Achieving least privilege

- Personas in Workshop
  1. CA Admin
  2. App Dev
  3. IOT Dev

Proposed IAM Design



Federation

CaAdmin Role

Permissions

CreateCertificateAuthority
All ACM PCA Resources

AppDev Role

Permissions

IssueCertificate
Specific Certificate Authority ARN
Certificates Templates for Default End Entity

IOTDev Role

Permissions

IssueCertificate
Specific Certificate Authority ARN
Certificates Templates for Default End Entity

AWS Certificate Manager

Root Certificate Authority

Subordinate Certificate Authority

Issuing Certificate Authority

CA Admin Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm-pca:TagCertificateAuthority",
                "acm-pca:CreateCertificateAuthority",
                "acm-pca:ImportCertificateAuthorityCertificate”,
                "acm-pca:CreatePermission"
            ],
            "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*",
            "Condition": {
                "StringLike": {
                    "acm-pca:TemplateArn": [
                        "arn:aws:acm-pca:::template/*CACertificate*/V*"
                    ]
                }
            },
                {
                "Effect": "Allow”,
                "Action": [
                    "acm-pca:ImportCertificateAuthorityCertificate"
                ],
                "Resource": "arn:aws:acm-pca:*:*:certificate-authority/*"
}
    .. (more)
    ]
}
```

App Dev Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm-pca:IssueCertificate"
            ],
            "Resource": "arn:aws:acm-pca:*:*:certificate-authority/12345678-1234-1234-123456789",
            "Condition": {
                "StringLike": {
                    "acm-pca:TemplateArn": "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
                }
            }
        }
     .. (more)
    ]
}
```

IoT Dev Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm-pca:IssueCertificate"
            ],
            "Resource": "arn:aws:acm-pca:*:*:certificate-authority/12345678-1234-1234-123456789",
            "Condition": {
                "StringLike": {
                   "acm-pca:TemplateArn": "arn:aws:acm-pca:::template/EndEntityCertificate/V*"
                }
            }
        }
     .. (more)
    ]
}
```