AWS USER GROUP

CREMONA, IT

23 Novembre 2022 - CoBOX

(-5 gg al Re:Invent)

More than 400 million
API calls per second

Replicated in 30+
Regions

A billion SMT query
for day

More than 400 million
API calls per second

Replicated in 30+
Regions

A billion SMT query
for day

AWS Identity and Access
Management (IAM)

Paolo Latella
AWS Hero / Partner Ambassador
Amazon Authorized Instructor

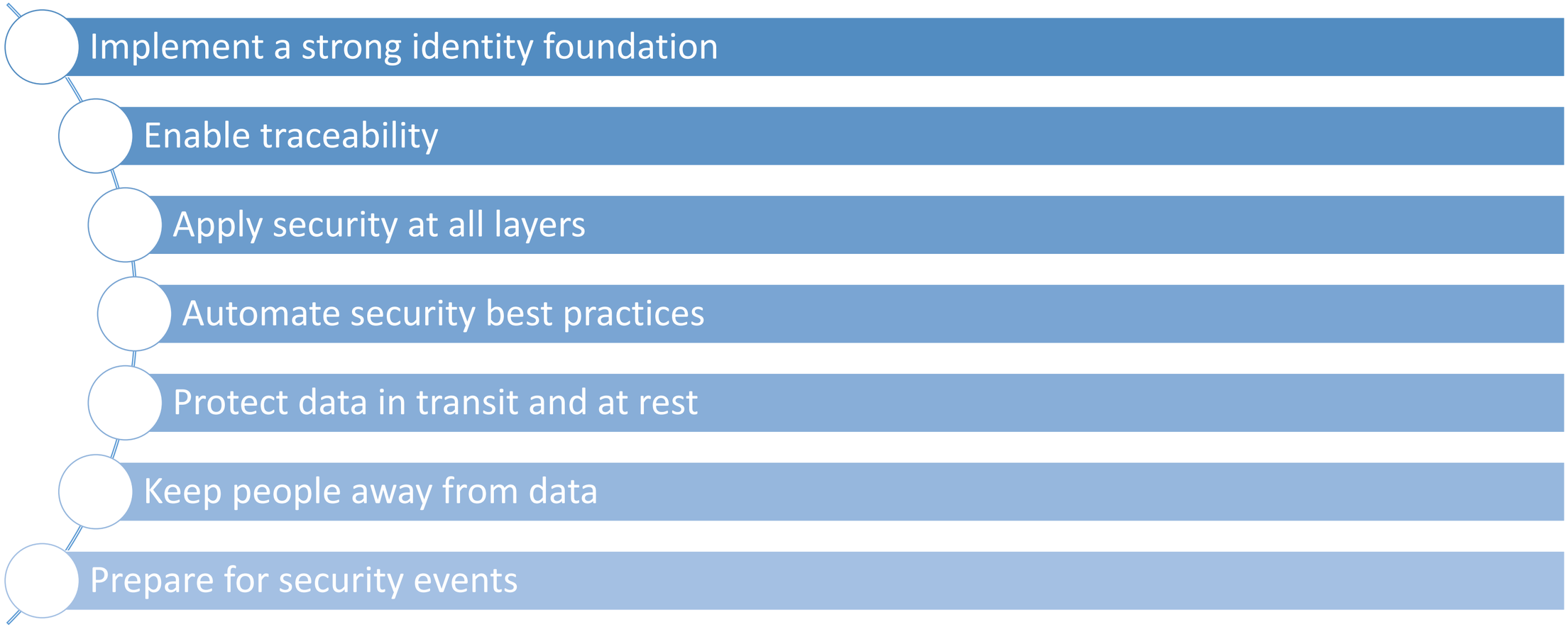
@LatellaPaolo

How to implement a strong identity foundation on AWS Cloud

The Well Architected Framework

Operational Excellence	Security	Reliability	Performance Efficiency	Cost Optimization	Sustainability Pillar
The ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.	The ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.	The ability of a system to recover from infrastructure or service disruptions, and dynamically acquire computing resources	The ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve.	The ability to run systems to deliver business value at the lowest price point.	focuses on minimizing the environmental impacts of running cloud workloads.

Well Architected Framework - 7 Design principles for security



Implement a strong identity foundation

*Implement the **principle of least privilege** and enforce **separation of duties** with appropriate authorization for each interaction with your AWS resources. **Centralize identity management**, and aim to **eliminate reliance on long-term static credentials**.*

Photo by Alexandre Chambon on Unsplash

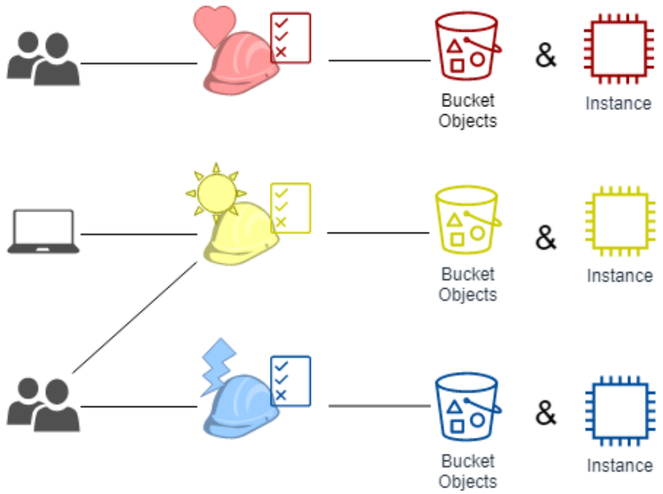
Principle of least privileges

- Prefer ABAC to RBAC authorization model
- Adopt behaviour driven policy design
- Work with permission guardrails
- Introduce check-point at all level
- Separate workload using multi-account strategies

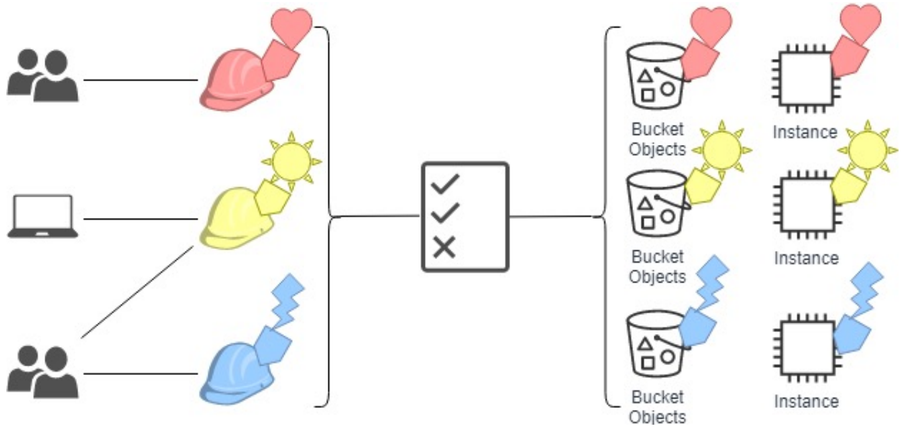
AWS USER GROUP
CREMONA, IT

Least Privileges - Prefer ABAC to RBAC model

RBAC defines permissions based only on a person's job function



ABAC defines permissions based on attributes of a person and the resource



ABAC Model – Example 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartStopIfTags",
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Project": "DataAnalytics",
                    "aws:PrincipalTag/Department": "Data"
                }
            }
        }
    ]
}
```

ABAC Model – Example 2

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"aws:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"}}
    }
}
```

Least Privileges - Adopt behaviour driven policy design

- Your developers are working on a new application
- Your application is in development environment
- To encourage experimentation you've configured IAM policy with broad permissions.
- Now the application is ready for production

- Your developers are working on a new application
- Your application is in development environment
- To guarantee the right level of security you've configured IAM policy with less or no permissions
- Analyze API activity log
- Create policy based on activity
- Iterate
- Now the application is ready for production

Least Privileges - IAM Access Analyzer

IAM Access Analyzer continuously monitors and analyzes resource policy to help you understand the potential security implications. It guides you toward least privilege permissions.

- Identify resources in your organization and accounts that are shared with an external entity.
  - Least Privileges focus on the borders
- Validates IAM policies against policy grammar and best practices.
  - Least Privileges focus on policy grammar
- Generate IAM policies based on access activity in your AWS CloudTrail logs.
  - Least Privileges focus on behaviour

```
maverick@Paolos-MacBook-Pro-2 CCMDLabs % aws accessanalyzer validate-policy --policy-type RESOURCE_POLICY --profile CCMD-EUCOM
t-PaoloLatella --policy-document file://./ValidatePolicy.json --region us-east-1
{
    "findings": [
        {
            "findingDetails": "Using Allow with NotPrincipal can be overly permissive. We recommend that you use Principal ins
            "findingType": "SECURITY_WARNING",
            "issueCode": "ALLOW_WITH_NOT_PRINCIPAL",
            "learnMoreLink": "https://docs.aws.amazon.com/IAM/latest/UserGuide/access-analyzer-reference-policy-checks.html#ac
zer-reference-policy-checks-security-warning-allow-with-not-principal",
            "locations": [
                {
                    "path": [
                        {
                            "value": "Statement"
                        },
                        {
                            "index": 0
                        },
                        {
                            "value": "Effect"
                        }
                    ],
                    "span": {
                        "end": {
                            "column": 25,
                            "line": 4,
                            "offset": 76
                        },
```

IAM Access Analyzer - Generate

```
aws accessanalyzer start-policy-generation \
--policy-generation-details principalArn=arn:aws:iam::278014156012:user/paolo.latella \
--cloud-trail-details '{"trails":[…],"startTime":"2022-10-15T10:30:00.000Z","endTime":"2022-10-15T18:30:00.000Z"}'
--profile CCMD-EUCOM-ThirdFleet-PaoloLatella \
--region eu-west-1
```

```
aws accessanalyzer get-generated-policy \
--job-id jobid \
--profile CCMD-EUCOM-ThirdFleet-PaoloLatella \
--region eu-west-1
```

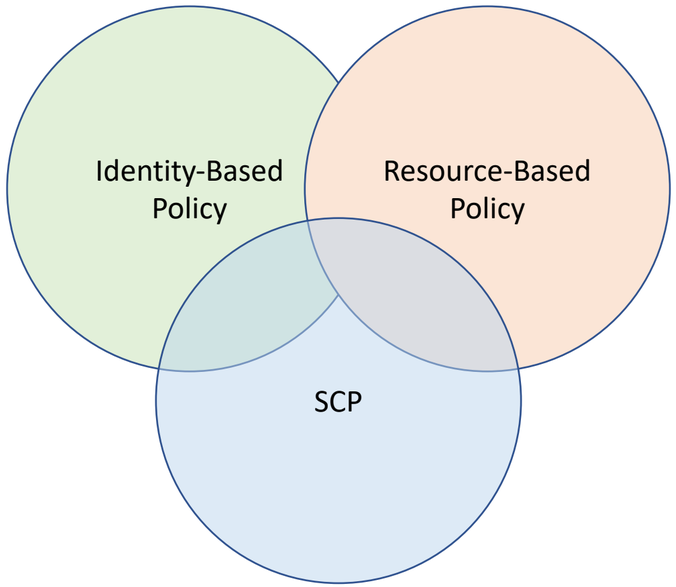
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/shared/*"
            ]
        }
    ]
}
```

AWS USER GROUP
CREMONA, IT

Least Privileges – Work with permissions guardrails

In any case, we must define a set of controls that prevents builders from going off-road (guardrails)

Work with permissions guardrails – SCP



Deny List Strategy - Actions are allowed by default, and you specify what services and actions are prohibited

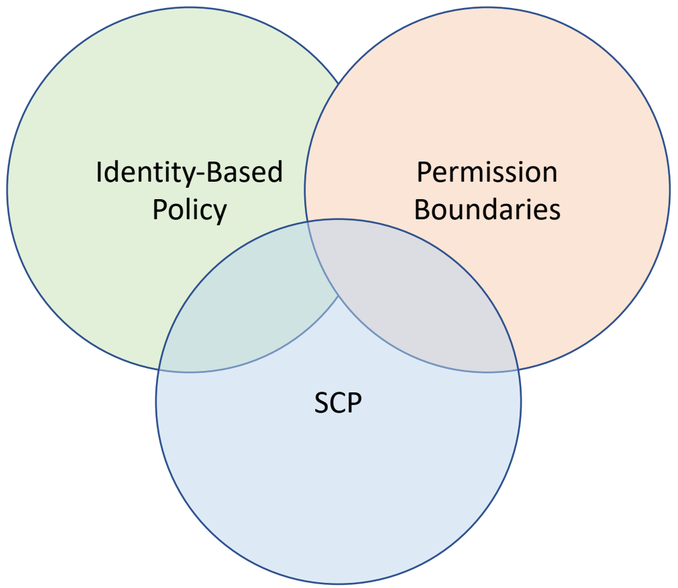
- **Require less maintenance**
- Policy require less space (max 5KB)

Allow List Stratey - Actions are prohibited by default, and you specify what services and actions are allowed

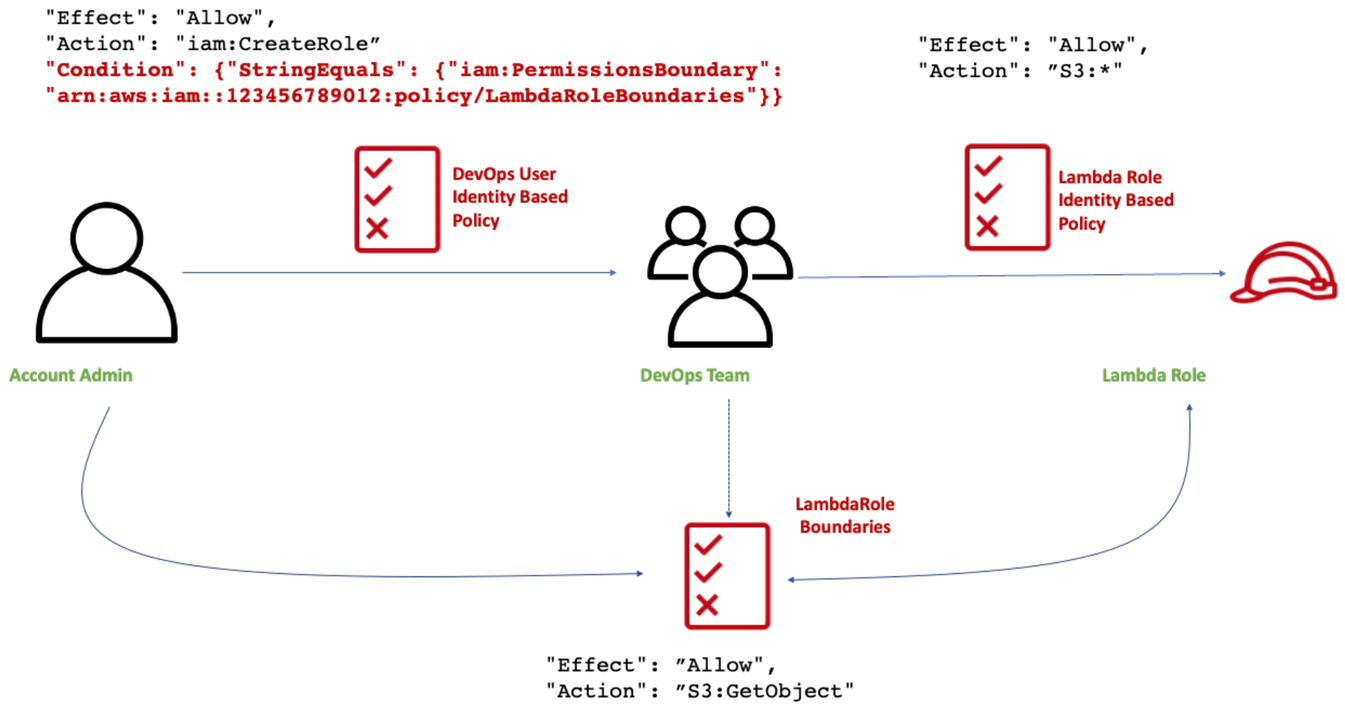
- The implicit deny impact on existing resources
- **Most aligned to principle of least privileges**

Deny List + Exception
- NotAction
- NotResource
- NotPrincipal
- StringNotLike
- ArnNotLike

Work with Permission Guardrails – Permission Boundaries



Delegate + Least Privileges = Prevent privilege escalation



Separation of Duties

Separation of duties or Segregation of duties (SOD) refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them – NIST Glossary.

- Separation of duties can be enforced either statically (by defining conflicting roles) or dynamically (by enforcing the control at access time).
- Separation of duties can be approached as sequential separation (two signatures principle), individual separation (four eyes principle), spatial separation (separate action in separate locations), factorial separation (several factors contribute to completion)

Separation of duties

Static SOD

- Best fit on RBAC model
- Secure Control Policies (SCP)
- Permission Boundaries

Dynamic SOD

- Best fit on ABAC model
- Temporary permission by STS
- Session Policies

Sequential SOD (two signatures)

- Codepipeline with approval actions
- Codecommit and Pull request
- Cloudformation WaitCondition/WaitConditionHandle

Individual SOD (four eyes)

- Role Trust Relationship
- VPC Peering / Transit GW Attachment
- Codepipeline with more approval actions
- Codecommit with more approvals needed

Spatial SOD

- Multi Account Strategies with Assume Role

Factorial SOD

- Require MFA to perform action

Dynamic SOD – Assume role

```
aws sts assume-role --role-arn "arn:aws:iam::278014156012:role/DevOpsPutInProduction" --role-session-name SOD-Demo-Session --profile DevSecOps --source-identity <username>
```

```
aws wafv2 associate-web-acl --web-acl-arn arn:aws:wafv2:eu-west-1:278014156012:regional/webacl/TestDynamicSOD/45289a92 --resource-arn arn:aws:elasticloadbalancing:eu-west-1:278014156012:loadbalancer/app/TestDynamicSOD/76da635f1d7d864d
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SetAwsUserNameAsSourceIdentity",
            "Effect": "Allow",
            "Action": "sts:SetSourceIdentity",
            "Resource": "arn:aws:iam::278014156012:role/CCMD-DevOpsPutInProduction",
            "Condition": {
                "StringLike": {
                    "sts:SourceIdentity": "${aws:username}"
                }
            }
        },
        {
            "Sid": "PermitWriteOnWebACL",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:UpdateWebACL"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

DevSecOps User (Policy)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1665562473928",
            "Action": [
                "wafv2:AssociateWebACL",
                "elasticloadbalancing:SetWebACL"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:wafv2:eu-west-1:278014156012:regional/webacl/*",
                "arn:aws:elasticloadbalancing:eu-west-1:278014156012:loadbalancer/app/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/Owner": "${aws:SourceIdentity}"
                },
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Production"
                }
            }
        }
    ]
}
```

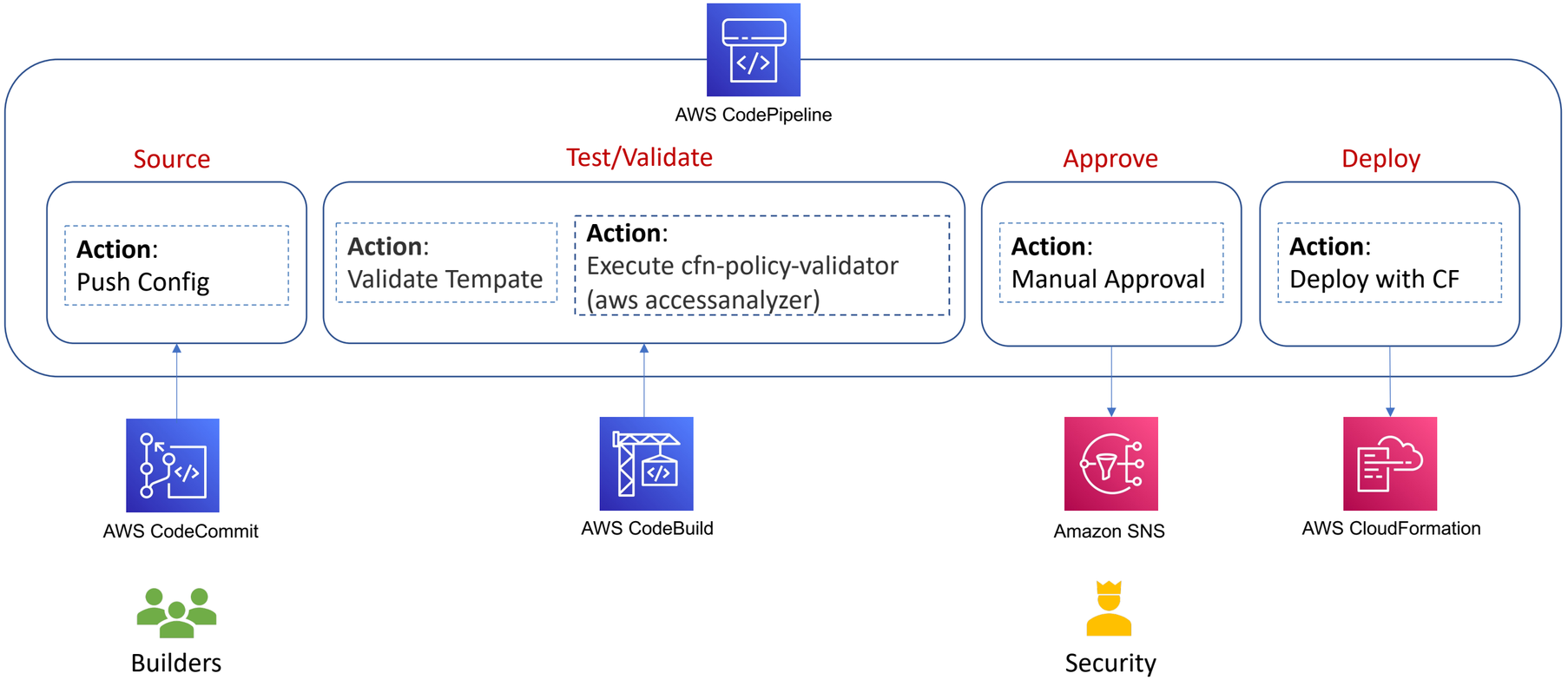
DevOpsPutInProduction Role (Policy)

Don't forget SCP to:

- Require TAG with keys **Environment** and **Owner** on resource creation
- Require **SourceIdentity**=Username in assume-role API

AWS USER GROUP
CREMONA, IT

Sequential SOD - CodePipeline



Separation of duties – Start from risk

- There is no a “Silver bullet” that organizations can use to ensure separation of duties.
- A separation of duties plan starting from a risk-assessment workshop which involves the following steps:
    1. Identify the assets
    2. Decompose the process that involves the asset
    3. Put in evidence the action-entity relationship
    4. Identify Collision that could produce a fraud or error
    5. Mitigate introducing one of the SOD practice

SOD in DevOps/DevSecOps

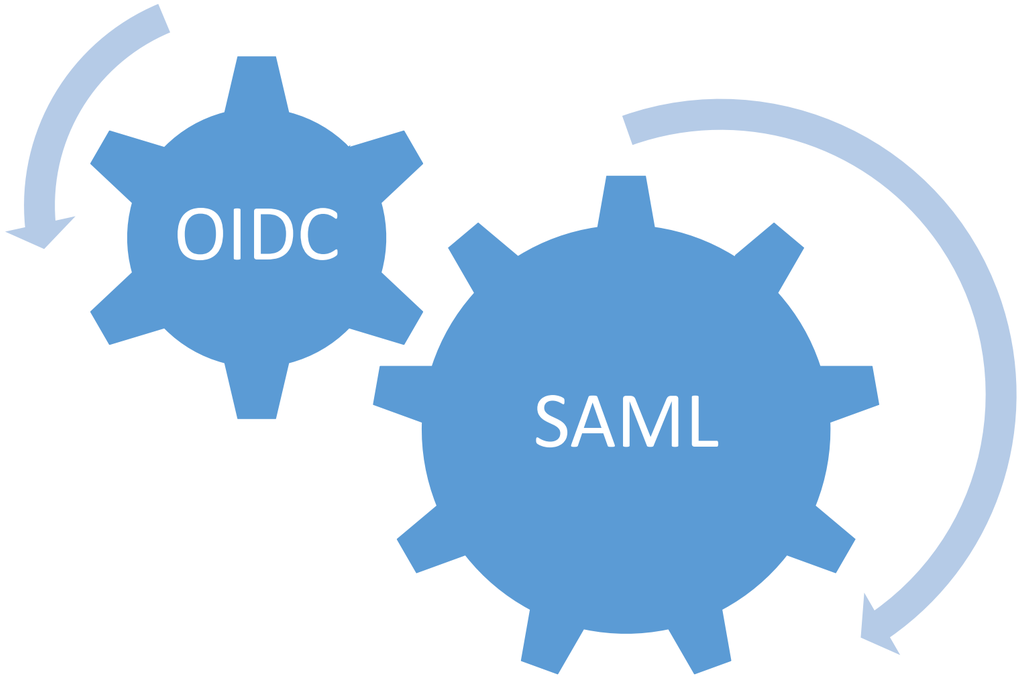
- Is the SOD practicable on a DevSecOps approach ?

SOD in DevOps/DevSecOps

- Is the SOD practicable on a DevSecOps approach ?
- DevSecOps posits that all participants in the development cycle have shared responsibility for the security of the application and its environment.
  - Shared responsibility -> different duties -> same team
- Even in cases where roles are initially played by the same people, it’s important to start with a separate set of functional roles (leveraging AWS Roles)
  - Permit to work with some kind of SOD
  - Simplify the adoption of SOD in the future

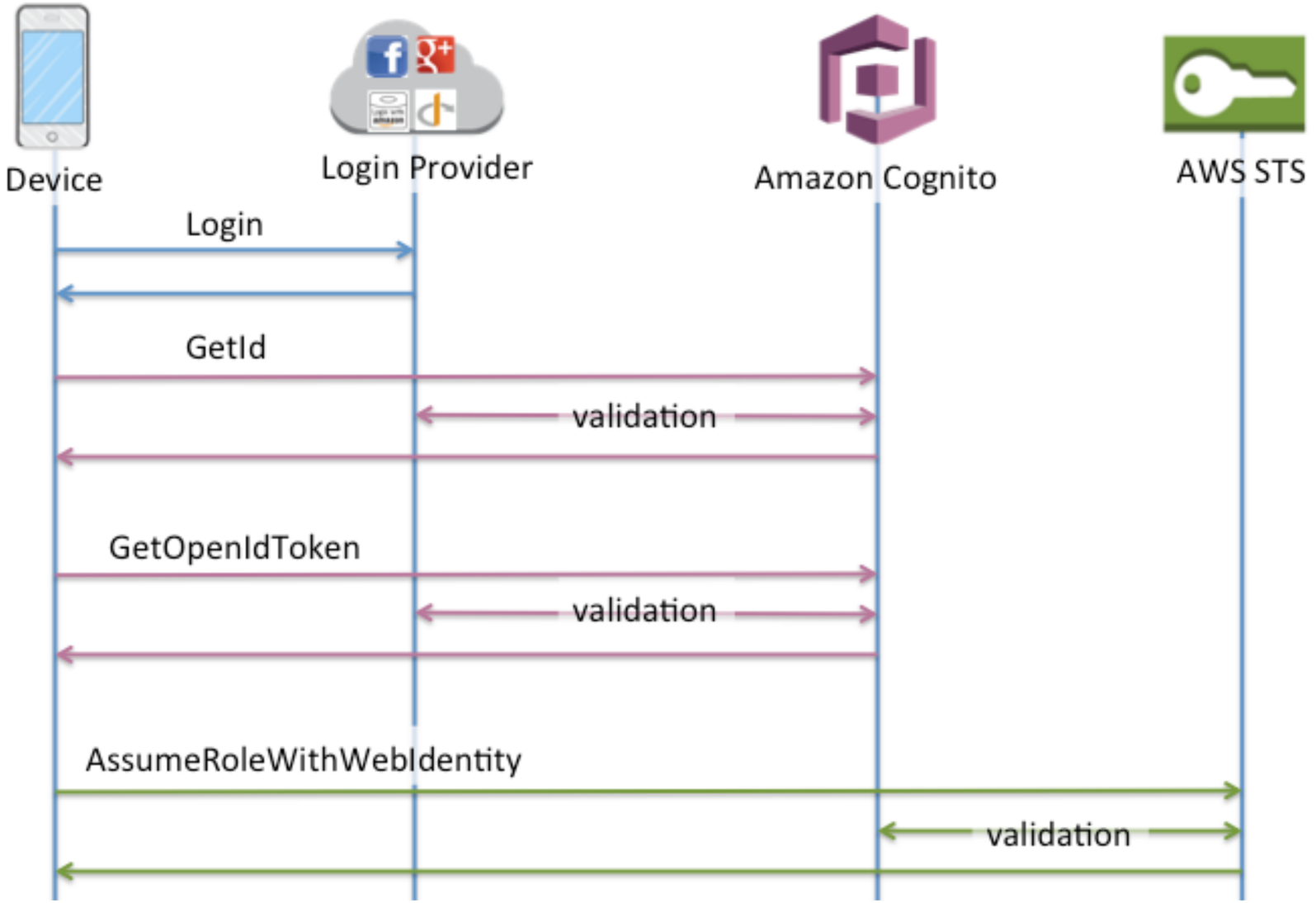
Centralize Identity Management

Amazon Cognito



AWS IAM Identity Center

Amazon Cognito - OIDC Workflow



Cognito - ABAC Example

Claims

Encoded PASTE A TOKEN HERE


```
eyJhbGciOiJSUzI1NiIsImN0eSI6IkpXVCIsImRlcGFydG1lbnQiOiJsZWdhbCIsImNsZWFyYW5jZSI6ImNvbmZpZGVudGlhbCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0IjoxNjAzMzc2MDExfQ.Sk0-4OYd2FvCECKRoa0P4sRKS2AsTS6r7TcXxSlzScwzvfm3mkFjp158Cnr7H4h2enss4D940NnBDm15kgwfd-WSzFQ4NL-ruQMn-8CVOrFjcXJWfa1gLXtvm9WR0iRcOUSQqbyx8nHsDMo1d_vqlR5xqTiPo_0_KN7VLFgop9wnHJLnlIxjH6UXj2zTaWJSSuXENrP4Cv4M1Ky-vTMNBKtlF6vT5En-s4egeXhCmKxbI3axzrpmgb0pCncCjlfusPJo5TNILUh6iGCakDSNkjbMr8KurrkLDWGfqirhSv7C_bHQURDvDw3oSGRGRJzlY2c_lYA5j5jV5c-1XDx_0A
```


Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE


```
{
  "alg": "RS256",
  "cty": "JWT",
  "department": "legal",
  "clearance": "confidential"
}
```


PAYLOAD: DATA


```
{
  "sub": "1234567890",
  "iat": 1603376011
}
```

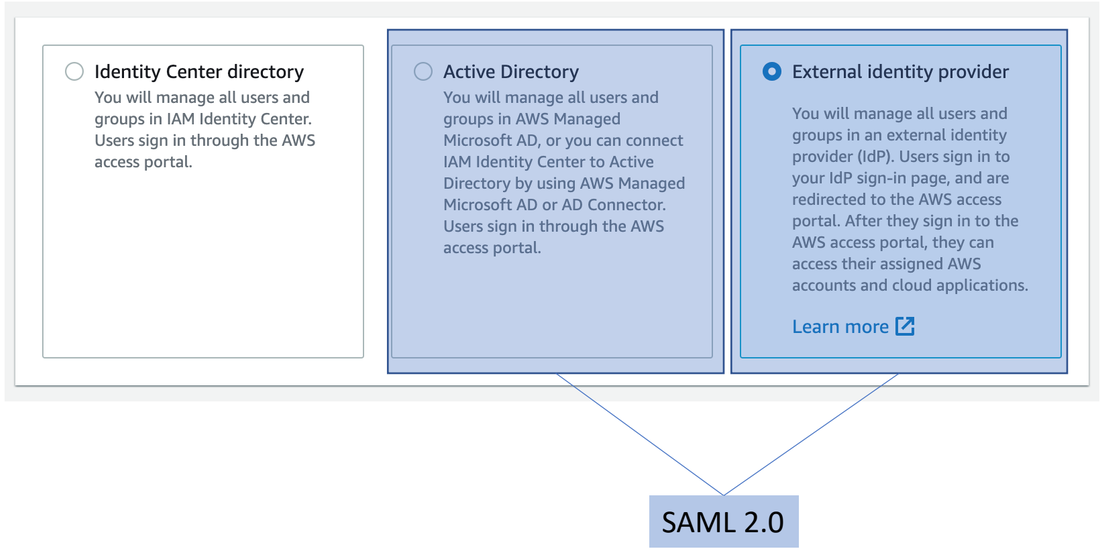

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
```

Permission Policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetObject*",
            "Resource": "arn:aws:s3:::*-${aws:PrincipalTag/department}/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:ExistingObjectTag/clearance": "${aws:PrincipalTag/clearance}"
                }
            }
        }
}
```

IAM Identity Center - SAML 2.0



IAM Identity Center - ABAC

${path:userName}
${path:name.familyName}
${path:name.givenName}
${path:displayName}
${path:nickName}
${path:emails[primary eq true].value}
${path:addresses[type eq "work"].streetAddress}
${path:addresses[type eq "work"].locality}
${path:addresses[type eq "work"].region}
${path:addresses[type eq "work"].postalCode}
${path:addresses[type eq "work"].country}
${path:addresses[type eq "work"].formatted}
${path:phoneNumbers[type eq "work"].value}
${path:userType}
${path:title}
${path:locale}
${path:timezone}
${path:enterprise.employeeNumber}
${path:enterprise.costCenter}
${path:enterprise.organization}
${path:enterprise.division}
${path:enterprise.department}
${path:enterprise.manager.value}

You can't use external IdP attribute values outside of this list for ABAC unless you use the option of passing attributes through the **SAML assertion.**

Key	Value (optional)	Remove
Department	${path:enterprise.department}	✖
CostCenter	${path:enterprise.costCenter}	✖
Add new key	*Add new value*	

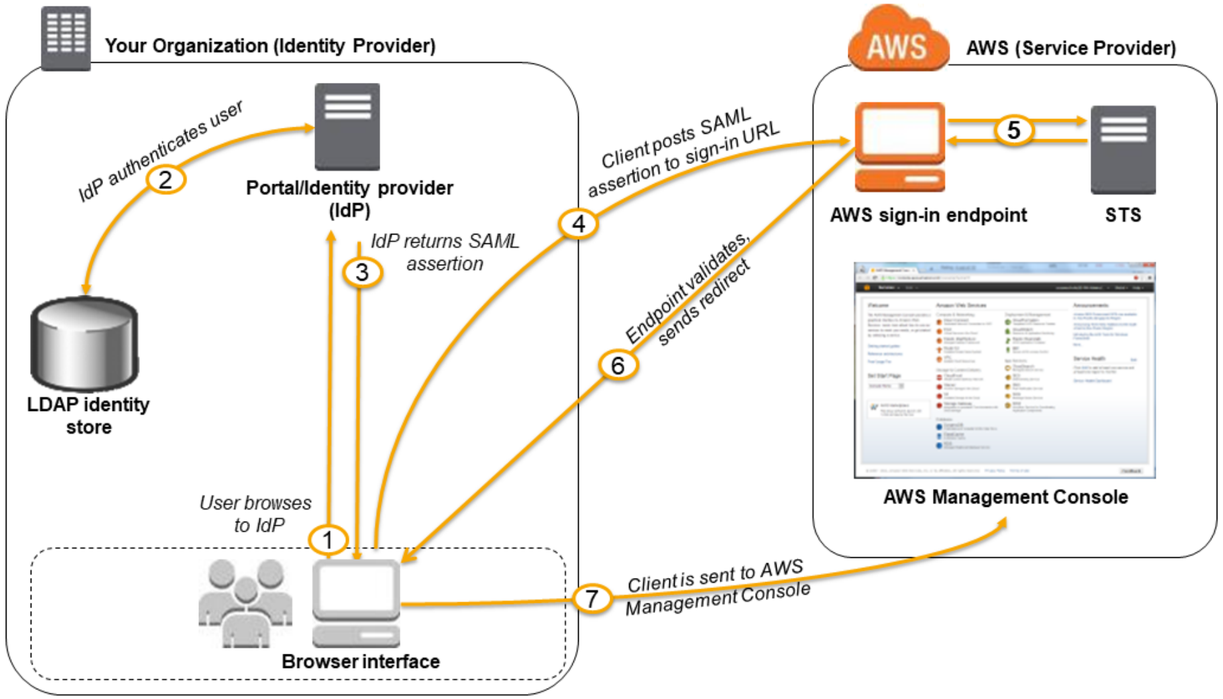
```
"${aws:PrincipalTag/CostCenter}"

"${aws:PrincipalTag/Department}"
```

AWS USER GROUP
CREMONA, IT

IAM Identity Center - ABAC - Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

SAML - Expand tags with SAML Assertion



3

```
<Attribute
Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:Project">
<AttributeValue>IAMDemo</AttributeValue> </Attribute> <Attribute
Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:CostCenter
"> <AttributeValue>DevOps</AttributeValue> </Attribute>
```

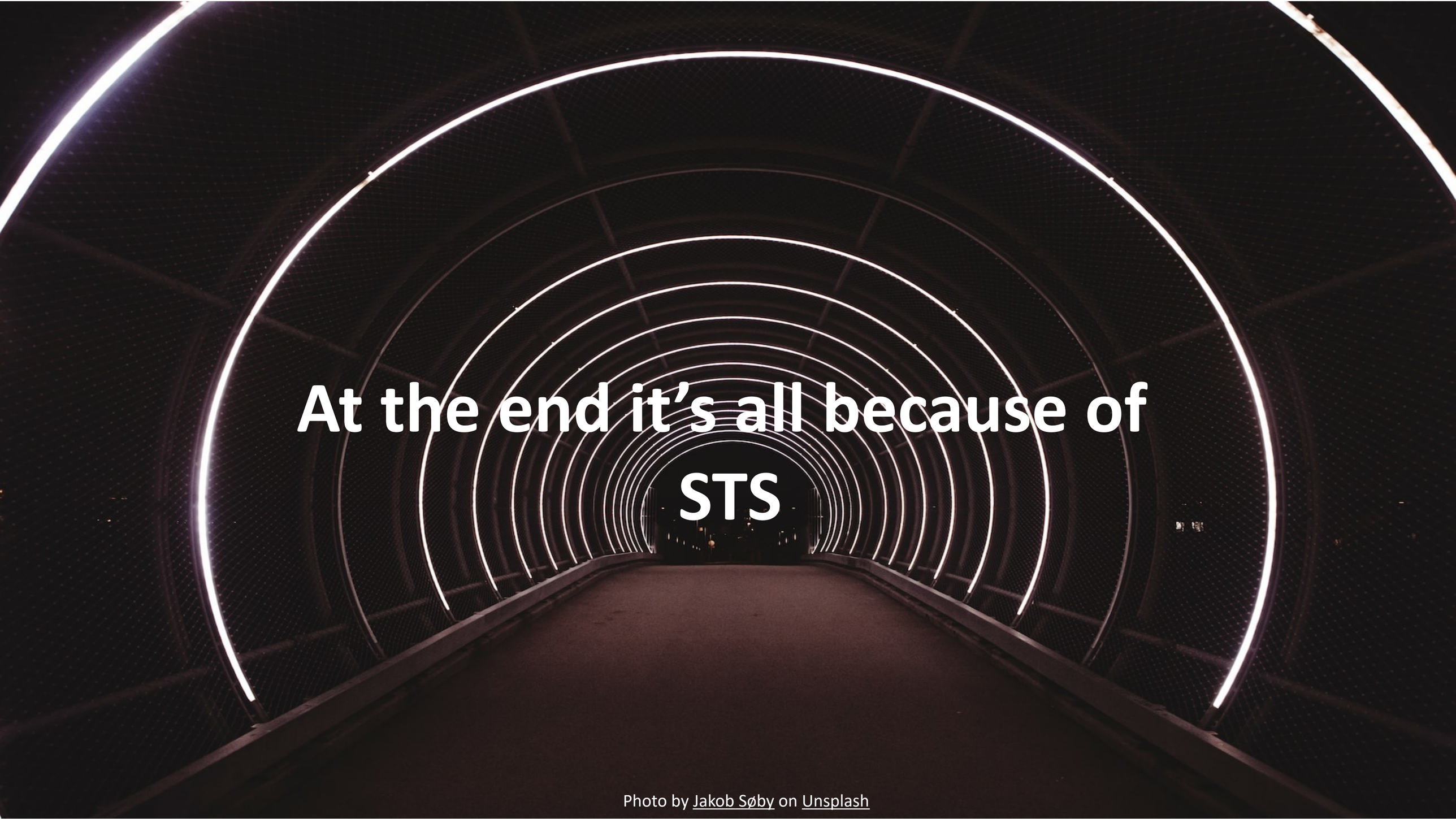


Photo by Jakob Søby on Unsplash

STS - API Comparison

AWS STS API	Who can call	Credential lifetime (min | max | default)	MFA	Session policy
AssumeRole	IAM user or IAM role with existing temporary security credentials	15 m | Maximum session duration setting[3] | 1 hr	Yes	Yes
AssumeRoleWithSAML	Any user; caller must pass a SAML authentication response that indicates authentication from a known identity provider	15 m | Maximum session duration setting[3] | 1 hr	No	Yes
AssumeRoleWithWebIdentity	Any user; caller must pass a web identity token that indicates authentication from a known identity provider	15 m | Maximum session duration setting[3] | 1 hr	No	Yes
GetFederationToken	IAM user or AWS account root user	IAM user: 15 m | 36 hr | 12 hr Root user: 15 m | 1 hr | 1 hr	No	Yes
GetSessionToken	IAM user or AWS account root user	IAM user: 15 m | 36 hr | 12 hr Root user: 15 m | 1 hr | 1 hr	Yes	No

AWS USER GROUP

CREMONA, IT

Grazie !