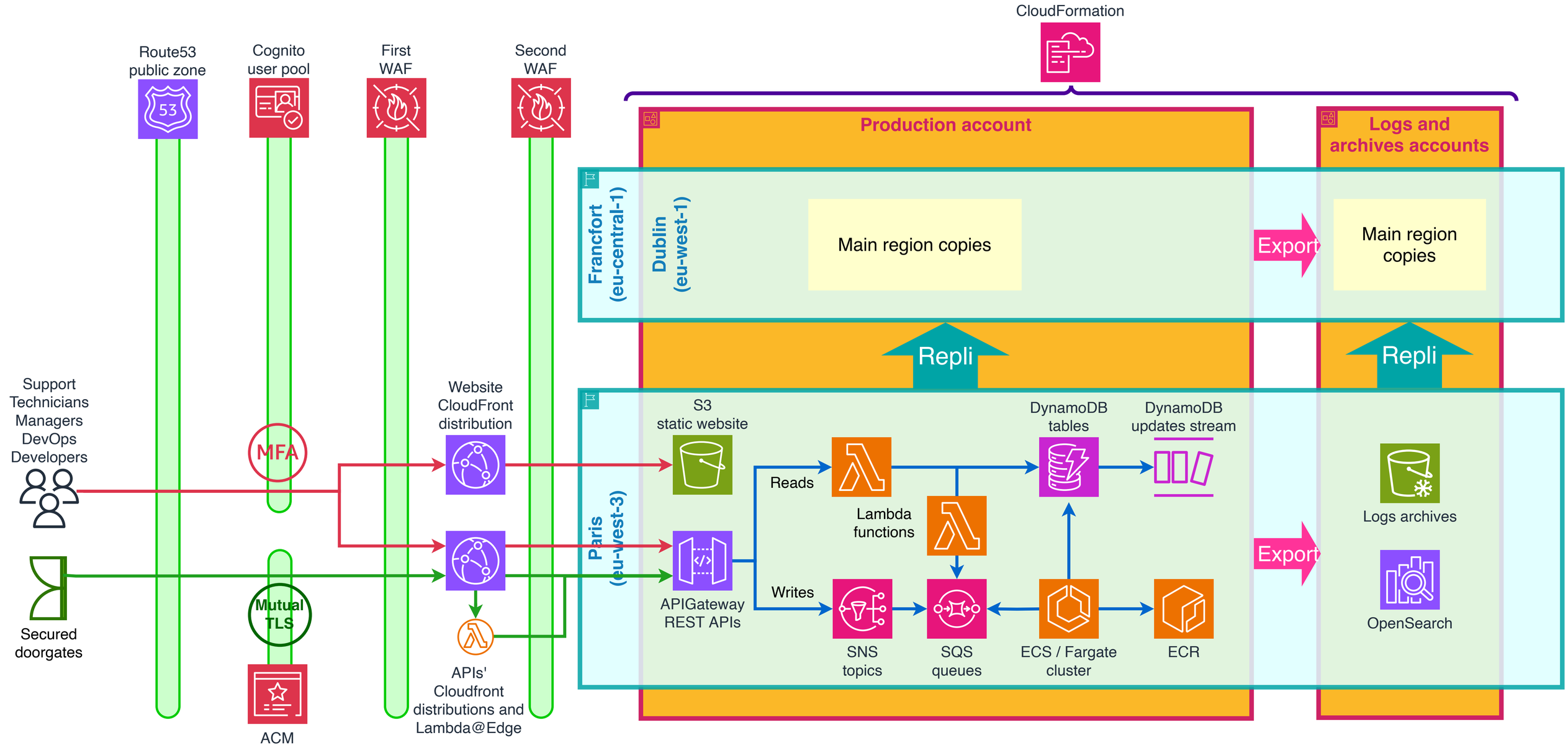
AccessGranted

Secure the accesses to your doorgates

General overview

- I have imagined a project that I named “AccessGranted” for a company of the type SME bearing the same name.
- Accessgranted allows secure and exclusive access to the parking lots to the residents of apartment buildings.
- In order to be able to establish a well-designed framework that meets the needs of the client (an imagined one), I have based myself primarily on the **Security** and **Reliability** pillars.
- **Serverless services** from AWS were privileged to reduce operational costs and optimizing maintenance costs.
- In case the business expands, the architecture remains valid.

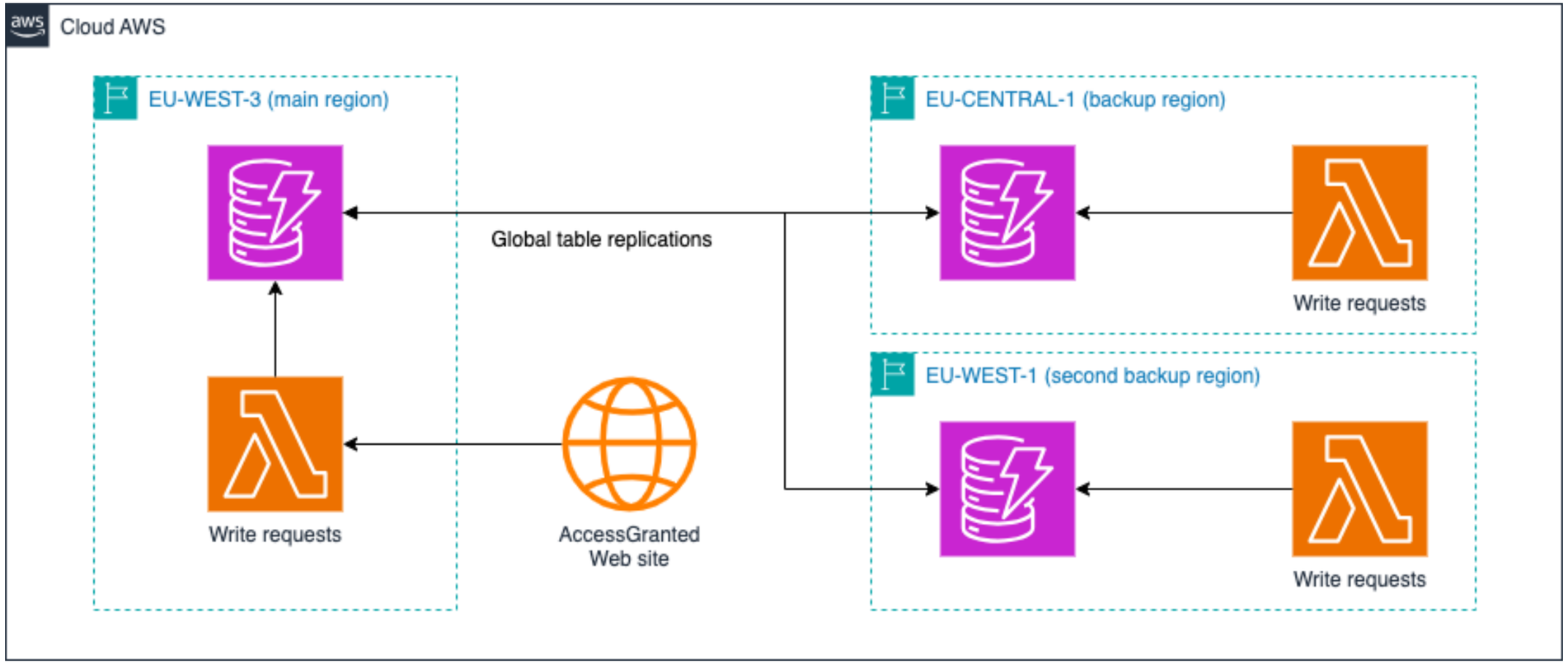
General overview



High Availability

DynamoDB

Active-active replication over 3 regions



DynamoDB

Global tables

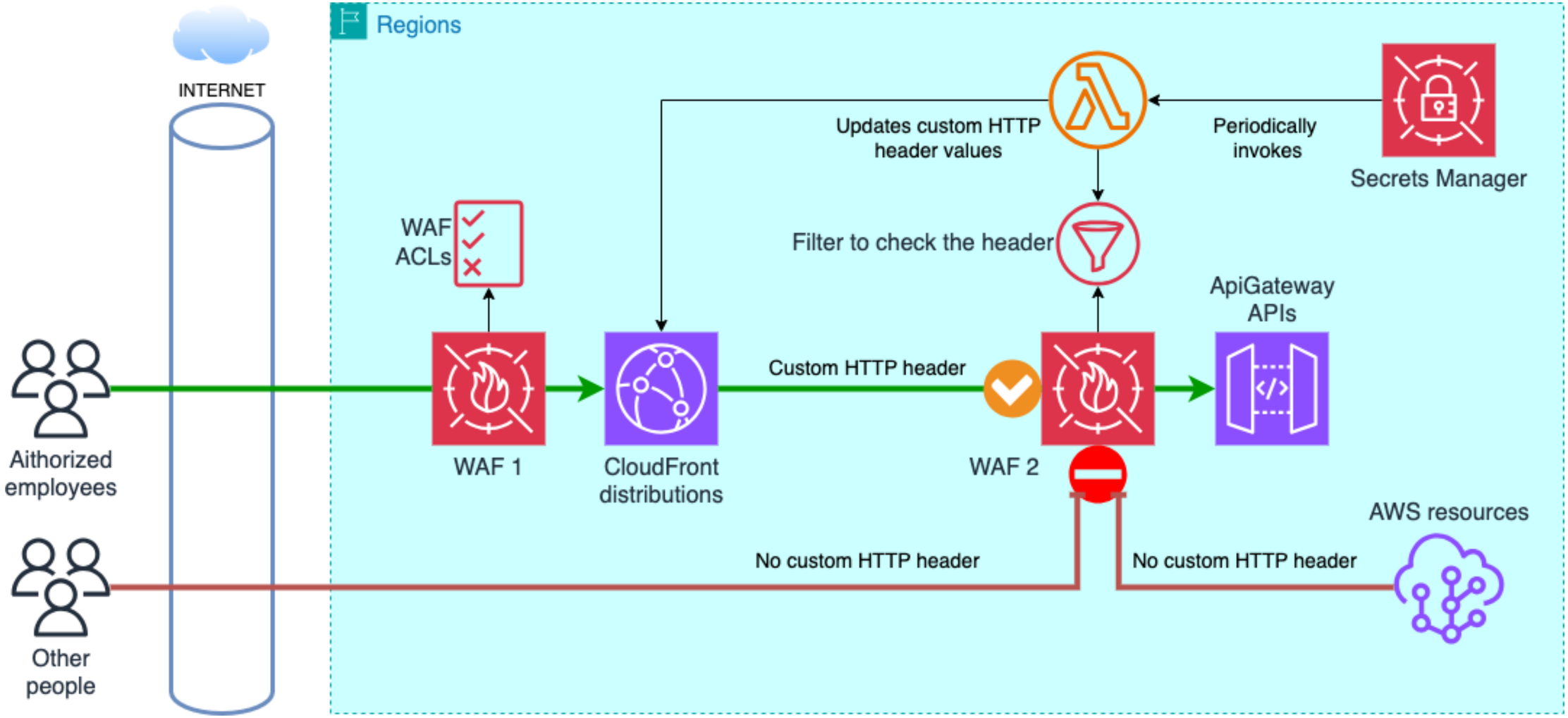
- When users change data (eg. registration of a new remote controller), these changes are automatically replicated in real time to the backup regions.
- The global distribution of this database (global table) across several regions not only allows multi-active replication (mentioned above), but also multi-regional fault tolerance.
- For accessgranted.com, in the event of a disaster, it becomes available again almost instantly (high availability of 99.999%).

Enforced security

Enhanced security for web queries

Double WAF combined with Secrets Manager

- Requests must go through two WAFs before reaching AccessGranted APIs.
  - The first WAF (deployed on CloudFront) adds a custom HTTP header to the request with a secret value.
  - The second WAF (deployed on the API GateWay APIs), only allows the request through if it holds the same secret value.
- Secrets Manager is set up with a Lambda function that changes periodically the custom HTTP header.
- Requests can’t reach AccessGranted APIs unless they’re checked by the first WAF, whether from the Internet or from inside AWS.


Regions
INTERNET
Updates custom HTTP header values
Periodically invokes
Secrets Manager
WAF ACLs
Filter to check the header
ApiGateway APIs
Custom HTTP header
Aithorized employees
WAF 1
CloudFront distributions
WAF 2
AWS resources
No custom HTTP header
No custom HTTP header
Other people

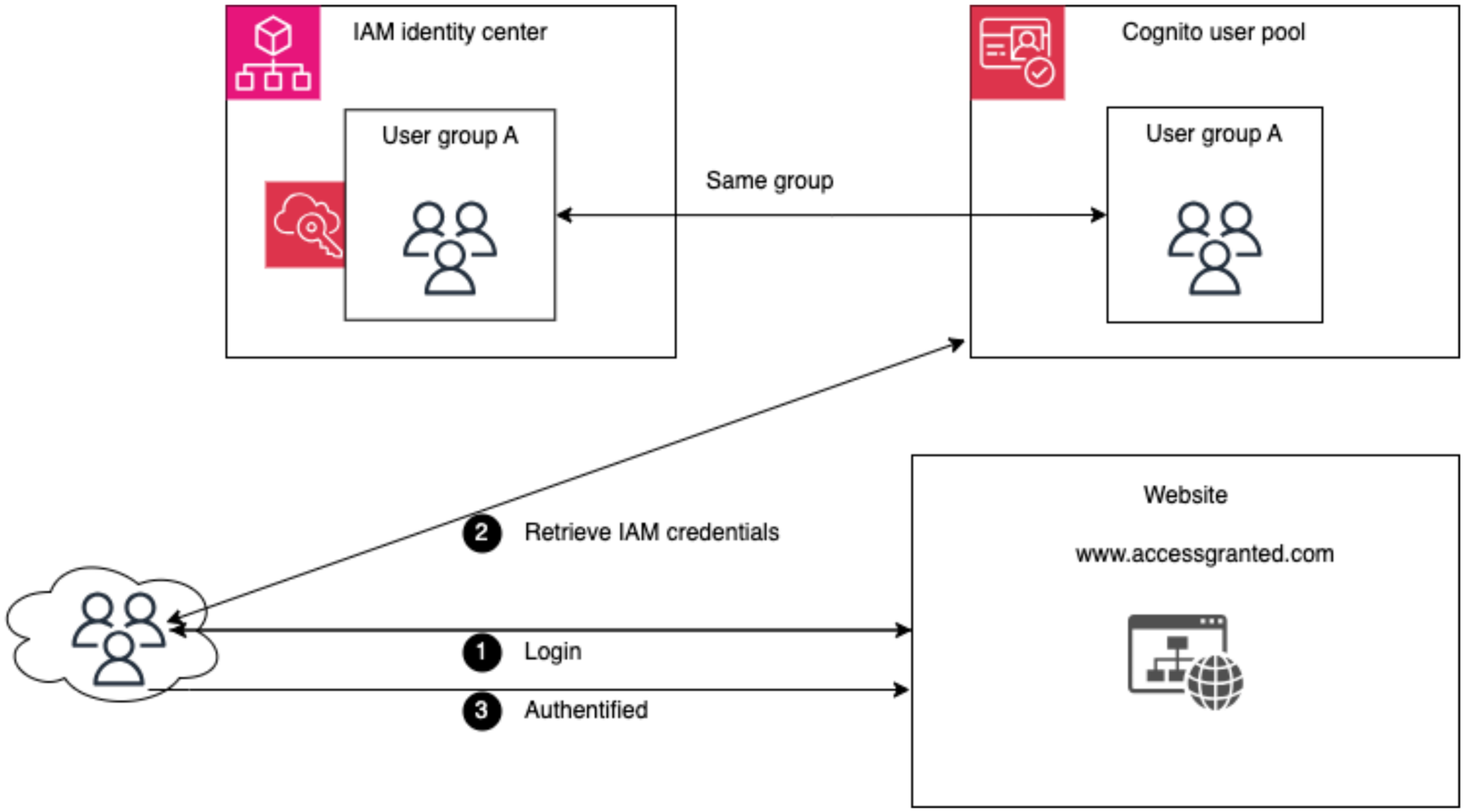
Enhanced security of the AccessGranted APIs

Authentification with AWS Cognito (and MFA)

- Users who are authorized to access the website are employees of the company AccessGranted.
- When users log on to the site, their authentication goes through AWS Cognito (with MFA) which acts as identity provider.
- The temporary token issued by AWS Cognito allows access authorization to the app site. It also contains their registered credentials in the IAM Identity Center which is the identity source.
- Users access the website with their permissions defined beforehand in IAM Identity Centre. The principle of “least privilege” was followed.

Enhanced security of the AccessGranted APIs

Cognito and IAM identity center



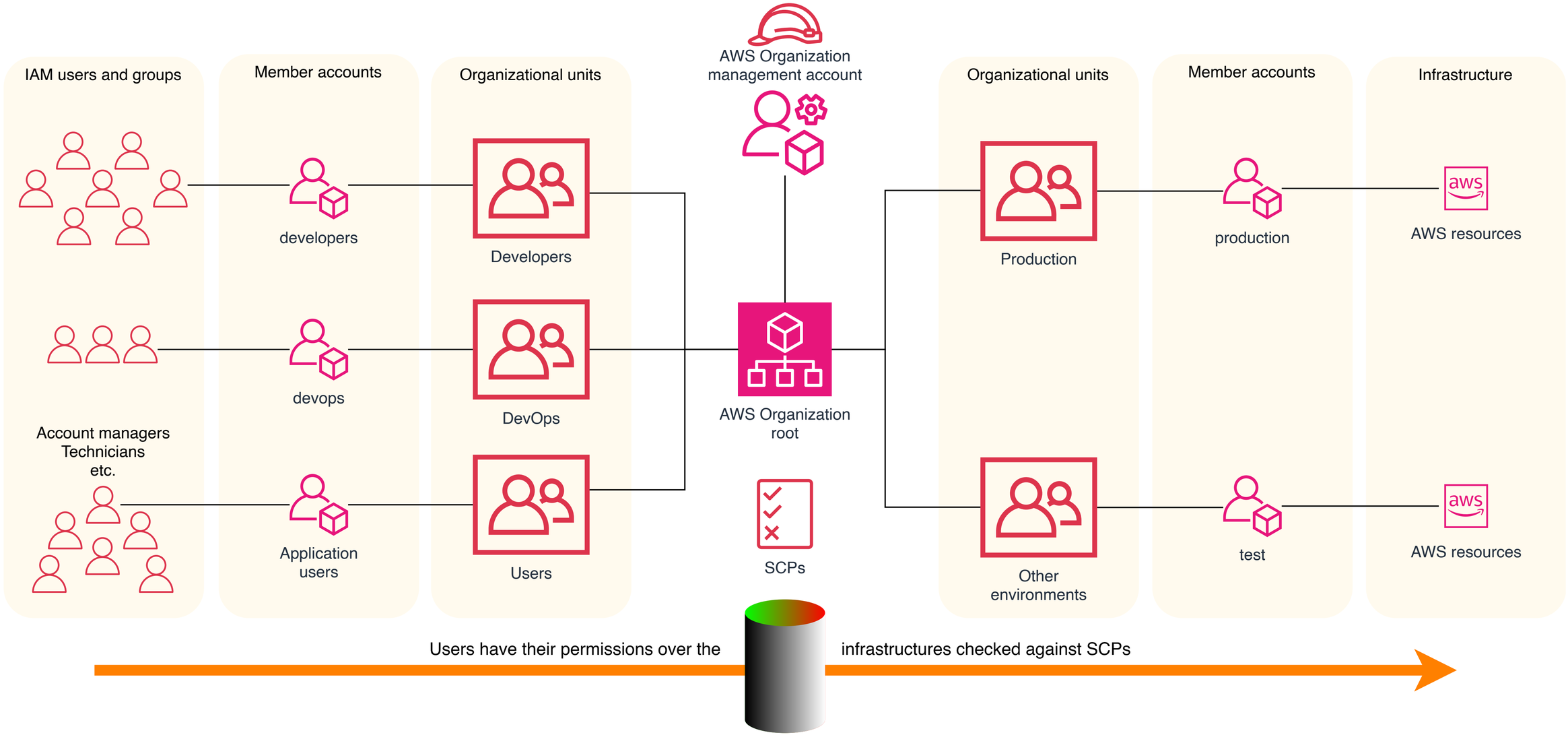
Enhanced security of the AccessGranted APIs

Doorgates authentification with mutual TLS

- Doorgates each have their certificate issued by AWS ACM.
- A Lambda@Edge function is used to request an mTLS enabled API Gateway so only known certificates are authorized.
- Certificates have short lifespan and doorgates receive a new one every month.

AWS Organizations

ORGANIZATIONS



ORGANIZATIONS

- The AccessGranted solution uses **AWS organizations**, a key service for managing access to different infrastructure environments (dev, test, prod, management etc.), where the “least privilege” principle is applied.
- The centralized management of the infrastructure is made up of different organizational units (OUs), employee accounts with different roles and permissions and CloudFormation StackSets.
- The deployment of resources is done in a secure way (thanks to identity / ressource-based policies, SCP, IAM Roles, tags, etc.), as well as their access to other AWS services. The principle of “least privilege” is strongly recommended to give IAM users (developers, managers, technicians) the necessary rights to carry out their tasks.

ORGANIZATIONS

Cost Optimization

- Sharing ressources between accounts via RAM (Ressource Access Manager).
- One invoice for incurred expenses (consolidated billing).
- Other administrative tasks (e.g. creation and management of other member accounts) are made from the root organizational unit management account.
- Monitoring and budget / cost thresholds with AWS Budgets, Cost Explorer, AWS Compute Optimizer.

Disaster Recovery Plan

DRP Pilot Light

RPO - under a minute, RTO - minutes

- As DynamoDB global tables are designed to recover automatically (multi-active replication and multi-regional fault tolerance are included), there is no need to configure what so ever.
- In the backup regions, via CloudFormation template, additional ECS clusters are created with their task and service definitions scaled down to 0 and other core resources like networking.
- Cross-region replication is enabled for static data and logs. The replicated data is encrypted in transit and at rest.
- The backup environment is tested regularly ensuring the latest updates and improvements for a smooth transition.