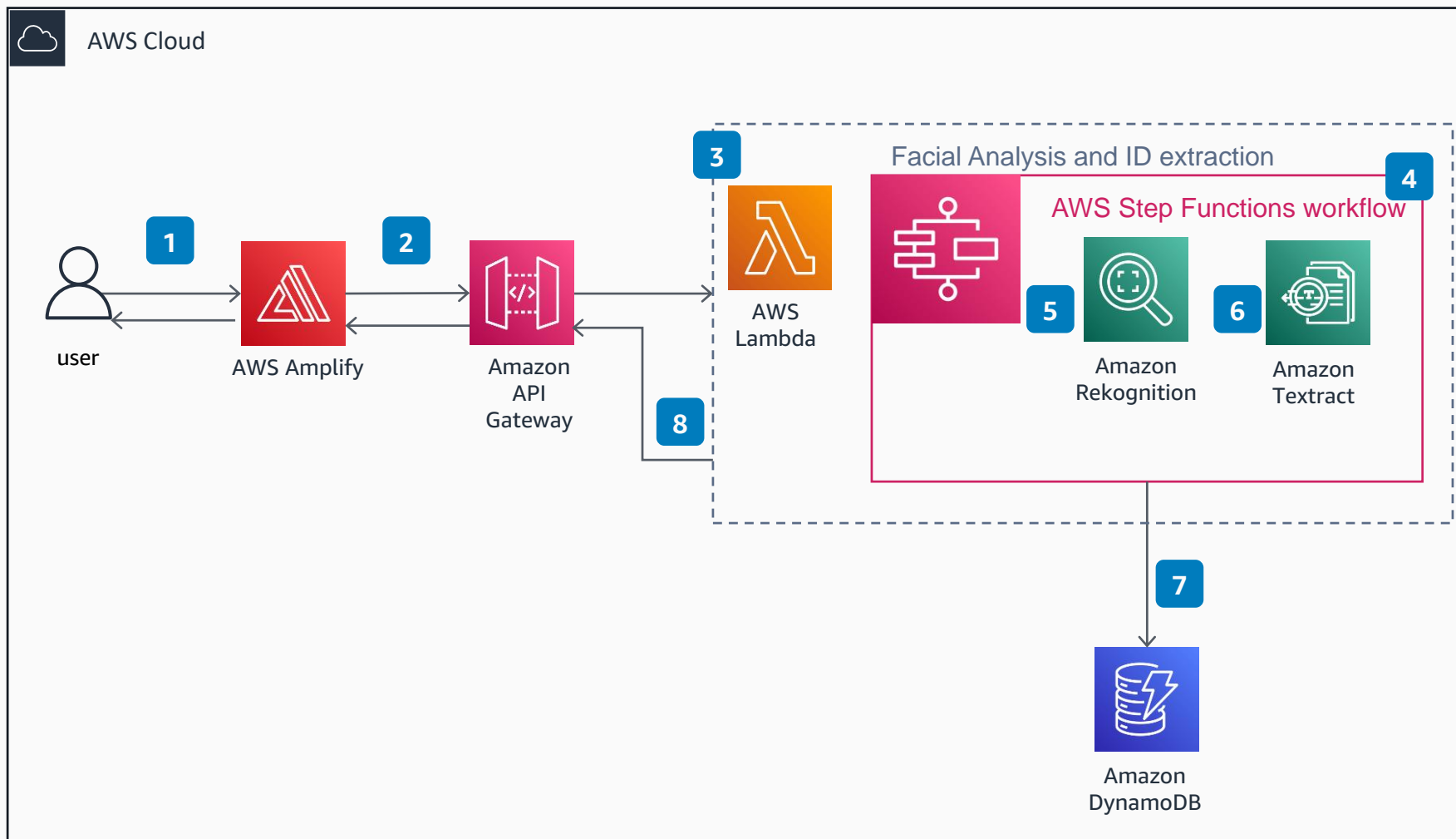


Guidance for Identity Verification on AWS

Onboard and authenticate users in seconds while detecting fraudulent or duplicate accounts

In-person user identity verification is slow to scale, costly, and high friction for users. Machine learning powered facial biometrics can enable online user identity verification.



- 1 Users access the front-end web portal hosted within the **AWS Amplify** and submit a selfie image and/or a valid ID card.
- 2 **AWS Amplify** routes the request to endpoints hosted in Amazon API Gateway
- 3 **Amazon API Gateway** invokes **AWS Lambda** functions to start analysis of submitted image
- 4 User registration and verification is built on **AWS Step Functions** to invoke **Amazon Rekognition** and **Amazon Textract**, which uses machine learning (ML) to understand the context of identity documents such as U.S. passports and driver's licenses without the need for templates or configuration.
- 5 Analysis of user submitted image is performed by **Amazon Rekognition**.
- 6 When user submits an ID card for registration, user information is extracted using **Amazon Textract**.
- 7 This information is stored in **Amazon DynamoDB**.
- 8 Verification status is returned to the front-end web portal.