Amazon Cognito

Amazon Cognito

- Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.
- Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0

Amazon Cognito

- Amazon Cognito User Pools provide a secure user directory that scales to hundreds of millions of users. As a fully managed service, User Pools are easy to set up without any worries about server infrastructure.
- User Pools provide user profiles and authentication tokens for users who sign up directly and for federated users who sign in with social and enterprise identity providers.

Amazon Cognito

- Amazon Cognito provides a built-in and customizable UI for user sign-up and sign-in. You can use Android, iOS, and JavaScript SDKs for Amazon Cognito to add user sign-up and sign-in pages to your apps.
- With Amazon Cognito, your users can sign-in through social identity providers such as Google, Facebook, and Amazon, and through enterprise identity providers such as Microsoft Active Directory using SAML.

Amazon Cognito

- Amazon Cognito provides solutions to control access to AWS resources from your app. You can define roles and map users to different roles so your app can access only the resources that are authorized for each user.
- Users can verify their identities using SMS or a Time-based One-time Password (TOTP) generator, such as Google Authenticator.
- When Amazon Cognito detects users have entered credentials that have been compromised elsewhere, it prompts them to change their password.
- Amazon Cognito is HIPAA eligible and PCI DSS, SOC, and ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

Amazon Cognito – Lambda Triggers

User Pool Flow	Operation	Description
Custom Authentication Flow	**Define Auth Challenge**	Determines the next challenge in a custom auth flow
	Create Auth Challenge	Creates a challenge in a custom auth flow
	Verify Auth Challenge Response	Determines if a response is correct in a custom auth flow
Authentication Events	**Pre Authentication Lambda Trigger**	Custom validation to accept or deny the sign-in request
	Post Authentication Lambda Trigger	Event logging for custom analytics
	Pre Token Generation Lambda Trigger	Augment or suppress token claims
Sign-Up	**Pre Sign-up Lambda Trigger**	Custom validation to accept or deny the sign-up request
	Post Confirmation Lambda Trigger	Custom welcome messages or event logging for custom analytics
	Migrate User Lambda Trigger	Migrate a user from an existing user directory to user pools
Messages	**Custom Message Lambda Trigger**	Advanced customization and localization of messages
Token Creation	**Pre Token Generation Lambda Trigger**	Add or remove attributes in Id tokens

Amazon Cognito – Email Settings

- Certain events in the client app for your user pool might cause Amazon Cognito to email your users. For example, if you configure your user pool to require email verification, Amazon Cognito sends an email when a user signs up for a new account in your app or resets their password.

To handle email delivery, you can use either of the following options:

- The default email functionality that is built into the Amazon Cognito service.
- Your Amazon SES configuration.

Amazon Cognito – App Clients & Domain

- After you create a user pool, you can create an app client to use the built-in webpages for signing up and signing in your users.
- One can specify the Identity Providers, Callback URL on successful sign in, Sign out URLs and the allowed OAuth flows and scopes.

- After setting up an app client, you can configure the address of your sign-up and sign-in webpages. You can use an Amazon Cognito hosted domain and choose an available domain prefix, or you can use your own web address as a custom domain.

Amazon Cognito – Identity Pools

Amazon Cognito identity pools enable you to create unique identities and assign permissions for users. Your identity pool can include:

- Users in an Amazon Cognito user pool
- Users who authenticate with external identity providers such as Facebook, Google, Apple, or a SAML-based identity provider
- Users authenticated via your own existing authentication process

With an identity pool, you can obtain temporary AWS credentials with permissions you define to directly access other AWS services or to access resources through Amazon API Gateway.

Amazon Cognito – Auth Flows

External Provider Authflow

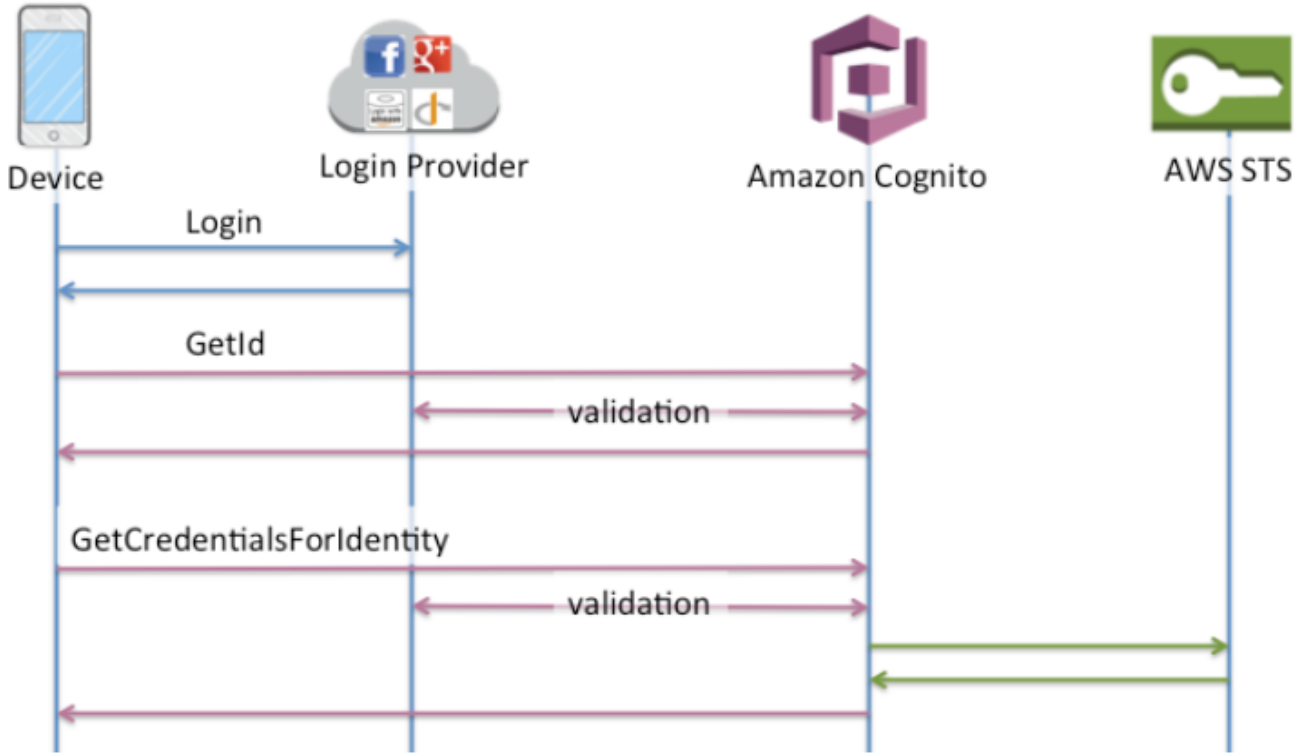
- Enhanced (Simplified) Authflow
- Basic (Classic) Authflow

Developer Authenticated Identities Authflow

- Enhanced Authflow
- Basic Authflow

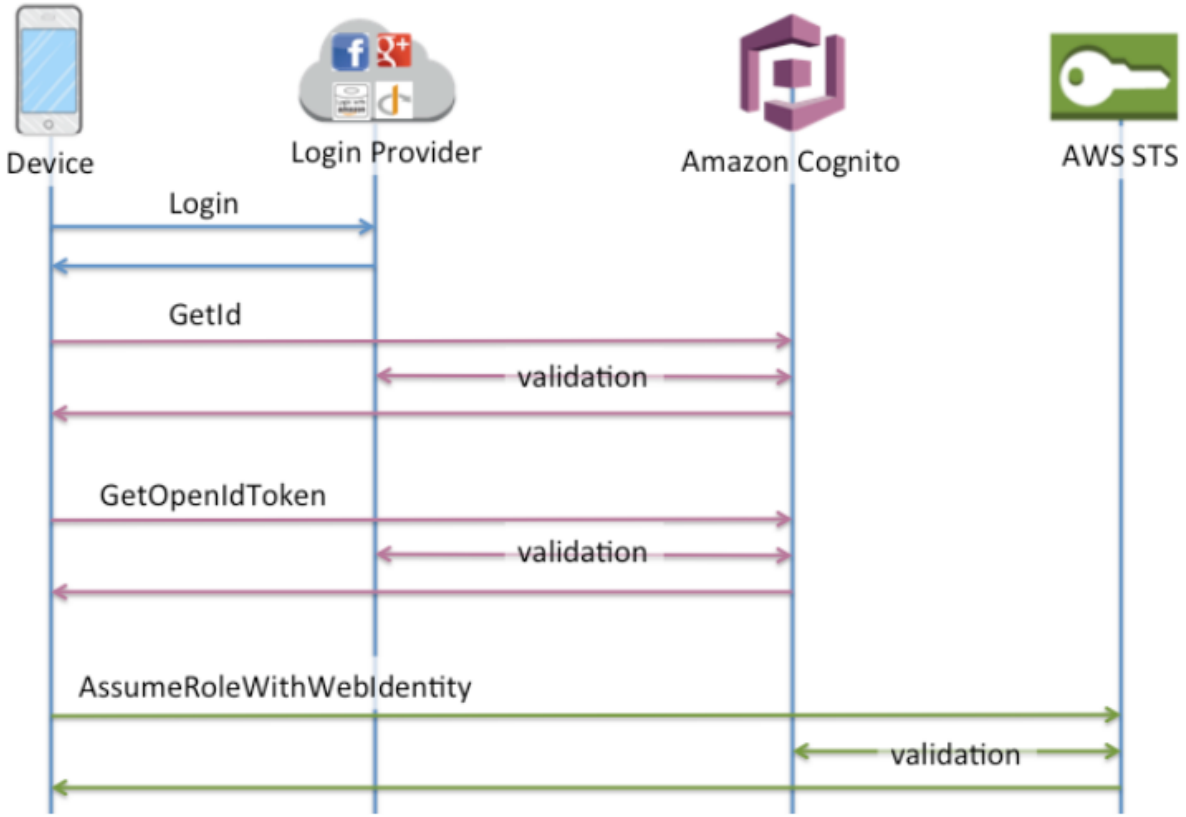
Amazon Cognito – Auth Flows

External Provider Authflow – Enchanced Simplified Authflow



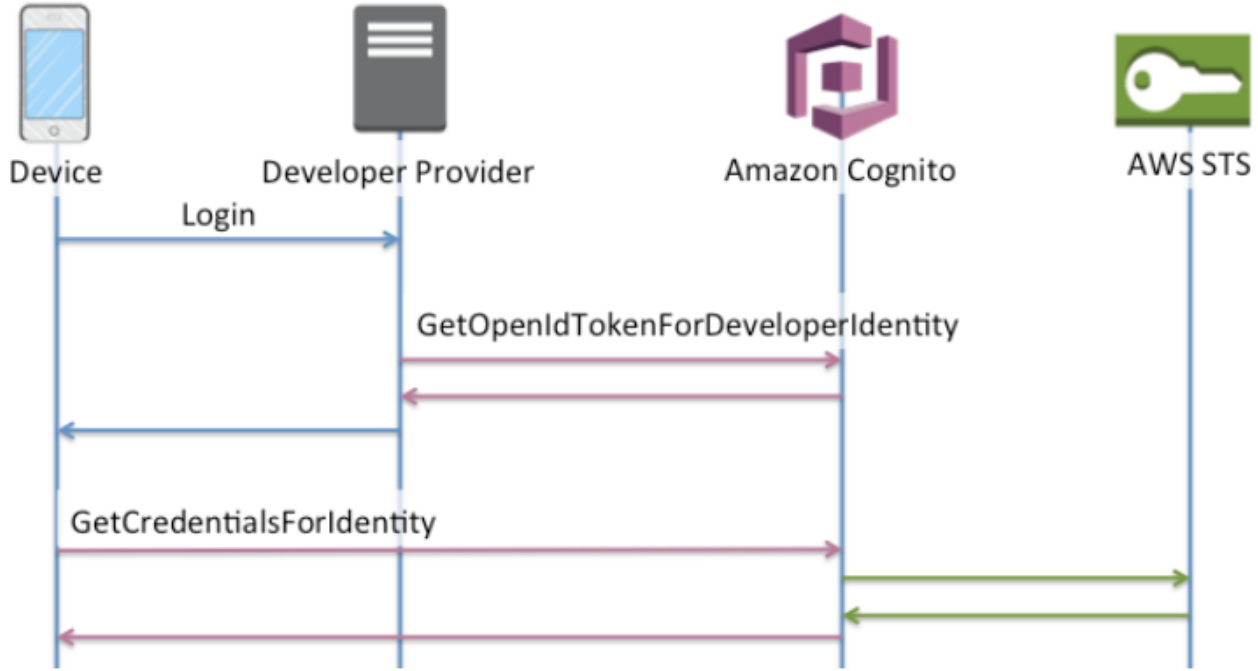
Amazon Cognito – Auth Flows

External Provider Authflow – Basic Classic Authflow



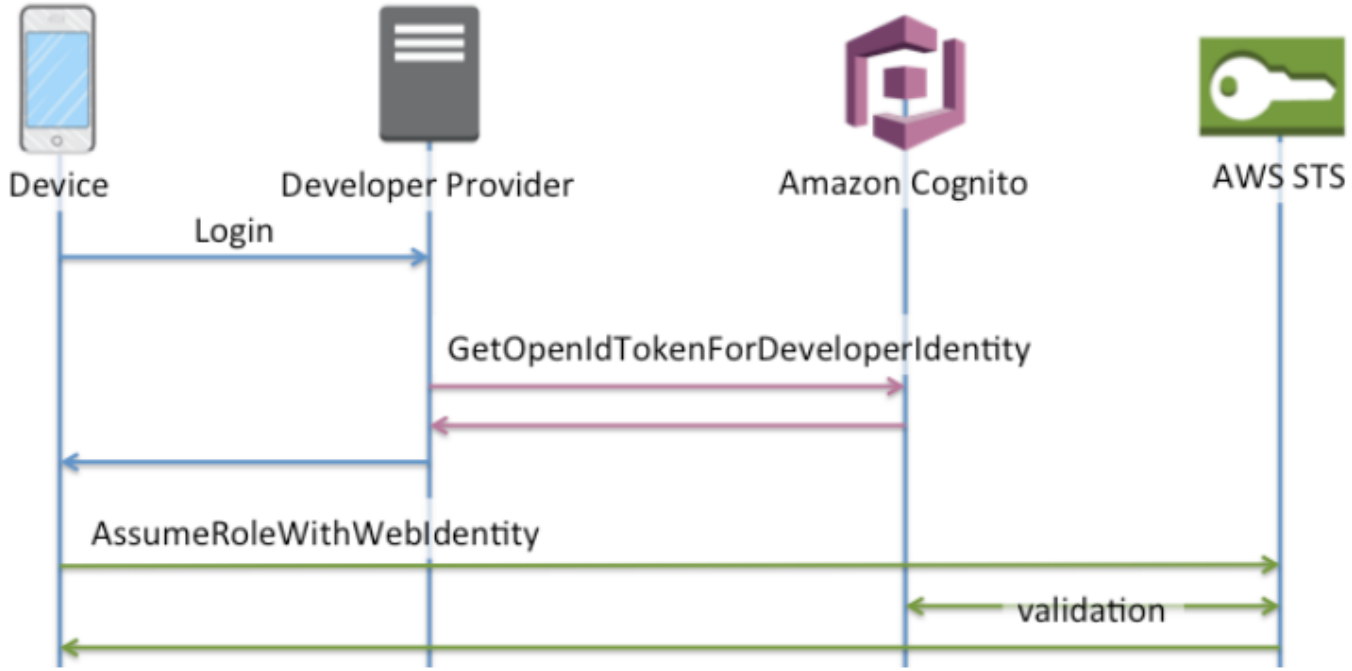
Amazon Cognito – Auth Flows

Developer Authenticated Identity Authflow – Enhanced Authflow



Amazon Cognito – Auth Flows

Developer Authenticated Identity Authflow – Basic Authflow



Amazon Cognito

- **AssumeRoleWithWebIdentity** - Returns a set of temporary security credentials for users who have been authenticated in a mobile or web application with a web identity provider. Example providers include Amazon Cognito, Login with Amazon, Facebook, Google, or any OpenID Connect-compatible identity provider. Temporary security credentials created by AssumeRoleWithWebIdentity last for one hour. This setting can have a value from 1 hour to 12 hours.

Amazon Cognito

- **AssumeRoleWithSAML** - Returns a set of temporary security credentials for users who have been authenticated via a SAML authentication response. This operation provides a mechanism for tying an enterprise identity store or directory to role-based AWS access without user-specific credentials or configuration

Amazon Cognito

- **Role Based Access Control** - Amazon Cognito identity pools assign your authenticated users a set of temporary, limited privilege credentials to access your AWS resources. The permissions for each user are controlled through IAM roles that you create. You can define rules to choose the role for each user based on claims in the user's ID token. You can define a default role for authenticated users. You can also define a separate IAM role with limited permissions for guest users who are not authenticated.

Amazon Cognito - Security

- Amazon Cognito conforms to the AWS shared responsibility model, which includes regulations and guidelines for data protection.
- For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM), so that each user is given only the permissions necessary to fulfill their job duties

Amazon Cognito - Security

- Use multi-factor authentication (MFA) with each account.
- Use TLS to communicate with AWS resources.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.

Amazon Cognito - Security

Encryption at Rest

- Data within Cognito is encrypted at rest in accordance with industry standards.

Encryption in Transit

- All requests to Cognito must be made over the Transport Layer Security protocol (TLS). Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Amazon Cognito – Logging & Monitoring

- Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Cognito and your other AWS solutions.
- Amazon Cloudwatch Metrics – SignUpSuccesses, SignInSuccesses etc
- AWS CloudTrail – CreateIdentityPool, DeleteIdentityPool, ListIdentityPools etc..

Amazon Cognito – Security Best Practices

- Multi-factor authentication (MFA) increases security for your app by adding another authentication method, and not relying solely on user name and password. You can choose to use SMS text messages, or time-based one-time (TOTP) passwords as second factors in signing in your users.