axway

Clear for takeoff? Make sure your open banking passes security first.

Open banking channels allow sensitive financial data to travel between a bank's core system and third-party providers (TPPs). But before open banking data heads to its destination, it must stop for what should be a thorough security screening.

Here's what a checkpoint should entail — and how Axway Amplify Open Banking acts as an always-on-duty security guard.

Axway's robust open banking security scan

Identity authentication

Confirms that the user's identity has been verified, whether the bank manages this directly (brokered) or provides templates for third-party validation (federated).

Consent grant interface

Checks that the user has explicitly consented. This step is managed via an interface with customizable options on what data is shared and with whom.

Advanced consent management

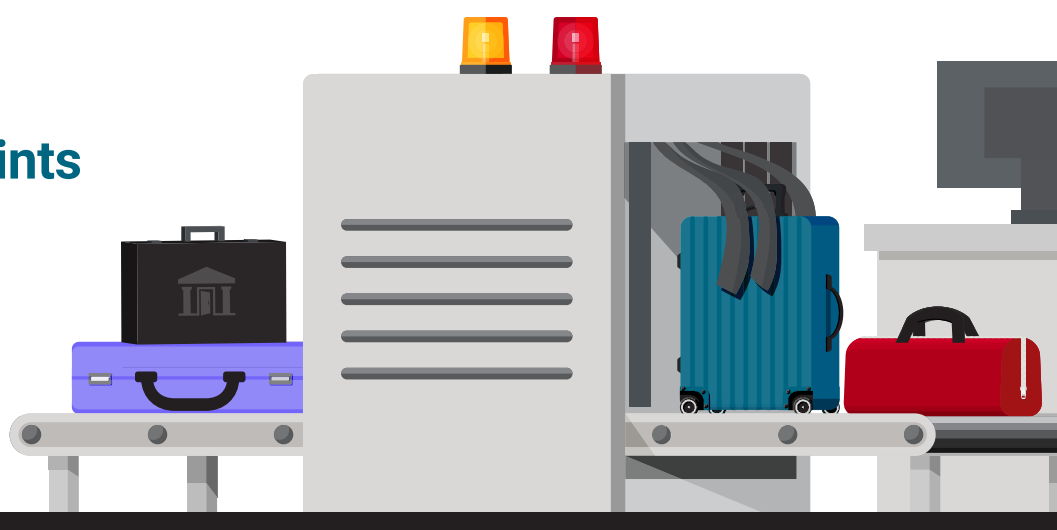
Verifies that end-user consent is still valid and hasn't been revoked. The bank can review and manage consents through a dashboard and offer customers control via mobile APIs.

Custom claims validation

Checks to see if any special data requests have been made — like additional fields outside standard open banking APIs. Verifies that claims are allowed and signed if required.

An open banking framework needs rigorous security checkpoints

With Amplify Open Banking, your financial institution can confidently clear data for departure.



Axway: your co-pilot for business growth

Securing data across open banking channels is about more than compliance. When TPPs know sensitive data is protected and customer privacy is respected, they're more likely to partner with you, expanding your ecosystem and generating new revenue.

Meet your need for open banking agility.

Watch the Demo

axway