Part B: Payment Flow Explanation

Key Steps:

When a customer checks out. The website calls the Backend or PaymentService to create PaymentRequest. First backend will create PaymentRequest with status PENDING and Idempotency-key to avoid duplicate payment. This request will save into 2 dbs PaymentRequests and PaymentLogs. PaymentRequests stores all requests and PaymentLogs created for store all action in our system using PaymentRequestId to access each record.

Then PaymentService calls PaymentGateway to make request payment intent. and paymentGateway return payment url to PaymentService and PaymentService return to Frontend. After frontend redirect user to paymentPage. Users enter their personal payment data directly to paymentGateway. After users submit their payment there will be a webhook to update paymentStatus back to PaymentService. And paymentService will also update db requests and logs.

After all payments finish paymentGateway will redirect the user back to frontend SuccessPage.

Handling Failures & Reliability:

Idempotency needs for avoid duplicate payment requests if user double submit.

The webhook is also idempotent. If the gateway retries sending the webhook, the system checks the current payment status before applying updates to prevent double processing.

If a paymentStatus is in PENDING for too long. it can be turn into EXPIRED to prevent too many requests.

If a webhook had failed, the system should return a failed response (500) so the gateway can retry.

Security Considerations:

Webhook requests are validated using signature verification to ensure they are sent by the payment gateway. Invalid requests are rejected.

Sensitive card information is never stored or processed on our PaymentService to avoid data leak and create trust for user that their data are secure.

Monitoring & Alerts:

I think if we had metrics, we would send every time payment process and send status and time. we can monitor on grafana how our system works. and also add alerts to slack or social apps to notify it-team when the system failed.