

# Buku payment gateway

*by Penerbit Seribu Bintang*

---

**Submission date:** 10-May-2023 08:55PM (UTC-0400)

**Submission ID:** 2089942783

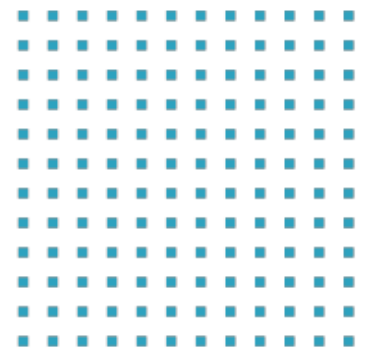
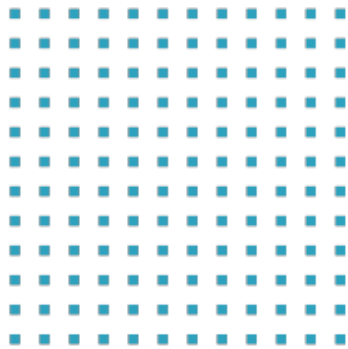
**File name:** Buku\_Payment.docx (8.45M)

**Word count:** 17670

**Character count:** 121376

**Soetam Rizky Wicaksono**

# Konsep Dasar Payment Gateway



# *Konsep Dasar Payment Gateway*

7

**Soetam Rizky Wicaksono**

## **Penerbit**

CV. Seribu Bintang

Malang – Jawa Timur - Indonesia

Profile : [www.SeribuBintang.co.id](http://www.SeribuBintang.co.id)

Katalog : [www.SeribuBintang.web.id](http://www.SeribuBintang.web.id)

Email : [info@seribubintang.co.id](mailto:info@seribubintang.co.id)

FB : [www.fb.com/cv.seribu.bintang](http://www.fb.com/cv.seribu.bintang)

IG : [@penerbitseribubintang](https://www.instagram.com/penerbitseribubintang)

Anggota IKAPI no. 320/JTI/2021



**e-ISBN :**

40

**Edisi Pertama, Desember 2021**  
**Hak Cipta dilindungi oleh Undang-undang**

# Pengantar

Buku ini disusun dengan tujuan untuk mengisi kekosongan literatur tentang payment gateway dalam bahasa Indonesia. Telah menjadi suatu kesadaran bahwa karya tulis yang membahas topik ini sangat jarang ditemukan, terutama dalam bahasa yang mudah diakses oleh masyarakat Indonesia. Oleh karena itu, buku ini diharapkan dapat menjadi referensi yang berharga bagi para akademisi dan praktisi yang tertarik untuk mempelajari dan menggali lebih dalam mengenai payment gateway.

Selain itu, buku ini juga dirancang untuk menjadi buku ajar yang dapat digunakan dalam proses pembelajaran di program studi manajemen maupun sistem informasi. Dengan pendekatan yang komprehensif dan terstruktur, buku ini mencakup berbagai aspek payment gateway mulai dari sejarah, perkembangan, prinsip kerja, regulasi, hingga integrasi dengan platform bisnis dan manajemen operasional.

Diharapkan buku ini dapat membantu para pembaca untuk meningkatkan pengetahuan dan keterampilan mereka dalam bidang payment gateway, serta menginspirasi mereka untuk terus belajar dan mengeksplorasi topik ini lebih lanjut. Dengan demikian, buku ini diharapkan dapat menjadi kontribusi yang

signifikan bagi perkembangan ilmu pengetahuan dan praktik di bidang manajemen dan sistem informasi, khususnya dalam konteks pembayaran digital dan payment gateway.

Setelah mempelajari konsep payment gateway melalui buku ini, para pembaca diharapkan dapat menggali lebih dalam keilmuan lain yang berkaitan dengan payment gateway dan sistem pembayaran digital. Dari sudut pandang manajemen, pembaca dapat mempelajari strategi bisnis, manajemen risiko, dan pemasaran dalam konteks industri fintech dan e-commerce. Topik seperti inovasi bisnis, inklusi keuangan, dan pengaruh teknologi terhadap perubahan perilaku konsumen juga relevan untuk dipelajari. Sementara itu, dari sudut pandang sistem informasi dan teknis, pembaca dapat memperdalam pemahaman mereka tentang teknologi yang mendukung payment gateway dan sistem pembayaran digital, seperti teknologi enkripsi, keamanan siber, dan pengembangan aplikasi.

***Malang, April 2023***

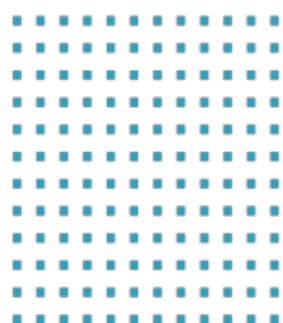
***Soetam Rizky Wicaksono***

# Daftar Isi

iii

<b>Konsep Dasar.....</b>	<b>1</b>
Pendahuluan.....	2
Mengapa dibutuhkan.....	5
Sejarah dan Perkembangan .....	11
<b>Prinsip Kerja.....</b>	<b>15</b>
Pendahuluan.....	16
Inisiasi Transaksi.....	20
Enkripsi Data .....	23
Pengiriman Data ke Processor .....	25
Otorisasi Transaksi.....	28
<b>Jenis Payment Gateway.....</b>	<b>34</b>
Jenis Utama .....	35
Hosted Payment Gateway .....	38
Non-Hosted Payment Gateway .....	40
API-Based Payment Gateway.....	42
Payment Gateway Lokal .....	45
Payment Gateway Internasional .....	50
<b>Regulasi dan Kepatuhan .....</b>	<b>56</b>
Pendahuluan.....	57
Peraturan BI 2016 .....	63
Peraturan BI 2018.....	67
Peraturan OJK.....	71
PCI DSS.....	74
Kartu .....	77
Regulasi Internasional .....	80
<b>Integrasi Platform Bisnis .....</b>	<b>84</b>
Pendahuluan.....	85
Pertimbangan Pemilihan .....	88

Integrasi Teknis.....	93
Integrasi perangkat keras dan perangkat lunak .....	97
Evaluasi Integrasi.....	99
<b>Manajemen Operasional .....</b>	<b>102</b>
Pendahuluan.....	103
Fraud.....	106
Refund dan Sengketa.....	118
<b>E-Money dan E-Wallet .....</b>	<b>123</b>
Relasi .....	124
QR Code.....	129
<b>Kondisi dan Peluang .....</b>	<b>132</b>
Kondisi .....	133
Integrasi Blockchain .....	136
Pembayaran lintas batas .....	140
Peluang di Indonesia .....	144
Peluang Riset.....	163
<b>Penutup .....</b>	<b>164</b>
<b>Referensi.....</b>	<b>164</b>
<b>Glosarium .....</b>	<b>164</b>



6

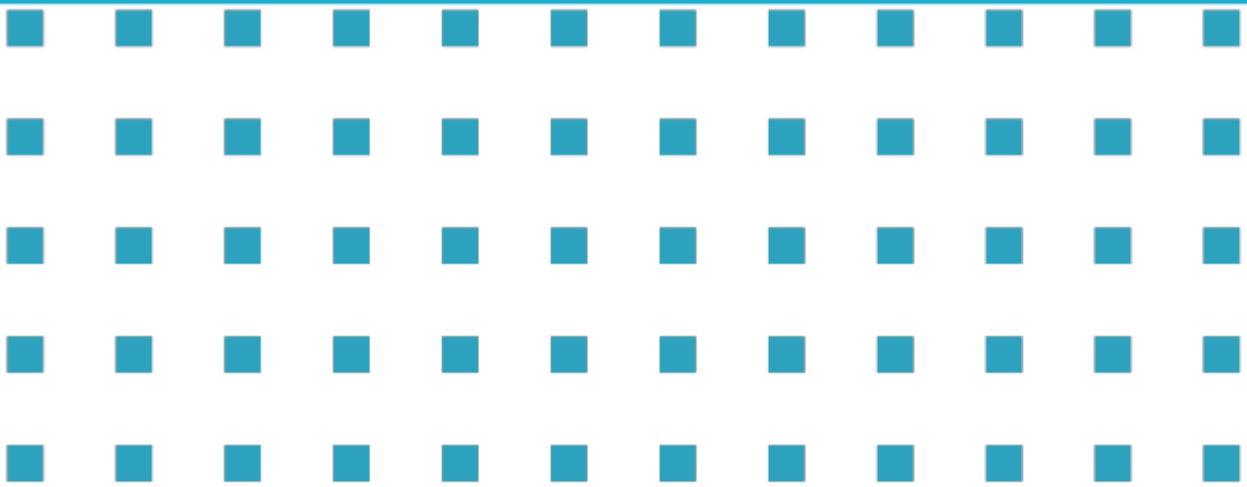
*Kekayaan adalah saat kita merasa cukup dengan apa yang kita miliki*

*Kemiskinan adalah saat kita merasa kurang dengan apa yang kita miliki*



1

# Konsep Dasar



# Pendahuluan

Sebelum memahami lebih jauh mengenai payment gateway, penting untuk mengetahui berbagai definisi payment gateway dari sudut pandang sistem informasi, manajemen, perbankan, dan keuangan.

## Sudut Pandang Sistem Informasi:

Dari sudut pandang sistem informasi, payment gateway adalah sistem perantara yang menghubungkan platform e-commerce atau aplikasi bisnis dengan sistem perbankan untuk mengotomatisasi dan memproses transaksi pembayaran secara online. Payment gateway bertindak sebagai penghubung antara penjual, pembeli, dan bank, memungkinkan pertukaran informasi dan verifikasi transaksi secara cepat dan aman.

### Sudut Pandang Manajemen:

Dalam konteks manajemen, payment gateway adalah alat yang memungkinkan bisnis untuk mengelola transaksi keuangan secara efisien dan efektif. Payment gateway membantu bisnis mengoptimalkan proses pembayaran, mengurangi biaya operasional, serta meningkatkan kepuasan pelanggan melalui kemudahan dan kecepatan pembayaran. Selain itu, payment gateway juga membantu perusahaan dalam mengelola risiko, seperti fraud, dan memastikan kepatuhan terhadap regulasi yang berlaku.

### Sudut Pandang Perbankan:

Dari perspektif perbankan, payment gateway adalah infrastruktur yang memfasilitasi transaksi pembayaran antara rekening bank, kartu kredit, atau metode pembayaran lainnya melalui internet. Payment gateway memungkinkan bank untuk memproses transaksi dengan cepat, akurat, dan aman, serta meningkatkan layanan yang diberikan kepada nasabah dalam bentuk transaksi yang lebih mudah dan fleksibel.

### Sudut Pandang Keuangan:

Dalam konteks keuangan, payment gateway adalah mekanisme yang memungkinkan transfer dana secara real-time antara pembeli dan penjual melalui sistem perbankan atau penyedia layanan keuangan lainnya. Payment gateway memfasilitasi transaksi keuangan dengan mengurangi hambatan dan biaya yang terkait dengan transaksi, serta memastikan keamanan dan integritas data yang dikirimkan selama proses pembayaran.

Secara keseluruhan, payment gateway adalah komponen penting dalam ekosistem <sup>127</sup> pembayaran online yang memungkinkan transaksi keuangan cepat, aman, dan mudah bagi semua pihak yang terlibat, baik itu bisnis, konsumen, atau institusi keuangan.



# Mengapa dibutuhkan

Payment gateway dibutuhkan karena sejumlah alasan penting, yang mencakup kecepatan, keamanan, kemudahan, integrasi, serta manajemen dan pengendalian risiko.

## Kecepatan Transaksi:

Dalam era digital saat ini, kecepatan menjadi salah satu faktor kunci dalam transaksi. Payment gateway memungkinkan transaksi pembayaran online yang cepat dan efisien. Hal ini sangat penting dalam bisnis e-commerce dan aplikasi berbasis layanan, di mana kecepatan transaksi memiliki dampak langsung pada kepuasan pelanggan dan volume penjualan.

## Keamanan:

Keamanan informasi dan data keuangan pelanggan sangat penting dalam transaksi online. Payment gateway membantu memastikan keamanan transaksi dengan mengenkripsi data sensitif seperti informasi kartu kredit atau rekening bank. Selain itu, payment gateway juga mematuhi standar keamanan internasional seperti PCI DSS (Payment Card Industry

Data Security Standard) yang menjamin perlindungan data keuangan pelanggan.

### **Kemudahan :**

Payment gateway menyederhanakan proses pembayaran dengan menyediakan berbagai metode pembayaran dalam satu platform, seperti kartu kredit, debit, e-wallet, dan transfer bank. Hal ini memudahkan pelanggan untuk melakukan pembayaran sesuai dengan pilihan mereka, sehingga meningkatkan kepuasan pelanggan dan mengurangi jumlah pembatalan transaksi.

### **Integrasi :**

Payment gateway memungkinkan integrasi yang mudah dengan platform e-commerce, aplikasi, dan sistem manajemen bisnis lainnya. Integrasi ini memungkinkan bisnis untuk mengotomatisasi proses pembayaran, mengurangi kesalahan manual, dan meningkatkan efisiensi operasional.

### **Manajemen dan Pengendalian Risiko:**

Payment gateway membantu bisnis mengelola dan mengendalikan risiko yang terkait dengan transaksi online, seperti fraud dan chargeback. Payment gateway memiliki sistem deteksi dan pencegahan penipuan yang canggih untuk mengidentifikasi

transaksi yang mencurigakan dan melindungi bisnis dari potensi kerugian.

### Kepatuhan Regulasi:

Payment gateway memastikan bisnis mematuhi regulasi dan peraturan yang berlaku di industri pembayaran, seperti anti pencucian uang (AML) dan perlindungan konsumen. Kepatuhan terhadap regulasi ini membantu bisnis menjaga reputasi yang baik dan menghindari denda atau sanksi hukum.

Secara keseluruhan, payment gateway sangat dibutuhkan dalam dunia bisnis saat ini, terutama dalam sektor e-commerce dan layanan berbasis aplikasi. Payment gateway membantu memastikan transaksi yang cepat, aman, dan mudah bagi pelanggan, serta memberikan dukungan dalam manajemen risiko dan kepatuhan regulasi bagi bisnis.



---

***Payment gateway membantu memastikan keamanan transaksi dengan mengenkripsi data sensitif seperti informasi kartu kredit atau rekening bank.***

---

## *Relasi dengan Perbankan*

---

Relasi antara payment gateway dan industri perbankan pada umumnya saling mendukung dan menguntungkan bagi kedua belah pihak. Payment gateway memfasilitasi transaksi online dan memungkinkan akses yang lebih luas terhadap layanan perbankan, sementara industri perbankan menyediakan infrastruktur dan dukungan yang diperlukan oleh payment gateway. Berikut adalah beberapa contoh dari Indonesia yang menunjukkan bagaimana payment gateway dan industri perbankan saling mendukung:

### **BRI (Bank Rakyat Indonesia) - BRIVA (BRI Virtual Account) :**

BRIVA adalah layanan Virtual Account dari Bank BRI yang memungkinkan bisnis untuk menerima pembayaran dari berbagai kanal seperti ATM, mobile banking, dan internet banking. Layanan ini memudahkan pengguna untuk melakukan pembayaran dengan mudah dan cepat. Bank BRI bekerja sama dengan berbagai payment gateway untuk mengintegrasikan BRIVA dalam sistem pembayaran online mereka, sehingga memungkinkan transaksi yang lebih lancar bagi pelanggan dan peningkatan pendapatan bagi bisnis.



## BRIVA

Kode unik untuk pembayaran pembelian langsung di aplikasi Anda

Buat API

Baca Docs



### Apa itu BRIVA?

Teknologi transaksi keuangan telah berkembang secara pesat. Dulu, untuk melakukan sebuah transaksi digital Anda pergi ke kantor cabang atau ke ATM. Saat ini, telah hadir berbagai solusi untuk menyelesaikan transaksi digital yang mudah dan praktis, salah satunya adalah fitur *virtual account*.

82

**BRIVA** (<https://developers.bri.co.id/id/product/briva>)

## BCA (Bank Central Asia) - BCA KlikPay:

---

BCA KlikPay adalah layanan e-payment dari Bank BCA yang memungkinkan pengguna kartu kredit dan debit BCA untuk melakukan pembayaran online melalui platform e-commerce dan aplikasi layanan. Payment gateway yang bekerja sama dengan BCA KlikPay memungkinkan pelanggan untuk melakukan transaksi dengan cepat dan aman menggunakan akun BCA mereka. Dalam hal ini, BCA dan payment gateway saling mendukung untuk menyediakan layanan yang memudahkan transaksi online bagi pelanggan.

## Tentang BCA KlikPay

Memperkenalkan  
**Cara Bayar Online  
Praktis dan Terpercaya**



### Apa itu BCA KlikPay ?

BCA KlikPay adalah cara bayar belanja online yang praktis dan terpercaya.

### Siapa yang dapat menggunakan BCA KlikPay?

Nasabah yang memiliki fasilitas KlikBCA Individu atau BCA Card.

### BCA Clickpay

(<https://www.klikbca.com/KlikPay/tentangklikpay.html>)

Dari contoh-contoh tersebut, terlihat bahwa relasi antara payment gateway dan industri perbankan di Indonesia pada umumnya saling mendukung dan menguntungkan bagi kedua belah pihak. Payment gateway memfasilitasi transaksi online dan memperluas jangkauan layanan perbankan, sementara bank menyediakan infrastruktur dan dukungan yang diperlukan oleh payment gateway. Kerja sama ini menciptakan ekosistem yang lebih baik bagi pelanggan dan bisnis, serta mendorong pertumbuhan industri e-commerce dan layanan digital di Indonesia.

# Sejarah dan Perkembangan

## Dekade 1990-an:

Pada awal dekade 1990-an, internet mulai berkembang pesat dan mengubah cara orang berkomunikasi, berbisnis, dan mengakses informasi. Pada tahun 1994, Netscape Navigator, salah satu browser web paling awal, diluncurkan. Pada tahun yang sama, SSL (Secure Sockets Layer) diciptakan oleh Netscape untuk menyediakan enkripsi data dan keamanan yang lebih baik dalam transaksi online.

Contoh: Pada tahun 1994, First Virtual Holdings meluncurkan salah satu payment gateway online pertama, yang memungkinkan bisnis untuk menerima pembayaran dengan kartu kredit melalui internet. Meskipun sistem ini memiliki keterbatasan dalam hal kecepatan dan keamanan, ini adalah langkah penting dalam evolusi sistem pembayaran online.

## Dekade 2000-an:

Pada dekade 2000-an, e-commerce mulai berkembang pesat, dan permintaan untuk solusi pembayaran online yang aman dan efisien meningkat. Payment gateway mulai menggunakan teknologi enkripsi

yang lebih canggih dan protokol keamanan seperti 3D Secure untuk melindungi data pelanggan dan mencegah penipuan.

Contoh: PayPal, yang didirikan pada tahun 1998, menjadi salah satu payment gateway paling populer pada dekade 2000-an. PayPal memungkinkan pengguna untuk mengirim dan menerima pembayaran secara online tanpa harus membagikan informasi kartu kredit atau rekening bank mereka. Layanan ini menjadi sangat populer dan diterima secara luas oleh berbagai platform e-commerce dan aplikasi layanan.

#### Dekade 2010-an:

Pada dekade 2010-an, mobile commerce (m-commerce) dan aplikasi layanan berbasis smartphone mulai mendominasi pasar. Payment gateway mulai mengintegrasikan solusi pembayaran seluler seperti e-wallet, NFC (Near Field Communication), dan QR code untuk memudahkan transaksi melalui perangkat seluler.

Contoh: Stripe, didirikan pada tahun 2010, adalah payment gateway yang menawarkan solusi pembayaran online dan seluler yang mudah diintegrasikan ke platform e-commerce dan aplikasi layanan. Stripe memungkinkan bisnis untuk menerima berbagai metode pembayaran, termasuk kartu kredit, e-wallet, dan transfer bank, dengan menggunakan API yang mudah digunakan dan fleksibel.

### Dekade 2020-an:

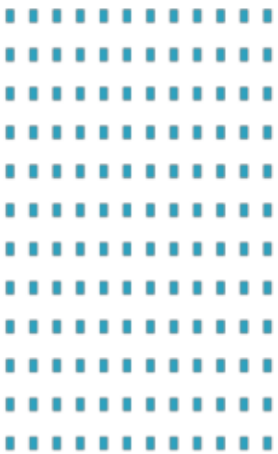
Di dekade 2020-an, payment gateway semakin berkembang untuk menyediakan layanan yang lebih luas dan mencakup berbagai aspek keuangan, seperti manajemen risiko, kepatuhan regulasi, dan analisis data. Selain itu, teknologi seperti blockchain dan mata uang digital mulai mempengaruhi industri pembayaran, yang mungkin mengarah pada inovasi lebih lanjut dalam payment gateway.

Contoh: Adyen, didirikan pada tahun 2006, adalah payment gateway global yang menawarkan solusi pembayaran yang komprehensif dan mencakup berbagai aspek keuangan. Adyen memungkinkan bisnis untuk menerima berbagai metode pembayaran, termasuk kartu kredit, e-wallet, transfer bank, dan mata uang digital, serta menyediakan alat untuk manajemen risiko, kepatuhan regulasi, dan analisis data. Layanan Adyen telah digunakan oleh perusahaan besar seperti Uber, Spotify, dan Microsoft.

Pada dekade 2020-an, kita juga melihat semakin banyak bank dan lembaga keuangan meluncurkan payment gateway mereka sendiri atau bekerja sama dengan penyedia payment gateway untuk menawarkan solusi pembayaran yang lebih terintegrasi dan aman bagi pelanggan.

Contoh: Square, didirikan pada tahun 2009 oleh Jack Dorsey, salah satu pendiri Twitter, adalah perusahaan teknologi keuangan yang menawarkan solusi pembayaran lengkap untuk bisnis kecil dan menengah. Selain payment gateway, Square juga menyediakan perangkat keras pembayaran seperti pembaca kartu dan sistem kasir, serta layanan seperti manajemen inventaris dan analisis data.

Dari sejarah dan perkembangan payment gateway ini, kita dapat melihat bagaimana teknologi telah mempengaruhi dan membentuk industri pembayaran sepanjang waktu. Payment gateway telah berkembang dari sistem pembayaran online sederhana menjadi solusi pembayaran yang kompleks dan komprehensif yang mencakup berbagai aspek keuangan, seperti manajemen risiko, kepatuhan regulasi, dan analisis data. Di masa depan, kita mungkin akan melihat lebih banyak inovasi dalam payment gateway yang akan terus mengubah cara kita melakukan transaksi dan mengelola keuangan.



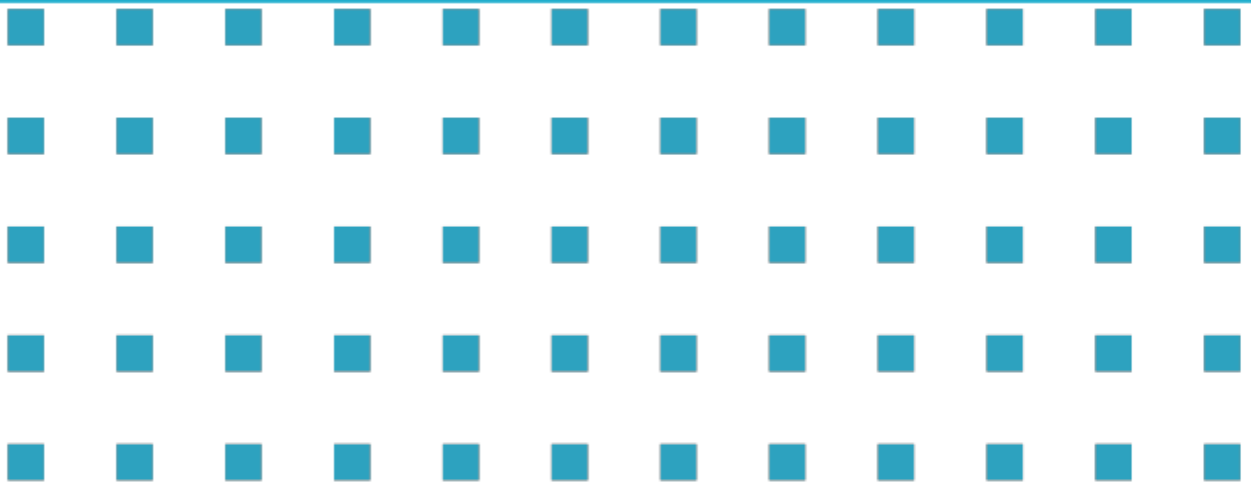
---

***Pada dekade 2010-an, mobile commerce (m-commerce) dan aplikasi layanan berbasis smartphone mulai mendominasi pasar. Payment gateway mulai mengintegrasikan solusi pembayaran seluler seperti e-wallet, NFC (Near Field Communication), dan QR code***

---

2

# Prinsip Kerja



# Pendahuluan

Payment gateway adalah layanan yang memfasilitasi transaksi pembayaran online antara penjual dan pembeli. Prinsip kerja payment gateway melibatkan beberapa langkah penting yang memastikan transaksi berjalan dengan cepat, aman, dan efisien. Berikut adalah penjelasan detail mengenai prinsip kerja dari payment gateway:

## Inisiasi Transaksi:

Pembeli memilih produk atau layanan yang ingin dibeli dari penjual dan melakukan Inisiasi Transaksi checkout melalui platform e-commerce atau aplikasi layanan. Pada titik ini, pembeli akan diminta untuk memasukkan informasi pembayaran, seperti nomor kartu kredit, alamat penagihan, atau informasi rekening bank.



---

***Prinsip kerja payment gateway melibatkan beberapa langkah penting yang memastikan transaksi berjalan dengan cepat, aman, dan efisien.***

---



### Enkripsi Data:

Setelah informasi pembayaran dimasukkan, data tersebut dienkripsi oleh payment gateway untuk melindungi informasi sensitif dari intersepsi atau pengaksesan yang tidak sah. Enkripsi ini biasanya dilakukan menggunakan teknologi SSL (Secure Sockets Layer) atau TLS (Transport Layer Security) yang mengamankan komunikasi antara browser pembeli dan server penjual.

### Pengiriman Data ke Processor:

Data yang telah dienkripsi kemudian dikirimkan oleh payment gateway ke processor (biasanya bank atau lembaga keuangan yang bekerja sama dengan payment gateway) untuk meminta otorisasi transaksi. Processor akan meneruskan informasi tersebut ke penerbit kartu kredit (jika menggunakan kartu kredit) atau bank penerima (jika menggunakan transfer bank atau metode pembayaran lainnya) untuk otorisasi.



---

***Payment gateway menerima pesan otorisasi dan mengirimkan konfirmasi transaksi ke platform e-commerce atau aplikasi layanan, yang kemudian akan memberi tahu penjual dan pembeli bahwa transaksi telah berhasil.***

---

### Otorisasi Transaksi:

Penerbit kartu kredit atau bank penerima akan memeriksa informasi pembayaran dan saldo yang tersedia untuk memastikan bahwa transaksi dapat dilakukan. Jika transaksi disetujui, mereka akan mengirimkan pesan otorisasi kembali ke processor, yang kemudian akan mengirimkannya ke payment gateway.

### Konfirmasi Transaksi:

Payment gateway menerima pesan otorisasi dan mengirimkan konfirmasi transaksi ke platform e-commerce atau aplikasi layanan, yang kemudian akan memberi tahu penjual dan pembeli bahwa transaksi telah berhasil. Proses ini biasanya berlangsung dalam hitungan detik.

### Penyelesaian Transaksi:

Setelah transaksi berhasil, dana akan dipindahkan dari rekening pembeli ke rekening penjual (biasanya melalui rekening merchant yang disediakan oleh payment gateway). Proses penyelesaian transaksi ini biasanya memerlukan waktu beberapa hari kerja, tergantung pada metode pembayaran yang digunakan dan kebijakan antar bank yang terlibat.

### Pemrosesan Biaya dan Komisi:

Sebagai imbalan atas layanan yang disediakan, payment gateway biasanya mengenakan biaya dan komisi atas setiap transaksi yang berhasil. Biaya ini dapat berupa persentase dari jumlah transaksi atau jumlah tetap per transaksi, tergantung pada model bisnis dan perjanjian antara penjual dan payment gateway.


Secara keseluruhan, prinsip kerja payment gateway melibatkan serangkaian langkah yang dirancang untuk memastikan transaksi pembayaran online berjalan dengan cepat, aman, dan efisien. Payment gateway memainkan peran penting dalam melindungi informasi pembayaran yang sensitif, mengelola proses



---

*Enkripsi ini biasanya dilakukan menggunakan teknologi **SSL (Secure Sockets Layer)** atau **TLS (Transport Layer Security)** yang mengamankan komunikasi antara browser pembeli dan server penjual.*

---



# Inisiasi Transaksi

Inisiasi Transaksi adalah langkah pertama dalam proses pembayaran online, di mana pembeli diminta untuk memasukkan informasi pembayaran yang relevan. Berikut adalah penjelasan lebih lanjut mengenai pengisian informasi pembayaran, termasuk metode yang tidak menggunakan kartu dan metode yang menggunakan kode seperti QR:

## Kartu Kredit atau Debit:

Pada metode ini, pembeli harus memasukkan informasi kartu kredit atau debit, seperti nomor kartu, tanggal kadaluwarsa, dan kode CVV (Card Verification Value) yang terdapat di bagian belakang kartu. Selain itu, pembeli juga perlu mengisi alamat penagihan yang terkait dengan kartu tersebut.

## Transfer Bank atau Bank Transfer:

Pembeli dapat memilih untuk melakukan pembayaran melalui transfer bank. Dalam hal ini, pembeli akan diminta untuk memasukkan informasi rekening bank mereka, seperti nomor rekening, nama bank, dan kode bank. Setelah informasi ini dimasukkan, pembeli

akan menerima instruksi tentang cara melakukan transfer ke rekening penjual.

112

### **E-Wallet:**

---

E-wallet atau dompet elektronik adalah metode pembayaran yang memungkinkan pengguna menyimpan informasi keuangan mereka secara digital dan melakukan transaksi tanpa harus memasukkan informasi kartu atau rekening bank setiap kali. Contoh e-wallet meliputi PayPal, Alipay, dan Google Pay. Saat menggunakan metode ini, pembeli akan diminta untuk login ke akun e-wallet mereka dan mengkonfirmasi pembayaran.

### **Pembayaran dengan Kode QR:**

---

Pembayaran dengan kode QR memungkinkan pembeli untuk melakukan transaksi dengan memindai kode QR yang disediakan oleh penjual. Kode QR ini mengandung informasi tentang transaksi, seperti jumlah pembayaran dan identifikasi penjual. Untuk menggunakan metode ini, pembeli akan membuka aplikasi pembayaran yang mendukung pembayaran QR (misalnya, aplikasi e-wallet atau aplikasi perbankan), memindai kode QR, dan mengkonfirmasi pembayaran.

### Mobile Payment (NFC) :

Pembayaran seluler menggunakan teknologi NFC (Near Field Communication) memungkinkan pembeli untuk melakukan transaksi dengan menempelkan perangkat seluler mereka (seperti smartphone) ke terminal pembayaran yang mendukung NFC. Metode ini sering digunakan dalam aplikasi pembayaran seperti Apple Pay, Google Pay, dan Samsung Pay. Untuk menggunakan metode ini, pembeli perlu mengaktifkan aplikasi pembayaran seluler dan menempelkan perangkat mereka ke terminal pembayaran untuk mengkonfirmasi transaksi.

Setiap metode pembayaran ini memiliki proses pengisian informasi pembayaran yang berbeda, dan platform e-commerce atau aplikasi layanan harus mendukung berbagai metode ini untuk memudahkan pembeli dalam melakukan transaksi.



---

***E-wallet atau dompet elektronik adalah metode pembayaran yang memungkinkan pengguna menyimpan informasi keuangan mereka secara digital dan melakukan transaksi tanpa harus memasukkan informasi kartu atau rekening bank***

---

# kripsi Data

8 SSL (Secure Sockets Layer) dan TLS (Transport Layer Security) adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi antara dua sistem (seperti antara browser web dan server web) melalui internet atau jaringan internal. SSL adalah pendahulu dari TLS, dan keduanya dirancang untuk melindungi integritas data dan menjaga kerahasiaan informasi yang dikirimkan antara sistem yang terlibat.

SSL dan TLS bekerja dengan mengenkripsi data yang dikirimkan antara sistem, sehingga informasi sensitif (seperti informasi pembayaran) tidak dapat diakses oleh pihak ketiga yang tidak berwenang. Protokol ini menggunakan sertifikat digital yang disediakan oleh otoritas sertifikasi (Certificate Authority, CA) untuk mengautentikasi identitas sistem yang terlibat dan memastikan bahwa komunikasi terjadi dengan pihak yang benar.

Di Indonesia, ada beberapa standar dan regulasi yang wajib dipenuhi oleh lembaga yang terlibat dalam penggunaan SSL/TLS, khususnya dalam konteks payment gateway dan transaksi keuangan:

1. **Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI)** mengatur kebijakan dan standar untuk industri perbankan dan keuangan. Lembaga yang terlibat dalam penyediaan payment gateway atau layanan keuangan lainnya diwajibkan untuk

mematuhi peraturan yang dikeluarkan oleh OJK dan BI. Peraturan ini mencakup kepatuhan terhadap standar keamanan, penggunaan sertifikat digital yang sah, dan penerapan protokol SSL/TLS yang tepat.

2. **Standar PCI DSS (Payment Card Industry Data Security Standard)** adalah standar keamanan global yang dirancang untuk melindungi data kartu kredit dan informasi pembayaran lainnya. Lembaga yang terlibat dalam penyimpanan, pemrosesan, atau pengiriman data kartu kredit diwajibkan untuk mematuhi standar PCI DSS. Standar ini mencakup persyaratan keamanan seperti penggunaan SSL/TLS yang tepat, enkripsi data yang kuat, dan kebijakan keamanan yang komprehensif.
3. **SNI (Standar Nasional Indonesia)** adalah standar yang dikeluarkan oleh Badan Standardisasi Nasional (BSN) untuk berbagai industri dan sektor di Indonesia, termasuk teknologi informasi dan komunikasi. Meskipun tidak secara spesifik mengatur SSL/TLS, standar SNI yang relevan dengan keamanan sistem informasi dan jaringan dapat mencakup persyaratan keamanan yang berhubungan dengan penggunaan SSL/TLS.

Lembaga yang terlibat dalam penyediaan payment gateway atau layanan keuangan lainnya di Indonesia harus memastikan bahwa mereka mematuhi standar dan regulasi yang berlaku, termasuk penggunaan SSL/TLS yang tepat untuk melindungi komunikasi dan informasi pembayaran.




# Pengiriman Data ke Processor

Jika terjadi kesalahan saat pengiriman data ke processor, berbagai skenario dapat terjadi tergantung pada sifat kesalahan itu sendiri. Berikut adalah beberapa contoh kesalahan yang mungkin terjadi dan dampak yang dapat dihasilkan:

## Kesalahan pada informasi pembayaran:

Jika informasi pembayaran yang dimasukkan oleh pembeli tidak lengkap atau tidak valid (seperti nomor kartu kredit yang salah, tanggal kadaluwarsa yang tidak sesuai, atau kode CVV yang salah), maka processor akan menolak permintaan otorisasi dan mengembalikan pesan kesalahan. Dalam kasus ini, pembeli akan diberitahu tentang kesalahan dan diminta untuk memeriksa dan memperbaiki informasi pembayaran sebelum mencoba lagi.



*Jika terjadi masalah koneksi atau komunikasi antara payment gateway dan processor (misalnya, jaringan internet yang tidak stabil, server yang sibuk, atau gangguan pada sistem), pengiriman data mungkin terhenti atau tertunda.*

### **Kesalahan pada koneksi atau komunikasi:**

---

Jika terjadi masalah koneksi atau komunikasi antara payment gateway dan processor (misalnya, jaringan internet yang tidak stabil, server yang sibuk, atau gangguan pada sistem), pengiriman data mungkin terhenti atau tertunda. Dalam hal ini, pembeli mungkin mengalami penundaan dalam mendapatkan konfirmasi transaksi atau, dalam beberapa kasus, transaksi mungkin gagal sama sekali. Penyedia payment gateway dan processor akan bekerja untuk mengatasi masalah koneksi atau komunikasi ini dan mengembalikan layanan ke kondisi normal sesegera mungkin.

### **Kesalahan pada sistem payment gateway atau processor:**

---

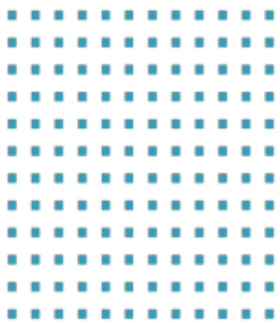
Jika terjadi kesalahan pada sistem payment gateway atau processor itu sendiri (seperti kesalahan perangkat lunak, masalah keamanan, atau kegagalan sistem), pengiriman data dan otorisasi transaksi mungkin terpengaruh. Dalam kasus ini, transaksi mungkin ditunda atau gagal, dan pembeli dan penjual mungkin mengalami gangguan layanan. Penyedia payment gateway dan processor akan berupaya segera untuk mengidentifikasi dan mengatasi masalah sistem ini.

### **Kesalahan pada autentikasi atau otorisasi:**

---

Jika terjadi kesalahan dalam proses autentikasi atau otorisasi (misalnya, sertifikat SSL/TLS yang kedaluwarsa atau tidak valid), maka pengiriman data ke processor mungkin tidak aman atau tidak dapat diverifikasi. Dalam hal ini, transaksi mungkin ditolak untuk melindungi data dan informasi pembayaran pembeli. Penyedia payment gateway dan processor harus memastikan bahwa sertifikat SSL/TLS dan protokol keamanan lainnya selalu up-to-date dan valid.

Dalam semua skenario ini, penyedia payment gateway dan processor harus bekerja sama untuk mengidentifikasi dan mengatasi kesalahan yang terjadi. Selain itu, mereka harus memberikan dukungan kepada pembeli dan penjual yang terkena dampak kesalahan ini, serta mengambil langkah-langkah pencegahan untuk mengurangi kemungkinan kesalahan serupa terjadi di masa mendatang.



---

***Otorisasi transaksi adalah proses verifikasi yang digunakan untuk memastikan bahwa transaksi yang dilakukan sah dan dilakukan oleh pihak yang berwenang.***

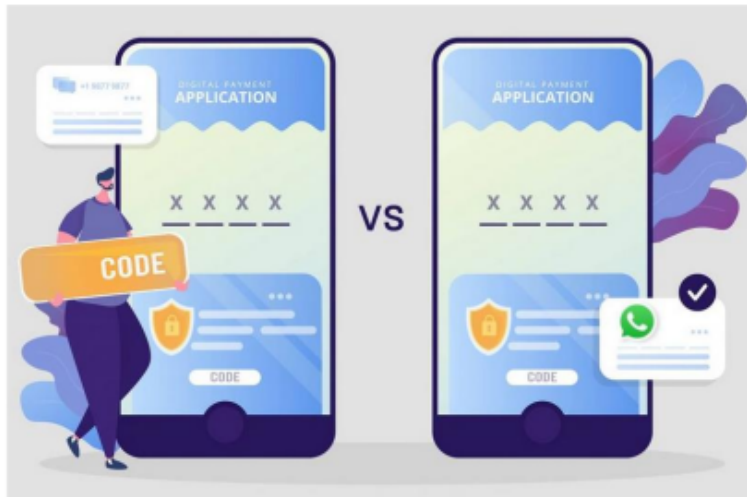
---

# Otorisasi Transaksi

Otorisasi transaksi adalah proses verifikasi yang digunakan untuk memastikan bahwa transaksi yang dilakukan sah dan dilakukan oleh pihak yang berwenang. Berbagai metode otorisasi dapat digunakan untuk mengonfirmasi identitas pengguna dan melindungi transaksi dari penipuan. Berikut adalah beberapa jenis metode otorisasi yang umum digunakan:

## Password atau PIN:

Metode otorisasi yang paling dasar dan umum adalah meminta pengguna memasukkan kata sandi atau nomor identifikasi pribadi (PIN) yang dikaitkan dengan akun mereka. Dalam konteks transaksi keuangan, ini sering digunakan saat melakukan transaksi melalui ATM atau terminal Point of Sale (POS).



Ilustrasi OTP (SMS ataupun WA)

### 50 OTP (One-Time Password) :

---

One-Time Password (OTP) adalah kode unik yang hanya berlaku untuk satu transaksi atau sesi login. Biasanya, OTP dikirimkan melalui SMS atau email ke nomor telepon atau alamat email yang terdaftar pada akun pengguna. Pengguna kemudian harus memasukkan OTP ini untuk mengotorisasi transaksi atau mengakses layanan tertentu. Metode ini menambahkan lapisan keamanan tambahan karena OTP hanya berlaku untuk waktu yang terbatas dan tidak dapat digunakan kembali.

### Token berbasis perangkat :

---

Token berbasis perangkat adalah alat keamanan fisik yang digunakan untuk mengotorisasi transaksi atau akses sistem. Token ini dapat berupa kartu pintar (smart card), kunci USB, atau perangkat lain yang harus dimasukkan atau terhubung ke sistem untuk mengotorisasi akses. Token ini sering kali mengandung sertifikat digital atau kunci enkripsi yang digunakan untuk mengidentifikasi pengguna dan mengamankan transaksi.



36 Contoh Token BCA (sumber: <https://www.bca.co.id/id/informasi/Edukatips/2022/07/28/08/52/yuk-kenal-lebih-dekat-dengan-keybca>)

### Autentikasi multi-faktor (MFA) :

Autentikasi multi-faktor (MFA) adalah pendekatan keamanan yang memerlukan pengguna untuk memberikan dua atau lebih metode otorisasi yang berbeda sebelum mengakses sistem atau layanan. MFA sering kali menggabungkan sesuatu yang diketahui pengguna (seperti kata sandi), sesuatu yang dimiliki pengguna (seperti token berbasis perangkat), dan/atau sesuatu yang merupakan pengguna (seperti data biometrik).

## Biometrik:

---

Otorisasi biometrik melibatkan penggunaan karakteristik fisik atau perilaku yang unik untuk mengidentifikasi dan mengotorisasi pengguna. Beberapa contoh metode biometrik meliputi:

1. **Sidik jari:** Penggunaan sidik jari yang unik untuk mengidentifikasi dan mengotorisasi pengguna. Teknologi ini telah diintegrasikan ke dalam banyak smartphone dan perangkat lain untuk mengamankan akses dan transaksi.
2. **Pengenalan wajah:** Menggunakan teknologi kamera dan pengenalan pola untuk memverifikasi identitas pengguna berdasarkan wajah mereka. Seperti sidik jari, teknologi ini semakin umum dalam smartphone dan perangkat lain.
3. **Pengenalan suara:** Memverifikasi identitas pengguna berdasarkan ciri-ciri unik dari suara mereka. Pengenalan suara sering digunakan dalam sistem otentikasi telepon.
4. **Scan retina atau iris:** Menggunakan teknologi pemindaian mata untuk mengidentifikasi dan mengotorisasi pengguna berdasarkan pola unik pada retina atau iris mereka. Meskipun teknologi ini kurang umum daripada sidik jari atau pengenalan wajah, beberapa perangkat keamanan tingkat tinggi dan sistem akses terkendali menggunakan metode ini.



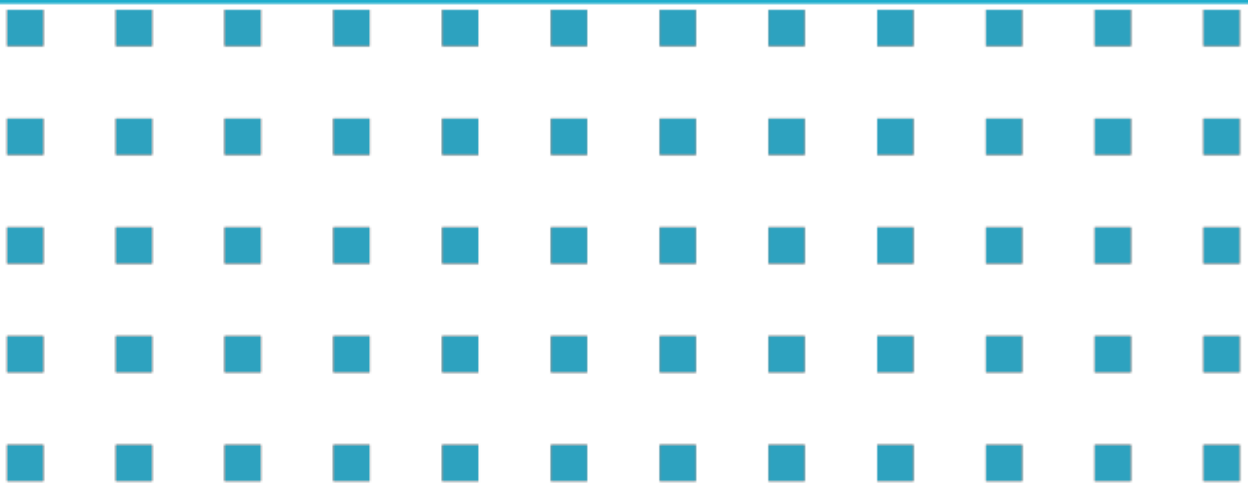
5. **Pengenalan vena:** Metode ini mengidentifikasi pengguna berdasarkan pola vena unik dalam tangan, jari, atau area tubuh lainnya. Sistem ini menggunakan pemindaian inframerah untuk menghasilkan gambar vena dan membandingkannya dengan data yang telah terdaftar sebelumnya.

Masing-masing metode otorisasi ini memiliki kelebihan dan kekurangan tersendiri. Beberapa metode, seperti biometrik, mungkin lebih aman dan nyaman bagi pengguna, tetapi memerlukan teknologi yang lebih canggih dan mungkin lebih rentan terhadap masalah privasi. Sementara itu, metode yang lebih sederhana, seperti password atau PIN, mungkin lebih mudah diimplementasikan tetapi lebih rentan terhadap penyerangan seperti peretasan atau phishing.

Dalam konteks payment gateway, penyedia layanan sering kali menawarkan berbagai pilihan metode otorisasi yang dapat disesuaikan dengan kebutuhan dan preferensi pengguna. Sebagai contoh, beberapa payment gateway mungkin mengizinkan pengguna untuk memilih antara otorisasi berbasis OTP atau biometrik, tergantung pada perangkat dan teknologi yang mereka gunakan. Yang terpenting adalah untuk menemukan keseimbangan antara keamanan, kemudahan penggunaan, dan kepatuhan terhadap standar industri yang relevan.

3

# Jenis Payment Gateway

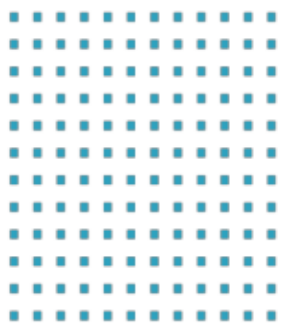


# enis Utama

Ada beberapa jenis payment gateway yang saat ini digunakan, dengan fokus utama pada kemudahan dan keamanan transaksi. Berikut adalah beberapa jenis payment gateway yang umum digunakan hingga saat ini:

## Hosted Payment Gateway:

Jenis payment gateway ini mengarahkan pengguna ke halaman pembayaran yang dihosting oleh penyedia payment gateway. Ketika pelanggan menyelesaikan transaksi, mereka akan kembali ke situs web merchant. Keuntungan dari metode ini adalah bahwa merchant tidak perlu menangani data kartu kredit secara langsung, sehingga mengurangi risiko keamanan dan memenuhi persyaratan kepatuhan seperti PCI DSS. Contoh dari hosted payment gateway termasuk PayPal, PayU, dan CCAvenue.



---

***Payment gateway lokal  
biasanya dirancang untuk  
melayani pasar dan kebutuhan  
spesifik suatu negara atau  
wilayah***

---

### Non-Hosted Payment Gateway (On-site payment gateway) :

Dalam non-hosted payment gateway, proses pembayaran terjadi di situs web merchant tanpa mengarahkan pelanggan ke halaman pembayaran eksternal. Sistem ini memberikan kontrol lebih besar kepada merchant atas proses pembayaran dan meningkatkan pengalaman pengguna. Namun, merchant harus memastikan kepatuhan dengan standar keamanan, seperti PCI DSS, karena mereka menangani data kartu kredit secara langsung. Contoh dari non-hosted payment gateway termasuk Stripe, Braintree, dan Authorize.Net.

### API-Based Payment Gateway:

Payment gateway berbasis API memungkinkan integrasi langsung antara situs web merchant dan penyedia payment gateway melalui API (Application Programming Interface). Hal ini memungkinkan transaksi diproses secara real-time tanpa mengarahkan pengguna ke halaman pembayaran eksternal. Seperti non-hosted payment gateway, merchant harus memastikan kepatuhan dengan standar keamanan. Contoh dari API-based payment gateway termasuk Stripe, Square, dan Adyen.

### Payment Gateway Lokal:

Payment gateway lokal biasanya dirancang untuk melayani pasar dan kebutuhan spesifik suatu negara atau wilayah. Mereka mungkin menawarkan dukungan untuk metode pembayaran lokal, mata uang, dan bahasa, serta mematuhi peraturan dan standar lokal. Di Indonesia, beberapa contoh payment gateway lokal termasuk DOKU, Midtrans, dan Xendit.

### Payment Gateway Internasional:

Payment gateway internasional memungkinkan merchant untuk menerima pembayaran dari pelanggan di seluruh dunia, mendukung berbagai metode pembayaran, mata uang, dan bahasa. Jenis payment gateway ini cocok untuk bisnis yang menjual produk atau layanan secara global. Contoh dari payment gateway internasional termasuk PayPal, 2Checkout, dan Skrill.

### Payment Gateway dengan fitur tambahan:

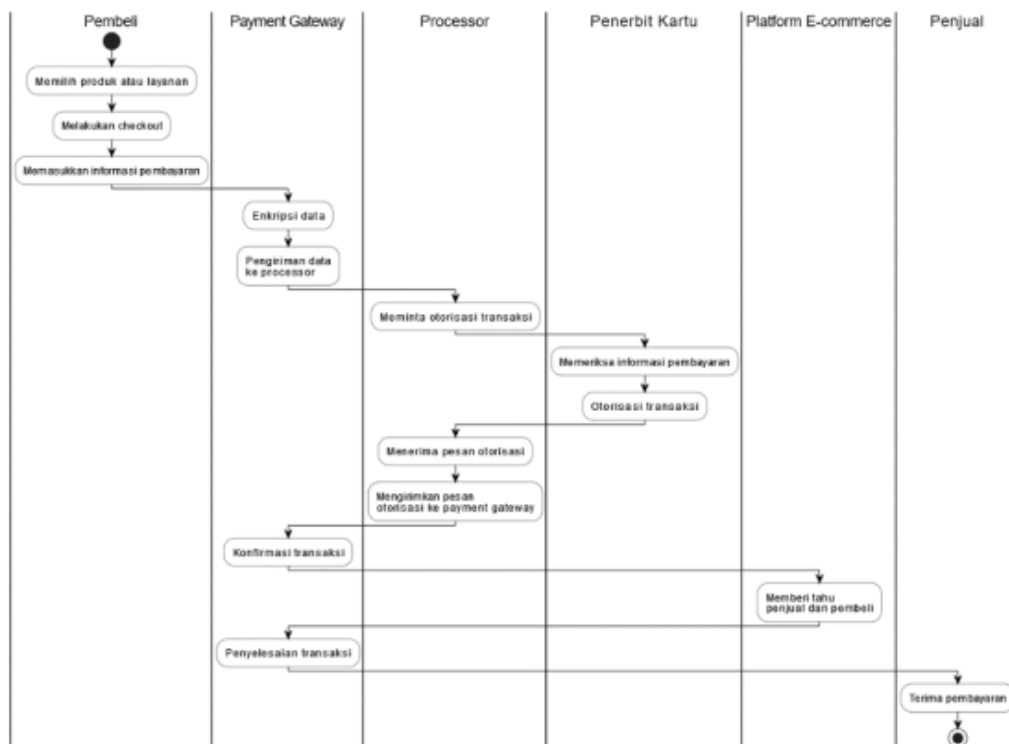
Beberapa payment gateway menawarkan fitur tambahan yang dirancang untuk memenuhi kebutuhan khusus dari merchant, seperti penanganan langganan, pembayaran berulang, atau fitur anti-fraud. Contoh dari payment gateway dengan fitur

tambahan ini termasuk Recurly, Chargify, dan Spreedly.

## Hosted Payment Gateway

Berikut langkah-langkah penerapan Hosted Payment Gateway:

1. **Mendaftar** dengan penyedia Hosted Payment Gateway yang dipilih (misalnya, PayPal, PayU, atau CCAvenue) dan membuat akun merchant.
2. **Mengintegrasikan** payment gateway ke situs web atau aplikasi dengan menggunakan API, plugin, atau kode yang disediakan oleh penyedia.
3. **Mengonfigurasi metode pembayaran**, mata uang, dan preferensi lain yang diinginkan melalui dasbor merchant.
4. **Menambahkan tombol atau tautan pembayaran** pada situs web atau aplikasi yang mengarahkan pelanggan ke halaman pembayaran dihosting oleh penyedia payment gateway.
5. **Mengatur notifikasi** atau callback yang akan memberi tahu merchant tentang status transaksi yang berhasil atau gagal.



#### Activity Diagram Hosted Payment Gateway

Diagram ini menggambarkan alur proses Hosted Payment Gateway dari perspektif pelanggan, payment gateway, dan merchant. Pelanggan memilih produk, menuju halaman checkout, dan mengklik tombol pembayaran yang mengarahkan mereka ke halaman pembayaran dihosting. Setelah memasukkan detail pembayaran dan melakukan verifikasi, payment gateway akan memberi tahu pelanggan dan merchant tentang status transaksi. Jika transaksi berhasil, merchant akan memproses pesanan dan pelanggan akan menerima konfirmasi. Jika gagal, pelanggan akan menerima pesan kesalahan.

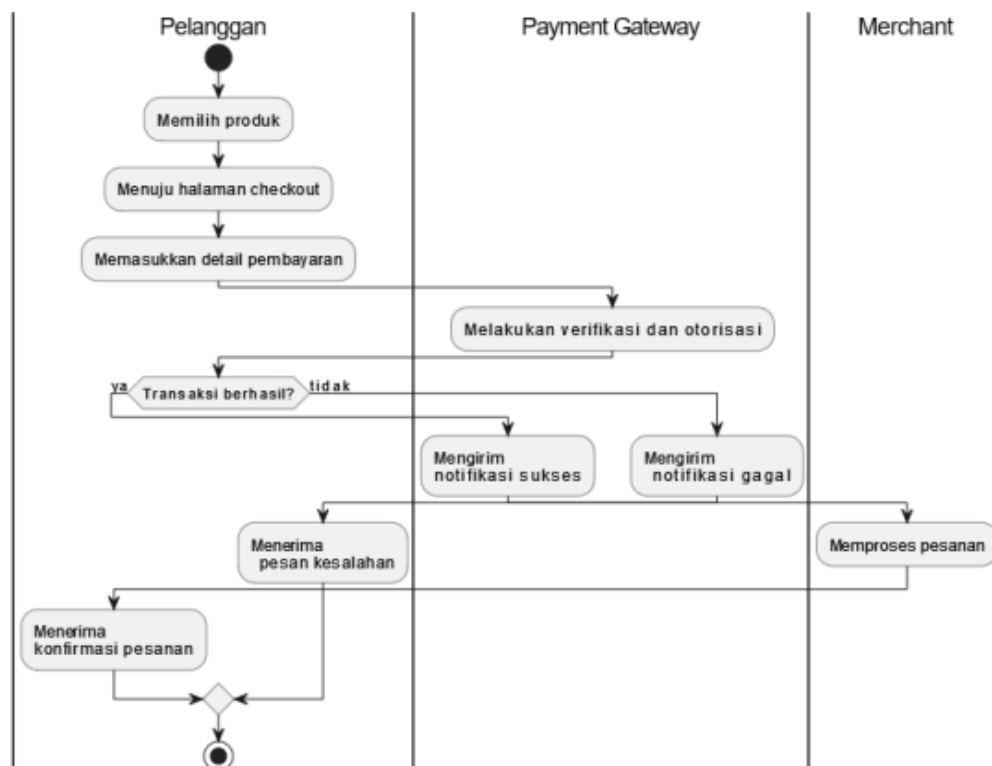


# Non-Hosted Payment Gateway

Berikut langkah-langkah penerapan Non-Hosted Payment Gateway (On-site payment gateway):

1. **Mendaftar** dengan penyedia Non-Hosted Payment Gateway yang dipilih (misalnya, Stripe, Braintree, atau Authorize.Net) dan membuat akun merchant.
2. **Mengintegrasikan payment gateway** ke situs web atau aplikasi menggunakan API, SDK, atau kode yang disediakan oleh penyedia.
3. **Mengonfigurasi metode pembayaran**, mata uang, dan preferensi lain yang diinginkan melalui dasbor merchant.
4. **Menambahkan formulir pembayaran** ke situs web atau aplikasi yang memungkinkan pelanggan untuk memasukkan detail pembayaran langsung di halaman checkout.
5. **Mengatur notifikasi atau callback** yang akan memberi tahu merchant tentang status transaksi yang berhasil atau gagal.





**Activity Diagram Non Hosted**

Diagram ini menggambarkan alur proses Non-Hosted Payment Gateway dari perspektif pelanggan, payment gateway, dan merchant. Pelanggan memilih produk, menuju halaman checkout, dan memasukkan detail pembayaran langsung di halaman tersebut. Payment gateway kemudian melakukan verifikasi dan otorisasi. Jika transaksi berhasil, merchant akan memproses pesanan dan pelanggan akan menerima konfirmasi. Jika gagal, pelanggan akan menerima pesan kesalahan.

# API-Based Payment Gateway

API (Application Programming Interface) adalah sekumpulan aturan, protokol, dan alat yang memungkinkan aplikasi berkomunikasi satu sama lain. Dalam konteks API-Based Payment Gateway, API menyediakan cara bagi developer untuk mengintegrasikan payment gateway ke dalam situs web atau aplikasi mereka dengan mudah dan efisien.

API-Based Payment Gateway menggunakan API untuk memungkinkan transaksi diproses secara real-time tanpa mengarahkan pengguna ke halaman pembayaran eksternal. Hal ini memberikan kontrol lebih besar kepada merchant atas proses pembayaran dan meningkatkan pengalaman pengguna. Berikut adalah beberapa aspek penting dari API pada API-Based Payment Gateway:

## Endpoint:

Endpoint adalah titik akses unik yang digunakan untuk mengirim permintaan dan menerima respons dari server. Dalam API-Based Payment Gateway, endpoint biasanya didefinisikan oleh penyedia gateway, dan developer diharuskan untuk mengirim permintaan ke endpoint ini untuk memproses transaksi.

### **Authentication:**

---

Autentikasi digunakan untuk memastikan bahwa hanya aplikasi yang sah dan berwenang yang dapat mengakses API. Penyedia API-Based Payment Gateway biasanya akan memberikan kredensial khusus, seperti kunci API atau token OAuth, yang harus digunakan saat mengirim permintaan ke API.

### **Request and Response:**

---

API menggunakan format standar untuk permintaan dan respons, seperti JSON atau XML. Developer harus memformat permintaan mereka sesuai dengan spesifikasi API, termasuk menyertakan data yang diperlukan seperti informasi pembayaran. Setelah permintaan diterima, server akan memprosesnya dan mengirimkan respons yang berisi status transaksi atau informasi lain yang relevan.

### **Error Handling:**

---

API juga menyediakan kode kesalahan standar dan pesan untuk membantu developer mengidentifikasi dan mengatasi masalah yang mungkin terjadi saat mengintegrasikan payment gateway. Dalam konteks payment gateway, kesalahan umum mungkin mencakup masalah seperti data kartu kredit yang tidak valid, kesalahan otorisasi, atau batasan transaksi.

### Documentation :

Penyedia API-Based Payment Gateway akan menyediakan dokumentasi yang mendetail mengenai cara menggunakan API mereka. Dokumentasi ini mencakup informasi tentang endpoint, parameter, format permintaan dan respons, kode kesalahan, dan contoh kode. Developer diharapkan untuk merujuk pada dokumentasi ini saat mengintegrasikan payment gateway ke dalam aplikasi mereka.

Contoh dari API-Based Payment Gateway termasuk Stripe, Square, dan Adyen. Menggunakan API memungkinkan merchant untuk menyesuaikan proses pembayaran sesuai dengan kebutuhan mereka, serta memastikan kecepatan dan keamanan transaksi yang lebih tinggi.



---

***API (Application Programming Interface) adalah sekumpulan aturan, protokol, dan alat yang memungkinkan aplikasi berkomunikasi satu sama lain***

---

# Payment Gateway Lokal

Di Indonesia, terdapat beberapa payment gateway lokal yang telah berkembang dan menawarkan layanan khusus untuk memenuhi kebutuhan pasar lokal. Beberapa di antaranya adalah:

## DOKU :

<sup>129</sup>  
DOKU merupakan salah satu payment gateway lokal terkemuka di Indonesia yang menyediakan beragam metode pembayaran seperti kartu kredit, transfer bank, e-wallet, dan pembayaran melalui gerai ritel. <sup>28</sup>  
DOKU telah bekerja sama dengan banyak merchant dan bisnis online, mulai dari e-commerce hingga penyedia layanan.



DOKU (<https://www.doku.com>)

## Midtrans :

---

Midtrans, sebelumnya dikenal sebagai Veritrans, adalah payment gateway lokal yang menawarkan integrasi dengan berbagai metode pembayaran populer di Indonesia, seperti kartu kredit, transfer bank, dan e-wallet. Midtrans juga menyediakan fitur keamanan yang canggih dan dukungan teknis yang baik untuk membantu merchant mengelola transaksi mereka.



midtrans Penggunaan ▾ Produk ▾ Panduan ▾ Biaya Hubungi Kami

bagian dari goto financial

### Payment Gateway Indonesia Terlengkap untuk Bisnis Anda

Bersama Midtrans, fokus pada bisnis Anda untuk kelola semua pembayaran dan kirim dana (disbursement) dengan mudah.

Daftar Sekarang

Midtrans (<https://midtrans.com>)

### Xendit:

---

Xendit adalah payment gateway lokal yang menawarkan solusi pembayaran yang mudah dan aman, dengan dukungan untuk kartu kredit, transfer bank, e-wallet, dan virtual account. Xendit juga memiliki fitur tambahan seperti pembayaran berulang dan disbursements untuk memudahkan pengelolaan keuangan.



Xendit (<https://www.xendit.co/>)

### Faspay:

---

Faspay adalah payment gateway lokal yang menyediakan berbagai metode pembayaran, termasuk kartu kredit, transfer bank, dan e-wallet. Faspay menawarkan solusi yang mudah diintegrasikan dengan berbagai platform e-commerce dan sistem manajemen bisnis.



Faspay (<https://faspay.co.id>)

### iPaymu:

---

iPaymu adalah payment gateway lokal yang mendukung metode pembayaran seperti transfer bank, e-wallet, dan pembayaran melalui gerai ritel. iPaymu menyediakan layanan yang mudah digunakan dan aman, serta integrasi yang mudah dengan platform e-commerce dan aplikasi lainnya.





Ipaymu (<https://ipaymu.com/>)

Pangsa pasar payment gateway lokal di Indonesia terus berkembang seiring dengan pertumbuhan industri e-commerce dan penetrasi internet di negara ini. Penyedia payment gateway lokal bersaing dengan pemain internasional seperti PayPal dan Stripe, serta dengan platform pembayaran yang dioperasikan oleh perusahaan teknologi lokal seperti GoPay dan OVO.

Salah satu keunggulan payment gateway lokal adalah dukungan untuk metode pembayaran yang khusus untuk pasar Indonesia, seperti pembayaran melalui gerai ritel dan e-wallet lokal. Selain itu, mereka juga memahami regulasi dan kebijakan lokal serta memberikan dukungan pelanggan dalam bahasa Indonesia. Faktor-faktor ini membuat payment gateway lokal menarik bagi bisnis lokal yang ingin menjangkau konsumen di seluruh Indonesia.

# Payment Gateway Internasional

Berikut adalah beberapa contoh payment gateway internasional dari berbagai benua dan kelebihan yang mereka tawarkan:

## 2 Amerika Utara:

### PayPal (AS) :

PayPal merupakan salah satu payment gateway paling populer dan telah menjadi standar di banyak negara. Kelebihan PayPal meliputi kemudahan penggunaan, pengenalan merek yang kuat, dan dukungan untuk lebih dari 200 negara dan lebih dari 25 mata uang.

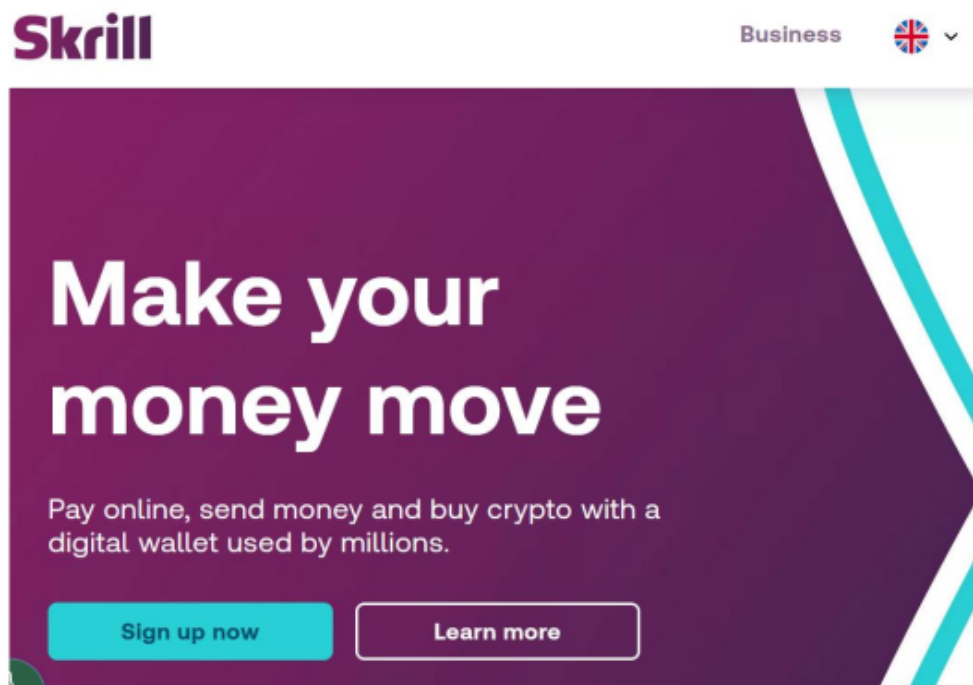


Paypal (<https://www.paypal.com/id/home>)



### Skrill (Inggris) :

Skrill adalah payment gateway internasional yang memungkinkan transfer uang dan pembayaran online cepat dan aman. Kelebihan Skrill meliputi biaya yang kompetitif, dukungan untuk lebih dari 40 mata uang, dan integrasi yang mudah dengan platform e-commerce populer.



Skrill (<https://www.skrill.com/>)

## Asia:

---

### Alipay (China) :

---

Alipay adalah payment gateway yang sangat populer di Tiongkok dan menawarkan berbagai metode pembayaran seperti kartu kredit, bank transfer, dan QR code. Kelebihan Alipay meliputi penetrasi pasar yang luas di Tiongkok, keamanan yang tinggi, dan fitur yang dirancang khusus untuk pasar Tiongkok.

### Paytm (India) :

---

Paytm adalah payment gateway terkemuka di India yang mendukung metode pembayaran seperti kartu kredit, transfer bank, e-wallet, dan UPI. Kelebihan Paytm meliputi dukungan untuk berbagai metode pembayaran lokal, keamanan yang tinggi, dan integrasi yang mudah dengan platform e-commerce dan aplikasi lainnya.



paytm UPI Paytm for Consumer Paytm For Business

## India's Most-loved Payments App

Recharge & pay bills, book flights & movie tickets, open a savings account, invest in stocks & mutual funds, and do a lot more.

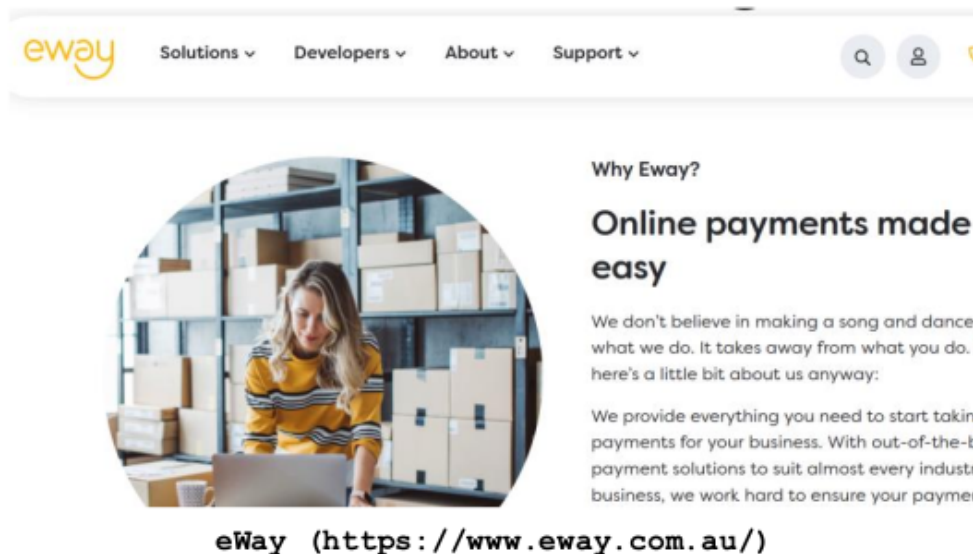
Download Paytm App

Paytm (<https://paytm.com/>)

## *Oseania – Amerika Selatan:*

### **eWAY (Australia) :**

eWAY adalah payment gateway yang berbasis di Australia dan menawarkan solusi pembayaran yang aman dan andal untuk bisnis di seluruh dunia. Kelebihan eWAY meliputi dukungan untuk berbagai mata uang, fitur keamanan yang canggih, dan integrasi yang mudah dengan platform e-commerce populer.



**eWay** (<https://www.eway.com.au/>)

## MercadoPago (Argentina) :

MercadoPago adalah payment gateway terkemuka di Amerika Latin yang menyediakan solusi pembayaran yang aman dan fleksibel. Kelebihannya meliputi dukungan untuk metode pembayaran lokal, seperti Boleto Bancário di Brasil, serta integrasi yang mudah dengan platform e-commerce dan aplikasi lainnya.



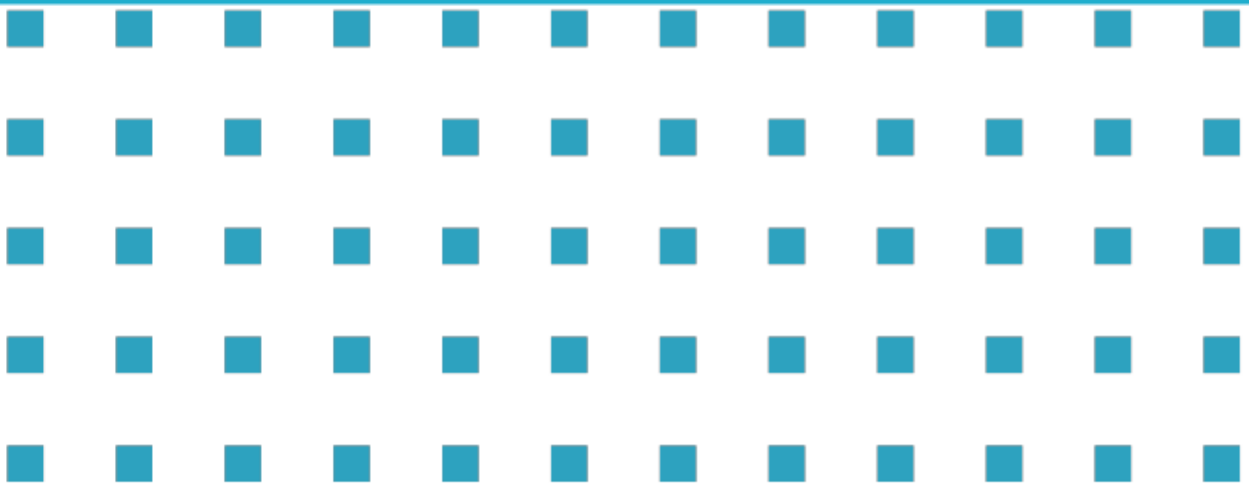
104

Mercado Pago (<https://www.mercadopago.com.ar/>)

Payment gateway internasional ini menawarkan berbagai kelebihan, seperti dukungan untuk berbagai mata uang dan metode pembayaran, integrasi yang mudah dengan platform e-commerce, serta fitur keamanan dan anti-fraud yang canggih.

# 4

## Regulasi dan Kepatuhan





# Pendahuluan

Di Indonesia, regulasi yang berkaitan dengan payment gateway melibatkan beberapa lembaga, seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK). Berikut ini beberapa regulasi yang relevan dengan payment gateway di Indonesia:

1. **Peraturan Bank Indonesia No. 18/40/PBI/2016** tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran (PTP): Peraturan ini mengatur penyelenggaraan PTP oleh perusahaan yang menyediakan layanan pembayaran, termasuk payment gateway. Peraturan ini mencakup persyaratan lisensi, kepatuhan teknis, keamanan data, serta tata kelola dan manajemen risiko.
2. **Peraturan Bank Indonesia No. 20/6/PBI/2018** tentang Uang Elektronik: Peraturan ini mengatur penyelenggaraan uang elektronik, yang sering digunakan dalam payment gateway sebagai metode pembayaran alternatif. Peraturan ini mencakup persyaratan izin, kepatuhan, dan tata kelola perusahaan yang menyediakan layanan uang elektronik.
3. **Peraturan Otoritas Jasa Keuangan No. 77/POJK.01/2016** tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (Fintech Peer-to-Peer Lending): Meskipun peraturan ini secara khusus mengatur industri fintech peer-to-peer

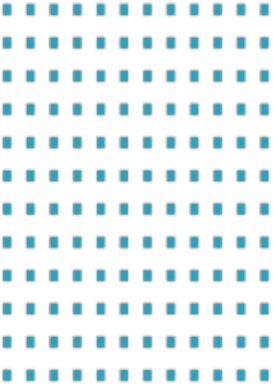
lending, beberapa aspeknya juga relevan bagi payment gateway, terutama yang bekerja sama dengan platform pinjam meminjam uang berbasis teknologi informasi. Peraturan ini mencakup persyaratan izin, tata kelola, dan perlindungan konsumen.

4. **Peraturan Otoritas Jasa Keuangan No. 13/POJK.02/2018** tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan: Peraturan ini menyediakan kerangka regulasi untuk inovasi keuangan digital, termasuk payment gateway, dengan tujuan untuk mendukung pertumbuhan industri fintech dan memastikan kepatuhan terhadap standar keamanan dan perlindungan konsumen.
5. **Peraturan Menteri Komunikasi dan Informatika No. 5/2020** tentang Penyelenggara Sistem Elektronik: Peraturan ini mengatur penyelenggara sistem elektronik, termasuk payment gateway, dan mencakup persyaratan keamanan siber, perlindungan data pribadi, dan kewajiban untuk memiliki pusat data dan pusat pemulihan bencana di Indonesia.

Selain peraturan di atas, payment gateway juga harus mematuhi peraturan lain yang relevan, seperti peraturan tentang anti pencucian uang (APU) dan pencegahan pendanaan terorisme (PPT) serta peraturan terkait pajak.

Untuk menjaga kepatuhan terhadap regulasi yang ada, penyedia payment gateway di Indonesia harus bekerja sama dengan regulator dan memastikan bahwa mereka memenuhi semua persyaratan lisensi, keamanan, dan perlindungan konsumen yang ditetapkan.

Relevansi regulasi anti pencucian uang (APU) dan pencegahan pendanaan terorisme (PPT) terhadap payment gateway sangat penting untuk memastikan integritas sistem pembayaran dan keamanan ekonomi secara keseluruhan. Payment gateway memainkan peran penting dalam memfasilitasi transaksi online, yang membuat mereka rentan terhadap penyalahgunaan oleh pelaku kejahatan untuk mencuci uang atau mendanai kegiatan teroris.



---

*payment gateway juga harus mematuhi peraturan lain yang relevan, seperti peraturan tentang anti pencucian uang (APU) dan pencegahan pendanaan terorisme (PPT) serta peraturan terkait pajak.*

---

## *Aspek Relevansi*

---

Berikut ini beberapa aspek yang menjelaskan relevansi regulasi APU dan PPT dalam konteks payment gateway:

### **Identifikasi dan verifikasi nasabah (KYC) :**

---

Payment gateway harus melakukan proses Know Your Customer (KYC) untuk mengidentifikasi dan memverifikasi identitas nasabah mereka, termasuk merchant dan konsumen. KYC membantu mencegah pencucian uang dan pendanaan terorisme dengan memastikan bahwa penyedia payment gateway mengetahui dengan siapa mereka bertransaksi dan memantau aktivitas mencurigakan.

### **Pemantauan transaksi:**

---

Payment gateway diharuskan untuk memantau transaksi yang dilakukan melalui platform mereka untuk mendeteksi aktivitas yang tidak biasa atau mencurigakan. Hal ini termasuk memantau volume dan frekuensi transaksi, serta transaksi dengan negara atau pihak yang terdaftar dalam daftar sanksi.

### Pelaporan aktivitas mencurigakan:

Jika payment gateway menemukan aktivitas yang mencurigakan atau tidak biasa yang mungkin terkait dengan pencucian uang atau pendanaan terorisme, mereka harus melaporkannya kepada otoritas yang relevan sesuai dengan peraturan APU dan PPT yang berlaku.

### Pendidikan dan pelatihan pegawai:

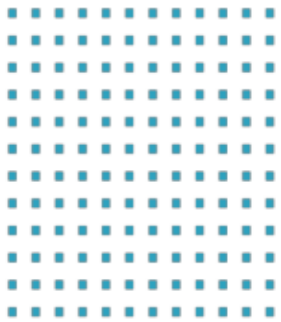
Penyedia payment gateway harus memberikan pendidikan dan pelatihan yang memadai kepada pegawainya mengenai regulasi APU dan PPT, serta prosedur internal yang harus diikuti untuk memastikan kepatuhan terhadap peraturan tersebut.

### Kebijakan dan prosedur intern:

Penyedia payment gateway harus memiliki kebijakan dan prosedur intern yang jelas dan efektif untuk memastikan kepatuhan terhadap peraturan APU dan PPT, termasuk tata kelola risiko, audit internal, dan sistem pelaporan.

102 Dalam konteks global, banyak negara telah mengadopsi rekomendasi Financial Action Task Force (FATF) sebagai standar internasional untuk melawan pencucian uang dan pendanaan terorisme. Oleh karena itu, penyedia payment gateway yang beroperasi di berbagai yurisdiksi juga harus memastikan kepatuhan terhadap rekomendasi FATF dan peraturan APU dan PPT yang relevan di negara-negara tempat mereka beroperasi.

Secara keseluruhan, kepatuhan terhadap regulasi APU dan PPT sangat penting bagi payment gateway untuk menjaga integritas sistem pembayaran, melindungi reputasi mereka, dan menghindari sanksi hukum yang mungkin timbul akibat pelanggaran peraturan tersebut.



---

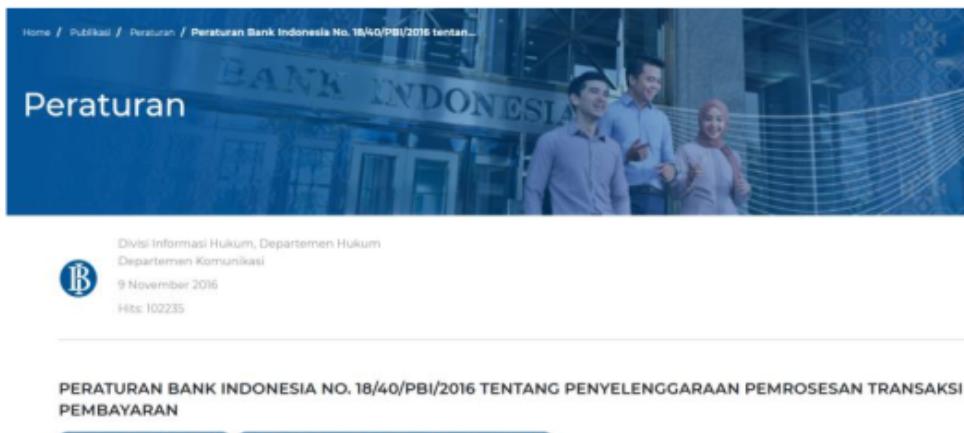
***Payment gateway memastikan bisnis mematuhi regulasi dan peraturan yang berlaku di industri pembayaran, seperti anti pencucian uang dan perlindungan konsumen.***

---

# Peraturan BI 2016

11

Peraturan Bank Indonesia No. 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran (PTP) merupakan peraturan yang mengatur penyelenggaraan PTP oleh perusahaan yang menyediakan layanan pembayaran, termasuk payment gateway.



62

## Situs Peraturan

([https://www.bi.go.id/id/publikasi/peraturan/Pages/pbi\\_184016.aspx](https://www.bi.go.id/id/publikasi/peraturan/Pages/pbi_184016.aspx))

Berikut adalah beberapa poin penting dari peraturan tersebut:

### Lisensi :

Penyelenggara PTP harus memiliki izin dari Bank Indonesia sebelum memulai kegiatan usahanya. Prosedur pemberian izin meliputi pengajuan permohonan, evaluasi, dan pemberian izin oleh Bank Indonesia.

### **Modal minimum:**

---

Penyelenggara PTP diharuskan <sup>44</sup> memiliki modal minimum yang ditetapkan oleh Bank Indonesia. Modal minimum ini bertujuan untuk memastikan penyelenggara memiliki kapabilitas keuangan yang memadai untuk menjalankan operasional mereka secara andal dan aman.

### **Tata kelola dan manajemen risiko:**

---

Penyelenggara PTP harus menerapkan <sup>16</sup> tata kelola perusahaan yang baik, termasuk manajemen risiko, kebijakan dan prosedur intern, audit internal, dan sistem pengendalian internal. Tujuannya adalah untuk menjaga stabilitas dan keandalan sistem pembayaran serta melindungi kepentingan para pengguna.

### **Kepatuhan teknis:**

---

Penyelenggara PTP diharuskan untuk mematuhi standar teknis yang ditetapkan oleh Bank Indonesia. Standar teknis ini mencakup persyaratan terkait interoperabilitas, keamanan sistem, dan kualitas layanan, serta ketersediaan sistem dan jaringan.



### Keamanan data:

Penyelenggara PTP harus menjaga keamanan data yang mereka proses, termasuk data transaksi dan data pribadi nasabah. Hal ini mencakup penerapan kebijakan dan prosedur keamanan yang sesuai, seperti enkripsi, pengendalian akses, dan langkah-langkah keamanan fisik.



---

***Penyelenggara PTP harus menerapkan tata kelola perusahaan yang baik, termasuk manajemen risiko, kebijakan dan prosedur intern, audit internal, dan sistem pengendalian internal***

---

### Perlindungan konsumen:

Penyelenggara PTP diharuskan untuk melindungi hak-hak konsumen dan memastikan transparansi dalam penyediaan layanan mereka. Hal ini mencakup penyediaan informasi yang jelas dan akurat tentang layanan, biaya, dan risiko yang terkait, serta penanganan keluhan konsumen secara efektif.

### Pelaporan dan kewajiban lainnya:

Penyelenggara PTP harus melaporkan kegiatan mereka kepada Bank Indonesia secara berkala, termasuk laporan keuangan, laporan operasional, dan laporan mengenai kepatuhan terhadap peraturan. Selain itu, penyelenggara juga harus mematuhi peraturan lain yang relevan, seperti peraturan anti pencucian uang dan pencegahan pendanaan terorisme.

Peraturan ini memastikan bahwa penyelenggara PTP, termasuk payment gateway, menjalankan operasional mereka secara andal, aman, dan transparan, sehingga melindungi kepentingan para pengguna dan menjaga integritas sistem pembayaran nasional.

# Peraturan BI 2018

11

Peraturan Bank Indonesia No. 20/6/PBI/2018 tentang Uang Elektronik merupakan peraturan yang mengatur penyelenggaraan uang elektronik di Indonesia. Uang elektronik adalah instrumen pembayaran yang sering digunakan dalam payment gateway sebagai metode pembayaran alternatif.

PERATURAN BANK INDONESIA  
NOMOR 20/6/PBI/2018  
TENTANG  
UANG ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR BANK INDONESIA,

Menimbang : a. bahwa kebutuhan masyarakat untuk menggunakan elektronik di Indonesia terus mengalami peningkatan

Situs Peraturan

66

(<https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI-200618.pdf>)

Berikut adalah beberapa poin penting dari peraturan tersebut:

#### Izin penyelenggaraan:

Untuk menyelenggarakan kegiatan uang elektronik, perusahaan harus memiliki izin dari Bank Indonesia. Prosedur pemberian izin meliputi pengajuan permohonan, evaluasi, dan pemberian izin oleh Bank Indonesia.

#### Modal minimum:

Penyelenggara uang elektronik diharuskan memiliki modal minimum yang ditetapkan oleh Bank Indonesia. Modal minimum ini bertujuan untuk memastikan penyelenggara memiliki kapabilitas keuangan yang memadai untuk menjalankan operasional mereka secara andal dan aman.

#### Tata kelola dan manajemen risiko:

Penyelenggara uang elektronik harus menerapkan tata kelola perusahaan yang baik, termasuk manajemen risiko, kebijakan dan prosedur intern, audit internal, dan sistem pengendalian internal. Tujuannya adalah untuk menjaga stabilitas dan keandalan sistem pembayaran serta melindungi kepentingan para pengguna.

### **Keamanan sistem:**

Penyelenggara uang elektronik diharuskan untuk mematuhi standar keamanan sistem yang ditetapkan oleh Bank Indonesia. Standar ini mencakup persyaratan terkait keamanan sistem dan jaringan, pengendalian akses, serta langkah-langkah keamanan fisik

### **Perlindungan konsumen:**

Penyelenggara uang elektronik diharuskan untuk melindungi hak-hak konsumen dan memastikan transparansi dalam penyediaan layanan mereka. Hal ini mencakup penyediaan informasi yang jelas dan akurat tentang layanan, biaya, dan risiko yang terkait, serta penanganan keluhan konsumen secara efektif.

### **Pelaporan dan kewajiban lainnya:**

Penyelenggara uang elektronik harus melaporkan kegiatan mereka kepada Bank Indonesia secara berkala, termasuk laporan keuangan, laporan operasional, dan laporan mengenai kepatuhan terhadap peraturan. Selain itu, penyelenggara juga harus mematuhi peraturan lain yang relevan, seperti peraturan anti pencucian uang dan pencegahan pendanaan terorisme.

## Penggunaan uang elektronik:

Peraturan ini juga mencakup ketentuan mengenai penggunaan uang elektronik, seperti batasan nilai transaksi, penarikan tunai, dan konversi uang elektronik ke mata uang fisik.

77 Peraturan Bank Indonesia No. 20/6/PBI/2018 bertujuan untuk memastikan penyelenggaraan uang elektronik yang aman, andal, dan transparan, serta melindungi kepentingan para pengguna.



---

***Penyelenggara uang elektronik harus melaporkan kegiatan mereka kepada Bank Indonesia secara berkala, termasuk laporan keuangan, laporan operasional, dan laporan mengenai kepatuhan terhadap peraturan***

---

# Peraturan OJK

Peraturan Otoritas Jasa Keuangan (OJK) No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital dalam Bidang Jasa Keuangan berfokus pada regulasi yang mengatur penyelenggaraan inovasi keuangan digital, termasuk fintech, yang berhubungan dengan sektor jasa keuangan.

Peraturan Otoritas Jasa Keuangan Nomor 13 /POJK.02/2018 Tahun 2018

## Inovasi Keuangan Digital Di Sektor Jasa Keuangan

### DETAIL PERATURAN

Jenis	Peraturan Otoritas Jasa Keuangan
Entitas	Otoritas Jasa Keuangan
Nomor	13 /POJK.02/2018
Tahun	2018
Judul	Peraturan Otoritas Jasa Keuangan tentang Inovasi Keuangan Digital
Ditetapkan Tanggal	15 Agustus 2018
Diundangkan Tanggal	16 Agustus 2018
Berlaku Tanggal	16 Agustus 2018

### Situs Peraturan

(<https://peraturan.bpk.go.id/Home/Details/128618/peraturan-ojk-no-13-pojk022018-tahun-2018>)

Berikut beberapa perbedaan utama antara peraturan OJK ini dan dua peraturan Bank Indonesia sebelumnya yang telah dijelaskan:

### Cakupan :

Peraturan ini mencakup berbagai aspek inovasi keuangan digital yang lebih luas, termasuk layanan keuangan berbasis teknologi seperti peer-to-peer lending, asuransi digital, investasi, dan layanan pembayaran. Sementara itu, Peraturan Bank Indonesia No. 18/40/PBI/2016 lebih fokus pada penyelenggaraan Pemrosesan Transaksi Pembayaran, dan Peraturan Bank Indonesia No. 20/6/PBI/2018 lebih fokus pada penyelenggaraan uang elektronik.

### Otoritas pengawas :

Peraturan ini diterbitkan dan diawasi oleh Otoritas Jasa Keuangan, yang bertanggung jawab atas pengaturan dan pengawasan sektor jasa keuangan non-perbankan. Sementara itu, dua peraturan Bank Indonesia sebelumnya diterbitkan dan diawasi oleh Bank Indonesia, yang bertanggung jawab atas pengaturan dan pengawasan sistem pembayaran dan uang elektronik.



### Regulasi sand-box:

Salah satu aspek penting dari Peraturan ini adalah pengaturan mengenai "regulatory sandbox," yaitu lingkungan uji coba yang memungkinkan penyelenggara inovasi keuangan digital untuk menguji produk dan layanan mereka dalam lingkungan terkendali sebelum diluncurkan secara komersial. Hal ini tidak terdapat dalam kedua peraturan Bank Indonesia yang disebutkan sebelumnya.

### Perlindungan konsumen:

Meskipun ketiga peraturan ini memiliki aspek perlindungan konsumen, Peraturan ini lebih fokus pada transparansi, keadilan, dan akuntabilitas dalam penyediaan layanan keuangan digital, termasuk ketentuan mengenai penanganan keluhan konsumen, pengungkapan informasi, dan periklanan.

PCI DSS (Payment Card Industry Data Security Standard) adalah suatu rangkaian standar keamanan yang dikembangkan oleh Payment Card Industry Security Standards Council (PCI SSC) untuk melindungi data kartu kredit dan debit. PCI SSC merupakan organisasi yang didirikan oleh lima perusahaan kartu kredit utama, yaitu Visa, MasterCard, American Express, Discover, dan JCB. PCI DSS bertujuan untuk mengurangi risiko kebocoran data, penipuan, dan gangguan keamanan yang terkait dengan transaksi kartu pembayaran.

Berikut adalah beberapa komponen utama dari PCI DSS:

#### Keamanan jaringan dan sistem:

1. Menginstal dan mengelola firewall untuk melindungi data kartu.
2. Menggunakan kata sandi dan konfigurasi keamanan yang diberikan oleh vendor untuk sistem dan komponen keamanan.

### Perlindungan data kartu:

1. Melindungi data kartu yang disimpan dan membatasi penyimpanan data kartu.
2. Menggunakan teknologi enkripsi untuk mengirimkan data kartu melintasi jaringan terbuka dan dalam transmisi.

### Pengelolaan akses:

1. Mengendalikan akses fisik dan virtual ke sistem dan data kartu.
2. Menetapkan ID pengguna unik untuk setiap individu yang memiliki akses ke data kartu dan memastikan mereka menggunakan autentikasi yang kuat.

### Pemantauan dan pengujian keamanan:

1. Melakukan pemantauan dan pengujian rutin terhadap sistem dan jaringan untuk mendeteksi dan mengatasi ancaman keamanan.
2. Menggunakan teknologi anti-malware dan menjaga program anti-virus tetap up-to-date.

### Kebijakan keamanan:

1. Membuat dan menjaga kebijakan keamanan informasi yang mencakup seluruh organisasi.
2. Melakukan penilaian risiko secara berkala dan mengidentifikasi kelemahan keamanan.

PCI DSS mencakup 12 persyaratan yang harus dipenuhi oleh semua organisasi yang menyimpan, memproses, atau mentransmisikan data kartu kredit dan debit. Kepatuhan terhadap PCI DSS diukur melalui proses penilaian keamanan tahunan yang dilakukan oleh Qualified Security Assessors (QSA) atau melalui Self-Assessment Questionnaire (SAQ) untuk organisasi yang lebih kecil.

Organisasi yang tidak mematuhi PCI DSS dapat dikenakan sanksi, seperti denda, pembatasan akses ke sistem pembayaran kartu, atau bahkan penghentian hak untuk memproses transaksi kartu. Selain itu, kegagalan mematuhi standar ini dapat mengakibatkan kerugian kepercayaan pelanggan dan potensi tuntutan hukum. Oleh karena itu, penting bagi penyelenggara payment gateway dan perusahaan yang terlibat dalam transaksi kartu pembayaran untuk mematuhi PCI DSS demi menjaga keamanan data dan integritas sistem pembayaran mereka.



10

---

***PCI DSS (Payment Card Industry Data Security Standard) adalah suatu rangkaian standar keamanan yang dikembangkan oleh Payment Card Industry Security Standards Council (PCI SSC) untuk melindungi data kartu kredit dan debit.***

---

# Kartu

Kartu kredit dan debit dapat dikategorikan berdasarkan teknologi keamanan yang digunakan untuk melindungi data dan transaksi. Berikut adalah beberapa jenis kartu kredit dan debit berdasarkan teknologi keamanannya:

## Kartu dengan strip magnetik (magnetic stripe cards):

Kartu dengan strip magnetik adalah teknologi kartu pembayaran yang paling lama digunakan. Strip magnetik pada bagian belakang kartu menyimpan informasi dasar seperti nomor kartu, tanggal kedaluwarsa, dan CVV (Card Verification Value). Namun, teknologi ini dianggap kurang aman karena rentan terhadap pembajakan data dan penipuan, seperti skimming.



---

***Kartu kontakles menggunakan teknologi Near Field Communication (NFC) untuk memungkinkan transaksi cepat dan aman tanpa menyentuh terminal pembayaran.***

---

### **Kartu dengan chip EMV (EMV chip cards) :**

---

EMV (Europay, MasterCard, Visa) adalah teknologi kartu dengan chip yang lebih aman daripada kartu dengan strip magnetik. Chip EMV menyimpan data kartu dan menggunakan proses autentikasi dinamis untuk setiap transaksi, yang membuatnya lebih sulit untuk dicuri atau dipalsukan. Teknologi ini mensyaratkan kartu harus dimasukkan ke dalam terminal pembayaran (dip) dan kadang-kadang memerlukan PIN atau tanda tangan sebagai langkah verifikasi tambahan.

### **Kartu kontakles (contactless cards) :**

---

Kartu kontakles menggunakan teknologi Near Field Communication (NFC) untuk memungkinkan transaksi cepat dan aman tanpa menyentuh terminal pembayaran. Pengguna cukup mengetuk atau mendekatkan kartu ke terminal untuk melakukan transaksi. Teknologi ini menggunakan enkripsi dan tokenisasi untuk melindungi data, sehingga transaksi menjadi lebih aman dan sulit untuk dipalsukan. Namun, batasan transaksi biasanya diterapkan untuk mencegah penyalahgunaan kartu yang hilang atau dicuri.

### Kartu dengan fitur biometrik:

Beberapa kartu kredit dan debit saat ini juga mencakup fitur biometrik, seperti sidik jari, sebagai metode autentikasi tambahan. Fitur ini meningkatkan keamanan transaksi dengan memastikan bahwa hanya pemilik kartu yang sah yang dapat menggunakan kartu tersebut. Kartu dengan fitur biometrik biasanya juga dilengkapi dengan teknologi EMV dan/atau NFC.



#### **Contoh Kartu Biometrik**

Dalam beberapa tahun terakhir, industri pembayaran telah beralih dari kartu dengan strip magnetik ke kartu dengan chip EMV dan kontakles, karena teknologi tersebut menawarkan tingkat keamanan yang lebih tinggi. Selain itu, metode pembayaran alternatif, seperti e-wallet dan aplikasi pembayaran mobile, juga semakin populer dan menawarkan berbagai fitur keamanan yang canggih untuk melindungi data dan transaksi pengguna.

# Regulasi Internasional

Regulasi dan standar internasional untuk payment gateway memastikan bahwa transaksi pembayaran dilakukan dengan aman, efisien, dan transparan, terutama saat melibatkan transaksi lintas batas. Berikut adalah beberapa regulasi dan standar internasional yang penting dalam industri payment gateway:

## <sup>10</sup> Payment Card Industry Data Security Standard (PCI DSS) :

Seperti yang telah dibahas sebelumnya, PCI <sup>88</sup> DSS adalah standar keamanan internasional yang dikembangkan oleh <sup>54</sup> Payment Card Industry Security Standards Council (PCI SSC) untuk melindungi data kartu kredit dan debit. Semua perusahaan yang menyimpan, memproses, atau mentransmisikan data kartu kredit dan debit diharuskan mematuhi PCI DSS.

## ISO 20022 :

ISO <sup>65</sup> 20022 adalah standar internasional yang dikembangkan oleh International Organization for Standardization (ISO) untuk sistem komunikasi elektronik di sektor keuangan. Standar ini menyediakan kerangka untuk pembuatan dan penggunaan pesan yang konsisten dan terstruktur



dalam berbagai sistem pembayaran, termasuk transaksi lintas batas. ISO 20022 memungkinkan interoperabilitas antara berbagai sistem dan layanan pembayaran, serta meningkatkan efisiensi dan pengurangan risiko.

### **PSD2 (Payment Services Directive 2) :**

---

PSD2 adalah direktif Uni Eropa yang bertujuan untuk meningkatkan inovasi, meningkatkan keamanan, dan meningkatkan perlindungan konsumen dalam industri pembayaran. Salah satu aspek kunci dari PSD2 adalah pembukaan akses ke sistem pembayaran bagi penyedia layanan pembayaran baru (seperti fintech dan payment gateway) melalui APIs (Application Programming Interfaces). PSD2 juga mengharuskan peningkatan langkah-langkah keamanan, seperti autentikasi kuat pelanggan (SCA, Strong Customer Authentication) untuk transaksi kartu dan pembayaran online.

### **92 AML (Anti-Money Laundering) dan CTF (Counter-Terrorist Financing) Regulations:**

---

47  
Regulasi AML dan CTF bertujuan untuk mencegah pencucian uang dan pendanaan terorisme dalam sistem keuangan global. Penyelenggara payment gateway diharuskan untuk mematuhi peraturan AML dan CTF, seperti melaksanakan prosedur Know Your 33

Customer (KYC) untuk mengidentifikasi dan memverifikasi identitas pelanggan, serta melaporkan transaksi mencurigakan kepada otoritas yang relevan. Beberapa peraturan internasional yang relevan termasuk FATF Recommendations (Financial Action Task Force) dan EU's AML Directives.

60

### **SWIFT (Society for Worldwide Interbank Financial Telecommunication) :**

---

SWIFT adalah organisasi internasional yang menyediakan jaringan komunikasi aman dan standar pesan untuk transaksi keuangan antarbank. Penyelenggara payment gateway yang terlibat dalam transaksi lintas batas sering kali bergantung pada sistem SWIFT untuk berkomunikasi dengan bank dan lembaga keuangan lainnya. Standar SWIFT memastikan bahwa pesan dan data yang ditransmisikan melalui jaringannya aman, andal, dan efisien.

Menerapkan dan mematuhi regulasi dan standar internasional ini memastikan bahwa penyelenggara payment gateway dapat mengoperasikan layanan mereka secara aman dan efisien, sambil mempertahankan kepercayaan konsumen dan mitra bisnis. Regulasi dan standar internasional ini membantu menjaga integritas sistem pembayaran global, mengurangi risiko penipuan, pencucian uang, dan pendanaan terorisme, serta

mempromosikan inovasi dan persaingan sehat di antara penyedia layanan pembayaran.

Selain itu, beberapa negara mungkin memiliki peraturan dan standar tambahan yang berlaku untuk payment gateway yang beroperasi di dalam yurisdiksi mereka. Oleh karena itu, penting bagi penyelenggara payment gateway untuk memahami dan mematuhi peraturan lokal yang relevan, serta menjaga kepatuhan dengan standar internasional.

Dalam konteks transaksi antar negara, penting bagi payment gateway untuk memastikan bahwa mereka mematuhi peraturan dan standar yang relevan di kedua negara yang terlibat dalam transaksi. Hal ini termasuk memahami perbedaan antara peraturan dan standar di masing-masing negara, serta menggabungkan praktik terbaik dan prosedur kepatuhan yang sesuai untuk memenuhi persyaratan yang berlaku.

Secara keseluruhan, kepatuhan terhadap regulasi dan standar internasional untuk payment gateway merupakan aspek penting dalam menjaga kepercayaan konsumen dan mitra bisnis, serta memastikan kelancaran operasional dan keamanan dalam transaksi pembayaran, terutama dalam transaksi lintas batas.

**5**

# **Integrasi Platform Bisnis**



# Pendahuluan

Integrasi payment gateway pada platform bisnis seperti e-commerce dan point of sales (POS) memungkinkan pemilik bisnis untuk menerima pembayaran dari pelanggan melalui berbagai metode, seperti kartu kredit, debit, e-wallet, dan transfer bank. Berikut adalah penjelasan mengenai proses integrasi payment gateway pada e-commerce dan sistem POS.

## *Integrasi Payment Gateway pada E-commerce:*

1. **Pilih payment gateway:** Pertama, pemilik bisnis perlu memilih payment gateway yang sesuai dengan kebutuhan bisnis mereka. Faktor yang perlu dipertimbangkan mencakup biaya transaksi, kecepatan pemrosesan, metode pembayaran yang didukung, keamanan, dan dukungan teknis.
2. **Mendaftar akun merchant:** Setelah memilih payment gateway, pemilik bisnis perlu mendaftar akun merchant dengan penyedia layanan. Ini melibatkan proses KYC (Know Your Customer) dan verifikasi informasi bisnis.

3. **Integrasi teknis:** Integrasi teknis melibatkan menggabungkan API (Application Programming Interface) atau plugin dari payment gateway ke platform e-commerce. Banyak platform e-commerce seperti Shopify, WooCommerce, dan Magento menyediakan plugin atau ekstensi yang memudahkan integrasi dengan payment gateway populer.
4. **Pengaturan dan konfigurasi:** Setelah integrasi teknis selesai, pemilik bisnis perlu mengkonfigurasi pengaturan payment gateway, seperti mata uang, metode pembayaran yang diaktifkan, dan batasan transaksi.
5. **Pengujian:** Sebelum meluncurkan payment gateway, penting untuk menguji fungsionalitas dan keamanannya. Hal ini melibatkan pengujian transaksi pembayaran, refund, dan penanganan kesalahan.
6. **Peluncuran:** Setelah pengujian berhasil, payment gateway siap untuk digunakan oleh pelanggan.

## *Integrasi Payment Gateway pada Point of Sales (POS):*

---

1. **Pilih payment gateway:** Sama seperti pada e-commerce, pemilik bisnis perlu memilih payment gateway yang sesuai dengan kebutuhan bisnis mereka.
2. **Mendaftar akun merchant:** Proses ini sama dengan mendaftar akun merchant untuk e-commerce.
3. **Integrasi perangkat keras dan perangkat lunak:** Integrasi payment gateway pada sistem POS melibatkan menggabungkan perangkat keras (seperti pembaca kartu, terminal kontakles, dan perangkat mobile) dan perangkat lunak (seperti aplikasi POS atau manajemen inventori) dengan payment gateway.
4. **Pengaturan dan konfigurasi:** Pemilik bisnis perlu mengkonfigurasi pengaturan payment gateway pada sistem POS, seperti metode pembayaran yang diaktifkan dan batasan transaksi.
5. **Pengujian:** Pastikan untuk menguji fungsionalitas dan keamanan sistem sebelum meluncurkannya.
6. **Peluncuran:** Setelah pengujian berhasil, payment gateway siap untuk digunakan pada sistem POS.

Dengan integrasi payment gateway pada platform bisnis, pemilik bisnis dapat menawarkan berbagai metode pembayaran kepada pelanggan, meningkatkan kemudahan dan keamanan transaksi, serta meningkatkan penjualan dan kepuasan pelanggan.

# Pertimbangan Pemilihan

Saat memilih payment gateway, ada beberapa faktor penting yang harus dipertimbangkan oleh pemilik bisnis untuk memastikan bahwa pilihan tersebut sesuai dengan kebutuhan bisnis dan pelanggan. Berikut adalah beberapa faktor yang perlu dipertimbangkan saat memilih payment gateway:

## Biaya dan Tarif:

Bandingkan biaya yang dikenakan oleh berbagai payment gateway, seperti biaya pendaftaran, biaya bulanan, biaya transaksi, dan biaya tambahan lainnya. Pilih payment gateway yang menawarkan struktur biaya yang wajar dan kompetitif tanpa mengorbankan fitur dan kualitas layanan.

## Metode Pembayaran yang Didukung:

Pastikan payment gateway mendukung metode pembayaran yang populer dan relevan dengan target pasar Anda, seperti kartu kredit, kartu debit, e-wallet, transfer bank, dan pembayaran melalui kode QR.



### **Keamanan :**

---

Keamanan adalah aspek penting dalam transaksi online. Pilih payment gateway yang mematuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi data seperti SSL/TLS untuk melindungi informasi pembayaran pelanggan.

### **Integrasi dengan Platform Bisnis :**

---

Pastikan payment gateway yang dipilih mudah diintegrasikan dengan platform bisnis Anda, seperti e-commerce atau sistem POS. Banyak penyedia payment gateway menawarkan API, plugin, atau ekstensi yang kompatibel dengan platform populer seperti Shopify, WooCommerce, dan Magento.

### **Ketersediaan Layanan :**

---

Periksa apakah payment gateway menawarkan layanan di negara atau wilayah di mana Anda beroperasi. Beberapa payment gateway hanya menawarkan layanan di negara tertentu atau memiliki batasan untuk transaksi lintas batas.

### **Waktu Proses Transaksi :**

---

Waktu yang diperlukan untuk memproses transaksi sangat penting dalam bisnis online. Pilih payment gateway yang menawarkan waktu pemrosesan yang cepat dan efisien.

### Dukungan Pelanggan dan Teknis:

Pastikan payment gateway yang Anda pilih menawarkan dukungan pelanggan dan teknis yang responsif dan efisien. Hal ini penting dalam mengatasi masalah dan pertanyaan yang mungkin timbul selama proses integrasi dan pengoperasian layanan.

### Reputasi dan Ulasan:

Baca ulasan dan testimoni dari pengguna lain tentang kinerja dan kualitas layanan payment gateway yang Anda pertimbangkan. Pilih penyedia dengan reputasi baik dan rekam jejak yang terbukti dalam industri.

### Skalabilitas:

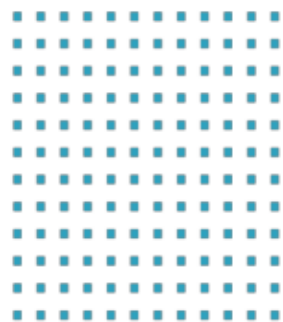
Pertimbangkan apakah payment gateway yang Anda pilih dapat mendukung pertumbuhan bisnis Anda di masa depan, baik dalam hal volume transaksi maupun ekspansi geografis.

### Fitur Tambahan:

Periksa fitur tambahan yang ditawarkan oleh payment gateway, seperti integrasi dengan alat analisis dan pelaporan, fitur manajemen penipuan, dan dukungan untuk pembayaran berulang atau langganan.

<b>Faktor</b>	<b>Deskripsi</b>
<b>Biaya dan Tarif</b>	Bandungkan biaya pendaftaran, biaya bulanan, biaya transaksi, dan biaya tambahan.
<b>Metode Pembayaran</b>	Pastikan dukungan untuk metode pembayaran yang relevan seperti kartu kredit, e-wallet, dan transfer bank.
<b>Keamanan</b>	Pilih payment gateway yang mematuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi.
<b>Integrasi Platform Bisnis</b>	Periksa kemudahan integrasi dengan platform bisnis Anda, seperti e-commerce atau sistem POS.
<b>Ketersediaan Layanan</b>	Pastikan layanan tersedia di negara atau wilayah di mana Anda beroperasi.
<b>Waktu Proses Transaksi</b>	Pilih payment gateway dengan waktu pemrosesan transaksi yang cepat dan efisien.
<b>Dukungan Pelanggan &amp; Teknis</b>	Pastikan dukungan pelanggan dan teknis yang responsif dan efisien.
<b>Reputasi dan Ulasan</b>	Pilih penyedia dengan reputasi baik dan rekam jejak yang terbukti dalam industri.

<b>Skalabilitas</b>	Pertimbangkan apakah payment gateway dapat mendukung pertumbuhan bisnis Anda di masa depan.
<b>Fitur Tambahan</b>	Periksa fitur tambahan seperti integrasi dengan alat analisis, fitur manajemen penipuan, dan pembayaran berulang.



---

*Pertimbangkan apakah payment gateway yang Anda pilih dapat mendukung pertumbuhan bisnis Anda di masa depan*

---

# Integrasi Teknis

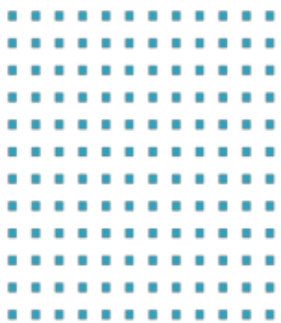
Berikut adalah beberapa jenis API yang populer digunakan dalam integrasi teknis payment gateway, beserta kelebihan dan kelemahannya:

Jenis API	Kelebihan	Kelemahan
<b>REST (Representational State Transfer)</b>	Mudah dipahami dan diimplementasikan, ringan, skalabilitas tinggi, dukungan luas.	Tidak memiliki fitur real-time bawaan, terbatas pada protokol HTTP.
<b>SOAP (Simple Object Access Protocol)</b>	Mendukung berbagai protokol (HTTP, SMTP, dll.), keamanan yang lebih baik, standar yang ketat.	Lebih kompleks, berat, kurang fleksibel dibandingkan dengan REST.
<b>GraphQL</b>	Fleksibilitas tinggi, hanya mengambil data yang dibutuhkan, dukungan real-time melalui subscriptions.	Belum banyak dukungan pustaka, kompleksitas tinggi dalam beberapa kasus, keamanan.

Jenis API	Kelebihan	Kelemahan
<b>gRPC (gRPC Remote Procedure Calls)</b>	Efisien, berbasis protokol HTTP/2, dukungan untuk streaming data, dukungan untuk berbagai bahasa pemrograman.	Tidak sepopuler REST atau GraphQL, lebih kompleks untuk diimplementasikan.

Dalam memilih jenis API untuk integrasi teknis payment gateway, penting untuk mempertimbangkan kebutuhan bisnis Anda, sumber daya yang tersedia, dan kemampuan tim pengembangan dalam menggunakan teknologi tersebut. Kelebihan dan kelemahan yang tercantum di atas dapat membantu Anda membuat keputusan yang lebih baik tentang jenis API yang paling sesuai untuk proyek Anda.

Berikut adalah beberapa jenis platform e-commerce yang populer digunakan dalam integrasi dengan payment gateway, beserta kelebihan dan kelemahannya:




---

***Shopify: Mudah digunakan, dukungan payment gateway beragam, tema dan aplikasi tambahan, dukungan pelanggan.***

---

<b>Platform E-commerce</b>	<b>Kelebihan</b>	<b>Kelemahan</b>
<b>Shopify</b>	Mudah digunakan, dukungan payment gateway beragam, tema dan aplikasi tambahan, dukungan pelanggan.	Biaya bulanan, biaya transaksi tambahan jika tidak menggunakan Shopify Payments, kurang fleksibel.
<b>WooCommerce</b>	Gratis dan open-source, fleksibel, banyak plugin dan tema, terintegrasi dengan WordPress.	Kurva belajar yang lebih tinggi, biaya hosting dan keamanan eksternal, pemeliharaan lebih tinggi.
<b>Magento</b>	Open-source, skalabilitas tinggi, fleksibel, banyak fitur, komunitas pengembang yang luas.	Kurva belajar yang tinggi, memerlukan sumber daya hosting yang lebih besar, pemeliharaan lebih tinggi.

<b>Platform E-commerce</b>	<b>Kelebihan</b>	<b>Kelemahan</b>
<b>BigCommerce</b>	Mudah digunakan, banyak fitur bawaan, tidak ada biaya transaksi, dukungan pelanggan.	Biaya bulanan, batasan penjualan tahunan, tema premium mahal, kurang fleksibel.
<b>PrestaShop</b>	Gratis dan open-source, fleksibel, banyak modul dan tema, komunitas dukungan yang luas.	Kurva belajar yang lebih tinggi, biaya hosting dan keamanan eksternal, modul premium mahal.

Dalam memilih platform e-commerce untuk integrasi dengan payment gateway, penting untuk mempertimbangkan kebutuhan bisnis Anda, anggaran yang tersedia, dan kemampuan tim Anda dalam menggunakan teknologi tersebut. Kelebihan dan kelemahan yang tercantum di atas dapat membantu Anda membuat keputusan yang lebih baik tentang platform e-commerce yang paling sesuai untuk proyek Anda.



# Integrasi perangkat keras dan perangkat lunak

Sebelum melakukan integrasi perangkat keras dan perangkat lunak di Point of Sale (POS), ada beberapa hal yang harus diperhatikan untuk memastikan proses berjalan lancar dan efisien:

1. **Kebutuhan Bisnis:** Pertimbangkan kebutuhan bisnis Anda dan pastikan bahwa solusi POS yang Anda pilih dapat memenuhi kebutuhan tersebut. Hal ini mencakup fitur seperti manajemen inventaris, pelaporan, dan dukungan untuk metode pembayaran yang beragam.
2. **Kemudahan Penggunaan:** Pilih perangkat keras dan perangkat lunak POS yang mudah digunakan oleh staf Anda. Hal ini akan membantu mengurangi waktu pelatihan dan memastikan bahwa sistem dapat dioperasikan dengan lancar.
3. **Konektivitas:** Pastikan perangkat keras dan perangkat lunak yang Anda pilih memiliki konektivitas yang baik, termasuk dukungan untuk jaringan nirkabel dan kabel. Konektivitas yang baik akan memastikan bahwa sistem POS Anda dapat berkomunikasi dengan payment gateway dan sistem lainnya dengan lancar.

4. **Keamanan:** Keamanan adalah aspek penting dalam sistem POS, terutama karena melibatkan data pelanggan dan informasi pembayaran. Pilih perangkat keras dan perangkat lunak yang mematuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi.
5. **Integrasi Payment Gateway:** Pastikan perangkat keras dan perangkat lunak yang Anda pilih dapat terintegrasi dengan payment gateway yang Anda gunakan. Ini akan memungkinkan Anda untuk menerima pembayaran melalui berbagai metode dengan mudah.
6. **Dukungan dan Pemeliharaan:** Pilih perangkat keras dan perangkat lunak yang menawarkan dukungan teknis dan pemeliharaan yang baik. Dukungan yang baik akan membantu Anda mengatasi masalah yang mungkin muncul dan memastikan sistem POS Anda tetap berfungsi dengan baik.
7. **Biaya:** Pertimbangkan biaya perangkat keras, perangkat lunak, dan biaya integrasi. Pastikan bahwa Anda memilih solusi yang efisien dan ekonomis tanpa mengorbankan fitur dan fungsionalitas yang penting.
8. **Skalabilitas:** Pilih sistem POS yang dapat skalabilitas untuk mendukung pertumbuhan bisnis Anda di masa depan. Hal ini mencakup kemampuan untuk menambahkan lebih banyak terminal atau fitur tambahan saat bisnis Anda berkembang.

# Evaluasi Integrasi

Evaluasi integrasi payment gateway penting untuk memastikan bahwa sistem pembayaran Anda berfungsi dengan baik dan memberikan pengalaman yang baik kepada pelanggan Anda. Berikut adalah beberapa metrik yang dapat Anda gunakan untuk mengevaluasi integrasi payment gateway:

1. **Tingkat Keberhasilan Transaksi:** Metrik ini mengukur persentase transaksi yang berhasil diselesaikan melalui payment gateway. Tingkat keberhasilan transaksi yang tinggi menunjukkan bahwa integrasi payment gateway berfungsi dengan baik dan pelanggan dapat melakukan pembayaran dengan lancar.
2. **Waktu Respon:** Waktu respon adalah waktu yang dibutuhkan sistem untuk memproses permintaan pembayaran dan mengirimkan respon. Waktu respon yang cepat menunjukkan bahwa integrasi payment gateway berfungsi dengan baik dan memberikan pengalaman yang baik kepada pelanggan.
3. **Tingkat Penolakan:** Metrik ini mengukur persentase transaksi yang ditolak oleh payment gateway karena berbagai alasan, seperti masalah dengan kartu kredit atau kesalahan input data. Tingkat penolakan yang rendah menunjukkan bahwa integrasi payment

gateway berfungsi dengan baik dan pelanggan dapat melakukan pembayaran dengan lancar.

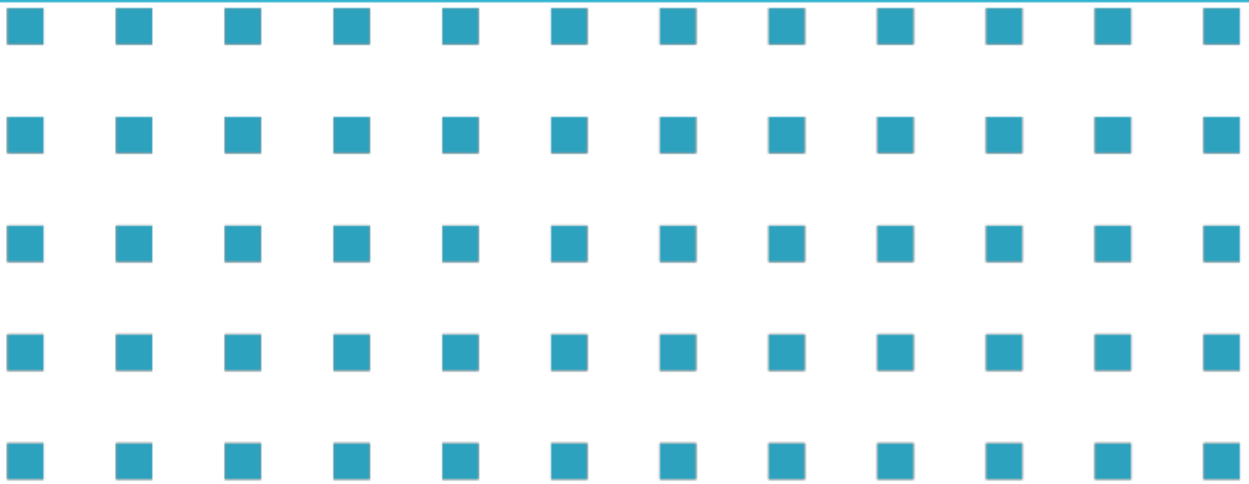
4. **Biaya Transaksi:** Biaya transaksi adalah biaya yang dikenakan oleh payment gateway untuk setiap transaksi yang berhasil. Dalam mengevaluasi integrasi payment gateway, penting untuk mempertimbangkan biaya transaksi dan memastikan bahwa mereka wajar dan kompetitif.
5. **Keamanan:** Evaluasi keamanan sistem pembayaran Anda dengan memeriksa apakah sistem memenuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi yang tepat. Keamanan yang baik menunjukkan bahwa integrasi payment gateway melindungi data pelanggan dan informasi pembayaran.
6. **Dukungan Pelanggan:** Metrik ini mengukur kualitas dukungan yang diberikan oleh penyedia payment gateway kepada Anda dan pelanggan Anda. Dukungan yang baik dapat membantu Anda mengatasi masalah dengan integrasi payment gateway dan memastikan pengalaman yang baik untuk pelanggan.
7. **Ketersediaan Sistem:** Metrik ini mengukur persentase waktu di mana sistem pembayaran Anda berfungsi tanpa gangguan. Ketersediaan sistem yang tinggi menunjukkan bahwa integrasi payment gateway berfungsi dengan baik dan dapat diandalkan.

Dengan mengukur metrik-metrik ini, Anda dapat mengevaluasi integrasi payment gateway dan memastikan bahwa sistem pembayaran Anda berfungsi

dengan baik, memberikan pengalaman yang baik kepada pelanggan, dan mendukung pertumbuhan bisnis Anda.

6

# Manajemen Operasional



# Pendahuluan

Pemantauan dan analisis transaksi adalah komponen penting dalam manajemen operasional payment gateway. Berikut adalah langkah-langkah pemantauan dan analisis transaksi dari sisi pebisnis dan pengelola payment gateway:

## *Dari sisi pebisnis:*

---

### **Memonitor transaksi:**

---

Pantau transaksi secara real-time melalui dashboard atau sistem manajemen yang disediakan oleh payment gateway. Ini akan membantu Anda mengidentifikasi tren penjualan, volume transaksi, dan metode pembayaran yang paling populer.

### **Mengevaluasi tingkat keberhasilan transaksi:**

---

Analisis tingkat keberhasilan transaksi untuk memastikan bahwa proses pembayaran berfungsi dengan baik dan pelanggan dapat melakukan pembayaran dengan lancar.

### Menganalisis tingkat penolakan:

Pantau tingkat penolakan untuk mengidentifikasi masalah yang mungkin terjadi, seperti masalah dengan kartu kredit atau kesalahan input data. Dengan mengatasi masalah ini, Anda dapat meningkatkan tingkat keberhasilan transaksi.

### Melacak biaya transaksi:

Tinjau biaya transaksi yang dikenakan oleh payment gateway untuk memastikan bahwa biaya tersebut wajar dan kompetitif.

### Menganalisis waktu respon:

Pantau waktu respon sistem untuk memastikan bahwa proses pembayaran berjalan lancar dan memberikan pengalaman yang baik kepada pelanggan.

### Memonitor keamanan:

Pastikan bahwa sistem pembayaran Anda mematuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi yang tepat.

### Melacak keluhan pelanggan:

Pantau dan tangani keluhan pelanggan terkait proses pembayaran untuk memastikan pengalaman yang baik bagi pelanggan.



## *Dari sisi pengelola payment gateway:*

### Memonitor kinerja sistem:

Pantau kinerja sistem secara real-time untuk mengidentifikasi masalah yang mungkin terjadi, seperti downtime atau masalah koneksi.

### Menganalisis volume transaksi:

Analisis volume transaksi untuk mengidentifikasi tren dan pola yang mungkin mempengaruhi kinerja sistem.

### Mengevaluasi tingkat keberhasilan transaksi:

Pantau tingkat keberhasilan transaksi untuk memastikan bahwa sistem pembayaran berfungsi dengan baik.

### Menganalisis tingkat penolakan:

Pantau tingkat penolakan untuk mengidentifikasi masalah yang mungkin terjadi dan mengambil tindakan yang diperlukan untuk mengatasi masalah tersebut.

### Melacak waktu respon:

Pantau waktu respon sistem untuk memastikan bahwa proses pembayaran berjalan lancar dan efisien.

### Memonitor keamanan:

Pastikan bahwa sistem pembayaran mematuhi standar keamanan seperti PCI DSS dan menggunakan teknologi enkripsi yang tepat.

### Mengelola dukungan pelanggan:

Menyediakan dukungan pelanggan yang efektif dan responsif untuk membantu pebisnis dan pelanggan dalam mengatasi masalah yang mungkin terjadi dengan proses pembayaran.

Dengan mengikuti langkah-langkah ini, baik pebisnis maupun pengelola payment gateway dapat memastikan bahwa sistem pembayaran berfungsi dengan baik, memberikan pengalaman yang baik kepada pelanggan, dan mendukung pertumbuhan

Bab ini akan membahas beberapa contoh advergames yang sukses dan efektif dalam mencapai tujuan pemasaran mereka. Dalam bab ini, kita akan menganalisis setiap studi kasus secara mendalam, melihat strategi yang digunakan, serta pelajaran yang dapat diambil dari kesuksesan mereka.

## Fraud

Dalam operasional payment gateway, ada beberapa jenis penipuan atau fraud yang mungkin terjadi. Berikut adalah beberapa contoh yang umum:

### ***Chargeback Fraud dan Friendly Fraud:***

---

Chargeback fraud terjadi ketika pelanggan mengajukan permintaan chargeback (pembalikan transaksi) kepada bank penerbit kartu kredit mereka dengan alasan yang tidak sah, seperti mengklaim bahwa mereka tidak menerima barang atau jasa yang telah dibayar. Tujuannya adalah untuk mendapatkan pengembalian dana sementara tetap mempertahankan produk atau jasa yang diperoleh.

Friendly fraud serupa dengan chargeback fraud, tetapi dilakukan oleh pelanggan yang mungkin tidak menyadari bahwa tindakan mereka merupakan penipuan. Pelanggan ini mungkin secara jujur merasa bahwa mereka memiliki alasan yang sah untuk mengajukan chargeback. Antisipasi dan penanganan chargeback fraud melibatkan beberapa langkah yang dapat membantu mengurangi risiko dan dampaknya pada bisnis Anda. Berikut adalah beberapa langkah yang dapat diambil:

#### **Kebijakan dan prosedur yang jelas:**

Pastikan bahwa kebijakan pengembalian dana, pengiriman, dan pembatalan Anda jelas dan mudah ditemukan oleh pelanggan. Hal ini dapat membantu

mengurangi kemungkinan chargeback yang diajukan karena kesalahpahaman.

### **Komunikasi yang baik dengan pelanggan:**

Tanggapi pertanyaan dan keluhan pelanggan secara cepat dan profesional. Jika pelanggan merasa dihargai dan didengarkan, mereka lebih mungkin untuk menyelesaikan masalah secara langsung daripada mengajukan chargeback.

### **Deskripsi produk yang akurat:**

Pastikan deskripsi produk di situs web Anda akurat dan informatif. Ini akan membantu mengurangi kemungkinan chargeback yang diajukan karena produk tidak sesuai dengan harapan pelanggan.

### **Verifikasi alamat pengiriman:**

Gunakan sistem verifikasi alamat (AVS = address verification system) untuk memastikan bahwa alamat pengiriman yang dimasukkan oleh pelanggan benar. Hal ini dapat membantu mengurangi chargeback yang diajukan karena produk tidak sampai ke pelanggan.

### **Penggunaan teknologi anti-fraud:**

Implementasikan teknologi anti-fraud seperti verifikasi kartu (CVV) dan verifikasi identitas (seperti

OTP) untuk membantu mengurangi kemungkinan transaksi yang tidak sah.



Letak CVV

## 2 Pemantauan transaksi:

Pantau transaksi secara real-time untuk mengidentifikasi pola yang mencurigakan dan mengambil tindakan segera jika diperlukan.

### **Bukti pengiriman:**

---

Simpan bukti pengiriman (seperti nomor pelacakan atau tanda terima) untuk setiap pesanan yang dikirim. Ini dapat digunakan sebagai bukti jika chargeback diajukan dan membantu dalam proses penyelesaian chargeback.

### **Pengelolaan chargeback yang efektif:**

---

Jika chargeback diajukan, tanggapilah dengan cepat dan lengkapi semua informasi yang diperlukan oleh bank atau penyedia payment gateway. Sediakan bukti yang relevan, seperti bukti pengiriman, komunikasi dengan pelanggan, atau catatan transaksi.

### **Edukasi pelanggan:**

---

Berikan informasi tentang chargeback dan dampaknya pada bisnis Anda kepada pelanggan. Hal ini dapat membantu mengurangi kemungkinan chargeback yang diajukan karena ketidaktahuan.

Dengan mengimplementasikan langkah-langkah ini, Anda dapat mengurangi risiko chargeback fraud dan melindungi bisnis Anda dari dampak negatif yang mungkin timbul akibat penipuan ini.

## ***Identitas Palsu:***

---

Penipuan ini melibatkan pencurian identitas, di mana penjahat menggunakan informasi pribadi yang dicuri (seperti nomor kartu kredit atau data pribadi) untuk melakukan pembelian secara ilegal. Untuk mencegah dan mengantisipasi identitas palsu dalam transaksi online, berikut beberapa langkah yang dapat diambil oleh pebisnis:

### **Verifikasi identitas pelanggan:**

---

Gunakan metode verifikasi identitas yang kuat, seperti verifikasi dua faktor, OTP, atau sistem autentikasi biometrik. Ini akan membantu memastikan bahwa transaksi dilakukan oleh pemilik kartu yang sebenarnya.

### **Pemeriksaan alamat:**

---

Gunakan sistem verifikasi alamat (AVS) untuk memeriksa kecocokan antara alamat penagihan yang dimasukkan oleh pelanggan dan alamat yang terdaftar di bank. Ini akan membantu mengidentifikasi transaksi yang mencurigakan dan mencegah penipuan identitas.

### **Verifikasi CVV:**

---

Meminta pelanggan memasukkan kode verifikasi kartu (CVV) saat melakukan pembayaran. Hal ini

menambahkan lapisan keamanan ekstra untuk memastikan bahwa pelanggan yang melakukan transaksi memiliki kartu fisik.

### Sistem deteksi penipuan:

Gunakan sistem deteksi penipuan yang canggih untuk menganalisis pola transaksi, perilaku pengguna, dan data lainnya yang dapat menunjukkan upaya penipuan identitas. Sistem ini akan memberi peringatan jika ada transaksi mencurigakan.

### Pemantauan transaksi:

Pantau transaksi secara real-time untuk mengidentifikasi aktivitas yang tidak biasa atau mencurigakan. Jika Anda melihat transaksi yang mencurigakan, hubungi pelanggan untuk memverifikasi transaksi tersebut.

### Edukasi pelanggan:

Beri tahu pelanggan tentang risiko penipuan identitas dan langkah-langkah yang mereka bisa ambil untuk melindungi diri mereka sendiri, seperti menjaga informasi pribadi dan keuangan mereka aman serta melaporkan kegiatan mencurigakan.



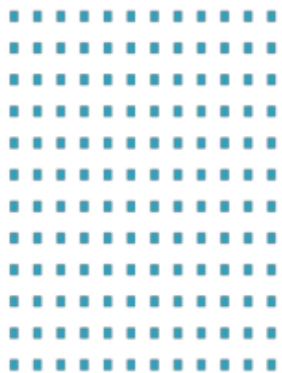
### Kebijakan keamanan yang kuat:

Pastikan Anda memiliki kebijakan keamanan yang kuat dan mematuhi standar industri, seperti PCI DSS. Kebijakan ini harus mencakup langkah-langkah untuk melindungi data pelanggan dan mencegah akses yang tidak sah.

### Pelatihan karyawan:

Berikan pelatihan kepada karyawan tentang penipuan identitas dan cara mengidentifikasi tanda-tanda peringatan. Karyawan yang terlatih dan sadar akan risiko penipuan lebih mampu mengidentifikasi dan mencegah aktivitas mencurigakan.

Dengan mengambil langkah-langkah ini, Anda dapat mengurangi risiko penipuan identitas dalam transaksi online dan melindungi bisnis Anda dari dampak negatif yang mungkin timbul akibat penipuan ini.



---

***Phishing adalah teknik yang digunakan oleh penjahat untuk memperoleh informasi kartu kredit dengan mengirimkan email atau pesan yang seolah-olah berasal dari bank atau lembaga keuangan***

---

## ***Pencurian Kartu Kredit:***

---

Penipuan ini melibatkan penggunaan kartu kredit yang dicuri untuk melakukan pembelian. Penjahat dapat mencuri informasi kartu fisik atau mencuri informasi kartu kredit secara online melalui teknik seperti phishing. Berikut beberapa teknik yang sering digunakan dalam pencurian kartu kredit:

### **Phishing:**

---

Phishing adalah teknik yang digunakan oleh penjahat untuk memperoleh informasi kartu kredit dengan mengirimkan email atau pesan yang seolah-olah berasal dari bank atau lembaga keuangan terkait. Email atau pesan ini biasanya mengandung tautan ke situs web palsu yang meniru situs resmi, di mana korban diminta untuk memasukkan informasi kartu kredit mereka.

### **Skimming:**

---

Skimming adalah teknik di mana perangkat yang disebut skimmer ditempatkan pada pembaca kartu di ATM, mesin bensin, atau terminal pembayaran lainnya. Skimmer ini menangkap informasi kartu kredit saat kartu digesek, dan data ini kemudian digunakan oleh penjahat untuk melakukan transaksi palsu.

### **Hacking atau peretasan:**

Penjahat sering mencoba meretas sistem perusahaan atau toko online untuk mencuri informasi kartu kredit yang disimpan. Mereka juga dapat mengakses jaringan Wi-Fi yang tidak aman atau menggunakan perangkat lunak jahat (malware) untuk menginfeksi komputer dan mencuri informasi kartu kredit.

### **Pencurian fisik:**

Pencurian fisik kartu kredit masih menjadi masalah, meskipun teknologi keamanan kartu telah meningkat. Penjahat dapat mencuri kartu kredit dari dompet, tas, atau surat dan kemudian menggunakan kartu tersebut untuk melakukan transaksi palsu.

### **Carding:**

Carding adalah teknik di mana penjahat menggunakan perangkat lunak atau alat khusus untuk menguji informasi kartu kredit yang dicuri pada situs web atau aplikasi dengan keamanan yang lemah. Tujuannya adalah untuk menemukan informasi kartu yang valid untuk digunakan dalam transaksi penipuan.

### Kejahatan lintas batas:

Penjahat sering menggunakan informasi kartu kredit yang dicuri untuk melakukan transaksi di negara lain, di mana pelacakan dan penegakan hukum lebih sulit. Transaksi lintas batas ini seringkali melibatkan pembelian barang-barang mahal yang kemudian dijual kembali untuk mendapatkan keuntungan.

### Penipuan Rekening Merchant:

Penipuan ini melibatkan penciptaan rekening merchant palsu atau penggunaan rekening merchant yang telah dikompromikan untuk memproses transaksi ilegal.

### Penipuan Refund:

Penipuan ini terjadi ketika penjahat mengajukan permintaan refund palsu untuk transaksi yang sebenarnya sah, dengan harapan untuk mendapatkan uang kembali sementara tetap memiliki produk atau jasa yang diperoleh.

### Triangulasi Penipuan:

Triangulasi penipuan melibatkan penjahat yang menjual produk dengan harga murah melalui situs e-commerce palsu. Ketika pembeli melakukan pembelian, penjahat menggunakan informasi kartu kredit yang dicuri untuk membeli produk dari penjual yang sah dan mengirimkannya ke pembeli. Dalam hal ini, pembeli mungkin tidak menyadari bahwa mereka telah terlibat dalam penipuan.

Untuk melindungi terhadap penipuan ini, payment gateway dan merchant harus mengimplementasikan langkah-langkah keamanan yang kuat, seperti verifikasi dua faktor, sistem pendeteksian penipuan, dan pemantauan transaksi secara real-time. Selain itu, edukasi konsumen tentang keamanan online dan cara menghindari penipuan juga penting dalam meminimalkan risiko penipuan.

Untuk melindungi diri dari pencurian kartu kredit, penting bagi konsumen dan bisnis untuk mengimplementasikan langkah-langkah keamanan yang kuat, seperti menggunakan sistem verifikasi pembayaran yang aman, melindungi informasi pribadi dan keuangan, serta menjaga komputer dan jaringan mereka dari peretasan dan malware.



# Refund dan Sengketa

Pemrosesan refund dan penyelesaian sengketa merupakan bagian penting dalam manajemen operasional payment gateway. Hal ini melibatkan pengembalian dana kepada pelanggan dan menyelesaikan perselisihan yang mungkin timbul karena berbagai alasan, seperti pembatalan pesanan, barang yang tidak sesuai, atau transaksi yang tidak sah.

Berikut ini adalah penjelasan detail mengenai proses pemrosesan refund dan penyelesaian sengketa:

## ***Pemrosesan Refund:***

---

### **Permintaan Refund:**

Pelanggan yang ingin meminta refund harus menghubungi penjual atau layanan pelanggan toko online terkait. Pelanggan perlu menyampaikan alasan pengembalian dana dan memberikan bukti yang relevan, seperti nomor pesanan, foto produk yang bermasalah, atau keterangan lainnya.

### Evaluasi Permintaan:

Penjual atau layanan pelanggan akan mengevaluasi permintaan refund berdasarkan kebijakan pengembalian dana yang berlaku dan bukti yang disampaikan oleh pelanggan. Jika permintaan dianggap valid, mereka akan melanjutkan proses refund.

### Pengajuan Refund:

Penjual akan mengajukan permintaan refund melalui sistem payment gateway yang digunakan. Permintaan ini akan mencakup informasi transaksi yang relevan, seperti nomor transaksi, jumlah pengembalian dana, dan alasan pengembalian.

### Pemrosesan oleh Payment Gateway:

Payment gateway akan memproses permintaan refund dan mengembalikan dana ke metode pembayaran yang digunakan oleh pelanggan (misalnya, kartu kredit, dompet digital, atau rekening bank). Proses ini bisa memakan waktu beberapa hari, tergantung pada kebijakan payment gateway dan metode pembayaran yang digunakan.

### Konfirmasi Refund:

Setelah dana dikembalikan, penjual atau layanan pelanggan akan menginformasikan pelanggan mengenai status refund. Pelanggan dapat memeriksa saldo rekening mereka untuk memastikan bahwa pengembalian dana telah diterima.



---

*Penjual atau layanan pelanggan akan mengevaluasi permintaan refund berdasarkan kebijakan pengembalian dana yang berlaku dan bukti yang disampaikan oleh pelanggan*

---



## ***Penyelesaian Sengketa:***

---

### **Pengajuan Sengketa:**

---

108

Jika pelanggan tidak puas dengan produk atau layanan yang diterima, atau jika terjadi transaksi yang tidak sah, mereka dapat mengajukan sengketa melalui sistem payment gateway atau lembaga keuangan yang mengeluarkan kartu kredit.

### **Pemberitahuan kepada Penjual:**

---

Payment gateway atau lembaga keuangan akan memberitahukan penjual tentang sengketa yang diajukan. Penjual diberi kesempatan untuk menanggapi sengketa dan memberikan bukti yang relevan untuk membela diri.

### **Evaluasi Sengketa:**

---

Payment gateway atau lembaga keuangan akan mengevaluasi bukti yang disampaikan oleh kedua pihak dan membuat keputusan mengenai penyelesaian sengketa. Keputusan ini bisa melibatkan pengembalian dana penuh atau sebagian kepada pelanggan, atau penolakan klaim sengketa.

### **Pelaksanaan Keputusan:**

Setelah keputusan dibuat, payment gateway atau lembaga keuangan akan melaksanakan keputusan tersebut. Jika pengembalian dana diperlukan, dana akan dikembalikan ke pelanggan sesuai dengan keputusan. Jika klaim sengketa ditolak, tidak ada tindakan lebih lanjut yang diambil.

### **Komunikasi Hasil:**

Payment gateway atau lembaga keuangan akan menginformasikan kedua pihak tentang hasil penyelesaian sengketa. Penjual dan pelanggan diharapkan untuk mematuhi keputusan yang dibuat.

### **Tindakan Lanjutan:**

Jika penjual atau pelanggan tidak puas dengan hasil penyelesaian sengketa, mereka dapat mencari tindakan lanjutan melalui jalur hukum atau alternatif lain yang sesuai, seperti mediasi atau arbitrase. Namun, proses ini biasanya memerlukan waktu, tenaga, dan biaya tambahan yang mungkin tidak efisien dalam beberapa kasus.

Penting bagi penjual dan pelanggan untuk memahami proses pemrosesan refund dan penyelesaian sengketa ini agar dapat mengelola transaksi secara efektif dan memastikan kepuasan pelanggan.

7

# E-Money dan E- Ewallet

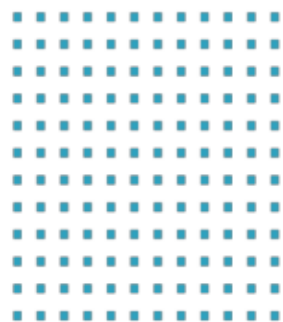


E-money (uang elektronik) dan e-wallet (dompet elektronik) adalah dua teknologi yang sering digunakan dalam transaksi digital. Mereka memiliki hubungan yang erat dengan payment gateway, karena keduanya merupakan metode pembayaran yang umum digunakan pada platform online. Berikut ini adalah penjelasan detail mengenai relasi antara payment gateway dengan e-money dan e-wallet:

## *Payment Gateway dan E-money:*

E-money adalah alat pembayaran elektronik yang memungkinkan pengguna untuk melakukan transaksi digital tanpa harus menggunakan uang tunai atau kartu kredit/debit fisik. E-money umumnya diterbitkan oleh lembaga keuangan atau perusahaan yang telah mendapatkan izin dari otoritas moneter yang relevan. Di Indonesia, Bank Indonesia adalah otoritas yang mengatur penerbitan e-money.

Payment gateway berperan sebagai penghubung antara e-money dan platform e-commerce atau aplikasi yang menerima pembayaran online. Ketika pengguna memilih untuk membayar dengan e-money, payment gateway akan mengirim permintaan otorisasi ke penerbit e-money untuk memverifikasi saldo dan mengurangi jumlah transaksi dari saldo e-money pengguna. Setelah otorisasi berhasil, payment gateway akan mengkonfirmasi transaksi dan memproses pembayaran.



---

***Payment gateway memiliki peran penting dalam integrasi e-wallet dengan platform e-commerce dan aplikasi lain yang menerima pembayaran online***

---

### *Payment Gateway dan E-wallet:*

---

E-wallet adalah aplikasi atau layanan yang menyimpan informasi keuangan pengguna, seperti nomor rekening bank, kartu kredit, dan saldo e-money. E-wallet memungkinkan pengguna untuk melakukan pembayaran digital dengan mudah dan cepat, tanpa harus memasukkan informasi keuangan setiap kali mereka melakukan transaksi.

Payment gateway memiliki peran penting dalam integrasi e-wallet dengan platform e-commerce dan aplikasi lain yang menerima pembayaran online. Ketika pengguna memilih untuk membayar dengan e-wallet, payment gateway akan mengakses informasi keuangan yang disimpan dalam e-wallet dan mengirimkan permintaan otorisasi ke metode pembayaran yang relevan (misalnya, penerbit kartu kredit atau e-money). Setelah otorisasi berhasil, payment gateway akan mengkonfirmasi transaksi dan memproses pembayaran.

Secara keseluruhan, payment gateway, e-money, dan e-wallet saling terkait dalam ekosistem pembayaran digital. Payment gateway memfasilitasi transaksi online antara pengguna yang menggunakan e-money atau e-wallet sebagai metode pembayaran dan penjual atau platform yang menerima pembayaran tersebut. Integrasi antara ketiganya memungkinkan transaksi yang lebih cepat, aman, dan nyaman bagi pengguna dan penjual.

	<b>E-money</b>	<b>E-wallet</b>
<b>Definisi</b>	Alat pembayaran elektronik yang memungkinkan transaksi digital tanpa uang tunai atau kartu fisik.	Aplikasi atau layanan yang menyimpan informasi keuangan pengguna seperti nomor rekening, kartu kredit, dan saldo e-money.
<b>Regulasi</b>	Diterbitkan oleh lembaga keuangan yang telah mendapatkan izin dari otoritas moneter yang relevan.	Tidak diatur secara langsung oleh otoritas moneter, tetapi harus mematuhi peraturan yang berlaku untuk metode pembayaran.
<b>Peran Payment Gateway</b>	Mengirim permintaan otorisasi ke penerbit e-money untuk memverifikasi saldo dan mengurangi jumlah transaksi.	Mengakses informasi keuangan yang disimpan dalam e-wallet dan mengirimkan permintaan otorisasi ke metode

	<b>E-money</b>	<b>E-wallet</b>
		pembayaran yang relevan.
<b>Integrasi</b>	Payment gateway berperan sebagai penghubung antara e-money dan platform yang menerima pembayaran online.	Payment gateway berperan dalam integrasi e-wallet dengan platform yang menerima pembayaran online.
<b>Kelebihan</b>	Kecepatan transaksi, kemudahan penggunaan, dan keamanan yang lebih tinggi.	Kemudahan dan kecepatan transaksi, keamanan informasi keuangan, dan kemampuan untuk menyimpan berbagai metode pembayaran.

130

Meskipun e-money dan e-wallet memiliki beberapa perbedaan dalam definisi dan regulasi, keduanya terintegrasi dengan payment gateway untuk memfasilitasi transaksi yang cepat, aman, dan nyaman bagi pengguna dan penjual.



# QR Code

122

QR Code, seperti QRIS (Quick Response Code Indonesian Standard), bukanlah payment gateway dalam pengertian tradisional. QRIS adalah standar yang dikembangkan oleh Bank Indonesia untuk menyederhanakan dan menyatukan pembayaran digital melalui QR Code di Indonesia.

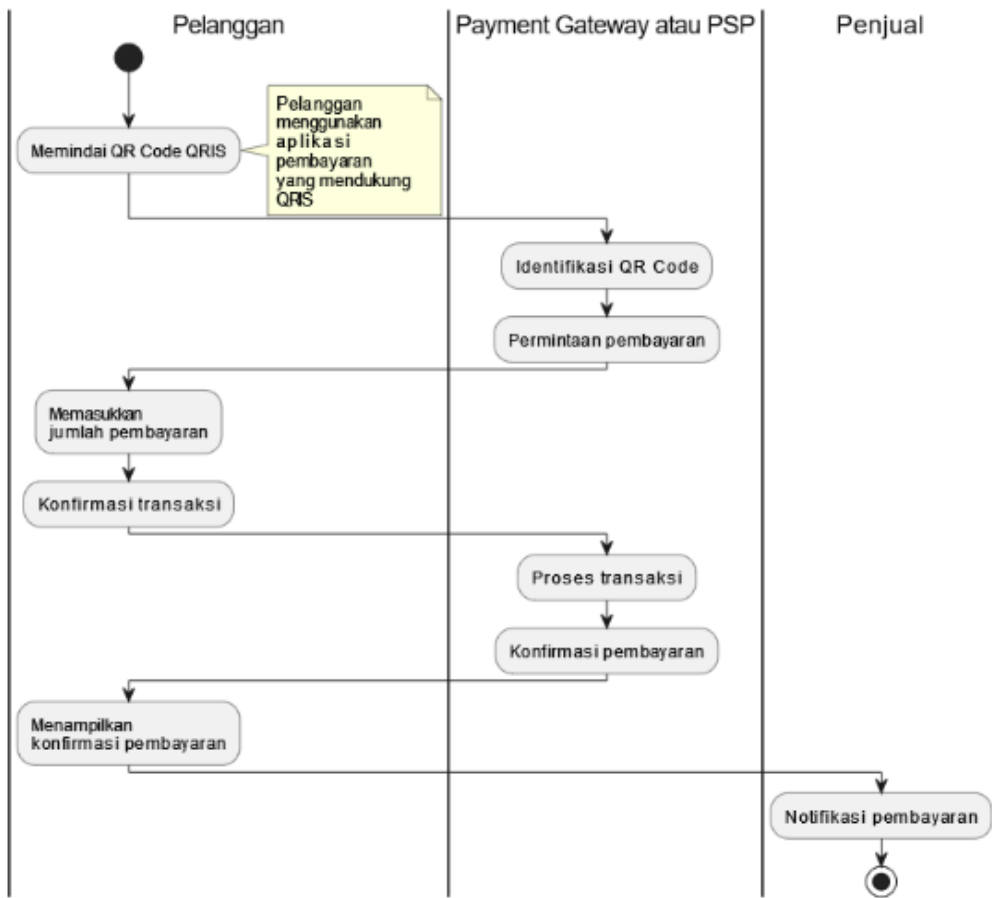


QRIS (<https://qris.id>)

Namun, QRIS berfungsi sebagai sistem pembayaran yang saling terhubung dengan berbagai payment gateway dan penyedia layanan pembayaran (PSP) di Indonesia. Ketika pengguna melakukan pembayaran dengan memindai QR Code QRIS, aplikasi pembayaran yang digunakan akan menghubungkan ke payment gateway atau PSP yang relevan untuk memproses transaksi tersebut.

Dalam konteks ini, QRIS memfasilitasi pembayaran digital dengan menyediakan cara yang mudah dan cepat untuk menghubungkan pelanggan dengan payment gateway atau PSP yang sesuai. Meskipun QRIS sendiri bukan payment gateway, penggunaannya dalam transaksi digital melibatkan koordinasi dan integrasi dengan payment gateway dan sistem pembayaran lainnya. Berikut adalah langkah-langkah yang melibatkan QRIS dalam menghubungkan pelanggan dengan payment gateway:

1. Penjual menampilkan QR Code QRIS yang telah terdaftar pada platform pembayaran mereka.
2. Pelanggan membuka aplikasi pembayaran yang mendukung QRIS di ponsel mereka.
3. Pelanggan memindai QR Code menggunakan aplikasi pembayaran.
4. Aplikasi pembayaran mengidentifikasi kode QR dan menghubungkan ke payment gateway atau Penyedia Layanan Pembayaran (PSP) yang relevan.
5. Pelanggan memasukkan jumlah pembayaran dan mengonfirmasi transaksi.
6. Aplikasi pembayaran mengirimkan permintaan pembayaran ke payment gateway atau PSP.
7. Payment gateway atau PSP memproses transaksi dan mengirimkan konfirmasi ke aplikasi pembayaran.
8. Aplikasi pembayaran menampilkan konfirmasi pembayaran kepada pelanggan.
9. Penjual menerima notifikasi pembayaran dari platform pembayaran mereka.



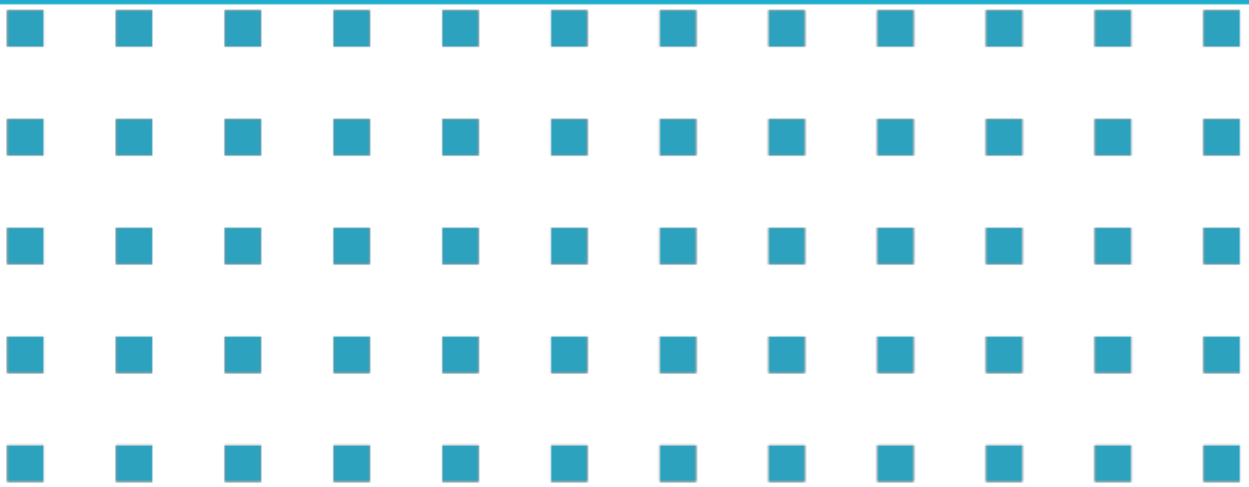
Activity Diagram QR Code



**QRIS berfungsi sebagai sistem pembayaran yang saling terhubung dengan berbagai payment gateway dan penyedia layanan pembayaran (PSP) di Indonesia**

7

# Kondisi dan Peluang



Kondisi saat ini dan masa depan payment gateway di tingkat internasional terus berkembang dan mengalami perubahan seiring dengan perkembangan teknologi, perubahan regulasi, dan kebutuhan konsumen. Berikut adalah beberapa tren dan perkembangan yang mempengaruhi payment gateway di tingkat internasional:

### Penetrasi pasar e-commerce:

E-commerce terus berkembang di seluruh dunia, yang mengakibatkan peningkatan kebutuhan akan payment gateway yang efisien, aman, dan mudah digunakan. Dengan pertumbuhan pesat dalam e-commerce, peran payment gateway semakin penting dalam menyediakan pengalaman pembayaran yang mulus bagi konsumen.

### Pembayaran seluler dan nirkontak:

Perkembangan teknologi seluler telah mengubah cara orang berbelanja dan melakukan transaksi. Hal ini menciptakan permintaan yang lebih besar untuk solusi pembayaran seluler dan nirkontak, seperti digital wallets, NFC, dan QR Code. Payment gateway perlu mengadaptasi layanan mereka untuk mendukung metode pembayaran ini.

### **Regulasi dan kepatuhan:**

---

Regulasi terus berkembang di berbagai negara untuk melindungi konsumen dan memastikan keamanan transaksi. Payment gateway perlu mengikuti perubahan dalam regulasi dan standar keamanan, seperti GDPR di Eropa, dan memastikan bahwa mereka mematuhi persyaratan tersebut.

### **Integrasi teknologi blockchain dan mata uang kripto:**

---

Blockchain dan mata uang kripto seperti Bitcoin dan Ethereum telah menjadi alternatif dalam transaksi digital. Beberapa payment gateway mulai menawarkan dukungan untuk pembayaran kripto dan mungkin akan melihat adopsi yang lebih luas di masa depan.

### **Kecerdasan buatan dan pembelajaran mesin:**

---

Payment gateway dapat menggunakan kecerdasan buatan (AI) dan pembelajaran mesin untuk meningkatkan keamanan, menganalisis pola transaksi, dan mendeteksi aktivitas mencurigakan. Dalam beberapa tahun ke depan, AI dan pembelajaran mesin akan menjadi semakin penting dalam operasi payment gateway.

### Pembayaran lintas batas:

Globalisasi ekonomi dan pertumbuhan e-commerce internasional menciptakan permintaan yang lebih besar untuk transaksi lintas batas. Payment gateway perlu mendukung berbagai mata uang dan sistem pembayaran untuk memfasilitasi transaksi antarnegara.

Kondisi saat ini dan masa depan payment gateway di tingkat internasional akan terus berubah seiring dengan perkembangan teknologi dan perubahan dalam kebiasaan konsumen. Payment gateway yang berhasil akan terus berinovasi dan menyesuaikan layanan mereka untuk memenuhi kebutuhan yang terus berkembang.



# Integrasi Blockchain

Integrasi blockchain dan kripto dalam payment gateway menawarkan beberapa peluang dan tantangan. Berikut adalah beberapa hal yang perlu diperhatikan saat mengintegrasikan teknologi ini ke dalam sistem pembayaran:

## Kecepatan transaksi:

Transaksi kripto, tergantung pada jaringan yang digunakan, mungkin memerlukan waktu lebih lama untuk diproses dibandingkan dengan metode pembayaran tradisional. Beberapa jaringan kripto memiliki waktu konfirmasi yang lebih cepat, tetapi mungkin perlu dipertimbangkan untuk mencari solusi yang mengoptimalkan kecepatan transaksi.

## Stabilitas nilai:

Volatilitas harga mata uang kripto bisa menjadi perhatian bagi pedagang dan konsumen. Sebagai solusi, beberapa payment gateway menawarkan konversi otomatis ke mata uang fiat untuk mengurangi risiko nilai tukar yang berfluktuasi.



### **Regulasi :**

---

Regulasi seputar mata uang kripto dan blockchain bervariasi di berbagai negara dan wilayah. Payment gateway yang mengintegrasikan teknologi ini harus memastikan kepatuhan terhadap regulasi setempat dan siap menghadapi perubahan regulasi yang mungkin terjadi.

### **Keamanan :**

---

Meskipun teknologi blockchain secara inheren aman, risiko keamanan tetap ada, terutama dalam hal penyimpanan dan pengelolaan kunci pribadi. Payment gateway harus memastikan bahwa mereka menerapkan praktik keamanan terbaik untuk melindungi data pengguna dan aset kripto.

### **Adopsi dan penggunaan :**

---

Tidak semua konsumen dan pedagang familiar dengan mata uang kripto dan teknologi blockchain. Oleh karena itu, penting bagi payment gateway untuk menyediakan dukungan dan pendidikan bagi pengguna serta menawarkan integrasi yang mudah dengan metode pembayaran tradisional.

### Biaya transaksi:

Biaya transaksi untuk beberapa mata uang kripto bisa menjadi perhatian, terutama dalam jaringan yang mengalami kemacetan. Payment gateway harus mencari solusi yang menawarkan biaya transaksi yang kompetitif dan wajar.

### Kepatuhan <sup>2</sup> Anti Pencucian Uang (APU) dan Pencegahan Pendanaan Terorisme (PPT) :

Payment gateway harus memastikan bahwa mereka mematuhi peraturan APU dan PPT yang berlaku saat mengintegrasikan mata uang kripto, termasuk melaksanakan prosedur Know Your Customer (KYC) dan melaporkan aktivitas mencurigakan.



---

*Meskipun teknologi blockchain secara inheren aman, risiko keamanan tetap ada, terutama dalam hal penyimpanan dan pengelolaan kunci pribadi*

---

Dengan mempertimbangkan tantangan ini, payment gateway dapat menggabungkan teknologi ini dengan cara yang efektif dan menguntungkan.

<b>Aspek</b>	<b>Keterangan</b>
<b>Keamanan</b>	Blockchain meningkatkan keamanan melalui enkripsi dan desentralisasi data
<b>Kecepatan</b>	Transaksi dengan crypto lebih cepat dibandingkan dengan metode pembayaran tradisional
<b>Biaya</b>	Biaya transaksi crypto cenderung lebih rendah
<b>Regulasi</b>	Regulasi crypto berbeda-beda di tiap negara dan mempengaruhi penerapan pada payment gateway
<b>Adopsi</b>	Adopsi crypto dan blockchain masih terbatas, terutama di beberapa sektor bisnis
<b>Volatilitas</b>	Volatilitas harga crypto dapat mempengaruhi stabilitas nilai transaksi

# Pembayaran lintas batas

Payment gateway dapat membantu memfasilitasi pembayaran lintas batas dan berpotensi memiliki dampak positif pada aktivitas ekspor-impor. Meskipun demikian, payment gateway tidak akan sepenuhnya menggantikan metode pembayaran lintas batas yang ada saat ini, seperti transfer bank internasional atau layanan pengiriman uang. Berikut beberapa alasan mengapa payment gateway akan menjadi pelengkap, bukan pengganti metode pembayaran lintas batas:

## Regulasi dan kepatuhan:

Setiap negara memiliki peraturan yang berbeda mengenai pembayaran lintas batas dan transfer uang. Payment gateway harus memastikan kepatuhan dengan regulasi di berbagai yurisdiksi, yang mungkin mempengaruhi kemampuannya untuk secara efektif menggantikan metode pembayaran tradisional.

### **Adopsi:**

---

Meskipun payment gateway semakin populer, tidak semua bisnis dan konsumen telah mengadopsinya. Dalam beberapa kasus, metode pembayaran tradisional mungkin lebih mudah diakses atau lebih diterima oleh pihak yang terlibat dalam transaksi lintas batas.

### **Likuiditas dan konversi mata uang:**

---

Metode pembayaran tradisional, seperti transfer bank internasional, seringkali menawarkan likuiditas yang lebih baik dan kemudahan konversi mata uang. Payment gateway mungkin tidak dapat menawarkan tingkat likuiditas yang sama, terutama jika mereka bergantung pada mata uang digital atau metode pembayaran alternatif.

### **Keamanan dan risiko:**

---

Meskipun payment gateway umumnya menawarkan tingkat keamanan yang tinggi, mereka juga rentan terhadap risiko keamanan, seperti serangan siber atau kegagalan teknis. Metode pembayaran tradisional mungkin dianggap lebih aman oleh beberapa pihak yang terlibat dalam transaksi lintas batas.

### Biaya :

---

Dalam beberapa kasus, payment gateway mungkin menawarkan biaya yang lebih rendah daripada metode pembayaran tradisional. Namun, hal ini tidak selalu menjadi kasus, dan beberapa payment gateway mungkin menambahkan biaya tambahan untuk transaksi lintas batas.

Secara keseluruhan, payment gateway dapat membantu meningkatkan efisiensi dan kemudahan pembayaran lintas batas, tetapi mereka tidak akan sepenuhnya menggantikan metode pembayaran tradisional. Mereka akan lebih mungkin menjadi pelengkap yang menawarkan solusi alternatif bagi bisnis dan konsumen yang ingin melakukan transaksi lintas batas dengan cara yang lebih cepat, lebih murah, dan lebih mudah.



---

***Metode pembayaran tradisional, seperti transfer bank internasional, seringkali menawarkan likuiditas yang lebih baik dan kemudahan konversi mata uang***

---

<b>Aspek</b>	<b>Payment Gateway</b>	<b>Metode Tradisional</b>
<b>Regulasi</b>	Harus mematuhi regulasi di berbagai yurisdiksi	Sudah sesuai dengan regulasi internasional
<b>Adopsi</b>	Semakin populer, namun belum diadopsi secara luas	Sudah diadopsi secara luas dan diterima
<b>Likuiditas</b>	Mungkin tidak menawarkan likuiditas yang sama	Menawarkan likuiditas yang lebih baik
<b>Konversi Mata Uang</b>	Mungkin kurang efisien dalam konversi mata uang	Lebih efisien dalam konversi mata uang
<b>Keamanan</b>	Rentan terhadap serangan siber dan kegagalan teknis	Dianggap lebih aman
<b>Biaya</b>	Dapat menawarkan biaya yang lebih rendah, namun tidak selalu	Biaya lebih tinggi, terutama untuk transfer lintas batas

# Peluang di Indonesia

105

Di Indonesia, kondisi saat ini dan masa depan payment gateway terlihat cukup menjanjikan karena beberapa alasan berikut:

17

## *Pertumbuhan e-commerce:*

---

Indonesia mengalami pertumbuhan pesat dalam sektor e-commerce. Perkembangan industri e-commerce ini secara langsung meningkatkan permintaan untuk solusi pembayaran yang efisien, aman, dan cepat, seperti payment gateway. Payment gateway memiliki potensi untuk menggantikan sebagian besar pembayaran konvensional di sektor e-commerce, tetapi sepenuhnya menggantikan metode pembayaran konvensional mungkin tidak akan terjadi dalam waktu dekat. Berikut beberapa alasan mengapa payment gateway akan terus berkembang dalam sektor e-commerce, tetapi pembayaran konvensional masih akan tetap ada:

## *Kemudahan dan kecepatan:*

---

98

Payment gateway menyediakan kemudahan dan kecepatan dalam melakukan transaksi online. Dengan sistem yang terintegrasi, pelanggan dapat membayar



pesanan mereka dengan cepat dan mudah tanpa harus mengunjungi bank atau outlet fisik.

### **Keamanan :**

---

Payment gateway menggunakan teknologi enkripsi canggih dan sistem keamanan yang ketat untuk melindungi data pelanggan dan mencegah penipuan. Hal ini membuat metode pembayaran digital lebih aman daripada beberapa bentuk pembayaran konvensional, seperti uang tunai atau cek.

### **Pilihan metode pembayaran:**

---

Payment gateway biasanya mendukung <sup>3</sup> berbagai metode pembayaran, seperti kartu kredit, e-wallet, dan <sup>29</sup> transfer bank. Hal ini memungkinkan pelanggan untuk <sup>29</sup> memilih metode pembayaran yang paling sesuai dengan kebutuhan dan preferensi mereka.

### **Integrasi dengan platform e-commerce :**

---

Sebagian besar platform e-commerce kini telah terintegrasi dengan payment gateway, yang memudahkan proses pembayaran dan meningkatkan konversi penjualan.

## *Faktor Keberlanjutan Pembayaran Konvensional*

---

Namun, beberapa faktor yang menjaga pembayaran konvensional tetap relevan di sektor e-commerce, antara lain:

### **Preferensi konsumen:**

Beberapa konsumen mungkin lebih nyaman menggunakan metode pembayaran konvensional, seperti pembayaran tunai atau transfer bank manual. Selain itu, beberapa konsumen mungkin tidak memiliki akses ke layanan perbankan online atau tidak ingin menggunakan metode pembayaran digital karena kekhawatiran akan keamanan dan privasi.

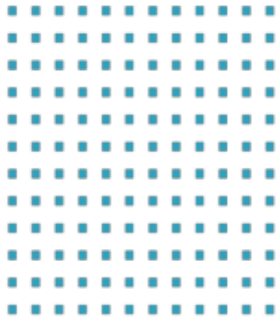
### **Infrastruktur:**

Meskipun infrastruktur teknologi terus berkembang, masih ada beberapa daerah yang memiliki konektivitas internet yang terbatas atau tidak stabil. Ini bisa menghambat penggunaan payment gateway dan mendorong konsumen untuk tetap menggunakan metode pembayaran konvensional.

### Adopsi oleh penjual:

Beberapa penjual mungkin lebih memilih untuk menerima pembayaran konvensional karena alasan biaya, kenyamanan, atau keamanan. Selama penjual ini terus menerima pembayaran konvensional, konsumen akan memiliki opsi untuk menggunakan metode pembayaran ini.

Kesimpulannya, payment gateway akan terus berkembang dan menjadi metode pembayaran yang semakin populer di sektor e-commerce. Namun, pembayaran konvensional masih akan tetap ada karena preferensi konsumen, infrastruktur, dan adopsi oleh penjual. Jadi, meskipun payment gateway memiliki potensi untuk menggantikan sebagian besar pembayaran konvensional, metode pembayaran konvensional akan tetap ada untuk waktu yang cukup lama.



---

***Meskipun infrastruktur teknologi terus berkembang, masih ada beberapa daerah yang memiliki konektivitas internet yang terbatas atau tidak stabil.***

---

<b>Faktor</b>	<b>Payment Gateway</b>	<b>Pembayaran Konvensional</b>
<b>Kemudahan dan Kecepatan</b>	Sangat cepat dan mudah	Relatif lebih lambat dan sulit
<b>Keamanan</b>	Tinggi dengan enkripsi canggih	Bervariasi, tergantung metode
<b>Pilihan Metode Pembayaran</b>	Beragam (kartu, e-wallet, dll.)	Terbatas (tunai, cek, transfer)
<b>Integrasi e-commerce</b>	Terintegrasi dengan platform	Kurang terintegrasi
<b>Preferensi Konsumen</b>	Terus meningkat	Ada yang masih setia
<b>Infrastruktur</b>	Bergantung pada koneksi internet	Tidak memerlukan internet
<b>Adopsi Penjual</b>	Meningkat di sektor e-commerce	Masih ada yang menerima

### ***Inklusi keuangan:***

---

Pemerintah Indonesia berkomitmen untuk meningkatkan inklusi keuangan di negara tersebut. Payment gateway dapat membantu mencapai tujuan ini dengan menyediakan akses yang lebih mudah ke layanan keuangan bagi penduduk yang sebelumnya tidak memiliki akses ke sistem perbankan tradisional. Payment gateway memiliki potensi untuk mendukung inklusi keuangan dengan memberikan akses yang lebih baik ke layanan keuangan bagi individu dan bisnis yang sebelumnya tidak terlayani atau kurang terlayani oleh sistem keuangan konvensional. Berikut adalah beberapa cara payment gateway dapat membantu inklusi keuangan:

### **Aksesibilitas:**

---

Payment gateway memungkinkan konsumen dan bisnis untuk melakukan transaksi keuangan melalui internet, yang dapat meningkatkan akses ke layanan keuangan bagi mereka yang berada di daerah terpencil atau tidak memiliki infrastruktur keuangan yang memadai.

### Biaya yang lebih rendah:

Payment gateway sering kali menawarkan biaya transaksi yang lebih rendah dibandingkan dengan metode pembayaran konvensional seperti transfer bank atau cek. Hal ini dapat mengurangi beban keuangan bagi individu dan bisnis yang beroperasi dengan margin yang ketat.

### Kemudahan penggunaan:

Payment gateway biasanya memiliki antarmuka yang mudah digunakan dan proses yang sederhana untuk melakukan transaksi. Hal ini dapat membantu individu yang mungkin kurang akrab dengan sistem keuangan konvensional untuk mengadopsi metode pembayaran digital dengan lebih mudah.

### Pilihan metode pembayaran:

Dengan mendukung berbagai metode pembayaran, seperti e-wallet dan transfer bank, payment gateway memberikan fleksibilitas bagi individu dan bisnis untuk memilih metode pembayaran yang paling sesuai dengan kebutuhan mereka.

### **Pengembangan layanan keuangan digital:**

---

Payment gateway juga berperan dalam mempromosikan pengembangan layanan keuangan digital, seperti pinjaman online dan layanan investasi. Ini dapat membuka akses ke produk dan layanan keuangan yang sebelumnya tidak tersedia bagi sebagian besar populasi.

### **Dukungan untuk UMKM:**

---

Payment gateway memudahkan UMKM untuk menerima pembayaran digital dan menjual produk atau jasa secara online. Hal ini dapat membantu UMKM untuk mengembangkan bisnis mereka, menciptakan lapangan kerja, dan mendukung pertumbuhan ekonomi.

Dengan demikian, payment gateway dapat memiliki dampak positif yang signifikan pada inklusi keuangan, terutama di negara-negara berkembang atau daerah dengan infrastruktur keuangan yang kurang berkembang. Namun, penting juga untuk mengatasi hambatan lain, seperti akses ke internet, literasi digital, dan regulasi yang tepat, agar manfaat dari payment gateway dapat dirasakan oleh seluruh masyarakat.

### *Regulasi yang mendukung:*

---

<sup>87</sup> Bank Indonesia dan Otoritas Jasa Keuangan (OJK) telah mengeluarkan sejumlah peraturan yang mendukung perkembangan payment gateway dan layanan keuangan digital lainnya, seperti e-money dan e-wallet. Regulasi ini menciptakan lingkungan yang kondusif bagi pertumbuhan payment gateway di Indonesia. Pemerintah Indonesia secara aktif mendukung pengembangan dan pertumbuhan industri payment gateway <sup>2</sup> sebagai bagian dari upaya mereka untuk meningkatkan inklusi keuangan dan mempromosikan digitalisasi ekonomi. Beberapa langkah yang telah diambil oleh pemerintah dan <sup>67</sup> regulator keuangan, seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK), mencakup:

### *Regulasi yang jelas:*

---

Pemerintah Indonesia telah mengeluarkan berbagai peraturan yang mengatur industri payment gateway. Misalnya, <sup>19</sup> Peraturan Bank Indonesia No. 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran dan Peraturan Otoritas Jasa Keuangan No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital. Regulasi ini memberikan kerangka hukum yang jelas bagi penyelenggara payment gateway untuk beroperasi dan tumbuh.



### Promosi standar keamanan:

Pemerintah dan regulator keuangan telah mendorong industri untuk mengadopsi standar keamanan internasional, seperti PCI DSS, guna melindungi konsumen dan bisnis dari risiko keamanan siber dan penipuan.

### Pengembangan infrastruktur:

Pemerintah Indonesia telah berinvestasi dalam pengembangan infrastruktur digital, termasuk jaringan internet dan sistem pembayaran nasional, yang akan memungkinkan industri payment gateway untuk berkembang lebih lanjut.

### Inisiatif QRIS:

Bank Indonesia <sup>35</sup> meluncurkan Quick Response Indonesian Standard (QRIS) pada tahun 2019, yang merupakan standar kode QR nasional untuk memudahkan transaksi pembayaran digital lintas platform. Inisiatif ini dirancang untuk mempromosikan inklusi keuangan dan membantu memperluas penggunaan payment gateway di berbagai sektor ekonomi.

### Kolaborasi dengan sektor swasta:

Pemerintah dan regulator keuangan telah bekerja sama dengan industri payment gateway, perbankan, dan fintech untuk mengembangkan solusi pembayaran digital yang aman, efisien, dan inklusif.

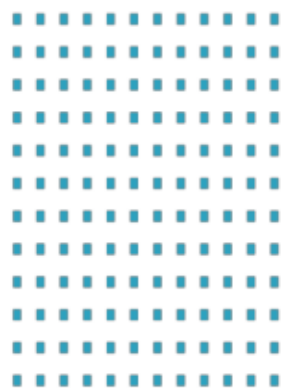
### Pendidikan dan kesadaran:

Pemerintah juga telah meluncurkan berbagai inisiatif untuk meningkatkan kesadaran masyarakat tentang manfaat dan risiko pembayaran digital, serta mengembangkan program pelatihan dan pendidikan untuk meningkatkan literasi keuangan dan digital.

Melalui langkah-langkah ini, pemerintah Indonesia telah menunjukkan komitmen yang kuat untuk mendukung pertumbuhan industri payment gateway dan memastikan bahwa manfaat dari digitalisasi ekonomi dapat dirasakan oleh seluruh masyarakat. Namun, penting untuk terus memantau perkembangan industri dan menyesuaikan regulasi dan kebijakan sesuai dengan kebutuhan dan tantangan yang muncul.

<b>Aspek</b>	<b>Respon Pemerintah Indonesia</b>
<b>Regulasi yang jelas</b>	Mengeluarkan peraturan yang mengatur industri payment gateway, seperti Peraturan BI No. 18/40/PBI/2016 dan Peraturan OJK No. 13/POJK.02/2018.
<b>Promosi standar keamanan</b>	Mendukung adopsi standar keamanan internasional seperti PCI DSS untuk melindungi konsumen dan bisnis dari risiko keamanan siber dan penipuan.
<b>Pengembangan infrastruktur</b>	Berinvestasi dalam pengembangan infrastruktur digital, termasuk jaringan internet dan sistem pembayaran nasional.
<b>Inisiatif QRIS</b>	Meluncurkan standar kode QR nasional (QRIS) untuk memudahkan transaksi pembayaran digital lintas platform dan mempromosikan inklusi keuangan.
<b>Kolaborasi dengan sektor swasta</b>	Bekerja sama dengan industri payment gateway, perbankan, dan fintech untuk mengembangkan solusi pembayaran digital yang aman, efisien, dan inklusif.

Aspek	Respon Pemerintah Indonesia
<b>Pendidikan dan kesadaran</b>	Meluncurkan inisiatif untuk meningkatkan kesadaran masyarakat tentang manfaat dan risiko pembayaran digital serta program pelatihan dan pendidikan untuk meningkatkan literasi keuangan dan digital.



*Pemerintah dan regulator keuangan telah bekerja sama dengan industri payment gateway, perbankan, dan fintech untuk mengembangkan solusi pembayaran digital yang aman, efisien, dan inklusif*

### *Inovasi dan adopsi teknologi:*

Indonesia memiliki pasar teknologi yang tumbuh pesat, dengan banyak perusahaan lokal dan internasional yang berinvestasi dalam teknologi finansial (fintech) dan layanan keuangan digital. Hal ini menciptakan basis pengguna yang siap menerima dan mengadopsi solusi pembayaran baru, seperti payment gateway. Inovasi dan adopsi teknologi adalah faktor kunci dalam perkembangan fintech di Indonesia, termasuk dalam sektor payment gateway. Beberapa faktor yang menunjukkan hubungan antara inovasi teknologi dan perkembangan fintech di Indonesia meliputi:

#### Kemajuan teknologi:

Kemajuan teknologi, seperti cloud computing, big data, AI, dan machine learning, telah memungkinkan fintech untuk mengembangkan produk dan layanan yang lebih canggih dan efisien. Hal ini juga memungkinkan fintech untuk menjangkau segmen pasar yang sebelumnya sulit dijangkau oleh institusi keuangan konvensional.

### Kecepatan adopsi:

Masyarakat Indonesia secara umum cepat mengadopsi teknologi baru, terutama dalam hal pembayaran digital. Hal ini terlihat dari peningkatan jumlah pengguna layanan fintech dan e-wallet dalam beberapa tahun terakhir.

### Kebutuhan inklusi keuangan:

Inovasi dalam sektor fintech membantu meningkatkan inklusi keuangan di Indonesia, terutama di daerah-daerah yang tidak terjangkau oleh layanan perbankan konvensional. Fintech, termasuk payment gateway, memudahkan akses masyarakat terhadap produk dan layanan keuangan.

### Regulasi yang mendukung:

Pemerintah Indonesia telah mengeluarkan regulasi yang mendukung perkembangan fintech, termasuk payment gateway, seperti Peraturan BI No. 18/40/PBI/2016 dan Peraturan OJK No. 13/POJK.02/2018. Regulasi ini mendorong inovasi dan adopsi teknologi serta meningkatkan kepercayaan konsumen terhadap layanan fintech.

### Kolaborasi dengan industri:

Fintech di Indonesia telah bekerja sama dengan berbagai sektor, seperti perbankan, e-commerce, dan telekomunikasi, untuk mengembangkan solusi pembayaran yang inovatif. Hal ini menciptakan ekosistem yang saling mendukung dan mempercepat adopsi teknologi.

### Investasi dan dukungan:

Terdapat peningkatan investasi dalam sektor fintech Indonesia, baik dari investor lokal maupun internasional. Hal ini menciptakan lingkungan yang kondusif bagi inovasi dan perkembangan fintech, termasuk payment gateway.

Kesimpulannya, inovasi dan adopsi teknologi memainkan peran penting dalam perkembangan fintech di Indonesia, termasuk dalam sektor payment gateway. Dukungan regulasi, investasi, dan kolaborasi industri juga berkontribusi pada pertumbuhan sektor ini, yang pada akhirnya membantu meningkatkan inklusi keuangan dan memudahkan akses masyarakat terhadap produk dan layanan keuangan.

## ***Infrastruktur dan konektivitas:***

---

Pemerintah Indonesia terus berupaya meningkatkan infrastruktur dan konektivitas internet di seluruh negeri. Hal ini akan memungkinkan lebih banyak orang untuk mengakses layanan pembayaran digital dan, pada akhirnya, akan meningkatkan penetrasi payment gateway. Indonesia telah menunjukkan peningkatan signifikan dalam kesiapan infrastruktur dan konektivitas untuk mendukung pengembangan payment gateway di masa depan. Berikut ini beberapa aspek yang menunjukkan kesiapan Indonesia:

### **Penyediaan jaringan internet:**

Pemerintah dan penyedia layanan telekomunikasi terus meningkatkan kualitas dan cakupan jaringan internet di seluruh negeri. Proyek Palapa Ring, yang bertujuan untuk menyediakan konektivitas serat optik ke seluruh kabupaten di Indonesia, adalah salah satu contoh upaya ini.

### **Ketersediaan perangkat:**

---

Akses masyarakat terhadap perangkat seperti ponsel pintar dan komputer telah meningkat pesat dalam beberapa tahun terakhir. Hal ini memungkinkan lebih banyak orang untuk memanfaatkan layanan fintech, termasuk payment gateway.



### Literasi digital:

Peningkatan literasi digital, terutama di kalangan generasi muda, memungkinkan penggunaan teknologi dan layanan berbasis internet, seperti payment gateway, lebih mudah dan cepat diterima oleh masyarakat.

### Pembangunan data center:

Pemerintah dan sektor swasta telah berinvestasi dalam pembangunan data center dan infrastruktur teknologi informasi untuk mendukung pertumbuhan industri digital, termasuk fintech dan payment gateway.

### Keamanan siber:

Pemerintah dan sektor swasta bekerja sama untuk meningkatkan keamanan siber dan melindungi data pengguna, termasuk dalam konteks payment gateway. Hal ini mencakup penerapan standar keamanan seperti PCI DSS dan penggunaan teknologi enkripsi seperti SSL dan TLS.

### Regulasi dan dukungan pemerintah:

Pemerintah Indonesia telah mengeluarkan regulasi yang mendukung perkembangan payment gateway dan fintech secara umum, menciptakan lingkungan yang kondusif bagi inovasi dan pertumbuhan sektor ini.

Meskipun ada kemajuan yang signifikan, masih ada tantangan yang perlu diatasi, seperti pemerataan infrastruktur dan konektivitas di daerah-daerah terpencil serta upaya peningkatan literasi digital dan keamanan siber. Namun, dengan komitmen pemerintah, sektor swasta, dan masyarakat dalam menghadapi tantangan ini, prospek pengembangan payment gateway di Indonesia sangat positif untuk masa depan.

Mengingat faktor-faktor ini, masa depan payment gateway di Indonesia terlihat cerah. Namun, masih ada beberapa tantangan yang perlu diatasi, seperti meningkatkan kesadaran masyarakat tentang layanan ini, memastikan keamanan dan privasi data pengguna, serta mengatasi potensi risiko penipuan dan kejahatan siber.

Namun, dengan dukungan pemerintah, peraturan yang mendukung, dan semakin banyaknya perusahaan yang berinvestasi dalam teknologi pembayaran digital, payment gateway di Indonesia kemungkinan akan terus tumbuh dan berkembang dalam beberapa tahun mendatang.

# luang Riset

Judul	Metode dan Output
"Pengaruh Kecepatan Transaksi Payment Gateway terhadap Kepuasan Pelanggan"	<b>Metode:</b> Kuantitatif <b>Output:</b> Hubungan antara kecepatan transaksi payment gateway dan tingkat kepuasan pelanggan.
"Analisis Keamanan dan Perlindungan Data pada Payment Gateway"	<b>Metode:</b> Kualitatif <b>Output:</b> Identifikasi kelemahan keamanan dan rekomendasi peningkatan keamanan payment gateway.
"Penggunaan Blockchain dalam Payment Gateway: Studi Kasus dan Implementasi"	<b>Metode:</b> Pengembangan <b>Output:</b> Prototipe payment gateway yang menggunakan teknologi blockchain dan analisis efektivitasnya.

Judul	Metode dan Output
"Faktor-faktor yang Mempengaruhi Adopsi Payment Gateway oleh UMKM"	<b>Metode:</b> Kuantitatif <b>Output:</b> Faktor-faktor yang berkontribusi pada keberhasilan adopsi payment gateway oleh UMKM.
"Studi Komparatif Payment Gateway Lokal dan Internasional: Keunggulan dan Kelemahan"	<b>Metode:</b> Kualitatif <b>Output:</b> Analisis perbandingan payment gateway lokal dan internasional serta rekomendasi bagi penyedia layanan.
"Optimalisasi Biaya dan Keuntungan dengan Payment Gateway: Strategi bagi Bisnis Online"	<b>Metode:</b> Kuantitatif <b>Output:</b> Strategi optimalisasi biaya dan peningkatan keuntungan dengan menggunakan payment gateway.
"Penerapan Kecerdasan Buatan dalam Deteksi Fraud pada Payment Gateway"	<b>Metode:</b> Pengembangan <b>Output:</b> Sistem deteksi fraud dengan kecerdasan buatan dan evaluasi efektivitasnya dalam mencegah fraud.

Judul	Metode dan Output
"Peran Payment Gateway dalam Inklusi Keuangan di Indonesia"	<b>Metode:</b> Kualitatif <b>Output:</b> Analisis dampak payment gateway dalam meningkatkan inklusi keuangan di Indonesia.
"Pengaruh User Experience pada Tingkat Adopsi Payment Gateway"	<b>Metode:</b> Kuantitatif <b>Output:</b> Hubungan antara user experience dan tingkat adopsi payment gateway.
"Pengembangan Payment Gateway Berbasis Mobile Wallet untuk Transaksi Mikro"	<b>Metode:</b> Pengembangan <b>Output:</b> Prototipe payment gateway berbasis mobile wallet untuk transaksi mikro dan evaluasi efektivitasnya.
"Evaluasi Kinerja Payment Gateway menggunakan Analytical Hierarchy Process (AHP)"	<b>Metode:</b> Kuantitatif <b>Output:</b> Evaluasi kinerja payment gateway dan peringkat berdasarkan kriteria yang ditetapkan.
"Pengaruh Perubahan Regulasi terhadap Pertumbuhan Payment Gateway di Indonesia"	<b>Metode:</b> Kualitatif <b>Output:</b> Analisis dampak perubahan regulasi terhadap pertumbuhan payment gateway di Indonesia.

Judul	Metode dan Output
"Analisis Faktor Risiko dalam Operasional Payment Gateway dan Mitigasi Risikonya"	<p><b>Metode:</b> Kualitatif</p> <p><b>Output:</b> Identifikasi faktor risiko dalam operasional payment gateway dan strategi mitigasi risikonya.</p>
"Studi Penerimaan dan Penggunaan Payment Gateway di Kalangan Generasi Z"	<p><b>Metode:</b> Kuantitatif</p> <p><b>Output:</b> Tingkat penerimaan dan pola penggunaan payment gateway di kalangan generasi Z.</p>
"Pengaruh Integrasi Payment Gateway pada Retensi Pelanggan dalam Bisnis E-commerce"	<p><b>Metode:</b> Kuantitatif</p> <p><b>Output:</b> Hubungan antara integrasi payment gateway dan retensi pelanggan dalam bisnis e-commerce.</p>
"Optimalisasi API Payment Gateway untuk Performa E-commerce yang Lebih Baik"	<p><b>Metode:</b> Pengembangan</p> <p><b>Output:</b> Solusi optimal dalam integrasi API payment gateway untuk meningkatkan performa e-commerce.</p>

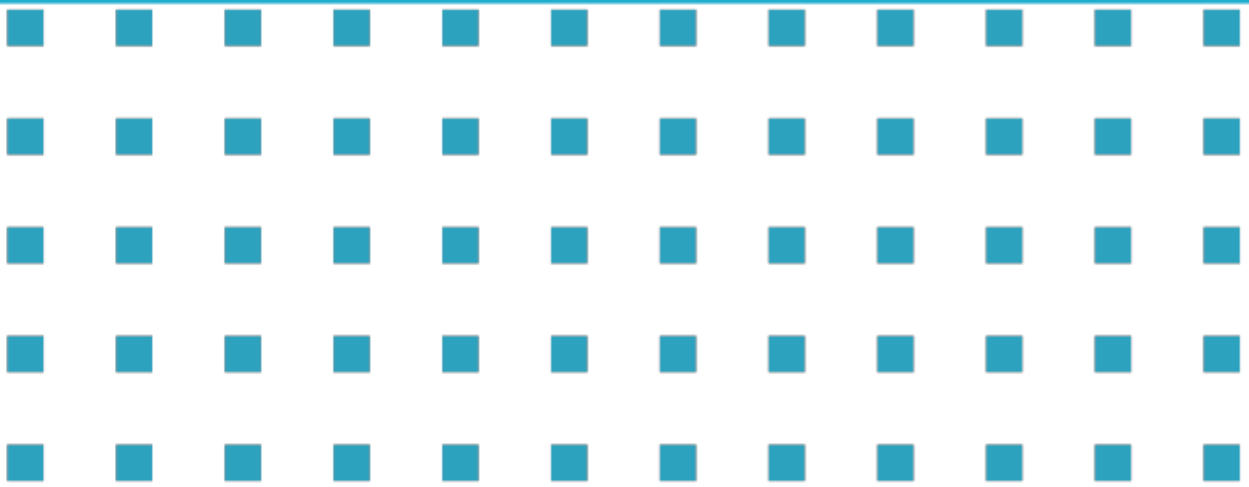
Judul	Metode dan Output
"Keamanan Data pada Payment Gateway: Studi Kasus Serangan Siber Terhadap Platform E-commerce"	<b>Metode:</b> Kualitatif <b>Output:</b> Analisis serangan siber pada platform e-commerce dan dampaknya pada keamanan data payment gateway.
"Pengaruh Latensi Koneksi API terhadap Kepuasan Pengguna Payment Gateway"	<b>Metode:</b> Kuantitatif <b>Output:</b> Hubungan antara latensi koneksi API dan kepuasan pengguna payment gateway.
"Analisis Kerentanan Payment Gateway pada E-commerce dan Strategi Mitigasi"	<b>Metode:</b> Kualitatif <b>Output:</b> Identifikasi kerentanan payment gateway pada e-commerce dan rekomendasi strategi mitigasi.
"Penerapan Teknologi Blockchain untuk Meningkatkan Keamanan Payment Gateway dalam E-commerce"	<b>Metode:</b> Pengembangan <b>Output:</b> Solusi teknologi blockchain yang terintegrasi dengan payment gateway untuk meningkatkan keamanan transaksi.

Judul	Metode dan Output
"Evaluasi Penggunaan RESTful API versus GraphQL API dalam Integrasi Payment Gateway pada E-commerce"	<p><b>Metode:</b> Kuantitatif</p> <p><b>Output:</b> Perbandingan antara penggunaan RESTful API dan GraphQL API dalam integrasi payment gateway.</p>
"Pengembangan Sistem Payment Gateway dengan Fitur Deteksi Fraud Berbasis Machine Learning"	<p><b>Metode:</b> Pengembangan</p> <p><b>Output:</b> Sistem payment gateway dengan fitur deteksi fraud menggunakan teknologi machine learning.</p>
"Analisis Faktor Keberhasilan Adopsi API Payment Gateway oleh Pengembang Aplikasi E-commerce"	<p><b>Metode:</b> Kuantitatif</p> <p><b>Output:</b> Faktor-faktor yang mempengaruhi keberhasilan adopsi API payment gateway oleh pengembang aplikasi e-commerce.</p>
"Studi Perbandingan Keamanan Data pada Berbagai Platform Payment Gateway"	<p><b>Metode:</b> Kualitatif</p> <p><b>Output:</b> Analisis perbandingan keamanan data pada berbagai platform payment gateway.</p>



8

**Penutup**



Buku ini telah membahas berbagai aspek terkait payment gateway, mulai dari konsep dasar, regulasi, hingga integrasi pada platform bisnis dan manajemen operasional. Pembahasan tentang e-money dan e-wallet juga menjadi bagian penting dalam menggambarkan hubungan antara payment gateway dengan metode pembayaran yang semakin populer. Diharapkan, pembaca dapat memperoleh pemahaman yang komprehensif mengenai payment gateway dan bagaimana peranannya dalam dunia bisnis dan teknologi saat ini.

Setelah memahami konsep dan prinsip-prinsip payment gateway, ada beberapa bidang keilmuan lain yang perlu dipelajari untuk memperdalam pengetahuan dan kemampuan di bidang ini:

#### Dari sudut pandang Manajemen:

1. **Manajemen Keuangan:** Untuk memahami lebih lanjut mengenai pengelolaan dana, investasi, dan manajemen risiko dalam bisnis yang terkait dengan payment gateway.
2. **Manajemen Pemasaran:** Untuk memahami strategi pemasaran dan promosi layanan payment gateway serta analisis perilaku konsumen.
3. **Manajemen Sumber Daya Manusia:** Untuk mengelola tim yang terlibat dalam pengoperasian dan pengembangan payment gateway secara efektif.

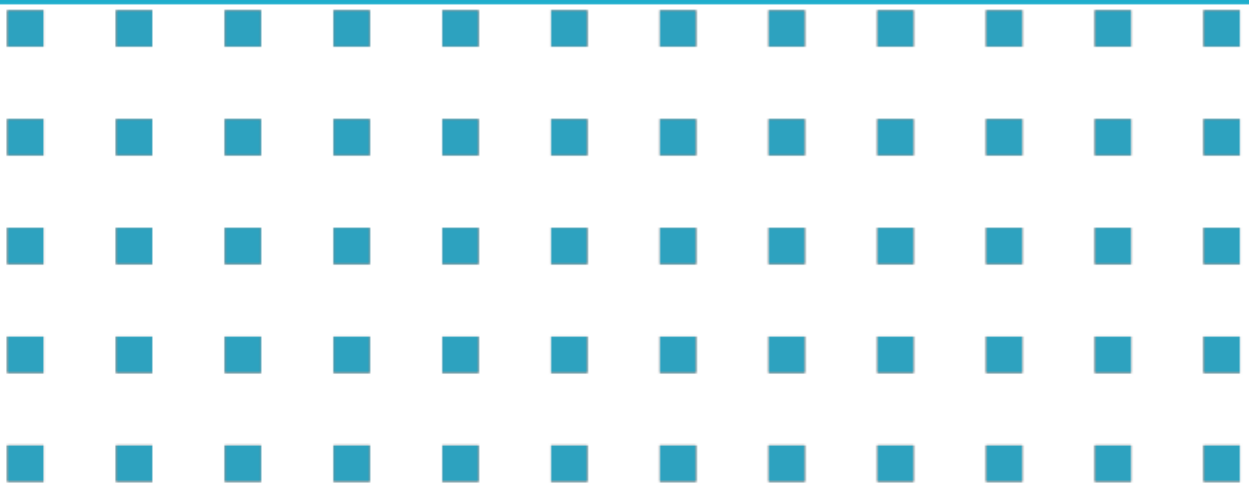
### Dari sudut pandang Sistem Informasi dan Teknikal:

---

1. **Keamanan Siber:** Untuk memahami teknik dan strategi dalam melindungi sistem payment gateway dari serangan siber dan menjaga keamanan data pelanggan.
2. **Pengembangan Aplikasi:** Untuk mempelajari teknik dan best practices dalam mengembangkan sistem payment gateway yang handal, aman, dan mudah diintegrasikan.
3. **Teknologi Blockchain:** Untuk memahami konsep dan aplikasi teknologi blockchain dalam meningkatkan keamanan dan efisiensi sistem payment gateway.
4. **Machine Learning dan AI:** Untuk mempelajari teknik dan metode dalam menggabungkan teknologi machine learning dan AI dalam sistem payment gateway, seperti deteksi fraud dan analisis pola transaksi.

Dengan mempelajari bidang-bidang keilmuan tersebut, pembaca diharapkan dapat mengembangkan pemahaman yang lebih luas dan terintegrasi tentang payment gateway, serta mampu menghadapi tantangan dan peluang di masa depan. Pemahaman yang komprehensif tentang payment gateway akan membantu pembaca dalam membuat keputusan yang tepat dan strategis dalam menghadapi perkembangan industri keuangan digital yang semakin pesat.

# Referensi



- 63  
Chaffey, D., & Ellis-Chadwick, F. (2019). *Digital marketing* (7th ed.). Pearson.
- 1  
Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, 14(5), 265-284. DOI: 10.1016/j.elerap.2015.07.006
- de Reuver, M., & Haaker, T. (2018). Digital platform ecosystems. *Electronic Markets*, 28(3), 243-249.
- 24  
Huang, Z., Benyoucef, M., & Liu, S. (2018). From e-commerce to social commerce: A close look at design features. *Electronic Commerce Research and Applications*, 27, 246-259.
- 42  
Kshetri, N. (2017). Can blockchain strengthen the internet of things?. *IT Professional*, 19(4), 68-72.
- 1  
Laukkanen, T. (2016). Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the Internet and mobile banking. *Journal of Business Research*, 69(7), 2432-2439. DOI: 10.1016/j.jbusres.2016.01.013
- Liu, Y., Li, H., & Hu, F. (2013). Website attributes in urging online impulse purchase: An empirical investigation on consumer perceptions. *Decision Support Systems*, 55(3), 829-837. DOI: 10.1016/j.dss.2013.04.001
- Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things: A systematic review of the business literature from the user and organisational perspectives. *Technological Forecasting and Social Change*, 136, 285-297. DOI: 10.1016/j.techfore.2018.01.022
- 39  
Mihart, C. (2012). Impact of Integrated Marketing Communication on Consumer Behaviour: Effects on Consumer Decision-Making Process. *International Journal of Marketing Studies*, 4(2). DOI: 10.5539/ijms.v4n2p121
- Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, 61, 404-414. DOI: 10.1016/j.chb.2016.03.030
- Rysman, Mark & Schuh, S. (2017). New innovations in payments. *Innovation Policy and the Economy*, 17(1), 27-48.
- 34  
Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM*, 46(4), 91-94.
- 18  
Sumanjeet, S. (2009). Emergence of Payment Systems in the Age of Electronic Commerce: The State of Art. *Global Journal of International Business Research*, 2(2), 17-36.

9

Tarhini, A., El-Masri, M., Ali, M., & Serrano, A. (2016). Extending the UTAUT model to understand the customers' acceptance and use of internet banking in Lebanon: A structural equation modeling approach. *Information Technology & People*, 29(4), 830-849.

Thakur, R., & Srivastava, M. (2014). Adoption readiness, personal innovativeness, perceived risk and usage intention across customer groups for mobile payment services in India. *Internet Research*, 24(3), 369-392. DOI: 10.1108/IntR-12-2012-0244

Turban, E., Outland, J., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. (2017). *Electronic commerce 2018: a managerial and social networks perspective*. Springer.

14

Wang, Y., Wang, Y., Lin, H., & Tang, T. (2003). Determinants of user acceptance of Internet banking: an empirical study. *International Journal of Service Industry Management*, 14(5), 501-519. DOI: 10.1108/09564230310500192



6

---

***Kekayaan adalah saat kita merasa cukup dengan apa yang kita miliki***

***Kemiskinan adalah saat kita merasa kurang dengan apa yang kita miliki***

---

# Glosarium



<b>Payment Gateway</b>	Sistem yang memfasilitasi transfer informasi antara situs web atau platform e-commerce dengan lembaga keuangan, seperti bank atau prosesor pembayaran. <sup>38</sup>
<b>Sistem Informasi</b>	Kumpulan komponen yang saling terkait untuk mengumpulkan, menyimpan, memproses, dan menyebarkan informasi untuk mendukung pengambilan keputusan, koordinasi, dan kontrol dalam suatu organisasi. <sup>116</sup>
<b>E-commerce</b>	Praktik membeli dan menjual barang atau jasa melalui internet.
<b>Point of Sale (POS)</b>	Tempat di mana transaksi pelanggan diselesaikan, seperti kasir di toko ritel.
<b>SSL (Secure Socket Layer)</b>	Protokol keamanan yang digunakan untuk mengenkripsi koneksi antara server dan klien dalam komunikasi web.



48

**TLS (Transport Layer Security)**

Protokol keamanan yang menggantikan SSL, dengan peningkatan keamanan dan fitur tambahan.

**OTP (One-Time Password)**

Sandi sekali pakai yang digunakan untuk mengautentikasi transaksi dalam sistem pembayaran.

**Biometrik**

Penggunaan karakteristik unik dari tubuh manusia, seperti sidik jari atau pengenalan wajah, untuk mengautentikasi identitas pengguna.

61

**PCI DSS (Payment Card Industry Data Security Standard)**

Standar keamanan yang ditetapkan oleh industri kartu pembayaran untuk melindungi data konsumen dan transaksi kartu.

**API (Application Programming Interface)**

Antarmuka yang memungkinkan komunikasi antara aplikasi atau sistem yang berbeda.

<b>E-money</b>	Uang elektronik yang disimpan dalam suatu perangkat atau sistem dan digunakan untuk melakukan transaksi pembayaran.
<b>E-wallet</b>	Aplikasi atau sistem yang memungkinkan pengguna untuk menyimpan dan mengelola uang elektronik dan kartu pembayaran secara digital.
<b>QR Code (Quick Response Code)</b>	Kode batang dua dimensi yang dapat dengan cepat dibaca oleh perangkat seperti ponsel pintar untuk mengakses informasi atau melakukan transaksi.
<b>QRIS (Quick Response Code Indonesian Standard)</b>	Sistem pembayaran menggunakan QR code yang dikembangkan oleh Bank Indonesia untuk memfasilitasi transaksi digital antar lembaga keuangan dan penyedia jasa pembayaran.

<b>Blockchain</b>	Teknologi yang menggunakan struktur data terdistribusi untuk mencatat transaksi dalam blok yang terhubung dan aman.
<b>Crypto</b>	Singkatan dari cryptocurrency, bentuk mata uang digital yang menggunakan teknologi kriptografi untuk mengamankan transaksi dan mengendalikan penciptaan unit baru.
<b>Regulasi Anti Pencucian Uang (APU) dan Pencegahan Pendanaan Terorisme (PPT)</b>	Aturan dan kebijakan yang dibuat oleh pemerintah dan lembaga pengawas untuk mencegah dan mendeteksi aktivitas pencucian uang dan pendanaan terorisme melalui sistem keuangan.

# Buku payment gateway

---

## ORIGINALITY REPORT

---

11%

SIMILARITY INDEX

11%

INTERNET SOURCES

4%

PUBLICATIONS

4%

STUDENT PAPERS

---

## PRIMARY SOURCES

---

1	<a href="http://www.igi-global.com">www.igi-global.com</a> Internet Source	<1%
2	<a href="http://islamicmarkets.com">islamicmarkets.com</a> Internet Source	<1%
3	<a href="http://koinworks.com">koinworks.com</a> Internet Source	<1%
4	<a href="http://eprints.undip.ac.id">eprints.undip.ac.id</a> Internet Source	<1%
5	<a href="http://ebin.pub">ebin.pub</a> Internet Source	<1%
6	<a href="http://sinaubareng.web.id">sinaubareng.web.id</a> Internet Source	<1%
7	<a href="http://eprints.machung.ac.id">eprints.machung.ac.id</a> Internet Source	<1%
8	<a href="http://library.binus.ac.id">library.binus.ac.id</a> Internet Source	<1%
9	<a href="http://www.businessperspectives.org">www.businessperspectives.org</a> Internet Source	<1%
10	<a href="http://torisetsu.cc">torisetsu.cc</a> Internet Source	<1%
11	<a href="http://repository.ub.ac.id">repository.ub.ac.id</a> Internet Source	<1%
12	<a href="http://ejournal.unsrat.ac.id">ejournal.unsrat.ac.id</a> Internet Source	<1%
13	<a href="http://issuu.com">issuu.com</a> Internet Source	<1%

---

14	<a href="http://realkm.com">realkm.com</a> Internet Source	<1 %
15	<a href="http://digilib.uin-suka.ac.id">digilib.uin-suka.ac.id</a> Internet Source	<1 %
16	<a href="http://www.ciputradevelopment.com">www.ciputradevelopment.com</a> Internet Source	<1 %
17	<a href="http://es.scribd.com">es.scribd.com</a> Internet Source	<1 %
18	<a href="http://link.springer.com">link.springer.com</a> Internet Source	<1 %
19	<a href="http://katadata.co.id">katadata.co.id</a> Internet Source	<1 %
20	<a href="http://www.baf.id">www.baf.id</a> Internet Source	<1 %
21	<a href="http://www.scribd.com">www.scribd.com</a> Internet Source	<1 %
22	<a href="http://hingga.maksi.ugm.ac.id">hingga.maksi.ugm.ac.id</a> Internet Source	<1 %
23	<a href="http://journals.ama.org">journals.ama.org</a> Internet Source	<1 %
24	<a href="http://ri.ufs.br">ri.ufs.br</a> Internet Source	<1 %
25	Submitted to Argosy University Student Paper	<1 %
26	Submitted to Universitas Islam Indonesia Student Paper	<1 %
27	<a href="http://accurate.id">accurate.id</a> Internet Source	<1 %
28	<a href="http://gizmologi.id">gizmologi.id</a> Internet Source	<1 %

---

[opennetworking.org](http://opennetworking.org)

29	Internet Source	<1 %
30	repositori.usu.ac.id Internet Source	<1 %
31	Submitted to Universitas Jember Student Paper	<1 %
32	banjarmasin.tribunnews.com Internet Source	<1 %
33	databoks-series.katadata.co.id Internet Source	<1 %
34	repository.up.ac.za Internet Source	<1 %
35	www.antaranews.com Internet Source	<1 %
36	www.bca.co.id Internet Source	<1 %
37	www.slideshare.net Internet Source	<1 %
38	repositori.uin-alauddin.ac.id Internet Source	<1 %
39	Submitted to Billy Blue Group Student Paper	<1 %
40	www.coursehero.com Internet Source	<1 %
41	www.hukumonline.com Internet Source	<1 %
42	ah.nccu.edu.tw Internet Source	<1 %
43	cdn.inst-fs-dub-prod.inscloudgate.net Internet Source	<1 %
44	dspace.uii.ac.id	

Internet Source

<1 %

45

[ejournal.uin-malang.ac.id](http://ejournal.uin-malang.ac.id)

Internet Source

<1 %

46

[gadgetdiva.id](http://gadgetdiva.id)

Internet Source

<1 %

47

[www.ejournal-s1.undip.ac.id](http://www.ejournal-s1.undip.ac.id)

Internet Source

<1 %

48

[www.researchgate.net](http://www.researchgate.net)

Internet Source

<1 %

49

[www.swarovskioutletonline.us.com](http://www.swarovskioutletonline.us.com)

Internet Source

<1 %

50

[jom.fti.budiluhur.ac.id](http://jom.fti.budiluhur.ac.id)

Internet Source

<1 %

51

[repository.unpar.ac.id](http://repository.unpar.ac.id)

Internet Source

<1 %

52

[translate.evernote.com](http://translate.evernote.com)

Internet Source

<1 %

53

[www.nhis.co.id](http://www.nhis.co.id)

Internet Source

<1 %

54

[ekd.montebellunabasket.it](http://ekd.montebellunabasket.it)

Internet Source

<1 %

55

[infobanknews.com](http://infobanknews.com)

Internet Source

<1 %

56

[bagaimanacaradanmengapa.blogspot.com](http://bagaimanacaradanmengapa.blogspot.com)

Internet Source

<1 %

57

[cnainforma.it](http://cnainforma.it)

Internet Source

<1 %

58

[dokument.pub](http://dokument.pub)

Internet Source

<1 %

59	Submitted to Fakultas Ekonomi dan Bisnis Universitas Gadjah Mada Student Paper	<1 %
60	Submitted to Universitas Sang Bumi Ruwa Jurai Student Paper	<1 %
61	<a href="http://www.safaricom.co.ke">www.safaricom.co.ke</a> Internet Source	<1 %
62	<a href="http://digilib.uinsby.ac.id">digilib.uinsby.ac.id</a> Internet Source	<1 %
63	<a href="http://digitalmarketing890149470.wordpress.com">digitalmarketing890149470.wordpress.com</a> Internet Source	<1 %
64	<a href="http://keamanan-informasi.stei.itb.ac.id">keamanan-informasi.stei.itb.ac.id</a> Internet Source	<1 %
65	<a href="http://maglearning.id">maglearning.id</a> Internet Source	<1 %
66	<a href="http://repository.unigal.ac.id">repository.unigal.ac.id</a> Internet Source	<1 %
67	<a href="http://www.biskom.web.id">www.biskom.web.id</a> Internet Source	<1 %
68	<a href="http://www.polooutletfactory.us.com">www.polooutletfactory.us.com</a> Internet Source	<1 %
69	<a href="http://ariezsina.blogspot.com">ariezsina.blogspot.com</a> Internet Source	<1 %
70	<a href="http://download.garuda.ristekdikti.go.id">download.garuda.ristekdikti.go.id</a> Internet Source	<1 %
71	<a href="http://ejournal.unib.ac.id">ejournal.unib.ac.id</a> Internet Source	<1 %
72	<a href="http://infoalternativa.org">infoalternativa.org</a> Internet Source	<1 %
73	<a href="http://repository.ubaya.ac.id">repository.ubaya.ac.id</a> Internet Source	<1 %



74	<a href="http://www.beritasatu.com">www.beritasatu.com</a> Internet Source	<1 %
75	<a href="http://www.jtrustbank.co.id">www.jtrustbank.co.id</a> Internet Source	<1 %
76	Rahayu Utami, Fadillah Fadillah, Eny Enawaty. "HASIL BELAJAR SISWA PADA MATERI KALOR MENGUNAKAN BAHAN AJAR BERBASIS E- LEARNING EDMODO", VOX EDUKASI: Jurnal Ilmiah Ilmu Pendidikan, 2021 Publication	<1 %
77	<a href="http://eprints.walisongo.ac.id">eprints.walisongo.ac.id</a> Internet Source	<1 %
78	<a href="http://fst.uinjkt.ac.id">fst.uinjkt.ac.id</a> Internet Source	<1 %
79	<a href="http://galihsoetawidjaya.wordpress.com">galihsoetawidjaya.wordpress.com</a> Internet Source	<1 %
80	<a href="http://hafri-kiko.blogspot.com">hafri-kiko.blogspot.com</a> Internet Source	<1 %
81	<a href="http://hidayahmnoor.wordpress.com">hidayahmnoor.wordpress.com</a> Internet Source	<1 %
82	<a href="http://jurnal.ugm.ac.id">jurnal.ugm.ac.id</a> Internet Source	<1 %
83	<a href="http://kabarinews.com">kabarinews.com</a> Internet Source	<1 %
84	<a href="http://kedaicrypto.wordpress.com">kedaicrypto.wordpress.com</a> Internet Source	<1 %
85	<a href="http://ms.livingeconomyadvisors.com">ms.livingeconomyadvisors.com</a> Internet Source	<1 %
86	<a href="http://repository.ar-raniry.ac.id">repository.ar-raniry.ac.id</a> Internet Source	<1 %
87	<a href="http://ubl.ac.id">ubl.ac.id</a> Internet Source	<1 %

88	<a href="http://www.abacus-ind.co.id">www.abacus-ind.co.id</a> Internet Source	<1 %
89	<a href="http://www.buanafinance.co.id">www.buanafinance.co.id</a> Internet Source	<1 %
90	<a href="http://www.coinbase.com">www.coinbase.com</a> Internet Source	<1 %
91	<a href="http://www.msn.com">www.msn.com</a> Internet Source	<1 %
92	<a href="http://www.orbitcoin.com">www.orbitcoin.com</a> Internet Source	<1 %
93	<a href="http://www.seotama.com">www.seotama.com</a> Internet Source	<1 %
94	<a href="http://www.westminsterbookstore.com">www.westminsterbookstore.com</a> Internet Source	<1 %
95	<a href="http://123dok.com">123dok.com</a> Internet Source	<1 %
96	Dinil Abrar Sulthani. "Konsep Pendidikan Agama pada Zaman Milenial", Indonesian Journal of Islamic Education Studies (IJIES), 2021 Publication	<1 %
97	Submitted to Indiana University Student Paper	<1 %
98	Lidya Namira. "Faktor-Faktor Yang Mempengaruhi Niat UMKM di Kota Padang Menggunakan e-Payment sebagai Metode Pembayaran", Owner, 2022 Publication	<1 %
99	Submitted to Universitas Sebelas Maret Student Paper	<1 %
100	<a href="http://akumulakandisini.blogspot.com">akumulakandisini.blogspot.com</a> Internet Source	<1 %

101	<a href="http://arifrohmadirblog.blogspot.com">arifrohmadirblog.blogspot.com</a> Internet Source	<1 %
102	<a href="http://bappebti.go.id">bappebti.go.id</a> Internet Source	<1 %
103	<a href="http://blogsabda.com">blogsabda.com</a> Internet Source	<1 %
104	<a href="http://compojoom.com">compojoom.com</a> Internet Source	<1 %
105	<a href="http://ghinaghufrona.blogspot.com">ghinaghufrona.blogspot.com</a> Internet Source	<1 %
106	<a href="http://id.123dok.com">id.123dok.com</a> Internet Source	<1 %
107	<a href="http://id.millionmakers.com">id.millionmakers.com</a> Internet Source	<1 %
108	<a href="http://indonesian.carenginefilter.com">indonesian.carenginefilter.com</a> Internet Source	<1 %
109	<a href="http://kaptengoogle.blogspot.com">kaptengoogle.blogspot.com</a> Internet Source	<1 %
110	<a href="http://mainsaham.id">mainsaham.id</a> Internet Source	<1 %
111	<a href="http://mtarget.co">mtarget.co</a> Internet Source	<1 %
112	<a href="http://myum.um.edu.my">myum.um.edu.my</a> Internet Source	<1 %
113	<a href="http://penerbit.lipi.go.id">penerbit.lipi.go.id</a> Internet Source	<1 %
114	<a href="http://repository.uin-suska.ac.id">repository.uin-suska.ac.id</a> Internet Source	<1 %
115	<a href="http://repository.uma.ac.id">repository.uma.ac.id</a> Internet Source	<1 %

[repository.umsu.ac.id](http://repository.umsu.ac.id)

116	Internet Source	<1 %
117	repository.unej.ac.id Internet Source	<1 %
118	repository.upi.edu Internet Source	<1 %
119	seminar.ilkom.unsri.ac.id Internet Source	<1 %
120	swa.co.id Internet Source	<1 %
121	today.line.me Internet Source	<1 %
122	ukmindonesia.id Internet Source	<1 %
123	www.erufucare.com Internet Source	<1 %
124	www.localgov.co.uk Internet Source	<1 %
125	www.suara.com Internet Source	<1 %
126	www.voyejstore.com Internet Source	<1 %
127	ypiq.eleamoroni.it Internet Source	<1 %
128	doku.pub Internet Source	<1 %
129	intd.animalbeauty.it Internet Source	<1 %
130	www.cermati.com Internet Source	<1 %

---

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off