BADAN SIBER DAN SANDI NEGARA

KEAMANAN INTEGRASI, INTEROPABILITAS, ENDPOINT API



Disampaikan oleh:

Aris Munandar, SST.MP | CISA, CCSP, LA-27001 | Manggala Informatika

Direktorat Keamanan Siber dan Sandi Pemerintah Pusat

Pada:

SOSIALISASI KEAMANAN DAN PEMANFAATAN DATA MELALUI SPLP

Jakarta, 10 Juni 2026

OUTLINE

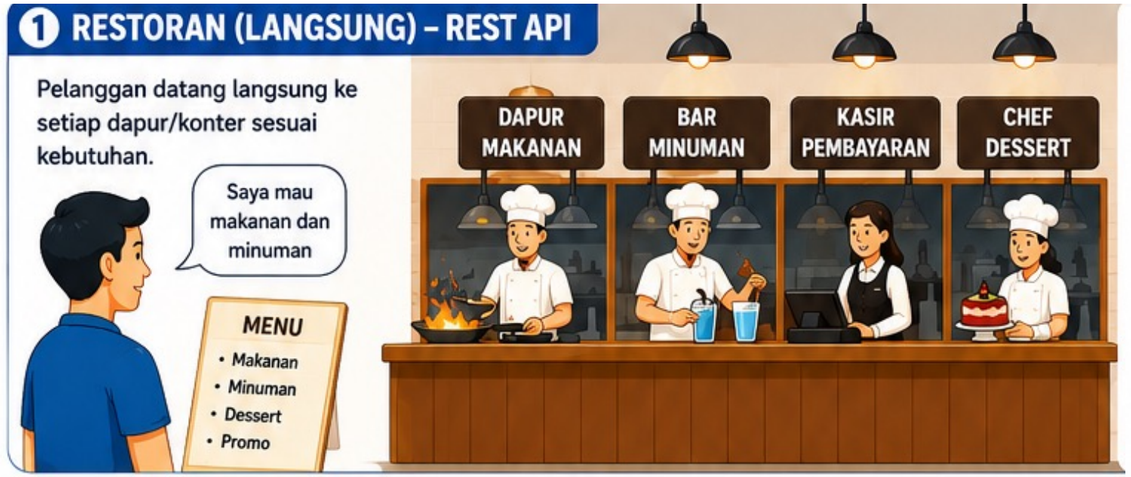
CONTENTS

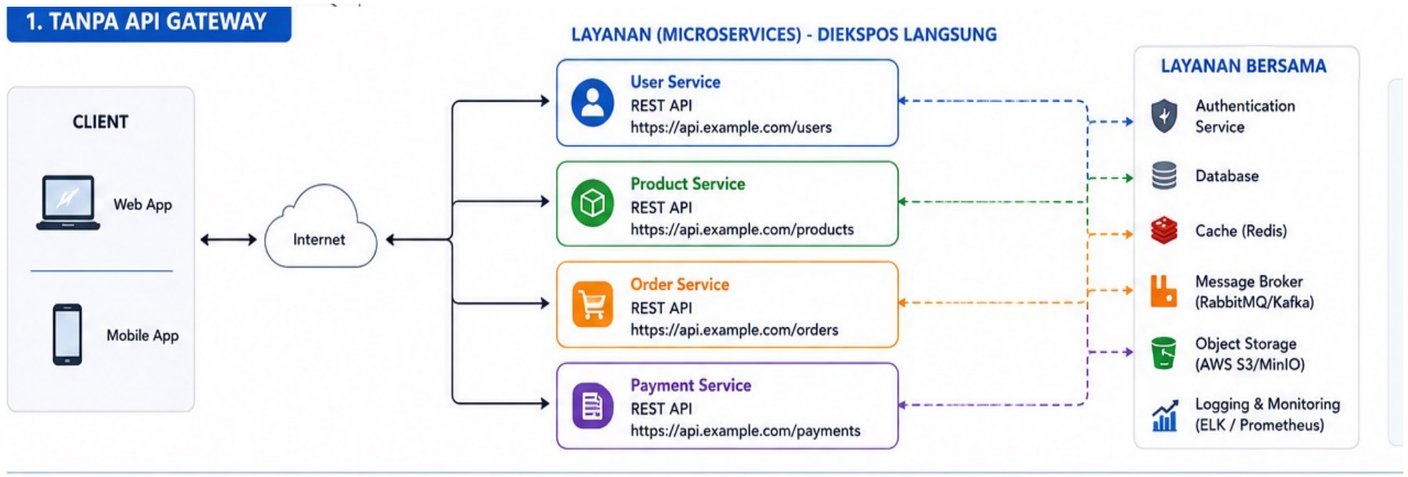
- **Pengantar API Security**
  Introduction to API Security
- **Kebijakan dan Standar Keamanan API**
  API Security Policies and Standards
- **Risiko dan Ancaman Keamanan API**
  API Security Risks and Threats
- **Best Practice dan Mitigasi**
  Best Practices and Mitigation Strategies

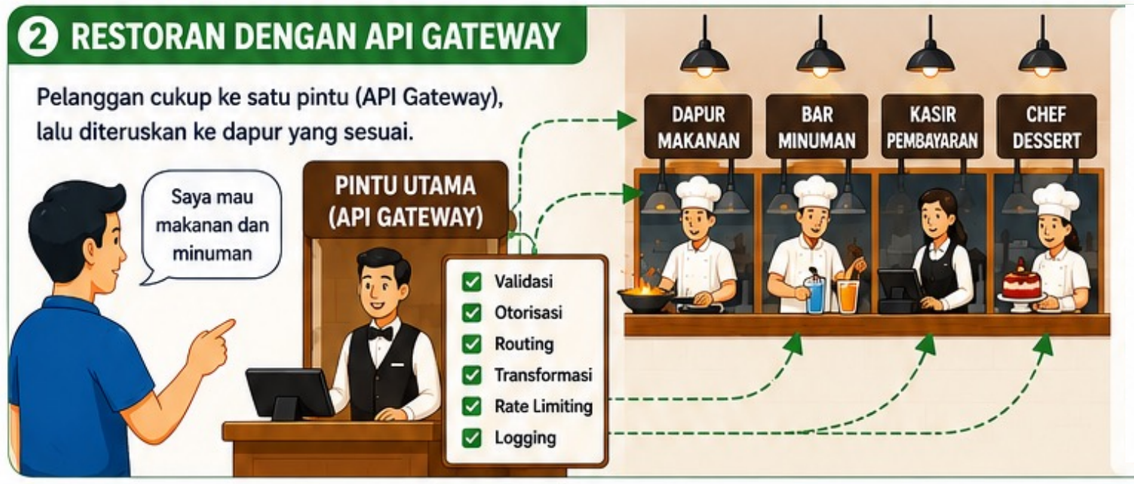
REFERENSI:

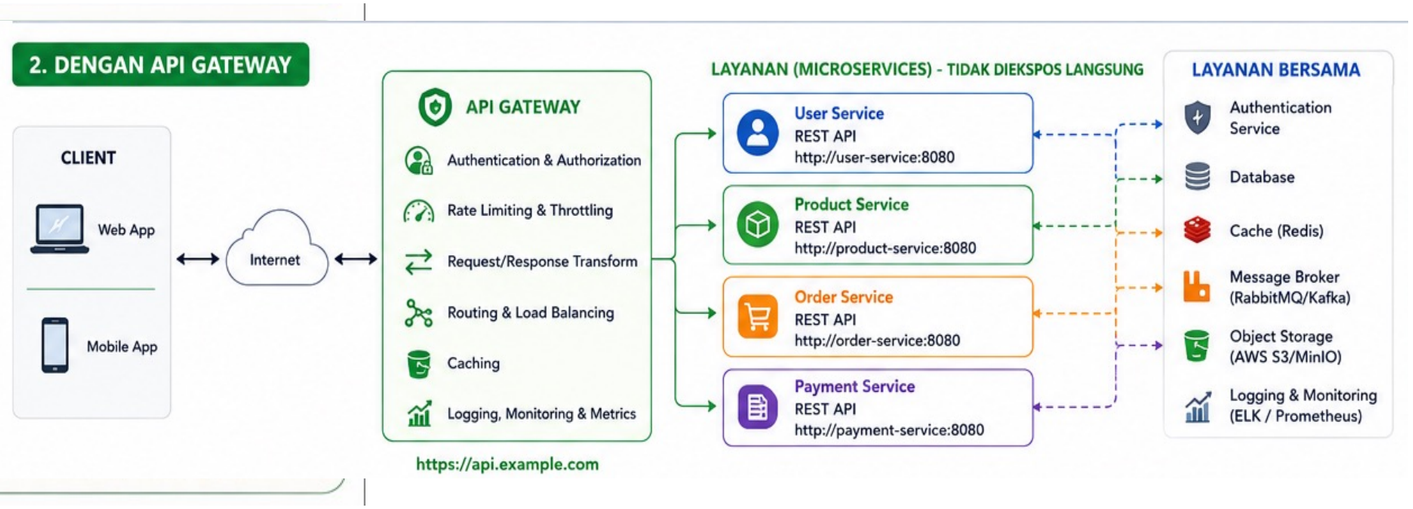
- Peraturan BSSN No.4 Tahun 2021;
- OWASP API Security Top 10 (2023);
- NIST 800-228;
- Paper Security Of Model (SoM) | Aris Munandar

DIRECT API DAN API GATEWAY









01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Definisi dan Konsep API Security

Apa itu API Security?

API Security adalah praktik melindungi **Application Programming Interfaces (API)** dari ancaman, serangan, penyalahgunaan, dan paparan tidak disengaja.

API berfungsi sebagai **"pintu gerbang"** komunikasi antar aplikasi, sistem, dan layanan dalam ekosistem digital.

Ruang Lingkup API Security

Mencakup seluruh upaya untuk **MEMASTIKAN:**

- Hanya pihak **berwenang** yang dapat mengakses API
- Hanya tindakan **diizinkan** yang dapat dilakukan
- Data yang dipertukarkan tetap **aman dan terlindungi**

Prinsip Keamanan API

Confidentiality
Kerahasiaan data dan informasi yang dipertukarkan

Integrity
Keutuhan data tidak dimanipulasi dalam transit

Availability
Ketersediaan layanan API bagi pengguna yang berhak

Non-Repudiation
Kenirsangkalan terhadap tindakan pengguna

Authentication
Verifikasi identitas pengguna, aplikasi, atau sistem yang mengakses API

Auhorization
Pembatasan akses sesuai hak dan kewenangan yang diberikan

Accounting
Pencatatan aktivitas API untuk audit, pelacakan, dan investigasi

API Security bukan hanya "mengamankan kode", melainkan mengamankan seluruh ekosistem — dari desain hingga operasional.

PRINSIP KEAMANAN [FOKUS API SECURITY]

BADAN SIBER DAN SANDI NEGARA | PROFESIONAL | ELABORATIF RESPONSIF | INTEGRATIF SOLID | AKUNTABEL INOVATIF

Cegah Akses Tidak Sah

Lindungi Data & Privasi

Jaga Integritas Data

Tersedia, Andal & Terpercaya

1 AUTHENTICATION

Siapa Anda?



Memastikan identitas klien atau aplikasi sebelum mengakses API.

Contoh Kontrol

- OAuth 2.0 / OpenID Connect (OIDC)
- JSON Web Token (JWT)
- Mutual TLS (mTLS)
- API Key Authentication
- Client Certificate Authentication

2 AUTHORIZATION

Apa yang boleh Anda lakukan?



Mengontrol akses ke endpoint dan resource berdasarkan kebijakan.

Contoh Kontrol

- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Scope-Based Access Control
- Claims-Based Authorization
- Least Privilege Principle
- Policy Enforcement (PDP/PEP)

3 CONFIDENTIALITY

Menjaga kerahasiaan



Melindungi data dari akses, penyadapan, dan kebocoran saat transit maupun saat disimpan.

Contoh Kontrol

- TLS 1.3 / HTTPS
- Mutual TLS (mTLS)
- Encryption at Rest
- JSON Web Encryption (JWE)
- Secret Management
- Data Classification

4 INTEGRITY

Menjaga keutuhan



Memastikan data tidak diubah atau dimusnahkan tanpa izin selama pertukaran melalui API.

Contoh Kontrol

- Digital Signature (HMAC/RSA/ECDSA)
- Message Digest (SHA-256)
- Payload / Schema Validation
- Input Validation & Output Encoding
- Checksum Verification

5 AVAILABILITY

Menjaga ketersediaan



Memastikan API selalu tersedia dan tahan terhadap serangan yang dapat mengganggu layanan.

Contoh Kontrol

- Rate Limiting
- Throttling
- DDoS Protection
- Load Balancing
- Circuit Breaker
- API Gateway Failover / Health Check

6 AUDITABILITY (ACCOUNTING)

Mencatat aktivitas



Merekam dan memantau semua aktivitas API untuk deteksi, analisis, dan kepatuhan keamanan.

Contoh Kontrol

- API Access Logging
- Request & Response Logging
- Correlation ID / Trace ID
- SIEM Integration
- Immutable Audit Trail
- Security Event Monitoring & Alerting

7 NON-REPUDIATION

Tidak dapat disangkal



Memastikan tindakan atau transaksi tidak dapat disangkal oleh pihak yang melakukannya.

Contoh Kontrol

- Digital Signature
- Signed JWT
- Timestamping
- Certificate Authority (CA)
- Immutable Logs
- Transaction Signature

TEKNOLOGI PENDUKUNG KEAMANAN API

API GATEWAY

Gerbang terpusat untuk otentikasi, otorisasi, routing, dan monitoring.

WEB APPLICATION FIREWALL (WAF)

Melindungi API dari serangan aplikasi web seperti OWASP Top 10.

SIEM

Mengumpulkan, menganalisis, dan mengkorelasikan log keamanan secara real-time.

KEY MANAGEMENT SYSTEM (KMS)

Mengelola kunci kriptografi secara aman dan terpusat.

SECRET MANAGER

Menyimpan dan mengelola secret seperti API key, token, dan kredensial.

API DISCOVERY & INVENTORY

Mendeteksi, memetakan, dan menginventarisasi seluruh API.

THREAT DETECTION PLATFORM

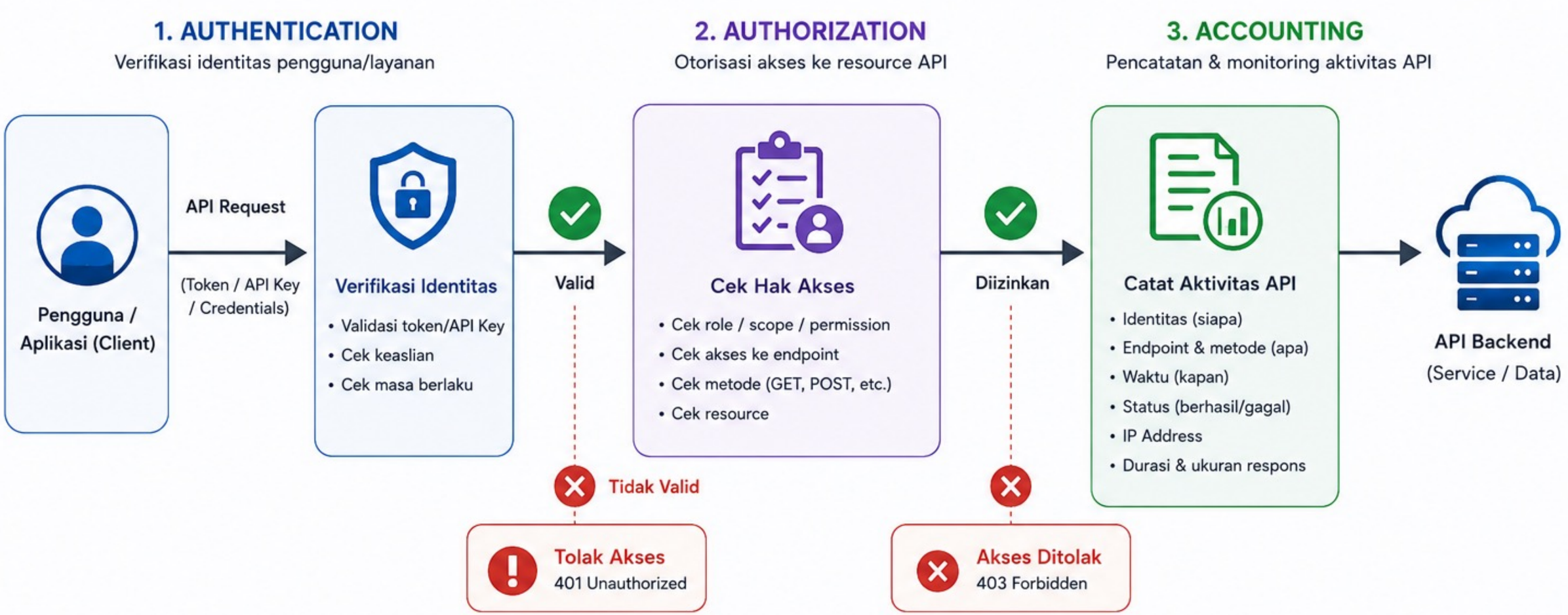
Mendeteksi ancaman, anomali, dan serangan terhadap API.

AI-DESIGNED, HUMAN-DRIVEN SUBSTANCE

Content based on "The Security Orientation Model : API Security" paper by Munandar Aris

PERISAI

AUTHENTICATION-AUTHORIZATION-ACCOUNTING (AAA)



AI-DESIGNED, HUMAN-DRIVEN SUBSTANCE

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Standar Internasional dan Framework Keamanan API

OWASP API Security Top 10

API1 Broken Object Level Authorization
API2 Broken Authentication
API3 Broken Object Property Level Authorization
API4 Unrestricted Resource Consumption
API5 Broken Function Level Authorization
API6 Unrestricted Access to Sensitive Business Flows
API7 Server Side Request Forgery (SSRF)
API8 Security Misconfiguration
API9 Improper Inventory Management
API10 Unsafe Consumption of APIs

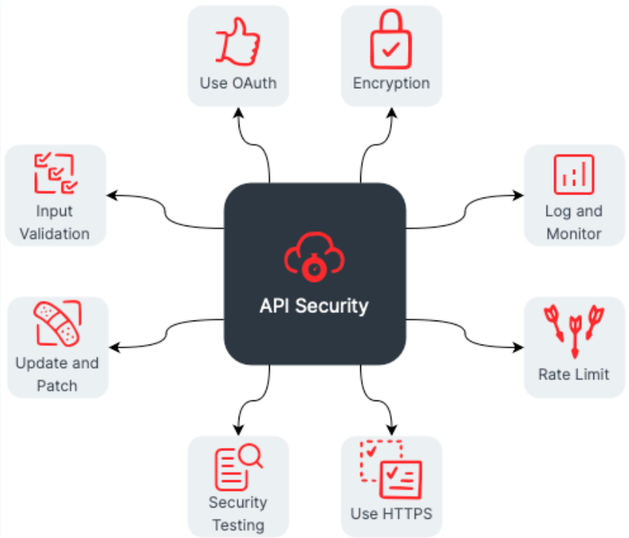
Standar Internasional Lainnya

- **NIST Cybersecurity Framework** untuk manajemen risiko
- **ISO/IEC 27001** untuk manajemen keamanan informasi
- **OpenAPI Specification (OAS)** untuk dokumentasi dan validasi API

Framework Autentikasi & Otorisasi

- · **OAuth 2.0 / 2.1** + OpenID Connect (OIDC)
- · **TLS 1.2/1.3** (HTTPS) wajib semua endpoint
- · **JWT** sebagai format token
- · PKCE untuk mobile dan SPA

Security Control based-On OWASP API Security Top 10 (2023)



NIST SP 800-228 (2025)

Identify — Inventori API, spesifikasi, shadow API discovery
Protect — Autentikasi kuat (OAuth/mTLS), otorisasi granular, TLS 1.3, rate limiting
Detect — Telemetri kontinu, anomaly detection, payload inspection
Respond — Alerting, forensic logging, token revocation

Baseline Safeguards
Enkripsi, autentikasi dasar, schema validation, rate limiting sederhana

Advanced Defences
Field-level authorization, ML anomaly detection, AI-specific protections

Fokus: Framework siklus hidup penuh berbasis Zero Trust — dari desain hingga retirement.

◆ **Catatan:** OWASP menjawab "apa yang harus dilindungi" (risiko spesifik), NIST menjawab "bagaimana melindungi" (kontrol komprehensif).

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Perban BSSN No.4 Tahun 2021 — Keamanan Sistem Penghubung Layanan (Ps. 30-31)

Dasar Hukum & Ruang Lingkup

Perban BSSN No.4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE.

Pasal 30 — Keamanan Sistem Penghubung Layanan:

- **Keamanan interoperabilitas data & informasi**
- **Kontrol sistem integrasi** & perangkat integrator
- **Keamanan API** dan web service
- Keamanan migrasi data

Fungsi Keamanan API (Ps.31 ayat 4)

- Menerapkan protokol **SSL/TLS** antara pengirim dan penerima API
- Menerapkan protokol **OAuth versi terkini** untuk interaksi
- Melindungi layanan web RESTful dari **CSRF**
- Memvalidasi parameter masuk oleh penerima API
- Menampilkan metode RESTful HTTP

Fungsi Kontrol Sistem Integrasi (Ps.31 ayat 2)

- SSL/TLS versi terkini
- IPsec untuk transmisi data
- Sistem anti-DDoS
- Autentikasi & manajemen sesi
- Pembatasan akses berbasis otorisasi
- Validasi input
- Kriptografi pada verifikasi statis
- Penanganan eror & pencatatan log
- Proteksi data & jalur komunikasi
- Pendeteksi virus
- SLA minimum 95%
- Pemastian tidak ada kerentanan

Kesimpulan: Organisasi perlu mengadopsi pendekatan berlapis dengan menggabungkan standar internasional (OWASP, NIST, ISO), framework autentikasi modern (OAuth 2.1, JWT), dan kepatuhan regulasi nasional (Peraturan BSSN No.4 Tahun 2021) untuk mencapai postur keamanan API yang komprehensif.

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

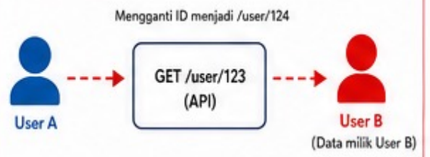
OWASP API Security Top 10 — Risiko Utama

01 BOLA (Broken Object Level Authorization)

Penjelasan
API tidak memeriksa apakah user berhak mengakses objek data tertentu.

Contoh
User A bisa mengakses data milik User B hanya dengan mengganti ID di URL.

Dampak
Kebocoran data pribadi, akses ilegal ke data penting.



02 Broken Authentication

Penjelasan
Autentikasi yang lemah/salah konfigurasi sehingga penyerang bisa masuk tanpa kredensial yang valid.

Contoh
API mengizinkan login tanpa rate limit, atau token mudah ditebak.

Dampak
Akun diambil alih, akses penuh oleh penyerang.



03 BOPLA (Broken Object Property Level Authorization)

Penjelasan
API tidak memvalidasi properti data yang diakses/dimodifikasi.

Contoh
User bisa mengubah harga produk jadi 0 karena API tidak memeriksa properti.

Dampak
Manipulasi data, fraud, perubahan data penting.



04 Excessive Data Exposure

Penjelasan
API mengembalikan data lebih banyak dari yang diperlukan.

Contoh
API mengirim nomor KTP, alamat, email padahal aplikasi hanya butuh nama.

Dampak
Kebocoran data sensitif, risiko privasi tinggi.

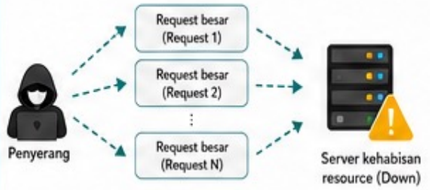


05 Unrestricted Resource

Penjelasan
Tidak ada batasan pada konsumsi resource (CPU, memori, bandwidth).

Contoh
API memungkinkan request besar bertubi-tubi hingga server kehabisan resource.

Dampak
Server down, layanan tidak tersedia (DoS).



06 Broken Function AuthZ (Broken Function Level Authorization)

Penjelasan
User bisa mengakses fungsi API yang tidak sesuai haknya.

Contoh
User biasa bisa mengakses endpoint untuk menghapus data.

Dampak
Perubahan atau penghapusan data penting.



07 SSRF (Server-Side Request Forgery)

Penjelasan
API memaksa server melakukan request ke sistem internal/eksternal.

Contoh
Penyerang menyuruh API mengakses http://localhost/admin.

Dampak
Akses ke sistem internal, kebocoran data.

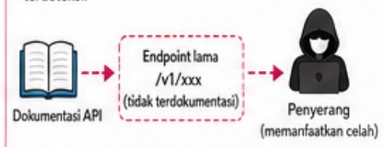


08 Improper Inventory

Penjelasan
API shadow/versi lama tidak terdokumentasi & tidak terkelola.

Contoh
Masih ada endpoint lama /v1/ yang memiliki celah keamanan.

Dampak
Celah lama dimanfaatkan, risiko tidak terdeteksi.



09 Unsafe API Consumption

Penjelasan
Aplikasi mengonsumsi API pihak ketiga tanpa verifikasi keamanan.

Contoh
Aplikasi menerima data dari API pihak ketiga tanpa memvalidasi signature.

Dampak
Data palsu, injeksi, pencurian data.



10 Security Misconfig

Penjelasan
Konfigurasi keamanan API tidak sesuai standar/best practice.

Contoh
CORS terbuka (*), debug mode aktif di produksi, TLS tidak dipaksa.

Dampak
Mudah dieksploitasi, kebocoran data.

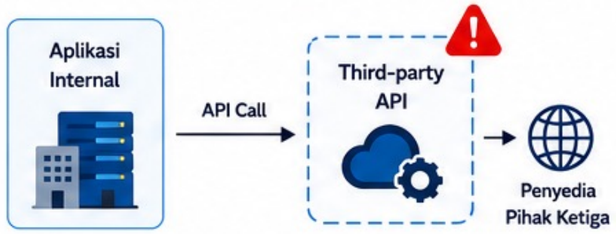


01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Risiko Integrasi API Khusus

1 Third-party API Tidak Terverifikasi

Risiko akibat integrasi API eksternal tanpa keamanan yang memadai.

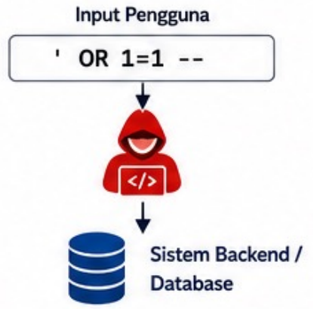


- Integrasi API eksternal tanpa security assessment
- Vendor tidak memiliki kontrol keamanan yang memadai
- Risiko supply chain attack melalui dependensi API
- Kebocoran API Key atau kredensial integrasi

Dampak: Kebocoran data · Kompromi sistem · Gangguan layanan · Pelanggaran kepatuhan

2 Injection Attacks

Eksploitasi input yang tidak divalidasi untuk menjalankan perintah berbahaya.



- Input API tidak divalidasi dengan baik
- SQL, NoSQL, LDAP, XPath, atau Command Injection
- Payload berbahaya dieksekusi oleh backend

Dampak: Akses tidak sah ke data · Manipulasi atau penghapusan data · Remote Code Execution (RCE) · Pengambilalihan sistem

3 Man-in-the-Middle & Data Leakage

Risiko penyadapan komunikasi dan kebocoran data sensitif melalui API.

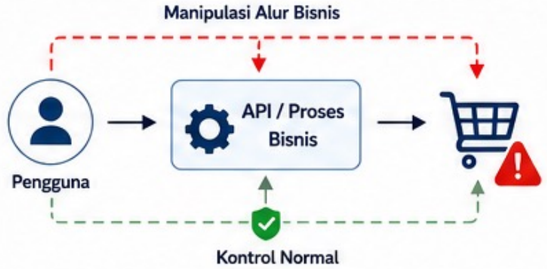


- Komunikasi API tidak diamankan dengan TLS yang kuat
- Validasi sertifikat tidak dilakukan dengan benar
- API mengembalikan data berlebihan (Excessive Data Exposure)
- Informasi sensitif tereksspos melalui response atau log

Dampak: Kebocoran data sensitif · Pelanggaran privasi · Pencurian identitas · Penyalahgunaan informasi

4 Business Logic Abuse

Penyalahgunaan proses bisnis yang sah untuk tujuan tidak sah.



- Penyalahgunaan fungsi bisnis yang valid untuk tujuan tidak sah
- Manipulasi transaksi, voucher, reward, atau workflow bisnis
- Otomasi penyalahgunaan menggunakan bot atau script

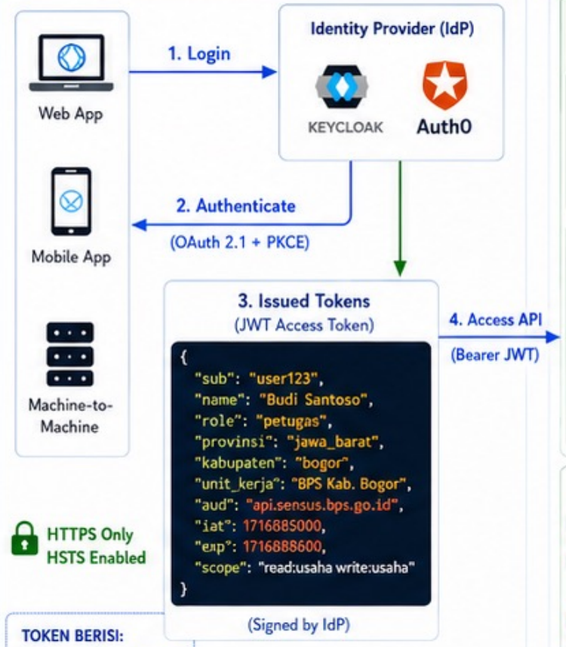
Dampak: Kerugian finansial · Fraud · Penyalahgunaan layanan · Kerusakan reputasi organisasi

Autentikasi & Otorisasi kuat · **Validasi input secara ketat** · **Gunakan TLS yang kuat** · **Terapkan prinsip least privilege** · **Monitoring & Logging berkelanjutan** · **Lakukan security test secara rutin**

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Best Practice Pengamanan API

1. AUTHENTICATION FLOW



2. AUTHORIZATION: RBAC vs ABAC (Perbedaan Cara Pengambilan Keputusan)

RBAC (Role-Based Access Control)

Keputusan berdasarkan ROLE / PERAN pengguna

Contoh Role di Sistem

Admin · Operator · Petugas · Auditor

Contoh Hak Akses per Role

Role	Hak Akses
Admin	CRUD semua data, kelola user, konfigurasi
Operator	Input & edit data, lihat data
Petugas	Input & edit data wilayah kerja sendiri
Auditor	Read-only, audit log

Cara Kerja RBAC

1. Sistem membaca role dari token (claim "role")
2. Mencocokkan role dengan hak akses yang sudah didefinisikan
3. Jika role memiliki hak tersebut → Izinkan
4. Jika tidak → Tolak (403 Forbidden)

Contoh RBAC (Petugas)

Token: { "role": "petugas" }

Request: POST /usaha

→ Diizinkan (karena role petugas boleh input data)

ABAC (Attribute-Based Access Control)

Keputusan berdasarkan ATRIBUT & KONTEKS

Contoh Atribut yang Dievaluasi

Atribut User	Atribut Resource	Atribut Environment
(provinsi, kabupaten, unit_kerja, jabatan)	(wilayah, klasifikasi, owner, status)	(waktu, lokasi, device, jaringan, risiko)

Contoh Rule ABAC

"Petugas hanya boleh mengakses data di wilayah kerjanya sendiri pada jam kerja dari perangkat terdaftar dan jaringan terpercaya."

Cara Kerja ABAC

1. Sistem mengambil atribut dari token, resource, dan environment
2. Mengevaluasi rule/policy (policy engine)
3. Jika semua kondisi terpenuhi → Izinkan
4. Jika salah satu kondisi gagal → Tolak (403 Forbidden)

Contoh ABAC (Petugas Bogor)

Rule: user.kabupaten == data.kabupaten
AND waktu_jam_kerja == true
AND device.terdaftar == true
AND network.trusted == true

Token: { "kabupaten": "bogor", "role": "petugas" }
Data: { "kabupaten": "bogor" }
→ Diizinkan (Bogor == Bogor & semua kondisi terpenuhi)

API GATEWAY

(Kong / NGINX / Apigee)

- TLS Termination
- JWT Validation (signature, exp, iss, aud)
- Scopes & Claims Check
- Rate Limiting
- Request Logging

4. Forward Request (setelah lolos RBAC & ABAC)

5A. RBAC CHECK (PERAN)

Cek role dari token
Apakah role memiliki hak akses dasar?

5B. ABAC CHECK (ATRIBUT & KONTEKS)

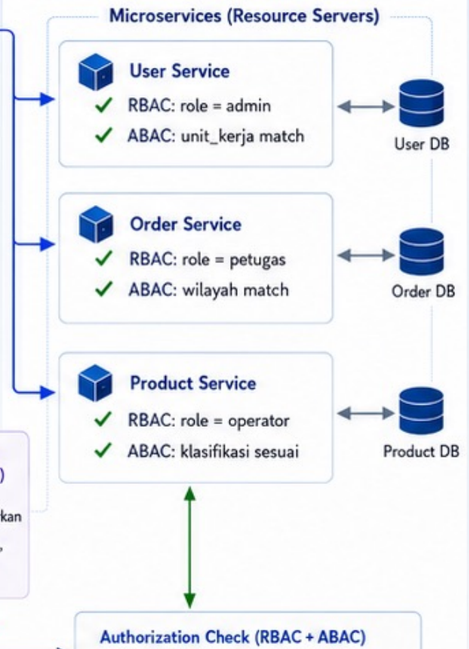
Evaluasi policy berdasarkan atribut user, resource, dan environment

200 OK Authorized

403 Forbidden (Insufficient Role)

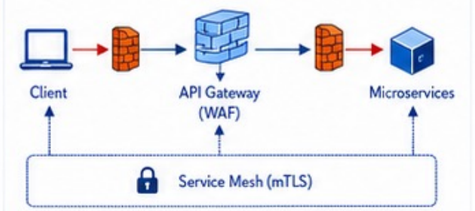
403 Forbidden (Policy Tidak Terpenuhi)

3. AUTHORIZATION FLOW (IMPLEMENTASI)



4. ZERO TRUST ARCHITECTURE

- No Implicit Trust
- Verify Every Request
- Least Privilege Access
- Micro-segmentation
- Continuous Monitoring
- Audit & Logging



5. TOKEN LIFECYCLE (BEST PRACTICE)

- Short-lived Access Token (5–15 menit)
- Refresh Token Rotation
- Revoke on Logout / Suspicious Activity
- Blacklist / Revocation List

6. OBSERVABILITY & AUDIT

- Centralized Logging (ELK / Loki)
- Audit Trail (Siapa, Kapan, Apa, dari Mana)
- Alerting & Monitoring (Prometheus / Grafana)
- Anomaly Detection

7. PERBANDINGAN RBAC vs ABAC

Aspek	RBAC	ABAC
Dasar Keputusan	Role / Peran	Atribut & Konteks
Fleksibilitas	Sedang	Sangat Tinggi
Kompleksitas	Sederhana	Lebih Kompleks
Cocok Untuk	Mayoritas aplikasi enterprise	Aturan akses dinamis, kontekstual
Contoh	Admin, Operator, Petugas	Jabatan, Wilayah, Waktu, Device, Data

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Mekanisme Autentikasi dan Otorisasi

Autentikasi — Siapa Anda?

API Keys

Untuk machine-to-machine, simple tetapi terbatas

Basic Auth

Hanya untuk internal, harus dengan HTTPS

JWT (JSON Web Tokens)

Stateless, scalable, cocok untuk microservices

OAuth 2.0 / 2.1

Authorization Code + PKCE paling aman untuk user-facing apps

Otorisasi — Apa yang Boleh Dilakukan?

RBAC

Role-Based Access Control berdasarkan peran pengguna

ABAC

Attribute-Based Access Control berdasarkan atribut kontekstual

Scopes & Claims

Scopes di OAuth / Claims di JWT untuk granular permission

Object & Function Level

Authorization check di setiap endpoint

Rekomendasi 2026: OAuth 2.1 + JWT + Short-lived tokens + Refresh token rotation + Zero Trust Architecture

01 Pengantar
02 Kebijakan
03 Risiko
04 Mitigasi

Monitoring dan Mitigasi Ancaman Keamanan API

Monitoring

- Real-time API traffic visibility
- AI/ML anomaly detection
- Logging lengkap (tanpa data sensitif)
- Alerting untuk breach & spike
- API Gateway + WAF + SIEM

Mitigasi Ancaman

- WAF khusus API
- Runtime Protection & Bot Mitigation
- Automated blocking/throttling
- Incident Response Plan
- Penetration Testing & Bug Bounty

Tools Populer

API Gateway:

Kong, Apigee, AWS, Azure

API Security:

Salt, Traceable, Wallarm

Testing:

OWASP ZAP, 42Crunch, Burp

Deteksi
Anomaly Detection → **Analisis**
Threat Intelligence → **Respons**
Auto-blocking → **Recovery & Lessons**
Learned

Doktrin Keamanan: Security is not a product but a process. Monitoring proaktif dan respons cepat terhadap ancaman adalah kunci menjaga keamanan API dalam jangka panjang. Kombinasi teknologi, proses, dan kesadaran tim membentuk postur keamanan yang tangguh.



BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
STHANA PAROKSHARTA BHAKTI
PROFESIONAL • ELABORATIF • RESPONSIF
INTEGRATIF • SOLID • AKUNTABEL • INOVATIF
PERISAI

Keamanan siber dan sandi adalah tanggung jawab bersama seluruh pemangku kepentingan ***(shared responsibility)***. Dalam penerapannya, **prinsip *segregation of duty* menjadi kunci:** pembagian tugas dan tanggung jawab yang jelas antara pemilik sistem elektronik dan BSSN sebagai penyusun, pelaksana, dan monitoring kebijakan di bidang keamanan siber dan sandi nasional.

MARI JAGA RUANG SIBER
AGAR KITA NYAMAN KARENA AMAN

www.bssn.go.id humas@bssn.go.id BSSN_RI
BADAN SIBER DAN SANDI NEGARA bssn_ri

PROFESIONAL | ELABORATIF | RESPONSIF | INTEGRATIF | SOLID | AKUNTABEL | INOVATIF