Caderno de API LPR

A TY Soluções entrega eventos de leitura de placas por webhook. O receptor da Condfy recebe um **POST HTTPS** com um objeto JSON por leitura.

Requisição de exemplo

Endpoint ilustrativo. O receptor deve aceitar POST via HTTPS na porta 443, com certificado válido e endereço público.

```
POST /webhooks/lpr HTTP/1.1
Host: receptor.example.com
Content-Type: application/json
X-LPR-Event: lpr.detection.v1
X-LPR-Timestamp: 1794661201
X-LPR-Signature: sha256=<hex de 64 caracteres>
Idempotency-Key: 36a62d182f56468aa0d8d369458a6b08
```

Corpo JSON

Dados fictícios. A indentação abaixo facilita a leitura. Para validar a assinatura use os bytes recebidos na requisição.

```
{
  "event": "lpr.detection.v1",
  "event_id": "36a62d182f56468aa0d8d369458a6b08",
  "occurred_at": "2026-11-14T13:00:00Z",
  "received_at": "2026-11-14T13:00:01Z",
  "site_id": "condominio-homologacao",
  "camera_id": "entrada-01",
  "plate": "ABC1D23",
  "confidence": 0.98,
  "decision": "allowed",
  "reason": "whitelist",
  "outcome": "allow"
}
```

JSON Schema 2020-12 | Documentação online

Contrato de dados

Os onze campos são obrigatórios. O receptor pode ignorar propriedades adicionais na versão atual. Uma versão incompatível terá outro valor em `event`.

Campo	Tipo	Descrição
`event`	`string`	Valor fixo `lpr.detection.v1`.
`event_id`	`string`	32 caracteres hexadecimais minúsculos. Identifica a leitura.
`occurred_at`	`date-time`	Hora da detecção em UTC (sufixo Z). Na falta de hora na origem, usa-se a hora de processamento.
`received_at`	`date-time`	Hora de registro da detecção, em UTC (sufixo Z).
`site_id`	`string`	ID acordado do condomínio.
`camera_id`	`string`	ID acordado da câmera no condomínio.
`plate`	`string`	Placa normalizada em sete caracteres, sem espaços ou hífen.
`confidence`	`number | null`	Confiança entre 0 e 1. `null` indica valor indisponível.
`decision`	`string`	Decisão do reconhecimento conforme a tabela abaixo.
`reason`	`string`	Regra que resultou na decisão.
`outcome`	`string`	Classificação correspondente para uso no receptor.

Combinações válidas

decision	reason	outcome	Interpretação
`allowed`	`whitelist`	`allow`	Placa autorizada
`denied`	`blacklist`	`deny`	Placa em lista de bloqueio
`denied`	`not_whitelisted`	`unknown`	Placa fora da lista de autorização

`unknown` representa uma placa válida lida e recusada por ausência na lista de autorização. A confirmação de passagem física ou abertura da cancela exige registro próprio.

Implementação do receptor

Autenticação e idempotência

1. Leia o corpo bruto e rejeite cabeçalhos de autenticação duplicados. Verifique se `X-LPR-Timestamp` contém dígitos ASCII e fica a até 300 s da hora Unix do receptor.

2. Calcule HMAC-SHA256 com o segredo compartilhado sobre o timestamp ASCII, um ponto e os bytes brutos do corpo. Compare em tempo constante com `X-LPR-Signature`, no formato `sha256=` seguido de 64 dígitos hexadecimais minúsculos.

3. Valide o schema, os IDs autorizados e a igualdade de `X-LPR-Event` com `event` e de `Idempotency-Key` com `event_id`.

4. Persista o evento e a chave única na mesma transação ou em fila durável. Mantenha a chave por pelo menos 24 h após o aceite. Para duplicata autenticada já aceita, retorne 2xx sem repetir o processamento.

Vetor de assinatura

Use o JSON da página 1 em UTF-8, na mesma ordem, sem espaços entre campos, BOM ou quebra de linha final (304 bytes). Chave sintética exclusiva deste teste. Fixe o relógio do teste no timestamp indicado.

```
chave: ty-lpr-signature-fixture-2026-demo-only
timestamp: 1794661201
assinatura:
sha256=6d32e284985b1da2e128d9657bb9b8452baba0354302cb0ec783d87ae7599754
```

Respostas HTTP e entrega

Resposta do receptor	Comportamento da entrega
2xx, por exemplo `204`	Confirma o aceite durável.
`408`, `429`, `5xx` ou falha de conexão	Provoca nova tentativa. `Retry-After` aceita segundos ou data HTTP.
Demais códigos, inclusive `3xx`	Encerra a entrega. Use `400` para corpo inválido, `401` para autenticação inválida e `403` para IDs fora do escopo.

Até 8 tentativas em 24 h. A espera começa em 30 s, dobra a cada falha e tem teto de 1 h. O corpo e o ID permanecem iguais. Timestamp e assinatura são calculados por tentativa. Ordene a linha do tempo por `occurred_at`.

Testes de aceite

Valide as três decisões, confiança nula, assinatura adulterada, timestamp expirado e IDs fora do escopo. Confirme um registro por ID em duplicata, reenvio com o mesmo ID após `503` e processamento de leituras fora de ordem.