



Quick Guide

SNMP vs. REST API

bei CyberPower RMCARD205 / RMCARD400

(Technische Entscheidungsgrundlage für Monitoring und Automatisierung)

Inhaltsverzeichnis

1. Einleitung.....	3
2. Technischer Überblick	4
SNMP – Der Industriestandard für Monitoring.....	4
REST API – Die Automatisierungs-Schnittstelle	4
3. Entscheidungsmatrix.....	5
4. Typische Szenarien	5
Enterprise Rechenzentrum	5
IT-Dienstleister mit Let's Encrypt Rotation.....	5
Industrie / Gebäudeautomation	5
5. Fazit.....	5
6. Fragen & Antworten	6
7. IT-Begriffe einfach erklärt	10

1. Einleitung

Die Remote Management Cards der CyberPower RMCARD-Serie bieten eine duale Kommunikationsarchitektur: den etablierten Industriestandard SNMP sowie eine moderne REST API.

Diese bewusste Trennung von Monitoring- und Automatisierungsarchitektur ermöglicht maximale Stabilität, Skalierbarkeit und Integrationsflexibilität.

Die RMCARD ist mehr als eine Netzwerkschnittstelle, sie ist eine Integrationsplattform für moderne USV-Umgebungen.

Unterstützte Technologien:

- Webinterface (Browser)
- SNMP (v1 / v3)
- REST API
- SSH
- Modbus TCP (205-Serie)
- PowerPanel Business Integration
- E-Mail, Syslog, SNMP-Traps

Die Architektur folgt dem Prinzip: Monitoring und Automatisierung sind bewusst getrennt.

SNMP Monitoring



REST API Automatisierung



Abbildung 1 – Architekturprinzip SNMP vs. REST API

2. Technischer Überblick

SNMP – Der Industriestandard für Monitoring

SNMP ist ein zustandsloses, hochstabiles Protokoll für kontinuierliche Statusüberwachung.

Typische Einsatzumgebungen:

- Rechenzentren
- Managed Service Provider
- Enterprise Monitoring-Systeme (CheckMK, PRTG, Zabbix, Nagios, Grafana)

Strategischer Nutzen:

- ✓ Extrem hohe Stabilität
- ✓ Kein Session-Handling
- ✓ Kein Token-Management
- ✓ Ideal für 5–10 Sekunden Polling
- ✓ Industriestandard-Kompatibilität

SNMP ist die empfohlene Schnittstelle für alle Monitoring-Szenarien.

REST API – Die Automatisierungs-Schnittstelle

Die REST API ermöglicht die vollständige Integration der RMCARD in moderne IT-Automatisierungsprozesse.

Typische Anwendungsfälle:

- Zertifikats-Rotation (z.B. Let's Encrypt)
- Remote-Reboot-Workflows
- Netzwerkkonfiguration per Script
- Infrastruktur als Code

Strategischer Nutzen:

- ✓ Automatisierung komplexer Prozesse
- ✓ Integration in DevOps-Umgebungen
- ✓ Zukunftssichere Web-Architektur

Einschränkungen (transparent kommunizieren):

- Token-basierte Authentifizierung
- Session-Architektur
- Nicht optimiert für hochfrequentes Monitoring

REST API ist die empfohlene Schnittstelle für Automatisierungs- und Integrationsprojekte.

3. Entscheidungsmatrix

Anforderung	Empfohlene Schnittstelle
Enterprise Monitoring (Grafana, CheckMK, Centreon, PRTG)	SNMP
Polling ≤ 10 Sekunden	SNMP
Automatisierte Zertifikatsverwaltung	REST API
Remote-Reboot-Workflows	REST API
Infrastruktur als Code	REST API
Hybrid-Architektur	SNMP + REST API

4. Typische Szenarien

Enterprise Rechenzentrum

- SNMP für Monitoring
- REST API für administrative Tasks

IT-Dienstleister mit Let's Encrypt Rotation

- REST API für Zertifikat Deployment

Industrie / Gebäudeautomation

- SNMP oder Modbus (bei 205-Serie)

5. Fazit

In über 90 % der Projekte lautet die empfohlene Architektur:

SNMP für Monitoring

REST API für Konfiguration und Automatisierung

Die bewusste Dual-Architektur der RMCARD-Serie bietet Investitionssicherheit, Integrationsflexibilität und Enterprise-Kompatibilität.

6. Fragen & Antworten

1. Welche Schnittstelle ist moderner?

Beide Schnittstellen sind modern, erfüllen jedoch unterschiedliche Aufgaben.

- **SNMP** ist der etablierte Standard für stabiles Monitoring.
- **REST API** ist die moderne Schnittstelle für Automatisierung und Integration.

Es geht nicht um „moderner“, sondern um den richtigen Einsatzzweck.

2. Warum wird die REST API nicht für Monitoring empfohlen?

Die REST API arbeitet mit Login-Sessions und zeitlich begrenzten Tokens.

Für dauerhaftes, regelmäßiges Abfragen (z. B. alle 5–10 Sekunden) ist SNMP technisch stabiler und effizienter.

3. Kann ich trotzdem Monitoring über die API durchführen?

Technisch ja, empfohlen wird es jedoch nicht.

Für kontinuierliche Überwachung ist SNMP deutlich besser geeignet.

4. Muss ich mich bei SNMP anmelden?

Nein.

SNMP arbeitet in der Regel ohne klassische Login-Sessions.
Es ist für dauerhaftes Monitoring ausgelegt.

5. Wann sollte ich die REST API einsetzen?

Die REST API ist ideal für:

- Automatisierte Zertifikatsverwaltung (z. B. Let's Encrypt)
- Remote-Neustarts
- Netzwerkkonfiguration per Script
- Integration in eigene Software
- Infrastruktur-als-Code-Projekte

6. Kann ich SNMP für Konfigurationsänderungen nutzen?

Nein.

SNMP ist primär für Statusabfragen und Alarmmeldungen gedacht, nicht für umfangreiche Konfigurationsänderungen.

7. Warum ist bei der RMCARD205 nur eine Login-Session möglich?

Die Architektur ist bewusst auf Stabilität und Hardware-Ressourcenschutz ausgelegt.

Eine begrenzte Anzahl gleichzeitiger Sessions verhindert Überlastung und erhöht die Betriebssicherheit.

8. Was passiert, wenn das API-Token abläuft?

Nach Ablauf des Tokens muss erneut ein Login durchgeführt werden.

Das erhöht die Sicherheit, da Zugriffe zeitlich begrenzt sind.

9. Was ist sicherer – SNMP oder REST API?

Beide können sicher betrieben werden.

- SNMPv3 bietet verschlüsselte Kommunikation.
- REST API arbeitet über HTTPS mit Token-Authentifizierung.

Die Sicherheit hängt von der Konfiguration ab.

10. Was passiert bei hoher Last oder kritischer Batterielage?

Bei Nutzung von SNMP kann das Monitoring-System sofort Alarm schlagen.

Bei REST API würde eine regelmäßige Abfrage notwendig sein, was weniger effizient ist.

11. Kann ich SNMP und REST API gleichzeitig nutzen?

Ja.

Dies ist sogar die empfohlene Architektur:

- SNMP für Monitoring
- REST API für administrative Aufgaben

12. Warum ist SNMP für Polling architektonisch überlegen?

SNMP ist zustandslos.

Das bedeutet:

- Keine Session-Verwaltung
- Kein Token-Handling
- Geringe Systembelastung

Die REST API ist dagegen für einzelne, gezielte Aktionen konzipiert.

13. Ist die REST API skalierbar?

Ja, insbesondere für Automatisierungsprojekte.

Für hochfrequentes Monitoring ist sie jedoch nicht optimiert.

14. Welche Architektur wird in 90 % der Projekte empfohlen?

Die empfohlene Standardarchitektur lautet:

- **SNMP für Monitoring**
- **REST API für Konfiguration und Automatisierung**

15. Warum gibt es zwei Schnittstellen und nicht nur eine?

Weil Monitoring und Automatisierung unterschiedliche technische Anforderungen haben.

Eine getrennte Architektur sorgt für:

- Höhere Stabilität
- Bessere Skalierbarkeit
- Klare Aufgabenverteilung
- Investitionssicherheit

16. Wie lange ist das API-Token gültig?

Standardmäßig ist das REST-API-Token **3 Minuten (180 Sekunden)** gültig.

Diese Zeit kann angepasst werden.

17. Sollte man die Token-Zeit verlängern?

Ja – in Automatisierungs-Szenarien ist es sinnvoll, die Token-Gültigkeit zu erhöhen.

Beispiel:

- Zertifikats-Upload
- Mehrere API-Befehle hintereinander
- Reboot + Konfiguration in einem Ablauf

Eine längere Gültigkeit verhindert unnötige Re-Logins während eines Scripts.

18. Welche empfohlene Token-Zeit ist praxisnah?

Empfehlung für produktive Umgebungen:

- **5 bis 10 Minuten** für Automatisierungsprozesse
- Nicht unnötig auf Maximum setzen
- Sicherheitsanforderungen berücksichtigen

Die maximale einstellbare Zeit beträgt **20 Minuten**.

19. Warum sollte man das Timeout nicht dauerhaft auf 20 Minuten setzen?

Längere Token-Zeiten erhöhen theoretisch das Sicherheitsrisiko.

Best Practice:

- Timeout nur so lang wie nötig
- Für Skripte 5–10 Minuten
- Für normale Nutzung Standard beibehalten

7. IT-Begriffe einfach erklärt

A

API (Programmierschnittstelle)

Eine API ist ein digitaler Helfer, über den Programme automatisch miteinander sprechen und Informationen austauschen.

Beispiel:

Ein Script lädt automatisch ein Zertifikat auf die RMCARD.

ACME (Automatic Certificate Management Environment)

Ein Standardverfahren zur automatischen Ausstellung und Erneuerung von Zertifikaten (z. B. Let's Encrypt).

Wichtig für Kunden, die Zertifikate automatisieren möchten.

Authentifizierung

Die Überprüfung der Identität eines Benutzers oder Systems. „Bist du wirklich berechtigt?“

Beispiel:

Benutzername und Passwort oder ein Token.

B

Bearer Token

Ein temporärer Zugriffsschlüssel, der nach dem API-Login automatisch erstellt wird.

Er ist standardmäßig 3 Minuten gültig und muss bei jeder Anfrage mitgesendet werden.

Vergleich:

Wie ein Besucherausweis im Büro, der nach kurzer Zeit wieder abläuft.

C

CheckMK / PRTG / Zabbix / Nagios

Programme zur Netzwerküberwachung.

Sie prüfen regelmäßig den Zustand von Geräten – meist über SNMP.

CI/CD (Continuous Integration / Continuous Deployment)

Automatische Software-Prozesse zur schnellen Bereitstellung von Änderungen.
REST API kann in solche Automatisierungsprozesse eingebunden werden.

D

Dauer-Polling

Regelmäßige automatische Abfrage eines Geräts, zum Beispiel alle 10 Sekunden.

Typisch für Monitoring-Systeme.
SNMP ist dafür optimiert.
REST API eher nicht.

Device Integration

Einbindung eines Geräts in bestehende IT-Systeme oder Monitoring-Plattformen.

E

Endpoint

Eine konkrete Adresse innerhalb einer API.

Beispiele:

```
/api/login/  
/api/upsinfo/  
/api/system/reboot/
```

Event / Ereignis

Eine Meldung der USV, z. B.:

- Stromausfall
- Batteriewarnung
- Überlast

Kann über SNMP-Trap oder Syslog weitergeleitet werden.

F

Failover

Automatischer Wechsel auf eine Ersatzlösung bei Ausfall.
Bei USV besonders relevant im Rechenzentrum.

Firmware

Die interne Software der RMCARD.
Sie steuert alle Funktionen wie Netzwerk, SNMP, API und Weboberfläche.

G

Grafana

Ein Visualisierungstool zur Darstellung von Monitoring-Daten (oft mit SNMP-Daten kombiniert).

H

High Availability (HA)

Hohe Verfügbarkeit eines Systems durch redundante Komponenten.

HTTPS

Eine verschlüsselte Webverbindung.
Schützt Daten vor unbefugtem Mitlesen.
Die REST API nutzt HTTPS.

I**Infrastruktur als Code (IaC)**

IT-Systeme werden automatisch per Script verwaltet statt manuell.

Beispiel:

Netzwerkeinstellungen ändern, Zertifikate verteilen oder Geräte neu starten.

L**Load (Last)**

Die aktuelle Auslastung der USV in Prozent.
Wichtiger Monitoring-Wert.

Login-Session

Eine aktive Anmeldung an einem Gerät.

Bei einigen RMCARD-Modellen (z. B. 205):
→ Es ist nur eine Session gleichzeitig möglich.

Grund:
Begrenzte Hardware-Ressourcen und Stabilitätsdesign.

M**Monitoring**

Die kontinuierliche Überwachung eines Systems.

Typische Werte:

- Batteriestatus
- Last in %
- Temperatur
- Alarmzustände

SNMP ist speziell für Monitoring entwickelt.

Modbus TCP

Ein Industrie-Kommunikationsprotokoll.
Wird häufig in Gebäudeleittechnik und Industrieumgebungen eingesetzt.

Nur bei bestimmten Modellen verfügbar (z. B. RMCARD205).

Microburst

Sehr kurze Lastspitzen im Stromverbrauch.
SNMP erkennt diese besser bei häufigem Polling.

N

NMS (Network Management System)

Ein zentrales Überwachungssystem für Netzwerke.

Beispiele:
CheckMK, PRTG, Zabbix

O

On-Premises

Systeme laufen im eigenen Unternehmen, nicht in der Cloud.

P

Polling

Aktive Abfrage eines Geräts.

Beispiel:
„Wie hoch ist deine aktuelle Last?“

SNMP = ideal
REST API = nicht optimal für Dauerabfragen

Push vs. Pull

Pull:

Monitoring-System fragt regelmäßig Daten ab (SNMP-Polling).

Push:

Gerät sendet aktiv eine Meldung (z. B. SNMP-Trap, Syslog).

R

REST API

Eine moderne Web-Schnittstelle für:

- Konfiguration
- Automatisierung
- Integration in eigene Software

Nicht primär für dauerhaftes Monitoring gedacht.

Retry-Logik

Automatisches Wiederholen einer Anfrage bei Fehlern.
Wichtig bei API-Reboot-Szenarien.

S

Session-Architektur

Das System verwaltet aktive Anmeldungen.
Bei manchen Modellen ist nur eine gleichzeitige Anmeldung möglich.

SNMP (Simple Network Management Protocol)

Ein Standard-Protokoll zur Geräteüberwachung.

Eigenschaften:

- Zustandslos
- Kein Token
- Sehr stabil
- Ideal für regelmäßige Abfragen

Kurz gesagt:
SNMP = Überwachen

SNMP Trap

Eine automatische Alarmmeldung der USV an ein Monitoring-System.
Wird bei Ereignissen versendet.

Syslog

Weiterleitung von Systemmeldungen an einen zentralen Server.
Hilft bei Analyse und Fehlerdiagnose.

T

Timeout

Maximale Gültigkeitsdauer eines Tokens oder einer Session.
Standard bei API: 3 Minuten (anpassbar).

Token-basierte Authentifizierung

Zugriff erfolgt über einen zeitlich begrenzten Schlüssel (Token).
Erhöht die Sicherheit der API.

U

USV (Unterbrechungsfreie Stromversorgung)

Ein Gerät zur Absicherung der Stromversorgung.
Die RMCARD macht die USV über das Netzwerk erreichbar.

W

Webinterface

Die browserbasierte Oberfläche der RMCARD.
Wird für manuelle Konfiguration verwendet.

A grayscale background image showing a close-up of server racks in a data center, with various components and cables visible.

CyberPower

CyberPower | USV Systeme, PDU, Überspannungsschutz |
Professionelle Stromversorgung Lösungen

CyberPower Systems GmbH
Edisonstr. 16,
85716 Unterschleissheim
Germany

T: +49-89-1 222 166 -0 F: +49-89-1 222 166 -29

E-mail: service@cyberpower.de

Web: www.cyberpower.de

CyberPower Wiki: [Home](#) | [CyberPower Wiki \(cyberpowersystems.de\)](#)

CyberPower und das CyberPower-Logo sind Marken von Cyber Power Systems, Inc. und/oder verbundenen Unternehmen, die in vielen Ländern und Regionen registriert. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.