QR SOLVE

Sicherheit

Authentifizierungsmethoden

ENDBENUTZER AUTHENTIFIZIERUNG, UM ZUGRIFF AUF RESSOURCEN ZU ERHALTEN

Der Endbenutzer mit gewährtem Zugriff autorisiert sich in der Anwendung mit starker Kundenauthentifizierung (SCA) / Zwei-Faktor-Authentifizierung (2FA) mit zwei Faktoren:

- Passwort / PIN
- Smartphone / Hardware-Token
- Biometrisch: TouchID / Fingerprint / FaceID

Mögliche Authentifizierungsmethoden (Kombination):

- Statisches Passwort
- Persönliche Identifikationsnummer (PIN)
- Digitales Zertifikat (x.509)
- App
- RSA/Youbico-Hardware-Token
- Touch-ID / Fingerabdruck
- Gesichts-ID
- Google / Microsoft 2FA-Authentifikator
- Apple ID
- Facebook
- Einmalige Passwörter (OTP)/SMS

Weitere Authentifizierungsmethoden

DAS GERÄT AUTHENTIFIZIERT SICH, UM ZUGRIFF AUF DIE RESSOURCEN ZU ERHALTEN

Das physische Gerät als Teil der IoT-Infrastruktur authentifiziert sich, um mithilfe einer einfachen Authentifizierung oder 2FA Zugriff auf die Ressourcen zu erhalten.
Mögliche Authentifizierungstools (Kombination):

- Digitales Zertifikat (x.509)
- Statisches Passwort
- PIN Nummer

DER ADMINISTRATOR AUTHENTIFIZIERT SICH UM ZUGANG ZU DEN RESSOURCEN ZU ERHALTEN

Der Backend-Benutzer authentifiziert sich, um Zugriff auf die in der geschützten Zone platzierten Ressourcen mit einfachem (Passwort/PIN) oder mit 2FA zu erhalten

DER ADMINISTRATOR VERWALTET DIE ENDBENUTZER UND BERECHTIGUNGEN

Der Administrator verwaltet die Benutzer in der Backoffice-Konsole oder direkt in der Authentifizierungsserver-Konsole. Er fügt Benutzer hinzu/entfernt/ändert Benutzer und definiert ihre Rollen/Berechtigungen.

Authentifizierung mittels Token

BENUTZER/GERÄT ERHALTEN AUTORISIERTEN ZUGRIFF AUF AUSGEWÄHLTE RESSOURCEN

Der authentifizierte Benutzer bzw. das Gerät erhält Zugriff auf entsprechende Ressourcen für seine Rolle/Rollen.
Wenn der Benutzer oder das Gerät authentifiziert wird, werden alle Berechtigungen für ihn berechnet und in ein Token eingebettet, das während des Authentifizierungsprozesses generiert wird.

Wenn ein Benutzer / Gerät Zugriff auf bestimmte Ressourcen erhalten möchte, übergibt er immer sein Token. Das Backend validiert dieses Token, überprüft die Berechtigungen:

- erlaubt, die angeforderten Ressourcen zu verwenden, wenn er die Berechtigung hat und das Token gültig ist.
- blockiert den Zugriff auf die angeforderten Ressourcen, wenn der Benutzer keine Berechtigung hat oder das Token ungültig / abgelaufen ist.

Security

Datensicherheit

Wo werden die Daten gespeichert

(Data at Rest) inkl. geografische Standorte, die den Datenschutzbestimmungen und Datenschutzrichtlinien entsprechen.

Wo werden die Daten offengelegt und benutzt

(Data in transit). Aktive Übertragung von Daten über das Netzwerk und Standorte.

Datenverschlüsselung

Datenverschlüsselung (wenn darauf zugegriffen und verarbeitet wird – ruhende Daten/Daten während der Übertragung) mit Verschlüsselungsschlüsseln

Tokenisierung

Schutz vor Offenlegung sensibler Daten. Stattdessen wird Hash/Token verwendet.

Datenisolierung

Datenisolierung (Im mandantenfähigen Modell)

Security

Infrastruktursicherheit

Gesicherte Verbindungen

Secure Socket Layer Protocol (SSL), Transport Layer Security (TLS) als Standard und Erweiterung von SSL, Mutual TLS (mTLS) als Erweiterung von Standard-TLS. Virtual Private Network (VPN) als gesicherte Verbindung zwischen Host und Server.

Eingeschränkte Zonen

Virtual Private Cloud (VPC) als isoliertes Netzwerk, Demilitarized Zone (DMZ) – zusätzliche Sicherheitsschicht für internen Netzwerkschutz, Private Zone.

Netzwerkverkehr

Netzwerkverkehr: Subnetze - Segmentierung von VPC, Access Control List (ACL)

Shields und Firewalls

S AWS Shield gegen DDoS-Angriffe. AWS WAF-Überwachung und Schutz vor Web-Exploits und -Angriffen.

Hardwareschutz

Hardwaresicherheitsmodul (HSM) ermöglicht es Ihnen, Ihre eigenen Verschlüsselungsschlüssel einfach zu generieren und zu verwenden.

Security

Backendsicherheit

API Security

Die API kann offen oder gesichert sein. Für gesicherte APIs unterstützen folgende Sicherheitsmechanismen den Ressourcenschutz: (oAuth2, JWT, Verschlüsselung, digitale Zertifikate).

Cross-Services-Kommunikation und asynchrone Kommunikation:

Low-Level-Kommunikation basierend auf Warteschlangen und Streamings (Kafka, Kinesis usw.). mit eingeschränktem Zugang zu Veranstaltungen.

Zugriff auf die Ressourcen

REST API HATEOAS Level 3 bedeutet, dass NUR das Backend entscheidet, welche Aktionen mit bestimmten Ressourcen möglich sind, Tokenisierung - Tokens anstelle von echten Daten werden verwendet, RBAC-Prinzip (Role Bases Access Control).

Komponentenschwachstellen

Modernste Lösungen und Komponenten ohne bekannte und kritische Schwachstellen.

Offenlegung sensibler Daten

Offenlegung sensibler Daten

Security

Frontendsicherheit

Autorisierter Zugriff

Authentifizierung und Autorisierung vor dem Zugriff auf die Ressourcen, basierend auf RBAC (Role Base Access Control)

REST API Stufe 3

Mögliche Aktionen für bestimmte Ressourcen werden vom Backend gesteuert

Einhaltung von OWASP

Das Open Web Application Security Project veröffentlicht ein Dokument, das die 10 kritischsten Sicherheitsbedenken für die Sicherheit von Webanwendungen beschreibt.

Komponentenschwachstellen

Modernste Lösungen und Komponenten ohne bekannte und kritische Schwachstellen.

Webserver-Konfiguration

DDoS-Prävention, HTTP-Methoden-Whitelist usw.

Konformität

Einhaltung von Vorschriften und Standards, um die beste Sicherheit zu bieten

Vorschriften

- Datenschutzrichtlinien
- Datenschutzbestimmungen
- GDPR
- Acts
- PSD/PSD2
- etc.

Normen

- ISO 27001
- IEC 62443 - Industrie
- IEC 61850 - Stromversorgungsunternehmen
- RFCs
- etc.

Grundlagen

Schutz vor nicht authentifiziertem und/oder unbefugtem Zugriff auf IT-Ressourcen.

Authentifizierung

Benutzerauthentifizierung:

Benutzeridentifikation (wer die App verwendet)

Tools zur Benutzerauthentifizierung

ermöglicht die Erfüllung von Vorschriften und Einschränkungen aus Datenschutzrichtlinien, z. B. statischer Pass, PIN, OTP, digitale Zertifikate, mobile Apps, Hardware-Token, Smartphones usw.

Einfache Authentifizierung:

Gut für die Backend-Mitarbeiter, die in einem privaten Netzwerk arbeiten

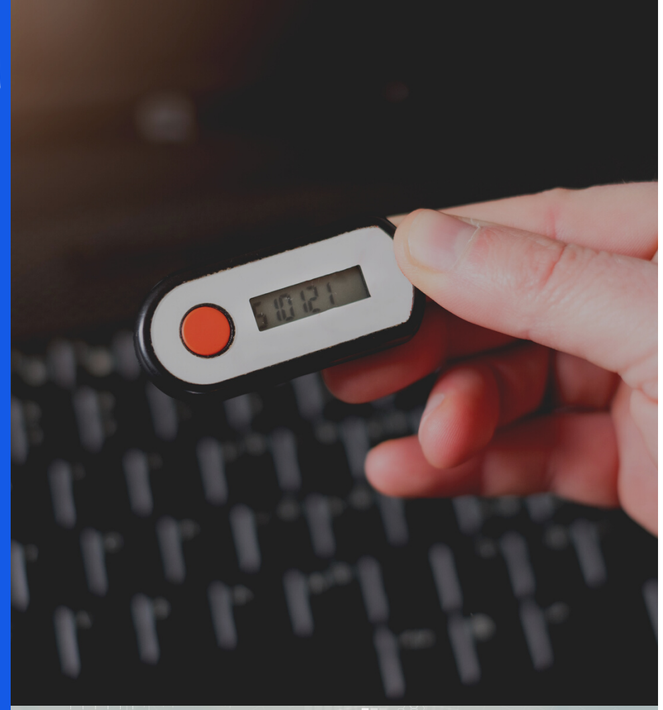
2-Faktor-Authentifizierung (2FA) / Starke Kundenauthentifizierung (SCA)

Zur Authentifizierung verwendet der Benutzer mindestens zwei der folgenden Kategorien von Authentifizierungswerkzeugen: Wissen, Besitz, Inhärenz

Multi Factor Authentication (MFA)

Zusätzliche Faktoren wie Ort und Zeit

Machine authentication



Grundlagen

Schutz vor nicht authentifiziertem und/oder unbefugtem Zugriff auf IT-Ressourcen.

Autorisierung

Rollen

Die Aggregationsebene für Hauptprivilegien. Der wichtigste im RBAC-Ansatz (Role Based Access Control)

Berechtigungen

Bestimmen Sie mögliche Aktionen, die der Benutzer ausführen kann, aggregiert in Rollen.

Zugriffskontrolle RBAC

Der Zugriff auf die Ressourcen ist auf eine bestimmte Rolle beschränkt.

Benutzerrechteverwaltung

Der Administrator kann Benutzerrechte (Rollen und Privilegien) direkt in der Autorisierungskomponente/ dem Server oder in der Bakcoffice-Dashboard-Konsole verwalten

Tracking-Aktivitäten

Prüfprotokolle von Benutzeraktivitäten

API-Zugriffskontrolle

Autorisiert / Nicht autorisiert

Integration

Integration mit bestehenden Autorisierungsservern oder Legacy-Systemen.

Single Sign-On

- Zentralisierter Authentifizierungsserver: Ein Authentifizierungsserver für die Organisation oder alle Kunden. Ermöglicht das Beibehalten von Anmeldeinformationen/Authentifizierungstools/Sicherheitsstandards für alle Benutzer.
- Umleitung: Der Benutzer wird zur Anmeldeseite des Authentifizierungsservers umgeleitet und authentifiziert
- Zugriff auf alle Systeme (inkl. Legacy).
- Inkrementelle Migration
- LDAP / Active Directory

Standards

Modernste Sicherheitsstandards

PKI / x.509

- Verschlüsselung / Digitale Signatur
- Private und öffentliche Schlüssel
- Digitale Zertifikate
- Zugriffskontrollliste
- Zertifikatsperrliste
- Qualifizierte und selbstsignierte Zertifikate

oAuth 2.0

- Auth-Flow für Mobilgeräte, Web, Geräte und Desktop
- Zugriffstoken
- Geltungsbereich (Stipendien)
- Protokolle: OpenID Connect, SAML

IEC / ISO

- Internationale Elektrotechnische Kommission
- Informationstechnologie (IT)
- Betriebstechnik (OT)

OWASP

- Standard für Webanwendung
- OWASP-Top 10
- API-Sicherheit
- Automatisiertes Testen

Penetration Tests

Untersuchung auf Software-Schwachstellen

Komponenten

- Web, Mobile & API gegen OWASP Top 10
- Erweiterte Sicherheitstests nach den neuesten Standards
- Systemintegrationen
- Infrastruktur
- Daten

Automatisierung

- Kontinuierliche Überprüfung von Software-Schwachstellen
- Statische Codeanalyse
- Qualitätstore
- CI/CD-Integration

CEH

- Zertifizierte ethische Hacker
- Code-Review
- Überprüfung der Infrastruktur
- BURP (Angriffssimulation)
- Rotes Teaming
- Black-Box, Grey-Box, White-Box
- Berichterstattung & Empfehlungen

Danke schön!

Testen Sie qrsolve

Ihr bewährter Technologiepartner

QR SOLVE

Addresse

Reformacka 6
35-026 Rzeszów
Poland

Telephon

+48 668 474 710
+48 694 150 492

Website

www.qrsolve.com