



taleor ist ein sicheres, agentenbasiertes Betriebssystem für Erlebnisorte: Inhalte, interaktive Anwendungen, Player und Hardware, gesteuert aus einer Konsole. Ein Assistent schlägt vor, eine namentlich benannte Person gibt frei, und jede Änderung wird im Audit-Protokoll festgehalten.

DREI SÄULEN
Sicher von Grund auf · Einrichtung durch einen Assistenten (Oli) · Analysen.

Sicher von Grund auf

SÄULE 01 · SICHERHEIT

IDENTITÄT Mutual TLS für jeden Player; eine Zertifizierungsstelle pro Standort, im gespeicherten Zustand versiegelt

INTEGRITÄT Ed25519-signierte Treiber; per Prüfsumme verifizierte Updates mit Rollback bei fehlgeschlagener Funktionsprüfung

FREIGABE Fünf Rollen, jede Route abgesichert; jeder Schreibvorgang im fortschreibbaren Audit-Protokoll

DATENSCHUTZ Besucherereignisse enthalten keine Kennung, durchgesetzt durch das Schema und einen Test, der den Build scheitern lässt

Einrichtung durch einen Assistenten (Oli)

SÄULE 02 · ASSISTENT

UMFANG Liest Exponate, Player, Reels, deklarierte Eingänge und Auslöser; schlägt Auslöser, Reel-Zuweisungen und das Aktivieren eines Auslösers vor

ERST PRÜFEN Planungswerkzeuge zeichnen nur Schritte auf; nichts wird ausgeführt, bevor eine Person „Übernehmen“ drückt; jede Änderung wird aufgelistet und anschließend protokolliert

BERECHTIGUNGEN Oli arbeitet als die angemeldete Person mit deren Rolle; im Audit-Protokoll als durch Oli für den benannten Benutzer übernommen erfasst

EHRLICHKEIT Ein veralteter Plan wird abgelehnt, nicht neu interpretiert; Vorschläge nur auf Basis deklarerter Eingänge; Oli benennt, was fehlt

MANUELL Jede Steuerung bleibt auch manuell verfügbar; Oli ergänzt die Konsole, ersetzt sie nie

Analysen (Statistiken)

SÄULE 03 · ANALYSEN

FREQUENZ, **VERWEILDAUER** Besucher pro Stunde, Tag oder Monat aus Sensoren und Touch-Eingaben; durchschnittliche Verweildauer bei engagierten Besuchern

ZONEN, **EXPONATE** Am stärksten frequentierte Zonen; Heatmap nach Zone und Stunde; Rangfolge der Exponate nach Besuchen und Verweildauer

WIEDERGABENACHWEIS Jedes Element, jede Wiedergabe, vollständig abgespielt oder nicht; CSV-Export mit demselben Umfang und Zeitraum

PLAYER-ZUSTAND Verfügbarkeit aus Zustands-Snapshots; ohne Snapshot in einem Zeitraum steht dort „unbekannt“, nie „fehlerfrei“

UMFANG, **ZEITRAUM** Standort, Etage, Zone oder Player; heute, Woche, Monat, Jahr, jeweils mit dem vorherigen Zeitraum. Nicht gemessene Werte lauten „nicht gemessen“, nie null

AUFBEWAHRUNG Präsenz und Berührungen 400 Tage; Wiedergabenachweis 1825 (Minimum 365); Player-Logs 30; Audit-Protokoll 730 (Minimum 180). Verkürzung nur bis zum Minimum

02 Betriebsmodelle

Dieselbe Software in jeder Edition

Cloud

SERVER LÄUFT app.taleor.net

INTERNET **ERFORDERLICH**

HINWEISE Keine Installation nötig; Medientechnik wird über Player-Agents angesteuert

Lokaler Server

SERVER LÄUFT Ein Rechner mit Windows, macOS oder Linux im Gebäude

INTERNET **OPTIONAL**

HINWEISE Eigene PostgreSQL-Instanz im Paket enthalten; keine Container-Laufzeitumgebung

Air-Gap

SERVER LÄUFT Wie lokaler Server, ohne Internet

INTERNET **KEINE VERBINDUNG**

HINWEISE Laufzeitumgebung und Datenbank im Paket enthalten; Updates werden von Hand eingebracht

Ein Build, eine Konsole; alle drei Editionen sind dieselbe Software

03 Plattformen

Version 1.0 · Oktober 2026

KOMPONENTE	WINDOWS	MACOS	LINUX	RASPBERRY PI	ANDROID	BROWSER
Konsole Bedienkonsole	App oder Browser	App oder Browser	App oder Browser	Browser	Browser	Jeder aktuelle
Player-Agent Offlinefähig, Hardware-E/A	Ja	Ja	Ja (.deb)	Browser-Player	Browser-Player	entfällt
Browser-Player Kopplung per sechsstelligem Code	Ja	Ja	Ja	Ja	Ja	Ja
Lokaler Server / Air-Gap-Server Dasselbe Paket, kein Internet nötig	x64	arm64, x64	x64, arm64	Nur Player	entfällt	entfällt

UNTERSTÜTZT ENTFÄLLT

04 Inhalte

Was die Konsole verwaltet

Objektmodell

Standort > Etage > Zone > Exponat > Player > Medientechnik; ein Player führt Reels und Auslöser aus

Reels

Geordnete Playlists aus Medien und Apps; einmal geändert, wird jeder Player aktualisiert, der das Reel abspielt

Auslöser

Eingang + Bedingung (zum Beispiel Abstand ≤ 100 cm) + Aktion + Ziel-Reel, optionale Ruhezeit

Eigener Speicher

Google Drive (Early Access). Dateien bleiben in Ihrem Drive; Bildschirme halten eine Kopie für die Offline-Wiedergabe

Vorlagen

Sechs integrierte interaktive Vorlagen, ein Baukasten für eigene Vorlagen, eigene App-Pakete (.zip)

Zeitplanung

Öffnungszeiten, Feiertage, Ausnahmen mit automatischer Rückkehr zum regulären Zeitplan; Inhaltsregeln nach Geltungsbereich mit der Vorschau „Was Vorrang hat“

Medien

Video, Bild, Audio, PDF, 3D und App-Pakete; 512 MB pro Datei (Cloud)

Offline-Wiedergabe

Der Agent hält standardmäßig eine lokale Kopie von 4 GB vor; spielt bei einem Serverausfall und nach einem Neustart weiter; Browser-Player ohne Gewähr (Best Effort)

05 Hardware und Protokolle

Treiber-Kit für eigene Geräte

Treiber sind mit Ed25519 signierte Pakete. Die Konsole gibt einen Befehl aus (Ein/Aus, Quelle, Lautstärke), und der Treiber spricht das Protokoll. Wir testen die Treiber mit Ihrer Medientechnik vor Ihrer Eröffnung; eigene Treiber entstehen mit dem Treiber-Kit.



Displays

Jeder Bildschirm an einem Computer mit dem taleor Player oder mit dem Browser-Player

TALEOR PLAYERBROWSER-PLAYERSHDMI



Projektoren

Jeder PJLink-Projektor; serielle Herstellerprotokolle

PJLINKESC/VP21RS-232TCP



Sensoren und Eingänge

Präsenz, Abstand, Radar, RFID, Drucktaster und berührungslose Taster, USB-Tasten, Touch

SERIELLUSBTCPUDPRS-232



Steuerungen

Lichtpulte und Showcontroller (OSC ein/aus), Mikrocontroller-Boards, Pedale, Handgerät für das Personal

OSCUSSSERIELLWEBSOCKET



Ton

Vernetzte Audioprozessoren und Lautsprecher

RESTTCP



Beleuchtung

DALI-/DALI-2-Gateways

DALI

OFFENE STANDARDS PJLINKRS-232TCPDALIMQTTOSCRESTWEBSOCKETSERIELLUSB

06 Sicherheitsmaßnahmen

Spezifikation

 Player-Identität	Mutual TLS; Schlüsselpaar wird auf dem Player erzeugt, der private Schlüssel verlässt ihn nie; Zertifikate nur für clientAuth, Subject vom Server festgelegt	 Zertifizierungsstelle	Eine CA pro Standort, im gespeicherten Zustand versiegelt; keine Schaltfläche „Zertifikat ausstellen“; der Modus „Erforderlich“ wird abgelehnt, solange dadurch ein Gerät ausgesperrt würde
 Zertifikate	398 Tage Laufzeit; Erneuerung in den letzten 30 Tagen über die eigene Verbindung des Players; ein neues Zertifikat widerruft das alte	 Prüfungen je Verbindung	Abgleich mit der Datenbank: nicht widerrufen, nicht abgelaufen, Gerät vorhanden, Gerät gehört zum Standort
 Transport	TLS 1.3 (1.2 für ältere Clients akzeptiert); HTTP wird auf HTTPS umgeleitet; Mutual-TLS-Listener auf Port 8443 (konfigurierbar)	 Anmeldung von Personen	E-Mail und Passwort (bcrypt, Kostenfaktor 12) oder OIDC; Sitzung 24 h; 5 Versuche/min; Sperre für 15 min nach 10 Fehlversuchen
 Bildschirm-Kopplung	Sechsstelliger Code, CSPRNG, 15-Minuten-Fenster, Ratenbegrenzung je IP und je Standort	 Treiberintegrität	Ed25519-Signatur über einen SHA-256-Hashwert jeder Datei; unsigned Treiber werden standardmäßig abgelehnt; Truststore des Betreibers
 Update-Integrität	Prüfsummenverifiziert (SHA-256 auf dem Player vor dem Austausch); Installation nur, während der Standort geschlossen ist; Opt-out je Gerät; eine fehlgeschlagene Funktionsprüfung innerhalb von zehn Minuten führt zum Rollback und sperrt das Update	 Zugriffskontrolle	Fünf Rollen: Netzwerk-Admin, Bereichs-Admin, Standort-Admin, Redakteur, Facility Manager; jede Route abgesichert; Facility Manager können einen Bildschirm neu starten, aber nicht löschen
 Audit-Protokoll	Jeder Schreibvorgang: Benutzer, Standort, Aktion, Objekt, Client-IP, Zeit; nur fortschreibbar (append-only); eine Löschung schwärzt die Identität, die Aktion bleibt erhalten; CSV-Export mit den in der Ansicht gesetzten Filtern; standardmäßig 730 Tage, Minimum 180	 Datenschutz für Besucher	Ereignisse enthalten nur Standort, Gerät, Zone, Zustand und Zeit; keine Kennung, durchgesetzt durch das Schema und einen Test, der den Build scheitern lässt; nächtliche Bereinigung nach Aufbewahrungsfrist, je Lauf nachgewiesen
 Isolation	Lokaler Server: eigene PostgreSQL-Instanz auf Loopback, zufälliges Passwort, das niemand eingibt; Medien und Audit-Protokoll bleiben im Gebäude	 Überwachung	Heartbeat 60 s; Störungen bei Offline-Status, knappem Speicherplatz und veralteter Version; schließen sich von selbst; wiederholte Fehler aktualisieren dieselbe Störung
 Notfallnachricht	Standort, Etage, Zone oder ausgewählte Player; Vollbild, Ton der Exponate stummgeschaltet; bis zu 12 Sprachen; über Konsole oder Handgerät	 Datensicherungen	Geplanter Export der gesamten Datenbank in lesbares JSON; rollierende Aufbewahrung; Wiederherstellung aus jeder Sicherung

07 Systemanforderungen

Server und Player

SERVER-BETRIEBSSYSTEM	Windows x64; macOS arm64 und x64; Linux x64 und arm64 (Ubuntu 24.04 LTS)
SERVER-LAUFZEITUMGEBUNG	Node.js 20 LTS und PostgreSQL 16 enthalten; ffmpeg nur unter Windows enthalten (macOS und Linux: aus den Paketen des Betriebssystems installieren, sonst werden Medien ohne Posterbilder, Miniaturansichten oder Spieldauer angenommen); Windows benötigt das Visual C++ Redistributable
SERVER-DIMENSIONIERUNG	Etwas 50 MB ohne Laufzeitumgebungen; Installation in unter einer Minute. Minimum: 1 CPU-Kern, 2 GB RAM, 10 GB freier Speicherplatz zuzüglich Ihrer Mediathek. Empfohlen für größere Standorte: 2 Kerne, 4 GB RAM. Der Speicherbedarf wächst mit Ihren Medien; gemessen an einer kleinen Installation
WINDOWS-AGENT	Windows 10 und 11, x64; läuft als Dienst; Node.js enthalten
LINUX-AGENT	Ubuntu 24.04 oder 26.04, .deb; Desktopsitzung mit Wayland oder X11
RASPBERRY-PI-BILDSCHIRME	Browser-Player auf Raspberry Pi 4 und 5, Raspberry Pi OS, Desktopsitzung; ein Pi 5 dekodiert H.264 in Software
MACOS-BILDSCHIRME	taleor Player-Agent auf einem 64-Bit-Mac mit Hardware-Videodekodierung. Der Browser-Player läuft außerdem in Safari 17.6 oder neuer und im aktuellen Chrome
ANDROID-BILDSCHIRME	Browser-Player im aktuellen Chrome, auch auf Android-Signage-Playern
PLAYER: CPU, RAM, SPEICHER	64-Bit-CPU mit Hardware-Videodekodierung für die Auflösung der Inhalte; 8 GB RAM empfohlen; 4 GB freier Speicherplatz für den Medien-Cache. 3D: Eine integrierte GPU der Klasse Apple M1 spielt etwa eine Million Splits in 1080p mit 30 bis 60 fps ab (gemessen); drei Millionen sind grenzwertig

PORTS

443 TCP Konsole, API, WebSockets

3401 TCP lokaler Server direkt

8443 TCP mTLS-Listener für Player

5433 TCP PostgreSQL nur auf Loopback

8000 UDP OSC eingehend

1883/1884 TCP MQTT, optional

Geräteports je Treiber

Player brauchen kein ausgehendes Internet in der lokalen und der Air-Gap-Edition.

08 Sprachen, Support und Lizenzierung

KONSOLE UND HANDGERÄT <div>ENDENLPL</div> Englisch, Deutsch, Niederländisch, Polnisch	DOKUMENTATION Whitepaper (EN, DE); Datenblatt (EN, DE, NL, PL); Benutzerhandbuch (EN, DE)	SUPPORT support@taleor.net	LIZENZIERUNG Für jeden Standort oder jedes Projekt erhalten Sie ein eigenes Lizenzangebot. Updates sind inbegriffen.	DATENSCHUTZRAHMEN Technische Maßnahmen gemäß ISO/IEC 27701 umgesetzt; eine Zertifizierung ist organisatorisch und wird nicht beansprucht
--	--	-----------------------------------	---	---

Vollständige Medientypen, Auslöser-Eingänge, OSC-Details, Treiberinterna und Aufbewahrungsklassen finden Sie im taleor Whitepaper und im Benutzerhandbuch.