ATOSS Time Control 11.2

ATOSS Time Control (Mobile)

Datensicherheit und Datenschutz

Technische Dokumentation

ATC_Mobile_Security
Letzte Aktualisierung: 07.04.2023

Die in diesen Unterlagen enthaltenen Informationen können ohne vorherige Ankündigung geändert werden.
Die ATOSS CSD Software GmbH geht hiermit keinerlei Verpflichtungen ein.
Die in diesen Unterlagen beschriebene Software wird unter einem Lizenzvertrag geliefert. Die Software darf daher nur im Einklang mit den Vertragsbedingungen verwendet oder vervielfältigt werden.
Das Kopieren der Software auf anderen als den im Lizenzvertrag ausdrücklich erlaubten Wegen ist rechtswidrig.
Ohne die schriftliche Genehmigung der ATOSS CSD Software GmbH darf kein Teil dieses Handbuchs, in welcher Form, mit welchen Mitteln und zu welchem Zweck auch immer, sei es auf elektronischem oder mechanischem Wege (einschließlich Fotokopien und Tonbandaufnahmen), vervielfältigt oder übermittelt werden.

Copyright 2023 ATOSS CSD Software GmbH. Alle Rechte vorbehalten.

ATOSS CSD Software GmbH
Rodinger Straße 19
93413 Cham, Deutschland

https://www.atoss.com/de/atoss-time-control

Alle geschützten Markennamen, Markenzeichen und Wortmarken sind Eigentum ihrer jeweiligen Inhaber.

Inhaltsverzeichnis

1 Allgemeine Hinweise....1
2 Systemarchitektur (ATC On Premises)....3
3 Systemarchitektur (ATC in der Cloud)....5
4 Datenspeicherung....9
4.1 Speicherung von App-Daten....9
4.2 Arten personenbezogener Daten....10
4.3 Inhaltsdaten....10
4.4 Datenschutzbestimmungen....10
4.5 Verschlüsselung....10
4.6 Logging....11
4.7 In-App-Browser-Engine....11
5 Bereitstellung der Anwendung....13
5.1 Sicherheit des Betriebssystems....13
5.2 Cloud-Lösung....13
5.3 Bezug über App-Stores....13
5.4 ATOSS Time Control (Mobile)-Berechtigungen....13
6 ATOSS Time Control (Mobile) verwenden....15
6.1 Anmeldung....15
6.2 Zugriffsschutz und Kennwörter....16
6.3 Push-Benachrichtigungen....16
6.4 Screenshots....16
6.5 Deaktivierung per Fernzugriff....17
7 Datenschutzerklärung....19
8 Glossar....21
8.1 AVV....21
8.2 Europäischer Wirtschaftsraum (EWR)....21
8.3 Google Remote Procedure Calls (gRPC)....21
8.4 Hypertext Transfer Protocol Secure (HTTPS)....21
8.5 Identity and Access Management (IAM)....21
8.6 Identity Provider (IdP)....22
8.7 IMEI-Nummer....22
8.8 Man-in-the-Middle-Angriff (MITM-Angriff)....22
8.9 On Premises....22
8.10 OpenID Connect (OIDC)....22
8.11 REST-Schnittstelle....23
8.12 Shoulder-Surfing....23
8.13 Transport Layer Security (TLS)....23
8.14 Zugriffs-Token....23

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

1 Allgemeine Hinweise

Gültigkeit dieses Dokuments

Diese Dokumentation betrifft die ATOSS Time Control (Mobile), die Mitarbeitern den Zugriff auf wichtige Informationen und Funktionen aus dem Umfeld des ATOSS Workforce Managements per Mobilgerät ermöglicht.

Hinweis: Die App wird aus Benutzersicht als ATOSS Time Control (Mobile) bezeichnet. ATOSS Time Control wird als technischer Namen des Web-Clients verwendet. Im Interesse einer besseren Lesbarkeit wird im weiteren Verlauf dieses Dokuments hauptsächlich ATOSS Time Control (Mobile) verwendet.

Zielsetzung und Zielgruppe

ATOSS Time Control (Mobile) ermöglicht den Zugriff auf wichtige Daten und Funktionen rund um das Thema Zeiterfassung und Personaleinsatzplanung über mobile Endgeräte, unabhängig von Einsatzzeit und Einsatzort. Datensicherheit und Datenschutz hat dabei oberste Priorität: So findet die Kommunikation zwischen den mobilen Endgeräten und der über ATOSS Cloud verfügbaren ATC-Anwendung ausschließlich verschlüsselt statt.

Die Dokumentation wendet sich an Berater, Kunden sowie Benutzer der ATOSS Time Control, die diese auf mobilen Endgeräten einsetzen.

Begriffsdefinition

Im vorliegenden Dokument werden folgende Abkürzungen und Begriffe verwendet:

- ATOSS Time Control: ATC
- Mobile Endgeräte bezeichnen Smartphones und Tablets.
- IAM-Service: zentraler Authentifizierungsdienst der ATOSS Software AG
- IdP: Identity Provider des Kunden, z. B. Microsoft Azure AD, PingOne
- HTTPS: HyperText Transfer Protocol Secure
- OIDC: OpenID Connect
- gRPC: google Remote Procedure Calls

Geschlechtsneutralität der Dokumentation

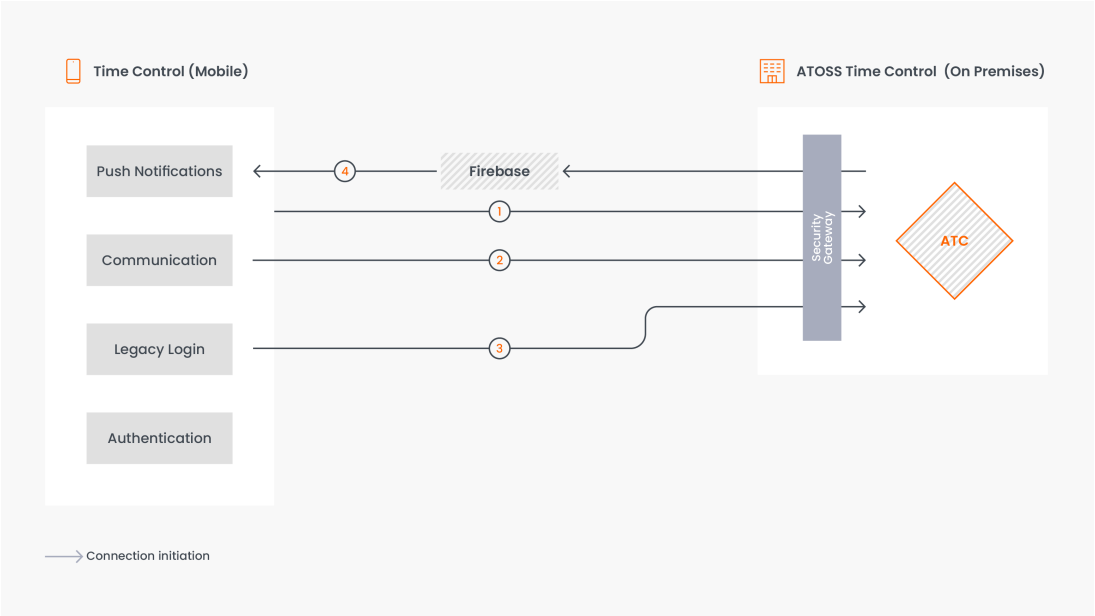
Im Interesse einer besseren Lesbarkeit wird davon abgesehen, bei Fehlen einer geschlechtsneutralen Formulierung sowohl die männliche als auch weitere Formen aufzuführen. Die gewählten Formulierungen gelten deshalb uneingeschränkt für die weiteren Geschlechter.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

2 Systemarchitektur (ATC On Premises)

Im Folgenden finden Sie einen Überblick über die Systemarchitektur von ATOSS Time Control (Mobile) für die ATOSS Time Control On Premises:



Pfeil Nr.	Abfrage von	Weitergabe an	Funktion	Protokoll	Ergebnis	Bemerkung
1	ATOSS Time Control (Mobile)	ATC	Verbindungsaufbau und Kommunikation	gRPC	Datenaustausch. Nur bei Nutzung von Push: Das Firebase-Plugin generiert ein Token in ATOSS Time Control (Mobile), das an die ATC gesendet und gespeichert wird.	Über diese Verbindung findet die Kommunikation zwischen ATOSS Time Control (Mobile) und der ATC statt.
2	ATOSS Time Control (Mobile)	ATC/<kunde> .app-atoss.com	Verbindung mit Server	HTTPS	Host, Port und Applikationsname der ATC	Eingabe von Host und Port oder Anmeldung über die Firmen-ID.
3	ATOSS Time Control (Mobile) – Authentication	ATC	Authentifizierung	gRPC	Nutzer und Passwort, PIN, biometrisches Verfahren	-
4	ATC	ATOSS Time Control (Mobile)	Versand von Push-Benachrichtigungen	HTTPS	Push-Benachrichtigungen werden über Firebase versendet. Nur mög-	Nur möglich bei funktionierender Internetverbindung.

ATOSS CSD Software GmbH, Copyright 2023

Pfeil Nr.	Abfrage von	Weitergabe an	Funktion	Protokoll	Ergebnis	Bemerkung
					lich, wenn Skripte eingestellt wurden.	
A	-	-	Gewährleistet einen sicheren Datenaustausch	-	Datenaustausch	Ist für die sichere Verbindung zwischen ATOSS Time Control (Mobile) sowie ATC zuständig. Weitere Informationen dazu finden Sie unter *Security Gateway (ATC On Premises)* auf Seite 4.

Security Gateway (ATC On Premises)

Um ATOSS Time Control (Mobile) bei einer On Premises-Installation verwenden zu können, ist eine sichere Verbindung zwischen der App und dem Server erforderlich. Diese muss bei einer On Premises-Installation vom Kunden selbständig konfiguriert werden. Dazu gibt es verschiedene Möglichkeiten, z. B. das Aufsetzen eines Reverse-Proxy.

Wichtig: Die gRPC-Calls müssen entsprechend durch den Security Gateway vom Server empfangen werden. Der Port kann in der Registry unter `Server/Daten-Server/gRPC/Port` oder die Umgebungs-Variable *ATC_SERVER_GRPC_PORT* gesetzt werden. Wenn kein Port festgelegt wird, wird standardmäßig Port 3711 verwendet.

Zusätzliche Informationen zur sicheren Anbindung

Die Möglichkeit des Einsatzes einer Web Application-Firewall, eines Reverse Proxy oder Ähnlichem zum Herstellen einer sicheren Verbindung hängt davon ab, ob das eingesetzte Verbindungs-Tool *Google Remote Procedure Calls (gRPC)* auf Seite 21 unterstützt. Da es viele verschiedene Anbieter auf dem Markt gibt, muss diese Information vom Kunden selbst überprüft werden.

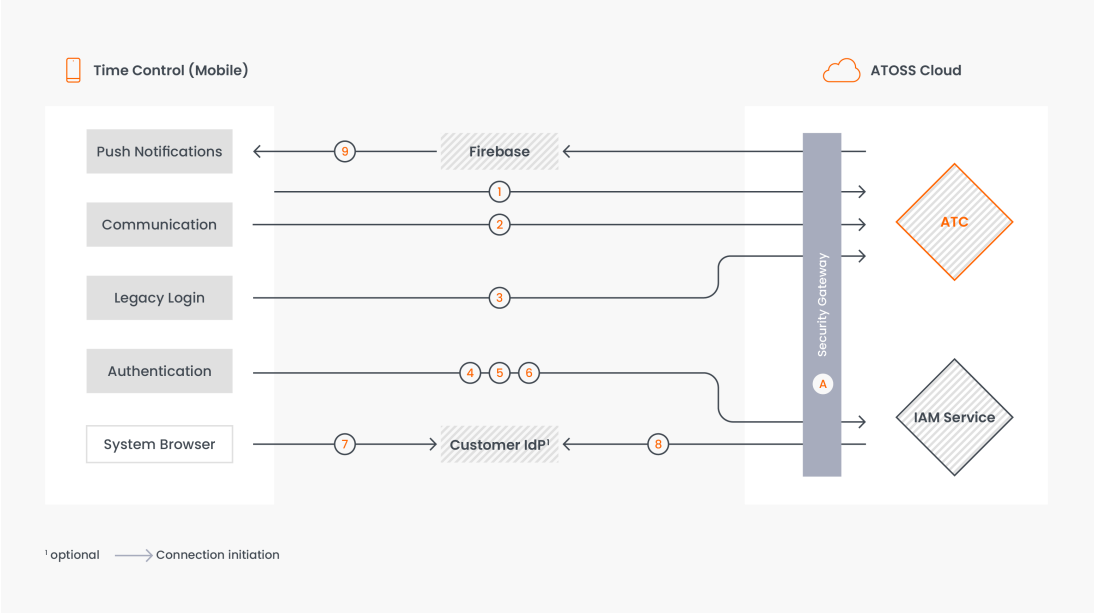
Eine zusätzliche Absicherung der Kommunikation können Sie durch das Verwenden von *Transport Layer Security (TLS)* auf Seite 23 mit Zertifikaten erreichen.

ATOSS CSD Software GmbH, Copyright 2023

3 Systemarchitektur (ATC in der Cloud)

Im Folgenden finden Sie einen Überblick über die Systemarchitektur von ATOSS Time Control (Mobile) für die ATOSS Time Control in der Cloud.

Hinweis: Für die Authentifizierung wird im Allgemeinen der mit Pfeil 3 gekennzeichnete Weg verwendet. Die Pfeile mit der Markierung 4, 5, 6, 7 und 8 sind optional: Die hiermit gekennzeichneten Wege werden nur bei Einsatz des kostenpflichtigen IAM-Services verwendet.



Pfeil Nr.	Abfrage von	Weitergabe an	Funktion	Protokoll	Ergebnis	Bemerkung
1	ATOSS Time Control (Mobile)	ATC	Verbindungsaufbau und Kommunikation	gRPC	Datenaustausch. Nur bei Nutzung von Push: Das Firebase-Plugin generiert ein Token in ATOSS Time Control (Mobile), das an die ATC gesendet und gespeichert wird.	Über diese Verbindung findet die Kommunikation zwischen ATOSS Time Control (Mobile) und der ATC statt.
2	ATOSS Time Control (Mobile)	<kunde> .app-atoss.com	Verbindung mit Server	HTTPS	Host, Port und Applikationsname der ATC	Eingabe von Host und Port oder Anmeldung über die Firmen-ID.
3	ATOSS Time Control (Mobile) – Authentica- ti- on	ATC	Authentifizierung	gRPC	Nutzer und Passwort, PIN, biometrisches Verfahren	-

ATOSS CSD Software GmbH, Copyright 2023

Pfeil Nr.	Abfrage von	Weitergabe an	Funktion	Protokoll	Ergebnis	Bemerkung
4	ATOSS Time Control (Mobile) – Authentication	IAM-Service	Authentifizierung	HTTPS (OIDC)	Redirect-URL zum föderierten IdP	-
5	ATOSS Time Control (Mobile) – Authentication	IAM-Service	Authentifizierung	HTTPS (OIDC)	Authorization Code (IAM-Service)	Bereitstellung des Authorization Code (IdP) mit dem Request
6	ATOSS Time Control (Mobile) – Authentication	IAM-Service	Authentifizierung	HTTPS (OIDC)	Access und Refresh Token	ATOSS Time Control (Mobile) stellt dem IAM-Service den Authorization Code (IAM-Service) bereit und erhält einen Access und Refresh Token. Der Access Token beinhaltet die Identität des Benutzers.
7	ATOSS Time Control (Mobile) – Authentication	Identity Provider (IdP)	Authentifizierung	HTTPS (OIDC)	Redirect-URL zum IAM-Service und Authorization Code (IdP), wenn Benutzer und Passwort korrekt sind.	Anmeldedialog: Eingabe von Benutzer und Passwort durch den Benutzer.
8	IAM-Service	IdP	Authentifizierung	HTTPS (OIDC)	Access Token	Der IAM-Service stellt dem Identity Provider (IdP) den Authorization Code (IdP) bereit und erhält einen Access Token.
9	ATC	ATOSS Time Control (Mobile)	Versand von Push-Benachrichtigungen	HTTPS	Push-Benachrichtigungen werden über Firebase versendet. Nur möglich, wenn Skripte eingestellt wurden.	Nur möglich bei funktionierender Internetverbindung.
A	-	-	Gewährleistet einen sicheren Datenaustausch	-	Datenaustausch	Ist für die sichere Verbindung zwischen ATOSS Time Control (Mobile) sowie ATC zuständig. Weitere Informatio-

ATOSS CSD Software GmbH, Copyright 2023

Pfeil Nr.	Abfrage von	Weitergabe an	Funktion	Protokoll	Ergebnis	Bemerkung
						nen dazu finden Sie unter *Security Gateway (ATC in der Cloud)* auf Seite 7.

Security Gateway (ATC in der Cloud)

ATOSS kümmert sich um das Aufsetzen des Security Gateways und gewährleistet einen sicheren Austausch der Daten.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

4 Datenspeicherung

Die Datenspeicherung umfasst folgende Unterthemen:

- *Speicherung von App-Daten* auf Seite 9
- *Arten personenbezogener Daten* auf Seite 10
- *Inhaltsdaten* auf Seite 10
- *Datenschutzbestimmungen* auf Seite 10
- *Verschlüsselung* auf Seite 10
- *Logging* auf Seite 11
- *In-App-Browser-Engine* auf Seite 11

4.1 Speicherung von App-Daten

Auf dem Mobilgerät werden folgende Daten verschlüsselt gespeichert:

Daten	Personenbezogen
Verbindungsdaten (Protokoll, Host, Port)	nein
Offline-Stempelung **Hinweis:** Wenn das Mobilgerät keine Verbindung zur ATC hat, wechselt es in den Offline-Modus. In diesem Zustand werden durchgeführte Stempelungen mit einer Hinweismeldung auf dem Mobilgerät gespeichert. Die Stempelungen werden an den Server übertragen, wenn das Mobilgerät wieder eine Verbindung zur ATC herstellen kann.	ja

Bei Offline-Buchungen werden folgende Daten auf dem Mobilgerät gespeichert:

Feld	Kommentar
Personalnummer	Zur Zuweisung des Mitarbeiters
Zeitkonto	Pflichtfeld
Online	Zeigt an, ob es sich bei der Buchung um eine Online- oder Offline-Buchung handelt.
Location Based Services (LBS, GPS, Standortdaten)	Nur, wenn die Übertragung des Standorts in der Software konfiguriert ist und wenn der Endnutzer der App die Standortermittlung erlaubt.
Kostenstelle	Nur bei Kostenstellenstempelung
Kommentar	Nur bei Eingabe eines Kommentars
Projekt	Nur bei Eingabe eines Projekts
Projektstatus	Nur bei Eingabe eines Projektstatus
Datum und Uhrzeit der Stempelung	Wird nur bei Offlinebuchungen initialisiert

ATOSS CSD Software GmbH, Copyright 2023

Feld	Kommentar
Zuletzt genutzte und Favoriten	Informationen zu zuletzt genutzten Stempelsätzen und Favoriten

Inhalts-oder Nutzungsdaten der ATOSS Time Control (Mobile) werden nicht durch einen Cloud-Backup-Mechanismus des Mobilgeräts gespeichert, auch wenn dieser grundsätzlich vom Benutzer aktiviert ist.

4.2 Arten personenbezogener Daten

Die von ATOSS Time Control (Mobile) automatisch verarbeiteten Nutzungsdaten (nach § 15 Abs. 1TMG) sind:

- Benutzer
- Host
- Port

Abhängig vom Lizenz -und Nutzungsumfang werden von ATOSS Time Control (Mobile) Ausschnitte der nachfolgend genannten Informationen automatisch verarbeitet:

- Mitarbeiterstammdaten und zeitwirtschaftliche Informationen
- Informationen aus der Personaleinsatzplanung
- Informationen aus Antragswesen
- Systembezogene Informationen

Detaillierte Auflistungen zu den einzelnen Informationen und den dazugehörigen Daten finden Sie in der 'Vereinbarung über die Datenverarbeitung im Auftrag' (*AVV* auf Seite 21).

4.3 Inhaltsdaten

In Bezug auf die Verarbeitung von personenbezogenen Inhaltsdaten werden die jeweiligen (ggf. besonderen) datenschutzrechtlichen Anforderungen nach dem jeweils einschlägigen Fachrecht beachtet.

4.4 Datenschutzbestimmungen

Zu den Datenschutzbestimmungen gelten folgende Punkte:

- Die Datenschutzbestimmungen sind bereits im App-Store einsehbar, z. B. über die von Google bereitgestellte Funktion 'Datenschutzerklärung für Entwickler'.
- Die Datenschutzbestimmungen sind innerhalb von ATOSS Time Control (Mobile) leicht auffindbar und einsehbar.
- In den Datenschutzbestimmungen wird die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ausreichend beschrieben.
- In den Datenschutzbestimmungen werden die ATOSS Time Control (Mobile)-Berechtigungen inklusive deren Verwendung ausreichend beschrieben.
- Ein den Anforderungen von § 5 TMG ('leicht erkennbar', 'unmittelbar erreichbar', 'ständig verfügbar'; zudem ggf. § 55 Abs. 2 RStV-Anforderung) entsprechendes Impressum liegt vor.

4.5 Verschlüsselung

ATOSS bietet keinen gesondert verschlüsselten Container für ATOSS Time Control (Mobile) an.

Folgende Verschlüsselungstechniken werden angewendet:

ATOSS CSD Software GmbH, Copyright 2023

- Die Übertragung über Transportprotokolle (*TLS*) erfolgt immer nur verschlüsselt.
- Das aktuelle ATOSS Cloud *HTTPS*-Zertifikat hat RSA 2048 Bit. Auf Kundenwunsch stellt ATOSS kostenpflichtig ein Zertifikat mit 4096 Bit bereit.
- Es werden vertrauenswürdige SSL-Zertifikate verwendet. Diese werden auch zur Verhinderung von *Man-in-the-Middle-Angriffen* überprüft.
- Die Authentifizierung kann bei Cloud-Installationen und entsprechender Einrichtung – hierzu wird ein kostenpflichtiger Zusatzdienst benötigt – über das *OpenID Connect (OIDC)* auf Seite 22-Protokoll erfolgen.

SSL-Pinning, d. h. eine feste 'Verdrahtung' des SSL-Zertifikats im ATOSS Time Control (Mobile), wird nicht eingesetzt, da das aktuelle ATOSS Cloud HTTPS-Zertifikat von DigiCert Global Root G2 (RapidSSLTLS RSA CA G1) ausgestellt ist.

4.6 Logging

In der Produktivversion der ATOSS Time Control (Mobile) werden folgende Logging-Varianten eingesetzt:

System-Log	nein
Remote-Log	nein
File-Log	ja
Crashlytics	nein
Andere	nein

Hinweis: Um Fehler zu finden, kann der gesamte Kommunikationsweg von der ATOSS Time Control (Mobile) zur ATC geloggt werden. Die Aktivierung der Protokollierung kann für jede Kommunikationskomponente einzeln erfolgen.

Bei den geloggten Daten handelt es sich um Nutzungsdaten (siehe *Arten personenbezogener Daten* auf Seite 10). Die Aktivierung des File-Logs erfolgt durch einen Systemadministrator.

4.7 In-App-Browser-Engine

In ATOSS Time Control (Mobile) wird ein In-App-Browser zum Anzeigen der Anmeldeseite (nur bei Nutzung von *OIDC*) und zur Anzeige der Datenschutzerklärung eingesetzt.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

5 Bereitstellung der Anwendung

Zur Bereitstellung der Anwendung finden Sie folgende Unterthemen:

- *Sicherheit des Betriebssystems* auf Seite 13
- *Cloud-Lösung* auf Seite 13
- *Bezug über App-Stores* auf Seite 13
- *ATOSS Time Control (Mobile)-Berechtigungen* auf Seite 13

5.1 Sicherheit des Betriebssystems

ATOSS Time Control (Mobile) kann nicht erkennen, ob es sich um eine unsichere Version des Betriebssystems handelt, und ist in einem solchen Fall nicht in der Lage, die Funktion zu blockieren.

5.2 Cloud-Lösung

Für die Cloud-Lösung gilt, dass bei einem Update von ATOSS Time Control (Mobile) über die App-Stores nicht zwangsweise das ATC-Release auf dem Server ebenfalls aktualisiert werden muss. Umgekehrt gilt auch, dass bei der Aktualisierung des ATC-Releases auf dem Server nicht unbedingt die App-Version ebenfalls aktualisiert werden muss. Unabhängig davon empfiehlt ATOSS in der Regel das Verwenden der neuesten App-Version und auch eines aktuellen ATC-Releases. Bei CLOUD24/7 ist dies automatisch der Fall.

Prinzipiell gilt: ATOSS Time Control (Mobile) ist versionsunabhängig und funktioniert mit den dafür freigegebenen ATC-Releases. Gegebenenfalls ist es erforderlich, für ATOSS Time Control (Mobile) ein Update aus den Stores zu beziehen.

5.3 Bezug über App-Stores

ATOSS Time Control(Mobile) wird über die offiziellen App-Stores 'Apple App Store' oder für Android-Geräte von 'Google Play' zum Herunterladen bereitgestellt:

- Google Play: *https://play.google.com/store/apps/details?id=com.atoss.atc.mobile*
- Apple App Store: *https://apps.apple.com/de/app/atoss-time-control/id1615949833*

Installationsvoraussetzungen

Weitere Informationen zu den Installationsvoraussetzungen finden Sie im Dokument 'Systemfreigaben und Voraussetzungen' unter 'ATOSS Time Control (Mobile)'.

5.4 ATOSS Time Control (Mobile)-Berechtigungen

ATOSS Time Control (Mobile) erhält folgende Berechtigungen auf dem Gerät:

Name und Art der Berechtigung	Android	iOS	Zugriff auf personenbezogene Daten möglich?
Verbindung mit dem Internet	durch das Betriebssystem erlaubt	durch das Betriebssystem erlaubt	nein

ATOSS CSD Software GmbH, Copyright 2023

Name und Art der Berechtigung	Android	iOS	Zugriff auf personenbezogene Daten möglich?
Informationen über Netzwerke und WIFI-Netzwerke	per Standardeinstellung erlaubt	nein	nein
Kamera, Bilder	nein	nein	ja Zum Erzeugen von Bildern für zukünftige Funktionen. Aktuell wird diese Berechtigung **nicht** genutzt (Stand: Oktober 2022).
Bildergalerie	nein	nein	ja Zum Erzeugen von Bildern für zukünftige Funktionen. Aktuell wird diese Berechtigung **nicht** genutzt (Stand: Oktober 2022).
Location Services	ja	ja	Wird bei Verwendung von GPS-Stempelungen verwendet. GPS-Koordinaten werden nur zum Abgleich verwendet und nicht gespeichert.
Push-Benachrichtigungen	per Standardeinstellung erlaubt	ja	**Hinweis:** Für Android muss diese Erlaubnis vom Benutzer über die Einstellungen des Mobilgeräts explizit ausgeschaltet werden.
Biometrische Anmeldung	per Standardeinstellung erlaubt	ja	Entsperren von ATOSS Time Control (Mobile) über Touch ID und Face ID

Es werden nur Berechtigungen, die für die Funktion des ATOSS Time Control (Mobile) zwingend erforderlich sind, eingefordert.

Vor dem Erteilen der Berechtigung wird eine (ausreichende) Einwilligung des Nutzers abgefragt (siehe § 13 Abs. 2, 3 TMG)

ATOSS CSD Software GmbH, Copyright 2023

6 ATOSS Time Control (Mobile) verwenden

Zu diesem Thema finden Sie folgende Unterthemen:

- *Anmeldung* auf Seite 15
- *Zugriffsschutz und Kennwörter* auf Seite 16
- *Push-Benachrichtigungen* auf Seite 16
- *Screenshots* auf Seite 16
- *Deaktivierung per Fernzugriff* auf Seite 17

6.1 Anmeldung

Eine Anmeldung an ATOSS Time Control (Mobile) erfolgt initial durch Eingeben der Login-Daten. Die Anmeldung bleibt bestehen, solange sich der Benutzer nicht aktiv über **Profil** > **Abmelden/Benutzer wechseln**abmeldet.

Wenn das mobile Endgerät das Anmelden mit biometrischen Daten (Fingerabdruck oder Gesichtserkennung) unterstützt und diese Verfahren auf dem Gerät aktiviert sind, wird der Benutzer bei der initialen Anmeldung gefragt, ob diese alternativen Verfahren eingesetzt werden sollen. Als Fallback-Lösung steht die Eingabe einer 4-stelligen PIN zur Verfügung.

Als Mindestanforderung zur Anmeldung an ATOSS Time Control (Mobile) ist das Festlegen einer vierstelligen PIN erforderlich.

Für die Anmeldung an ATOSS Time Control (Mobile) stehen folgende Verfahren zur Verfügung:

- PIN (verpflichtend)
- Fingerabdruck (optional, wenn unterstützt und Berechtigung vorhanden)
- Gesichtserkennung (optional, wenn unterstützt und Berechtigung vorhanden)

Nach erfolgter initialer Anmeldung kann ATOSS Time Control (Mobile) jederzeit und unabhängig von einer bestehenden Internetverbindung gestartet werden. Im Offlinefall stehen jedoch nur bestimmte Funktionen (z. B. Stempelung durchführen) zur Verfügung. Um die ATOSS Time Control (Mobile) Offline nutzen zu können, ist es erforderlich, dass der Nutzer bereits angemeldet ist.

Die Anmeldung für Cloud-Kunden mit entsprechend gebuchtem Service und der dazugehörigen Einrichtung besteht aus zwei Teilen: der Authentifizierung und der Autorisierung.

Authentifizierung

Anmelden mit Open ID Connect

Hinweis: Die folgende Authentifizierung erfolgt nur bei Einsatz des kostenpflichtigen IAM-Services.

Die Anmeldung an ATOSS Time Control (Mobile) erfolgt über das *OIDC*-Protokoll gegen den *IAM*-Service bzw. den *Identity Provider (IdP)* auf Seite 22 des Kunden. Bei der Anmeldung wird dem Benutzer eine Anmeldeseite angezeigt, die vom IdP des Kunden stammt. Hier gibt der Benutzer seinen Benutzernamen und sein Passwort ein. Wenn dieser Schritt erfolgreich durchgeführt ist, hat der Benutzer im weiteren Verlauf der Anmeldung eine Identität in Form eines *Zugriffs-Tokens*, die von der ATC als Service Provider überprüft wird.

Anmelden ohne IAM-Service

Die Anmeldung mit ATOSS Time Control (Mobile) ohne IAM-Service erfolgt durch Eingabe des Benutzernamens (Nummer oder Alias) sowie des Passworts.

ATOSS CSD Software GmbH, Copyright 2023

6.2 Zugriffsschutz und Kennwörter

Anmelden mit Open ID Connect

Hinweis: Die folgende Authentifizierung erfolgt nur bei Einsatz des kostenpflichtigen IAM-Services.

Da die Authentifizierung bei Cloud-Installationen und vorhandenem ATOSS IAM-Service komplett über den *IdP* des Kunden abgewickelt wird, gelten auch die dort getroffenen Einstellungen bezüglich der Kennwortsicherheit (Länge und Zeichenkombination). Gegebenenfalls vorgenommene Einstellungen innerhalb der ATOSS Time Control greifen hier nicht.

Um ein *Shoulder-Surfing* auf Seite 23zu verhindern, wird das Kennwort bei der Eingabe im System-Browser von ATOSS Time Control (Mobile) maskiert.

Da die Anmeldung über den System-Browser des mobilen Endgeräts abläuft, hat ATOSS Time Control (Mobile) keinen Zugriff auf das eingegebene Kennwort.

Andere gerätebezogene Daten (z. B. *IMEI-Nummer* auf Seite 22) werden nicht als Identifizierungswert im Rahmen der Authentifizierung verwendet.

Anmelden ohne IAM-Service

Kennwörter werden geschützt, da sie über starke Hashes in der Datenbank abgespeichert werden.

Um ein *Shoulder-Surfing* auf Seite 23zu verhindern, wird das Kennwort bei der Eingabe in ATOSS Time Control (Mobile) maskiert.

Deaktivieren eines Benutzerkontos

Anmelden mit Open ID Connect

Hinweis: Die folgende Authentifizierung erfolgt nur bei Einsatz des kostenpflichtigen IAM-Services.

Ein Benutzerkonto wird ausschließlich über den IdP des Kunden deaktiviert.

Anmelden ohne IAM-Service

Innerhalb des Browserclients können Mitarbeiter inaktiv gesetzt oder gelöscht werden.

Entziehen/Ändern der Berechtigungen innerhalb der ATC

Die Zugriffsberechtigungen für einen Benutzer (Autorisierung) können durch Ändern der entsprechenden Berechtigungen in der ATOSS Time Control angepasst werden.

6.3 Push-Benachrichtigungen

Die Verarbeitung der Daten von ATOSS Mobile-Kunden erfolgt auf Basis des in der Auftragsverarbeitungsvereinbarung (*AVV* auf Seite 21) niedergelegten Standards ab Einsatz des Releases 10.5 mit aktuellem Service Release der ATOSS Time Control.

Push-Benachrichtigungen sind nur verfügbar, wenn diese mithilfe eines Skriptes umgesetzt wurden.

Der Mechanismus der Push-Benachrichtigungen wird im Diagramm unter *Systemarchitektur (ATC in der Cloud)* auf Seite 5 mit dem Schritt 9 abgebildet.

6.4 Screenshots

Das Erstellen von Screenshots mit Funktionen des Betriebssystems kann nicht unterbunden werden.

ATOSS CSD Software GmbH, Copyright 2023

6.5 Deaktivierung per Fernzugriff

Für den Fall, dass ein Gerät verloren geht, gestohlen oder gehackt wird, ist eine Deaktivierung von ATOSS Time Control (Mobile) per Fernzugriff bzw. eine Fernlöschung nicht möglich.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

7 Datenschutzerklärung

Weitere Informationen finden Sie in der Datenschutzerklärung unter *https://www.atoss.com/de/datenschutzerklaerung-fuer-die-app-atoss-time-control-mobile*.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023

8 Glossar

Das Glossar enthält Definitionen von wichtigen und häufig verwendeten Begriffen.

8.1 AVV

Auftragsverarbeitungsvereinbarung: Dokument 'Vereinbarung über die Datenverarbeitung im Auftrag'.

8.2 Europäischer Wirtschaftsraum (EWR)

Der Europäische Wirtschaftsraum (EWR) wurde 1994 mit dem Ziel eingerichtet, die EU-Bestimmungen über den Binnenmarkt auf die Länder der Europäischen Freihandelszone (EFTA) auszudehnen. Norwegen, Island und Liechtenstein gehören dem EWR an. Die Schweiz ist Mitglied der EFTA, gehört aber nicht zum EWR. Die EU und ihre EWR-Partner (Norwegen und Island) sind zudem durch verschiedene 'nördliche Politikbereiche' und Foren mit Schwerpunkt auf den sich schnell entwickelnden nördlichen Ausläufern Europas und der gesamten Arktis verbunden.

8.3 Google Remote Procedure Calls (gRPC)

Google Remote Procedure Calls (gRPC) ist ein Open Source Remote Procedure Call (RPC) Framework. Dieses wurde ursprünglich von Google entwickelt. Es verwendet das HTTP/2-Protokoll für den Transport von Datenströmen. Für die Struktur sowie die Verarbeitung von Daten werden Protocol Buffer eingesetzt.

8.4 Hypertext Transfer Protocol Secure (HTTPS)

Kommunikationsprotokoll im World Wide Web, mit dem Daten abhörsicher übertragen werden können (Transportverschlüsselung).

HTTPS wurde von der Firma Netscape entwickelt und zusammen mit SSL 1.0 erstmals 1994 mit deren Browser veröffentlicht. Technisch definiert wurde es als URI-Schema, eine zusätzliche Schicht zwischen HTTP und TCP.

8.5 Identity and Access Management (IAM)

Das Identity and Access Management (IAM) stellt einen Oberbegriff für alle Prozesse und Anwendungen dar, die für die Administration von Identitäten und die Verwaltung von Zugriffsrechten auf verschiedene Applikationen, Systeme und Ressourcen zuständig sind. IAM sorgt in Unternehmen für eine zentrale Verwaltung von Identitäten und Zugriffsberechtigungen. Zentrale Funktionen des IAM sind Authentifizierung und gegebenenfalls Autorisierung der User.

Die wichtigste Funktion des Identitäts- und Zugangsmanagements ist die Verwaltung von Benutzerkonten und Zugangsberechtigungen. Um Zugangsberechtigungen zu erteilen, muss das System die Benutzer authentifizieren und autorisieren. Bei der Authentifizierung beweist der Benutzer dem System, dass er derjenige ist, der er vorgibt zu sein. Dazu können einfache Abfragen von Benutzername und Passwort verwendet werden, aber auch Multi-Faktor-Verfahren mit Sicherheits-Token oder biometrischen Merkmalen. Wenn die Identität des Benutzers zweifelsfrei feststeht, wird er im nächsten Schritt autorisiert. Die Autorisierung legt fest, zu welchen Systemen oder Ressourcen der Benutzer Zugang erhält. Die Autorisierung basiert auf mehr oder weniger komplexen Regeln und Rollenkonzepten, die in der Regel in einer Datenbank gespeichert sind. Diese Regeln und Rollen können frei definiert werden oder hängen von der Organisationsstruktur des Unternehmens und dem Arbeitsbereich des Benutzers ab.

ATOSS CSD Software GmbH, Copyright 2023

8.6 Identity Provider (IdP)

Ein Identitätsanbieter (IdP) speichert und verwaltet die digitalen Identitäten der Benutzer. Man kann sich einen IdP als eine Gästeliste für digitale und in der Cloud gehostete Anwendungen vorstellen. Ein IdP kann zum Beispiel Benutzeridentitäten anhand von Kombinationen aus Benutzernamen und Passwort überprüfen. Alternativ kann er einem anderen Dienstanbieter, z. B. einem SSO-Dienst, eine Liste von Benutzeridentitäten zur Verfügung stellen, um diese zu überprüfen.

Technisch gesehen kann ein IdP jede Entität authentifizieren, die mit einem Netz oder System verbunden ist, einschließlich Computern und anderen Geräten. Jede von einem IdP gespeicherte Entität wird als 'Prinzipal' (anstelle von 'Benutzer') bezeichnet. Am häufigsten werden IdPs beim Cloud Computing zur Verwaltung von Benutzeridentitäten eingesetzt.

8.7 IMEI-Nummer

Jedes mobile Gerät mit einem Mobilfunkchip besitzt eine sogenannte IMEI-Nummer. Die Abkürzung steht für 'International Mobile Equipment Identity'. Die Nummer besteht aus 15 Ziffern und ist für jedes Gerät weltweit einmalig. Diese Gerätekennung ermöglicht es, ein mobiles Gerät eindeutig zuzuordnen.

8.8 Man-in-the-Middle-Angriff (MITM-Angriff)

Auch: 'Janusangriff', nach dem doppelgesichtigen Janus der römischen Mythologie.

Angriff in Rechnernetzen. Der Angreifer steht dabei entweder physisch oder heute meist logisch zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Die Janusköpfigkeit des Angreifers besteht darin, dass er den Kommunikationspartnern vortäuscht, das jeweilige Gegenüber zu sein.

8.9 On Premises

Auch: On Prem, deutsch: 'in den eigenen Räumlichkeiten', 'vor Ort' oder 'lokal', Gegenteil von: 'Auslagerung in die Cloud'.

Nutzungs- und Lizenzmodell für serverbasierte Computerprogramme (Software). Bis ca. 2010 war die lokale Nutzung bzw. die Lizenzierung für die lokale Nutzung von Software der Normalfall und hatte daher keine besondere Bezeichnung. Seitdem die lokale Nutzung zunehmend von 'Software as a Service' (SaaS) oder Cloud Computing verdrängt wird, ist der Begriff Off-Premises als Antonym entstanden.

Bei kommerzieller On Prem-Software erwirbt oder mietet der Lizenznehmer Software und betreibt diese in eigener Verantwortung auf eigener Hardware, ggf. in einem eigenen Rechenzentrum oder auf gemieteten Servern eines fremden Rechenzentrums, in jedem Fall also auf Hardware, die nicht vom Anbieter der Software bereitgestellt wird. Neben den Anschaffungs- und Betriebskosten fallen hierbei normalerweise zusätzliche Wartungsgebühren an, um den Kunden an der Weiterentwicklung der Software durch deren Anbieter zu beteiligen oder die weitere Unterstützung durch den Hersteller abzusichern.

Bei Open-Source-Software besteht kein Gewährleistungsanspruch. Der Kunde verlässt sich darauf, dass die Entwicklergemeinschaft für die Software Support leistet, sie weiterentwickelt und Fehler behebt. Alternativ kann er gesondert Support bei entsprechenden Dienstleistern aus dem Open-Source-Umfeld einkaufen. Betrieb und Anpassungsmöglichkeiten verhalten sich ähnlich wie bei kommerzieller Software.

8.10 OpenID Connect (OIDC)

OpenID Connect (OIDC) ist eine einfache Authentifizierungsschicht, die auf dem Protokoll OAuth 2.0 aufbaut. Der Standard wird durch die OpenID Foundation überwacht.

ATOSS CSD Software GmbH, Copyright 2023

OpenID Connect ermöglicht es Clients, die Identität des Endbenutzers auf der Grundlage der von einem Autorisierungsserver durchgeführten Authentifizierung zu überprüfen und grundlegende Profilinformationen über den Endbenutzer auf interoperable und REST-ähnliche Weise zu erhalten. Mit OpenID Connect können Clients aller Art, einschließlich webbasierter, mobiler und JavaScript-Clients, Informationen über authentifizierte Sitzungen und Endbenutzer anfordern und empfangen.

8.11 REST-Schnittstelle

Die Representational State Transfer-Schnittstelle ist eine Programmierschnittstelle, die den Austausch von Daten auf verteilten Systemen, insbesondere für Web-Services, ermöglicht.

Die REST-Schnittstelle nutzt HTTP-Anfragen, um per `PUT`, `GET`, `POST` und `DELETE` auf Informationen zuzugreifen. Sie erlaubt das Verbinden mit Cloud-Diensten und ermöglicht eine Interaktion. Im Wesentlichen geht es darum, Transaktionen aufzuschlüsseln und anhand dieser eine gewisse Anzahl kleiner Module zu erstellen.

8.12 Shoulder-Surfing

Dient dem Ausspähen von Passwörtern, der persönlichen Identifikationsnummer (PIN) oder anderen sensitiven Informationen. Beim Shoulder-Surfing (Deutsch: 'über die Schulter schauen') wird die Eingabefolge von unautorisierten Dritten auf Tastaturen beobachtet, um sie später für den unerlaubten Zugriff auf das Internet, auf Computersysteme, Konten oder in Datenbanken zu verwenden. Shoulder-Surfing kann bei Eingabe der PIN-Nummer in Geldautomaten, beim Einloggen in Konten über Smartphones oder über den Desktop, bei Sicherheitscodes oder bei anderen sensitiven Eingabedaten angewendet werden.

8.13 Transport Layer Security (TLS)

Deutsch: 'Transportschichtsicherheit', weitläufiger bekannt unter der Vorgängerbezeichnung 'Secure Sockets Layer' (SSL).

Hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Die letzte Version des SSL-Protokolls war die Version 3.0. Danach wurde das Protokoll unter dem neuen Namen TLS, beginnend mit Version 1.0, weiterentwickelt und standardisiert.

Version	Erscheinungsjahr	Bemerkungen
SSL 1.0	1994	Wird nicht mehr unterstützt.
SSL 2.0	1995	Wird nicht mehr unterstützt.
SSL 3.0	1996	Wird nicht mehr unterstützt.
SSL 3.1 bzw. TLS 1.0	1999	Wird nicht mehr unterstützt.
TLS 1.1	2006	Wird nicht mehr unterstützt.
TLS 1.2	2008	Ältere Version, wird noch unterstützt.
TLS 1.3	2018	Aktuelle Version

8.14 Zugriffs-Token

Ein Zugriffs-Token (Englisch: Access Token) ist eine Zeichenfolge, die einen Benutzer identifiziert und den Zugriff auf andere Anwendungen authentifiziert.

ATOSS CSD Software GmbH, Copyright 2023

ATOSS CSD Software GmbH, Copyright 2023