SIEMENS

Datenblatt

Security Manager

Security Manager / Mobile Access ist ein cloud-basiertes Angebot innerhalb von Building X, mit dem Sie Türen mithilfe Ihres Smartphones öffnen können.

- Virtueller Berechtigungsnachweis für Kartenlesegeräte
- Zugang mit Berechtigungsnachweis für intelligente Schlösser
- Apple Wallet Berechtigungsnachweis
- Mobile App SDK
- Vor-Ort-Virtual Credentials für SIPORT
- Mobile Ausweisverwaltung
- Foto-Upload
- Verbinden Sie ACC-AP Tür-Controller
- Verbinden Sie vor Ort befindliche Zugangskontrollsysteme
- Activity Log

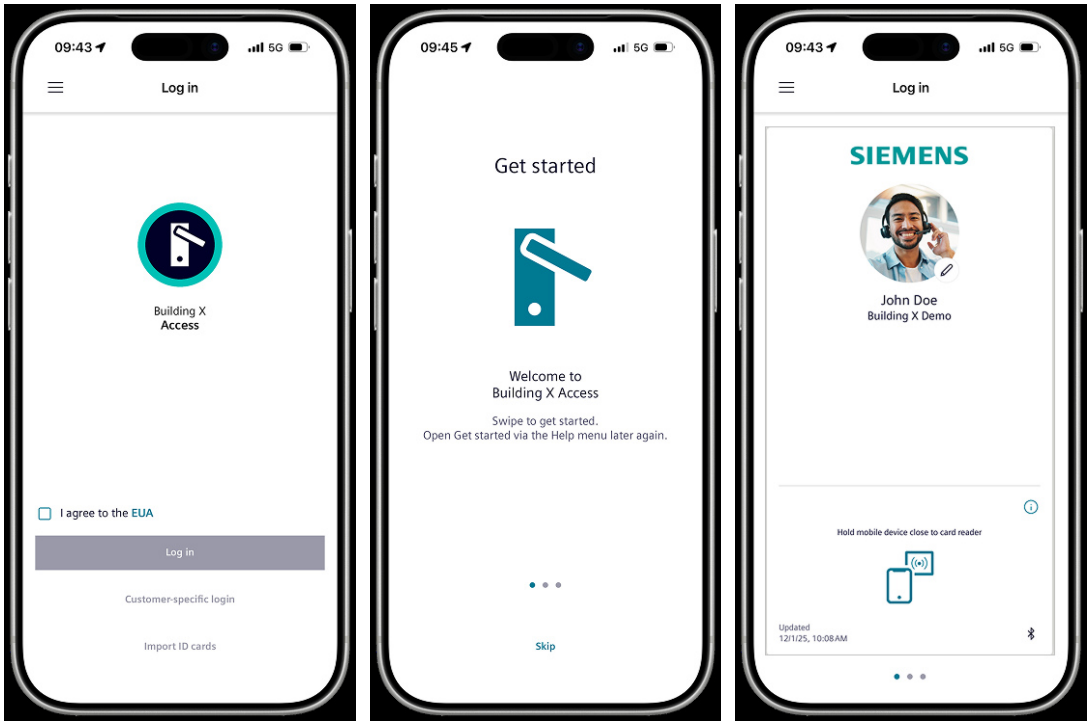
URL

Web: securitymanager.siemens.com

iOS: https://apps.apple.com/app/building-x-access/id1483078094

Android: https://play.google.com/store/apps/details?id=com.siemens.accessmobile&hl=gsw

Virtueller Berechtigungsnachweis für Kartenlesegeräte



Verwendung des Smartphones des Kunden zum Öffnen von Türen, die durch einen LEGIC Connect-fähigen Kartenleser gesichert sind, der entweder an einen SiPass- oder SIPORT-Controller oder an einen mit der Cloud verbundenen ACC-AP-Türcontroller angeschlossen ist.

Es gelten die folgenden Bedingungen:

- Ein Nutzer kann die Geräte bis zu dreimal pro Jahr ohne zusätzliche Kosten wechseln.
- Die Deaktivierung und Reaktivierung eines Geräts verursacht keine zusätzlichen Kosten.
- Die Meldung eines gestohlenen Geräts und seine Reaktivierung nach dem Wiederauffinden verursachen keine zusätzlichen Kosten.
- Das Deaktivieren und erneute Aktivieren der Option "Virtuelle Berechtigungsnachweise aktivieren" im Sicherheitsmanager / Identitäten erzeugt neue virtuelle Berechtigungsnachweise für alle Geräte des Benutzers, was zu zusätzlichen Kosten führt.

Zugang mit Berechtigungsnachweis für intelligente Schlösser

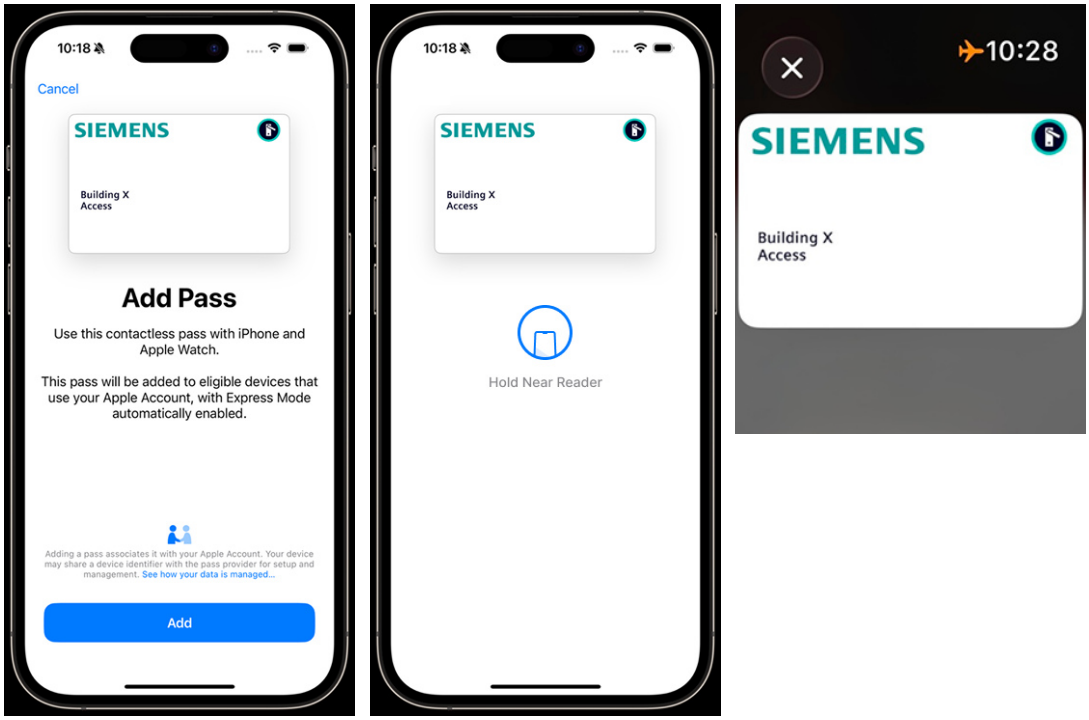
Verwendung des Smartphones des Kunden oder einer physischen Karte zum Öffnen von Türen, die mit SALTO Smartlocks gesichert sind.

Es gelten die folgenden Bedingungen:

- Ein Nutzer kann die Geräte bis zu dreimal pro Jahr ohne zusätzliche Kosten wechseln.
- Die Deaktivierung und Reaktivierung eines Geräts verursacht keine zusätzlichen Kosten.
- Die Meldung eines gestohlenen Geräts und seine Reaktivierung nach dem Wiederauffinden verursachen keine zusätzlichen Kosten.

Apple Wallet Berechtigungsnachweis

iPhone: Apple Watch:



Apple Wallet ermöglicht den sofortigen Zugriff, wenn der Nutzer sein iPhone oder seine Apple Watch in die Nähe eines kompatiblen Kartenlesegeräts hält. Die Verzögerung, die bei Bluetooth Low Energy (BLE) Systemen auftritt, entfällt.

Für die Nutzung des Dienstes mit Apple Wallet sind zusätzliche Geschäftsbedingungen erforderlich, die im Voraus unterzeichnet werden müssen. Für weitere Informationen wenden Sie sich bitte an securitymanager.si@siemens.com.

Mobile App SDK

Verwendung der Mobile App SDK zur Integration der mobilen Zugriffsfunktionen in Ihre eigene mobile Anwendung.

Vor-Ort-Virtual Credentials für SIPORT

Unterstützung von virtuellen Anmeldedaten vor Ort durch Offline-Import für SIPORT-Kunden.

Mobile Ausweisverwaltung

Der Servicetechniker kann Folgendes konfigurieren:

- Wie viele mobile Berechtigungsnachweise können einer Identität zugewiesen werden
- Wie viele mobile Zugangsdaten können gleichzeitig aktiviert werden
- Wie viele mobile Geräte können von einem Nutzer gleichzeitig aktiviert werden, um zusätzliche Kosten zu vermeiden

Security Manager kann virtuelle IDs und virtuelle Zugangsdaten aktivieren/deaktivieren:

- Mit dem Flag "Enable virtual ID card in Building X Access app" kann die virtuelle ID-Karte (Ausweis) für eine bestimmte Identität aktiviert oder deaktiviert werden. Wenn sie aktiviert ist, zeigt die Building X Access-App dem Benutzer die virtuelle ID-Karte sowie alle verfügbaren digitalen Schlüssel an. Ist sie deaktiviert, werden der virtuelle Ausweis und alle digitalen Schlüssel ausgeblendet, und der Zugang zu den Türen ist nicht möglich.

Foto-Upload

Mit der Building X Access-App können Nutzer ganz einfach ein neues Profilbild hochladen und ihr Foto in der App, im Identitätsmanagement und auf gedruckten Zugangsausweisen anzeigen lassen.

Connect ACC-AP Door Controller

Verbinden Sie bis zu 10 Türen mit einem Tür-Controller ACC-AP über Building X Devices.

Verbinden Sie vor Ort befindliche Zugangskontrollsysteme

Anschluss an bis zu 5 SiPass- und SIPORT-Systeme. Anbindung von 3rd Party PACS über das PACS SDK. Exportierte Profilbilder aus SiPass- und SIPORT-Systemen können manuell über den Connection Manager importiert werden.

Hinweis: Sync Agent 2.x kann nicht auf Servern installiert werden, auf denen bereits ein anderer Siemens Building Connect Agent installiert ist.

PACS SDK

Verwenden Sie das PACS SDK, um Zutrittskontrollsysteme von Drittanbietern integrieren zu können.

Activity Log

Der Activity Log bietet eine überprüfbare Dokumentation der prüfungsrelevanten Aktionen, wobei sowohl vom Benutzer initiierte als auch systembedingte Änderungen erfasst werden.

Zu den derzeit verfolgten Aktivitäten gehören:

- Benutzeraktionen innerhalb der Punktvertikalen (z. B. Ändern von Punktwerten)
- Benutzeraktionen innerhalb der Benutzervertikale (z. B. Hinzufügen von Benutzern, Zuweisen von Gruppen)
- Vollständige Aktivitätsprotokolle von Security Manager
- Vollständige Aktivitätsprotokolle von Visitor Manager

Benutzerverwaltung

Bietet rollenbasierte Zugriffskontrolle. Die Kundschaft aktiviert das Abo in der Building X Accounts-Applikation. Benutzer und Rollenzuweisungen werden im Security Manager verwaltet (linker Navigationsbereich, Kategorie: Zutritt, Menübefehl: Identitäten).

Datenhosting und Datennutzung

Hostet und verarbeitet personenbezogene und nicht-personenbezogene Daten in Rechenzentren in Europa. Informationen zur Verarbeitung personenbezogener Daten und Orte finden Sie in den Data Privacy Terms.

Abo

Der Aboplan richtet sich nach der Vereinbarung zwischen der Kundschaft und Siemens.

1) Standard-Aboplan, falls die Kundschaft das Abo über den Siemens Online-Shop kauft

Security Manager / Mobile Access					
	Mobiler Zugang - Virtueller Ausweis für Kartenleser	**Mobiler Zugang - Zugang mit Berechtigungsnachweis für intelligente Schlösser**	**Mobiler Zugang - Apple Wallet Credential**	**Connectivity – Physical Access Control Systems (PACS)**	**Connectivity – Cloud-based Access Control**
Voraussetzung	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) Für die Verwendung mit der cloudbasierten Zugangskontrolle müssen die folgenden Abos aktiv sein: ● Connectivity – Cloud-based Access Control ● Building Access Essential or Building Access Standard ● Foto-Upload	Eines der folgenden Abos muss aktiv sein: ● Connectivity – Cloud-based Access Control ● Building Access Essential or Building Access Standard ● Foto-Upload	Für die Verwendung mit PACS muss das folgende Abo aktiv sein: ● Connectivity – Physical Access Control Systems (PACS) Für die Verwendung mit der cloudbasierten Zugangskontrolle müssen die folgenden Abos aktiv sein: ● Connectivity – Cloud-based Access Control ● Building Access Essential or Building Access Standard	-	

Security Manager / Mobile Access					
	Mobiler Zugang - Virtueller Ausweis für Kartenleser	**Mobiler Zugang - Zugang mit Berechtigungsnachweis für intelligente Schlösser**	**Mobiler Zugang - Apple Wallet Credential**	**Connectivity – Physical Access Control Systems (PACS)**	**Connectivity – Cloud-based Access Control**
Funktionen	Benutzerverwaltung Activity Log				
	Virtueller Berechtigungsnachweis für Kartenlesegeräte Mobile App SDK Mobile Ausweisverwaltung Vor-Ort-Virtual Credentials für SIPORT	Zugang mit Berechtigungsnachweis für intelligente Schlösser Mobile App SDK Hochladen von Porträtbildern mit dem Smartphone Mobile Ausweisverwaltung	Apple Wallet Berechtigungsnachweis	Verbinden Sie vor Ort befindliche Zugangskontrollsysteme PACS SDK	Verbinden Sie ACC-AP Tür-Controller
Abometriken	pro Gerät und Jahr Das Abo kann in Paketen von 1 Gerät		pro 1 Apple-ID-Benutzer pro Jahr erworben werden Das Abo kann in Paketen von 1 Apple-ID-Benutzer	pro 1 Tür pro Jahr erworben werden Das Abo kann in Paketen von 1 Tür erworben werden	
Abodauer	Jährliche, automatische Verlängerung				
Abrechnungszeit	Jährlich, Vorauszahlung				
Upscaling	Gültig ab sofort, anteilige Abrechnung				
Downscaling/ Kündigung	Gültig zum Ende der Abolaufzeit				
Angeschlossene Geräte	Separat zu erwerben				
Zugelassene Benutzer	Bis zu 10.000; Erweiterte Nutzung				

Das Abo für Security Manager / Mobile Access entspricht dem regulären, skalierbaren Angebot für diesen Cloud-Dienst. Die Abolaufzeit beträgt zwölf (12) Monate mit automatischer Verlängerung; die Gebühr für den Cloud-Dienst wird im Voraus bezahlt. Für das Abo kann jederzeit ein Upgrade erworben werden, wobei die Gebühren anteilig berechnet werden. Zu Ende der aktuellen Abolaufzeit kann der Cloud-Dienst auch herabgestuft werden. Die Abogebühr wird an den kommenden Abrechnungszeitraum angepasst. Der Cloud-Dienst kann jederzeit mit Wirkung zum Ende der aktuellen Abolaufzeit gekündigt werden.

Die Kundschaft kann die erforderlichen, verbundenen Geräte separat erstehen.

Mit einer erweiterten Nutzung kann die Kundschaft Partnern und Drittparteien den Zugriff und die Nutzung der Cloud-Dienste mit den in den Nutzungsbedingungen aufgeführten Rechten gewähren.

2) Benutzerdefiniertes Abo

Abos, die nicht im Siemens Online-Shop gekauft werden, sind benutzerdefinierte Abos. Im Rahmen eines benutzerdefinierten Abos werden die Details zu Funktionen, Abo-Metrik, Laufzeit, Abrechnung, Up- und Downscaling, verbundenen Geräten sowie zugelassenen Identitäten in der Vereinbarung zwischen dem Kunden und Siemens festgelegt.

Für kundenspezifische Anwendungsfälle wie beispielsweise bei einer sehr hohen Anzahl Türen und Identitäten pro Standort (z. B. mehr als 10.000 Identitäten und/oder 1.000 Türen), kann sich die Kundschaft für ein individuelles Abo an den zuständigen Vertriebspartner wenden.

Voraussetzungen

Unterstützte verbundene Geräte

Der Cloud-Dienst ist zur Zeit mit den handelsüblichen verbundenen Geräten von Siemens kompatibel. Connected Devices ermöglichen dem Cloud Service den Datenaustausch mit der technischen Gebäudeinfrastruktur. Im Folgenden finden Sie eine Beschreibung der verfügbaren Connected Devices.

	Liste von unterstützten verbundenen Geräten
SIEMENS: SiPass	SiPass mit Sync Agent 2.x: Das Softwareprodukt SiPass läuft auf Windows-Computerhardware. Die unterstützte Softwareversion ist SiPass MP2.95 (HF11) oder höher. SiPass enthält mehrere Softwareapplikationen, die im Weiteren als "Software" bezeichnet werden und Gebäudedaten an den Cloud-Dienst übermitteln. Die folgenden Kartenleser unterstützen die Funktion des virtuellen Ausweises: ● Autec: XMP-TMC2170+XMP-TMC2180+XMP-TMC3070, XMP-TMC3080 Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC Apple Wallet Credential wird von allen ECP2-zertifizierten Kartenlesern unterstützt
SIEMENS: SIPORT	SIPORT mit Sync Agent 2.x: Das Softwareprodukt SIPORT läuft auf Windows-Computerhardware. Die unterstützte Softwareversion ist SIPORT V3.5.0.127 oder höher und SIPORT 3.4.1.321 oder höher. SIPORT enthält mehrere Softwareapplikationen, die im Weiteren als "Software" bezeichnet werden und Gebäudedaten an den Cloud-Dienst übermitteln. Die folgenden Kartenleser unterstützen die Funktion des virtuellen Ausweises: ● Autec: XMP-TMC2170+XMP-TMC2180+XMP-TMC3070, XMP-TMC3080 Apple Wallet Credential wird von allen ECP2-zertifizierten Kartenlesern unterstützt
SALTO Nebula Elektronikschloss	Neo-Zylinder, Neoxx-Vorhängeschloss, XS4 Original+, XS4 One und XS4 One S (nur Modelle, die HSE unterstützen), XS4 Mini, DBolt. **Einschränkung**: Es werden nur Schlösser ohne Tastenfeld unterstützt, da der Security Manager noch keine PIN-Funktionalität bietet.
SALTO Nebula Gateways	IQ3, IQ3 Mini
SIEMENS: ACC-AP	ACC-AP ACC-AP Die folgenden Kartenleser unterstützen die Funktion des virtuellen Ausweises: ● Autec: XMP-TMC2170+XMP-TMC2180+XMP-TMC3070, XMP-TMC3080 ● Elatec: Secustos SQ80 Legic, Secustos SQ80 K Legic, Secustos MU20 LEGIC, Secustos MU20 K LEGIC Apple Wallet Credential wird von allen ECP2-zertifizierten Kartenlesern unterstützt.

Um den Cloud-Service nutzen zu können, muss ein angeschlossenes Gerät vor Ort installiert, voll funktionsfähig und mit dem Internet verbunden sein. Der Kunde ist für die Bereitstellung des Connected Device vor Ort und alle damit verbundenen Kosten für die Bereitstellung des Cloud-Dienstes in Übereinstimmung mit der zugehörigen Dokumentation für das Connected Device verantwortlich.

Webbrowser und Anzeigegeräte

Für die Nutzung des Cloud-Dienstes wird Chrome empfohlen, aber auch andere Standardbrowser können eingesetzt werden. Für ein optimales Benutzererlebnis wird eine Bildschirmauflösung von 1920 x 1080 Pixel oder höher empfohlen.

Mobile Geräte

Für die Installation der mobilen App ist iOS 16.0 und höher oder Android 10 und höher erforderlich.

Internetverbindung

Die Bandbreite der Internetverbindung des Kunden bestimmt die Leistung des Cloud-Dienstes.

Bestellung

Um den Cloud-Dienst zum ersten Mal zu bestellen, muss die Kundschaft ein Angebot von seinem Siemens-Vertriebspartner anfordern.

Produktdokumentation

1) Produktdokumentation im Rahmen eines Standardabos

Allgemeine Vertragsdokumente	Links
Building X - Security Manager / Mobile Access Datenblatt	www.siemens.com/buildingx/data-sheet/de/security-manager-mobile-access
Ergänzende Richtlinien für Gebäudeprodukte	www.siemens.com/buildingx/data-sheet/supplemental-terms
General Software Terms and Cloud Supplemental Terms	https://www.siemens.com/si/cloud/terms
Base Terms International	https://www.siemens.com/si/cloud/terms
Zu akzeptierende Nutzungsrichtlinien von Siemens	https://www.siemens.com/si/cloud/terms
Min. Nutzungsbedingungen	www.siemens.com/buildingx/data-sheet/minimum-terms
Datenschutzbestimmungen	https://www.siemens.com/dpt/si
Datenschutz Anhang	https://www.siemens.com/dpt/si
EU Data Act	https://www.siemens.com/buildingx/terms

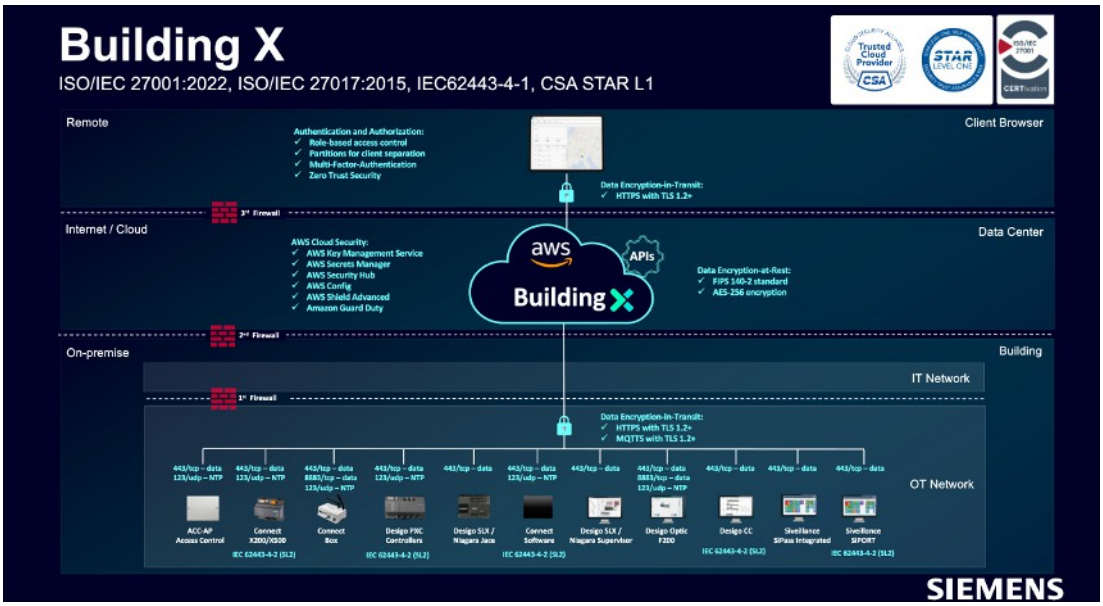
2) Produktdokumentation im Rahmen eines Benutzerdefinierten Abos

Die Vertragsdokumente und die Produktdokumentation werden im Angebot von Siemens an die Kundschaft aufgeführt.

3) Technische Dokumente

Technische Dokumente	Link
Building X- Online-Hilfe	www.siemens.com/buildingx/sid

Topologie



Die Topologie zeigt die Gesamtheit der Möglichkeiten für die Verbindung von Daten mit Gebäude X. Die für diesen digitalen Dienst verfügbaren Optionen finden Sie in der Liste der unterstützten angeschlossenen Geräte und der Softwarekonnektivität von Drittanbietern.

Für die Datenkommunikation zwischen den verbundenen Geräten vor Ort und der Cloud ist eine Internetverbindung erforderlich (von der Kundschaft bereitzustellen).

Spezifische Bedingungen

Allgemeine Geschäftsbedingungen für die Nutzung der Apple Wallet-Funktionalität

1. Als Voraussetzung für die Nutzung der Apple-Wallet-Funktionalität erhält der Kunde die Pass-Through-Bedingungen von Apple (einschliesslich der Apple-Markenrichtlinien) und stimmt diesen mit der Legic Identsystems AG mit Sitz in CH-8620 Wetzikon, Schweiz, zu.
2. Der Kunde stellt sicher, dass keiner seiner Nutzer durch die Nutzung der Apple-Wallet-Funktionalität gegen eine Nutzungsvereinbarung verstößt und wird die Nutzungsvereinbarung bei Bedarf ändern.
3. Der Kunde stellt die relevanten Führungskräfte, Kundenbetreuer und Ingenieure für die Teilnahme an Besprechungen (persönlich, per Telefon oder per Videokonferenz) zur Verfügung, die von Apple angefordert und von Siemens dem Kunden von Zeit zu Zeit mitgeteilt werden.

Verwendung mit hohem Risiko

Die Kundschaft erkennt an und stimmt zu, dass:

a) die Angebote nicht dazu bestimmt sind, für den Betrieb eines Hochrisikosystems oder innerhalb eines Hochrisikosystems verwendet zu werden, wenn das Funktionieren des Hochrisikosystems vom ordnungsgemäßen Funktionieren der Angebote abhängig ist; und

b) das Ergebnis der Verarbeitung von Daten durch die Nutzung der Angebote außerhalb der Kontrolle von Siemens liegt.

Servicelevel-Vereinbarung

Siemens ist gehalten, bei einem kommerziell zumutbaren Aufwand die Cloud-Dienste während eines jeden Monats bei einer Laufzeit von 98% verfügbar zu machen.

Ausnahmen:

a) Geplante Ausfallzeiten, vereinbarte Ausfallzeiten, Routine- und Notwartung,
b) Cyberangriffe,
c) öffentliche, Dritt- und/oder Kundschafts-Internet- und Kommunikationsnetzwerke,
d) Daten, Software, Hardware, Telekommunikation, Infrastruktur, Leistung, Build-Packs oder Netzwerkeinrichtungen anderer Hersteller als Siemens,
e) Nachlässigkeit seitens Kundschaft oder Nutzern beim Einsatz der Cloud-Dienste und/oder durch Nichteinhaltung der Anweisungen veröffentlicher Dokumentation,
f) Systemkonfigurationen und Plattformen anderer Hersteller, nicht unterstützt durch

Siemens,
g) Systemadministration, Aktionen, Befehle und Dateiübermittlungen von Kundschaft oder Nutzern,
h) Änderungen durch andere Parteien als Siemens,
i) nicht autorisierter Zugriff über Kundenanmeldeinformationen und/oder
j) alle weiteren, beliebigen Ausfälle ausserhalb der Kontrolle von Siemens.

Customer Support

Siemens bietet Helpdesk-Unterstützung. Die Kundschaft kann sich für weitere Informationen an seinen Siemens-Vertriebspartner wenden. Kunden können auch online eine Supportanfrage stellen: https://www.siemens.com/support-request.

Herausgegeben von
Siemens Schweiz AG
Smart Infrastructure
Global Headquarters
Theilerstrasse 1a
CH-6300 Zug
+41 58 724 2424
www.siemens.com/buildingtechnologies

Dokument-ID	A6V15573372_de--
Ausgabe	16.12.2025