Leistungsbeschreibung

Mobile ID

Inhaltsverzeichnis

1 Übersicht zum Service

Der Service Mobile ID ermöglicht Unternehmen und Anwendungsanbietern mit eigenen oder ausgelagerten (hosted) Applikationen oder Infrastrukturen die starke Authentisierung von einem personifizierten Mobile ID-Anschluss aus.

Der Service umfasst folgende Leistungen (detaillierte Definition, siehe Kapitel 3):

- Bereitstellen einer standardisierten Schnittstelle (basierend auf ETSI TS 102 204) für digital signierte Bestätigungen und/oder Willensbekundungen (als Webservices)
- Sicherstellen der Interoperabilität mit weiteren beteiligten Mobilfunkanbietern
- Distribution, Verwaltung und Lifecycle Management der für die starke Authentisierung notwendigen Token (SIM-Karte)
- 7x24 Service Desk und Support für den Anwendungsanbieter sowie dessen Nutzer
- Betrieb und Wartung der zugrunde liegenden Infrastruktur
- Beratung und Dienstleistungen, die für den serverseitigen Betrieb und die Nutzung notwendig sind
- Optional zum Service sind Geo Location, Mobile ID Token und Beratungsdienstleistungen verfügbar

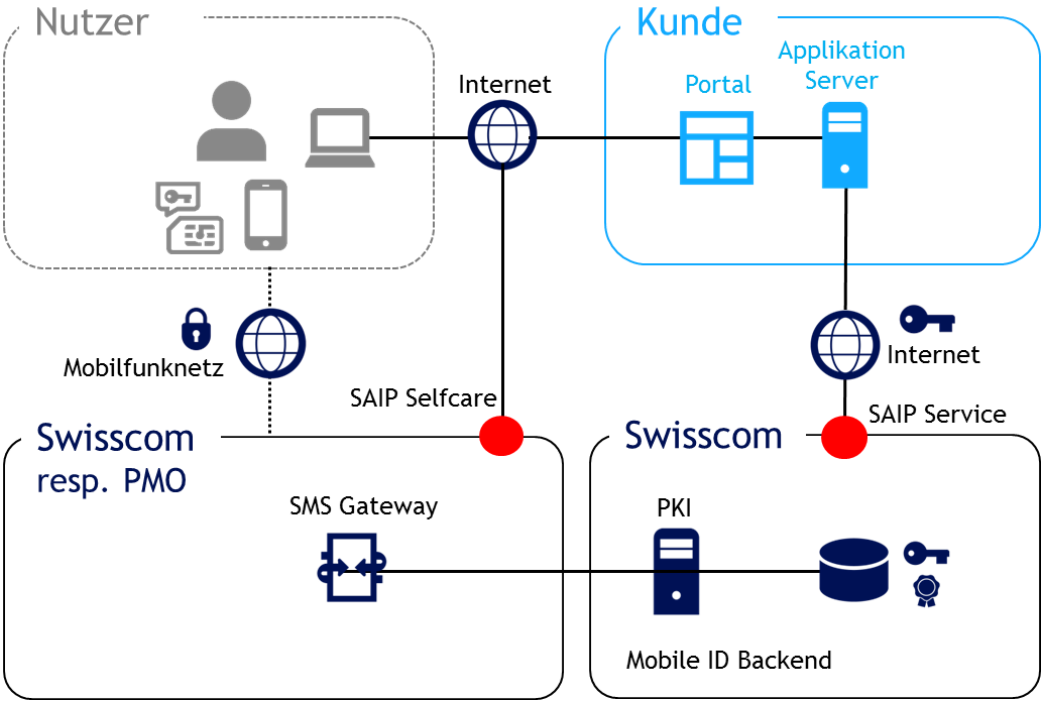
Der Service wird in den Rechenzentren von Swisscom in der Schweiz bereitgestellt, unter Berücksichtigung von angemessenen Sicherheitsanforderungen.

2 Definitionen

2.1 Service Access Interface Point SAIP

Der Service Access Interface Point (SAIP) ist der vertraglich vereinbarte, geografische und/oder logische Punkt, an dem ein Service dem Leistungsbezüger bereitgestellt, überwacht und die erbrachten Service Level ausgewiesen werden.

Folgende Darstellung verdeutlicht die Leistungen des Services und die darin verwendeten Leistungskomponenten:



Der SAIP Service ist für den Kunden (=Anwendungsanbieter) die Schnittstelle (vgl. 3.3), über welche die Anwendungen die Mobile ID Anfragen an das Swisscom Mobile ID Backend sendet und empfängt.

Der SAIP Selfcare ermöglicht dem Nutzer Zugriff auf das Online Selfcare Portal (vgl. Ziff 3.4), welches das zentrale Tool für die Verwaltung seiner Mobile ID darstellt. Dieser SAIP Selfcare ist abhängig vom Mobilfunkanbieter des Nutzers und wird entsprechnend von Swisscom oder von einem Drittanbieter (PMO) bereitgestellt.

2.2 Nutzungsmodelle

Der Service ist in zwei Nutzungsmodellen erhältlich, dem Business to Business (B2B) und dem Business to Consumer (B2C) Modell.

Nutzungsmodell	Beschreibung
B2B	Für Unternehmen, welche eine starke Authentisierung ihrer internen und externen Mitarbeitenden zum Eigenbedarf (d.h. unternehmensintern) nutzen.
B2C	Für Anwendungsanbieter, welche eine starke Authentisierungs-Lösung ihrer eigenen Kunden einsetzen. Dieses Modell dient somit ausschliesslich für Anwendungen, bei welchen externe Kunden der Anwendungsanbieter die Mobile ID nutzen.

Beide Modelle haben grundsätzlich dasselbe Preismodell, unterscheiden sich jedoch in den dafür zur Anwendung gelangenden Preisen. Der Service wird für beide Modelle gemäss Standardpreisliste abgerechnet.

2.3 Weitere Servicespezifische Definitionen

Nutzungsmodell	Beschreibung
PMO	PMOs (Participating Mobile Operator) sind alle Mobilfunkanbieter, deren Telco-Kunden die Mobile ID nutzen können. Ein PMO setzt auf die Swisscom Mobile ID Infrastruktur auf und kann entweder seine eigene Mobilnetz-Infrastruktur betreiben oder als virtueller Anbieter agieren. Alle PMO haben auf ihren SIM-Karten die Swisscom Mobile ID Applet installiert. Eine Liste der aktuellen PMOs ist bei Swisscom auf Anfrage erhältlich.
SIM Toolkit Applet	Ein SIM-Toolkit Applet ist eine Anwendung, welche auf der SIM Karte installiert und speziell geschützt ist. Das SIM Toolkit ist ein GSM-Standard, welche die Interaktion der SIM Karte mit dem Mobilgerät ermöglicht.
MSISDN	Ist die weltweit eindeutige mobile Rufnummer. Bei Mobile ID wird die Zuweisung auf die MSISDN gemacht und der eigentliche Nutzer dieser Nummer bleibt im Service anonym.
Anwendungsanbieter (Kunde)	Dies ist der Kunde der Mobile ID, welcher mit Swisscom einen Mobile ID Vertrag abschliesst und somit direkter Vertragspartner von Swisscom ist. Der Anwendungsanbieter wiederum bietet ihren Nutzern den Service Mobile ID für ihre Applikationen an.
Nutzer	Ein Nutzer der Mobile ID ist der Endkunde dieses Services. Dieser kann sowohl ein interner Mitarbeitender wie auch ein externer Nutzer sein. Ein Nutzer muss über ein gültiges Mobilfunk-Abonnement und eine SIM-Karte der neusten Generation von Swisscom resp. des PMOs verfügen.

3 Ausprägungen und Optionen

Für den Service sind folgenden Ausprägungen und Optionen erhältlich:

Standardleistungen	Swisscom	PMO
Sicherheitselemente auf SIM-Karte	●	●
Token Management	●	●
Webservice	●	
Online Selfcare Portal für Nutzer	●	●
Kompatibilitätstest von Mobilgeräten	●	
Support für Anwendungsanbieter	●	
Support für Nutzer	●	●
Sicherheit	●	●
Business Continuity Management	●	
Datenschutz	●	●

Optionen		
Beratungsdienstleistungen	⊙	⊙
Geo Location	⊙	⊗
Mobile ID Token	⊙	⊗

● = Standard ⊙ = gegen Aufpreis ⊗ = nicht erhältlich

3.1 Sicherheitselemente auf SIM-Karte

Sichere Umgebung

Die Mobile ID ist als SIM Toolkit Applet (STK Applet) direkt auf der SIM-Karte vorinstalliert. Dadurch funktioniert die Mobile ID unabhängig vom Betriebssystem auf allen Mobilgeräten, welche dem GSM-Standard (GSM 11.14 bzw. 3GPP 31.111) entsprechen. Das STK Applet wird direkt beim Lieferanten der SIM-Karten in einer geschützten Umgebung auf die SIM-Karte geladen. Nach dem Laden und Initialisieren werden alle lokalen Zugriffe blockiert. Auf das Applet kann nur noch der Mobilfunkanbieter „Over the Air“ (OTA) mittels der richtigen Identifikationsschlüssel zugreifen. Diese Kommunikationsschlüssel werden beim Lieferanten der SIM-Karte für jede einzelne SIM-Karte nach dem Zufallsprinzip und individuell erstellt.

Zertifizierte Hardware

Um die Sicherheit des STK Applets und des anfänglich aufgebrachten SIM-spezifischen Schlüssels und später des generierten benutzerspezifischen Schlüssels zu garantieren, ist die Mobile ID auf einer mindestens nach EAL4 des Standards ISO/IEC 15408:2005 oder Level E3 Hoch der ITSEC Version 1.2 zertifizierten Hardware erhältlich.

Persönliche Authentisierungsmerkmale

Die benutzerspezifischen 2048bit RSA Schlüssel werden auf der SIM Karte generiert und sind durch einen vom Benutzer gewählten PIN geschützt. Der private Schlüssel und die PIN verlassen die SIM Karte nie und sind weder für Swisscom noch für Dritte zugreifbar oder auslesbar. Der PIN ist 6-stellig und wird nach fünfmaliger Falscheingabe blockiert.

3.2 Token Management

Swisscom resp. der PMO übernimmt im Bereich des Token Management für ihre jeweiligen Abonnenten (Telco-Kunden) folgende Leistungen:

Ereignis	Bedingung	Leistung von Swisscom resp. PMO
Mobile ID Bestellung	Abonnement/Vertrag mit Mobiltelefonieanbieter	Über das Selfcare Portal von Swisscom resp. des PMOs kann die Mobile ID Bestellung ausgelöst werden
Identifikation	Mobile ID Bestellung	Die Mobilnummer wird geprüft
Aktivierung	Positive Identifikation	Der Mobile ID Anschlussinhaber muss seinen individuellen Mobile ID PIN festlegen und erhält ein eindeutiges Zertifikat
Verlust / Diebstahl / Defekt	Mobile Abonnement und positive Identifikation	Der Mobile ID Anschlussinhaber bestellt via Selfcare Portal oder Service Desk (Support) einen Ersatz
Mobile ID PIN zurücksetzen	Mobile ID und positive Identifikation	Der Mobile ID Anschlussinhaber kann via Selfcare Portal oder Service Desk (Support) einen neuen Mobile ID PIN beantragen
Mobile Abonnementskündigung	Mobile Abonnement und positive Identifikation	Nach Kündigung wird der Zugriff auf die Mobile ID gesperrt
Abonnementsablauf	Mobile Abonnement	Der Zugriff auf die Mobile ID wird gesperrt
Zertifikatserneuerung	Mobile Abonnement und anstehende Authentisierung	Bei anstehendem Zertifikatsablauf wird das Zertifikat verlängert
SIM-Austausch	Abonnement/Vertrag mit Mobiltelefonieanbieter	Je nach Technologiestand proaktiver oder reaktiver Austausch durch Swisscom resp. PMO

3.3 Webservice

Die Dienstleistung Mobile ID bietet folgende Funktionen gemäss dem Standard ETSI TS 102 204 als Web-Service (SOAP oder RESTful) an:

- MSS Signature Request: Versenden von Textmeldungen an bestimmte Mobile ID Abonnenten (UTF-8, max. 119 Zeichen; GSMDA, max. 239 Zeichen).
- MSS Signature Response: Erhalt von signierten Bestätigungen der versendeten Meldungen.
- MSS Status Request: Versenden von Statusanfragen zu einer vorgängigen Anfrage.
- MSS Status Response: Empfangen der Antwort zu einer vorgängigen Statusanfrage.
- MSS Profile Request: Versenden von Anfragen zum Status einer beliebigen Mobilfunknummer.
- MSS Profile Response: Empfangen der Antwort zu einer vorgängigen Statusanfrage.
- MSS Receipt Request: Versenden von verschlüsselter Meldung im Anschluss an eine vorgängige Anfrage (UTF-8, max. 119 Zeichen; GSMDA, max. 239 Zeichen).
- MSS Receipt Response: Empfangen der Antwort zu einer verschlüsselten Meldung.

Ergänzende Angaben zu den Funktionen und Parametern werden auf der Swisscom Webseite www.swisscom.ch/mid im „Mobile ID Client Reference Guide“ publiziert.

Schnittstellenänderungen
Im Falle von Weiterentwicklungen an der Service-Schnittstelle gegenüber den Kundenanwendungen wird Swisscom den Kunden über Anpassungen mindestens 6 Monate im Voraus informieren. Swisscom wird den Kunden die Anleitungen zu den Veränderungen rechtzeitig zur Verfügung stellen. Die bestehende Schnittstelle wird für mindestens 12 Monate ab der Information über die Weiterentwicklung noch verfügbar sein- dies bedeutet, dass der Kunde die Nutzung der bisherigen Schnittstelle für die Dauer von 12 Monaten weiter nutzen kann. Support und Wartung werden für denselben Zeitrahmen ohne zusätzliche Kosten durch Swisscom weiterhin gewährleistet.

Schnittstellenänderungen müssen vom Kunden innerhalb 12 Monate ab der Information über die Weiterentwicklung umgesetzt werden.

Schnittstellenänderungen werden in maximal zwei Releases pro Jahr durchgeführt.

Wichtige Änderungen aufgrund von Sicherheitsanforderungen können von Swisscom unabhängig von einer Ankündigungsfrist durchgeführt und sofort implementiert werden.

In jedem Fall werden dem Kunden Änderungen möglichst frühzeitig mitgeteilt.

3.4 Online Selfcare Portal für Nutzer

Das Online Selfcare Portal bietet dem Nutzer eine einfache Möglichkeit der Bestellung, Aktivierung und Verwaltung (PIN vergessen oder gesperrt) der Mobile ID.

Auf dem webbasierten Portal sind auch Informationen zu Mobile ID in Form einer User Community und FAQ aufgeschaltet sowie Hinweise zu Geräten, welche die Mobile ID Funktion nicht unterstützen.

Die Leistungen im Selfcare Portal umfassen:

- Mobile ID (SIM-Karte) bestellen
- Mobile ID aktivieren
- Mobile ID testen
- Mobile ID PIN zurücksetzen
- Weitere Informationen (z.B. Liste der Geräte, welche nicht Mobile ID fähig sind, FAQ, User Community)

Das Online Selfcare Portal ist für den Nutzer das zentrale Tool für die Verwaltung seiner Mobile ID.

3.5 Kompatibilitätstest von Mobilgeräten

Swisscom testet periodich die wichtigsten auf dem Markt angebotenen Mobile-Geräte und deren Betriebssysteme auf Kompatibilität zur Mobile ID und publiziert die nicht funktionsfähigen Devices regelmässig auf dem Internet. Die Vollständigkeit dieser Liste kann von Swisscom nicht garantiert werden.

3.6 Support für Anwendungsanbieter

Die zentrale Anlaufstelle für Support der Anwendungsanbieter ist der Swisscom Service Desk. Die Requests können von definierten berechtigten Personen des Anwendungsanbieters telefonisch abgesetzt werden. Für jedes Kundenanliegen wird ein Ticket eröffnet. Dieser 1st Level Support kümmert sich rund um die Uhr (7x24h) um das Incident Management des Services. Er koordiniert und überwacht auch die nachgelagerten Bereiche von 2nd und 3rd Level Support sowie die angrenzenden Prozesse des Eskalation- und Problem-Managements. Der Service Desk informiert den Anwendungsanbieter regelmässig über den Status eines Tickets, meldet den erfolgreichen Abschluss des Kundenanliegens und schliesst das Ticket ab. Der Support (Service Desk) steht in den Sprachen Deutsch, Französisch, Italienisch und Englisch zur Verfügung.

Auf einer öffentlich im Internet zugänglichen Seite informiert Swisscom den Kunden und die Mobile ID Nutzer über aktuelle Störungen, geplante Wartungsfenster und bereits behobene Störungen. Dem Kunden werden diese Informationen zusätzlich in maschinenverwertbarer Form zur Verfügung gestellt.

3.7 Support für den Nutzer

Der primäre Support für den Nutzer ist mittels eines Online Selfcare Portals (vgl. Ziff. 3.4 oben) sichergestellt.

Für weitergehende Anliegen steht zusätzlich ein Service Desk des jeweiligen PMO zur Verfügung. Die Support-Dienstleistungen stehen in der Regel in den Sprachen Deutsch, Französisch, Italienisch und Englisch zur Verfügung und stehen unter alleiniger Kontrolle und Verantwortung des jeweiligen PMO.

3.8 Sicherheit

IT Security Level Basic (ITSLB)

Die für die Mobile ID umgesetzten Sicherheitsmassnahmen richten sich nach dem IT Grundschutzkonzept und werden fortlaufend überprüft und nötigenfalls verbessert. Die Einhaltung wird mittels eines periodischen ISO/IEC 27001 Audits bestätigt. Details der umgesetzten Massnahmen sind in der Beilage „Information Security“ beschrieben.

IT Security Level Advanced (ITSLA)

Zusätzlich zu den Vorkehrungen gemäss ITSLB sind im Service standardmässig folgende Mobile ID – spezifischen Sicherheitsmassnahmen umgesetzt:

- Schutz der benutzerspezifischen privaten Schlüssel in einer zertifizieren Hardware
- Jede Schlüsselverwendung erfordert Eingabe der persönlichen vom Inhaber festgelegten PIN
- Nachweis jeder Willensäusserung mittels persönlichen digitalen Signaturen
- Transportverschlüsselung der Mobile ID Meldungen von Swisscom Backend bis auf SIM
- Einsatz von digitalen Zertifikaten aus einer nach internationalen Standards zertifizierten Umgebung (ETSI TS 102 280)
- Jeder Anwendungsanbieter wird durch eine eindeutige Anruferidentifikation (Präfix) erkennbar gemacht

IT Security Level Customized (ITSLC)

Kunden mit erweiterten Sicherheitsanforderungen können in Workshops die umgesetzten Sicherheitskonzepte prüfen und Bestätigungen zur Umsetzung einzelnen Massnahmen einsehen. Diese Workshops sind kostenpflichtig. Zusätzlich können im einzelfall gegen zusätzliche Vergütung Massnahmen und Nachweise zur Erfüllung eigener regulatorischer Auflagen der Kunden vereinbart werden.

3.9 Business Continuity Management (BCM)

Ziel

Das BCM von Swisscom dient der Sicherstellung des Service im Falle eines BCM-Ereignisses (IT Krise, Katastrophe). Swisscom verfügt über Prozesse und Vorkehrungen mit dem Ziel, Unterbrechungen des Service entgegenzuwirken und Kunden vor den Auswirkungen wesentlicher Ausfälle oder Katastrophen zu schützen.

Business Recovery Levels

Die Verfügbarkeit des Services wird gemäss den unter „Continuity“ definierten Recovery Levels sichergestellt (vgl. Ziff. 5.1 unten).

- RTO bestimmt die maximal zulässige Zeitspanne für die Wiederherstellung eines Service nach dem Ausrufen einer IT Krise. (Details siehe Anhang SLA Definitionen)
- RPO definiert den am weitesten zurückliegenden Zeitpunkt, auf den ein System im Falle einer IT Krise nach der Wiederherstellung wieder aufgesetzt wird. (Details siehe Anhang SLA Definitionen)

Krisenmanagement

Bei Eintritt eines BCM-Ereignisses werden von Swisscom folgende Leistungen erbracht:

- Ein Krisenstab von Swisscom hat die Verantwortung für die Wiederherstellung der Services und arbeitet mit dem Krisenstab des Kunden zusammen.
- Die Massnahmen zur Wiederherstellung des Services werden durch den Krisenstab von Swisscom initiier und überwacht
- Swisscom trifft Massnahmen zur Rückführung in den Normalbetrieb.

3.10 Datenschutz

Es gelten die Regelungen der Allgemeinen Geschäftsbedingungen resp. des Rahmenvertrages.

3.11 Service Optionen

Beratungsdienstleistungen

Swisscom bietet den Kunden Beratungsdienstleistungen in den Bereichen Sicherheit, Konzeptionierung und Planung von Mobile ID Projekten und deren Anbindung an bestehende Kundenumgebungen an.

Geo Location

Die Geo Location bietet zusätzlich Informationen für eine weitergehende Prüfung der Authentisierung der Nutzer. Beim Login bezieht die Mobile ID Anfrage mit der Geo Location zwei zusätzliche aktuelle Datenparameter ein:

- Land (Mobile Country Code)
- Verwendeter Mobilfunkanbieter (Mobile Network Code)

Dies ermöglicht dem Kunden den Zugriff des Nutzers auf gewisse Applikationen und/oder Daten je nach Land und verwendetem Mobile Mobilfunkanbiete einzuschränken.

Im Gegensatz zu Geo-IP können die Daten der Mobile ID Geo Location nicht durch die Verwendung von VPNs, Proxys oder ähnlichen Massnahmen umgangen werden. Auch die lokale Modifikation von Daten wie bei der GPS-Lokalisierung des Benutzers ist mit Mobile ID Geo Location nicht möglich.

Aus datenschutzrechtlichen Vorgaben muss der Anwendungsanbieter in seiner Verantwortung das Einverständnis der Nutzer zur Auswertung der Geo Location Informationen vorgängig einholen.

Mobile ID Token

Der Mobile ID Token ist ein dediziertes Authentisierungs-Token für die Nutzer. Dank dem Token können alle Nutzer auch ohne geeigneten Mobilfunkvertrag die Anwendungen der Anwendungsanbieter mit Mobile ID nutzen.

Dieser Token ist eine Swisscom SIM-Karte, bei welcher ausser Mobile ID alle Dienste (Voice, Daten, SMS sowie SIM PIN/PUK) technisch gesperrt sind. Der Anwendungsanbieter verwaltet dabei die Mobile ID Token selber (Verteilung an die Nutzer). Bei Verlust oder Ersatz ist der Anwendungsanbieter primäre Anlaufstelle der Nutzer.

4 Leistungsdarstellung und Verantwortlichkeiten

Einmalige Leistungen

Tätigkeiten (S= Swisscom / K = Kunde)	S	K
Bereitstellung des Services		
1. Bereitstellung der Mobile ID Infrastruktur	X	
2. Zusenden von Präfix, IP-Adressen und SSL-Verbindungszertifikat		X
3. Konfiguration der Firewall		X
4. Aufschalten des Anwendungsanbieters und Zusenden der kundenspezifischen Zugangsdaten	X	
5. Einbindung der Mobile ID in die kundenspezifische(n) Anwendung(en)		X
Weitere einmalige Tätigkeiten		
1. Bestellung der Zusatzoptionen		X
2. Bereitstellung der Zusatzoptionen	X	
Beendigung des Services		
1. Entfernern der Firewall Konfigurationen	X	
2. Löschen der Kundenberechtigungen in der Mobile ID Infrastruktur	X	

Wiederkehrende Leistungen

Tätigkeiten (S= Swisscom / K = Kunde**)**	S	K
Standardleistungen		
1. Betrieb und Wartung der Mobile ID Infrastruktur	X	
2. Bereitstellung der Supportdienstleistungen (Service Desk, Incident Management etc.)	X	
3. Nachführen der kundenspezifischen Informationen (Kontaktpersonen, Zertifikat etc.)		X
4. Lifecycle Management (Infrastruktur, Selfcare Portal, SIM-Karten etc.)	X	
5. Proaktive Kundeninformation bei Störungen (Major Incidents) und Wartungen	X	
6. Informationen liefern über die erwartete Nutzung für die fortlaufende Kapazitätsplanung		X
Bereitstellen Software Lizenzen		
1. Im Service enthalten	X	

5 Service Level und -Reporting

5.1 Service Level

Die Beschreibung der Service Levels (Operation Time, Support Time, Availability, Process, Performance, Security und Continuity), der Messverfahren und des Reporting zu folgenden Standard Service Levels ist im Dokument „SLA Definitionen“ hinterlegt.

Folgende Service Levels werden für die Angebotsvarianten (siehe Kapitel 3) erbracht. Bei mehreren möglichen Service Levels pro Variante erfolgt die Auswahl des Service Levels im Einzelvertrag.

Service Level & Zielwerte		SAIP Service	SAIP Selfcare
Operation Time			
Operation Time	7x24	●	
Provider Maintenance Window	Di 23:00 – Mi 02:00	●	⊗
Support Time			
Support Time	Mo-Fr 07:00-18:00	⊗	●
	Mo-So 00:00-24:00	●	⊗
Störungsannahme	Mo-So 00:00-24:00	●	●
Availability			
Service Availability	Best Effort	⊗	●
	99.90%	●	⊙
Security			
	Basic (ITSLB)	⊗	●
	Advanced (ITSLA)	●	⊗
	Customized (ITSLC)	⊙	⊗
Continuity			
	RTO/RPO Best Effort	●	●

● = Standard ⊙ = Option gegen Aufpreis ⊗ = nicht erhältlich

5.2 Service Level Reporting

Im Umfang des Services erhält der Kunde das folgende Standard Level Reporting.

Service Level Report		SAIP Service	SAIP Selfcare	Berichts-periode
Availability	Verfügbarkeit in %	⊙	⊗	monatlich
Security	ISO 27001 Zertifikat	●	●	jährlich
	ETSI 102 280 Zertifikat	●	⊗	jährlich

● = Standard ⊙ = gegen Aufpreis ⊗ = nicht erhältlich

6 Rechnungsstellung und Mengenreport

6.1 Rechnungsstellung

Die Rechnungsstellung erfolgt jeweils rückwirkend für den vergangenen Monat.

Die folgenden Angaben werden auf der Rechnung ausgewiesen bzw. sind für die Rechnungsstellung relevant:

Preisposition	Einheit/Periode	Minimalbezug/ -Verrechnung	Maximalbezug/ -Verrechnung	Inkludierte Menge
Preis pro Nutzer	MSISDN/Monat	0	Uneingeschränkt	0
Setup- und Anschlussgebühr	Anschluss/Jahr	1	Uneingeschränkt	0

Der Preis pro Nutzer (B2B und B2C Modell) fällt in einem jeden Monat an, in welchem der betreffende User mindestens einmal den Mobile ID Service aktiv verwendet.

6.2 Mengenreport

Für den Service können die folgenden Daten und Informationen zu den erbrachten Leistungen ausgewiesen werden:

Produktleistungen/Optionen	Reporting-Informationen zur Rechnungsstellung
Anonymisierte MSISDN	Liste aller in der Nutzungsperiode verrechnete Mobilfunknummer