IBM Trusteer Mobile

Diese Servicebeschreibung beschreibt den Cloud-Service. Die anwendbaren Auftragsdokumente enthalten Preisangaben und weitere Einzelheiten zur Bestellung des Kunden.

1. Cloud-Service

IBM Trusteer Mobile unterstützt das Erkennen von Risiken für Echtzeitgeräte und -sitzungen. Es hilft Anwendern, die Integrität der Anwendung, in die es eingebettet ist, mithilfe von intelligenten Analysen und der Risikoerkennung bei Echtzeitgeräten aufrechtzuerhalten. Trusteer Mobile prüft das Gerät auf Infizierungen, wie Malware, Remote Access Trojans, Jailbraking/Rooting, Overlay Attack Evidence und Apps, die SMS abfangen. Zusätzliche kanalübergreifende Indikatoren werden fortlaufend verarbeitet, die innovative Technologien nutzen, wie Erkennung von Verhaltensanomalien, Unregelmäßigkeiten bei der Navigation und Phishing-Schäden.

1.1 Angebote

Folgende Angebote stehen für den Kunden zur Wahl.

1.1.1 IBM Trusteer Mobile SDK for Business und/oder IBM Trusteer Mobile SDK for Retail

Die IBM Trusteer Mobile SDK-Cloud-Services sorgen für zusätzlichen Schutz, indem sie sicheren Webzugriff auf die Business- und/oder Retail-Anwendungen ermöglichen, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat, und bieten Risikobewertungen für Geräte sowie Pharming-Schutz. Die Erkennung sicherer WiFi-Umgebungen ist nur für Android-Plattformen verfügbar.

Die IBM Trusteer Mobile SDK-Cloud-Services enthalten ein proprietäres Mobile Software Developer Kit („SDK“) (dabei handelt es sich um ein Softwarepaket, das Dokumentation, proprietäre Softwareprogrammierbibliotheken sowie weitere zugehörige Dateien und Elemente enthält, die sogenannte IBM Trusteer Mobile Library) sowie die „Run-time-Komponente“ bzw. „weiterverteilbare Komponente (Redistributable)“, einen proprietären Code, der vom IBM Trusteer Mobile SDK generiert wird und in die geschützten eigenständigen mobilen iOS- oder Android-Anwendungen eingebettet und integriert werden kann, für die der Kunde eine Abdeckung über eine Subscription für Cloud-Services erworben hat („Integrierte mobile App des Kunden“).

IBM Trusteer Mobile SDK for Retail ist in Paketen mit jeweils 100 berechtigten Teilnehmern oder 100 Clienteinheiten verfügbar und IBM Trusteer Mobile SDK for Business ist in Paketen mit jeweils 10 berechtigten Teilnehmern oder 10 Clienteinheiten verfügbar.

Über die TMA kann der Kunde (und eine unbegrenzte Zahl seiner autorisierten Mitarbeiter) Ereignisdatenberichte und Einschätzungen zu Risikobewertungen empfangen. IBM Trusteer Pinpoint Detect und IBM Trusteer Pinpoint Verify werden als Teil der TMA-Anmeldung verwendet. Über die integrierte mobile App kann der Kunde Risikoanalyseinformationen und Informationen empfangen, die sich auf die mobilen Geräte der berechtigten Teilnehmer beziehen, die seine integrierte mobile App heruntergeladen haben. Diese Informationen ermöglichen dem Kunden die Definition einer Betrugspräventionsrichtlinie, um Maßnahmen zur Minderung dieser Risiken durchzusetzen. Für die Zwecke dieses Angebots schließt der Begriff „mobile Geräte“ nur unterstützte Mobiltelefone und Tablets ein, aber keine PCs oder Mac-Computer.

Der Kunde darf:

a. das IBM Trusteer Mobile SDK ausschließlich intern für die Entwicklung der integrierten mobilen App des Kunden nutzen.

b. die weiterverteilbare Komponente (nur in Objektcodeformat) als festen, untrennbaren Bestandteil in seine integrierte mobile App einbetten. Jeder geänderte oder eingefügte Bestandteil einer weiterverteilbaren Komponente unterliegt gemäß der Lizenz den Bestimmungen dieser Servicebeschreibung; und

c. die weiterverteilbare Komponente zum Download auf die mobilen Geräte der berechtigten Teilnehmer oder des Inhabers der Clienteinheit vertreiben und weitergeben, sofern folgende Bedingungen eingehalten werden:

- Soweit nicht ausdrücklich in dieser Vereinbarung vorgesehen, ist es dem Kunden untersagt, (1) das SDK zu verwenden, zu kopieren, zu ändern oder weiterzugeben, (2) das SDK rückumzuwandeln (reverse assemble, reverse compile), in anderer Weise zu übersetzen oder rückzuentwickeln, sofern eine solche Umwandlung nicht durch ausdrückliche gesetzliche Regelung unabdingbar vorgesehen ist, (3) das SDK zu vermieten, zu verleasen oder diesbezügliche Unterlizenzen zu erteilen; (4) Copyright- oder Notice-Dateien zu entfernen, die in der weiterverteilbaren Komponente enthalten sind, (5) dieselben Pfadnamen wie für die Dateien/Module der ursprünglichen weiterverteilbaren Komponente zu verwenden und (6) die Namen oder Marken von IBM, ihren Lizenzgebern oder Distributoren ohne ihre vorherige schriftliche Zustimmung in Verbindung mit der Vermarktung seiner integrierten mobilen App zu verwenden.
- Die weiterverteilbare Komponente muss als fester, untrennbarer Bestandteil in die integrierte mobile App des Kunden eingebettet bleiben. Sie darf nur in Objektcodeformat vorhanden sein und muss allen Anweisungen, Instruktionen und Spezifikationen im SDK und der zugehörigen Dokumentation entsprechen. In der Endbenutzerlizenzvereinbarung für die integrierte mobile App des Kunden muss ein Hinweis für den Endbenutzer enthalten sein, dass die weiterverteilbare Komponente i) nur zur Aktivierung der integrierten mobilen App des Kunden verwendet werden darf, ii) nicht kopiert werden darf (außer für Sicherungszwecke), iii) nicht weitergegeben oder übertragen werden darf und iv) nicht rückumgewandelt (reverse assemble, reverse compile) oder in anderer Weise übersetzt werden darf, soweit nicht durch gesetzliche Regelung etwas anderes zwingend vorgeschrieben ist. Die Lizenzvereinbarung des Kunden muss die Rechte von IBM in mindestens demselben Maße schützen, wie sie durch die Bedingungen dieser Vereinbarung geschützt werden.
- Das SDK darf nur für interne Entwicklungszwecke und Komponententests auf den angegebenen mobilen Testgeräten des Kunden eingesetzt werden. Der Kunde ist nicht berechtigt, das SDK zur Verarbeitung oder Simulation von Produktionsworkloads oder zum Testen der Skalierbarkeit von Code, Anwendungen oder Systemen zu nutzen. Er ist ferner nicht berechtigt, Teile des SDK für andere Zwecke zu verwenden.

Der Kunde ist allein verantwortlich für die Entwicklung, das Testen und die Unterstützung seiner integrierten mobilen App. Der Kunde trägt die Verantwortung für die gesamte technische Unterstützung seiner integrierten mobilen App sowie für sämtliche von ihm durchgeführten Bearbeitungen der weiterverteilbaren Komponenten, die gemäß diesem Dokument zulässig sind.

Der Kunde darf die weiterverteilbare Komponente und das IBM Security Mobile SDK nur zur Unterstützung seiner Nutzung der Cloud-Services installieren und verwenden.

IBM garantiert nicht, dass eine Anwendung oder Ausgabe, die mit den mobilen Tools im IBM Security Mobile SDK erstellt wird, mit einer bestimmten mobilen Betriebssystemplattform oder einem bestimmten Mobilgerät funktioniert, interoperabel oder kompatibel ist.

Quellenkomponenten und Beispielmaterialien – Das IBM Trusteer Mobile SDK kann einige Komponenten in Quellcodeform (nachfolgend „Quellenkomponenten“ genannt) und sonstige Materialien enthalten, die als Beispielmaterialien gekennzeichnet sind. Der Kunde darf die Quellenkomponenten und Beispielmaterialien nur zur internen Verwendung kopieren und ändern, sofern eine solche Verwendung im Rahmen der Lizenzrechte unter dieser Vereinbarung erfolgt und keine in den Quellenkomponenten oder Beispielmaterialien enthaltenen Copyrightvermerke geändert oder gelöscht werden. IBM stellt die Quellenkomponenten und Beispielmaterialien ohne Verpflichtung zur Unterstützung im gegenwärtigen Zustand (auf „as-is“-Basis) zur Verfügung. Es wird ausdrücklich darauf hingewiesen, dass die Quellenkomponenten oder Beispielmaterialien lediglich als Beispiel für die Implementierung der Embeddable in das CIMA bereitgestellt werden. Die Quellenkomponenten oder Beispielmaterialien sind mit der Entwicklungsumgebung des Kunden unter Umständen nicht kompatibel, und der Kunde ist allein für das Testen und die Implementierung der Embeddable in das CIMA verantwortlich.

Die folgenden Bestimmungen dieses Absatzes kommen zur Anwendung, wenn die Cloud-Services gemäß dieser Vereinbarung von einem anderen Unternehmen als der International Business Machines Corporation mit Sitz im US-Bundesstaat New York („IBM Corporation“) bereitgestellt werden. Die Rechte an dem SDK und der weiterverteilbaren Komponente im Rahmen dieser Vereinbarung werden von der

IBM Corporation erteilt. IBM agiert als Distributor, der die Weitergabe des SDK und der weiterverteilbaren Komponente gemäß dieser Vereinbarung übernimmt, und ist verantwortlich für die Durchsetzung der Bedingungen sowie die Erfüllung aller Verpflichtungen in Bezug auf das SDK und die weiterverteilbare Komponente. Aus dieser Vereinbarung ergeben sich keine Rechte oder Ansprüche des Kunden gegenüber der IBM Corporation. Der Kunde verzichtet auf sämtliche Rechte und Ansprüche gegen die IBM Corporation und wird sich bezüglich rechtlicher Schritte im Zusammenhang mit dem SDK und der weiterverteilbaren Komponente ausschließlich an IBM wenden.

2. Datenblätter für Datenverarbeitung und Datenschutz

Die Ergänzenden Bedingungen zur Auftragsverarbeitung von IBM unter http://ibm.com/dpa (EB-AV) und die Datenblätter für Datenverarbeitung und Datenschutz (Data Processing and Protection Data Sheet(s), nachfolgend „Datenblätter“ oder „Anlagen zu den EB-AV“ genannt) unter den nachstehenden Links enthalten zusätzliche Datenschutzinformationen für die Cloud-Services und deren Optionen in Bezug auf die Arten der Inhalte, die verarbeitet werden können, die damit verbundenen Verarbeitungstätigkeiten, die Datenschutzfunktionen und die Besonderheiten hinsichtlich der Aufbewahrung und Rückgabe der Inhalte. Die EB-AV finden Anwendung, wenn und soweit IBM personenbezogene Daten im Auftrag des Kunden verarbeitet und i) die europäische Datenschutz-Grundverordnung (EU/2016/679) (DSGVO) oder ii) eines der unter http://ibm.com/dpa/dpl aufgeführten weiteren Datenschutzgesetze auf diese Verarbeitung Anwendung findet.

Dazu ist anzumerken, dass in den Datenblättern im Allgemeinen alle Standorte aufgelistet werden, an denen IBM (sowie die externen Unterauftragsverarbeiter) personenbezogene Daten hosten und verarbeiten, ungeachtet des Rechenzentrums, von dem die Services erbracht werden. Eine Liste der Hosting- und Verarbeitungsstandorte, die dem Rechenzentrum zugeordnet sind, von dem die Services erbracht werden, ist in Abschnitt 5.1 (Zusätzliche Informationen über den Verarbeitungsstandort) zu finden.

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Mobile Secure Browser

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492579396

3. Service-Levels und technische Unterstützung

3.1 Service-Level-Agreement

IBM stellt dem Kunden das folgende Verfügbarkeits-Service-Level-Agreement („SLA“) bereit. IBM wird die höchstmögliche Entschädigung basierend auf der kumulierten Verfügbarkeit des Cloud-Service anwenden (siehe die nachstehende Tabelle). Der Prozentsatz der Verfügbarkeit wird berechnet als Gesamtzahl der Minuten in einem Vertragsmonat, minus der Gesamtzahl der Serviceausfallminuten in dem betreffenden Vertragsmonat, dividiert durch die Gesamtzahl der Minuten in dem Vertragsmonat. Die Definition von Serviceausfall, der Prozess zur Bearbeitung von Ansprüchen und die Kontaktaufnahme mit IBM bei Problemen mit der Serviceverfügbarkeit sind im IBM Cloud Service-Supporthandbuch unter https://www.ibm.com/software/support/saas_support_overview.html enthalten.

Verfügbarkeit	Gutschrift (in Prozent (%) der monatlichen Subscription-Gebühr*)
Unter 99,9 %	2 %
Unter 99,0 %	5 %
Unter 95,0 %	10 %

* Die Subscription-Gebühr ist der vertraglich vereinbarte Preis für den Monat, der Gegenstand des Anspruchs ist.

3.2 Technischer Support

Eine Beschreibung der technischen Unterstützung für den Cloud-Service, einschließlich Support-Kontaktinformationen, Fehlerklassen, Unterstützungszeiten, Reaktionszeiten und sonstiger

Unterstützungsinformationen und -prozesse, finden Sie durch Auswahl des Cloud-Service im IBM Support Guide, der unter https://www.ibm.com/support/home/pages/support-guide/ verfügbar ist.

4. Gebühren

4.1 Gebührenmetriken

Die Gebührenmetriken für den Cloud-Service sind im Auftragsdokument angegeben.

Für diesen Cloud-Service gelten die folgenden Gebührenmetriken:

- „Berechtigter Teilnehmer“ ist eine Einzelperson oder Entität, die zur Teilnahme an einem von den Cloud-Services verwalteten oder überwachten Servicebereitstellungsprogramm berechtigt ist.
- „Clienteinheit“ ist jede Einheit, die Ausführungsbefehle, Prozeduren oder Anwendungen von einer Serverumgebung, die auf die Cloud-Services zugreift, anfordert oder empfängt.

5. Zusätzliche Bedingungen

Für Vereinbarungen für Cloud-Services (oder vergleichbare Cloud-Basisvereinbarungen), die vor dem 1. Januar 2019 unterzeichnet wurden, finden die Bedingungen unter https://www.ibm.com/acs Anwendung.

5.1 Zusätzliche Informationen zum Verarbeitungsstandort

Alle personenbezogenen Daten werden an den nachstehend angegebenen Standorten gehostet und verarbeitet, auch wenn das Hosting und die Verarbeitung von den im Datenblatt angegebenen externen Unterauftragsverarbeitern durchgeführt wird:

Bei allen Services, die über das Rechenzentrum in Deutschland erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Deutschland, Israel, Irland und die Niederlande.

Bei allen Services, die über das Rechenzentrum in Japan erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: Japan, Israel und Irland.

Bei allen Services, die über das Rechenzentrum in den USA erbracht werden, beschränkt IBM das Hosting und die Verarbeitung personenbezogener Daten auf das Land, in dem die IBM Vertragspartei ihren Sitz hat, sowie auf die folgenden Länder: USA, Israel, Irland, Singapur und Australien.

Hinsichtlich aller Services, die über Rechenzentren in Deutschland, Japan und den USA erbracht werden, können zusätzlich zu den obigen Standorten unterstützende Daten in Deutschland und Frankreich von Salesforce.Com als externem Unterauftragsverarbeiter von IBM gehostet und verarbeitet werden.

IBM Trusteer-Support- und Kontowartungsservices können bei Bedarf ebenfalls erbracht werden und richten sich nach der Verfügbarkeit der entsprechenden IBM Mitarbeiter, dem Standort des Kunden und dem Rechenzentrum, in dem die Daten gehostet sind.

5.2 Integrierte Lösungen

Es wird ausdrücklich darauf hingewiesen, dass die verschiedenen Angebote der Marke Trusteer als integrierte Lösung implementiert sein können. Selbst wenn der Kunde einen dieser Cloud-Services kündigt, kann IBM Kundendaten aufbewahren, damit sowohl die übrigen Cloud-Services, die durch diese Servicebeschreibung abgedeckt sind, als auch andere Trusteer-Services gemäß den für sie anwendbaren Servicebeschreibungen erbracht werden können.

5.3 Prüfung

Der Kunde wird i) Aufzeichnungen und Ausgaben von Systemtools aufbewahren und auf Anforderung bereitstellen, soweit dies für IBM und ihre beauftragten externen Prüfer erforderlich ist, um die Einhaltung der Vereinbarung durch den Kunden zu überprüfen, und ii) unverzüglich alle erforderlichen Berechtigungen bestellen und zu den zum jeweiligen Zeitpunkt gültigen Preisen von IBM bezahlen und andere Verbindlichkeiten, die sich aufgrund der Prüfung ergeben und in einer Rechnung von IBM angegeben sind, begleichen. Die Verpflichtungen im Rahmen dieses Abschnitts bleiben während der Laufzeit des Cloud-Service und eines Zeitraums von zwei Jahren danach in Kraft.

5.4 Datenerfassung im Rahmen der Bereitstellung

Bei der Bereitstellung des Cloud-Service können bestimmte Daten des Kunden an IBM weitergegeben werden. Richtlinien für Daten, die im Rahmen der Bereitstellung an IBM weitergegeben werden, sind in den Trusteer Deployment Guidelines zu finden, die dem Kunden zur Verfügung gestellt werden müssen.

6. Übergeordnete Bedingungen

6.1 Nutzung von Daten

Folgende Bestimmung hat Vorrang vor gegenteiligen Bestimmungen im Abschnitt „Inhalte und Datenschutz“ der Basisbedingungen für Cloud-Services zwischen den Vertragsparteien: IBM wird die Ergebnisse, die sich aus der Nutzung des Cloud-Service durch den Kunden ergeben und sich eindeutig auf Kundeninhalte beziehen (Erkenntnisse) oder den Kunden anderweitig identifizieren, weder verwenden noch offenlegen. IBM ist jedoch berechtigt, Inhalte und andere Informationen, die sich im Rahmen des Cloud-Service aus den Inhalten (ausgenommen Erkenntnissen) ergeben, für die Verbesserung des Cloud-Service zu verwenden. Des Weiteren ist IBM berechtigt, Bedrohungs-IDs und weitere Sicherheitsinformationen, die in Inhalten eingebettet sind, zum Zweck der Erkennung von Sicherheitsbedrohungen und zum Schutz vor Sicherheitsbedrohungen weiterzugeben.