

Symantec Benutzerauthentifizierung Service-Level-Vereinbarung (SLA)

Übersicht und Gültigkeitsbereich

Diese Service-Level-Vereinbarung ("**SLA**") für Symantec Benutzerauthentifizierung gilt für Symantec Benutzerauthentifizierungsprodukte/-services (z. B. VeriSign MPKI, VIP, FDS, TrustCenter und andere von Symantec von Zeit zu Zeit identifizierte Benutzerauthentifizierungslösungen, die jeweils als "**Benutzerauthentifizierungsservice**" bezeichnet werden). Diese SLA sollte in Verbindung mit der geltenden Servicebeschreibung für den betreffenden Benutzerauthentifizierungsservice gelesen werden. Die in einer aktuell veröffentlichten Servicebeschreibung beschriebene Serviceebene hat Vorrang vor dieser SLA, falls Konflikte zwischen diesen beiden Dokumenten bestehen.

Diese SLA gilt für Neu- oder Verlängerungsserviceperioden des Benutzerauthentifizierungsservice, der am oder nach dem in diesem Dokument angegebenen Datum der SLA-Version ausgeführt wird. Für Kunden, die Benutzerauthentifizierungsservices vor dem Datum der SLA-Version gekauft haben, gelten die jeweils früheren VeriSign- oder TrustCenter-Service-Level-Vereinbarungen bis zum Ablauf der aktuellen jährlichen Serviceperiode, so dass diese SLA ab der nächsten jährlichen Serviceperiode gilt. Dieses SLA-Dokument ist wie folgt aufgebaut:

- **SLA-Informationen zum Technischen Support**
- **SLA-Informationen zur Serviceleistung**
- **Definitionen**

SLA für den Technischen Support

Kundenadministratoren

Der Kunde kann so genannte Kundenadministratoren nominieren, die befugt sind, mit Symantec zusammenzuarbeiten, um Probleme bei Benutzerauthentifizierungsservices zu melden, technischen Support anzufordern und gemeinsam mit dem Technischen Support von Symantec an der Behebung gemeldeter Probleme zu arbeiten. Die Anzahl dieser Kundenadministratoren hängt von der Supportstufe (Bronze, Gold, Platinum) des gekauften Services ab (siehe die Beschreibung weiter unten).

Der Kunde ernennt die Kundenadministratoren, die er von Zeit zu Zeit auch ändern kann, mithilfe der dann gültigen Prozesse des Technischen Supports von Symantec.

Schweregradstufen

Die Kunden müssen jedem Problem, das dem Technischen Support von Symantec gemeldet wird, einen Schweregrad zuweisen. Der Schweregrad gibt den Grad der potenziellen Auswirkungen auf Ihren Geschäftsbetrieb wider. Die Reaktionszeiten für die Bereitstellung von technischen Supportleistungen durch Symantec gegenüber dem Kunden in Verbindung mit den Benutzerauthentifizierungsservices basiert teilweise wie folgt auf der Klassifizierung gemeldeter Probleme nach dem Schweregrad:

Schweregrad	Auswirkung oder Bedeutung des Problems
Schweregrad 1 (Kritische Ereignisse)	<p>Zu Problemen des Schweregrads 1 zählen alle Ereignisse, die erhebliche negative Auswirkungen auf die Betriebsbereitschaft des Systems und die Verwendung des/der Benutzerauthentifizierungsservices durch den Benutzer haben, wie beispielsweise die im Folgenden beschriebenen Problemtypen. Ein Kunde kann ein Problem nicht als Schweregrad 1 klassifizieren, und Symantec klassifiziert für ein Problem nur dann den Schweregrad 1, wenn sich ein Kundenadministrator mit sofortigem Zugang zu den betroffenen Systemen und den entsprechenden Informationen mit Symantec telefonisch in Verbindung setzt, um Support anzufordern.</p> <ul style="list-style-type: none"> ○ Nichtverfügbarkeit eines Systems oder einer Anwendung, die die Verarbeitung kritischer Transaktionen verhindert ○ Ausfälle von Online-Anwendungen, die die Online-Verfügbarkeit des/der Benutzerauthentifizierungsservices erheblich beeinträchtigen ○ Telekommunikationsunterbrechungen, die zu einer größeren Störung des/der Benutzerauthentifizierungsservices führen ○ Ständige Beeinträchtigung der Verfügbarkeit, die die Verwendung des/der Benutzerauthentifizierungsservices erheblich behindert
Schweregrad 2 (Ereignisse von hoher Bedeutung)	<p>Zu Problemen des Schweregrads 2 zählen alle Ereignisse (mit Ausnahme der Probleme des Schweregrads 1), die moderate negative Auswirkungen auf die Betriebsbereitschaft des Systems und die Verwendung des/der Benutzerauthentifizierungsservices durch den Benutzer haben, wie beispielsweise die im Folgenden beschriebenen Problemtypen:</p> <ul style="list-style-type: none"> ○ Fehler, durch die nur bestimmte unwichtige Funktionen des/der Benutzerauthentifizierungsservices deaktiviert werden und die zu einer Beeinträchtigung der Betriebsbereitschaft führen können, einschließlich, aber nicht beschränkt auf Fehler, die erhebliche Verzögerungen bei der Verarbeitung von Transaktionen verursachen ○ Zeitweise Beeinträchtigung der Verfügbarkeit, die die Verwendung des/der Benutzerauthentifizierungsservices moderat behindert
Schweregrad 3 (Ereignisse von mittlerer Bedeutung)	<p>Zu Problemen des Schweregrads 3 zählen alle Ereignisse (mit Ausnahme der Probleme des Schweregrads 1 und 2), die geringfügige negative Auswirkungen auf die Betriebsbereitschaft des Systems und die Verwendung des/der Benutzerauthentifizierungsservices durch den Benutzer haben.</p>

Reaktionszeit des Technischen Supports – Symantec unternimmt alle wirtschaftlich vertretbaren Anstrengungen, um die folgenden Aktivitäten auszuführen:

Für Bronze-Service: Symantec bietet wie folgt bis zu zwei (2) Kundenadministratoren Support per Telefon und E-Mail:

- (i) Für Probleme des Schweregrads 1 rund um die Uhr, sieben Tage pro Woche, 52 Wochen im Jahr und
- (ii) auf Wunsch des Kunden für Probleme des Schweregrads 2 und 3 wie folgt:
 - Zwischen 5:00 und 18:00 Uhr Pacific Standard Time, Montag bis Freitag, 52 Wochen im Jahr, mit Ausnahme von nationalen Feiertagen in den USA und geplanten Ausfallzeiten
 - Zwischen 8:00 und 18:00 Uhr MEZ, Montag bis Freitag, 52 Wochen im Jahr, mit Ausnahme von nationalen Feiertagen in Irland und geplanten Ausfallzeiten
 - Zwischen 8:30 und 17:00 AEST, Montag bis Freitag, 52 Wochen im Jahr, mit Ausnahme von australischen nationalen Feiertagen, Feiertagen in Melbourne und Victoria sowie geplanten Ausfallzeiten
- (iii) Während der oben beschriebenen ortsüblichen Geschäftszeiten können sich Kunden des Bronze-Service an den betreffenden regionalen Technischen Support von Symantec für die Benutzerauthentifizierung wenden, und zwar basierend auf dem Standort des Kunden gemäß der Angabe im Serviceauftrag des Kunden (und nicht basierend auf dem Standort des/der Kundenadministratoren).

Für Gold- und Platinum-Service: Symantec bietet Support per Telefon und E-Mail für bis zu zwei (2) Kundenadministratoren für den Gold-Service bzw. fünf (5) Kundenadministratoren für den Platinum-Service bei Problemen des Schweregrads 1, 2 und 3, rund um die Uhr, sieben Tage pro Woche und 52 Wochen im Jahr.

In dieser Zeit werden eingehende Anrufe beim Technischen Support von einem automatisierten Telefonsystem entgegengenommen. Symantec bietet über dieses Telefonsystem die Option, dass der Kunde direkt mit einem geschulten Mitarbeiter des Technischen Supports spricht. In 80 Prozent der Fälle, in denen diese Option gewählt wird (gemessen auf der Basis von 90 aufeinander folgenden Tagen), werden die Kunden innerhalb von 120 Sekunden mit einem geschulten Mitarbeiter des Technischen Supports verbunden.

Zielreaktionszeiten. In der folgenden Tabelle finden Sie die Zielreaktionszeiten von Symantec für Rückrufe und den E-Mail-Support, gegliedert nach Servicetyp und Schweregrad. Beachten Sie, dass "**Reaktionszeit**" den Zeitraum bezeichnet, der zwischen der Meldung eines Software- oder Serviceproblems durch den Kunden an Symantec und der Reaktion von Symantec durch die Bestätigung der Meldung und den Hinweis, dass entsprechende Maßnahmen eingeleitet wurden, verstreicht. Folgendes sind Zielvorgaben, keine verbindlichen Zusagen.

Schweregrad (Während der oben angegebenen Zeiten)	Bronze-Service – Zielvorgaben für Reaktionszeiten	Gold-Service – Zielvorgaben für Reaktionszeiten	Platinum-Service – Zielvorgaben für Reaktionszeiten
Schweregrad 1 (Meldung durch den Kunden per Telefon)	Innerhalb einer Stunde	Innerhalb einer Stunde	Innerhalb von 30 Minuten
Schweregrad 2 (Meldung durch den Kunden per Telefon oder E-Mail*)	Innerhalb von sechs Stunden während der Geschäftszeiten	Innerhalb von sechs Stunden	Innerhalb von zwei Stunden
Schweregrad 3 (Meldung durch den Kunden per Telefon oder E-Mail*)	Nächster Arbeitstag	Innerhalb von acht Stunden	Innerhalb von acht Stunden

*Die Bearbeitung von E-Mail-Anfragen dauert möglicherweise länger als die Bearbeitung von telefonischen Anfragen

Wartung und Serviceversion

Bronze-, Gold- und Platinum-Supportleistungen umfassen einen Wartungsplan, nach dem Symantec Software-Upgrades, Fehlerreparaturen, Patches, Fehlerkorrekturen und Funktionserweiterungen bereitstellt, die von Symantec entwickelt und Symantec-Kunden für diese Angebote zur Verfügung gestellt werden, soweit und sobald sie verfügbar sind. SYMANTEC BIETET DIESEN WARTUNGSPLAN UND KUNDENSERVICE ZU JEDEM ZEITPUNKT GEMÄSS DIESER SLA NUR FÜR DIE DANN AKTUELLE VERSION DER SERVICES ODER SOFTWARE UND DIE UNMITTELBAR VORAUSGEHENE HAUPTVERSION AN.

Problemverwaltung und Eskalationsprozess

Jeder Eskalation ist ein entsprechender Mitarbeiter des Technischen Supports zugewiesen, der für alle Aspekte der Supportanfrage zuständig ist. Die für Eskalationen zuständigen Mitarbeiter des Technischen Supports sind für die Beurteilung der Situation verantwortlich, sie koordinieren die Behebung des Problems auf globaler Ebene und vertreten Ihre Interessen.

Eskalation von Problemen. Probleme des Schweregrads 1 und 2 werden intern wie folgt eskaliert:

Schweregrad 1:

- *Stunde 0 bis Stunde 1:* Für andere als systemweite Probleme im Zusammenhang mit Back-End-Systemen von Symantec werden der Technical Support Manager von Symantec und bei Bedarf der Backline Maintenance und Escalation Manager von Symantec, oder Personen in gleichwertigen Positionen, über das Problem informiert und arbeiten aktiv an einer Lösung. Für systemweite Probleme im Zusammenhang mit Back-End-Systemen von Symantec wird der Production Services Manager von Symantec, oder eine Person in gleichwertiger Position, ebenfalls informiert und arbeitet aktiv an einer Lösung.
- *Stunde 2 bis Stunde 4:* Für andere als systemweite Probleme im Zusammenhang mit Back-End-Systemen von Symantec wird der Director of Technical Support von Symantec, oder eine Person in gleichwertiger Position, benachrichtigt und bei Bedarf zur Lösung des Problems herangezogen. Für systemweite Probleme im Zusammenhang mit Back-End-Systemen von Symantec werden der Vice President of Production Services und der Vice President of Technical Support, oder Personen in gleichwertigen Positionen, ebenfalls benachrichtigt und bei Bedarf zur Lösung des Problems herangezogen.

- *Stunde 5:* Der Vice President of Technical Support von Symantec, oder eine Person in gleichwertiger Position, wird über andere als systemweite Probleme im Zusammenhang mit Back-End-Systemen von Symantec informiert.

Schweregrad 2:

- *Stunde 0 bis Stunde 72:* Symantec arbeitet an der Lösung des Problems und versucht, innerhalb von 72 Stunden nach der Problemerkennung eine Lösung bereitzustellen. Falls Symantec innerhalb von 72 Stunden nach der Meldung des Problems keinen Plan für die Behebung des Problems innerhalb von 10 Tagen nach dem 72-stündigen Zeitfenster entwickelt, und vorausgesetzt, dass das Problem nicht auf ein Verschulden des Kunden zurückzuführen ist, eskaliert Symantec das Problem auf die ausdrückliche Bitte des Kunden hin gemäß den weiter oben beschriebenen Eskalationsverfahren für den Schweregrad 1.

Kontaktinformationen und Telefonnummern für den Technischen Support finden Sie unter:

<http://www.verisign.com/support/contact/index.html>

SLA zur Serviceleistung

Benutzerauthentifizierungsservices des TrustCenter

Weitere Informationen finden Sie in der entsprechenden SLA zur Serviceleistung für unseren Gold- und/oder Platinum-Service gemäß der geltenden TrustCenter-Servicebeschreibung. Die nachfolgende SLA zur Serviceleistung gilt nicht für TrustCenter-Services.

Zusätzliche Bestimmungen für Platinum-Service-Kunden

Customer Relationship Manager

Symantec nominiert nur für den Platinum-Service einen qualifizierten Symantec-Mitarbeiter als Customer Relationship Manager für die Koordination von Implementierungsaktivitäten sowie für die Verwaltung der Problembehebung und der Eskalationsprozesse. Der Customer Relationship Manager überprüft außerdem auf Anfrage des Kunden einmal im Quartal die Leistungen des Supportservice.

Berichte

Symantec stellt nur für den Platinum-Service dem Kunden monatliche Berichte mit den folgenden Informationen zum monatlichen Berichtszeitraum zur Verfügung:

- Prozentualer Anteil der Betriebszeit
- Maximale Ausfallzeiten (außer geplanten Ausfallzeiten) (in Stunden) für:
 - Anforderung von Zertifikaten
 - Überprüfung von Zertifikaten mithilfe von OCSP
- Maximale Verarbeitungszeit (in Minuten) für:
 - Anforderung von Zertifikaten
 - Widerruf/Sperrung/Aufhebung der Sperrung von Zertifikaten
- Maximale Anzahl von Operationen (pro Tag und pro Minute) für:
 - Anforderung und Ausstellung von Zertifikaten
 - Widerruf/Sperrung/Aufhebung der Sperrung von Zertifikaten
 - Überprüfung von Zertifikaten mithilfe von OCSP

Symantec MPKI, VIP und andere Benutzerauthentifizierungsservices von VeriSign

Die nachfolgenden SLA-Informationen beschreiben die Symantec-Standardbestimmungen der SLA zur Serviceleistung für Kunden des Bronze-Service sowie bestimmte zusätzliche Verpflichtungen der SLA zur Serviceleistung für Kunden, die die Premium-SLA-Pakete von Symantec ("Gold-Service" und "Platinum-Service") kaufen (soweit zutreffend):

Serviceverfügbarkeit

- **Messung der Betriebszeit.** Die Betriebszeit wird auf der Basis von 90 aufeinander folgenden Tagen wie folgt gemessen: als Prozentsatz (i) der Gesamtanzahl von Minuten, in denen die Systeme von Symantec während des Zeitraums von 90 Tagen verfügbar sind und Daten von Kunden empfangen und verarbeiten können, dividiert durch (ii) die Gesamtanzahl von Minuten in diesem Zeitraum.
- **Prozentuale Betriebszeit.** Die prozentuale Betriebszeit von Symantec während eines Zeitraums von 90 Tagen darf folgende Werte nicht unterschreiten:
 - Für Managed PKI: 99 Prozent für Bronze- und Gold-Service, und nicht weniger als 99,5 Prozent für Platinum-Service.

- Für VIP: 99,5 Prozent. Nur für die Überprüfung der VIP-Identifikationsdaten darf die prozentuale Aktivzeit von Symantec nicht niedriger als 99,95 Prozent sein.
- **Geplante Ausfallzeiten.** Symantec informiert den Kunden mindestens dreißig (30) Stunden im Voraus per E-Mail über geplante Ausfallzeiten und die voraussichtlichen Auswirkungen auf die Funktionalität im Zusammenhang mit dem Benutzerauthentifizierungsservice. Geplante Ausfallzeiten dürfen vier (4) Stunden pro Kalenderwoche nicht überschreiten.

Produktionsvorbereitende Umgebung für VIP

- Der Kunde hat, soweit dies für den/die bereitgestellten VIP Benutzerauthentifizierungsservice(s) zutrifft, für einen Zeitraum von 60 Tagen nach Beginn des Bronze- oder Gold-Service bzw. für einen Zeitraum von einem (1) Jahr nach Beginn des Platinum-Service Zugang zur produktionsvorbereitenden Umgebung von Symantec.
- Für die Verfügbarkeit oder Leistungsfähigkeit der produktionsvorbereitenden Umgebung gelten keine anderen Klauseln dieser SLA.

Zusätzliche Bestimmungen für Platinum-Service-Kunden

Serviceleistung für Managed PKI

Die Managed PKI-Services (soweit zutreffend) werden nur für den Platinum-Service gemäß den folgenden Standards für die Serviceleistung bereitgestellt (hiervon ausgenommen ist zusätzliche Latenz aufgrund der Verwendung der Managed PKI-Services in Verbindung mit anderen Benutzerauthentifizierungsservices), die der durchschnittlichen Serviceleistung für Kunden im Laufe eines Kalendermonats entsprechen:

- 90 Prozent aller Genehmigungen eines digitalen Zertifikats durch einen Kundenadministrator erfolgen innerhalb von zehn Sekunden
- 90 Prozent aller Widerrufe eines digitalen Zertifikats durch einen Kundenadministrator erfolgen innerhalb von fünf Sekunden
- 90 Prozent aller Anfragen für eine Zertifikatsperrliste (Certificate Revocation List, CRL) durch einen Kundenadministrator erfolgen innerhalb von fünf Sekunden
- 90 Prozent aller Anforderungen für ein digitales Zertifikat durch Benutzer erfolgen innerhalb von fünf Sekunden
- 90 Prozent aller Abrufe genehmigter digitaler Zertifikate durch Benutzer erfolgen innerhalb von fünf Sekunden
- 90 Prozent aller Widerrufe des eigenen digitalen Zertifikats durch Benutzer erfolgen innerhalb von fünf Sekunden
- 99 Prozent aller obigen Anforderungen oder Aktionen erfolgen innerhalb von zwei Minuten

Customer Relationship Manager

Syantec nominiert nur für den Platinum-Service einen qualifizierten Symantec-Mitarbeiter als Customer Relationship Manager für die Koordination von Implementierungsaktivitäten sowie für die Verwaltung der Problembehebung und der Eskalationsprozesse. Der Customer Relationship Manager überprüft außerdem auf Anfrage des Kunden einmal im Quartal die Leistungen des Supportservice.

Berichte

Syantec stellt nur für den Platinum-Service dem Kunden monatliche Berichte mit den folgenden Informationen zum monatlichen Berichtszeitraum zur Verfügung:

- Prozentualer Gesamtanteil der Betriebszeit
- Anzahl der geplanten Ausfallzeiten
- Prozentsatz der geplanten Ausfallzeiten, die innerhalb des in der Mitteilung von Symantec angegebenen geplanten Zeitfensters abgeschlossen wurden
- Auf Anfrage Schweregradklassifikationen und der aktuelle Fehlerbehebungsstatus für gemeldete Probleme

- Nur für Managed PKI-Services die eigentlichen Zahlen zur Serviceleistung gemäß den in dieser SLA angegebenen Standards (zusammengefasst für alle Kunden des Managed PKI-Services)

Definitionen

Sofern in dieser SLA nicht anderweitig definiert, sind die folgenden Begriffe wie folgt definiert.

"**AEST**" bedeutet "Australian Eastern Standard Time" (GMT +10:00)

"**MEZ**" bedeutet "Mitteleuropäische Zeit" (GMT +01:00)

"**Kundenadministrator**" bezeichnet eine benannte, vertrauenswürdige Person des Kunden, die vom Kunden für Symantec als Administrator für die entsprechenden Services zugewiesen wird und die der Kunde für die Interaktion mit Symantec bei technischen Problemen mit dem Service beauftragt.

"**FDS**" bedeutet "Fraud Detection Service".

"**GMT**" bedeutet "Greenwich Mean Time".

"**PKI**" bedeutet "Public Key Infrastructure".

"**PST**" bedeutet "Pacific Standard Time" (GMT -08:00)

"**Geplante Ausfallzeit**" bezeichnet Zeiträume geplanter Nichtverfügbarkeit des Symantec-Systems und des Benutzerauthentifizierungsservice, um routinemäßige Wartungsmaßnahmen, Upgrades und Tests für den Service auszuführen.

"**Laufzeit bestellter Services**" ist die vereinbarte Laufzeit des Kunden für die Benutzerauthentifizierungsservices, die in Abhängigkeit von der Bestellung des Kunden 12 Monate überschreiten kann.

"**Serviceleistung**" bezeichnet den Zeitraum, der zwischen dem Eintreffen von durch den Kunden gesendete Daten im Back-End-System von Symantec und der Übertragung der entsprechenden Antwort oder automatisierten Aktion von Symantec im Zusammenhang mit dem entsprechenden Benutzerauthentifizierungsservice vom Back-End-System von Symantec verstreicht.

"**Serviceleistung**" bezieht sich nur auf die Leistung des Back-End-Systems von Symantec und beinhaltet nicht die Systemverfügbarkeit, Leistungsfähigkeit oder Reaktionsverzögerung Dritter.

"**Serviceperiode**" ist jedes Servicejahr im Rahmen der Laufzeit bestellter Services.

"**Betriebszeit**" bezeichnet den prozentualen Zeitraum, in dem die Systeme von Symantec verfügbar sind und Daten vom Kunden in Verbindung mit den entsprechenden Benutzerauthentifizierungsservices empfangen und verarbeiten können. Geplante Ausfallzeit gilt nicht als Ausfallzeit im Sinne dieser SLA. Sofern nichts anderes angegeben ist, bezieht sich "Betriebszeit" nur auf die Verfügbarkeit der Systeme von Symantec und nicht auf die Systemverfügbarkeit oder Leistungsfähigkeit der Systeme anderer Anbieter.

"**VIP**" bedeutet "Validation & ID Protection" (ehemals als "VeriSign Identity Protection" bezeichnet).

"**TrustCenter**" bezeichnet die Benutzerauthentifizierungsservices der TrustCenter-Abteilung von Symantec.