

Schnittstellenbeschreibung SMS Gateway Internext GmbH

Stand: 20.01.2011

Kurzbeschreibung

Das folgende Dokument beschreibt die Schnittstelle des SMS Gateways zum Versenden von Kurzmitteilungen (SMS). Dieses Dokument richtet sich an Software-Entwickler, die den Versand von SMS als Funktion in eigene Anwendungen realisieren möchten.

Voraussetzungen

Folgende Voraussetzungen müssen gegeben sein, damit der Versand von Kurzmitteilungen erfolgen kann:

- Sie benötigen einen Kunden-Account.
- Sie benötigen ausreichend Guthaben auf Ihrem Kundenkonto.

Der Zugang zum SMS Gateway unterliegt unseren Allgemeinen Geschäftsbedingungen, abrufbar unter <http://www.sms-discount.de>

Kontakt

Bei allgemeinen Fragen zum SMS-Versand, wenden Sie sich bitte an:

Internext GmbH
Friedrichsplatz 4-5
76133 Karlsruhe

Tel: +49 (0)721 – 1613 010

Fax +49 (0)721 – 1613 029

Email: service@sms-discount.de

Haben Sie technische Fragen, richten Sie diese bitte an:

technik@internext.de

Aufruf der Schnittstelle

Die Übergabe einer SMS an das SMS Gateway erfolgt mittels eines HTTP-Requests (GET oder POST) .Die aufzurufende URL lautet hierbei:

http://sms-discount.de/cgi-perl/http2sms/smsversand.cgi?PARAMETER

Pro Aufruf kann ein Empfänger angegeben werden.

Die Schnittstelle liefert einen String im Klartext zurück, der über Erfolg oder Misserfolg berichtet. Er hat für den positiven Fall folgenden Aufbau:

Rückgabewert - Ausgabestring - Anzahl verbrauchter SMS

Beispiel: 200 - Inland anonyme Textmitteilung - 1

Textmitteilungen sind auf eine SMS (160 Zeichen) beschränkt.

Im negativen Fall wird nur ein Fehlercode ausgegeben, dessen Bedeutung aus Anhang A entnommen werden kann.

Authentifizierung

Zur Authentifizierung stehen 2 Möglichkeiten zur Wahl, die Sie bei der Einrichtung der Schnittstelle wählen:

- IP-Adresse

Hier wird die IP-Adresse des Aufrufers mit der für Sie im System hinterlegten IP-Adresse verglichen. Stimmt diese Adresse mit der Ihres Kunden-Accounts überein, darf die weitere Verarbeitung statt finden. Es ist möglich, mehr als eine IP-Adresse zur Authentifikation zu hinterlegen.

- MD5-Verschlüsselung

Hierfür wird ein Passwort für Ihren Kunden-Account im System hinterlegt. Als weiteren Übergabe-Parameter geben Sie ein Passwort an, welches aus einem MD5-Hash besteht, der die Parameter **to**, **text** und Ihr im System hinterlegtes **Passwort** enthält.

Der Hash-Wert muss nach folgender Formel berechnet werden:

`md5($password + $to + $text)`

Diese Authentifizierung eignet sich für Kunden, die über keine feste IP-Adresse verfügen. Einem vermeintlichen Angreifer wird es somit unmöglich gemacht, den Adressaten oder den Inhalt Ihrer Nachricht bei der Übertragung im Netz zu ändern.

Formale Beschreibung der möglichen Parameter

Parametername	Wert	Beschreibung	Detail
user	alphanumerisch	Benutzername	
art	[1]	Versand-Art	1 = Text
to	[0-9]	Empfänger-Nummer	Bsp: 00491711234567
absender	[anonym eigen]	Absenderkennung	
from	[0-9a-z]	Absender	11 Zeichen alphanumerisch 16 Zeichen numerisch
passwd	[0-9a-z]	Passwort	32 Zeichen bei einer Passwort gestützten Authentifizierung
text	Text ISO-8859-1	Mitteilung	Max. 160 Zeichen
simulate	[1]	Simulationsmodus	1 = Versand wird simuliert

Benötigte Parameter bei den Versandarten

	user	art	to	absender	from	text
Text anonym Inland	X	X	X	X		X
Text eigen Inland	X	X	X	X	X	X
Text anonym Ausland	X	X	X	X		X
Text eigen Ausland	X	X	X	X	X	X

Beteiligte Parameter für die Erstellung des Passwortes auf Basis einer MD5-Verschlüsselung

	passwd	to	text
Text anonym Inland	X	X	X
Text eigen Inland	X	X	X
Text anonym Ausland	X	X	X
Text eigen Ausland	X	X	X

Beispiele

- **Versand einer Textmitteilung mit anonymer Absenderkennung**

Um an die Zielnummer 01601234567 eine Textmitteilung mit der Nachricht „Hallo Du“ zu versenden, sieht der Parameterstring folgendermaßen aus:

```
user=BENUTZER&art=1&to=00491601234567&absender=anonym&text=Hallo+Du
```

- **Versand einer Textmitteilung mit eigener Absenderkennung**

Um an die Zielnummer 01601234567 eine Textmitteilung mit der Nachricht „Servus“ mit der Absenderkennung 01607654321 zu versenden, sieht der Parameterstring folgendermaßen aus:

```
user=BENUTZER&art=1&to=00491601234567&absender=eigen&from=00491607654321&text=Servus
```

Anhang A – Fehlercodes

400	allgemeiner Fehler
401	Authentifizierungsfehler
402	Versandmethode nicht autorisiert
403	Tageslimit erreicht
404	Guthaben nicht ausreichend
550	keine Versandart angegeben
551	keine Zielrufnummer angegeben
552	kein Benutzername angegeben
571	keine gültige deutsche Rufnummer
572	keine Unterstützung des Zielnetzes (Inland)
573	keine Unterstützung des Zielnetzes (Ausland)
574	Empfänger gesperrt
575	Absender zu lang
576	Absender enthält ungültige Zeichen
580	keine Mitteilung angegeben
581	keine Art der Absenderkennung
582	Nachricht zu lang

Anhang B – Beispielskripte

Folgendes Perl-Skript demonstriert den Aufruf der http-Schnittstelle zum Versenden einer SMS mit anonymer Absenderkennung:

```
#!/usr/local/bin/perl

use LWP::UserAgent;
use Data::Dumper;

my $user = "username";
my $empfaenger = "00491601234567";
my $text = "Hallo+Welt";

my $query = "user=$user&art=1&absender=anonym&to=$empfaenger&text=$text";

my $ua = new LWP::UserAgent;
    $ua->timeout(30);
my $req = new HTTP::Request 'GET' => " http://sms-discount.de/cgi-perl/http2sms/smsversand.cgi?$query";
my $res = $ua->request($req);

if ($res->{'_rc'} eq "200") {
    print "HTTP-Request erfolgreich abgesetzt\n";

    if ($res->{'_content'} =~ m/^200#) {
        print "SMS erfolgreich verschickt !\n";
    } else {
        print "SMS nicht verschickt, Fehlercode: ", $res->{'_content'}, "\n";
    }
} else {
    print "HTTP-Schnittstelle konnte nicht angesprochen werden\n";
    print Data::Dumper::Dumper($res);
}
```

Folgendes Perl-Skript demonstriert die Erzeugung des Passwortes auf Basis einer MD5-Verschlüsselung:

```
#!/usr/local/bin/perl

use Digest::MD5;

my $kundePassword = "kundenPasswort";
my $text = „Hallo Welt“;
my $to = "01621234567";

my $md5pass = Digest::MD5->new;
$md5pass->add($kundePassword.$to.$text);

my $password = $md5pass-> hexdigest;
```

Wobei *\$kundePassword* das vom Kunden gewählte und in der Schnittstelle hinterlegte Passwort ist. Die Variable *\$password* wird hingegen bei dem HTTP-Request übergeben. Bei der Erzeugung des Passwortes ist darauf zu achten, eine hexadezimal basierte, auf 32 Zeichen begrenzte Schreibweise zu wählen.

Welche Parameter in die Berechnung des Passwortes eingehen, entnehmen Sie bitte der Tabelle auf Seite 3 dieser Beschreibung.