InfoSMS, Chatbots und Telegram

Martin Weissenböck

1 InfoSMS

1.1 Die Ziele

Seit nun mehr 10 Jahren setzt sich die Initiative „SCHUL.InfoSMS“ **(Logo rechts)** (http://www.infosms.org) für eine Verbesserung der Kommunikation zwischen Schule und Eltern ein. Vor 10 Jahren war Verständigung mittels SMS die besten Wahl und auch heute haben SMS eine wichtige Rolle für Eltern, deren Handy nur für den SMS-Empfang ausgerüstet ist.

Die Kommunikation über SMS verläuft nur in eine Richtung - monodirektional. Abgesehen von kurzen Bestätigungsmeldungen sind SMS für eine bidirektionale Kommunikation ziemlich ungeeignet. Also eine App? Oder etwas besseres?

1.2 Telegram

Wer über ein Smartphone oder ein Tablett oder einen Laptop- oder einen Desktop-Computer kommunizieren möchte, kann ein wesentlich komfortableres Angebot nutzen. Wir haben uns entschlossen, für die Weiterentwicklung von SCHUL.InfoSMS den Messenger-Dienst *Telegram* (http://telegram.org) zu verwenden.

Telegram stellt für alle genannten Gerätetypen eine einheitliche Benutzerplattform zur Verfügung. Und noch ein Vorteil von *Telegram*: mehrere Geräte können gleichzeitig angemeldet sein, Mitteilungen werden an allen Geräten gleichzeitig empfangen und können von jedem Gerät beantwortet werden.

1.3 Kommunikation mit Chatbots

„Alexa, dreh das Licht auf!“ Ein derartiger Dialog ist sehr bequem und die Sprachsteuerung dringt in immer weitere Bereiche vor. Computer-Programme, die einen Dialog erlauben, nennt man *Chatterbots* oder *Chatbots*. Programme, die nicht versuchen, wie ein menschlicher Gesprächspartner zu wirken, sind *Chatbots* im engeren Sinn.

Der **Screenshot rechts oben** zeigt in einer typischen *Telegram*-Seite den Beginn eines Dialogs, über den ein Termin vereinbart wird.

1.4 Ein Telegram Chatbot

Optisch ähnelt die *Telegram*-Seite oder die *Telegram*-App anderen Messenger-Programmen. Zu den Vorteilen von *Telegram* gehört aber, dass eine gut dokumentierte Benutzerschnittstelle existiert (https://core.telegram.org/bots/api) und dass diese Benutzerschnittstelle mit vielen Funktionen ausgerüstet ist, die den Aufbau eines Chatbots erlauben und unterstützen. Die neuen Funktionen, die

SCHUL.INFOSMS

Telegram für unsere Initiative bietet, gehen weit über die Anwendungen von SMS hinaus. Diese neuen Serviceleistungen fassen wir unter dem Namen SCHUL.InfoService **(Logo unten)** zusammen.

Eine Chatbot ist in *Telegram* von einem menschlichen Dialogpartner dadurch zu unterscheiden, dass sein Name verpflichtend mit "bot" endet

(Bild rechts).

SCHUL.INFOSERVICE

Wie wird nun mit dem Chatbot kommuniziert? Der Chatbot wird über https-Aufrufe gesteuert. Jeder Aufruf besteht aus folgenden Teilen:

- URI von Telegram
- Der Token des Bot (dient zur Identifizierung, vergleichbar mit einem Login)
- Der Name der auszuführenden Anweisung (in der Sprache der objektorientierten Programmierung: der Name der Methode
- Die Parameter der Anweisung (da steht zum Beispiel der Name des Empfängers und der zu sendende Text drinnen)

Ein Beispiel (allgemein):

```
https://api.telegram.org/botToken/
MethodName?Parameter
```

Ein Beispiel (konkret):

```
https://api.telegram.org/
bot100941153:AAFU6w4lGVyxmGiyGXyTRGAy4agyR_
nRiww/sendMessage?
chat_id=24817025&text=Hallo+Welt
```

Oder, zur bessern Übersicht aufgeteilt auf mehrere Zeilen, mit Kommentaren:

`https://api.telegram.org/`	Telegram URI
`bot100741153:AAFU6w4lGVyxmGiyGXy-TRGAy4agyR_nRiww/`	"bot", gefolgt vom Token. Dabei ist der ersten Teil vor dem Doppelpunkt (100741153) die chat_id des Bot
`sendMessage?`	Was soll geschehen? Der Name der Methode
`chat_id=24817025&`	die Identifikation des Empfängers, seine chat_id
`text=Hallo+Welt`	der zu sendende Text

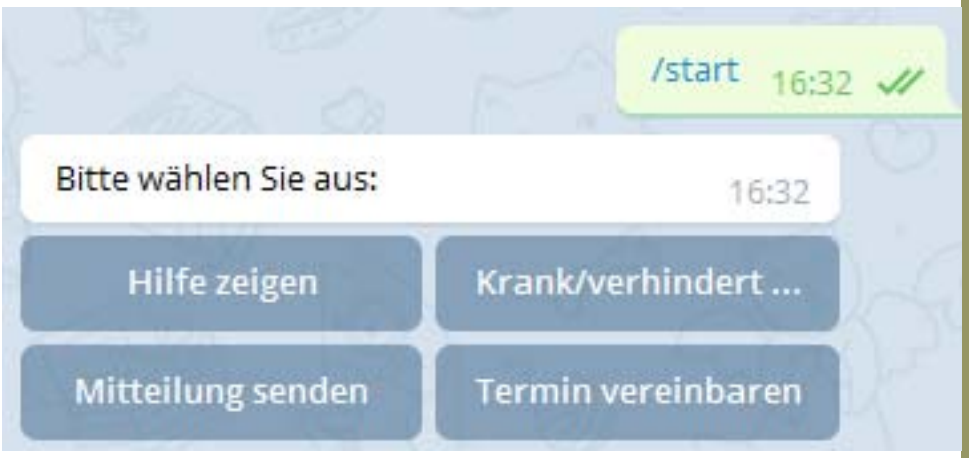
1.6 Beispiel für einen Dialog

Wenn ein Kind z.B. wegen einer Erkrankung nicht zur Schule gehen kann, ist die Schule zu verständigen. Und wie?

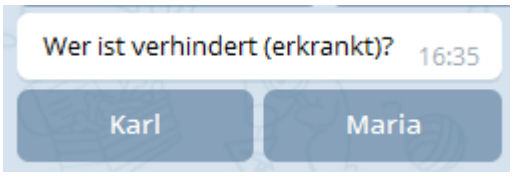
- Per Telefon? Da sind die Leitungen oft besetzt.
- Per E-Mail ? Dann muss die Schule jede E-Mail einzeln aufmachen und bearbeiten.
- Über eine Webseite? Der Login-Vorgang ist lästig, gerade in der Früh, wenn alle keine Zeit haben.
- Oder über einen *Telegram*-Dialog? Dauert 10 Sekunden!

Wer eine App nur selten verwendet, muss sich orientieren und die Auswahlmöglichkeit suchen. Ein Chat ist dagegen ein Dialog, der immer nur das anzeigt, was gerade für den nächsten Schritt wichtig ist. Wie erwähnt: in diesem Beispiel wollen die Eltern ihr Kind krank melden.

Die folgenden Screenshots zeigen eine (vereinfachte) Darstellung dieses Dialogs, der von Eltern eröffnet wird.

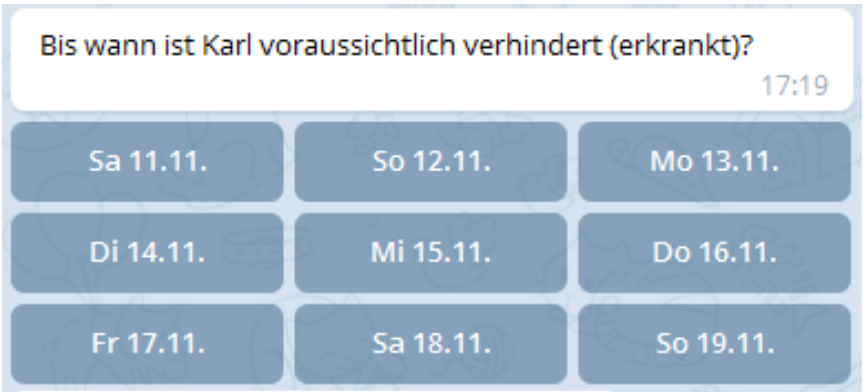


Nach der Wahl „Krank/verhindert“ ist anzugeben, welches Kind krank ist. Ist nur ein Kind registriert, entfällt dieser Schritt natürlich:



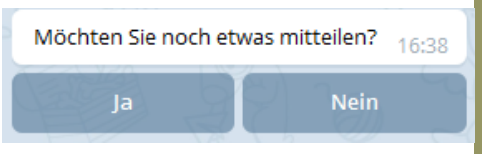
„Karl“ wird gewählt.

Nächster Schritt: wie lange ist Karl voraussichtlich krank (verhindert)?



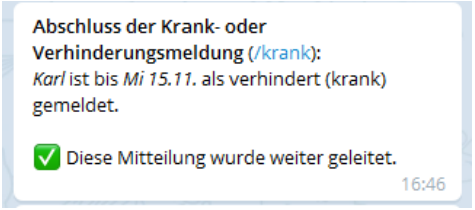
Gewählt wird der 15.11.

Soll noch etwas zur Erklärung angefügt werden?



„Nein“

Damit ist die Eingabe der Mitteilung beendet. Zur Bestätigung wird die Mitteilung noch einmal zusammen gefasst. Die letzte Zeile ist die Bestätigung, dass die Mitteilung angekommen ist und verarbeitet wurde.



2 Fragen zur Bewertung der Kommunikation

Bei der Kommunikation zwischen Schule und Eltern tritt bald die Frage auf,

- wie eine Bestätigung über den Empfang einer Mitteilung registriert werden kann,
- wie sicher gestellt werden kann, dass eine Entscheidung wirklich um Adressaten kommt und
- wie ein Dokument rechtsgültig unterschrieben werden kann – Fragen, die auch bei anderen Formen der Kommunikation interessant sind.

2.1 Rückmeldungen

Hier geht es um Formen der Kommunikation (Senden, Empfangen), die *computergesteuert* durchgeführt werden. Dabei wird untersucht:

- Wie kann festgestellt werden, ob eine Mitteilung den Empfänger erreicht hat? *Empfangsbestätigung*
- Wie kann die Reaktion des Empfängers registriert und verarbeitet werden? *Entscheidung*, *Rückmeldung*
- Wer hat die Mitteilung empfangen oder eine bestimmte Entscheidung getroffen? *Authentifizierung*

2.2 Empfangsbestätigung

Es ist der Nachweis zu erbringen, dass die Nachricht angekommen ist.

2.2.1 Automatische Empfangsbestätigung

Das Empfangsgerät sendet selbständig ein Signal, das automatisch ausgewertet werden kann. Damit ist aber nicht notwendigerweise sicher gestellt, dass der Empfänger die Antwort auch zur Kenntnis genommen hat. Besser: die Bestätigung wird erst nach dem *Öffnen* der Mitteilung verschickt.

2.2.2 Rückantwort als Empfangsbestätigung

Der Empfänger der Nachricht sendet manuell ein Empfangsbestätigung zurück, das dann vom Chatbot, dem ursprünglichen Sender(programm), wieder automatisch ausgewertet werden kann.

2.3 Entscheidung

Der Empfänger der Nachricht wird um eine Entscheidung gebeten, die er manuell zurück sendet und die dann vom ursprünglichen Sender(programm) wieder automatisch ausgewertet werden kann.

2.4 Authentifizierung

Es ist der Nachweis zu erbringen, dass die Nachricht beim vorgesehen Empfänger angekommen ist und dass die Empfangsbestätigung vom vorgesehenen Empfänger kommt

2.4.1 Authentifizierung mit PIN

Für jeden Empfänger wird eine persönliche Identifikationsnummer (PIN) verschlüsselt hinterlegt. Wird der Empfang mit dieser Nummer quittiert, gilt sie als vom Empfänger bestätigt.

- **Vorteil**: sehr einfach zu implementieren
- **Problem**: die PIN ist unbedingt geheim zu halten.

2.4.2 Zwei-Faktor Authentifizierung

Mindestens zwei Faktoren werden benötigt. Die Faktoren können sein:

- **Wissen**: etwas, das der Nutzer weiß, z.B. eine PIN
- **Besitz**: etwas, das der Benutzer hat, z.B. eine Chipkarte oder ein Mobiltelefon
- **Körperliches Charakteristikum**, z.B. der Fingerabdruck, das Muster der Iris, die menschliche Stimme

Zur Authentifizierung werden zwei benötigt. Das Mobiltelefon kann verwendet werden, um eine Bestätigungs-SMS zu empfangen oder einen speziellen Code zu errechnen (siehe Einmal-Passwort im nächsten Abschnitt). Wegen Sicherheitsbedenken wird von der SMS als Bestätigung abgeraten.

- **Vorteil**: wesentlich erhöhte Sicherheit durch zwei notwendige „Faktoren“ (z.B. Gerät und Wissen):

Beispiel:

- **Wissen:** Kenntnis einer Geheimzahl
- **Besitz**: ein Gerät mit installiertem Authentifizierungsprogramm
  (Beispiel: Authenticator von Google),

2.4.3 Einmal-Passwort (OTP One Time Password)

Zwei Varianten:

- Auf dem Gerät des Empfängers ist ein kleines Programm installiert: Der Empfänger gibt seinen Benutzernamen und eine Geheimzahl ein, das Programm errechnet daraus und aus der Uhrzeit einen Code. Der Code ist nur eine kurze Zeit gültig und wird an den ursprünglichen Sender (den Chatbot) übermittelt. Besteht der Code die Überprüfung, war die Authentifizierung erfolgreich.
  - Beide Partner (Sender und Empfänger) müssen die genaue Uhrzeit wissen – ist durch LAN, WLAN oder GPS sicher gestellt.
- Ein Einmal-Passwort (Transaktionsnummer, TAN) wird an den Nutzer per SMS oder E-Mail übermittelt. Es wird davon ausgegangen, dass nur der rechtmäßige Nutzer diese TAN empfangen kann. Häufig verwendet von Banken; allerdings tendieren Banken wegen Sicherheitsbedenken beim Empfang von SMS zu eigenen Lösungen.

2.4.4 PGP oder GPG als digitale Unterschrift

PGP / GPG verwendet asymmetrische Kryptographie. Die Empfangsbestätigung oder Entscheidung des Empfängers wird mit dem privaten Code des Empfängers verschlüsselt und gesendet. Der ursprüngliche Sender entschlüsselt die Nachricht mit dem öffentlichen Code des Empfängers. Damit ist die Authentizität des Empfängers gesichert. Zum Thema PGP (oder GPG) gibt es umfangreiche Literatur und Erklärungen im Internet.

- **Vorteil**: weit verbreitet, über verschiedenste Programmbibliotheken leicht zu installieren. Einfach anwendbar.
- **Problem**: der öffentliche Schlüssel (und der private) Schlüssel wird selbst erzeugt. Die Gültigkeit wird (nur) durch das „Netz des Vertrauens“ garantiert.
- **Nachteil**: da die Keys von keiner staatlichen Stelle bestätigt. werden, kann damit nicht rechtsgültig unterschrieben werden.

Die Sicherheit der PGP-Methode hängt vor allem von dem Vertrauen ab, dass der hinterlegte öffentliche Schlüssel tatsächlich einer bestimmten Person zuzuordnen ist. Wenn aber der Personenkreis – wie im Fall einer Schule – überschaubar ist, kann diese „Netz des Vertrauens“ in der Schule selbst errichtet werden.

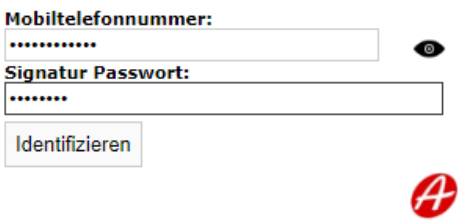
2.4.5 Digitale Signatur

Gemäß Signaturgesetz (Signatur- und Vertrauensdienstegesetz (SVG), BGBl. I Nr. 50/2016) ist in Österreich eine digitale Unterschrift einer händischen Unterschrift gleich gestellt. Die ersten Implementierungen haben einen speziellen Kartenleser (meist mit USB-Anschluss) sowie die Registrierung von bestimmen Karten (z.B. eCard) erfordert, Die komplizierte und umständliche Handhabung hat die Verwendung auf einen kleinen Kreis von Personen beschränkt, die die digitale Signatur berufsbedingt unbedingt benötigt haben.

Erst mit der Einführung der Handysignatur hat das Verfahren eine nennenswerte, aber immer noch nicht besonders hohe Verbreitung gefunden. Für Schulen und das Schulpersonal wurde ein recht einfaches Verfahren zur Registrierung entwickelt, leider nicht auch für die Eltern.

Wie funktioniert die Authentifizierung? Auf einer Webseite wird (oft als Iframe) ein vom Signierdienstleister erzeugtes Fenster angezeigt, in das die Handynummer und eine Geheimzahl des Nutzers einzugeben sind.

Der Signierdienstleister erzeugt daraus eine TAN (Transaktionsnummer), die per SMS oder QR-Code an den Nutzer geschickt wird.



Der Nutzer trägt nun die empfangene TAN in das Fenster ein oder fotografiert den QR-Code über eine App. Damit ist die Authentizität des Nutzers sicher gestellt.

Die Sicherheit ist durch die Verwendung von zwei Elementen sehr hoch:

- Das Mobiltelefon (Besitz) und
- die Geheimzahl (Wissen).

Die Eigenschaften

- **Vorteil**: das einzige Verfahren, das die rechtliche Gleichstellung mit einer händischen Unterschrift sichert
- **Problem**: der Nutzer muss seine Mobiltelefonnummer registrieren lassen. Neue rechtliche Vorschriften werden das in Zukunft vereinfachen, da mit der Ausstellung eines Reisepasses die digitale Signatur gleichzeitig vergeben wird. Bei einer Gültigkeitsdauer des Reisepasses von 10 Jahren dauert es aber bis zur flächendeckend verbreiteten digitalen Signatur noch lange.
- **Nachteil**: bei der Entwicklung der Handysignatur wurde es als selbstverständlich angesehen, dass die notwendigen Eingaben auf einem (Stand-)PC durchgeführt werden und zur Sicherung ein Mobiltelefon eingesetzt wird. Das entspricht aber nicht dem heutigen Nutzerverhalten: der Einsatz leistungsfähiger Smartphones oder Tabletts und auch der Wunsch nach größtmöglicher Mobilität führt dazu, dass Desktop-PCs vor allem im privaten Bereich immer seltener werden. Die sinkenden Verkaufszahlen bestätigen das.

  Natürlich kann der Authentifizierung auch mit nur *einem* Smartphone oder Tablett (dann aber ohne die Bequemlichkeit des QR-Codes) durchgeführt werden. Seitens der verantwortlichen Stellen wird das aber „wegen geringerer Sicherheit“ (?) nicht gewünscht. Nun, es kann wohl niemand vorgeschrieben werden, auf welchem Gerät er eine Webseite betrachten will. Somit ist zu hoffen, dass die Handysignatur oder nachfolgende Verfahren in Zukunft mit dem Smartphone allein möglichst benutzerfreundlich eingesetzt werden können.

2.4.6 Biometrische Authentifizierung

Die Abfrage des Fingerabdrucks funktioniert bei manchen Mobiltelefonen schon sehr zuverlässig. Weitere Verfahren: Auswerten der Sprache oder Gesichtserkennung. Es ist geplant, in einem späteren Artikel diese Möglichkeiten zu untersuchen.

3 Verwendung von SMS

3.1 Empfangsbestätigung

3.1.1 Automatische Empfangsbestätigung

Beim Versand von SMS über einen professionellen Betreiber wird eine Zustellbestätigung automatisch erzeugt. Manche Provider verrechnen dafür allerdings Gebühren wie für den Versand selbst.

- **Vorteil**: automatische Verarbeitung möglich
- **Nachteil**: ggf. Kosten für jede Empfangsbestätigung

3.1.2 Rückantwort als Empfangsbestätigung

Für die Auswertung einer Rückantwort ist eine eigene „Telefonnummer“ für den Empfang von SMS notwendig. Leider ist die Grundgebühr für eine Empfangsnummer sehr hoch, sodass für *alle* Nutzer eines SMS-basierten Kommunikationsdienstes nur *eine* Nummer verwendet wird.

- **Vorteil**: (fast) jeder hat ein Handy mit SMS-Dienst
- **Nachteil**: die Rückantwort muss einem exakten Schema folgen, sonst kann sie nicht ausgewertet werden

3.2 Abfragen einer Entscheidung

Der Empfänger wird gebeten, per SMS seine Meinung bekannt zu geben.

- **Vorteil**: (fast) jeder hat ein Handy mit SMS-Dienst
- **Nachteil**: die Rückantwort muss einem exakten Schema folgen, sonst kann sie nicht ausgewertet werden. Eine Rückantwort kann nur dann als authentisch gelten, wenn sicher gestellt ist, dass das Mobiltelefon nur vom vorgesehen Empfänger benutzt wird.

3.3 Authentifizierung

3.3.1 Authentifizierung mit PIN

- **achteil**: Mobiltelefone und Smartphones speichern meist die Dialoge, somit auch die Eingabe der Geheimzahl. Eine verdeckte Eingabe ist nicht möglich. Damit wird sie aber für alle sichtbar, die das Mobiltelefon (Smartphone) in die Hand bekommen. Vom Standpunkt der Sicherheit daher nicht brauchbar.

3.3.2 Zwei-Faktor Authentifizierung und Einmal-Passwort

Nur in Verwendung mit einem Webbrowser möglich. Die Codezahl kann am Handy / Laptop / Computer erzeugt werden oder ein Einmal-Passwort (Transaktionsnummer, TAN) kann per SMS empfangen werden.

- **Vorteil**: da jedes Mal eine andere Codezahl erzeugt wird, macht es nichts, wenn die Zahl sichtbar bleibt.
- **Nachteil**: da eine App zur Berechnung der Codezahl benötigt wird, ist zumindest ein Smartphone oder Tablett notwendig.

3.3.3 PGP als digitale Unterschrift

Es gab Apps, mit denen eines SMS mittels PGP verschlüsselt wird. Durch verschlüsselte Messenger-Kommunikation nicht mehr aktuell, diese Apps werden kaum weiter entwickelt.

3.3.4 Digitale Signatur

Erfordert einen Internet-Zugang, mit SMS allein nicht möglich

4 Verwendung von E-Mails

4.1 Empfangsbestätigung

4.1.1 Automatische Empfangsbestätigung

Für bestimmte E-Mail-Systeme möglich, solange nur innerhalb dieses Systems E-Mails versendet werden. Sobald aber nicht alle Nutzer dasselbe E-Mail-System verwenden, ist eine automatische Empfangsbestätigung nicht möglich.

4.2 Rückantwort als Empfangsbestätigung

In die E-Mail wird ein Link zur Bestätigung eingefügt. Die Auswertung eines derartigen Links ist technisch einfach.

4.3 Abfragen einer Entscheidung

In die E-Mail wird für jede Alternative ein Link zur Bestätigung eingefügt. Die Auswertung eines derartigen Links ist technisch einfach.

4.4 Authentifizierung

4.4.1 Authentifizierung mit PIN

In der E-Mail ist ein Link enthalten, der zu einer Webseite zur Eingabe der PIN führt.

- **Vorteil**: einfach zu Implementieren
- **Nachteil**: die PIN könnte durch ein Key-Logger Programm ausgelesen werden

4.4.2 Zwei-Faktor Authentifizierung und Einmal-Passwort

Nur in Verwendung mit einem Webbrowser oder einem Zusatzprogramm möglich. Die Codezahl kann am Handy / Laptop / Computer erzeugt werden oder ein Einmal-Passwort (Transaktionsnummer, TAN) kann per E-Mail empfangen werden.

4.4.3 PGP als digitale Unterschrift

Technisch gesehen sehr zu empfehlen, da viele E-Mail-Programm dies unterstützen und PGP-signierte Mitteilungen leicht zu verfassen sind.

4.4.4 Digitale Signatur

In einer E-Mails kann auf eine Webseite verwiesen werden, auf der eine digitale Unterschrift geleistet werden kann.

5 Verwendung des Messenger-Dienstes Telegram

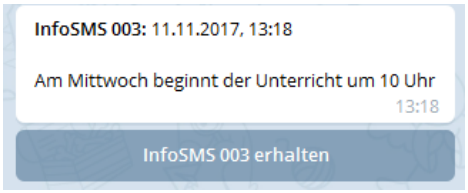
5.1 Empfangsbestätigung

5.1.1 Automatische Empfangsbestätigung

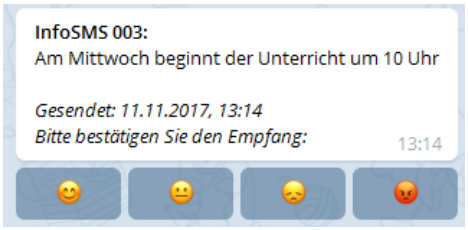
Obwohl Messenger-Programme im direkten Dialog zwischen zwei Nutzern eine Bestätigung austauschen, dass eine Mitteilung angekommen ist, und eine andere Bestätigung, dass eine Mitteilung zum Lesen geöffnet wurde, ist diese Rückmeldung im Messenger-Dienst *Telegram* nicht möglich, sobald Mitteilungen per Computer gesendet oder empfangen werden.

5.1.2 Rückantwort als Empfangsbestätigung

Die Empfangsbestätigung per Rückantwort geht in *Telegram* besonders einfach: am Ende der Mitteilung wird bei einem Chatbot beispielsweise ein Bestätigungsbutton angezeigt, der nur gedrückt zu werden braucht.

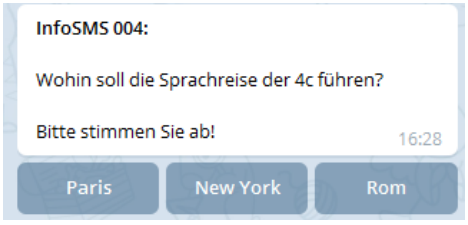


Will man dem Empfänger die Möglichkeit geben, seine Emotionen auszudrücken, können auch mehrere Buttons angeboten werden.



5.2 Abfragen einer Entscheidung

Auch alle Arten von Rundfragen und Abstimmungen sind über Telegram besonders einfach, benutzerfreundlich und schnell möglich. Es ist zu hoffen, dass der Einsatz dieses Werkzeugs verstärkt zur Meinungsbildung in der Schule genutzt wird.



Oder:

5.3 Authentifizierung

Da alle Geräte, auf denen der Messenger-Dienst läuft, üblicherweise schon nach dem Einschalten eine Anmeldung erfordern, ist bei *Telegram* keine weitere Identifikation zwingend notwendig, kann aber aktiviert werden. Trotzdem bietet das allein keine hundertprozentige Sicherheit. Nur bei der Webvariante und der portable Variante (Nutzung auf einem PC ohne Installation, z.B. von einem USB-Stick aus) muss der Nutzer zusätzlich über eine TAN identifiziert werden.

5.3.1 Authentifizierung mit PIN

Telegram sieht leider (noch?) keine verdeckte Eingabe von Text (für die Eingabe von Passwörtern) vor. Im Programm SCHUL.InfoService wurde das aber behoben, sodass PINs zur Identifikation benutzt werden können und und auch keine Gefahr besteht, dass diese PINs ausgelesen werden.

5.3.2 Zwei-Faktor Authentifizierung

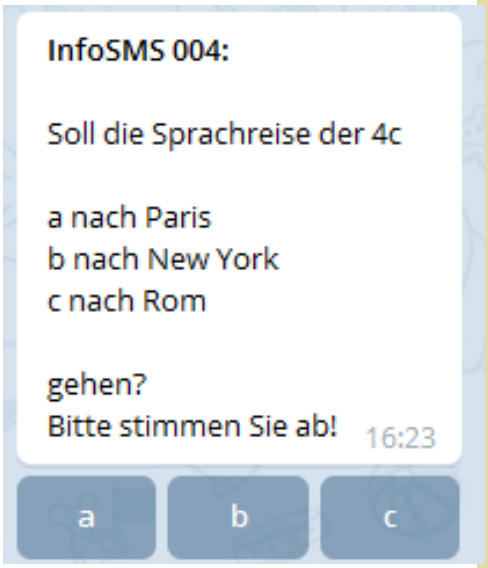
Natürlich kann auch eine App, wie der Google Authenticator, zur Zwei-Faktor Authentifizierung eingesetzt werden.

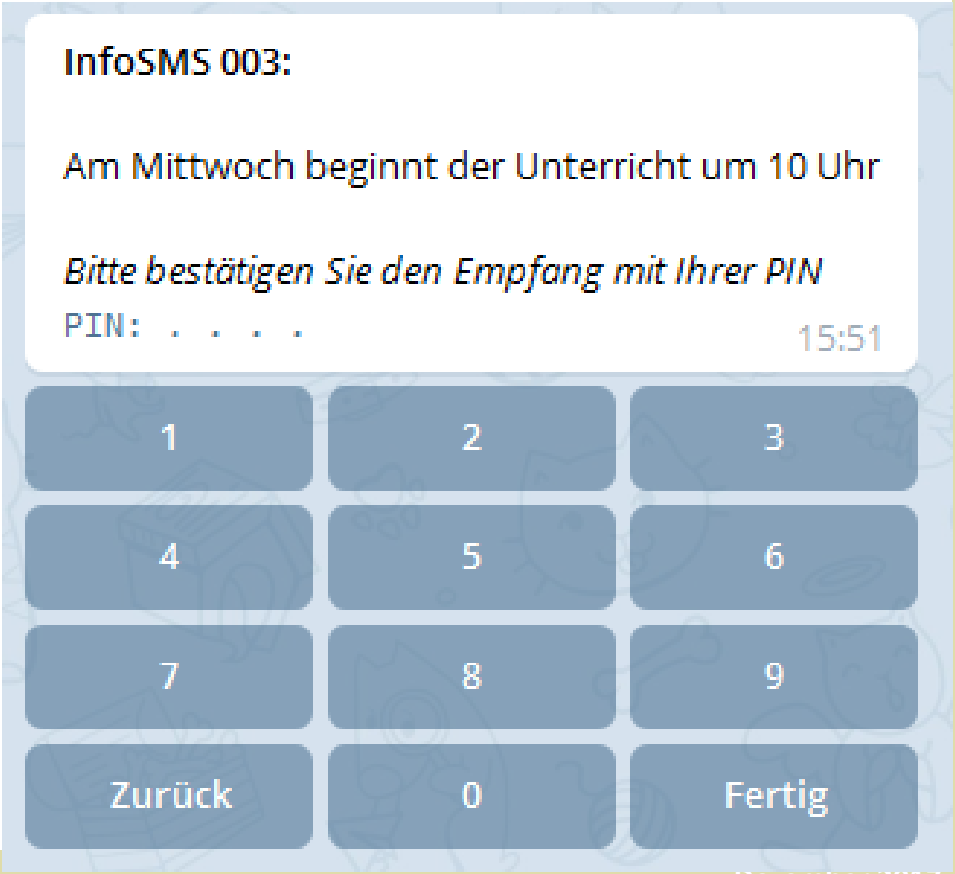
5.3.3 PGP als digitale Unterschrift

Telegram verschlüsselt die Nachrichten selbst. Es ist kein Programm bekannt, in dem *Telegram* und PGP zusammen arbeiten. In jeder Telegram-Nachricht ist der Absender enthalten.

5.3.4 Digitale Signatur

SCHUL.InfoService bietet eine sehr bequeme Möglichkeit, Umfragen, Entscheidungen, Dokumente usw. mit der Handysignatur digital zu signieren.





6 Telegram

6.1 Die Sicherheit von Telegram

Der Messenger-Dienst *Telegram* bietet für die Kommunikation zwischen Schule und Eltern viele Vorteile, manche Dienste sind anders nur mit hohen Kosten oder technisch überhaupt nicht umsetzbar. In Diskussionsforen wird *Telegram* oft wegen seiner eigenentwickelten Verschlüsselungsmethode kritisiert. *Telegram* hat einen Preis von 200.000 $ für einen erfolgreichen Hacker ausgesetzt – der Preis ist bisher nicht eingelöst worden.

6.2 Telegram installieren

Sie möchten gerne *Telegram* nutzen? Falls Sie SCHUL.InfoService mit allen Diensten verwenden wollen, ist das notwendig. *Telegram* läuft

- auf fast jedem Smartphone oder Tablett mit Android, iPhone oder Windows Mobile,
- jedem Laptop- oder Desktop-Computer unter Windows, macOS oder Linux,
- ja sogar von einem USB-Stick als Portable Version für Windows
- oder schließlich einfach über einen Webbrowser.

Rufen Sie https://telegram.org/dt auf: je nach verwendetem Gerät wird Ihnen eine Version vorgeschlagen oder Sie wählen selbst aus. Die Installation selbst ist sehr einfach und selbsterklärend.

6.3 Zweistufige Bestätigung einschalten

Telegram erlaubt, mehrere Geräte für einen Nutzer zu registrieren. Das ist sehr nützlich, erlaubt aber auch eine Registrierung auf einem fremden Gerät, wenn beispielsweise das Mobiltelefon auch nur kurz jemand anderem überlassen wird. **Daher wird unbedingt empfohlen, die zweistufige Bestätigung zu aktivieren.** Für jede Neuinstallation oder Aktivierung ist dann die Eingabe eines selbst gewählten Codes notwendig.

So geht's:

Auf das Menü-Symbol (drei waagrechte Striche) links oben klicken. **(Bild 6.1)**

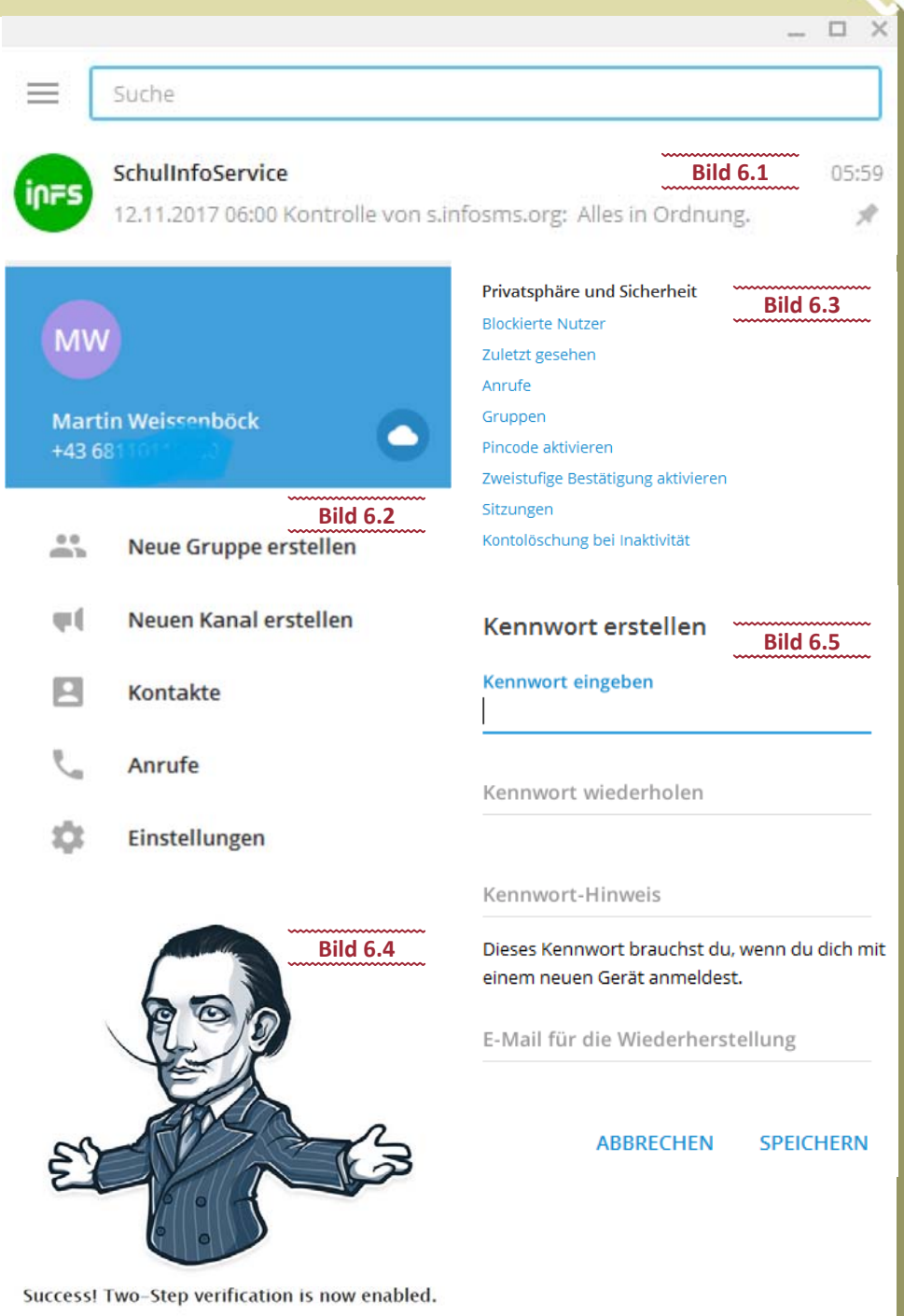
„Einstellungen" wählen **(Bild 6.2)**

Nach unten zu „Privatsphäre und Sicherheit" scrollen **(Bild 6.3)**

In dieser Gruppe gibt es eine Reihe von interessanten Einstellungen: lästige Nutzer können blockiert werden, ein Pincode sichert *Telegram* zusätzlich, parallel Sitzungen werden angezeigt und bei Bedarf geschlossen und die „Lebensdauer" des Telegramkontos bei Inaktivität kann festgelegt werden. Zuerst wird aber die zweistufige Bestätigung aktiviert:

„Zweistufige Bestätigung aktivieren" anklicken **(Bild 6.4)** – legen Sie ein Kennwort fest:

Kennwort festlegen, wiederholen, eventuell einen Hinweis und eine E-Mail-Adresse eintragen. Dann: die E-Mail abfragen und bestätigen! Damit ist die Zwei-Faktor Authentifizierung (die zweistufige Verifikation) aktiviert. **(Bild 6.5)**



Das Bild ist übrigens ein Beispiel für einen Sticker, der bei einer Mitteilung einfach mit geschickt werden kann.

Weitere Option, bei Bedarf verwenden:

Pincode aktivieren

Damit kann *Telegram* gesperrt werden und nur mit einem persönlichen *Pincode* geöffnet werden.

Sitzungen

Damit kann überprüft werden, auf welchen Geräten die eigene Telegram-Instanz zuletzt aktiviert wurde. Wenn der Verdacht eines Missbrauchs besteht oder wenn nicht alle genannten Geräte „in Reichweite" sind, können alle Geräte außer dem gerade verwendeten hier abgemeldet werden.

7 Schlussfolgerungen für InfoSMS / InfoService

SCHUL.INFOSMS

SCHUL.INFOSERVICE

- Für Einwegbotschaften, bei denen nur eine automatische Empfangsbestätigung notwendig ist, haben sich SMS bewährt und werden auch weiterhin eingesetzt.
- Nutzer, die ein Smartphone, ein Tablett, einen Laptop-Computer oder einen anderen PC einsetzen, werden eingeladen, *Telegram* zu installieren und die komfortableren Kommunikationsmöglichkeit verwenden zu können.
- Die Authentifizierung mittels SMS oder E-Mail setzt voraus, dass durch eine schriftliche Vereinbarung sicher gestellt wird, dass nur der rechtmäßige Empfänger Antworten verfasst.
- Zur Authentifizierung über *Telegram* ist in den meisten Fällen eine PIN ausreichend.
- Mit der Zwei-Faktor Authentifizierung wird eine Sicherheitsstufe erreicht, die mit den in Banken eingesetzten Sicherheitsstufen vergleichbar ist. Es darf angenommen werden, dass das für schulische Zwecke auch reicht.
- Abläufe, bei denen eine nachweisliche Zustellung erforderlich ist, wären auf elektronischem Weg nur in folgender Form umzusetzen:
  - Der Empfänger signiert mit der Handysignatur. Das geht natürlich nur, wenn im Kreis der Empfänger die Handysignatur ausreichend vertreten ist. Daher sollten parallel Werbemaßnahmen erfolgen, die die Eltern zum Einsatz der Handysignatur bewegen.
  - Der Empfänger enthält die Information und bestätigt durch konkludentes Handeln den Empfang. Beispiel: Eltern bekommen eine Frühwarnung und melden sich zu einer Sprechstunde an. Mittels *Telegram* lässt sich das besonders zeitsparend umsetzen.
- Vorgänge, bei denen eine rechtsgültige Unterschrift erforderlich ist, wären auf elektronischem Weg nur in folgenden Fällen möglich:
  - Der Empfänger signiert mit der Handysignatur. Das geht natürlich nur, wenn im Kreis der Empfänger die Handysignatur ausreichend vertreten ist. Daher sollten parallel Werbemaßnahmen erfolgen, die die Eltern zum Einsatz der Handysignatur bewegen.
  - Eine Einverständniserklärung der Empfänger (z.B. der Eltern), dass eine besonders (z.B. durch eine PIN oder eine Zwei-Faktor-Authentifizierung) gesicherte Willenserklärung wie eine händische Unterschrift zu werten ist. Privatschulen haben in diesem Zusammenhang den Vorteil, derartige Vereinbarungen in den Ausbildungsvertrag aufnehmen zu können.
  - PGP kommt dabei eine besondere Bedeutung zu: wird das „Netz des Vertrauens“ in der Schule selbst eingerichtet, sollte es kein Problem sein, eine PGP-gesicherte Einverständniserklärung der Empfänger wie eine händische Unterschrift zu werten. Auch hier haben Privatschulen den Vorteil, derartige Vereinbarungen in den Ausbildungsvertrag aufnehmen zu können.

Der SCHUL.InfoService Chatbot kann nur von registrierten Usern verwendet werden. Möchten Sie diesen Dienst in einer Schule einsetzen? Derzeit sind rund 100 Schulen registriert. Zur Anmeldung schreiben Sie eine E-Mail an office@infosms.org. Sie können auch gerne einen Testbetrieb mit einer Klasse anmelden!

Für die nächste Ausgabe der PCNEWS sind weitere Details über SCHUL.InfoSMS und SCHUL.InfoService geplant.