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.