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.