QR-Codes auf Verwaltungsdokumenten*

Feinkonzeption zur Infrastruktur und zur Erfüllung des Schriftformerfordernis

Arbeitsgruppe *QR-Codes auf Verwaltungsdokumenten*
des IT-Planungsrats

* QR Code ist eine eingetragene Wortmarke der DENSO WAVE INCORPORATED.

Historie

Version	Datum	Bearbeiter	Status/Bemerkung
0.1	16.06.2017	<Heiko Glandt>	Initiale Erstellung
0.2	06.10.2017	<Heiko Glandt>	Abschluss der Erstbefüllung
0.3	17.10.2017	<Heiko Glandt>	Einarbeitung von Rückmeldungen
0.4	11.11.2017	<Heiko Glandt>	Weitere Ausarbeitung
0.5	17.11.2017	<Heiko Glandt>	Einarbeitung von Rückmeldungen
0.6	24.11.2017	<Heiko Glandt>	Weitere Ausarbeitung
0.7	30.11.2017	<Heiko Glandt>	Einarbeitung von Rückmeldungen
0.8	18.12.2017	<Heiko Glandt>	Einarbeitung von Rückmeldungen
1.0	30.12.2017	<Heiko Glandt>	Finale Version

Autoren

Firma / Behörde	Name	Rolle
<Finanzbehörde 172>	<Heiko Glandt>	<Verantwortlicher>

INHALT

Abbildungsverzeichnis

Tabellenverzeichnis

Management Summary

Im Rahmen der Maßnahme „QR-Codes auf Verwaltungsdokumenten“ hat der IT-Planungsrat zum einen beschlossen, eine Feinkonzeption im Hinblick auf die Infrastruktur zu erstellen und zum anderen zu prüfen, ob QR-Codes in Verbindung mit einem Servicekonto das Schriftformerfordernis erfüllen können.

Im Hinblick auf die Infrastruktur wird davon ausgegangen, dass Portale und Servicekonten gegeben sind. Die Infrastruktur ist fachneutral, so dass je nach fachlichen Anforderungen unterschiedliche QR-Codes mit einfachen und komplexen Inhalten erstellt und geprüft werden können. Die Erstellung soll grundsätzlich in zwei verschiedenen Formen betrieben werden können, in einer über das Internet erreichbaren Cloud oder lokal im eigenen Rechenzentrum. Die Erstellfunktion muss über robuste, leicht implementierbare Schnittstellen aufrufbar sein. Die Prüfung wird sowohl online als auch offline ermöglicht.

QR-Codes können nur von Mitarbeiterinnen und Mitarbeitern der Verwaltung und Fachanwendungen der öffentlichen Verwaltung erstellt werden. Erstell- und Prüfkomponenten sind jeweils skalierbar. Instanzen einer Komponente lassen sich mehrfach bzw. parallel starten, um flexibel auf Anfragen reagieren zu können.

Über das konkrete Anforderungsniveau hinsichtlich Verfügbarkeit und Ausfallsicherheit entscheidet grundsätzlich die Organisation der Fachanwendung. Es wird aber empfohlen, hohe Anforderungen an die Erstell- und Prüfkomponenten zu stellen.

Im Hinblick auf das Schriftformerfordernis erfüllt die vorgeschlagene Lösung von QR-Codes in Verbindung mit Servicekonten die rechtlichen Anforderungen an Authentizität, Integrität und Barrierefreiheit, die an ein „sonstiges sicheres Verfahren“ im Sinne des § 3 a Absatz 2 Nr. 4 VwVfG gestellt werden.

Die Registrierung und Anmeldung entsprechend der Richtlinie TR-03107 (Elektronische Identiäten und Vertrauensdienste im E-Government) erfüllt die Anforderungen an die Authentizität. Das notwendige Anmeldeniveau (normal, substanziell, hoch) legt das anwendende Fachverfahren fest. Die Verwaltungskundin bzw. der Verwaltungskunde identifiziert sich dabei gegenüber der Verwaltung und eröffnet den Zustellweg. Bei der Zustellung und dem Empfang werden zudem folgende Funktionen der Schriftform erfüllt: Willenserklärung, Beweisfunktion, Klarstellungsfunktion

Die Integrität wird zum einen durch die im QR-Code verschlüsselten Daten und zum anderen durch die Nutzung eines Hashwertes oder eines Zertifikates gewährleistet. Bei der Erzeugung werden zudem folgende Funktionen der Schriftform erfüllt: Willenserklärung, Beweisfunktion, Klarstellungsfunktion. Die Verwaltungskundin bzw. der Verwaltungskunde oder eine dritte Person bzw. Instanz kann das Verwaltungsdokument mit Hilfe des QR-Codes on- oder

offline auf Authentizität und Integrität prüfen. Dadurch werden folgende Funktionen der Schriftform erfüllt: Beweisfunktion, Klarstellungsfunktion, Warnfunktion / Hinweisfunktion.

Die Weboberfläche, über die die Registrierung und Anmeldung im Servicekonto geschieht, ist gemäß den entsprechenden Vorschriften ebenso barrierefrei wie die Bedienung des Postfaches. Der QR-Code, insbesondere die Prüfinstanz ist über entsprechende Hard- und Software barrierefrei zugänglich.

Die Arbeitsgruppe zu den QR-Codes auf Verwaltungsdokumenten empfiehlt dem IT-Planungsrat daher folgende Beschlussfassung:

1. Der IT-Planungsrat nimmt die Konzeption zum Aufbau einer Infrastruktur zum Erstellen sowie zum Prüfen zur Feststellung der Validität (der Inhalte) der Dokumente zur Kenntnis.

2. Der IT-Planungsrat hält QR-Codes in Verbindung mit Servicekonten für ein geeignetes Verfahren im Sinne des § 3a Abs.2 Nr. 4 VwVfG zur Erfüllung des Schriftformerfordernisses.

3. Der IT-Planungsrat empfiehlt der Bundesregierung, QR-Codes in Verbindung mit Servicekonten im Sinne des § 3a Abs.2 Nr. 4 VwVfG als „sonstiges sicheres Verfahren“ in einer entsprechenden Rechtsverordnung festzulegen.

4. Nach der Verabschiedung der Rechtsverordnung setzt der IT-Planungsrat eine neue Arbeitsgruppe ein, um konkrete Maßnahmen zum Aufbau der notwendigen Infrastruktur als Anwendung des IT-Planungsrats zu ergreifen.

1 Einführung

Im Jahr 2016 wurde im Auftrag des IT-Planungsrats eine Maßnahme zu „QR-Codes auf Verwaltungsdokumenten“ durchgeführt. Dazu wurde aus den Ländern und dem Bund eine entsprechende Arbeitsgruppe gebildet. Über die Arbeitsgruppe wurden Themen und Fragestellungen zu den QR-Codes erarbeitet, wie diese im Verwaltungskontext eingesetzt werden können. Das Ergebnis der Maßnahme ist ein umfängliches Rahmenwerk, welches zu den Themen und Fragestellungen Erläuterungen, Beschreibungen und Lösungsansätze bereitstellt.

Aus dem Rahmenwerk haben sich zwei besondere Aspekte herauskristallisiert, auf die hier näher eingegangen wird:

(1) Feinkonzeption zu einer Infrastruktur für die QR-Code-Erstellung und –Prüfung bzw. -Validierung

(2) QR-Codes in Verbindung mit Servicekonten zur Erfüllung des Schriftformerfordernisses nach den Verwaltungsverfahrensgesetzen

Auf der 22. Sitzung des IT-Planungsrats im März 2017 wurde daher beschlossen, zur Ende 2016 abgeschlossenen Maßnahme „QR-Codes auf Verwaltungsdokumenten“ eine Anschlussmaßnahme zum Thema der QR-Code-Verwendung mit folgender Beschlussformulierung anzusetzen:

1. Der IT-Planungsrat nimmt den Abschlussbericht der Arbeitsgruppe zur Maßnahme „QR-Codes auf Verwaltungsdokumenten“ zur Kenntnis.

2. Der IT-Planungsrat bittet die Arbeitsgruppe auf Basis des Abschlussberichtes um:

- die Erstellung einer Feinkonzeption zum Aufbau einer Infrastruktur zum Erstellen von QR-Codes für Verwaltungsdokumente sowie zum Prüfen dieser QR-Codes zur Feststellung der Validität der (Inhalte der) Dokumente

- Prüfung, ob Ausgangsdokumente mit einem (durch die Verwaltung) prüfbaren QR-Code, welche zukünftig in Verbindung mit einem Servicekonto dem Verwaltungskunden bereitgestellt werden, das Schriftformerfordernis nach § 3a der Verwaltungsverfahrensgesetze der Länder und des Bundes erfüllen können.

Die Verwendung von QR-Codes und die sich daraus ergebenden Vorteile (z.B. schnelleres Einlesen von Fachdaten, Prüfen von Fachdaten (vgl. im Einzelnen die Ausführungen im Rahmenwerk)) steigen mit der Zahl der Anwendungsfälle. Weitere Vorteile sind dem Rahmenwerk zu entnehmen. Bei Verwaltungsverfahren, deren Fallzahl unter 500 Vorgängen pro Jahr liegt, d.h. weniger als 500 QR-Codes pro Jahr benötigt werden, sollte der wirtschaftliche Nutzen einer Anbindung an die Infrastruktur entsprechend geprüft werden.

Dieses Dokument erläutert die Konzeptionsüberlegungen im Hinblick auf die Infrastruktur und die Erfüllung des Schriftformerfordernisses und das Vorgehen für mögliche Umsetzungsschritte.

2 Infrastruktur

Im folgenden Kapitel werden die technischen Rahmenbedingungen sowie die Struktur und der Aufbau der Infrastruktur für die Erzeugung und Prüfung des QR-Codes erläutert. Schließlich werden die nutzbaren Funktionen der Architektur im Detail eruiert.

2.1 Rahmenbedingungen

Die vorliegende Konzeption zur Erstellung und Prüfung von QR-Codes bezieht sich auf den technischen Kontext des QR-Codes, d.h. es können je nach fachlicher Anforderung inhaltlich völlig unterschiedliche QR-Codes (mit einfachen oder komplexeren Inhalten) erstellt und geprüft werden. Zudem wird die vorgeschlagene Infrastruktur klar von anderen Komponenten wie beispielsweise Portalen und Servicekonten abgegrenzt. Es wird hier davon ausgegangen, dass diese Komponenten gegeben sind.

2.1.1 Erstellen von QR-Codes durch Nutzer für Fachanwendungen

Das Erstellen von QR-Codes über die Infrastruktur ist nur für Verwaltungsmitarbeiterinnen und –mitarbeiter sowie Fachanwendungen der öffentlichen Verwaltung möglich. Bürgerinnen bzw. Bürger sowie Firmenkunden können keine QR-Codes mit der Infrastruktur erstellen.

Da die Infrastruktur fachneutral gehalten wird, können QR-Codes für unterschiedliche fachliche Einsatzszenarien erzeugt werden. Eine Einschränkung qualitativer Art auf bestimmte fachliche Kontexte gibt es nicht. Die Beschränkungen richten sich eher nach dem fachlichen Umfang der in den QR-Codes zu codierenden Informationen. Im folgenden Kapitel 2.1.2 wird auf die Kapazität von QR-Codes eingegangen.

2.1.2 Funktionsumfang der QR-Codes

Art des QR-Codes

Die Infrastruktur erstellt und prüft QR-Codes nach dem Standard ISO/IEC 18004:2015 (Version Model 2). Damit werden folgende Arten von QR-Codes nicht verwendet: Micro-QR-Codes, iQR-Codes, Secure-QR-Codes (SQRC) sowie Logo-QR- bzw. Design-QR-Codes.

Im Einzelfall sollte entsprechend den Anforderungen von anzubindenden Fachverfahren geprüft werden, ob die Infrastruktur in einer weiteren Ausbaustufe auch andere zweidimensionale Codes (z.B. DataMatrix-Code, Aztec-Code) erzeugen und prüfen kann. Hierbei sollte dargelegt werden, warum Standard-QR-Codes diese Anforderungen erfüllen oder nicht erfüllen können.

Um in einer ersten Stufe eine Standardisierung der Infrastruktur zu gewährleisten, wird die Infrastruktur sich zunächst auf Standard-QR-Codes (Version Model 2) beschränken (vgl. nähere Ausführungen Rahmenwerk QR-Codes auf Verwaltungsdokumenten, IT-Planungsrat, 2016).

Speicherumfang des QR-Codes

Standard-QR-Codes besitzen eine Datenkapazität von 2.953 Bytes. Damit die Infrastruktur stabil funktionierende QR-Codes erzeugen kann, wird die zu codierende Information auf ihren Datenumfang geprüft. Es wird aus Stabilitätsgründen nur ein Datenumfang zugelassen, der 2.900 Bytes nicht überschreitet. Der „Erstellende Service“ (siehe Kapitel 2.2.1.) wird diese Grenze von 2.900 Bytes automatisch prüfen.

Konkretere Beschreibungen zu den „Services“ („Erstellender Service“ und „Konsumierender Service“) und den in den QR-Codes verwendeten Daten und Datenstrukturen finden sich in den Kapiteln 2.2 und 2.3.

2.1.3 Durchsatz und Antwortzeiten der Infrastruktur

Hinsichtlich des Durchsatzes und der Antwortzeiten werden bei der Erstellung und der Prüfung unterschiedliche Anforderungen an die Infrastruktur gestellt.

In der täglichen Arbeit kommt es bei der *Erzeugung* von QR-Codes vor allem auf den Durchsatz an. Der Durchsatz erfasst die Mengen gleichzeitig zu verarbeitenden Anfragen. Im Verwaltungsalltag werden täglich sehr viele Dokumente in verschiedenen Abteilungen einer Verwaltungseinheit erzeugt und geprüft. Daher müssen pro Tag größere Mengen an Anfragen für Erzeugung und Prüfung gleichzeitig zu verarbeiten sein. Die Infrastruktur sollte aus diesem Grund nach einer ersten Einschätzung in der ersten Stufe 3.000 QR-Codes pro Stunde erzeugen können. Die Antwortzeit bzw. Fertigstellungszeit für jeden zu erstellenden QR-Code sollte dabei zehn Sekunden nicht überschreiten, um die täglichen Verwaltungsprozesse im Fluss zu halten. Es wird von der Annahme ausgegangen, dass deutlich mehr QR-Codes erzeugt, als später geprüft werden, da viele QR-Codes keine zu prüfenden Inhalte haben, sondern z.B. nur Links auf Webseiten enthalten.

Bei der *Prüfung* von QR-Codes wird von einem geringeren Durchsatz als bei der Erstellung ausgegangen. Die beteiligten Prüfungskomponenten müssen daher 1.000 Prüfungsvorgänge pro Stunde abwickeln können. Bei den Antwortzeiten der Prüfungsaktionen sind maximal drei Sekunden zugelassen, um zügig eine Antwort an die prüfende Person bereitzustellen und Irritationen zu vermeiden.

Als Grundlage für die geschätzte Anzahl an zu prüfenden QR-Codes wird eine, vor allem in Schleswig-Holstein und Hamburg eingesetzte vergleichbare IT-Infrastruktur („Nachrichtenbroker“) als Orientierung verwendet. Dort werden pro Stunde knapp 1.000 Nachrichten verarbeitet.

Grundsätzlich wird die Software zum Erstellen und Prüfen der QR-Codes jeweils als eine Komponente vorgesehen, die skalierbar ist. Es lassen sich mehrfache Instanzen der Komponente parallel starten, um auf schwankende Anzahl an Anfragen reagieren zu können (Durchsatz). Zudem muss sich die Software zur Vermeidung von Netzwerkverkehr und zur Einbindung in andere Anwendungen nicht nur extern, sondern auch in einem lokalen Rechenzentrum betreiben lassen. Auf den Transportweg wird im Kapitel 2.2.2. eingegangen.

Hinsichtlich der Verfügbarkeit bzw. Ausfallsicherheit wird empfohlen, sowohl an die Erstellungs- als auch an die Prüfungskomponenten relativ hohe Anforderungen zu stellen. Im Einzelfall entscheidet die Organisation der Fachanwendung über das konkrete Anforderungsniveau und die damit verbundenen Maßnahmen. Hingewiesen sei an dieser Stelle auf die Dokumentation des BSI zu Bausteinen mit Architekturen und Maßnahmenempfehlungen im Hinblick auf die Realisierung einer hohen Verfügbarkeit („Band B“). Insbesondere der „Band B 7“ mit der „mit der konkreten Realisierung von IT-Diensten sowie Verfahren zur Steigerung derer Verfügbarkeit“ ist in diesem Zusammenhang von Bedeutung.

2.2 Struktur auf Aufbau der Infrastruktur

2.2.1 Nutzbare Funktionen und deren Verbindung

Nachfolgend werden die bereitgestellten Services und nutzbaren Funktionen der Infrastruktur dargestellt und die Schnittstellen der Kommunikation und Transportwege erläutert.

Die Infrastruktur stellt eine Erstellungsfunktion für QR-Codes bereit und ermöglicht eine On- und Offline-Prüfung. Die Prüfinstanzen befinden sich dabei immer in der Hoheit der Verwaltung.

Die Kommunikationspartner in dieser erstellenden Infrastruktur werden dabei repräsentiert durch zwei Services:

- „Konsumierender Service“ (z.B. Fachanwendung)
- „Erstellender Service“ (Infrastrukturkomponente)

Ausgangspunkt ist, dass der „Konsumierende Service“ für seine fachlichen Aufgaben QR-Codes benötigt. Er kann diesen QR-Code vom „Erstellenden Service“ erzeugen und übermitteln lassen. Ddies geht nur in eine Richtung(vgl. Abbildung 1). Grundlage für die Erstellung ist, dass der „Konsumierende Service“ dem „Erstellenden Service“ die Metadaten (z.B. Verschlüsselung ja/nein) sowie die (fachlichen) Inhalte (= bereitzustellender Payload vgl. Tabelle 2) bereitstellt, welche im QR-Code codiert werden sollen. Der „Erstellende Service“ übermittelt dann den angeforderten QR-Code.

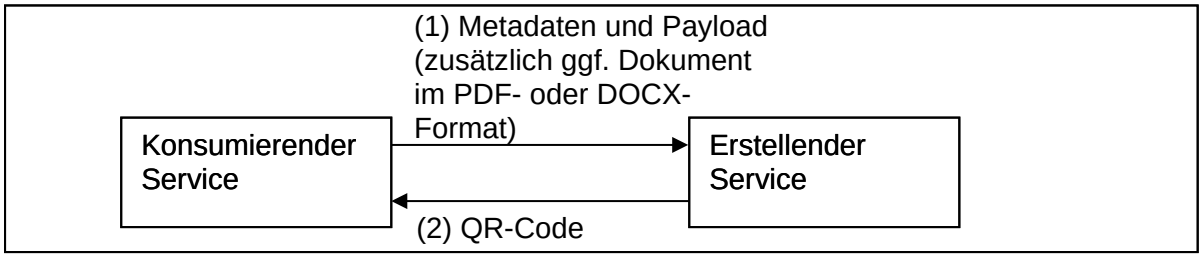

Abbildung 1: Erstellungsfunktion für QR-Codes

Der Erstellungsservice muss als Komponente entwickelt werden, die grundsätzlich in zwei verschiedenen Formen betrieben werden kann:

- Verteilter (Cloud-)Service (in externen Rechenzentren (RZ) mit automatisiertem Updatemechanismus) 1
- Lokaler Service (im eigenen Rechenzentrum (RZ) mit automatisiertem Update-Mechanismus) mit Zugriff über ein internes Netz 2 (z.B. als Webservice) bzw. ggf. direkt (als Softwarebibliothek) in den „Konsumierenden Service“ integriert 3

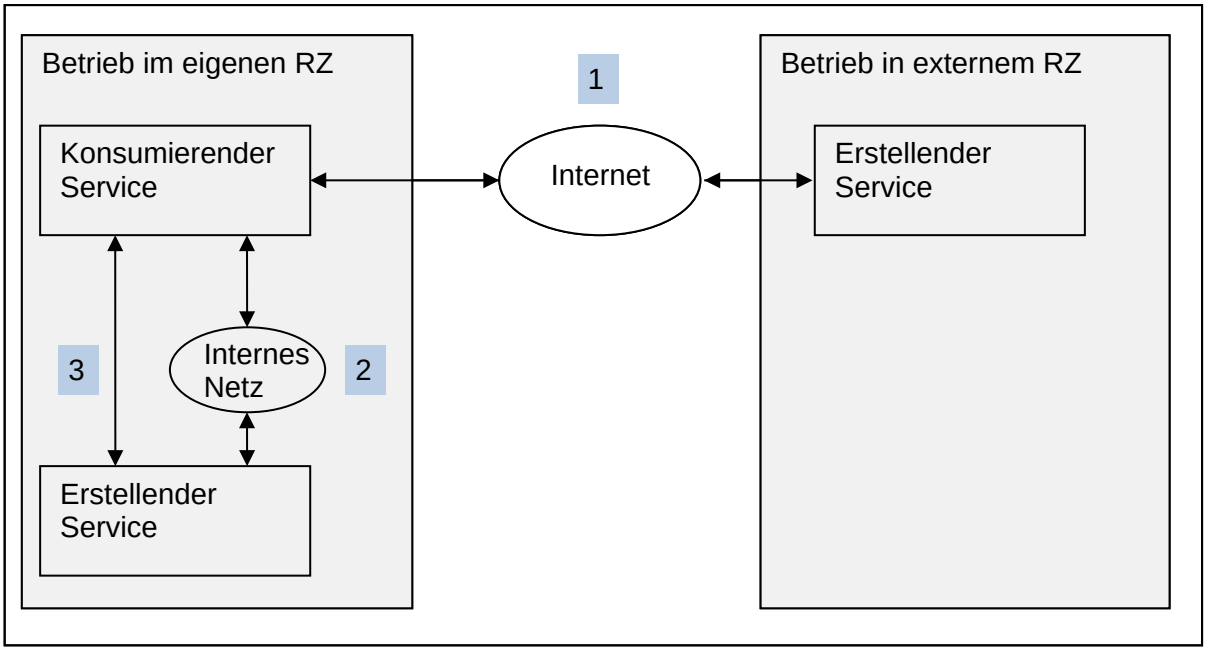

Abbildung 2: Erstellungskontexte für QR-Codes

Grundsätzlich gibt es die Möglichkeit, dem „Erstellenden Service“ neben dem Payload auch ein Dokument im PDF- oder DOCX-Format mitzugeben. Danach richtet sich auch das Ausgabeformat, d.h. das technische Datenformat, welches der „Erstellende Service“ dem „Konsumierenden Service“ bereitstellt.

Wird ausschließlich ein Payload (ohne zusätzliches Dokument) bereitgestellt, antwortet der „Erstellende Service“ in Form einer Bilddatei im PNG-Format. Das Bildformat PNG hat den Vorteil, dass es sowohl Metadaten inkludieren kann, als auch universell ohne Anpassung in verschiedenen Kontexten (z.B. in HTML-Seiten) verwendbar ist.

Wird ein Payload sowie ein Dokument in einem bestimmten Eingabeformat (PDF, DOCX) bereitgestellt, antwortet der „Erstellende Service“ in Form einer Ausgabedatei im entsprechenden Eingabeformat mit inkludiertem, entsprechend des Payload, erstelltem QR-Code.

Im Hinblick auf die Prüfung sind zwei Szenarien, eine „Online-Prüfung“ und eine „Offline-Prüfung“, vorgesehen, auf die näher im Kapitel 2.3.2. eingegangen wird.

Eine „Offline-Prüfung“ ist vorgesehen, wenn die Prüfaktivitäten in Umgebungen stattfinden (können), in denen es keine bzw. nur eine sehr eingeschränkte Verfügbarkeit eines Internetzugangs gibt.

Wenn die Prüfaktivitäten sich (mit wenigen Ausnahmen) auf die Verfügbarkeit einer Internetverbindung verlassen können, ist auch eine „Online-Prüfung“ nutzbar. Ein erstellter QR-Code wird dazu auch die Möglichkeit bereitstellen, in diesem eine URL / einen Hyperlink am Anfang zu platzieren (siehe auch Kapital 2.3.1.). Darüber kann beim Einlesen des QR-Codes direkt eine über diese URL / diesen Hyperlink erreichbare Prüfinstanz im Sinne einer „Online-Prüfung“ aufgerufen werden. Durch das Prinzip der URLs / Hyperlinks ist es grundsätzlich möglich, Prüfinstanzen zu verwenden, die sich entweder in der eigenen Verwaltungshoheit oder in der Hoheit einer anderen öffentlichen Verwaltung befinden können.

2.2.2 Technische Kommunikationsschnittstellen und Transportwege

Die Funktion zum Erstellen von QR-Codes muss über robuste und leicht implementierbare Schnittstellen aufrufbar sein. Hinsichtlich des Transportprotokolls bieten sich dafür folgende technische Option an:

- Hypertext Transfer Protocol Secure (HTTPS)
- Simple Mail Transfer Protocol (SMTP)

Das Transportprotokoll SMTP, das nicht Ende-zu-Ende verschlüsselt ist, bzw. ein unverschlüsseltes HTTP-Protokoll darf nur verwendet werden, wenn der „Erstellende Service“ im eigenen Rechenzentrum betrieben wird und der Nachrichtenaustausch zwischen dem „Konsumierenden Service“ und dem „Erstellenden Service“ komplett im eigenen Rechenzentrum stattfindet.

Der Transportweg über HTTPS lässt sich wiederum als Webservice mit zwei verschiedenen Ausprägungen nutzen:

- Webservice auf Basis des Simple Object Access Protocol (SOAP)
- Webservice auf Basis des Representational State Transfer (REST)

Zudem wird für die direkte Integration des „Erstellenden Service“ in einen „Konsumierenden Service“ eine Bibliothek mit entsprechender Programmierschnittstelle (API) angeboten.

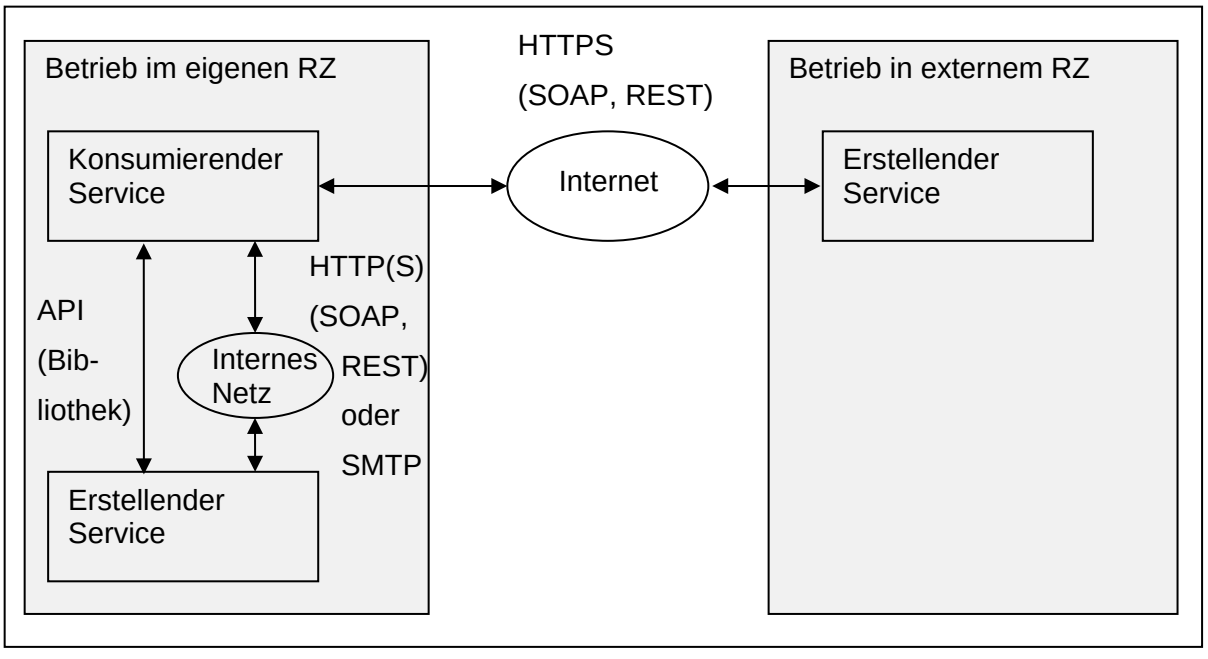

Abbildung 3: Kommunikationsschnittstellen und Transportwege für QR-Codes

Die Schnittstellenbeschreibungen für die verschiedenen Kommunikationsschnittstellen sowie der zugehörigen Transportprotokolle können der folgenden Tabelle entnommen werden:

Schnittstelle	**Transportprotokoll**	**Erläuterungen**
Webservice (SOAP)	HTTPS (ggf. HTTP im eigenen Rechenzentrum)	Es wird eine WSDL bereitgestellt, welche die Funktionsweise des Webservice beschreibt. Zudem wird dort auch erläutert, wie die strukturierten Daten für den QR-Code inkludiert werden (siehe auch Kapitel 2.3.1).
Webservice (REST)	HTTPS (ggf. HTTP im eigenen Rechenzentrum)	Es wird eine REST-API auf Basis von HTTP beschrieben (POST-Methode inkl. Beschreibung wie die strukturierten Daten für den QR-Code mitgegeben werden (siehe auch Kapitel 2.3.1)).
E-Mail	SMTP	Es wird beschrieben, wie eine E-Mail (Header, Body) aussehen muss, damit die strukturierten Daten für den QR-Code mitgegeben werden können (siehe auch Kapitel 2.3.1).
Softwarebibliothek	z.B. Java-Klassen (ggf. Java Native Interface), C#-Klassen (.NET), JavaScript-Funktionen	Es wird beschrieben, wie die Klassen und Methoden bzw. Funktionen der Bibliothek aussehen, damit die strukturierten Daten für den QR-Code mitgegeben werden können (siehe auch Kapitel 2.3.1).

Tabelle 1: Kommunikationsschnittstellen und Transportprotokolle

Die Erfüllung der mit dem Transport verbundenen rechtlichen Anforderungen obliegen der Organisation der jeweiligen Verwaltung.

2.3 Die nutzbaren Funktionen der Infrastruktur im Detail

In diesem Unterkapitel wird im Detail die Erstellung- und Prüffunktion des QR-Codes beschrieben. Schließlich werden die Risiken und Maßnahmen im Zusammenhang mit der Erstellung und Verwendung von QR-Codes eruiert.

2.3.1 Erstellungsfunktion

In der einfachsten Form besteht der Payload beim Aufruf des „Erstellenden Services“ aus Daten, deren Bedeutung und Struktur nur dem „Konsumierenden Service“ bekannt sind. Dies kann beispielsweise ein Verwaltungsverfahren sein, welches auf Dokumenten QR-Codes platziert, die einen Link (inkl. zusätzlicher Daten als URL-Parameter) auf eine Webseite mit aktuellen (ergänzenden) Informationen enthalten (z.B. Flyer mit öffentlichen Bauentwicklungsplanungen). Der „Erstellende Service“ kümmert sich ausschließlich um eine Übertragung des Payload in einen entsprechenden QR-Code. In dieser Form hat der „Konsumierende Service“ die vollständige Hoheit über den Prozess. Er kümmert sich auch um die Details der Schnittstelle zum „Erstellenden Service“.

Um fachliche Daten strukturiert im QR-Code ablegen zu können, ist die Schnittstelle so generisch und erweiterbar, dass aus einer in der Infrastruktur hinterlegten Basis-Datenstruktur der „Konsumierende Service“ (ausgewählte) dem „Erstellenden Service“ fachliche Daten bereitstellen kann, die dieser entsprechend strukturiert im QR-Code für eine spätere Verarbeitung (z.B. Prüfungsvorgänge) hinterlegen kann.

Um sowohl aus Sicht des „Erstellenden Services“ einfache bzw. wenig strukturierte Daten als auch fachlich durchgängig strukturierte Daten im QR-Code abbilden zu können wird folgende Basis-Datenstruktur definiert:

Id	Inhaltliche / fachliche Bedeutung	Zulässige Werte
Metadaten		
`sch`	Schema	Angabe eines Schemanamens (mit drei Zeichen) Standard- bzw. Defaultwert: `std`
`enc`	Verschlüsselung	0 = keine Verschlüsselung 1 = Verschlüsselung Hinweis: Zertifikat wird inkl. Hashwert mit in den QR-Code integriert
`zer`	Zertifikat	0 = kein Zertifikat über Payload hinzufügen 1 = Zertifikat über Payload hinzufügen (Standard- bzw. Defaultwert) Hinweis: Es wird entweder ein Zertifikat oder ein Hashwert hinzugefügt.

`hsh`	Hashwert	0 = kein Hashwert über Payload 1 = Hashwert über Payload Hinweis: Es wird entweder ein Zertifikat oder ein Hashwert hinzugefügt.
`url`	URL / Hyperlink: Am Beginn des QR-Codes einzufügende URL / einzufügender Hyperlink	
`uid`	UUID: Durch die UUID lässt sich ein QR-Code erzeugen, der einmalig ist und nicht nochmals erzeugt werden kann (= einmaliger QR-Code)	0 = keine UUID hinzufügen 1 = UUID hinzufügen
Inhaltliche Daten (Payload)		
`txt`	Freitext	Die Anzahl Zeichen ist abhängig von den gewählten Metadaten und den weiteren Daten (z.B. Erstellungsdatum)
`erd`	Erstellungsdatum	Datum im Format JJJJMMTT
`dgv`	Gültig von Datum	Datum im Format JJJJMMTT
`dgb`	Gültig bis Datum	Datum im Format JJJJMMTT
`vnr`	Vorgangsnummer	maximal 40 Zeichen
…	…	…

Tabelle 2: Basis-Datenstruktur der Schnittstelle zur Erstellung von QR-Codes

Die Daten aus der Basis-Datenstruktur werden durch den „konsumierenden Service“ in Form von einem mit XML strukturierten Datensatz an den „Erstellenden Service“ gesendet.

Es wird dabei folgende (Speicherplatzsparende) Strukturierung verwendet:

- (Root-)Element <q>: Umfasst den Datensatz für den QR-Code
- Element <d> mit Attribut i: Das Element umfasst ein Datum mit Angabe einer Id aus der Basis-Datenstruktur

Beispiel-Datensatz (Eingabe) mit Angabe eines Links bzw. einer URL:

```
<q>
  <d i=”sch”>std</d>
  <d i=”enc”>0</d>
  <d i=”zer”>0</d>
  <d i=”hsh”>0</d>
  <d i=”url”>https://www.hamburg.de</d>
  <d i=”uid”>1</d>
  <d i=”txt”>Dies ist ein im QR-Code codierter Freitext</d>
</q>
```

Der aus den Metadaten und dem Payload resultierende Umfang des Datensatzes darf maximal 2900 Bytes umfassen. Ist ein Link bzw. eine URL im Rahmen der QR-Code-Erzeugung mitgegeben worden, erfolgt die Codierung des resultierenden XML als URL-Parameter.

```
https://www.hamburg.de?q=%3Cq%3E%3Cd%20i%3D%22sch%22%3Estd%3C%2Fd%3E
%3Cd%20i%3D%22uid%22%3E445c6c8f-ab35-4374-8466-
a220e575d23b%3C%2Fd%3E%3Cd%20i%3D%22txt%22%3EDies%20ist%20ein%20im%2
0QR-Code%20codierter%20Freitext%3C%2Fd%3E%3C%2Fq%3E
```

= Inhalt des QR-Codes

Beispiel-Datensatz (Eingabe) ohne Angabe eines Links bzw. einer URL:

```
<q>
  <d i=”sch”>std</d>
  <d i=”enc”>0</d>
  <d i=”zer”>0</d>
  <d i=”hsh”>0</d>
  <d i=”url”></d>
  <d i=”uid”>1</d>
  <d i=”txt”>Dies ist ein im QR-Code codierter Freitext</d>
</q>
```

Ist kein Link bzw. keine URL im Rahmen der QR-Code-Erzeugung mitgegeben worden, wird das resultierende XML entsprechend wie folgt im QR-Code abgebildet:

```
<q><d i="sch">std</d><d i="uid">445c6c8f-ab35-4374-8466-
a220e575d23b</d><d i="txt">Dies ist ein im QR-Code codierter Frei-
text</d></q>
```

= Inhalt des QR-Codes

Für die Verschlüsselung von Daten (Id: `zer`) werden Software-Zertifikate verwendet. Die Verschlüsselung erfolgt dabei auf Basis einer asymmetrischen RSA-Verfahrens. Im QR-Code ist dann entsprechend das Software-Zertifikat (mit Hashwert) hinterlegt, welches zur Verschlüsselung des Payload verwendet worden ist.

Die Basis-Datenstruktur kann jederzeit (je nach Anforderung durch neue „Konsumierende Services“) um zusätzliche fachliche Datenelemente (Id, inhaltliche / fachliche Bedeutung, zulässige Werte) erweitert werden. Dadurch kann schrittweise ein Katalog von Datenelementen fortgeschrieben werden, mit dem sich unterschiedliche Anforderungen der Fachanwendungen abbilden lassen.

In allen Fällen entscheidet eindeutig der „Konsumierende Service“, welche Daten im QR-Code abgebildet werden, in dem er die Schnittstelle mit den aus seiner Sicht passenden Datenelementen anspricht. Durch die Kombinationsmöglichkeit der Datenelemente kann der „Konsumierende Service“ damit den für ihn passenden QR-Code erzeugen lassen. Der „Konsumierende Service“ ist dadurch eindeutig die steuernde Instanz.

Ziel ist es, dadurch auf Anwenderseite Vertrauen zu erzeugen, dass im QR-Code nur Daten hinterlegt werden, welche durch den „Konsumierenden Service“ vorgegeben wurden. Dies ist für den „Konsumierenden Service“ jederzeit transparent und nachvollziehbar.

2.3.2 Prüfungs- und Validierungsfunktion

Wie im Kapitel 2.2.1 einführend dargestellt, kann die Prüfung- und Validierung von QR-Codes bzw. deren codierten Informationen entweder im Rahmen einer „Offline-Prüfung“ oder einer „Online-Prüfung“ erfolgen.

Offline-Prüfung

Die „Offline-Prüfung“ ist dabei auf die Informationen beschränkt, welche im QR-Code codiert sind. Daher ist der Prüfungsrahmen auf folgende Prüfungsaktivitäten beschränkt:

- Bei verschlüsselten Daten: Prüfung ob die Verschlüsselung korrekt ist
- Einfache Darstellung der codierten Informationen (ggf. zum Sichtvergleich mit auf einem Dokument dargestellten Informationen)

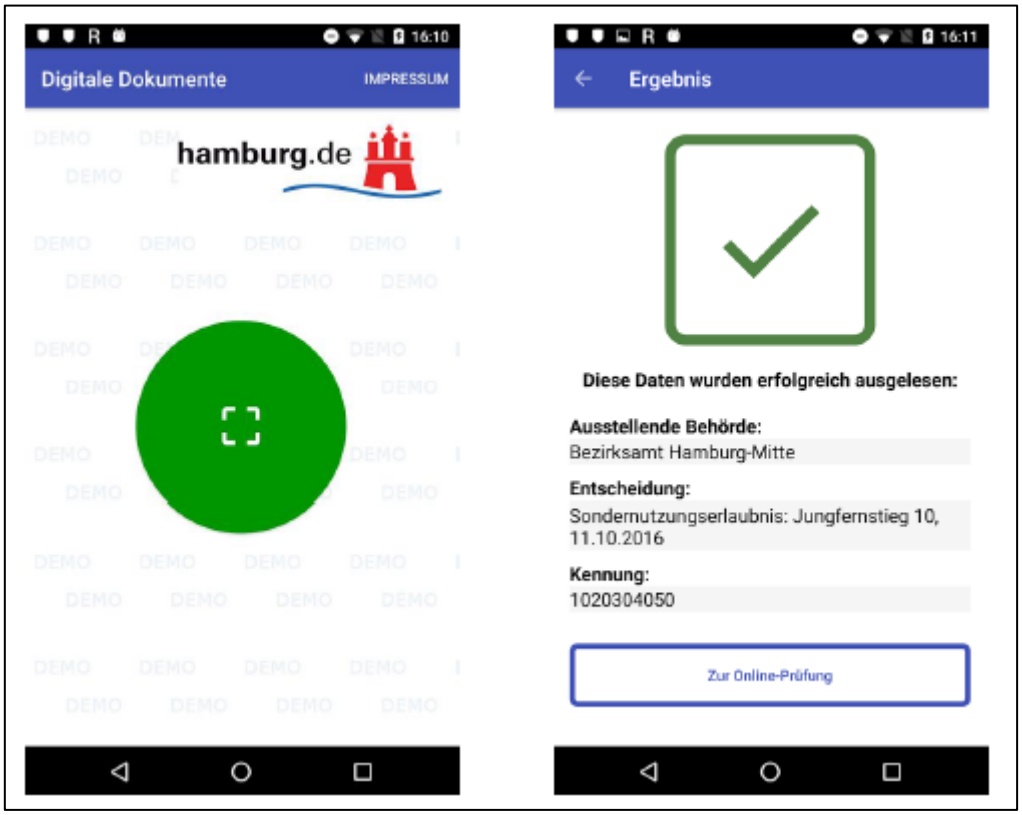

Abbildung 4: Anwendung („App“) einer Offline-Prüfung

Wenn nicht nur die Inhalte der QR-Codes im Rahmen einer „Offline-Prüfung“ ausgelesen und dargestellt werden sollen, sondern auch eine (Gegen-)Prüfung anhand eines Datenbestandes (z.B. an erstellten QR-Codes) erfolgen soll, müssen die entsprechenden Prüfungsdaten regelmäßig auf die für die Prüfungsaktivitäten verwendeten Geräte übertragen werden. Dies ist nur bei einer geringen Anzahl an Geräten dauerhaft leistbar.

Online-Prüfung

Eine „Online-Prüfung“ benötigt zwar eine stabile Internetverbindung als Voraussetzung, ermöglicht jedoch sowohl umfangreichere Prüfungsaktivitäten als auch eine übersichtlichere Darstellung des Prüfungsergebnisses. Das Prüfungsergebnis einer „Online-Prüfung“ muss dabei in zwei Formen bereitgestellt werden können:

- Ausgabe als Benutzer-Schnittstelle (mit Oberflächendarstellung, „UI“)
- Ausgabe als Daten(-struktur) (ohne Oberflächendarstellung, „Non-UI“)

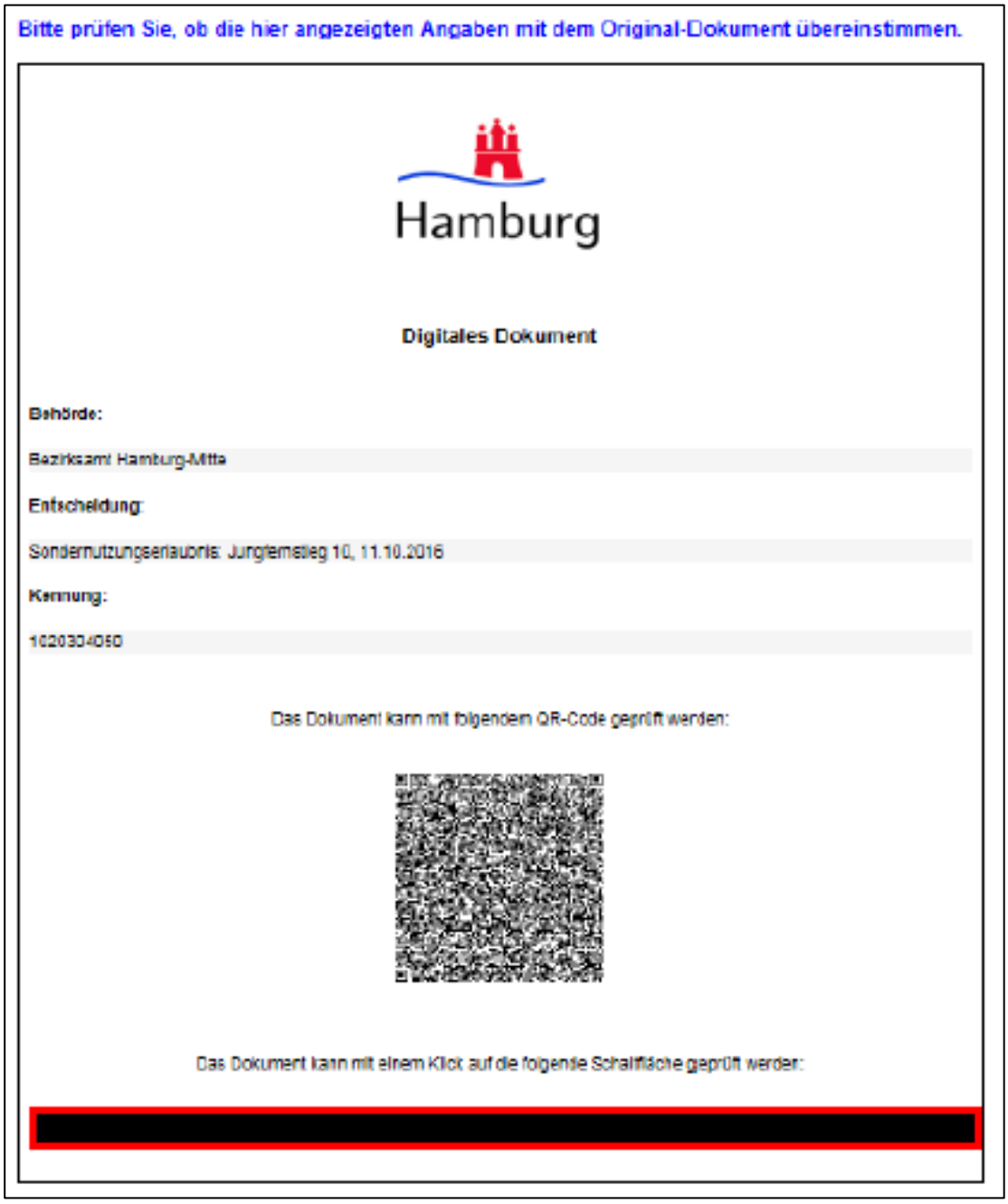

Abbildung 5: Beispiel einer Online-Prüfung mittels eines QR-Codes

Grundlage für die Verwendung der „Online-Prüfung“ ist eine Internetverbindung, die hinsichtlich des Uploads (=Datenübertragung für zu erstellende bzw. prüfende QR-Codes) und Downloads (=PNG-Bilddatei eines erstellten QR-Codes bzw. zurückgeliefertes Prüfungsergebnis eins QR-Codes) folgende Qualitätsmerkmale aufweisen muss:

- Download-Transferrate: 2048 Kbit/s
- Upload-Transferrate: 192 Kbit/s

Im Bereich fester Anschlüsse entspricht dies einer durchschnittlichen DSL-Verbindung, im Mobilbereich können diese Transferraten mit dem Universal Mobile Telecommunications System (UMTS) erreicht werden.

Bei einer Ausgabe des Prüfungsergebnisses als Benutzer-Schnittstelle, d.h. inklusive einer Oberflächendarstellung ist ein sog. Responsive Design / Layout möglich, welches sich automatisch der Displaygröße des Endgeräts anpasst.

Wird die Prüfungsinstanz in der eigenen Verwaltung bereitgestellt, kann auch die eigene Corporate Identity (CI) integriert werden.

Die „Online-Prüfung“ hat die Möglichkeit, sowohl die Prüfungsaktivitäten einer „Offline-Prüfung“ abzubilden als auch weitergehende Prüfungsaktivitäten umzusetzen. Dies umfasst folgende Aktivitäten:

- Bei verschlüsselten Daten: Prüfung ob die Verschlüsselung korrekt ist
- Darstellung der codierten Informationen (ggf. zum Sichtvergleich mit auf einem Dokument dargestellten Informationen)
- Einbindung weiterer (nicht im QR-Code enthaltener) (Prüfungs-)Parameter (z.B. geänderte rechtliche Rahmenbedingungen, Veränderungen von Fristangaben, ergänzende aktuelle Informationen)

2.3.3 Risiken und Maßnahmen

Die Erstellung und Verwendung von QR-Codes beinhaltet auch Risiken. Aus derzeitiger Sicht relevante Risiken werden hier benannt und entsprechende Maßnahmen beschrieben.

Aktion	Risiko	Gegenmaßnahmen
Erstellung des QR-Codes	Durch Umstrukturierung der Server o. ä. funktionieren die Codes nicht mehr oder Inhaltliche Veränderung der gewünschten Information	Erstellen von dynamischen Codes, so dass Inhalte und Links nicht im Nachhinein geändert werden können; alternativ Hash-Wert oder Zertifikat
Erstellung des QR-Codes	Erzeugung fehlerhafter Codes	Prüfung der erstellten QR-Codes auf Korrektheit (Qualitätssicherung)
Erstellung des QR-Codes	Zielort nicht für mobile Anwendungen optimiert, dadurch fehlerhafte Anzeige	Optimierung für mobile Anwendungen
Verwendung des QR-Codes	Benutzer kann mit dem Code nicht umgehen	Zeigen der Information auch im Klartext, alternativer Weg mit einem Link zu den hinterlegten Information, Hilfestellung zum Downloaden (z.B. eines Scanners)
Verwendung des QR-Codes	Durch Versendung von „Fake-Codes“ über Fake E-Mails oder Homepages; Verlinkung zu Male-Ware, Fishing, Tagging, Trojanern oder anderer Schadsoftware	Ausschließliche Nutzung über ein Bürgerserviceportal, Aufklärung, Virenscanner schon in der QR-App
Verwendung des QR-Codes	QR-Code wird von manchen Readern nicht erkannt	Testen verschiedener Reader und Software zum Erstellen sowie Vorhalten des QR-Codes bzw. Inhalts in der Verwaltung zur Wiederherstellung

Tabelle 3: Risiken von QR-Codes und Maßnahmen

3 Erfüllung des Schriftformerfordernis mit Hilfe von QR-Codes

In dem Kapitel werden die Rahmenbedingungen und Anforderungen im Zusammenhang mit der Erfüllung des Schriftformerfordernisses von QR-Codes erläutert.

3.1 Rahmenbedingungen

Ziel des Konzeptes ist es, über die bestehenden elektronischen Verfahren wie qualifizierte elektronische Signatur, Online-Ausweisfunktion des neuen Personalausweises, De-Mail) hinaus, eine attraktive Alternative zu schaffen, welche sowohl von den Verwaltungskunden (Bürgerinnen und Bürger, Unternehmen/Firmen) als auch von der Verwaltung leicht zu handhaben ist.

In dem Verwaltungsverfahrensgesetz des Bundes (und in den entsprechenden Gesetzen der Länder) sind die Möglichkeiten zur „Elektronischen Kommunikation“ im § 3a VwVfG geregelt. Zur besseren Nachvollziehbarkeit und Einordnung ist der Auszug aus dem Verwaltungsverfahrensgesetz des Bundes hier eingefügt:

Verwaltungsverfahrensgesetz (VwVfG)

§ 3a Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, soweit der Empfänger hierfür einen Zugang eröffnet.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur versehen ist. Die Signierung mit einem Pseudonym, das die Identifizierung der Person des Signaturschlüsselinhabers nicht unmittelbar durch die Behörde ermöglicht, ist nicht zulässig. Die Schriftform kann auch ersetzt werden

1.

durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;

2.

bei Anträgen und Anzeigen durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des De-Mail-Gesetzes;

3.

bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des De-Mail-Gesetzes, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;

4.

durch sonstige sichere Verfahren, die durch Rechtsverordnung der Bundesregierung mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab.

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach § 18 des Personalausweisgesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.

(3) Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, hat sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück zu übermitteln.

Das hier dargestellte Verfahren knüpft an § 3a Absatz 2 Nr. 4 VwVfG an und eröffnet zunächst für durch die Verwaltung bereitgestellte Ausgangsdokumente die zusätzliche Möglichkeit, die Schriftform durch QR-Codes in Verbindung mit Servicekonten sowie deren zugehörige Postfächer alternativ im Rahmen eines „sonstigen sicheren Verfahrens“ zu erfüllen. Der IT-Planungsrat kann entsprechende Empfehlungen zu „sonstigen sicheren Verfahren“ abgeben.

3.2 Anforderungen an den QR-Code als „sonstiges sicheres Verfahren“

Ein „sonstiges sicheres Verfahren“, welches QR-Codes und Servicekonten inkl. Postfächer verwendet, soll den Verwaltungen die zusätzliche Möglichkeit bieten, die Schriftform zu ersetzen. Dafür müssen nachfolgende Anforderungen erfüllt werden.

3.2.1 Anforderung aus dem Schriftformerfordernis

Grundsätzlich wird die Schriftform im Rechtsverkehr dann benötigt, wenn rechtlich vorgeschriebe ist, dass Dokumente der handschriftlichen Unterschrift bedürfen.

Durch die Verwendung der Schriftform werden im Rechtsverkehr folgende Aufgaben bzw. Funktionen erfüllt:

- Willenserklärung: Formulierung des Willens durch Textform und Unterschrift

- Warnfunktion / Hinweisfunktion: Hinweis auf die besondere Bedeutung (ggf. damit verbundene Risiken) der Willenserklärung
- Beweisfunktion: Nachweis des Zustandekommens der Willenserklärung sowie des Inhalts und der Beteiligten
- Klarstellungsfunktion: Definition des Inhalts und der Beteiligten

Die Konzeption bezieht sich im Folgenden auf die Schriftform (als Erweiterung der Textform) und beinhaltet nicht (weitergehende) Formerfordernisse, wie beispielsweise die Beglaubigung oder die Beurkundung. Im Fokus steht dabei die Transparenz des Verwaltungshandelns. Besondere Verschwiegenheitsanforderungen, wie sie bei besonderen Berufsgruppen (wie beispielsweise bei Rechtsanwälten) erforderlich sind, existieren in diesem Kontext nicht.

3.2.2 Anforderungen an ein „sonstiges sicheres Verfahren“

Die Schriftform kann durch ein „sonstiges sicheres Verfahren“ gemäß § 3 a Abs. 2 Nr. 4 VwVfG ersetzt werden. Ein „sonstiges sicheres Verfahren“, welches QR-Codes mit Servicekonten inkl. Postfächern verwendet, muss entsprechend § 3 a Abs. 2 Nr. 4 VwVfG die Anforderungen an Authentizität, Integrität und Barrierefreiheit erfüllen.

Die Begriffe konkretisieren sich wie folgt:

- **Authentizität** (= identifizierte Kommunikationspartner): Authentisierung durch
  - geheime Informationen (z.B. Passwort) oder
  - Identifizierungsgegenstand (z.B. Personalausweis) oder
  - Identifizierungsobjekt (z.B. Fingerabdruck)
- **Integrität** (= Schutz vor Manipulation bzw. unberechtigter Veränderung der kommunizierten Inhalte): Informationssicherheit über
  - Sicherstellung der Unversehrtheit, Intaktheit, Vollständigkeit der Inhalte
  - Ziele: Datenintegrität, Verfügbarkeit und Vertraulichkeit
- **Barrierefreiheit** (= hürdenfreier bzw. hürdenarmer Zugang zu den kommunizierten Inhalten): Grundlagen sind
  - Umfassender Zugang und uneingeschränkte Nutzungschancen für alle
  - Grundlagen: Behindertengleichstellungsgesetz (BBG), § 16 EGovG, BITVO

3.2.3 Analogien zum „sonstigen sicheren Verfahren“

Da die Anforderungen an „sonstiges sicheres Verfahren“, insbesondere in Bezug auf Authentizität und Integrität in den rechtlichen Grundlagen nicht näher ausdifferenziert sind, bezieht sich das vorliegende Konzept auch auf andere sichere Verfahren (z.B. De-Mail, besonderes elektronisches Anwaltspostfach (beA)) mit Analogien, um die Erfüllung der Anforderungen an Integrität und Authentizität aufzuzeigen. Auf die Barrierefreiheit wird im Kapitel 3.3.3 eingegangen. Im Übrigen bestehen im Hinblick auf die Barrierefreiheit konkrete rechtliche Vorgaben, die eingehalten werden müssen.

Beim **De-Mail-Verfahren** werden die Anforderungen nach Authentizität und Integrität wie folgt abgedeckt:

Authentisierung / Authentifizierung	**Vertraulichkeit / Integrität**
§ 4 Abs. 1 Satz 2,3 De-MailG	§ 5 Abs. 3 De-MailG
● Identitätsprüfung durch: - Ausweiskontrolle oder - online via elektronischem Personalausweis mit eID-Funktion oder - mit PIN-Eingabe, wenn eine verifizierte Rechnungsadresse gegeben ist ● Zugangseröffnung durch Nutzer ● Zwei-Faktor-Authentifizierung erforderlich: Besitz (Token: eID, Signaturkarte oder Mobiltelefon) und Wissen (Kennwort oder PIN))	● Geschlossenes System ● Grds. Transportverschlüsselung (Punkt-zu-Punkt) ● Zusätzlich möglich: Ende-zu-Ende-Verschlüsselung ● Zusätzlich möglich: qualifiziert elektronisch signieren ● Verzeichnisdienst der Anbieter für Schlüssel / Verschlüsselungszertifikate

Tabelle 4: Authentizität und Integrität beim De-Mail-Verfahren

Beim **besonderen Anwaltspostfach (beA)** werden die Anforderungen nach Authentizität und Integrität mit nachstehenden Regelungen und Maßnahmen abgebildet:

Authentisierung / Authentifizierung	**Vertraulichkeit / Integrität**
§ 31 a Abs. 3 Bundesrechtsanwaltsordnung (BRAO)	Verordnung über die Rechtsanwaltsverzeichnisse und die besonderen elektronischen Anwaltspostfächer (RAVPV)
● Jede Rechtsanwaltskammer führt ein Verzeichnis ● SAFE-Verzeichnis der BRAK ● Mit Zulassung erhält der RA eine Identifika-	● Pflicht der BRAK, beA auf der Grundlage des Protokollstandards „Online Services Computer Interface – OSCI“ oder einem künftig nach dem Stand der Technik an dessen Stelle tretenden Standard zu betreiben

tionsNr. (SAFE-ID) und ein Postfach ● Erstanmeldung ● Zugangseröffnung ● Zwei-Faktor-Authentifizierung: Besitz (Token:beA-Karte, Softwarezertifikat) und Wissen (PIN) ● Pflicht zur Datensicherheit (§ 26 RAVPV)	● Geschlossenes System ● Passive Nutzungspflicht des RA ● Ende-zu-Ende-Verschlüsselung ● Qualifizierte elektronische Signatur nur zusätzlich notwendig, wenn der RA nicht selbst verschickt

Tabelle 5: Authentizität und Integrität beim besonderen Anwaltspostfach

3.2.4 Sonstige Anforderungen an den QR-Code

Diese grundsätzlichen Rahmenbedingungen und Anforderungen werden um die aus dem im Jahr 2016 innerhalb der Maßnahme „QR-Codes auf Verwaltungsdokumenten“ erarbeiteten Empfehlungen entsprechend ergänzt (Rahmenwerk QR-Codes auf Verwaltungsdokumenten, IT-Planungsrat, 2016, S. 27):

- Verschlüsselte Dokumentendaten
- Speicherung der verschlüsselten Dokumentendaten in einem geschützten (Archiv-) System in der Verwaltung
- Generierung eines QR-Code (mit verschlüsselten Dokumentendaten) und Platzierung auf dem Verwaltungsdokument sowie einem Link zur Online-Prüfung
- Zustellung des elektronischen Dokuments (mit QR-Code) über das Postfach des Service- bzw. Bürgerkontos des Verwaltungskunden
- Online-Prüfung mit Abgleich der verschlüsselten Dokumentendaten aus dem QR-Code mit den Dokumentendaten aus dem (Archiv-)System

Zusammenfassend beschreibt das Unterkapitel wie die aufgeführten Aufgaben bzw. Funktionen der Schriftform bzw. die Anforderungen an Authentizität und Integrität durch die Verwendung von QR-Codes und Servicekonten (inkl. Postfächern) abgebildet bzw. erfüllt werden können (Näheres zu den Servicekonten wird in Unterkapitel 3.3 erläutert.) Die Konzeption zielt dabei nicht nur auf (tatsächliche) Schriftformerfordernisse (nach Normenscreening) ab, sondern auch auf Verfahren, bei denen eine „tradierte Schriftform“ vorliegt. Die „tradierte Schriftform“ ist dadurch gekennzeichnet, dass es kein rechtliches Erfordernis für die Schriftform gibt. Dennoch wird bei entsprechenden Verwaltungsprozessen aus „Traditionsgründen“ von den Beteiligten auf die Erfüllung der Schriftform bestanden.

3.3 Verwendung von QR-Codes in Verbindung mit Servicekonten

Nachfolgend wird dargelegt, wie die QR-Codes in Verbindung mit Servicekonten die Anforderungen an Authentizität und Integrität erfüllen können. Schließlich wird die Verknüpfung der erstellten und geprüften QR-Codes mit dem bereitgestellten Servicekonto dargestellt.

3.3.1 Einbindung von Servicekonten und Postfächern

Mit dem Beschluss des IT-Planungsrats werden im Bund, den Ländern und Kommunen Servicekonten für die Verwaltungskundinnen und Verwaltungskunden bereitgestellt. Über das Servicekonto ist den Verwaltungskundinnen und Verwaltungskunden mit der Anmeldung möglich, die bereitgestellten Online-Dienste der Verwaltung zu nutzen.

Der Funktionsumfang des Servicekontos umfasst auch ein zugehöriges Postfach, mit dem Ziel, dass Verwaltungskundinnen und Verwaltungskunden asynchron Nachrichten der Verwaltung erhalten bzw. empfangen können (z.B. elektronischer Bescheid).

Der große Vorteil des Servicekontos stellt die Interoperabilität aller Servicekonten dar, d.h. eine Verwaltungskundin oder ein Verwaltungskunde kann sich künftig beispielsweise mit einem Servicekonto aus der Freien und Hansestadt Hamburg auch im Portal der Stadt München anmelden und entsprechend dort Online-Dienste mit diesem Servicekonto nutzen. Hier knüpft die vorgestellte Lösung an und setzt das voraus.

Die folgende Abbildung verdeutlicht in vereinfachter Form die relevanten Bausteine inkl. der Interoperabilität der Servicekonten (Hinweis: Die grünen Pfeile stellen die Verwendung der Servicekonten für die Online-Dienste dar). Über die Online-Dienste werden die Verwaltungsleistungen in Anspruch genommen. Die Verwaltungskunden können die interoperablen Servicekonten verwenden, um auf die Online-Dienste der Portale zuzugreifen. Die Online-Dienste stellen die Verbindung zu den Fachanwendungen in den Behörden dar und können den Verwaltungskunden Ausgangsdokumente bzw. elektronische Bescheide mit einem QR-Code über das Postfach des Servicekontos bereitstellen.

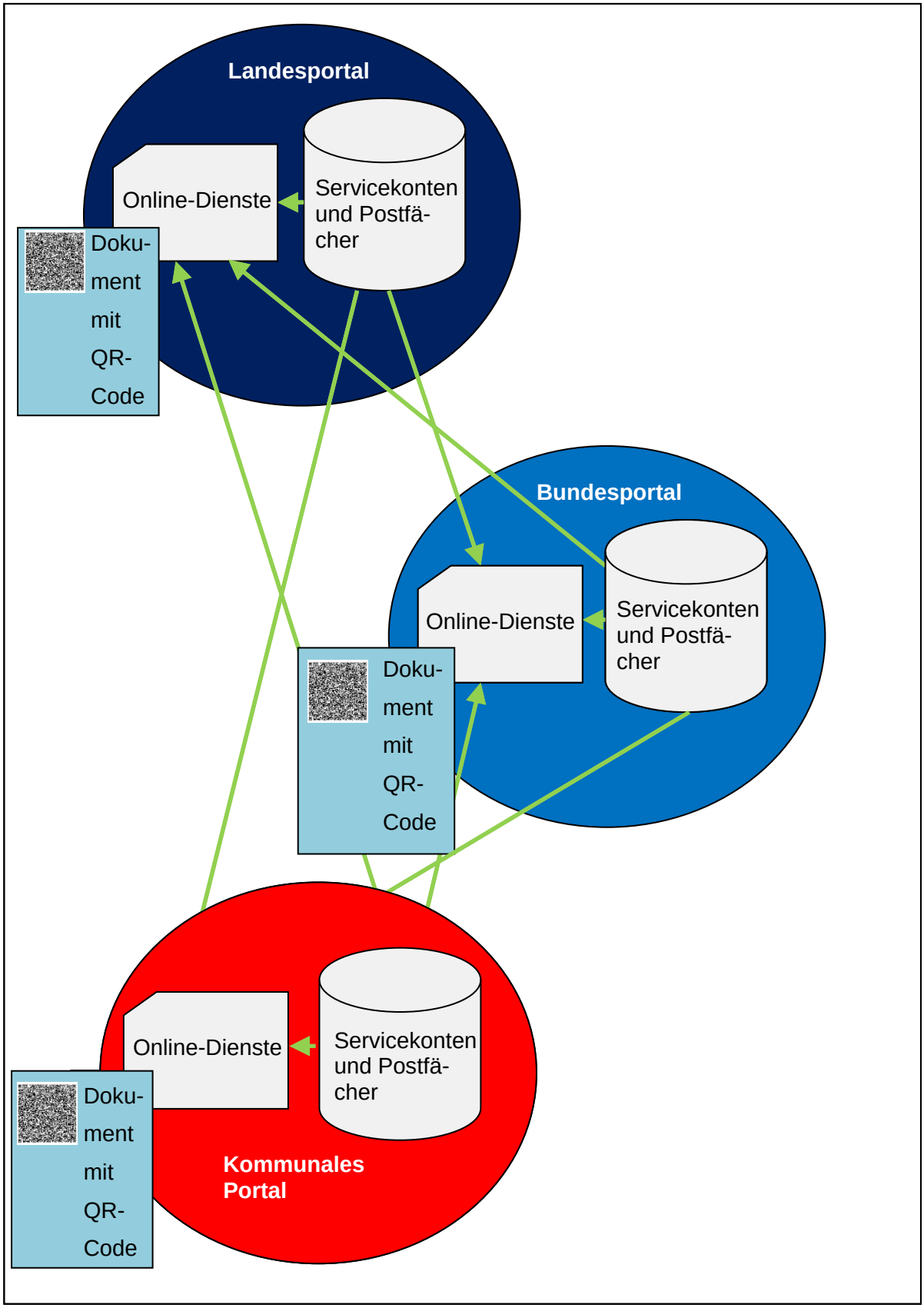

Abbildung 6: Zusammenspiel der Servicekonten im Portalverbund

3.3.2 Einbindung des QR-Codes

Durch die im QR-Code codierten Informationen sollen die Rahmenbedingungen erfüllt bzw. Anforderungen an die Integrität umgesetzt werden:

- Verschlüsselte Codierung der wichtigsten auf dem Dokument sichtbaren Aussagen bzw. Texte des Dokuments zur Verhinderung der nachträglichen unberechtigten Änderung von entscheidenden Aussagen des Dokuments
- Datengrundlage für die elektronische Prüfung des Dokuments hinsichtlich des Nachweises der Korrektheit bzw. Gültigkeit der Inhalte und des Nachweises des Erstellers bzw. Senders des Dokuments („Online-Prüfung“).

Im Einzelnen sollen folgende Daten aus Sicht der Verwaltung (für Ausgangsdokumente) im QR-Code enthalten sein. In der Tabelle ist jeweils dokumentiert, welche Aufgaben bzw. Funktionen der Schriftform dadurch gefördert bzw. erfüllt werden:

Zu codierendes Datum	Datentyp	Erfüllende Aufgabe bzw. Funktion	Pflichtangabe (Ja/Nein)
Hyperlink zur Prüfungsinstanz	String (250 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Zertifikat der ausstellenden Organisation / der Behörde	String (250 Zeichen)	Willenserklärung, (Beweisfunktion), Klarstellungsfunktion	Ja
Straße der ausstellenden Organisation / Behörde	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Hausnummer der ausstellenden Organisation / Behörde	String (20 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Postleitzahl der ausstellenden Organisation / Behörde	String (10 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Ort der ausstellenden Organisation / Behörde	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Vorname der ausstellenden Person (Sachbearbeitung)	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Nein
Nachname der ausstellenden Person (Sachbearbeitung)	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Nein

Abgabedatum der Willenserklärung / Ausstelldatum	Datum (JJJJMMTT)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Ja
Willenserklärung ist gültig bis Datum	Datum (JJJJMMTT)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Nein
Aussage bzw. Inhalt der Willenserklärung	String (500 Zeichen)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Ja
Hyperlink zu Zusatzinformationen	String (250 Zeichen)	Warnfunktion / Hinweisfunktion	Nein

Tabelle 6: Daten zur Erfüllung der Schriftform aus Verwaltungssicht (Ausgangsdokument)

Auch wenn zum aktuellen Zeitpunkt Eingangsdokumente noch nicht fokussiert werden, könnte es zukünftig relevant werden, auch diesen Kanal zu bedienen.

Die Tabelle 7 gibt daher einen Überblick, welche Aufgaben bzw. Funktionen der Schriftform zukünftig gefördert bzw. erfüllt werden könnten. Aus Sicht der Verwaltungskundin bzw. des Verwaltungskunden (für Eingangsdokumente) sind im QR-Code folgende Daten zu codieren:

Zu codierendes Datum	**Datentyp**	**Erfüllende Aufgabe bzw. Funktion**	**Pflichtangabe (Ja/Nein)**
Zertifikat der akzeptierenden Organisation / der Behörde	String (250 Zeichen)	Willenserklärung, (Beweisfunktion), Klarstellungsfunktion	Ja
Name der einreichenden Firma	String (120 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Nein
Vorname der einreichenden Person / des einreichenden Firmenvertreters	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Nachname der einreichenden Person / des einreichenden Firmenvertreters	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Adresse: Straße der einreichenden Person / Firma	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja

Adresse: Hausnummer der einreichenden Person / Firma	String (20 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Adresse: Postleitzahl der einreichenden Person / Firma	String (10 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Adresse: Ort der einreichenden Person / Firma	String (80 Zeichen)	Willenserklärung, Beweisfunktion, Klarstellungsfunktion	Ja
Abgabedatum der Willenserklärung	Datum (JJJJMMTT)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Ja
Willenserklärung ist gültig bis Datum	Datum (JJJJMMTT)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Nein
Aussage bzw. Inhalt der Willenserklärung	String (500 Zeichen)	Willenserklärung, Warnfunktion / Hinweisfunktion, Klarstellungsfunktion	Ja

Tabelle 7: Daten zur Erfüllung der Schriftform aus Kundensicht (Eingangsdokument)

3.3.3 Ergebnis zum Schriftformerfordernis

Alle Dokumente, welche mittels QR-Codes mit Servicekonten die Schriftform erfüllen, können als eine Variante jeweils über ein entsprechendes Postfach des Servicekontos übermittelt werden. Durch das Servicekonto wird die eindeutige Verbindung bzw. Zugehörigkeit des Dokuments zur adressierten Person bzw. zur sendenden Person sichergestellt.

Verknüpfung von QR-Codes mit Servicekonten

Die im Kapitel 3.1. dargestellten Anforderungen im Hinblick auf Authentizität, Integrität und Barrierefreiheit können mit QR-Codes und Servicekonto wie nachstehend beschrieben erfüllt werden:

- **Authentizität:** Die Registrierung („Identifizierung“) und Anmeldung (analog der Technischen Richtlinie TR-03107 „Elektronische Identitäten und Vertrauensdienste im E-Government“ des Bundesamt für Sicherheit in der Informationstechnologie (BSI)) im Servicekonto erfüllt die Anforderung, dass bei Ausgangsdokumenten (der Verwaltung) der Adressat bzw. der bei Eingangsdokumenten der Absender eindeutig identifiziert und nachvollziehbar ist. Der adressierte Verwaltungskunde ist gleichzeitig der

Eigentümer des Servicekontos sowie des damit technisch eindeutig verknüpften Postfachs. Das notwendige Anmeldeniveau im Servicekonto („normal“, „substanziell“, „hoch“) legt entsprechend das anwendende Fachverfahren fest. Der Verwaltungskunde eröffnet damit den Zustellweg. Damit entspricht die Verbindung von Servicekonto und Postfach dem Postfachzugang beim De-Mail-Dienst oder dem besonderen Anwaltspostfach (beA). Der Unterschied ist, dass die Kundin bzw. der Kunde sich beim Servicekonto gegenüber der Verwaltung identifizieren muss und diesen Zustellweg eröffnet, während bei der Einrichtung eines De-Mail-Postfachs dies gegenüber dem De-Mail-Dienstanbieter erfolgt. Beim beA erfolgt die Einrichtung und Freischaltung des Postfachs durch die Bundesrechtsanwaltskammer (BRAK). Das Postfach ist damit sogar unabhängig von einer eigenständigen Erstregistrierung durch die Rechtsanwälte und einer aktiven Nutzung durch diese empfangsbereit.

- **Integrität:** Die Unveränderlichkeit der Informationen eines Verwaltungsdokuments lässt sich mit dem QR-Code und den darin enthaltenen verschlüsselten Daten herstellen. Zudem können Manipulationsversuche mit Hilfe des QR-Codes und der darüber ansteuerbaren Prüffunktion aufgedeckt werden. Hier hilft zusätzlich der Hashwert oder das Zertifikat. Der verschlüsselte Dokumentendownload (=Transportverschlüsselung) sorgt dafür, dass der Transfer aus dem Postfach des Servicekontos sicher erfolgt. Manipulationsversuche Dritter sind erkennbar. Der Mehrwert gegenüber De-Mail liegt hier in der Transportverschlüsselung sowie dem zusätzlich verschlüsselten QR-Code in Verbindung mit dem Hashwert oder dem Zertifikat.
- **Barrierefreiheit:** Die Registrierung und Anmeldung im Servicekonto geschieht über eine Weboberfläche, welche barrierefrei mit Hilfe eines Webbrowsers bedienbar ist. Entsprechendes gilt auch für die Bedienung des Postfachs. Grundlage ist (wie für jeden Online-Dienst) grundsätzlich das *Behindertengleichstellungsgesetz (BBG)* und die *Barrierefreie Informationstechnik-Verordnung (BITVO)*. Der QR-Code ist über entsprechende Geräte und Software barrierefrei zugängig.

4 Umsetzung des Schriftformerfordernisses mit QR-Codes in Verbindung mit Servicekonten

Nachfolgend wird der Prozess der Anwendung von QR-Codes im Verwaltungsdienst, der die Schriftform als „sonstiges sicheres Verfahren“ erfüllt, erläutert.

Voraussetzung für den Empfang von Verwaltungsdokumenten ist die Registrierung eines Servicekontos. Durch die Registrierung eines Servicekontos auf Basis der Vertrauensniveaus „substanziell“ oder „hoch“ kann sich die Eigentümerin bzw. der Eigentümer des Servicekontos (inkl. Postfach) sicher authentisieren und wird authentifiziert. Damit ist die Grundvoraussetzung für ein "sonstiges sicheres Verfahren“ erfüllt.

Folgende Prozessphasen (vgl. Abbildung 7) schließen sich im Hinblick auf ein „sonstiges sicheres Verfahren“ an:

- Anmeldung im bestehenden Servicekonto
- Erzeugen von QR-Codes **1**
- Zustellen **2** und Abholen **3** des Dokuments über das Postfach
- Prüfung des Dokuments **4**

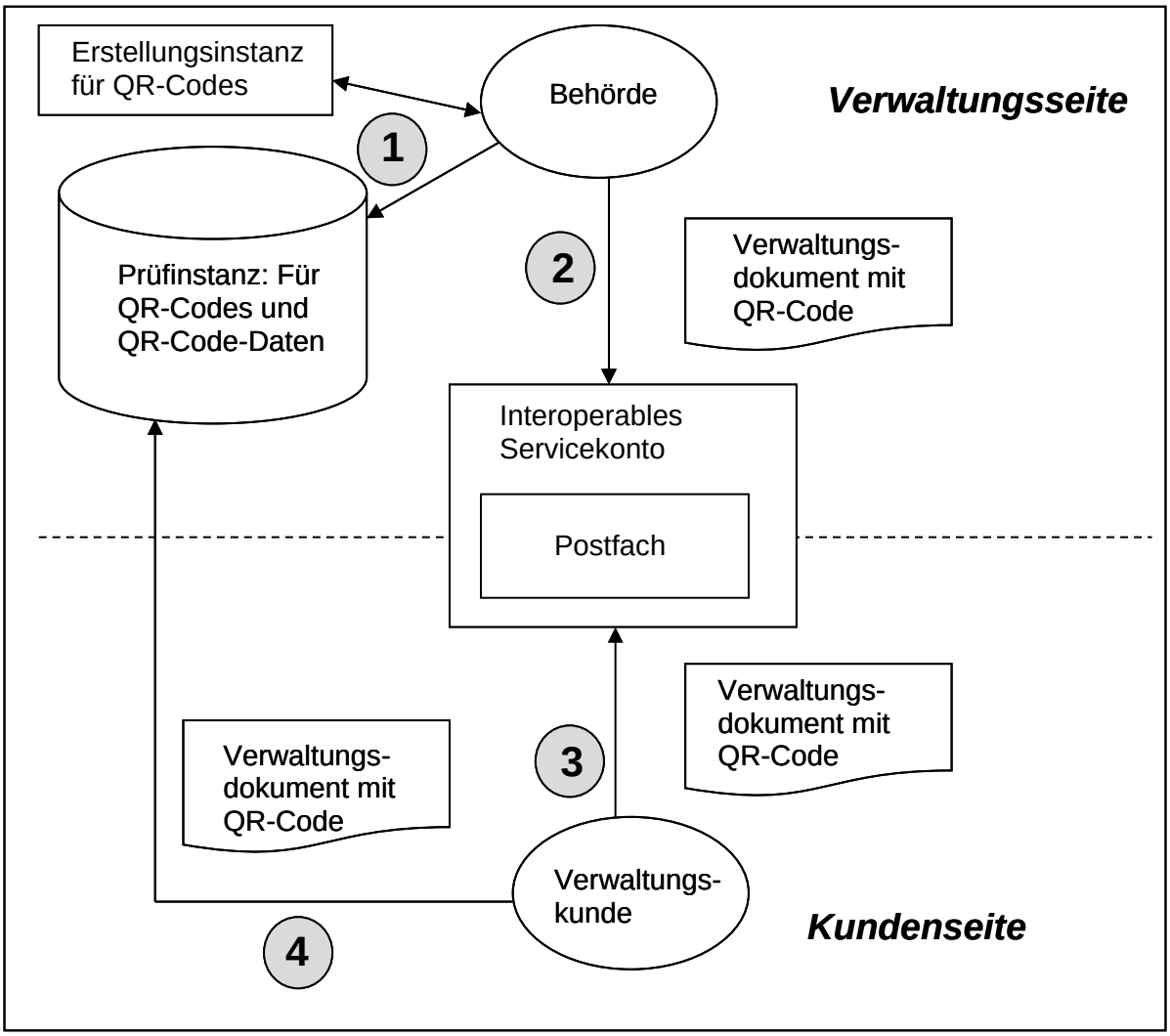

Abbildung 7: Prozess zur Erfüllung der Schriftform für ausgehende Dokumente

Im Servicekonto der Freien und Hansestadt Hamburg (FHH) sieht der Anwendungsfall der Registrierung sowie danach möglichen Anmeldung wie folgt aus:

Anlage eines Servicekontos

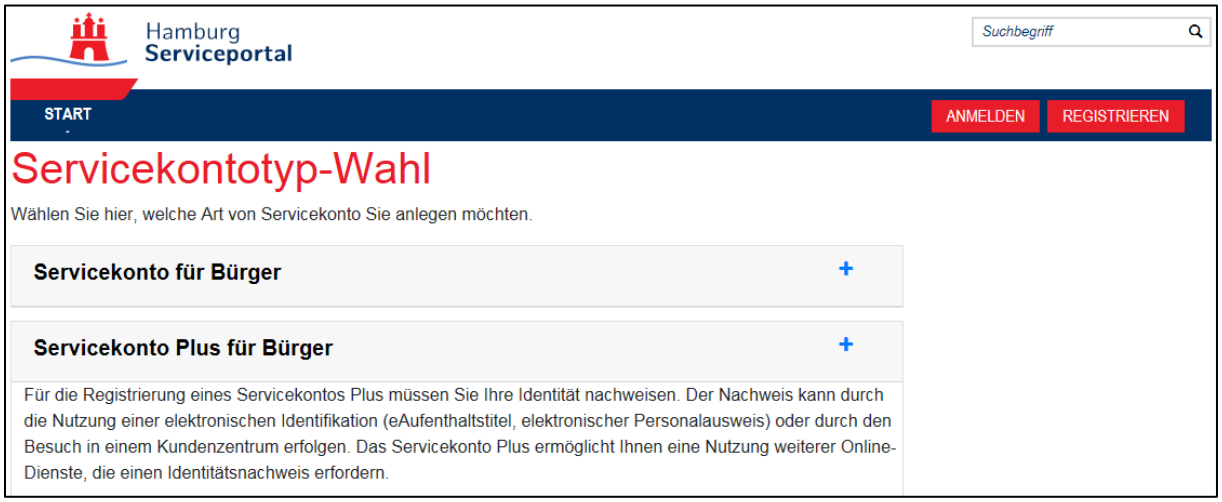

Abbildung 8: Anlage eines Servicekontos (Teil 1)

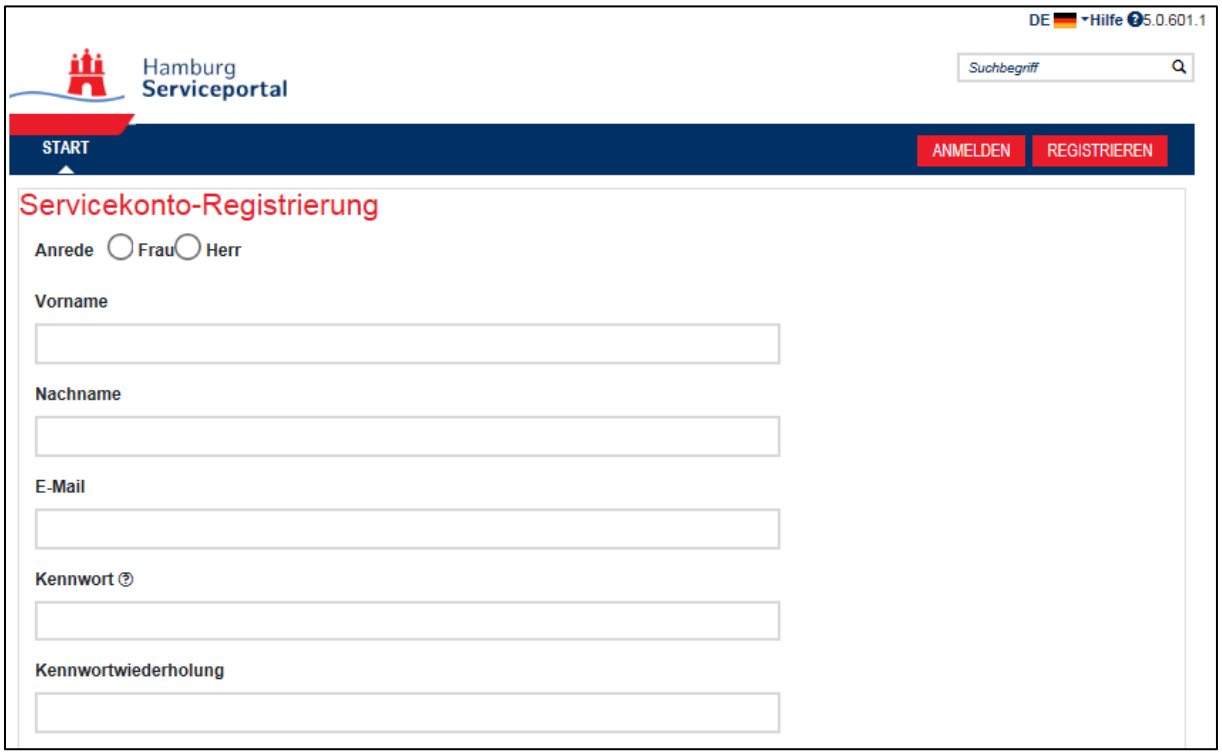

Abbildung 9: Anlage eines Servicekontos (Teil 2)

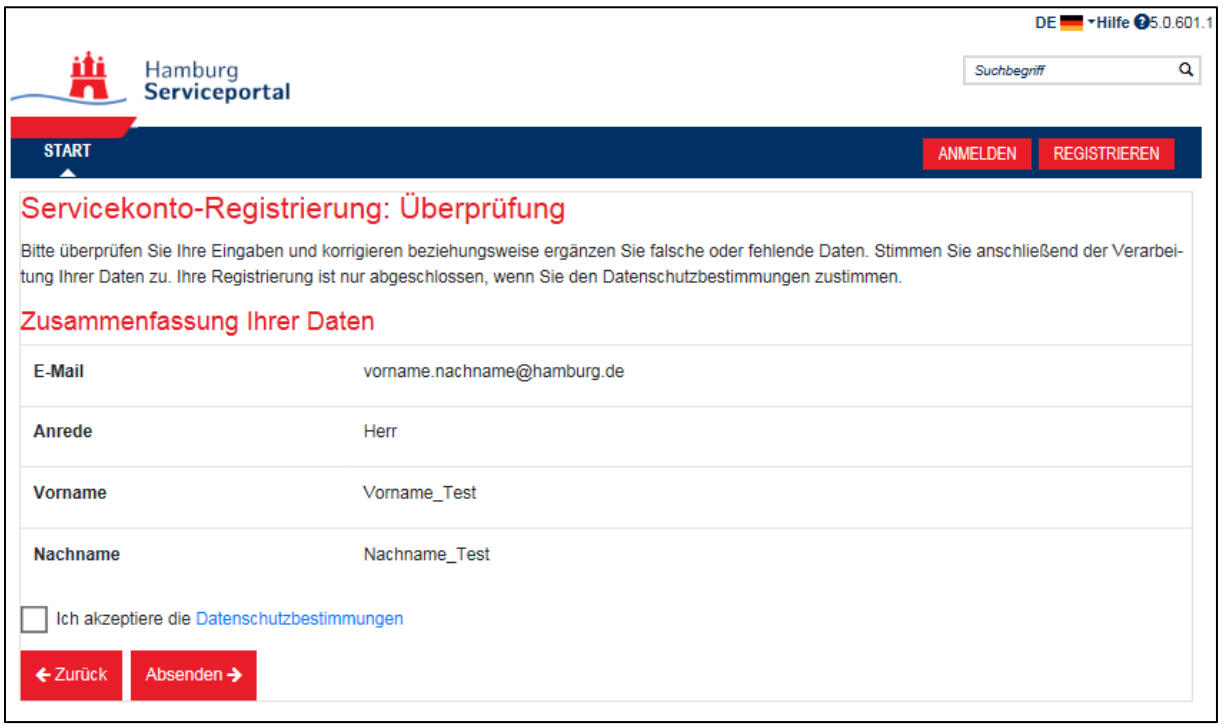

Abbildung 10: Anlage eines Servicekontos (Teil 3)

Anmeldung mit dem Servicekonto im Serviceportal

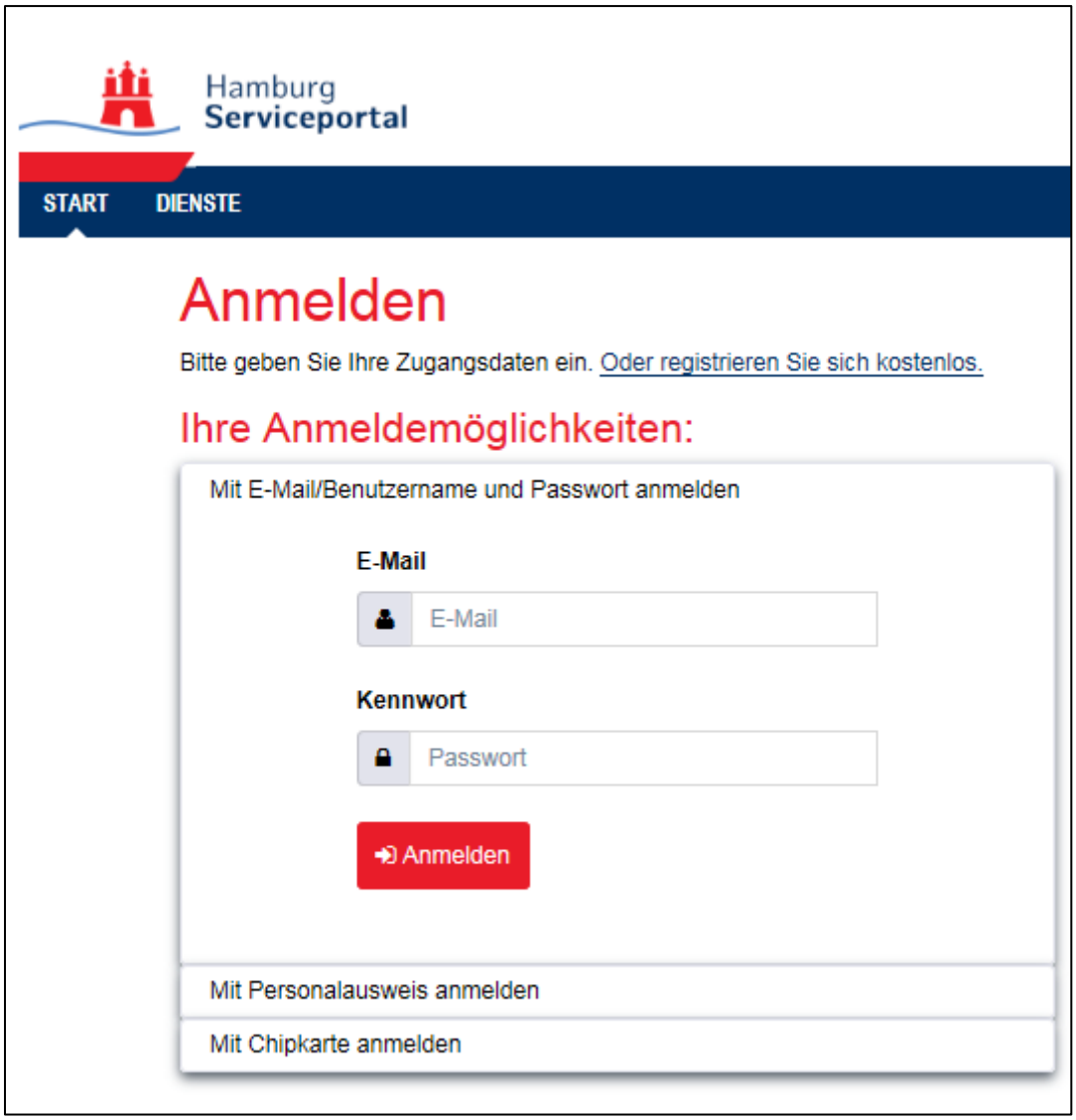

Abbildung 11: Anmeldung im Servicekonto

Der Nutzer meldet sich durch die Angabe der E-Mail-Adresse (=Benutzername) und des Kennworts im Servicekonto an.

Erzeugung von QR-Code auf dem Dokument

Die Verwaltung erzeugt den QR-Code und speichert diesen sowie die zugehörigen (Roh-)Daten in einem internen Datenspeicher. Die Daten des QR-Codes werden mit einem Hashwert oder Zertifikat versehen und verschlüsselt. Dadurch wird die Integrität der Dokumenteninhalte gewahrt. Durch diesen Prozessschritt werden folgende Aufgaben bzw. Funktionen der Schriftform gefördert bzw. erfüllt: Willenserklärung, Beweisfunktion, Klarstellungsfunktion.

Der Anwendungsfall zur Erzeugung eines QR-Codes mittels der Infrastruktur, welche im Kapitel 2 beschrieben wurde, könnte wie nachstehend beispielhaft dargestellt ablaufen:

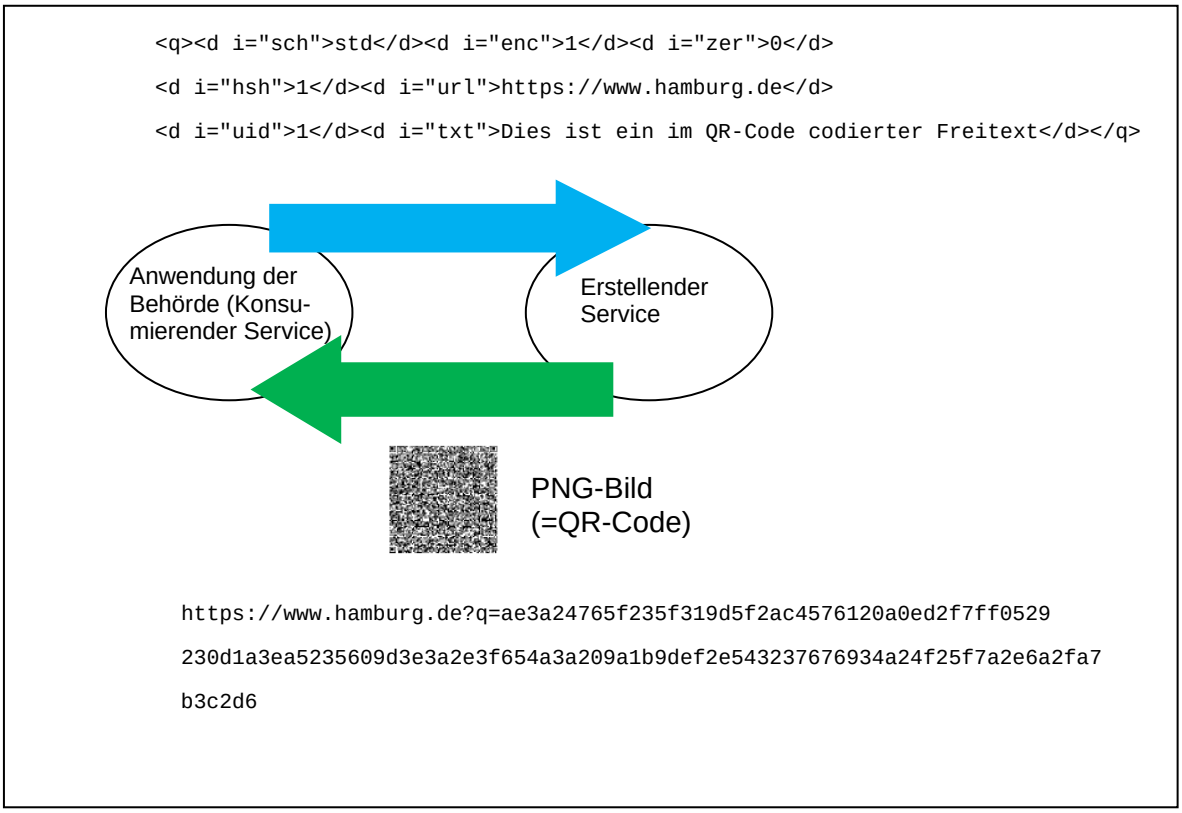

Abbildung 12: Erstellung eines QR-Codes

Zustellung und Empfang des Verwaltungsdokuments

Das Verwaltungsdokument mit dem erzeugten QR-Code wird dem Verwaltungskunden über sein zugehöriges Servicekonto bzw. das zugehörige Postfach zugestellt. Durch diesen Prozessschritt werden folgende Aufgaben bzw. Funktionen der Schriftform gefördert bzw. erfüllt: Willenserklärung, Beweisfunktion, Klarstellungsfunktion.

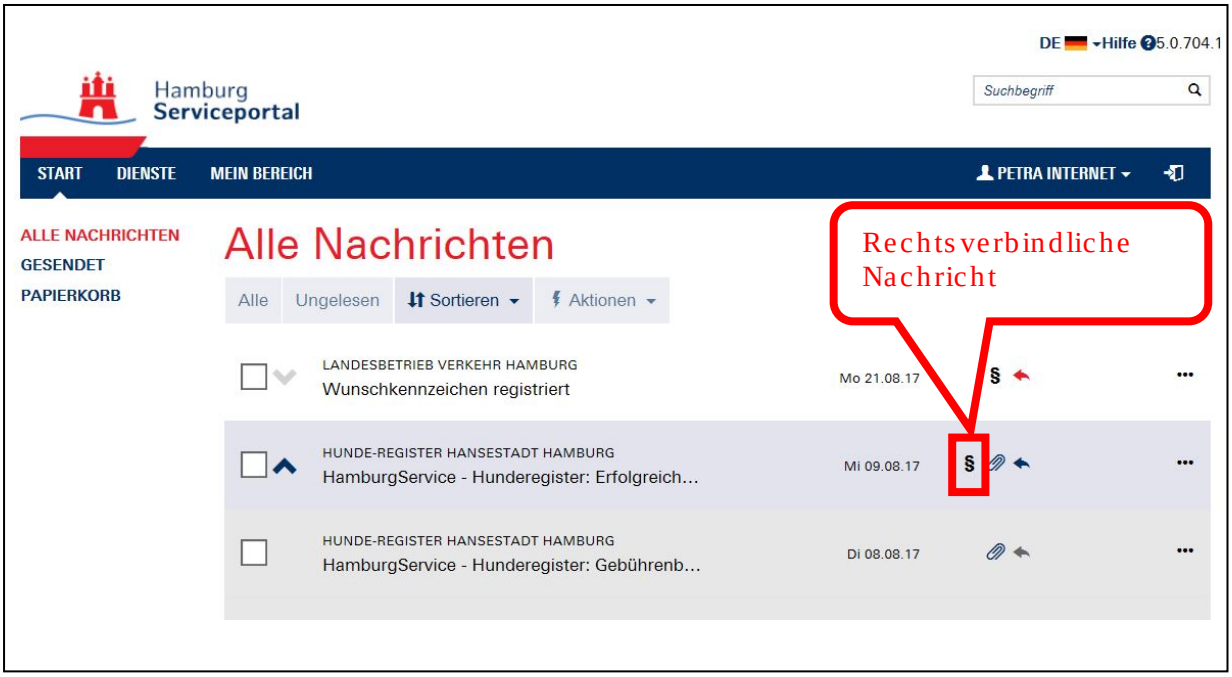

Abbildung 13: Postfacheingang (mit Rechtsverbindlichkeit) in einem Servicekonto

Das Verwaltungsdokument kann durch den Verwaltungskunden über das Servicekonto bzw. das zugehörige Postfach heruntergeladen werden. Die erfolgt analog (d.h. transportverschlüsselt) zu den webbasierten Postfächer der De-Mail-Dienstanbieter. Durch diesen Prozessschritt werden folgende Aufgaben bzw. Funktionen der Schriftform gefördert bzw. erfüllt: Beweisfunktion, Klarstellungsfunktion, Warnfunktion / Hinweisfunktion.

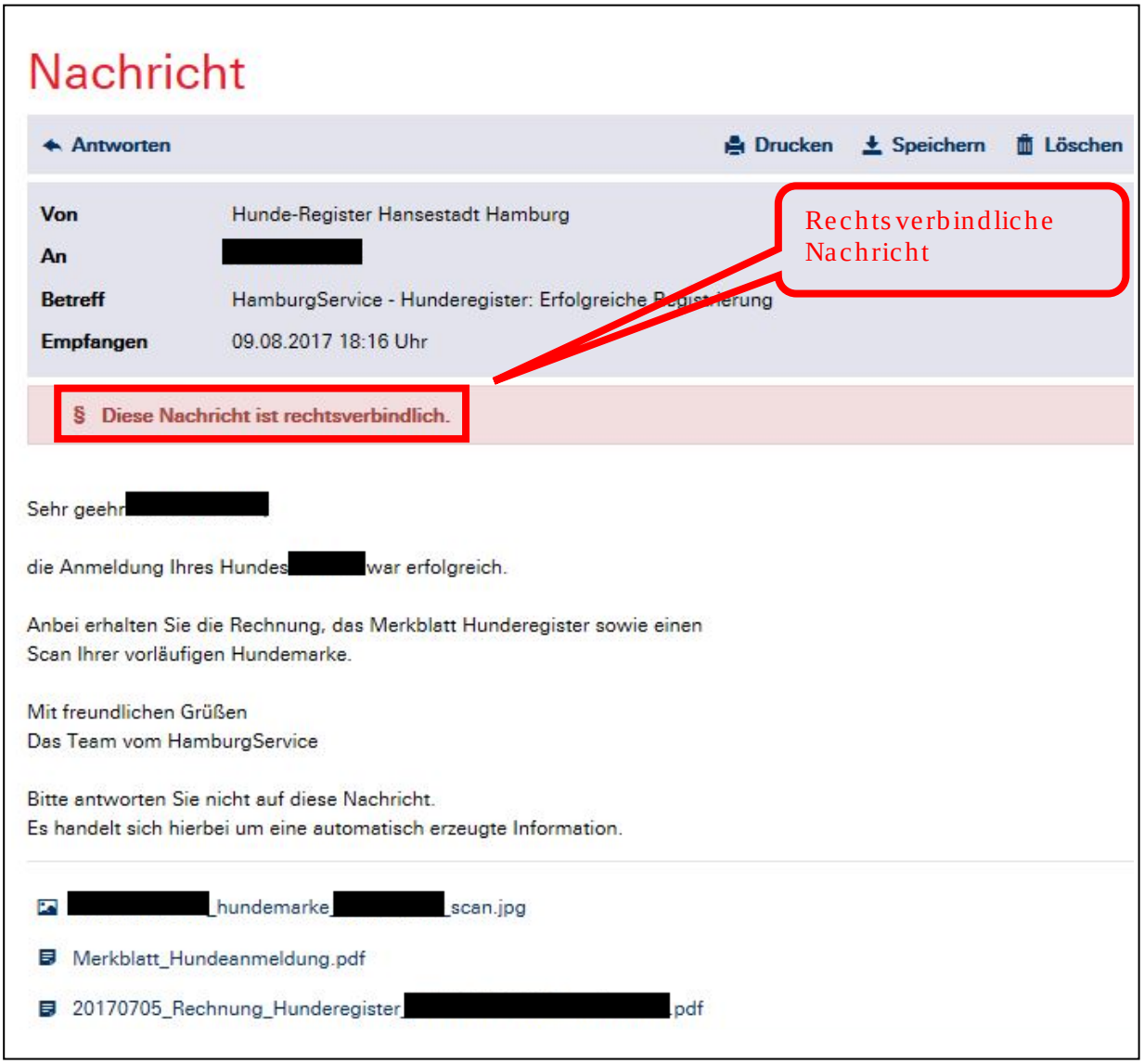

Abbildung 14: Postfachnachricht (mit Rechtsverbindlichkeit) in einem Servicekonto

Prüfung des QR-Codes auf dem Dokument

Das Verwaltungsdokument kann durch den Verwaltungskunden (bzw. ggf. einer dritten Person oder Instanz) mit Hilfe des QR-Codes und des darin codierten Hyperlinks zur Prüfungsinstanz auf die entsprechende Authentizität und Integrität geprüft werden. Durch diesen Prozessschritt werden folgende Aufgaben bzw. Funktionen der Schriftform gefördert bzw. erfüllt: Beweisfunktion, Klarstellungsfunktion, Warnfunktion / Hinweisfunktion.

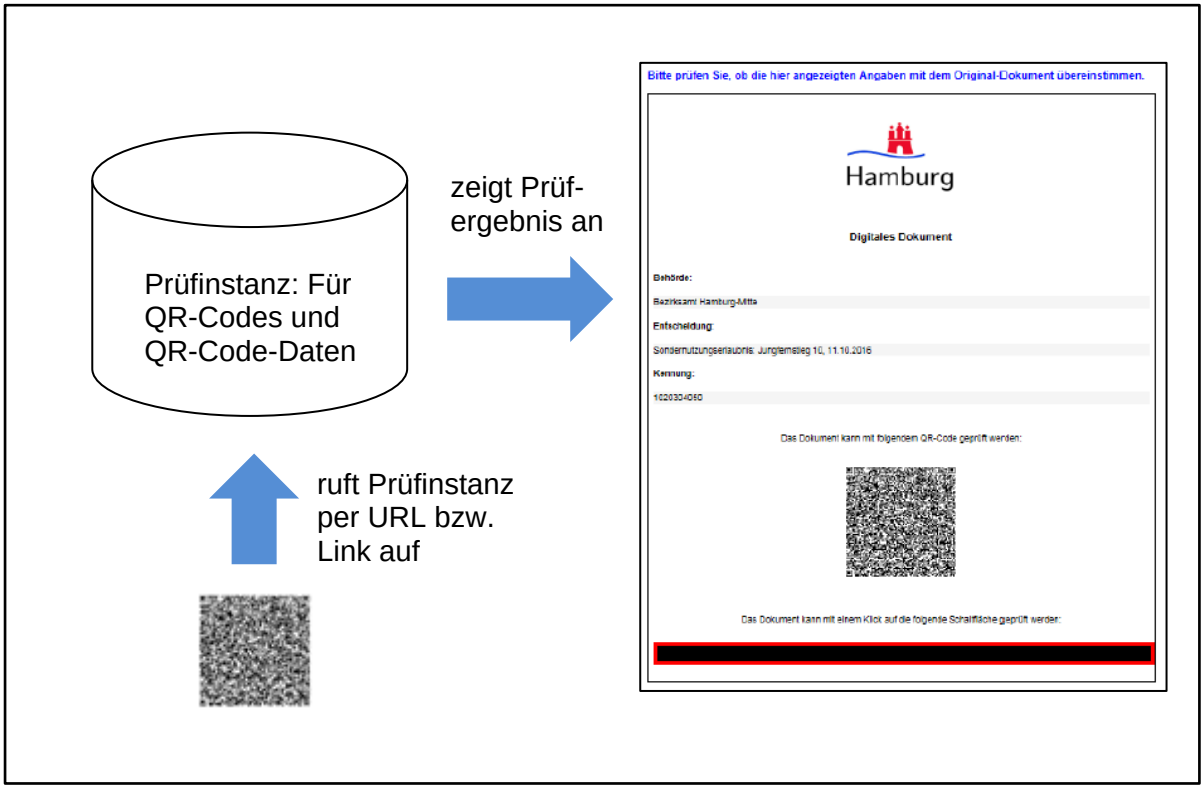

Abbildung 15: Prüfung des QR-Codes auf dem Dokument

Der verschlüsselte QR-Code mit Hashwert oder Zertifikat macht bei Prüfungen, gleichsam einer qualifizierten elektronischen Signatur, eine Manipulation sichtbar. Dadurch kann die Integrität der Dokumenteninhalte sichergestellt werden. Gegenüber der De-Mail-Anwendung ist das ein Mehrwert, da dort ein Dokument nach dem Verlassen der De-Mail nicht mehr geprüft werden kann.

5 Handlungsempfehlungen

Hinsichtlich der zu verwendenden Verschlüsselungsverfahren, Hashverfahren und Zertifikate wird empfohlen, im Rahmen der Umsetzungsaktivitäten zum betreffenden Zeitpunkt entsprechend geeignete und einsetzbare Technologien zu evaluieren und auszuwählen.

Die Arbeitsgruppe zu den QR-Codes auf Verwaltungsdokumenten empfiehlt dem IT-Planungsrat zum weiteren Vorgehen folgende Beschlussfassung:

1. Der IT-Planungsrat nimmt die Konzeption zum Aufbau einer Infrastruktur zum Erstellen sowie zum Prüfen zur Feststellung der Validität (der Inhalte) der Dokumente zur Kenntnis.
2. Der IT-Planungsrat hält QR-Codes in Verbindung mit Servicekonten für ein geeignetes Verfahren im Sinne des § 3a Abs.2 Nr. 4 VwVfG zur Erfüllung des Schriftformerfordernisses.
3. Der IT-Planungsrat empfiehlt der Bundesregierung, QR-Codes in Verbindung mit Servicekonten im Sinne des § 3a Abs.2 Nr. 4 VwVfG als „sonstiges sicheres Verfahren“ in einer entsprechenden Rechtsverordnung festzulegen.
4. Nach der Verabschiedung der Rechtsverordnung setzt der IT-Planungsrat eine neue Arbeitsgruppe ein, um konkrete Maßnahmen zum Aufbau der notwendigen Infrastruktur als Anwendung des IT-Planungsrats zu ergreifen.

6 Glossar

1D-Code

1D-Codes sind eindimensionale Strichcodes, die auch als Balkencode, Streifencode oder Barcode bezeichnet werden. Dabei handelt es sich um eine opto-elektronisch lesbare Markierung, die aus verschieden breiten, parallelen Strichen besteht. Die Daten in einem1D-Code werden mit optischen Lesegeräten, wie z. B. Barcodelesegeräten (Scanner) oder Kameras, maschinell eingelesen und elektronisch weiterverarbeitet.

2D-Code

Im Gegensatz zu eindimensionalen Strichcodes sind die Daten in 2D-Codes nicht nur in einer Richtung (eindimensional) codiert, sondern in Form einer Fläche über zwei Dimensionen. Dadurch wird eine wesentliche höhere Informationsdichte erreicht. Bekannte Beispiele sind der QR-Code, der DataMatrix Code und der Aztec Code.

Data Encryption Standard (3DES/Triple-DES)

Der Data Encryption Standard (DES) ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus. Die Schlüssellänge von 56 Bits gilt heute nicht mehr als ausreichend sicher. Durch Mehrfachanwendung des DES kann die Schlüssellänge jedoch auf einfache Weise vergrößert werden. Dieses Verfahren wird als 3DES oder Triple-DES bezeichnet.

Advanced Encryption Standard (AES)

AES ist ein symmetrisches Verschlüsselungsverfahren, das nach heutigem Kenntnisstand ein sehr hohes Maß an Sicherheit bietet. Es gibt insgesamt drei AES-Varianten (AES-128, AES-192 und AES-256). Die unterschiedlichen Bezeichnungen beziehen sich jeweils auf die gewählte Schlüssellänge.

Atagging

Der Begriff bezeichnet die Manipulation von QR-Codes. Dabei werden Original-QR-Codes z. B. auf Plakaten oder Flyern mit präparierten QR-Codes überklebt, die auf fremde Internetseiten verweisen, welche Schadcode enthalten, um bestimmte Funktionen des Smartphones auszuführen oder Daten von Nutzern abzufragen.

Aztec Code

Der Aztec Code ist ein standardisierter und frei verfügbarer 2D-Code (ISO/IEC 24778).

Bibliothek

Eine Bibliothek (Library) dient der Kapselung von Funktionen bei der Softwareentwicklung, so dass diese Funktionen in unterschiedlichen Systemen der gleichen Programmiersprache und auch von anderen Komponenten genutzt werden können.

Certificate Revocation List (CRL)

Bei der Zertifikatsperrliste handelt es sich um eine öffentlich verfügbare Liste von Zertifikaten, die vor Ablauf der Gültigkeit zurückgezogen wurden. Die CRL ist Bestandteil einer PKI und wird zur Statusprüfung von Zertifikaten verwendet.

Client-Server Architektur

Unter einem Client versteht man hier die Applikation (App), die über das Internet mit einem Server kommuniziert. Der Client ruft die Daten von dem Server ab, so können alle Ressourcen zentral verwaltet werden.

DataMatrix Code

Der DataMatrix Code ist ein standardisierter und weit verbreiteter 2D-Code (ISO/IEC 16022:2006).

Digitales Siegel / Elektronisches Siegel

Ein digitales Siegel / elektronisches Siegel ist die elektronische Abbildung eines analogen (papierbezogenen) Siegels. Auf europäischer Ebene ist durch die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-Verordnung) eine einheitliche Basis dafür geschaffen. Ein digitales Siegel / elektronisches Siegel lässt sich beispielsweise mit Hilfe eines QR-Codes darstellen.

Fortgeschrittene Signatur

Elektronische Signatur mit Hilfe derer sich die Authentizität und die Ursprünglichkeit eines digitalen Dokuments bzw. einer Datei prüfen lässt.

JavaScript Object Notation (JSON)

JSON ist eine JavaScript basierte Notation und wird zum Austausch von Daten verwendet. Das Datenformat ist für Mensch und Maschine lesbar.

Hashwert

Durch einen Hashwert wird eine Zeichenmenge auf einen Wert abgebildet. Dieser Wert umfasst weniger Zeichen als die ursprüngliche Zeichenmenge. Ziel einer entsprechenden Hash-

funktion ist es, das äußerst wenige unterschiedliche Zeichenmengen zum gleichen Hashwert (Kollision) führen.

Hypertext Transfer Protocol Secure (HTTPS)

Im Unterschied zu HTTP werden alle Daten verschlüsselt übertragen. Zu erkennen ist die Verwendung des HTTPS an dem führenden https:// in der URL-Eingabezeile des Browsers.

Mobile Computing

Unter Mobile Computing versteht man die Datenkommunikation eines mobil betriebenen Computers mit anderen stationären oder mobilen Computern. Die Kommunikation kann dabei unter Benutzung des Internet über Mobilfunknetze und WLANs erfolgen.

Mobile Tagging

Das Mobile Tagging ist das bekannteste Einsatzgebiet von QR-Codes. Dabei wird eine beliebige URL im QR-Code kodiert und über eine Scanner App im mobilen Endgerät ausgelesen und aufgerufen.

Maschine Readable Zone (MRZ)

Bei Reisedokumenten ein zweizeiliger Textbereich im ID-3-Format, der in der maschinenlesbaren Schrift OCR-B gesetzt ist und die wichtigsten Daten enthält. Dieser sogenannte maschinenlesbare Bereich kann optisch durch ein entsprechendes Lesegerät ausgelesen werden.

Online-Anwendung

Eine Online-Anwendung ist eine über das Internet über ein spezifisches Protokoll (z. B. HTTP oder HTTPS) erreichbare Applikation, welche in der Regel ohne zeitliche Einschränkungen („24 Stunden und 7 Tage in der Woche“) erreichbar ist.

Qualifizierte elektronische Signatur (qeS)

Eine qualifizierte elektronische Signatur (qeS) ist in Deutschland die Erweiterung einer fortgeschrittenen Signatur, welche mit einem qualifizierten Zertifikat sowie einer sicheren Signaturerstellungseinheit erstellt worden ist.

QR-Code

Der QR-Codes ist eine weit verbreitete Form des 2D-Codes. Die technische Spezifikation des QR-Codes ist in dem Standard ISO/IEC 18004:2015 festgelegt. Die aktuelle Version ist Model 2.

Reed-Solon Codierung

Die Reed-Solon Codierung wird zum Erkennen und Korrigieren von Übertragungs- oder Speicherfehlern bei 2D-Codes eingesetzt. Er findet auch Anwendung beim DVB-Standard zur Aussendung von digitalen Fernsehsignalen, in verschiedenen Mobilfunkstandards, im Digital Audio Broadcasting (DAB) und bei allen gängigen 2D-Codes.

REST-konforme Schnittstellen

Beim REST-Prinzip wird eine Anfrage über HTTP an einen Web-Server gestellt. Anstatt entfernte Operationen aufzurufen und Argumente in einem XML-Dokument zu übergeben, kodiert die URL die Ressource, die eindeutig adressierbar ist. Es stellt neben SOAP und XML-RPC eine weitere Alternative für die Realisierung von Webservices dar.

Software Development Kit (SDK)

Stellt eine Sammlung von Werkzeugen und Anwendungen dar, um eine Software zu erstellen. SDKs werden oft als Bibliothek zusammen mit der Dokumentation zum Download bereitgestellt. Mit diesen ist es Entwicklern möglich, eigene darauf basierende Anwendungen zu erstellen. Der Bezug eines SDKs kann an die Einhaltung bestimmter Regeln, insbesondere die Wahrung der Vertraulichkeit von Informationen, geknüpft werden.

SOAP-basierte Web-Services

SOAP (ursprünglich für Simple Object Access Protocol) ist ein standardisiertes Protokoll, bei dem XML-Nachrichten übertragen werden. SOAP ist ähnlich wie RMI eine Technologie zum entfernten Methodenaufruf, durch die Argumente übergeben werden können und eine Rückgabe erwartet wird. Die Parameter und Rückgaben sind exakt in einer WSDL-Datei beschrieben (ebenfalls im XML-Format). Es lassen sich gut Generatoren einsetzen, die mit Hilfe dieser WSDL-Datei Zugriffsklassen in sämtlichen Programmiersprachen generieren.

URL

Die Abkürzung steht für einen Uniform Resource Locator, welcher ein standardisiertes Format für Netzwerkressourcen darstellt wie beispielsweise eine Webseite.

Digitales Zertifikat

Ein Zertifikat ist ein digitaler Datensatz dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Die Ausstellung des Zertifikats erfolgt durch eine offizielle Zertifizierungsstelle, die Certification Authority (CA).

7 Anhang

8 Weiterführende Links

Bibliothek / SDK (Open Source)	https://github.com/zxing/zxing http://fukuchi.org/works/qrencode http://phpqrcode.sourceforge.net https://www.nuget.org/packages/MessagingToolkit.QRCode http://jeromeetienne.github.io/jquery-qrcode/
Bibliothek / SDK (Drittanbieter)	https://www.leadtools.com/sdk/barcode/2d-qr-code http://www.mw6tech.com/
API Schnittstelle	https://developer.apple.com/reference/avfoundation https://developers.google.com/android/reference/com/google/android/gms/vision/barcode/Barcode?utm_campaign=barcode-815&utm_source=dac&utm_medium=blog https://developers.google.com/chart/infographics/docs/overview http://goqr.me/de/api http://qrickit.com/qrickit_apps/qrickit_api.php
Internet Generator	http://www.qrcode-generator.de http://www.qrcode-monkey.de/
Payment-Lösung	https://www.girocode.de/rechnungssteller/ https://www.cashpaymentsolutions.com/de/geschaeftskunden/branchenloesungen/oeffentliche-verwaltung