Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Konzept des Anwender-Moduls zur Erprobung der Plattformdienste QES (QES-Client)

Version:	1.0.0
Revision:	\main\rel_online\21
Stand:	30.05.2013
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemKPT_QES-Client]

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung Kommentare

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
	03.13	alle	Erstellung	P77
0.9.0	22.03.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare	P77
0.10.0	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare LA	P77
1.0.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.0.0	06.06.13		freigegeben	gematik

Inhaltsverzeichnis

1 Einführung

Der QES-Client ermöglicht dem Anwender die direkte Nutzung der Plattformdienste QES indem er dem Anwender folgende Leistungen des Konnektors zugänglich macht:

- Erstellen und Prüfen einer QES
- Erstellen und Prüfen einer einfachen digitalen elektronischen Signatur
- Ver- und entschlüsseln von Daten
- PIN-Management

Der QES-Client ist der Consumer Zone zugeordnet und kein Teil der TI. Er wird aber genutzt, um Leistungen der TI welche an der PS-Schnittstelle des Konnektors angeboten werden, dem Anwender über eine GUI zugänglich zu machen.

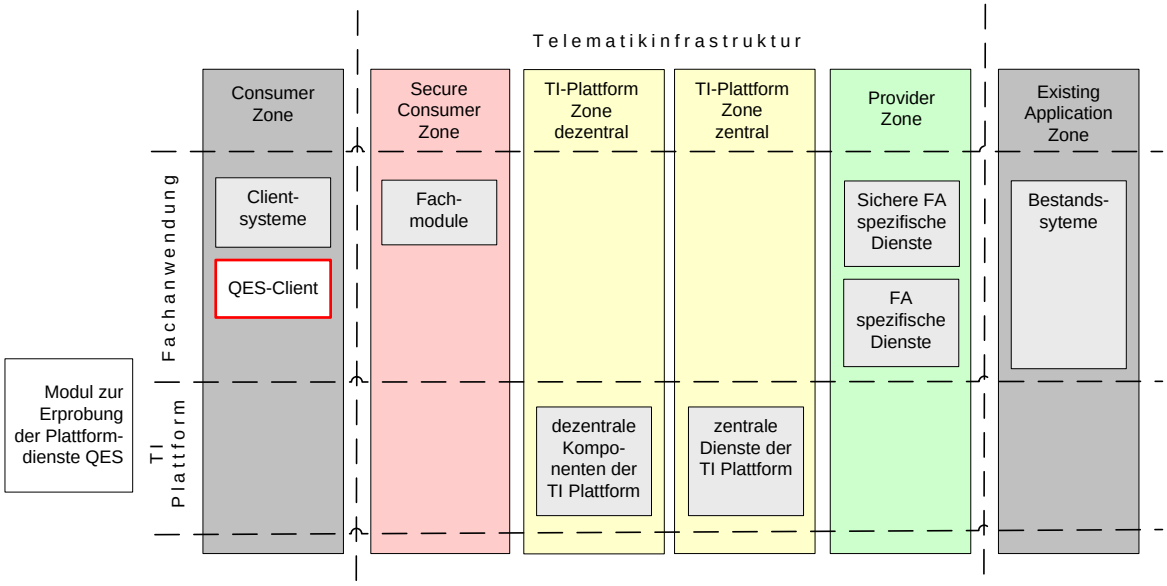

Abbildung 1 – Einordnung des QES-Clients

2 Anforderungen an den QES-Client

2.1 Zu erfüllende Anwendungsfälle

Die unterstützten Anwendungsfälle des QES-Client orientieren sich an den folgenden an der Primärsystemschnittstelle des Konnektors angebotenen Leistungen der TI-Plattform:

- Qualifizierte elektronische Signatur
- Einfache digitale elektronische Signatur
- Ver- und Entschlüsselung inkl. Export von Zertifikaten
- PIN-Management

⌦ **LH-QESC-A_1001 QES-Client – Nutzung der TI-Plattform**

Der QES-Client MUSS für alle Anwendungsfälle ausschließlich die von der TI-Plattform angebotenen Leistungen zur qualifizierten elektronischen Signatur, zur einfachen digitalen elektronischen Signatur und zur Ver- und Entschlüsselung nutzen.⌫

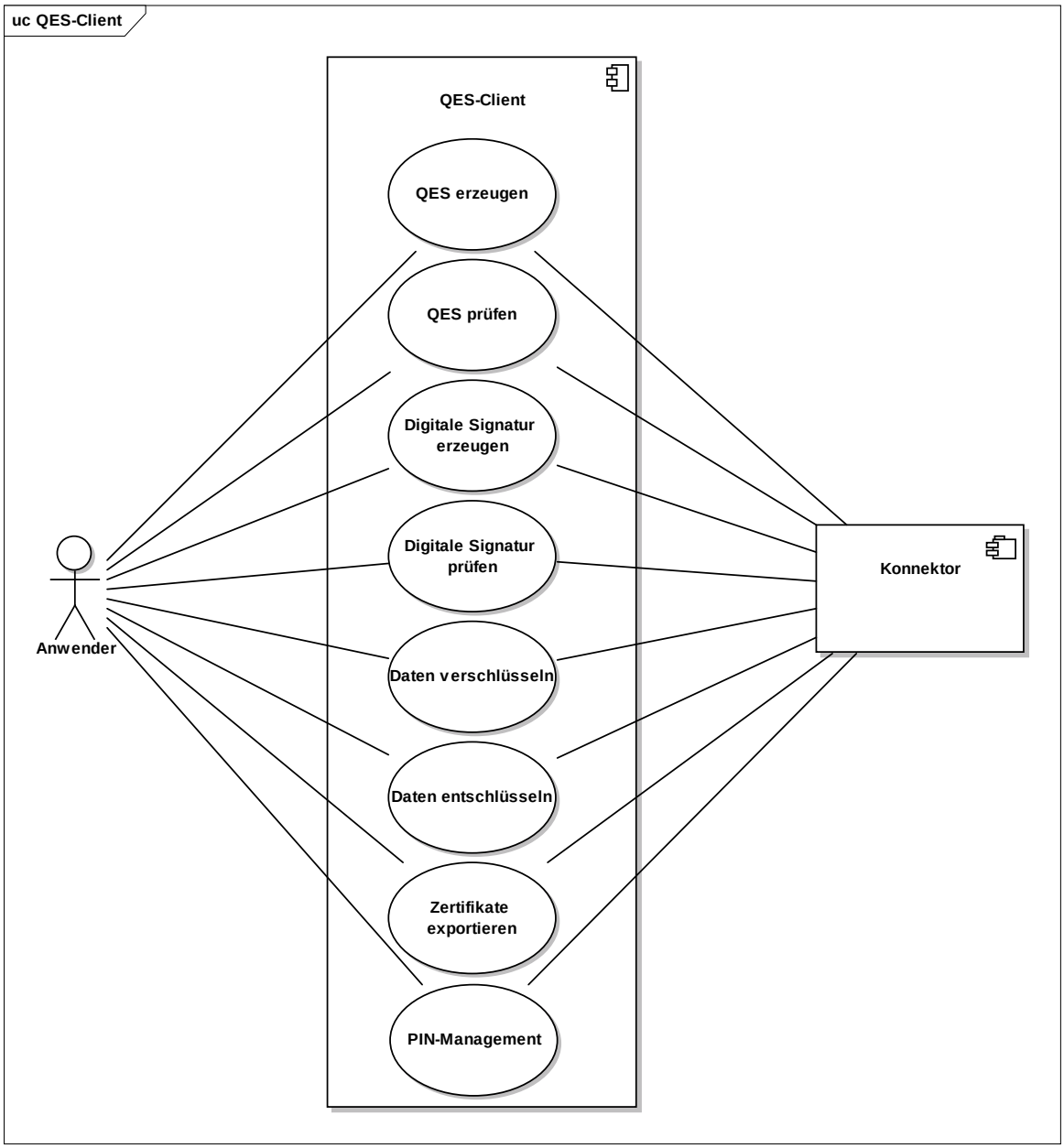

Abbildung 2 - Anwendungsfälle des QES-Clients

2.1.1 QES erzeugen

⌧ LH-QESC-A_1029 UC QES erzeugen – unterstützte Formate, Signaturformen und Identitäten

Der QES-Client MUSS es ermöglichen, eine qualifizierte elektronische Signatur (QES) mit allen in [gemSpec_Kon] an der Operation SignDocument (nonQES und QES) für die QES definierten Optionen zu erstellen.⌫

2.1.2 QES prüfen

⌦ **LH-QESC-A_1030 UC QES prüfen – unterstützte Formate, Signaturformen und Identitäten**

Der QES-Client MUSS es ermöglichen, eine qualifizierte elektronische Signatur (QES) mit allen in [gemSpec_Kon] an der Operation VerifyDocument (nonQES und QES) für die QES definierten Optionen zu prüfen.⌫

2.1.3 Einfache digitale elektronische Signatur erzeugen

⌦ **LH-QESC-A_1010 UC Einfache Signatur erzeugen – Selektion von XML-Elementen**

Der QES-Client MUSS bei der einfachen digitalen elektronischen Signatur von XML-Dokumenten die Selektion der zu signierenden XML-Elemente ermöglichen.⌫

⌦ **LH-QESC-A_1031 UC Einfache Signatur erzeugen – unterstützte Formate, Signaturformen und Identitäten**

Der QES-Client MUSS es ermöglichen, eine einfache digitale elektronische Signatur mit allen in [gemSpec_Kon] an der Operation SignDocument (nonQES und QES) für die nonQES definierten Optionen zu erstellen.⌫

2.1.4 Einfache digitale elektronische Signatur prüfen

⌦ **LH-QESC-A_1032 UC Einfache Signatur prüfen – unterstützte Formate, Signaturformen und Identitäten**

Der QES-Client MUSS es ermöglichen, eine einfache digitale elektronische Signatur mit allen in [gemSpec_Kon] an der Operation VerifyDocument (nonQES und QES) für die nonQES definierten Optionen zu prüfen.⌫

2.1.5 Daten verschlüsseln

⌦ **LH-QESC-A_1015 UC Daten verschlüsseln – Selektion von XML-Elementen**

Der QES-Client MUSS bei der Verschlüsselung von XML-Dokumenten die Selektion der zu verschlüsselnden XML-Elemente ermöglichen.⌫

⌦ **LH-QESC-A_1033 UC Daten verschlüsseln – unterstützte Formate und Identitäten**

Der QES-Client MUSS es ermöglichen, Daten mit allen in [gemSpec_Kon] an der Operation EncryptDocument definierten Optionen zu verschlüsseln.⌫

2.1.6 Daten entschlüsseln

⌦ **LH-QESC-A_1034 UC Daten entschlüsseln – unterstützte Formate und Identitäten**

Der QES-Client MUSS es ermöglichen, Daten mit allen in [gemSpec_Kon] an der Operation DecryptDocument definierten Optionen zu entschlüsseln.⌫

2.1.7 Zertifikate exportieren

⌦ **LH-QESC-A_1035 UC Zertifikate exportieren – Export in Datei**

Der QES-Client MUSS ermöglichen, dass das Verschlüsselungszertifikat eines HBAx oder eines SM-B unter Verwendung der Operation ReadCardCertificate [gemSpec_Kon] des Konnektors ausgelesen, in einer lokalen Datei abgespeichert und im Anwendungsfall „Daten verschlüsseln“ als Parameter verwendet werden kann. Es ist pro Datei nur ein Zertifikat erlaubt.⌫

⌦ **LH-QESC-A_1036 UC Zertifikate exportieren – Datei übermittelbar**

Der QES-Client MUSS die Dateien zur lokalen Speicherung von Verschlüsselungszertifikaten so gestalten, dass sie an andere Anwender übergeben werden können.⌫

Anmerkung: Zukünftig wird der QES-Client ggf. Zertifikate aus einem Verzeichnisdienst abrufen. Diese könnten dann im Anwendungsfall „Daten verschlüsseln“ ergänzend zu den Dateien zur Speicherung von Verschlüsselungszertifikaten verwendet werden.

2.1.8 PIN-Management

⌦ **LH-QESC-A_1039 QES-Client – UC PIN-Management**

Der QES-Client MUSS es ermöglichen, dass der Anwender ein PIN-Management mit allen in [gemSpec_Kon] an den Operationen ChangePin und UnblockPin definierten Optionen durchführen kann.⌫

2.2 Sonstige Merkmale des QES-Clients

Neben den beschrieben Anwendungsfällen setzt der QES-Client auch die nachfolgenden Anforderungen um:

⌦ **LH-QESC-A_1019 QES-Client – Betriebssystemunabhängigkeit**

Der QES-Client SOLL als betriebssystemunabhängige Lösung realisiert werden.⌫

⌦ **LH-QESC-A_1020 QES-Client – Mindestens unterstützte Betriebssysteme**

Wird der QES-Client betriebssystemabhängig realisiert, so MUSS dessen Realisierung mindestens die durch den Konnektor in TIP1-A_4631 [gemSpec_Kon] für den xTV festgelegten Betriebssysteme unterstützen.

⌦ **LH-QESC-A_1021 QES-Client – Sichere Anbindung an den Konnektor**

Der QES-Client MUSS alle in der Spezifikation des Konnektors [gemSpec_Kon] beschriebenen Mechanismen für die sichere Anbindung von Clientsystemen an den Konnektor unterstützen können.⌫

LH-QESC-A_1022 QES-Client – Schnittstelle zum Anwender

Der QES-Client MUSS seine Leistungen dem Anwender über ein Graphical User Interface (GUI) anbieten über das der Anwender alle für einen Anwendungsfall möglichen Optionen auswählen und nötige Parameter übergeben kann.⌫

LH-QESC-A_1040 QES-Client – Default-Werte an der Schnittstelle zum Anwender

Der QES-Client MUSS an seiner Schnittstelle zum Anwender alle Parameter mit sinnvollen Default-Werten vorbefüllen.⌫

LH-QESC-A_1041 QES-Client – Schnittstelle zum Anwender mit zwei Modi

Der QES-Client MUSS an seiner Schnittstelle zum Anwender über zwei Anzeigemodi verfügen, einen Standardmodus in dem nur gebräuchliche Parameter abgefragt werden und einen Expertenmodus in dem alle möglichen Parameter abgefragt werden.⌫

LH-QESC-A_1037 QES-Client – Schnittstelle dateiorientiert

Der QES-Client MUSS an seiner Schnittstelle zum Anwender dateiorientiert arbeiten. Dokumente zur Bearbeitung durch den QES-Client werden in Form von Dateien übergeben.⌫

LH-QESC-A_1038 QES-Client – beliebige Dateiendungen

Der QES-Client MUSS an seiner Schnittstelle zum Anwender Dateien mit beliebigen Dateiendungen akzeptieren.⌫

LH-QESC-A_1023 QES-Client – Integrationsmöglichkeit

Der QES-Client SOLL eine Möglichkeit bieten, sich in bestehende Mechanismen der Anwenderinteraktion (z.B. Kontextmenüs) integrieren zu lassen.⌫

LH-QESC-A_1024 QES-Client – Verwendbarkeit mit allen Konnektor-Produkten

Der QES-Client MUSS ausschließlich die standardisierte Clientsystemschnittstelle des Konnektors benutzen.⌫

Hinweis: Aus LH-QESC-A_1024 ergibt sich, dass der QES-Client mit allen Konnektor-Produkten verwendbar ist, die die standardisierte Clientsystemschnittstelle implementieren.

LH-QESC-A_1025 QES-Client – Leistungsanforderungen Dokumentengröße

Der QES-Client MUSS bei allen Anwendungsfällen Dokumente bis zu einer Größe von mindestens 25 MB unterstützen.⌫

LH-QESC-A_1026 QES-Client – Leistungsanforderungen Verarbeitungszeit

Der QES-Client DARF bei der Verarbeitung eines Anwendungsfalles mit einem Dokument der Größe 25MB – unabhängig von Benutzerinteraktionen – intern NICHT mehr als 500 ms benötigen.⌫

LH-QESC-A_1027 QES-Client – Einsatz in RU, TU, PU

Der QES-Client MUSS für den Einsatz in RU, TU und PU geeignet sein.⌫

⌦ **LH-QESC-A_1028 QES-Client – Installation**

Die Installation des QES-Client MUSS durch einen versierten Benutzer von Computersystemen gemäß Handlungsanweisungen des Benutzerhandbuches eigenständig durchführbar sein.⌫

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
GUI	Graphical User Interface
LH	Lastenheft
MIME	Multipurpose Internet Mail Extensions
PDF/A	Portable Document Format für Archivierung
PS	Primärsystem
PU	Produktivumgebung
QES	Qualifizierte Elektronische Signatur
RU	Referenzumgebung
S/MIME	Secure / Multipurpose Internet Mail Extensions
TI	Telematikinfrastruktur
TIFF	Tagged Image File Format
TU	Testumgebung
UC	Use Case (dt. Anwendungsfall)
XML	Extensible Markup Language

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A5 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird

pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellsten, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemSpec_Kon]	gematik: Spezifikation Konnektor

Weitere Referenzierungen:

[Quelle]	Herausgeber (Erscheinungsdatum): Titel