

Vereinheitlichung Bürgerkartenumgebung

Vorschlag einer einheitlichen Benutzerschnittstelle als Teil der Bürgerkartenspezifikation

Graz, am 31. März 2006

DI Thomas Rössler – thomas.roessler@egiz.gv.at

Zusammenfassung: Aus den Erfahrungen in der Verwendung der Bürgerkarte bzw. der Bürgerkartenumgebung (BKU) durch die AnwenderInnen sind Einstiegshürden für nicht Technik-versierte weniger Probleme technischer Natur, als viel mehr Probleme aufgrund der unterschiedlichen Formen der Handhabe und Benutzerführung (User Interface – UI). Es ließe sich hier eine Verbesserung der Benutzerfreundlichkeit erzielen, wenn über konsistente Verwendung von Layouts, Piktogrammen und Informationsverweisen Vertrautheit gefördert wird.

Dieses Dokument gibt daher einen Vorschlag einer einheitlichen Benutzerschnittstelle zu Bürgerkartenumgebungen und skizziert Standarddialoge und Vereinfachungen für die Standardfunktionen der Bürgerkarte (basierend auf der Bürgerkarten-Spezifikation 1.2.1).

Inhaltsverzeichnis:

Schlüsselwörter	3
Anmerkung	3
Revision History	3
1 Einleitung.....	4
2 Grunderfordernisse an das UI	4
2.1 Klassen von UI-Elementen	4
2.2 Grundstruktur der UI-Dialoge.....	5
3 Grundbegriffe der Bürgerkarte	5
3.1 PIN-Bezeichnung.....	5
3.1.1 PIN-Code zur Anwendung des SecureSignatureKeypair	5
3.1.2 PIN-Code zur Anwendung des CertifiedKeypair.....	5
3.1.3 Sonstige PIN-Codes	6
4 User Interface (UI) für Basisfunktionen der Bürgerkarte	7
4.1 Signaturerstellung.....	7
4.2 Signaturprüfung	9
4.2.1 Anzeige verschiedener Signaturteile (Signaturreferenzen)	9
4.2.2 Anzeige der signierten Daten	13
4.3 Verschlüsselung	14
4.4 Entschlüsselung.....	17
4.5 Hashwert Berechnung	19
4.5.1 Detailanzeige der Hashwert-Berechnung.....	21
4.6 Hashwert Verifikation.....	22
5 Menüführung	25
5.1 Menüeinträge des Einstiegsmenüs – Ebene 0:	25
5.2 Menüeinträge zu ‚Bürgerkartenfunktionalitäten‘ – Ebene 1:	26
5.3 Menüeinträge zu ‚Bürgerkartenumgebung anhalten‘ – Ebene 2:.....	29
5.4 Menüeinträge zu ‚PIN Verwaltung‘ – Ebene 2:	29
Referenzen.....	31

Schlüsselwörter

Dieses Dokument verwendet die Schlüsselwörter muß, darf nicht, erforderlich, sollte, sollte nicht, empfohlen, darf und optional zur Kategorisierung der Anforderungen. Diese Schlüsselwörter sind analog zu ihren englischsprachigen Entsprechungen must, must not, required, should, should not, recommended, may, und optional zu handhaben, deren Interpretation in [1] festgelegt ist.

Insbesondere sei an dieser Stelle auf die schwerwiegend unterschiedliche Bedeutung von sollte (bzw. dessen Entsprechungen) im Gegensatz zu darf (bzw. dessen Entsprechungen) hingewiesen (vgl. [1], Abschnitte 3 und 5).

Anmerkung

Zur besseren Lesbarkeit wurde in diesem Dokument teilweise auf geschlechtsspezifische Formulierungen verzichtet. Die verwendeten Formulierungen richten sich jedoch ausdrücklich an beide Geschlechter.

Revision History

Version	Datum	Autor(en)	
1.0.0	31.03.2006	Thomas Rössler	erstellt.

1 Einleitung

Aus den Erfahrungen in der Verwendung der Bürgerkarte bzw. der Bürgerkartenumgebung (BKU) durch die AnwenderInnen sind Einstiegshürden für nicht Technik-versierte weniger Probleme technischer Natur, als viel mehr Probleme aufgrund der unterschiedlichen Formen der Handhabe und Benutzerführung (User Interface – UI). Es ließe sich hier eine Verbesserung der Benutzerfreundlichkeit erzielen, wenn über konsistente Verwendung von Layouts, Piktogrammen und Informationsverweisen Vertrautheit gefördert wird.

Dieses Dokument gibt daher einen Vorschlag einer einheitlichen Benutzerschnittstelle zu Bürgerkartenumgebungen und skizziert Standarddialoge und Vereinfachungen für die Standardfunktionen der Bürgerkarte (basierend auf der Bürgerkarten-Spezifikation 1.2.1 [3]).

Dieser Vorschlag wird in weiterer Folge den einzelnen BKU-Herstellern zur Diskussion gestellt. Dabei sollen bereits von deren Seite gesammelte Erfahrungen einfließen und zur Weiterentwicklung dieses UI-Konzepts beitragen.

Die in diesem Dokument getroffenen bzw. vorgeschlagenen Mindestanforderungen beziehen sich ausschließlich und ausdrücklich auf die Standardfunktionen der Bürgerkarte. Es lehnt sich daher an die im Spezifikationsdokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkartenumgebung der österreichischen Bürgerkarte“ [2] getroffenen Vorgaben an, und konkretisiert diese anhand illustrativer Vorschläge. Normativ bleiben nach wie vor die in [2] – bzw. im Allgemeinen in [3] – getroffenen Definitionen, insbesondere dann, wenn die in diesem Dokument enthaltenen Vorschläge dazu in Widerspruch stehen sollten.

Ziel dieser Initiative ist es letztendlich auch die UI-Basiselemente der BKU, d.h. die Grundformen der Benutzerführung und –dialoge, ebenfalls im Rahmen der Spezifikation „Bürgerkarte“ festzulegen und dort verbindlich zu regeln. Dazu legt dieses Dokument eine Basis.

2 Grunderfordernisse an das UI

Das UI muß intuitiv, klar und in Bezug auf Standardfunktionen einheitlich strukturiert sein. Jeder BKU-Hersteller sollte auch die Verwendbarkeit seiner Implementierung des UI für Personen mit besonderen Bedürfnissen prüfen und dahingehend optimieren. So ist zum Beispiel auf die Darstellbarkeit durch Brailleschrift achten.

2.1 Klassen von UI-Elementen

Bei der Beschreibung der Grundstruktur des UI in diesem Dokument wird auf folgende Klassen von UI-Elementen zurückgegriffen:

- a) **Information**
... Elemente dieses Typs dienen rein zur Darstellung von Informationen, wie zum Beispiel Text-Panels, etc.
- b) **Interaktion**
... Elemente dieses Typs dienen der einfachen Interaktion mit der BKU, wie zum Beispiel Schaltflächen, Check-Boxen, etc.
- c) **Eingabe**
... Elemente dieses Typs dienen zur Eingabe von Werten, wie zum Beispiel Text-Felder, etc.

Die in den exemplarischen Strukturdarstellungen verwendeten konkreten UI-Elemente, wie Buttons, etc., stehen stellvertretend für die entsprechende Klasse von UI-Elementen. Variationen bei der Implementierung des UI sind selbstverständlich möglich. Entscheidend ist, daß die entsprechende Klasse bzw. die damit verbundene Interaktion möglich ist.

2.2 Grundstruktur der UI-Dialoge

Dieses Dokument skizziert die einzelnen UI-Dialoge anhand von exemplarischen Strukturdarstellungen in Form von Screenshots, zusätzlich werden Details zu den einzelnen UI-Elementen textuell beschrieben.

Besonders die Strukturdarstellungen sollen nur das Layout verdeutlichen und die grundlegende Struktur widerspiegeln. Hersteller- bzw. produktspezifische Variationen sind möglich, bspw. durch Hinzufügen von Hersteller-/Produktlogos am Kopf oder am Ende des Dialogs; diese dürfen aber keinesfalls die hier festgelegte Grundstruktur des UI zerstören.

3 Grundbegriffe der Bürgerkarte

Vereinheitlichung ist nicht nur in Bezug auf das grafischen Layout des UI sinnvoll, sondern auch bezüglich der verwendeten Terminologie zu fordern. Gerade die diversen Bezeichnungen der verschiedenen PIN-Codes müssen einheitlich gehandhabt werden.

3.1 PIN-Bezeichnung

Die Bürgerkartenspezifikation bedient sich zweier Schlüsselpaare, dem SecureSignatureKeypair zur Erzeugung sicherer Signaturen, und dem CertifiedKeypair zur Erstellung einfacher, elektronischer Signaturen. Beide Schlüsselpaare sind durch PIN-Codes unterschiedlicher Länge geschützt. Zudem können die Infoboxen einer Bürgerkarte selbst – zum Beispiel die Infobox der Personenbindung – ebenfalls durch entsprechende PIN-Codes gesichert sein.

Da das Konzept Bürgerkarte unabhängig von ihrer konkreten technischen Ausformung ist, können je nach verwendeter Technologie bzw. Implementierung weitere PIN-Codes notwendig sein. Durch die Vielfalt an PIN-Codes und den damit einhergehenden Bezeichnern ist der Anwender oft restlos überfordert. Daher werden einheitlich folgende Begriffe für die Bürgerkarte festgelegt.

Dieser Abschnitt wird bei Aufkommen weiterer eindeutig festzulegender Bezeichner erweitert.

3.1.1 PIN-Code zur Anwendung des SecureSignatureKeypair

Dieser PIN-Code ist mindestens 6-stellig.

Es müssen folgende Bezeichnungen verwendet werden:

Kurzbezeichnung: **Signatur PIN**

Hilfsbezeichnung: **6+ stelliger PIN**

Langbezeichnung: **PIN zum Auslösen der sicheren Signatur**

3.1.2 PIN-Code zur Anwendung des CertifiedKeypair

Dieser PIN-Code ist mindestens 4-stellig.

Es müssen folgende Bezeichnungen verwendet werden:

Kurzbezeichnung: **Geheimhaltungs PIN**

Hilfsbezeichnung: **4+ stelliger PIN**

Langbezeichnung: **PIN zum Auslösen der einfachen Signatur und zur Ver-/Entschlüsselung**

3.1.3 Sonstige PIN-Codes

Alle weiteren PIN-Codes sind kartenspezifisch und müssen so wie auf der zur Grunde liegenden Hardware bzw. Signatur-Karte festgelegt bezeichnet werden. Es dürfen dabei aber keinesfalls Widersprüche oder Mehrdeutigkeiten bezgl. der in den vorhergegangenen Abschnitten definierten Bezeichnungen auftreten. So zum Beispiel darf der PIN-Code zur Auslösung der sicheren Signatur nur wie in Abschnitt 3.1.1 spezifiziert bezeichnet werden (sofern nichts Anderes im Rahmen der Bürgerkartenspezifikationen [3] festgelegt wird).

4 User Interface (UI) für Basisfunktionen der Bürgerkarte

In diesem Abschnitt werden die UI-Elemente für die Basisfunktionen der BKU skizziert – in Anlehnung an die in [2] getroffenen Mindestanforderungen.

Viele der hier beschriebenen Funktionalitäten sind in der Bürgerkartenspezifikation in verschiedenen Ausprägungen definiert – so zum Beispiel die Erstellung/Prüfung von Signaturen entweder nach XML-DSig [4] oder nach CMS [5]. Sofern sich aufgrund dieser unterschiedlichen Ausprägungen keine unmittelbare Auswirkung auf das UI entfaltet, wird darauf hier nicht näher eingegangen, und das definierten UI ist auf alle Ausprägungen sinngemäß anzuwenden.

4.1 Signaturerstellung

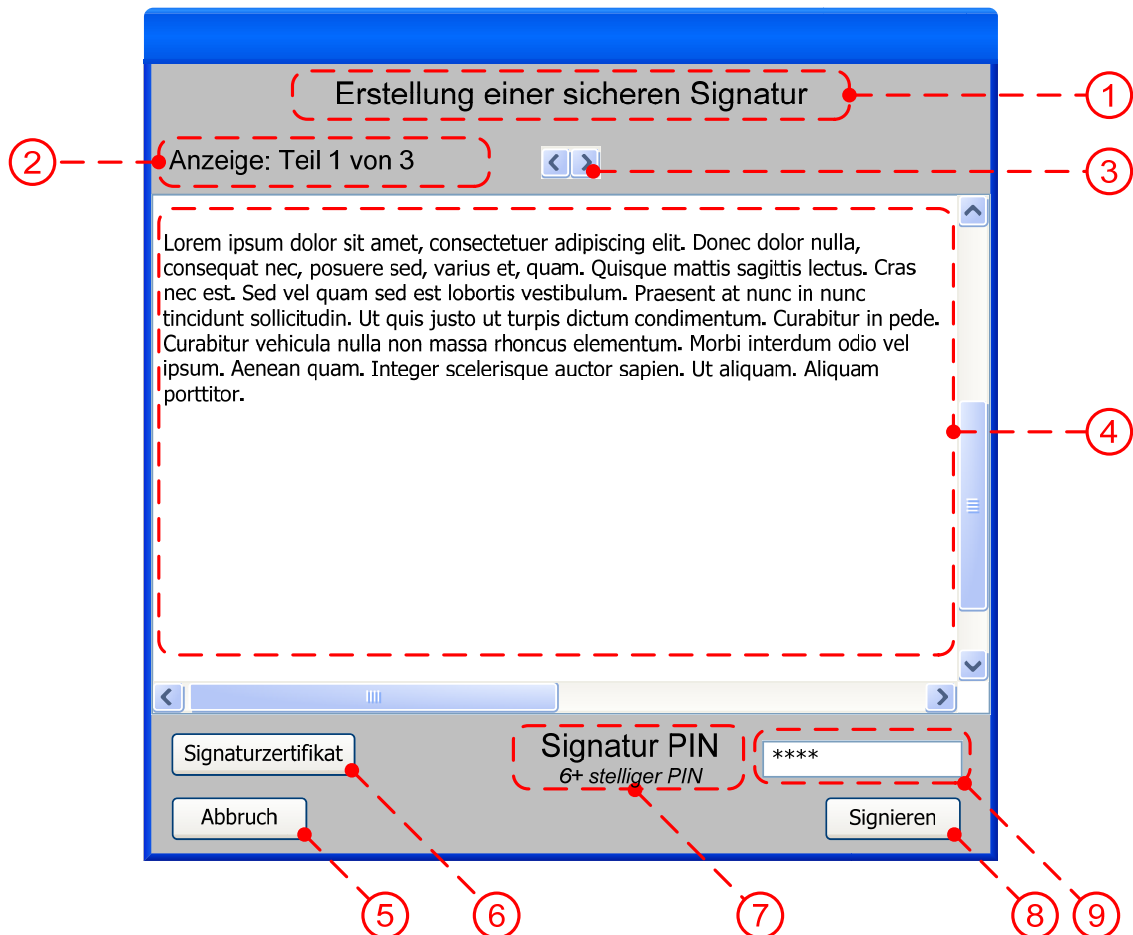
Im Zuge der Signaturerstellung werden die zu signierenden Dokumente/Daten im Secure-Viewer zur Anzeige gebracht. Hier ist auf eine kompakte und intuitive Form der Anzeige zu achten.

Um den Interaktionsaufwand mit dem Bürger zu reduzieren, sollte im Zuge der sicheren Anzeige auch gleich die PIN-Eingabe realisiert werden.

Die hier beschriebene UI-Struktur gilt sowohl für Signaturen nach XML-DSig als auch für die Signaturerstellung nach CMS.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.1, zu finden.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Erstellung einer sicheren Signatur“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Aktuell dargestellter Signaturteil	Information	Angabe welcher Teil der zu signierenden Daten gerade angezeigt wird. Signaturen können in einer Signatur verschiedene und sogar von einander unabhängige Daten beinhalten. Jede dieser Daten bzw. Signaturteile sind gesondert anzuzeigen. Mit diesem Element wird der Anwender darüber informiert, welcher Teil soeben dargestellt wird.
3	Navigation Signaturteile	Interaktion	Der Anwender soll die Möglichkeit haben einfach durch die verschiedenen Signaturteile bzw. durch die zu signierenden Daten zu navigieren.
4	Sichere Anzeige	Information	Anzeige der zu signierenden Daten.
5	Abbruch-Button	Interaktion	Schließt die Anzeige und bricht den Signaturerstellungsprozeß ab.
6	Signaturzertifikat-Button	Interaktion	Button bewirkt Anzeige des zur Signatur verwendeten Signaturzertifikats. Zur Darstellung des Zertifikats selbst soll entweder direkt der durch das Betriebssystem des Anwenders zur Verfügung gestellte Zertifikats-Viewer herangezogen werden, oder aber eine dem entsprechende gängige Repräsentation gewählt werden, um den Anwender die Zertifikatsdaten in gewohnter Weise zu visualisieren.
7	Bezeichnung des geforderten PIN-Codes	Information	Anzeige des einzugebenden PIN-Codes nach den in 3.1 definierten Bezeichnungen. Hier muß die ‚Kurzbezeichnung‘ angeführt werden, z.B. „Signatur PIN“. Zudem soll auch die ‚Hilfsbezeichnung‘ mitangegeben werden, z.B. „6+ stelliger PIN“; es soll auch die ‚Langbezeichnung‘ anzeigbar sein, beispielsweise über zusätzliche Hilfstexte oder per Mouse-Rollover.
8	Eingabefeld PIN-Code	Eingabe	Feld zur PIN-Code Eingabe. Im Falle der PIN-Code Eingabe per Software ist in

			dieses Feld der PIN-Code einzugeben. Im Falle der PIN-Code Eingabe via PIN-Pad des Kartenlesegerätes bleibt dieses Eingabefenster deaktiviert oder kann gänzlich entfallen.
9	Signier-Button	Interaktion	Interaktionselement löst den Signaturvorgang aus. Ist die Eingabe des PIN-Codes per Software-Eingabe gefordert, so wird der in Feld-Nr. 8 eingegebene PIN-Code verwendet. Ansonst erfolgt die PIN-Code-Abfrage via PIN-Pad bzw. Treiber des verwendeten Kartenlesers.

4.2 Signaturprüfung

Infolge der Signaturprüfung ist sowohl die möglichst einfache Darstellung des Prüfergebnisses als auch die Anzeige der signierten Daten notwendig. Zudem können Signaturen mehrere Signaturreferenzen/-teile beinhalten, die ihrerseits wiederum unabhängige Teile des Dokuments repräsentieren können.

Nicht zuletzt daher ist die korrekte und intuitive Aufbereitung bzw. Visualisierung der geprüften Signaturen und deren Signaturreferenzen, bzw. den dahinterstehenden tatsächlich signierten Daten, entscheidend.

Neben der kryptographischen Aufbereitung der zu prüfenden Signatur(-teile) ist auch die Darstellung des Zertifikatsprüfungsergebnisses entsprechend zu gestalten. Das Signaturzertifikat bzw. die Zertifikatskette hin zum vertrauenswürdigen (Wurzel-)Zertifikat des ausstellenden Zertifizierungsdiensteanbieters muß visualisiert werden.

Nachfolgend werden zwei Visualisierungselemente zur Darstellung des Signaturprüfprozesses bzw. dessen Ergebnisses skizziert. Zum einen wird eine kompakte Darstellung des Prüfergebnisses definiert; zum anderen die Anzeige der signierten Daten selbst festgelegt.

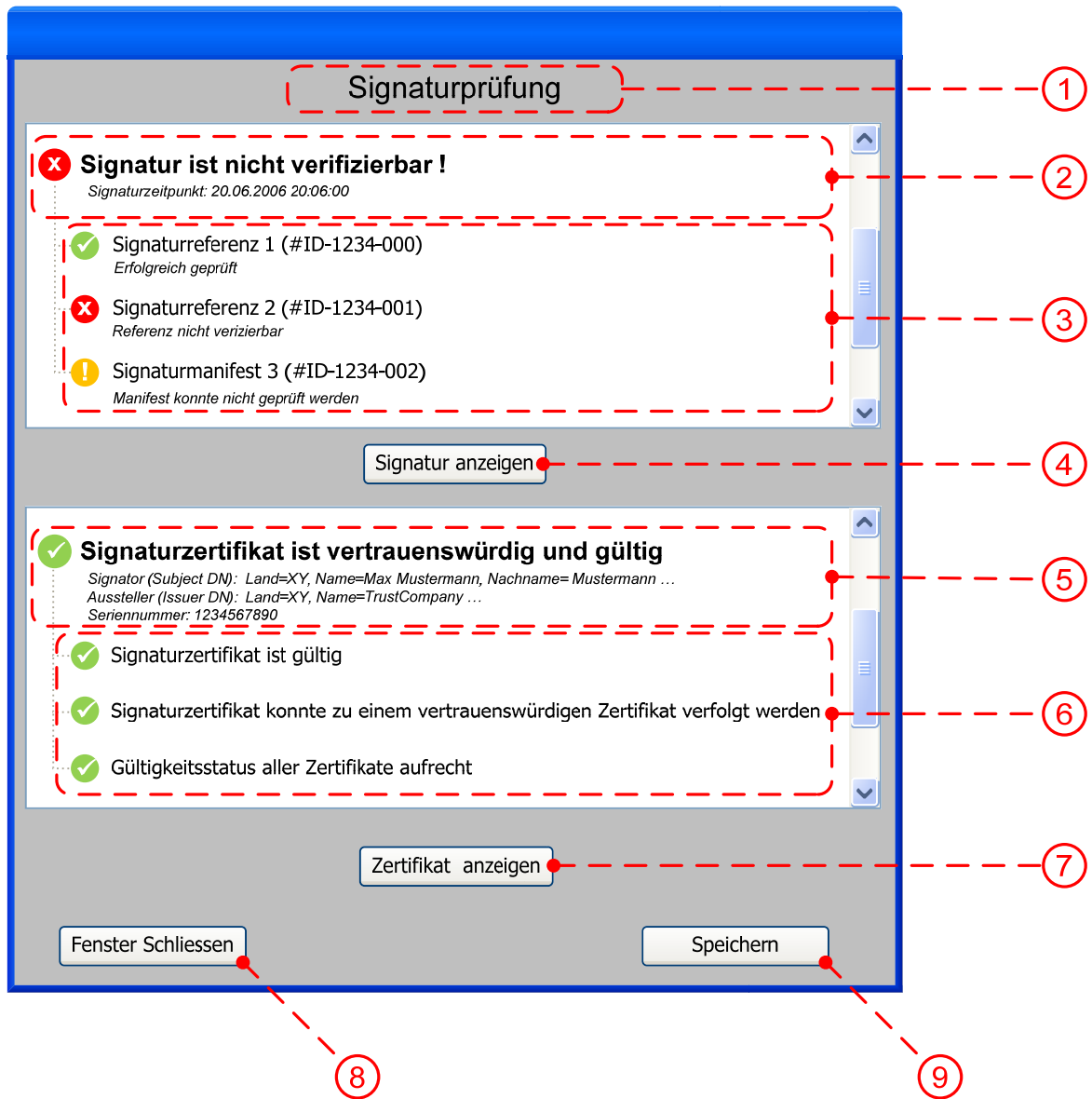
Die hier beschriebene UI-Struktur gilt sowohl für Signaturen nach XML-DSig als auch für die Signaturerstellung nach CMS.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.2, zu finden.

4.2.1 Anzeige verschiedener Signaturteile (Signaturreferenzen)




Elektronische Signaturen können mehrere einzelne, auch voneinander unabhängige Daten referenzieren. Die BKU muß daher die einzelnen Teile einer Signatur eindeutig ausweisen und prüfen, und wenn möglich das Resultat der kryptographischen Verifikation der einzelnen Teile gesondert anzeigen. Auf Wunsch des Anwenders muß es auch möglich sein, die signierten Daten jedes einzelnen Signaturteils/-referenz auszuwählen und anzeigen zu lassen.




Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Signaturprüfung“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Gesamtergebnis Signaturprüfung	Information / Interaktion	Zusammenfassender Status der kryptographischen Signaturprüfung. Als einfach interpretierbare Anzeige können entsprechende Symbole zur Repräsentation des Status verwendet werden. In dem hier

			<p>gezeigten Beispiel werden drei Status-Symbole exemplarisch verwendet:   </p> <p>Zusätzlich sollten dem Anwender durch Klicken auf ein Status-Symbol allfällige Hilfstexte gesondert angezeigt werden (z.B. via Popup).</p> <p>Hier sollen auch die Mindestinformation (lt. Spezifikation Bürgerkarte [2]) der geprüften Signatur dargestellt werden, wie beispielsweise der behauptete Signaturzeitpunkt, falls feststellbar.</p>
3	Detailergebnisse Signaturprüfung	Information / Interaktion	<p>Für jede gefundene Signaturreferenz/-teil muß ein eigener Statusbericht in den Detailergebnissen angeführt werden. Hier müssen auch Details zum einzelnen Prüfergebnis gegeben werden (bspw. direkt im Text wie im Beispiel angedeutet).</p> <p>Als einfach interpretierbare Anzeige können entsprechende Symbole zur Repräsentation des Status verwendet werden. In dem hier gezeigten Beispiel werden drei Status-Symbole exemplarisch verwendet:   </p> <p>Zusätzlich sollten dem Anwender durch Klicken auf ein Status-Symbol oder auf den Statustext selbst allfällige Hilfstexte bzw. weitere Informationen gesondert angezeigt werden (z.B. via Popup). Auch können durch entsprechende Interaktionsmechanismen – bspw. Schaltflächen, o.ä. – die durch die jeweilige Signaturreferenz/-teil signierten Daten zur Anzeige gebracht werden können (siehe dazu 4.2.2).</p>
4	Anzeigen der signierten Daten	Interaktion	<p>Bewirkt die Anzeige der signierten Daten. Hier müssen alle signierten Daten aus allen Signaturteilen/-referenzen angezeigt werden. Näheres dazu siehe 4.2.2.</p>
5	Gesamtergebnis Zertifikatsprüfung	Information	<p>Zusammenfassender Status der Prüfung des Signaturzertifikats.</p> <p>Als einfach interpretierbare Anzeige können entsprechende Symbole zur Repräsentation des Status verwendet werden. In dem hier gezeigten Beispiel werden drei Status-Symbole exemplarisch verwendet:   </p> <p>Zusätzlich sollten dem Anwender durch Klicken auf ein Status-Symbol allfällige Hilfstexte oder Details gesondert angezeigt werden (z.B. via Popup).</p>

			Hier sollen auch die Mindestinformation (lt. Spezifikation Bürgerkarte [2]) des geprüften Signaturzertifikats dargestellt werden, wie beispielsweise die Daten des Signators, des Zertifikatsausstellers und die Seriennummer des Zertifikats.
6	Detailergebnisse Zertifikatsprüfung	Information / Interaktion	<p>Die Zertifikatsprüfung erfolgt in mehreren Schritten. Zum einen wird die Gültigkeit des Zertifikats geprüft, weiters die Rückführbarkeit zu einem vertrauenswürdigen Wurzelzertifikat, und letztlich ob das Zertifikat widerrufen worden ist oder nicht. Für jede dieser Detailprüfungen soll das Prüfergebn gesondert angezeigt werden.</p> <p>Als einfach interpretierbare Anzeige können entsprechende Symbole zur Repräsentation des Prüfergebnisses verwendet werden. In dem hier gezeigten Beispiel werden drei Status-Symbole exemplarisch verwendet:   </p> <p>Zusätzlich sollten dem Anwender durch Klicken auf ein Status-Symbol oder auf den Statustext selbst allfällige Hilfstexte bzw. weitere Informationen gesondert angezeigt werden (z.B. via Popup).</p>
7	Anzeige des geprüften Signaturzertifikats	Interaktion	<p>Durch dieses Element wird das Signaturzertifikat selbst geöffnet und dargestellt.</p> <p>Zur Darstellung des Zertifikats selbst soll entweder direkt der durch das Betriebssystem des Anwenders zur Verfügung gestellte Zertifikats-Viewer herangezogen werden, oder aber eine dem entsprechende gängige Repräsentation gewählt werden, um den Anwender die Zertifikatsdaten in gewohnter Weise zu visualisieren.</p>
8	Fenster schließen	Interaktion	Mit diesem Element wird das Signaturprüffenster geschlossen und der Prüfprozess beendet.
9	Speichern	Interaktion	<p>Mit diesem Element wird das Prüfergebn und/oder die dargestellten signierten Daten gespeichert, wie lt. Spezifikation Bürgerkarte [2] gefordert.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI wird dem Hersteller der BKU überlassen.</p>

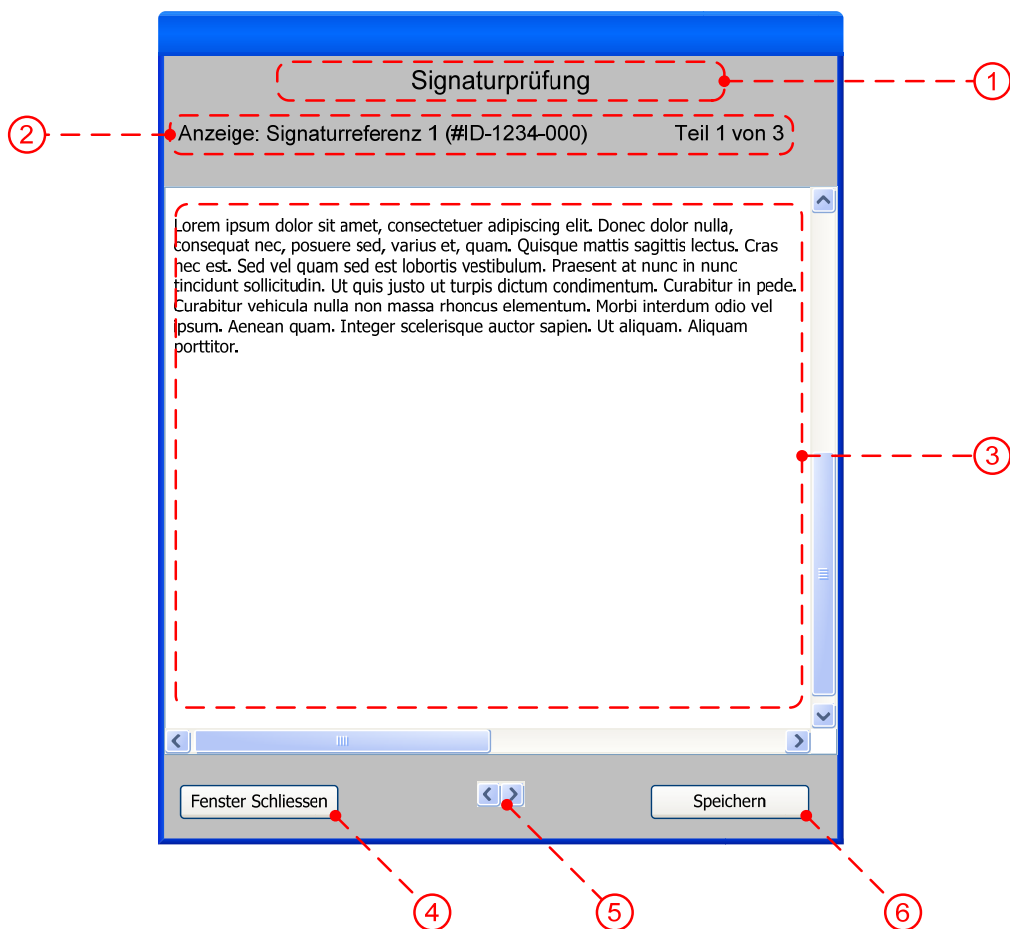
4.2.2 Anzeige der signierten Daten

Ähnlich wie im Signaturerstellungsprozeß muß auch im Zuge der Signaturverifikation dem Anwender die Möglichkeit geboten werden, die signierten Daten angezeigt zu bekommen.

Wie im vorherigen Abschnitt beschrieben, können elektronische Signaturen aus verschiedenen, auch unabhängigen, Signaturteilen bzw. –referenzen bestehen. Jeder Teil repräsentiert signierte Daten, die auch im Prüfprozeß angezeigt werden müssen. Somit muß jeder dieser Teile dem Anwender durch die in diesem Abschnitt skizzierte Anzeige dargestellt werden können, unter Berücksichtigung der in Abschnitt 3.2 aus [2] festgelegten Einschränkungen.

Die Darstellung wird dabei durch die in Abschnitt 4.2.1 dieses Dokuments definierte Prüfergebnisanzeige initiiert; die Anzeige erfolgt entweder für einen/eine ausgewählten Signaturteil/-referenz oder für alle Signaturteile gesamt. Der Anwender soll zudem in der hier beschriebenen Anzeige Komponente einfach zu den weiteren Signaturteilen – falls vorhanden – wechseln können.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Signaturprüfung“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.

2	Bezeichnung des angezeigten Signaturteils	Information	<p>Element zeigt die Kennung des/der aktuell in diesem Fenster angezeigten Signaturteils/-referenz an.</p> <p>Der Anwender muß daran die angezeigten Daten eindeutig dem/der zugehörigen Signaturteil/-referenz zuweisen können.</p> <p>Es soll auch angeführt werden, der wievielte Signaturteil von wie vielen insgesamt gerade angezeigt wird (z.B.: Teil 1 von 3).</p>
3	Anzeige der Signaturdaten	Information	Anzeige des signierten Textes des/der aktuell angezeigten Signaturteils/-referenz.
4	Fenster schließen	Interaktion	Mit diesem Element wird das Anzeigefenster geschlossen.
5	Navigation Signaturteile	Interaktion	<p>Der Anwender soll die Möglichkeit haben einfach durch die verschiedenen Signaturteile bzw. durch die signierten Daten zu navigieren, falls mehrere vorhanden sind.</p> <p>Mit derartigen Navigationselementen soll der Anwender einfach die Anzeige auf den nächsten, unmittelbar nachfolgenden Signaturteil umschalten können (analog der Reihenfolge wie in Überblicksdarstellung der Signaturteile/-referenzen in Abschnitt 4.2.1 festgelegt).</p>
6	Speichern	Interaktion	<p>Mit diesem Element werden die aktuell angezeigten signierten Daten des betreffenden Signaturteils lokal gespeichert, wie lt. Spezifikation Bürgerkarte [2] gefordert.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI wird dem Hersteller der BKU überlassen.</p>

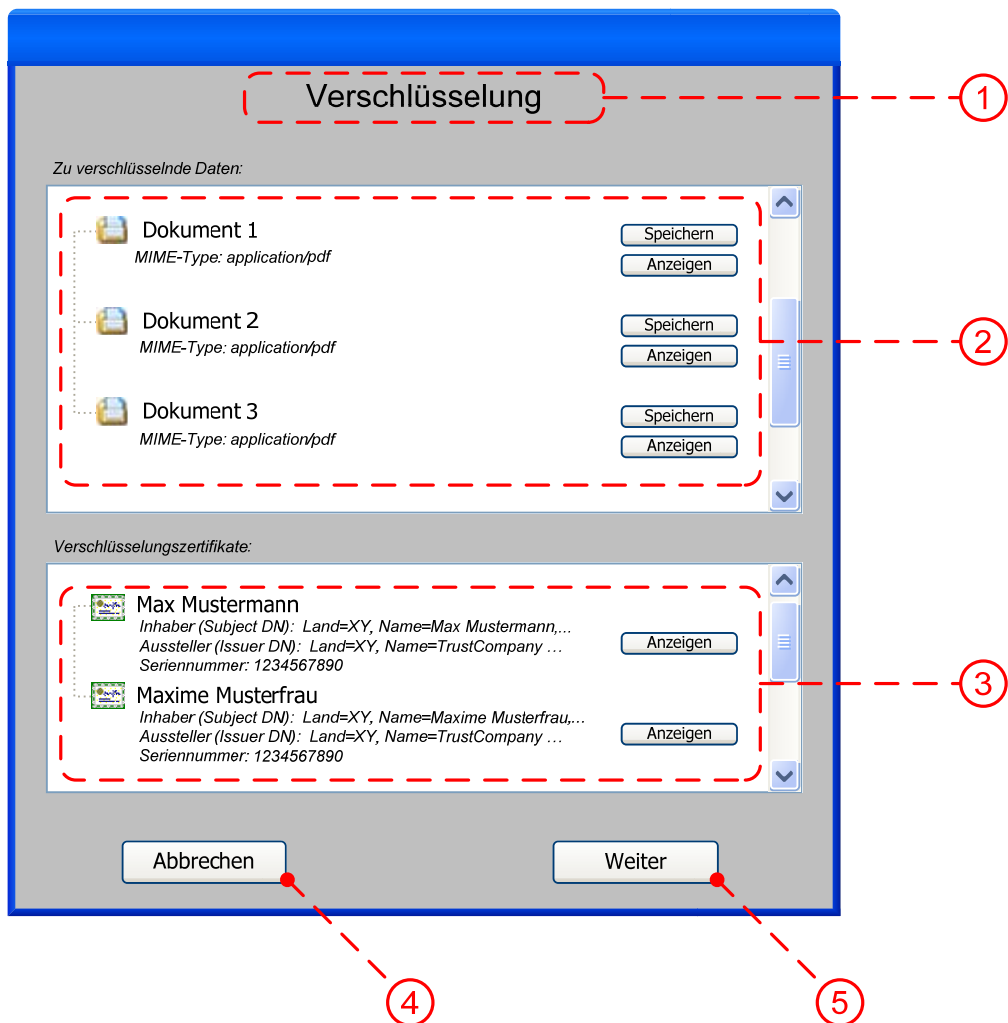
4.3 Verschlüsselung

Vor Verschlüsselung von Daten bzw. Dokumenten sind alle einzelnen zu verschlüsselnden Dokumente anzuzeigen und zur lokalen Speicherung anzubieten. Zudem müssen die Verschlüsselungszertifikate, mit denen die Daten letztendlich verschlüsselt werden, dem Anwender klar zur Kenntnis gebracht werden.

Die hier beschriebene UI-Struktur gilt sowohl für Verschlüsselung nach dem XML-Encryption-Standard [6] als auch für die Verschlüsselung nach CMS.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.3, zu finden.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Verschlüsselung“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Details der einzelnen zu verschlüsselnden Dokumententeile	Information / Interaktion	Für jedes zu verschlüsselnde (Teil-)Dokument sollen nach Möglichkeiten Meta-Daten, wie etwa MIME-Type, etc., angezeigt werden, sofern diese aus dem Verschlüsselungs-Request ableitbar sind. Zudem muß zu jedem (Teil-)Dokument die Möglichkeit der Anzeige gegeben sein (lt. Abschnitt 3.3 [2]). Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro (Teil-)Dokument

			<p>vorgesehen werden. Alternativ kann auch durch Klicken auf das gesamte Detail-Ergebnis die Darstellung erfolgen. Die Anzeige der Daten oder (Teil-) Dokumente erfolgt analog der Anzeige der signierten Daten im Zuge der Signaturprüfung (siehe Abschnitt 4.2.2); der Aktionstitel ist sinngemäß zu ersetzen.</p> <p>Gemäß Abschnitt 3.3 [2] muß auch die Möglichkeit der lokalen Speicherung der Daten bzw. (Teil-)Dokumente geboten werden. Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Eintrag vorgesehen werden.</p>
3	Details der einzelnen Verschlüsselungszertifikate	Information / Interaktion	<p>Jedes Verschlüsselungszertifikat, mit dem die in Element 2 dargestellten (Teil-) Dokumente verschlüsselt werden, muß angezeigt werden.</p> <p>Pro Verschlüsselungszertifikat sollen auch grundlegende Informationen, bspw. wie Inhaber (Subject), Aussteller (Issuer) oder Seriennummer, angeführt werden.</p> <p>Zudem muß für jedes Zertifikat die Möglichkeit einer Detail-Anzeige gegeben sein (lt. Abschnitt 3.4 [2]). Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Zertifikat vorgesehen werden. Alternativ kann auch durch Klicken auf das gesamte Detail-Element die Darstellung erfolgen.</p> <p>Zur Darstellung des Zertifikats selbst soll entweder direkt der durch das Betriebssystem des Anwenders zur Verfügung gestellte Zertifikats-Viewer herangezogen werden, oder aber eine dem entsprechende gängige Repräsentation gewählt werden, um den Anwender die Zertifikatsdaten in gewohnter Weise zu visualisieren.</p>
4	Abbrechen	Interaktion	<p>Mit diesem Element wird das Anzeigefenster geschlossen und der Vorgang abgebrochen.</p>
5	Weiter	Interaktion	<p>Mit diesem Element wird der Fortgang des Verschlüsselungsprozesses initiiert.</p>

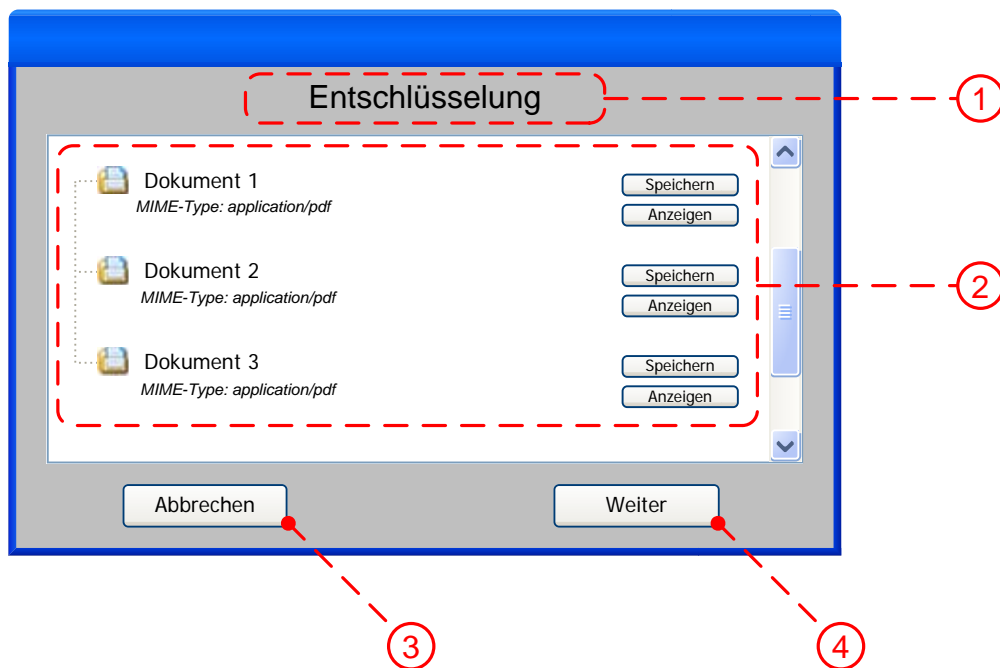
4.4 Entschlüsselung

Im Zuge der Entschlüsselung muß nach erfolgreicher Entschlüsselung ein Dialog zur Anzeige und lokalen Speicherung der entschlüsselten (Teil-)Dokumente gegeben sein (lt. 3.4 [2]).

Die hier beschriebene UI-Struktur gilt sowohl für Entschlüsselung nach dem XML-Encryption-Standard als auch für die Entschlüsselung nach CMS.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.4, zu finden.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Entschlüsselung“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Details der einzelnen entschlüsselten Dokumententeile	Information / Interaktion	Für jedes entschlüsselte (Teil-)Dokument sollen nach Möglichkeiten Meta-Daten, wie etwa MIME-Type, etc., angezeigt werden, sofern aus dem entschlüsselten Ergebnis ableitbar. Zudem muß zu jedem entschlüsselten (Teil-)Dokument die Möglichkeit der Detail-Anzeige gegeben sein (lt. Abschnitt 3.4 [2]).

Vereinheitlichung Bürgerkartenumgebung

			<p>Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Dokument vorgesehen werden. Alternativ kann auch durch Klicken auf das gesamte Detail-Ergebnis die Darstellung erfolgen. Die Anzeige der entschlüsselten Daten oder (Teil-)Dokumente erfolgt analog der Anzeige der signierten Daten im Zuge der Signaturprüfung (siehe Abschnitt 4.2.2); der Aktionstitel ist sinngemäß zu ersetzen.</p> <p>Gemäß Abschnitt 3.4 [2] muß auch die Möglichkeit der lokalen Speicherung der entschlüsselten Daten bzw. (Teil-)Dokumente geboten werden. Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Dokument vorgesehen werden.</p>
3	Abbrechen	Interaktion	Mit diesem Element wird das Anzeigefenster geschlossen und der Vorgang abgebrochen.
4	Weiter	Interaktion	Mit diesem Element wird der Fortgang des Entschlüsselungsprozesses initiiert.

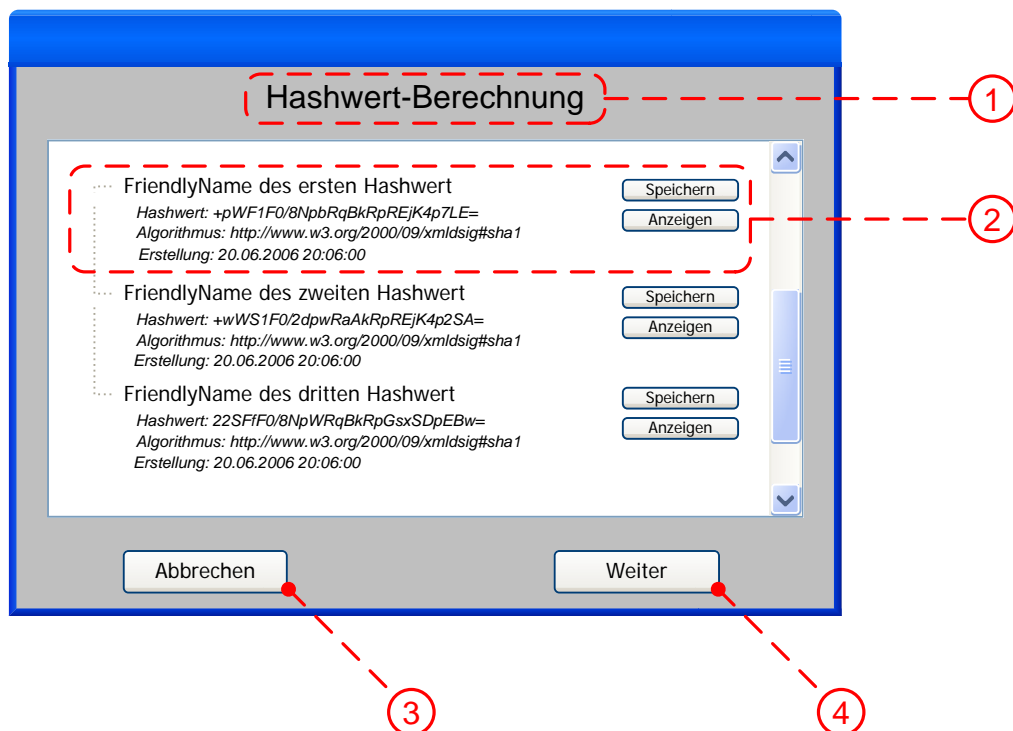
4.5 Hashwert Berechnung

Bevor eine Hashwert-Berechnung durchgeführt wird – sei es auf Basis eines entsprechenden Security-Layer-Requests oder per Menü initiiert – sind dem Anwender folgende Informationen anzuzeigen (lt. Abschnitt 3.5 aus [2]):

- den zur Hashwert-Berechnung verwendeten Algorithmus;
- den resultierenden Hashwert;
- den im Request angegebenen „Friendly Name“ für das zu hashende Dokument;
- eine Möglichkeit zur Anzeige sowie zur lokalen Speicherung des zu hashenden Dokuments.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.5, zu finden.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Hashwert-Berechnung“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Ergebnis der Hashwert-	Information /	Für jeden zu berechnenden Hashwert muß

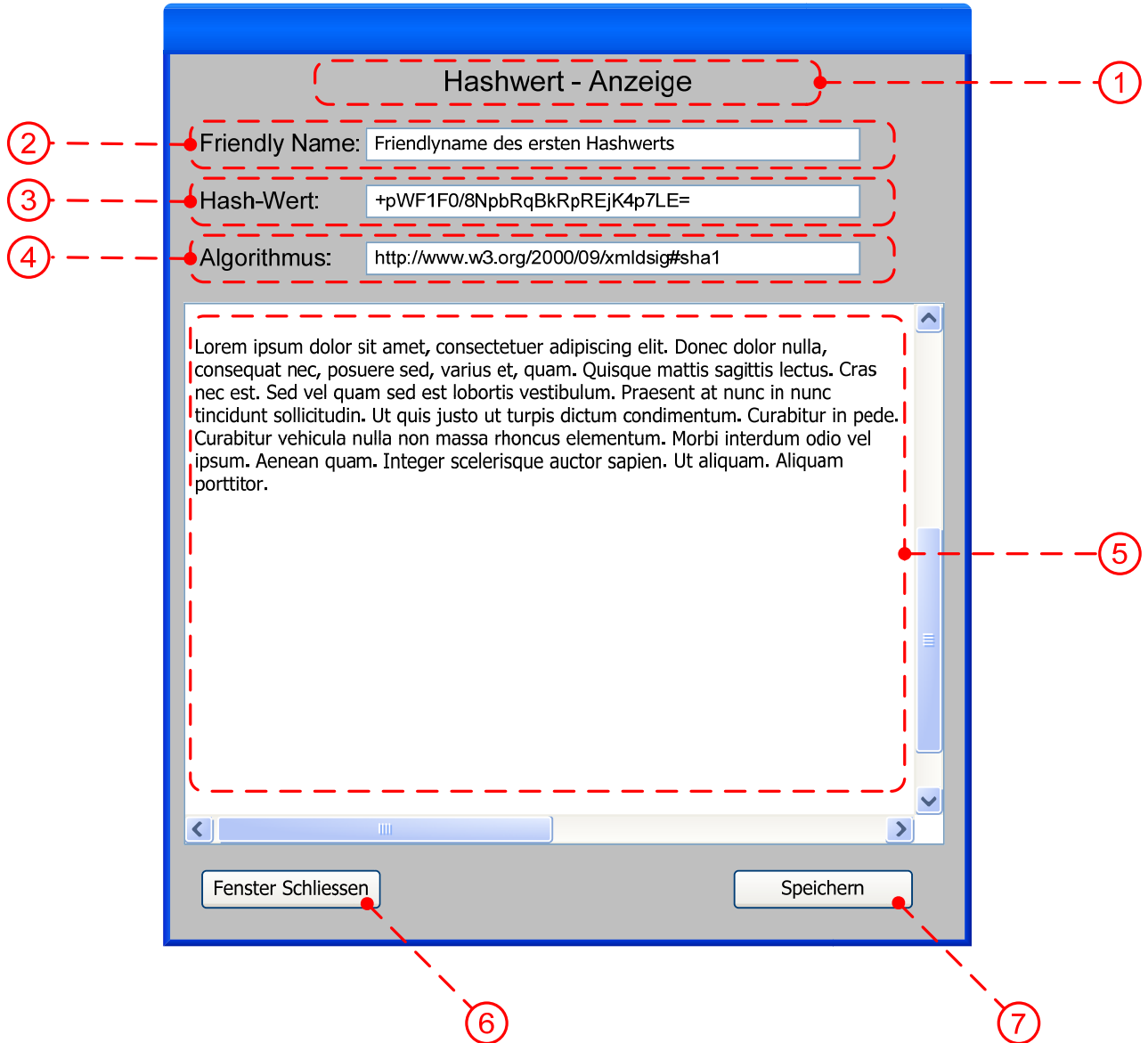
Vereinheitlichung Bürgerkartenumgebung

	Berechnung	Interaktion	<p>angezeigt werden:</p> <ul style="list-style-type: none"> - Friendly Name - berechneter Hashwert - verwendeter Algorithmus <p>Zudem muß zu jedem berechneten Hashwert die Möglichkeit der Anzeige der zur Berechnung herangezogenen Basisdaten gegeben sein (lt. Abschnitt 3.5 [2]). Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Dokument bzw. Detail-Element vorgesehen werden. Alternativ kann auch durch Klicken auf das Detail-Ergebnis die Darstellung der Basisdaten erfolgen. Für Details zur Anzeige der Basisdaten siehe Abschnitt 4.5.1.</p> <p>Gemäß Abschnitt 3.5 [2] muß auch die Möglichkeit der lokalen Speicherung der zu hashenden Daten geboten werden. Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Eintrag vorgesehen werden.</p>
3	Abbrechen	Interaktion	Mit diesem Element wird das Anzeigefenster geschlossen und der Vorgang der Hashwert-Berechnung abgebrochen.
4	Weiter	Interaktion	Mit diesem Element wird der Fortgang des Hashwert-Berechnungsprozesses initiiert.

4.5.1 Detailanzeige der Hashwert-Berechnung

Bei der Hashwert-Berechnung, aber auch in weiterer Folge im Zuge der Hashwert-Verifikation, sind die Basisdaten der Hashwert-Berechnung anzuzeigen, unter Beachtung der Einschränkungen bezgl. Anzeigbarkeit aus Abschnitt 3.5 [2].

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Hashwert-Anzeige“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.

2	Friendly Name	Information	Anzeige des im Request angegebenen „Friendly Name“ für das zu hashende Dokument.
3	Hashwert	Information	Anzeige des resultierenden Hashwerts.
4	Algorithmus	Information	Anzeige des zur Hashwert-Berechnung verwendeten Algorithmus.
5	Anzeige des zu hashenden Dokuments	Information	Anzeige des zu hashenden Dokuments.
6	Fenster schliessen	Interaktion	Mit diesem Element wird das Anzeigefenster geschlossen.
7	Speichern	Interaktion	Mit diesem Element werden die aktuell angezeigten zu hashenden Daten lokal gespeichert. Die Ausgestaltung des weiterführenden Dialogs/UI wird dem Hersteller der BKU überlassen.

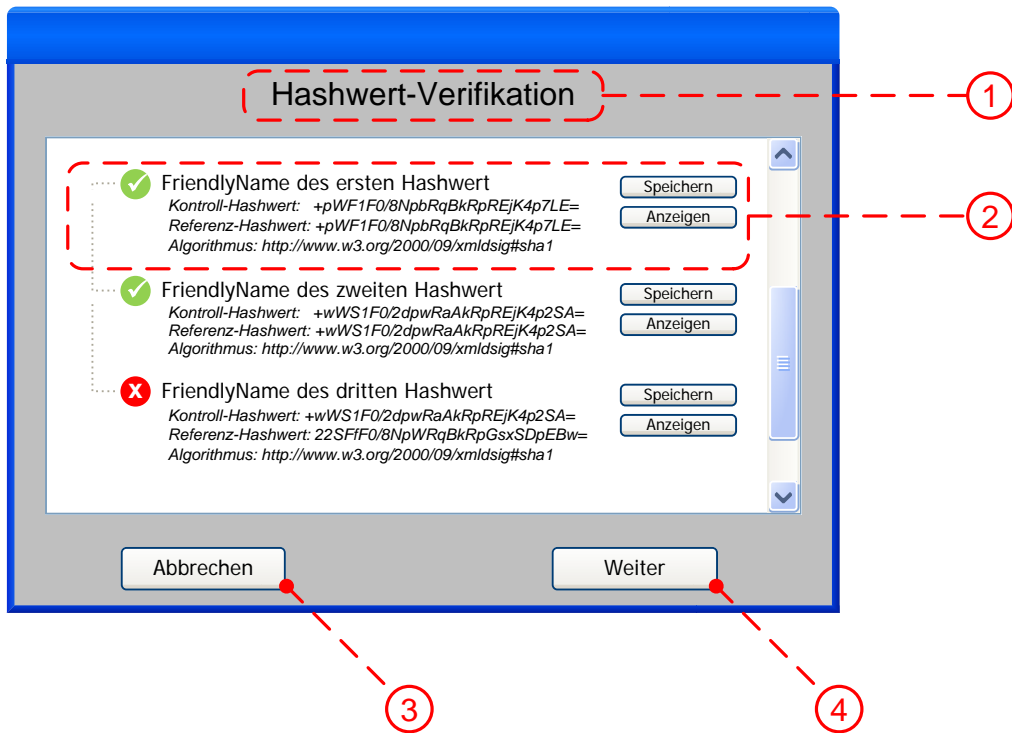
4.6 Hashwert Verifikation

Wird eine Hashwert-Verifikation durchgeführt wird – sei es auf Basis eines entsprechenden Security-Layer-Requests oder per Menü initiiert – sind dem Anwender folgende Informationen anzuzeigen (lt. Abschnitt 3.6 aus [2]):

- den zur Hashwert-Verifikation verwendeten Algorithmus;
- den Referenz-Hashwert aus der Befehlsanfrage;
- den berechneten Kontroll-Hashwert;
- das Ergebnis der Hashwert-Verifikation;
- den im Request angegebenen Friendly Name für das zu hashende Dokument;
- eine Möglichkeit zur Anzeige sowie zur lokalen Speicherung des zu hashenden Dokuments.

Grundlegende, normative Anforderungen zur Benutzerinteraktion sind im Dokument „Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte“ [2] der Bürgerkartenspezifikation, Abschnitt 3.6, zu finden.

Beispielhafte Grundstruktur:



Mindestinhalte/Begriffe:

Nr.	Feld	Interaktionstyp	Beschreibung / Funktion
1	Aktionsbezeichnung	Information	Bezeichnung der Aktion – zum Beispiel: „Hashwert-Verifikation“. In diesem Element können auch weitere, die Aktion näher beschreibende Hinweise angebracht werden.
2	Ergebnis der Hashwert-Verifikation	Information / Interaktion	Für jeden zu verifizierenden Hashwert muß angezeigt werden: <ul style="list-style-type: none"> - Friendly Name - berechneter Hashwert (Kontrollwert) - Referenz-Hashwert (aus Request) - verwendeter Algorithmus - Ergebnis der Hashwert-Verifikation bzw. des Vergleichs zwischen Referenz-Hashwert und Kontrollwert Als einfach interpretierbare Anzeige des Verifikationsergebnisses können entsprechende intuitive Symbole verwendet werden. In dem hier gezeigten Beispiel werden zwei Symbole exemplarisch verwendet: ✓✗

Vereinheitlichung Bürgerkartenumgebung

			<p>Es sollten dem Anwender durch Klicken auf diese Symbole allfällige Hilfstexte oder Details gesondert angezeigt werden (z.B. via Popup).</p> <p>Zudem muß zu jedem verifizierten Hashwert die Möglichkeit der Anzeige der zur Berechnung des Referenzwertes herangezogenen Basisdaten gegeben sein (lt. Abschnitt 3.6 [2]). Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Eintrag vorgesehen werden. Alternativ kann auch durch Klicken auf das gesamte Ergebnis die Darstellung der Basisdaten erfolgen. Für Details zur Anzeige der Basisdaten siehe Abschnitt 4.5.1.</p> <p>Gemäß Abschnitt 3.5 [2] muß auch die Möglichkeit der lokalen Speicherung der zur Berechnung des Kontrollwerts herangezogenen Basisdaten geboten werden. Dazu kann eine Schaltfläche oder ein adäquates anderes Interaktionselement pro Eintrag vorgesehen werden.</p>
3	Abbrechen	Interaktion	Mit diesem Element wird das Anzeigefenster geschlossen und der Vorgang der Hashwert-Verifikation abgebrochen.
4	Weiter	Interaktion	Mit diesem Element wird der Fortgang des Verifikationsprozesses initiiert.

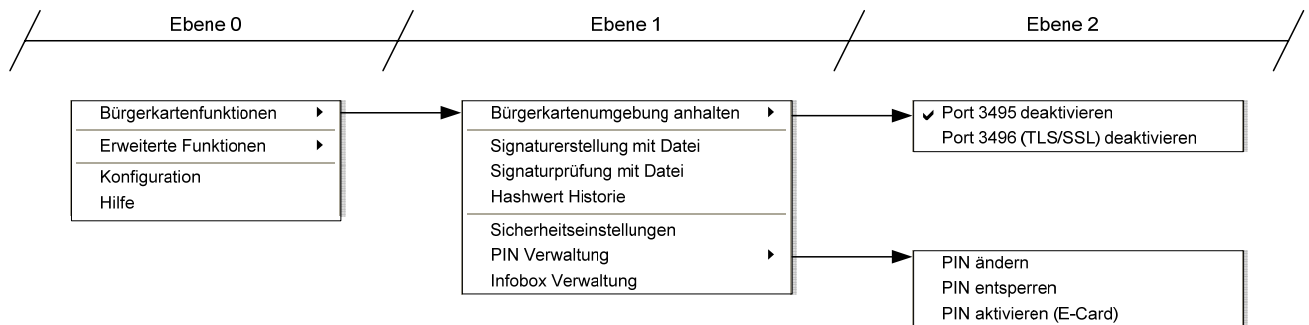
5 Menüführung

Bedient sich die BKU eines eigenen Menüs – bspw. erreichbar via Tray-Icon – so ist auch hier eine einheitliches Bild, zumindest für die Standardfunktionalitäten der Bürgerkartenumgebung, für den Anwender zu wünschen. Aus diesem Grund wird in diesem Abschnitt eine Menüstruktur definiert, die zumindest bezgl. Standard-Bürgerkartenfunktionen, wie Infobox- oder PIN-Management, von BKU-Herstellern umgesetzt werden muß.

Darüber hinaus werden für produktspezifische Variationen und Funktionen in der Menüstruktur Raum gelassen. Lediglich die Standard-Bürgerkartenfunktionen sollen in jeder BKU gleich bedient werden können.

Die hier gezeigte Menüstruktur gliedert sich in drei Ebenen – Ebene 0 bis Ebene 2. Dabei stellt Ebene 0 den Einstiegspunkt dar. In den nachfolgenden Abschnitten werden die einzelnen Menü-Ebenen detailliert beschrieben:

Menüstruktur:



5.1 Menüeinträge des Einstiegsmenüs – Ebene 0:

Erweiterungen des hier skizzierten Einstiegsmenüs sollen nicht vorgenommen werden.

Ebene	Menüeintrag	erforderlich / optional / empfohlen	Beschreibung / Funktion
0	Bürgerkartenfunktionen	erforderlich	Dieser Eintrag führt den Anwender zu einem Sub-Menü der Standard-Bürgerkartenfunktionalitäten. Details des Sub-Menüs – siehe 5.2.
0	Erweiterte Funktionen	optional	Dieser Menüeintrag führt den Anwender zu zusätzlichen, ggf. herstellerspezifischen Funktionen der BKU. Hier kann der Hersteller eigene Funktionen als Erweiterung zu den Standardfunktionalitäten vorsehen.

			Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen.
0	Konfiguration	erforderlich	Dieser Menüeintrag führt zu den Konfigurationsmöglichkeiten der BKU. Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen.
0	Hilfe	erforderlich	Hier kann der Anwender Hilfestellungen, Beschreibungen, Anwenderhandbücher, etc. abrufen. Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen.

5.2 Menüeinträge zu ‚Bürgerkartenfunktionalitäten‘ – Ebene 1:

Erweiterungen des Menüs ‚Bürgerkartenfunktionalitäten‘ dürfen nicht vorgenommen werden.

Ebene	Menüeintrag	erforderlich / optional / empfohlen	Beschreibung / Funktion
1	Bürgerkarten- umgebung anhalten	erforderlich	Dieses Element ermöglicht die Deaktivierung BKU. In einem weiteren Sub-Menü sollen die einzelnen, von der jeweiligen BKU implementierten Bindungen – zum Beispiel TCP/HTTP via Port 3495 oder TLS/HTTPS via Port 3496 – unabhängig voneinander deaktiviert werden können. Details des Sub-Menüs – siehe 5.3.
1	Signaturerstellung mit Datei	optional	Dieser Menüantrag ermöglicht die Erstellung von Signaturen – nach XML-DSig oder CMS – auf Basis der in einer Datei übergebenen Daten. Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem

			<p>Hersteller der BKU überlassen.</p> <p>Beispielhaft könnte in einem nachfolgenden Dialog der Anwender zur Auswahl einer Datei aufgefordert werden, die letztlich die zu signierenden Daten enthält. In einem weiteren Schritt ist der Typ der Signatur zu entscheiden, d.h. entweder Signatur nach XML-DSig oder nach CMS.</p> <p>Der Prozeß und auch der Dialog zur Signaturerstellung selbst muß alle bezgl. Signaturerstellung getroffenen Anforderungen erfüllen. Hier ist besonders die Darstellung des zu signierenden Inhalts zu beachten – siehe Abschnitt 4.1.</p>
1	Signaturprüfung mit Datei	optional	<p>Dieser Menüantrag ermöglicht die Prüfung einer Signatur – nach XML-DSig oder CMS – auf Basis der in einer Datei übergebenen Daten.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen.</p> <p>Beispielhaft könnte in einem nachfolgenden Dialog der Anwender zur Auswahl einer Datei aufgefordert werden, die letztlich die zu prüfende Signatur enthält. In weiterer Folge wird die Signaturprüfung eingeleitet.</p> <p>Der Signaturprüfprozeß und auch der Dialog zur Anzeige des Prüfergebnisses selbst muß alle bezgl. Signaturprüfung getroffenen Anforderungen erfüllen. Hier muß besonders die Darstellung und die Anzeige des Prüfergebnisses nach den Vorgaben aus Abschnitt 4.2 erfolgen.</p>
1	Hashwert Historie	erforderlich	<p>Mit diesem Eintrag wird die Hashwert-Historie – wie in Abschnitt 3.5 in [2] definiert – zur Anzeige gebracht.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI bleibt dem Hersteller der BKU überlassen.</p>
1	Sicherheits-einstellungen	erforderlich	<p>Mit diesem Eintrag wird der Anwender zu sicherheitsrelevanten Einstellungen geführt. Hier sollen in weiteren Sub-Menüs oder Dialogen bspw. folgende Einstellungen möglich sein:</p> <ul style="list-style-type: none"> - Zertifikatsmanagement (vertrauenswürdige Zertifikate, etc.)

Vereinheitlichung Bürgerkartenumgebung

			<ul style="list-style-type: none"> - Widerrufsmanagement (evt. Caching-Mechanismen, etc.) - Konfiguration des Zugriffsschutz - etc. <p>Die Ausgestaltung des weiterführenden Dialogs/UI, bleibt dem Hersteller der BKU überlassen, und hängt ganz von der technischen Umsetzung der BKU ab.</p>
1	PIN Verwaltung	erforderlich	<p>Mit diesem Eintrag gelangt der Anwender zu einem weiteren Sub-Menü, durch das die PIN-Codes verwaltet werden.</p> <p>Details des Sub-Menüs – siehe 5.4.</p>
1	Infobox-Verwaltung	erforderlich	<p>Dieser Eintrag führt den Anwender zur Infobox-Verwaltung. Hier muß dem Anwender die Möglichkeit gegeben werden, die Inhalte der Infoboxen seiner Bürgerkarte – sowohl Software-Infoboxen als auch physisch in der ‚Bürgerkarte‘ gespeicherte Infoboxen – zu administrieren, d.h. diese einzusehen, deren Inhalte ggf. extern abzuspeichern (je nach Typ von Infobox bzw. je nach Inhalt zulässig), etc.</p> <p>Auch soll der Anwender im Rahmen der Infobox-Verwaltung neue Infoboxen anlegen bzw. existierende Infoboxen löschen können. Das Schützen vor Zugriffen – sowohl lesend als auch schreibend – von Infoboxen soll möglich sein.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen.</p> <p>Auch bleibt die Funktionsvielfalt dem Hersteller überlassen, sofern diese im Einklang mit der Spezifikation der Bürgerkarte [3] steht.</p>

5.3 Menüeinträge zu ‚Bürgerkartenumgebung anhalten‘ – Ebene 2:

Sollte die BKU weitere Transportbindungen zur Verfügung stellen, so soll für jede Bindung ein weiterer Menüeintrag zur Deaktivierung vorgesehen werden, wie hier skizziert.

Ebene	Menüeintrag	erforderlich / optional / empfohlen	Beschreibung / Funktion
2	Port XXXX deaktivieren	optional	Deaktiviert die Standard-Bindung der BKU. Deaktiviert die BKU am angegebenen Port XXXX, zum Beispiel 3495, Security-Layer-Requests zu empfangen. Anstelle von XXXX soll die in der Grundeinstellung der BKU für diese Art der Transport-Bindung konfigurierte Port-Nummer angegeben werden.
2	Port XXXX (TLS/SSL) deaktivieren	optional	Deaktiviert die SSL/TLS-gesicherte Bindung der BKU. Deaktiviert die BKU am angegebenen Port XXXX, zum Beispiel 3496, Security-Layer-Requests zu empfangen. Anstelle von XXXX soll die in der Grundeinstellung der BKU für diese Art der Transport-Bindung (TLS/SSL) konfigurierte Port-Nummer angegeben werden.

5.4 Menüeinträge zu ‚PIN Verwaltung‘ – Ebene 2:

Erweiterungen des Menüs ‚PIN Verwaltung‘ sollen nicht vorgenommen werden.

Ebene	Menüeintrag	erforderlich / optional / empfohlen	Beschreibung / Funktion
2	PIN ändern	erforderlich	Eintrag öffnet Dialog zum Ändern von PIN-Codes. Je nach verwendetem Signaturerstellungsgerät (Signaturkarte) bzw. je nach dessen Ausprägung können verschiedene PIN-Codes geändert werden. Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen. Auch sind Abhängigkeiten je nach verwendetem

Vereinheitlichung Bürgerkartenumgebung

			Kartenlesegerät – mit oder ohne PIN-Pad – und je nach verwendetem Signaturerstellungsgerät (Signaturkarte) gegeben und zu beachten.
2	PIN entsperren	erforderlich	<p>Eintrag öffnet Dialog zum Entsperren von PIN-Codes mittels PUK. Je nach verwendetem Signaturerstellungsgerät (Signaturkarte) bzw. je nach dessen Ausprägung können einzelne PIN-Codes entsperrenbar sein.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen. Auch sind Abhängigkeiten je nach verwendetem Kartenlesegerät– mit oder ohne PIN-Pad – und je nach verwendetem Signaturerstellungsgerät (Signaturkarte) gegeben und zu beachten.</p>
2	PIN aktivieren (E-Card)	optional	<p>Unterstützt die BKU auch die Aktivierung der E-Card, so muß diese Funktionalität unter diesem Menüpunkt angeboten werden.</p> <p>Die Ausgestaltung des weiterführenden Dialogs/UI, d.h. ob der Anwender über Dialoge, Assistenten oder weitere Sub-Menüs weitergeführt wird, bleibt dem Hersteller der BKU überlassen. Auch sind Abhängigkeiten je nach verwendetem Kartenlesegerät– mit oder ohne PIN-Pad – und je nach verwendetem Signaturerstellungsgerät (Signaturkarte) gegeben und zu beachten.</p>

Referenzen

- [1] S. Bradner: RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. IETF Request For Comment, März 1997. Abgerufen aus dem World Wide Web am 14. 05. 2004 unter <http://www.ietf.org/rfc/rfc2119.txt>.
- [2] A. Hollosi, G. Karlinger: Anforderungen an die Benutzer-Schnittstelle zur Bürgerkarten-Umgebung der österreichischen Bürgerkarte. Version 1.2.0. vom 14. Mai 2005. Abgerufen aus dem World Wide Web am 01.03.2006 unter <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/userinterface/UserInterface.html>
- [3] A. Hollosi, G. Karlinger: Die österreichische Bürgerkarte, Version 1.2.1 vom 14. Mai 2005. Abgerufen aus dem World Wide Web am 01.03.2006 unter <http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/>
- [4] Eastlake, Donald, Reagle, Joseph und Solo, David: XML-Signature Syntax and Processing. W3C Recommendation, Februar 2002. Abgerufen aus dem World Wide Web am 14. 05. 2004 unter <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>
- [5] Hously, R.: RFC 3369: Cryptographic Message Syntax (CMS). IETF Request For Comment, August 2002. Abgerufen aus dem World Wide Web am 14. 05. 2004 unter <http://www.ietf.org/rfc/rfc3369.txt>
- [6] Eastlake, Donald und Reagle, Joseph: XML Encryption Syntax and Processing. W3C Recommendation, Dezember 2002. Abgerufen aus dem World Wide Web am 14. 05. 2004 unter <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>