




**Auswahl von
Bürgerkartenumgebungen
2003-04-08**

Konvention

bkuwahl – 1.0.0

Entwurf öffentlich

Bezeichnung	Auswahl von Bürgerkartenumgebungen
Kurzbezeichnung	BKU Auswahl
Version	1.0.0
Datum	2003-04-08
Dokumentenklasse	Konvention
Dokumentenstadium	Entwurf öffentlich
Kurzbeschreibung	Die Bürgerkartenumgebung (BKU) hat die Rolle eines Mittlers zwischen der technologieneutralen Schnittstelle Security-Layer und der spezifisch verwendeten Technologie der Bürgerkarte. Im Falle von öffentlichen Terminals, die nach Möglichkeit alle am Markt befindlichen Bürgerkarten unterstützen können sollen, wird es erforderlich sein verschiedene BKUs zu unterstützen, um damit verschiedene Ausprägungen der Bürgerkarte servicieren zu können. Um diesen Vorgang zu ermöglichen ist es erforderlich, dass Applikationen die Auswahl einer BKU erlauben.
Autor	Arno Hollosi, arno.hollosi@cio.gv.at
Arbeitsgruppe	 Stabsstelle IKT-Strategie des Bundes Operative Unit – Technik

Inhalt

1	Einleitung.....	2
2	Grundlagen zur HTTP-Bindung.....	3
2	Technische und organisatorische Rahmenbedingungen.....	3
3	Zentraler Auswahldienst.....	3
4.1	Vollständige HTML-Auswahl.....	4
4.1.1	Beispiel.....	4
4.2	HTML-Code für Auswahl.....	4
4.2.1	Beispiel.....	4
4.3	XML-Daten für Auswahl.....	5
4.3.1	Schema für XML-Daten.....	5
4.3.2	Beispiel für XML Daten.....	6
5	Anbieter eines zentralen Auswahldienstes.....	6

1 Einleitung

Das Bürgerkartenkonzept ist technologieneutral und von der eingesetzten Technologie und der speziellen Ausprägung der Bürgerkarte unabhängig. Dabei kommt der Bürgerkartenumgebung die Rolle des Mittlers zwischen der technologieneutralen Schnittstelle Security-Layer und der spezifisch verwendeten Technologie der Bürgerkarte zu. Im Falle von öffentlichen Terminals, die nach Möglichkeit alle am Markt befindlichen Bürgerkarten unterstützen können sollen, wird es erforderlich sein verschiedene Bürgerkartenumgebungen zu unterstützen, um damit verschiedene Ausprägungen der Bürgerkarte servieren zu können. Um diesen Vorgang zu ermöglichen ist es aus technischer Sicht erforderlich, dass Applikationen die Auswahl einer Bürgerkartenumgebung erlauben.

Im Folgenden werden technische und organisatorische Empfehlungen beschrieben, die Applikationsentwickler beim Design von Applikationen berücksichtigen sollen, um den gleichzeitigen Betrieb mehrerer Bürgerkartenumgebungen zu ermöglichen. Es wird dabei besonders auf die HTTP bzw. HTTPS-Bindung des Security-Layers eingegangen. Bei der TCP bzw. TLS-Bindung, die direkt von Programmen angesteuert wird, genügt es, die Lokation der Security-Layer Schnittstelle als durch vom User steuerbaren Parameter im Programm zu berücksichtigen (bzw. kann auf die XML-Variante zurückgegriffen werden – siehe 4.1.2 unten).

2 Grundlagen und Rahmenbedingungen

In den Spezifikationen zum Konzept Bürgerkarte wird in der Regel davon ausgegangen, dass sich die Bürgerkartenumgebung an einer vordefinierten Lokation befindet. So definiert z.B. die Security-Layer Spezifikation Version 1.1 den Default-Port der Verbindung als localhost:3495.

Aus Applikationssicht verhält sich die Security-Layer Schnittstelle wie ein regulärer Webserver. Die möglichen Parameter des Security-Layer Requests Stylesheet-URI, Redirect-URI und Data-URI spezifizieren dabei externe Daten bzw. Dienste. Die Verbindung zu diesen URIs findet nicht über den Browser statt, sondern über die Bürgerkartenumgebung. D.h. für diese Daten oder Dienste ist es (und muss es) irrelevant sein, von wo sie abgerufen bzw. in Anspruch genommen werden. Diese Parameter werden deshalb nicht näher berücksichtigt.

Wenn die Applikation die Bürgerkarte verwenden will, setzt sie eine entsprechende Anfrage (Security-Layer Request) ab. Zu diesem Zeitpunkt muss die URI des Security-Layers bekannt sein, die Default-URI ist `http://localhost:3495/http-security-layer-request`. Wenn also eine nicht lokale Bürgerkartenumgebung zum Einsatz kommt, muss die Applikation von der geänderten URI Kenntnis haben.

3 Technische und organisatorische Rahmenbedingungen

Die Verwendung alternativer (nicht lokaler) Bürgerkartenumgebungen muss auf allen gängigen Webbrowsern ohne Verwendung aktiver Komponenten möglich sein. Damit bleibt als einzige Möglichkeit, dass die Applikation **selbst** in geeigneter Weise eine Auswahl bzw. Abfrage der URI der verwendeten Bürgerkartenumgebung (BKU) anbietet.

Aus organisatorischer Sicht ist zu berücksichtigen, dass einerseits die Wartung der Auswahlliste für BKUs bei den (erwartet vielen) Applikationen automatisiert möglich ist, zum Beispiel im Falle des Auftretens eines neuen Anbieters bzw. der Änderung von Daten bestehender BKUs. Andererseits soll die Applikation die Hoheit über Aussehen und Benutzerführung bezüglich dieser Auswahlliste behalten können.

4 Zentraler Auswahldienst

Aus den Rahmenbedingungen und Anforderungen bietet sich die Lösung eines zentralen Auswahldienstes an, der folgende drei Varianten anbietet:

- Vollständige HTML-Auswahl
- HTML-Code für Auswahl
- XML-Daten für Auswahl

Obwohl von einem zentralen Auswahldienst die Rede ist, können verschiedene solcher Dienste existieren. Es wird aber wohl die Anzahl dieser Dienste wesentlich geringer sein, als die Anzahl der Applikationen, die Bürgerkarten einsetzen.

4.1 Vollständige HTML-Auswahl

Die vollständige HTML-Auswahl erlaubt es Applikationsentwicklern, eine vorgefertigte Auswahl zu verwenden und damit schnell und einfach auf einen Auswahlmechanismus zurückgreifen zu können. Der Nachteil ist, dass die Auswahl im Design in der Regel nicht dem Applikationsdesign entspricht.

Dabei wird wie folgt vorgegangen:

1. Die Applikation lenkt den Benutzer auf die Auswahl-URI des zentralen Dienstes. Die URI enthält als Parameter im GET-Request „*returnURI*“, die die URI jener Applikationsseite enthält, die nach der Auswahl aufgerufen werden soll.
2. Es wird eine entsprechende Auswahl mit Hilfetexten etc. vom zentralen Auswahldienst angezeigt
3. BenutzerIn wählt eine Bürgerkartenumgebung aus
4. Der Auswahldienst lenkt den Benutzer zurück auf die in „*returnURI*“ spezifizierte Seite. Der Applikation wird als query-part der *returnURI* der Parameter „*bkuURI*“, der die URI der HTTP bzw. HTTPS Bindung enthält, zurückgeliefert.

4.1.1 Beispiel

- Applikation lenkt BenutzerIn auf:
https://auswahl.buergerkarte.at/auswahl?returnURI=https://applikation.gv.at/seite3
- Nach Auswahl von z.B. Provider1 lenkt der Auswahldienst BenutzerIn auf
https://applikation.gv.at/seite3?bkuURI=https://bku.provider1.at:3496/https-security-layer-request

4.2 HTML-Code für Auswahl

Bei der Variante „HTML-Code für Auswahl“ wird ein Stück HTML-Code zur Verfügung gestellt, das in die Applikationsseiten eingebunden werden kann. Der HTML-Code umfasst die HTML Elemente in Form eines `<SELECT>` Eingabefeldes. Der HTML-Code umfasst dabei **nicht** das notwendige umschließende `<FORM>`-Element. Dieser muss von der Applikation selbst beigesteuert werden. Die Eingabevariable hat den Namen „*bkuURI*“ und liefert eine vollständige URI zurück. Der HTML-Code ist XHTML bzw. HTML 4.1 konform.

4.2.1 Beispiel

```
<select name="bkuURI">
  <option value="http://localhost:3495/http-security-layer-
request">Lokale B&uuml;rgerkarte</option>
  <option value="https://provider1.at:3496/https-security-layer-
request">Provider Eins</option>
  <option value="https://provider2.at:3496/https-security-layer-
request">Provider Zwei</option>
</select>
```

4.3 XML-Daten für Auswahl

Benötigen Applikationen noch mehr Flexibilität, werden die Daten der Anbieter auch in einem strukturierten XML-File angeboten. Im XML finden sich neben den URIs der Bürgerkartenumgebungen zusätzlich noch weiterführende Informationen zum Anbieter selbst.

4.3.1 Schema für XML-Daten

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="CitizenCardEnvironments">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="CitizenCardEnvironment"
          maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="CitizenCardEnvironment">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="ProviderDetails"/>
        <xs:element ref="Binding" maxOccurs="4"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ProviderDetails">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Name" type="xs:string"/>
        <xs:element name="Image">
          <xs:complexType>
            <xs:simpleContent>
              <xs:extension base="xs:anyURI">
                <xs:attribute name="width"
                  type="xs:positiveInteger"
                  use="required"/>
                <xs:attribute name="height"
                  type="xs:positiveInteger"
                  use="required"/>
              </xs:extension>
            </xs:simpleContent>
          </xs:complexType>
        </xs:element>
        <xs:element name="HomepageURI" type="xs:anyURI"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="Binding">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Type">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="TCP/IP"/>
              <xs:enumeration value="TLS"/>
              <xs:enumeration value="HTTP"/>
              <xs:enumeration value="HTTPS"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="SelectionText" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

```

        <xs:choice>
          <xs:element name="URI" type="xs:anyURI"/>
          <xs:sequence>
            <xs:element name="Host" type="xs:token"/>
            <xs:element name="Port" type="xs:positiveInteger"/>
          </xs:sequence>
        </xs:choice>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

4.3.2 Beispiel für XML Daten

```

<?xml version="1.0" encoding="UTF-8"?>
<CitizenCardEnvironments>
  <CitizenCardEnvironment>
    <ProviderDetails>
      <Name>Provider Eins Ges.m.b.H.</Name>
      <Image width="40" height="40">
        http://provider1.at/logo.jpg
      </Image>
      <HomepageURI>http://provider1.at/</HomepageURI>
    </ProviderDetails>
    <Binding>
      <Type>TCP/IP</Type>
      <SelectionText>Provider 1</SelectionText>
      <Host>localhost</Host>
      <Port>3495</Port>
    </Binding>
    <Binding>
      <Type>HTTP</Type>
      <SelectionText>Provider 1</SelectionText>
      <URI>http://localhost:3495/http-security-layer-request</URI>
    </Binding>
  </CitizenCardEnvironment>
  <CitizenCardEnvironment>
    <ProviderDetails>
      <Name>Provider Zwei AG</Name>
      <Image width="40" height="40">
        http://provider2.at/images/logo/small.png
      </Image>
      <HomepageURI>http://provider2.at/</HomepageURI>
    </ProviderDetails>
    <Binding>
      <Type>TLS</Type>
      <SelectionText>Provider 2</SelectionText>
      <Host>bku.provider2.at</Host>
      <Port>3496</Port>
    </Binding>
    <Binding>
      <Type>HTTPS</Type>
      <SelectionText>Provider 2</SelectionText>
      <URI>
        https://bku.provider2.at:3496/https-security-layer-request
      </URI>
    </Binding>
  </CitizenCardEnvironment>
</CitizenCardEnvironments>

```

5 Anbieter eines zentralen Auswahldienstes

Wie bereits erwähnt können verschiedene Betreiber einen solchen zentralen Auswahldienst anbieten. Jedenfalls wird ein solcher Dienst unter der Domain **auswahl.buergerkarte.at** angeboten.

Die URIs der verschiedenen Varianten sind:

- Vollständige HTML-Auswahl
 - *<https://auswahl.buergerkarte.at/auswahl>*
 - *<http://auswahl.buergerkarte.at/auswahl>*
- HTML-Code für Auswahl
 - *<https://auswahl.buergerkarte.at/htmlcode>*
 - *<http://auswahl.buergerkarte.at/htmlcode>*
- XML-Daten für Auswahl
 - *<https://auswahl.buergerkarte.at/xmldata>*
 - *<http://auswahl.buergerkarte.at/xmldata>*

Wo immer möglich sollte die HTTPS Variante der HTTP Variante vorgezogen werden.