

Usability-Evaluierung der österreichischen Handy-Signatur

Thomas Zefferer · Vesna Krnjic

IAIK – Technische Universität Graz

{thomas.zefferer | vesna.krnjic}@iaik.tugraz.at

Zusammenfassung

Sicherheit ist eine zentrale Anforderung vieler E-Government-Lösungen. Das nötige Maß an Sicherheit wird dabei in der Regel durch den Einsatz von Chipkarten, die an Bürgerinnen und Bürger ausgegeben werden, erfüllt. Diese weisen jedoch eine Reihe von Nachteilen in Bezug auf Benutzerfreundlichkeit auf. Vor allem die Notwendigkeit eines Chipkartenlesegeräts stellte sich in der Vergangenheit oft als Problem heraus. In Österreich wurde aus diesem Grund vor einigen Jahren die Handy-Signatur entwickelt, die eine Alternative zu chipkartenbasierten Ansätzen darstellt. Die Handy-Signatur erlaubt österreichischen Bürgerinnen und Bürgern eine sichere Authentifizierung an E-Government-Anwendungen und die Erstellung qualifizierter elektronischer Signaturen.

Eine Erhöhung der Benutzerfreundlichkeit und in weiterer Folge eine Steigerung der Akzeptanz österreichischer E-Government-Lösungen war ein zentrales Motiv für die Entwicklung der Handy-Signatur. Im Rahmen einer Usability-Studie wurde überprüft, ob dieses Ziel erreicht werden konnte. Zwanzig Testpersonen wurden dazu gebeten, einige typische Abläufe sowohl mit der Handy-Signatur, als auch mit chipkartenbasierten Lösungen durchzuführen. Die erhaltenen Ergebnisse zeigen, dass die Handy-Signatur in Bezug auf Benutzerfreundlichkeit und Akzeptanz chipkartenbasierten Ansätzen durchwegs überlegen ist und von einem Großteil der Testpersonen positiv bewertet wurde. Die durchgeführte Usability-Analyse zeigte damit, dass die österreichische Handy-Signatur sowohl gegebene Sicherheitsanforderungen erfüllt, als auch ein entsprechendes Maß an Benutzerfreundlichkeit und Akzeptanz gewährleistet.

1 Einleitung

Sicherheit spielt in E-Government-Anwendungen eine zentrale Rolle. Der Schutz persönlicher Daten, die im Rahmen von E-Government-Verfahren übertragen und verarbeitet werden, muss jederzeit höchste Priorität haben. Zur geeigneten Absicherung von E-Government-Verfahren kommen daher in der Regel erprobte kryptographische Methoden zur Anwendung. Um Bürgerinnen und Bürger geeignet über das Internet authentifizieren zu können – passwortbasierte Verfahren bieten bekanntermaßen im Allgemeinen kein ausreichendes Sicherheitsniveau – kommen häufig Hardware-Token, die die Implementierung von Zwei-Faktor-Authentifizierungen ermöglichen, zum Einsatz. In den meisten europäischen Ländern sind für diesen Zweck Chipkarten das Mittel der Wahl.

Die Integration dieser Hardware-Token in zumeist webbasierte E-Government-Anwendungen stellt Diensteanbieter immer wieder vor Herausforderungen. Vor allem wenn zusätzliche Anforderungen wie Plattform- oder Browserunabhängigkeit die Implementierungsalternativen einschränken, müssen zur Integration von Hardware-Token in E-Government-Anwendungen

mitunter komplexe Lösungswege beschrrieben werden. In vielen Fällen werden Hardware-Token über entsprechende Middleware-Lösungen in bestehende E-Government-Verfahren integriert. Dieser Ansatz wird unter anderem in Österreich verfolgt und konnte sich aus rein funktionaler Sicht bereits seit vielen Jahren bewähren.

Die österreichische E-Government-Strategie sieht eine größtmögliche Flexibilität in Bezug auf die zu verwendenden Technologien vor. Als gemeinsame Basis dient die Bürgerkarten-Spezifikation [BÜR12], die abstrakte Anforderungen an zu verwendende Hardware-Token definiert, jedoch keine Einschränkungen bezüglich derer Umsetzung macht. Durch diese Flexibilität entstand in den letzten Jahren in Österreich ein Ökosystem an unterschiedlichen Lösungen. So können österreichische Bürgerinnen und Bürger neben verschiedenen Chipkarten auch ihre Mobiltelefone verwenden, um sich sicher an E-Government-Anwendungen zu authentifizieren und um qualifizierte elektronische Signaturen gemäß EU Signaturrechtlinie zu erstellen.

Bei der Entwicklung all dieser Lösungen hatte verständlicherweise die Erfüllung gegebener Sicherheitsanforderungen oberste Priorität. Für den Erfolg und die Akzeptanz von IT-Lösungen im Allgemeinen und E-Government-Lösungen im Speziellen spielt neben der Sicherheit jedoch auch die Benutzerfreundlichkeit eine entscheidende Rolle. Diese wurde in Vergangenheit jedoch oft nur am Rande beachtet und im Design- und Entwicklungsprozess verschiedenster E-Government-Lösungen nicht geeignet berücksichtigt.

Vor allem die Verwendung von Mobiltelefonen anstelle von Chipkarten als Hardware-Token scheint jedoch ein vielversprechender Schritt in Richtung einer verbesserten Benutzerfreundlichkeit zu sein, entfällt bei der Verwendung von Mobiltelefonen doch die Notwendigkeit eines Chipkartenlesegeräts. Eine genaue Untersuchung der Benutzerfreundlichkeit und Akzeptanz der auf Mobiltelefonen beruhenden Lösung im Vergleich zu etablierten chipkartenbasierten Lösungen wurde bisher jedoch in Österreich noch nicht durchgeführt.

Um diese Lücke zu schließen, wurde im Rahmen einer Usability-Analyse die Benutzerfreundlichkeit und Akzeptanz chipkartenbasierter und mobiltelefonbasierter E-Government-Lösungen in Österreich verglichen. Dieser Artikel stellt die evaluierten Komponenten vor, beschreibt Design und Durchführung des zur Evaluierung angewendeten Usability-Tests und diskutiert schließlich im Detail die erhaltenen Resultate.

2 Bürgerkarten-Implementierungen

Die *Bürgerkarte* ist die zentrale Grundlage aller E-Government-Lösungen in Österreich und erfüllt prinzipiell zwei Aufgaben. Mit der Bürgerkarte können sich österreichische Bürgerinnen und Bürger einerseits sicher über das Internet an E-Government-Applikationen authentifizieren und andererseits qualifizierte elektronische Signaturen erstellen. Die Bürgerkarte fungiert damit als sichere Signaturerstellungseinheit und ist in der Lage, sämtliche Anforderungen der Signaturrechtlinie der Europäischen Union für die Erstellung qualifizierter Signaturen [EuPa99] zu erfüllen.

Obwohl der Begriff Bürgerkarte die Verwendung von Chipkarten zu suggerieren scheint, ist das Konzept der österreichischen Bürgerkarte tatsächlich weitgehend technologieneutral und erlaubt grundsätzlich verschiedene Implementierungsvarianten. Aktuell können in Österreich sowohl Chipkarten als auch Mobiltelefone als Bürgerkarte verwendet werden. Die Unterstützung verschiedener Implementierungen ist aus Sicht der Bürgerinnen und Bürger durchaus vorteilhaft, können diese doch die von ihnen präferierte Implementierungsvariante wählen.

Aus Sicht von Diensteanbietern kann sich daraus jedoch ein beträchtlicher Mehraufwand ergeben, da mehrere verschiedene Bürgerkarten-Implementierungen (Chipkarten, Mobiltelefone, etc.) unterstützt werden müssen.

Um die Komplexität in Grenzen zu halten, wurde für das österreichische Bürgerkartenkonzept ein middlewarebasierter Ansatz vorgesehen. Zentrales Element der gewählten Architektur ist der sogenannte *Security Layer*, der in [LeHP02] vorgestellt und diskutiert wurde. Der Security Layer ist eine abstrakte XML-basierte Schnittstelle zwischen E-Government-Applikationen und verschiedenen Bürgerkarten-Implementierungen. Applikationen können über diese abstrakte Schnittstelle auf Bürgerkartenfunktionalität (Authentifizierung, Signatur, etc.) zugreifen, ohne über Implementierungsdetails der verwendeten Bürgerkarte Bescheid wissen zu müssen.

Da in der Regel weder Chipkarten noch Mobiltelefone in der Lage sind, eine XML-basierte Schnittstelle zu implementieren, bedarf es einer Middlewarekomponente, die diese Aufgabe übernimmt. Gemäß der Nomenklatur des österreichischen E-Governments wird diese Middlewarekomponente *Bürgerkartenumgebung (BKU)* genannt. Abb. 1 zeigt das prinzipielle Zusammenspiel von Security Layer und Bürgerkartenumgebung. Durch die offene Spezifikation der Security Layer Schnittstelle gibt es in Österreich aktuell mehrere verschiedene Bürgerkartenumgebungen (d.h. Middleware-Implementierungen) [MOWS12][TrDB12]. Auch hier können Bürgerinnen und Bürger die von ihnen präferierte Lösung wählen. Jene BKUs, deren Benutzerfreundlichkeit in weiterer Folge näher untersucht werden soll, werden in den folgenden Unterabschnitten ausführlicher vorgestellt.

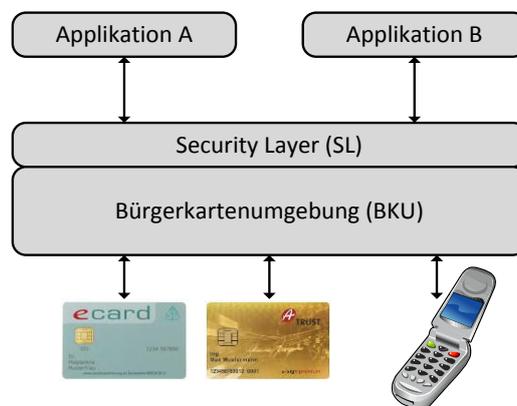


Abb. 1. Die Bürgerkartenumgebung implementiert die Security Layer Schnittstelle und fungiert als Middleware zwischen Applikationen und Bürgerkarten-Implementierungen.

2.1 MOCCA Lokal

Die Integration von Chipkarten in (zumeist webbasierte) E-Government-Applikationen ist eine nicht-triviale Aufgabe. Nahezu alle verfügbaren Bürgerkartenumgebungen verfolgen zur Lösung dieses Problems einen sogenannten *lokalen* Ansatz. Bei diesem muss am lokalen System der Bürgerin bzw. des Bürgers eine Software installiert werden, die in der Lage ist, mit der lokal am System der Benutzerin bzw. des Benutzers vorhandenen Chipkarte (z.B. über das PC/SC-Protokoll) zu kommunizieren. Die Software stellt außerdem das Security Layer Interface über einen lokalen Netzwerk-Port zur Verfügung. Webbasierte E-Government Applikationen können damit auf dieses Interface und in weiterer Folge auf die Bürgerkarte einfach über den Web-Browser der Benutzerin bzw. des Benutzers zugreifen. Abb. 2 zeigt den prinzipiellen Aufbau von BKUs, die dem lokalen Ansatz folgen.

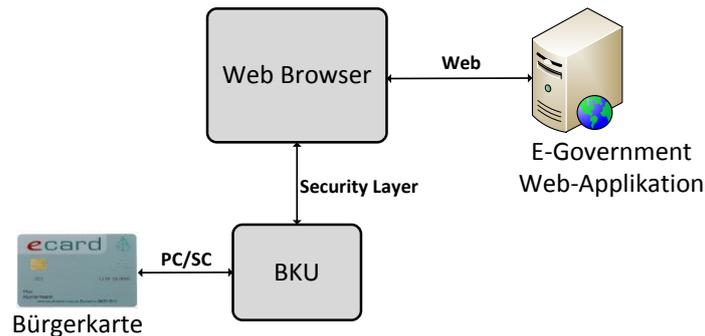


Abb. 2. Der lokale Ansatz beruht auf Software, die am lokalen System installiert werden muss.

Aktuell ist in Österreich eine Reihe von BKUs, die dem lokalen Ansatz folgen, verfügbar (z.B. [TrDB12]). *MOCCA Lokal* [MOWS12] ist jedoch derzeit die einzige Lösung, die als Open Source zur Verfügung steht. *MOCCA Lokal* wurde im Rahmen des *MOCCA* Projekts [MOCC12] entwickelt und stellt derzeit eine der meistverwendeten BKUs für den Zugriff auf chipkartenbasierte Bürgerkarten-Implementierungen dar.

2.2 MOCCA Online

Während der im vorherigen Abschnitt beschriebene lokale Ansatz durchaus zuverlässig funktioniert, ergeben sich für diesen diverse Mängel in Bezug auf die Benutzerfreundlichkeit. Vor allem die Notwendigkeit der Installation einer lokalen Softwarekomponente erwies sich in der Praxis in vielen Fällen vor allem für wenig erfahrene Computerbenutzerinnen und Benutzer als problematisch. Um diesem Problem entgegenzuwirken, wurde im Rahmen des oben erwähnten *MOCCA*-Projekts eine installationsfreie BKU-Alternative namens *MOCCA Online* entwickelt.

MOCCA Online wurde in [CeOB10] bereits ausführlich vorgestellt und diskutiert. Der prinzipielle Aufbau von *MOCCA Online* ist in Abb. 3 dargestellt. *MOCCA Online* besteht aus einer zentralen Server-Komponente und einem lokal im Web-Browser der Bürgerin bzw. des Bürgers gestarteten Java Applets. Die zentrale *MOCCA*-Komponente implementiert das Security Layer Interface. Das am lokalen System laufende Java Applet ist hingegen für den Zugriff auf die Chipkarte am lokalen System verantwortlich. Die beiden Komponenten kommunizieren über ein internes, proprietäres Interface.

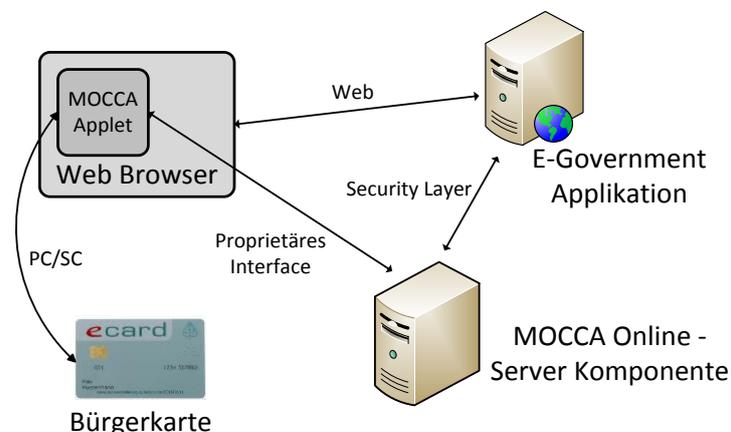


Abb. 3. *MOCCA Online* beruht auf einer verteilten Architektur bestehend aus einer zentralen Server-Komponente und einem lokalen Java Applet.

Durch die Auslagerung eines Teils der BKU-Funktionalität auf eine zentrale Komponente und die Verwendung eines Java Applets ist bei diesem Ansatz auf dem lokalen Systems der Bürgerin bzw. des Bürgers keinerlei Softwareinstallation nötig. Die einzige Anforderung an das lokale System ist eine entsprechend aktuelle Java Laufzeitumgebung zur Ausführung des Java Applets.

2.3 Österreichische Handy-Signatur

Für chipkartenbasierte Bürgerkarten-Implementierungen konnte durch MOCCA Online bereits eine signifikante Verbesserung der Usability erreicht werden. Generell bergen chipkartenbasierte Ansätze jedoch das Problem, dass Bürgerinnen und Bürger über ein entsprechendes Chipkartenlesegerät verfügen müssen. Die Erfahrung zeigte, dass dies in der Praxis oft eine ernstzunehmende Hürde darstellte.

Um dieses Problem zu umgehen, wurde in Österreich die *Handy-Signatur* als Alternative zu chipkartenbasierten Bürgerkarten-Implementierungen entwickelt. Die Handy-Signatur wurde in [OrCK10] vorgestellt und diskutiert. Der prinzipielle Aufbau der Handy-Signatur ist in Abb. 4 dargestellt. Kernkomponente der Handy-Signatur ist das zentrale Handy-Signatur Service. Dieses stellt ähnlich wie MOCCA Online die Security Layer-Schnittstelle zur Verfügung, über die E-Government-Applikationen Zugriff auf die Bürgerkartenfunktionalität erlangen können. Im Gegensatz zu MOCCA Online werden bei der Handy-Signatur alle Schlüssel und Zertifikate zentral vom Handy-Signatur Service sicher in einem HSM gehalten. Für einen Zugriff auf diese Daten bedarf es einer entsprechenden Autorisierung der Bürgerin bzw. des Bürgers. Dazu muss in einem ersten Schritt ein geheimes Passwort zusammen mit der Mobiltelefonnummer über ein abgesichertes Web-Formular an das Handy-Signatur Service übermittelt werden. Konnte dieses Passwort positiv verifiziert werden, wird ein zeitlich begrenzt gültiges Einmalpasswort (TAN) an das Mobiltelefon der Bürgerin bzw. des Bürgers gesendet. Zur endgültigen Autorisierung des Zugriffs auf die Bürgerkartenfunktionalität muss dieses Einmalpasswort über das Web-Formular ebenfalls an das Handy-Signatur Service übermittelt werden.

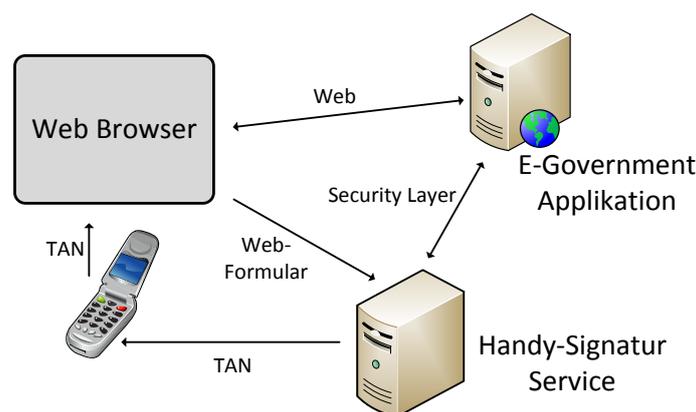


Abb. 4. Die Handy-Signatur sieht eine zentrale Signaturerstellung in einem serverseitigen HSM vor.

Wie bei chipkartenbasierten Lösungen implementiert auch die Handy-Signatur eine Zwei-Faktor-Authentifizierung. Die Sicherheit dieses Verfahrens ist damit vergleichbar zu jener von chipkartenbasierten Ansätzen. Eine ausführliche Diskussion der Sicherheit der österreichischen Handy-Signatur und ein Vergleich zu anderen mobilen Signaturerstellungsvarianten kann unter anderem in [ZeTL11] nachgelesen werden.

Die Handy-Signatur funktioniert unabhängig von chipkartenbasierten Lösungen. Österreichische Bürgerinnen und Bürger können daher die Handy-Signatur und alternative chipkartenbasierte Lösungen parallel verwenden. Personen, die bereits über eine gültige chipkartenbasierte Bürgerkarte verfügen, können diese zudem verwenden, um die Bürgerkartenfunktionalität auf ihrem Mobiltelefon über ein entsprechendes Web-Portal freischalten zu lassen. Das Aufsuchen einer Registrierungsstelle ist in diesem Fall nicht mehr nötig.

3 Test-Design

Alle drei in Abschnitt 2 vorgestellten Bürgerkarten-Implementierungen (bzw. BKU-Implementierungen) kommen in Österreich regelmäßig zur Anwendung. Während der Fokus im Rahmen der Entwicklung dieser Komponenten hauptsächlich auf Funktionalität und Sicherheit lag, wurde Aspekten der Benutzerfreundlichkeit oft zu wenig Aufmerksamkeit zuteil. Im Rahmen einer umfangreichen Usability-Analyse wurde diesem Umstand Rechnung getragen und die Benutzerfreundlichkeit der in Abschnitt 2 beschriebenen Komponenten (MOCCA Lokal, MOCCA Online, Handy-Signatur) evaluiert. Dazu wurde ein Thinking-Aloud-Test [BoRa99] mit insgesamt zwanzig Testbenutzern durchgeführt. Durch diesen Test sollte vor allem festgestellt werden, ob die Handy-Signatur gegenüber chipkartenbasierten Lösungen aus Sicht von Benutzerinnen und Benutzern signifikante Vorteile aufweist. Das gewählte Test-Design, sowie Details zu dessen Umsetzung werden in diesem Abschnitt diskutiert.

3.1 Fragestellungen

Zur Sicherstellung einer strukturierten Vorgehensweise wurden in einem ersten Schritt spezifische Fragestellungen definiert. Ziel der durchgeführten Usability-Analyse war es, geeignete Antworten auf die im Folgenden angeführten Fragestellungen zu finden.

- Wie wird die Benutzerfreundlichkeit der Aktivierung der Handy-Signatur aus Sicht der Benutzerinnen und Benutzer wahrgenommen?
- Wie wird die Benutzerfreundlichkeit der Verwendung der Handy-Signatur aus Sicht der Benutzerinnen und Benutzer wahrgenommen?
- Welche Bürgerkarten-Implementierung wird von Benutzerinnen und Benutzern generell bevorzugt?
- Wie wird die Sicherheit und Vertrauenswürdigkeit der einzelnen Bürgerkarten-Implementierungen durch Benutzerinnen und Benutzer bewertet?

Die durch die durchgeführte Usability-Evaluierung erhaltenen Antworten zu diesen Fragestellungen werden in Abschnitt 4 dieses Artikels ausführlich diskutiert.

3.2 Testmethode und Setup

Die Benutzerfreundlichkeit der evaluierten Komponenten wurde im Rahmen eines Thinking-Aloud-Tests untersucht. Bei einem Thinking-Aloud-Test werden Benutzerinnen und Benutzer gebeten, eine Reihe von praktischen Aufgaben durchzuführen. Die Tätigkeiten der Testpersonen werden dabei beobachtet und mit technischen Hilfsmitteln aufgezeichnet. Dadurch können in einem folgenden Analyseschritt auffällige Verhaltensweisen im Umgang mit den zu evaluierenden Komponenten analysiert und das Verhalten verschiedener Testpersonen verglichen werden.

Im Rahmen des durchgeführten Usability-Tests kam eine spezielle Software zum Einsatz¹. Diese erlaubte die Aufzeichnung sämtlicher Benutzereingaben und ermöglichte zudem die Aufnahme der von den Testpersonen während des Tests getätigten Äußerungen. Zusätzlich wurde das Gesicht der Testpersonen aufgezeichnet, um etwaige Stimmungsschwankungen über deren Mimik ablesen und analysieren zu können. Die eingesetzte Software ermöglichte eine strukturierte Aufzeichnung und Speicherung der gesammelten Daten und bot zudem Unterstützung bei deren nachfolgenden Auswertung.

Die Aufzeichnung der Benutzerinteraktion ermöglichte eine objektive Analyse verschiedener Aspekte der evaluierten Komponenten. Darüber hinaus war jedoch auch der subjektive Eindruck der Testpersonen, den diese von den untersuchten Komponenten hatten, von Interesse. Um diesen festhalten zu können, wurden alle Testpersonen gebeten, nach Durchführung der einzelnen ihnen gestellten Aufgaben die verwendeten Komponenten über einen Fragebogen zu bewerten. Zusätzlich wurden alle Testpersonen im Rahmen eines abschließenden Interviews gebeten, persönliche Eindrücke und Präferenzen zu artikulieren.

Nach Abschluss des Thinking-Aloud-Tests wurden die gesammelten Daten analysiert und entsprechend statistisch aufbereitet. Dadurch war es schlussendlich möglich die zu Beginn der Usability-Überprüfung definierten Fragestellungen zu beantworten und somit wertvolle Erkenntnisse in Bezug auf die Benutzerfreundlichkeit der evaluierten Komponenten zu gewinnen.

3.3 Aufgabenstellungen

Um bestmögliche Antworten auf die definierten Fragen zu erhalten, wurden die im Rahmen des Thinking-Aloud-Tests durchzuführenden Aufgaben auf die gegebenen Fragestellungen zugeschnitten. Aus den gegebenen Fragestellungen wurden daher folgende Aufgaben generiert und den Testpersonen zur Ausführung vorgelegt.

- Führen Sie ein gegebenes E-Government-Verfahren unter Verwendung ihrer chipkartenbasierten Bürgerkarte und MOCCA Lokal durch!
- Führen Sie ein gegebenes E-Government-Verfahren unter Verwendung ihrer chipkartenbasierten Bürgerkarte und MOCCA Online durch!
- Aktivieren Sie die Handy-Signatur mit Hilfe Ihrer chipkartenbasierten Bürgerkarte!
- Führen Sie ein gegebenes E-Government-Verfahren unter Verwendung der Handy-Signatur durch!

Um etwaige Verfälschungen der Resultate, die sich durch Lerneffekte ergeben hätten können, zu verhindern, wurden die oben genannten Aufgaben teilweise in unterschiedlicher Reihenfolge ausgeführt. Dadurch konnte die Auswirkung von Lerneffekten größtenteils ausgeglichen und die Gültigkeit und Aussagekraft der erhaltenen Resultate verbessert werden.

3.4 Testpersonen

Zur Evaluierung der Benutzerfreundlichkeit der verschiedenen österreichischen Bürgerkarten-Implementierungen wurde der Thinking-Aloud-Test mit insgesamt zwanzig Testpersonen

¹ Für die Durchführung der Tests wurden die Softwareprodukte Morae® Recorder, Morae® Observer und Morae® Manager der Firma TechSmith® verwendet. Weitere Informationen zu diesen Softwarelösungen finden sich unter <http://www.techsmith.com/morae.html>.

durchgeführt. Bei der Auswahl der Testkandidatinnen und Testkandidaten wurde darauf geachtet, die österreichische Bevölkerung möglichst genau abzubilden. Es wurden daher Personen unterschiedlichen Alters und mit verschiedenem Bildungsniveau zur Teilnahme eingeladen. Ebenso wurde darauf geachtet, dass auch technisch wenig versierte Bürgerinnen und Bürger an diesem Usability-Test teilnahmen.

Die folgenden Abbildungen zeigen die Verteilung der an dem Usability-Test teilnehmenden Testpersonen in Bezug auf Alter, Ausbildungsniveau und technischem Vorwissen. Die personenbezogenen Daten wurden für jede Testkandidatin bzw. jeden Testkandidaten vor Durchführung des Tests im Rahmen eines Einführungsgesprächs erhoben. Wie aus den Abbildungen ersichtlich ist, konnte für jede Kategorie eine entsprechend ausgewogene Verteilung erreicht werden.

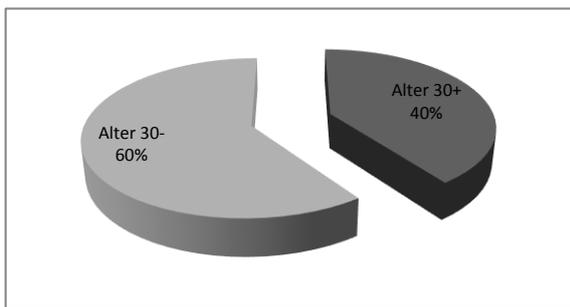


Abb. 5: Altersverteilung der teilnehmenden Testpersonen.

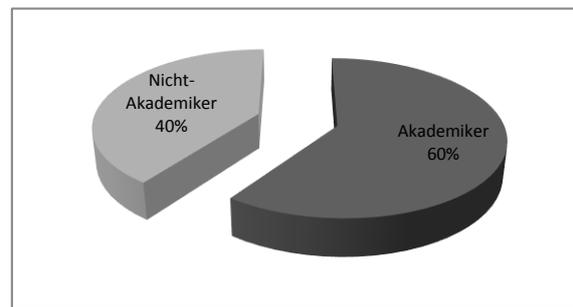


Abb. 6: Ausbildungsniveau der teilnehmenden Testpersonen.

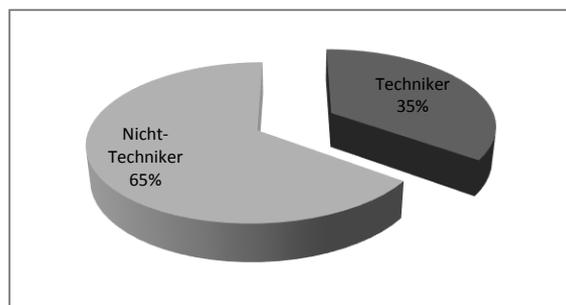


Abb. 7: Technisches Vorwissen der teilnehmenden Testpersonen.

4 Resultate

Ziel des durchgeführten Usability-Tests war die Evaluierung der Benutzerfreundlichkeit und Akzeptanz der österreichischen E-Government-Komponenten MOCCA Lokal, MOCCA Online und Handy-Signatur. Dadurch sollte überprüft werden, ob durch die chipkartenlose mobile Alternative die Akzeptanz von E-Government-Applikationen generell entscheidend erhöht werden kann. In diesem Abschnitt werden die erhaltenen Resultate des durchgeführten Usability-Tests präsentiert und diskutiert. Die folgenden vier Unterabschnitte geben dabei Antworten auf die vier zu Beginn des Usability-Tests festgelegten Fragestellungen.

4.1 Aktivierung der Handy-Signatur

Bevor die österreichische Handy-Signatur als Alternative zu chipkartenbasierten Lösungen verwendet werden kann, muss diese für das Mobiltelefon der Bürgerin bzw. des Bürgers aktiviert werden. Die Aktivierung kann in eigens dafür vorgesehenen Registrierungsstellen oder unter Verwendung einer chipkartenbasierten Bürgerkarte von der Bürgerin bzw. dem Bürger selbst vorgenommen werden. Die Benutzerfreundlichkeit letzterer Variante wurde im Rahmen des Usability-Tests überprüft.

Abb. 8 zeigt, dass die Aktivierung der Handy-Signatur von den Testpersonen durchwegs positiv bewertet wurde. Der Aktivierungsvorgang konnte in allen abgefragten Kategorien gute bis sehr gute Ergebnisse erreichen. Insgesamt kann festgehalten werden, dass die Aktivierung der Handy-Signatur von beinahe allen Testpersonen selbstständig und problemlos durchgeführt werden konnte und diesbezüglich keine groben Mängel festgestellt werden konnten.

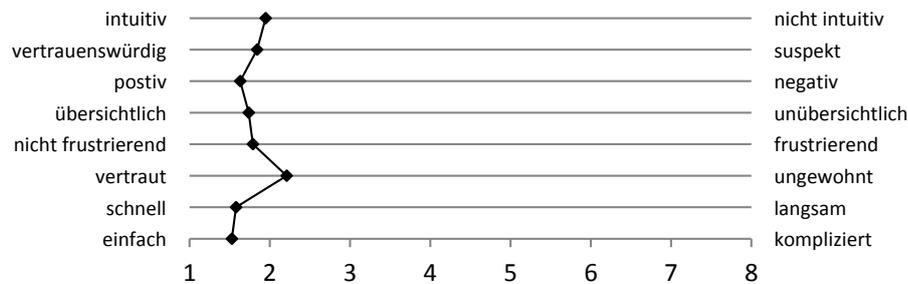


Abb. 8: Die Aktivierung der Handy-Signatur wurde von allen Testpersonen positiv bewertet.

4.2 Verwendung der Handy-Signatur

Die wohl interessanteste Frage, die im Rahmen des Usability-Tests untersucht wurde, betraf die Verwendung der Handy-Signatur und deren Abschneiden im Vergleich zu chipkartenbasierten Bürgerkarten-Implementierungen. Die Testpersonen wurden aufgefordert, ein typisches E-Government-Verfahren sowohl mit einer chipkartenbasierten Bürgerkarte (unter Verwendung von MOCCA Lokal und MOCCA Online), als auch mit der Handy-Signatur durchzuführen und danach verschiedene Aspekte der Benutzerfreundlichkeit zu bewerten. Abb. 9 zeigt die erhaltenen Resultate.

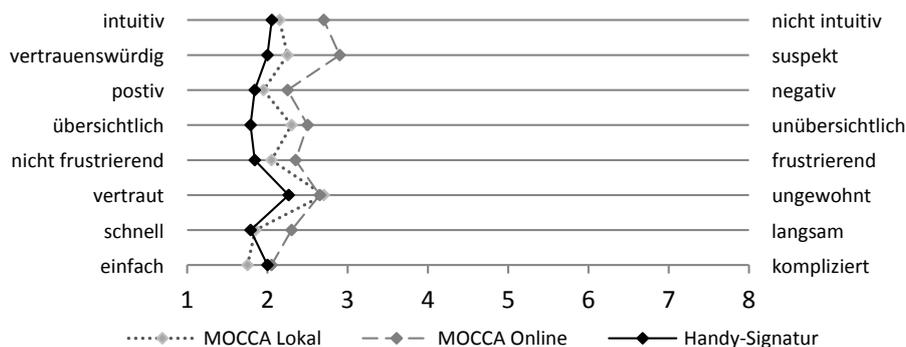


Abb. 9. Die Handy-Signatur wurde in fast allen Aspekten positiver bewertet als chipkartenbasierte Lösungen.

Die Handy-Signatur wurde im Vergleich zu chipkartenbasierten Lösungen in fast allen Kategorien positiver bewertet. Diese Beobachtung gilt unabhängig von der verwendeten Bürgerkartenumgebung bei der Verwendung von Chipkarten. Einzig in der Kategorie Einfachheit konnte sich MOCCA Lokal knapp gegenüber der Handy-Signatur durchsetzen.

4.3 Bevorzugte Implementierung

Nach Abschluss der Tests wurden alle Testpersonen gefragt, welche Bürgerkarten-Implementierung (Chipkarte oder Handy-Signatur) bzw. welche BKU (MOCCA Lokal,

MOCCA Online, etc.) sie im Rahmen einer zukünftigen privaten Nutzung der Bürgerkarte bevorzugen würden. Auch hier ging die Handy-Signatur als klarer Sieger hervor. Abb. 10 illustriert die erhaltenen Resultate im Detail.

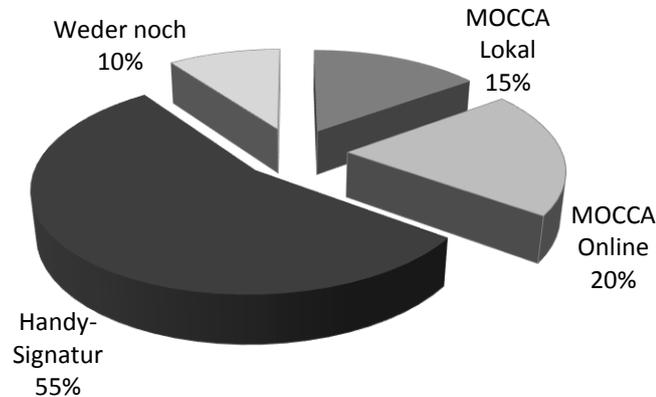


Abb. 10. Mehr als die Hälfte aller Testpersonen würde die Handy-Signatur im Rahmen einer zukünftigen privaten Verwendung der Bürgerkarte bevorzugen.

Wie erwartet erreichte MOCCA Online etwas besserer Werte als MOCCA Lokal. Hier wurde von den Testpersonen unter anderem der Umstand gewürdigt, dass MOCCA Online im Gegensatz zu MOCCA Lokal keiner Softwareinstallation bedarf. Sowohl MOCCA Online als auch MOCCA Lokal liegen jedoch deutlich hinter der Handy-Signatur zurück, die insgesamt 55% der Testbenutzerinnen und Benutzer überzeugen konnte.

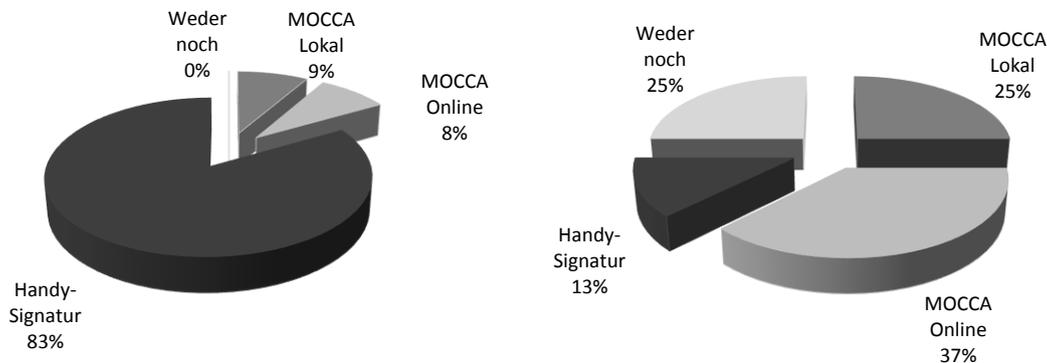


Abb. 11. Linkes Diagramm: Bei unter 30-jährigen Testpersonen konnte sich die Handy-Signatur klar durchsetzen. Rechtes Diagramm: Bei älteren Testpersonen wurden chipkartenbasierte Lösungen klar bevorzugt (rechts).

Eine getrennte Betrachtung der Resultate älterer und jüngerer Testpersonen führte zu überraschend deutlichen Ergebnissen. Abb. 11 zeigt, dass die Handy-Signatur offenbar vor allem bei Benutzerinnen und Benutzern, die jünger als 30 Jahre sind, außerordentlich beliebt ist. Bei älteren Testpersonen konnten sich in dieser Frage hingegen chipkartenbasierte Ansätze (MOCCA Lokal und MOCCA Online) durchsetzen. Auch in dieser Gruppe behielt MOCCA Online klar die Oberhand gegenüber MOCCA Lokal.

4.4 Sicherheit und Vertrauenswürdigkeit

Aus Sicht von Diensteanbietern und Applikationsbetreibern ist auch das Maß an Sicherheit und Vertrauenswürdigkeit, das Benutzerinnen und Benutzer den verwendeten Lösungen attestieren, von Interesse. Alle Testpersonen wurden daher nach Absolvierung der ihnen gestellten

Aufgaben gefragt, ob sie die verwendeten Bürgerkarten-Implementierungen und Softwarekomponenten als sicher und vertrauenswürdig einstufen würden.

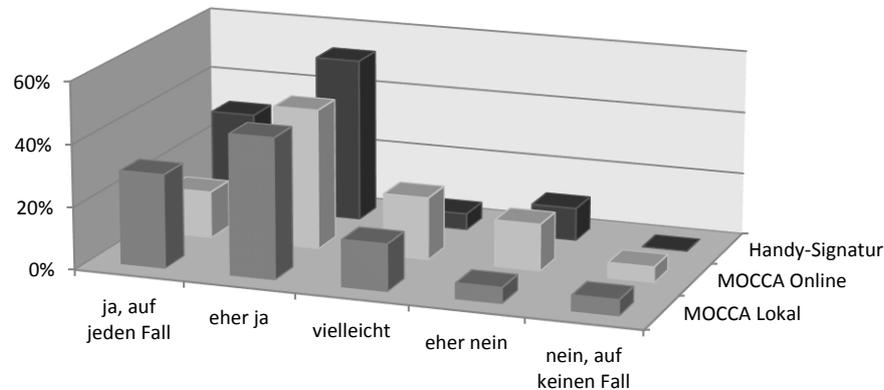


Abb. 12. Testbenutzerinnen und Testbenutzer hatten das Gefühl, dass alle Versionen der Bürgerkartenumgebungen eher vertrauenswürdig sind.

Die in Abb. 12 dargestellten Ergebnisse zeigen, dass generell allen evaluierten Implementierungen ein entsprechendes Maß an Sicherheit und Vertrauenswürdigkeit attestiert wurde. Auch bei dieser Frage konnte sich die Handy-Signatur schlussendlich gegenüber chipkartenbasierten Lösungen durchsetzen. Die Unterschiede waren hier jedoch nicht so signifikant wie bei den zuvor diskutierten Fragestellungen.

5 Fazit

Seit der Vorstellung des Konzepts der Bürgerkarte in Österreich wurden beträchtliche Ressourcen in die Entwicklung entsprechender Implementierungen investiert. Erste Varianten lokaler Bürgerkartenumgebungen für chipkartenbasierte Bürgerkarten-Implementierungen konnten funktionale Anforderungen erfüllen, waren jedoch oft nicht in der Lage, ein geeignetes Maß an Benutzerfreundlichkeit zu bieten. Die nachfolgende Entwicklung von MOCCA Online konnte einige dieser Nachteile beseitigen, beruhte jedoch ebenfalls noch auf der Chipkartentechnologie. Die österreichische Handy-Signatur repräsentiert die aktuelle Stufe der Entwicklung, in der erstmals eine vollständige Alternative zu chipkartenbasierten Lösungen geboten wird.

Die durchgeführte Usability-Analyse zeigte, dass der eingeschlagene Weg stimmt. In den meisten evaluierten Punkten konnte sich MOCCA Online gegenüber der lokalen BKU-Implementierung durchsetzen. Die Abkehr vom lokalen Ansatz und die Entwicklung einer installationsfreien BKU-Alternative für chipkartenbasierte Bürgerkarten-Implementierungen kann im Nachhinein daher als richtige Entscheidung bewertet werden.

Noch deutlicher fiel das Ergebnis der Evaluierung der Benutzerfreundlichkeit in Bezug auf die Handy-Signatur aus. Diese konnte in allen untersuchten Punkten die ebenfalls evaluierten chipkartenbasierten Lösungen klar übertreffen. Sowohl in puncto Benutzerfreundlichkeit, als auch in Bezug auf die Akzeptanz ging die Handy-Signatur jeweils als klarer Sieger hervor. Die Entscheidung, eine mobile Alternative zu chipkartenbasierten Bürgerkarten-Implementierungen zu entwickeln stellte sich damit im Nachhinein als richtig heraus.

Die erhaltenen Resultate der durchgeführten Usability-Analyse decken sich größtenteils mit den Erfahrungen des Alltags. Diese zeigen, dass die Handy-Signatur in der österreichischen

Bevölkerung im Vergleich zu chipkartenbasierten Lösungen eine breitere Akzeptanz findet. Die österreichische Handy-Signatur scheint damit in der Lage zu sein, den Spagat zwischen strikten Sicherheitsanforderungen und einem adäquaten Level an Benutzerfreundlichkeit zur Zufriedenheit der der österreichischen Bevölkerung zu meistern.

Literatur

- [EuPa99] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal of the European Communities L 013, (2000) 12-20.
- [LeHP02] Leitold, H., Hollosi, A., Posch, R.: Security Architecture of the Austrian Citizen Card Concept. Proceedings of the 18th Annual Computer Security Applications Conference, Washington, DC, USA, IEEE Computer Society, (2002) 391–400.
- [CeOB10] Centner, M., Orthacker C., Bauer, W.: Minimal-Footprint Middleware for the Creation of Qualified Signatures. Proceedings of the 6th International Conference on Web Information Systems and Technologies, Portugal, (2010) 64–69.
- [MOCC12] Modular Open Citizen Card Architecture, <http://mocca.egovlabs.gv.at/>, (2012).
- [BoRa99] M. Ted Boren, J. Ramey: Thinking Aloud: Reconciling Theory and Practice. In: IEEE Transactions on Professional Communication Vol. 43, No. 3 (2000) 261-278.
- [BÜRG12] Bürgerkarte – Spezifikationen, <http://alt.buergerkarte.at/de/spezifikation/index.html>, (2012).
- [MOWS12] Bürgerkartenumgebung MOCCA Webstart, <http://webstart.buergerkarte.at/mocca/>, (2012).
- [TrDB12] ITSolution: trustDesk basic, <http://www.itsolution.at/trustDesk-basic.html>, (2012).
- [OrCK10] Orthacker, C., Centner, M., Kittl, C.: Qualified Mobile Server Signature. Proceedings of the 25th TC 11 International Information Security Conference, SEC 2010, (2010).
- [ZeTL11] Zefferer, T., Teufl, P., Leitold, H.: Mobile qualifizierte Signaturen in Europa. Datenschutz und Datensicherheit 11|2011, (2011).