Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

STELLUNGNAHME ZUR SICHERHEIT VON SIGNATUR- UND BÜRGERKARTEN

Einleitung

In den vergangenen Monaten häuften sich Pressemeldungen zu diversen Attacken (Phishing, Trojanische Pferde) auf österreichische Online-Banking Systeme. Im Zuge dieser Meldungen wurden auch Zweifel daran publiziert, dass die Verwendung von Signatur- und Bürgerkarten gegen derartige Attacken ausreichenden Schutz bieten könnte.

Diese Stellungnahme gibt eine kurze vergleichende Darstellung der bei unterschiedlichen Verfahren auftretenden Risiken wieder und geht im Anschluss auf die konkreten Sicherheitsvorteile, die Lösungen basierend auf Bürgerkarten bieten, ein.

Risikovergleich

	Risiko gegenüber Diebstahl von Zugangscodes (Phishing, etc)	Risiko gegenüber Angriffen über das Netz (Man in the Middle)	Risiko gegenüber Angriffen am Benutzer-PC (Trojanische Pferde)	Risiko bei strikter Einhaltung der Benutzer-Policies
Benutzername & Passwort				
PIN/TAN Verfahren				
PIN/iTAN Verfahren				
PIN/mTAN (TAC) Verfahren				
Authentifizierung mittels Signatur				
Signatur über Inhalte				
Bürgerkarte				

Legende:

erhöhtes Risiko	relativ geringes Risiko	äußerst geringes Risiko

Erläuterungen zur Tabelle:

Angriffe über das Netz: Gemeint sind sog. „Man in the Middle Attacken“, bei denen sich der Angreifer in die Kommunikationsverbindung einschaltet (z.B. durch Umleitung der Browserverbindung auf einen falschen Server) und dabei die übertragenen Daten abhört bzw. fälscht.

Angriffe am Benutzer-PC: Gemeint sind Angriffe, bei denen Schadsoftware (Trojanische Pferde) am Benutzer-PC installiert wird (z.B. im Zuge der Installation scheinbar harmloser Programme), die dann am Benutzer-PC eingegebene Daten abhört und an einen Angreifer versendet, bzw. am Benutzer-PC eingegebene Daten vor der Übertragung an den Zielserver (z.B. Bankserver) fälscht.

Risiko bei strikter Einhaltung der Benutzer-Policies: Werden die von den verwendeten Systemen vorgegebenen Richtlinien (z.B. Überprüfen auf Bestehen einer SSL-Verbindung, Überprüfen von Server-Zertifikaten) von den Benutzern strikt eingehalten, lässt sich in den meisten Fällen das Risiko stark reduzieren.

Benutzername & Passwort: Zugänge, die lediglich mittels Eingabe von Benutzername & Passwort abgesichert sind, bieten nur einen geringen Schutz. Neben der Anfälligkeit gegen die o.g. Angriffsszenarien bestehen noch zusätzliche Risiken (z.B. können Passwörter durch Beobachten der Eingabe ausgespäht werden, „schwache“ Passwörter können erraten werden, etc.). Ein Angreifer hat die Möglichkeit gestohlene Zugangsdaten mehrmalig zu nutzen und zwar so lange bis der betreffende Zugang gesperrt wird. Die Tatsache, dass ein Angriff erfolgt ist, d.h. dass das Passwort von Unbefugten verwendet worden ist, kann meist erst nach Eintreten eines Schadens entdeckt werden.

PIN/TAN Verfahren: Das klassische PIN/TAN Verfahren hat gegenüber der Verwendung von Benutzername & Passwort den kleinen Vorteil, dass „Einmalpasswörter“ (=TAN) verwendet werden, um eine Transaktion auszulösen. D.h. eine gestohlene TAN kann von einem Angreifer nur einmal verwendet werden. Die Tatsache, dass eine TAN gestohlen wurde, kann jedoch auch hier meist erst nach Eintreten eines Schadens entdeckt werden.

PIN/iTAN Verfahren: Beim diesem Verfahren werden indizierte TAN (=iTAN) verwendet. D.h. für eine bestimmte Transaktion ist nur die Verwendung einer bestimmten TAN aus einer durchnummerierten Liste möglich, die Gültigkeit der iTAN ist auf einen kurzen Zeitraum (in der Regel etwa 5 Minuten) beschränkt. D.h. eine gestohlene iTAN kann von einem Angreifer (etwa über eine Man in the Middle Attacke) nur direkt im Zuge der Abwicklung einer Transaktion genutzt werden.

PIN/mTAN (TAC) Verfahren: Bei diesem Verfahren wird, um die Authentifizierung des Benutzers zusätzlich abzusichern, auch das Mobiltelefon des Benutzers verwendet. Der für die Transaktion benötigte Einmalcode (mTAN oder auch TAC-Key genannt) wird auf einem alternativen Kommunikationskanal per SMS auf ein Mobiltelefon des Benutzers übertragen. Die mTAN bzw. der TAC-Key ist nur für eine Transaktion und für einen kurzen Zeitraum (in der Regel etwa 5 Minuten) gültig. Angriffe, die auf Diebstahl bzw. Kopieren von TAN-Listen beruhen sind bei diesem Verfahren nicht mehr möglich.

Authentifizierung mittels Signatur: Wird zur Authentifizierung des Benutzers eine digitale Signatur eingesetzt, kann der Authentifizierungsvorgang nur mit dem privaten Signaturschlüssel des Benutzers vorgenommen werden. Ist dieser Schlüssel auf einer sicheren Hardwareeinheit (z.B. Chipkarte, USB-Token, Mobiltelefon) gespeichert, ist eine Authentifizierung nur bei Vorhandensein dieser Hardwareeinheit möglich. Hier spricht man von einer sicheren 2-Faktor-Authentifizierung. Der Diebstahl bzw. Verlust der Hardware kann rasch erkannt werden, und der Benutzer kann sofort entsprechende Maßnahmen (Sperre des Zugangs, Widerruf des Zertifikats)

einleiten. Dadurch sind Angriffe, die auf das Ausspionieren bzw. Stehlen von Zugangsdaten (z.B. durch Phishing, Keylogger, Password-Stealing-Trojans, etc.) beruhen nicht wirksam.

Bei allen o.g. Verfahren werden lediglich Maßnahmen gesetzt, um einen Benutzer zu authentifizieren, bzw. eine Transaktion (mittels TAN) zu autorisieren. Die Verfahren beinhalten jedoch keine Maßnahmen um einen sicheren Bezug zwischen den Inhalten einer Transaktion und dem Benutzer zu erzeugen. Ein derartiger Bezug wird durch die digitale Signatur über die Inhalte einer Transaktion hergestellt.

Signatur über Inhalte: Werden die Transaktionsdaten mit einer digitalen Signatur des Benutzer versehen, ist auch die betreffende Transaktion eindeutig dem Benutzer zuzuordnen. Werden dabei auch - wie bereits oben erwähnt - entsprechend sichere Hardwareeinheiten eingesetzt, ist sichergestellt, dass die Transaktion nur dann durchgeführt werden kann, wenn der Auslöser tatsächlich im Besitz dieser Hardwareeinheit ist. Ein Restrisiko besteht noch dadurch, dass ein Angreifer versuchen könnte, dem Benutzer (durch eine Man in the Middle Attacke oder über ein Trojanisches Pferd) gefälschte Daten zur Signatur vorzulegen. Dieses Risiko kann jedoch dadurch ausgeschlossen werden, dass entsprechend sichere Programme zur Anzeige der Daten verwendet werden, bzw. dass der Benutzer nach dem Signaturvorgang eine Signaturprüfung vornimmt und dadurch auch eindeutig erkennen kann, was er signiert hat.

Bürgerkarte: Bei Einsatz der Bürgerkarte ist vorgesehen, dass immer auch eine Signatur über die Inhalte erfolgt. Zusätzlich wird durch die Verwendung der Personenbindung auch eine eindeutige Identifizierung des Benutzers ermöglicht. Die im Konzept Bürgerkarte beim Benutzer eingesetzte Software („Bürgerkartenumgebung“) verbindet sich nur mit definierten Servern, dadurch sind „Man in the Middle Attacken“ auszuschließen und es besteht eine Ende-zu-Ende Sicherheit.

Vorteile von Bürgerkartenlösungen

Die nachfolgenden Aussagen treffen auch für Dienstkarten, die dem Konzept Bürgerkarte entsprechen (z.B. Dienstkarte gem. Beamten-Dienstrechtsgesetz) vollinhaltlich zu.

Die sichere Signatur ist tatsächlich sicher.

Bürgerkartenlösungen verwenden sichere Signaturen laut Signaturgesetz bzw. Verwaltungssignaturen laut E-Government-Gesetz. Verwaltungssignaturen entsprechen in technischer Hinsicht den hohen Anforderungen für sichere Signaturen.

Die Regelungen im Signaturgesetz und der Signaturverordnung stellen sicher dass:

- Der Benutzer **das angezeigt** bekommt, **was er signiert**.
- Der Benutzer **sicher** sein kann, **wozu er sich verpflichtet**.
- Die Signatur **nicht gefälscht** werden kann.
- Die signierten **Inhalte nicht veränderlich** sind.

Seit Bestehen der sicheren Signatur, sind keine Rechtsfälle anhängig, bei denen die Sicherheit der Signatur in Frage gestellt wird.

Die Bürgerkarte „spricht“ nur mit ihr „bekannten“ Kommunikationspartnern.

Ein Prinzip des E-Government ist **Ende-zu-Ende Sicherheit.** Die im Konzept Bürgerkarte beim Benutzer eingesetzte Software („Bürgerkartenumgebung“) ist daher so konfiguriert:

- Dokumente zur Signatur werden nur vom eigenen Gerät angenommen.
- Der Benutzer kann entscheiden, mit welchen Servern er eine Kommunikationsverbindung zulassen will bzw. für welche Server eine Verbindung ausgeschlossen ist.
- Eine Antwort wird nur an Server mit „bekannten Sicherheitszertifikaten“ geschickt.

Die Bürgerkarte signiert Inhalte und macht sie dadurch unveränderlich.

Das Prinzip der Bürgerkarte baut nicht auf einen bloßen Login-Vorgang auf, nach dem beliebig Transaktionen durchgeführt werden können. Bei sicherheitsrelevanten Vorgängen ist eine Signatur über die entsprechenden Inhalte vorgesehen, die anschließend serverseitig von der Anwendung geprüft wird. Dadurch wird eine **Modifikation** der signierten Inhalte **automatisch erkannt**.

Solange die Bürgerkartenumgebung nicht ausgetauscht wird, ist eine Kompromittierung nicht möglich.

Die Bürgerkarte schützt die Privatsphäre des Benutzers.

Auf der Bürgerkarte sind nur Daten zur Identifikation und für die Signatur vorhanden.

Der externe Zugang zu weiteren in E-Government Anwendungen gespeicherten personenbezogenen Daten ist nur für die betreffende Person unter Verwendung ihrer Bürgerkarte möglich.

Unabhängig von der Verwendung der Bürgerkarte kann ein Angreifer weder Informationen zur Person noch sonstige über die Identifikation hinausgehende Daten erfahren.

Alle Informationen auf der Bürgerkarte können mit einem **Zugriffsschutz (PIN)** versehen werden. Der **Benutzer** hat dadurch **immer** die **Kontrolle** darüber, wer welche Daten auf seiner Bürgerkarte abfragen kann.

Die Bürgerkarte ermöglicht eine sichere Identifikation.

Die Bürgerkarte ist nicht nur Signaturkarte sondern stellt durch die sog. „Personenbindung“ auch einen **eindeutigen Zusammenhang** zwischen einer **Person** und der **Signatur** her.

„Vorgetäuschte“ Identitäten bzw. „vorgetäuschte“ Signaturen werden dadurch verlässlich verhindert.

Prüfung von signierten Dokumenten.

Die Bürgerkartenumgebung ermöglicht das **unabhängige Prüfen** signierter Dokumente. Dadurch ist sowohl das **Erkennen von Manipulationen** an eigenen, signierten Dokumenten möglich, als auch die **Feststellung der Authentizität** von z.B. durch Behörden mittels Amtssignatur signierten Dokumenten möglich.

Sicherheit auch für die Wirtschaft.

Das Konzept der Bürgerkarte wurde von Beginn an so entwickelt, dass es nicht nur im Behördenbereich sondern auch in der Wirtschaft einsetzbar ist.

Die Verwendung von Signatur und Personenbindung auf der Bürgerkarte bringt wesentliche Vorteile auch für Anwendungen der Wirtschaft:

- Sicherheit, Authentizität und Dokumentation von Eingaben
- Sicherheit, Authentizität und Verbindlichkeit von Antworten
- Sichere Authentifizierung und Identifikation von Kunden, Geschäftspartnern, etc.

Der zunehmenden Verunsicherung bei E-Commerce Transaktionen kann somit am besten entgegengewirkt werden, indem auch die Wirtschaft auf die Sicherheit des im E-Government eingesetzten Bürgerkartenkonzepts zurückgreift.

Wien, April 2006

A-SIT Zentrum für sichere Informationstechnologie – Austria