Sicherheitsstufen für die Kommunikation Bürger – Behörde im Bereich e-Government

Bezeichnung	Sicherheitsstufen für die Kommunikation Bürger – Behörde im Bereich e-Government
Kurzbezeichnung	Sicherheitsstufen
Dokumentenklasse	Konvention
Dokumentenstadium	Empfehlung
Version	1.3.1
Datum	24. August 2003
Kurzbeschreibung	In der Umsetzung von e-Government bedingt die Kommunikation über offene Netze, dass entsprechende Sicherheitsstufen vorzusehen sind, um den Anforderungen der Identifikation der Verfahrensbeteiligten, der Unverfälschtheit und Vertraulichkeit der übermittelten Informationen und des Datenschutzes zu genügen. Dieses Dokument definiert und beschreibt diese Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich e-Government.
Autoren *E-Mail*	Wolfgang Besenmatter; *wolfgang.besenmatter@cio.gv.at*
Arbeitsgruppe	Stabsstelle IKT-Strategie des Bundes Operative Unit – Technik

Sicherheitsstufen in der Kommunikation Bürger – Behörde im Bereich e-Government

Zu den klaren Strategien von e-Government zählen, als eine zentrale Komponente, auch die Methoden der identifizierten und vertraulichen Kommunikation. In der Umsetzung von e-Government bedingt diese Kommunikation über offene Netze, dass entsprechende Sicherheitsstufen vorzusehen sind, um den Anforderungen der Identifikation der Verfahrensbeteiligten, der Unverfälschtheit und Vertraulichkeit der übermittelten Informationen und des Datenschutzes zu genügen. Neben gesetzlichen Anforderungen können darüber hinaus zur Verfügung stehende Sicherheitsstufen bei den Anwendern ein erhöhtes Maß an Vertrauen in e-Government hervorrufen.

In diesem Zusammenhang werden unterschiedliche Sicherheitsstufen der Kommunikation Bürger – Behörde (beziehungsweise deren Dienstleister), deren Sicherheitsziele und damit die Anwendbarkeit definiert. Diese Sicherheitsstufen stellen eine Ergänzung zu den Sicherheitsklassen[1] im Portalverbund dar, welche auf die Kommunikation innerhalb des Portalverbundes abzielen. Für die Beurteilung der einzusetzenden Sicherheitsstufe ist eine Analyse des Schutzbedarfes analog zu den Sicherheitsklassen durchzuführen.

IT-Applikationen im Bereich des e-Government werden in Abhängigkeit vom Grad der Sicherheit in drei Stufen unterschiedlicher Qualität abgegrenzt:

1. Sicherheitsstufe I, kein besonderer Sicherheitsbedarf
2. Sicherheitsstufe II, sichere Kommunikation im Verwaltungsverfahren
3. Sicherheitsstufe III, Kommunikation mit besonderem Sicherheitsbedarf

Das Thema Verfügbarkeit wird hier nicht weiter ausgeführt; es wird im Dokument *Katastrophenvorsorge und Ausfallsicherheitsüberlegungen im IT-Bereich*[2] behandelt.

Serversicherheit

Zusätzlich zu den Sicherheitsstufen sind, für das österreichische e-Government gekennzeichnete, Serverzertifikate[3] zu verwenden; das heißt, es müssen Zertifikate mit Verwaltungseigenschaft eingesetzt werden (das Behördenkennzeichen wird als Extension in das Zertifikat mit aufgenommen).

[1] Konvention *Spezifikation Sicherheitsklassen im Portalverbund-System* vom 15.10.2002

[2] Beschuss in der 11. IKT-Board Sitzung vom 5.11.2002

[3] CIO-Konventionen *Object Identifier der öffentlichen Verwaltung* und *X.509 Zertifikatserweiterungen für die Verwaltung* vom 18.2.2003

1 Sicherheitsstufe I, kein besonderer Sicherheitsbedarf

1.1 Anforderungen und Sicherheitsziele

Viele Anwendungen im Bereich des e-Government stellen nur geringe Anforderungen an die Sicherheit; es sind daher auch keine besonderen Maßnahmen notwendig. Zentraler Aspekt in diesem Bereich ist es, mit Standardsystemen und damit auch an öffentlichen Geräten arbeiten zu können und dennoch nicht gänzlich auf Sicherheit zu verzichten.

Ein Unterschreiten dieser Sicherheitsstufe ist bei Anwendungen, bei denen Bürger, Verwaltungsbedienstete oder Unternehmen in Interaktion treten und nicht nur Information abrufen, nicht vorgesehen. In der Regel werden auch Informationsangebote der Verwaltung dieser Sicherheitsstufe zu unterstellen sein, um ein Täuschen der Kunden zu vermeiden.

1.2 Identifikation, Unverfälschtheit und Vertraulichkeit

Ab dieser Sicherheitsstufe wird eine serverseitig authentifizierte TLS[4]-Verbindung mit mindestens 100 Bit effektiver Schlüssellänge und einem Zertifikat mit Verwaltungseigenschaft angewendet. Bei der dabei stattfindenden Identifikation des Servers ist es in der alleinigen Entscheidung des Kunden die Authentizität der verwaltungsseitigen Einrichtung zu prüfen; die Verwaltung ist in diesem Zusammenhang nicht in der Lage, die Identität des Kunden einer Prüfung zu unterziehen. Weiters wird durch die TLS-Verbindung eine beschränkte Integrität der Daten erreicht.

1.3 Erläuterungen

Diese Sicherheitsstufe ist geeignet für den Zugang zu Informationen, die an sich keiner Geheimhaltung oder dem Datenschutz unterliegen oder für Interaktionen, bei der die Absicherung vor Missbrauch auf einer anderen Ebene stattfinden kann wie z.B.

- durch die elektronische Signatur des eingebrachten Stückes,
- durch einmalige Erledigung, die keine direkten Personenbezug erfordert oder
- wegen des geringfügigen Wertes der Interaktion.

Die Kommunikation findet ohne ein Zertifikat auf der Clientseite statt. Damit ist für den normalen Benutzer davon auszugehen, dass, wenn der Kunde das Serverzertifikat nicht entsprechend überprüft:

[4]IETF, RFC 2246 *The TLS Protocol Version 1.0*, RFC 2818 *HTTP Over TLS* und andere

- ein Mitlesen durch einen Dritten mit entsprechenden Täuschungsmanövern möglich ist (man-in-the-middle Attacke) und
- ein Täuschen mit einem falschen Service durchführbar ist.

Beispiele für diese Sicherheitsstufe sind Informationsdienste, die keine Übermittlung signifikanter Information, wie verfahrens- oder personenspezifischer Daten, beinhalten (analog Sicherheitsklasse 1 im Portalverbund).

2 Sicherheitsstufe II, sichere Kommunikation im Verwaltungsverfahren

2.1 Anforderungen und Sicherheitsziele

Bei der zweiten Stufe der Sicherheit wurde darauf geachtet, dass die Identifikation und Vertraulichkeit so gewählt sind, dass sie nicht manipulierten Endgeräten stand hält und den Anforderungen des Datenschutzes genügt. Bei sorgfältiger Verwendung dieser Sicherheitstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

2.2 Identifikation, Unverfälschtheit und Vertraulichkeit

Es wird eine TLS-Verbindung wie in der Sicherheitsstufe I verwendet und dadurch die verwaltungsseitige Einrichtung identifiziert. Zusätzlich findet eine Identifizierung und Authentifizierung von Kunden mittels Bürgerkarte (d.h. durch Wissen und Besitz) durch MOA ID[5] bzw. äquivalenter Dienste statt.

Als Übergangslösung kann statt der Identifizierung und Authentifizierung mittels Bürgerkarte vorübergehend auch auf der Applikationsebene mittels Benutzerkennung und Passwort gearbeitet werden.

2.3 Erläuterungen

Da die Sicherheitsstufe II höhere Anforderungen an die Qualität der Sicherheit stellt als Stufe I bedarf es zusätzlich einer vertrauenswürdigen, clientseitigen Komponente. Bei den geforderten vertrauenswürdigen Infrastrukturen kann die Kommunikation auf einem challenge-response Mechanismus beruhen, der im Wesentlichen auf eine gegenseitigen Authentifizierung unter Verwendung digitaler Signaturen aufbaut.

Die Anwendbarkeit dieser Sicherungsmethode ist für alle Verfahren und Kommunikationen inklusive des Gesundheitsbereiches möglich. Nicht anzuwenden ist

[5] CIO-Konvention *Spezifikation Module für Online Applikationen – Identifikation* vom 8.10.2002

diese Sicherheitsstufe, wenn man gegen eine manipulierte Hardware- oder Software-Umgebung des Client Schutz bieten muss. Die Sicherung der Nachweisbarkeit ist wegen der symmetrischen kryptographischen Verfahren im strengen Sinne nicht gegeben, so dass aus diesem, aber auch aus rechtlichen Gründen eine elektronische Signatur zum Absichern wesentlicher Inhalte eingesetzt werden soll. Eine man-in-the-middle Attacke ist nur mehr unter sehr eingeschränkten Umständen (d.h. bei Fahrlässigkeit des Kunden) möglich.

Diese Sicherheitsstufe ist beispielsweise für Transaktionen mit personenbezogenen Daten nach dem Datenschutzgesetz geeignet (analog Sicherheitsklasse 2 im Portalverbund).

3 Sicherheitsstufe III, Kommunikation mit besonderem Sicherheitsbedarf

3.1 Anforderungen und Sicherheitsziele

Die höchste Sicherheitsstufe im Bereich e-Government, die auch für die Kommunikation Verwaltung – Verwaltung angewandt werden kann, wenn dies die Vertraulichkeit erfordert, wurde darauf ausgelegt, dass sie kompromittierten Endgeräten stand hält. Bei Anwendung dieser Sicherheitstufe haben Client und Server Klarheit darüber, wer kommuniziert und können auch von der Vertraulichkeit im Rahmen der Sicherheit der kryptographischen Schlüssel und Algorithmen ausgehen.

3.2 Identifikation, Unverfälschtheit und Vertraulichkeit

Die Sicherheit wird mit einer TLS-Verbindung erreicht und basiert auf Zertifikaten mit Verwaltungseigenschaft. Die Bindung der Zertifikate an Client und Server ist technisch so abzusichern, dass sie auch kompromittierten Endsystemen standhält. Die für den Ablauf notwendigen Zertifikate werden direkt vom Server bzw. Client in die sichere TLS-Verbindung eingebunden. Es wird somit, anders als bei Stufe II, eine automatische und in die Verbindungsprotokolle integrierte Überprüfung der Serveridentität möglich. Dieser Mechanismus kann nun auch automatisch man-in-the-middle Attacken erkennen.

3.3 Erläuterungen

Die Zertifikate des Clients und des Serves der TLS-Verbindung werden in vertrauenswürdigen Komponenten gehalten und sind technisch vor Modifikation geschützt. Dies kann zum Beispiel durch den Einsatz von *hardware security modules* (HSM), auch Kryptoboxen genannt, erreicht werden. Diese Sicherheitsmodule sind in verschiedenen Formaten (Box, Tischgerät, PC-Karte, Chipkarte) erhältlich und werden in der Regel als interne Karten, als periphere Geräte oder über

einen Adapter (für die Chipkarte) an den Hostrechner (Zentralrechner, Server, PCs) angeschlossen. Eine weitere Möglichkeit zur Absicherung besteht im Schaffen einer vertrauenswürdigen Softwareumgebung, unter anderem mit sicherem boot - Prozess, zuverlässigem Betriebssystem und digital signierter Software.

Diese Sicherheitsstufe ist für Transaktionen mit sensiblen Daten nach dem Datenschutzgesetz geeignet (analog Sicherheitsklasse 3 im Portalverbund).

A Tabellarische Zusammenfassung

Tabellarische Zusammenfassung der Sicherheitsstufen im Bereich e-Government:

Sicherheitsstufe	**Sicherheitsziele**	**Maßnahmen**
Sicherheitsstufe I, kein besonderer Sicherheitsbedarf	Standardsysteme und öffentliche Geräte	TLS-Verbindung mit OID
Sicherheitsstufe II, sichere Kommunikation im Verwaltungsverfahren	nicht manipulierte Endgeräte	MOA ID
Sicherheitsstufe III, Kommunikation mit besonderem Sicherheitsbedarf	kompromittierte Endgeräte	vertrauenswürdige Komponenten