



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

A-1040 Wien, Weyringergasse 35A-8010 Graz, Inffeldgasse 1

Tel.: ++43 1 – 503 19 63 – 0      Tel.: ++43 316 – 873 5514

Fax: ++43 1 – 503 19 63 – 66      Fax: ++43 316 – 873 5520

Homepage: [www.a-sit.at](http://www.a-sit.at)

E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

# STRATEGIEPAPIER ZUR SSL/TLS-KOMMUNIKATIONSSICHERHEIT FÜR ONLINE E-GOVERNMENT VERFAHREN EMPFOHLENE CIPHERSUITES UND KEYSTORES

<b>Kurzbeschreibung</b>	Empfohlene SSL/TLS CipherSuites und KeyStores für e-Government
<b>Projektnummer</b>	<b>A-SIT 4.043</b>
<b>Auftraggeber</b>	<b>Stabsstelle IKT-Strategie des Bundes</b>
<b>Ansprechperson</b>	BSc. Ing. Gerald Trost
<b>Projektanfang</b>	<b>2003-01</b>
<b>Vertraulichkeit</b>	Durch Auftraggeber festzulegen

## 1 Auftrag

Der Auftragsgegenstand teilt sich in drei Aufgaben:

1. Es ist ein Strategiepapier zur SSL- und TLS-Kommunikationssicherheit für Online e-Government Verfahren zu erstellen. Es sollen Empfehlungen von Verschlüsselungsverfahren (bzw. Cipher Suites), die dem Konzept "Sicherheitsstufen in der Kommunikation im Bereich e-Government" [IKT\_01] entsprechen, enthalten. Dazu gehören auch Mindestschlüssellängen etc.
2. Weiters soll eine Empfehlung erarbeitet werden, in welchem Format SSL/TLS-Zertifikate zwischen Organisationen auszutauschen sind.
3. Zusätzlich soll ein Web-basierendes Testtool entwickelt werden, das für Clients und Server die Eignung hinsichtlich der Verfahren des Strategiepapiers feststellt.

## 2 Zusammenfassung

In vorliegendem Strategiepapier werden Empfehlungen für Secure Socket Layer (SSL) [SSL3] und Transport Layer Security (TLS) [TLS] Cipher Suites gegeben, wie sie zur vertraulichen Kommunikation im e-Government sinnvoller Weise einzusetzen sind, um den Anforderungen der Konvention "Sicherheitsstufen in der Kommunikation im Bereich e-Government" [IKT\_01] zu genügen. Transferformate für Zertifikate und private Schlüssel werden empfohlen.

Neben den technischen Aspekten, die sich vornehmlich auf die technische Sicherheit der Verfahren bezieht, wurde berücksichtigt, inwieweit die in den Standards spezifizierten CipherSuites durch gängige Browser- und Server-Lösungen umgesetzt sind. Damit soll vermieden werden, dass durch spezifische Wahl von CipherSuites Einschränkungen entstehen, nach denen Anwender nicht mehr auf WebBrowser ihrer Wahl zurückgreifen können.

Ein Web-basierendes Tool zur Prüfung von Servern und Clients steht auf <http://demo.a-sit.at/ssltool/> zur Verfügung.

### 3 Grundlagen

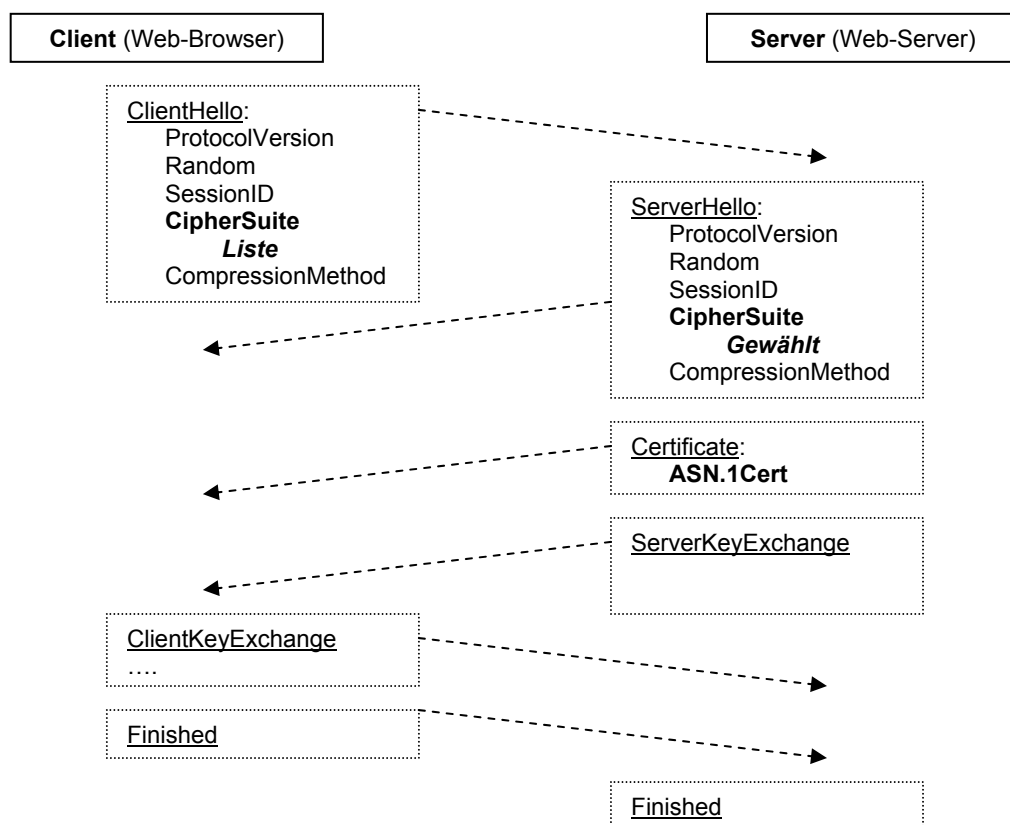
Das Konzept "Sicherheitsstufen in der Kommunikation im Bereich e-Government" [IKT\_01] legt drei Sicherheitsstufen für Online-Verfahren fest, die wie folgt zusammengefasst werden können:

- **Stufe I** fordert serverseitig authentifizierte TLS-Verbindungen mit Schlüssellängen von mindestens 100 Bit. Der Server soll dabei „Verwaltungseigenschaft“ haben, d.h. der Object Identifier (OID) für österreichisches e-Government zu verwenden ist [IKT\_02, IKT\_03].
- **Stufe II** fordert zusätzlich zur TLS-Verbindung die Identifikation über die so genannten Module für Online Applikationen – ID MOA-ID [IKT\_04].
- **Stufe III** soll weiters kompromittierten Endgeräten standhalten, etwa über den Einsatz von Hardware Security Modulen.

Allen Stufen ist die Anforderung gemein, dass die Online-Verbindung über Hypertext Transfer Protocol (HTTP) über SSL bzw. TLS (HTTPS) [HTTPS] abzusichern ist. HTTPS stellt den Stand der Technik dar und wird von gängigen Clients und Servern unterstützt. Dabei wird als „Client“ das eine Kommunikationsbeziehung initiiierende Endsystem bezeichnet, der „Server“ ist das diese Anforderung annehmende System.

Die kryptographischen Protokolle zur Authentifikation der Kommunikationspartner, die Mechanismen zur Wahrung der Integrität und der Vertraulichkeit der übermittelten Daten werden in so genannten „CipherSuites“ zusammengefasst, wobei die Standards [SSL2, SSL3, TLS] eine Vielzahl solcher CipherSuites vorgeben, die unterschiedliche Schlüssellängen und somit unterschiedliche Qualitäten der technischen Sicherheit der Verbindung vorsehen.

Die Auswahl der CipherSuite erfolgt im Zuge des SSL/TLS Handshake Protokolls. Dabei bietet der Client beim Initiieren der Kommunikationsbeziehung im „ClientHello“ eine Liste der unterstützten CipherSuites an, der Server teilt die gewählte CipherSuite im „ServerHello“ mit. In derselben Meldung wird das Server-Zertifikat übermittelt, das in den obig skizzierten Sicherheitsstufen die Verwaltungseigenschaft über einen OID anzeigt. Folgende Figur zeigt schematisch und vereinfacht das Handshake Protokoll, wobei die für dieses Papier wesentlichen Elements **fett** gedruckt sind.



Figur 1 SSL/TLS Handshake (vereinfacht)

Um die SSL/TLS Kommunikationsbeziehung in entsprechender technischer Qualität sicherzustellen, bestehen nach dem in Figur 1 skizzierten Protokoll theoretisch zwei Möglichkeiten:

1. Der Client bietet in der ClientHello-Meldung nur entsprechend starke CipherSuites an.
2. Der Server wählt in der ServerHello-Meldung nur eine starke CipherSuite aus.

Da gängige Clients auch schwache CipherSuites implementieren und dem Server in ihren default-Konfigurationen anbieten, ist die erste Möglichkeit nicht praktikabel – man kann nicht davon ausgehen, dass die BürgerInnen über die technischen Kenntnisse verfügen, Web-Browser auf starke CipherSuites einzustellen. Um die technische Sicherheit der Sicherheitsstufen gemäß [IKT\_01] durchzusetzen, ist die zweite Möglichkeit vorzusehen, das heißt dass der Server nur entsprechend starke CipherSuites auswählen darf.

**Kernaussage 1:** Die Server sind so zu konfigurieren, dass sie nur starke CipherSuites unterstützen. Entsprechende CipherSuites werden in diesem Papier empfohlen.

Neben der technischen Sicherheit sollte beachtet werden, dass gängige Web-Browser unterschiedlicher Hersteller verschiedenen CipherSuites unterstützen (Anhang A gibt einen Überblick). Es gilt zu vermeiden, dass durch die Einschränkung des Servers auf wenige spezifische CipherSuites die BürgerInnen in der Wahl des Web-Browsers dadurch eingeschränkt sind, dass die Server nur CipherSuites auswählen, die nur von bestimmten Web-Browsern unterstützt werden. Es wurden deshalb gängige Web-Browser und Web-Server hinsichtlich der unterstützten CipherSuites untersucht. Die untersuchten Systeme sind:

Web-Browser

- Internet Explorer 6 (V.6.0.2800.1106.xpsp1)
- Netscape 7.02 (V.7.02, Gecko/20030208)
- Mozilla 1.3 (V.1.3.1, Gecko/20030425) [MOZ\_DOC]

Web-Server

- Netscape Enterprise (CMS V 6.01) [NS\_ENT]
- Apache (Open SSL) (V.2.0) [APA\_DOC]
- Oracle (V.9.0.1) [ORA\_ADM]
- IBM Websphere (V.5.0) [SEC\_WS]
- Internet Information Server (V.5.0) [MSTN\_IIS, MSKB\_IIS]

Um die Einschränkung der verwendbaren Web-Browser zu vermeiden, werden nur CipherSuites empfohlen, die neben der technischen Sicherheit auch von mehreren Web-Browsern unterstützt werden, wobei die CipherSuites von gängigen Web-Servern unterstützt werden sollen. Sinnvollerweise ist der Web-Server so zu konfigurieren, dass möglichst viele der empfohlenen CipherSuites unterstützt werden. Zusätzlich zu empfohlenen CipherSuites solche zu unterstützen, die nur von einigen Web-Browsern umgesetzt sind, ist möglich, sofern die technische Sicherheit gegeben ist.

**Kernaussage 2:** In Online-Verfahren sollen für SSL und TLS am Server jene CipherSuites unterstützt werden, die von mehreren gängigen Web-Browsern umgesetzt sind. Es sollen möglichst viele der empfohlenen CipherSuites am Server aktiviert werden. Das Unterstützen zusätzlicher weiterer CipherSuites ist dann möglich, wenn diese die notwendige technische Sicherheit gewährleisten.

Unter diesen Grundlagen werden in Folge Empfehlungen für die CipherSuites gegeben.

## 4 Empfehlungen

### 1. *Empfohlene Mindest-Schlüssellängen*

Das Konzept "Sicherheitsstufen in der Kommunikation im Bereich e-Government" [IKT\_01] sieht für die SSL/TLS Verbindungen eine Mindestschlüssellänge von 100 Bit vor. Für symmetrische Verfahren sind 100 Bit effektive Schlüssellänge bei derzeitigem Stand der Technik als hinreichend sicher anzusehen. Dies ist etwa auch aus [LENVER] abzuleiten.

**Kernaussage 3:** Der in [IKT\_01] gegebene Mindestwert von 100 Bit effektiver Schlüssellänge entspricht für die Inhaltsverschlüsselung den Anforderungen für sichere Online-Verfahren.

### 2. *Empfohlene Versionen von SSL und TLS*

SSL geht auf eine Initiative der Firma Netscape zurück. Die aktuelle Version 3.0 [SSL3] war Basis des von der IETF standardisierten TLS [TLS]. Beide, TLS und SSL Version 3.0 sind als für Online-Verfahren im e-Government anwendbar zu bewerten. Die Vorgängerversion SSL 2.0 weist Schwachstellen auf und sollte nicht mehr verwendet werden.

**Kernaussage 4:** SSL Version 2.0 soll nicht weiter verwendet und Server-seitig deaktiviert werden.

**Kernaussage 5:** Es sind SSL Version 3.0 oder TLS Version 1.0 zu verwenden

### 3. *Empfohlene CipherSuites*

Alle drei Sicherheitsstufen aus [IKT\_01] basieren auf SSL bzw. TLS Kommunikation, wobei die für Sicherheitsstufe I definierte Mindestlänge von 100 Bit auch für die Sicherheitsstufen II und III anwendbar ist. Hier in den CipherSuites zu differenzieren, erscheint nicht sinnvoll.

**Kernaussage 4:** Die empfohlenen CipherSuites sind für die Sicherheitsstufen I, II und III aus [IKT\_01] anwendbar. Die neben den Mindest-Schlüssellängen für diese Sicherheitsstufen in [IKT\_01] zusätzlich gegebenen Anforderungen (e-Government OID, MOA-ID, HSMs, ...) sind zu beachten.

Nachfolgend werden jene CipherSuites gelistet, die entsprechend „Kernaussage 2“ von mehreren gängigen Web-Browsern unterstützt werden und somit anzunehmen ist, dass die BürgerInnen in der Wahl des Web-Browsers nicht eingeschränkt sind, wenn mehrere der empfohlenen CipherSuites unterstützt werden (sinnvoll ist, möglichst viele der empfohlenen CipherSuites zu unterstützen<sup>1</sup>)

Es werden hier nur jene CipherSuites empfohlen, die in den Standards [SSL3] für SSL Version 3.0, sowie [TLS] für TLS 1.0 mit den Erweiterungen um den Advanced Encryption Standard (AES) gemäß [TLS\_AES] spezifiziert sind. Herstellerspezifische CipherSuites einiger Web-Browser und Web-Server sind nicht berücksichtigt (z.B. SSL\_RSA\_EXPORT1024\_\* CipherSuites).

#### Empfohlene CipherSuites für SSL 3.0

<u>CipherSuite</u>	<u>Effektive Schlüssellänge</u>	<u>CipherSuite Code [SSL3]</u>
SSL_RSA_WITH_RC4_128_MD5	128 Bit	0x00, 0x04
SSL_RSA_WITH_RC4_128_SHA	128 Bit	0x00, 0x05
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	168 Bit	0x00, 0x13
SSL_RSA_WITH_3DES_EDE_CBC_SHA	168 Bit	0x00, 0x0A

<sup>1</sup> Anmerkung: Sind die kryptographischen Mechanismen vom Web-Server in Software umgesetzt, ist es im Allgemeinen unkritisch, möglichst viele der unterstützten und hier empfohlenen CipherSuites zu aktivieren. Einschränkungen, etwa höhere Kosten, können sich durch eine Vielzahl an Algorithmen dann ergeben, wenn Hardware Security Module zur Performancesteigerung notwendig sind.

## Empfohlene CipherSuites für TLS 1.0

<u>CipherSuite</u>	<u>Effektive Schlüssellänge</u>	<u>CipherSuite Code [TLS]</u>
TLS_RSA_WITH_RC4_128_MD5	128 Bit	0x00, 0x04
TLS_RSA_WITH_RC4_128_SHA	128 Bit	0x00, 0x05
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA <sup>2</sup>	128 Bit	0x00, 0x13 <sup>2</sup>
TLS_RSA_WITH_3DES_EDE_CBC_SHA	168 Bit	0x00, 0x0A

**Kernaussage 7:** Aus den obig empfohlen CipherSuites soll die in der konkreten Server-Lösung maximal mögliche Menge ausgewählt und aktiviert werden, um Einschränkungen an der Client Seite zu minimieren.

**Kernaussage 8:** Zusätzliche CipherSuites können dann als Erweiterung zu den empfohlenen dienen, wenn die technische Sicherheit wie die Mindest-Schlüssellänge gewährleistet ist.

Einige der untersuchten Web-Clients unterstützen CipherSuites, die die technische Voraussetzung der Mindestschlüssellänge erfüllen, jedoch von anderen Web-Clients nicht unterstützt werden. Es spricht aus technischer Sicht nichts dagegen, die folgenden CipherSuites zusätzlich zu empfohlenen zu aktivieren. CipherSuites die durch von keinen der untersuchten Web-Servern unterstützt wurden, bleiben unberücksichtigt (etwa SSL\_FORTEZZA\_\* CipherSuites)

### Zusätzlich zu empfohlenen CipherSuites mögliche SSL 3.0 CipherSuites

(von gängigen Web-Browsern und Web-Server unterstützt)

<u>CipherSuite</u>	<u>Effektive Schlüssellänge</u>	<u>CipherSuite Code [SSL3]</u>
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	168 Bit	0x00, 0x16

### Zusätzlich zu empfohlenen CipherSuites mögliche TLS 1.0 CipherSuites

(von gängigen Web-Browsern und Web-Server unterstützt)

<u>CipherSuite</u>	<u>Effektive Schlüssellänge</u>	<u>CipherSuite Code [TLS]</u>
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	128 Bit	0x00, 0x32 [TLS_AES]
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	128 Bit	0x00, 0x33 [TLS_AES]
TLS_RSA_WITH_AES_128_CBC_SHA	128 Bit	0x00, 0x2F [TLS_AES]
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	168 Bit	0x00, 0x13
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	256 Bit	0x00, 0x38 [TLS_AES]
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	256 Bit	0x00, 0x39 [TLS_AES]
TLS_RSA_WITH_AES_256_CBC_SHA	256 Bit	0x00, 0x35 [TLS_AES]

## 4. Empfohlene Transferformate

In Folge werden Formate für den Transfer von Zertifikaten oder privaten Schlüsseln empfohlen. Es ist bei der Speicherung, Übermittlung und Verwahrung privater Schlüssel zu beachten, dass dies ein kritisches Element hinsichtlich der Sicherheit darstellt. Es sind besondere Sicherheitsmaßnahmen vorzusehen, um eine Kompromittierung effektiv zu verhindern.

**Kernaussage 9:** Backup oder Transfer privater Schlüssel stellt ein besonderes Gefährdungspotential dar. Es werden hier keine Empfehlungen für die Sicherung eines solchen Backups oder Transfers gegeben, sondern nur Formate definiert, die Interoperabilität zwischen gängigen Produkten erlauben.

<sup>2</sup> Anm.: TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA ist nach [TLS] Kap. 9 für eine TLS-compliant Lösung umzusetzen.

Es wurden für die empfohlenen Formate die für die Empfehlungen der CipherSuites untersuchten Web-Server herangezogen. Es sind dies:

- |                               |              |                      |
|-------------------------------|--------------|----------------------|
| - Netscape Enterprise         | (CMS V 6.01) | [NS_ENT]             |
| - Apache (Open SSL)           | (V.2.0)      | [APA_DOC]            |
| - Oracle                      | (V.9.0.1)    | [ORA_ADM]            |
| - IBM Websphere               | (V.5.0)      | [SEC_WS]             |
| - Internet Information Server | (V.5.0)      | [MSTN_IIS, MSKB_IIS] |

Diese Web-Server können die empfohlenen Formate entweder direkt verarbeiten, oder diese in ein direkt verarbeitbares Format konvertieren<sup>3</sup>.

#### **Empfohlene Transferformate für private Schlüssel**

Für die Speicherung privater Schlüssel wird das Format PKCS#12 [PKCS12] empfohlen.

Zur Speicherung und Weitergabe von Zertifikaten (bzw. Zertifikatsketten) ohne Mitgabe des privaten Schlüssels wird folgendes Format empfohlen:

#### **Empfohlene Transferformate für Zertifikate**

Für die Speicherung der Server-Zertifikate wird das Format PKCS#7 [PKCS7] empfohlen.

In diesem Format sind Zertifikate in einer festgelegten ASN.1-Struktur und nach den Distinguished Encoding Rules (DER) kodiert abgespeichert. Eine zusätzliche BASE64-Kodierung ist optional möglich, jedoch nicht notwendig.

Es wird empfohlen, den gesamten Zertifizierungspfad inklusive des Root-Zertifikats (self-signed Zertifikat) zu speichern.

## **5 SSL/TLS Client-/Server-Prüftool**

Ein Web-basierendes Tool zur Prüfung von Servern und Clients steht auf <http://demo.a-sit.at/ssltool/> zur Verfügung. Dieses Tool klassifiziert Web-Clients und Web-Server entsprechend der hier gegebenen Empfehlungen.

<sup>3</sup> Etwa Apache, der für den Private Key das Format Base64 Encoded Binary verlangt – dieses ist aus dem empfohlenen PKCS#12 mit der OpenSSL Toolsuite konvertierbar. Dies ist auf Apache Servern typischerweise vorhanden, da OpenSSL Basis der Apache SSL-Unterstützung ist.

## 6 Referenzen

### 1. Relevante Unterlagen der Stabsstelle IKT-Strategie des Bundes

Int. Bez.	Titel/Version/Autor	Form/Umfang
IKT_01	Konzept: Sicherheitsstufen im Bereich e-Government, Stabsstelle IKT-Strategie des Bundes, Version 1.2, 8.4.2003, Wolfgang Besenmatter.	PDF, 7 Seiten inkl. Deckblatt
IKT_02	Konvention: Object Identifier der öffentlichen Verwaltung, Version 1.0.2, 18.2.2002, Arno Hollosi.	PDF, 7 Seiten inkl. Deckblatt
IKT_03	Konvention: X.509 Zertifikatserweiterungen für die Verwaltung, Version 1.0.2, 18.2.2002, Arno Hollosi,	PDF, 5 Seiten inkl. Deckblatt
IKT_04	Konvention: Spezifikation Module für Online Applikationen - ID, Version 1.0, 8.10.2002, Rudolf Schamberger, Ludwig Moser, ARGE Spezifikation MOA.	PDF, 29 Seiten inkl. Deckblatt

### 2. Referenzen

Int. Bez.	Titel/Version/Autor	Online-Verfügbarkeit (as of 19.05.2003)
HTTPS	RFC2812, HTTP Over TLS, May 2000, E. Rescorla.	<a href="http://rfc.net/rfc2818.html">http://rfc.net/rfc2818.html</a>
LENVER	Selecting cryptographic key sizes, J. of Cryptology, 14 (2001) 255-293, A.K. Lenstra, E.R. Verheul,	
SSL2	The SSL Protocol, Netscape Communications Corp., Feb 9, 1995, Hickman, Kipp.	<a href="http://wp.netscape.com/eng/security/SSL_2.html">http://wp.netscape.com/eng/security/SSL_2.html</a>
SSL3	The SSL 3.0 Protocol, Netscape Communications Corp., Nov 18, 1996., A. Frier, P. Karlton, and P. Kocher.	IETF draft <a href="http://wp.netscape.com/eng/ssl3/draft302.txt">http://wp.netscape.com/eng/ssl3/draft302.txt</a>
PKCS7	RFC 2315: PKCS #7: Cryptographic Message Syntax Version 1.5. March 1998, B. Kaliski.	<a href="http://rfc.net/rfc2315.html">http://rfc.net/rfc2315.html</a>
PKCS12	PKCS#12: Personal Information Exchange Syntax Standard, Version 1.0, 24.6.1999, RSA Laboratories.	<a href="http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html">http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html</a>
TLS	RFC2246, The TLS Protocol Version 1.0, January 1999, T. Dierks, C. Allen.	<a href="http://rfc.net/rfc2246.html">http://rfc.net/rfc2246.html</a>
TLS_AES	RFC3268 Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002, P. Chown.	<a href="http://rfc.net/rfc3268.html">http://rfc.net/rfc3268.html</a>

### 3. Spezifikationen der untersuchten Web-Browser und Web-Server

Int. Bez.	Titel/Version/Autor	Online-Verfügbarkeit (as of 19.05.2003)
APA_DOC	Dokumentation zum Apache HTTP Server Version 2.0	<a href="http://httpd.apache.org/docs-2.0/">http://httpd.apache.org/docs-2.0/</a>
MOZ_DOC	mozilla.org: Mozilla Documentation	<a href="http://www.mozilla.org/catalog/">http://www.mozilla.org/catalog/</a>
MSTN_IIS	Microsoft TechNet: Internet Information Services	<a href="http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/iiswelcome.asp">http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/iiswelcome.asp</a>
MSKB_IIS	Microsoft Knowledge Base Article – 245030: How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll, 20.05.2003	<a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;245030">http://support.microsoft.com/default.aspx?scid=kb;en-us;245030</a>
NS_ENT	Managing Servers with Netscape Console - Netscape Console and Administration Server, Version 6.01	<a href="http://enterprise.netscape.com/docs/cms/601/admin/ag/contents.htm">http://enterprise.netscape.com/docs/cms/601/admin/ag/contents.htm</a>
ORA_ADM	Oracle Advanced Security Administrator's Guide, Release 9.0.1	<a href="http://www.cs.uvm.edu/oracle9doc/index.htm">http://www.cs.uvm.edu/oracle9doc/index.htm</a>
SEC_WS	Security documentation for distributed operating systems - WebSphere Application Server, Version 5, 21.11.2002	<a href="ftp://ftp.software.ibm.com/software/webserver/appserv/library/wasv5base_sec.pdf">ftp://ftp.software.ibm.com/software/webserver/appserv/library/wasv5base_sec.pdf</a>

Graz 31.05.2003

A-SIT Zentrum für sichere Informationstechnologie - Austria

Dipl.-Ing Herbert Leitold



## A.2 Cipher Suites für TLS 1.0

Key-bits	Cipher Suite Name	Web-Browser			Web-Server				
		Netscape 7.02	Mozilla 1.3.1	IE 6	Netscape Enterprise	Apache (Open SSL)	Oracle 9.0.1	Websphere 5.0	IIS 5.0
0	TLS_NULL_WITH_NULL_NULL								
0	TLS_RSA_WITH_NULL_MD5	X	X		X	X		X	
0	TLS_RSA_WITH_NULL_SHA		X		X	X		X	
40	TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA					X	X	X	
40	TLS_DH_anon_EXPORT_WITH_RC4_40_MD5					X	X	X	
40	TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA					X			
40	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA					X		X	
40	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA				X	X		X	
40	TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA								
40	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA				X	X	X	X	X
40	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	X	X	X	X	X		X	X
40	TLS_RSA_EXPORT_WITH_RC4_40_MD5	X	X	X	X	X	X	X	X
56	TLS_DH_anon_WITH_DES_CBC_SHA					X	X	X	
56	TLS_DH_DSS_WITH_DES_CBC_SHA								
56	TLS_DHE_DSS_WITH_DES_CBC_SHA		X	X		X		X	
56	TLS_DHE_RSA_WITH_DES_CBC_SHA		X			X		X	
56	TLS_DH_RSA_WITH_DES_CBC_SHA								
56	TLS_RSA_WITH_DES_CBC_SHA	X	X	X	X	X	X	X	X
128	TLS_DH_anon_WITH_AES_128_CBC_SHA					X			
128	TLS_DH_anon_WITH_RC4_128_MD5					X	X	X	
128	TLS_DH_DSS_WITH_AES_128_CBC_SHA								
128	TLS_DHE_DSS_WITH_AES_128_CBC_SHA		X			X			
128	TLS_DHE_RSA_WITH_AES_128_CBC_SHA		X			X			
128	TLS_DH_RSA_WITH_AES_128_CBC_SHA								
128	TLS_RSA_WITH_AES_128_CBC_SHA		X			X			
128	TLS_RSA_WITH_IDEA_CBC_SHA					X			
128	TLS_RSA_WITH_RC4_128_MD5	X	X	X	X	X	X	X	X
128	TLS_RSA_WITH_RC4_128_SHA		X	X		X	X	X	X
168	TLS_DH_anon_WITH_3DES_EDE_CBC_SHA					X	X	X	
168	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA								
168	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA		X	X		X		X	
168	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA		X			X		X	

168	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA								
168	TLS_RSA_WITH_3DES_EDE_CBC_SHA	X	X	X	X	X	X	X	X
256	TLS_DH_anon_WITH_AES_256_CBC_SHA					X			
256	TLS_DH_DSS_WITH_AES_256_CBC_SHA								
256	TLS_DHE_DSS_WITH_AES_256_CBC_SHA		X			X			
256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA		X			X			
256	TLS_DH_RSA_WITH_AES_256_CBC_SHA								
256	TLS_RSA_WITH_AES_256_CBC_SHA		X			X			

Anmerkung: Tabellen A.1 und A.2 wurden sowohl auf Basis der Produktdokumentationen und –spezifikationen (siehe Referenzen 6.3) als auch anhand der mit dem Prüf-Tool ermittelten Ergebnisse erstellt. Je nach Konfiguration der Software und in Abhängigkeit eventuell durchgeführter Updates können die tatsächlich unterstützten CipherSuites von den Angaben in diesen Tabellen abweichen.