E-DEMOCRACY IN WASSENAAR

Alexander Prosser

Professor, Wirtschaftsuniversität Wien, Department für Informationsverarbeitung und Prozessmanagement
Welthandelsplatz 1, A-1020 Wien, AT
alexander.prosser@wu.ac.at, http://e-voting.at

Schlagworte: ***Wassenaarer Arrangement, Kryptographie, e-Democracy, e-Government***

Abstract: *Der Beitrag untersucht die Verwendung von Anwendungen der e-Democracy (und auch eGovernment) aus dem Ausland unter Berücksichtigung des Wassenaarer Arrangements. Der Beitrag kommt zum Ergebnis, dass die Nutzung derartiger Anwendungen in mehrfacher Hinsicht mit den Einschränkungen des Wassenaarer Arrangements kollidieren und es lediglich an einer einzigen Anmerkung in einem Anhang liegt, dass diese letztendlich aus dem Nicht-Wassenaar-Ausland – zumindest in einigen, wenn auch nicht allen Szenarien – doch legal nutzbar sein dürften. Die Nutzung von e-Democracy und e-Government aus dem Nicht-Wassenaar-Raum kann daher im besten Fall als rechtlich prekär bezeichnet werden.*

1. Einführung

1.1. Problemstellung

Einer der wesentlichen Vorteile von elektronischer Bürgerbeteiligung ist die grundsätzliche Erreichbarkeit von jedem Punkt der Erde, was in Zeiten erhöhter beruflicher bzw. privater Mobilität ein wesentlicher Vorteil ist.[1] Dies setzt aber sowohl die physische wie auch die rechtliche Nutzbarkeit derartiger Systeme in anderen Staaten voraus. Eine mögliche Einschränkung ist dabei das Wassenaarer Arrangement (im folgenden WA)[2], das Exportrestriktionen für bestimmte Rüstungs- aber auch Dual Use-Güter vorsieht. Teilnehmende Staaten sind u.a. sämtliche EU-Staaten außer Zypern, die USA und Canada, Japan, Südafrika, Australien, einige lateinamerikanische Staaten und Russland. Die *rechtliche* Verbindlichkeit des Wassenaarer Arrangements ist dabei offenbar eingeschränkt[3] – unbeschadet allfälliger politischer Konsequenzen einer Verletzung. Jährlich wird dabei eine «list of dual-use goods and technologies and munitions» (WA-Liste) herausgegeben, zuletzt im Dezember 2015.[4]

---

1 Vgl. dazu auch die einschlägige Empfehlung des Europarates Rec.CM/Rec(2009)1 zu e-Democracy, etwa in Guideline 74: «E-democracy should offer special opportunities to persons unable to be physically present at democratic meetings and elections, such as those travelling or living abroad, those with reduced mobility and those with pressing personal obligations».

2 The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, http://www.wassenaar.org/ (alle Links wurden per 24. Januar 2016 geprüft).

3 Nach dem Schweizer Staatssekretariat für Wirtschaft ist das WA «eines der vier bestehenden internationalen Exportkontrollregime … Das WA ist das einzige Exportkontrollregime für konventionelle Rüstungsgüter, während die anderen Regime auf die Nichtverbreitung von Massenvernichtungswaffen und deren Trägersystemen ausgerichtet sind. Es wurde 1996 als Ersatz für das während des Kalten Krieges aktive CoCom (Coordinating Committee on Multilateral Export Controls) ins Leben gerufen», wobei das WA «kein völkerrechtlich verbindliches Instrument darstellt.» (Download unter http://www.seco.admin.ch/themen/00513/00600/00601/00603/index.html).

4 Vergleiche die aktuelle Liste unter http://www.wassenaar.org/control-lists/ sowie die Aufstellung der historischen Listen unter http://www.wassenaar.org/control-lists-previous-years/.

Kategorie 5, Teil 2 dieser Liste beschäftigt sich mit Informationssicherheit. Im Beitrag werden kryptographische Komponenten typischer e-Democracy-Systeme durchgegangen und deren Relevanz in Bezug auf das WA untersucht.

1.2. Wassenaar und die Europäische Union

In der Europäischen Union wird dieser Bereich mit Verordnung (EG) 428/2009 abgedeckt.[5] Neben einem Bewilligungsmechanismus (siehe insbesondere Art. 3 und 9) enthält Annex I eine Aufstellung der Dual Use-Güter, die das WA und andere Anti-Proliferationsabkommen implementieren. Diese Liste ist in Abschnitt 5, Teil 2 weitgehend wortgleich mit der (zum Zeitpunkt der Veröffentlichung der Verordnung gültigen) WA-Liste vom Dezember 2008, wurde in den Folgejahren offenbar nicht angepasst, sodass sich Abweichungen zwischen der jeweils aktuellen WA-Liste und Annex I der Verordnung ergaben. Dieser Zustand war nicht optimal und wurde auch von der EU-Kommission in ihrem Bericht aus 2014 zu WA thematisiert:[6] «The Commission could consider setting up an effective mechanism for a regular update of EU control lists».

Diese grundsätzliche Problematik erschließt sich vollumfänglich in der Aktualisierung der Verordnung aus 2009 in 2015/2420 vom 12. Oktober 2015, die als delegierter Rechtsakt am 24. Dezember 2015 publiziert wurde.[7] 2015/2420 stellt eine Wiederveröffentlichung des Annex I aus der Verordnung 428/2009 dar, basiert aber auf der Version der WA-Liste aus 2014 in der korrigierten Fassung vom 25. März 2015[8]. Das bedeutet, dass Rechtsakt 2015/2420 bei seiner Veröffentlichung gemessen an der aktuellen WA-Liste bereits wieder *veraltet* war.

Dies ist umso unverständlicher als alle EU-Mitglieder mit Ausnahme Zyperns auch Teilnehmerstaaten im WA sind und damit – unter Einstimmigkeitsprinzip[9] – auch die jeweilige Fassung der WA-Liste mitbeschließen. Zudem erscheinen die Updates der WA-Liste *regelmäßig* im Dezember des jeweiligen Jahres. Derartige Inkonsistenzen könnten – so rechtlich zulässig – am einfachsten durch einen einmaligen Verweis auf die jeweils gültige WA-Liste aufgelöst bzw. verhindert werden.

Der Unterschied zwischen den WA-Listen 2014 und 2015 ist in Teil 5.2 erheblich. So fielen in Punkt 5.A.2.a. Unterpunkte .2 bis .9 weg (5A002, Punkte 2–9). Diese tauchen zum Teil in veränderter Form an anderer Stelle wieder auf; sie betreffen beispielsweise kryptoanalytische Systeme, Frequenzsprung- und -spreizungssysteme oder die Quantenkryptographie. Für die gegenständliche Fragestellung sind diese Systeme zwar nicht relevant, sie stellen allerdings im militärischen und Sicherheitsbereich wohl zentrale Baugruppen dar.

Diese Inkonsistenz bedeutet letztlich, dass sich beispielsweise Österreich im Rahmen des WA zur Version der WA-Liste 2015 – wenn auch nicht rechtsverbindlich[10] – kommittiert hat, das unmittelbar auch für Österreich geltende EU-Recht allerdings die WA-Liste 2014 reflektiert und nicht unerheblich davon abweicht. In weiterer Folge wird die Diskussion anhand der aktuellen WA-Liste 2015 geführt.

---

5 Verordnung (EG) 428/2009 des Rates vom 5. Mai 2009 über eine Gemeinschaftsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung und der Durchfuhr von Gütern mit doppeltem Verwendungszweck. Falls nicht anders angegeben, können alle im folgenden referenzierten EU-Dokumente von folgender Seite geladen werden: http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

6 COM(2014) 244 – The Review of export control policy: ensuring security and competitiveness in a changing world, S. 7.

7 Commission Delegated Regulation (EU) 2015/2420 of 12 October 2015 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual use items; Download unter http://trade.ec.europa.eu/doclib/docs/2016/january/tradoc_154129.2015-2420.pdf.

8 Zur Quelle vgl. FN4.

9 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies; 1996, VII.5; Download i.d.g.F. http://www.wassenaar.org/wp-content/uploads/2016/01/Guidelines-and-procedures-including-the-Initial-Elements-2015.pdf.

10 Siehe Wassenaar Arrangement (FN9), Explanatory Note, 3. Absatz.

2. Kryptographische Komponenten

2.1. https – Transport Layer Security (TLS)

Hier handelt es sich streng genommen nicht um eine applikatorische Komponente, nichtsdestoweniger wird kaum eine Anwendung im öffentlichen Bereich ohne eine solche Absicherung auskommen. Dies gilt sogar für eine ganze Reihe von reinen Informationsangeboten, wie etwa help.gv.at oder dem Unternehmensserviceportal in Österreich, um sicherzustellen, dass die gebotene Information authentisch ist. TLS (gegenwärtig Version 1.2) ist standardisiert[11] und setzt folgende kryptographische Komponenten ein:

- Ein asymmetrisches Verschlüsselungsverfahren zum «Aushandeln» der für die eigentliche Verschlüsselung des Datenstroms verwendeten symmetrischen Verschlüsselung; hier wird üblicherweise RSA[12] oder eine Variante von Diffie-Hellman (DH)[13] verwendet.
- Digitale Signaturen (ebenfalls entweder RSA- oder DH-basiert), mit denen der öffentliche Schlüssel des Servers und dessen Identität gesichert wird.
- Im Rahmen dieser Signaturen auch ein Hashverfahren, meist wohl SHA-1 oder SHA-256.[14]
- Das mit diesen Komponenten ausgehandelte symmetrische Verfahren zur eigentlichen Verschlüsselung des Datenstroms, typischerweise heute wohl AES[15], ältere Verfahren, wie DES oder TripleDES[16] oder RC2 bzw. RC4[17] werden nicht empfohlen oder wurden mittlerweile von der IETF explizit verboten.[18]

Die eingesetzten Komponenten sind in einem digitalen Zertifikat für jedermann ersichtlich, Abbildung 1 zeigt die Details des Zertifikats von www.bundesschatz.at. Im Menüpunkt «Öffentlicher Schlüssel des Inhabers» können dann Modulus und Public Exponent abgerufen und für die initiale Nachricht an den Server zum Aushandeln des symmetrischen Schlüssels verwendet werden. Unter «Zertifikatsunterzeichnungs-Algorithmus» und «Signaturwert des Zertifikats» finden sich die Informationen zur Prüfung der Signatur des Zertifikats durch den «well-known» Zertifikatsaussteller (hier Thawte Inc.), dessen öffentlicher Schlüssel zur Signaturprüfung den Browsern weltweit bekannt ist. In der aktuellen (Dezember 2015) WA-Liste unterliegen folgende für TLS relevante Technologien einer Exportbeschränkung:

- Symmetrische Algorithmen mit Schlüssellängen über 56 bit (5.A.2.a.1.a);
- Asymmetrische Verfahren auf Primzahlenbasis (etwa RSA) über 512 bit Schlüssellänge (5.A.2.a.1.b);
- Asymmetrische auf Logarithmen basierende Verfahren (etwa DH) über 512 bit bzw. bei Verwendung elliptischer Kurven über 112 bit Schlüssellänge (5.A.2.a.1.b).

[11] Dierks/Rescorla, RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2, IETF, 2008.
[12] Rivest/Shamir/Adleman, U.S. Patent 4,405,829, 14. Dezember 1977.
[13] Rescorla, RFC 2631, The Diffie-Hellman Key Agreement Method, IETF, 1999.
[14] Vgl. dazu Eastlake/Jones, RFC 3174, US Secure Hash Algorithm 1 (SHA1), IETF, 2001 sowie Eastlake/Hansen, RFC 6234, US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), IETF, 2011.
[15] Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), NIST, 2001.
[16] Vgl. die historischen FIPS-Standards 46 (1977), 46-1 (1988) und 46-2 (1993).
[17] Rivest, RFC 2268, A Description of the RC2(r) Encryption Algorithm, IETF, 1998.
[18] Popov, RFC 7465, Prohibiting RC4 Cipher Suites, IETF, 2015.

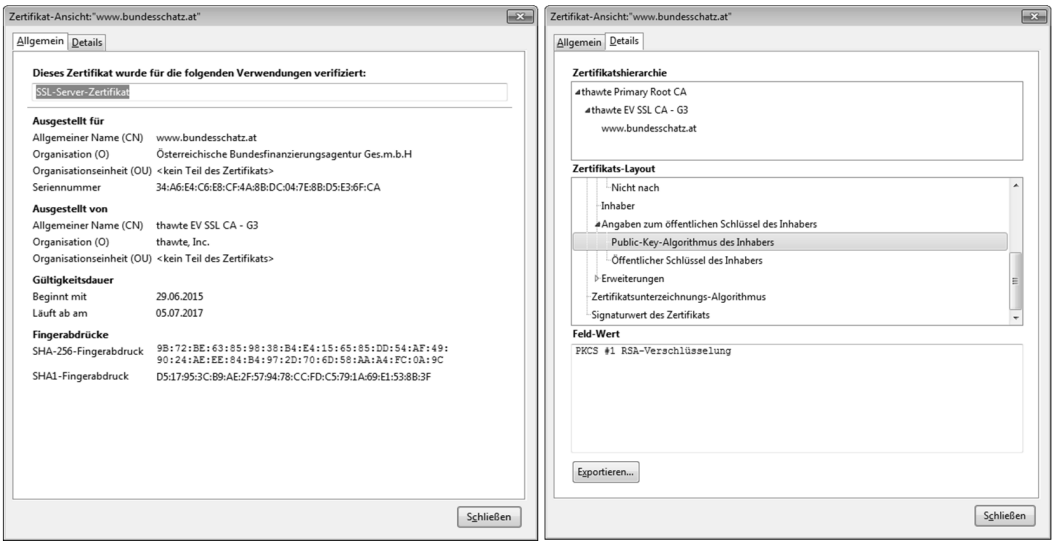

Abbildung 1: Kryptographische Komponenten in einem digitalen Zertifikat

Zu diesen Einschränkungen besteht eine Liste von Ausnahmen (siehe dazu auch Abschnitt 2.3), die allerdings im Falle der allgemeinen Browserverschlüsselung nicht greifen. Zu Hashing äußert sich die WA-Liste nicht. Mit den erlaubten Techniken ist jedenfalls keine sichere TLS- (https-) Verbindung herstellbar. Bei den symmetrischen Verfahren nutzt selbst die einfache Version von AES 128 bit lange Schlüssel (s. FN15) für RSA-Verfahren wird heute 2048 bit als minimale Schlüssellänge empfohlen.[19]

2.2. TLS und das Wo?

Eine gesonderte Fragestellung bezieht sich auf den Ort, an dem diese Technologien eingesetzt werden – ob es sich also rein räumlich um WA-relevante Vorgänge handelt.

Es liegt am Wesen der symmetrischen Verschlüsselung, dass diese gleichermaßen an beiden Orten – dem Server und dem Browser des Nutzers – eingesetzt werden muss. Auch die Verschlüsselung der Anfrage des Browsers an den Server zur Erlangung einer symmetrisch gesicherten Verbindung erfolgt aus dem Browser des Nutzers heraus. Dasselbe gilt für die Signaturprüfung des Zertifikats des Servers, mit dem der öffentliche Schlüssel des Servers propagiert wird.

Damit aber sind sämtliche im letzten Abschnitt genannten Komponenten auch für die Exekution am Client relevant – und erfolgen damit gegebenenfalls technisch außerhalb des Wassenaarer Raumes.

[19] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS); Download unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html. Die in der Richtlinie empfohlene Minimallänge von 2000 bit ergibt idR unter praktischen Gesichtspunkten 2048 bit Schlüssel.

2.3. Digitale Signatur

Dies ist wohl eine absolute Basisfunktionalität auch für e-Government-Anwendungen, ohne diese Komponente kommen nur wenige derartige Anwendungen aus. Diese Anforderungen sind zum Großteil bereits in 2.1. abgedeckt, allerdings kommt bei der digitalen Signatur unter Umständen noch die Bindung an eine Signaturkarte hinzu. Genau das macht auch einen entscheidenden Unterschied zu TLS aus: die WA-Liste kennt eine Reihe von Ausnahmen zu den Einschränkungen zu symmetrischen und asymmetrischen Kryptosystemen:[20]

- Smart Card-basierte («token coin, e-passport) Systeme fallen nicht unter die Restriktionen, falls sie
  - nicht reprogrammierbar sind oder
  - eine der folgenden Bedingungen erfüllt wird:
    - die kryptographischen Funktionen können nicht direkt vom Nutzer angesteuert werden oder
    - sie dienen zum Schutz «persönlicher Daten» auf der Karte und sie können nur für kommerzielle Transaktionen oder die individuelle Identifikation verwendet werden und die kryptographischen Funktionen vom Nutzer nicht direkt – also eventuell für andere Zwecke – angesteuert werden können.
  - Die Lesegeräte fallen ebenfalls unter diese Bestimmung;
- Ebenso wenig ist Ausrüstung («equipment») für Geldtransaktionen betroffen, hier sind wohl vor allem ATM-/Kreditkarten und die entsprechenden Lesegeräte gemeint;
- Eine weitere Ausnahme gibt es für «mobile radiotelephones for civil use», allerdings mit folgender bemerkenswerter Einschränkung:

  «*…that are not capable of transmitting encrypted data directly to another radiotelephone or equipment (other than Radio Access Network (RAN) equipment), nor of passing encrypted data through RAN equipment (e.g., Radio Network Controller (RNC) or Base Station Controller (BSC))*»

  Damit würde eine End-zu-End-Verschlüsselung zwischen Mobiltelefonen bzw. Apps, die auf diesen Geräten laufen, auch dann unter das WA fallen, wenn die verschlüsselten Daten über den RAN (also den Mobilfunkprovider) laufen und nicht direkt ausgetauscht werden.

Der Ort der Ausführung ist in diesen Fällen jedenfalls «vor Ort» (siehe die Erörterung im letzten Abschnitt), da der Nutzer ja an seinem Endgerät und – bei Verwendung einer entsprechenden Karte mit seinem Lesegerät – die kryptographischen Operationen durchführt; es ist also nicht nur die Abarbeitung der Protokolle am Server betroffen.

[20] Siehe die «Note» zu 5.A.2.a.

2.4. Anonymisierungstechniken

Gerade beim e-Voting, aber auch bei gesichert anonymisierter und dennoch an eine geschlossene Mitgliedschaft gebundener Deliberation sind starke Anonymisierungstechniken entscheidend. In den gängigen Verfahren kommen vor allem blinde Signatur[21] oder homomorphe Verfahren[22] zum Einsatz.[23] Mixer-gestützte Verfahren sind an sich keine eigene Klasse von eVoting-Protokollen, da sie im Kern nicht kryptographisch sind. Sie setzen aber zur Absicherung oftmals asymmetrische Verfahren wie RSA ein. Hier gelten die bereits oben erwähnten Restriktionen aus 5.A.2.a.

Anonymisierungstechniken erfordern jedenfalls, dass zumindest ein entscheidender Teil des Protokolls vor Ort – im Falle e-Voting etwa beim Wähler – abläuft. Nur so kann das Stimmgeheimnis beim e-Voting sichergestellt werden. Dies erfordert dann auch regelmäßig eine lokal ausgeführte Komponente, typischerweise ein Java Applet. Eine reine Web-Applikation, die am Server ausgeführt wird, und die die Daten (etwa den Stimmzettel) vom Browser des Benutzers erhält, kann – *unabhängig vom eingesetzten kryptographischen Wahlprotokoll* – das Stimmgeheimnis niemals sichern, da ja der Server (und damit auch ein frauduleuser Administrator) diese Daten sehen und abgreifen kann.[24] Damit fällt diese lokal exekutierte «Hälfte» des kryptographischen Protokolls rein räumlich grundsätzlich immer unter das WA.

3. Ausnahmen zur WA-Liste, Abschnitt 5.A, Teil 2

3.1. Systembezogene Ausnahmen

Kategorie 5, Teil 2 beginnt mit einer Serie von vier «Notes», die die nachfolgenden Bestimmungen relativieren, wobei **Note 1** beim Übergang zwischen WA-Liste 2014 auf 2015 aufgelassen wurde. Note 1 betraf bis 2014 «embedded» Funktionen, die Abschnitt 5.2 unterzogen wurden, obwohl sie an eine bestimmte Hardware gebunden sind. Dies betrifft wohl vor allem Funktionen des Internet of Things. Per 2015 wurde diese Note nicht mehr aufrechterhalten.

Note 3.a ist eine weitere systembezogene Ausnahme. Sie betrifft der Öffentlichkeit allgemein zugängliche Systeme, die «over-the-counter» oder im (auch rein elektronischen) Versandhandel erhältlich sind und deren kryptographische Funktionen für den Nutzer nicht einfach zu verändern und für den Nutzer einfach zu installieren sind (Note 3.a). Zusätzlich wird noch in einer Anmerkung zu Note 3.a (und auch der im Folgenden behandelten Note 3.b) als Kriterium verlangt, dass das System für eine breite Öffentlichkeit von Interesse ist sowie Preis und Information über die hauptsächliche Funktionalität für den Kunden ohne Anfrage beim Hersteller bekannt sind.

Es sei erwähnt, dass nach Meinung des Autors durchaus starke kryptographische Systeme – bis hin zur Quantenkryptographie – unter Note 3.a fallen können. Ein starkes System für die Verschlüsselung von Daten etwa kann durchaus im elektronischen Versandhandel vertrieben werden, seine Funktionalität kann fix und für den Kunden nicht veränderbar sein und es kann absolute Klarheit über Funktion und Preis des Produkts beim Kun-

[21] Vgl. die Verfahren nach Prosser/Müller-Török, E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. Wirtschaftinformatik, 6, 545–556 sowie nach Fujioka/Okamoto/Ohta, A practical secret voting scheme for large scale elections. In Advances in Cryptology – AUSCRYPT «92, 1993, 244–251 sowie jeweils darauf aufbauenden Protokollen und Implementierungen. Zur blinden Signatur vgl. Chaum, Blind signatures for untraceable payments, Advances in Cryptology Proceedings of Crypto 82 (3), 199–203.

[22] Vgl. Schoenmakers, A Simple Publicly Verifyable Secret Sharing Scheme and its Application to Electronic Voting», Lecture Notes in Computer Science Vol. 1666, 148–164.

[23] Siehe auch die animationsgestützten Einführungen in http://www.wu.ac.at/evoting/e-votingsysteme/e-voting-prozesse-und-angriffe/.

[24] Vgl. dazu die Darstellung in Prosser/Müller-Török, E-Voting: Lessons Learnt. In: *Kaplan/Balci/Aktan/Dalbay*, International Conference on eGovernment and eGovernance, Ankara, 2009, 265–280.

den herrschen. Das Interesse der breiten Öffentlichkeit kann vorausgesetzt werden. Etwa ein aus dem Internet im Wege des Downloads bezogener Internetbrowser würde mitsamt seiner TLS-bezogenen kryptographischen Funktionalitäten nach Meinung des Autors Note 3.a erfüllen. Die einzige Unsicherheit bezieht sich auf die Einschränkung zu Note 3.a auf *gekaufte* Produkte[25] – ein Browser steht heute üblicherweise im Gratisdownload zur Verfügung. Ob Smart Card-basierte Systeme auch unter Note 3.a fallen, wäre getrennt zu klären.

Gemäß **Note 3.b** sind Hardwaresysteme und «executable software» unter bestimmten Bedingungen weitgehend ausgenommen, vor allem wenn die kryptographischen Funktionalitäten unveränderbar sind und der Gegenstand des Systems nicht Informationssicherheit ist. Diese Freigabe aus Note 3.b wird allerdings durch eine weitere Note zur Note eingeschränkt: «'Executable software» does not include complete binary images of the «software» running on an end-item.» Der Autor ist sich nicht sicher, wie diese Formulierung einzuordnen ist. Jede «executable software» ist letztlich ein Image des Originals, das auf eine entsprechende Hardware – sei es eine frei bespielbare Hardware oder in Form eines embedded Systems – installiert wird. Man kann vermuten, dass hier die Kopie eines solchen executable Systems auf einer Dritthardware («end-item»?) gemeint ist – allerdings stellt sich dann die Frage, warum man das in der WA-Liste nicht auch so formuliert hat. Für die gegenständlichen Fragestellungen ist Note 3.b jedenfalls ohne Belang, da sie wie erwähnt nur für Systeme ohne Zweck der Informationssicherheit gilt.

Note 4 definiert eine Ausnahme für alle Systeme, deren Zweck nicht Informationssicherheit ist. Hier ergeben sich gewisse Redundanzen zu Note 3.

3.2. Nutzungsbezogene Ausnahme

Note 2 definiert anders als die im letzten Abschnitt erwähnten Freigaben eine anwendungsbezogene Freigabe, die auf den *ersten* Blick sehr weitgehend erscheint: «Category 5 – Part 2 does not apply to products when accompanying their user for the user's personal use.» Definitiv ist damit der klassische Reisende umfasst, der beispielsweise seine österreichische Bürgerkarte samt Software und Lesegerät in die VR China mitnimmt.[26] Ob dies auch einen elektronischen Bezug (Update?) aus dem Ausland heraus bzw. durch über einen längeren Zeitraum im Ausland lebende Bürger umfasst, darf bezweifelt werden. Auch der Aufruf einer Applikation, die entsprechende Komponenten enthält – beispielsweise eines Java-Applets zu e-Voting, das eine RSA-basierte blinde Signatur implementiert, erscheint höchst fragwürdig, da hier kein «accompanying their user» vorliegt – der Nutzer ruft das Applet vielmehr aus dem Ausland heraus auf und hat es bei Einreise nicht dabei.

4. Wassenaar und Open Source

Die gesamten Restriktionen erscheinen allerdings im Zeitalter der Open Source-Bewegung insgesamt höchst zweifelhaft zu sein. Ein Beispiel mag dies illustrieren. Der Export eines adaptierbaren, im Source Code und dokumentiert vorliegenden Softwaresystems für AES 256 an ein nordkoreanisches Rüstungsunternehmen ist wohl von des Restriktionen des WA umfasst:

- Note 2 kann nicht ziehen, da kein «personal use» vorliegen wird;
- Note 3a zieht nicht, da es im Wesen des Source Code liegt, dass das System angepasst werden kann;
- Note 3b und 4 beziehen sich nicht auf Systeme zur Informationssicherheit;
- AES 256 liegt über der 56bit-Grenze in 5.A.2.a.1.a.

[25] «… by being sold, without restriction, from stock …»

[26] Unbeschadet allfälliger Import- und Nutzungsrestriktionen im Zielland, man vergleiche nur die chinesische State Council Directive 273 – dies ist aber ein anderes Themenfeld und wird gesondert abzuhandeln sein.

Am Beginn der WA-Liste gibt es zwei «General Notes» zu Software bzw. Information Security Items:

- Die General Software Note definiert drei Ausnahmen für Softwaresysteme, für die das WA nicht gilt, eine davon ist Software «in the public domain». Während die beiden anderen Ausnahmen in dieser Note explizit nicht für Systeme unter Kategorie 5, Teil 2 (Information Security) gelten, liegt diese Einschränkung für die Freistellung der Public Domain nicht vor. Dies würde darauf hindeuten, dass Open Source-Systeme nicht vom WA umfasst sind.
- Die unmittelbar darauffolgende General Information Security Note hingegen legt fest, dass alle Systeme die unter Kategorie 5, Teil 2 fallen, ausschließlich nach den dortigen Bestimmungen – *also auch ohne die vorherige General Software Note* – gelten. Kategorie 5, Teil 2 sieht keine Public Domain-Ausnahme vor.

Der Autor sieht sich nicht im Stande, sich hier eine finale Meinung zu bilden, die Freistellung von Open Source-Systemen erscheint jedenfalls im besten Fall prekär. Unbeschadet dessen kann die oben erwähnte AES-Implementierung im Source Code von Hunderten Open Source-Seiten bezogen werden. Dies zeigt, dass hier das WA von der Entwicklung vollkommen überholt ist, wie auch immer die erwähnten Notes zu interpretieren sind.

5. Fazit

Die Nutzung kryptographischer Systeme jenseits eines standardisierten Web Browsers außerhalb des Wassenaarer Raumes kann zusammenfassend als höchst prekär bezeichnet werden. Ohne Note 2 wären qualitativ hochwertige e-Democracy-Applikationen definitiv nicht freigestellt und selbst die Nutzung der digitalen Signatur wäre fraglich. Note 2 ist allerdings wie angemerkt aufgrund der Einschränkung «accompanying their user» mit höchster Vorsicht zu betrachten; sie setzen wohl voraus, dass der Nutzer diese Komponente bei der Einreise bei sich hat und nicht erst aus dem Ausland heraus – zwecks dauerhafter Installation oder temporärer Nutzung – aufruft.

Insgesamt ergibt sich hier ein überstaatlicher Regelungsbedarf, um den prekären Charakter der Nutzung derartiger Komponenten zu beenden und auf eine rechtlich gesicherte – und für den Nutzer risikolose – Grundlage zu stellen.

Abschließend empfiehlt es sich für die EU-Kommission zu einer redundanzfreien und konsistenten Abstimmungsmethode mit der WA-Liste zu gelangen.