Conformance Testing a Set of Criteria for Assessing Trust

Omar Batarfi
School of Computing Science, Newcastle University, Newcastle upon Tyne, UK
Email: Omar.Batarfi@ncl.ac.uk

Lindsay Marshall
School of Computing Science , Newcastle University, Newcastle upon Tyne, UK
Email: Lindsay.Marshall@ncl.ac.uk

***Abstract*—The ability to authenticate the identity of an entity in an open and insecure environment such as the Internet plays an important role in reducing potential threats and Public key Infrastructure techniques assist in verifying the identity of entities participating in online transactions. A Certification Authority (CA) issues certificates to entities and vouches for the identity embodied in them. These certificates inherit their trustworthiness from the fact that their issuer is a known (trusted) CA. We have developed criteria for authenticating an entity's identity when there is no trusted CA (untrusted domain) to vouch for the trust embodied in a certificate. This paper describes conformance testing of the criteria we developed; the ultimate objective of this being to show their efficiency and robustness.**

***Index Terms*—certificate, criteria, CA, criterion, subject, CP**

I. Introduction

Our paper "Defining Criteria for Rating an Entity's Trustworthiness Based on Its Certificate Policy" [1] defines a set of requirements and some criteria that meet them. The motivation was to allow the relying party to examine the Certificate Policy (CP) of a subject certificate in an untrusted domain, and based upon that, the relying party will be able to decide the degree of trust that can put in the subject's certificate.

The approach started with developing a formalisation method for describing CPs, and the preliminary work is described in [2]. We found that applying what was defined there will produce nonidentical representations for CPs that were formalised which would lead to inefficiency when we applied the comparison process between them. We realized that identical representations could be obtained by defining certain criteria with the same name in all the CPs' formalisations but differing in their values.

With applying this technique, we have defined 43 criteria. A filter process was applied to decrease the number of criteria to 27. The scope of these criteria covers crucial issue for rating the trustworthiness of the subject. These criteria have to be applied to the subject's CP in order to show the compliance of the subject's CP with these criteria.

In this paper, we examine these criteria, demonstrating how they handle the articles identified by the Commission of the United Nations in the law of international trade (UNCITRAL Model Law on Electronic Signatures). The following table shows the 27 criteria:

TABLE I.
THE 27 CRITERIA

Number	Criteria
1	Liability and capability of the subject
2	Allowance for Registration Authority (RA) to issue certificate
3	Financial covering
4	National law enforcement
5	Dispute reference
6	Service assessment
7	Frequency of service assessment
8	Action on deficiency
9	Confidentiality of personal information
10	Authentication of organization identity
11	Authentication of individual identity
12	Knowledgeable subject
13	CRL update interval time
14	Validity period of a CRL
15	Comprehensive security audit
16	Security audit log examination
17	Vulnerability assessment
18	Archiving procedure
19	Disaster recovery plan
20	Trusted roles
21	Personnel controls
22	Subject keys
23	Private key length
24	Keys validity period
25	CA machine security
26	Hardware and software integrity
27	Network security

II. Analysis On Uncitral Model

The UNCITRAL Model Law on Electronic Signatures [3], hereafter referred to as UNCITRAL law, was created by the United Nations to further the progressive harmonization and unification of international trade law and in this respect considers the interests of everyone, in

particular those in developing countries so as to guarantee more extensive development of international trade. In addition, it aims to ensure legal security in the context of the broadest possible use of automated data processing in international trade.

By using the UNCITRAL law to test the criteria we have developed, we aim to see the convergence of the criteria and the degree of their effectiveness with respect to what has been defined in the UNCITRAL law which contains 12 articles:

Article 1. Sphere of application
Article 2. Definitions
Article 3. Equal treatment of signature technologies
Article 4. Interpretation
Article 5. Variation by agreement
Article 6. Compliance with a requirement for a signature
Article 7. Satisfaction of article 6
Article 8. Conduct of the signatory
Article 9. Conduct of the certification service provider
Article 10. Trustworthiness
Article 11. Conduct of the relying party
Article 12. Recognition of foreign certificates and electronic signatures

First we must clarify four points with respect to the implementation of the UNCITRAL law in our testing:

1. Digital signature has as one of its functions validation of the identity of a user [4], which is the same as the scope of our criteria; therefore, it is reasonable to use the UNCITRAL law to test our criteria. Moreover, Article 2 of UNCITRAL law states the function of digital signature as follows:

   > *"Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;*

2. Some of the articles could not be used for testing because they are articles which provide interpretation and description of the UNCITRAL law. Table II illustrates the purpose of the articles and the reasons behind decision not considered some of them.

TABLE II.
ALL UNCITRAL'S ARTICLES WITH THEIR PURPOSES AND REASON TO NOT BE SELECTED

UNCITRAL law articles	**Purpose of the Article**	**Reason to exclude**
Article 1	Defines the scope of application of the law	Criteria application is Certificate Policy
Article 2	Giving the definition for a number of key terms	These definition are known
Article 3	Decides the acceptance of any electronic signature method that meets the requirement	Specific to electronic signature
Article 4.	Gives the interpretation of the law	Interpretation of criteria is clear
Article 5.	Allows variation by agreement	Not applied in the criteria
Article 6	Specifies the legal requirements for a signature	
Article 7	Makes the applicability of article 6	Not applied in the criteria
Article 8.	Establishes the responsibilities and obligations of signatory	
Article 9	Establishes the responsibilities and obligations of signatory	
Article 10.	Interprets the notion of trustworthy	
Article 11	Establishes the responsibilities and obligations of relying party	Not covered in the criteria
Article 12.	States recognition of foreign certificates and electronic signatures	Not applied in the criteria

3. There are a number of paragraphs or factors in the articles that we either consider as fundamental functions or are out of the scope of the criteria. In this case we will define their relation to the criteria or their pre-implementation in the CP.
4. There are a number of criteria applicable to more than one article; we will relate the criteria to the most relevant article. By selecting this option we want to create 1-to1 link which leads to simple the process of comparison. We think that repeating list the applicable criteria with more than one articles will not add any significant.

III. CRITERIA EXAMINATION

A. Article 6. Compliance with a Requirement for a Signature

> *1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

Paragraph 1 specifies that a digital signature should have the same legality as a handwritten signature which leads us to consider whether a digital signature is as reliable as a handwritten signature. This case is a special rule applied only in the case of digital signature; it is not applicable to the case of certificates; so is out of the scope of our criteria.

> *2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.*

Paragraph 2 applies only to the case of a digital signature, and therefore it is also irrelevant to the criteria's scope.

> *3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;*

Paragraph 1 (a) is relevant when a subject requests a certificate, and the RA validates documents presented by the subject and makes sure that they belong to that subject. The paragraph refers to a fundamental task that is an early stage of the certificate issuing process, thus paragraph 1(a) is not covered by our criteria.

> *(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;*

What has been said about factor (a) is also true here.

> *(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and*

In the case of the certificate, the CA public key and the CP assists in detecting any alteration, in other words, they work as a validator for the certificate. This technique is considered an essential function of PKI, and the criteria will not cover this factor.

> *(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.*

A certificate validates a subject's identity, and in the case where there is any suspicious behaviour the owner of the certificate should easily discover it and revoke the certificate [5]. Our criteria concern the repository of the revoked certificates, the CRL, and they define the interval time that is need between CRL updates and the validity period of the CRL.

> *4. Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or*

Increasing the reliability of certificates is the main goal of a CA and this is achieved through compliance with the CP. There is no requirement on a CA to define or use anything that leads to an increase in the reliability of a certificate [6]. Our criteria examine a number of issues that are defined in the subject CP which yield an evaluation of the reliability of the subject certificate.

> *(b) To adduce evidence of the non-reliability of an electronic signature.*

This mechanism is guaranteed by the CP and allows for revocation or suspension of a certificate if there is any doubt regarding its validity.

B. Article 8. Conduct of the Signatory

> *1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall: (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;*

Two criteria deal with the subject CP practices for avoiding unauthorized use. Criterion 9 obliges a CA not to disclose subject certificate-related data to any third party, and criterion 22 requests a subject to generate its own key pair to avoid key compromise and unauthorized use.

> *(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if: (i) The signatory knows that the signature creation data have been compromised; or*

Factor (b) is one of the core functions of PKI [7], and it is an obligation on a subject to notify the CA immediately there is any compromise. The CA provides more information about carrying out this function in the CP in the section "Certificate Suspension and Revocation". If the CA's private key is compromised or suspected of being compromised, the CA shall inform subjects and relying parties, and terminate the certificates and produce a CRL.

> *(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;*

The CP contains different security practices that help show any violation in using certificates and that will result in the revocation or suspension of the violated certificate.

> *(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.*

Certificates are issued by a CA after it validates the subject data, and this remains true through the lifecycle of the certificate. In other words, if the data related to the certificate becomes inaccurate, the CA immediately suspends the subject certificate.

> 2. *A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.*

In the case of a certificate, this request is satisfied when the subject accepts the provisions of the contract before the issue of the certificate [8]; our criterion 12 requires that subjects should be fully informed of their rights and obligations.

C. Article 9. Conduct of the Certification Service Provider

> 1. *Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall: (a) Act in accordance with representations made by it with respect to its policies and practices;*

Criterion 6 shows if the CA is in compliance with what has been stated in the CP by performing an assessment called a "compliance audit".

> *(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;*

Our criteria meet the contents of paragraph 1 (b) with a number of criteria that test a CA's policies and practices which it operates throughout the lifecycle of its certificates to ensure accuracy and reliability. These are:

- Criterion 1 checks the liability and capability of the future CA, known as a subordinate CA, in performing all the controls and checks detailed in the CP.
- Criterion 2 restricts the issuing of a certificate only to the CA and prohibits an RA from doing this.
- Criterion 15 requires a comprehensive security audit.
- Criterion 16 asks for periodical review and analysis of audit logs.
- Criterion 17 requires vulnerability assessment.
- Criterion 19 asks for a disaster recovery plan.
- Criterion 22 restricts the issuing of subject keys to the subject.
- Criterion 23 defines a minimum length for the subject's private key.
- Criterion 24 specifies the validity period for private and public keys.
- Criterion 25 sets rules for protecting the CA system.
- Criterion 27 defines procedures for securing networks.

> *(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate: (i) The identity of the certification service provider;*

The identity of the CA is readily determined from the certificates that it issues and from its CP.

> *(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;*

Basically, a certificate will not be issued if the RA finds any deficiency related to the subject data.

> *(iii) That signature creation data were valid at or before the time when the certificate was issued;*

The previous sub-paragraph clarification also applies here.

> *(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise: (i) The method used to identify the signatory;*

This request is specified in the CA's CP, and our criteria accept two identification methods. First to identify the organization, is covered by criterion 10 and the second specifies the identification method for the individual subject and is covered in criterion 11.

> *(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;*

Any limitation on the use of the subject certificate is easily determined from the certificate. The criteria will apply if the certificate is not restricted to purposes which the CA has specified.

> *(iii) That the signature creation data are valid and have not been compromised;*

The RA function is one of the trusted roles, and it checks the subject's data to make sure of its validity before a CA issues the subject's certificate.

> *(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;*

The CA's CP explicitly declares any limitation or the extent of the CA's liability.

> *(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law;*

As we stated in paragraph 6.2.2 1 (b) above, this mechanism is essential to prevent malicious attacks; thus all CPs explain in detail how a subject carries this out.

> *(vi) Whether a timely revocation service is offered;*

A timely revocation service is offered by the PKI, and it is easy to check if this mechanism is offered by a CA by looking at its CP.

> *(e) Where services under sub-paragraph (d) (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 (b), of this Law and, where services under subparagraph (d) (vi) are offered, ensure the availability of a timely revocation service;*

Our criteria look at the availability of a timely revocation service using two aspects of the CRL. The first is the interval time needed for a CA to revoke a certificate and upload an updated version of the CRL (Criterion 13). Second, criterion 14, examines the validity period of the CRL.

> *(f) Utilize trustworthy systems, procedures and human resources in performing its services.*

The most important part of a CA is the personnel who perform the duties of CA or RA. Our criteria ensure the trustworthiness of a CA's personnel by examining two constraints; first, if the subject CP provides a separation of duties for critical CA functions known as "trusted roles"; this constraint is covered by criterion 20. Second, to check if personnel controls are adopted in the subject's CP and this constraint is met by criterion 21.

I. *A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.*

Criterion 4 considers National law as covering any agreement, and this means if the CA's CP does not cover this requirement, our criteria guarantee that National law complies at least with paragraph 2.

D. Article 10. Trustworthiness

> *For the purposes of article 9, paragraph 1 (f), of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors: (a) Financial and human resources, including existence of assets;*

The criteria meet this requirement through 3 which requests financial cover.

> *(b) Quality of hardware and software systems;*

This requirement is satisfied by criterion 26 which has the aim of maintaining hardware and software integrity.

> *(c) Procedures for processing of certificates and applications for certificates and retention of records;*

Procedures relating to certificates are fully described in the CA's CP, and these procedures are tested and audited by the CA to grantee their integrity. Our criteria are concerned with evidence in the case of legal disputes i.e. data archiving. Criterion 18 deals with this requirement.

> *(d) Availability of information to signatories identified in certificates and to potential relying parties;*

Information that addresses issues related to certificates is available to subjects and relying parties; this is outlined in the CP under the section titled "Publication and Repository".

> *(e) Regularity and extent of audit by an independent body;*

Criterion 7 defines the frequency of compliance audit carried out by an external body, and this constraint is specified in criterion 6 which is covered under article 9, paragraph 1 (a).

> *(f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or*

The result of the compliance test conducted by an external body will be declared according to the CP section titled "Communication of results". Our criteria require that when there are irregularities in complying with the CP an action should be taken: criterion 8.

IV. Results And Analysis

We have used the UNCITRAL law to examine the developed criteria and to summarize this assessment, table III shows the correspondence between the developed criteria and the UNCITRAL law articles:

TABLE III.
CORRESPONDENCE BETWEEN THE DEVELOPED CRITERIA AND THE UNCITRAL LAW ARTICLES

Developed criteria	**UNCITRAL law articles**
Criterion 1	Article 9, paragraph 1 (b)
Criterion 2	Article 9, paragraph 1 (b)
Criterion 3	Article 10 (a)
Criterion 4	Article 9, paragraph 2
Criterion 5	
Criterion 6	Article 9, paragraph 1
Criterion 7	Article 10 (e)
Criterion 8	Article 10 (f)

Criterion 9	Article 8, paragraph 1
Criterion 10	Article 9, paragraph 1 (d)
Criterion 11	Article 9, paragraph 1 (d)
Criterion 12	Article 8, paragraph 2
Criterion 13	Article 9, paragraph 1 (e)
Criterion 14	Article 9, paragraph 1 (e)
Criterion 15	Article 9, paragraph 1 (b)
Criterion 16	Article 9, paragraph 1 (b)
Criterion 17	Article 9, paragraph 1 (b)
Criterion 18	Article 10 (c)
Criterion 19	Article 9, paragraph 1 (b)
Criterion 20	Article 9, paragraph 1 (f)
Criterion 21	Article 9, paragraph 1 (f)
Criterion 22	Article 8, paragraph 1
Criterion 23	Article 9, paragraph 1 (b)
Criterion 24	Article 9, paragraph 1 (b)
Criterion 25	Article 9, paragraph 1 (b)
Criterion 26	Article 10 (b)
Criterion 27	Article 9, paragraph 1 (b)

Table III shows that criterion 5 does not link to any of the UNCITRAL law articles, and criterion 5 requires that there should be a dispute referee or arbitrator if there is any dispute arising between a CA and a subject. This requirement is met by the role and mission of the United Nations because one of the purposes of the United Nations is to play the role of arbitrator in solving international economic, social, cultural and humanitarian problems [9].

We conclude that the criteria have been defined adequately based on the fact that they handled all the relevant UNCITRAL law articles, and this implies that they have a basis in the law of international trade which can be considered as strong supportive evidence for the accuracy of the decisions made using the criteria when used for comparison.

V. Conclusion

In this paper, we have examined the criteria we developed to show, first, their extent in complying with requirements stated in international law and second, to measure their degree of effectiveness when comparing practices embedded in international law. As an example of international law, we used the United Nations Commission on International Trade Law (UNCITRAL) which defines a legal framework for using electronic signatures. We show that conformance testing which carry out in this paper concludes these criteria demonstrate their ability to handle the articles identified by the Commission of the United Nations in the law of international trade (UNCITRAL Model Law on Electronic Signatures).

References

1. Omar Batarfi and Lindsay Marshall. *Defining Criteria for Rating an Entity's Trustworthiness Based on Its Certificate Policy*. 2006 [cited.
2. Omar Batarfi and C.R.Snow. *An Approach to the Formalisation of a Certification Policy*. [PDF] 2005 [cited.
3. UNITED NATIONS. *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. [PDF] 2002 [cited.
4. James Currall. *Digital Signatures: not a solution, simply a link in the process chain*. [PDF] 2002 [cited.
5. closely Mitrakas. *GlobalSign CA Certificate Policy*. [PDF] 2005 [cited; Version 2.0:[
6. By Kien Keong Wong. *ELECTRONIC COMMERCE LAWS OF SINGAPORE AND MALAYSIA*. 1999 [cited.
7. Carl A. Gunter and Trevor Jim. *Generalized Certificate Revocation*. [cited.
8. Commonwealth of Australia. *Online authentication*. 2002 [cited.
9. United Nations Department of Public Information. *THE UNITED NATIONS: ORGANIZATION*. 2004 [cited; Available from: http://www.un.org/aboutun/basicfacts/unorg.htm.

Omar Batarfi is a PHD STUDENT at School of Computing, Newcastle University. His area of research is security in computer networks. Since he started his PhD in September 2002, he has published four conference papers. He has received his M.Sc. degree in computer science from George Washington University in 1996.

Dr. **Lindsay Marshall** is a SENIOR LECTURER in the School of Computing Science at Newcastle University. His researchs interests lie in several areas including e-learning, web development and anonymous systems. He has a BSc Hons from Edinburgh University and a PhD from Newcastle University.