A Semantic Model for the Validation of ePassport Certificate Chain of Trust

Elwaleed Elmana, Hind Zantout, Hani Ragab Hassen
School of Mathematical & Computer Sciences
Heriot-Watt University
Dubai, UAE
Email: Eke1@hw.ac.uk
Email: H.Zantout@hw.ac.uk
Email: H.Ragabhassen@hw.ac.uk

***Abstract*—Chip-enabled passport (ePassport) data is secured by Public Key Infrastructure (PKI) Digital Certificates to validate that the digitally signed data has not been tampered with, thus creating trust. Border ePassport verification processes in place are diverse; each country defines its own rules taking into account the International Civil Aviation Organization (ICAO) published recommendations. This project attempted to represent the ePassport PKI domain and its related policies using semantic technologies based on the Resources Description Framework (RDF) and the Web Ontology Language (OWL). The objective is to help border authorities rely on a standardised and unified trust classification process. The ontology was built using Protege following the Ontology Development 101 Methodology. The results show that not only can the PKI certificate chain be represented, but also the related certificate policy and practice statement. Semantic Web Rule Language (SWRL) rules successfully managed to represent essential aspects of the borders validation policy. The pilot demonstrates that a reliable implementation to automate the trust level classification process is achievable.**

Keywords-ePassport; PKI; Border Control; Semantic Technologies.

I. INTRODUCTION

The introduction of chip technology into the identification document domain enabled passport and national ID documents with increased security features. The chip contains all the information printed on the document data page, and the relevant data is stored on the chip using encryption, making the document tamper-proof. The encryption methods applied to use Public Key Infrastructure (PKI) digital certificates, assuring that the document is not forged.

When travelers pass through a border checkpoint, a personal information and identification process takes place to verify that the passport holder information matches the data on the chip. This matching or authentication process utilises the biometric information stored on the chip, such as fingerprints or iris scans. Biometric authentication, however, is outside the scope of this paper. The validation process being considered here is the application of decryption mechanisms to read the data from the chip, something that includes managing a complex PKI system.

This border control validation process also has a political aspect to it as it depends on the general practice of a country's Certification Authority (CA) sharing the distributing digital certificates with the relevant authority in another country. The Country Signer Certificate Authority (CSCA) and the Document Signer (DS) certificates are crucial as they form a chain of trust. ICAO plays an important advisory role through its suggested roadmap and Public Key Directory (PKD) [1]. To date, the validation policies still vary from a country to a country despite the various recommendations and technical reports that aim to regulate how to trust a chip-enabled document, using protocols like passive authentication [1] [2]. However, the actual implementation on the ground will vary because verifying an electronic document involves not only checking the data on the chip against the real documents, but it also includes the verification of the trust level of the PKI system behind it. Therefore, a comprehensive solution must have a check of personal information and validate the trust level of the country's digital certificate. Also, it must automatically process both the Certificate Policy (CP) and Certificate Practice Statement (CPS) of the relevant CA. The CP and CPS will indicate how the CA is performing its duties.

We propose a solution that will use semantic technologies to create a system that can process both the digital certificates as well as the PKI policies relating to a travel document. The resulting decision support system will enhance the ability of the border control officer to determine the trust level of a travel document.

The rest of the paper is organised as follows. Section II reviews the literature on Machine Readable Travel Document (MRTD) and policies that govern the validation process with proposed solutions. Section III describes the objectives, requirements, and validation methods for the project. Section IV introduces the model, the design process, and discusses system capability. Implementation details are included in Section V, and the results are discussed in Section VI, followed by the conclusion and future work.

II. RELATED WORK

The ICAO recommendations are published in document 9303 [1], and several other regulators like The German Federal Office for Information Security (BSI) publish related technical reports [2]. Such publications advocate a general framework for the validation process and policies that include guidelines for trusting PKI certificates issued by other countries. These certificates should be distributed through verification means on the ICAO own PKD portal, or through bilateral exchange agreements between countries. Currently, the details of checking a travel document depend

 ISBN: 978-1-61208-738-2

on the practices in place in each state as well as existing collaborations between countries. Several studies tried to address the gap between the validation result and the trust decision of a travel document, by proposing a centralised service with frameworks that utilise the certificate path validation as a tool to achieve trust, along with other PKI elements like the CP, the CPS and the Certificate Revocation List (CRL). However, CP and CPS documents are written in a natural language like English or German, which means the involvement of a human interpreter is an essential part of the validation process.

We start by discussing the attempts to include the quality of the CP and the commitment through CPS during the PKI certificate validation process. We then review the work related to the semantic representation of the policies which is needed for an automated system.

Sato and Kubo [3] in their patent application classified CA policies based on their level of assurance, and the paper proposes a dynamic chain or trust validation using a single certificate policy service provider. It manages the CP lifecycle independent of its corresponding CA, by pre-registering CA based on their compliance with a regularly published CP/CPS and classifying the trust level based on their CP/CPS level of assurance. In a multi-country situation, this will require all countries to share their CP/CPS with the single certificate policy provider. Currently, this ideal scenario of all countries around the globe sharing this information is not in place and unlikely to be in place in the foreseeable future.

Roh et al. [4] provide a solution that involves a server which upon receipt of the object certificate to be validated, the certificate of a trusted certification authority and the certificate policy proceeds to create a certification path for the object certificate as a first stage. If it is valid, it continues to the next step of validating the certificate path itself. This method was applied for as a patent in 2004.

Another ongoing research track investigates how to represent PKI CP and CPS in a machine-readable format. As described earlier, the CP defines the applicability of the CA certificate and the rules that govern it. The CPS describes in detail how the CA certificate has been managed and includes specifics of the issuing, the distribution and the revocation of a CA certificate [12]. The representation of the underlying rules is an essential step towards an automated system that can process both the PKI certificates as well as their policies.

Smith [5] worked on a Computational Framework for Certificate Policy Operations, using a machine-readable language to represent the CP elements as an object identifier. It based the CP representation on an encoding technique called “Canonical Text Services Uniform Resource Name (CTS-URN)", which provides the advantage of a validation system to read a semi-machine-readable CP without human interaction.

Grill [6] modelled X.509 Certificate Policies using Description Logics, his paper divided their approach, which used an ontology to represent policies into three stages.

1) Defining the domain schema classification or the taxonomy.
2) Having a reference ontology for usability purposes.
3) Working on the specific policy elements with an approach to compare CPs rather than to infer from them.

However, there were no proposals to include functionality that supports both the processing of the PKI certificate and their respective policies. Grill’s use of descriptive logic shows the potential role that semantic technologies can play in representing the PKI domain. The fact that the semantic technologies stack is built with security in mind and uses digital certificates as a means of trust can be leveraged to that end.

In our proposed solution, the RDF representation gives us the advantage to keep writing CP/CPS in a natural language while having rich metadata about the document that can be used by machines to evaluate the policy. Furthermore, OWL, coupled with rule-based reasoners, can provide a decision to trust or not to trust an MRTD based on predefined rules that reflect the actual practice in the real world.

The first step towards such a system is to build a knowledge-base that incorporates all the must-have elements of MRTD, PKI components, as well as the CP/CPS definition, and the border validation policy. Once the ontology that is comprehensive in nature is defined, it can be coupled with valuable inference rules and applied to specific instances. To do so, we followed the Ontology Development 101 Methodology [7] which enables the building of ontologies based on existing ones and uses the Certificate Ontology specification as outlined in the W3C standard as a baseline [8]. The domain knowledge is taken from MRTD regulator’s publications such as the ICAO Machine Readable Travel Documents Doc 9303 -part-11 [9] and Part-12 [1], as well as the BSI Technical Guideline BSI TR-03135 Machine Authentication of MRTDs for Public Sector Applications [10].

III. THE MODEL REQUIREMENTS AND DESIGN

The primary objective of the proposed system is to answer questions related to how countries can develop an MRTD local border verification policy. The solution will have to incorporate the root certificate CSCA, document signers, together with their policies and practices statement. This can be achieved by building an ontology-based model that captures elements of the border validation process based on the current recommendation and best practice of border control validation policies and procedures.

The knowledge-base will represent the CSCA certificate policy along with DS certificates and ePassport chip Document Security Object (SOD) elements using OWL coupled with SWRL rules, a combination that provides rich vocabulary and a full inference capability [11]. The Protégé reasoner will be used to verify the ability of the rules in creating a model that can deliver a reliable trust decision capability.

In the design phase, we recap what we highlighted in Section II, the need for a system that is capable of processing PKI certificates and their respective policies. Figure 1 depicts the general framework design. In the first stage, the passport document Security Object SOD that contains a hash of all the data groups and the associated DS is processed. In

 ISBN: 978-1-61208-738-2

the second stage, the data is prepared in a format that is compatible with the knowledge base. The preparation process is not within the scope of this paper. However, we assume that the data is RDF/OWL compatible. The third stage consists of applying an inference engine like Protégé DRool with the capability to run SWRL rules that will deliver the decision.

In Figure 2, we identify the concepts, properties, and relationships using the 101 Methodology. In that structure, the properties of the MRTD, CA, DS, and Policies were defined. For example, the main properties of the CP and CPS were listed based on Request for Comment (RFC) 3647 [12].

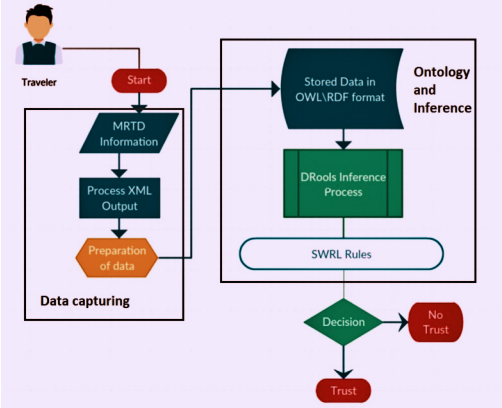

Figure 1. The Framework Design

In our work, the ontology is focused on answering the following four questions:

1) What is the type of the Document: is it an ID or passport?
2) Does the passport have a valid certificate chain or trusted path?
3) Does the passport root CA or CSCA have a trusted Policy?
4) Is the root CA or DS Trusted?

IV. Ontology Implementation

We used Protégé [13] as a primary tool to develop and validate the ontology. The tool provides a framework that has many add-on tabs that serve different functions such as the Entities tab where classes and their corresponding properties and individuals can be defined. In addition, Protégé provides integrated SWRL rules processing using the DRool extension as well as the option of using different reasoners.

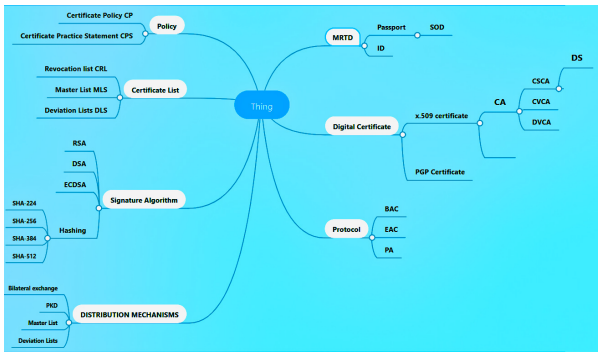

Figure 2. Concepts and Terms

For the system to answer the questions mentioned above, the knowledge base must include a sufficiently rich representation of concepts and their relationships to infer the required result correctly. A top-down approach is used to define the classes, object properties, and individuals. Figure 3 shows the main classes which are identified. An object property captures the relationship between classes and individuals [14] and can be used to specify the domain and the range [15]. In Table 1, the main pillars of the PKI are described and linked.

A. Use Cases Scenarios and SWRL Rules

We build the use cases to show that the ontology can simulate the current border validation scenario summarised below [10]:

1) The reader captures EMRTD information and uses BAC or PEAC protocols to access the chip.
2) Based on the document type information, it determines if it is a passport or ID.
3) Using the Passive Authentication protocol, it checks the digital signature of the DS.
4) The path validation checks if the DS has a valid CSCA signer or not.

When we add a new individual eMTRD instance to the system, the reasoner will be able to identify and classify it.

For example, the first primary use case will answer Question 1 above. Figure 4 shows the introduction of an individual with name Pass124 and has datatype property “hasPassportType” with value 3. The reasoner was able to identify that this individual is of class passport.

A more advanced use case is one where the reasoner had to process more than two classes with their various properties, to infer a result. In this complicated case, the system was able to answer Question 2 above.

 ISBN: 978-1-61208-738-2

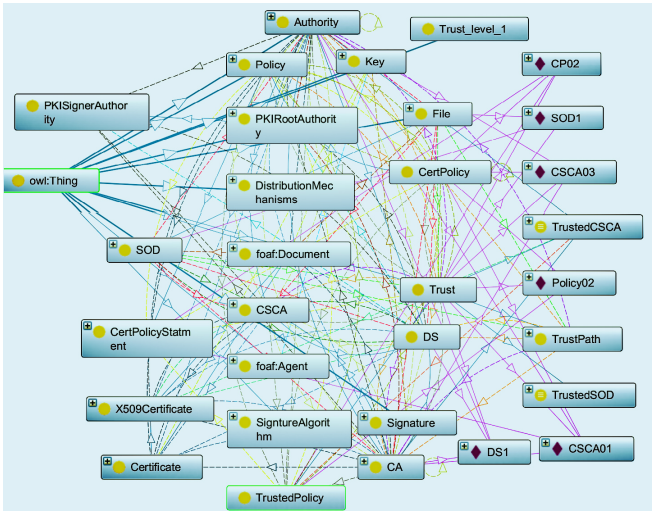

Figure 3. Main Classes

Here, an additional instance and its properties were identified as follow:

1) Add the instances Pass124 of class Passport, SOD1 of class SOD, DS1 of class DS, and CSCA01 of class CSCA to the knowledge base.

TABLE.1 OBJECT PROPERTIES

Object Properties		
Domain Class	**Object Property**	**Range Class**
Passport	AssociatedwithA	SOD
Digital Signature	CreatedBy	Private Key
Certificate	HasAKey Private Key and	Private Key and Public Key
CSCA OR DS	HasCertificateType	X.509Certificate
CSCA	RootCertificateType	X.509Certificate
DS	SignerCertificateType	X.509Certificate
SOD	HasSodIn	TrustPath
TrustPath	HasValidPathfrom SCATo	Policy
Domain Class	Object Property	Range Class
TrustPath	HasValidPathfrom DSTo	CSCA
TrustPath	HasValidPathfromSODTo	DS
SDO OR Certificate	Holds	Digital Signature
DS	IsKindOf	PKI SignerAuthoriy
CSCA	IsTypeOf	PKI RootAuthority
CSCA	Sign	DS
SOD	SignedBy	DS

2) Determine the instance to have general object properties CSCA01 Sign DS1, and SOD1 is Signed by DS1, and Pass124 AssociatedWith SOD1.

3) Define the main class called Trust, and a Subclass called Trusted path with Axiom:

(**HasValidPathfromCSCATo** Some Policy, and **HasValidPathfromDSTo** Only CSCA, and **HasValidPathFromSodT**o DS).

In Figure 5, the reasoner inferred that only the individuals SOD1, DS1, CSCA1 are part of the trusted path, although there were other individuals within the same domain.

The result of this use case as an example to prove that normal Protégé reasoner like HermiT and Pellet can give valuable outcome. Nevertheless, they were limited in that they cannot infer further results based on previously inferred results. Any result that is needed for further processing must be added as a new assertion to the knowledge base first.

B. *SWRL Rules*

The results obtained by the reasoned can also be reached using SWRL Rules. The SWRLAPI uses the DRool rule engine for inference purposes based on OWL 2 RL [13]. It uses the ontology as input, applies the rules, and returns inferred and asserted results.

Four rules have been developed using assumptions based on industry best practice. In a fully mature system, it is expected to have a much larger number of rules based on a formal written border validation policy.

1) Rule 1:

If a Document Signer signs a passport SOD, and a CSCA signs that Document Signer, then this passport component belongs to a Trusted Path class. Rule (1) shows the SWRL representation.

$$Passport(?P) \wedge SOD(?S) \wedge SignedBy(?D,?S) \wedge CSCA(?C) \wedge Sign(?C,?D) \Rightarrow TrustedPath(?P) \quad (1)$$

2) Rule 2

If a CSCA certificate was distributed through a mechanism such as ICAO PKD and found to have some properties like a Trusted Policy, a signature algorithm of type ECDSA, and a signature hash algorithm of type SHA 256, then this CSCA certificate can be classified as Trusted CSCA.

Figure 6 shows the SWRL representation and result of Rule (2).

$$CSCA(?C) \wedge TrustedPolicy(?TPO) \wedge HasLinkFromCSCATo(?TPO,?C) \wedge HasCSCASignAlgorithm(?SA,?"ECDSA") \wedge HasCSCADistributionMechanism(?DM,"PKD") \wedge CSCASigntureHashAlgorithms(?SHA,\text{sha256}) \Rightarrow TrustedCSCA(?C) \quad (2)$$

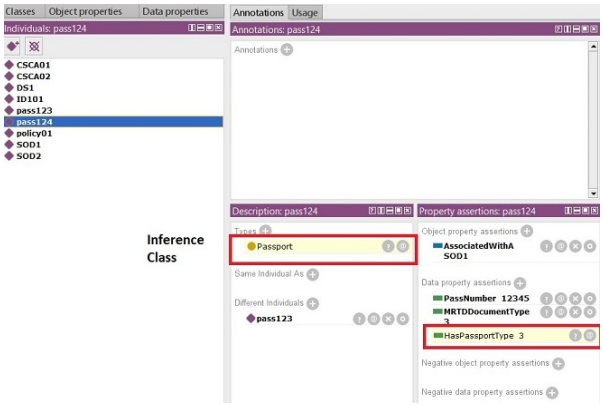

Figure 4. Inference class of use case one

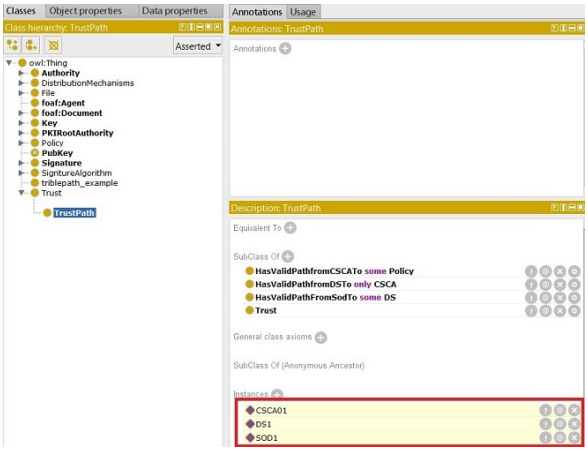

Figure 5. Inferred Trusted Path Class members

3) Rule 3

If a policy CP or CPS is found to have a CRL Issuing Frequency of 2 weeks, and a rigorous Certificate Rekey process, as well as a publication frequency of 3 months, then it can be classified as a Trusted Policy.
Rule (3) shows the SWRL representation.

$$Policy(?PO) \wedge PolicyPropCRLIssuingFreq(?CRLIF, "2weeks") \wedge PolicyPropCertRekeyProcess(?CRKP, yes) \wedge PolicyPropPublicationFreq(?PF, 3months) \Rightarrow TrustedPolicy(?TP) \quad (3)$$

4) Rule 4

This rule depends on the result of previous rules. The aim here is to classify the CSCA of a country based on their trust level. If a CSCA certificate is a member of a Trusted path class, and a Trusted CSCA class, in addition to having a Trusted Policy class and a trusted SOD class, then this CSCA belongs to a Trust level 1 class.
Rule (4) shows the SWRL representation.

$$TrustPath(?P) \wedge TrustedCSCA(?C) \wedge TrustedPolicy(?PO) \wedge TrustedSOD(?TSOD) \Rightarrow TrustLevel1(?C) \quad (4)$$

V. RESULTS AND DISCUSSION

The evaluation of the work is based on cross-checking the ontology against the most important criteria such as consistency and coherence, clarity and modularity and reusability. These are defined by the Ontology Quality Evaluation and Requirements Framework (OQuaRE) [16].

A) Consistency and Coherence

1) Protégé has set of reasoners and Debugger tools, which run through the Ontology axioms, object properties, and data properties to infer result. The Debugger run over 837 axiom and the result is "The ontology is consistent and coherent".

2) We used The Ontology Pitfall Scanner developed by the Ontology Engineering group [17], as a comprehensive online tool that checks the consistency. The result showed the existence of critical cases related to using multiple domains or ranges in properties, and some crucial cases due to the use of recursive definitions, which refer to the use of a class name within its equivalent class axiom. As this was only detectable after the DRool inference result, we believe that it is due to Protégé internal ontology processes, and it should not harm the original ontology structure.

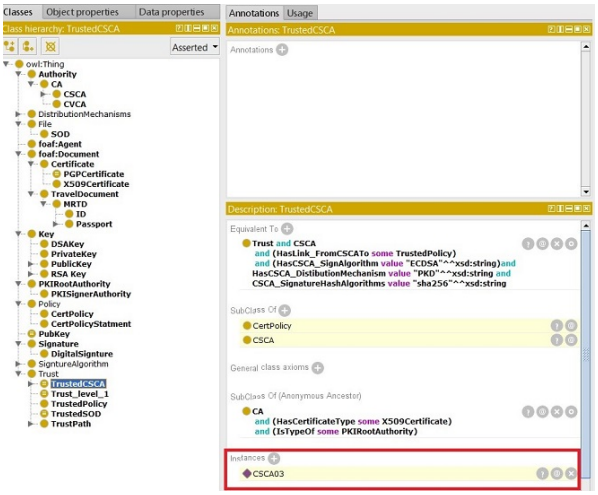

Figure 6. Inference of trusted CSCA

B) Clarity

The OntOlogy Pitfall Scanner result for clarity shows only minor remarks, suggesting more annotation and a unified naming convention should be used. Further clarification of the annotation definition can be discussed with the domain experts.

C) Modularity and Reusability

The extendibility or modulatory criteria check depicts the level of change in the ontology that can be introduced without affecting the overall function. We used the following OQuaRE metrics:

 ISBN: 978-1-61208-738-2

The Weighted Count Method (WMCOnto) is a metric, which can be measured by calculating the average number of properties and relationship per class.

$$WMCOnto = (\Sigma|PCi| + \Sigma|RCi|/\Sigma|Ci|$$

Our ontology scored 0.45, which is considered very low comparing to well-defined Ontologies that scores between 5-11 [16].

The DITOnto is a reusability metric, which counts the maximum length of the path from the leaf to the ontology root point "Thing".

$$DITOnto = Max\,\Sigma|Ci|$$

The NOMOnto is another reusability metric that considers the number of properties per class

$$NOMOnto = \Sigma|PCi\,/\,|\Sigma|Ci|$$

The result of the DITOnto is 5. Moreover, NOMOnto is 0.36.

Comparing to the result of other well-defined ontologies that score between 2-8 on DITOnto and NOMOnto, the above result is an indication that the Ontology has its limitations concerning reusability.

VI. Conclusion and Future Work

With the model that we proposed and the ontology described, we were able to demonstrate that that ePassport PKI elements can be semantically represented, linked to relevant policies and classified based on Trust rules. Thus, a precise border control ontology-based validation procedure can be achieved. The ontology within the model can be considered as a core to an industry-ready solution, customizable to suit each border control authority rules and procedures. The initial knowledge base will need to be expanded with other countries' certificates. Combined with the semantic representation of the CP and CPS we believe it will make border classification process more transparent, in addition to helping border control authorities build an ICAO recommended Master List [1] through the PKD portal.

Although the ontology did not score highly in the technical evaluation process, however, we were able to answer all key four questions and reach the goal of having a decision to trust or not to trust a given eMRTD. The taxonomies captured were modest, and the border validation elements and rules were not comprehensive. Nevertheless, within the defined scope, the ontology was able to demonstrate the validity of the concept of CP and CPS representation using ontologies.

Finally, this approach closes a severe gap in providing a meaningful border control solution. The issue of how countries are maintaining their PKI CA and the issuing of DS certificates needs to be addressed in a structured way as proposed by this project.

This project can be considered as a base for the following future work:

1) The semantic representation of the CP and CPS elements, having both Policies entirely written in RDF/OWL means they can be processed by a system without the need of a human expert and can make ePassport PKI classification an automated process.

2) The current model using SWRL rules is only intended as a proof of concept. In a real-world situation, we expect a comperhensive list of rules that covers the ePassport border validation process and procedures.

References

[1] ICAO Recommendation 9303, "Machine Readable Travel Documents - Part 12: Public Key Infrastructure for MRTDs", Seventh Edition, 2015, INTERNATIONAL CIVIL AVIATION ORGANIZATION,[Online].Available:www.icao.int/Security/FAL/TRIP [Accessed: 06-Aug-2019].

[2] German Federal Office for Information Security, "Machine Authentication of MRTDs for Public Sector Applications Part 1: Overview and Functional Requirements," Bonn, 2017.

[3] H. Sato and A. Kubo, "Graded Trust of Certificates and Its Management with Extended Path Validation," Inf. Media Technol. J. Inf. Process., vol. 6, no. 19, pp. 980–990, 2011.

[4] Jong Hyuk Roh et al., "Method of Validating Certificate By Certificate Validation Server Using Certificate Policies And Certificate Policy Mapping In Public Key Infrastructure," " ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUT" 21-May-2002.

[5] G. A. Weaver, S. Rea, and S. W. Smith, "for Certificate Policy Operations", Public Key Infrastructures, Serv. Appl., vol. EuroPKI, 20, no. 2006, pp. 17–33, 2010.

[6] S. W Grill, "Modeling X.509 Certificate Policies Using Description Logics - Semantic Scholar," 2007. [Online]. Available: https://www.semanticscholar.org/paper/Certificate-Policies-Using-Description-Logics Grill/37fab24f8de082c7e3ff2e23879cf2979a610a99. [Accessed: 06-Aug-2019].

[7] N. F. Noy and D. L. McGuinness, "A Guide to Creating Your First Ontology," in Biomedical Informatics Reseach, 2001.

[8] W3C WebID Incubator Group, "The Cert Ontology Specification," 2008. [Online]. Available: https://www.w3.org/ns/auth/cert#PublicKey. [Accessed: 06-Aug-2019].

[9] ICAO Recommendation, "Machine Readable Travel Documents - 9303 Part 11," Montréal, 2015, INTERNATIONAL CIVIL AVIATION ORGANIZATION, [Online]. Available: www.icao.int/Security/FAL/TRIP [Accessed: 06-Aug-2019].

[10] BSI, "Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token-Part 1," 2015, BSI Publications [Online].Available:https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html.

[11] D. S. R. P.Hitzler, and M.Krötzsch, "Foundations Of Semantic Web Technologies", Taylor and Francis Group, 2010.

[12] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," 2003.

[13] stanford.edu, "Protege 3.5 Release Notes - Protege Wiki." [Online]. Available: https://protegewiki.stanford.edu/wiki/Protege_3.5_Release_Notes. [Accessed: 06-Aug-2019].

[14] J. D. Allen and Unicode Consortium., "The Unicode standard 5.0", Addison-Wesley, 2007.

[15] U. Prot et al., "Tutorial Protege OWL," Copyr. C Univ. Manchester, March 24, 2011.

[16] A. Duque-Ramos, J. T. Fernández-Breis, R. Stevens, and N. Aussenac-Gilles, "OQuaRE: A square-based approach for evaluating the quality of ontologies", J. Res. Pract. Inf. Technol., vol. 43, no. 2, pp. 159–176, 2011.

[17] Ontology Engineering group, "OOPS! - OntOlogy Pitfall Scanner!Results."[Online].Available:http://oops.linkeddata.es/response.jsp. [Accessed: 21-Nov-2018].

 ISBN: 978-1-61208-738-2