Static evaluation of Certificate Policies for GRID PKIs interoperability

Valentina Casola, Nicola Mazzocca
University of Naples, Federico II,
Dipartimento di Informatica e Sistemistica
Naples, Italy
{casolav,n.mazzocca}@unina.it

Jesus Luna, Oscar Manso, Manel Medina
Universitat Politècnica de Catalunya
Computer Architecture Department
Barcelona, Spain
{jluna, omanso,medina}@ac.upc.edu

Massimiliano Rak
Second University of Naples
Dipartimento di Ingegneria dell'Informazione
Aversa (CE), Italy
massimiliano.rak@unina2.it

Abstract

Validating an end-entity X.509 digital certificate prior to authorizing it for using a resource into the computational Grid has become a widely studied topic due to its importance for security. A more comprehensive validation process involves not only a real-time check on the credential's status, but also an evaluation of the trust level applicable to its Certification Authority. Nowadays Policy Management Authorities (PMAs) gather Grid CAs fulfilling a minimum set of requirements defined in an Authentication Profile thus guaranteeing a trusted interoperability environment for Grid projects. Currently this is a manual process that only results in a binary decision (the CA is able to become part of the PMA or not), however in practice, different CAs offer different security levels.

In this paper we present ways to apply the Reference Evaluation Methodology (REM) to automatically obtain the security level of a CA. The described process is based on the building of a formalized policy template for Grid Certificate Policies. This methodology has been used to evaluate the security level offered by a set of EUGridPMA's CAs; the obtained results are then conveyed to relying parties using an infrastructure composed of CertiVeR's Validation Service and the Open GRid Ocsp (OGRO) middleware for the Globus Toolkit 4, thus providing enough information for a comprehensive certificate validation decision.

1. Introduction

In the last years, security research activities in the computational Grid context have been focused on the definition of infrastructures that enable Single Sign On (SSO) mechanisms to access distributed resources that belong to, and are administrated by, different and independent domains. SSO mechanisms allow an end user to authenticate upon his first access to a resource and let him use those verified credentials for the following accesses to resources that belong to different machines in the same Virtual Organization (VO). From a security point of view, this problem is faced first of all by adopting Authentication and Authorization (AA) systems, implemented in different ways that include organizational and technical procedures described by policies, and security mechanisms enforcing them.

Lately it is a common approach to demand authentication-related operations to external Authorities that act as Trusted Third Parties (TTP). Specifically in Grid contexts, available solutions are based on the adoption of Public Key Infrastructures that enable the implementation of authentication and authorization mechanisms on the basis of X.509 digital certificates issued and signed by Certification Authorities (CA).

The VOs require the use of certificates that are trusted by all the involved parties, each one of them issued by their home institution's Certification Authority. These cryptographic credentials are the basis not only of entities authentication (end-users and machines), but also of job delegation mechanisms and even of further authorization processes.

As Grid computing became more popular also VOs proliferated at the same rate, and this finally resulted in the breed of several Certification Authorities (a common practice as each organization installing a Grid environment was also used to define its own Certification Authority). Soon this represented a big interoperability problem between the users and resources belonging to different institutions: their computing resources where in different domains, but the need of cooperation through a Grid environment required to share them all.

A suitable solution for this problem was given by the Policy Management Authorities (PMAs) which define a minimum set of security provisions (in the form of an Authentication Profile as in [1]) that must be accomplished by all the Grid-PKIs wishing to interoperate between them. Three regional Grid PMAs currently exist around the globe (Europe's EUGridPMA [2], America's TAGPMA [3] and Asia-Pacific's APGridPMA [4]) and nowadays they are being harmonized and synchronized through IGTF, the International Grid Trust Federation [5]. In the case of these PMAs, compliance with their respective Authentication Profile is given through a well-defined, but mostly manual process involving a careful analysis of the applicant CA's Certification Policy (CP). This is performed just once when the new Grid-PKI wishes to be part of an existing PMA and it is commonly called the "accreditation process".

Even though all PMA's members Grid CAs must pass the accreditation process, not all of them accomplish the respective Authentication Profile on the same level. This information is very important to build trust relationships between Grid PKI's, and also for Authentication and Authorization processes, however to date there is no automatic way to obtain it.

The research presented in this paper is focused on the problem of building a technique aimed for PMAs to automatically perform the CA accreditation process by evaluating its Certification Policy and obtaining a security level for the Grid context. Afterwards this security level shall be conveyed and used by relying parties to enhance the process of validating any client submitting a job to the computational Grid. In this paper we propose the main components for validating digital certificates under these premises. These are:

- An evaluation methodology, based on the formalization of the CA's Certification Policy [6], to *i)* determine if a CA is compliant with the Authentication Profile defined by the PMA and *ii)* by defining a security metric to quantitatively compute a Global Security Level (GSL) representing how much better the CP's security provisions are when compared against the PMA's Authentication Profile.
- A Grid Validation Infrastructure extended from our previous research in [7] and able to convey the status and associated GSL of any end-entity certificate through the Online Certificate Status Protocol (OCSP [8]).

The technique proposed in this paper could be adopted both as a mechanism to help the PMAs in the Certificate Policy analysis during the CA's accreditation process, and to perform finer-grained validation decisions at Grid relying parties before authorizing any Grid client request. Due to its level of detail, most of this paper is focused on the evaluation methodology.

The remainder of the paper is structured as follows: in Section 2 we will review the PMA architecture, introducing both its technical and the organizational aspects. Section 3 will illustrate in detail the evaluation methodology and the Grid Validation Infrastructure. Then, in Section 4 we will present the formalization of EUGridPMA's Authentication Profile. Section 5 will illustrate the use of the proposed evaluation methodology by applying it to some CAs members of EuroGridPMA. Finally in section 6 we present our conclusions and future work.

2. THE ROLE OF THE GRID POLICY MANAGEMENT AUTHORITIES (PMA)

To provide a better view of the advantages given by our proposal, this section lists some details related with the PMA's architecture and procedures, mostly based on the practices developed by the EUGridPMA [9].

The PMA's Authentication Profile document describes the minimum set of requirements imposed on Certification Authorities (CA) that traditionally issue long-term X.509 credentials to end-entities, who will themselves possess and control their key pair and their activation data. These CAs act as an independent trusted third party for both subscribers and relying parties within the infrastructure.

In general, any CA requesting membership to a PMA must present its Certification Policy (CP) document which will be in turn evaluated by experts against a set of rules or minimum security provisions defined into the PMA's "Authentication Profile", thus determining whether it is fulfilled or not. Obviously a further auditing process could determine if in practice the CP itself is also being satisfied by the PKI.

According to our practical experience in this field, it is possible for all the Grid-PKI members of a certain PMA to not only fully satisfy the appropriate "Authentication Profile", but also to do so in different levels. Quantifying this "security level" may be useful

to take finer-grained validation decisions at the relying parties.

Let us take the following example to clarify our point of view:

Example 1. Suppose that both *PKIa* and *PKIb* are part of the same PMA whose Authentication Profile document requires an end-entities's private key minimum length of 1024 bits. On the other hand, *PKIa*'s CP states that its users own private keys of at least 1024 bits while PKIb's CP states a minimum of 2048 bits. Even though both PKIs fulfill the PMA minimum requirement, a certificate issued by *PKIa* may have a private key smaller than one issued by *PKIb*. In a broad sense of the word, it could mean that for this particular provision *PKIa* is less secure than *PKIb*. If the rest of the CP's provisions for both PKIs are exactly the same, the global security level of *PKIa* should be less than *PKIb*'s. Under these conditions a Grid resource owner may decide to give access only to users from *PKIb*.

To perform validation decisions as the one presented in the previous example, it is necessary to evaluate accurately the security distance between any Grid-CA's Certification Policy and a reference PMA's Authentication Profile.

The following section introduces our proposal for validating digital certificates in the computational Grid.

3. Validating digital certificates

To perform a comprehensive certificate validation process, it is necessary to query in real-time its status and evaluate the security level of the issuing CA. For the first task we will use a Grid Validation System able to retrieve the status of a digital certificate through OCSP in a CA federation; this system, composed of CertiVeR and OGRO, was developed at the Universitat Politècnica de Catalunya and introduced in [7]. Afterwards, for the evaluation of a CA, we will illustrate the Reference Evaluation Methodology (REM) developed by the University of Naples that is based on the formalization of a Certificate Policy to i) determine if this CA is compliant with the Authentication Profile and ii) define a security metric to quantitatively compute a global security level representing how much better the CP's security provisions are when compared to the Authentication Profile. Figure 1 presents the overall validation infrastructure, which will be further explained in the rest of this paper.

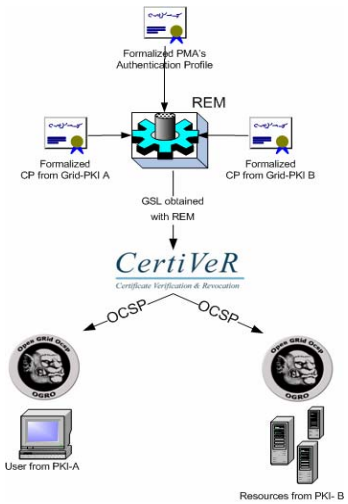

Figure 1. The validation architecture.

3.1 The validation architecture

A first step to validate a Proxy Certificate in the computational Grid requires to iteratively validate the end-entity and issuer's credentials until a trust anchor has been found; this process is often called Certificate Path Validation and traditionally involves looking up Certificate Revocation Lists (CRL) to ensure that these credentials have not been revoked. However, this solution tends to be cumbersome for both the CA and the application. In terms of the CA it is difficult to manage because it involves providing revocation information efficiently (in some scenarios near real time notification is a must). Also on the client side such a solution penalizes efficiency, because it is obliged to periodically download and parse the whole list of revoked certificates, which can be extremely large, in order to perform the validation process. In consequence, more efficient mechanisms to allow for the provision of near real time certificate status information to relying parties have begun to be adopted in some demanding environments, where highly efficient and secure solutions are required. Proposed in 1999 on RFC 2560 [8], the Online Certificate Status Protocol (OCSP) is one such mechanism, even though it poses very special requirements during its planning and deploying into the computational Grid, as documented in [10]. Such requirements have been fulfilled by the validation infrastructure shown in figure 1 thanks to the OCSP subsystem composed of the following two elements.

3.1.1 CertiVeR

It is an EU funded project [11] that offers a comprehensive validation service that, on top of providing status information of a X.509 certificate in real time through the Online Certificate Status Protocol

(OCSP) it also implements a CRL Updater module, which is in charge of retrieving revocation information directly from the CA's CRL through protocols like LDAP and HTTP. This information is stored in a local cache. Through a customizable set of extensions on the OCSP response, CertiVeR can report information at several levels, such as the global security level of a CA obtained through the REM evaluation technique.

For each organization member of the Grid's VO, CertiVeR's OCSP responder can be configured in trusted or authorized mode as defined in [8]. Finally fault tolerance (through replication techniques, backup sites and load balancers) and high performance (using cryptographic hardware) are also provided for those organizations requiring them.

3.1.2 OGRO

In previous work [7] we introduced the idea of an enhanced OCSP client for the Globus Toolkit 4, able to use CertiVeR for End-Entity certificate's OCSP path validation and also to request authorization information into OCSP extensions from such service. This client has evolved since then adopting several of the recommendation of the CAOPS-WG and now it has been published as open source with the name of OGRO (Open GRid OCSP [12]). By being Open Source and 100% Java, OGRO has been fully integrated into the Java Commodity Grid Kit [13] and the WSRF Grid Services Container (GT4's Java core). The OGRO API does not implement its own OCSP client classes; instead it relies upon well known JCE providers.

OGRO's main contribution for Grids is the use of a set of rules written in XML and called the Grid Validation Policy or simply GVP, which customizes relying parties' OCSP behavior in concordance with the recommendations given in [10]. The GVP, its structure (DTD) and rules have been thoughtfully explained in [14] and [15] and more than being a set of configuration directives, they represent a mechanism that contributes to enhancing relying parties' security level.

3.2 The CA evaluation methodology

In [6], [16] we have proposed a Reference Evaluation Model (REM) to evaluate and compare different security policies, quantifying both their global security level [6] and their compliance to a declared SLA (Service Level Agreement [17]).

In particular the REM is made of three different components:

1. *The policy formalization:* defines how to express a security policy in a rigorous way.
2. *The evaluation technique:* the process to evaluate a previously formalized policy.
3. *The reference levels:* denotes how to get a security level relative to a minimum policy used as reference

Next we are going to present at a coarse view how this methodology can be used to obtain the security level offered by a certificate policy. Further details on the REM are available in [6, 16, 18].

3.2.1 The policy formalization

Policies may be expressed in both, a formal or an informal way. Despite its advantages for automatic processing, a formalized policy is more difficult to manage and understand. So, security policies are often expressed in a simple, semi-formal way, but then again even though their structure is easier to understand, even for non technical people, they are still difficult to be automated. A formalized policy instance expresses in a rigorous way who, how and where security provisions will be applied. The way in which we formalize a policy depends strongly on the technique we intend to adopt.

3.2.2 The evaluation technique

Different evaluation techniques represent and characterize the security level associated with a security policy in different ways, for example with a numerical value [19], a fuzzy number [16] or a verbal judgment representing its security level. The REM includes a proprietary evaluation technique based on the definition of a metric policy space which allows the representation of policies as a homogeneous space on which we have defined a distance criteria and a metric function.

The main features of the homogeneous metric space could be summarized as follows:

- Any policy is formalized as a tree containing all the policy's provisions;
- Given any tree-policy formalization, the evaluation process only takes into account the provisions of the policy which are represented by the leaves of the tree structure.
- Our formalization represents each provision as an enumerative and ordered data-type; the policy space "*P*" which is defined as the vector product of all n provisions K_i i.e. $P = K_1 \times K_2 \times \ldots \times K_n$.
- The policy space "*P*" is been transformed into an homogeneous one, denoted "*PS*", thanks to a family of threshold functions (F-functions) which allows us to associate a Local Security Level (LSL for short) to each provision. This is an important step as it allows the evaluator to treat every element

from the CPS with equal importance.

- "*PS*" is represented by a *n x 4* matrix whose *n* rows represent the single provisions K_i and 4 is the chosen number of LSLs admissible for each provision (which is a very realistic value for Grids; [21] defines four certificate policies representing different assurance levels: rudimentary, basic, medium and high). For example, if the LSL associated to a provision called "Policy Applicability" is L_3, then the vector corresponding to its row in the matrix would be (1,1,1,0).
- The distance criteria, which will be used to define the Global Security Level, is the Euclidean distance among matrices, defined as:

$$d(A,B) = \sqrt{(\sigma(A-B, A-B))}$$

Where $\sigma(A-B, A-B) = Tr\left((A-B)(A-B)^T\right)$

To show that the distance just defined in fact represents the distance between the policies being evaluated, in figure 2 are shown 3 policies (*P*, *X* and *Y*) with 10 provisions each. *P* is then compared against *X* and *Y*, both are globally stronger than P since they have several provisions with a higher Local Security Level.

P =				*X* =				*Y* =			
1	1	0	0	1	1	1	0	1	1	1	1
1	1	0	0	1	1	1	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	1	0
1	0	0	0	1	0	0	0	1	1	0	0
1	0	0	0	1	0	0	0	1	1	1	0
1	0	0	0	1	1	0	0	1	1	1	1
1	0	0	0	1	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0
1	1	0	0	1	0	0	0	1	1	0	0
1	0	0	0	1	0	0	0	1	1	1	1

Figure 2. Comparing three policies with different LSLs.

The following conclusions can be drawn from the previous figure:

- Just by looking at the levels of the single provisions, *X* is a policy that is stronger than *P*. First we calculate:

$$Tr\left((Y-P)(Y-P)^T\right) = 6$$

So the distance between *X* and *P* is: *d*= 2.45

That mirrors the fact that *X* is just a little stronger than *P*.

- *Y* is a policy that is stronger than *X* and much stronger than *P:*

$$Tr\left((Y-P)(Y-P)^T\right) = 19$$

In this case the distance between Y and P is: d= 4.36 and this shows the evident security difference between the both policies.

The previous examples show that it is very simple to evaluate the distance between formalized security policies, once they have been represented as a matrix. The distance criteria will be adopted to define the metric function as explained next.

3.2.3 The reference levels

The last component of the REM is the set of reference security levels from a minimum policy, which can be used as a scale for the numerical evaluation of trustability. When these references are not available, the REM can be used for direct comparison among two or more policies as explained above.

At this point, in order to define the metric function we must represent the reference levels according to the REM's procedure and then proceed to evaluate the target policy against them. So, we first compute the distances among the different references (denoted as $REFL_i$) and the origin of the metric space (denoted as Ø) which is represented as $d_{REFLi,\phi}$

Finally, to evaluate the Global Security Level (GSL) associated to a target policy P_x we will adopt the following security metric function:

$$Lp_x = \begin{cases} L_0 & \text{iff } d_{x0} \le d_{10} \\ L_1 & \text{iff } d_{10} < d_{x0} < d_{20} \\ L_2 & \text{iff } d_{20} < d_{x0} < d_{30} \\ L_3 & \text{iff } d_{30} < d_{x0} < d_{40} \\ L_4 & \text{iff } d_{40} \le d_{x0} \end{cases}$$

Where Lp_x is the Global Security Level associated to P_x and $d_{i,0} = d_{REFLi,\phi}$ are the distances among the references and the origin of the metric space. This function gives a numerical result of the security level guaranteed by any CA; so, through the evaluation of the Certification Policy associated to this CA we are in reality measuring the GSL. Being an aggregated value, the GSL has a critical limitation: it is not able to take into account single provisions which could be more critical than others. To face such problems, we are working on the improvement of the REM evaluation technique by applying weights to provisions and introducing a constraint-vector by which could be guaranteed that during the evaluation even when the aggregated evaluation gives a high GSL, some critical provisions do not go under a desired threshold. For brevity's sake, we do not describe this improvement, but more details can be found in [20].

4. Policy Formalization

To evaluate the different Grid-PKI's CPs, first a Certification Policy Template must be produced representing a high-level abstraction or model for any of these documents. This section explains how this template was built in our research for the evaluation of Grid-PKI's CP.

We decided to use the "Global Grid Forum Certificate Policy Model" (GGF) [21] as the document upon which the REM's template could be built. This was not only because it is a common practice for the Grid community to use it for writing their own CPs, but also because all of the provisions from EUGridPMA's Authentication Profile [1] can be easily mapped to it.

Parsing the GGF's model CP into the form required by the REM is a thought process as it requires not only clearly identifying each one of the possible security-related provisions, but also organizing and placing them into the leaves of our fomalization tree. The first levels of this tree are precisely those defined in the RFC3647 [22]; this document is actually the most important reference to a Certificate Policy structure, so for the first level we have allocated the following sections:

1. Introduction,
2. General Provisions,
3. Identification and Authentication,
4. Operational Requirements,
5. Physical, Procedural and Personnel Security,
6. Technical Security Control,
7. Certificate and Certificate Revocation List (CRL) Profiles,
8. Specification Administration.

Second level provisions try to describe all the details regarding every macro-provisions by stating objects that despite their complexity, bring more security bounded information. Let us take for example the "Technical Security Control" provision which includes: "Key Pair Generation", "Private Key Protection", "Other Aspects of Key Pair Management", "Activation Data", "Computer Security Controls", "Life Cycle Technical Control", "Network Security Control" and "Cryptographic module engineering controls".

As was briefly explained in Section 3, we have formalized such policies to build a policy matrix space made of *n*-dimensions; each dimension representing a provision which can assume a finite number of values that are associated to different Local Security Levels. The remainder of this section briefly presents how to build a formal template that can be adopted to map the policy to evaluate. Interested readers may find further details on the formalization step in [18]. Table 1 shows some rows of the policy matrix obtained after applying the formalization step to the "Technical Security Control" provisions from the Global Grid Forum's Certificate Policy Model [21]. The second column of the table, represents the ordered[1] sets of all possible Local Security Levels (LSL) that were defined for each provision and according to our experience and common Grid community practices. For a better understanding of the information that can be extracted from the policy matrix, let us discuss the following example:

Table 1: provisions from "Technical Security Control"

Key pair generation and installation	generatedByCA<generatedByEntity
Private key delivery to Entity	EnclosedEnvelope<EnclodeEnvelopeSplittedBtPIN<OwnedByEEC

Example 2. For the provision called "Key Pair generation and installation" we have chosen | LSL | = 2, which represents the ordered values: *generatedByCA* and *generatedByEntity*. In this case it is feasible to think that a user-generated key-pair provides more privacy and security than a CA-generated key-pair, therefore the order relationship shown between them.

Once the template and assigned the corresponding LSLs are built, it is possible to proceed directly to evaluate the CPs from the Grid-PKIs just as explained next.

5. Evaluating Certificate Policies from EUGridPMA's Grid-PKIs

The goal of this section is to show the applicability of our validation methodology by using the policy matrix obtained in section 4 from [21] and the Reference Evaluation Model (REM) presented in section 3.2, to quantify a Global Security Level (GSL) for the Certification Policies corresponding to the Grid-PKIs members of EUGridPMA.

At this aim, we need to "translate" all the Certification Policy documents into a policy matrix instance. This translation process is *i)* asynchronous (can be performed at anytime prior to the Grid user validation), *ii)* semi-automatic (at this time CP's parsing is performed by a human) and *iii)* repeated

[1] From less-secure to most-secure.

every time the Certification Policy changes (which in practice happens not very often).

When translating a CP, what we are really doing is to parse and map each provision from this document to the policy matrix template obtained in the previous section. This is very easy to perform (at least for a human) if we consider that most Grid-PKIs CPs are an instance of the GGF's CP model [21] and therefore its provisions may be directly mapped to the template. Despite its apparent easiness, our goal is to find in the near future an automatic way to perform this translation.

In our particular case, the first CP to evaluate must be the EUGridPMA's Authentication Profile [1], because its evaluation will determine the reference GSL for the policy space. It is expected that any other Grid-PKI's GSL should be equal or greater than this value (considering that all the evaluated CPs are coming from EUGridPMA members).

When evaluating a CP it is important to highlight two special cases: *i)* those provisions found only into the CP under evaluation and not into the template will be omitted from the evaluation process and, *ii)* those present in the template, but not in the policy, will be mapped to the worst LSL (in the policy matrix this means a row with zero in every column) and shall be considered *notStipulated* clauses. These two choices were motivated because the PMA's minimum requirements document defines by itself which provisions must be considered in the evaluation process to accredit a new Grid-PKI, thus our methodology only extrapolated this criteria Once the CP has been translated, an automatic procedure implementing the evaluation technique is used to obtain the GSL.

Applying the methodology presented in this paper we have obtained the GSL for each one of the Certification Authorities members of the EUGridPMA [2]. Figure 3 compares these levels in a graphical way for a sample composed of the EUGridPMA's minimum Authentication Profile [1] and the Certification Policies from IRIS Grid CA [23], US Department of Energy Grids CA [24], CERN CA [25] and INFN CA [26].

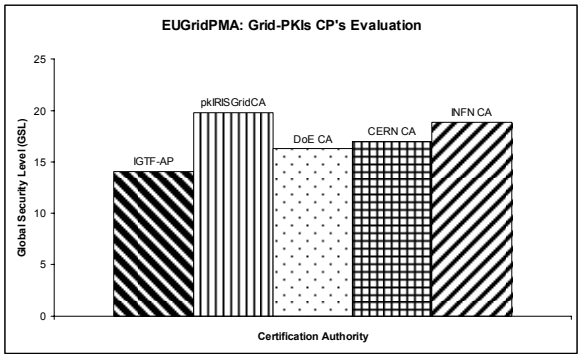

Figure 3. GSLs from EUGridPMA's Certification Authorities

First of all, it is easy to note that every CA has a GSL greater than the reference (the distance between CPs is very large). This was an expected result as every CA complies with EUGridPMA's minimum requirements (that is a GSL greater than IGTF-AP's which GSL=14.03). However we have found that -just as stated at the beginning of this paper- these GSLs differ from one member CA to another, therefore this new information may give the opportunity to a Grid-PKI to dynamically decide to interoperate only with those institutions whose GSL is equal or greater than its own. Let us take the following scenario as an example.

Example 3. INFN Certification Authority has a GSL=18.86, so it is possible to believe that they could choose to work only in some projects with end-entities coming from the IRISGrid CA (GSL=19.77). Moreover they also could establish their own minimum requirements for some project -in other words a new CP template- and then work only with those institutions fulfilling this new set of provisions.

As already said, the GSL is an aggregated value and by itself can not give information about specific provisions of the Certification Policy; this could be a problem in those contexts where it is mandatory that all provisions respect the minimal requirements.

Fortunately, thanks to the proposed formalization process it is even possible to evaluate each section of the Certification Policy to obtain *partial-GSLs* that may allow the relying party to perform a finer validation decision. Table 2 shows, for EUGridPMA's chosen set of CAs, the partial GSLs from each one of the sections composing our Certification Policy template. In this table it is interesting to note the degree of detail that can be obtained when further comparing these Grid-PKIs; it is particularly noticeable the fact that even though all of them have an overall GSL greater than EUGridPMA's, there are some CA's partial-GSLs that do not follow this criteria (i.e. for the

"Technical security controls" section: $partialGSL_{pkIRISGrid} < partialGSL_{IGTF-AP}$).

Apart from using this information for the validation process, our belief is that it can be also very useful for the PMAs to aid Certification Authorities (members or applicants) to better refine or correct their security policies by analyzing very specific sets of provisions. In general, which may be the finest-grained GSL that can be obtained from our methodology? The answer is simple, as it is feasible to get the *GSL for each one of the individual provisions* from the Certification Policy being analyzed and the set of GSLs can be successfully used by both, the PMA to accurately assists the CAs in improving weak provisions, and the relying party itself to take very granular validation decisions according to a predefined template.

Table 2: Partial GSLs from EUGridPMA's CAs

CP Section	IGTF-AP	pkIRISGrid	DoE	CERN	INFN
Introduction	5.00	5.57	5.48	5.66	5.39
General Provisions	7.00	10.05	8.37	9.06	9.43
Identification & Authentication	4.90	5.10	4.69	5.29	5.92
Operation Requirements	5.39	10.00	6.93	7.87	9.80
Physical, procedural and personnel security	1.73	7.35	3.32	2.45	4.69
Technical security controls	5.83	5.48	5.48	6.00	5.92
CA Certificates	3.87	5.39	5.66	5.00	5.83
Certificate and CRL profiles	2.00	2.83	3.46	3.46	2.83
Administration of Specifications	3.16	2.45	2.45	0.00	1.41
Others	2.00	2.45	2.00	2.45	2.45

A suitable way to graphically represent and compare the GSL for individual provisions is through a Kiviat Diagram, where each provision is represented by an axis with one division for each possible Local Security Level in our case, four. In this way, given an axis representing a particular provision, we can depict the LSLs corresponding to one or more Certification Policies, which facilitates their comparison at such level of detail.

Let us take for example figure 4, where a Kiviat diagram, representing the CP provisions related with the identification and authentication features, contains the LSLs for the IRIS Grid CA and INFN CA. We can see that for provisions like "Need for names to be meaningful", the EUGridPMA's minimum requirement (IGTF-AP graph) is fulfilled by the CAs. Also there are some others like "Rekey after Revocation" where the minimum requirement is also fulfilled, but with a different LSL by each one of the CAs being evaluated.

On the other hand, we have found a third group of provisions (i.e. "Authentication of organization identity") where the EUGridPMA's minimum requirement (face to face identification with the Registration Authority) is not fulfilled by the IRIS Grid CA.

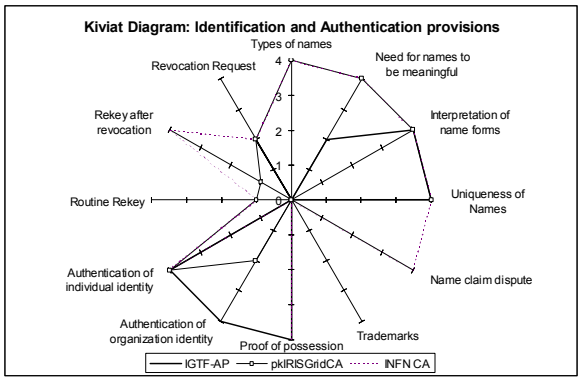

Figure 4. Kiviat Diagram for CP's Identification and Authentication provisions.

6. Conclusions and Future Works

In this paper we have proposed a comprehensive Validation Infrastructure for X.509 certificates used into the computational Grid. This system is based on two elements *i)* a Grid-OCSP service composed of the CertiVeR's OCSP Responder and the OGRO middleware for the Globus Toolkit, and ii) the Reference Evaluation Methodology (REM) which is able to automatically compare certificate policies properly formalized from a set of CAs thanks to the computation of a Global Security Level (GSL) that quantifies the Certification Policy itself. Thanks to the REM we are able to not only aid Grid-PMAs into the accreditation process, but also to provide advises to applicant-PKIs by identifying weak provisons from their certification policy. On the other hand, the overall Validation System presented in this paper can be used by Grid relying parties to provide finer-grainer validation decisions over users requesting access to their resources, by conveying not only certificate status information through OCSP but also the Global Security Level obtained with the REM.

To prove our hypothesis the REM was applied to a set of EUGridPMA's CAs therefore allowing us to evaluate both the GSL guaranteed by their CPs and the partial-GSL for each single provision. In order to apply the methodology, we have built a formalized policy template according to the GGF CP model. Then we translated a set of certificate policies from CAs accreditated by the EUGridPMA, and at the end we have evaluated them against the respective Authentication Profile. Just as expected all the

evaluated CAs had a GSL higher than the chosen reference (EUGridPMA) thus showing REM's correctness in Grid environments. Moreover, we have found that these GSLs differ from one member CA to another, so we have used a finer-grained evaluation to obtain new information which gives the opportunity to a Grid-PKI to locate and eventually improve its security.

As future work we intend to use the GSL value by linking it to the Grid-PKI data already stored into CertiVeR, to help building a dynamic validation system. Such system can be enhanced to evaluate multiple certificate policies on real-time when a relying party requests a certificate validation, thus dynamically building a network of interoperable Grid PKI's.

7. References

[1] "Classic AP Profile Version 4.03". Approved by the EUGridPMA. Edited by David Groep. 2005. http://www.eugridpma.org/igtf/IGTF-AP-classic-20050905-4-03.pdf

[2] "European Policy Management Authority for Grid Authentication". Octuber, 2006. http://www.eugridpma.org/

[3] "The Americas Grid Policy Management Authority". Octuber, 2006. http://www.tagpma.org/

[4] "Asia-Pacific Grid Policy Management Authority". Octuber, 2006. http://www.apgridpma.org/

[5] "International Grid Trust Federation". Octuber, 2006. http://www.gridpma.org/

[6] "An innovative Policy-based Cross Certification methodology for Public Key Infrastructures". Casola V., Mazzeo A., Mazzocca N., Rak M. 2nd EuroPKI Workshop. Springer-Verlag LNCS 3545, pp 100-117, Editors: D. Chadwick, G. Zhao. 2005.

[7] "Towards a Unified Authentication and Authorization Infrastructure for Grid Services: Implementing an enhanced OCSP Service Provider into GT4". Luna J., Manso O., Manel M. 2nd EuroPKI 2005 Workshop. Springer-Verlag LNCS 3545, pp 36-54, Editors: David Chadwick, Gansen Zhao. 2005. http://sec.cs.kent.ac.uk/europki2005/

[8] "RFC 2560: X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol". Myers M, et. al. June 1999. http://www.ietf.org/rfc/rfc2560.txt?number=2560

[9] "EUGridPMA Charter document Version 1.0". Approved by the EUGridPMA. 2004. http://www.eugridpma.org/charter/EUGridPMA-charter-20040401-1-0.pdf

[10] "OCSP Requirements for Grids". Global Grid Forum, CA Operations Work Group. Working Document. May 2005. https://forge.gridforum.org/sf/go/doc4852?nav=1

[11] "CertiVeR: Certificate Revocation and Validation Service". June 2006. http://www.certiver.com/

[12] "OGRO - The Open GRid Ocsp client API". June 2006. http://globus-grid.certiver.com/info/ogro

[13] "A Java Commodity Grid Kit" Gregor von Laszewski, Ian Foster, Jarek Gawor, and Peter Lane, Concurrency and Computation: Practice and Experience, vol. 13, no. 8-9, pp. 643-662, 2001, http:/www.cogkit.org/

[14] "Using OGRO and CertiVeR to improve OCSP validation for Grids". Luna J., Manso O., Manel M. 1st Grid and Pervasive Conference. Springer-Verlag LNCS 3947, pp 12-21, Editors: Yeh-Ching Chung, José E. Moreira. 2006. http://hpc.csie.thu.edu.tw/gpc2006/

[15] "OCSP for Grids: Comparing Prevalidation versus Caching". Luna J., Manso O., Manel M. In 7th IEEE/ACM International Conference on Grid Computing, Barcelona. 2006, pp. 202-209. http://www.grid2006.org/

[16] "A Reference Model for Security Level Evaluation: Policy and Fuzzy Techniques". Casola V., Preziosi R., Rak M., Troiano L. JUCS - Journal of Universal Computer Science. Editors: Ajith Abraham, L.C. January, pp 150-175 , 2005.

[17] "A SLA evaluation methodology in Service Oriented Architectures". Casola V., Mazzeo A., Mazzocca N., Rak M" in Proceedings of Quality of Protection Workshop 05, 15 September, 2005, Milan, pp. 119-130, Springer-Verlag

[18] "A Policy Based Methodology for the Analysis, Modelling and Implementation of Security Infrastructures". Casola V., PhD Thesis, Second University of Naples, 2004.

[19] "OSSTMM: Open Source Security Testing Methodology Manual." August 2006. http://www.isecom.info/mirror/osstmm.en.2.1.1.pdf

[20] Casola V., Coppolino L., Rak M., "An Architectural Model for Trusted Domains in Web Services", in JIAS, Journal of Information Assurance and Security - Volume 1, Issue 2, pp. 29-40, June 2006 edited by A. Abraham, USA; Published by Dynamic Publishers Inc., USA

[21] "Global Grid Forum Certificate Policy Model". Butler, R.. Genovese, T. Global Grid Forum. June, 2003. http://www.ggf.org/documents/GFD.16.pdf

[22] "RFC 3647: X.509 Internet Public Key Infrastructure, Certificate Policy and Certification Practices Framework". Chokhani S., et. al. November 2003. http://www.ietf.org/rfc/rfc3647.txt?number=3647

[23] "pkIRIS Grid Certification Authority: Certification Policy". August 2006. http://www.irisgrid.es/pki/policy/

[24] "US Department of energy Grids: Certification Policy". August 2006. http://www.doegrids.org/Docs/CP-CPS.pdf

[25] "CERN Certification Authority: Certification Policy". August 2006. http://service-grid-ca.web.cern.ch/service-grid-ca/cp_cps/cp_cps.html

[26] "INFN Certification Authority: Certification Policy". August 2006. http://security.fi.infn.it/CA/CPS/