GWD-C
Category:

CAOPS Working Group

Paul Madsen, Entrust
Mike Helm, ESnet/LBNL
Tony J. Genovese, ESnet/LBNL
March 4, 2003

Machine Assisted Trust Mechanisms for Grids

1 Abstract

This paper proposes a simple low-cost alternative to the CertificatePolicy/Certificate Practices Statement model for the establishment of bi-lateral trust relationships between Grid entities. By publishing their public keys, along with the obligations, commitments, and liabilities associated with its use, in a machine readable format, a Grid entity will both facilitate other potential users/resources discovering this key, and ultimately, simplify the process by which those other entities determine if that key is relevant for their application and decide to trust it.

2 Introduction

Public key certificates can be characterized by a number of different aspects – including the nature of the registration process that preceded their issuance, how active is their lifecycle-management, and the level of protection afforded to the associated private key.

The relevance of a particular certificate to a given application may depend on these characteristics, as they will together determine the level of assurance that a relying party can place in that certificate. Other factors that may impact whether or not a certificate is appropriate to a given application include: the level of liability the issuing CA is willing to assume if the certificate is shown to be fraudulent and the obligations of entities (subject's and relying parties) who may use that certificate.

RFC-2527 [1] defines a framework for expressing this information in two related but separate documents - the Certificate Policy (CP) and Certificate Practices Statement (CPS) – a common (but not universally accepted) distinction is that the CP contains **what** is to be adhered to, while the CPS states **how** it is adhered to. In this interpretation then, the CP is thus seen as more fundamental; a Relying Party decision to trust a particular certificate is ultimately determined by the assertions that the CA makes with respect to the CP requirements, the Relying Party could choose not to concern itself with the details of how the CA meets these requirements.

The legal complexity and size (sometime on the order of 100 pages) of CPs and CPs prevent them from being readily read and understood; consequently they may not adequately support the necessary legal concept of clear 'disclosure' to be legally meaningful. This issue, as well as some CAs being reluctant to publish the details of their internal security practices for external review through a CPS, has motivated the specification of a simpler mechanism for policy disclosure – the so called PKI Disclosure Statement (PDS) [2]. The PDS is a more succinct representation (typically two pages) of the most salient information of both the CP and the CPS.

While the PDS addresses the complexity of the CP and CPS model, it still suffers from limitations, including

- There is no binding between the statements made within the PDS (some implying a legal obligation) and the CA. Consequently, the CA could later deny making those statements.
- It is not machine processable – preventing both automated discovery and interpretation.
- It does not define how it might be published to facilitate discovery by potential relying parties

Paul Madsen, Entrust
Mike Helm, ESnet/LBNL
Tony J. Genovese, ESnet/LBNL

- It is unnecessarily hierarchic. It is a set of statements made by a certification authority regarding the certificates it issues to its subscribers. It does not support the ability for an end-entity key-owner (one who will not issue certificates to other parties) to make similar assertions about appropriate uses of its own public-key.
- Reflecting its authority-centric nature, it is unable to provide detail on the applications for which a particular certificate class is appropriate - this because the authority may have little or no insight into the eventual business applications for which its certificates may be used. Consequently, although it is able to list the obligations of the actors who will use the certificates, it is unable to list these obligations against particular key applications.

In this paper we propose a new mechanism for distributing PKI policy information. We believe that that the emerging Web Services architecture, this built around XML and a publish-and-subscribe model, offers a simpler alternative to the CP/CPS/CPS model - one which has the potential to enable bi-lateral trust relationships to be established between Grid entities in a semi-automated fashion – reducing the cost and effort involved.

3 Qualified Installation of Keys

We have named this model Qualified Installation of Keys (QIK), 'qualified' because the trust that a Relying Party may place in a particular public key need not be unconstrained – it can be qualified by the applications for which it is appropriate, and 'installation' because a Relying Party decision to trust some key will often be made manifest in the installation of that key into some 'trusted store'.

The QIK model has a key-owner publish their public verification key to all potential relying parties – the key itself appended with the necessary additional information that will allow those relying parties to assess its relevance for a particular application, i.e. whether or not they should trust it for that application.

The key is published as part of an XML document. QIK is an XML Schema by which the key can be published along with the key-owners commitments and associated conditions for use.
The basic principle behind QIK is a simple one, illustrated in Figure 1.

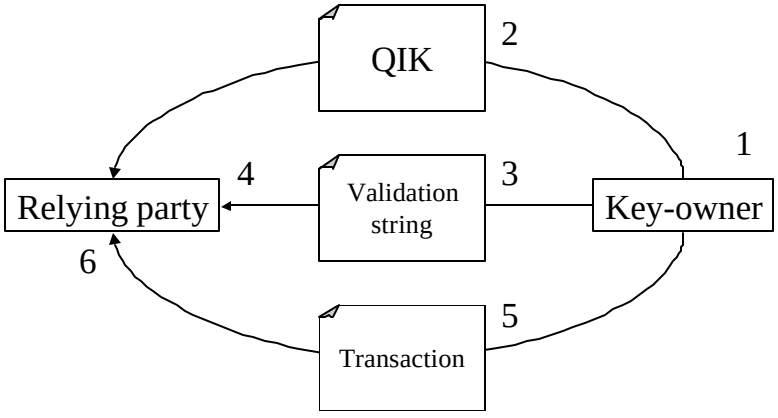

Figure 1: Basic QIK process flow

The process proceeds by the following steps:

1. The owner of a digital-signature key-pair creates a QIK statement, containing the public verification key and the conditions of use for that key.
2. It publishes the QIK statement, either on the Web or by some other means, e.g. through WSDL or UDDI.
3. It creates a validation string by digesting the QIK statement and makes the digest available by an authentic channel, such as by email, telephone, company letterhead, business card, https, etc. (similar to PGP's fingerprint mechanism)
4. The relying party retrieves and validates the QIK statement, using the digest.
5. The relying party examines the QIK statement and confirms the suitability of its conditions of use to the intended application and, if these checks pass, installs the key – qualified for use by mapping to appropriate internal policies. It is expected that this decision will be accomplished through a combination of machine and human processing of the information within the QIK statement. Further details are provided below in Section 4
6. Subsequent to the installation of the key, the key owner sends signed messages to the relying party.
7. The relying party validates the messages using the public verification key from the QIK statement.
8. The relying party proceeds with the processing of the business transaction if the key-owner has the appropriate authorizations.

4 Relying-party Key Installation

Upon receiving the QIK statement of the respective key-owner, a relying-party must compare the approved uses and obligations within the QIK statement to both their intended application and their ability to satisfy the stated relying-party obligations in order to determine whether or not the key within the QIK statement is appropriate. This process is shown in Figure 2 below:

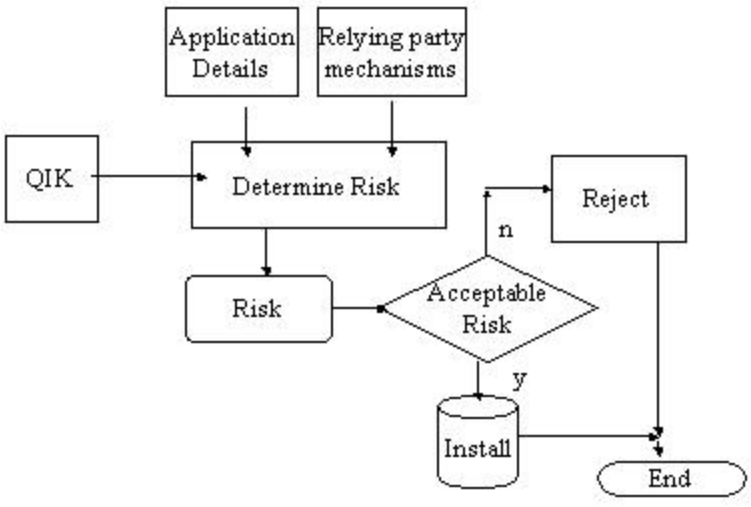

Figure 2: Relying Party Trust Decision Process

Paul Madsen, Entrust
Mike Helm, ESnet/LBNL
Tony J. Genovese, ESnet/LBNL

We expect that this process would be a combination of machine processing and human interpretation – machine processing to determine if the QIK statement is compatible (i.e. does it allow the intended application, is the stated keyowner liability limit acceptable) but the ultimate trust decision being made by some administrator.

It is expected that the key, once installed by the relying-party, would be indexed by the applications for which it would be appropriate. This is the qualified nature of the trust that the relying-party is able to place in the key; trust in the key is not absolute but relative to the nature of the application for which that key might be used in deriving security. When the relying-party subsequently receives a signed message from the key-owner (this message in the context of a specific business transaction) the relying-party is able to determine if the previously installed key is appropriate for this context. If so, the signature is considered to be valid for this context (beyond any revocation status checking etc) and the transaction is allowed to proceed; if not, the request is denied.

5 Certificate Authority Variant

The QIK model can support trust hierarchies to address the scaling problem inherent in pair-wise trust. Both the key-owner and the relying-party may be certification authorities.

When the key-owner is a certification authority, it may use the public key distributed in the QIK statement to sign (with the associated private key) the certificates of its subscribers. The QIK statement will indicate the CA's commitments and obligations with respect to *its* public verification-key, which may include obligations on both the eventual relying parties as well as its subscribers.

When the relying-party is a certification authority, a decision to assign some qualified trust to a public key contained within a QIK statement it has received from another CA may involve the relying-party CA issuing a cross-certificate to the key-owner CA. The issued cross-certificate would contain the key and other information extracted from the QIK statement, the QIK assertions as to commitments, obligations, and application usage mapped into the appropriate policy extensions within the issued cross-certificate. Once issued, the cross-certificate would be made available to the relying-party CA's community through existing mechanisms such that this community would be able to place qualified trust in the subscribers of the key-owner CA. This concept is shown in Figure 3 below.

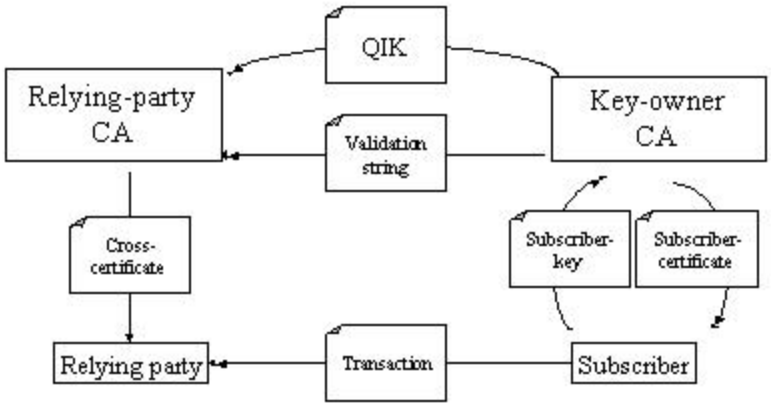

Figure 3: CA as Key-owner and Relying-party

Paul Madsen, Entrust
Mike Helm, ESnet/LBNL
Tony J. Genovese, ESnet/LBNL

6 QIK & Grids

This section briefly explores how the QIK model might be applied to the Grid certificate-based authentication infrastructure.

6.1 CA Key installation

The QIK model could facilitate this process of installing a new CA certificate into a system's trusted store ('*etc/grid-security/certificates')*

The following paragraphs were extracted from 'Adding a new trusted CA to a Globus Installation' (http://www-fp.globus.org/security/v2.0/adding_trusted_ca.html)

'Installing a trusted CA (Certificate Authority) certificate on a system means that the system now completely trusts that CA in terms of authentication. This is a major policy decision and should not be taken lightly. You want to understand who is running the CA, how it is being run, and to whom and how is it issuing certificates. Then you need to decide that this CA is acceptable to trust for your resources.'

'You need to get the certificate from a trusted source and be certain that it is actually the certificate for the CA - i.e. make sure no one has substituted a different certificate either accidentally or maliciously.'

The QIK model could facilitate this process by:

1. Presenting the necessary and relevant information on which the trust decision is based in a machine and human readable manner. For example, the following XML sample represents the CA assertion that it will notify those Grid entities (that it is aware of) if its private key is compromised and lists the maximum liability that the CA is willing to assume in this scenario.

```
<KeyApplication>
  <KeyApplicationId>globus:grid:authentication</KeyApplicationId>
  <Description>Proxy-certificate SSL Authentication</Description>
     <Commitment>
       <Description>The key-owner will notify all known relying parties
within 24 hours if the private key is compromised.</Description>
       <Liability maximum = "1000" scope = "aggregate" />
     </Commitment>
</KeyApplication>
```

This XML could be machine-queried (searching to determine if the maximum liability is acceptable) as well as rendered for human consumption in a variety ways (e.g. through an XSLT conversion to HTML)

2. Providing an authentic channel for the retrieval of the CA's public key through its Validation String mechanism.

6.2 CA Signing Policy

Paul Madsen, Entrust
Mike Helm, ESnet/LBNL
Tony J. Genovese, ESnet/LBNL

When installing a new CA certificate, the namespaces under which this new CA issues certificates must be configured. If proxy certificates are subsequently presented under a different namespace (but still chaining to the trusted CA), they will be rejected.

QIK could facilitate how the delivery of this information from the new CA to the admin responsible for configuring systems to trust this CA through a <SubjectNamespace> element, as shown below

```
<KeyOwnerCategory>
   <Authority>
       <SubjectsNamespace>
          <SubjectNamespace>"C=US/O=Globus/O=Grid/O=CA/*</SubjectNamespace>
       </SubjectsNamespace>
   </Authority>
</KeyOwnerCategory>
```

6.3 Proxy Certificate Restrictions

If it is the case that restrictions are to be placed on the proxy certificates signed by end-entity certificates issued by the key-owner CA, then the CA can state its policy for these restrictions in the QIK document. As an example, a CA, concerned about the possibility of proxy certificate private key compromise, could stipulate that any Policy Certificates (issued by one of its subscribers) should inherit no rights from the issuing end-entity certificate and should be treated as an 'independent' entity as far as authorizations are concerned.

This is shown below with the relevant portion of a QIK document.

```
<KeyOwnerCategory>
    <Authority>
       <ProxyRestrictions Authorize=”Independent”/>
    </Authority>
</KeyOwnerCategory>
```

7 References

[1] S. Chokhani, W. Ford, “Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework”, RFC 2527, March 1999

[2] ‘Policy requirements for certification authorities issuing qualified certificates’, ETSI TS 101 456, December 2000

[3] S. Tuecke, D. Engert, I. Foster, V. Welch, M. Thompson, L. Pearlman, C. Kesselman, “Internet X.509 Public Key Infrastructure Proxy Certificate Profile”, October 2002