QUATRO Plus: Quality You Can Trust?

Phil Archer[1], Elena Ferrari[2], Vangelis Karkaletsis[3], Stasinos Konstantopoulos[3], Antonis Koukourikos[3], and Andrea Perego[2]

[1] i-sieve technologies, Athens, Greece
phil@i-sieve.com
[2] DICOM, Università degli Studi dell'Insubria, Varese, Italy
{elena.ferrari,andrea.perego}@uninsubria.it
[3] IIT, NCSR 'Demokritos', Athens, Greece
{vangelis,konstant,kukurik}@iit.demokritos.gr

Abstract. The QUATRO Plus project, a follow on from the original QUATRO Project, aims to balance the wisdom of the crowds with the knowledge of the experts. It uses a mixture of authenticated data sources and the opinions of end users expressed through social networking software to build a dataset that is authoritative and trustworthy. The dataset describes online resources using RDF with the upcoming W3C Recommendation, POWDER, as the underlying transport and storage mechanism. Data can be added to or queried through a variety of tools provided by the project, some of which are described in detail in this paper.

1 Introduction

There is a great deal of opinion online that is an expression of 'the wisdom of the crowds,' the classic example of this being Wikipedia. Much of this material is recognised as being extremely good. Mistakes and occasional deliberate falsehoods do occur however—something that Wikipedia itself recognises.[4] On the other hand, there are many experts whose opinions are expressed on the Web and whose opinions are open to authentication: trustmark operators. Well known examples of this include TRUSTe, Health on the Net (HON), and VeriSign.

The Quality Content And Description project (QUATRO Plus)[5] seeks to balance the wisdom of the crowds with the wisdom of the experts. QUATRO Plus follows on directly from an earlier project and has been instrumental in the development of the new W3C Protocol for Web Description Resources (POWDER). This paper presents the QUATRO Plus project with particular emphasis on its creation of POWDER documents, exposure of their provenance and their potential trustworthiness based on the reputation of the individual or organisation that created them.

The rest of this paper is organised as follows. Section 2 briefly introduces the POWDER specification and especially its trust and authentication features. Section 3 outlines the architecture of the QUATRO Plus platform and discusses

[4] See http://en.wikipedia.org/wiki/Wisdom_of_the_crowds.
[5] Project website: http://www.quatro-project.org/

```
1  <powder xmlns="http://www.w3.org/2007/05/powder#"
       xmlns:ex="http://example.org/vocab#">
2    <attribution>
3      <issuedby src="http://authority.example.org/company.rdf#me"/>
4      <issued>2007-12-14T00:00:00</issued>
5    </attribution>
6    <dr>
7      <iriset>
8        <includehosts>example.com</includehosts>
9      </iriset>
10     <descriptorset>
11       <displaytext>Everything on example.com is red and square</displaytext>
12       <displayicon src="http://authority.example.org/icons/red-square.png"/>
13       <ex:colour rdf:resource="http://rgb.org/vocab#red" />
14       <ex:shape>square</ex:shape>
15     </descriptorset>
16   </dr>
17 </powder>
```

Fig. 1. A simple POWDER document

how it serves metadata, whereas Sect. 4 focuses on one of its main metadata creation components, the Quality Social Network. Finally, Sect. 5 discusses related work, whereas Sect. 6 concludes the paper and outlines future research directions.

2 The POWDER Specification

The *Protocol for Web Description Resources* (POWDER) is a general purpose content and quality labelling protocol based on Semantic Web technologies, developed by the W3C POWDER Working Group.[6]

POWDER was designed as a practical means of adding RDF to collections of resources. To take a simple example, POWDER expresses statements such as 'everything on example.com is red and square; this statement was asserted by the entity described at http://authority.example.org/company.rdf#me on 14th December 2007.' This statement is exemplified in Fig. 1.

At the core of POWDER is the *Description Resource* (DR) [1], an association between:

- the DR *scope*, a set of resources [2]. Scope is expressed as an iriset, a series of restrictions on the IRIs of resources that are in scope (lines 7-9 in Fig. 1).
- a *formal description* of all resources in scope (lines 13 & 14 in Fig. 1). This is expressed by the descriptorset, which comprises RDF properties defined in external vocabularies (as ex:colour and ex:shape at lines 13 & 14 in Fig. 1). And

[6] The POWDER Working Group was chartered in March 2007 and is due to complete its work in June 2009. More details on the WG and the specification are available at http://www.w3.org/2007/powder/.

```
<?xml version="1.0" encoding="utf-8"?>
<rdf:RDF xmlns="http://www.w3.org/2007/05/powder-s#"
      xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
      xmlns:ex="http://example.org/vocab#">
  <rdf:Description rdf:about="http://www.example.com/foo/">
    <text>Everything on example.com is red and square</text>
    <logo rdf:resource="http://authority.example.org/icons/red-square.png"/>
    <ex:colour rdf:resource="http://rgb.org/vocab#red" />
    <ex:shape>square</ex:shape>
  </rdf:Description>
</rdf:RDF>
```

Fig. 2. The output of the *describe*(u, D) function, where D set includes as element the POWDER document in Fig. 1 and $u =$ http://www.example.com/foo/. Note that properties text and logo map from elements displaytext and displayicon, respectively, in Fig. 1.

- a *textual* and/or *pictorial summary* of the formal description. This is expressed as descriptorset members using the POWDER-defined displaytext and displayicon elements (lines 11 & 12 in Fig. 1).

Furthermore, POWDER documents associate *attribution* blocks (lines 2–5 in Fig. 1) with one or more DR blocks. Attribution blocks provide information that can be used assess the trustworthiness of the DRs in a document, including the labelling authority that created it, creation time, validity period, and so on.

Note that POWDER attribution blocks have the only purpose of denoting the authorship of a given POWDER document, thus making users able to verify its authenticity, and to decide its degree of trustworthiness. Such an approach is more specific with respet to the one of the Open Provenance Model (OPM) [3], which aims at providing a detailed description of the creation, usage, and derivation of a given artifact along its whole lifecycle. However, although OPM addresses issues that are not requirements according to the POWDER specification, such technology can be effectively applied to POWDER in order to document the history of POWDER documents.

Finally, POWDER documents can be explicitly associated with the resources they apply to by using a variety of methods. For this purpose, the describedby relationship has been defined to be used in (X)HTML link elements, HTTP `Link` headers [4], ATOM entries [5], and RDFa [6]. As illustrated in Sect. 2.1, POWDER processors allow one to apply arbitrary POWDER documents to a resource by specifying the IRI of a specific POWDER document, or by accessing a repository of POWDER documents. For a detailed description of all the possible options, we refer the reader to Sect. 4 of [1].

2.1 Processing POWDER Documents

POWDER processors implement a *describe*(u, D) function that returns an rdf:Description of resource u given a set D of POWDER documents (see Fig. 2 for an example).

```
@prefix owl:   <http://www.w3.org/2002/07/owl#> .
@prefix ex:    <http://example.org/vocab#> .
@prefix rdfs:  <http://www.w3.org/2000/01/rdf-schema#> .
@prefix wdrs:  <http://www.w3.org/2007/05/powder-s#> .
@prefix xsd:   <http://www.w3.org/2001/XMLSchema#> .

<> a owl:Ontology;
   wdrs:issued "2007-12-14T00:00:00";
   wdrs:issuedby <http://authority.example.org/company.rdf#me> .

_:iriset_1 a owl:Class; owl:equivalentClass [
   a owl:Class;
   owl:intersectionOf  (
      [ a :Restriction; owl:onProperty wdrs:matchesregex;
        owl:hasValue
          "\:\/\/(([^\/\?\#]*)\@)?([^\:\/\?\#\@]+\.)?(example\.com)(:([0-9]+))?\/"^^xsd:string; ] ) ] .
_:descriptorset_1 a owl:Class;
   rdfs:subClassOf [ a owl:Class;
      owl:intersectionOf (
         [ a owl:Restriction; owl:onProperty ex:color; owl:hasValue <http://rgb.org/vocab#red> ]
         [ a owl:Restriction; owl:onProperty ex:shape; owl:hasValue "square" ]
      ) ];
   wdrs:logo <http://authority.example.org/icons/red-square.png>;
   wdrs:text "Everything on example.com is red and square" .

_:iriset_1 rdfs:subClassOf _:descriptorset_1 .
```

Fig. 3. The OWL/RDF transform of the POWDER document in Fig. 1 in N3 syntax [9,10]. Note how attribution is expressed as owl:Ontology annotations and POWDER-defined descriptors as descriptorset annotations; POWDER-defined properties are instances of owl:AnnotationProperty.

POWDER documents can, to a large degree, be processed entirely as XML but are, in fact, transporting OWL/RDF graphs that can be accessed by performing a transformation on the XML (see Fig. 3 for an example). In *Semantic POWDER* (POWDER-S), DRs express an rdfs:subClassOf relation between the class of resources that fall within scope and the class of resources that have the given RDF description. The POWDER document as a whole is an owl:Ontology instance containing a number of such assertions, and the attribution block expresses owl:AnnotationProperty triples with the owl:Ontology instance as subject. This achieves the same goal as Named Graphs [7] as used for example by Bizer and Cyganiak in [8]: the explicit declaration of provenance information, but within existing RDF/OWL specifications.

A semantic extension bridges abstract (but named) resources and the string representations of their IRIs. This extension reflects the basic premise of POWDER, absent from RDF semantics, that the structure of a resource's IRI is a property of the corresponding resource, upon which inference can be drawn; this allows POWDER documents to assert propositions about 'all resources on example.com.'

POWDER-S offers processors the option of using standard semantic inference and querying tools to process POWDER/XML documents. The process of transforming POWDER/XML documents into POWDER-S documents is detailed in the POWDER specification [11] and also implemented as an XSLT script [12] associated with the POWDER namespace via GRDDL [13]. Together with the fact that POWDER processors respond with RDF descriptions even when only processing XML, this transformation makes POWDER tools fully compatible with other Semantic Web tools and technologies.

```
<foaf:Organization rdf:ID="me">
 <foaf:homepage rdf:resource="http://authority.example.org/"/>
 <foaf:name>The Exemplary Description Authority</foaf:name>
 <foaf:nick>EDA</foaf:nick>
 <wdrs:authenticate rdf:resource="http://authority.example.org/auth.html" />
</foaf:Organization>
```

Fig. 4. A simple FOAF Agent

2.2 Attribution and Authentication

Trust is a human quality and is rarely deterministic in an absolute sense; whether trust is conferred on any data is always a balance between the likelihood of it being true and the consequence of it being false. If a DR says that a particular cake recipe is really good but following it produces an inedible lump, little harm is done. If a DR states that some medical advice is peer reviewed and can be used as the basis for diagnosis and treatment, then the consequences of falsehood are clearly much more serious and a more robust authentication method is appropriate.

Although the POWDER specification is very detailed on the form and meaning of POWDER documents and the output of conforming processors, it is deliberately non-prescriptive about trust and authentication methods; any method can be defined by a DR publisher that is appropriate for the particular context (the choice of method made by the publisher may itself be a factor in a user's assessment of trust!). What POWDER does offer is a detailed specification of how to endow DRs with attribution and authentication *credentials*, the raw information upon which a variety of trust methodologies can operate.

The issuedby attribution element is mandatory for all POWDER documents and provides the IRI that identifies a description of the entity that created the document and that is therefore responsible for the claims made in the DR(s) it contains. The strong recommendation is that such descriptions are provided as instances of the Agent class in either of the widely used FOAF [14] or Dublin Core [15] vocabularies.[7]

An RDF-aware system can use the IRI to retrieve the properties of the creator (see Fig. 4 for an example) and use them to decide if the document is trustworthy. Besides whatever properties are defined by the vocabulary used to describe the creator, POWDER also defines the authenticate property that points to a resource that gives information on how to authenticate any POWDER documents that were created by this Agent. Such a resource may be a machine readable document, such as a WSDL[8] file, that can be read and acted upon automatically. However, it is equally valid for the resource to be a simple text document that needs to be read by a person who then implements a suitable system to take advantage of the available authentication mechanism. This approach is in

[7] foaf:Agent is defined at http://xmlns.com/foaf/spec/#term_Agent. dcterms:Agent is defined at http://dublincore.org/documents/dcmi-terms/#classes-Agent.

[8] Web Services Description Language. See [16].

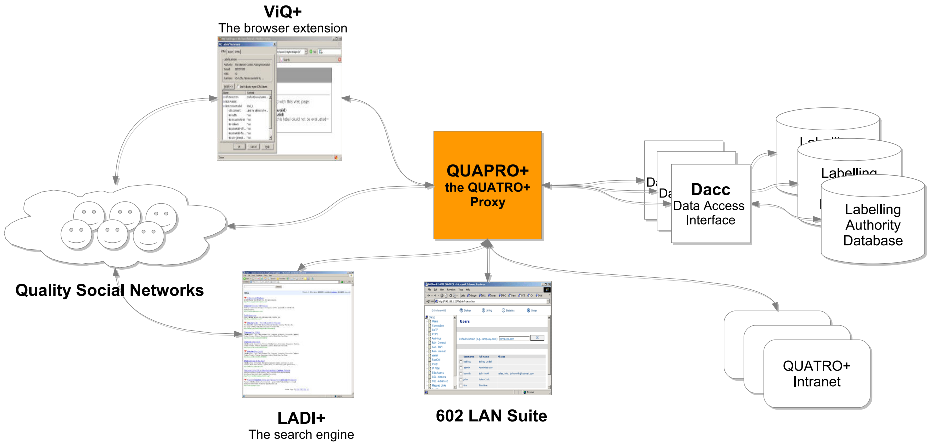

Fig. 5. The architecture of the QUATRO Plus platform

tune with the POWDER paradigm as the aim is to provide strong assurance of the identity of the creator of a given description. Such a data source will almost always require a human stage in assessing trustworthiness. Furthermore, as already noted, trust is very context-sensitive so that prescribing a single authentication mechanism would have been inappropriate. Section 3 discusses the particular authentication system used by QUATRO Plus.

There are other features of POWDER designed to facilitate trust in the data. These include certification, that is, where a DR has a scope of exactly one resource and a descriptor set that includes either or both of two descriptors: `certified`, which has a range of `xsd:boolean`, and `sha1sum`, the value of which is a SHA-1 checksum of the described resource. Using these, it's possible for a DR to certify the veracity of another. Another feature designed to increase the trust that can be placed in a POWDER document is the `supportedby` property. This can link to any form of data published by a third party that agrees with the assertions in the DR. This data may be in any form, the assumption being that an application will be built with a specific data source in mind. As an example, a POWDER document may assert that a website is suitable for children. Supporting evidence might come from a commercial content classification service.

3 Working with Trustmarks: The QUATRO Proxy

The full suite of QUATRO Plus software (whose architecture is depicted in Fig. 5) includes a search result annotation tool, LADI+ and a browser extension, ViQ+, both of which recognise the presence of links to DRs and provide authentication information to end users. A further tool, the Label Management

Environment (LME), was developed under a related project, MedIEQ.[9] In this paper, we focus on two components of QUATRO Plus suite: The QUATRO Proxy and the Quality Social Network (QSN).

The QUATRO Proxy is a set of Web services provided by multiple servers that, among other functionalities, is able to describe resources by locating, processing and authenticating POWDER documents. Given the IRI of a Web resource, QUATRO Proxy locates relevant POWDER documents, authenticates them and uses them to compose a description of the resource. The description is returned to the client along with details of the provenance and authenticity of the data.

As mentioned earlier in this section, relevant POWDER documents are located by implementing a cascade of discovery techniques. In increasing order of efficiency these are: by checking the website itself and following links to POWDER documents (using the 'describedby' relationship type); by following a link to a POWDER document provided in the request to the proxy made by the client; and by looking the site up directly in the trustmark operators' databases to which it has access. Except in the latter case, once the relevant POWDER documents have been identified, they are authenticated by looking them up in the relevant trustmark operator's database—an automated version of the 'click to verify' model operated by all online trustmarks.

The security of the transactions and the authenticity of the server and the databases to which the proxy connects are guaranteed via message signing and SSL tunnelling. Equally importantly, trustmark operators can be confident that their data is secure.

4 Creating Descriptions: The Quality Social Network

Recent years have seen an increasing diffusion of *Web-based social networks* (WBSNs) giving their members the ability to specify and share metadata concerning online resources. Examples of such WBSNs are del.icio.us (http://del.icio.us), RawSugar (http://rawsugar.com), Flickr (http://flickr.com), and Last.fm (http://last.fm), which support the so-called *social* or *collaborative tagging*.

Although, so far, users' tags and content providers' content labels have evolved separately, we think it desirable that a convergence is established between them. The ideas underlying collaborative tagging may contribute in addressing some of the main open issues which prevented the success of content labelling. In particular, existing content labels describe a very limited subset of the Web, thus making impossible to widely exploit their advantages in term of information filtering and discovery. Moreover, content labels must be consistent with the resources they describe. However, since Web resources may change very frequently, this requires an effort which is not acceptable to content providers. In such a scenario, collaborative tagging can make any end user a possible label author, thus increasing not only the number of labelled resources, but also the

[9] MedIEQ focused on the labelling of medical resources. Please see http://medieq.org/ for more details.

number of labels associated with the same resource. Thanks to this, it would be simpler to verify whether a label actually describes the associated resource, and it would be also possible to assess the trustworthiness of a given description by statistically analysing the whole set of labels associated with a resource.

Based on these considerations, the QUATRO Plus platform includes a social networking service, referred to as *Quality Social Network* (QSN), giving its members the ability to specify user-defined POWDER documents (referred to as *labels*) and *ratings*. As any POWDER document, besides containing a set of descriptors (the DR descriptorset component), a label states who has created it (POWDER attribution block), the set of resources it applies to (the DR iriset), and its validity period (corresponding to the validfrom and validuntil attribution elements available in POWDER). By contrast, ratings are used by WBSN members to endorse part or all the descriptors in an existing label, or to express their disagreement about the claims it contains. Three types of ratings are supported: *positive* (agreement), *negative* (disagreement), and *neutral* ('I don't know'). The trustworthiness of the descriptors contained in a label is then statistically determined based on the number of positive/negative/neutral ratings associated with them. The results of such an evaluation are made available to the other components of the QUATRO Plus architecture, and to their end users.

QUATRO Plus plans to use these features as a basis to enforce personalised access to Web resources through the support for *user preferences*. User preferences give end users the ability to state which action should be performed by their user agent upon detection of resources carrying labels with given descriptors and trustworthiness. For instance, an end user may ask to be notified when a given resource does or does not satisfy a given set of requirements concerning medical resources, or decide that the user agent must block access to a resource if more than 20% of the existing labels state that it contains pornographic content.

It is important to note that, although a publicly accessible QSN will be set up,[10] the QSN is a service which can be installed and run by any institution/organisation that wishes to set up a social network supporting collaborative labelling and rating. For this reason, the QSN gives system administrators the ability to configure the service depending on the requirements of the institution/organisation running it.

In the following section, we provide an overview of the main features supported by the QSN. The work reported here is a partial implementation of the multi-layer personalisation framework we have proposed in [17], which provides the foundations of the approach adopted in QUATRO Plus for supporting Web access personalisation through the use of Semantic Web technologies and social networking.

4.1 Labels and Ratings Evaluation and Aggregation

The main purpose of supporting collaborative labelling and rating of Web resources, is to statistically analyse the labels and ratings specified by WBSN

[10] A prototype version of the QSN, accessible only by invited members, is currently available at http://dawsec.dicom.uninsubria.it/qui/

members and identify the most objective descriptions of a resource which may then be used for content/service personalisation. In order to achieve this, the labels associated with a resource are aggregated, and for each descriptor they contain, a *trust value* is computed.

There are several different formulae which may be used for trust computation, each addressing the requirements of given application domains, granting different degrees of accuracy, and having different computational costs. For these reasons, we plan to support a set of trust computation algorithms, among which QSN administrators can choose the one which is most suitable to their purposes, also taking into account the trade-off between efficiency and accuracy.

Basically, we plan to support two main trust computation solutions. According to the basic option, all QSN members as equally trustworthy. Consequently, the trustworthiness of a label is determined only by the more or less wide consensus on the claims it contains. Such consensus dependes on the possible existence of multiple occurrences of the same label, specified by different authors, and on the positive, negative, and neutral ratings associated it. All this information is then used to compute a trust score for a given label. There exist several algorithms proposed for reputation systems [18], such as Eigentrust [19] and PeerTrust [20], which might provide a suitable solution.

Such an approach can be enhanced by associating each QSN member with a reputation score, which can then be used to assign a specific weight to his/her labels and ratings. This is an issue that has been thoroughly investigated by recommender systems [21], among which there exist examples of online communities, such as MovieLens [22] and MyWOT (http://mywot.com).

Reputation can determine the trustworthiness of a given QSN member for all the users in a community. However, it may be often the case that a given member A considers more trustworthy the opinions of member B than the ones of member C, even though the reputation of C is higher than the one of B. Recommender systems have addressed such issue by computing a similarity measure between user profiles. More recently, a different approach has been adopted by a few WBSNs. For instance, FilmTrust [23] and Moleskiing [24] propose algorithms which make use of trust relationships explicitly established between WBSN members to predict the degree of trust existing even between members not directly connected. Finally, in an earlier paper [17], we have explored also the possibility of using *trust policies*, thanks to which a given QSN member can denote the set of users he/she considers as trustworthy based on either their identity or characteristics.

4.2 Privacy Issues

Labels and ratings are not sensitive by themselves, but they may convey sensitive information about end users' opinions and tastes, which can be misused. On the other hand, labels' and ratings' accountability is fundamental in order to make their authors responsible of what they claim. QUATRO Plus raises other issues surrounding privacy protection and accountability. If user-defined labels and ratings are public (i.e., accessible by everyone, even by people who are not members of the QSN), the whole Web community can benefit of them. However, this may result in an inappropriate disclosure of private information.

Based on this, when specifying a label or a rating, QSN members are given various protection options:

- the label/rating is private—it can be seen only by the QSN member who created it;
- the label/rating is visible only to the direct contacts of the QSN member who created it;
- the label/rating is visible only to the group members of the QSN member who created it;
- the label/rating is visible to any QSN member;
- the label/rating is public—also non QSN members can access it.

When aggregated, labels and ratings no longer carry information concerning their authors, so they do not explicitly disclose private information. Nonetheless, QSN administrators are given the possibility of setting which labels and ratings must be taken into account (i.e. any label, only public labels, etc.) and whether the aggregate view is a service available only to QSN members or also to non QSN members.

4.3 Web Access Personalisation

As mentioned earlier, we plan to use the aggregate view of labels and ratings as a basis to enforce Web access personalisation. In order to achieve this, QSN members will be given the ability of specifying *user preferences* denoting the action to be performed when detecting a resource associated with a given set of descriptors, having a given trustworthiness. The supported actions are *block* and *notify*. In case of a block action, access to the requested resource is denied, and the user agent returns the notification message. In case of a notify action, access is granted, and the user agent returns the notification message. In both cases, the end users will be given the possibility of verifying why a given action has been performed by displaying (a) the content of the labels associated with the accessed resource, (b) the corresponding aggregate view, and (c) the user preferences which have been satisfied. Note however that, as far as single labels are concerned, the end user will be able to display only the ones he/she is authorised to see, based on the disclosure policies specified by their authors (see Sect. 4.2).

The language and the tools to be used for user preference specification and enforcement are currently one of the issues we are investigating. A possible option is to use a rule language, such as N3 Rules [9,10], and a reasoner (e.g., Cwm[11]). However, languages such as N3 Rules have an expressivity which is far higher than the one required by our user preferences, and they are not necessarily the best solution, in terms of efficiency. For this reason, an alternative option is to develop a user preference language which could be efficiently processed by a piece of software designed specifically for this purpose.

[11] See http://www.w3.org/2000/10/swap/doc/cwm.html.

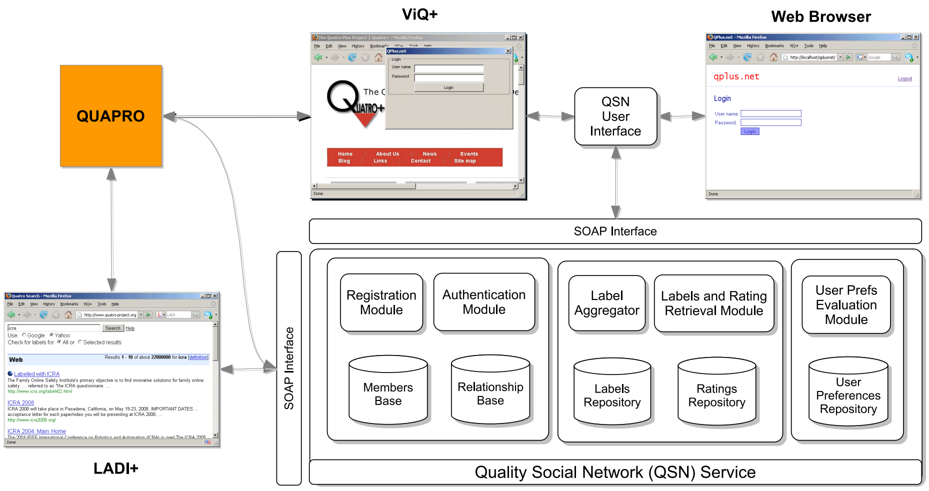

Fig. 6. QSN architecture

4.4 QSN Architecture

The QSN architecture, depicted by Fig. 6, consists of a set of repositories (the member base, which stores members' data and relationships, the user preferences repository, the labels and ratings repositories), storing all QSN data, and of a set of modules in charge of carrying out the supported services (members' registration and authentication, user preferences evaluation, labels and ratings retrieval and aggregation).

In particular, the labels and ratings retrieval module will be in charge of returning the set of labels and ratings satisfying a query, which may concern all the labels and ratings associated with a resource, all the labels and ratings specified by a given member, etc. Such a service will be used by the label aggregator, which is in charge of aggregating and evaluating labels. In turn, the service provided by the label aggregator will be used by the user preferences evaluation module, which will verify whether a given resource satisfies one or more of the user preferences specified by the end user, and then returns the action to be performed by the user agent (ViQ+).

All QSN services will be accessed by the other components of the QUATRO Plus platform through SOAP interfaces. For example, LADI+ will use the results of the statistical analyses of labels and ratings to associate trust values of any available descriptors with search results whilst QUAPRO+ can return the aggregated data regarding the users' ratings on labels applied to a given resource when returning descriptions of it.

The QSN user interface (QUI) will allow end users to register/authenticate on the network, manage their personal data and relationships, specify user-defined labels and ratings, and browse them as a full list or as an aggregate view. As far as the specification of user-defined labels and ratings is concerned, this task will be performed either by an annotation tool, developed specifically for the QSN, or by the Label Management Environment (LME), which end users will be able to transparently access, directly from the QUI. Finally, the QUI can be accessed by QSN members either from ViQ+ or directly through the browser.

5 Related Work

The idea of annotating Web content is not new. It has been proposed as a means of allowing content consumers to easily identify the content that best fits their needs, by means of using established vocabularies to describe the latter.

Such annotations might relate a variety of content aspects, such as language or languages the content is available in, thematic categorisation, suitability for certain devices, suitability for certain age groups, etc. Web content annotation has many analogies that precede the Web and Web content, such as book and film ratings or food and consumer goods labelling for health and safety reasons.

5.1 Visible Trustmarks

Trustmarks of varying kinds have been in existence for as long as people have communicated. The established online form is a logo on a Web page that, when clicked, returns a certificate delivered from the trustmark operator's system confirming that the trustmark is genuine. This has a number of problems however:

- The user must manually follow a link, check that the certificate is genuine and still valid, and so on.
- The website must permit the content provider to add the logo linking back to trustmark operator, which is not always the case.
- Trustmarks are, typically, only visible on a specific page but refer to the whole site, so they can be missed when following search results or external links.
- The trustmarks are invisible to search engines and linked data systems.

These are precisely the problems that the QUATRO Plus project sets out to address. The 'click to verify' action, and all the authentication, can be done automatically. The result can then be presented to the user through the browser chrome (or some other method independent of the Web page) while the data is also made available in a machine-readable format.

5.2 Semantic Web Approaches to Trust

A great deal of work has been done to enable the assessment of the quality, relevance and trustworthiness of online resources using Semantic Web technologies. Mention has already been made of the WIQA Policy Framework [8]. In that paper, Bizer and Cyganiak identify three metrics for assessing quality: content-based (i.e., analyzing the information content itself), context-based (the available metadata) and ratings-based. The QUATRO Plus / POWDER approach is a potential source of both context and ratings-based data. A DR may provide any kind of description of one or more resources, including ratings and details such as who created the resource(s) and when, whether a document was created by a company with a commercial interest and so on. Crucially, such descriptions always carry metadata about themselves so that trustworthiness of the context and ratings-based metrics can themselves be assessed.

In [25], Heath and Motta found that in their particular field of study (travel recommendations), *experience* and *affinity* were the key terms for building a system that personalised search results. Since recommendations about travel destinations is inherently subjective, the wisdom of the crowds (mediated through semantic relationships) is entirely appropriate. QUATRO Plus has the potential to contribute additional information to the system such as awards given to restaurants by professional food critics, clean beach awards given by environmental health experts and so on.

In both these cases, QUATRO Plus offers reliable data of known provenance that complements the approach taken.

5.3 Platform for Internet Content Selection (PICS)

One of the W3C's earliest efforts at content labelling was the *Platform for Internet Content Selection* (PICS) [26], addressing some of the issues with using HTTP headers and HTML meta elements to annotate Web content.

PICS specified a format for bundling content annotations along with scoping and attribution information. Scoping amounted to coupling annotations with a URL prefix, including the ability to specify how more specific prefixes override more generic ones. Although this mechanism allowed for the mass-annotation of websites, it was far too restrictive as URL prefixes cannot capture very commonly encountered groupings. Imagine, for example, a site where all pages under http://www.red.example.com/ share features that pages under http://www.green.example.com/ do not.

An important feature of PICS was the *rating system*, a unique identifier for a vocabulary of rating terms. A client application still had to know how to interpret the terms in the vocabulary, but the rating-system mechanism avoided the danger of misinterpreted annotations.

Finally, clients requested PICS documents through a specific HTTP request-for-labels made to either the content provider's Web server or third-party services known as *label bureaux*. This mechanism allowed for independent annotation services, so that content consumers can decide which annotation provider to trust. Client-side trust policies could also refer further attribution information (such as validity dates) included in PICS documents. The major drawbacks of the HTTP request-for-labels mechanism, however, was the requirement for an extension to the HTTP protocol to handle the PICS-specific HTTP request for labels, and that it did not provide for discovery mechanisms so that user agents had to know in advance which label bureaux to ask.

6 Conclusions and Future Work

The linear model of content annotation that posits a label at one end of a chain and a user agent/gateway at the other was developed in the 1990s and promoted particularly by child protection organisations. Experience shows that such a system, for all its political attractions, is very unlikely to gain widespread adoption. In contrast, social networking and shared tags have been phenomenally successful. The QUATRO Plus project and its forerunner (simply called QUATRO) have tried to marry these two facts together as the fundamental point remains: some people really do know more than others about given subjects. In some situations, experience and knowledge must be allowed to counterbalance public perceptions that may or may not be well-informed. By helping to develop a technical platform to support its aims, one that fits in with much broader efforts to develop the Semantic Web; by providing a suitable software infrastructure and by encouraging the publication of interoperable data, complete with an assessment of trust, we believe that balance can be realised.

Any system needs ongoing technical development and maintenance, together with an infrastructure to support it. Alongside that is the need for dissemination and community building, The latter drives the former and it is the building of that community to which the QUATRO Plus partners are now turning their attention.

Acknowledgements QUATRO Plus is co-funded by the European Union's Safer Internet Programme (SIP-2006-211001) and includes partners from industry, academia and the non-profit sector.

References

1. Archer, P., Smith, K., Perego, A.: Protocol for Web description resources (POWDER): Description Resources. W3C Working Draft (April 2009) http://www.w3.org/TR/powder-dr/.
2. Archer, P., Perego, A., Smith, K.: Protocol for Web description resources (POWDER): Grouping of Resources. W3C Working Draft (April 2009) http://www.w3.org/TR/powder-grouping/.
3. Plale, B., Miles, S., Goble, C., Missier, P., Barga, R., Simmhan, Y., Futrelle, J., McGrath, R., Myers, J., Paulson, P., Bowers, S., Ludaescher, B., Kwasnikowska, N., den Bussche, J.V., Ellkvist, T., Freire, J., Groth, P.: The Open Provenance Model (v1.01). Technical Report 16148, University of Southampton, School of Electronics and Computer Science (July 2008) http://eprints.ecs.soton.ac.uk/16148/.
4. Nottingham, M.: Web linking. IETF Internet-Draft, Internet Engineering Task Force (April 2009) http://www.ietf.org/internet-drafts/draft-nottingham-http-link-header-05.txt.
5. Nottingham, M., Sayre, R.: The Atom syndication format. IETF RFC 4287, Internet Engineering Task Force (December 2005) http://www.ietf.org/rfc/rfc4287.txt.
6. Adida, B., Birbeck, M.: RDFa primer: Bridging the human and data Webs. W3C Working Group Note, W3C (October 2008)

7. Carroll, J.J., Bizer, C., Hayes, P.J., Stickler, P.: Named graphs. Journal of Web Semantics **3**(4) (December 2005) 247–267
8. Bizer, C., Cyganiak, R.: Quality-driven information filtering using the WIQA policy framework. Journal of Web Semantics **7**(1) (January 2009) 1–10
9. Berners-Lee, T., Connolly, D.: Notation3 (N3): A readable RDF syntax. W3C Team Submission (January 2008) http://www.w3.org/TeamSubmission/n3/.
10. Berners-Lee, T., Connolly, D., Kagal, L., Scharf, Y., Hendler, J.: N3Logic: A logical framework for the World Wide Web. Theory and Practice of Logic Programming **8**(3) (May 2008) 249–269
11. Konstantopoulos, S., Archer, P.: Protocol for Web description resources (POWDER): Formal semantics. W3C Working Draft (April 2009) http://www.w3.org/TR/powder-formal/.
12. Clark, J.: XSL Transformations (XSLT) — Version 1.0. W3C Recommendation, W3C (November 1999)
13. Connolly, D.: Gleaning resource descriptions from dialects of languages (GRDDL). W3C Recommendation, W3C (September 2007) http://www.w3.org/TR/grddl/.
14. Brickley, D., Miller, L.: FOAF Vocabulary Specification v0.91. Namespace Document (November 2007)
15. DCMI Usage Board: DCMI metadata terms. DCMI Recommendation, Dublin Core Metadata Initiative (January 2008)
16. Booth, D., Liu, C.K.: Web Services Description Language (WSDL) — Version 2.0 Part 0: Primer. W3C Recommendation, W3C (June 2007) http://www.w3.org/TR/wsdl20-primer/.
17. Carminati, B., Ferrari, E., Perego, A.: Combining social networks and Semantic Web technologies for personalizing Web access. In: CollaborateCom 2008. (November 2008) http://www.dicom.uninsubria.it/dawsec/pubs/collaboratecom2008.pdf.
18. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems **43**(2) (2007) 618–644
19. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The Eigentrust algorithm for reputation management in P2P networks. In: WWW 2003. (2003) 640–651
20. Xiong, L., Liu, L.: PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering **16**(7) (2004) 843–857
21. Adomavicius, G., Tuzhilin, A.: Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. IEEE Transactions on Knowledge & Data Engineering **17**(6) (June 2005) 734–749
22. Sen, S., Lam, S.K., Rashid, A.M., Cosley, D., Frankowski, D., Osterhouse, J., Harper, F.M., Riedl, J.: tagging, communities, vocabulary, evolution. In: CSCW 2006. (2006) 181–190
23. Golbeck, J.A.: Generating predictive movie recommendations from trust in social networks. In: iTrust 2006. (2006) 93–104
24. Avesani, P., Massa, P., Tiella, R.: A trust-enhanced recommender system application: Moleskiing. In: ACM SAC 2005. (2005) 1589–1593
25. Heath, T., Motta, E.: Personalizing relevance on the Semantic Web through trusted recommendations from a social network. In: ESWC'06 SWP Workshop. (2006)
26. Resnick, P., Miller, J.: PICS: Internet access controls without censorship. Communications of the ACM **39**(10) (1996) 87–93