



SWAD-Europe: Deliverable 11.1: Framework for Security and Trust Standards



Project name:

Semantic Web Advanced Development for Europe (SWAD-Europe)

Project Number:

IST-2001-34732

Workpackage name:

WP 11: Distributed Trust Systems

Workpackage description:



<http://www.w3.org/2001/sw/Europe/plan/workpackages/live/esw-wp-11.html>

Deliverable title:


Framework for Security and Trust Standards


URI:

Authors:

 [Brian Matthews](#), CCLRC.

Jan Grant, ILRT

 [Graham Klyne](#), Ninebynine.org.

 [Theo Dimitrakos](#), CCLRC.


 [Juan Bicarregui](#), CCLRC.

Abstract:

The goal of this deliverable is to explore the interaction between various security- and trust-related mechanisms, and to identify enough of the purpose and content of these existing standards to indicate how they might be integrated in a Semantic Web trust and policy management framework.

Status:

Completed report, last modified 2004-07-15.


Comments on this document should be sent to the public SWAD-Europe mailing list,  public-esw@w3.org,

Introduction

The goal of this deliverable is to explore the interaction between various security- and trust-related mechanisms, and to identify enough of the purpose and content of these existing standards to indicate how they might be integrated in a Semantic Web trust and policy management framework.

The scope of this deliverable is extremely wide and accordingly, the deliverable is divided into several major parts, set out in this introductory document.

The following documents form SWAD-Europe deliverable 11.1:

-  [Framework for Security and Trust Standards](#), by Graham Klyne and Brian Matthews

- [Scenarios for using RDF in support of Trust and Access Control](#), by Graham Klyne and Brian Matthews
- [Trust Issues Underpinning Scalable Virtual Organisations](#) by Brian Matthews, Theo Dimitrakos, Juan Bicarregu
- [A Framework for Deploying Trust Policies on the Semantic Web](#), by Brian Matthews, Theo Dimitrakos
- [Recommendation systems as a basis for trust on the Semantic Web](#), by Jan Grant

These documents are described in context below.

Survey of available Web standards for Security and Trust

The field of study for trust is extremely wide. Thus we have carried out some survey work to collect current standards and activities which are relevant to the problem of maintaining trust in its various aspects on the web, and their relevance to the Semantic Web.

- [Framework for Security and Trust Standards](#), by Graham Klyne and Brian Matthews

Scenarios for Trust in the Semantic Web

To illustrate the use of Trust and security in web applications where the Semantic Web can provide some useful tools, we discuss some scenarios for using RDF in support of Trust and Access Control.

- [Scenarios for using RDF in support of Trust and Access Control](#), by Graham Klyne and Brian Matthews

Trust, the Semantic Web and Virtual Organisations

Research on the trust and the Semantic Web has split into several related themes. One is closely related to the work of the *Grid* and web services, where virtual collaborations are set up between entities who are participating in some work towards a common goal across organisational and national barriers. Such *Virtual Organisations* wish to set up a "virtual firewall" to ensure that they can control the information flows between members of the virtual organisation.

Thus we present two documents on this topic. The first illustrates the problems encountered in working with virtual organisations, through an extended example. The other is a short paper which sets out the role of the semantic web in virtual organisations. This paper was published in the *2nd International Conference on Trust Management* Oxford, UK, (March 2004)

- [Trust Issues Underpinning Scalable Virtual Organisations](#), by Brian Matthews, Theo Dimitrakos, Juan Bicarregu
- [A Framework for Deploying Trust Policies on the Semantic Web](#), by Brian Matthews, Theo Dimitrakos

Community based trust-networks and recommendation systems

Another major strand of work which has arisen in the last two years has been the work on *Community based trust-networks*. This has especially been focused on the work of Jennifer Golbeck at the University of Maryland: [Trust and Reputation in Web Based Social Networks](#). See also the [Trust Metrics Evaluation Project](#).

In particular, technologies like FOAF are being used as the basis for many promising social networking applications. The following document by Jan Grant discusses the issues involved with such systems and the use of Dempster-Schafer opinion systems for evaluating trust metrics. It also gives strawman vocabulary for expressing subjective logic opinions (and those expressed using other trust metrics).

- [Trust Metrics Evaluation Project](#)
- [Recommendation systems as a basis for trust on the Semantic Web](#), by Jan Grant

Digital Signatures and RDF

The need arises in many applications to assure the integrity and origin of data. Digital signatures are often used to achieve this. In many applications, a signature can be attached to a serialised form of the RDF in question (that is, the RDF/XML itself is signed using the mechanisms set out in the [XML-Signature Syntax and Processing W3C Recommendation](#)). In those cases, where a document is available, the choice then remains to select from the available technologies to digitally sign documents: either to use a PKI for key management or to adopt a distributed trust-network-based signature system such as PGP; and whether to wrap the payload document with an enclosing signature or to provide a detached signature.

However, in some cases the original serialisation of a graph may be unavailable. It is desirable that, given an RDF graph, a canonical form of the graph can be recovered. Providing that the original signature was of the serialised canonical form, then an equivalent document can be retrieved for signature verification.

In general, graph canonicalisation is a hard problem; however, Jeremy Carroll of HP Labs offers a reasonable compromise solution: [Signing RDF Graphs \(pdf\)](#) by Jeremy Carroll.

In summary, Carroll's approach is to replace an RDF graph with a *semantically equivalent* one - that is, a graph that both entails and is entailed by the original graph - that is amenable to a simple canonicalisation.