



SWAD-Europe: Deliverable 11.1: Scenarios for using RDF in support of Trust and Access Control



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:

[Graham Klyne](mailto:Graham.Klyne@Ninebynine.org), Ninebynine.org.

[Brian Matthews](mailto:Brian.Matthews@CCLRC.ac.uk), CCLRC.

Abstract:

This memo describes some scenarios in which RDF might be used to model trust and access control in networked systems.

Status:

First draft: 2002-12-22

Deliverable release: 2004-06-15

Comments on this document should be sent to the public SWAD-Europe mailing list,

public-esw@w3.org,

-
- [1. Introduction](#)**
 - [1.1 Structure of this memo](#)**
 - [2. Access control](#)**
 - [2.1 Simple access control](#)**
 - [2.2 Access control requiring additional disclosure](#)**
 - [2.3 Role based access control](#)**
 - [2.4 Medical record access](#)**
 - [3. Web provisioned e-commerce service](#)**
 - [3.1 Online software purchase](#)**
 - [3.2 Book purchase](#)**
 - [3.3 Laptop computer purchase](#)**
 - [3.4 Online auction](#)**
 - [4. Home control](#)**
 - [4.1 Home heating and power management](#)**
 - [4.2 Home security](#)**
 - [4.3 Personalized presentation of controls](#)**
 - [5. Network management](#)**
 - [5.1 Internet access from a home network](#)**
 - [5.2 Firewall configuration](#)**
 - [5.3 Virtual Private Network \(VPN\) configuration](#)**
 - [6. Further Work](#)**

7. Acknowledgements

§ References

1. Introduction -

TOC&nb sp:

This memo describes some scenarios in which RDF [2][3] might be used to model trust and access control in networked systems. The intent is to propose some systems that could form the basis of some experimental modelling in RDF, to learn if and how RDF can be used to support trust in open systems.

The scenarios examined are based around the following themes, in each case considering a number of variations of increasing complexity:

- Access control to a data resource on a network.
- Web provisioned e-commerce service.
- Home control.
- Network management.

1.1 Structure of this memo

Each of the following sections 2-5 develops scenarios inspired by one of the trust management themes mentioned above. Within each theme, the various scenarios are presented in a sequence that is believed to allow an experimental implementation of each to be based on, and extend, implementations of the preceding, simpler, cases.

2. Access control -

TOC&nb sp:

Access control is concerned with controlling access to network resources by means of policies which associate access rights directly or indirectly with a user's authenticated identity, and possibly some additional information.

The role based access control scenarios considered are:

- Simple access control
- Access control with additional disclosure and privacy policy
- Role based access control
- Medical record access

In advanced scenarios, not described here in detail, access control maybe based on authorizing decisions made in different administrative domains. A common example of this is access to the member-only area of the W3C web site: employees of member organizations are permitted such access. A member organization designates a person who is authorized by W3C to name individuals who are employees of the member organization. The combination of these authorizing decisions is used as the basis of access control. (This idea is described more fully in Semantic Web Development Technical Proposal[8] and W3C Semantic Web Activity[9]; see also Weaving a Web of Trust[10]). The role based access control scenario describes the first steps to creating such a distributed access control decision structure.

Note that access control may be applied in a very direct sense, i.e. controlling simple access to some information, or in a more comprehensive fashion, dealing not only with access, but addition, change or removal of information, or performing actions that affect resources other than just information.

2.1 Simple access control

This scenario considers very simple access control to a network resource, keyed directly from the identity of the principal who is requesting access. (How that identity is determined and verified is

not covered in this scenario.)

The access control is described in terms of:

- a Principal (P) who attempts to access some network resource,
- a Resource Server (RS) that provides access to the resource, and
- an Access Control policy decision server (AC) that makes decisions about whether or not access is permitted.

The process for accessing the resource is:

1. The Principal (P) requiring access sends a request to the resource server (RS).
2. RS fields request and forwards details to access control policy decision server (AC).
3. AC returns a decision on access to RS (permit, deny + obligations).
4. RS checks obligations, and performs any required actions.
5. RS acts on original request.
6. RS returns response containing resource data to P.

Obligations are mentioned above. These refer to the idea that there is some action associated with granting access to a resource. For example, it may be that all access must be logged, or a payment is required. Some obligations may be under control of the resource server (e.g. logging) and others may require cooperation of the principal to whom access is granted (e.g. payment).

2.2 Access control requiring additional disclosure

The simple access control scenario is extended by a requirement that the requesting principal discloses some additional information before access to the resource is granted. This information may be sensitive in nature, and the resource server must indicate what use will be made of this data (e.g. using [P3P](#) [4].)

The access control is described in terms of the same parties that participate in the simple access control scenario.

The process for accessing the resource is:

1. The Principal (P) requiring access sends a request to the resource server (RS).
2. RS fields request and forwards details to access control policy decision server (AC).
3. AC needs additional information from requester: sends request back to RS.
4. RS sends request for additional to P, accompanied by privacy policy information (e.g. P3P).
5. P checks privacy policy, and provides requested information to RS. This requires a trust assessment on the part of P.
6. RS passes the additional information to AC.
7. AC returns a decision on access to RS (permit, deny + obligations).
8. RS checks obligations, and performs any required actions.
9. RS acts on original request.
10. RS returns response containing resource data to P.

2.3 Role based access control

Role based access control is concerned with controlling access to network resources by means of policies which associate access rights with assigned roles.

This scenario is essentially similar to the previous scenarios (with or without a requirement to disclose additional information), in which the principal first performs an authentication step that verifies they have been authorized to operate in some given role. Access rights are then specified in terms of authorized roles rather than the identity of the accessing party. Thus, a role serves as a level of indirection between authentication and access control policy, creating scope for simplification of some management tasks.

The access control is described in terms of the same components considered previously, with the addition of:

- An Identification Server (IS) that accepts identifying credentials from a principal, verifies

them in some way, and indicates the roles in which the principal may act;

The process for accessing a resource is revised as:

1. The Principal (P) connecting to the system contacts the Identity Server (IS), supplying appropriate credentials. IS checks the credentials and determines the roles in which P is allowed to act.
2. P, requiring access to some resource, sends a request to the resource server (RS), indicating the role in which it is acting.
3. RS fields the request and verifies that P is authenticated and authorized for the requested role. Various verification mechanisms are possible: P may provide cryptographically secured credentials issued by IS as part of the authentication step; or RS may contact IS directly to check the role is authenticated to the requesting party (assuming some secure form of identification is available).
4. RS forwards details of the request and role to the access control policy decision server (AC).
5. AC returns a decision on access to RS (e.g. permit, deny + obligations).
6. RS checks obligations, and performs any required actions.
7. RS acts on the original request.
8. RS returns a response containing resource data to P.

Roles could be viewed as a kind of ontology of users, and ontological reasoning may be an effective way of mapping policies to access decisions.

When using role based access control, the access control decision may extend to requiring additional information from the Principal, for which there may be privacy considerations (see previous scenario). Role based access control is based on role rather than personal details; privacy concern suggests a personalized level of access, which might therefore be not entirely consistent with role based access control.

2.4 Medical record access

This scenario is taken directly from the OASIS XACML technical committee [Use Cases document](#)[5]. It introduces a number of specific access control considerations concerning access to medical records in a variety of circumstances.

Refer to pages 1-4 of [XACML Use Cases](#)[5] for details of this scenario and its variants.

3. Web provisioned e-commerce service -

[TOC sp;](#)

These scenarios are concerned with payment for and subsequent delivery of a service.

The scenarios considered are:

- Online software purchase.
- Book purchase.
- Laptop computer purchase.
- Online auction.

In the future, consideration may be given to extensions of this theme to brokerage and composition of services. See the section [Further work](#).

3.1 Online software purchase

This scenario is about the simplest online purchase I could conceive. By focusing on online delivery, and assuming that the software product has been evaluated, the complications of physical delivery and trust that the delivered product will perform as required are avoided.

The purchase is described in terms of:

- a Purchaser (P) who is paying for some product or service,
- a merchant (M) who is providing the product or service, and
- a customer payment service (PS), e.g. bank or credit card company, who the purchaser authorizes to make payment on their behalf.
- a merchant payment collection service (MS) that collects funds from PS and transfers them to the vendor.

The process for purchasing the product or service is:

1. The Purchaser (P) initiates a transaction with the merchant (M), indicating details of the product to be purchased.
2. M fields the request and requests payment details from P. The request is accompanied by a privacy policy statement that indicates what use will be made of any information collected.
3. P evaluates the privacy policy and provides payment details. This requires P to make some trust evaluations: that M will use the information provided for only the disclosed purposes, and, on receipt of confirmation of payment, M will make the purchased product or service available to P. P must also trust the payment service (PS) that only the agreed payment will be transferred.
4. M receives payment details and passes them to the payment collection service MS. This may require that M have some reasonable degree of trust in the details provided, because there may be costs associated with presenting bad payment details.
5. MS confirms that the payment details are valid. If MS has a trusting relationship with PS, confirmation may be by direct communication with PS, otherwise with some other party with whom both MS and PS have a trusting relationship.
6. MS returns confirmation of payment authorization to M. In some cases, this may be a provisional confirmation, and M must make a trusting decision whether or not to proceed with the transaction.
7. M authorizes P to access the software product or service, and sends details of how to exercise the permission granted.
8. P accesses the product or service.
9. M submits payment authorization details to MS for subsequent transfer of funds. This should be linked to some kind of audit trail so that M can demonstrate that the transaction for which payment is claimed was in fact completed.
10. MS interacts with PS to effect the funds transfer.

Future consideration may be given to extensions of this scenario to deal with claims by P that a funds transfer was not properly authorized. A number of different models may exist for apportioning risk in such circumstances.

3.2 Book purchase

This scenario extends the previous one in that a physical delivery from merchant (M) to purchaser (P) must be performed in order to complete the transaction.

The basic procedure is the same as the previous scenario, except that a trusted delivery service is needed, and some kind of evidence of delivery may augment or replace the online transaction audit.

The required trust relationships are also similar, except that M incurs real costs in procuring and shipping physical goods, so the details of risk analysis may vary.

A possible variation of the procedure would be cash on delivery, in which payment for the goods is collected by the delivery service and passed to the merchant. This may greatly reduce the required trust between P and M, but M, and possibly P, must have some kind of trusting relationship with the delivery service.

3.3 Laptop computer purchase

This scenario extends the previous one in a number of respects:

- The value of goods is very much higher, so the risks are correspondingly different.
- There is a significant possibility that the goods are not suitable, or may be broken. (While this may be possible with books, it is not normally an issue.)
- Buying a "big ticket" item online, without actually being present to evaluate the goods, the purchaser (P) may choose to rely on some reviewing (or rating) service (R) to provide an evaluation of the product and its suitability for some purpose(s).
- In selecting goods to be purchased, the purchaser may take into account the brand reputation of the manufacturer (B).

The issue noted above as "brand reputation" touches on a key area for trust management: direct and indirect experience with a given supplier may have a significant effect on the level of trust that is appropriate to extend in a given circumstance.

In view of the above, the following steps may take place prior to the purchasing transaction:

1. The Purchaser (P) consults one or more reviewing (or rating) services (R) for evaluations of products of interest. This implies that P has some degree of trust in R.
2. Based on reviews consulted, P makes a decision about what product to purchase. In making this decision, P must have some level of trust in the brand manufacturer (B) that an instance of the chosen product will correspond in important respects to that which was reviewed.
3. In selecting a merchant (M) from which to make a purchase, P must make a trust evaluation concerning the service quality and after sales support provided by the combination of B and M (which may also be informed by consulting reviewing services).
4. In some cases (notably, credit card companies), the payment service (PS) may provide some additional guarantee of compensation in the event that the goods supplied are inappropriate or broken on arrival.

Once P has made a purchasing decision, the purchase transaction is the same as the previous scenario, except that the higher value of the goods will affect the risk assessment for all parties.

3.4 Online auction

The previous scenarios assume that the purchaser (P) has some knowledge of the merchant (M) from whom they are purchasing. The online auction scenario may change this, in that it is a means for any person or company to offer one-off items for sale.

In an on-line auction, the auction service (A) is an intermediary between P and M for the purposes of agreeing a sale, though P and M alone may be responsible for completing an agreed transaction.

Also different in an online auction is that when the purchaser makes an offer, they don't know if it will be accepted.

So, in an online auction, the trust relationship is significantly more difficult to evaluate:

- P may have little or no information about M upon which to make a trust assessment.
- P may have to rely on secondary guarantees (e.g. from a payment service (PS) or from A).
- M may not have a trusting relationship with any payment collection service. So it may be necessary for P and M to establish some kind of direct trust relationship in order to complete an agreed purchase transaction.
- Taken together, the above points mean that both P and M must exercise greater levels of trust and have less information on which to make trust assessments, compared with a normal merchant/customer relationship.
- Both P and M must trust A that all valid bids will be properly tallied, without any form of discrimination among bidders.

The auction itself is a process which takes place prior to the purchasing transaction between P and M, which (apart from the trust issues already noted) should not be greatly different from purchase transaction processes described previously.

It is difficult to discern a clear pattern of trust relationship in an online auction, and this could be a fruitful area for investigation of various possible trust relationships.

The eBay auction model extends the role of the auction service in two significant ways,

both of which aim to address the issue of trust:

1. The service operates a "rating forum", in which users offer feedback from their experience of trading with other parties. These are presented back to all users in the form of a rating, which has the intended effect of discouraging or exposing bad faith behaviour and increasing overall levels of trust.
2. The auction service is a "matchmaker", and does not have any direct participation in the final transaction between seller and buyer. But it does (in the UK) act as a guarantor of last resort: see <http://pages.ebay.co.uk/help/community/fpp.html>. (In the US, there is a product warranty service: see http://pages.ebay.com/help/warranty/seller_overview.html.)

4. Home control -

[TOC SP;](#)

This theme examines the role of trust and access control in a home control network that includes a number of simple embedded devices.

In these scenarios, we are concerned with interactions between:

- embedded home control and sensor devices (which may not of themselves be capable of implementing any meaningful security),
- web-accessible personal information (which may be of a personal or confidential nature), and
- remote access (via Internet) to physical aspects of one's personal space.

The scenarios considered here are:

- Home heating and power management
- Home security
- Personalized presentation of controls

4.1 Home heating and power management

This scenario considers the following elements:

- A continuous process switches the home heating to maintain a target temperature indoor temperature, and lighting to achieve appropriate levels of illumination, dependent on occupancy and time of day.
- A web calendaring service provides planned occupancy information (at home, away during daytime, away for several days) for each of the home's normal occupants.
- Occupancy information may be temporarily overridden by local control, or by remote command
- Alternative occupants may be specified for scheduled intervals (e.g. visitors).

The following security concerns should be considered:

- Authority to set system configuration details, such as target temperature under certain circumstances. Inappropriate setting could lead to wasted energy, discomfort or frost damage.
- Authority to set information about occupancy. Inappropriate setting could lead to wasted energy or discomfort.
- Authority to remotely override normal settings.
- Access to information about normal occupants, and especially to information about their movements.
- Access to information about alternative occupants, and especially to information about their movements.

4.2 Home security

The previous example is extended to home security, where more complex behaviours may be needed to ensure that security is maintained.

The following elements are considered:

- occupancy detectors,
- occupants' schedules,
- lights,
- alarms, and
- door lock operation.

The following actions and situations might be considered:

- Doors can be opened by local key or authenticated remote command.
- Occupancy detectors trigger alarm when there is no authorized occupancy.
- Opening a door with key together with some form of authentication indicates that there is authorized occupancy.
- Open door with remote command indicates authorized occupancy which may be for a limited time interval.
- Using a key to lock the doors indicates that authorized occupancy is finished.
- A short period of no detected occupancy at a time when occupancy is not scheduled terminates any authorization of occupancy.
- A longer period of no detected occupancy at a time when occupancy is scheduled cancels any authorization of occupancy.
- At night time without any detected occupancy, lights are operated in a pattern suggesting people are present.
- Any authorized occupancy not in accordance with schedule triggers an alert (not an alarm), which can be received up remotely (e.g. by web access or phone message).

The possible combinations of trigger events and responses here become quite complex, so this scenario would challenge the use of RDF to represent rules, and using them to determine appropriate responses to different combinations of events.

A possibly important capability to explore in this scenario is the detection of conflicting or otherwise conflicting rules.

4.3 Personalized presentation of controls

A typical home has very many different permanent and temporary occupants, with very different levels of trust and ability; e.g. the home owner, children, family friends, visiting traders, etc.

The following elements are considered:

- occupancy detectors,
- temperature sensors,
- light sensors,
- door sensors,
- cameras and camera controls,
- voice messages,
- lights,
- alarms,
- door controls,
- remote access, and
- possibly many other forms of system interface.

Operation of facilities that are needed by all (e.g. local operation of lights) should be simple and direct. Access to other facilities, and disclosure of associated information, should be limited to those with the authority and ability to use them.

A number of different devices might participate in the control scenario, including many with "soft" interfaces (e.g. mobile telephones, PDAs with infrared or Bluetooth interface, universal remote control devices, computer terminals). The interface that is presented to an authenticated user of such a device could be tailored to present only those interface elements that they are

authorized to use.

Thus, when accessing the system, a user interface is constructed to dynamically reflect the information and controls available to the authenticated user. For example, some may have access to all facilities; others may be permitted only to access their own voice messages and turn lights on and off.

This is another scenario that could be used to test the use of RDF to represent rules, and using such descriptions to determine system behaviour. The selection of access rights must be based on trust assessments of the various users.

5. Network management -

[TOC sp:](#)

This theme examines the interactions between network management, access control and trust. Network devices enforces access control, and are also subject to access control.

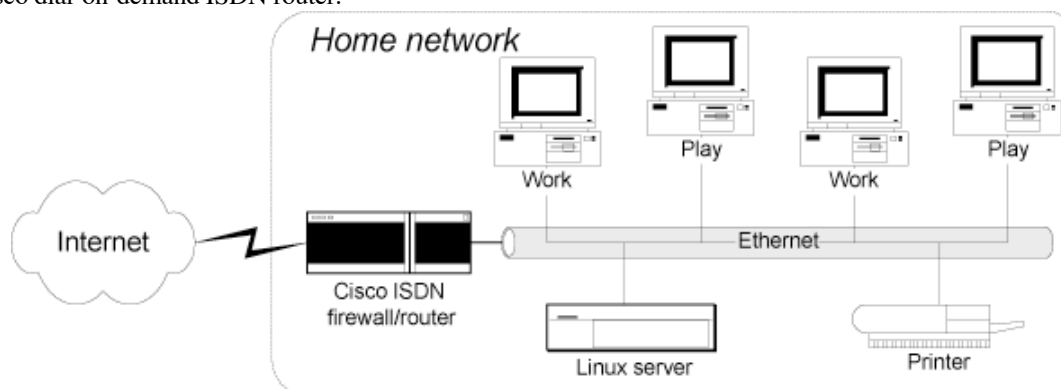
An important feature is the ability to fully utilize existing network security enforcement devices, as well as suggesting design directions for new security components.

The scenarios considered are:

- Internet access from a home network.
- Firewall configuration.
- Virtual Private Network (VPN) configuration.

5.1 Internet access from a home network

This scenario uses RDF metadata in a home business network connected to the Internet by a Cisco dial-on-demand ISDN router.



This illustration is also available in [PDF format](#)

Network access is provided by an ISP dial-up account that provides unmetered access up to a specified weekly limit.

The network users are two parents who use the Internet for business, and two children who use it for play and social purposes. The working adults require occasional access at any time. The children's access has to be restricted, otherwise they would quickly exceed the total connect time allowed by the ISP.

The Cisco ISDN router runs Cisco's proprietary IOS software, which has a system of IP-addressed based filters that are quite capable of restricting access at different times based on the IP address of the internal host. Creating the correct IOS configuration files for this kind of selective filtering is quite a tricky task. The router can accept an externally defined configuration via the TFTP protocol.

Within the local network, machines are assigned IP addresses using DHCP. The DHCP service is provided by a Linux host running DHCPD and a local DNS service.

Given all this, the goal is to use RDF to specify the access policy and device configuration requirements, and use RDF tools to generate the desired configuration files for the Cisco ISDN router and the Linux-based services.

A demonstration of this scenario has been implemented. The implementation is described by [Using RDF for Home Network Configuration\[7\]](#). See also <http://www.ninebynine.org/SWAD-E/Intro.html#HomeNetAccessDemo>.

5.2 Firewall configuration

Using common Linux system and software to implement a router/firewall, extend the tools described in the previous scenario to generate all necessary firewall system configuration files from an access policy description presented in RDF.

This might be extended to include corporate network security configuration, where multiple configuration files are generated for the various firewall and other security policy enforcement devices in a network.

5.3 Virtual Private Network (VPN) configuration

Virtual Private Network (VPN) configuration involves not only the establishment of appropriate security policies for network access, and protecting the network from unauthorized access, but also the marshalling of resources to provide secure connectivity, possibly stretching over several administrative domains.

The capability to work with a range of different network device types is crucial, as different administrative domains may use different kinds of equipment. Driving configuration of diverse devices from a common policy file, as illustrated above, would be a key goal of this scenario. Also required is that the configuration details are bound to appropriate authenticating information so that property security and charge-back arrangements can be maintained across multiple domains. Authenticated priority information is also required, so that appropriate allocation of resources can be achieved.

The various levels of authentication will be derived from trust relations between the various participants. In some cases, proof-carrying authentications might be used to permit participation of principals who are not themselves known to the party who is providing them with access to resources.

Details of this scenario are rather vague. To develop this more fully will require some greater knowledge of VPN technologies than I possess. The scenario is mentioned here because I understand there is a real desire for adequate solutions to this problem, and it seems to be a well defined problem that shares many requirements with grid computing.

6. Further Work -

[TOC&nb
sp;](#)

These scenarios only scratch the surface of the possible role of semantic web technologies in authorization and trust management.

This work is motivated in part by a need for a manageable framework for trust and security in grid services, which involves the composition of a service from component parts that are generally under control of different administrative domains.

Just a few possible areas of further work are:

- Automatic contract formation: automated interaction that may determine the terms and conditions for a service, the cost and the conditions under which payment will become due.
- Extending e-commerce scenarios to include brokerage, where one party may act as a sub-contractor, composing a service from third party suppliers, handling risk analysis issues to deliver a required quality of service. This is a significant extension of the online auction scenario in which a service acts as a transaction intermediary.
- Develop the VPM scenario to fully define a scenario involving delegation of authorization and resource allocation decisions across administrative domains.
- Dynamic access control configuration: the scenarios described here deal only with checking access control against some (presumed) static database; when access control permissions update dynamically, some additional mechanisms may need to be considered.

7. Acknowledgements -

[TOC&nb
sp;](#)

Some of the scenarios described here have resulted from discussions with Brian Matthews and Michael Wilson of Rutherford Appleton Laboratory. The network configuration ideas have been inspired in part by an architectural proposal for network configuration using XML [\[16\]](#).

This document has been authored in XML using the format described in RFC 2629 [\[11\]](#), and converted to HTML using the XML2RFC utility developed by Marshall Rose (<http://xml.resource.org/>).

References -

[TOC sp;](#)

- [1] [Rose, M.](#), "[Writing I-Ds and RFCs using XML](#)", RFC 2629, June 1999.
- [2] [Lassila, O.](#) and [R. Swick](#), "[Resource Description Framework \(RDF\) Model and Syntax Specification](#)", W3C Recommendation rdf-syntax, February 1999.
- [3] Brickley, D. and R. Guha, "[Resource Description Framework \(RDF\) Schema Specification 1.0](#)", W3C Candidate Recommendation CR-rdf-schema, March 2000.
- [4] [Marchiori, M.](#), Cranor, L., Langheinrich, M., [Presler-Marshall, M.](#) and J. Reagle, "[The Platform for Privacy Preferences 1.0 \(P3P1.0\) Specification](#)", W3C Recommendation REC-PICS-services, April 2002.
- [5] Moses, F., "[Clinical Record Use Cases](#)", OASIS Committee Working Draft draft-xacml-usecase-01a, September 2001.
- [6] Atarashi, R., Shimojo, T., Atarashi, Y., Miyake, S., Kitani, M., Baker, F. and M. Wasserman, "[XML Configuration Architecture](#)", draft-atara shi-xmlconf-architecture-00 (work in progress), October 2002.
- [7] Klyne, G., "[Using RDF for Home Network Configuration](#)", December 2002.
- [8] Berners-Lee, T., "[Semantic Web Development: Technical Proposal](#)", February 2001.
- [9] Koivunen, M. and E. Miller, "[W3C Semantic Web Activity](#)", November 2001.
- [10] Khare, R. and A. Adam, "[Weaving a Web of Trust](#)", November 1997.

Appendix A. Revision history -

[TOC sp;](#)

2002-12-17:

- *Document initially created.*
- *Created content scenarios outline.*
- *Added descriptions of access control and home network Internet access scenarios.*

2002-12-18:

- *Added CCLRC copyright notice.*
- *Added description of home control and network management scenarios.*

2002-12-22:

- *Revised content of document following hand-over review with Brian Matthews.*
- *Added scenario for role based access control. Suggest use of ontological reasoning for role-based authorization decisions.*
- *Added references to W3C web site member access control.*
- *Mention that access control can be more than just access to data.*
- *Say something about the nature of obligations in access control.*
- *Add note about access control across administrative domains.*
- *Add note of possible further work to explore contract formation, transaction intermediaries and and composed services.*
- *Note the role of brand reputation in establishing trust.*
- *Mention use-case of auction service as transaction intermediary. Mention the eBay rating system and guarantee of last resort.*

- *In home control systems, note that the scenarios involve interaction between embedded devices and internet services and data.*
- *Add note about detection of rule conflicts as a topic for home security.*
- *Spell-checked content.*