TrustCoM

Deliverable

43

Standardisation Roadmap v3

WP13 Standards and Collaboration

Joris Claessens (editor)

European Microsoft Innovation Center

May 2006

Version 1.0

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

LEGAL NOTICE

The following organisations are members of the Trustcom Consortium:

Atos Origin,
Council of the Central Laboratory of the Research Councils,
BAE Systems,
British Telecommunications PLC,
Universitaet Stuttgart,
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,
Swedish Institute of Computer Science AB,
Europaeisches Microsoft Innovations Center GMBH,
Eidgenoessische Technische Hoschschule Zuerich,
Imperial College of Science Technology and Medicine,
King's College London,
Universitetet I Oslo,
Stiftelsen for industriell og Teknisk Forskning ved Norges Tekniske Hoegskole,
Universita degli studi di Milano,
The University of Salford,
International Business Machines Belgium SA .

Neither the Trustcom Consortium, any member organisation nor any person acting on behalf of those organisations is responsible for the use that might be made of the following information.

The views expressed in this publication are the sole responsibility of the authors and do not necessarily reflect the views of the European Commission or the member organisations of the Trustcom Consortium.

All information provided in this document is provided 'as-is' with all faults without warranty of any kind, either expressed or implied. This publication is for general guidance only. All reasonable care and skill has been used in the compilation of this document. Although the authors have attempted to provide accurate information in this document, the Trustcom Consortium assumes no responsibility for the accuracy of the information.

Information is subject to change without notice.

Mention of products or services from vendors is for information purposes only and constitutes neither an endorsement nor a recommendation.

IBM, the IBM logo, ibm.com, Lotus and Lotus Notes are trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries or both.

SAP is a trademark of SAP AG in the United States, other countries or both.

'BT' and 'BTexact' are registered trademarks of British Telecommunications Plc. in the United Kingdom, other countries or both.

Other company, product and service names may be trademarks, or service marks of others. All third-party trademarks are hereby acknowledged.

Deliverable datasheet

Project acronym: TrustCoM

Project full title: *A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations*

Action Line:	**4**
Activity:	**4.1**
Work Package:	**13**
Task:	**13.1**

Document title:	**Standardisation Roadmap v3**
Version:	**1.0**
Document reference:	
Official delivery date:	**30 April 2006**
Actual publication date:	
File name:	
Type of document:	Report
Nature:	Public

Authors: Alvaro Arenas (CCLRC), Jesus Benedicto (AtosOrigin), David Chadwick (UoK), Joris Claessens (EMIC), Theo Dimitrakos (BT), Ivan Djordjevic (BT), Pablo Giambiagi (SICS), Jochen Haller (SAP), Yücel Karabulut (SAP), Nikolaos Oikonomidis (SAP), Erik Rissanen (SICS), Philip Robinson (SAP), J Sairamesh (IBM), Lutz Schubert (HLRS), Ignacio Soler (AtosOrigin).

Reviewers: Michael Wilson (CCLRC),
Ignacio Soler (AtosOrigin)

Approved by:

Version	Date	Sections Affected
1.0	August 2004	First published version of the Standardisation Roadmap.
2.0	September 2005	Standardisation Roadmap v2
3.0	May 2006	Standardisation Roadmap v3

Table of Content

1 Executive summary

The TrustCoM project is developing a framework for trust, security, and contract management for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. TrustCoM is committed to the adoption of open standards, and intends to build upon and extend interoperability specifications where necessary and appropriate.

Standards and collaboration are a way to promote and achieve interoperability between technologies across different vendors. While businesses need to balance between agreed functionality, competitive advantage, and need for interoperability, interoperability is a key requirement in today's multi-vendor market. Standardisation is an important part of successful exploitation. TrustCoM therefore aims at building upon existing well established and accepted standards and published specifications, where appropriate. TrustCoM furthermore intends to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM participates in European project clustering activities in order to maximize impact of the project and avoid duplication of effort.

This document is the TrustCoM deliverable D43, and is version 3 of the project's Standardisation Roadmap. The Standardisation Roadmap supports and documents the standardisation activities within the TrustCoM project, and is regularly updated throughout the lifetime of the project.

This deliverable focuses on the project's status and plans for promoting interoperability of the technical work in each of the TrustCoM subsystems, with the outside world. The concrete impact from (using) and to (contributing) standards as well as collaborative efforts is assessed and planned. The main reference is the TrustCoM Framework V2 – see deliverable D29-35-36 (February 2006) – and the corresponding ongoing software developments.

For each of the TrustCoM subsystems, this deliverable:

- analyses the relevance of interoperability for each of the artefacts in the subsystem,
- provides an updated positioning of the relevant existing standards and specifications,
- provides concrete results, plans, or expectations for future standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of TrustCoM work.

Besides the above mentioned deliverable D29-35-36, the main input/reference deliverables for this work are deliverable D24 TrustCoM Standardisation Roadmap v2, deliverable D28 State-of-the-Art Update, and deliverable D40 Collaboration Activities Report.

This deliverable provides feedback to the standards world on the applicability of existing specifications within the TrustCoM framework. We also inform the outside world of the standards choices made for V2 of the framework, in order to get feedback and to promote interoperability with products and services as well as research work in other projects.

It is important to emphasise that TrustCoM is an *integrated* project addressing trust, security, and contract management, for collaborative business processing, as a whole, focusing on the relationships and interactions between, and integration of, these issues, rather than investigating each of these issues separately and independently. The primary focus of the TrustCoM standardisation activity is expected to be in the creation of profiles that integrate existing standards *across* the different areas. While there are already numerous specifications addressing various issues within most of the identified areas, there are almost no concrete guidelines at all with respect to combining different specifications into a single interoperable framework.

2 Introduction

The TrustCoM project [http://www.eu-trustcom.com/] is developing a framework for trust, security, and contract management for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. TrustCoM is committed to the adoption of open standards, and intends to liaise closely with the relevant industry and standardisation forums, in order to ensure that the TrustCoM framework builds upon and extends existing and emerging interoperability standards.

The term "TrustCoM Framework" stands for the principles and paradigms, the processes and functions, and the architecture and the technology that underpin trustworthy, secure, and contract-driven operations of Virtual Organisations. However, when using the term "TrustCoM framework" in this deliverable, we mainly refer to the technological aspects, and how these are related to ICT standards and specifications. Other aspects of the TrustCoM framework, such as the socio-economic and legal analysis, have less bearing on this workpackage.

2.1 TrustCoM standardisation and collaboration objectives

Achieving the scientific and technological objectives of TrustCoM necessitates integration in several dimensions, including standards. Standards and collaboration are a way to promote and achieve interoperability between technologies across different vendors. While businesses need to balance between agreed functionality, competitive advantage, and need for interoperability, interoperability is a key requirement in today's multi-vendor market. Standardisation is an important part of successful exploitation. TrustCoM therefore aims at building upon – where appropriate – existing well established and accepted standards and published specifications, as the basis for the TrustCoM framework. If new technology is not compatible with existing standards that are well established in the market, then it may be more difficult to commercialize this into products and services which can interact with products and services provided by others. TrustCoM furthermore plays a significant role in testing and enhancing emerging standards and interoperability guidelines, and intends to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM participates in European project clustering activities in order to maximize impact of the project and avoid duplication of effort.

The overall objectives of the TrustCoM standardisation activity are twofold:

1. The standardisation activity must ensure that TrustCoM leverages the most up to date relevant standards and interoperability guidelines within its framework specifications and reference architecture. Existing / candidate open standards, and their associated software and systems engineering paradigms, will provide the basis for the applied research and technological development of TrustCoM.
2. The standardisation activity must ensure that the results of TrustCoM contribute to the future developments of standards for trust, security and contract management, where appropriate. Proposed improvements of these standards will be realised as interoperable extensions or revisions. TrustCoM will also be breaking ground in areas where no candidate specifications exist. In such areas, TrustCoM will propose new standards based on its Framework specifications, which are put forward to the appropriate technical committees for development and eventual ratification.

These standards activities – and further supported by collaboration activities – must promote interoperability from a technical ("standards") as well as a business objective (business models) perspective.

It is important to emphasise that TrustCoM is an *integrated* project addressing trust, security, and contract management, for collaborative business processing, as a whole, focusing on the relationships and interactions between, and integration of, these issues, rather than investigating each of these issues separately and independently. The primary focus of the TrustCoM standardisation activity is expected to be in the creation of profiles that integrate existing standards *across* the different areas. While there are already numerous specifications addressing various issues within most of the identified areas, there are almost no concrete guidelines at all with respect to combining different specifications into a single interoperable framework.

2.2 TrustCoM Standardisation Roadmap

The TrustCoM Standardisation Roadmap supports and documents the standardisation activities within the TrustCoM project, and is regularly updated throughout the lifetime of the project.

D6 Standardisation Roadmap v1 (August 2004) was made available at the end of the project's initial scoping and requirements phase, and established a first baseline for further standardisation activities. Version 1 of the roadmap identified the standardisation areas which are relevant to the project, and provided an initial assessment of the state of standardisation in each of these areas.

The identified TrustCoM standardisation areas are:

- Trust, PMI and PKI
- Contracts and SLAs
- Policies and Security
- Collaborative business processes
- Web and Grid services
- Semantic technologies[1]
- Model driven security[2]

D24 Standardisation Roadmap v2 (September 2005) gave a precise positioning status for each relevant standard and published specification, with respect to each subsystem in the first implemented version of the TrustCoM framework. D24 also formulated a forward look for standards impact to/from TrustCoM in each area, updating the broad standards assessments given in the first version of the roadmap, and concentrating on the envisaged adoption of standards in v2 of the framework (i.e., expected future impact from standards on TrustCoM), and on potential profiles or other specific standards contributions arising in each area – and particularly across areas – from the developments so far (i.e., potential envisaged impact from TrustCoM on standards).

The assessed subsystems of the TrustCoM framework were:

- VO Management
- Business Process Management
- SLA Management
- Trust and Security Services
- Policy Control
- EN/VO Infrastructure
- Methods & Tools[2]
- Applications

[1] We indicated in D24 that TrustCoM does not intend to contribute nor use Semantic technologies.

[2] We indicated in D24 that TrustCoM does not intend to pursue standards work in the Model driven security area or for the Methods & Tools subsystem.

2.3 Scope of this deliverable

This deliverable is version 3 of the project's Standardisation Roadmap, and focuses on the project's status and plans for promoting interoperability of the technical work in each of the TrustCoM subsystems, with the outside world. The concrete impact from (using) and to (contributing) standards as well as collaborative efforts is assessed and planned. The emphasis in this deliverable is on the technical perspective of interoperability, and less on the business models.

The main reference is the TrustCoM Framework V2 – see deliverable D29-35-36 (February 2006) – and the corresponding ongoing software developments. The TrustCoM subsystems relevant in this deliverable are:

- VO Management
- Business Process Management
- SLA Management
- Trust and Security Services
- Policy Control
- EN/VO Infrastructure
- Applications

For each of the TrustCoM subsystems, this deliverable:

- analyses the relevance of interoperability for each of the artefacts in the subsystem,
- provides an updated positioning of the relevant existing standards and specifications,
- provides concrete results, plans, or expectations for future standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of TrustCoM work.

Besides the above mentioned deliverable D29-35-36, the main input/reference deliverables for this work are deliverable D24 TrustCoM Standardisation Roadmap v2, deliverable D28 State-of-the-Art Update, and deliverable D40 Collaboration Activities Report.

As with the previous versions of the standardisation roadmap, this deliverable collects the positioning status across the technical WPs, but does not intend to provide an in-depth justification for each specific positioning. We refer to the technical deliverables for specific technical details.

2.4 Outline of this deliverable

Chapter 3 explains the TrustCoM standardisation approach, and discusses the concept and role of standards, and the relevance to TrustCoM, in more detail. This chapter is entirely taken from the Standardisation Roadmap v2, and included again in this deliverable. Chapter 4 presents the standards positioning and roadmap for each of the TrustCoM framework subsystems. Chapter 5 gives some concluding remarks. Chapter 6 provides a table of the standards and specifications that are relevant to the TrustCoM framework, and as the references list of this document.

3 TrustCoM standardisation approach

This section provides some background as to what TrustCoM considers as being a "standard", which standards areas are generally relevant to TrustCoM, and which kind of standards contributions are envisaged.

3.1 The concept of "Standard"

3.1.1 Role of "standards"

The main role of IT "standards" is to *promote interoperability across different vendors' platforms*. However, vendors are businesses who need to maintain competitive advantage through their own unique selling points. Therefore, successful standards are defined at a core layer in the information architecture at which most major vendors agree that the advantage of interoperability outweighs the need for competitive advantage.

In the web and web services areas, URL's, HTTP and XML are standardised, since the need for interoperability outweighs competitive advantage for these core technologies. The packaging technology of SOAP, and the Web Service Description Language (WSDL) are also examples of core technologies where the required functionality is agreed, and the need for interoperability outweighs the need for competitive advantage.

Our initial assessment of the currently available standards relevant to TrustCoM – as outlined in version 1 of the roadmap – revealed that higher up the stack (see also Figure 1 below) there is not always clear agreement on either the required functionality or how competitive advantage can be supported by standards. Chapter 4 of this document gives a detailed overview of the positioning of the TrustCoM project with respect to various existing standards and specifications, in the context of the second version of the framework and the corresponding software developments.

3.1.2 Different notions of "standard"

The term "standard" can cover different notions, ranging from a public specification issued by a set of companies, to a 'real' standard issued by a recognized standardisation body. We distinguish between the following types of "standards":

a. *De facto standards* – a technology that is used by a vast majority of the users of a function. It may for example be in a product from a single supplier that dominates the market; or it may be a patented technology that is used in a range of products under license; etc. A *de facto* standard may be embraced by a standardisation initiative, and eventually become a consortium recommendation, or a *de jure* standard. The important thing is that it is very widely used, meets the needs for functionality, and supports interoperability.

b. *De jure standards* – standards from entities with a legal status in international or national law such the ISO, national standards bodies (e.g. BSI in the UK, ANSI in the US) or continental standards (e.g. European standards). These are strong in the health and safety related areas, in business quality measures and in long term IT areas. In IT these standards do not have to be implemented, or ever used; they just have to be agreed by the appropriate committee procedure – which can take many years.

c. *Consortium recommendations* – Groups of companies agree that a technology is recommended by them to provide some functionality. Such consortia vary in size from groups of a few large manufacturers (e.g. Microsoft, IBM and BEA), through OASIS and W3C to IETF. They also vary in the time it takes to establish a recommendation and the consensus that is behind it.[3]

For clarity, one can further divide the latter category into the following subcategories distinguishing between the formality (e.g. institutionalised or not) and rigour (e.g. public review, interoperability requirement test, etc.) of the process of producing a recommendation:

i. *Standardisation Consortia.* These include institutionalised entities that have established a charter that defines a thorough review process and a member voting procedure that indicates a widespread approval of the recommended specification. Examples of such bodies are IETF, FIPA, OASIS, OMG, W3C and WS-I.

ii. *Issue specific forums.* This includes community alliances and forums that are discussing and formulating specifications of particular interest for a community and then may pursue further standardisation approval. This includes groups such as the Global Grid Forum and Internet2. Other initiatives such as the Liberty Alliance project fall in between this and the previous category in that they often act as single-issue standards bodies.

iii. *Ad-hoc consortia, programmes* and *vendor groups*. This is the most diverse category that varies from groupings of major vendors (e.g. groups led by Microsoft, IBM and BEA) to government supported projects such as the DAML programme, and the Globus Alliance. Typically these consortia propose specifications supported by their own tools and will depend either on combined market share or on influencing another standards body or forum in order to ensure adoption. Again there are initiatives that fall in between this category and the previous one.

[3] W3C takes 6 months to establish a working group on a technology, and then 18 months to 3 years to agree on a recommendation, which is only released if there are working interoperable implementations of all functions in the technology, and enough of the members of W3C support it. In contrast, OASIS in theory may allow three (3) individuals to set up an OASIS Technical Committee (TC) to work on a draft standard specification. Upon completion of a specification the TC may approve the work as a Committee Draft. The approval of a Committee Draft requires at least 2/3 of the total membership of a TC voting to approve and no more than 1/4 voting to disapprove. Before the TC can submit its Committee Draft to OASIS membership for review and approval as an OASIS Standard, the TC must conduct a public review of the work. Review must take place for a minimum of 30 days. Unlike W3C, however, approval of an OASIS TC draft as an OASIS standard does *not* necessitate that there are working interoperable implementations of all functions in the technology.

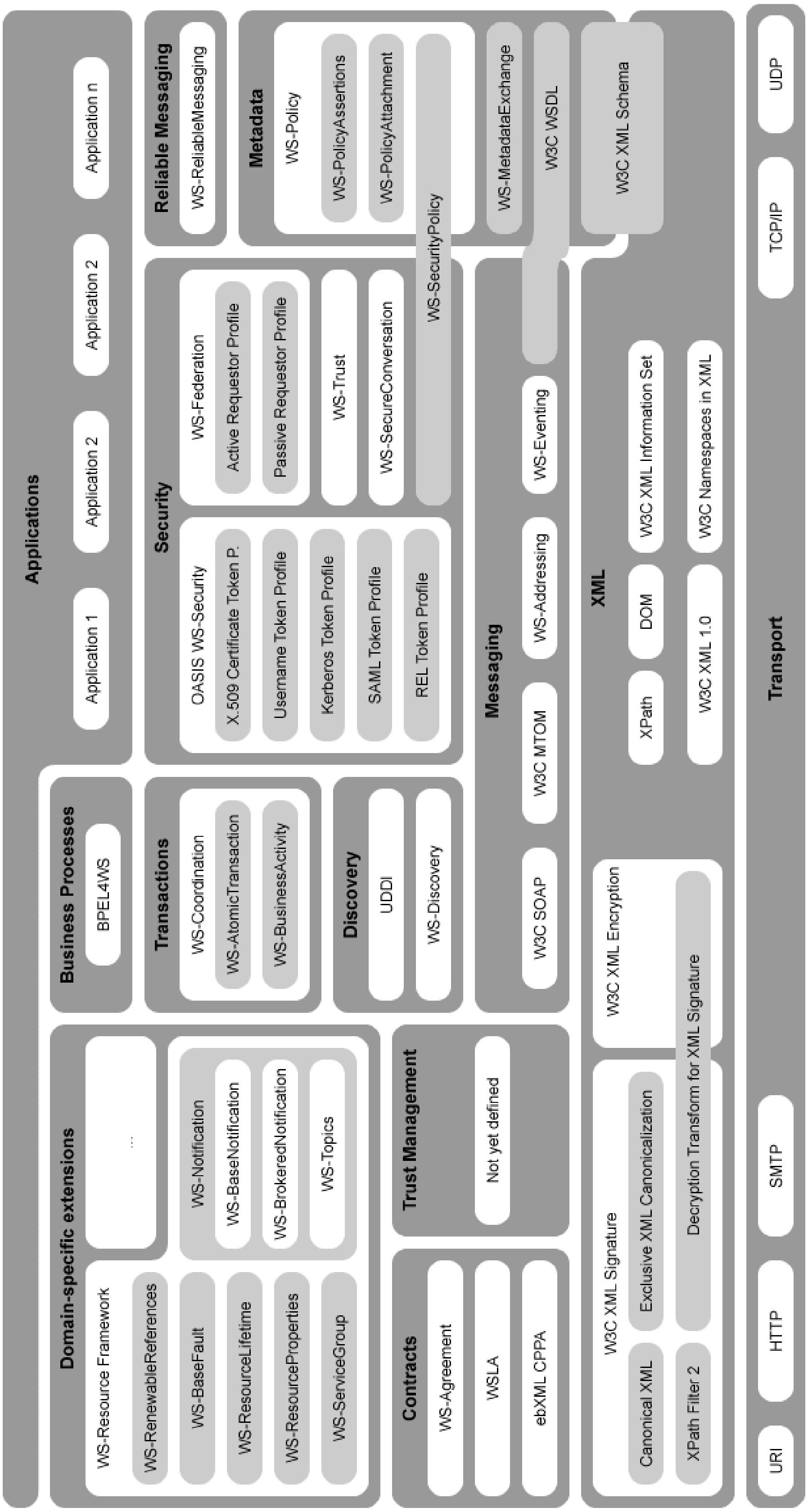

Figure 1: An architectural overview of some widely agreed and/or proposed web services related standards and published specifications relevant to TrustCoM

There is not an a priori preference to any of these different standardisation forums for TrustCoM standards adoption or contribution. As standards are market-driven[4], the involvement of key stakeholders (platform vendors, application developers, users) is an important criterion.

For further information on the concept, types, and importance of standardisation, we also refer to the paper on "Standardisation Issues: Basic Aspects within EU-funded RTD Activities" by the IPR Helpdesk[5], to the generic standardisation guidelines by COPRAS[6], and to [7] and [8].

3.2 Standards relevant to TrustCoM

TrustCoM is developing a framework for trust, security, and contract management, for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. For a common platform of interoperability, TrustCoM is building upon Web Services as the underlying Service Oriented Architecture technology.

Figure 1 gives an architectural overview of a (non-exhaustive) set of widely agreed upon and/or proposed web services related standards and published specifications that are relevant to TrustCoM. The overview includes specifications that are below as well as above the borderline that sets the balance between agreed functionality, business advantage and the need for interoperability.

The architectural stack of relevant standards and specifications illustrates once more that TrustCoM is an integrated project addressing trust, security, and contract management, for collaborative business processing, as a whole, focusing on the relationships and interactions between, and integration of, these issues, rather than investigating each of these issues separately and independently.

Chapter 4 of this document gives a detailed overview of the positioning of TrustCoM to the relevant standards and specifications, with respect to the second version of the framework and the corresponding software developments.

3.3 Standardisation contributions

One of the main objectives of the TrustCoM standardisation activities is to ensure that the results of the TrustCoM project contribute to the future developments of interoperable standards for trust, security, and contract management for collaborative business processing in dynamic Virtual Organisations, where necessary and appropriate.

So what are the expected potential contributions to this already vast landscape of numerous relevant standards and specifications?

As part of establishing a first baseline for further activities, we identified the following possible types of contributions:

1. Profiles, to integrate existing and new specifications within and across areas;

[4] Note that technology needs to be compliant to legal and policy regulations. In areas such as privacy, qualified signatures, spectrum usage, etc, the technology compliance itself may be the subject of standardization.

[5] IPR Helpdesk. "Standardisation Issues: Basic Aspects within EU-funded RTD Activities". http://www.ipr-helpdesk.org/documentos/docsPublicacion/html_xml/8_standardisation%5B0000004709_00%5D.html.

[6] COPRAS. Generic guidelines for IST research projects interfacing with ICT standards organizations. July 2005.

[7] Michael Wilson. The Future of the Web. http://www.w3c.rl.ac.uk/pasttalks/BNCOD_MDW.pdf.

[8] Chari and Seshadri, (2004). Demystifying Integration, Communications of the ACM, July, Vol 47(7), 59-63.

2. New contributions in specific areas, where appropriate;
3. Adaptations of existing standards, only where really needed;
4. Dissemination of TrustCoM results within standardisation initiatives.

3.3.1 Profiles

TrustCoM will focus on, and expects to have its main impact with respect to standardisation in the creation of *profiles*. A profile identifies how different specifications should be used together to support complex applications. This specifically applies to (but is not limited to) interoperable web services. If individual web services standards are metaphorically seen as pieces of a jigsaw puzzle, that each capture some autonomous functionality, then profiles can be seen as recommended designs of jigsaws and “best practice” guidelines that support work towards implementing comprehensive and potentially complex business functions. Profiles are created in response to the ever-growing number of interrelated specifications, all at different version levels and different stages of development and adoption, and often with conflicting requirements. Profiles integrate and refine dominant web services standard specifications by resolving potential conflicts between them, constraining their extensibility options where necessary, and exploiting their complementarity and composability characteristics.

In the context of TrustCoM, we are interested in developing profiles relating to Autonomic Security, Trust and Contract Management, and Secure Business Processes Enactment in dynamic Virtual Organisations.

3.3.2 New contributions in specific areas

Where appropriate, TrustCoM may also propose new contributions, based on its framework specifications. These new contributions may be introduced as new standards, or, preferably, as extensions on top of existing standards. For new contributions, we want to adhere to the principle of composability, and want to avoid unnecessary expansion of existing specifications.

Specific contributions may be done in the areas of trust, contracts, security, and business processing. These specific contributions would be pre-standardisation proposals arising from research laboratories and individual teams. They need to be presented to the community, and shown to provide the required functionality before they will be considered for standardisation. Because TrustCoM is a consortium including several large vendors, it provides a forum for exposing such proposals internally to a wide range of considerations before they are publicly released. When that happens, any proposals will have the weight of the TrustCoM partners' names behind them. Individual company proposals do not have this advantage, and may just become one of many proposals for the community to consider.

Note that the latter observation also illustrates that such new contributions do not necessarily have to be completed within the life-time or scope of the TrustCoM project, as initiated work based on TrustCoM contributions may be continued by the partnering organisations after the end of the project.

3.3.3 Adaptations of existing standards

Only if really needed, revisions or adaptations of existing standards or specifications may be proposed. This may be required within the context of newly proposed profiles, or for existing standards or specifications to be able to work together with new contributions.

3.3.4 Dissemination of TrustCoM results within standardisation initiatives

Last, but not least, a substantial part of the standardisation activities consists of disseminating and discussing (intermediate) TrustCoM results within standardisation initiatives, and within the individual partner organisations, with the people who are active in the existing standardisation efforts.

One way of initiating and materialising the contributions mentioned above, is to liaise with the appropriate bodies and people, present specific relevant TrustCoM results at appropriate events, give reasons for the need for profiles, indicate potential impact or contribution to standardisation, and gather feedback. Dissemination and discussion of TrustCoM results within the overall individual partner organisations, and with people inside these organisations, who are active in the existing standardisation efforts, is a pre-requisite to the adoption and success of potential TrustCoM standardisation contributions.

This effort is clearly part of the overall TrustCoM dissemination activities, and has a strong link with exploitation.

4 Standards roadmap TrustCoM framework V2

For each of the TrustCoM subsystems, this chapter:

- analyses the relevance of interoperability for each of the artefacts in the subsystem,
- provides an updated positioning of the relevant existing standards and specifications,
- provides concrete results, plans, or expectations for future standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of TrustCoM work.

The main reference is the TrustCoM Framework V2 – see deliverable D29-35-36 (February 2006) – and the corresponding ongoing software developments. The following sections are covered for each of the TrustCoM subsystems relevant in this deliverable:

- Framework artefacts and relevance to interoperability – We list the relevant artefacts in the subsystem and assess the importance of interoperability based on whether the artefact needs to interact across subsystems and/or across organizations.
- Specifications adopted in Framework V2 – We provide an updated positioning of the relevant existing standards and specifications for each artefact, and indicate which specifications (standards or other) are being used in the current implementation.
- Specifications relevant in future – We explain which specifications (standards or other) should be closely monitored further. These may or may not be leveraged in current and future implementation.
- New specifications or profiles being developed – We identify concrete specification/profiling work related to the artefact, for which no existing specifications are available or suitable. These are essential TrustCoM results, and are a prerequisite for eventual standards contribution.[9]
- Standards roadmap – We describe concrete results, plans, expectations, or dependencies for ongoing and future standards impact. These may be within and/or beyond the TrustCoM project time frame
- Collaboration efforts – We outline the concrete collaborative efforts (e.g., with other EU projects) promoting interoperability and adoption of specific TrustCoM framework artefacts. We particularly highlight those cases where there is collaboration at the technical and development level.

Besides the above mentioned deliverable D29-35-36, the main input/reference deliverables for this work are deliverable D24 TrustCoM Standardisation Roadmap v2, deliverable D28 State-of-the-Art Update, and deliverable D40 Collaboration Activities Report.

As with the previous versions of the standardisation roadmap, this deliverable collects the positioning status across the technical WPs, but does not intend to provide an in-depth justification for each specific positioning. We refer to the technical deliverables for specific technical details.

[9] Note that WP13 plays an important role in creating awareness of the importance of specifications for the software developments, and in pushing the project further in providing specifications and profiles for the technical work, particularly in these areas where interoperability matters.

4.1 VO Management

4.1.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
VO-ID (VO Identifier)	Schema	yes	yes	The unique identifier of a VO, including its purpose and namespace.
VO Member and VO Member List	Schema	yes	yes	List of current members in a VO. A VO Member is a description that extends UDDI's BusinessEntity, which provides the details of a selected member in a VO.
VO Membership Mgmt	Service	yes	yes	Maintains membership information for different VOs. May be hosted centrally by a single host or distributed.
VO Lifecycle Manager	Service	yes	no	Informs about the state of a VO and coordinates the activities that belong to that state.
GVOA	Schema	no	yes	Description of the general agreement for a VO
GVOA Manager	Service	no	yes	Manages general agreement in the VO (core operations are: createVO, formVO, operateVO, pauseVO, resumeVO, terminateVO)

4.1.2 Specifications adopted in Framework V2

- UDDI – We extend the BusinessEntity field for the VO Member description.
- WS-Agreement – GVOA and GVOA Manager design is influenced by WS-Agreement.

4.1.3 Specifications relevant in future

- Existing protocols for generation of UUIDs and URNs – as basis for VO-ID.
- WS-Agreement, WSLA, WS-Policy – as relevant for the GVOA description.
- WSDM and Globus VOMS – as relevant for comparison with our VO Management approach.
- WSDM, Globus VOMS, as well as results from OASIS eContract WG on contract management – may be relevant in context of GVOA Manager.
- WS-Eventing / WS-Notification – will become relevant when integrating with the notification subsystem.

4.1.4 New specifications or profiles being developed

- VO-ID (VO Identifier) – TrustCoM proprietary specification for a UUID surrounded by an XML structure that describes the creation date, objective and host of the VO. Will have to integrate this with the security token service and schema.
- VO Member and VO Member List – Current extensions are simply the identifier of the VO in which the VO-Member is a member, as well as the unique participant role being played in the VO. We are considering the usage of UDDI categorization in order to define additional attributes on members registered with a UDDI registry.

- VO Membership Mgmt – All developed specifications are TrustCoM proprietary. Administration profile for a shared membership manager that manages members of different VO's. We're also looking into a UDDI profile for querying the members in a VO based on different parameters, such as role and state.
- VO Lifecycle Manager – TrustCoM proprietary query interface for asking details of a VO's state.
- GVOA – A schema specifying how to express general agreements in VO, integrating business/legal terms and conditions and technical terms and conditions (QoS) within the same framework.
- GVOA Manager – Specification of the protocol for managing the GVOA schema.

4.1.5 Standards roadmap

- VO Member and VO Membership Mgmt – There will be a need to standardize the protocols for managing the list of actual and potential members in a VO, indicating their participant role, status and additional domain information. This is however beyond the scope of TrustCoM, as we first need to complete implementation and validation of these protocols.
- VO Lifecycle Manager – Use of a standard incident notification may be beneficial.
- GVOA and GVOA Manager – Both the service and the schema are going to be promoted to CCLRC E-Science Centre, expecting this work can be leveraged and integrated into other projects.
- IBM is investigating ways for TrustCoM to influence WS-Agreement based on the Industry Business Contracts, GVOA and SLA work that is currently underway in AL6/AL1/AL2.

4.1.6 Collaboration efforts

It is planned to promote the GVOA and GVOA Manager in the interoperability cluster as well as the Grid community (TG6 and CoreGRID).

4.2 Business Process Management

4.2.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
BP Repository	Service	yes	yes	Maintains collaboration definition templates (store/update/retrieve).
Collaboration Description	Schema	yes	yes	A collaborative business process model capturing the global view, across multiple VO member roles, of business process activities. (This includes Goal description, Role requirements, etc.)
BP Description	Schema	no	no	A process model (for private and public processes) enacted within one VO member domain (local, partner internal view on process activities); may encompass additional artefacts such as deployment descriptors for implementation reasons.
TSC Service	Service	no	no	Maintains (store/update/delete) configurations for BP relevant security controls which require to contact TSC

				subsystems during BP enactment.
TSC Task	Schema	yes	no	A BP pattern that enforces BP relevant security decisions from TSC subsystems during BP enactment; a BP control that is part of the BP Description and affects the process control flow; becomes configured at runtime by data from the TSC service.
Knowledge Base	Service	no	no	A composed subservice for the CDL++2BPEL service; matches parts/patterns of the collaboration definition to corresponding private/public process arts/patterns; does additional tailoring (e.g. process variable initialization, correlation, etc.) that the BP parts can be appended to a executable BP Description.
CDL++2BPEL	Service	yes	no	A service that implements an algorithm to derive a executable BP Description for a given role from a Collaboration Definition; uses the Knowledge Base Service; it also inserts TSC Tasks into those derived BP models where the corresponding Collaboration Definition activity includes an annotated TSC Extension Role.

4.2.2 Specifications adopted in Framework V2

- WS-CDL – Collaboration Description.
- BPEL – Business Process Description.
- WSDL – Services interfaces are using standard WSDL based description.

4.2.3 Specifications relevant in future

- WS-CDL and BPEL

4.2.4 New specifications or profiles being developed

- There is a WSDL specification of the BP Repository (and a corresponding design document).
- Specification for TSC Extension Roles

4.2.5 Standards roadmap

- A "security" profile for WS-CDL is being developed that allows stating of BP description relevant security requirements from the initial collaboration design from a global perspective. The entire concept of TSC for secure collaborative BPs is more complex and entails service operations (and their implementations) across various other services that mainly deal with operational BPM. The CDL++2BPEL service is a good example for that. An initial implementation (of all required pieces) is there and we are currently verifying the concept and implementation based on the VO collaboration definitions from integration scenario 3.
- TrustCoM is following a top-down approach that is suitable for VOs in collaborative business processing; the traditional approach is bottom-up, as the outside world is not so much a VO yet. If the world will support the existence of VOs there are immediate interesting consequences. SAP has discussed specific issues with Sun and Pi4Tech on the WS-Chor

mailing list. The currently favoured bottom-up approach requires concepts such as behavioural runtime monitoring of collaborative BP endpoints to verify that processes and roles (partners) stick to the agreed upon collaboration definition. Our approach assuming a more ordered/controlled VO environment simplifies this problem since we expect that the top-down derived public ("interface") processes automatically play along and therefore interoperate on the BP level.

4.2.6 Collaboration efforts

- TrustCoM adopted a process model based on process views (private/public processes) which is used in several other EU projects such as Athena.

4.3 SLA Management

4.3.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
SLA Template	Schema	yes	yes	Document that constrains the potential QoS properties of a service. Depending on the negotiation model, the SLA template may define ranges for QoS metrics that need to be respected by the final, agreed SLA document. This is very important for standardisation ("like a WSDL for SLAs").
SLA document (including SLA reference)	Schema	no	yes	The Service Level Agreement stating obligations and guarantees about the provision of a service (instance). It may or not be signed by the obliged parties. Before it is signed, an SLA is not binding. A particular issue to pursue is the (potential) legal implication of SLA and the corresponding requirements for the specification (to make it legally binding).
SLA and SLA Template Repositories	Service	yes	yes	Stores SLAs. Stores SLA templates for the application services which may be used within a VO. In its simplest incarnation, this is a database of SLA templates (XML documents) indexed by the SLA template ID.
SLA Negotiator	Service	yes	yes	Provides application-independent support for the execution of the SLA negotiation protocol.
SLA Signer / Notary	Service	no	yes	Provides application-independent support for the execution of the SLA signing protocol. A Trusted Third Party (TTP) service that serves as witness to the signing of an SLA document. In signing protocols that require the participation of a TTP, the Notary may play also this role.

Signed SLA	Schema	no	yes	An SLA document that has been signed by all obliged parties, resulting from the successful execution of a signing protocol. This protocol is expected to guarantee properties like fairness and non-repudiation.
SLA Evaluator	Service	yes	yes	Service that receives/pulls metric values from one or more SLA monitors, evaluates the obligations and guarantees in an SLA document, and, if any has been violated, notifies it using the Notification subsystem. The (non-)violation information is of interest for standardisation to allow uniform treatment.
SLA Monitor	Service	no	no	Computes QoS metrics about the execution of a service instance (included in service status). A monitor could be located at the host level (for example, to measure CPU usage) or at the level of the PEP in a EN/VO virtual node (acting like a message interceptor). It can also be a TTP that aggregates metrics produced by other monitors.
SLA Manager	Service	no	no	A distributed service used to configure and manage the components of the SLA Management subsystem. For instance, the SLA Manager is responsible for configuring monitors and evaluators.
SLA config information	Schema	no	no	Subset of the information in an SLA document that is used to configure SLA monitors and evaluators.

4.3.2 Specifications adopted in Framework V2

- WSLA – The current SLA document description is based on WSLA.
- WS-RF, WS-Notification, WSLA – SLA Evaluator, SLA Monitor, and SLA Manager are built on top of these specifications.

4.3.3 Specifications relevant in future

- WS-Agreement – TrustCoM will move from WSLA to WS-Agreement as the basis for the SLA profile.
- A standard spec for a repository, such as UDDI, may be of interest. TrustCoM focuses on the SLA template content rather than on the repository. WS-Agreement may come up with its own specification.
- WS-Negotiation, WS-Agreement, WS-AgreementNegotiation, FIPA Iterated Contract Net Interaction Protocol – We will investigate these in the context of SLA Negotiation.
- XML Signature – should be used as format for Signed SLAs.
- WSDM, WS-Management, WS-Coordination – We will investigate these further in the context of the SLA Manager.

- WSLA (SDI) Service Deployment Information, WS-Agreement – We will investigate these for use for SLA config information.

4.3.4 New specifications or profiles being developed

- SICS and HLRS aim at realising a profile that captures all of the SLA relevant structures. This will be a mixture of WSLA and WS-Agreement, and will i.e. have (a) a general protocol (like a "header" to the SLA, most likely basing on WS-Agreement) that contains no detailed information about the parameters, conditions & terms, but general data like identifiers of involved parties etc; and (b) a "body" dependent of the actual usage, i.e. different for the specific issues. This part contains the actual concrete information and bases roughly on the WSLA-specifications. (The profile is not in a "publishable" state yet.)
- For the SLA Repository we build upon a TrustCoM proprietary specification for prototype purposes. There is no SLA Template Repository spec yet.
- Currently, SLA monitors and evaluators are configured using the whole SLA document. For security and privacy reasons it may be convenient that these components get only the information they need to operate, and no more. However, this is not a priority at the moment.

4.3.5 Standards roadmap

- TrustCoM is planning to adopt the format for SLA templates defined in WS-Agreement. Since this format is underspecified, the next version of the SLA profile will describe how WS-Agreement templates are instantiated within TrustCoM. At the moment we envision that, like SLA documents, templates will result from a combination of WS-Agreement with WSLA SLO substructures. Similarly for SLA documents, TrustCoM will replace WSLA with WS-Agreement, keeping WSLA's sub-language for the specification of Service Level Objectives (SLO).
- TrustCoM expects that this part of the profile becomes of particular interest to the WS-Agreement standard committee (probably beyond the project time frame). HLRS has established contact with Heiko Ludwig from IBM and discussion has started.
- SICS and HLRS expect to develop a secure negotiation protocol as an adaptation of the FIPA Iterated Contract Net Interaction Protocol that would fulfill the security requirements for SLA Negotiation in VOs. This may lead to standardization efforts beyond the project time frame.
- Once the appropriate signing protocol is chosen, we expect to define an application-independent interface to a signing service that each VO partner will use to sign its own contracts. It is highly unlikely though that this will become part of any standard or profile proposal within the project's time frame.
- In at least one other place, TrustCoM is developing a profile for signing XML documents (e.g. signed policies). We expect that work to influence a schema for signed SLA documents. An important note is that SLAs need to be signed by at least two parties, whereas policies need to be signed by the policy issuer.
- Note that the SLA config information is derived from the SLA document and different for each service provider - it is potentially not even XML but some proprietary data structure, individual to each Service Provider. Hence, not for standardisation, but only as recommendation.

4.3.6 Collaboration efforts

- The SLA developments in TrustCoM are performed in collaboration with AKoGriMo and NextGRID, with specific aspects being pursued further in the upcoming project BREIN.

4.4 Trust and Security Services

4.4.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
Security Token	Schema	yes	yes	A Security Token is issued by a VO partner and asserts that the requestor and owner of the token has specific claims as configured by the VO partner.
Security Token Service (issuance and validation)	Service	yes	yes	The Security Token Service (STS) issues and validates security tokens for cross-organizational and scoped interactions within a VO.
Security Token Service (management)	Service	yes	no	An organization's Security Token Service has a management interface allowing creation and dynamic configuration of VO federations.
Reputation Management Service	Service	yes	yes	includes Update and Retrieval of reputation
Reputation data	Schema	yes	yes	The format of the reputation metrics
Secure Audit Log	Service	yes	no	A secure log service for any relevant event to be audited. This is typically only invoked within a single organizational trust boundary, but cross-organizational invocation could be possible in principle.
Secure Audit Log Message/Container	Schema	yes	no	SAWS takes any binary data and stores it.

4.4.2 Specifications adopted in Framework V2

- SAML assertions – Adopting SAML assertions for TrustCoM cross-org token and validation tokens.
- WS-Trust – Using WS-Trust for issuance and validation of security tokens.
- Supporting KerberosToken and X509Token (and thus X.509 certificates) for intra-org authentication, in particular between a service and a security token service. UsernameToken is also supported by the platforms on which the TrustCoM framework is implemented.
- WS-Federation – Applying WS-Federation Active Requestor Profile ("U-type" interaction model).
- Possibility of using e-bay metrics for reputation service.
- Using SSL/TLS for secure transport to audit log service.

4.4.3 Specifications relevant in future

- Other possible token profiles (e.g., RELToken) can be monitored, but these are not directly relevant anymore within the time frame and scope of the TrustCoM project.
- WS-MetadataExchange – The security policy requirements of a service should be exposed through WS-MetadataExchange; these requirements are related to the 'AppliesTo' as well as the 'Claims' that are included in a WS-Trust RequestSecurityToken; while there are no profiles standardized yet at this point, the progress here needs to be monitored.

- GGF OGSA Authorization profile – The GGF OGSA-Authz WG is working on a profile for authorization in Grid architectures, which is relevant in the context of TrustCoM Trust & Security services.
- "Identity metasystem" specifications and federated identity/attribute frameworks (e.g., Liberty) – These are particularly relevant for 'intra-org' authentication; they also cover metadata aspects which may be relevant as described above.
- WS-Federation profiles: we need to keep in mind and monitor other interaction models (i.e., "W-type").
- WSDM and WS-Management approaches may also be relevant, but these are much more service/resource generic, than the federation-specific needs of security token service management.

4.4.4 New specifications or profiles being developed

- Security Token – Implementing a specific profile for SAML tokens in the context of scoped federations in a VO.
- Security Token Service (issuance and validation) – Implementing a specific profile for WS-Trust issuance and validation in the context of scoped federations in a VO.
- Security Token Service (management) – Implemented a demo web interface; this is a browser-based interface so a specification is not required. We are looking into a custom web service interface.
- Reputation data – Besides e-bay metrics, a TrustCoM proprietary specification is being developed, based on +1,0,-1 and 3 valued logic of trusted, untrusted and unknown.
- TrustCoM proprietary specifications are being developed for Reputation management service and Secure audit log.

4.4.5 Standards roadmap

- The WS-Trust and SAML token profile is disseminated by EMIC to the relevant people in Microsoft as part of EMIC's aim to integrate the results of the project in the appropriate Microsoft technologies and products.
- David Chadwick (UoK) is co-chairing the GGF OGSA-Authz WG and may influence the specifications that are being developed in this WG with the TrustCoM-specific WS-Trust and SAML token profile.
- We first need to further refine and validate the STS management concepts within the context of the project and the collaborations. In any case, there is no existing specification or working group which would need to be directly influenced by TrustCoM results in this area.

4.4.6 Collaboration efforts

- The WS-Trust and SAML token scoped federations profile is promoted in the NextGRID and MOSQUITO projects through the FP6 Grid Trust and Security concertation and through EMIC as a common partner in these projects.
- The STS management developments are carried out across the FP6 TrustCoM, NextGRID, and MOSQUITO projects. With EMIC as a common partner, alignment and consistency of the results in each of the project frameworks are further pursued.
- Prof. Marty Humphreys has submitted a bid for grid auditing to NSF that uses our SAWS implementation.
- The UK JISC DyCOM project is using SAWS to implement Separation of Duties.

4.5 Policy Control

4.5.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
Policy Service (PDP)	Service	yes	yes	The PDP includes an interface for access requests, and an interface to load signed policies. The interfaces to load a root policy (root of trust), to do debugging/testing, and to remove a policy are not considered relevant in the context of standardization.
Policy (authorization)	Schema	yes	yes	TrustCoM develops a profile for the structure and content of (access control) policies in the context of Virtual Organizations.
Policy (ECA)	Service and Schema	yes	yes	Policy language, policy-relevant actions and events, and policy management protocols for ECA-style policy.
Claims (relevant to authorization policy); including VO claims	Schema	yes	yes	Claims are statements about entities that are relevant for security in Virtual Organizations. Claims are asserted in security tokens. Claims include cross-organizational claims, as well as validated claims for use in an access policy.
Signed Policy format	Schema	no	yes	A format for digital signatures which allows to authenticate the origin of a policy.

4.5.2 Specifications adopted in Framework V2

- XACML 1.1 – For the PDP, we use the XACML Request context as a message format, similarly to the SAML profile for XACML. For an authorization policy, we use XACML 1.1 with some extensions (within the official extension points of the standard) for delegation. Token claims are translated into XACML attributes before feeding them into the PDP, and for use inside the access control policies.

4.5.3 Specifications relevant in future

- SAML profile for XACML – The SAML profile defines a message format for invoking an XACML PDP. That message format uses the request context like we do, so currently it does not provide anything we don't already have, but there are plans for adding other useful features to it.
- XACML 3.0.The XACML spec also has a format for SAML attribute assertions that are ready to be translated into XACML attributes. This should be used as the validated claims to be fed into the PDP.
- DMTF's Policy Core Information Model (PCIM) and TM-forum's NGOSS; WS-Policy and to a lesser extent WS-SecurityPolicy.

- Researchers from ETRI, Korea submitted a paper to W3C on ECA policies.[10] The presented framework on event-driven coordination of distributed Web Services-enabled devices intends to contribute to emerging ubiquitous service-based systems, and states the belief that related standardization activities are required within W3C in this context.
- Specifications around the Policy Middleware for Autonomic Computing (PMAC) framework developed as part of IBM's autonomic computing initiative.
- The GGF OGSA-Authz WG may suggest relevant formats and values for claims.
- XML Signature – as basis for Signed Policy format. XACML is not expected to ever define a signature format; the SAML profile defines a signature format using XML Signature which may be relevant.

4.5.4 New specifications or profiles being developed

- Authorization Policy and PDP – The TrustCoM profile for XACML will contain more specific details on how to use XACML in a VO, and also covers the PDP interface aspects.
- Claims – TrustCoM proprietary token claims and XACML attribute assertions values are used. A profile for consistency between token claims and policy attributes as used in respectively the T&S and Policy subsystems may be developed.
- Signed Policy – TrustCoM may develop a profile for XML Signature and XACML policies.

4.5.5 Standards roadmap

- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use. Erik Rissanen is a member of the XACML TC and is participating in the discussions. The plan is to continue to learn from the TrustCoM experience and bring in the results into the TC work at an appropriate time. In this way the relevant TrustCoM results could eventually be moved into the standard. Specific TrustCoM requirements to address in the XACML TC is the need for signing with security tokens other than X.509 certificates, and the expansion of the PDP interface with methods for loading signed policies.
- In particular, XACML 3.0 will contain the delegation functions used in TrustCoM in native and more clean form.
- David Chadwick (UoK) will further liaise TrustCoM developments and possible work done (initial suggestions for relevant formats have been made) within the GGF OGSA-Authz WG in this area.

4.5.6 Collaboration efforts

- Policy (ECA) – Collaboration with DIADEM FIREWALL project for alignment of policy models.

4.6 EN/VO Infrastructure

4.6.1 Framework artefacts and relevance to interoperability

TrustCoM Framework	*Nature*	*Cross-*	*Cross-*	*Description / Notes*

[10] Kangchan Lee, Wonsuk Lee, Jonghong Jeon, Seungyun Lee, Jonghun Park. Event-driven Coordination Rule of Web Services enabled Devices in Ubiquitous environments. February 2006. http://www.w3.org/2006/02/WS-ECA.pdf.

Artefact		*Subsystem?*	*Org?*	
Service/resource information	Schema	yes	yes	Refers to both management related information of service access point, as well as to application service related info.
Instantiator / Instantiator service	Service	yes	no	The Instantiator subsystem allows configuration (via the Instantiator service) of the infrastructure for exposing and virtualising a service offered by a service provider. The Instantiator service receives a request providing a "virtual endpoint", VO identifier and optionally SLA identifier and reference to the location of the access control policies. Configuration includes: 1. creating a per-service policy enforcement profile (configuration) stored in a resource properties document associated with the management interface enforcement component 2. obtaining a certificate (X.509) identifying the service within the scope of the provider's realm 3. storing the certificate within the enforcement component and referencing it via the abovementioned resource properties document representing a per service enforcement configuration 4. initiating configuration of the enforcement component by uploading an enforcement configuration policy at the abovementioned resource properties document representing a per-service enforcement configuration 5. initiating configuration of the STS by making available the internal identity certificate (e.g. X.509) to the STS 6. initiating configuration of the PDP by providing the "virtual" endpoint of the service (target name) and the endpoint of the corresponding PDP to the Policy service 7. initiating the configuration of the SLA monitoring by providing the "SLA identifier" to the SLA manager component(s)
Instantiator / Service Instance Registry	Service	yes	no	An internal SQL database accessible by the instantiator serivce that includes for each service: VO-ID, Virtual Endpoint, Actual Endpoint, Associated PEP management endpoint, PDP endpoint, STS endpoint, SLA identifier, etc.
Instantiator / X.509 STS	Service	no	no	Provides X.509 certificates to identify internal services (if required)

Enforcement / Enforcement Component	Service	yes	yes	Intercepts incoming and outgoing messages from a service and applies security and messaging policy based on a per-service configuration. Can be deployed as a standalone messaging component ('message interceptor') or as handler chain (e.g., 'PEP') within a web service host / deployment environment. Identifies based on content (i.e. WS-Addressing header) which per-service configuration policy to apply, internally retrieves the information kept in the appropriate WS-ResourceProperties relating to that service, and implements the actions by calling the appropriate handlers per action using the configuration stated in the corresponding Interceptor Reference policy.
Enforcement / Enforcement Management Service	Service	yes	no	Only a management interface is exposed at the control plane; the component is transparent at the SOAP message layer of the data-plane. Enforcement Management Service is exposed as a WS-RF enabled web service that contains one resource property document per virtualised service which keeps the following information: - virtual endpoint of the service - Enforcement configuration policy: which enforcement actions (e.g. encryption, token validation, signature check, etc.) to be performed per protected service - Interceptor Reference policy: configuration information mapping each enforcement action to a group of handlers - endpoints of STS and of PDP used for the protected service - X.509 certificate identifying the protected service within a partners VO - active contexts whithin which the protected service is participating Enforcement Management Service: Configuration factory: A service that is invoked (WSRF/ WSDM) to create a new WS-Resource containing enforcement configuration information for a protected service.
Coordination: Activation Service, Registration Service, Context Token STS, Coordination Policies	Service and Schema	yes	yes	The Coordination subystem provides a way to create and manage distributed (application) context, register services participating in the context, and book-keep who is registered with which context.
Notification Proxy and Broker	Service	yes	yes	HLRS has implemented a notification proxy that is used on a per service provider / VO partner and not on a per service basis. This may be integrated to the enforcement middleware or remain separate depending on progress with

				integration.

4.6.2 Specifications adopted in Framework V2

- SOAP, WSDL, and WS-Addressing – Foundation for messaging, description, and addressing of basic, stateless web services.
- WSRF and WSDM – Used, in addition, to support manageable, stateful web service resources.
- SOAP Message Security – Foundation for secure messaging between services within VO.
- WS-Trust with X.509 profile and SAML token processing – Leveraged for interaction between (message) policy enforcement point and STS.
- XACML – Leveraged for interaction between (message) policy enforcement point and PDP; also used for authorization policies controlling the creation of, or registration with, a context.
- WS-Coordination – Used by coordination system in combination with WS-Trust for Context Token issuing by Activation Service and Context Token validation by Registration Service.
- WS-Context – To support WS-Context tokens in combination with Proof of Registration tokens.
- WS-Notification – Notification/Eventing support.

4.6.3 Specifications relevant in future

- WS-MetadataExchange, WS-PolicyAttachment – to support exposure of (security) policy requirements of deployed service.
- WS-Management, WS-Transfer, WS-Enumeration – For prototyping reasons, TrustCoM has opted for the WSRF/WSDM web services stack. The WS-Transfer/WS-Management stack is an alternative proposal. While there are different such protocol stacks at this point, the industry is committed to define new specifications and enhancements enabling further convergence of these platforms.[11]
- WS-Eventing – For prototyping reasons, TrustCoM has opted for the WS-Notification suite. WS-Eventing is an alternative approach. While there are different approaches at this point, the industry is committed to define new specifications and enhancements enabling further convergence of these platforms.[11]
- UDDI – Could have been used for the Service Instance Registry, but it is not at this point because this component is not exposed outside of a partner's domain.
- WS-CAF – Follow-up as coordination approach.
- WS-AT and WS-BA – Specific coordination protocols on top of WS-Coordination.

4.6.4 New specifications or profiles being developed

- WSRF ResourceProperties document(s) that holds trust/security, SLA, and configuration policy information for service, and (possibly) application state; all this in relation to a context.
- Profile for service management service exposed as a WS-RF enabled web service that contains one resource property document per virtualized service.

[11] Toward Converging Web Service Standards for Resources, Events, and Management. A Joint White Paper from Hewlett Packard Corporation, IBM Corporation, Intel Corporation and Microsoft Corporation. 15 March 2006.

- TrustCoM proprietary schema (based on WS-Policy) for enforcement configuration.
- Profiles for WS-Trust:
  - X.509 profile
  - token validation WS-Trust + SAML+X509+VO-claims in token validation response)
  - access control WS-Addressing + XACML + (SAML/XACML profile)
  - context sharing WS-Trust + WS-Security (or WS-SC) + WS-Coordination
- Content transformation based on XSLT rules/policies
- Profile for use of WS-Context in WS-Coordination.
- XACML-based coordination policies.

4.6.5 Standards roadmap

- We try to avoid instigating a modification of existing standards to the extend that this is possible.
- We expect to produce an instantiation design pattern for WS.
- We expect to produce a factory design pattern for WS.
- There is a high probability of producing a security configuration language.
- We are looking further into coordinator interposition for federation bootstrapping.
- There is a high probability of defining atomic transaction types for VO/EN configuration processes.
- None specific for notification yet – however, we may want to improve WS-Topics depending on project results.

4.6.6 Collaboration efforts

- BT has been interacting with GUIDE, Akogrimo, ELeGI, BEinGRID and influenced the plan of the BEinGRID initative with which we anticipate to closely collaborate once the project starts in June. We have also been looking into ways of interacting with projects in the identity management area such as FIDIS. We have been in close contact with BT standards team and taken part into web services security and XML messaging early deployment initiatives.
- HLRS' notification work is performed in collaboration with AKoGriMo, and ELeGi.

4.7 Applications

4.7.1 Framework artefacts and relevance to interoperability

TrustCoM Framework Artefact	*Nature*	*Cross-Subsystem?*	*Cross-Org?*	*Description / Notes*
Storage Provider	Service	yes	yes	Stores information to allow different services to store and retrieve certain types of information as a middleware repository
PDD (Product Database Designer)	Service	yes	yes	Stores designs from different designers.

TC (Training Consultant)	Service	yes	yes	Training consultant defines a path to the learner in order to improve their new skills.
Content Provider	Service	yes	yes	Provides the resources to the learner.
e-learning Portal	Service	yes	yes	Gateway to get in to MetaCampus.
LP2BPEL (Learning Path to BPEL)	Service	yes	yes	Parser to translate to BPEL the learning path provided by TC

4.7.2 Specifications adopted in Framework V2

- All application services build on the Web Services foundations, including SOAP, WSDL, WS-Addressing, and some are also using MTOM and WSRF.
- Business processing related developments are supporting BPEL, ebXML, WS-CDL, and WS-Choreography.

4.7.3 Specifications relevant in future

Various non-functional specifications will become relevant when the applications are further integrated with the different subsystems.

4.7.4 New specifications or profiles being developed

Besides specifications for the application services, we are mainly interested in identifying any specific restrictions, requirements, issues, related to the use of WSRF, WS-Addressing, MTOM, and other relevant specifications, preventing, enabling, the integration, use, of TrustCoM framework components.

The following comments can be made from the EN/VO Infrastructure perspective:

- The internal deployment of an application specific service via WS-RF helps integration to the extent that it allows us to keep within the deployment environment state about which context (VO, transaction, etc) each service participates and to distinguish between context references. That way we do not have to assume that application services are developed to be aware of the collaboration scope within which they participate, if this is not part of their business logic.
- Other use of WSRF/WSDM is internal to the configuration of the enforcement infrastructure and, although important for the integration within TrustCoM, they are not exposed across partners in a TrustCoM VO.
- WS-Addressing: the "reference properties" is being used in some cases, inherited of the current implementations of WS-Addressing and WSDM that were used as a baseline for development (e.g. Open Source Apache project).
- We have not made an assessment for MTOM as yet.

4.7.5 Standards roadmap

There is no specific standards roadmap since the application-specific developments are intended to validate the TrustCoM framework, but are not part of the framework itself.

4.7.6 Collaboration efforts

- Some of the application-specific developments (such as the storage provider) are performed in collaboration with the Akogrimo project.

5 Summary and concluding remarks

Standards and collaboration are a way to promote and achieve interoperability between technologies across different vendors. TrustCoM therefore aims at building upon existing well established and accepted standards and published specifications, where appropriate. TrustCoM furthermore intends to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM also participates in European project clustering activities.

The following sections summarize the concrete impact and plans from/to standards and collaborative efforts with respect to the TrustCoM Framework V2 and the corresponding ongoing software developments.

5.1 Awareness and relevance of interoperability

As a pre-requisite for any standards adoption or contribution, WP13 further analyzed the TrustCoM framework subsystems in order to get a more concrete picture of the different artefacts in the TrustCoM framework subsystems, particularly where these are relevant to interoperability. WP13 further stimulated the conceptual work as well as the ongoing software developments to explicitly take into account interoperability requirements and to define clear and concrete specifications, which can be validated in the integration scenarios.

5.2 Adoption of existing standards and specifications

TrustCoM aims at building upon existing well established and accepted standards and published specifications, where appropriate. Particularly within the baseline infrastructure, TrustCoM has made a good choice in adopting various WS-* standards and specifications.

At this point there are still multiple, alternative web services specifications suites (i.e., WSRF/WSDM vs. WS-Transfer/WS-Management, and WS-Notification vs. WS-Eventing). For short-term prototyping reasons, TrustCoM has opted for the use of WSRF/WSDM and WS-Notification in selected cases. Within the context of the TrustCoM framework, there are however no fundamental reasons to adopt one or another. Specific profiles are moreover defined to allow easy migration from one to the other. This fits very well together with the recent commitment from the industry to define new specifications and enhancements which will enable further convergence of the different platforms.

5.3 Profiles

The primary focus of the TrustCoM standards and collaboration activity is in the creation of profiles that integrate existing standards *across* the different areas. While there are already numerous specifications addressing various issues *within* most of the identified areas, there are almost no concrete guidelines at all with respect to combining different specifications into a single interoperable framework.

The following concrete profiles have been and/or are being developed:

- A WSRF ResourceProperties document is specified that holds trust/security, SLA, and configuration policy information for a virtualized service, (possibly) including application state, and all this in relation to a context. This is accompanied with a profile for a service management service exposed as a WSRF enabled web service that contains a single resource property document per virtualized service. The restriction to a single RP allows easy migration to WS-Transfer.

- Related to this, TrustCoM has the expectation to produce specific design patterns for web services, particularly addressing instantiation and factory of web services.
- A security profile for WS-CDL is being developed that allows stating of BP description relevant security requirements.
- A profile that captures all SLA relevant structures is being developed. This profile is strongly influenced by both WS-Agreement and WSLA specifications. Interest from the WS-Agreement working group is being attracted.
- A profile for WS-Trust and SAML assertions for scoped federations is defined. This profile mainly covers specifications within the security domain, and addresses some cross-issues with Policy (XACML).
- A profile for using XACML in a VO context is defined. As highlighted below, SICS is contributing to future versions of the SAML profile for XACML being a member of the OASIS XACML TC.
- Profiles around coordination are being developed, particularly combining WS-Coordination with WS-Context, and including the use of WS-Trust security token services and XACML policies for issuing and validating such WS-Context based context tokens. TrustCoM is also looking further into coordinator interposition for federation bootstrapping. There is a high probability of defining atomic transaction types for EN/VO configuration processes.
- We identified the requirement for a profile for signing documents in a VO context. This is currently needed for signing SLA as well as policies within a VO.

The different subsystems are ultimately integrated through the General VO Agreement (GVOA) which is the central place for defining, linking, and agreeing specific terms that are relevant in the various subsystems.

The work in the application scenarios does not only validate the above profiles with respect to addressing the security, contract, and business processing requirements, but also provides useful experience in how the TrustCoM framework can be integrated into application services. For example, the current approach for service management does not mandate application services to be aware of the collaboration scope within which they participate, if this is not part of their business logic.

5.4 Specific new contributions

Where appropriate, TrustCoM may propose new contributions, based on its framework specifications. These new contributions may be introduced as new standards, or, preferably, as extensions on top of existing standards. For new contributions, we want to adhere to the principle of composability, and want to avoid unnecessary expansion of existing specifications.

In addition to various extensions which are part of the profiles listed above, the following separate extensions are defined in the TrustCoM framework:

- An extension of the UDDI BusinessEntity element for VO Member description is defined. TrustCoM is also considering the use of UDDI Categorization to define additional attributes on VO members.
- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use. In particular, XACML 3.0 will contain the delegation functions used in TrustCoM in native and more clean form.

Besides these extensions, a number of TrustCoM proprietary specifications are developed for specific functionalities needing interoperability, typically within a single subsystem.

5.5 Adaptations of existing standards

Only if really needed, revisions or adaptations of existing standards or specifications may be proposed. This may be required within the context of newly proposed profiles, or for existing standards or specifications to be able to work together with new contributions.

No specific adaptations of existing standards have been required so far.

5.6 Dissemination within standardisation initiatives

A substantial part of the standardisation activities consists of disseminating and discussing (intermediate) TrustCoM results within standardisation initiatives, and within the individual partner organisations, with the people who are active in the existing standardisation efforts.

The following activities must be highlighted:

- HLRS and SICS are realising a profile that captures all SLA relevant structures, with a strong influence of both WS-Agreement and WSLA specifications. Interest from the WS-Agreement working group is being attracted.
- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use. Erik Rissanen is a member of the XACML TC and is participating in the discussions. The plan is to continue to learn from the TrustCoM experience and bring in the results into the TC work at an appropriate time. In this way the relevant TrustCoM results could eventually be moved into the standard. Specific TrustCoM requirements to address in the XACML TC is the need for signing with security tokens other than X.509 certificates, and the expansion of the PDP interface with methods for loading signed policies. In particular, XACML 3.0 will contain the delegation functions used in TrustCoM in native and more clean form.
- SAP is promoting TrustCoM’s top-down approach for VOs in collaborative business processing with relevant organizations, and has particularly brought up specific issues arising with the currently favoured bottom-up approach.
- UoK is co-chairing the GGF OGSA-Authz WG, and relevant trust, security, and policy TrustCoM work is influencing the specifications that are being developed in this working group.
- EMIC is disseminating the WS-Trust and SAML assertion profile to the relevant people inside Microsoft Corporation.
- BT promotes and aligns TrustCoM work with corporate internal web services initiatives.
- CCLRC promotes TrustCoM work, particularly around GVOA, within the CCLRC E-Science Centre, expecting this work can be leveraged and integrated into other projects.
- IBM is investigating ways for TrustCoM to influence WS-Agreement based on the Industry Business Contracts, GVOA and SLA work that is currently underway in AL6/AL1/AL2.

5.7 Collaboration with other projects

TrustCoM participates in European project clustering activities, and establishes collaborations with other initiatives, in order to maximize impact of the project and avoid duplication of effort.

The following specific collaborations are promoting interoperability of concrete technical work:

- The GVOA work is promoted within the Grid Trust and Security TG6 technical concertation group, and particularly within the CoreGrid project.
- TrustCoM adopts the same process model for collaborative business processing as used in Athena and other projects.

- The SLA developments in TrustCoM are performed in collaboration with AKoGriMo and NextGrid, with specific aspects being pursued further in the upcoming project BREIN.
- The TrustCoM security token and security token services work is being carried out by EMIC across and in collaboration with the NextGRID and MOSQUITO projects.
- The TrustCoM secure audit service is being used in a US NSF proposal and a UK JISC project.
- The TrustCoM policy models have been aligned with a UK project.
- There is a close general technical interaction on various aspects with Akogrimo, ELeGi, and GUIDE.
- TrustCoM influenced the plan of the BEinGRID project with which close collaboration is anticipated once this project starts in June.

5.8 Concluding remarks

TrustCoM has been taking a wide range of actions to promote interoperability and take-up of its framework for trust, security, contract, and business processing in VOs. TrustCoM is also having a significant impact to standards.

Firstly, within the project, and driven by WP13 in particular, the ongoing software developments are further stimulated to address interoperability, and to define concrete specifications where interoperability matters.

The TrustCoM framework builds upon a WS-* infrastructure, which now is proving to be a solid service-oriented baseline, with a broad industrial support. While there are still alternative platforms at this point, the industry has recently announced a commitment for further convergence of these platforms. The TrustCoM framework already takes this convergence into account in its profiles, and is ensuring easy migration between these platforms.

A number of concrete profiles of existing specifications, including some new extensions, are being developed, which aim at covering the complete TrustCoM framework, as well as at addressing approaches for the integration of this framework into application scenarios.

Specific results are being disseminated to standards activities directly, and have already had a significant impact. Specific profiles are also being promoted by partners within their corporate organizations.

Last but not least, there are substantial collaborations with other projects to promote interoperability of concrete technical work. It is important to note that there is not only collaboration with ongoing projects, but that TrustCoM has also ensured take-up of its framework technologies in future projects, such as BREIN and BEinGRID.

The TrustCoM standards roadmap focuses on impact and plans aligned with concrete technical developments in AL2 of the project. As a consequence, this deliverable mainly focuses on the technical ICT standards (particularly web services related), and less on for example industry standards on integration between systems and applications.

The contributions and plans described above impact on many initiatives in individual ways. The sum of the impacts is to direct the existing initiatives involving many organisations to conform to, or take into account, the TrustCoM framework, without explicitly generating a separate standard suite for the whole TrustCoM framework (which would consume a substantial budget and time), and without these initiatives even being explicitly aware about the TrustCoM framework as such in some cases. The goal is that industrial solutions which conform to the relevant standards, are largely meeting the requirements identified by TrustCoM, and for which TrustCoM is demonstrating technology which is meeting these requirements.

6 References

The table below is intended as a complete reference list of standards and specifications that are somehow relevant to TrustCoM. This list has significantly grown since the first version of the standardisation roadmap.

By providing this list, we do not imply that we consider all these referenced standards and specifications within our main focus. On the contrary, in Chapter 4, we position the relevance of each of these specs in a fine-grained, qualitative way. Within each of the TrustCoM subsystems this leads to a clear identification of (a more limited set of) standards and specifications that are being adopted in the TrustCoM framework, and standards and specifications that may become relevant in future versions of the framework, and are kept within the relevance horizon for further investigation if time permits.

Standard or Specification	Standards initiative	Version / Status	Date	Reference
X.509 (PKI)	ISO/IEC ITU-T	REC (4th Edition)	2001	ISO 9594-8/ITU-T Rec. X.509 (2001) The Directory: Public-key and attribute certificate frameworks
X.509 PKI Profile	IETF	RFC	Apr 2002	http://www.ietf.org/rfc/rfc3280.txt
X.509 PMI	ISO/IEC ITU-T	REC (4th Edition)	2001	ISO 9594-8/ITU-T Rec. X.509 (2001) The Directory: Public-key and attribute certificate frameworks
X.509 AC Profile	IETF	RFC	Apr 2002	http://www.ietf.org/rfc/rfc3281.txt
PAC	Ecma International	Standard ECMA-219	Mar 1996	http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-219.pdf
ebXML CPPA	OASIS	2.0	23 Sep 2002	http://www.oasis-open.org/committees/download.php/204/ebcpp-2.0.pdf
ebXML Registry	OASIS	3.0 Standard	May 2005	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep
WS-Agreement	GGF	2005/09	20 Sep 2005	https://forge.gridforum.org/projects/graap-wg/document/WS-AgreementSpecificationDraft.doc/en/19
WSLA	industry	IBM	28 Jan 2003	http://www.research.ibm.com/wsla/WSLASpecV1-20030128.pdf
SSL/TLS	IETF	1.0 RFC	Jan 1999	http://www.ietf.org/rfc/rfc2246.txt
HTTP Auth	IETF	RFC	Jun 1999	http://www.ietf.org/rfc/rfc2617.txt
XML Signature	W3C	1.0 REC	12 Feb 2002	http://www.w3.org/TR/xmldsig-core/
XML Encryption	W3C	1.0 REC	10 Dec 2002	http://www.w3.org/TR/xmlenc-core/
XML Key Management (XKMS)	W3C	2.0 REC	28 Jun 2005	http://www.w3.org/TR/xkms2/
WSS "WS-Security"	OASIS	1.0 Standard 1.1 Standard	Mar 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15407/
WSS X.509Token	OASIS	1.0 Standard 1.1 Standard	Mar 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15413/
WSS UsernameToken	OASIS	1.0 Standard 1.1 Standard	Mar 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15410/
Kerberos Token Profile	WS-I	1.0 WGD	29 Aug 2005	http://www.ws-i.org/Profiles/KerberosTokenProfile-1.0.html
WSS KerberosToken	OASIS	1.1 Standard	14 Nov 2005	http://www.oasis-

Standard or Specification	Standards initiative	Version / Status	Date	Reference
				open.org/committees/download.php/15401/
SAML Token Profile	WS-I	1.0 WGD	13 May 2005	http://www.ws-i.org/Profiles/SAMLTokenProfile-1.0.html
WSS SAMLToken	OASIS	1.0 Standard 1.1 Standard	1 Dec 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15458/
REL Token Profile	WS-I	1.0 WGD	13 May 2005	http://www.ws-i.org/Profiles/RELTokenProfile-1.0.html
WSS RELToken	OASIS	1.0 Standard 1.1 Standard	19 Dec 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15404/
WSS Mprof	OASIS	1.0 WD	7 Mar 2003	http://www.oasis-open.org/committees/download.php/1720/WSS-MinimalistProfile-20030307.pdf
WSS SwA	OASIS	1.0 CD 1.1 Standard	23 Dec 2004 14 Nov 2005	http://www.oasis-open.org/committees/download.php/15419/
WS-SecureConversation	OASIS	Actional, BEA, Computer Associates, IBM, Layer7, Microsoft, Oblix, OpenNetwork, Ping Identity, Reactivity, RSA Security, and VeriSign (version submitted to OASIS WS-SX TC)	Feb 2005	http://msdn.microsoft.com/ws/2005/02/ws-secure-conversation/
WS-SecurityPolicy	OASIS	IBM, Microsoft, RSA Security, and VeriSign (version submitted to OASIS WS-SX TC)	July 2005	http://msdn.microsoft.com/ws/2005/07/ws-security-policy/
WS-Trust	OASIS	Actional, BEA, Computer Associates, IBM, Layer7, Microsoft, Oblix, OpenNetwork, Ping Identity, Reactivity, RSA Security, and VeriSign (version submitted to OASIS WS-SX TC)	Feb 2005	http://msdn.microsoft.com/ws/2005/02/ws-trust/
WS-Federation	industry	BEA, IBM, Microsoft, RSA Security and VeriSign	8 Jul 2003	http://msdn.microsoft.com/ws/2003/07/ws-federation/
WS-Federation Active Requestor Profile	industry	BEA, IBM, Microsoft, RSA Security and VeriSign	8 Jul 2003	http://msdn.microsoft.com/ws/2003/07/ws-active-profile/
WS-Federation Passive Requestor Profile	industry	BEA, IBM, Microsoft, RSA Security and VeriSign	8 Jul 2003	http://msdn.microsoft.com/ws/2003/07/ws-passive-profile/
Basic Security Profile	WS-I	1.0 WGD	29 Aug 2005	http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html
SAML	OASIS	2.0 Standard	15 Mar 2005	http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
Use of SAML for OGSA Authorisation Profile	GGF	Last Call	Feb 2005	https://forge.gridforum.org/projects/ogsa-authz
XACML	OASIS	2.0 Standard	1 Feb 2005	http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip
Liberty	Liberty Alliance	-	-	http://www.projectliberty.org/resources/specdiagram.php
Shibboleth	Internet2	WD	28 Feb 2005	http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-arch-protocols-latest.pdf
Web Single Sign-On Interoperability Profile	industry	Microsoft and Sun Microsystems	Apr 2005	http://msdn.microsoft.com/ws/2005/04/ssi/websso/
Web Single Sign-On Metadata Exchange	industry	Microsoft and Sun Microsystems	Apr 2005	http://msdn.microsoft.com/ws/2005/04/ssi/websso-mex/

Standard or Specification	Standards initiative	Version / Status	Date	Reference
Protocol				
WS-Policy	W3C	Member Submission (BEA, IBM, Microsoft, SAP, Sonic Software, and VeriSign)	25 Apr 2006	http://www.w3.org/Submission/WS-Policy/
WS-PolicyAssertions	industry	BEA, IBM, Microsoft, and SAP	28 May 2003	http://msdn.microsoft.com/ws/2002/12/PolicyAssertions/
WS-PolicyAttachment	W3C	Member Submission (BEA, IBM, Microsoft, SAP, Sonic Software, and VeriSign)	25 Apr 2006	http://www.w3.org/Submission/WS-PolicyAttachment/
WSBPEL	OASIS	CD1	1 Sep 2005	http://www.oasis-open.org/committees/download.php/14616/wsbpel-specification-draft.htm
WS-CDL	W3C	1.0 WD	17 Dec 2004	http://www.w3.org/TR/ws-cdl-10/
BPML	BPMI	1.0	8 Mar 2001	http://www.bpmi.org/
WSCI	W3C	1.0 NOTE	8 Aug 2002	http://www.w3.org/TR/wsci/
WS-Coordination	OASIS	BEA, IBM, and Microsoft (version submitted to OASIS WS-TX TC)	Nov 2004	http://msdn.microsoft.com/ws/2004/10/ws-coordination/
WS-AtomicTransaction	OASIS	BEA, IBM, and Microsoft (version submitted to OASIS WS-TX TC)	Nov 2004	http://msdn.microsoft.com/ws/2004/10/ws-atomictransaction/
WS-BusinessActivity	OASIS	BEA, IBM, and Microsoft (version submitted to OASIS WS-TX TC)	Nov 2004	http://msdn.microsoft.com/ws/2004/10/ws-businessactivity/
XML	W3C	1.0 (3rd) REC	4 Feb 2004	http://www.w3.org/TR/REC-xml
SOAP	W3C	1.2 REC	24 Jun 2003	http://www.w3.org/TR/soap12-part0/
HTTP	IETF	1.1 RFC	Jun 1999	http://www.ietf.org/rfc/rfc2616.txt
MTOM	W3C	1.0 REC	25 Jan 2005	http://www.w3.org/TR/soap12-mtom/
XOP	W3C	1.0 REC	25 Jan 2005	http://www.w3.org/TR/xop10/
Resource Representation SOAP Header Block	W3C	1.0 REC	25 Jan 2005	http://www.w3.org/TR/soap12-rep/
WSDL	W3C	2.0 WD	3 Aug 2004	http://www.w3.org/TR/wsdl20
UDDI	OASIS	3.0.2 Standard	Feb 2005	http://uddi.org/pubs/uddi-v3.0.2-20041019.pdf
Basic Profile	WS-I	1.1 Final	24 Aug 2004	http://www.ws-i.org/Profiles/BasicProfile-1.1.html
Attachments Profile	WS-I	1.0 Final	24 Aug 2004	http://www.ws-i.org/Profiles/AttachmentsProfile-1.0.html
Simple SOAP Binding Profile	WS-I	1.0 Final	24 Aug 2004	http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html
WS-ReliableMessaging	OASIS	CD1	26 Sep 2005	http://www.oasis-open.org/committees/download.php/15177/wsrm-1.1-spec-cd-01.pdf
WS-RM Policy	OASIS	CD1	19 Oct 2005	http://www.oasis-open.org/committees/download.php/15189/wsrmp-1.1-spec-cd-01.pdf
Web Services Reliable Exchange (WS-RX)	OASIS	-	(Jun 2005)	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-rx
WS-Reliability	OASIS	1.1 Standard	24 Aug 2004	http://www.oasis-open.org/committees/download.php/9330/WS-Reliability-CD1.086.zip
WS-Addressing	W3C	1.0 PR	21 Mar 2006	http://www.w3.org/TR/ws-addr-core
WS-Eventing	W3C	Member Submission (BEA, Computer Associates, IBM, Sun Microsystems, and TIBCO Software)	15 Mar 2006	http://www.w3.org/Submission/WS-Eventing/
WS-Enumeration	W3C	Member Submission (BEA,	15 Mar 2006	http://www.w3.org/Submission/WS-

Standard or Specification	Standards initiative	Version / Status	Date	Reference
		Computer Associates, Microsoft, Sonic Software, and Systinet)		Enumeration/
WS-Transfer	W3C	Member Submission (BEA, Computer Associates, Microsoft, Sonic Software, and Systinet)	15 Mar 2006	http://www.w3.org/Submission/WS-Transfer/
SOAP-over-UDP	industry	BEA, Lexmark, Microsoft, and Ricoh	Sep 2004	http://msdn.microsoft.com/ws/2004/09/soap-over-udp/
WS-MetadataExchange	industry	BEA, Computer Associates, IBM, Microsoft, SAP, Sun Microsystems, and webMethods	Sep 2004	http://msdn.microsoft.com/ws/2004/09/mex/
WS-Discovery	industry	BEA, Canon, Intel, Microsoft, and webMethods	Apr 2005	http://msdn.microsoft.com/ws/2005/04/ws-discovery/
WSRF WS-Resource	OASIS	1.2 Standard	9 Jan 2006	http://docs.oasis-open.org/wsrf/wsrf-ws_resource-1.2-spec-cs-01.pdf
WSRF WS-ResourceProperties	OASIS	1.2 Standard	20 Jan 2006	http://docs.oasis-open.org/wsrf/wsrf-ws_resource_properties-1.2-spec-cs-01.pdf
WSRF WS-ResourceLifetime	OASIS	1.2 Standard	9 Jan 2006	http://docs.oasis-open.org/wsrf/wsrf-ws_resource_lifetime-1.2-spec-cs-01.pdf
WSRF WS-ServiceGroup	OASIS	1.2 Standard	9 Jan 2006	http://docs.oasis-open.org/wsrf/wsrf-ws_service_group-1.2-spec-cs-01.pdf
WSRF WS-BaseFaults	OASIS	1.2 Standard	9 Jan 2006	http://docs.oasis-open.org/wsrf/wsrf-ws_base_faults-1.2-spec-cs-01.pdf
WSRF Application Notes	OASIS	1.2 PRD1	13 June 2005	http://docs.oasis-open.org/wsrf/wsrf-application_notes-1.2-notes-pr-01.pdf
WSRF WS-RenewableReferences	OASIS	-	-	-
WSN WS-BaseNotification	OASIS	1.3 PRD2	28 Nov 2005	http://www.oasis-open.org/committees/download.php/15846/wsn-pr-02.zip
WSN WS-Topics	OASIS	1.3 PRD1	16 Dec 2005	http://www.oasis-open.org/committees/download.php/15982/wsn_topics_pr.zip
WSN WS-BrokeredNotification	OASIS	1.3 PRD2	28 Nov 2005	http://www.oasis-open.org/committees/download.php/15846/wsn-pr-02.zip
WSDM MUWS	OASIS	1.1 CD	16 Feb 2006	http://www.oasis-open.org/committees/download.php/17238/wsdm-1.1-cd-01.zip
WSDM MOWS	OASIS	1.1 CD	23 Feb 2006	http://www.oasis-open.org/committees/download.php/17238/wsdm-1.1-cd-01.zip
WS-Management	DMTF	(previously: AMD, BMC Software, Dell, Intel, Microsoft, Sun Microsystems, and WBEM Solutions)	5 Apr 2006	http://www.dmtf.org/standards/wsman/
WS-Management Catalog	industry (submitted to DMTF)	AMD, BMC Software, Dell, Intel, Microsoft, Sun Microsystems, and WBEM Solutions	June 2005	http://msdn.microsoft.com/ws/2005/08/ws-managementcatalog/
WS-Context	OASIS	CD1	24 Oct 2005	http://www.oasis-open.org/committees/download.php/15518/WS-Context.zip
WS-CF (Coordination Framework)	OASIS	CD1	24 Oct 2005	http://www.oasis-open.org/committees/download.php/16734/WS-CF.zip
RDF	W3C	REC	10 Feb 2004	http://www.w3.org/TR/REC-rdf-syntax/

Standard or Specification	Standards initiative	Version / Status	Date	Reference
OWL	W3C	REC	10 Feb 2004	http://www.w3.org/TR/owl-features/
OWL-S	W3C	1.0 SUBM	22 Nov 2004	http://www.w3.org/Submission/OWL-S
MDA UML	OMG	1.5 (stable) 2.0 (current)	-	http://www.omg.org/technology/documents/formal/uml.htm
MDA MOF	OMG	1.4 (stable) 2.0 (current)	-	http://www.omg.org/technology/documents/formal/mof.htm
XML Metadata Interchange (XMI)	OMG	2.0 (stable) 2.1 (current)	-	http://www.omg.org/technology/documents/formal/xmi.htm
UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms	OMG	Adopted Specification	1 Jun 2004	http://www.omg.org/docs/ptc/04-06-01.pdf
BPMN	BPMI	1.0	3 May 2004	http://www.bpmn.org/
GSS-API	IETF	RFC	Jan 2000	http://www.ietf.org/rfc/rfc2743.txt
IODEF	IETF	ID	8 Aug 2005	http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-04.txt
Learning Object Metadata (LOM)	IEEE (LTSC)	Draft Standard	15 Jul 2002	http://ltsc.ieee.org/wg12/20020612-Final-LOM-Draft.html
Learner Information Package (IMS-LIP)	IMS Global Learning Consortium	1.0.1	17 Jan 2005	http://www.imsglobal.org/profiles/
initiative for open authentication	OATH	-	-	http://www.openauthentication.org/
OTP-WSS-Token	(RSA)	1.0	22 Sep 2005	http://www.rsasecurity.com/rsalabs/node.asp?id=2821
WS-Polling	(IBM)	Member Submission	26 Oct 2005	http://www.w3.org/Submission/ws-polling/
WS-Naming	GGF	Draft	Nov 2005	https://forge.gridforum.org/projects/ogsa-naming-wg/
ByteIO	GGF	Draft	28 Oct 2005	https://forge.gridforum.org/projects/byteio-wg/document/draft-byteio-rec-doc-v1-1/en/4
DIPAL	OASIS	discussion list	-	http://lists.oasis-open.org/archives/dipal-discuss/