Deliverable

71

# Final Standardisation Report

## WP13 Standards and Collaboration

Joris Claessens (editor)

European Microsoft Innovation Center

May 2007

Version 1.1

**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.

Reproduction is authorised provided the source is acknowledged.

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**: | **Final Standardisation Report** |
| **Version:** | **4.0** |
| **Document reference:** | |
| **Official delivery date:** | **31 January 2007** |
| **Actual publication date:** | |
| **File name:** | |
| **Type of document:** | Report |
| **Nature:** | Public |

**Authors:** Alvaro Arenas (CCLRC), Jesus Benedicto (Atos Origin), David Brossard (BT), David Chadwick (UoK), Joris Claessens (EMIC), Shirley Crompton (CCLRC), Theo Dimitrakos (BT), Ivan Djordjevic (BT), Pablo Giambiagi (SICS), Jochen Haller (SAP), Yücel Karabulut (SAP), Florian Kerschbaum (SAP), Emil Lupu (IC), Andreas Maierhofer (BT), Nikolaos Oikonomidis (SAP), Erik Rissanen (SICS), Philip Robinson (SAP), J Sairamesh (IBM), Lutz Schubert (HLRS), Ignacio Soler (Atos Origin), Bernhard Thurm (SAP).

**Reviewers:** Michael Wilson (CCLRC),
J Sairamesh (IBM)

**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 |
| 4.0 | February 2007 | Final Standardisation Report |
| 4.1 | May 2007 | Final Standardisation Report |

# Table of Content

# 1 Executive summary

The TrustCoM project has developed a framework for trust, security, and contract management for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. TrustCoM has been committed to the adoption of open standards, and intended 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 aimed at building upon existing well established and accepted standards and published specifications, where appropriate. TrustCoM furthermore intended to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM has participated in European project clustering activities in order to maximize impact of the project and avoid duplication of effort.

This document is the TrustCoM deliverable D71. As the Final Standardisation Report, it is the 4th and last version of the project's Standardisation Roadmap which documented the standardisation activities within the TrustCoM project, and was regularly updated throughout the lifetime of the project.

This deliverable focuses on the project's achievements 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. The main reference is the TrustCoM Framework V4 – see deliverable D63 – and the corresponding software developments – see deliverable D64.

For each of the TrustCoM subsystems, this deliverable:

- analyses the relevance of interoperability for each of the artefacts in the subsystem,
- provides a final positioning of the relevant existing standards and specifications,
- provides concrete results of, and expectations for, standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of project work.

Based on the above, this deliverable summarizes in an appendix the relationship between the project and its technical developments, and all the relevant standardisation initiatives.

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 V4 of the framework, in order 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 has been 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/] has developed a framework for trust, security, and contract management for secure, collaborative business processing and resource sharing in dynamically-evolving Virtual Organisations. TrustCoM has been committed to the adoption of open standards, and intended 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 had less bearing on this workpackage.

## 2.1 TrustCoM standardisation and collaboration objectives

Achieving the scientific and technological objectives of TrustCoM necessitated 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 aimed 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 has played a significant role in testing and enhancing emerging standards and interoperability guidelines, and intended to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM has participated 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 have been twofold:

1. The standardisation activity had to ensure that TrustCoM leveraged 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, have provided the basis for the applied research and technological development of TrustCoM.

2. The standardisation activity had to ensure that the results of TrustCoM contributed to the future developments of standards for trust, security and contract management, where appropriate. Proposed improvements of these standards were to be realised as interoperable extensions or revisions. In areas where no candidate specifications exist, TrustCoM has sought to propose new standards based on its Framework specifications, to be put forward to the appropriate technical committees for development and eventual ratification.

These standards activities – and further supported by collaboration activities – have promoted 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 has been 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 supported and documents the standardisation activities within the TrustCoM project, and was 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 were: 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.

D43 Standardisation Roadmap v3 (May 2006) focused 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 was assessed and planned. The main reference was the TrustCoM Framework V2 – see deliverable D29-35-36 (February 2006) – and the corresponding ongoing software developments. The TrustCoM subsystems relevant in this deliverable were: VO Management; Business Process Management; SLA Management; Trust and Security Services; Policy Control; EN/VO Infrastructure; Applications.

## 2.3 Scope and outline of this deliverable

As the Final Standardisation Report, this deliverable is the 4th and last version of the project's Standardisation Roadmap. It,reports about the project's achievements 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. The main reference is the TrustCoM Framework V4 – see deliverable D63 – and the corresponding software developments – see deliverable D64. The TrustCoM subsystems relevant in this deliverable are:

- VO Management

[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.

- 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 a final positioning of the relevant existing standards and specifications,
- provides concrete results of, and expectations for, standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of project work.

Note that this deliverable collects the positioning status across the technical architecture and development work in TrustCoM, but does not intend to provide an in-depth justification for each specific positioning. We refer to the technical deliverables for specific technical details.

The outline of this deliverable is as follows. Chapter 3 explains the TrustCoM standardisation approach, and discusses the concept and role of standards, and the relevance to TrustCoM, in more detail. 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 is the references list of this document. Lastly, Chapter 7 is an appendix to this deliverable, summarizing the project's relationship with all relevant standardisation initiatives.

# 3 TrustCoM standardisation approach

This chapter explains the standardisation approach that was taken by the TrustCoM project. Standards were important within the project as a whole. The main driver of considering adoption of standards as well as contributing to standards is to promote interoperability. The TrustCoM project therefore considered various types of standards and specifications (Sect. 3.1), and did not have a a-priori preference to any specific type; the involvement of key stakeholders (platform vendors, application developers, users) has been an important criterion though. The TrustCoM project focused on building upon Web Services specifications as the underlying Service Oriented Architecture technology (Sect. 3.2). Furthermore, to ensure that the results of the TrustCoM project contribute to the relevant future developments of interoperable standards for trust, security, and contract management for collaborative business processing in dynamic Virtual Organisations, the project envisaged different types of standards contributions, and has put an emphasis on the development of standards and specifications profiles (Sect. 3.3).

A separate workpackage on standardisation specifically supported the standards activities. Particularly, as part of the TrustCoM standardisation approach, the efforts in this workpackage were key in creating awareness and relevance of interoperability within the project. The workpackage also stimulated collaboration as an additional important activity towards interoperability – not necessarily directly related to driving forward standards contributions. Last but not least, this deliverable reports about many individual contributions to existing initiatives involving many organisations. An important element in the TrustCoM standardisation approach has been to direct these existing initiatives to conform to, or take into account, the TrustCoM framework, without explicitly generating a separate standards suite for the whole TrustCoM framework.

## 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.

Already in the beginning of the project, our initial assessment of the standards relevant to TrustCoM 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 final positioning of the TrustCoM project with respect to various existing standards and specifications, in the context of the 4th 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 distinguished 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.

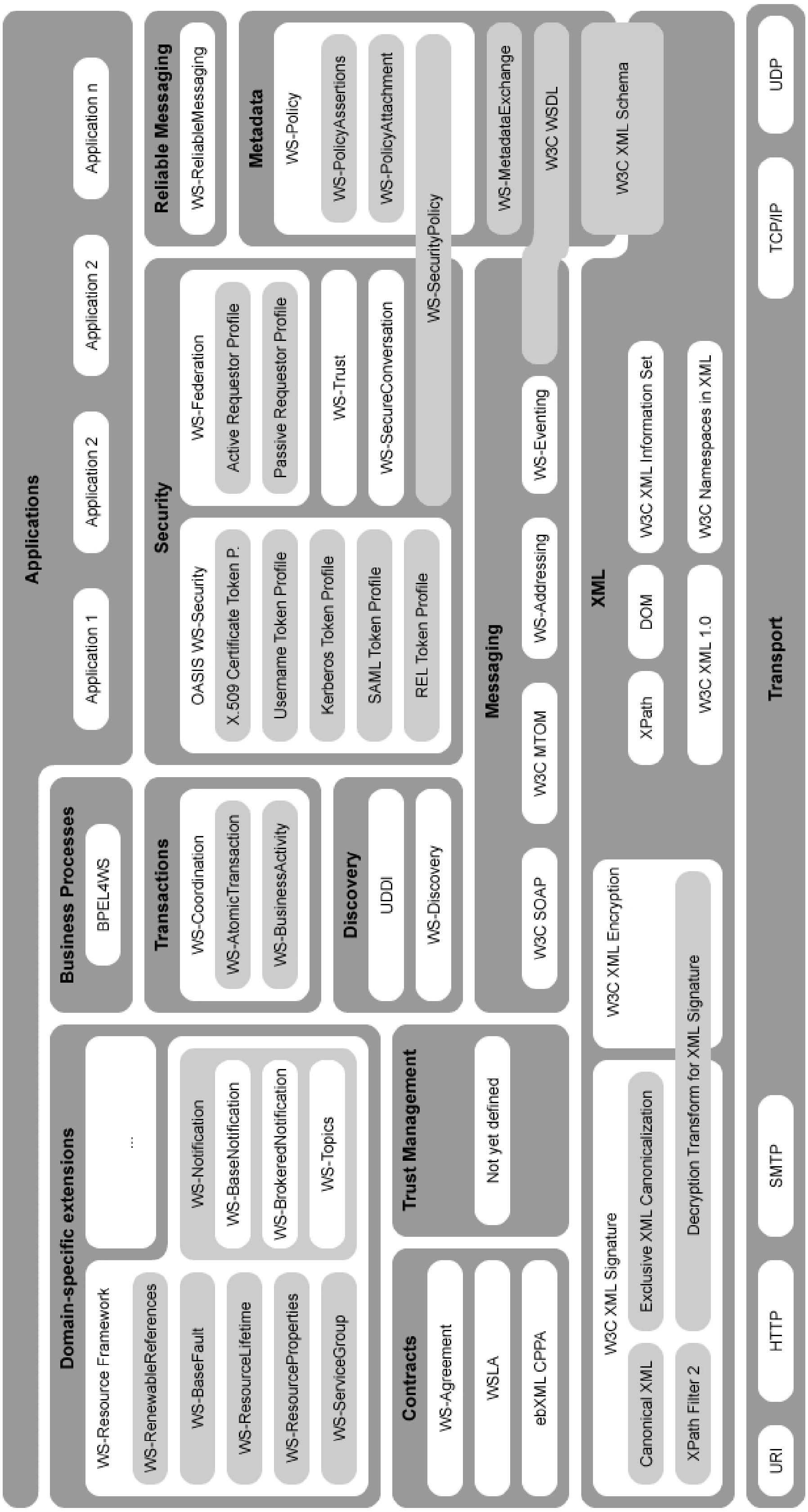


Figure 1: An architectural overview of some widely agreed and/or proposed web services related specifications relevant to TrustCoM, as existent in the first phase of the project

There has not been 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 has developed 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 has built 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, as existent in the first phase of the project. 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 that TrustCoM is an integrated project addressing trust, security, and contract management, for collaborative business processing, as a whole, and that TrustCoM has been 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 final positioning of TrustCoM to the relevant standards and specifications, with respect to the 4th version of the framework and the corresponding software developments.

## 3.3 Standardisation contributions

One of the main objectives of the TrustCoM standardisation activities has been 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 were the expected potential contributions to this already vast landscape of numerous relevant standards and specifications?

In the initial phase of the project, as part of establishing a first baseline for further activities, we identified the following possible types of contributions:

[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.

1. Profiles, to integrate existing and new specifications within and across areas;
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 has focused on the creation of *profiles* relating to Autonomic Security, Trust and Contract Management, and Secure Business Processes Enactment in dynamic Virtual Organisations. 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. Chapter 4 summarizes the concrete profiling work in each of the TrustCoM subsystems.

### 3.3.2 New contributions in specific areas

TrustCoM has proposed new contributions, based on its framework specifications, in all the TrustCoM areas of trust, contracts, security, and business processing. Some of these new specification contributions are being introduced as new standards or as extensions or updates of existing standards. Many of the contributions are specific extensions which form part of the created specification profiles. Note that we aimed at adhering to the principle of composability, and to avoiding unnecessary expansion of existing specifications. Chapter 4 details the concrete specification work in each of the TrustCoM subsystems.

### 3.3.3 Adaptations of existing standards

TrustCoM has not introduced any specific adaptations of existing standards. Only if really needed, for example if required within the context of newly proposed profiles, or for existing standards or specifications to be able to work together with new contributions, such revisions or adaptations of existing standards or specifications could have been proposed.

### 3.3.4 Dissemination of TrustCoM results within standardisation initiatives

Last but not least, a substantial part of the standardisation activities of specific TrustCoM partners consisted 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. Liaising with the appropriate bodies and people, presenting specific relevant TrustCoM results at appropriate events, giving reasons for the need for profiles, indicating potential impact or contribution to standardisation, and gathering feedback, were important for initiating and materialising specific TrustCoM standardisation contributions, and are a pre-requisite to their potential adoption and success. This effort was clearly part of the overall TrustCoM dissemination activities, and has a strong link with exploitation.

# 4 Standards roadmap TrustCoM Framework V4

This chapter reports about how the TrustCoM framework was impacted by standards, and which contributions the TrustCoM framework made to the standards world. This deliverable is complementing the deliverables D63 – TrustCoM Framework V4 – and D64 – the corresponding software developments. This deliverable therefore compiles the standards positioning across the technical architecture and development work in TrustCoM, but does not intend to provide an in-depth justification for each specific positioning. We particularly chose to structure the standardisation issues around the TrustCoM non-functional subsystems and their components – instead of e.g. around the VO lifecycle phases or the high-level TrustCoM framework relationship or deployment models – as this is mapping best to the standards world. The technical deliverables D63 and D64 are the main references for this document, and we refer to these for specific details.

For each of the TrustCoM subsystems, this deliverable:

- analyses the relevance of interoperability for each of the artefacts in the subsystem,
- provides a final positioning of the relevant existing standards and specifications,
- provides concrete results of, and expectations for, standards impact, and
- outlines concrete collaborative efforts promoting interoperability and adoption of project work.

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 TrustCoM subsystem and assess the importance of interoperability based on whether the artefact needs to interact with other subsystems and/or across organizations.
- Specifications adopted in Framework V4 – We provide a final positioning of the relevant existing standards and specifications for each artefact, and indicate which specifications (standards or other) are being used in the final TrustCoM implementation.
- Specifications relevant in future – We explain which specifications (standards or other) should be closely monitored in the future when taking the TrustCoM results further beyond the project lifetime.
- New specifications or profiles developed – We summarize the concrete specification/profiling work related to the artefact, for which no existing specifications were 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) which have been promoting interoperability and adoption of specific TrustCoM framework artefacts. We particularly highlight those cases where there has been collaboration at the technical and development level, and where there are activities which will take the TrustCoM concepts further beyond the lifetime of the project.

[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 Initiator | Service | yes | yes | Implements a reusable specification of the operations, protocols and VO-specific data for managing a VO throughout its lifetime. |
| VO management registry | Database Schema | no | no | Stores relevant VO information accessible fully to a VO Initiator and limited to VO Members in the format: (id,name,objective,state_id); |
| 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 V4

- UDDI – We use the UDDI Business-Entity-Description field for a specific, structured format for describing business entities. Similarly, the UDDI Service Description Field is populated with particular keywords that map to roles a business entity can provide, i.e. general functionality for specified collaboration descriptions and VO objectives.
- WS-Agreement – The design of the GVOA and GVOA Manager is influenced by the WS-Agreement specification.
- SOAP and WSDL – Basic Message transfer and services interface.

### 4.1.3 Specifications relevant in future

- Protocols for generation of UUIDs and URNs – as basis for VO-ID.
- WS-Agreement, WSLA, WS-Policy – as relevant for the GVOA description.
- WS-Management: in case a standardized, remote service/application management interface is necessary.
- WSDM and Globus VOMS – as possible pre-existing specifications for which profiles could be created, given the VO management concepts were to be realized in a Grid Services context.
- 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 – relevant for integration of VO management framework with non-proprietary notification subsystems.

### 4.1.4 New specifications or profiles 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.
- 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.
- VO Membership Mgmt – All developed specifications are TrustCoM proprietary. One specification that has potential for standardization is the registry query profile for selectively querying the members in a VO based on different parameters, such as their role and state. Pursuing this as a standard was however beyond the project, and this was treated as a purely technical result.
- VO Lifecycle Manager – TrustCoM proprietary query interface for asking details of a VO's state.
- GeneralGVOAContext – a schema for specifying and distributing VO-specific descriptive context information to be agreed by all members.
- Priority queue – a construct for ordering the IDs of multiple selected members in such a way that member replacement occurs by replacing the current head of the queue with the next. If there is no next member in the queue, then replacement fails when using automated replacement.
- 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 – with the rise in expectations for supporting automation and heterogeneity in VO management, especially membership management, there will be a need to standardize the protocols for managing the list of actual and potential members in a VO. This includes indicating their participant role, status and additional domain information. As membership management is a distributed process, the incorrect implementation of these protocols would lead to inconsistencies arising in the VO. This is however beyond the scope of TrustCoM, as the environment within which these protocols have assumed homogeneity, such that the needs for interoperability have never been fully explored, and consider violation of member replacement procedures as grounds for removal from the VO.
- The usage of UDDI categorization in order to define taxonomies for business entities registered with a UDDI registry is a viable alternative implementation of the keywords selection.
- 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 continue to promote the GVOA and GVOA Manager in the interoperability cluster as well as the Grid community (TG6 and CoreGRID).

The work on virtual organization management is promoted in another integrated EU project, XtreemOS. XtreemOS will develop an operating system (OS) for Grids based on a Linux kernel. TrustCoM has provided a concept for VOs where the resources are web services. XtreemOS will extend this concept to other resources such as storage, memory, hardware and CPU time, where the isolation mechanisms are implemented within the OS.

## 4.2 Business Process Management

### 4.2.1 Framework artefacts and relevance to interoperability

| *TrustCoM Framework Artefact* | *Nature* | *Cross-Subsystem?* | *Cross-Org?* | *Description / Notes* |
|---|---|---|---|---|
| BPM service | Service | no | no | Deployment and runtime control of business processes, providing a generic interface for underlying business process engines. |
| 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. |
| BP Pattern | Schema | no | no | An abstracted segment of an overall business process, which can be instantiated and composed with others for a given concrete scenario. |
| BP Control | Schema | no | no | An abstract specification of a decision point in a business process, which is evaluated by one or more services at runtime. |
| 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 | Schema and Service | no | no | (1) A DB schema for storing the various elements required to create an executable BP description from a collaboration description; (2) 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 V4

- WS-CDL – Collaboration Description, specifying the overall business collaboration involving multiple roles and partners.
- BPEL (Business Process Execution Language) – Business Process Description used to describe how a particular participant in the collaboration description executes and coordinates its internal workflows for the roles it plays
- UDDI – Universal Description Discovery and Integration. Directory storing information about involved business entities.
- SOAP and WSDL – Basic Message transfer and services interface.

### 4.2.3 Specifications relevant in future

- WS-CDL – updated version of the choreography description language may contain new elements important to the business process management part of the TrustCoM framework.
- BPEL - version 2.0 introduces new features, includes improvements and addresses shortcomings from version 1.1.
- WS-Management: for provisioning a remote management interface of the BP-related services.
- WS-BPEL Extension for People (BPEL4People): Integrating human user interactions in business processes may be beneficial in the future.

### 4.2.4 New specifications or profiles developed

- There is a WSDL specification of the BP Repository (and a corresponding design document).
- Specification for TSC (Trust, Security, Contract) Extension Roles.
- Profile in order to identify the first (initial) role in a VO from the CDL file.
- WSDL specifications of the services TSC Service, Knowledge Base, and CDL++2BPEL.

### 4.2.5 Standards roadmap

- A "control" profile for WS-CDL has been developed that allows the specification of trust, security and contract management requirements at the level of the choreography design. These requirements are then refined to specific service calls when the choreography is translated into the distributed BPEL processes at each member involved. The implementation of the profile contains three parts: the TSC (Trust, Security, Contract) Roles, the TSC Context and the TSC Services. While this has been considered as an advanced option in VOs, it has been implemented and integrated with the VO Management subsystem, with the option of enabling it only when the appropriate tags are included in the choreography description.

- The TrustCoM framework is following a top-down approach that is suitable for VOs in collaborative business processing; the traditional approach is bottom-up, following the concept of composition by mapping as opposed to via derivation. SAP has discussed specific issues with Sun and Pi4Tech on the WS-Chor mailing list concerning these two methodologies for service and process composition. 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 collaboration definition (i.e. choreography). Our approach assumes a stepwise process of integrating participants in a VO, including contractual agreements. Constant monitoring is therefore optional as partners use the choreography as a basic contract for their behavioural specifications. We proposed protocols for a top-down approach to derive private processes from a collaborative specification.
- SAP contributes to the OASIS WS-BPEL (Web Services Business Process Execution Language) Committee. In this role it may influence the further development of upcoming standards in this area drawing upon the experiences from TrustCoM and other projects.

### 4.2.6 Collaboration efforts

- TrustCoM adopted a process model based on process views (private/public processes) which is also used in other EU projects such as Athena.
- The idea of deriving access control policies from business process descriptions was injected into IFIP TC 11.3 (Security and Protection in Information Processing Systems / Data and Application Security) over a corresponding paper.
- SAP and IBM published a BPEL4People whitepaper which generally describes how the Web Services Business Process Execution Language (WS-BPEL) needs to be extended in principle to cover user interactions with business processes.
- TrustCoM contributed its requirements for WS-CDL and examples of the WS-CDL to BPEL transformations to the W3C working group developing the WS-CDL standard who took them into account in generating the Candidate Recommendation in Nov 2005 and in subsequent changes as the standard moves towards a W3C Recommendation.

## 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 V4

- WS-Agreement, WSLA – The TrustCoM SLA document description is based on a combination of two standards: WS-Agreement, for the general document structure, and WSLA, for the description of QoS requirements.
- WS-RF, WS-Notification, WS-Agreement, WSLA – SLA Evaluator, SLA Monitor, and SLA Manager are built on top of these specifications.

### 4.3.3 Specifications relevant in future

- A standard spec for a repository, such as UDDI, may be of interest. TrustCoM has focused 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 – When building further on the TrustCoM framework, it is worthwhile investigating these specifications in the context of SLA Negotiation. Initial investigations suggested that a modified FIPA Iterated CNet protocol has the potential to fulfil the general requirements on contract negotiation for virtual organizations[10].
- XML Signature – should be used as format for Signed SLAs and VO contracts. TrustCoM created a profile for signing policy 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.
- WSDM, WS-Management, WS-Coordination – The work on at least one of the demonstrators (WP38) aimed at enhancing several SLA Management components, in particular the SLA Manager and Monitors, with a management interface in accordance to the WSDM standard.

### 4.3.4 New specifications or profiles developed

- SICS and HLRS have realised a profile that captures all of the SLA relevant structures, including both agreements and templates. This profile consists of a mixture of WSLA and WS-Agreement, and can be described as a combination of (a) a general protocol (like a "header" to the SLA, based 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.
- For the SLA Repository we have built upon a TrustCoM proprietary specification for prototyping purposes. The interface of this service is specified using the corresponding WSDL document.
- 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.

### 4.3.5 Standards roadmap

- TrustCoM has adopted the format for SLA templates defined in WS-Agreement. Since this format is underspecified, the SLA profile describes how WS-Agreement templates are instantiated within TrustCoM. As for SLA documents, TrustCoM has replaced 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.

### 4.3.6 Collaboration efforts

- The SLA developments in TrustCoM have been performed in collaboration with AKoGriMo and NextGRID, with specific aspects being pursued further in the FP6 project BREIN.

[10] Pablo Giambiagi, Sakyibea Darko-Ampem and Maria Katsoufi. *Secure Negotiation in Virtual Organizations*. Advances in Quality of Service Management (AQuSerM 2006), October 2006.

## 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 (issuing 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 may have a management interface to dynamically update the configuration that controls the creation and validation of security tokens. |
| 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 V4

- SAML assertions – The TrustCoM framework adopts SAML assertions for TrustCoM cross-org security tokens and validation tokens.
- WS-Trust – The TrustCoM framework uses WS-Trust for issuing and validation of security tokens.
- The TrustCoM framework supports 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 – The TrustCoM framework applies the WS-Federation Active Requestor Profile ("U-type" interaction model).
- The TrustCoM framework uses SSL/TLS for secure transport to the audit log service.

### 4.4.3 Specifications relevant in future

- Other possible token profiles (e.g., RELToken) could be leveraged in the TrustCoM framework.
- 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 when adding this functionality to the TrustCoM framework.

- OGF OGSA Authorization profile – The OGF OGSA-Authz WG is working on a profile for authorization in Grid architectures, which is relevant in the context of the TrustCoM Trust & Security services.
- "Identity metasystem" specifications and federated identity/attribute frameworks (e.g., Liberty and Shibboleth) – These are particularly relevant for 'intra-org' authentication; they also cover metadata aspects which may be relevant as described above.
- WS-Federation profiles – Dynamic federation is essential in the TrustCoM framework; any evolutions and new profiles in this area need to be monitored when building further on the TrustCoM security services.
- WSDM and WS-Management approaches may be relevant for extending the TrustCoM support for security management; these specifications are much more service/resource generic though, than the federation-specific needs of security token service management.

#### 4.4.4 New specifications or profiles developed

- Security Token – The TrustCoM framework implements a specific profile for SAML tokens in the context of scoped federations in a VO.
- Security Token Service (issuing and validation) – The TrustCoM framework implements a specific profile for WS-Trust issuing and validation in the context of scoped federations in a VO.
- Security Token Service (management) – The TrustCoM STS supports a custom web service interface for management of TrustCoM federations.
- Reputation data – in order to integrate with the supplier scoring system TrustCoM uses a reputation metric in the range 0 (untrustworthy) to 1 (trustworthy) – real number –, with a score of 0.5 meaning neither trusted nor untrusted. The reputation algorithm was devised by Doug Kuhlman of Motorola.
- TrustCoM proprietary specifications have being developed for Reputation management service and Secure audit log.

#### 4.4.5 Standards roadmap

- The WS-Trust and SAML token profile has been 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. The updated WS-Federation specification now includes the notion of FederationID, which aligns very much with the TrustCoM federation identifier concept.
- David Chadwick (UoK) is co-chairing the OGF OGSA-Authz WG and has written specifications of WS-Trust and XACML/SAML profiles for progression as OGF standards, influenced by TrustCoM work.
- David Chadwick (UoK) is the UK (BSI) representative to ITU-T X.509 standards meetings and the editor of the authorization extensions to X.509 (2009) for recognition of authority between VO members.

#### 4.4.6 Collaboration efforts

- The WS-Trust and SAML token scoped federations profile has been significantly promoted in the NextGRID project through the FP6 Grid Trust and Security concertation and through EMIC as a common partner in these projects. As a consequence, the TrustCoM web service security model has been adopted in NextGRID.

- The STS developments were 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 were pursued.
- Prof. Marty Humphreys has submitted a bid for grid auditing to NSF that uses the 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 Decision Point (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 (access control) | 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 | yes | yes | A format for digital signatures which allows to authenticate the origin of a policy. |

### 4.5.2 Specifications adopted in Framework V4

- XACML 3.0 (upcoming) – For the PDP, we use the XACML Request context as a message format. For an access control policy, we use XACML 3.0. Token claims are translated into XACML attributes before feeding them into the PDP for use inside the access control policies. A signed access control policy is in the format specified in the SAML profile for XACML (upcoming update for XACML 3.0) where the signature is made with a X.509 certificate/private key.

### 4.5.3 Specifications relevant in future

- SAML profile for XACML – The SAML profile developed by the XACML TC defines a message format for invoking an XACML PDP. The profile is being updated for XACML 3.0.
- OGF OGSA-Authz WG is also producing an alternative SAML/XACML protocol profile for communication between the PEP and PDP.
- DMTF's Policy Core Information Model (PCIM) and TM-forum's NGOSS.[11]

[11] PCIM and NGOSS also encode an ECA model. The NGOSS model in particular is based in part on Imperial College's Ponder work (see Chapter 5 in Strassner, J. "Policy Based Network

- Researchers from ETRI, Korea submitted a paper to W3C on ECA policies.[12] 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.

### 4.5.4 New specifications or profiles developed

- Access Control Policy and PDP – The TrustCoM profile for XACML contains specific details on how to use XACML in a VO for delegation of authority, and also covers the PDP interface aspects.
- Claims – TrustCoM proprietary token claims, LDAP attributes, X.509 ACs and XACML attribute assertions values are used. A profile for consistency between token claims and policy attributes as used has been developed based on X.509 ACs.

### 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 standardized PDP interfaces with methods for loading signed policies.
- David Chadwick (UoK) is the joint chair of the OGF OGSA-Authz WG and is the editor of the XACML/SAML profile for PEP-PDP interactions and WS-Trust profile for PEP-STS (validation) interactions.

### 4.5.6 Collaboration efforts

- Policy (ECA) – TrustCoM has collaborated with the DIADEM FIREWALL project for alignment of policy models. Imperial College London is also an active participant in the EMANICS (European Network of Excellence for the Management of Internet Technologies and Complex Services) network of excellence in network and systems management, and is involved in aspects relating to policy-based management and autonomic computing.

## 4.6 EN/VO Infrastructure

### 4.6.1 Framework artefacts and relevance to interoperability

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

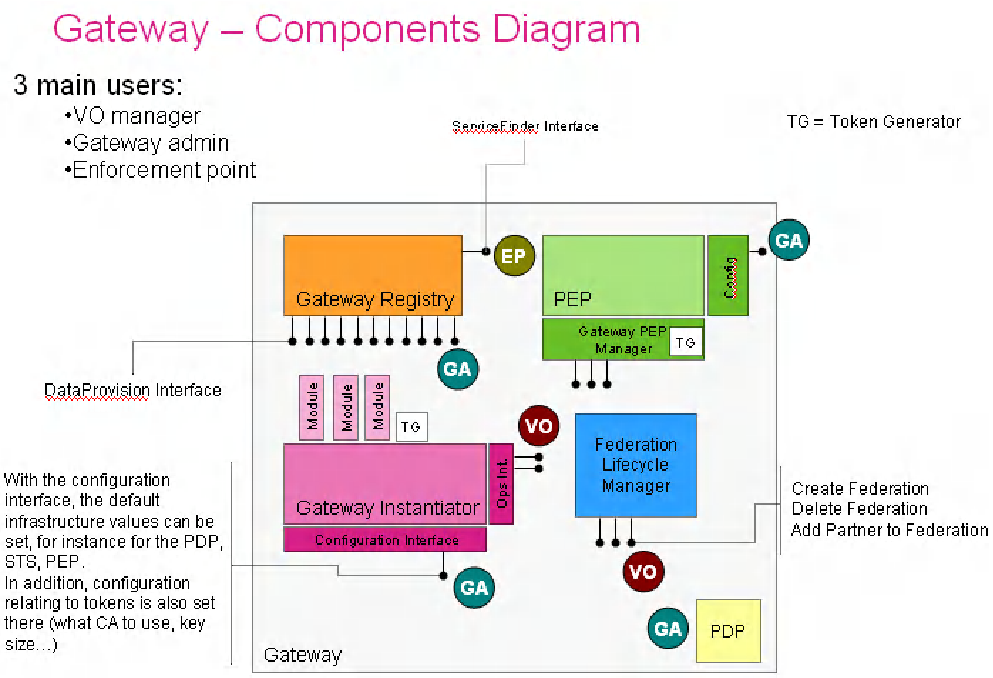
Management", Morgan Kaufmann, 2003, ISBN: 1558608591). However both assume an environment which is not present in TrustCoM (i.e. CIM information model, and NGOSS environment respectively).

[12] 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. |
| Gateway Federation Lifecycle Manager | Service | yes | no | The Gateway Federation Life-cycle Manager implements a process that configures the Gateway Registry and the Security Token Service with information about the creation, deletion and life-cycle management of Circles of Trust that underpin the operation of a Federation. It also has “extension hooks” that allow<br>(a) coordinating state between Gateways across organisations,<br>(b) coordinating and synchronising state across multiple STS within the same organisation,<br>(c) configuration management interface for an advance administrator experience |
| Gateway Instantiator: Virtualization service | Service | yes | no | The Instantiator subsystem by BT 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.<br>Configuration includes:<br>1. creating a per-service policy enforcement profile (configuration) stored in a resource properties document associated with the management interface enforcement component<br>2. obtaining a certificate (X.509) identifying the service within the scope of the provider's realm<br>3. storing the certificate within the enforcement component and referencing it via the abovementioned resource properties document representing a per service enforcement configuration<br>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<br>5. initiating configuration of the STS by making available the internal identity certificate (e.g. X.509) to the STS<br>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<br>7. optional: initiating the configuration of the SLA monitoring by providing the "SLA identifier" to the SLA manager component(s) |
| Gateway Instantiator: Service Instance Registry | Service | yes | no | An internal SQL database accessible by the instantiator service 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) |

| | | | | |
|---|---|---|---|---|
| Gateway Enforcement: Policy Enforcement Point 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. |
| Gateway 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.<br>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:<br>- virtual endpoint of the service<br>- Enforcement configuration policy: which enforcement actions (e.g. encryption, token validation, signature check, etc.) to be performed per protected service<br>- Interceptor Reference policy: configuration information mapping each enforcement action to a group of handlers<br>- endpoints of STS and of PDP used for the protected service<br>- X.509 certificate identifying the protected service within a partners VO<br>- active contexts within which the protected service is participating<br>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 subsystem 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 | Service | yes | yes | HLRS has implemented a system for supporting notification distribution that is used on a per service provider / VO partner and not on a per service (resource) basis.<br>The proxy principally fulfils an independent role and may be used standalone – accordingly, integration with the enforcement middleware depends on the overall progress. |
| Notification Broker | Service | no | no | The Broker’s functionalities are two-fold: in addition to brokering (notification) messages, it acts as a subscription manager that can maintain all notification sources and sink within a VO. |

The diagram below shows a high-level Architecture of the business-to-business Gateway (GW), a central capability of TrustCoM EN/VO infrastructure.



Gateway – Components Diagram

3 main users:

- VO manager
- Gateway admin
- Enforcement point

TG = Token Generator

With the configuration interface, the default infrastructure values can be set, for instance for the PDP, STS, PEP. In addition, configuration relating to tokens is also set there (what CA to use, key size…)

Create Federation
Delete Federation
Add Partner to Federation

### 4.6.2 Specifications adopted in Framework V4

The table below maps standards to the GW components:

| **Component / Service** | **Standards Used** |
|---|---|
| Gateway Registry | ▪ Non-WS interface: standard JAVA API<br>▪ WS Interface: SOAP 1.1; WSDL |
| Token Generator (X509 STS) | ▪ Non-WS interface: standard JAVA API |
| Gateway Federation Lifecycle Manager | ▪ WS Interface: SOAP 1.1<br>▪ Client interface to the STS: WS-Security + WS-Addressing |
| Gateway Instantiator (Virtualization service) | ▪ WS Interface: SOAP 1.1<br>▪ Client interface to the STS: WS-Security |
| Security Token Service Security (STS) | ▪ WS-Trust<br>▪ WS-Addressing<br>▪ XACML (for assertion values)<br>▪ SAML (for assertion elements) |
| Policy Decision Point (PDP) | ▪ XACML (access control policy and for PEP2PDP protocol) |
| Policy Service | ▪ XML with WS-N compatible data-types |
| Policy Enforcement Point (PEP) | ▪ WS-Addressing<br>▪ WS-Trust<br>▪ XACML<br>▪ WSDM<br>▪ WS-Notification |
| Notification | ▪ WS-Notification<br>▪ WSRF |

- 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 has committed to define new specifications and enhancements enabling further convergence of these platforms.[13] WS-ResourceTransfer is the first specification in this direction.
- 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 has committed to define new specifications and enhancements enabling further convergence of these platforms.[13]
- UDDI – The TrustCoM framework could have used UDDI for the Service Instance Registry, but it did not 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 developed

- WSRF ResourceProperties document 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.
- 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

[13] 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. http://msdn2.microsoft.com/en-us/library/aa480724.aspx

- 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 have tried to avoid instigating a modification of existing standards to the extent that this is possible. Specifically, by consolidating all relevant service information into a single WSRF ResourceProperties document per virtualized service, the TrustCoM framework in principle supports easy migration from WSRF to WS-Transfer or converged WS stack.
- Based on the TrustCoM experience, BT expects to produce instantiation and factory design patterns for WS.
- Based on the TrustCoM experience, we have identified that it would be worthwhile to look further into coordinator interposition for federation bootstrapping, and to define atomic transaction types for VO/EN configuration processes.

### 4.6.6 Collaboration efforts

- BT has been interacting with the 21 Century Network initiative towards which intends to exploit much of the work on the Gateway architecture and parts of its implementation.
- BT has been interacting with the FP6 European Projects GUIDE, Akogrimo, ELeGI and BEinGRID. An enhanced implementation of the Gateway architecture described above will be made available to BEinGRID (subject to usage / license restrictions) and will be used by at least one BEinGRID Business Experiment. We have been in close contact with BT standards teams in both W3C and OASIS in order to ensure durability of exploitation.
- BT has been in discussions with SOA security appliance vendors and plans to enhance the implementation of the security Gateway by selectively replacing the implementation of enforcement & message processing components with an enhance implementation over SOA security appliances and optimized crypto / XML co-possessor hardware.
- HLRS' notification work has been performed in collaboration with European Projects 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. |

| | | | | |
|---|---|---|---|---|
| SLAManager | Service | yes | yes | SLA Manager is the interface that allows to the initialize/manage the system for monitoring services. It works jointly with the notification system and the Monitor service. |
| MMStorage | Service | yes | yes | MMStorage, service to store and manage the different kind of metrics, that the monitor service monitors (ResponseTime, InvocationCount, etc.) |
| MonitorService | Service | yes | yes | MonitorService, service that monitors the different metric ones, indicated in document SLA, and send the values to the notification system. |
| 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 V4

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

#### 4.7.3 Specifications relevant in future

There are no specifications identified as relevant for the future since the application-specific developments were intended to validate the TrustCoM framework, but were not part of the framework itself.

#### 4.7.4 New specifications or profiles developed

Besides specifications for the application services, we have mainly been 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 has helped integration to the extent that it allowed 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 did 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 was internal to the configuration of the enforcement infrastructure and, although important for the integration within TrustCoM, they were not exposed across partners in a TrustCoM VO.
- WS-Addressing: the "reference properties" has been used in some cases, inherited from the current implementations of WS-Addressing and WSDM that were used as a baseline for development (e.g. Open Source Apache project).

#### 4.7.5 Standards roadmap

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

### 4.7.6 Collaboration efforts

- Some of the application-specific developments (such as the storage provider) have been 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 aimed at building upon existing well established and accepted standards and published specifications, where appropriate. TrustCoM furthermore intended to contribute to the evolution of, and feed research results into, standards, where and in which way appropriate. TrustCoM has also participated 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 V4 and the corresponding developed software components.

## 5.1 Using standards within the TrustCoM framework

### 5.1.1 Awareness and relevance of interoperability

As a pre-requisite for any standards adoption or contribution, the standards workpackage 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. The standards workpackage stimulated the conceptual work as well as the ongoing software developments within the project to explicitly take into account interoperability requirements and to define clear and concrete specifications, which can be validated in the integration scenarios.

### 5.1.2 Adoption of existing standards and specifications

TrustCoM has built 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 have moreover been 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. [13]

Conformance to these developing standards has cost the project extra effort and delays which it would not have faced if it had chosen to develop independent approaches which did not rely upon others. However, as these approaches taken by industry are converging, and that convergence has been taken into account by the project, the conformance puts TrustCoM in a much better position to have an impact on industrial development than it would have had if it had chosen to go its own way.

## 5.2 Contributing to interoperability and standards

### 5.2.1 Profiles

The primary focus of the TrustCoM standards and collaboration activity has been 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 developed:

- A "control" profile for WS-CDL has been developed that allows the specification of trust, security and contract management requirements at the level of the choreography design. These requirements are then refined to specific service calls when the choreography is translated into the distributed BPEL processes at each member involved. The implementation of the profile contains three parts: the TSC (Trust, Security, Contract) Roles, the TSC Context and the TSC Services.
- A profile that captures all SLA relevant structures, including both agreements and templates, has been 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 has been 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 has been defined. As highlighted below, SICS is contributing to future versions of the SAML profile for XACML being a member of the OASIS XACML TC.
- A WSRF ResourceProperties document has been 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.
- TrustCoM has suggested to develop profiles around coordination, particularly combining WS-Coordination with WS-Context, and for XACML-based coordination policies, and to define atomic transaction types for EN/VO configuration processes.
- TrustCoM has identified the requirement for a profile for signing documents in a VO context. This is needed for signing SLA as well as policies within a VO.

The different subsystems have ultimately been 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 has not only validated the above profiles with respect to addressing the security, contract, and business processing requirements, but also provided 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.

### 5.2.2 Specific new contributions

TrustCoM has proposed new contributions, based on its framework specifications. Some of these new contributions are being introduced as new standards or as extensions or updates of existing standards. Note that we aimed at adhering to the principle of composability, and to avoiding unnecessary expansion of existing specifications.

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

- A TrustCoM proprietary specification (VO-ID) for a UUID surrounded by an XML structure that describes the creation date, objective and host of the VO, is developed.

- An extension to the UDDI BusinessEntity element, consisting of the VO identifier, for VO Member description is defined. The usage of UDDI categorization in order to define taxonomies for business entities registered with a UDDI registry is considered.
- The VO Membership Mgmt registry query profile for selectively querying the members in a VO based on different parameters, such as their role and state, has the potential for standardisation.
- GVOA and GeneralGVOAContext schemas have been specified for respectively expressing general agreements in VOs, integrating business/legal terms and conditions and technical terms and conditions (QoS) within the same framework, and for specifying and distributing VO-specific descriptive context information to be agreed by all members.
- A TrustCoM proprietary WSDL specification of the BP Repository has been developed.
- A TrustCoM proprietary WSDL specification for the SLA Repository has been developed.
- TrustCoM proprietary specifications have been developed for Reputation management service and Secure audit log.
- SICS is contributing to future versions of the SAML profile for XACML, which would be more suitable for delegated use.

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

### 5.2.3 Dissemination within standardisation initiatives

A substantial part of the standardisation activities consisted 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:

- SAP promoted 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.
- SAP contributes to the OASIS WS-BPEL (Web Services Business Process Execution Language) Committee. In this role it may influence the further development of upcoming standards in this area drawing upon the experiences from projects such as TrustCoM.
- HLRS and SICS have realized 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.
- 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.
- The WS-Trust and SAML token profile is disseminated by EMIC to the relevant people in Microsoft. The updated WS-Federation specification was influenced and now includes a FederationID.
- UoK is co-chairing the OGF OGSA-Authz WG and has written specifications of WS-Trust and XACML/SAML profiles for progression as OGF standards, influenced by TrustCoM work.
- UoK is the UK (BSI) representative to ITU-T X.509 standards meetings and the editor of the authorization extensions to X.509 (2009) for recognition of authority between VO members.
- 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 standardized PDP interfaces with methods for loading signed policies.

- David Chadwick (UoK) is the joint chair of the OGF OGSA-Authz WG and is the editor of the XACML/SAML profile for PEP-PDP interactions and WS-Trust profile for PEP-STS (validation) interactions.
- BT has been interacting with the 21 Century Network initiative towards which intends to exploit much of the work on the Gateway architecture and parts of its implementation. BT has also been in close contact with BT standards teams in both W3C and OASIS in order to ensure durability of exploitation.

### 5.2.4 Collaboration with other projects

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

The following specific collaborations have been promoting interoperability of concrete technical work:

- The GVOA work has been promoted within the FP6 Grid Trust and Security TG6 technical concertation group, and particularly within the FP6 CoreGrid project. CCLRC is also promoting this work within the CCLRC E-Science Centre, expecting this work can be leveraged and integrated into other projects.
- The work on VO management is promoted in the FP6 XtreemOS project.
- The TrustCoM framework adopts the same process model for collaborative business processing as used in FP6 Athena and other projects.
- The SLA developments in TrustCoM have been performed in collaboration with FP6 AKoGriMo and FP6 NextGRID, with specific aspects being pursued further in the FP6 BREIN project.
- The WS-Trust and SAML token scoped federations profile has been significantly promoted in the FP6 NextGRID project through the FP6 Grid Trust and Security concertation and through EMIC as a common partner in these projects. The TrustCoM web service security model has been adopted in NextGRID.
- 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.
- BT has been interacting with the FP6 European Projects GUIDE, Akogrimo, ELeGI and BEinGRID. An enhanced implementation of the Gateway architecture described above will be made available to BEinGRID (subject to usage / license restrictions) and will be used by at least one BEinGRID Business Experiment.
- BT has been in discussions with SOA security appliance vendors and plans to enhance the implementation of the security Gateway by selectively replacing the implementation of enforcement & message processing components with an enhance implementation over SOA security appliances and optimized crypto / XML co-possessor hardware.
- HLRS' notification work has been performed in collaboration with the FP6 projects AKoGriMo, and ELeGi.

## 5.3 Conclusion

This deliverable has focused on the project's achievements 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 has been assessed.

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 the standards workpackage in particular, the ongoing software developments were 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.

Conformance to these developing standards has cost the project extra effort and delays which it would not have faced if it had chosen to develop independent approaches which did not rely upon others. However, as these approaches taken by industry are converging, and that convergence has been taken into account by the project, the conformance puts TrustCoM in a much better position to have an impact on industrial development than it would have had if it had chosen to go its own way.

A number of concrete profiles of existing specifications, including some new extensions, have been 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 have been substantial collaborations with other projects to promote interoperability of concrete technical work. It is important to note that there has not only been a collaboration with projects running in parallel to TrustCoM, such as Akogrimo, Athena, NextGRID, CoreGrid, and others; but that TrustCoM has also ensured take-up of its framework technologies in future projects, such as GridTrust, BREIN, XtreemOS, and BEinGRID.

The TrustCoM standards roadmap has focused on impact and plans aligned with concrete technical developments in AL2 of the project. As a consequence, this deliverable mainly focused 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.

In summary, we believe that the TrustCoM project has achieved and initiated a significant impact on standards. Various partners in the project have pushed forward specific contributions based on TrustCoM results in the form of individual technology enhancements as well as specification profiles. These contributions have been presented to the appropriate community, and have shown to provide the required functionality amongst the TrustCoM project partners as well as to the community. Evolving standards are taking into account the project's contributions. The actual completion of these standards is happening beyond the project's lifetime, and various partners are taking forward their TrustCoM activities beyond the project's lifetime in that respect.

# 6 References

The table below is a complete reference list of standards and specifications that are relevant to TrustCoM – as positioned in Chapter 4. These standards and specifications have either been adopted in the TrustCoM Framework V4, or they have been identified as relevant for future work beyond TrustCoM.

| Standard or Specification | Standards initiative | Version / Status | Date | Reference |
|---|---|---|---|---|
| SOAP | W3C | 1.2 REC | 24 Jun 2003 | http://www.w3.org/TR/soap12-part0/ |
| WSDL | W3C | 2.0 CR | 27 Mar 2006 | http://www.w3.org/TR/wsdl20/ |
| WS-Addressing | W3C | 1.0 REC | 9 May 2006 | http://www.w3.org/TR/ws-addr-core/ |
| MTOM | W3C | 1.0 REC | 25 Jan 2005 | http://www.w3.org/TR/soap12-mtom/ |
| WSRF (Resource, ResourceProperties, ResourceLifetime, ServiceGroup, BaseFaults | OASIS | 1.2 Standard | 1 Apr 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrf |
| WS-Notification (BaseNotification, BrokeredNotification, Topics) | OASIS | 1.3 Standard | 1 Oct 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsn |
| WS-Transfer | W3C | Member Submission (BEA, Computer Associates, Microsoft, Sonic Software, and Systinet) | 15 Mar 2006 | http://www.w3.org/Submission/WS-Transfer/ |
| 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, Computer Associates, Microsoft, Sonic Software, and Systinet) | 15 Mar 2006 | http://www.w3.org/Submission/WS-Enumeration/ |
| WS-ResourceTransfer | Industry | HP, IBM, Intel, Microsoft | Aug 2006 | http://msdn.microsoft.com/ws/2006/08/ws-resourcetransfer/ |
| WSDM MUWS/MOWS | OASIS | 1.1 Standard | 1 Aug 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm |
| WS-Management | DMTF | 1.0 | 5 Apr 2006 | http://www.dmtf.org/standards/wsman/ |
| UDDI | OASIS | 3.0.2 Standard | Feb 2005 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec |
| WS-CDL | W3C | 1.0 CR | 9 Nov 2005 | http://www.w3.org/TR/ws-cdl-10/ |
| WSBPEL | OASIS | 2.0 CD | 21 Dec 2005 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel |
| WSBPEL4People | Industry | IBM+SAP | July 2005 | ftp://www6.software.ibm.com/software/developer/library/ws-bpel4people.pdf |
| ebXML CPPA | OASIS | 2.0 | 23 Sep 2002 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa |
| WS-Agreement and AgreementNegotiation | OGF | 2006/09 Draft | 7 Sep 2006 | https://forge.gridforum.org/sf/projects/graap-wg |
| WSLA | Industry | IBM | 28 Jan 2003 | http://www.research.ibm.com/wsla/WSLASpecV1-20030128.pdf |
| Iterated Contract Net Interaction Protocol | FIPA | Standard | 3 Dec 2002 | http://www.fipa.org/specs/fipa00030/SC00030H.pdf |

| Standard or Specification | Standards initiative | Version / Status | Date | Reference |
|---|---|---|---|---|
| WS-Coordination, WS-AtomicTransaction, WS-BusinessActivity | OASIS | 1.1 CS | 4 Dec 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-tx |
| WS-Context | OASIS | 1.0 CS | 11 Aug 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-caf |
| X.509 PKI and 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 |
| SSL/TLS | IETF | 1.1 RFC | April 2006 | http://www.ietf.org/rfc/rfc4346.txt |
| XML Signature | W3C | 1.0 REC | 12 Feb 2002 | http://www.w3.org/TR/xmldsig-core/ |
| SAML (assertions) | OASIS | 2.0 Standard | 15 Mar 2005 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security |
| SOAP Message Security (incl. X.509, Username, Kerberos, REL, and SAML Token Profiles) | OASIS | 1.1 Standard | 1 Feb 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss |
| WS-Trust (and WS-SecureConversation, WS-SecurityPolicy) | OASIS | 1.3 CS | 29 Nov 2006 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ws-sx |
| WS-Federation | Industry | 1.1; BEA, BMC Software, CA, IBM, Layer 7 Technologies, Microsoft, Novell, and VeriSign | 8 Dec 2006 | http://specs.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf |
| WS-MetadataExchange | Industry | 1.1; BEA, Computer Associates, IBM, Microsoft, SAP, Sun Microsystems, and webMethods | Aug 2006 | http://specs.xmlsoap.org/ws/2004/09/mex/ws-metadataexchange.pdf |
| WS-Policy (and WS-PolicyAttachment) | W3C | 1.5 WD | 17 Nov 2006 | http://www.w3.org/TR/ws-policy/ |
| XACML | OASIS | 2.0 Standard | 1 Feb 2005 | http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml |
| OGSA-Authz WG | OGF | Authorization profiles | - | https://forge.gridforum.org/sf/projects/ogsa-authz |
| Web Single Sign-On Interoperability Profile | industry | Microsoft and Sun Microsystems | Apr 2005 | http://xml.coverpages.org/WebSSO-InteropProfile200505.pdf |
| Liberty | Liberty Alliance | - | - | http://www.projectliberty.org/ |
| Shibboleth | Internet2 | - | - | http://shibboleth.internet2.edu/ |
| Basic Profiles and Basic Security Profiles | WS-I | - | - | http://www.ws-i.org/ |

# 7 Appendix: Standardisation initiatives

This appendix lists all the standardisation initiatives relevant to TrustCoM. For each initiative, we summarize the concrete impact from/to standards with respect to the TrustCoM Framework V4 and the corresponding developed software components.

The list of relevant standardisation initiatives includes: W3C, OASIS, WS-* industry specifications, WS-I, OGF, DMTF, ETSI, Liberty Alliance, Internet2, OMG, FIPA, IETF, ISO, Ecma International, UN/CEFACT, and a number of industry/domain-specific initiatives.

## 7.1 W3C

The World Wide Web Consortium [http://www.w3.org/] was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 350 Member organizations from all over the world and has earned international recognition for its contributions to the growth of the Web.

*Impact from W3C on the TrustCoM framework*

Essentially all corporate and governmental partners of TrustCoM are active within W3C and they include two regional W3C offices (CCLRC and SICS) where the individuals leading the office are directly involved in the project.

W3C provides the fundamental web services baseline for TrustCoM. The TrustCoM Framework V4 builds on top of the SOAP, WSDL, WS-Addressing, and MTOM specifications. The TrustCoM security elements leverage XML Signature and Encryption, and draw upon WS-Policy which is progressing towards standardisation in W3C. The member submissions WS-Transfer, WS-Eventing, and WS-Enumeration, are considered for future work.

*Impact from TrustCoM on W3C*

TrustCoM particularly developed a "control" profile for WS-CDL that allows the specification of trust, security and contract management requirements at the level of the choreography design. The TrustCoM activity in WS-CDL has been used by the working group developing WS-CDL as an advanced demonstrator and test case.

## 7.2 OASIS

OASIS stands for Organization for the Advancement of Structured Information Standards [http://www.oasis-open.org/]. OASIS is a global consortium aiming to drive the development, convergence and adoption of XML-based standards for e-business. This is currently a primary forum for the development of higher level XML specifications into accepted standards. OASIS is, according to the mission statement, a “not-for-profit, global consortium that drives the development, convergence and adoption of e-business standards".

*Impact from OASIS on the TrustCoM framework*

Of the TrustCoM partners, SAP, IBM, Microsoft, BAE Systems and BT are all OASIS members at various levels.

With respect to TrustCoM, OASIS provides standards for more advanced web services concepts on top of the web services baseline. Actual and/or candidate standards adopted by, or important in, the TrustCoM Framework V4 include: “WS-Security” and relevant token profiles, SAML assertions, WS-Trust, XACML, WS-ResourceFramework, WS-Notifications, WS-Coordination (with WS-AtomicTransaction and WS-BusinessActivity), WC-Context coordination framework, WSBPEL, ebXML CPPA, UDDI, and WSDM.

*Impact from TrustCoM on OASIS*

The development of the TrustCoM Framework V4 resulted in substantial profiles combining multiple OASIS specifications. The UDDI BusinessEntity element is extended to indicate VO membership. A profile for WS-Trust and SAML assertions for scoped federations has been defined, addressing cross-issues with XACML. A profile for using XACML in a VO context has been defined. A WSRF ResourceProperties document has been 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; the restriction to a single RP allows easy migration to WS-Transfer. TrustCoM proposed to further look into profiles for the use of WS-Context in WS-Coordination, and for XACML-based coordination policies.

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 standardized PDP interfaces with methods for loading signed policies. SAP contributes to the OASIS WSBPEL TC. In this role it may influence the further development of upcoming standards in this area drawing upon the experiences from projects such as TrustCoM.

## 7.3 WS-* industry specifications

Various WS-* specifications are put forward by industry. IBM and Microsoft, along with a number of other organisations, are creating an interoperable set of web service related specifications. This effort is not intended as an alternative standardisation initiative, and the specifications should eventually move to the appropriate, existing standardisation bodies. The specifications are put forward on customer demand, in order to make Web services more secure, more reliable, and better able to support transactions, and in addition to provide these capabilities while retaining the essential simplicity and interoperability found in Web services today. The majority of the work on technology cooperation is defined in an initial white paper[14]. The specifications are designed in a modular and composable fashion such that developers can utilize just the capabilities they require. This allows developers to create powerful Web services in a simple and flexible manner, while only introducing just the level of complexity dictated by the specific application.

*Impact from WS-* specifications on TrustCoM framework*

Particularly within the baseline infrastructure, TrustCoM has made a good choice in adopting various WS-* standards and specifications. Since the start of the project, WS-* specifications are increasingly supported in web services developer tools, and many of the relevant WS-* specifications have now moved to standards initiatives such as W3C (e.g. WS-Policy), OASIS (e.g. WS-Trust, WS-Coordination), and DMTF (e.g. WS-Management). Remaining relevant specifications include WS-Federation, WS-MetadataExchange, and the Web Single Sign-On Interoperability Profile.

At this point there are still multiple, alternative web services specifications suites (i.e., OASIS WSRF/WSDM vs. WS-Transfer/WS-Management, and OASIS 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

[14] Don Ferguson et al., “Secure, Reliable, Transaction Web Services: Architecture and Composition,” White Paper, October, 2003, URL: http://www-106.ibm.com/developerworks/webservices/library/ws-securtrans/.

the different platforms. [13] WS-ResourceTransfer is the first of such specifications that recently has been published.

*Impact from TrustCoM on WS-* specifications*

The WS-Trust and SAML token profile is disseminated by EMIC to the relevant people in Microsoft. The updated WS-Federation specification now includes the notion of FederationID, which aligns very much with the TrustCoM federation identifier concept.

## 7.4 WS-I

The Web Services Interoperability (WS-I) organization [http://www.ws-i.org/] is an open, industry forum promoting Web services interoperability, working across industry and standards organizations. In addition to the various individual Web Services standards developed in different standardization bodies, WS-I is developing implementation guidelines, tools, and a core collection of profiles that support interoperability for Web services functionality. A profile is a named group of Web services specifications at specific version levels, along with conventions about how they work together.

*Impact from WS-I on TrustCoM framework*

The WS-I has currently specified various Basic and Basic Security Profiles for guaranteeing web services interoperability. The scope of WS-I in principle covers all Web services related aspects in TrustCoM, provided that mature enough standards dealing with these aspects have emerged in the regular standardization bodies.

*Impact from TrustCoM on WS-I*

As WS-I develops interoperability profiles based on standards from other standardization bodies, WS-I is not the right target for introducing new standards, or contributing to existing standards, with specific TrustCoM functionality. WS-I may be a target for feedback and input related to interoperability experiences of existing standards in the scope of further experiments with TrustCoM results.

## 7.5 OGF

The Open Grid Forum (OGF) [http://www.ogf.org/] is a community of users, developers, and vendors leading the global standardization effort for Grid computing. The objectives of the OGF are the creation and documentation of "best practices" - technical specifications, user experiences, and implementation guidelines for Grid technologies and applications. Within its standards function, the OGF has research and working groups in the following areas: Applications, Architecture, Compute, Data, Infrastructure, Liaison, Management, and Security.

*Impact from OGF on TrustCoM framework*

The TrustCoM Framework V4 adopts the GRAAP-WG's WS-Agreement specification. HLRS and SICS have furthermore realised a profile that captures all SLA relevant structures, with a strong influence of both WS-Agreement and WSLA specifications.

*Impact from TrustCoM on OGF*

TrustCoM is particularly impacting the Grid Resource Allocation Agreement Protocol WG (GRAAP) in the Compute area, and the OGSA Authorisation WG in the Security area. Interest from the WS-Agreement working group is being attracted for the TrustCoM SLA profile. David Chadwick (UoK) is co-chairing the OGF OGSA-Authz WG and has written specifications of WS-Trust and XACML/SAML profiles for progression as OGF standards, influenced by TrustCoM work.

## 7.6 DMTF

With more than 3,500 active participants representing 39 countries and nearly 200 organizations, the Distributed Management Task Force, Inc. (DMTF) [http://www.dmtf.org/] is the industry organization leading the development, adoption and promotion of interoperable management initiatives and standards. DMTF management technologies include the Common Diagnostic Model (CDM) initiative, the Systems Management Architecture for Server Hardware (SMASH) initiative, Web-Based Enterprise Management (WBEM) - including protocols such as CIM-XML and Web Services for Management (WS-Management) - which are all based on the Common Information Model (CIM).

*Impact from DMTF on TrustCoM framework*

The TrustCoM Framework V4 is not adopting any DMTF standard, but the WS-Management specification has been identified as relevant for future work in the area of manageable web services.

*Impact from TrustCoM on DMTF*

TrustCoM did not have a specific impact on DMTF within the lifetime of the project.

## 7.7 ETSI

Based in Sophia Antipolis (France), the European Telecommunications Standards Institute (ETSI) [http://www.etsi.org/] is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics.

The ETSI GRID Technical Committee has started (June 2006) to work on defining formal European standards and test specifications for Grid interoperability. The ETSI GRID TC's initial goal is to address issues associated with the convergence between IT (Information Technology) and Telecommunications, with particular reference to the lack of interoperable GRID solutions in situations which involve contributions from both the IT and Telecom industries. This places the focus on scenarios where connectivity goes beyond the local network. The TC GRID activities have an emphasis on interoperable GRID applications and services based on global standards and the validation tools to support these standards.

*Impact from ETSI on TrustCoM framework*

The TrustCoM Framework V4 was not directly impacted by this initiative.

*Impact from TrustCoM on ETSI*

The ETSI GRID initiative may be relevant in the future when further applying and/or extending TrustCoM technologies in Grid scenarios. Mike Fisher from BT is the ETSI GRID Chairman.

## 7.8 Liberty Alliance

The Liberty Alliance Project [http://www.projectliberty.org/] is an alliance of more than 150 companies, non-profit and government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees and consumers, a more convenient and secures way to control identity information in today's digital economy, and is a key component in driving the use of e-commerce, personalized data services, as well as web-based services.

*Impact from Liberty Alliance on TrustCoM framework*

As Liberty focuses on providing a specific solution for federated identity management for mobile and web-based communications and transactions, the TrustCoM Framework V4 – with more generic security objectives – is not using the Liberty specifications. However, federated security is also a key element in the TrustCoM security framework. Interoperation between TrustCoM-enhanced services and Liberty-enabled clients or services may be beneficial.

*Impact from TrustCoM on Liberty Alliance*

TrustCoM did not have a specific impact on Liberty Alliance within the lifetime of the project.

## 7.9 Internet2

Internet2 [http://www.internet2.edu/] is a USA-driven consortium being led by 206 universities working in partnership with industry and government to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet. Internet2 is not a standardisation body as such, but through its middleware and network development programme it has brought about frameworks such as Shibboleth [http://shibboleth.internet2.edu/], which are rapidly being established as de-facto standards technologies for research and educational networks.

*Impact from Internet2 on TrustCoM framework*

As Shibboleth focuses on providing a specific solution for federated identity management in research and educational networks, the TrustCoM Framework V4 – with more generic security objectives – is not using the Shibboleth specifications. However, federated security is also a key element in the TrustCoM security framework. Interoperation between TrustCoM-enhanced services and Shibboleth-enabled clients or services may be beneficial.

*Impact from TrustCoM on Internet2*

TrustCoM did not have a specific impact on Internet2 within the lifetime of the project.

## 7.10 OMG

The Object Management Group (OMG) [http://www.omg.org/] is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications. The OMG membership includes virtually every large company in the computer industry, and hundreds of smaller ones. Many of the companies that shape enterprise and Internet computing today are represented in the Board of Directors. The OMG's flagship specification is the multi-platform Model Driven Architecture (MDA), recently underway but already well known in the industry. It is based on the modeling specifications MOF, UML, XMI, and CWM.

*Impact from OMG on TrustCoM framework*

TrustCoM has done some work in the model driven security area, which is technically relevant to specific OMG efforts.

*Impact from TrustCoM on OMG*

As TrustCoM did not pursue any standards work in the direction of model driven security, there was no specific impact on OMG within the lifetime of the project.

## 7.11 FIPA

The Foundation for Intelligent Physical Agents (FIPA) [http://www.fipa.org/] is an IEEE Computer Society standards organization that promotes agent-based technology and the interoperability of its standards with other technologies.

*Impact of FIPA on TrustCoM framework*

Agent concepts are generally not relevant to the TrustCoM Framework V4. However, for the specific aspect of SLA negotiation, TrustCoM has concluded that it is worthwhile seeking inspiration in the FIPA Iterated Contract Net Interaction Protocol.

*Impact of TrustCoM on FIPA*

TrustCoM did not have a specific impact on FIPA within the lifetime of the project.

## 7.12 IETF

The primary focus of the Internet Engineering Task Force (IETF) [http://www.ietf.org/] is to standardise protocols for the Internet. The IETF has 8 areas, each governed by 2 area directors, which are: Applications, General, Internet, Operations and Management, Real-time Applications and Infrastructure, Routing, Security, and Transport.

*Impact of IETF on TrustCoM framework*

The TrustCoM Framework V4 obviously leverages the base Internet standards underneath the web services layer, including TCP/IP and HTTP. Specifically, the TrustCoM Framework V4 allows the usage of SSL/TLS for transport layer security.

*Impact of TrustCoM on IETF*

David Chadwick (UoK) has been active in the PKIX working group standardizing X.509 PKI and PMI infrastructures, which are of specific relevance in the TrustCoM framework.

## 7.13 ISO

The International Organization for Standardization (ISO) [http://www.iso.org/] is the world's largest developer of standards. Although ISO's principal activity is the development of technical standards, ISO standards also have important economic and social repercussions. Therefore, ISO standards make a positive difference, not just to engineers and manufacturers for whom they solve basic problems in production and distribution, but to society as a whole. ISO's work concerns all the fields of standardization, except electrical and electronic engineering standards, which fall within the scope of the IEC (International Electrotechnical Commission). Most IT standards are established by the joint technical committee between ISO and IEC called ISO/IEC JTC1. JTC1 has a number of sub-committees. Sub-committees relevant to TrustCoM include SC 27 (IT Security techniques) and also SC 25 (Interconnection of information technology equipment) or SC 32 (Data management and interchange). SC 6 (Telecommunications and information exchange between systems) is the group responsible for the X.509 standardisation work. Proposals for standardisation normally go to ISO from national standards bodies. Usually the chairs (or rapporteurs) of the national committees sit on the ISO sub-committee that develops an ISO standard.

*Impact of ISO on TrustCoM framework*

The TrustCoM Framework V4 uses X.509 public key certificates in its trust and security subsystem.

*Impact of TrustCoM on ISO*

From the TrustCoM consortium, David Chadwick (UoK) is the UK (BSI) representative to ITU-T X.509 standards meetings and the editor of the authorization extensions to X.509 (2009) for recognition of authority between VO members.

## 7.14 Ecma International

Ecma International [http://www.ecma-international.org/] is an industry association founded in 1961 and dedicated to the standardisation of Information and Communication Technology (ICT) Systems. Originally, “ECMA” stood for “European Computer Manufacturers’ Association”. Ecma International consists of various Technical Committees and Task Groups in the areas of Information and Communications Technology and Consumer Electronics. Ecma International usually submits approved work to ISO, ISO/IEC JTC1 and/or ETSI for publication.

*Impact of Ecma International on TrustCoM framework*

The Standard ECMA-219 – Authentication and Privilege Attribute Security Application with related Key Distribution Functions – Part 1, 2 and 3, 2nd edition (March 1996) – was conceptually relevant to TrustCoM, but was not leveraged as X.509 Attribute Certificates or SAML assertions replaced this functionality.

*Impact of TrustCoM on Ecma International*

TrustCoM did not have a specific impact on Ecma International within the lifetime of the project.

## 7.15 UN/CEFACT

UN/CEFACT [http://www.unece.org/cefact/] is the United Nations Centre for Trade Facilitation and Electronic Business. It is open to participation from Member States, intergovernmental organizations, and sectoral and industry associations recognized by the Economic and Social Council of the United Nations (ECOSOC). The Centre's objective is to be "inclusive" and it actively encourages organizations to contribute and help develop its recommendations and standards. The mission of UN/CEFACT is to improve the ability of business, trade and administrative organizations, from developed, developing and transitional economies, to exchange products and relevant services effectively - and so contribute to the growth of global commerce. Its main focus is the worldwide facilitation of international transactions, through the simplification and harmonization of procedures and information flows.

*Impact of UN/CEFACT on TrustCoM framework*

UN/CEFACT has been developing a significant number of standards, often in collaboration with other standardization bodies or consortia including ISO, IEC, ITU and OASIS. UN/CEFACT standards of particular interest to TrustCoM include: the Trade Partner Agreement (TPA)[15] proposed by RosettaNet, EDIFICE, ESIA and UN/CEFACT; UN/EDIFACT including "ISO 9735 : Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules"; ebXML that has been developed in conjunction with OASIS; ISO 7372 Trade Data Element Directory by UNECE; and Trade Facilitation Code Lists.

The approach of generic B2B contracts and agreements, such as ebXML, is highly relevant in the context of the TrustCoM framework for trust and contract management.

*Impact of TrustCoM on UN/CEFACT*

TrustCoM did not have a specific impact on UN/CEFACT within the lifetime of the project.

## 7.16 Industry/domain-specific initiatives

TrustCoM is aware of specific standards in various particular industry domains such as electronics, telecommunications, solution provisioning, manufacturing, automotive, aerospace, etc. These industries are moving towards their own standards based on their way of specifying business information, interfaces, exchanges, protocols, reliability and business objects. Examples are RosettaNet (electronics, telecommunications and others) and AIAG (Automotive Technical Standards). These industry specific standards are becoming key to the actual implementations of the B2B transactions and collaborations in specific sectors.

RosettaNet is the farthest in its implementation and well recognized in the industry as the leading standard for supply-chain and demand-chain integration standards in several industrial sectors (e.g.

[15] The TPA Program, a project started in May 2001 and closed at the end of December 2001, was carried out as a Foundational Program of RosettaNet. Contributors to this effort were EDIFICE, the European Semiconductor Industry Association (ESIA), and the Legal Working Group (LWG) of the UN/CEFACT, with each involved in the review of the initial draft TPA.

Electronics, Telecommunications, Manufacturing, Solution providers and others). RosettaNet is a non-profit organization founded in 1998, and includes over 500 of the world's leading businesses in the consortium. RosettaNet is dedicated to open standards for ebusiness processes for global trading networks. RosettaNet focuses on closing the gaps in technology standards for e-Business exchanges, trading partner relationships, value-net efficiencies and transparencies. RosettaNet provides a language and tools (dictionaries and grammer) to specifiy eBusiness process interfaces and interactions. RosettaNet leverages existing standards such as HTML, XML and others to implement Partner Interface Processes (or PIPs) for B2B exchanges of transactional information. RosettaNet is beginning to embrace ebXML and Web Services. Similarly, OASIS and other standards bodies are utilizing some of the established RosettaNet PIPs for enabling better B2B transactions and collaboration. RosettaNet also provides a framework based on dictionaries and naming (DUNS) for identifying companies, their business interfaces and functions.

AIAG is another Industry specific standards body that has a strong eBusiness group that focuses on defining the eBusiness standards for B2B transactions and collaboration within the Automotive Industry. They tend to leverage RosettaNet and ebXML and other relevant standards for their B2B processes, messages and business objects. AIAG was founded in 1982 to address the business integration, product quality, collaboration and supply chain management needs of the ever expanding and complex Automotive Industry. AIAG includes 1600 members from all over the world focussing on standards with a primary goal of reducing costs and complexity, and improving safety in the automotive value chain. One of the most important areas of focus for AIAG is collaborative engineering and product development. This area involves complex supply chain integration of business processes for product design and sharing. The goal of the working group on Collaborative engineering is to improve cost savings, lead-time reduction, and quality improvement in the global automotive supply chain through collaborative means and technologies. Another major area of standardization is the ecommerce and EDI integration. Automotive manufacturers depend on EDI for most of their business interaction with their suppliers and partners. The workgroup focuses on EDI messaging, real-time collaboration, EDI over XML and business modelling.

Another industry specific standard is PapiNet. This is global initiative to bring buyers, sellers, and all relevant parties engaged in buying, selling and transporting paper and paper related products worldwide. PapiNet focuses on XML standards for business to business exchange messages and interfaces for the paper industry.

Similar in spirit to the above three industry specific standards, several industries have taken a similar approach of forming consortia and leveraging the existing Internet, HTML and XML standards.

*Impact of industry/domain-specific initiatives on TrustCoM framework*

Taking into account the various industry/domain-specific initiatives, the TrustCoM framework intends to be generic and flexible enough, such that its components and services can be leveraged in any web services based environments.

*Impact of TrustCoM on industry/domain-specific initiatives*

In the coming years, with better adoption of ebXML and Web Services, the industry specific standards bodies will adopt and customize these standards to their own use, and may hopefully leverage some of the TrustCoM framework concepts.