



A8.D2.3 - Contribution to standardization draft plan

D. Gabrijelčič, T. Klančnik

Document Number	A8.D2.3
Document Title	A8.D2.3 - Contribution to standardization draft plan
Version	V1.1
Status	Final
Work Package	WP8.2
Deliverable Type	Report
Contractual Date of Delivery	30 June 2007
Actual Date of Delivery	01 August 2007
Responsible Unit	SET
Contributors	
Keyword List	contribution to standardization, draft plan, contribution to standardization candidates, related research, related standardization organizations, evaluation
Dissemination level	PU

Executive summary

The “Contribution to standardization draft plan” report proposes a SERENITY project plan for contribution to standardization. To be able to understand standardization issues, the report introduces briefly the standardization and standardization process in the section 2. In the same section common steps needed to finish the process are outlined. The scope of the possible contribution to standardization is sketched in the section 3 through discussion on domains the project is addressing and on potential candidates for contribution to standardization. Two core domains, the ambient intelligence and security and dependability were identified together with secondary domains such as e-health, e-business and e-government. A number of possible contributions are identified and discussed besides commonly recognized, such as new standards or modifications and extensions to existing ones.

The draft plan is proposed in the section 4. Its conceptual model and the time plan are presented together with the initial evaluation criteria for the potential contribution to standardization candidates evaluation. The plan propose a broad evaluation of the research work performed in the project with an aim to define a mature set of candidates on the end of the evaluation period as defined in the time plan. To facilitate quicker inclusion of the candidates in the standardization process this report overviews related research efforts and standardization organizations in the sections 5 and 6. In this way the report contributes to the project related dissemination and liaisons efforts as well. On the end in the section 7 an initial list of the contribution to standardization candidates is proposed. The list will enable a start of the iterative evaluation process that will proceed in line with other research and dissemination activities in the project.

Contents

1	Introduction	4
2	Standardization and standardization process	4
3	Contributions to standardization	5
4	Contribution to standardization draft plan	7
5	Related research efforts	9
6	Related standardization organizations	11
7	Contribution to standardization candidates	13
8	Conclusions	15
	References	16

1 Introduction

The primary aims of this report are to outline the SERENITY project contribution to standardization draft plan and to identify initial candidates for contribution to standardization resulting from the project research work. The secondary aims are to initiate focused discussion on potentials for standardization in the project, to identify appropriate target standardization organizations for standardization and to overview standardization related possibilities for collaboration with ongoing EU research efforts.

For this purpose standardization related concepts are briefly introduced in the section 2 and possible contributions to standardization and relevant technology domains are discussed in the section 3. The contribution to standardization draft plan is sketched together with the time plan in the section 4. An overview of related research efforts is reported in the section 5 and possible target standardization organizations are introduced in the section 6. The report concludes with initial set of contribution to standardization candidates in the section 7.

2 Standardization and standardization process

Standardization can be understood as the process aiming to define common and mutually agreed (technical) solutions between relevant stakeholders, for the benefit of all. Standardization processes are carried out in many different types of organizations on a national, regional or global level. The final result of the standardization processes are standards, which can be formal, informal or private specifications. The standards can be normative, describing with which something should comply and informative, providing helpful information and guidance. The formal or often referred as de jure standards are followed because of (more or less) legally binding contracts and documents other can be de facto, which means they are followed for convenience. Formal and informal standards are usually open, developed in an open process and are publicly available under so called fair, reasonable and non-discriminatory (FRaND) terms. Private specifications are usually proprietary but can be submitted to formal standardization organizations as well.

Important and well known standardization organizations on the national level, which have international impact as well, are DIN[26], ANSI[9] or BSI[16]. On the European, regional level there are three formal standardization organizations, CEN[19], CENELEC[20] and ETSI[30]. Their global counterparts are ISO[51], IEC[42] and ITU[52]. These organizations produce formal standards and have cooperation arrangements in place so that standards produced by one organization are often accepted by the other. Many aspects of standardization are covered by other forums, which are usually technology specific. Such organizations produce informal standards, like IETF[45], W3C[84] and IEEE[43].

Standardization processes, though carried out by different organizations, are more or less identical[22]. In general, for a new standard or standardization activity, there is a need for (1) consensus on market needs and (2) constituency between sufficient number of members of a standardization organization. Subsequently, the (3) consensus on requirements is needed, which is followed by (4) technical work. Once the specification or activity result drafts is finalized the (5) formal approval process can be conducted. Arrangements are often made or required for (6) testing for interoperability between different implementations of the same specification. Specifications are often periodically reviewed for (7) maintenance to ensure that it will remain in sync with market requirements. Time for standardization process varies from organization to organization. It is often considered that time needed for standardization is shorter for informal than formal technical specifications. Nevertheless, the time

needed to finish the process is estimated to be between one to three years, though it can be even longer. For example, European standards have a three year maximum target preparation time, but not counting first two steps and in IETF, which has supposedly fast standardization policy “rough consensus and running code”, the elapsed process time can be over eight years.¹

To get involved into the standardization process either the project partners or the project has to be a member of the target standardization organizations. Guidance for interaction with such organizations, together with reasons why certain stakeholders (industrial, academia, institutions, project consortia, etc.) should participate in standardization, are given in EU founded COPRAS project[21] report “Standardization guidelines for IST research projects interfacing with ICT standardization organizations”[22]. The comprehensive guide was prepared by a number of standardization organizations, namely CEN, CENELEC, ETSI, W3C and The Open Group[61] in cooperation with ICT Standards Board[40].

3 Contributions to standardization

The aim of this section is to discuss the scope and type of possible contributions to standardization. For this purpose COPRAS project characteristics which lead to the standardization will be reviewed and standardization domains in which SERENITY project could contribute will be discussed.

The COPRAS report describes the following possible reasons or characteristics that can lead to standardization, four out of five can be related to SERENITY project:

1. adding domain specific elements to existing standards, a consensus is needed within the specific domain concerning the new elements
2. using an existing standard for an application originally not envisioned, which can require modifications or extension to the existing standard
3. integration of different standards into a platform, framework or architecture, which is more complex and requires modifications to one or more of the standards to avoid clumsy workarounds
4. research results are intended as basis for new generation products or services.

SERENITY project has multidisciplinary scope and its possible contributions to standardization are related to multiple domains. The domains are not clearly separated and are often intersected. Two core domains the project is addressing are ambient intelligence (AmI) and security and dependability (S&D). Technical solutions are rounded by a general system framework supporting design/deployment and runtime operations. A number of new elements, solutions, algorithms, information models, processing procedures, etc., are interweaved with existing technological solutions (and standards) for dynamic security and dependability provisioning. Each technological solution is often represented by its own domain for standardization. SERENITY scenarios[17] that the general framework will support are related to e-health, e-government, e-business, mobile communications and air traffic control. Each domain, either already well established or emerging, can be considered again as a separate regarding the standardization. The domains tend to reuse existing standards or are in struggle to standardize the gaps resulting from arrival of new technologies and paradigms. Nice example of such work is attempt for consolidation of the standardization efforts in the e-health domain done by ETSI[64].

¹For example, the standardization process for Intrusion Detection Message Exchange Format (IDMEF), with strong consensus on market needs but long technical work time, from 1999 to 2007.

Presented COPRAS characteristics can be divided in two groups. The first, related to the characteristics from 1 to 3, covers the work in domains where the standards are already well defined. The latter, related to the characteristics 4, covers domains and work in the project that is well above the technology layer covered with existing standards.

The first group is mainly related to the general system framework, technological solutions and domains defined with the proposed SERENITY scenarios. The work in these domains can result, because of SERENITY specific requirements and solutions, in modifications, additions or extensions to existing standards. By the project proposed usage of the technological solutions through S&D patterns and surrounding solutions will, very likely, result in best practice solutions for provisioning target S&D properties of the system. Best practice documents and reports of the usage of the technological solutions could be a welcome contribution to standardization. There is number of standardization organizations that prepare, collect and publish such contributions, a catalog of such organizations is available in [46], a byproduct of the IETF OPSEC charter. Best practices are used by the organizations to shape the future road maps for standards, see for example recent documents of the ITU-T study group 17[50]. The scenarios as developed and modeled in SERENITY are often used by the standardization organizations as well. Some of them are using them, in more system design oriented approach, as a basis for new standards, like Digital Living Network ALiance[25].

The second group is related to core research activities of the project. Standardization in the emerging domain of ambient intelligence still covers only lower technology layers. The domain standardization takes place, or is planned, in various standardization organizations. There is no technical or industrial group that has taken a leading role in the domain standardization, as for example, the Global Grid Forum[35] is performing for Grid domain. The standardization of pre-competitive research on higher technological layers, as performed in SERENITY project, is therefore quite difficult.

The security and dependability domain has been a subject of standardization for quite a long time. Various standardization organizations, from global to technology specific, have already standardized numerous S&D aspects of the ICT, like cryptographic algorithms, security protocols, authentication and authorizations architectures, etc. An innovative approach of SERENITY project enabling automated, dynamic, validated, combined, etc. runtime usage of S&D patterns concept will use many of existing S&D standards and other design and architecture related standardized solutions. But the essence of the approach is well above standardized technology layers. The patterns has been a research topic for almost three decades. There exists a number of non formal pattern repositories[39] [34][85] which collect ICT related design, architecture and solutions patterns. But pattern languages[66], used to describe them, are only simple textual descriptions. They are not suitable for reuse in the SERENITY approach. Among standardization organizations only The Open Group[61] has published two S&D pattern related standards. A technical guide[82] and an introduction to security patterns[81] cover availability and protection patterns. The work is well in scope of SERENITY project but again, the language used, does not allow much of elements of the pattern descriptions to be reused.

The research work in the described domains has potential that could result even in new standards in the field. Before new standards in these domains could be expected a lot of research and preparatory activities are needed. The activities, related to early phases of the standardization process as presented in section 2, can be various, such as preparing coherent requirements, comprehensive use cases, identifying potential market needs, constituency building with potential stakeholders, providing technical reports to target standardization organizations and many others.

4 Contribution to standardization draft plan

Work in SERENITY has potential to contribute to many different standardization domains. Possible contributions to standardizations are not limited only to new standards and modification, additions or extensions to existing ones. Following from the discussion in previous section, there are many other types of contributions to standardization as well, like best practice reports, use cases, scenarios, identification of gaps or welcome changes in current standards, feedbacks or views on particular standardization organization reports, indication of market needs, technical reports, scientific publishing, requirements and their analyzes, etc. Any possible type of contribution to standardization in this report will be therefor named a **contribution to standardization candidate** or simple a **candidate** in the rest of the report.

The draft plan overview is presented in the figure 1. The figure presents rough relations between different standardization concepts. The contribution to standardization candidates are result of research work in SERENITY project. The research can result in number of contribution to standardization candidates in different domains. The candidates needs to be evaluated to be able to found most reasonable selection of them. The evaluation and examination of the candidates can result in contributions to standardization when the candidates become involved in the standardization process of target standardization organizations, as discussed in section 2. The research in the project is influenced by liaisons with related research efforts as well with liaisons with standardization organizations. From the standardization point of view the liaisons can have important impact on the evaluation of the candidates. The lines connecting the liaisons and the contribution to standardization with the related research and standardization organizations are deliberately drawn as dashed. In contrast to the full lines, which are clearly only project related, these lines mark relations outside the project and relations, that do not depend solely on the project, but require involvement of the individual project partners as well.

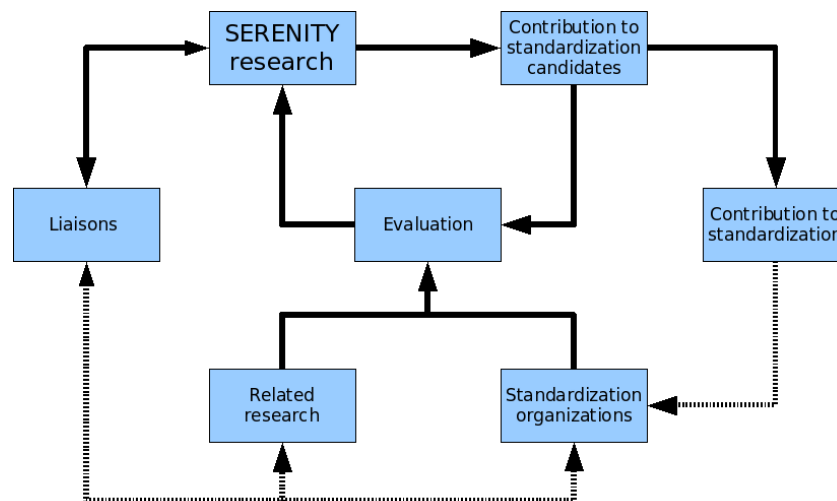


Figure 1: Contribution to standardization draft plan overview

There can be a number of possible candidates for standardization. The draft plan as presented is not a single cycle of defining the candidates and contributing to standardization organizations. The plan is a continuous process of defining or redefining the candidates, their evaluation, monitoring of related research and progress in relevant standardization organizations, resulting in direct or indirect

(through publishing, etc.) contribution to standardization. The process needs to be continuous because of (1) the nature of research as performed in the project, with constantly evolving designs and prototypes reported in project deliverables and other results, (2) progress of work and paradigm shifts in standardization organizations, (3) new research initiatives, specially newly founded projects in EU FP7 program, (4) changes in potential stakeholders interest in standardization, etc.

The aim of the contribution to standardization plan is twofold: first, to build a broad view on a standardization landscape in core and other domains that SERENITY project is tackling and second, to establish between the project partners, they are potential stakeholders, a consensus on contribution to standardization candidates. The consensus will be build through the evaluation process of the candidates. There are number of criteria the candidates can be evaluated against, the following list is build from the project point of view and it is likely that it will be in next period evolved further:

- the candidate appropriateness from technical and conceptual point of view,
- the candidate readiness from technical point of view,
- importance of the candidate for the project goals, the core domains are likely to have higher priority
- importance of the candidate for the stakeholders, eg. project partners that will be involved in the candidate standardization
- importance of the candidate for the standardization process, some of the candidates can be dependent on each other and their submission to the standardization process is meaningful only if they are submitted jointly
- matching of the candidate to the standardization organization, some candidates can match well to the target organization goals and scope, others can be matched only indirectly
- stakeholders relation with the target standardization organization, the submission and the success of the standardization process is highly dependent on involvement of the project partners in the standardization organization
- time to complete the standardization activity, though the standardization processes are usually longer than the project lifetime some candidates can have impact only on the part of the process
- commitment of the stakeholders to continue standardization activity after the project life time, for example, some of the stakeholders can commit to continue to support the process after the project end,
- matching of the candidate for standardization with other research efforts, most promising are related EU founded projects and possible individual stakeholders as partners in these projects
- matching of methods, processes and principles of the standardization bodies to the project objectives,
- IPR related issues, these issues should not be neglected before the submission of the candidate to the standardization activity.

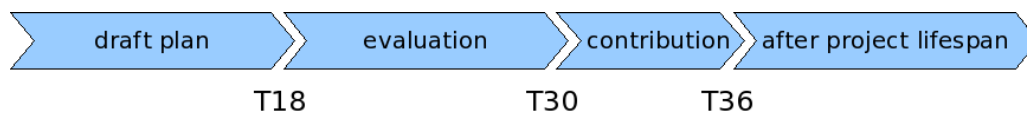


Figure 2: Contribution to standardization time line

The contribution to standardization draft plan, as presented, has to match the reality of resources available in SERENITY project, both in terms of men months as well the lifespan of the project. The time line for the contribution to standardization activities is presented in the figure 2. The time line is divided in four periods, each of them is represented with a most prominent task for the period.

The first period corresponds to the draft plan as is outlined in this document. It is followed by a period when the contribution to standardization candidates are evaluated. As is the case already in the draft period, the evaluation period will involve even more contacts with the target standardization organizations and related research efforts. The results of this period will be evaluated and focused candidates. The results of the evaluation will be reported in “Contribution to standardization plan” at month 30 (T30), as is planned by SERENITY technical annex. Standardization wise the third period should be prevailed by the contribution to standardization. The amount of contribution highly depends on interest in standardization among individual stakeholders in the project. As proposed in this section, this will be one of criteria for the candidates evaluation, so more efforts can be devoted to right candidates. But it has to be noted, that the research in the project is pre-competitive and the expected results of the project are prototypes, not commercial products. It is likely, that some of the contributions can be submitted by individual stakeholders in the project only after the project lifespan, as noted in the time line by the fourth period. A broad view on standardization landscape in particular domain for certain candidate, as proposed in this draft plan, can help such post lifespan contribution to standardization.

To initiate the work on the contribution to standardization candidates, the related research efforts and target standardization organizations will be reviewed in next two sections. The initial set of the candidates will be proposed in the section 7.

5 Related research efforts

Related research efforts are important because of the possible standardization synergy between them and SERENITY project. The main focus in this report are EU founded research projects that target the same or related technology domain. The reviewed projects are divided into three domains, ambient intelligence, security and dependability and general area of services, components and systems. The list of the project is not final and it will be reviewed during the evaluation period, of special interest are projects that will be founded in 7th framework programme. The review is standardization oriented and points out technological relations when applicable.

Related research efforts from the standardization point of view in the domain of:

— ambient intelligence and pervasive systems

- Ambient Networks phase 2 project[6], addressing mobile and wireless networks beyond 3G. Standardization efforts are related to the physical, link and network layer aiming at integration of fixed and mobile beyond the 3GPP[5] work. From the SERENITY project point of view is interesting an aim to standardize the interface between the applications

and network layer called Ambient Service Interface[7]. The target standard organization is OMA[4], they plan to liaison for standardization with project SPICE[78]

- e-SENSE project[28], Ambient Intelligence for Beyond 3G Mobile Communication Systems through Wireless Sensor Networks. Standardization outlooks are focused at physical, link and network (global) layer and at service platform interfaces. In service context they foresee collaboration with OMA, 3GPP [1] (IMS systems) and ETSI OSA[31]
- ASK-IT project[11] standardization plan[12] is oriented towards impaired persons, could be of interest to SERENITY in connection with e-Health scenario and general security usability
- projects with no specific, published or disclosed standardization plan: AMIGO[8], NET-CARITY[54], PALCOM[65], BIONET[13], CASCADAS[18]

— security and dependability:

- SecureIST project has published some initial standardization issues in the field of security and dependability in its recommendation[74] and final strategy[73]. In the first they expose the issue of standardization on higher, abstract layer, in the context of interoperability between different security models and a need to involve end users into the standardization process. In the latter, besides mentioned issues, they expose a need to shorten the time of standardization development process and a need for certification and interoperability testing. Project efforts are organized in “security initiatives”, standardization is partly covered in the initiative “Methods Standards and Certification Initiative” (MSCI). It is not clear how the framework and the initiatives will function after the project lifespan, the project has ended in April 2007
- ESFORS project[29] addresses directions in security research for web services, software and systems. No particular focus is set on standardization in the area of security and dependability, though the project emphasis regulation, government policies and best practices that should be incorporated in the service platforms and architectures
- PRIME project[68] has rational approach to standardization through relevant stakeholders and a broad view on possible standardization candidates. Some of them, related to anonymous credentials and authorization policies can be of interest to SERENITY project as well
- BIOSECURE project[14] as NoE project has no specific standardization plan but has published on line handbook on biometric standards[15] that can be of interest for SERENITY project
- OPEN_TC project[62] is developing trusted computing environment. Its standardization is oriented towards Trusted Computing Group[83][63] as one of the crucial elements of S&D
- CRUTIAL project[23] is oriented towards resilience in CII sees possible channels for dissemination, among the others, through working groups that could of interest to SERENITY project as well, like IFIP[47] and IEEE CS dependable computing and fault tolerance [77] working group
- SWAMI project[79] has researched the social, economic, legal, technological and ethical issues related to identity, privacy and security in the forecasted, but not yet deployed ambient intelligence (AmI) environment. The projects overviews a range of possible safeguards

in AmI environment and has given a number of recommendations. Recommendations are related to legal and regulatory framework but very limited from the standardization point of view

- projects with no specific, published or disclosed standardization plan: PEPERS[67], MOBIUS[3], S3MS[70], ReSIST[69], AntiPhish[10], IRRIS[2] and DESEREC[24]. INSPIRED[48] is not planning broad standardization efforts but it reports on influenced standardization bodies[49]. DISCREET has no specific standardization plan but provides rough report on depending regulation and standards[27]

— service/component/system:

- HIDENETS[37] will report its standardization plan only at the end of the project. The project is working partly on similar research issues[38] as SERENITY project. It is possible that they are standardization wise looking to similar direction as SERENITY, reusing various existing standards specifications, such as SysML[80][57], OMG[59] reusable assets specification[36], OMG Testing profile[58], OMG Profile for QoS and Fault tolerance[60], Service Availability Forum[76] API specification, etc.
- SeCSE project[71] researches service centric system engineering. Its standardization[72] is planned in few areas. Some of them, like monitoring, could be aligned with SERENITY efforts
- project with no specific, published or disclosed standardization plan in this domain is SENSORIA[75].

6 Related standardization organizations

There is number of standardization organizations that are of interest to SERENITY project. The SERENITY related domains, as discussed in the section 3, are subject to standardization in many of them. In this section they will be reviewed as they were introduced in the section 2, from global, to regional and technology based standardization organizations.

Standardization organizations and their activities that are of interest to SERENITY project:

- ITU-T[52]; The ITU Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU). The ITU-T work is performed in number of study groups (SG). Of particular interest to the project is study group 17 with initial time span from 2005 to 2008. The group focus is telecommunications security and has recently published the document “ICT Security Standards Roadmap”[50] with an aim to assist in the development of security standards by bringing together information about existing standards and current standards work in key standards development organizations. Of particular interest can be section five of the roadmap related to the security-related best practices that could be contributed by community
- ICTSB[40]; The ICT Standards Board is an initiative from the three recognized European standards organizations CEN[19], CENELEC[20] and ETSI[30] with the participation of specification providers² as partners to co-ordinate specification activities in the field of Information and Communications Technologies (ICT). The ICTSB has three main objectives: analyze and

²Called standardization organizations in this report.

coordinate requirements, translate requirements into standardization programmes or projects and allocate the work to most appropriate specifying body . Some of the specifying bodies that are partners in ICTSB, are of interest to SERENITY project as well, and will be reviewed in this section, like W3C, OASIS, OMA and The Open Group. The ICTSB work is performed in working groups. The most related to the core SERENITY domains is “Network & Information Security Steering Group” which has recently published a report on “Network and Information Security Standards Report”[41]. The group is cooperating with the ITU-T SG 17 on the security standards roadmap.

- ETSI[30]; The European Telecommunications Standards Institute (ETSI) is an independent, non-profit, standardization organization of the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. Of interest to the SERENITY project can be work of “Specialist Task Force 292”[32] on TISpan security, covering NGN (New Generation Networks) security aspects. ETSI has recently published an overview of applicability of existing ETSI and ETSI/3GPP specifications to vertical e-Health domain, covering security aspects of the domain as well
- IETF[45]; The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF scope of work is related to some domains addressed in the SERENITY project, some working groups of interest are organized in IETF Security Area, like LTANS WG (Long-term Archive and Notary Services). There are other interesting S&D related working groups as well, like NEA (Network Endpoint Assessment) or OPSEC (Operational Security Capabilities for IP Network Infrastructure)
- W3C[84]; The World Wide Web Consortium (W3C) is the main international standards organization for the World Wide Web. Domains that W3C is standardizing in are interweaved with the work in the SERENITY project, like Web Services, Web Security, Privacy and P3P, Quality Assurance, Ubiquitous Web Applications, etc.
- OASIS[56]; Organization for the Advancement of Structured Information Standards is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS covers domains like security, targeting security for business and web service applications with standards like SAML, WS-SX, etc., and web services, providing infrastructure and implementation standards for interoperable business process. Some of the SERENITY domains are using these standards as a basis for implementation
- OMG[59]; The Object Management Group develops enterprise integration standards for a wide range of technologies. OMG’s modeling standards enable powerful visual design, execution and maintenance of software and other processes. OMG covers multiple domains that are of interest to SERENITY and covers both design and runtime issues of software systems. On the other hand the group covers standardization wise the vertical domains as well, like healthcare, government and business
- The Open Group[61]; The Open Group is a vendor- and technology-neutral consortium, whose vision is to enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group standardization work is organized in forums. The Security Forum has, as has been already pointed out in the section 3, the

only standardization organization that has published security and dependability patterns related standardization documents[82][81].

Some smaller technical groups, forums or councils could be of interest to SERENITY project as well. All of them are active but for some is difficult to estimate an activity level or potential impact on community. Some of them have been mentioned in the section 5 already. Of interest can be the Trusted computing group[83], developing and promoting open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms, IEEE groups, like Computer Society “Technical Committee on Dependable Computing and Fault Tolerance”[77], “Information System Security Assurance Architecture working group” that is actively working on architecture standard[44], FIPA group “The Foundation for Intelligent Physical Agents”[33] IFIP[47] (International Federation for Information Processing) group WG 10.4 on “Dependable Computing and Fault Tolerance”, NRIC (The Network Reliability and Interoperability Council)[55] groups, Service availability forum[76] and many others.

7 Contribution to standardization candidates

In this section an initial list of the contribution to standardization candidates will be identified. The identification, as proposed in the section 4, is iterative process used to define a broad, but focused list of candidates followed by the evaluation, aiming at estimation of the candidate appropriateness for standardization. For example, the SERENITY framework, as defined in the specification of the SERENITY architecture[53], could be considered as a contribution to standardization candidate. Due to the framework broad scope such candidate is highly unrealistic. It makes sense to split the framework (as in the system design) in smaller and more sound parts in the next iteration. These become new candidates, which will be further evaluated according to the criteria as proposed in the section 4. An initial high level view and split of the architecture is presented in the figure 3. The main focus of this iteration are runtime framework external interfaces and high level concepts that facilitate the design and run time usage of S&D patterns. The external interfaces are application, monitoring and negotiation interfaces, as defined in [53]. The high level pattern related concepts are S&D Solutions, S&D Properties and S&D Library.

The initial candidates will be briefly described in this report and further evaluated towards more mature candidates in the next iterations. Other possible contributions, related for example to non core domains as discussed in the section 3, can be added to the list of candidates in the next period. The initial contribution to standardization candidates are:

- SERENITY Run-Time Framework Negotiation Interface; The Serenity Run-Time Framework (SRF) controls the security and dependability (S&D) properties of a number of AmI devices within a domain. Two or more SRFs may require inter-SRF communication to coordinate the provision of S&D solutions across different domains. The inter-SRF communication is done through the SRF negotiation interface. This interface will be specified by SERENITY. An SRF implementation will be required to implement the negotiation interface. In order to help promote adoption of the SERENITY concept, this interface could be made into a standard
- SERENITY Run-Time Framework interface with Serenity-aware applications; SERENITY-aware applications (SAA) must implement an interface for communication with the Serenity Run-Time Framework. Through this interface, the SAA can request from the SRF an S&D solution, and receive as a result an S&D solution in the form of an S&D pattern implementation,

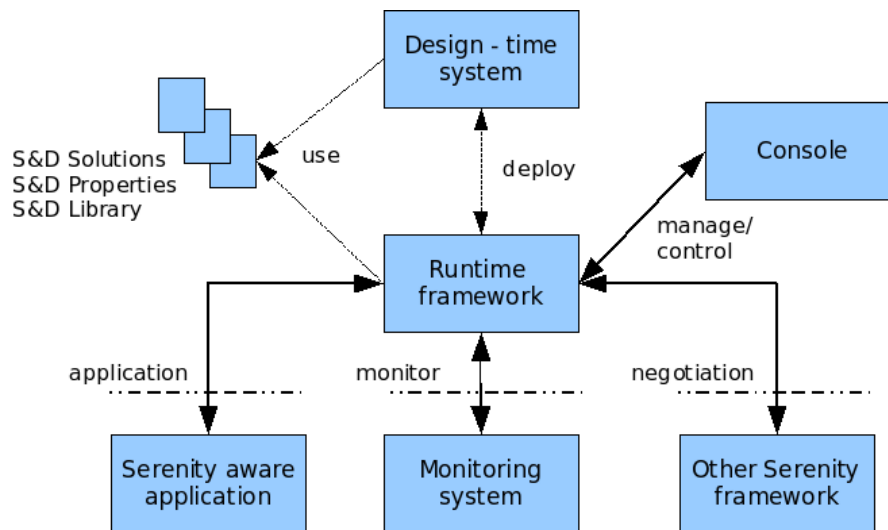


Figure 3: High level view of the SERENITY framework

for use by the SAA to make use of the S&D solution. A standard describing this interface will be necessary to ensure proper development of SERENITY aware applications to conform to the SERENITY SRF operation

- **SERENITY Monitoring Interface**; The monitoring interface of the SRF is a candidate for standardization. This interface must be followed by any monitoring service modules that aim to support the SRF with their monitoring capabilities. The protocol for communication between a monitoring service and an SRF include both a set of message exchanges and a definition of the message contents
- **S&D Solutions**; S&D solutions define mechanisms for realizing the S&D requirements and provide one or more S&D properties. The candidate is complex and it will be possibly split in further iterations in number of new candidates. Possible candidates are SERENITY artifacts like S&D Patterns, S&D Classes, S&D Implementations and SERENITY monitoring subsystem. The candidates are likely to be resolved to their information models, languages, procedures of their usage and collections for particular type of solutions related to the application domain or ability to fulfill certain S&D property
- **S&D Properties**; The S&D Properties fulfill the specific S&D requirements of the system at design and run time. The SERENITY project work is focused on formal framework for expressing S&D Properties and related mechanisms for their publication, retrieval and reasoning. The properties language and information model, abstracting different domains addressed by the project, verification process, using the specified language and project verification tools, and design time processing model providing S&D solutions to the system developer are candidates for contribution to standardization
- **S&D Library**; The S&D Library is a collection of S&D Patterns, like organizational, workflow and network patterns. The patterns describe, at different levels of abstraction, S&D solutions that provide different S&D properties. The candidate was selected at this level as possible public interface that enables access to the collection of patterns.

8 Conclusions

The approach proposed in this report as draft contribution to standardization plan intends to initiate the SERENITY project work on standardization issues. It defines the starting points of the evaluation of contribution to standardization candidates which will be primary task of the next, evaluation period. The initial list of the candidates is focused on one hand on external interfaces of the SERENITY framework and on the other on broad, high level candidates supporting S&D patterns. Both sets will be further extended during the evaluation. The final aim of the evaluation is to have a clear view on possible contributions to standardization as a result of the approach proposed by the project. New candidates can emerge as a result of applying the project approach to other, non core project domains. To facilitate the standardization process, the report provides the overview of related standardization organizations and research efforts. In the following period the overview will help to find matching standardization organizations and candidates related standards as well. The related research efforts overview is contributing to already existing project efforts to liaison with ongoing EU founded projects and existing research groups.

References

- [1] 3GPP (3rd Generation Partnership Project). Home page. <http://www.3gpp.org/>.
- [2] IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems) 2006 - 2009. Home page. <http://www.irriis.eu/>.
- [3] Mobius project (mobility, ubiquity, security) 2005 - 2009. Home page. <http://mobius.inria.fr/>.
- [4] Open Mobile Alliance (OMA). <http://www.openmobilealliance.org/>.
- [5] 3rd Generation Partnership Project (3GPP). TSG Service and System Aspects WG3 (Security). Home Page. <http://www.3gpp.org/tb/SA/SA3/SA3.htm>.
- [6] Ambient Networks project 2006 - 2008. Home page. <http://www.ambient-networks.org/>.
- [7] Ambient Networks project, 2006. D1-A1 Ambient Networks Project Description and Dissemination Plan. Public deliverable. http://www.ambient-networks.org/Files/deliverables/D1_A1_AN2_\%20Project\%20Description.pdf.
- [8] AMIGO (Ambient Intelligence for the networked home environment) 2004 - 2008. Home page. <http://www.hitech-projects.com/euprojects/amigo/>.
- [9] American National Standards Institute (ANSI). Home page. <http://www.ansi.org>.
- [10] AntiPhish (Anticipatory Learning for Reliable Phishing Prevention) 2006 - 2008. Home page. <http://www.antiphishresearch.org/>.
- [11] ASK-IT (Ambient Intelligence System of Agents for Knowledge-based and Integrated Services for Mobility Impaired users) 2004 - 2008. Home page. <http://www.ask-it.org/>.
- [12] ASK-IT project, 2005. D5.3.1 - dissemination plan. Deliverable.
- [13] BIONET (BIOlogically inspired NETwork and Services) 2006 - 2010. Home page. <http://www.bionets.org/>.
- [14] BIOSECURE (Biometrics for Secure Authentication) 2004 - 2007. Home page. <http://www.biosecure.info>.
- [15] BIOSECURE project, 2007. BIOSECURE Handbook of Biometrics Standards. Web page. <http://www.cilab.upf.edu/biosecure1/wiki/index.php/Standards>.
- [16] British Standards Institution (BSI). Home page. <http://www.bsi-global.com>.
- [17] S. Campadello, L. Compagna, D. Gidoïn, S. Holtmanns, V. Meduri, and J.C. Pazzaglia, 2006. A7.D1.1 - Scenario selection and definition. Technical report, SERENITY.
- [18] CASCADAS (Componentware for Autonomic, Situation-aware Communications and Dynamically Adaptable Services) 2006-2009. Home page. <http://www.cascadas-project.org/>.
- [19] European Committee for Standardization (CEN). Home page. <http://www.cen.eu>.

- [20] European Committee for Electrotechnical Standardization (CENELEC). Home page. <http://www.cenelec.org>.
- [21] COPRAS (COoperation Platform for Research And Standards) 2004 - 2007. Home page. <http://www.w3.org/2004/copras/>.
- [22] COPRAS, 2007. Standardization Guidelines. Technical report, Cooperation Platform for Research and Standards project.
- [23] CRUTIAL (CRitical UTility InfrastructurAL Resilience) 2006 - 2009. Home page. <http://crutial.cesiricerca.it/>.
- [24] DESEREC (DEpendability and Security by Enhanced REConfigurability) 2006 - 2009. Web page. <http://www.deserec.org>.
- [25] Digital Living Network Alliance (DLNA), 2004. Use Case Scenarios. White paper. <http://www.dlna.org/en/industry/home/>.
- [26] Deutsches Institut für Normung (DIN). Home page. <http://www.din.de>.
- [27] DISCREET (Discrete Service Provisioning in Smart Environments) 2005 - 2008, 2006. D2401 - Preliminary Regulatory and performance assessment. Deliverable. <http://www.ist-discreet.org/>.
- [28] e-SENSE project (Ambient Intelligence for Beyond 3G Mobile Communication Systems through Wireless Sensor Networks) 2006 - 2008. Home page. <http://www.ist-esense.org/>.
- [29] ESFORS (European Security Forum for Web Services, Software and Systems) 2005 - 2007. Home page. <http://www.esfors.org/>.
- [30] European Telecommunications Standards Institute (ETSI). Home page. <http://www.etsi.org>.
- [31] ETSI. Osa api joint working group. Web page. <http://portal.etsi.org/docbox/TISPAN/Open/OSA/Index.html>.
- [32] ETSI Specialist Task Force 292. TISPAN security: Standards development in support of the eEurope secure and trusted network environment. Home page. http://portal.etsi.org/stfs/STF_HomePages/STF292/STF292.asp.
- [33] FIPA, 2005. The Foundation for Intelligent Physical Agents. IEEE Computer Society standards organization. <http://www.fipa.org/>.
- [34] Security Patterns Forum. Web page. <http://www.securitypatterns.org/>.
- [35] Global Grid Forum - Grid Resource Allocation Agreement Protocol (GRAAP) WG, 2007. Web Services Agreement Specification (WS - Agreement). Recommendation.
- [36] Object Management Group, 2005. Reusable Assets Specification. OMG Specification. <http://www.omg.org/technology/documents/formal/ras.htm>.

- [37] HIDENETS (Highly DEpendable ip-based NETworks and Services). Home page. <http://www.hidenets.aau.dk/>.
- [38] HIDENETS, 2007. UML profile and design pattern library (preliminary version). Project deliverable.
- [39] Hillside.net. Pattern catalog. Web page. <http://hillside.net/patterns/onlinepatterncatalog.htm>.
- [40] ICT Standards Board. Home page. <http://www.ictsb.org/>.
- [41] ICTSB Network and Information Security Steering Group, 2007. Network and information security standards report. Report. http://www.ictsb.org/NISSG_home.htm.
- [42] International Electrotechnical Commission (IEC). Home page. <http://www.iec.ch>.
- [43] Institute of Electrical and Electronics Engineers, Inc. (IEEE). Home page. <http://www.ieee.org>.
- [44] IEEE Computer Society ISSAA WG, 2007. IEEE P 1700: INFORMATION SYSTEM SECURITY ASSURANCE ARCHITECTURE (ISSAA) STANDARD v21.0. Standard.
- [45] Internet Engineering Task Force (IETF). Home page. <http://www.ietf.org>.
- [46] IETF Network working group: Operational Security Capabilities for IP Network Infrastructure (opsec), 2007. Security Best Practices Efforts and Documents. Internet-Draft. <http://www.ietf.org/html.charters/opsec-charter.html>.
- [47] IFIP (International Federation for Information Processing). Wg 10.4 on dependable computing and fault tolerance. Web page.
- [48] INSPIRED (INtegrated Secure Platform for Interactive tRusted pErsonal Devices) 2006 - 2009. Home page. <http://www.inspiredproject.com/>.
- [49] INSPIRED project, 2007. D13.1 - Final dissemination plan. Deliverable report.
- [50] International Telecommunications Union (ITU) Study Group 17, 2007. Ict security standards roadmap. Web Page. <http://www.itu.int/ITU-T/studygroups/com17/ict/>.
- [51] International Organization for Standardization (ISO). Home page. <http://www.iso.org>.
- [52] International Telecommunication Union (ITU). Home page. <http://www.itu.int>.
- [53] Antonio Maña, Ana Piñuela, Daniel Serrano, Pedro Soria, and Athanasios-Dimitrios Sotiriou, 2007. A6.D3.1 - Specification of SERENITY Architecture. Technical report, SERENITY.
- [54] NETCARITY (A NETworked multi-sensor system for elderly people: health CARE, safety and securITY in home environment) 2007 - 2011. <http://www.netcarity.org/>.
- [55] Network Reliability and Interoperability Council, 2007. NIRC. <http://www.nric.org/index.html>.
- [56] OASIS. Organization for the Advancement of Structured Information Standards. Home page. <http://www.oasis-open.org/home/index.php>.

- [57] Object Management Group, 2006. OMG SysML specification. Final adopted specification. <http://www.omgsysml.org/>.
- [58] Object Management Group, 2007. UML Testing Profile, v 1.0. OMG specification. http://www.omg.org/technology/documents/formal/test_profile.htm.
- [59] OMG. Unified Modeling Language (UML). <http://www.uml.org/>.
- [60] OMG, 2006. UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics and Mechanisms. Formal standard.
- [61] The Open Group. Home page. <http://www.opengroup.org>.
- [62] OPEN_TC (Open Trusted Computing) 2005 - 2009. Home page. <http://www.opentc.net>.
- [63] OPEN_TC project, 2006. D10.1 intermediate report about all external cooperation and activities. Deliverable.
- [64] ETSI Advisory Committee Operational Co ordination Group (OCG), 2007. SR 002 564 - V2.0.0 - Applicability of existing ETSI and ETSI/2GPP deliverables to eHealth.
- [65] PALCOM project (making computing palpable) 2004 - 2008. Home page. <http://www.ist-palcom.org/>.
- [66] Pattern language. Wikipedia. http://en.wikipedia.org/wiki/Pattern_language.
- [67] PEPERS (Mobile Peer-to-Peer Security Infrastructure) 2006 - 2008. Home page. <http://www.pepers.org/>.
- [68] PRIME (Privacy and Identity Management for Europe) 2004 -2008. Home page. <https://www.prime-project.eu/>.
- [69] ReSIST (Resilience for survivability in IST) 2006 - 2009. Home page. <http://www.laas.fr/RESIST/>.
- [70] S3MS project (Security of software services of mobile systems). Home page. <http://www.s3ms.org>.
- [71] SeCSE (Service Centric System Engeeniring) 2004 - 2008. Home page. <http://secse.eng.it/>.
- [72] SeCSE project, 2006. A8D5 - Standardization Plan. Deliverable.
- [73] SecureIST project, 2007. D3.3 - ICT Security & Dependability Research beyond 2010: Final strategy. Report. <http://www.securitytaskforce.org/>.
- [74] SecureIST project Advisory Board, 2007. Recommendations for a Security and Dependability Research Framework. Report. <http://www.securitytaskforce.org/>.
- [75] SENSORIA (Software Engineering for Service-Oriented Overlay Computers) 2005 - 2009. Home page. <http://www.sensoria-ist.eu/>.
- [76] Service Availability Forum. Home page. <http://www.saforum.org/home>.

- [77] IEEE Computer Society, 2007. Technical committee on dependable computing and fault tolerance. Web page. <http://www.dependability.org/>.
- [78] SPICE project (Service Platform for Innovative Communication Environment) 2006 - 2008. Home page. <http://www.ist-spice.org/>.
- [79] SWAMI project (Safeguards in a World of Ambient Intelligence) 2005 - 2006. Home page. <http://swami.jrc.es/>.
- [80] SysML Forum. Home page. <http://www.sysmlforum.org/>.
- [81] The Open Group Security Forum, 2004. Introduction to Security Design Patterns. Guide.
- [82] The Open Group Security Forum, 2004. Security Design Patterns (SDP) technical guide. Technical Guide. <http://www.opengroup.org/security/gsp.htm>.
- [83] Trusted Computing Group. Home page. <https://www.trustedcomputinggroup.org/home>.
- [84] The World Wide Web Consortium (W3C). Home page. <http://www.w3c.org>.
- [85] Yahoo. Design pattern library. Web page. <http://developer.yahoo.com/ypatterns/>.