ICT-32-2014: Cybersecurity, Trustworthy ICT

WITDOM
“empowering privacy and security in non-trusted environments”

D7.8 – Preliminary Standardisation Reports

Due date of deliverable: 30 June 2016
Actual submission date: 30 June 2016

Grant agreement number: 644371  Lead contractor: Atos Spain SA (ATOS)
Start date of project: 1 January 2015  Duration: 36 months
Revision 1.0

Project co-funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020, and the Swiss State Secretariat for Education, Research and Innovation (SERI)

<table>
<thead>
<tr>
<th>Dissemination Level</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PU = Public, fully open</td>
<td>X</td>
</tr>
<tr>
<td>CO = Confidential, restricted under conditions set out in the Grant Agreement</td>
<td></td>
</tr>
<tr>
<td>CI = Classified, information as referred to in Commission Decision 2001/844/EC</td>
<td></td>
</tr>
</tbody>
</table>
D7.8

Preliminary Standardisation Reports

Editor
Ero Balsa (KU Leuven)

Contributors
Lilian Adkinson (UVIGO), Archana Bindu Sunil (KU Leuven), Marcus Brandenburger (IBM), Eduarda Freire (IBM), Ilia Iliashenko (KU Leuven), Nicolás Notario (Atos), Sujoy Sinha Roy (KU Leuven), Juan Ramón Troncoso (UVIGO)

Reviewers
Fernando Carmona (Atos), Jolanda Modic (XLAB)

30 June 2016
Revision 1.0

The work described in this document has been conducted within the project WITDOM, started in January 2015. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 64437. This work was supported in part by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0098.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission or the Swiss Government.

©Copyright by the WITDOM Consortium
Executive Summary

This deliverable, WITDOM’s D7.8, is the first of two standardisation reports that are planned within the lifetime of this project. Standardisation activities are, together with dissemination, communication and exploitation activities, the backbone of WITDOM’s work package 7, whose main focus is to promote and achieve a high impact and visibility of the research and innovation outcomes resulting from this project. Standardisation efforts are essential to ensure that existing standards are used by the project whenever possible as well as to contribute to current standardisation efforts and promote new standards. In this first report we provide a description of the different activities related to standardisation that we have carried out so far in the first half of this project.

Our standardisation activities can be classified along two main lines. Firstly, we have pursued the adoption of existing standards, namely, we have mapped out existing standards relevant to the problems and envisioned solutions being considered in this project. Not only we consider general security, privacy and cloud-related standards key for our work but also standards specific to the research and innovation fields that underlie the solutions being developed in WITDOM, this is, secure computation, secure processing and privacy technologies. We describe these standards and how they are relevant for our project.

Secondly, we have sought to lay out a plan to contribute to current drafts and potential new standards. We have engaged with several standardisation organisations in order to explore different collaboration possibilities. Among these the most notable is ISO, the International Organization for Standardization, with whom we have requested a liaison\(^1\) for collaboration. The liaison allows us to provide input and actively contribute to standards in the field of cryptography and privacy technologies, both underlying disciplines to the solutions being designed and deployed in WITDOM. In addition to the contacts we have established with standardisation organisations, we report which standards are currently under development that we should consider and potentially contribute to, focusing on ISO/IEC JTC 1/SC 27 standards due to the potential offered by the liaison for contribution. Besides, we also show how the research and innovation outcomes stemming from WITDOM are too novel to consider their standardisation a realistic or feasible task within the length of this project. The standardisation process requires thorough discussions and broad consensus that usually take longer than the length of this project.

Lastly, we conclude with an outlook of the standardisation activities we plan to focus our efforts on during the second half of this project, namely, keep exploring standards relevant to our project as well as contributing to ISO standards currently under development through our liaison.

\(^1\)Currently approved by the working groups we have applied to and pending endorsement by ISO/IEC JTC 1.
Contents

1 Introduction
   1.1 Purpose of this document .......................... 1
   1.2 Relation to other project work ...................... 1
   1.3 Structure of the document .......................... 2
   1.4 Acronyms used in this document .................... 3

2 About Standardisation .................................... 4
   2.1 WITDOM’s Approach to Standardisation ............... 4

3 Adopting Existing Standards .............................. 6
   3.1 Standardisation Bodies and Related Organisations .... 6
   3.2 Standards Considered ................................ 8
      3.2.1 General Security and Privacy Standards .......... 8
      3.2.2 WITDOM Technology-Specific Standards .......... 10

4 Contributing to Current Drafts and Future Standards ... 15
   4.1 Engaging with Standardisation Bodies .............. 15
      4.1.1 ISO/IEC SC27 Category C Liaison ................ 16
      4.1.2 IPEN ........................................ 17
      4.1.3 OASIS ........................................ 17
      4.1.4 Other Contacts ................................ 17
   4.2 Contributing to Working Drafts ..................... 17
      4.2.1 General Security and Privacy Working Drafts .... 17
      4.2.2 ISO 21089 – Trusted End-to-End Information Flows .. 18
      4.2.3 WITDOM Technology-Specific Standards .......... 18
   4.3 Mapping Out Potential New Standards ............... 19
      4.3.1 Secure Computation ................................ 19

5 Conclusion and Outlook .................................. 21
Chapter 1

Introduction

1.1 Purpose of this document

The purpose of this document is to report on the standardisation activities carried out by WITDOM in the first half of its lifetime. This is the first of two reports on standardisation planned to be delivered during the whole duration of the project. This first report focuses on the mapping out of existing standards, both those already published and accepted by the community, and those that only recently have started to be drafted out. Our first goal is to provide an overview of those standards that are relevant to the project and those that could potentially be.

The second goal of this report is to expose gaps in the standardisation, namely, to report on those research areas that WITDOM is involved in where no relevant standards exist or have been published or initiated so far. We couple this with an analysis of how realistic or feasible it is to expect standardisation activities in these non-standardized domains.

The third goal of this document is to inform the reader about our initial contacts with standardisation bodies and other working groups. From the type of standardisation activities they are carrying out at the moment, together with their methods and requirements to the standardisation process, we provide a first outline of the future possibilities we have so far considered promising for the research outcomes stemming from WITDOM. This will be further explored during the second half of the project, when the research outcomes are mature and can be properly explained to and understood by the rest of the research community and standardisation bodies.

1.2 Relation to other project work

Standardisation activities are linked to several other tasks being carried out in this project. As part of a work package on “Dissemination, communication, exploitation and standardisation” it is clear that all these types of activities are closely related to each other. Standardisation has an impact on all dissemination, communication and exploitation, and vice versa.

Our standardisation efforts contribute to these three activities in several ways. On the one hand, by engaging with standardisation bodies and contributing to the standards they are developing we bring their attention to the work being done in WITDOM, which necessarily results in wider dissemination of our work. By explaining to others the kind of solutions that WITDOM is developing and how we plan to contribute to standardisation, we necessarily need to communicate to others the kind of problems WITDOM is dealing with, the challenges involved and the possible solutions we have envisioned to address those problems. This helps raising awareness among the business and academic community about the types of problems and solutions we are currently working on. Both dissemination and communication and thus clearly linked to standardisation activities, as shown in deliverable D7.3 [ABv+16]. On the other hand, contributing to standards currently under development or even promoting or spurring a new standard helps defining a model of exploitation. Regardless of whether the standard relates to a
component of our solution or to the system as a whole, a standard specification can contribute to further adoption and exploitation.

In addition to these activities, standardisation efforts also have an impact on the fundamental research and innovation activities related to WITDOM. Some of the requirements elicited in the initial phase of this project (see deliverable D2.1 [VAB+15]) can be addressed with a solution or technology for which a standard is already available. Prioritising the standard over other alternative solutions ultimately has an impact on the compatibility and wide acceptance of our design.

1.3 Structure of the document

This document is structured as follows. In Chapter 2 we motivate the need for standardisation and introduce and describe the types of activities we have carried out so far in the project. In Chapter 3 we describe the standardisation bodies and the standards that apply to our work, while in Chapter 4 we report on our contacts with standardisation bodies and the standards under development or even future standards that we have considered contributing to. Lastly, in Chapter 5 we conclude by providing a short discussion on what has been done in terms of standardisation so far and an outlook of what the focus of our activities will be in the remaining half of the project.
1.4 Acronyms used in this document

CEN  European Committee for Standardisation
CENELEC  European Committee for Electrotechnical Standardisation
CSA  Cloud Security Alliance
ENISA  European Union Agency for Network and Information Security
ETSI  European Telecommunications Standards Institute
FHE  Fully Homomorphic Encryption
HE  Homomorphic Encryption
HIPAA  Health Insurance Portability and Accountability Act
IEC  International Electrotechnical Commission
IEEE  Institute of Electrical and Electronics Engineers
IEEE-SA  Institute of Electrical and Electronics Engineers Standards Association
IETF  Internet Engineering Task Force
IPEN  Internet Privacy Engineering Network
ISO  International Organization for Standardization
OASIS  Organization for the Advancement of Structured Information
OWASP  Open Web Application Security Project
PII  Personally Identifiable Information
SHE  Somewhat Homomorphic Encryption
SSP  Secure Signal Processing
W3C  World Wide Web Consortium
Chapter 2

About Standardisation

Standardisation is increasingly viewed as an essential activity to secure a robust foundation for research and innovation efforts. Standardisation efforts bring several advantages to the research and innovation community. They prevent the emergence of compatibility and interoperability problems by bringing teams working on similar problems closer, which in turn allows different teams to build on each others’ efforts and test each others’ advances, overall resulting in better quality control and thorough experimentation.

The importance of standardisation has been recognised by the European authorities as key for innovation and sustainable economic growth and has therefore become an important component of current and future research and innovation actions [BRT15].

Still, it is important to note that standardisation can also pose certain problems. Too early attempts to standardise a technology still in its infancy may stiffen and wither innovation, preventing better solutions to arise due to the constraints imposed by a premature standard. Also, pushing standards through without enough consensus can result in multiple standards that must compete with each other, thereby defeating one of the very purposes of the standardisation process, harmonisation.

In WITDOM, this is an especially sensitive issue. Our research spans several research areas still in its infancy, therefore making the task of producing robust and reliable standards a true challenge. Still, contributing to standardisation involves much more than producing new standards. Adopting previous standards and understanding and influencing standards currently underway is just as important. In WITDOM we aim to explore all avenues and thus our standardisation efforts are being carried out on various fronts.

2.1 WITDOM’s Approach to Standardisation

WITDOM standardisation activities can be classified according to three main types of actions. We devote subsequent chapters of this report to detail what advances have been achieved so far with respect to each of these activities.

Adoption and revision of existing standards. First, we are adopting, where possible, international standards that are relevant to our project. By doing so, we support previous innovation efforts and contribute to the strengthening of existing standards. Moreover, adopting existing standards involves a critical revision that helps finding gaps and shortcomings. This analysis is key to revise and ultimately improve existing standards.

Contributing to current standardisation efforts. Second, we are trying to engage, to the best of our ability, with standardisation bodies and their respective working groups in an attempt to contribute to their standardisation efforts. Rather than launching or proposing standards ourselves, our goal is to join in already existing standardisation initiatives, providing input and participating in the discussions to assist to the elaboration of better standards. Our input can be valuable in that we are developing new technologies and solutions, both at a fundamental research and commercial innovation levels, respectively.
Mapping out potential new standards. Lastly, we outline some of the research outcomes and advances that could be subject for standardisation. This means not only identifying WITDOM innovations that could potentially become a reference for future standards but also those very recent research outcomes whose novelty makes them unsuitable for standardisation at this moment. This way, we aim to map out the most promising WITDOM components for standardisation that we should focus on in the remainder of this project.
Chapter 3

Adopting Existing Standards

One of the main standardisation activities of WITDOM is the adoption and follow-up of existing standards. Adopting existing standards has several advantages for our project. On the one hand, it offers a systematic and organised methodology to tackle development issues central to the solution being designed in the project. Moreover, standards offer a reference terminology that often stems from the consensus of different stakeholders, thus helping us using concepts that are broadly understood and agreed upon outside of our own research communities. On the other hand, the critical evaluation of a standard before deciding whether it is relevant or suitable for our project also provides us opportunities to challenge and put into question standards that may need to be updated or revisited. In this section we first outline standardisation bodies and other related organisations that work on issues similar to the ones WITDOM focuses on. Then, we provide a description of those standards that we have found to be more central and relevant to our work and will therefore be followed throughout the duration of this project.

3.1 Standardisation Bodies and Related Organisations

Before embarking on the description of the standardisation activities carried out within WITDOM, we must provide an overview of those standardisation bodies, organisations and working groups that are leading the standardisation effort globally. These are the organisations that have produced the standards that WITDOM is adopting, those that we as a project aim to contribute to and even those that may be initiated from this project’s research and innovation outcomes. Hence, these are the organisations that we follow and look up for collaboration in WITDOM.

ISO

ISO, the International Organization for Standardization, is the largest international organisation devoted to the promotion of standards. With more than 21 000 International standards, ISO is a popular standardisation body with standards published in virtually any domain.

ISO is composed of over 250 technical committees working on different areas of research and innovation. Of those technical committees, one is of particularly relevant to WITDOM, the technical committee ISO/IEC JTC 1, jointly led with the IEC (the International Electrotechnical Commission). Technical committees are in turn internally organised and divided into subcommittees of which the SC 27 IT on “Security Techniques” is of special interest to WITDOM. Lastly, the subcommittee ISO/IEC JTC 1 SC 27 IT Security Techniques is composed of the following working groups: WG 1 on “Information security management systems”, WG 2 on “Cryptography and security mechanisms”, WG 3 on “Security evaluation, testing and specification”, WG 4 on “Security controls and services”, WG 5 on “Identity management and privacy technologies”.

Since the scope of this standardisation subcommittee spans a broad breadth of IT systems and scenarios, the whole body of standards comprised in ISO/IEC JTC 1 SC 27 IT Security Techniques is potentially relevant to the
D7.8 – Preliminary Standardisation Reports

project. In the next section we provide a sub-selection of the most relevant standards for WITDOM. We point out that this list should be considered as a tentative proposal and the applicable standards are to be regularly revised during the next half of the project.

OASIS

OASIS, the Organization for the Advancement of Structured Information, is a non-profit consortium that promotes the development and adoption of standards in several domains of which internet security and cloud computing are the most relevant to WITDOM. It differs from ISO in that participation is open to everyone at the organisation level, whereas in ISO it must be mediated by the national bodies that are part of it or through liaisons that do not necessarily bestow the right to vote. As a result of all this, the process of standardisation through OASIS can be faster.

CEN, CENELEC & ETSI

CEN, CENELEC and ETSI are the three officially recognised European Standardisation Organisations. CEN, the European Committee for Standardisation, and CENELEC, the European Committee for Electrotechnical Standardisation, seek to promote the adoption of standards at the European level to ensure the quality and interoperability of different technologies as well as the lawfulness according to European regulation. Composed of the national standards agencies of 33 European countries, they also cooperate with ISO and IEC to reach consensus on standards at the international level.

ETSI, the European Telecommunications Standards Institute, seeks to develop international standards in the field of ICT technologies. They develop standards on various fields such as the cloud, the Internet of Things, smart applications, wireless systems, smart cards, cyber security or security algorithms, among others.

W3C

The World Wide Web Consortium (W3C) is an organisation devoted to the development and adoption of standards related to the World Wide Web. The focus of WITDOM is not the development of technologies or tools for the World Wide Web per se, which means that few of the standards developed or being developed by the W3C are related to the research being done in WITDOM. Still, as a standards organisation, the W3C can provide valuable advise and know-how in the process of standardisation. This is, how to organise a standardisation working group, what are the best procedures to follow, how to best reach a consensus and so on. It is for this reason that we consider interaction with the W3C as part of our standardisation activities.

IETF

IETF, the Internet Engineering Task Force, is an open community of designers, operators, vendors and researchers concerned with the architecture of the Internet. Because of its focus on infrastructure, it has a great impact on the development of technology and the correct functioning of the Internet. However, this also means that the abstraction level they are concerned with is considerably “lower” than the one we work at WITDOM, where infrastructure is assumed as “a given” and thus we make no attempts at or expect to change it. Still, similarly to the W3C, IETF can provide advise with respect to the standardisation process.

IEEE-SA & IEEE Cloud Computing

IEEE-SA, the Institute of Electrical and Electronics Engineers Standards Association, is an organisation within IEEE responsible for the development and promotion of international standards on a range of fields, including information technology and assurance. Still, and similarly to IETF, their main focus of activity is at the infrastructure level so the IEEE is of minor interest to WITDOM and we do not expect to directly contribute or adopt any of their standards.
Having said that, a new sub-community *IEEE Cloud Computing* has emerged within, originating a few working groups and respective standards related to the cloud.

**CSA**

Not strictly a standards organisation, the Cloud Security Alliance (CSA) is an organisation that seeks to promote the use of best practices to ensure security in the domain of cloud computing. As an organisation focused on the cloud, it is key for the innovation actions being carried out in WITDOM. CSA has several operating working groups on cloud-related sub-areas such as those focused on mobile technology, big data, security or governance. As an organisation entirely focused on the security of the cloud, it is key for the research goals of WITDOM.

**OWASP**

OWASP, the Open Web Application Security Project, is an open community devoted to the development and dissemination of information as well as practical tools related to web application security. The goal of OWASP is to promote a secure online environment through application development. Many of its publications such as the “Top Ten” or the OWASP Development guide have become a reference in the application development community and have also had an impact in posterior standards development.

**ENISA**

Another not standards organisation, ENISA, the European Union Agency for Network and Information Security, seeks to improve network and information security in the European Union. To that end ENISA advises and assists the European Commission and the member states on information security, collects and analyses data related to security incidents in the European Union and promotes risk assessment and risk management. ENISA periodically publishes the results of their analyses together with recommendations to raise awareness and contribute to a better understanding of the security risks faced by European industry. Lately, they have published several key reports on cloud vulnerabilities [CH09] or the implementation of privacy technologies [DDFH+15], among other WITDOM-related topics.

Our interest in ENISA is two-fold. On the one hand, they provide valuable advise and recommendations on the development and implementation of technology. On the other hand, they focus on the particular context of the European Union, taking into account current European legislation and the particularities of the European market.

**NIST**

NIST, the National Institute of Standards and Technology, could be regarded as the CEN/CENELEC/ETSI equivalent in the United States. Among other activities, NIST produces *Standard Reference Materials* (SRMs) that define the features and characteristics that certain technologies should meet. Of particular importance in the domain of cryptography, the NIST has defined the current Advanced Encryption Standard (AES) and secure hash SHA-3 Standard.

### 3.2 Standards Considered

#### 3.2.1 General Security and Privacy Standards

At the beginning of the project we compiled a list of general security and privacy standards that could be potentially relevant to our use cases and technologies. An overview and description of this list was already reported in deliverable D.2.1. [VAB+15] During the requirements elicitation phase and the design of the solution, we selected those standards that were directly applicable to the project and those that were not. In this section we
review those that we have so far taken into account in this project. This is by no means an exhaustive list of all available standards but a selection of those that seem to best suit the needs of our research so far. The list will most likely be updated as we engage with standardisation efforts in the second half of this project and continue to develop our system and technologies, i.e., additional standards may become relevant for issues and research challenges we have not encountered yet.

We note that some standards and guidelines are influenced by or supersede other, previous standards by the same or different organisations. For example, many ISO standards reference and already take into account other ISO related standards that describe, e.g., terminology or more high/low-level related issues. More concretely, ENISA’s report “Privacy and Data Protection by Design” takes into account several ISO and OASIS standards. This means that, in this particular case, by following ENISA’s recommendations and guidelines we are implicitly taking up the set of underlying standards that were considered in the elaboration on that report.

Moreover, oftentimes the work being carried out by different standardisation bodies overlaps, each of them having their own practices and focusing on a defined set of goals. This leads to the publication of multiple standards that deal with similar issues, albeit their particular differences. In this report we have attempted to group standards produced by different standardisation bodies along three thematic ways, namely, security, privacy and cloud-specific, rather than separately addressing the work of each of the standardisation bodies working on which issues. Note that in this document we do not deal with standards related to the specific use-case scenarios demonstrated in WITDOM. Whereas we also welcome standardisation advances in these specific domains, our standardisation activities focus on general solutions, techniques and research outcomes rather than on their application to specific use cases. Relevant standards related to the use cases being showcased in WITDOM have already been listed in D.2.1 [VAB +15] as part of the requirements elicitation phase.

Security Standards

The family of ISO standards under the 27000 series has been specially relevant and useful so far for the project. Examples include “ISO/IEC 27000 – Information security management systems – Overview and vocabulary” that sets a terminology for information security issues or “ISO/IEC 27002 – Code of practice for Information Security Controls”, “ISO/IEC 27003 – Information security management system implementation guidance” or “ISO/IEC 27004 – Information security management – Measurement” that provide guidelines to issues such as how to classify information and the risks and harms that a potential leak and disclosure may cause to different stakeholders, implementation of access control and evaluation measurements, respectively. Note however that not all sections of these standards are applicable to our work, e.g., those relating to physical security or human resources are out of the scope of this project.

OWASP Top 10[1] provides a list of 10 web application security risks that are deemed to the most critical for security of web application development. This Top 10 is being considered in the implementation of the WITDOM solution. Besides, OWASP Application Security Verification Standard (ASVS), provides metrics and guidance to evaluate the extent to which application technical security controls can be relied on to protect against certain vulnerabilities such as Cross-Site Scripting and SQL injection.

Privacy Standards

In the context of privacy, the family of ISO/IEC 29100 standards is specially relevant for our project. The ISO/IEC 29100 can be understood as the ISO/IEC 27000 series on general security counterpart for privacy and in fact adapts and links the concepts and terminology that are used in both series of standards. Important standards for our project from the 29100 series include the Privacy framework in ISO/IEC 29100 or the Privacy reference architecture in 29101.

ENISA’s report on Privacy and Data Protection by Design provides a comprehensive set of guidelines to implement privacy and data protection by design [DDFH +15] that are particularly relevant to our project and inspire and guide our design decisions. This document combines both regulatory and standardisation efforts

---

from international bodies such as ISO and OASIS with the latest research outcomes in the emerging field of privacy engineering [GTD15, Hoe14]. The report provides extensive advise about how to cover privacy and data protection by design requirements, providing a taxonomy and description of the privacy enhancing technologies currently available to address privacy issues online.

Cloud Standards

The cloud has received an unprecedented amount of attention in the last years. This has prompted the emergence of new standards that attempt to define terminology and set the framework to address typical problems specific to the cloud.

ISO/IEC 27017 extends the security controls described in ISO/IEC 27002 in the context of the cloud, which makes it a straightforward extension of the guidelines provided in other ISO standards for cloud-specific problems WITDOM deals with, even if not all of its content are relevant for our work. Cloud-specific concepts and terminology are especially useful, as well as other provisions regarding the use of cryptography, key management or access control in a cloud environment, even if many of these considerations link back to the generic security standard ISO/IEC 27002.

The ITU-T X.1600 Series on “Cloud Computing Security” is also important for our work, including ITU-T Recommendation X.1601 “Security framework for cloud computing” that provides a comprehensive, even if high-level, description of the types of threats specific to a cloud environment that should be considered.

Lastly, we follow CSA's Cloud Control Matrix[2] and CSA's Practices for Secure Development of Cloud Applications as guidance to implement secure cloud applications.

3.2.2 WITDOM Technology-Specific Standards

In addition to the general security and privacy standards that apply to the whole system design of the solution envisioned as the result of this project, it is important to have an understanding of what the landscape of current standards applicable to each of the specific technologies being developed within the project is. In D3.3 [TAB+15] we introduced the main fundamental research lines that we are exploring in WITDOM to address the requirements of the use cases being considered. These lines are secure computation (with a clear focus on homomorphic cryptography), secure signal processing, privacy technologies such as anonymisation and data masking as well as data verifiability. We list below existing standards relevant to these areas of research. Note that some of these areas are still too novel to having been subject to standardisation efforts yet. This is to be considered a potential opportunity to develop new standards, as we show in Section 4.3.

Homomorphic Encryption

Part of WITDOM’s fundamental research efforts are being geared towards the improvement of homomorphic encryption cryptosystems. A fully homomorphic encryption (FHE) cryptosystem supports arbitrary function computation on ciphertexts. This would allow the computation of any function on encrypted data, which would in turn solve many of the security and privacy issues related to the outsourcing of data processing to the cloud. Even if the idea of a FHE cryptosystem was formulated since the development of RSA, the construction of FHE appeared to be a difficult challenge. It took nearly 30 years when Craig Gentry came up with the first FHE using ideal lattices in 2009 [Gen09]. Although in theory the scheme enables the computation of functions of arbitrary complexity, in practice Gentry’s proposed scheme was very inefficient and thus impractical in a real case scenario. Since then, many researchers have followed the blueprint set out by Gentry’s proposal with an objective to improve the performance of FHE. Up to this date the most efficient versions of FHE have been constructed based on the ring learning with errors (Ring-LWE) problem [BV11] or NTRU [HPS98]. The recent schemes are faster by orders of magnitude in comparison to the Gentry’s scheme, yet too slow to be used in cloud computing. For example, the YASHE somewhat encryption scheme, currently one of the fastest constructions,
takes more than an hour to evaluate a simple block cipher. The construction of an ‘efficient and practical’ FHE remains an unresolved research problem and therefore has not yet been subject to standardisation. Only when sufficiently fast FHE schemes are developed, standardisation will make sense.

In addition to the above, homomorphic encryption has been considered a solution in several other documents like ETSI’s Group Specification on Network Functions Virtualisation Security (ETSI GS NFV-SEC 001) and ETSI’s Group Specification on Identity and access management for Networks and Services (ETSI GS INS 009). Still, these documents propose it as a scheme which is currently not practically feasible. ‘Report on Post-Quantum Cryptography’ is NIST’s initiative for standardisation of post-quantum cryptography and lists lattice-based cryptography (on which many of the fully homomorphic encryption schemes are based) as a quantum-resistant cryptography technique. Cryptographic techniques based on hard problems over lattices are specified in IEEE P1363.1. Lastly, ISO/IEC 19592-2 ‘Fundamental mechanisms for Secret Sharing’ includes homomorphic secret sharing.

**Lattice-based cryptography.** The dawn of cryptographic primitives based on lattices started in 1996 with a seminal paper by Ajtai [Ajt96]. Since that time researchers discovered few computational problems with security assumptions relying on well-known and still open problems in theory of lattices. NTRU, LWE and Ring-LWE are the most studied among them. Having a flaw of big key sizes these cryptographic primitives were not considered in the beginning as a substitution of existing encryption standards. But they turned out to be a fruitful source for construction of such desirable concepts as fully homomorphic-encryption, attribute-based encryption for arbitrary access policies and general-purpose code obfuscation.

Additionally, more and more promising news come from the field of quantum computing. Last year NSA and NIST made official statements about their concern on coming quantum computers with powerful cryptanalytic capabilities [CJL+16, nsa16]. Lattice-based schemes are believed to be hard for quantum adversary. So they definitely will be among the most discussed candidates for post-quantum future.

There are still no standards in lattice-based cryptography due to its young age but the ice is already broken. The IEEE P1363 group working on standard specifications for public-key cryptography included NTRU as a core for a future standard in lattice-based public-key cryptography. It implies using NTRUEncrypt and NTRUSign procedures for encryption and digital signature schemes, respectively.

Moreover, lattice-based cryptography is considered as a tool for establishing new standards in secret sharing. In particular, the standards

- ISO/IEC 19592-2 - Fundamental mechanisms for Secret Sharing;
- ETSI GS NFV-SEC 001 - Network Functions Virtualisation (NFV); NFV Security;
- ETSI GS INS 009 - Identity and access management for Networks and Services (INS); Security and privacy requirements for collaborative cross domain network monitoring

take into account the state of the art in homomorphic encryption research.

**Secure Signal Processing**

Secure signal processing (SSP) is a relatively recent discipline. Born in 2007 by the joint efforts of the cryptographic and the signal processing communities, it studies how to provide efficient solutions to privacy-aware scenarios where traditional signal processing algorithms are applied by enabling encrypted or protected processing. The achieved solutions in this discipline may make use of some basic standard cryptographic primitives and protocols, but they resort mainly to state-of-the-art or novel approaches which combine the security of cryptographic primitives (like lattice-based homomorphic encryption) with the efficiency of signal processing algorithms. Due to this fact, there are not many applicable standards in this discipline besides those referring to essential cryptographic primitives.

11
Leaving aside homomorphic encryption and lattice-based cryptography, for which the current standards have been introduced in the previous paragraphs, SSP also relies on other cryptographic techniques like secret sharing, multiparty computation or searchable encryption. ENISA’s report “Privacy and Data Protection by Design” \cite{ENISA15} mentions both searchable encryption and secure multiparty computation (MPC) together with two of its main primitives, oblivious transfer and secret sharing. Secret sharing is the main subject of some ongoing standards like ISO/IEC 19592, from the IST/33/2 Cryptography and Security Mechanisms committee, and the OASIS KMIP (Key Management Interoperability Protocol, current version 1.4 in development), which includes recommendations for managing and interchanging split keys with different types of secret sharing mechanisms. To the best of our knowledge, currently there are no relevant standards for the other aforementioned primitives.

Privacy Technologies

There are two main types of privacy technologies that we will be relying on to address the privacy requirements of the two case scenarios considered in this project: data anonymisation and data masking. Whereas the previously mentioned report from ENISA \cite{ENISA15} provides a good overview and guidance to the implementation of privacy and data protection by design, we also rely on standards specific to these two technologies we will be implementing.

Data Anonymisation. Article 29 Working Party’s Opinion on Anonymisation Techniques has become the cornerstone to a practical guide to anonymisation \cite{Par14}. The document provides a detailed definition of anonymisation under EU legislation, making a clear distinction between what is to be considered anonymisation and what is pseudonymisation. In addition to that, it describes the types of techniques that can be implemented to anonymise data and a number of measures that can be used to assess the anonymisation guarantees of the techniques in use. We use this document as the main guidance to the design of WITDOM’s data anonymisation component.

Additionally, we also summarize here some specific standards related to anonymisation techniques which are specifically focused on a concrete application field (e.g., health data), even when they are not necessarily applicable in the European landscape. WITDOM keeps vigilance on these standards to maintain an adequate interoperability where possible.

ISO/TS 25237:2008 – Pseudonymization. This standard contains privacy principles and requirements for the protection of personal health information using pseudonymisation services. The standard defines pseudonymisation and gives an overview of different use cases in which it can be reversible or irreversible. It also defines a methodology for pseudonymisation services, including organisational and technical aspects, and gives a guide to assess the re-identification risk. Furthermore, it defines a policy framework and it specifies the minimal requirements for the operations of a pseudonymisation service and a controlled re-identification, and specifies some interfaces in order to enable interoperability.

ISB 1523 - Anonymisation Standard for Publishing Health and Social Care Data. The purpose of this standard is to assist UK health and social care organisations transforming data that identify individuals into data that are not identifying and fit for publishing. The standard gives some recommendations on how to assess the level of risk of a dataset, considering also the existence of external information, and defines some criteria regarding the selection of anonymisation algorithms.

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual. The Privacy Rule provides two methods by which health information can be designated as de-identified, as shown in Fig. 3.1: 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual.
**Data Masking.** In order to ensure that organisations meet minimum levels of security when they store, process, or transmit sensitive data, several regulations and standards have been created by governments and enterprises. As examples, in the financial area, we have the Payment Card Industry Data Security Standard (PCI-DSS) [CIP06], which provides a guideline of requirements to protect card holder data, and in the health care area we have the Health Insurance Portability Act of 1996 (HIPAA), which requires the protection and confidential handling of protected health information. These standards, however, do not recommend specific algorithms.

Data masking is a set of various techniques used to obfuscate sensitive data. Encryption is one of the techniques that are used by organisations. Previously approved encryption schemes have been announced by standardisation bodies, such as the Advanced Encryption Standard (AES) [NIS01]. Yet, the encryption modes were only designed for binary data, which do not include names, credit card numbers or social security numbers, i.e., common data types stored in organisation’s databases.

Format Preserving Encryption (FPE) is an encryption method designed for any kind of data. It encrypts data in a way that the data format remains the same, e.g., the encryption of a social security number (SSN) results in another social security number. NIST has recently made available a special publication, NIST SP-800-38G [Dwo16], which specifies two methods for FPE, called FF1 and FF3. These methods are specific modes of operation for the AES algorithm.

Having said that, the research being developed by WITDOM in the area of data masking focuses on alternative techniques, unrelated to FPE. We rely on provable secure techniques covering features like irreversibility and unlinkability of the masked data, meaning that sensitive information cannot be linked back from masked data and that masked data cannot be cross-linked. To the best of our knowledge, no standards have been published dealing with this type of techniques yet.

**Data Verifiability**

Two standards are particularly relevant, providing guidance and reference to the research on data verifiability being conducted in WITDOM:

**ISO/IEC JTC 1/SC 27/WG 4 FDIS 27040 Storage Security.** Of special relevant for WITDOM’s Integrity Verification Protection Component is Section 6.7 of this standard, which provides specific guidelines relating to object storage in the cloud. Also, Section 7.5 of this standard, provides general design and implementation guidelines related to data confidentiality and integrity.
CSAs Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union. Section 4 of this document is relevant for WITDOM’s Integrity Verification Protection Component as it refers to data integrity.
Chapter 4

Contributing to Current Drafts and Future Standards

In addition to adopting published standards or revising and assessing whether they are suitable for the needs of the project, there is also an opportunity to participate in the standardisation process by contributing to standards that are currently in the making or, even further, proposing new standards. Needless to say, the former is a less ambitious task but at the same time and in the context of this project more manageable and realistic. This is due to two main reasons: (1) Current working drafts are a joint effort of several entities and thus do not exclusively depend on our effort and commitment. This means that we can provide input to several standards without the burden of leading and managing them. (2) Most current technologies underlying the envisioned WITDOM solutions involve cutting-edge research not ripe for standardisation, making standardisation prospects uncertain. Standardisation of new technologies is a lengthy process that is not always possible in the duration of a 3-year project. This is further complicated by the fact that research results and solutions are only produced near the end of the project.

In the remainder of this chapter we describe how we have invested our efforts in these two tasks. First, we describe our efforts at establishing contact with the standardisation community. In this regard, our main result is our liaison with ISO/IEC JTC 1/SC 27 WG2 and WG5, which enables us to actively contribute to ISO standards dealing with cryptographic and privacy solutions. Then, we outline a number of standards currently under development that are relevant to the project and we are paying attention to. Lastly, we outline potential avenues for the standardisation of research and innovation results stemming from WITDOM.

4.1 Engaging with Standardisation Bodies

Part of our effort towards standardisation, whether to contribute to existing standards or to promote new ones, has involved (and will still do in the second half of the project) seeking the expertise of standardisation bodies and working groups to be able to collaborate with them and take advantage of their expertise and advise.

These groups are after all the true experts on standardisation. They have a greater insight on current standardisation efforts than we do, are aware of the procedures and steps required to succeed at producing new standards and are also better at assessing what is the right moment and scope to standardise a new solution or technology.

In WITDOM we have therefore sought and will continue seeking to join forces with those standardisation groups that can assist us at optimising our standardisation efforts. We expect this to happen at two different levels. On the one hand, by talking and being in touch with standardisation experts, introducing them to the main themes WITDOM deals with and to the research advances that are taking place in the project, they will be able to point us to working groups developing standards that we could collaborate or be involved with. As we show in the remainder of this section, this has already happened at different instances, notably at the last general ISO meeting where several participants showed considerable interest and pointed us out to standards which they found to be key to the project. On the other hand, we also expect these standardisation experts to
assist us in deciding what is worth standardising, which technologies are ready and can benefit from a push from standardisation.

In the remainder of this section we thus introduce and detail the collaborations we have already initiated and other contacts we have established.

### 4.1.1 ISO/IEC SC27 Category C Liaison

As mentioned earlier in Section 3.1 ISO is the largest and one of the most important organisations developing worldwide standards. Hence the possibility of collaborating with ISO and contribute to its standards became a priority from the beginning of the project.

In May 2015, WITDOM applied for a **Category C Liaison** with the following ISO/IEC SC27 working groups WG1, WG2, WG4 and WG5 (see Section 3.1 for a short description of each group’s domain of interest). A Category C liaison is a special type of association reserved for ISO/IEC JTC 1 that enables external organisations to participate in the standardisation processes within an ISO working group. This particular type of liaison would allow WITDOM to participate in the working group meetings, contribute to the ongoing discussions and submit comments to current draft standards as well as submit our own technical reports and recommendations for new standards. This type of liaison does not however grant the right to vote in the working group decisions.

The application was accepted and earlier this year WITDOM was invited to join the General ISO Meeting on April 11-15th 2016 in Tampa (FL, USA) to introduce the project to the different working groups we had applied to establish a liaison with. A representative of WITDOM presented the project to the assistants, who then proceeded to decide on whether the liaison would be interesting for both ISO and WITDOM and hence should be accepted. Two out of the four working groups accepted the liaison\(^1\), namely, WG2 on “Cryptography and Security mechanisms” and WG5 on “Identity Management and Privacy Technologies”, while the other two groups, and specially WG4, pointed out several other standards and groups that could be interesting for WITDOM. Antonio Kung, the current rapporteur of ISO SC27/WG5, has been assigned to WITDOM as liaison officer. WITDOM has already contacted him and we are currently working together to lay out a strategy for WITDOM to contribute to ISO’s standardisation activities.

Moreover and, as expected, we received feedback from the different working groups on standards that we should pay attention to and try to contribute to. Specifically, WG5 participants suggested to take into consideration the following:

- ISO/IEC AWI 20889, a proposal for a new work item on *Privacy enhancing data de-identification techniques*. The goal is to aid and guide organisations in implementing robust de-identification of data for analyses purposes. Work in this proposal has just started, so WITDOM will be able to join and participate from the beginning.


- ISO/TC 46/SC11, the ISO committee responsible for developing standards related to record and archive management. This subcommittee is especially relevant to our work on financial and genomic records.

From WG4, participants suggested to consider the following:

- ISO/IEC 27034 on Application Security, that intends to provide guidance to organisations concerned with implementing security in their processes and applications, whether these are developed in-house or acquired from or provided by third parties.

- ISO/IEC CD 19944 - Cloud Computing - Data and their Flow across Devices and Cloud Services. This is a working draft being developed not within SC27 but SC38. SC38 is ISO’s subcommittee on Cloud Computing and Distributed Platforms.

\(^1\)Currently pending endorsement from ISO JTC 1.
We are currently examining these standards to assess whether and how WITDOM could contribute to their development.

4.1.2 IPEN

As part of our plan to contribute to ISO standards we have joined the Internet Privacy Engineering Network (IPEN). IPEN is an informally organised (no official membership is required) community of researchers and developers interested in the emerging field of privacy engineering. Among other activities, IPEN keeps a Privacy Standards Wiki\(^2\) that brings together the community of researchers and developers interested in privacy standards from different standardisation bodies. This Wiki helps organising the work for contributors by pointing out which standards are currently being drafted and would benefit from input. We therefore plan to use this tool and further leverage the IPEN community to contribute to current standardisation efforts.

4.1.3 OASIS

WITDOM partners are collaborating with OASIS in privacy-related technical committees such as the Privacy Management Reference Model and the Privacy by Design Documentation for Software Engineers where there are potential links with the expected outcomes of this project.

Moreover, any other possibility to contribute or promote a standard would be facilitated by the fact that IBM, one of WITDOM partners, is a foundational sponsor of this organisation.

4.1.4 Other Contacts

In addition to the above, WITDOM has established informal contact with representatives of other standardisation bodies such as CEN-CENELEC, W3C, NIST and the IETF by participating in workshops and events related to standardisation, such as the workshop “Towards secure and trusted cloud services in Europe” organised by the project CloudWATCH on September 2015 and the upcoming “Unique Identifier for Personal Data Usage Control in Big Data” on July 2016. A description of our conversations in the former event has already been reported in WITDOM’s D7.3 First Dissemination Report and Material \[ABv^{+}16\]. In short, most representatives agreed that our standardisation activity could be either done informally, by joining the conversation being carried out in mailing lists by open working groups, or formally, once we have a mature definition of our advances and technologies, by submitting a proposal to a working group or standardisation body that is currently working on the field. We further elaborate on these two strategies in sections 4.2 and 4.3 below, respectively.

4.2 Contributing to Working Drafts

In addition to the standards under development that participants at the last ISO meeting have pointed us to, we have also identified a set of working drafts that are relevant for the project.

4.2.1 General Security and Privacy Working Drafts

From ISO, we have identified the following working drafts:

- ISO/IEC JTC 1/SC 27/WG5 SD2 – Privacy References list
- ISO/IEC JTC 1/SC 27/WG5 WD 29134 Privacy impact assessment

\(^2\)See http://ipen.trialog.com/wiki/Wiki_for_Privacy_Standards
Input to these standards will be coordinated through IPEN as part of our liaison with ISO/IEC WG5. Standards from other working groups that WITDOM does not have a liaison with are also relevant for our work, including:

- ISO/IEC JTC 1/SC 27 WG 1 WD 27017 Code of practice for information security controls for cloud computing based on ISO/IEC 27002
- ISO/IEC JTC 1/SC 27 WG 4 WD 27036, Information security for supplier relationships Part 4: Guidelines for security of cloud services
- ISO/IEC JTC 1/SC 27 WG 4 FDIS 27040 Storage Security

Even if we will take into account these standards we do not plan on actively contributing to them as we will focus our efforts on the working groups that we are in liaison with.

4.2.2 ISO 21089 – Trusted End-to-End Information Flows

In August last year WITDOM’s project manager was made aware of the re-activation of standard ISO 21089 – Health Informatics – Trusted End-to-End Information Flows. Witdom requested the current working draft through one of its members bodies and provided comments directly to the ISO contact person for this standard. We have focused on articulating a coherent terminology that could be adopted in our project. This working draft is still being currently discussed. We will strive to stay up-to-date and provide comments as necessary.

4.2.3 WITDOM Technology-Specific Standards

In addition to general security and privacy standards under development we also consider working drafts specific to the research areas or technologies that WITDOM is working on.

Homomorphic Encryption

We have already mentioned that there are no standards on homomorphic encryption yet. Still, current work of the ISO/IEC JTC 1/SC 27 WG2 is devoted to the upcoming standard ISO/IEC 18033-6 on Homomorphic encryption. This is an upcoming standard on partially homomorphic encryption i.e., supporting one homomorphic operation (either addition or multiplication). Partially homomorphic cryptosystems have been available for many years (i.e. RSA is multiplicatively homomorphic) and researchers have a solid understanding of their performance. Promotion of the eventual emergence of a standard for homomorphic encryption is one of the main goals of the HEAT H2020-ICT-644209 project, that unites many leading researchers in the field. In particular, the participant of the project Pascal Paillier is the main editor of the upcoming standard ISO/IEC 18033-6. We note that KU Leuven-COSIC, one of the partners in Witdom, is also involved in the HEAT project. Also, thanks to WITDOM’s liaison to ISO/IEC JTC 1/SC 27 WG2 we will be directly involved in the development of this standard.

Secure Signal Processing

There are no ongoing standards or specific committees working in the standardisation of the field of secure signal processing. Therefore, there are no plans to directly contribute to the standardisation of the developed primitives or protocols in this discipline; in any case, WITDOM will keep vigilance on the ongoing related standards for secret sharing and homomorphic encryption, specially through the liaison request to ISO/IEC JTC 1/SC 27 WG2, to promote the algorithms, protocols and used parameterisations that WITDOM research outcomes in secure signal processing show as the most appropriate and efficient for secure processing.
Privacy Technologies

Data Anonymisation Currently ISO is working on the development of one standard key to data anonymisation, namely, ISO/IEC AWI 20889 Privacy enhancing data de-identification techniques. We are planning to contribute to this standard as part of our liaison with ISO.

Data Masking NIST is actively considering Vance and Belare’s DFF proposal for format-preserving encryption [VB14], to supplement the FF1 and FF3 modes specified in Special Publication 800-38G. DFF was submitted as an extension of the VAES3 mode [DP15] that NIST has specified under the name FF2 in the public comment draft of that publication.

As we have already mentioned in Section 3.2.2 whereas the standards above are relevant to the field of data masking, WITDOM’s approach to data masking relies on provable security techniques for which no standardisation efforts have yet been initiated.

4.3 Mapping Out Potential New Standards

Lastly, in this section we provide insight into those technologies or WITDOM research outcomes that could be potentially interesting to standardise.

4.3.1 Secure Computation

We consider two potential avenues for standardisation related to homomorphic encryption: (1) lattice-based cryptography underlying current homomorphic encryption schemes and (2) homomorphic encryption schemes themselves.

Lattice-based cryptography. There are plenty of cryptographic primitives used in lattice-based cryptography. The main features of such systems are

- Fast and highly parallelizable algorithms,
- Conjectured security against quantum computers,
- Strong security reduction to worst-case lattice problems.

By now the crucial point of research is how to optimize key sizes of lattice systems in order to incorporate them in real applications. At this moment, NTRU [HPS98] and Ring-LWE problems [BVT11] seem to be the most promising in that direction. Indeed, for the NTRU scheme Stehlé and Steinfeld constructed a provably secure version that is assumed to be a potential European standard [SS13]. Still, it is not fully understood yet which parameters are more suitable for systems based on Ring-LWE in order to preserve both efficiency and security.

Homomorphic Encryption Schemes. As far as we know there is no fully nor somewhat homomorphic encryption scheme that avoids lattices. Hence at this moment the future standardisation of homomorphic encryption (HE) schemes is expected to be based on computational problems on lattices. Today the main obstacle for fully homomorphic encryption (FHE) schemes on the way to real world practice is the bootstrapping procedure. This is a costly operation that allows to “refresh noise” in a ciphertext and thus avoid decryption errors. All known FHE schemes are essentially somewhat homomorphic encryption (FHE) schemes with bootstrapping. The most efficient and compact SHE scheme is preferable for standardisation. In this sense, NTRU and Ring-LWE problems are once again the most appropriate choice. There are two main HE schemes built upon these primitives:

- YASHE, by Bos, Lauter, Loftus and Naehrig [BLLN13].

3See http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html
Fan and Vercauteren’s modification of Brakerski’s fully homomorphic scheme based on the Learning With Errors (LWE) problem [FV12].

Both of them have already been implemented in SEAL and HElib libraries and thus can be assessed in real applications. However, the viability of YASHE has been called into question. In a recent paper Albrecht et al. have found that there could be security issues with the YASHE scheme [ABD16]. To overcome these issues, we have started redesigning our system to move from YASHE to the FV scheme [FV12]. This scheme is slightly less efficient than YASHE, but it remains secure against known attacks. Since the development of homomorphic encryption schemes is a very recent (and challenging) research area, the research community is trying to find more efficient schemes, and at the same time identify security vulnerabilities in the existing schemes. As a result, it is not possible to carry any significant standardisation efforts in this direction yet.

Secure Processing

There are no ongoing standards in Secure Signal Processing, so there are no plans to standardize the techniques developed in WITDOM within this discipline. In any case, due to the fact that WITDOM SSP protocols make use of lattice-based homomorphic cryptography and secret sharing, the available liaisons with the working groups on the related standards will be used to inform these groups about the results of the project in secure signal processing and to try to promote those schemes and parameterisations with better efficiency and security within WITDOM framework and scenarios.

Privacy Technologies

Data Anonymisation. WITDOM anonymisation techniques take into account the recommendations of the current and ongoing privacy-related standards, but most of these standards are not technology-specific, and they mainly cope with data protection. Additionally, the used anonymisation techniques are very recent and still need to become more mature and show their usage and applicability in scenarios like those considered in WITDOM before they can be standardized. In light of the advances in the privacy-related ongoing standards during the course of the project, the possibility of standardizing WITDOM anonymisation technology will be re-evaluated and compiled in deliverable D7.9.

Data Masking. As we have already mentioned in Sect. 3.2.2, the research being developed by WITDOM in the area of data masking relies on provable secure techniques. This is an innovative area of research that still needs some maturity in the sense that other algorithms need to be proposed and analysed before any standardisation efforts begin.
Chapter 5

Conclusion and Outlook

Standards are important for research and innovation projects like WITDOM for a number of reasons. On the one hand, existing standards help addressing well known problems with what has been adopted and agreed upon by the community as a good solution, which in turn helps encouraging further adoption, prevents compatibility problems and broadens the opportunities for exploitation, among other benefits. On the other hand, contributing to standards gives the opportunity to discuss and challenge our project results with a wider community of experts and researchers, thereby enabling communication across different communities and helping us find better solutions and research outcomes.

In this deliverable we have described the standardisation activities carried out by WITDOM during the first half of the project. We have focused on three main types of activities relevant to standardisation: adopting existing standards, engaging with standardisation organisations and outlining future contributions to standards currently under development or standards-to-be. We have shown that several standards are relevant for our work and we have mapped out the current gaps for standardisation in the research domains that we are exploring in WITDOM. Moreover, we have established a formal liaison with ISO as well as informal communications with other standardisation bodies.

These are however preliminary results. We have an understanding of which standards are relevant for our solution and which standardisation bodies are engaged in areas that we are currently working on. However, in this first half of the project most of the work has involved outlining and designing a solution and many important decisions with respect to the whole architecture or the several components involved are still to be made (to be described and reported in upcoming deliverables). As such, there are little research outcomes to be used to actively contribute to current standardisation efforts yet. While we have engaged with standardisation bodies and examined relevant existing standards, a more active role where we use part of our results to inform standardisation processes currently underway is expected to take place in the second half of the project.

Our recent liaison with ISO/IEC JTC 1/SC 27 offers a promising opportunity to do that. As part of ISO, we will have the opportunity to provide direct output to standards being currently discussed and agreed upon. We hope that part of our research outcomes enable us to provide helpful feedback to these standards. The potential for standardisation of the whole WITDOM solution or WITDOM components seems however bleak. Most of our expected research outcomes would be too novel to have any realistic expectation on standardising them as this is a lengthy process, it requires a broad consensus that takes time to achieve.

In short, during this first half of the project we have focused on identifying relevant standards and standardisation gaps as well as establishing contacts with relevant organisations. During the remaining of this project we plan to contribute in a more active way to current standardisation efforts in our research domains.
Bibliography


D7.8 – Preliminary Standardisation Reports


