



# **CACE**

## **Computer Aided Cryptography Engineering**

Project number: 216499  
FP7-ICT-2007-1

### **D6.4**

#### **Midterm standardisation report**

Due date of deliverable: 30. June 2009

Actual submission date: 30. June 2009

WP contributing to the deliverable: WP6

Start date of project: 1. January 2008

Duration: 3 years

Coordinator:  
Technikon Forschungs- und Planungsgesellschaft mbH  
Burgplatz 3a, 9500 Villach, Austria  
Phone: +43 4242 233 550  
Email: [coordination@cace-project.eu](mailto:coordination@cace-project.eu)  
[www.cace-project.eu](http://www.cace-project.eu)

Revision 1.0

<b>Project co-funded by the European Commission within the 7th Framework Programme</b>		
<b>Dissemination Level</b>		
<b>PU</b>	Public	<b>X</b>
<b>PP</b>	Restricted to other programme participants (including the Commission services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission services)	
<b>CO</b>	Confidential, only for members of the consortium (including the Commission services)	



## **D6.4**

# **Midterm standardisation report**

### **Editor**

Silke Rebernig (TEC)  
Klaus-Michael Koch (TEC)

### **Contributors**

Input from all CACE partners

30. June 2009  
Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the FP7 program under project number 216499. The information in this document is provided as is, and no warranty is given or implied that the information is for any particular purpose. The user thereof uses the information at its sole risk and liability.

## **Abstract**

This deliverable defines an interim report of the standardisation activities of the CACE consortium and provides the reader with an overview of the standardisation topic within CACE.

It identifies relevant standardisation bodies as well as applicable standardisation documents. Further it describes the involvement of some of the CACE partners with some of those bodies.

# Contents

- 1 Introduction ..... 6
- 2 Standardisation within CACE ..... 7
  - 2.1 Relevant standardisation bodies, applicable standards and memberships ..... 8
    - 2.1.1 ISO/IEC/ITU ..... 8
    - 2.1.2 NIST/FIPS..... 9
    - 2.1.3 ANSI..... 9
    - 2.1.4 ETSI ..... 9
    - 2.1.5 IEEE .....10
    - 2.1.6 IETF .....10
    - 2.1.7 PKCS .....11
    - 2.1.8 Common Criteria .....11
    - 2.1.9 SECG.....11
    - 2.1.10 TCG.....11
    - 2.1.11 TeleTrusT .....12
  - 2.2 Synergies with the EC Project ECRYPT .....12
  - 2.3 Standardisation until M18 .....12
  - 2.4 Standardisation plan .....13
- 3 Conclusion .....14
- 4 List of Abbreviations .....15
- 5 References.....16

# 1 Introduction

Active monitoring of, and participation in, relevant standardisation bodies are of vital importance for the CACE project. The aim of this deliverable is to provide the reader with an overview of the standardisation situation within the CACE project. The main emphasis will be in the description of the standardisation landscape in cryptographic software and in identifying standardisation groups relevant to the work done in CACE.

Within the CACE project plan standardisation is part of task 6.2 "Dissemination and Standardisation" in WP6, but only the coordinator TEC and to a minor part RUB as the technical leader is officially participating in this work package. However, it is nevertheless clear that also other project partners – mainly the industrial companies – will actively participate in the standardisation activities, into which they have the best insight. In fact some of the CACE partners have strong and active links with relevant specification and standardisation bodies, which they will use to promote the work of the CACE project. The ways to perform such an activity may range from setting up working groups specifically targeted by the CACE topics to the creation of formal liaisons between already existing committees and the CACE consortium. Therefore this deliverable contains an overview of the standardisation involvement of all partners, who participate in standardisation activities within their RTD project work.

The ability to have first hand information concerning standard developments is essential to steer the different research activities in the right direction. One of the goals of the CACE project is to widely disseminate the results at different levels and to different communities in order to spread the culture and technologies in the field of design. One target for such dissemination is a set of standardisation working groups whose activities are or can be put in relation with the knowledge developed in CACE.

Since the CACE project is clearly dominated by academic partners and the industrial partners are the minority, the interest of pushing CACE results into different standards is not as high as in projects dominated by industry. Therefore the interaction between the different standardisation bodies and CACE will be more of a monitoring kind from a CACE perspective. Although it is highly desired that results from the work performed within CACE would be disseminated within one or more of the standards, it is not considered as a must.

Anyhow, a lot of dissemination activities are performed and a very big amount of high-quality scientific papers and contributions to scientific journals have been compiled. This adds a lot of visibility to CACE since the project goal is to widely disseminate the project results and to build consensus based on these results by using the appropriate standardisation bodies or synergies to other EC projects respectively. Furthermore it is an objective to maintain the strong position of European research while strengthening the position of European industry in cryptography.

With respect to standardisation the state-of-the-art at the beginning of the CACE project was that virtually nothing existed that overlapped with the planned activities. The reason for this is simple: while there are many existing standards in the security and cryptography area, they typically describe particular algorithms (e.g. for encryption) and protocols (e.g. for network security). To be in compliance with a standard in this area, usually means that your program exhibits a certain input/output behavior. This, however, is independent of the process that produces the program, which is what we focus on in CACE.

We also emphasise that the goal of CACE is not to set new standards for encryption algorithms, but to make it easier to write programs that implement and use them securely. However, this should not be taken to mean that the project is not contributing to standardisation. On the contrary, the above mentioned makes it clear that existing standards tend to leave open an important area that CACE can contribute to, namely standards that address not only the cryptographic algorithms and protocols used in applications, but also the tools used to develop them, thus assuring a certain level of security for the entire product.

The remaining part of this report is organised as follows. In Section 2, important issues for standardisation within CACE are clarified including in subsection 2.1 a description of the relevant standardisation bodies and appropriate standards as well as the memberships of CACE partners in these bodies. Subsection 2.2 briefly discusses the existing synergy with another EC project called ECRYPT, 2.3 gives an overview on the standardisation work done during the first 18 months and 2.4 discusses the further standardisation plan. Finally, in Section 3, brief conclusions are provided.

## 2 Standardisation within CACE

The central objective of the CACE project is the development of a toolbox that supports the production of high quality cryptographic software. The proposed toolbox will allow non-experts to develop high-level cryptographic applications by means of security-aware high-level programming languages and compilers. The description of such applications in this way will allow automatic analysis and transformation of cryptographic software to detect or avoid security critical implementation failures.

Based on this objective, the standards relevant for the CACE project are falling into the category of cryptography standards.

*"**Cryptography standards** are needed to create interoperability in the information security world. Essentially they are conditions and protocols set forth to allow uniformity within communication, transactions and virtually all computer activity. The continual evolution of information technology motivates the development of more standards, which in turn helps guide this evolution.*

*The main motivation behind standards is to allow technology from different manufacturers to "speak the same language", that is, to interact effectively. Perhaps this is best seen in the familiar standard VHS for video cassette recorders (VCRs). A few years ago there were two competing standards in the VCR industry, VHS and BETA. A VHS tape could not be played in a BETA machine and vice versa; they were incompatible formats. Imagine the chaos if all VCR manufacturers had different formats. People could only rent movies that were available on the format compatible with their VCR. Standards are necessary to insure that products from different companies are compatible.*

*In cryptography, standardisation serves an additional purpose; it can serve as a proving ground for cryptographic techniques because complex protocols are prone to design flaws. By establishing a well-examined standard, the industry can produce a more trustworthy product. Even a safe protocol is more trusted by customers after it becomes a standard, because of the ratification process involved.*

*The government, private industry, and other organisations contribute to the vast collection of standards on cryptography. A few of these are ISO, ANSI, IEEE, NIST, and IETF. There are many types of standards, some used within the banking industry, some internationally and others within the government. Standardisation helps developers design new products. Instead of spending time developing a new standard, they can follow a pre-existing standard throughout the development process. With this process in place consumers have the chance to choose among competing products or services." [01]*

In fact, the CACE project will implement cryptography at different system layers. This leads to the fact that the results of these implementations could be applicable for a lot of different standards of different standardisation bodies. Several CACE partners are involved in different standardisation bodies, therefore it will always be an option to promote outcomes of the CACE project as inputs for draft standards to corresponding technical communities.

The selection of the most relevant standardisation bodies and their standardisation documents provided in the following chapter is based on the focus of the standards. Principally the CACE project focuses on the enhancement of standards in the areas of architectural aspects, security aware languages and on compilers for designing security protocols. Further standards regarding component interfaces and libraries, evaluation and rating criteria as well as testing methodologies are rated as relevant.

All in all it can be said that it is a great benefit for the CACE consortium that some of the partners are involved in standardisation bodies. This provides the CACE consortium insight in currently ongoing standardisation activities which provides one possibility to ensure state-of-the art and further ensures the potential to bring in relevant CACE outcomes to the adequate standardisation bodies if desired by the consortium.

## **2.1 Relevant standardisation bodies, applicable standards and memberships**

This chapter gives an overview of the most relevant standardisation bodies for CACE as well as of the relevant standards which may influence a cryptographic software implementation. Furthermore certain adequate groups of the different standardisation bodies where CACE partners are involved are described in more detail. The below mentioned standardisation bodies could benefit from CACE results either directly or indirectly.

This section is not providing an exhaustive description of all standards which may influence a cryptographic software implementation. Anyhow many of the standards published by different bodies overlap in the techniques that they normalise.

### **2.1.1 ISO/IEC/ITU**

The International Standards Organisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunications Union (ITU) publish a series of standards covering a wide range of topics related to security and cryptography under the Information technology - Security techniques category. Some of the most relevant for the CACE-project are listed as follows:

- ISO/IEC 9796 Digital signature schemes giving message recovery.
- ISO/IEC 9797 Message Authentication Codes (MACs).
- ISO/IEC 9798 Entity authentication.
- ISO/IEC 10116 Modes of operation for an n-bit block cipher
- ISO/IEC 10118 Hash-functions
- ISO/IEC 11770 Key management
- ISO/IEC 15946 Cryptographic techniques based on elliptic curves
- ISO/IEC 18031 Random bit generation
- ISO/IEC 18032 Prime number generation
- ISO/IEC 18033 Encryption algorithms
- ISO/IEC 19790 Security requirements for cryptographic modules
- ISO/IEC DIS 11889-1 Trusted Platform Module -- Part 1: Overview
- ISO/IEC DIS 11889-2 Trusted Platform Module -- Part 2: Design principles
- ISO/IEC DIS 11889-3 Trusted Platform Module -- Part 3: Structures
- ISO/IEC DIS 11889-4 - Trusted Platform Module -- Part 4: Commands

#### **2.1.1.1 JTC 1/SC 27 "IT Security Techniques"**

The SC27 "IT Security techniques", is a subcommittee of the ISO/IEC Joint Technical Committee 1 and is responsible for the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems (ISMS), security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security;
- Security evaluation criteria and methodology.

SC27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas.

In fact the SC27 working group is the most relevant group within ISO/IEC for the CACE project since all above mentioned relevant standards within ISO/IEC are developed within this group. The technical leader RUB is involved in this group via industrial contacts. They take care of monitoring of those standards in order to be aware of any changes in this area. They will be able to take care of contributions resulting from outcomes of the CACE project to any of those standards if requested by the CACE consortium. One option for the integration into future ISO standards of the TPM could be the ZK-POK protocols generated with the help of the compiler developed in WP3.

## 2.1.2 NIST/FIPS

The National Institute of Standards and Technology (NIST) maintains the Federal Information Processing Standards (FIPS) which cover many aspects of the use of cryptography by government agencies in the US. The following FIPS publications are relevant for the CACE project:

- FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
- FIPS 197 Advanced Encryption Standard
- FIPS 196 Entity Authentication Using Public Key Cryptography
- FIPS 186 Digital Signature Standard (DSS)
- FIPS 185 Escrowed Encryption Standard
- FIPS 180 Secure Hash Standard (SHS)
- FIPS 140 Security Requirements for Cryptographic Modules

## 2.1.3 ANSI

The committee X9 of the American National Standards Institute (ANSI) develops standards for the financial industry. Inside this committee, the X9F1 working group is responsible for developing the core cryptography standards that specify symmetric-key and public-key algorithms for encryption and authentication. Some of the relevant ANSI cryptographic standards for the CACE project are:

- X9.30:1 The Digital Signature Algorithm
- X9.30:2 The Secure Hash Algorithm
- X9.31 Digital Signatures Using Reversible Public Key Cryptography
- X9.42 Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
- X9.52 Triple Data Encryption Algorithm Modes of Operation
- X9.62 Elliptic Curve Digital Signature Algorithm (ECDSA)
- X9.63 Key Agreement and Key Transport Using Elliptic Curve Cryptography
- X9.80 Prime Number Generation, Primality Testing, and Primality Certificate

## 2.1.4 ETSI

The European Telecommunications Standards Institute (ETSI) is recognised by the European Commission as an European Standards Organisation. It produces standards for Information and Communications Technologies (ICT), namely for the mobile communications arena, although not all documents are in the public domain. Some of the most relevant standards for the CACE project are the following:

- ETSI Algorithms (DECT Standard Authentication Algorithm, DECT Standard Encryption Algorithm, etc.)
- 3GPP TMCon\_dentiality and Integrity Algorithms (UEA, UIA, KASUMI, etc.)
- DVB Common Scrambling Algorithm (CSA and CSA3)
- A5/3 encryption algorithms for GSM and EDGE
- GEA3 encryption algorithm for GPRS

#### 2.1.4.1 **SAGE expert group**

Nokia, the biggest industrial partner in the project is a member of the Security Algorithms Group of Experts (SAGE) within the ETSI organisation. This group is responsible for creating ETSI reports (containing confidential specifications), draft I-ETSS and ETSS in the area of cryptographic algorithms and protocols specific to fraud prevention/unauthorised access to public/private telecommunications networks and user data privacy.

If the CACE consortium decides that project results would be relevant for any reports developed within this experts group, Nokia will take care of the necessary process.

### 2.1.5 IEEE

The Institution of Electrical and Electronic Engineers (IEEE) also publishes standards related to cryptography, the most relevant of which are those under P1363 Standard Specifications for Public-Key Cryptography that are described as a reference for specifications of a variety of techniques from which applications may select. The maintained standards are:

- P1363 Traditional Public-Key Cryptography
- P1363.1 Lattice-Based Public-Key Cryptography
- P1363.2 Password-Based Public Key Cryptography
- P1363.3 Identity-Based Public Key Cryptography using Pairings

#### 2.1.5.1 **IEEE P1363 Working Group**

The University of Bristol is involved in the P1363 working group within IEEE, which in addition to continued work on the above projects accepts contributions and discusses issues related to these and other types of public key cryptography that may be relevant to future standards projects.

In this context the University of Bristol could discuss CACE contributions with the group in case of relevant project results.

### 2.1.6 IETF

The Internet Engineering Task Force (IETF) develops and promotes internet standards, namely transposing to the internet context some of the telecommunications standards published by the International Telecommunications Union (ITU). The IETF maintains a series of important Requests For Comments (RFC) and Internet Drafts related to the use of cryptography in internet technologies. The most relevant of these documents are published by the following working groups within the IETF security area:

- Transport Layer Security
- S/MIME Mail Security
- Public-Key Infrastructure (X.509)
- Kerberos
- Secure Shell

#### 2.1.6.1 **IETF - Security Area**

The Internet Engineering Task Force is divided into certain areas and further into different working groups. For the CACE project the IETF area applicable is the Security Area, covering all the above mentioned working groups.

IETF in general 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. It is open to any interested individual. Nokia is one of the members in this community. In the framework of the CACE project Nokia is in the position to take care of contributing proper CACE results to adequate IETF working groups within the security area.

## 2.1.7 PKCS

RSA Laboratories maintain the Public Key Cryptography Standards (PKCS), which aim to contribute to the standardisation of cryptographic techniques by laying down specifications that can be used by early adopters. Many of these specifications subsequently make their way into other norms. The most relevant documents published by RSA Laboratories for the purpose of the CACE project are:

- PKCS #1 RSA Cryptography Standard
- PKCS #3 Diffie-Hellman Key Agreement Standard
- PKCS #5 Password-Based Cryptography Standard
- PKCS #13 Elliptic Curve Cryptography Standard

## 2.1.8 Common Criteria

The Common Criteria (CC) is a multi-part standard that serves as a shared framework for the evaluation of security properties of IT products. It provides a common set of requirements for the security functionality of IT products (hardware, firmware or software) and for the applicable assurance measures. Relevant Protection Profiles for the CACE project include:

- Secure Signature-Creation Device
- Cryptographic Module for CSP Signing Operations
- Smartcard embedded software
- Public Key Enabled Applications

## 2.1.9 SECG

The Standards for Efficient Cryptography Group (SECG), an industry consortium, was founded in 1998 to develop commercial standards that facilitate the adoption of efficient cryptography and interoperability across a wide range of computing platforms. The SECG represents the first standards organisation that is devoted exclusively to developing standards based on Elliptic Curve Cryptography (ECC). Where standards already exist, SECG may promote a refined, peer-reviewed profile of the broader standard to promote adoption and interoperability since one of the goals of the SECG is to support the ANSI, IEEE, IETF and ISO standards organisations in their development of advanced cryptographic standards and wants to facilitate interoperability of today's commercial cryptographic solutions .

University of Bristol is a member of the SECG and is contributing to the ECC Standards development process.

## 2.1.10 TCG

The Trusted Computing Group (TCG) is an international industry standards group. The TCG develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and implementation by the industry.

The TCG publicizes the specifications and uses membership implementations as examples of the use of TCG Technology. The TCG is organised into a work group model whereby experts from each technology category can work together to develop the specifications. This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.

The two industrial partners Nokia and Sirrix are both TCG contributor members and are actively involved in the work done within TCG. If CACE achieves results, which could be relevant for the TCG both partners could promote the adoption of these results into TCG specifications.

### 2.1.11 TeleTrusT

TeleTrusT was founded in 1989 as a non profit association to promote the trustworthiness of information and communication technology in an open systems environment. Accordant to the demands of the every day practice TeleTrusT supports the area wide implementation of data encryption as well as Identification, Authentication and Signature (I-A-S) in eBusiness applications within industry and administration. In this connection the conformity of standards plays a decisive role as a foundation for interoperable Hard- and Software as well as for services.

Together with institutions from other countries TeleTrusT works on harmonising aims and standards within the European Union. Of particular concern is a technical and organisational security that is appropriate for the concrete application context.

The CACE partner Sirrix is heavily involved in this standardisation body. They support the association with core competencies in the area of Trustworthy Computing, provable security functions and open systems and offer them their experience and technological know-how in cryptography and information security. Sirrix and furthermore the CACE consortium can benefit of the technical know-how of all the other members regarding research, development and public management.

## 2.2 Synergies with the EC Project ECRYPT

In the first 12 months, CACE has worked towards the strategic goal of supporting Security Critical ICT Projects mainly through informally collaborating with ECRYPT (European Network of Excellence in Cryptology), which is a network of excellence in FP7, on the project eBACS benchmarking efficient software. This helped CACE to systematically study the speed of the implementation of the easy-to-use high-speed software library NaCl. In particular the API development was coordinated and the fast AES implementations using qasm were integrated into the eBACS benchmarking.

Since three of the CACE partners are also partners in the ECRYPT project the synergy between the projects is guaranteed.

## 2.3 Standardisation until M18

One of the goals of the CACE project is to widely disseminate the results at different levels and to different communities in order to spread the culture and technologies in the field of design. One aspect for such dissemination is a set of standardisation working groups whose activities are put in relation with the knowledge developed in CACE. The activities in the field of standardisation have been performed at different levels: creation of formal liaisons between already existing bodies and the CACE consortium, direct participation in existing bodies, or by interaction with members of existing bodies.

Cryptographic research, including that supported by the EU via projects such as NESSIE, ECRYPT and to a lesser extent SCARD, traditionally produces outputs that are primarily of academic interest. A strategic objective of the CACE project is to enable knowledge transfer from such results into tools usable directly by non-expert software engineers.

CACE has worked towards this strategic objective together with the project partner NOKIA and through the very useful input of the industrial Advisory Board (HP, IBM, Intel and Philips) The intensive joint work with NOKIA was very fruitful and CACE has received valuable input from an industry perspective. For instance, NOKIA put together a list of "desirable" features for the tools that will implement cryptographic primitives with respect to performance and security. Based on the input from NOKIA, CACE partners investigated the role of signature schemes with subliminal channels. These inputs are vital for designing secure mobile platforms given the fact that mobile and embedded computer systems are increasingly used in the context of security critical applications. Furthermore, NOKIA delivered a Nokia N810 Internet Tablet to a CACE partner, and assisted with software development tools and performance metrics on N810 in order to harness the qasm tool on this platform. To support evaluation, NOKIA wrote generic elliptic curve cryptography (ECC) code that is tested with NIST P256 curve parameters. The implementation is based on IEEE P1363 working group specification, and uses Montgomery arithmetic in order to avoid patents concerning the usage of generalised Mersenne primes. All the code except the underlying prime field arithmetic is written from

scratch. The idea is to use this as a benchmark against which the output from CAO and qhasm can be compared.

Overall, at the beginning of the project the partners involved in standardisation bodies were in charge to take care, that current standards were considered in the requirements and design process. Actually this task of monitoring relevant standards for CACE is a continuous task of all partners involved in standardisation bodies, since this is essential to guarantee the up-to-dateness of the project.

In the first project year some efforts have been spent in order to locate and document a wider range of cryptography standards which could be relevant for CACE. The Deliverable D5.1 called 'Security Policies for Cryptographic Software' has been created within WP5 (Formal Verification and Validation). It included one chapter dedicated to Security and Cryptography Standards. There an analysis of the security properties of cryptographic software that may stem from the need to adhere to a particular standard was made. The analysis concerned two parts, on the one hand the common security requirements that arise when a developer has to transpose the specification of a cryptographic algorithm or protocol from a standard document into a software implementation, and on the other hand the security requirements that may arise when the goal of the developer is to obtain a certification that the software product provides a standardised level of assurance.

## ***2.4 Standardisation plan***

Standardisation is one of the key elements to ensure our projects long term technological impact. Future intermediate results, which are gained throughout the project and which could be relevant for certain standards will be processed and fed into the relevant standardisation bodies by the respective consortium members.

A tight relation to other industry developments can furthermore be ensured for the rest of the project through the consortium members and the Advisory Board (HP, IBM, Intel and Philips).

Influencing standardisation activities will be achieved through the CACE project partners. In fact many of them have strong and active links with relevant specification and standardisation bodies as can be seen in chapter 2.1.

### 3 Conclusion

This deliverable defines the midterm standardisation plan for the CACE project. The main objective of this document is to provide the reader with a brief overview of the standardisation topic within CACE. On the one hand it explains the importance of considering standardisation aspects within the project and on the other hand it describes all relevant standardisation bodies and lists potential standard documents.

All in all it can be said that the CACE project is clearly dominated by universities, therefore the involvement in several standardisation activities is not as high as with projects where lots of industrial partners are represented. Even though the percentage of industrial partners directly involved in the project is not so high, the industrial involvement in the project is assured through the support of an Advisory Board (HP, IBM, Intel and Philips).

Until now all defined project objectives have been successfully achieved and finished and the CACE project made excellent progress and is consistent with the original planning. Therefore also the standardisation plan is in line with the original planning. In case relevant results for any standards evolve within CACE they will be delivered to the appropriate standardisation body / working group by the partner involved with this organisation.

Furthermore, through close cooperation with industrial partners inside and outside the CACE consortium its results and benefits will be introduced to the relevant industry as well as to standardisation bodies.

## 4 List of Abbreviations

ANSI	American National Standards Institute
CC	Common Criteria
CSA	Common Scrambling Algorithm
DECT	Digital Enhanced Cordless Telecommunications
DVB	Digital Video Broadcast
eBACS	ECRYPT Benchmarking of Cryptographic Systems
ECC	Elliptic Curve Cryptography
ECRYPT	European Network of Excellence in Cryptology
EDGE	Enhanced Data Rates for GSM Evolution
ETS	European Telecommunication Standard
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
ICT	Information and Communications Technologies
IEC	International Electrotechnical Commission
IEEE	Institution of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
I-ETS	Interim European Telecommunications Standard
ISMS	Information Security Management Systems
ISO	International Standards Organisation
ITU	International Telecommunications Union
KASUMI	Cryptography Algorithm used in 3G Mobile Networks
NESSIE	New European Schemes for Signatures, Integrity and Encryption
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standards
SAGE	Security Algorithms Group of Experts
SCARD	SCA Resistant Design
SECG	Standards for Efficient Cryptography Group
TCG	Trusted Computing Group
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm

## 5 References

- [01] <http://www.rsa.com/rsalabs/node.asp?id=2160>
- [02] <http://grouper.ieee.org/groups/1363/>
- [03] [http://portal.etsi.org/portal\\_common/home.asp?tbkey1=SAGE](http://portal.etsi.org/portal_common/home.asp?tbkey1=SAGE)
- [04] <http://www.secg.org/>
- [05] <http://www.jtc1sc27.din.de/cmd?level=tpl-home&contextid=jtc1sc27>
- [06] <http://www.teletrust.org/>
- [07] <http://www.ietf.org/>
- [08] <http://www.trustedcomputinggroup.org/>
- [09] <http://www.3gpp.org/>