Study on the use of cryptographic techniques in Europe

[Deliverable – 2011-12-19]

Updated on 2012-04-20

Contributors to this report

Authors:

- Edward Hamilton and Mischa Kriens of Analysys Mason Ltd
- Rodica Tirtea of ENISA

Supervisor of the project: Rodica Tirtea of ENISA

ENISA staff involved in the project: Demosthenes Ikonomou, Stefan Schiffner

Agreements or Acknowledgements

ENISA would like to thank the contributors and reviewers of this study.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on cryptography, please use the following details:

- E-mail: sta@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Contents

List of Tables

1 Executive Summary

The increasing use of e-government services has led to significant growth in the amount of citizens' sensitive data being transmitted over public networks (e.g. the Internet) and stored within applications that are accessible from anywhere on the Internet. Data leakage or security breaches in such systems have a direct impact on the right to privacy and may have legal implications. Moreover, citizens are exposed to financial risks, if financial information (e.g. banking details) is disclosed. Lastly, due to the quality and the quantity of data, leakages expose citizens to various risks and can cause substantial reputational damage to official bodies.

Beside other measures, the correct use of cryptography minimises certain threats and secures e-government services. This study examined the cryptographic documents and specifications defined by European Union (EU) Member States (MS) related to the encryption of unclassified information stored and transmitted by e-government services.

This study surveys cryptographic guidelines, requirements and specifications defined and used by the Member States (MS). It relies on answers received from 13 MS, covering almost 75% of the EU population; detailed answers for the questionnaire have been received from 11 countries covering more than 61% of the EU population.

Additionally, selected members of the European ICT industry have been asked to provide feedback on their experience of working with, deploying, auditing and testing MS cryptographic solutions.

The survey indicates that many cryptographic specifications/recommendations prepared and used for e-government services recommend good practice encryption algorithms. However, according to the feedback provided by IT industry, many of the cryptographic solutions that they audit and test are poorly deployed; in many cases the deployment teams for systems/services handling unclassified information are lacking cryptographic expertise. This all leads to the following findings and recommendations.

- Cryptography is continuously evolving. This is driven by increasing processing power, enabling weaker cryptographic solutions to be broken by brute force, weaknesses being identified in certain cryptographic solutions and technological advances. To overcome these challenges designers must consider the system's expected lifespan and ensure that the selected encryption algorithms have the potential to last for at least that period. Organisations must pro-actively review their encryption documents and solutions, updating them in line with the changing circumstances. Clear processes for withdrawal of compromised or algorithms, or those that are too weak, must be included in the policies.
- Many encryption policies assume that the reader has a good level of knowledge of cryptography. However, often this is not the case – especially for services handling unclassified information – and readers struggle to grasp essential information. Cryptographic guidelines need to target such a readership and need to be tailored for their

use in order to maximise the benefits. Best practice needs to be promoted; clear guidelines and policies need to be developed.

Many of the MS, the USA and Japan have government programmes and bodies to define cryptography standards, specifications and/or recommendations, which are used to secure e-government services. However, still some MS develop cryptographic recommendations for each e-government service in isolation. The authors strongly recommend bundling such efforts, at least at an MS level. Significant benefits are expected from an EU-wide initiative to specify a common minimum standard for cryptography of unclassified data in e-government services. From a long-term perspective this would not only ensure a certain level of protection for all EU citizens, but also would simplify the exchange of government data between MS – which becomes increasingly important with the increasing mobility of citizens. Providing these guidelines publicly, other stakeholders will benefit from such an initiative, for instance could bring economies of scale to the commercial market outside e-government services.

2 Introduction

Over the last decade there has been a significant migration to e-government services, with numerous government departments offering their services online. According to EUROSTAT, in 2010, in the EU 27 MS, the online availability and interactivity of public services reached 84%, up from 58% in 2007.[1] This shift in service provision has meant significant growth in the number of applications that provide services over public networks (e.g. the Internet) that are marked as 'unclassified[2]'. Just because a system is unclassified, it does not mean that there are no issues concerning IT security. Data leakage or security breaches in such systems have a direct impact on a citizen's right to privacy and may have legal implications. Furthermore, they can have a significant impact on, and cause substantial reputational damage to, official bodies. One area of security controls that can be used to minimise the threat and secure these applications is cryptography.

In its proposal for a European Digital Agenda[3], the European Commission is aiming towards "*building people's trust in using the Internet*", thereby creating conditions for the Internet ecosystem to flourish.[4] This can be achieved by safeguarding the integrity of information, protecting the source of information and protecting personal data, securing the privacy of the individuals; while protecting the underlying network infrastructure and supporting services.

The cryptographic recommendations and specifications that MS promote have a direct impact on the privacy of European citizens. When configuring encryption for instance, there are many settings, and management choices to be made, that have direct implications on the level of security and privacy that the encryption solution provides.

---

1 *Online availability and interactivity of public services (supply side) [isoc_bde15ess], Last update: 04-03-2011, available from EUROSTAT website: http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database#*

2 *The term 'UNCLASSIFIED' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed. These markings can be applied to any government assets (in UK), although they are most commonly applied to information held electronically or in paper documents. The methodology used to assess these principles within information systems is expressed in Business Impact levels. Other Member states have their own definitions of 'unclassified'. http://interim.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf-*

3 *A Digital Agenda for Europe, COM(2010)245, May, 2010, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245%2801%29:EN:NOT*

4 *Even if according to previous footnotes, the online availability of public services is high, the percentage of population interacting online with public authorities is relatively low (41% in 2010); according to: Individuals using the Internet for interacting with public authorities [isoc_bde15ei], Last update: 27-05-2011, available from EUROSTAT website: http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database#*

2.1 Terminology

This study is structured such that a general audience can understand sections of the report (Sections 1, 2, 5 and 6), while significant parts of other sections (Sections 3 and 4) would benefit from an understanding of cryptography.

Background information regarding cryptography is summarised in Annex C, while a Terminology and Abbreviations list is provided in Annex D. Furthermore, there are numerous books, (a small selection is outlined in a footnote[5]) and online books[6], which the reader could refer to for a wider understanding of cryptography.

2.2 Scope

This study investigated the cryptographic specifications and recommendations used by governments to protect unclassified data. 'Unclassified' is the lowest level of government protective marking. This study does not cover the use of cryptography to protect classified information.

2.3 Methodology

In undertaking this study, the business requirements for communicating and holding unclassified data were examined. For this purpose three core categories of information exchange and storage requiring cryptographic techniques were identified:

- communications between citizens and their governments, typically using web services
- data being shared between government bodies across public networks (e.g. the Internet)
- unclassified data being stored within publicly accessible web applications, which because of the aggregation of stored data could have a significant impact on governments if a security breach was to occur (for example, reputational damage from an unclassified web service being compromised).

To undertake this study, a survey has been prepared: The authors identified the key government bodies responsible for the definition of cryptographic documents for protecting unclas-

---

[5] *Some books are listed here, ordered, from basic introduction to advance level: Cryptography: a very short introduction, Fred Piper & Sean Murphy, ISBN-10: 0192803158, ISBN-13: 978-0192803153; Cryptography for Dummies, Chey Cobb, ISBN-10: 0764541889, ISBN-13: 978-0764541889; Cryptography engineering: Design, Principles and Practical Applications, Niels Ferguson, Bruce Schneier & Tadayoshi Kohno, ISBN-10: 0470068523, ISBN-13: 978-0470068526*

[6] *Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press, ISBN: 0-8493-8523-7, October 1996, 816 pages, rePrinting August 2001, available at: http://www.cacr.math.uwaterloo.ca/hac/; Cryptography, An Introduction (Third Edition,2011) Nigel P. Smart, available at: http://www.cs.bris.ac.uk/~nigel/Crypto_Book/*

sified data within EU MS, and requested that they complete the survey. In parallel, we contacted a range of IT service organisations across the EU to obtain their opinion regarding the experience with government bodies when implementing/testing/auditing/consulting e-government cryptographic solutions.

2.4 Limitations

This study relies on the responses provided by experts and contacts from EU MS on a voluntary basis to our questionnaire. In a number of countries, the agencies maintaining cryptographic specifications for the use in the context of classified information are also providing guidelines/recommendations for the use of unclassified information; experts from some MS avoided discussing the cryptographic specifications for unclassified information.[7]

2.5 Target audience

The intended audience for this report includes policymakers and e-government departments defining national and departmental documents on the subject of cryptography.

This report is also of interest to organisations designing, implementing and utilising online services that require cryptography and which wish to educate themselves about the practices of their peers with regard to cryptography.

2.6 Short overview of findings

Outlined below is an overview of the core findings of this study.

- Some policies allow the use of encryption and signature algorithms that are considered to be weak by experts in the cryptographic community.
- A relatively large number of MS recommendations allow the storage of encryption keys within the operating system of a device. If the security of the device is compromised the key can be extracted easily and used to decrypt the data.
- Many documents treating the subject of encryption assume the reader has a good level of cryptographic knowledge, however, often teams developing solutions lack experts in cryptography (when developing services for unclassified information).

---

[7] *Some respondents indicated as classified information, according to their policies, some specific cryptographic settings used to protect unclassified data and cover by our questionnaire.*

It should be noted that in 2003 the US government has announced that AES (Advanced Encryption Standard) can be used for classified, secret and top secret data (http://csrc.nist.gov/groups/STM/cmvp/documents/CNSS15FS.pdf). This is a significant step in the area supporting the fact that algorithms to protect classified data need not be classified themselves.

- Good cryptographic solutions not only consist of technology, but also of a set of processes. Many of the solutions that are currently being deployed do not have the appropriate level of supporting processes.
- Cryptography is continuously developing. Weaknesses are identified in cryptographic algorithms every day and the processing power of IT systems is continuously improving. This means that cryptographic algorithms that were once considered secure may no longer be secure in practice.
- Some government bodies appear to be developing cryptographic policies in isolation. Many MS, the USA and Japan have government programmes to define cryptography standards and recommendations.

2.7 Structure of the study

This sub-section outlines the structure of the study. This report is laid out as follows:

- Section 3 – a presentation and analysis of the results of the surveys
- Section 4 – an overview of the cryptographic specifications (and how they are developed and maintained) outside the EU and some initiatives at EU level
- Section 5 – concluding remarks
- Section 6 – our recommendations
- Section 7 – references.

The report includes a number of annexes containing supplementary material:

- Annex A includes the most relevant cryptographic specifications in MS (based on the survey); the standards which were mentioned in the answers to the questionnaires; and some recommended standards (based on the industry interviews)
- Annex B is a summary of the commonality of the cryptographic specifications outlined in the survey
- Annex B list the questions from questionnaire addressed to MS bodies and from the interviews with industry experts
- Annex C provides background information regarding cryptography
- Annex D lists the terminology, abbreviations and references used within this document with a description.

3 Survey results

The survey consisted of two core parts: the primary part, a questionnaire sent to a wide range of government departments across MS that are involved in designing and implementing unclassified government services, such as e-government, telemedicine, e-procurement and e-identity. The secondary part supported the investigation and consisted in conducting interviews with cryptographic specialists working in organisations providing services to EU governments.

Three different types of process and service have been considered within this study:

- secure access for citizens to web services
- encrypting communications between servers
- encrypting data within applications.

This section of the report provides a breakdown of the results of the survey, and provides recommendations to improve security practices.

The survey defined four areas of interest:

- **general information** regarding the information sources that are used to define an organisation's cryptographic policy
- the type of cryptographic tools used **to protect network traffic between citizens' PCs and e-government applications**
- the cryptographic techniques recommended for **protecting data stored within e-government applications and databases**
- the cryptographic techniques used to **protect network communications between servers,** e.g. the exchange of data between two different departments.

Each MS was contacted to request their participation in this study. Outlined in Figure 3.1 is a graphical representation of the MS who responded to this study.

ENISA received information from 13 countries consisting of 74.9% of the EU population.[8]

Outlined in the sections below are the core findings of the survey:

- From Sub-section 3.1 to 3.12 inclusive, the content and analysis rely on the answers received, based on the questionnaire, from the countries where encryption policies have been identified (covering 61.3% of the EU population)
- Sub-section 3.13 covers the responses of industry experts that participated in the interviews.

[8] *According to EUROSTAT data, checked on 23.08.2011, available at: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&language=en&pcode=tps00001&tableSelection=1&footnotes=yes&labeling=labels&plugin=1*

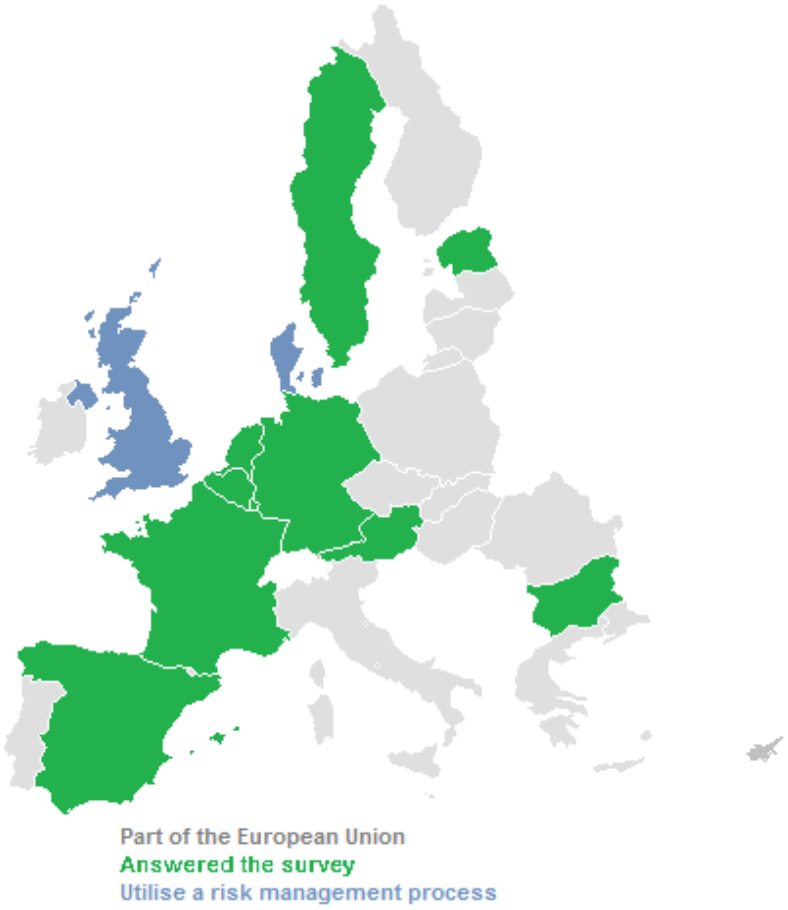

Figure 3.1: Map of participation in the study[9]

3.1 Availability of cryptographic policies

A cryptographic policy is a document that defines how a cryptographic solution should be configured and operated. Outlined, in Figure 3.2 is a representation of the survey results by population. At the time of the survey, 61.3% (by population) of European citizens' government bodies had a defined encryption policy for unclassified information, and 13.5% utilised a risk management process[10].

[9] *Based on responses received till end of October 2011. Greece provided feedback after that.*

[10] *Using such a process, local security managers decide on the most appropriate security measures for the solution they implement. For instance, in the case of UK, at the following link the risk assessment tool and process are described: http://www.cesg.gov.uk/policy_technologies/policy/risk-tool.shtml*

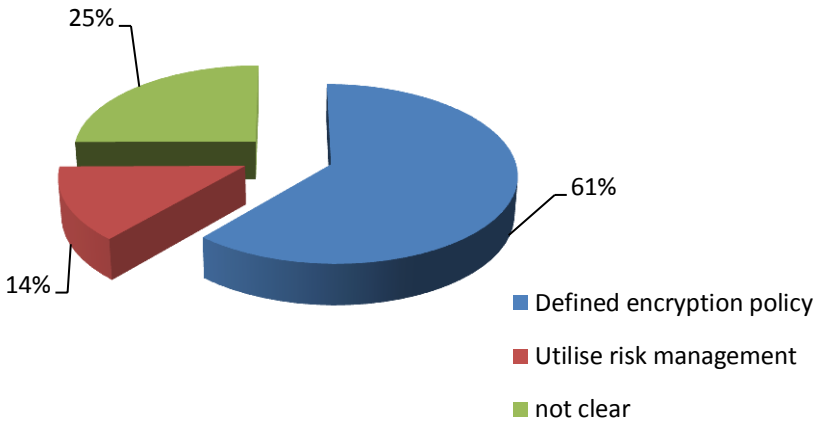

Figure 3.2: Survey results regarding encryption policies (by covered population of EU)

3.2 Surveyed cryptographic policies (by type of application)

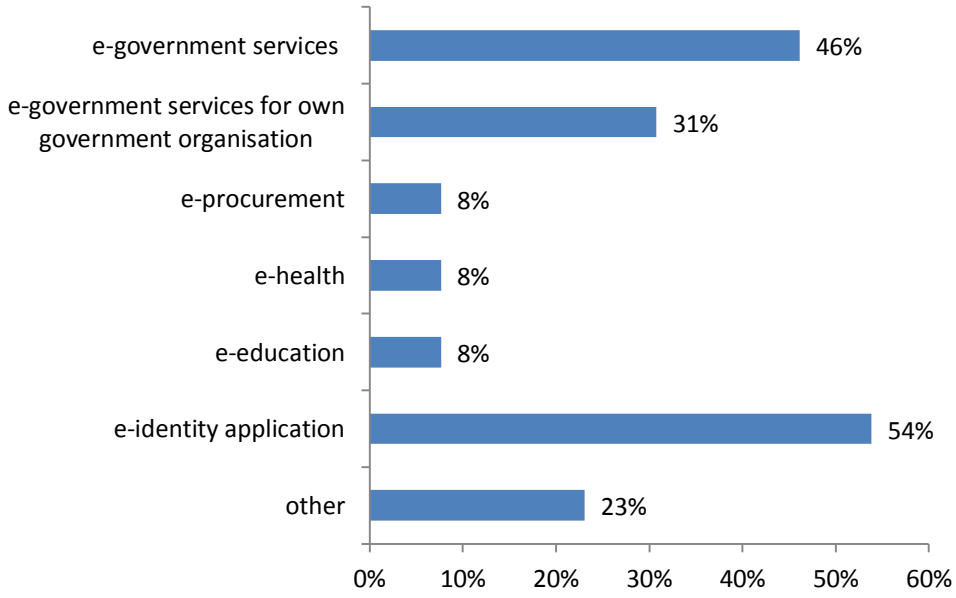

Figure 3.3: Type of application for the cryptographic policy (all that apply)

The surveyed cryptographic policies were mostly designated for e-government services and e-identity applications (46% and 54% respectively) while only some of them were addressing e-health, e-education or e-procurement. Figure 3.3 provides the answers for the question: 'what application types are you/your team/your organisation responsible for defining/implementing cryptography (select all that apply)?'

Recommendation 1 – Different governmental bodies should combine their efforts to develop cryptographic policies/recommendations, even if particularities apply for certain applications.

3.3 Data recommended to be encrypted

When and how encryption should be used is often a source of confusion. In fact, 64% of respondents to the survey stated that they recommend encrypting all data that is traversing a public network from the citizen to e-government applications.

With web applications, encrypting the whole session can cause issues in terms of web caching (of graphics and other static information) and significant slowing of page load times. However, the performance impact of encryption is decreasing through hardware improvements[11], and confidentiality of information could be compromised by partial encryption.[12] It is recommended that when deploying web services, sensitive data is encrypted while trying to maximise the performance of the application.

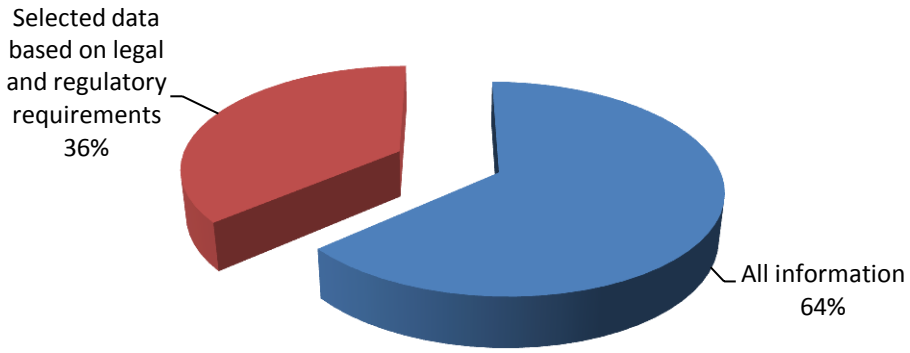

Figure 3.4: Types of data to be encrypted when transferred using public networks (from the citizen to e-government applications)

3.4 Encryption of data between the citizens and e-government services

Across Europe, numerous MS have migrated their citizen services to Internet-based applications, enabling citizens to access services by simply using a standard web browser. By default, the communication between a web browser and an application is not encrypted. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are the main encryption protocols that can be used to encrypt this type of network traffic. Within SSL and TLS there are multiple versions

[11] *For example, since 2010 Intel offers hardware AES support in its high-end processors.*

[12] *Encrypting only text and not pictures may leak sensitive information, e.g. when consulting a website with medical information even generic pictures may reveal (just like the URL) the disease for which the patient is being treated.*

and the new versions are considered more secure than the old ones. For more information regarding SSL/TLS see Annex C.

Outlined in Figure 3.5 are the cryptographic protocols that are recommended for use by respondents.

A small number of the MS still support legacy weak cryptographic protocols (e.g. SSL version 2) that are not recommended for use. It is important to note that deploying solutions utilising weak cryptography does not provide a suitable level of security.

In some MS, the cryptographic policies do not name specific algorithms as being recommended; however recommendations are made regarding key sizes. Also vulnerabilities are identified and flagged.

Recommendation 2 –MS should ensure that all new IT systems only support strong cryptography in line with good practice recommendations such as the ECRYPT[13] study and that appropriate policies and procedures are in place to upgrade the cryptographic algorithms and protocols when needed.[14]

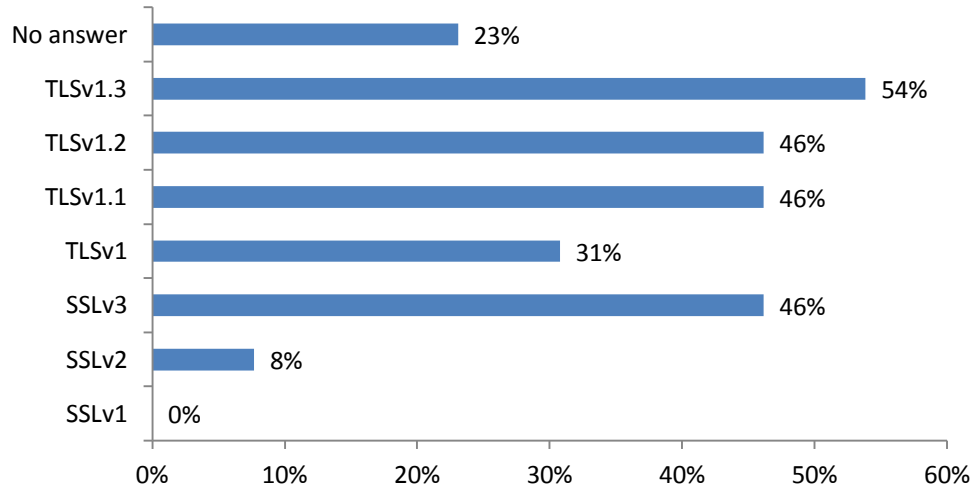

Figure 3.5: Use of SSL and TLS encryption[15]

13 *Last version, ECRYPT (European Network of Excellence for Cryptology) II Yearly Report on Algorithms and Key Lengths (2011), available at: http://www.ecrypt.eu.org/*

14 *As can be noticed later in the study, some MS use ECRYPT as a reference when developing their national recommendations.*

15 *As mentioned in the text, for certain countries the policies do not include recommendations for the use of a specific algorithm. However, references are made to parameters (i.e. key sizes) which are specified; vulnerable or weak algorithms are identified and marked as 'not recommended'.*

3.5 Encryption of data shared between government systems

As more systems are connected to the Internet and public networks, an increasing number of government systems are using these networks as a cost-effective mechanism for exchanging data. Data must be suitably protected when transmitted on these public networks. Respondents to the survey use a range of cryptographic protocols to secure the communications, as shown in Figure 3.6.

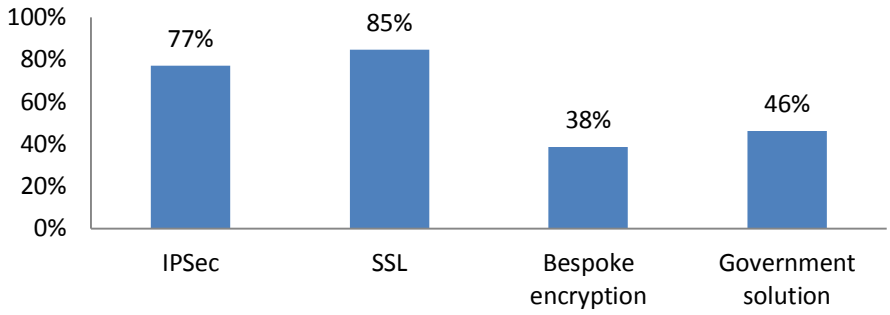

Figure 3.6: System-to-system encryption, recommended encryption solutions

For more information regarding SSL/TLS and IPSec see Annex C.

Many MS develop and use non-standard cryptographic protocols. In the past, the deployment of this proprietary cryptography has complicated the sharing of government data across national boundaries.

Recommendation 3 – In order to promote and facilitate secure cross-border communications, a common European wide cryptographic policy should be developed by EU Member States using standard cryptographic algorithms and techniques for the protection of unclassified data while at rest and in transit over networks, for the protection of data processed by applications and for the secure authentication of users and devices.

3.6 Protection of data at rest

The types of data that are protected while stored within e-government applications vary greatly from country to country, as shown in Figure 3.7.

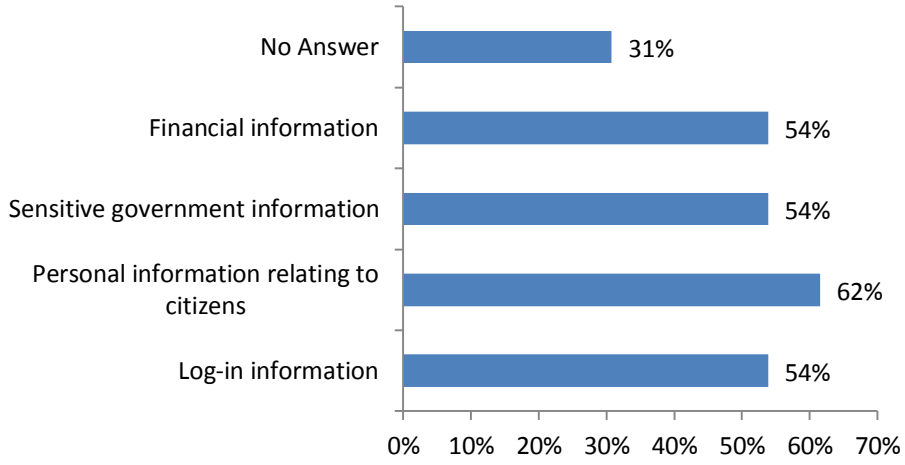

Figure 3.7: Data to be protected while stored in an e-government application

When considering what data needs to be protected using cryptographic techniques, it is essential that industry-specific regulation (e.g. health), and local and European legislation are considered.

Recommendation 4 – Government bodies and project teams should utilise an IT security risk assessment process to identify the data that needs to be cryptographically protected. This risk assessment should be updated annually to ensure that new IT security threats are identified and mitigated appropriately.

Figure 3.8 shows that mainly commercial encryption (publically available off-the-shelf) products are used by respondents to encrypt data at rest that is stored within e-government applications.

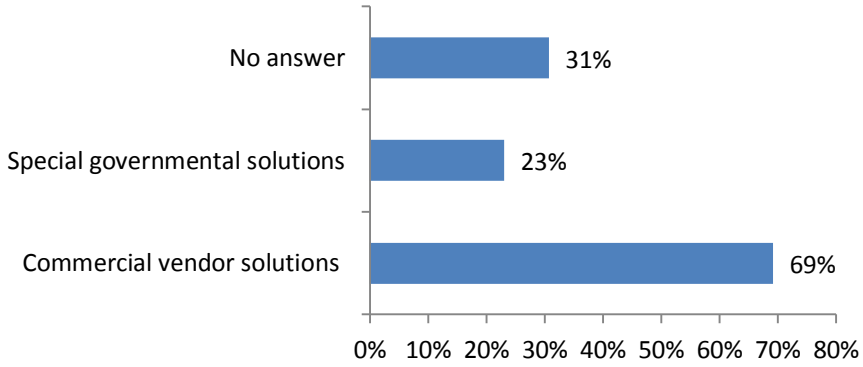

Figure 3.8: Solutions used to encrypt data at rest

3.7 Recommended cryptographic techniques

The selection of the cryptographic algorithms that make up a cryptographic solution (cipher suite[16]) is one of the most important elements to consider when designing a cryptographic solution. Mistakes in selecting cipher suite components can leave a solution open to compromise, while the selection of very robust cipher suite components could affect the performance of a system. It is essential that the correct cipher suite algorithms are selected appropriately to secure the data while at rest and in transit.

The following sub-sections outline the results of the survey regarding some of the cipher suite elements that policies recommend.

3.7.1 Key exchange algorithms

Key exchange algorithms are used to establish a common 'secret' among parties over an unsecure communication channel. This secret usually results in one or more agreed (symmetric) keys for efficient communication. Any public key encryption system can be used as key exchange protocol by encrypting a symmetric key with the public key of the recipient. Note that key exchange protocols might not provide authentication of the communication partner. Common key exchange algorithms rely on Diffie-Hellman (DH)[17] and Rivest, Shamir and Adleman (RSA).[18]

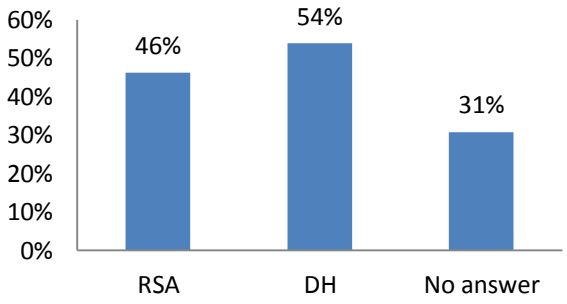

Figure 3.9: Use of protocols to secure key exchange

16 *For the case of SSL/TLS and IPSec, the cipher suite consists of four components: a key exchange algorithm, a digital signature algorithm, a data encryption algorithm, and a data integrity algorithm. Storage applications do not need a key exchange algorithm; in some settings one may only need a suite consisting of a digital signature algorithm and a hash function.*

17 *Diffie-Hellman can be used for key establishment (but a secure key exchange algorithm also needs a digital signature algorithm and a pseudo-random function).*

18 *RSA is a mathematical primitive that can be used to design a digital signature algorithm and a public key encryption algorithm. A public key algorithm based on RSA can be used for key establishment (but much more is needed).*

3.7.2 Signature schemes

Signature schemes are used to generate electronic signatures. These are used, for example, to demonstrate the authenticity of a message: a message can be signed only by the owner of the private key of the signature scheme, but can be checked by anyone else who has access to the corresponding public key. The signed message might be a public key of another party, which is called certification. Some of the common signature algorithms are using Digital Signature Algorithm (DSA) and RSA schemes.

Figure 3.10 shows the wide range of signature schemes that European governments recommend. The majority of MS are recommending a range of signature schemes[19] . Key lengths can only be interpreted when the associated signature scheme is identified.

Recommendation 5 – MS should review their cryptographic policies to consider if it is possible to remove any recommendations supporting the use of cryptographic algorithms with serious weaknesses and cryptographic algorithms with low security levels as recommended by ECRYPT.

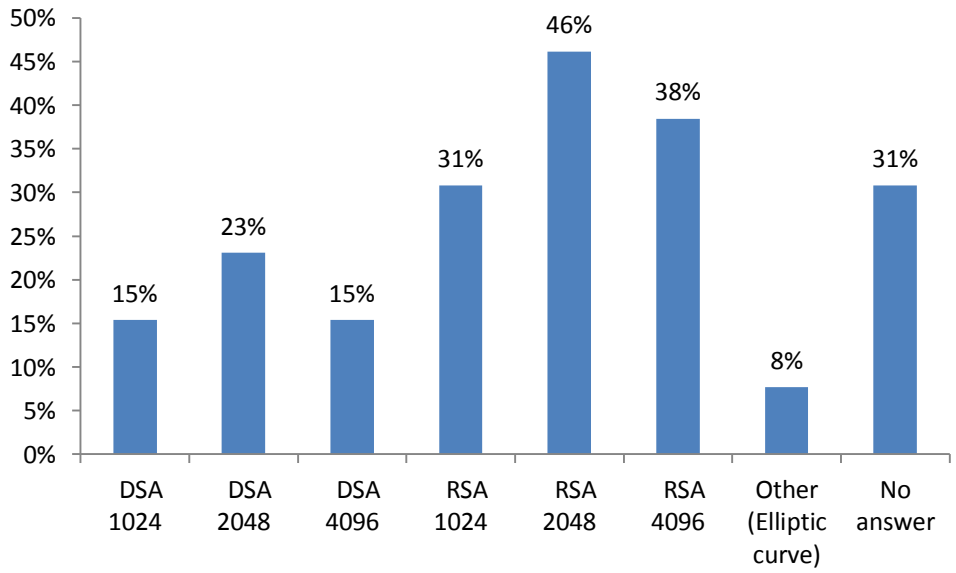

Figure 3.10: Use of signature algorithms[20]

[19] *The strength of a digital signature scheme depends on the output length of the hash function and the key and parameter lengths of the digital signature algorithm.*

[20] *As mentioned before, for certain countries the policies do not include recommendations for the use of a specific algorithm. However references are made to parameters (i.e. key sizes) which are specified; vulnerable or weak algorithms are identified and marked as 'not recommended'. Some MS are using Elliptic Curve Digital Signature Algorithm (ECDSA).*

3.7.3 Data encryption algorithms

Data encryption algorithms are the method by which data is encrypted. Well known encryption algorithms include Advanced Encryption Standards (AES) and the currently weaker Data Encryption Standard (DES).

As outlined in Figure **3**.11, 77% of the survey respondents recommend using AES 256. Encouragingly, no organisations recommended using the encryption protocols that are commonly considered as broken, namely DES 40 and 56.

However, within some commonly used applications and devices, it is common for the weaker encryption algorithms to be enabled by default.

Recommendation 6 – It is recommended that all weak encryption algorithms which are not recommended anymore by relevant authorities in the field[21] (as in recommendation 5) should been disabled on all government services and applications.

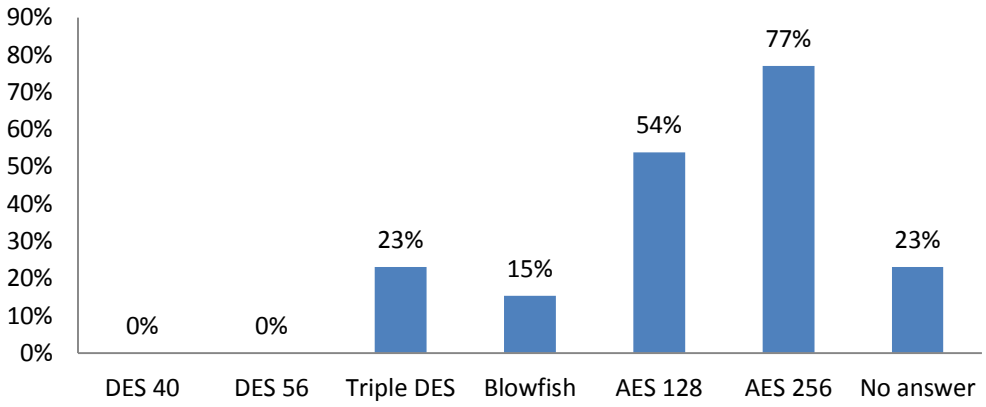

Figure 3.11: Recommended encryption ciphers[22]

Modes of operation[23] describe how the encryption is applied to data blocks. For ECB (Electronic Code Book) the message is divided in blocks and encryption is applied for each sepa-

[21] *Examples are notional or international bodies and their publications, some mentioned in Annex A.*

[22] *At the moment the questionnaire was developed we made no differentiation between existing 2-key Triple-DES and 3-key Triple-DES. However, it should be noted that NIST has withdrawn its support for 2-key Triple-DES (more information is available at: http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf), after previous withdrawal of its support for DES in 2005 (available at:. http://csrc.nist.gov/publications/fips/05-9945-DES-Withdrawl.pdf)*

[23] *For further information on performance and error propagations etc. please refer for ECB, CBC, CFB, OFB and CTR to NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, published in 2001, available at: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf*

For XTS mode to NIST SP800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, published in 2010, adding XTS-AES mode, available at http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

rately. The other modes are used to generate different encryption result when the same key is applied to a combination of clear text blocks. Cipher Block chaining (CBC) for example renders the encryption of block n dependent upon the previous n-1 blocks, which means that blocks of ciphertext cannot be decrypted on an individual basis. ECB mode does not hide patterns. Regarding the modes of operation used with block algorithms in MS cryptographic policies, ECB is not recommended; CBC, OFB (Output Feedback) and CFB (Cipher Feedback) are recommended by 62% of the respondents; CTR (Counter Mode) is recommended by 38% and XTS by 15%. 38% of participants in the survey do not make recommendations on modes of operation.

3.7.4 Hash functions

A cryptographic hash function takes a possible unbounded amount of data and calculates a digest of fixed length, called a hash. For a good hash function it is very efficient to calculate the hash of a given message, but hard to find a message given a hash (this is the concept of a 'one-way function'). Hashes are essential for practical signature schemes since signature algorithms make assumptions about message size and statistical properties, which are not valid for natural messages. Furthermore, hash functions are used to build Message Authentication Code (MAC) algorithms, which are used for data integrity. These are symmetric mechanisms, i.e. the same key is used to check and generate a MAC. These schemes are very efficient and can be used to detect if a message was altered on the network or on the drive. Well known hash functions are the Message Digest Algorithm (MD5) and the Secure Hash Algorithm (SHA).

As outlined in Figure **3**.11, 85% and 69% of the survey respondents recommend using SHA2-256 or SHA2-512respectively, with 15% of surveyed organisations allowing the use of SHA-1.[24]

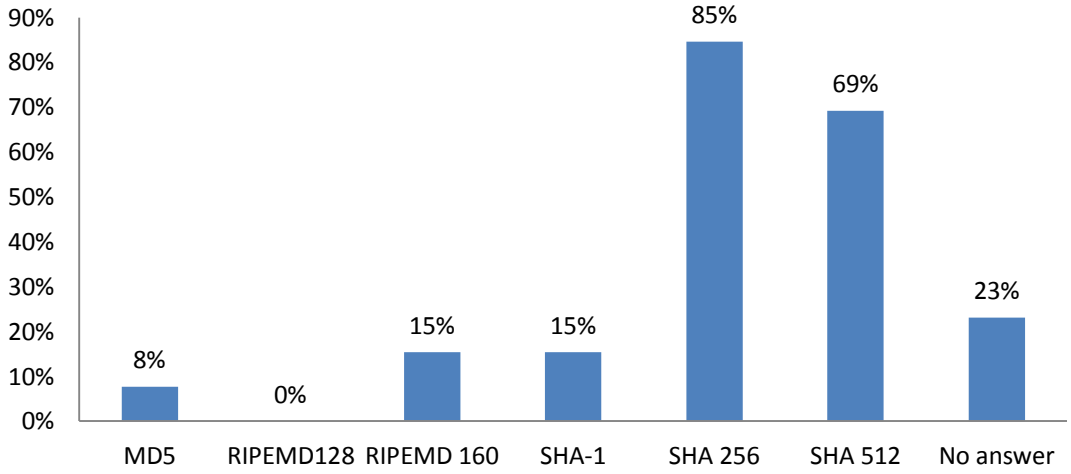

Figure 3.12: Hash algorithms recommended

[24] *SHA-1 should no longer be used in a digital signature scheme.*

The findings from the survey demonstrate that the majority of governments are promoting the use of the stronger, good practice hash algorithms. Where no specific algorithm is recommended, recommendations include information regarding minimum accepted length of hash.

3.8 Consistency of cryptography specifications

To obtain a comprehensive understanding of the cryptographic specifications that are used across Europe, ENISA approached a range of government bodies that have migrated some of their provision of services to unclassified web services on the Internet.

Where ENISA received multiple responses from a country, we expected to see cryptographic standards with each government body referencing national standards. However, this does not appear to be the case. Government bodies appear to be developing cryptographic policies in isolation.

Recommendation 7 –When a government body is defining cryptographic recommendations for the provision of unclassified services, it should discuss with its e-government department whether or not a national specification or a specific good practice guide already exists.

3.9 Key management

Key management does not seem to be well addressed according to the results of our survey.

There should be separate specifications for key management including key generation, key storage, key establishment, key archiving and key deletion.

Based on the feedback provided by IT industry (section 3.13), in practice, the majority of cases where encryption has been compromised involve the compromise of encryption keys (i.e. use of vendor default or weak pre-shared keys), rather than attackers breaking the encryption itself.

According to the survey, 77% of respondents used certificates[25], pre-shared keys[26] are used by 23% (some of them use both), and 23% did not provide an answer.

Once certificates are being used, it is essential that the signing keys of the signing authority are appropriately secured. In one interview with an IT auditor, it was suggested that it is very common to find such keys stored within the operating system. To secure keys, there are spe-

[25] *A certificate is a small file which is created by a certificate authority and contains: the identity of the certification authority issuing it, names or identifies it's who or what it belongs to , public key to identify who or what the certificate belongs to, its operational period of use, and is digitally signed by the certification authority issuing it.*

[26] *A pre-shared key can be distributed manually or with a key distribution device, e.g. a USB stick or a smart card. Pre-shared keys for AES-256 can consist of 256 random bits.*

cialist devices that can be used such as Hardware Security Modules (HSMs) and smart cards. Both these devices are highly secure and provide the keys with significant protection.

The results from the survey (Figure 3.13) support such comments, with 23% of specifications allowing keys to be stored within operating systems.

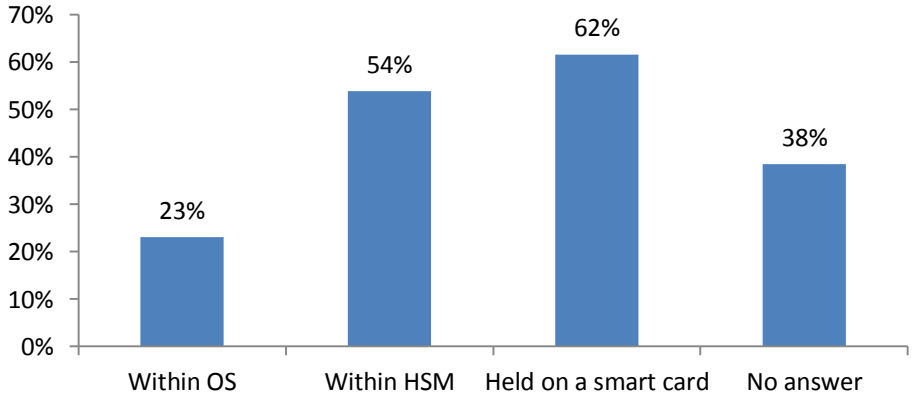

Figure 3.13: Storage of encryption keys

Recommendation 8 –Key management should be part of cryptographic specifications. For sensitive applications, sensitive keys (shared secret keys, private decryption keys, signing keys) must not be stored within the operating system. The use of tamper-resistant cryptographic hardware such as HSMs and smart cards should be promoted.

3.10 Auditing

Auditing and security testing is essential to ensure that the cryptography is configured in line with the adequate cryptographic documents, and that any weaknesses, default settings, or misconfigurations are identified and removed.

All of the survey respondents reported having well defined, robust auditing and testing of the configuration of their cryptographic solutions.

3.11 Maintaining policies and guidelines

The world of cryptography is changing quickly, virtually every day new vulnerabilities are found, most of which are revealed by the academic community; however, as the BEAST[27] vulnerability showed, they might also have an impact on widely used protocols. Thus policies and guidelines need to be reviewed regularly.

[27] *Browser Exploit Against SSL/TLS, About it (BEAST) – see 'Hackers break SSL encryption used by millions of sites', http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/*

All the survey respondents stated that they regularly review their cryptographic policies to ensure that they are in alignment with good practice. Typically, this review originated from their incident management process, taking information that is available from their national Computer Emergency Reponses Team (CERT) and other sources (such as ECRYPT[28]) to identify new weaknesses in the cryptographic solutions and their configurations.

Recommendation 9 –Each year, government organisations should undertake a comprehensive review of their cryptographic policies, to ensure that the latest research and new cryptographic developments have been taken into account. Additionally government bodies should be continuously identifying and reviewing the latest security vulnerabilities to identify any potential cryptography threat.

3.12 Information resources used for defining recommendations and policies

To ensure consistency in the deployment of cryptography, it is essential that each country defines a cryptographic policy regarding the minimum level of acceptable security. Figure 3.14 illustrates the breadth of information sources that are used to create these cryptographic policies.

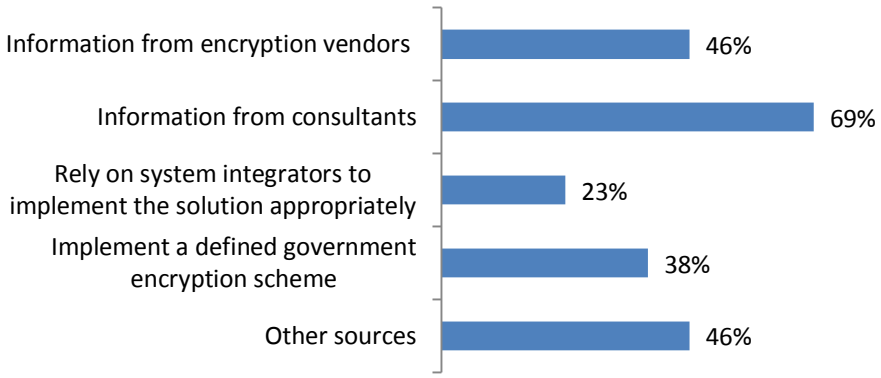

Figure 3.14: Information sources uses in defining cryptographic policies

Two thirds of the 'other sources' responses are covered by in-house expertise driven by continuous monitoring of the state-of-the-art in the field.

Using this wide range of sources ensures that a cryptographic policy is well thought through and that it covers the diverse range of topics that need be considered when defining cryptography documents.

[28] *http://www.ecrypt.eu.org/index.html*

3.13 Perceptions of the IT industry

After seeing in previous sections the responses and the findings from the questionnaire addressed to e-Government bodies, this section looks at the perspective of the IT industry, which is working with MS cryptographic specifications, and deploying, auditing and testing MS cryptographic solutions. The findings of this section rely on interviews with six experts[29]: two from organisations providing cryptographic products and services[30], two from system integrators[31], one consultant and one expert in testing cryptographic solutions.[32]

3.13.1 General level of expertise and knowledge of specific standards

All interviewees recognised two levels of knowledge and expertise within government organisations regarding cryptography: when working on highly secure systems with elevated protective markings, the level of knowledge was outstanding; while on unclassified systems (the focus of this study), the general level of knowledge was regarded as being generally poor.

Recommendation 10 –Project teams implementing unclassified solutions must ensure they have access to appropriately skilled cryptographic resources to enable the cryptography solution to be deployed in line with relevant policies and within good security practice.

In the opinion of the IT industry experts interviewed, there is generally a good awareness of international cryptographic standards, especially when related to a product.

The understanding of specific, country-level cryptographic standards appears to be directly related to the experience of the project team and the previous projects on which they have worked.

Recommendation 11 –MS should promote their cryptographic policies within all relevant government departments. Specific guidance should be developed for a range of target audiences (for example, project managers and solution architects) to assist these audiences in understanding when and how cryptography should be deployed and what is appropriate.

29 *The experts provided their opinion anonymously.*

30 *Both organisations have more than 20 years in industry, with global markets and more than 100 employees.*

31 *The organisations have more than 12 years of experience with EU governmental bodies and are based in Europe.*

32 *The two experts, both have more than 20 years of experience with commercial and governmental products.*

3.13.2 How cryptographic parameters are selected

Interviewees suggested that in many circumstances, the architect designing the solution cannot identify the relevant government standard to use, and in these circumstances it generally appears that the cryptographic configuration depends on:

- information available on the Internet or coming from equipment suppliers (e.g. technical whitepapers from vendors on how to configure cryptography for the device or software)
- the default configuration
- selecting the latest version or the largest number (e.g. SHA2-512 over SHA2-256 over SHA-1) for each of the cipher suite options.

Recommendation 12 – It is recommended that government bodies pro-actively promote cryptographic documents with clear guidance on who to approach for further advice and assistance.

3.13.3 Common errors in the configuration of cryptography

The most common fault that the interviewees identified was the lack of any key management process or procedures. The use of vendor default or weak pre-shared keys is a common mistake that is made. This leads to weak cryptographic keys being used and those keys not being appropriately secured, which is mainly due to the lack of a suitable certificate solution or budgetary constraints preventing the design and deployment of a suitable certificate solution.

Another area of concern that was identified by the interviewees was in the use of vendor guidance, with some users following the provided guides step by step and command by command, without actually understanding what they are configuring. Vendor guidance is primarily provided to enable the configuration of the solution. By following vendor guidance the solution will often work and protect data, but the cryptographic techniques that have been configured may include weak ciphers.

Recommendation 13 – It is recommended that government bodies designing and deploying cryptographic solutions ensure that basic cryptographic training is available, explaining the basics of cryptography and its importance in ensuring citizen privacy. In addition, they should ensure that specialised cryptographic expertise is available to verify that all recommendations and implementations are in line with the latest research developments

For a non-cryptography expert, working through the various standards available on the Internet is very complex and challenging. It is very hard for somebody who is trying to configure a system to understand how these various cryptography algorithms, ciphers, keys and hashing techniques work together to enable the relevant data to be protected.

The consequence of not utilising specialised trained staff is that the cryptographic solution is deployed, but the level of protection that it provides is variable. Tasks such as defining the key management processes may not have been completed, making the solution considerably more complex to manage and upgrade.

> *Recommendation 14 – It is recommended that clear and concise cryptographic guidance is developed and made freely available. This guidance must explain the elements of a cipher suite, the appropriate algorithms and the correct cipher suite configurations for specific situations e.g. a citizen accessing a government website, data at rest, etc.*

This guidance should be in a format that those implementing different solutions can understand, explaining how cryptography is configured within applications and devices. It should be targeted at technical staff, but taking into account that they may have limited knowledge of cryptography.

Within many training courses organised by vendors, the basics of symmetric and asymmetric cryptography are taught. What is not taught is what constitutes a good cipher suite.

> *Recommendation 15 – It is recommended that the MS consider developing training courses to train technical specialists in configuring strong cryptographic solutions and managing them.*

3.13.4 What should European governments do to improve the deployment of cryptography?

The experts that were interviewed agreed that there needs to be:

- simple, easy-to-understand guidance on deployment of cryptography, outlining what constitutes good configuration (as one interviewee stated, not everybody deploying cryptography will have a doctorate, and lack of knowledge of cryptography can lead to serious problems)
- a promotion of the fact that cryptography is not just about the initial configuration, but also about the long-term management of all the cryptographic keys.

4 Cryptographic specifications beyond MS borders

This section provides a short summary on initiatives to:

- evaluate and select cryptographic algorithms to be used for e-government services in the USA and Japan
- a range of initiatives funded by the EU.

Reference is made to global organisations and standardisation bodies. Further information is available in Annex B.

4.1 Cryptographic specifications in USA and Japan

This section provides a short summary on initiatives to evaluate and select cryptographic algorithms in the USA and Japan. Some of the standards have a global use, and when this is the case references are provided.

4.1.1 USA and NIST standards[33]

The National Institute of Standards and Technology (NIST) [34] is the US federal technology agency that works with the industry to develop and apply technology, measurements, and standards. NIST develops standards and guidelines for federal computer systems to address requirements for security and interoperability that are not covered by other industry standards and/or solutions. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS)[35]. Some examples are FIPS 140-2 (Security Requirements for Cryptographic Modules, 2001), FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems, 2004), FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems, 2006). An overview of the key FIPS cryptographic standard 140 is outlined in Annex C.

NIST opens public consultations for the selection of the cryptographic algorithms. For example, FIPS 197, Advanced Encryption Standard (AES)[36] was published in 2001 following a public competition for which NIST requested the assistance of the cryptographic research communi-

---

33 *Besides NIST there are other organisations and bodies, located in USA, supporting the area of cryptography i.e. RSA Laboratories with PKCS group of public-key cryptography standards. Some of these standards are processed by IETF (The Internet Engineering Task Force).*

34 *NIST, Information Technology Laboratory, website available at: http://www.nist.gov/itl/fipsinfo.cfm*

35 *Current FIPS, available at: http://www.nist.gov/itl/fipscurrent.cfm*

36 *AES Algorithm (Rijndael) Information, available at: http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html*

ty[37] in analysing the algorithms. Currently the Cryptographic Hash Algorithm Competition[38] has been opened for the selection of a new hash function SHA-3 that will be used for Secure Hash Standard (FIPS 180-3).

NIST publishes the *800 Special Publications*[39] (SP) series. The SP series covers recommendations and guidelines in computer security. Examples are SP 800-38 A (Recommendation for Block Cipher Modes of Operation – Methods and Techniques, 2001), SP 800-38 E (Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, 2010), SP 800-57 (Recommendation for Key Management, 2007).

4.1.2 Japan and CRYPTREC IPA research project

The Information-technology Promotion Agency (IPA) in Japan has initiated the CRYPTography Research and Evaluation Committees (CRYPTREC) project with the scope to define standard cryptographic algorithms for use within the Japanese e-Government infrastructure[40].

CRYPTREC evaluated and examined cryptographic techniques; based on these evaluation results, the list of ciphers that are recommended for the procurement of e-Government (e-Government Recommended Ciphers List) was published in 2003 followed shortly by a *Policy for the use of ciphers in information system procurement of each governmental agency*.

The activities of the CRYPTREC project have been extended since then to monitor and investigate the security of ciphers enumerated in the e-Government Recommended Ciphers List. CRYPTREC Reports[41] are updated every year.

A new round of CRYPTREC evaluations was started in 2010 and is scheduled to be completed in 2012.

While CRYPTREC uses independent outside experts for evaluations and publishes their reports, there are entry barriers, such as the use of Japanese language in the workshops and the delay in translating documents.

4.2 EU-funded initiatives related to the use of cryptographic techniques

Until now similar initiatives have been limited at a European level. Most national bodies publish their own cryptographic specifications and make general recommendations for the use of cryptographic algorithms. In this field, a European approach would maximise the results of the

---

37 *The selection process was supported by the international community. The selected algorithm (Rijndael) has been created in Europe.*

38 *Cryptographic Hash Algorithm Competition, available page: http://www.nist.gov/itl/csd/ct/hash_competition.cfm*

39 *NIST Special Publications (800 Series), available at: http://csrc.nist.gov/publications/PubsSPs.html*

40 *CRYPTREC, http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html*

41 *CRYPTREC Report, list of publications, available at: http://www.cryptrec.go.jp/english/report.html*

investments, in research and development of cryptographic specifications, made by governmental bodies and the cryptography industry. Some initiatives outlined in this section could serve as a valuable starting point for such an approach. For instance, as a result of research initiatives (projects, or Networks of Excellences (NoE)) we can identify recommendations for the use of cryptographic techniques. Also, at a European level an Action Plan has been initiated on e-signatures and e-identification.[42]

4.2.1 ECRYPT

The European Network of Excellence for Cryptology II (ECRYPT II) is a four-year project, with 11 partners, funded by the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7). ECRYPT II started on 01 August 2008. Its predecessor was the Network of Excellence ECRYPT (2004–2008). The objective of ECRYPT II is to continue intensifying the collaboration of European researchers in information security.

Every year ECRYPT publishes a study entitled *ECRYPT II Yearly Report on Algorithms and Key Lengths*[43]. The last version available is dated 30 June 2011. The report provides a list of recommended cryptographic algorithms (e.g. block ciphers, hash functions, signature schemes, etc.) and recommended key sizes and other parameter settings (where applicable) to reach specified security objectives. The report respects state-of-the-art technology at the time of writing. It builds upon a series of earlier reports produced by the ECRYPT NoE from the Sixth Framework Programme (FP6).

Based on the questionnaire responses, the ECRYPT yearly report is a reference used by some of the MS.

The ECRYPT project has run an open evaluation of stream ciphers; the results of the eSTREAM project are available on the ECRYPT II website and are documented in the ECRYPT yearly report.

4.2.2 NESSIE

New European Schemes for Signatures, Integrity and Encryption (NESSIE) was a European research project funded from 2000–2003 to identify secure cryptographic primitives. Due to the evaluation process addressing different cryptographic primitives, the project[44] scope was

---

42 *COM (2008) 798, COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, available from: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF*

43 *ECRYPT II Yearly Report on Algorithms and Key Lengths (2011), available at: http://www.ecrypt.eu.org/*

44 *NESSIE portfolio of recommended cryptographic primitives can be located at https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf.*

somehow comparable at that time to the NIST AES process and the Japanese government-sponsored CRYPTREC project. However, the output of NESSIE was a portfolio of algorithms that was submitted to standardisation bodies; no European governmental agency has adopted or promoted the NESSIE results.

4.2.3 Action Plan on e-signatures and e-identification and ESI

The mutual recognition of e-identification and e-authentication across the EU is identified as a top priority of the Digital Agenda for Europe. The same applies in the support for seamless cross-border e-government services in the single market. Some steps towards this have already been made. For instance, in the Cross-Border Interoperability of Electronic Signatures (CROBIES[45]) study, launched by the European Commission in August 2008 in support of the Action Plan on e-signature and e-identification, solutions are proposed to remove barriers to cross-border interoperability of qualified electronic signatures and advanced electronic signatures based on qualified certificates. In one[46] of the work package of the CROBIES study, issues and tasks are identified for electronic signatures. Reference is made to the possible involvement of ENISA in the process of establishing the lists[47] of algorithms and parameters for secure electronic signatures.

On 28 November 2008, the European Commission adopted the *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market* (COM(2008) 798). On 22 December 2009, the European Commission issued a standardisation mandate on electronic signatures (M/460) for the definition of a rationalised standardisation framework.

In 2010, ETSI's Electronic Signatures and Infrastructures (ESI) Technical Committee prepared the first phase of its response to the European Commission Mandate on Electronic Signature Standardisation (M/460), which was issued in December 2009. The goal of this mandate is to achieve the interoperability of electronic signatures throughout Europe, by providing a rationalised European electronic signature standardisation framework which will allow mutual recognition and the cross-border interoperability of electronic signatures.

Further work is needed in this area as the existing technical specifications in this field have not been updated on a regular basis.

---

45 *CROBIES: Study on Cross-Border Interoperability of eSignatures, last version July 2010, available at: http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm*

46 *Note on the "Algo Paper" issue, CROBIES deliverable, July 2010, available at: http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf*

47 *Reference is made to ETSI TS 102 176-1 V2.0.0 (2007-11), Technical Specification, Electronic Signatures and Infrastructures (ESI);Algorithms and Parameters for Secure Electronic Signatures; available at: http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf*

Recommendation 16 – Reports such as the one published by ECRYPT should be continued beyond a NoE or a project's lifetime. An EU body (new or existing) should take responsibility for co-ordinating such activities, including permanent evaluation and examination of cryptographic techniques. It would be essential that such a process was fully open and transparent and involved stakeholders from academia, government and industry. Such co-ordination would improve information security and cross border interoperability in the EU.

5 Concluding remarks

One of the most complex areas of the security industry is cryptography. This complexity makes it challenging to select the most appropriate cryptographic configuration for a solution –the reader needs to have significant background knowledge to understand many of the numerous cryptographic standards.

In a large number of MS that have been surveyed, the cryptographic specifications designed for unclassified information are difficult to locate. The level of cryptographic specifications is heterogeneous. While some MS/government bodies recommend certain algorithms (and parameters) others are only naming parameters (key sizes, hash length, etc.). Key management is not covered in every specification. Annex A lists the most relevant cryptographic specifications that have been indicated during the survey (some MS are more advanced and could be used as a reference point for others). It also lists some of the industry standards that are recommended by experts.

The survey of the MS cryptographic specifications indicated that many recommend good practice cryptographic algorithms. In contrast, the survey of the IT industry experts identified that many of the cryptographic solutions that they audit and test are poorly deployed and insecure.

Outlined below is a consolidated view of this study's recommendations.

Appropriate use of security – data to be protected

When operating unclassified systems, the data that requires encryption can vary greatly. It is essential that during the design of the solution the appropriate data is identified for encryption. Government bodies need to consider carefully what data needs to be encrypted and how best to encrypt it.

Identifying the appropriate cryptographic policy

Currently, finding specific advice and guidance on what is considered to be strong cryptography is complex. Many MS have cryptographic policies for use by their government organisations. Locating these policies is challenging. MS must make sure their cryptographic policies are easily identifiable and accessible.

Deploying the solution in compliance with good security practices

To understand many of these policies you need to have a good understanding of cryptography. Cryptography can be a complex issue because of the advanced mathematics that are at the foundations of cryptographic algorithms. Only cryptographic experts with a good understanding of system security should develop implementations of cryptographic algorithms and protocols. Cryptographic libraries should be provided with clear and simple interfaces.

The technicians deploying cryptography should have access to simple, clear deployment guidance on the specific cipher suite elements they need to configure.

Understand the audience for the cryptographic policies

Many cryptographic policies assume a good level of cryptography knowledge. Some policies define requirements that cannot be configured on many standard commercial cryptographic products. Consequently, when implementing cryptographic solutions, it is a complex process to try and take the policy and cross-reference it to the way software and hardware vendors present the cryptographic options. This complexity leads to misunderstandings. When developing cryptographic policies, MS should consider the intended readership and how the information will be used in order to maximise the benefits and use of the policy.

Auditing

Many commercial products have default cipher suite policies that are automatically enabled, and many vendors enable weak cipher suites to make the solution as simple as possible to configure and deploy. To minimise the risk of this occurring, MS should ensure that all cryptographic solutions are audited by a suitable cryptographic expert before the solutions are used to secure citizen data.

Processes

Selecting and deploying good practice cryptographic algorithms is just the start. A cryptographic solution consists of more than just the technology, it also requires a comprehensive set of processes, and the solution needs to be kept up to date (as weaknesses are identified in the cryptographic algorithms, the solution must be updated to ensure its continuing security). It is essential that MS develop clear guidance on developing the essential cryptographic processes that are required for every solution that uses cryptography.

Building solutions for longevity and keeping up to date with the latest risks

Many government IT systems have an expected lifespan of over five years. Even algorithms believed to be strong during their design, might show vulnerabilities by the time the solution is decommissioned. Updating a cryptographic solution once a system is in operation is very complex, challenging and costly. However, this risk can be mitigated if the design foresees procedures to replace relevant modules.

Moore's Law (Gordon E. Moore[48]) describes a trend that the number of components in integrated circuits had doubled every year from the invention of the integrated circuit in 1958 until 1966, and it predicted that the trend will continue "for at least ten years". His prediction has proved to be accurate. This development in processing power means that when designing a cryptographic solution, the architect must consider the expected lifespan for the system and ensure the cryptographic algorithms selected have the potential to be appropriate for the expected lifespan of the solution.

---

48 ftp://download.intel.com/museum/Moores_Law/Articles-press_Releases/Gordon_Moore_1965_Article.pdf

Cryptographic technologies are continuously developing. This is driven by:

- increasing processing power enabling weaker cryptographic solutions to be broken by brute force (i.e. testing every combination of the encryption key)
- weaknesses being identified in cipher suite elements
- technological advances that support new cryptographic mechanisms.

To ensure the cryptographic policies that the government bodies recommend, all organisations must pro-actively review their cryptographic policies and solutions, and update them in line with changing circumstances.

A pan-European approach for setting cryptographic policies, evaluation and recommendation of minimum requirements

Initiatives and studies, such as the one published by the ECRYPT project (the annual report), could be initiated at European level for the use of minimum cryptographic requirements in e-government services. Furthermore, NIST or CRYPTREC projects could be used as examples of successful instances of such initiatives. This could be set as a permanent activity, with annual recommendations reports, to which all stakeholders, namely from academia, government, and industry, could contribute. Such an activity would maximise the effect of investments made currently in a distributed manner in most of the MS. In this way, those research funds could be channelled for new technologies or new solutions that are needed. An independent organisation such as ENISA could support such a pan-European initiative.

6 List of recommendations

Outlined below is a summary of the recommendations made within this report.

Recommendation 1 – Different governmental bodies should combine their efforts to develop cryptographic policies/recommendations, even if particularities apply for certain applications. 10

Recommendation 2 –MS should ensure that all new IT systems only support strong cryptography in line with good practice recommendations such as the ECRYPT study and that appropriate policies and procedures are in place to upgrade the cryptographic algorithms and protocols when needed. 11

Recommendation 3 – In order to promote and facilitate secure cross-border communications, a common European wide cryptographic policy should be developed by EU Member States using standard cryptographic algorithms and techniques for the protection of unclassified data while at rest and in transit over networks, for the protection of data processed by applications and for the secure authentication of users and devices. 12

Recommendation 4 – Government bodies and project teams should utilise an IT security risk assessment process to identify the data that needs to be cryptographically protected. This risk assessment should be updated annually to ensure that new IT security threats are identified and mitigated appropriately. 13

Recommendation 5 – MS should review their cryptographic policies to consider if it is possible to remove any recommendations supporting the use of cryptographic algorithms with serious weaknesses and cryptographic algorithms with low security levels as recommended by ECRYPT. 15

Recommendation 6 – It is recommended that all weak encryption algorithms which are not recommended anymore by relevant authorities in the field (as in recommendation 5) should been disabled on all government services and applications. 16

Recommendation 7 –When a government body is defining cryptographic recommendations for the provision of unclassified services, it should discuss with its e-government department whether or not a national specification or a specific good practice guide already exists. 18

Recommendation 8 –Key management should be part of cryptographic specifications. For sensitive applications, sensitive keys (shared secret keys, private decryption keys, signing keys) must not be stored within the operating system. The use of tamper-resistant cryptographic hardware such as HSMs and smart cards should be promoted. 19

Recommendation 9 –Each year, government organisations should undertake a comprehensive review of their cryptographic policies, to ensure that the latest research and new cryptographic developments have been taken into account. Additionally government bodies

7 References

The European Parliament and the Council of the European Union: ENISA Regulation, Official Journal L 077, 13/03/2004 P. 0001 – 0011 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

Dan Goodin: "Hackers break SSL encryption used by millions of sites", 19/09/2011 http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

European Commission: "Online availability and interactivity of public services", 04/03/2011, http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database#

Cabinet Office: "HMG Security Policy Framework", May 2010, http://interim.cabinetoffice.gov.uk/media/207318/hmg_security_policy.pdf

European Commission: "A European Digital Agenda", May 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission: "Individuals using the Internet for interacting with public authorities", http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/search_database#

E-government Bund-Länder-Gemeinden: "Spezifikation Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen" (Portal Group Security Classes), 08/02/2008, http://www.ref.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf

Secure Information Technology Center – Austria: "Strategiepapier zur SSL/TLS-kommunikationssicherheit für online e-government verfahren, empfohlene ciphersuites und keystores" (Recommended cipher suites for SSL/TLS in e-government), January 2003, http://demo.a-sit.at/it_sicherheit/ssl_check/resources/SSL_TLS_fuer_eGovernment.pdf

European Network of Excellence in Cryptology II: "ECRYPT II Yearly Report on Algorithms and Keysizes" (2009-2010), http://www.ecrypt.eu.org/documents/D.SPA.13.pdf

European Network of Excellence in Cryptology II: "ECRYPT II Yearly Report on Algorithms and Keysizes" (2010-2011), http://www.ecrypt.eu.org/documents/D.SPA.17.pdf

National Institute of Standards and Technology: "Recommendation for Key Management, Part 3: Application-Specific Key Management Guide", Special Publication 800-57, December 2009, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

Agence nationale de la sécurité des systèmes d'information: "Référentiel Général de Sécurité, version 1.20", 26/01/2010, http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf

Die Beauftragte des Bundesregierung für Informationstechnik: "Standards und Architekturen für E-government Anwendungen", http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga_node.html

Die Beauftragte des Bundesregierung für Informationstechnik: "IT-Grundschutz-Standards", https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html

Die Beauftragte des Bundesregierung für Informationstechnik: "Technische Richtlinien", https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/index_htm.html

Die Beauftragte des Bundesregierung für Informationstechnik: Algorithmen Katalog, http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: PKI Overheid http://www.logius.nl/producten/toegang/pkioverheid/

OASIS: Web Services Security, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

OASIS: "Security Assertion Markup Language, V2.0 Technical Overview", 25/04/2008, http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf

OASIS: eXtensible Access Control Markup, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

CCN-CERT: Computer Security Incident Response Capability, https://www.ccn-cert.cni.es/

NIST, Information Technology Laboratory, http://www.nist.gov/itl/fipsinfo.cfm

NIST: Current FIPS, http://www.nist.gov/itl/fipscurrent.cfm

NIST: FIPS 197 Advanced Encryption Standard Algorithm (Rijndael) Information, http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html

NIST: Cryptographic Hash Algorithm Competition, November 2007, http://www.nist.gov/itl/csd/ct/hash_competition.cfm

NIST: Computer Security Division, Resource Center, Special Publications (800 Series), http://csrc.nist.gov/publications/PubsSPs.html

Information-Technology Promotion Agency, Japan: CRYPTREC, http://www.ipa.go.jp/security/enc/CRYPTREC/index-e.html

Commission of the European Communities: "Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Action Plan on e-signatures and e-identification to facilitate the provision of crossborder public services in the Single Market", 28/11/2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:EN:PDF

CROBIES: "Study on Cross-Border Interoperability of eSignatures", June 2010, http://ec.europa.eu/information_society/policy/esignature/crobies_study/index_en.htm

CROBIES: "Note on the "Algo Paper" issue", July 2010, http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd5.3.pdf

ETSI: "Technical Specification, Electronic Signatures and infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures", TS 102 176-1 V2.0.0 (2007-11) http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.00.00_60/ts_10217601v020000p.pdf

Annex A Cryptographic specifications and recommended standards

List of relevant MS specifications (based on the survey)

- Portal Group Security Classes[49],
- Recommended cipher suites for SSL/TLS in E-Government[50],
- Standards und Architekturen fur E-government andwendungen (SAGA)[51],
- BSI Grundschutz Standards[52], BSI TR-02102 & BSI TR-03111[53],
- Algorithmenkatalog 2011[54]
- Référentiel général de sécurité (in French)[55],
- PKI Overheid[56],
- CCN-STIC[57]

Some recommended standards/specifications/reports (based on the survey)

- NESSIE / ECRYPT and ECRYPT II Yearly report on Algorithms and Keysizes[58]
- Recommendation for key management[59]
- Electronic signatures (ETSI 102 176-1, ETSI 102 176-2[60])
- OASIS: WebServices[61]
- OASIS Standard: SAML[62] WebSSO profile'
- OASIS Standard: XACML[63]

---

49 *http://www.ref.gv.at/uploads/media/SecClass_2-1-0_2007-12-14.pdf*

50 *http://demo.a-sit.at/it_sicherheit/ssl_check/resources/SSL_TLS_fuer_eGovernment.pdf*

51 *http://www.cio.bund.de/DE/Architekturen-und-Standards/SAGA/saga_node.html*

52 *https://www.bsi.bund.de/ContentBSI/Publikationen/BSI_Standard/it_grundschutzstandards.html*

53 *https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/index_htm.html*

54 *http://www.bundesnetzagentur.de/cln_1932/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html*

55 *http:/www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf*

56 *www.pkioverheid.nl*

57 *www.ccn-cert.cni.es*

58 *http://www.ecrypt.eu.org/documents/D.SPA.13.pdf*

59 *http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf*

60 *www.etsi.org*

61 *http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss*

62 *http://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf*

63 *http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml*

Some standards recommended as reference (based on interviews)

In discussions with the IT industry, numerous encryption standards where referred to as improving the level and configuration of encrypted solutions. Table below outlines the most common standards that where mentioned by the interviewees

Standards bodies	Standard	Comment
Payment Card Industry security Standards Council	PCI-DSS	Provides good guidance regarding the type of encryption required to protect financial information
ISO/IEC JTC/SC27	ISO/IEC 2700x series	Security technologies, Information security controls and Information security risk management
ISO	ISO 21188	Provides advice and guidance on setting up public key infrastructures (PKIs)
T-Scheme	Various industry vertical standards	An accreditation scheme for PKIs
ITU and the IETF	numerous	Provides guidance regarding encryption

Figure A3: Common standards that are used when defining encryption policies

Commonality in cryptographic specification

Using the information gathered from the survey respondents, there is significant commonality in the encryption standards that are recommended across Europe. This commonality enables a common standard to be proposed, which could enable and simplify the secure exchange of unclassified data between European governments, and could assist Europe in defining a cryptographic baseline to improve the overall level of trust that citizens can have in electronic communications and e-government services. The proposed standard, outlined below, is designed to be achievable with existing commercially available products.

Certified products should be used

When installing encryption solutions it can be very hard to ensure that the product is encrypting the data to the desired level. One method of ensuring that the products, namely, the encryption hardware and software, operates as desired, and that the cipher suites also operate as defined in the relevant Request For Comments (RFC) or international standards, is to utilise certified products.

Recommendations for citizen access to e-government services

Typically, governments use HTTPS to secure communications from citizen devices to e-government web servers. Below is a high-level proposed outline for the core elements of an encryption policy for encrypted web services based on the collated survey results:

Common element	Comments
Use TLS 1 or greater	Compliant with ECRYPT report[64]; Due to the new BEAST security vulnerability government bodies should be promoting TLS 1.1 or greater
Key exchange algorithm using – ephemeral Diffie Hellman or RSA	Compliant with ECRYPT[65] report
Signature scheme, with a hash function, i.e. SHA2 or higher	ECRYPT recommends new systems have greater key length
Data encryption algorithm – AES 128 or AES 256	Compliant with ECRYPT report
Use web server certificates from a government source or a suitably trusted commercial organisation, with a three-year certificate lifetime	

Figure B.1: Encrypted web access to government services

Recommendations for sharing data between government systems over a public network

A wide range of technologies are used to encrypt data while it is being transmitted between government bodies. Two of the most common encryption protocols are SSL/TLS or IPsec. Below is a high-level proposed outline for the core elements of an encryption policy for encrypting data while in transit between government bodies, based on the collated survey results.

Common element	Comments
Use TLS 1 or greater	Compliant with ECRYPT study. Due to the new BEAST security vulnerability, government bodies should be promoting TLS 1.1 or greater
Key exchange algorithm – ephemeral Diffie Hellman or RSA	Compliant with ECRYPT findings
Signature scheme, with a hash function, i.e. SHA2 or higher	ECRYPT recommends new systems have greater key length
Data encryption algorithm – AES 128 or AES 256	Compliant with ECRYPT report
Use certificates – certificates should be generated by an appropriate Public Key Infrastructure (PKI) with a 1–3-year certificate lifetime	
Certificates should be stored on an appropriate HSM or smart card	

Figure B.2: SSL/TLS virtual private network

64 *Due to a recent security vulnerability in SSL v3.0 and TLS 1.0, organisations should be updating their policies to utilise TLS v1.1 and above.*

65 *ECRYPT II Yearly Report on Algorithms and Key Lengths (2011), available from: http://www.ecrypt.eu.org/, last version at: http://www.ecrypt.eu.org/documents/D.SPA.17.pdf*

Common element	Comment
Key exchange algorithm – Diffie Hellman group 5 or above	Not specifically covered to this level of detail by ECRYPT study
Signature scheme, with a hash function, i.e. SHA2 or higher	ECRYPT recommends new systems have greater key length
Security associations must not exceed four hours or 2^{31}-1 bytes	
Data encryption algorithm – AES 128 or AES 256	Compliant with ECRYPT report
IPsec virtual private network: IKE key exchanges should utilise Perfect Forward Secrecy (PFS)	Compliant with ECRYPT report
Certificates – should be generated by an appropriate PKI with a 1–3 year certificate lifetime (pre-shared keys should not be used)	
Certificates should be stored on an appropriate HSM or smart card	

Figure B.3: IPsec virtual private network

Data at rest

While attacking data in transit is a realistic possibility, the majority of successful security breaches have been against applications that *hold* the data. To protect data while it is held within applications, it is possible to encrypt the data. Below is a high-level proposed outline for the core elements of an encryption policy for encrypting data while stored within an application, based on the collated survey results.

Common element	Comments
Key exchange algorithm or RSA	Compliant with ECRYPT findings
Signature algorithm	ECRYPT recommends new systems have greater key length
Data encryption algorithm – AES 128 or AES 256	Compliant with ECRYPT report
Use certificates – certificates should be generated by an appropriate PKI with a 1–3-year certificate lifetime	
Certificates should be stored on an appropriate HSM or smart card.	

Figure B.4: Data at rest

Recommendations for key management

Encryption keys must be suitably stored in HSMs or on smartcards with an appropriate common criteria rating.

One of the most common denial-of-service events is when certificates expire. To overcome this issue, it is recommended that a key diary is maintained to record when certificates are going to expire.

Recommendations for auditing

Prior to the sensitive data being transmitted or loaded into an application, the encryption must be suitably tested to ensure that the data will be encrypted as defined, and to identify any weaknesses in the deployment.

On an annual basis, the encryption solution must be validated to ensure that the data is being encrypted as defined in the encryption policy, and to identify any potential weaknesses in the deployment.

Annex B Simplified lists of questions

Outlined below is an overview of the questionnaire sent to MS and to the IT industry.

Member State questionnaire

1. For what application types are you responsible for defining/implementing encryption?
2. In the definition of your encryption policy what information sources (such as government standards or public good practices) did you utilise to assist you?
3. Is the use of encryption products restricted within your country?
4. How does your organisation review the encryption standards it defines?
5. Does your organisation have a security incident plan to enable the investigation of a security incident?
6. What types of data do you recommend are encrypted while being transmitted over public networks?
7. Which cryptographic protocols do you recommend?
8. Which hashing algorithm do you recommend?
9. Which encryption cipher do you recommend?
10. Which mode of operation do you recommend to be used with the chosen cipher?
11. What format and key sizes are recommended?
12. Where are keys generated?
13. How do you secure the encryption keys?
14. How do you recommend that encryption keys are stored?
15. Please describe the key generation, renewal and distribution process?
16. If pre-shared keys are recommended please describe the length and complexity you recommend for the pre-shared key?
17. What lifespan do you recommended for server certificates?
18. What procedures do you utilise to ensure that the encryption that has been configured on the e-government servers is appropriate and to your defined standards?
19. What types of data do you recommend are encrypted while stored in an e-government application and when should traffic between systems be encrypted?
20. What encryption solutions are recommended to encrypt the data?
21. Within Internet Key Exchange, which modes do you recommended?
22. What protocols do you recommend to secure the key exchange?
23. What is the maximum duration of the security association that you recommend (amount of data and duration)?
24. Which cryptographic protocols do you recommend?

IT industry interviews

1. What experiences do you have installing, consulting on testing European government systems looking at crypto?
2. In your opinion what is the level of knowledge and expertise in configuring crypto?

3. Does each nation state provide the team implementing the system with information on how they would recommend the crypto is configured?
4. Are any nations better than others? If so why.
5. What public sources of crypto configuration information do you use and recommend?
6. What are the common cryptography errors/faults that you have identified when reviewing encryption deployments?
7. Are there any standards that you perceive that are / have improved the deployment of crypto?

What should the European governments be doing to improve the deployment of crypto?

Annex C Background information

Symmetric and asymmetric techniques

There are two basic techniques for encrypting information: symmetric encryption and asymmetric encryption (also called public key encryption). In the case of s*ymmetric* encryption, a secret key, is applied to the text of a message to change the content in a specific way. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. The difficulty with secret keys is exchanging them in a secure manner: anyone who knows the secret key can decrypt the message.

For *asymmetric* encryption, there are two related keys – a *key pair*. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only the key owner knows it. Any data that is encrypted using the public key can only be decrypted by applying the same encryption algorithm, but by using the matching private key. The authenticity of the public key needs to be protected while passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires more processing power to both encrypt and decrypt the content of the message. That is why one uses in practice hybrid encryption: asymmetric techniques are used to establish a secret key, and subsequently symmetric techniques are used to guarantee data confidentiality and authentication.

Besides encryption – used for confidentiality purposes, one needs also entity and message authentication, data integrity, non-repudiation etc., objectives which are achieved using cryptographic techniques (symmetric keys or asymmetric keys primitives).

Data origin authentication or *message authentication* techniques provide to one party which receives a message assurance of the identity of the party which originated the message. Data origin authentication implicitly provides data integrity since, if the message was modified during transmission, the originator is not the same. *Message authentication codes* (MACs) allows message authentication by symmetric techniques. MAC algorithms take two distinct inputs, a message and a secret key, and produce a fixed-size output; should be impossible to produce the same output without knowing the key. Digital signatures schemes are also used for message authentication, and provide additionally non-repudiation of data origin.

When designing an encryption solution it is necessary to select the algorithms i.e. used for encrypting data and for computing the message authentication code. The collection of these algorithms is often called a *cipher suite*. In case of SSL/TLS[66], IPsec, a cipher suite consists of four components:

---

[66] *NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf.*

- **Key establishment algorithm** – the method by which cryptographic keys are exchanged between parties.
- **Digital signature algorithm –** i.e. for entity authentication. Entity authentication is the process whereby one party is assured of the identity of a second party involved in a protocol.
- **Data encryption algorithm** – used to encrypt data. As mentioned above, there are two basic types of encryption algorithm, symmetric and asymmetric. Example of algorithms includes Advanced Encryption Standards (AES) and Data Encryption Standard (DES).
- **Data integrity algorithm** – used to check the integrity of the data. E.g. MAC algorithms (SHA-1, etc.)

Business roles for cryptography covered within this study

This study investigated three types of cryptographic solution:

- Cryptography used to secure citizens' access to e-government websites
- Cryptography used to secure a network connection between government machines
- Encryption of data stored within e-government applications.

The sections below provide a selection of background information regarding these three types of encryption solutions.

Secure access to web services

When a user accesses a website using a web browser, typically it will utilise a protocol called hypertext transfer protocol (HTTP). This protocol is not encrypted; the data passes over the network between the user's PC to the web server in clear text. This information could be intercepted and the data reconstructed. The most common way to secure such a communication is by encrypting the data using hypertext transfer protocol secure (HTTPS). HTTPS can utilise the encryption protocol's secure socket layer (SSL) and transport layer security (TLS) to encrypt the data. SSL was originally developed by Netscape. Version 1.0 was never publicly released; version 2.0 was released in February 1995, and version 3.0 in 1996. There have been a number of releases of TLS, TLS 1.0 (RFC 2246, in 1999), etc., TLS 1.2 (RFC 5246 defined in 2008) and TLS 1.2 (RFC 6176 further refined in March 2011).

Secure communications between nodes

When developing systems and applications, there is often a business requirement to collate data from a variety of sources and to exchange data between systems. Sometimes these systems are geographically separated and have no appropriate network connection. For large and complex systems, it can be appropriate to connect the systems through a dedicated network connection, but often this is not cost-effective so the connection is established over a

public network such as the Internet. In these cases, cryptography should be utilised to secure the data while in transit over the public network. With this, an encrypted tunnel is constructed between two end points. Date is encrypted when it enters the tunnel and decrypted when it leaves. Typically three types of encryption protocol are used: SSL/TLS, as described above; Internet protocol security (IPsec) and Government-developed encryption.

IPsec was originally defined in RFC 1825 and RFC 1829, published in 1995. In 1998, these documents were superseded by RFC 2401 and RFC 2412. In 2005, updated standards were defined in RFC 4301 and RFC 4309.

Encrypting data within applications

While attacking data in transit is a realistic possibility, the majority of successful security breaches have been against the applications that *hold* the data. To protect the data while it is held within the applications, it is possible to encrypt the data. In this context there are two basic types of encryption[67] – encryption that works at the operating system level, and encryption that is built into the application.

With encryption that works at the operating system level, it is possible to encrypt all the data on the system, or just a specific area of the hard disk. If the data is being held within an application, then depending on the nature of the application and any supporting database, it may be possible to encrypt a selection of the data held within that application or database. The cipher suite and the encryption capabilities are directly linked to the applications that are selected.

NIST standards – Federal Information Processing Standard (FIPS)

The National Institute of Standards and Technology (NIST) is the USA's federal technology agency, which has developed cryptographic standards, notably the Federal Information Processing Standard (FIPS) 140 security requirements for cryptographic modules and the recommendations in the Special Publication (SP) 800-57 for key management. NIST SP 800-57 is cross-referenced by the PCI DSS standard.

[67] *There is also encryption built-in the hard disk or in the USB drive.*

Annex D Terminology and abbreviations

Defined below is the core terminology and abbreviations utilised within this document.

access control	*restricting access to resources to privileged entities*
AES	*Advanced Encryption Standard (AES) is a data encryption algorithm. It has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits.*
Certification	*endorsement of information by a trusted entity*
Confidentiality	*keeping information secret from all but those who are authorized to see it*
Data encryption algorithm	*The method by which data is encrypted. There are two basic types of encryption algorithms: symmetric and asymmetric. Common encryption algorithms include Advanced Encryption Standards (AES) and Data Encryption Standard (DES).*
data integrity	*ensuring information has not been altered by unauthorized or unknown means*
Data integrity algorithm	*The method by which to check the integrity of the data. Hash functions are used to build Message Authentication Codes (MAC) algorithms; MAC algorithms are used for data integrity.*
DES	*Data Encryption Standard (DES) is a block cipher that is used to encrypt data. It is based on a symmetric key algorithm that uses a 56-bit key.*
Diffie Hellman	*Diffie Hellman (DH) is a key exchange mechanism that allows two parties that have prior knowledge of each other to jointly establish a shared secret key over an authenticated communications channel.*
Digital Signature algorithm (DSA)	*The Digital Signature Algorithm (DSA) is a US Federal Government standard for digital signatures.*
DSS	*The Digital Signature Standard is a government document mandating the use of DSA. The terms DSA and DSS are interchangeable.*
entity authentication or identification	*Corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.)*
FIPS	*Federal Information Processing Standards (FIPS) are publicly defined standards that have been developed by the US NIST organisation for use in computer systems.*
Hash functions	*Hash functions are typically publicly known and involve no secret keys. When used to detect whether the message input has been altered, they are called* modification detection codes *(MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication as well as data integrity; these are called* message authentication codes *(MACs).*
HSM	*A Hardware Security Module (HSM) is a type of secure cryptographic processor utilised to securely manage encryption keys. These modules are physical devices that traditionally come in the form of a plug-in card or an external device.*
HTTP	*The Hypertext Transfer Protocol (HTTP) is a networking protocol for distributed, collaborative hypermedia information systems. It's at the foundation of data communication for the World Wide Web.*
HTTPS	*The Hypertext Transfer Protocol Secure (HTTPS) is a combination of HTTP with SSL/TLS protocol to provide encrypted communication and secure identification of different servers on the web. These protocols are often used for online payment transactions.*
Key establishment algorithm	*The method by which cryptographic asymmetric keys are exchanged between parties*
MD5	*The Message Digest Algorithm is used as a data integrity algorithm. MD5 is vulnerable to collision attacks and has been superseded by SHA-1 and by the SHA-2 family of algorithms.*
Message authentication	*Corroborating the source of information; also known as data origin authentication*
MAC	*Message Authentication Code, hash functions which involve a secret key, and provide data origin authentication as well as data integrity*
NIST	*National Institute of Standards and Technology (NIST) is the USA's federal technology agency, which has developed the FIPS cryptographic standards*
non-repudiation	*preventing the denial of previous commitments or actions*
PCI-DSS	*The Payment Card Industry Data Security Standard (PCI-DSS) is an information security*

	standard for organizations handling cardholder information.
PFS	*Perfect Forward Secrecy (PFS) is the property that ensures that a session key derived from one or more long-term public-private key pairs will remain secure even if later one of the private keys is compromised.*
revocation	*retraction of certification or authorization*
RFC	*A Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force, describing methods, behaviours, research or innovations applicable to the working of the Internet and Internet-connected systems.*
RSA	*Stands for Rivest, Shamir and Adleman (RSA) who publicly described this algorithm, which uses both a public and a private key. Can be used for signing as well as encrypting data.*
SHA	*Secure Hash Algorithm, examples: SHA-0, SHA-1, SHA-2.,.It is a cryptographic hash function; one of the applications of hash function is data integrity checks.*
signature	*a means to bind information to an entity*
Smartcard	*A pocket-sized card with embedded integrated circuits. It contains volatile memory and microprocessor components and can provide identification, authentication, data storage and application processing.*
SSL	*Secure Socket Layer (SSL) is a cryptographic protocol that encrypts and authenticates segments of network connections at the transport layer to prevent eavesdropping and tampering. See section 0 for more information.*
Symmetric cryptography	*Symmetric-key cryptography is an encryption and data authentication method in which both the sender and receiver share the same key. [See also Asymmetric cryptography]*
TLS	*Transport Layer Security (TLS) is the successor of the SSL protocol and was published in 1999. See Annex D for more information.*
Triple DES	*Triple DES provides a method of increasing the key size of DES to protect against brute force attacks, without the need to design a completely new block cipher algorithm. Triple DES encrypts the data three times with 2 or 3 different keys of 56 bit (i.e. 2-key Triple-DES and 3-key Triple-DES). Should be noted that NIST withdrawn its support for 2-key Triple-DES, after previous withdrawal of its support for DES in 2005.*

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu