Stabile Usage of Export Regulatory Standards in Data Security Process

Boris Plejić[*], Marin Šilić[**] and Marin Golub[**]

[*] Ericsson Nikola Tesla/ZGD, Zagreb, Croatia

[**] Faculty of Electrical Engineering and Computing/ZEMRIS, Zagreb, Croatia

boris.plejic@ericsson.com, marin.silic@fer.hr and marin.golub@fer.hr

***Abstract* - The amount of data that contemporary companies generate is rapidly increasing. Due to data explosion, security and privacy are becoming crucial concerns for companies. Therefore, companies must ensure security to remain a priority, and set the rules that will keep company at a desired security level. In addition to their internal security rules, a company may need to comply with one or more standard defined by external parties. Weak implementation of strict standards may lead to procedural gaps where the critical point is delivering the data to customers. In this paper, we define terms and concepts behind the security standards that are related to encryption algorithms and describe the correlation between security and regulatory standards while exporting sensitive data to customers. In addition, we provide a case study to demonstrate how weak implementation of export regulatory standards can lead to human errors, where lack of security competence can trigger high level damage after commercial product roll up. Finally, we show how minor modification in the implementation of standards can mitigate the security breach.**

Keywords - Cryptography; Protocols; Algorithms

DISCLAIMER - some companies, products and services are mentioned in this tutorial. Such mention is for example purposes only and should not be taken as a recommendation or endorsement by the authors.

I. Introduction

To mitigate the risk of losing data, the companies introduce security frameworks that define a life cycle for managing the security of data and technology within the company. The updates of security frameworks need to be prioritized during the product development or otherwise desired security level will not be reached. There are known methods to enforce security rules, however the implementation often does not comply with the defined standards which may result in severe security breach [1].

In the first part of the paper we provide an overview of cryptographic algorithms used in Ericsson company. Also, we explore future emerging environments where cryptographic solutions are yet to be adopted.

In the second part of the paper, we specially focus on security aspects of complex product development process in a large company where various teams need to cooperate and communicate to produce the product and deliver it to their customers. For instance, companies that operate internationally and offer their products abroad, should obey certain regulations according to the export rules [2]. This is especially important in case the exported product is using cryptography and product's usage is restricted. Failing to meet the export rules can cause large penalties for exporting companies. As part of the paper, we deliver a case study that analyses the Panama case [3], where Ericsson company paid large fines due to export rules violations. We also identify the main cause that led to violation of export rules as a weak implementation of security standards within the company and miscommunication between teams responsible as well. Finally, we propose a better implementation of security standards that would prevent the export violation in Panama case to happen.

Section 2 provides an overview of cryptographic algorithms currently used in company Ericsson during the product design phase. Section 3 will introduce some future contexts where cryptographic solutions need to be adopted. Section 4 describes the behaviour of products at commercial roll up and export where data security must follow specific regulatory standards. Section 5 brings the case study where human behaviour in process of export control is main part of discussion. Finally, Section 6 concludes the paper.

II. CRYPTOGRAPHIC ALGORITHM

An overview of cryptographic algorithms used in Ericsson telecommunication company can be found in their Technology Review [4], where is stated that algorithms developed by 3GPP and GSMA for confidentiality, integrity, authentication, and key derivation have evolved dramatically since they were first introduced. The original algorithms deployed in 2G/3G networks were kept secret and designed to meet the restrictions related to encryption of that time but found to have weaknesses. The encryption algorithms developed for 3G and LTE have been made available for public analysis. They use well-known and standardized algorithms such as AES, SNOW and SHA-3 and to date, no weaknesses have been found.

Commonly used algorithms, will be briefly mention in the next three sub-chapters [5].

A. Symmetric algorithms

Symmetric algorithms encrypt and decrypt a message using the same key. However, there is certain risk in handling same keys. Once a key gets in the wrong hands, there is no going back. A person who possesses the key can read all past messages and create new messages that are indistinguishable from valid data. Several symmetric algorithms have been used in the past: Blowfish, DES, 3DES (Triple DES), AES.

The first three algorithms are generally considered obsolete and are followed with comments in literature, as "*should be avoided due to poor security*", "*has been phased-out from standard due to poor security*" or even "*considered weak, not to be used today*".

Ericsson [4] conducted a study about usage of symmetric algorithms and concluded that processes of encryption and integrity protection are separated. By instead combining them, newer AEAD [6] algorithms achieve huge performance gains over their legacy counterparts. For example, when AES is used in Galois Counter Mode (AES-GCM), AES has outstanding performance on modern processors and is today's solution for many high-end software applications.

B. Asymmetric Algorithms

Asymmetric algorithms use different keys for encryption and decryption. The encrypting key is called the public key while the decrypting key is the private key. In a public key encryption system, any person can encrypt a message using the receiver's public key. That encrypted message can only be decrypted with the receiver's private key. The receiver has confidence that the message came from the right source, because only someone who holds private key could have produced a working signature. There are two dominantly used asymmetric algorithms today: RSA and Elliptic Curve. In addition, a Diffie-Hellman protocol is commonly used today for key exchange over a public channel.

Diffie-Hellman is not quite suitable for establishing identity as it needs to be protected from Man-In-The-Middle Attack [7]. RSA is most commonly used today, while Elliptic Curve appears to be on its way to become the next standard [8].

An example of asymmetric algorithms usage is described in [4], where is stated that data encrypted with the public key can only be decrypted by the private key and signatures created with the private key can be verified with the public key. Typically, public-key algorithms like RSA are used for authentication and key exchange during session setup and not for the protection of data traffic.

Improved security and performance can be accomplished with Elliptic Curve Cryptography (ECC). ECC can achieve better performance by using smaller key size. The key sizes used in asymmetric algorithms need to be longer than those used in symmetric algorithms of comparable strength. The ECC signature algorithm ECDSA (with the NIST p-256 curve) uses significantly smaller key sizes than RSA (256 bits compared with 3072 bits) and delivers significantly better performance in use case where both signing, and verification are needed. New faster ECC algorithm Ed25519 [9] will further improve the performance of ECC.

C. Hash Algorithms

Ordinary hash functions are not suitable for digital signatures because they are easily reversible. Instead, there are special cryptographic hash functions which produce hashes that are hard to reverse [5]. In other words, given a hash, it's hard to generate a document that produces that hash. Cryptographic hash functions include: MD5, SHA 1, SHA 2 family (SHA-128/-192/-256), SHA 3 family. MD5 has been found to contain weaknesses and is therefore no longer recommended for use. SHA 1 is a little stronger but should still be phased out now. SHA 2 is secure, but its disadvantage is that the NSA invented it. SHA 3 is secure and was invented using an open selection process.

III. USAGE OF ALGORITHMS IN THE FUTURE [4]

ICT industry is in the process of abandoning the use of several legacy algorithms and protocols including 3DES, RC4, CBC-mode, RSA, SHA-1 and TLS 1.1, changing them with newer, more secure, and faster algorithms such as AES-GCM, ECC, SHA-2, SHA-3 and TLS 1.2 and later versions.

One company has recently initiated an upgrade of the 3GPP security profiles for certificates and security protocols such as TLS, IPsec and SRTP [10]. That will lead to security strategy that should be implemented using efficient and tested algorithms that will offer a cryptographic strength equivalent of at least 128-bit security for AES, as minimum requirement for wireless technologies as IoT or Cloud storage.

Messaging patterns that are used in IoT device communication nowadays are *store-forward* and *publish-subscribe*. Those devices are communicating using middleboxes, which limits the possibility for end-to-end security. The solution is usage of fully trusted intermediaries, which make access to IoT data sensitive services difficult for enterprises and governments. The aim of object security is to provide end-to-end protection of sensitive data, while enabling services to be outsourced at the same time.

Homomorphic encryption [11] is one of the key breakthrough technologies that came from cryptographic research. In contrast to AES, this approach allows operations to be performed directly on encrypted data without using the data in its decrypted form. To support arbitrary computations on encrypted data using fully homomorphic encryption, some performance issues still need to be overcome. However, many specialized methods like partially homomorphic encryption, deterministic encryption, order-preserving encryption, and searchable encryption, allow a specific set of computations to be performed on encrypted data with a sufficient performance so that they can be applied to real-life scenarios. Research [12] has shown a performance increase of orders of magnitude, which makes it suitable for high-throughput scenarios. By using homographic encryption, clients with large datasets, such as network operators, health care providers and process/engineering industry players, would be able to outsource both storage and analysis of the data to the cloud service provider. Once outside the client's network, data is encrypted, thereby preserving confidentiality, and allowing the cloud provider to perform analytics directly on the encrypted data.

In post-quantum cryptography era, the existing algorithms that are considered secure nowadays, will become weak to special attack algorithms invented and are ready for a quantum computer to execute on. As an example of such attacks, Grover's algorithm can be easily used to break symmetric cryptographic algorithms. Grover's algorithm inverts a function using only √N evaluations of the function, where N is the number of possible inputs. For a symmetric 128-bit key algorithm, such as AES-128, Grover's algorithm enables an attacker to find a secret key 200 quintillion times faster, using roughly 264 evaluations instead of 2128. The quantum computing therefore weakens the effective security of symmetric key cryptography by half. Research [4] state that situation for public-key algorithms is even worse; for example, Shor's algorithm for integer factorization directly impacts the security of RSA. With Shor's algorithm, today's public-key algorithms lose almost all security and would no longer be secure in the presence of quantum computing.

Although current research is far from the point where quantum computing can address the size of numbers used today in crypto schemes, the ability to perform quantum computing is increasing. In 2014, ETSI organized a workshop on quantum-safe cryptography and in 2015 the US National Security Agency (NSA) said it would initiate a transition to quantum-resistant algorithms, as the potential impact of quantum computing has reached the level of industry awareness [13].

IV. CRYPTOGRAPHY EXPORT CONTROL

An encryption functionality can be provided by a software, encryption chips, integrated circuits, application specific encryption toolkits, executable or linkable modules, e.g. that alone are incapable of performing complete cryptographic functions, and any encryption commodity that is designed or intended for use in or in the production of another encryption item [14]. So, it is visible that awareness of encryption is increasing and there has been a surge in the number of companies that want to encrypt products over the entire product life-cycle. The market for encryption of products is growing and more developers are building software that integrates data security using encryption. This raises important questions about the legal frameworks that regulate the distribution of encryption technology.

Part of data security concept, responsible for distribution and standards defined by external parties and internal company trade compliance directives is called Export control. Export control must guarantee that product using cryptography is not delivered to certain end-users or for certain end-uses without permission from a competent authority. For example, dual-use items (items that have both commercial and military or proliferation applications) [15] should be subject to effective control when they are exported.

One of few agreements which regulates export of cryptography internationally is called the Wassenaar Arrangement. The Wassenaar Arrangement (WA) [16] has been established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States seek, through their national policies, to ensure that transfers of items do not contribute to the development or enhancement of military capabilities which undermine these goals and are not diverted to support such capabilities. The aim is also to prevent the acquisition of these items by terrorists. Participating States apply export controls to all items set forth in the List of Dual-Use Goods and Technologies and the Munitions List, with the objective of preventing unauthorized transfers or re-transfers of those items. To assist in developing common understandings of transfer risks, Participating States regularly exchange information of both a general and a specific nature. Participating States are required to report their arms transfers and transfers/denials of certain dual-use goods and technologies to destinations outside the Arrangement on a six-monthly basis. In some cases, shorter reporting time-frames apply. In fulfilling the purposes of the Arrangement as described above, Participating States have, inter alia, agreed to many guidelines, elements, and procedures as a basis for decision-making through the application of their own national legislation and policies. The decision to transfer or deny the transfer of any item is the sole responsibility of each Participating State. All measures with respect to the Arrangement are taken in accordance with national legislation and policies and are implemented based on national discretion. For specifics on Export Controls in Participating States National Contacts.

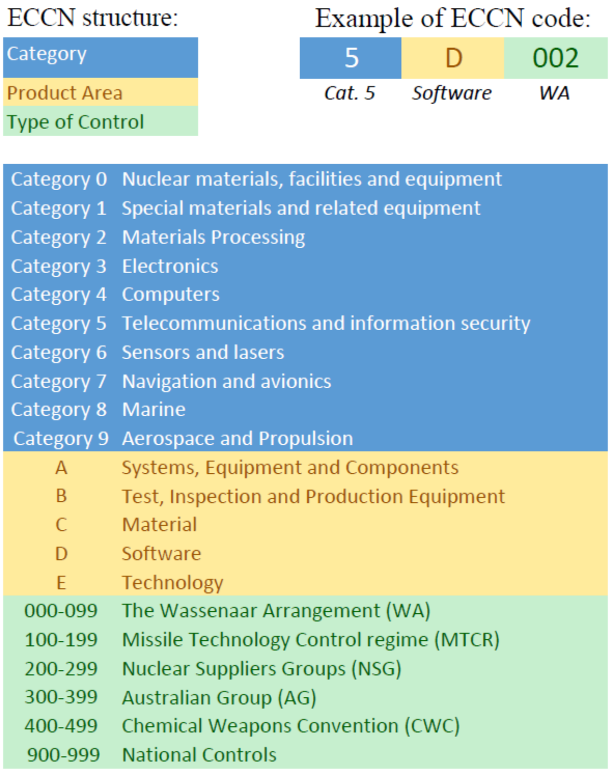
Usage of export regulations is mainly defined and communicated to authorities through specific Product Classification codes, called Export Control Classification Number (ECCN) and Harmonized System Tariff (HST).

A. *Export Control Classification Number code [17]*

Export Controls regulates the shipment or transfer, by whatever means, of controlled items, software, technology, or services, as classification of controlled goods is mandatory part of export.

The ECCN code refers to Export Control Classification Number (the U.S. term for an export classification code). The export of cryptographic technology and devices from the United States is severely restricted by U.S. Law. The ECCN code is national code specific to the United States, although it has a similar form as used in other countries because most countries participate in multilateral export control regimes like the mentioned WA. Accordingly, regulations were introduced as part of munitions controls which required licenses to export cryptographic methods. The regulations established that cryptography beyond a certain strength would not be licensed for export except on a case-by-case basis. This policy was also adopted elsewhere for various reasons. The ECCN code identifies the relevant category and paragraph of a classification, as they are maintained under the EAR's Commerce Control List [18].

ECCN code structure contains 3 parts: Category, Product area and Type of control, described on Figure 1



ECCN structure:

- Category
- Product Area
- Type of Control

Example of ECCN code:

5	D	002
Cat. 5	Software	WA

Category 0	Nuclear materials, facilities and equipment
Category 1	Special materials and related equipment
Category 2	Materials Processing
Category 3	Electronics
Category 4	Computers
Category 5	Telecommunications and information security
Category 6	Sensors and lasers
Category 7	Navigation and avionics
Category 8	Marine
Category 9	Aerospace and Propulsion
A	Systems, Equipment and Components
B	Test, Inspection and Production Equipment
C	Material
D	Software
E	Technology
000-099	The Wassenaar Arrangement (WA)
100-199	Missile Technology Control regime (MTCR)
200-299	Nuclear Suppliers Groups (NSG)
300-399	Australian Group (AG)
400-499	Chemical Weapons Convention (CWC)
900-999	National Controls

Figure 1 ECCN code structure

B. Harmonized System Tariff (HST)

The Harmonized Commodity Description and Coding System [19] generally known as Harmonized System (HS) is a multipurpose international product nomenclature developed by the World Customs Organization (WCO). All goods that cross international borders must be classified with an HS code.

The HS is a complete classification system (i.e. it covers all merchandise). It was designed as a core system so that countries adopting it could make further subdivisions according to their tariff and statistical needs. Goods in trade generally appear in the HS in categories or product headings in a progression beginning with crude and natural products and continuing in further degrees of complexity through advanced manufactured goods.

Developed and managed by the WCO, the HS Code:

- consists of 5,000 commodity groups covered in 99 Chapters containing 21 Sections;
- is identified by a six-digit code;
- is arranged in a legal and logical structure; and
- is supported by well-defined rules to achieve uniform classification all over the world.

HS code structure contains 4 parts: Chapters, Headings, Subheadings, and Country-specific details[1] described in Figure 2, where example of code used in telecommunication sector is shown.

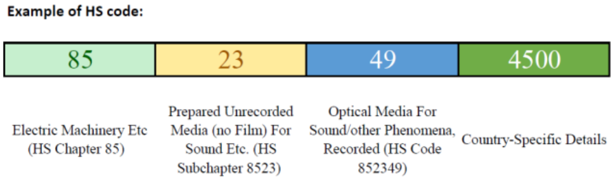

Example of HS code:
85
23
49
4500
Electric Machinery Etc (HS Chapter 85)
Prepared Unrecorded Media (no Film) For Sound Etc. (HS Subchapter 8523)
Optical Media For Sound/other Phenomena, Recorded (HS Code 852349)
Country-Specific Details

Figure 2 HS code structure

V. Case Study

Order process in companies is formed according to the customers wishes. Products are packaged in groups to meet reusable functions of sales process, common in customers' orders. Those reusable groups of products are called packages. When package reaches general availability state then every aspect of product security should already be implemented. This means that mandatory cryptographic algorithms should be known, export control information on package level should be strictly defined, export control codes should be stated and approved by trade responsible and set as package data. The key point is export control procedure involves several roles, usually spread over few different departments. If there is no correct communication between included parties export control process is prone to human errors. A critical part is related to setting the right security data on the package level. Failing to set the appropriate security data on the package level for some reason can lead to a high level of damage while exporting goods. A known example is the case of Panama where Ericsson company paid $1.7 Million to settle 262 violations of the Export Administration Regulations (EAR).

A. Issue

In a company as Ericsson, Trade department (TC) handle export regulations deployment and control security information's connected with each package [20]. The TC department is well known by handling strict security policy and managing trade information on high

[1] The remaining numbers may include national tariff rates (generally 8-digits) or a 10-digit number may be used for statistical use, quotas, and analysis. In the United States, for example, the full 10-digit number is called the Harmonized Tariff Schedule of the United States (HTSUS) code. Not all countries, such as India, have full 10-digit codes.

level and is not responsible for setting data on package level or releasing packages. The department that is responsible for release is the Product Packaging department (PP), where technical responsibility and crucial structure knowledge is situated.

In the Panama example, a problem occurred when Ericsson de Panama knowingly implemented a scheme to route items from Cuba through Panama, repackaged the items to conceal their Cuban markings. Then, they forwarded the items to the U.S. for repair and replacement and then returned the items to Cuba. Classified under Export Control Classification Numbers 5A002, 4A994, 5A991, 5B991 or designated EAR99, the items' distribution to Cuba were controlled for national security, antiterrorism, encryption, and sanctions reasons. In this case the issue was that products didn't have right export control data set. However, issues can also appear if there is no adequate amount of communication between departments involved in the trade process.

The PP department is mainly involved in pre-sale phases but is not familiar with mandatory trade knowledge. As not obligated to contact TC department when release of product is ongoing, the product can be automatically moved to the commercial phase with predefined trade data without trade responsible confirmation. In such a scenario, the released package has non-confirmed or lack of export control strength, where transport of such product can lead to high level of damage.

B. Solution

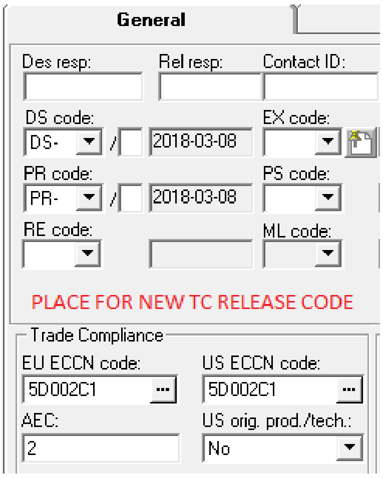
The guidelines for handling cryptography found in company documentation advise as follows:

- All non-public information, especially about customers, partners or suppliers must be encrypted to ensure proper and effective use of cryptography and to protect the confidentiality, authenticity and integrity of information;
- No individuals in company shall take steps to bypass encryption or decrypt information for which they are not authorized to access. Equipment used to generate, store and archive keys must be protected;
- Systems that are providing cryptographic functionalities must reveal used algorithms. If possible, standard cryptographic algorithms and libraries should be used;
- Some countries restrict usage of cryptographic technology, others restrict the import of encrypted data and still others restrict or prohibit the use of encryption within their borders. Local laws and legislation regarding the use of cryptographic technology must be respected;

Cryptographic keys must be treated as company's confidential asset. They must be provided on request from an authorized security function within company and be part of export control process, where coordination between TC and PP departments is crucial in providing stabile usage of export regulatory standards in data security process.

PP and TC responsible should do the release of the package together when all predefined rules are confirmed:

- All design information and substructure should be created and connected with the package;
- All trade information and documentation should be released and connected with the package;
- When the package is ready for release, release confirmation should be confirmed by PP and TC responsible by setting unique state of the package; TC responsible should set a new added trade (TC) code and PP responsible should set a common design code for release;



General

Des resp:
Rel resp:
Contact ID:
DS code: DS- / 2018-03-08
EX code:
PR code: PR- / 2018-03-08
PS code:
RE code:
ML code:

PLACE FOR NEW TC RELEASE CODE

Trade Compliance
EU ECCN code: 5D002C1
US ECCN code: 5D002C1
AEC: 2
US orig. prod./tech.: No

Figure 3 Package data update with TC code

- When the trade code and the design code are set product can be released.

Packages released by following the above-mentioned rules are secured of lack of release information. Therefore, huge damage triggered when the order reaches customers would be avoided.

C. Lesson learned

It's important that there is a regular time for reporting both progress and potential pitfalls between the teams. This keeps people on track and gives everyone the discipline of a team check-in. Export control process is all about knowing guidelines, elements, and procedures, that are strictly connected with agreements and trade rules, but team spirit and communication is something that lies in human hands and should be mandatory in trade work.

VI. Conclusion

The top priorities in data secure process is to define stable security and privacy framework as the key to protect the privacy of individuals and company's knowledge. Companies must take steps to ensure that they follow encryption regulations in all countries where they do business and at the same time must adopt best practices to maximize information security, despite restrictions on cryptography use.

Overcoming these concerns is a non-negotiable element of the product export process, where encryption techniques are applied across the entire product line system. This, together with new, more complex communication services places new demands on cryptography usage [5].

Implementation of security policy should be applied to all company's product/packages that are ready for commercial usage. As described in case study, key role is sharing knowledge and information between all parties included in export process. In mentioned example, passing information between TC and PP department should be defined as part of release process where more stable and security driven packages will be placed and sent to customers.

References

[1] Applied Trust, Every company needs to have a security program, https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program, 2008.

[2] Michigan Tech, Export Controls Laws and Regulations, http://www.mtu.edu/research/administration/integrity-compliance/export-controls-foreign-nationals/export-control/

[3] Office of Public Affairs, "Ericsson de Panama Pays $1.753 Million to Settle Charges of Unlicensed Transshipments to Cuba", BIS, May 2012.

[4] C. Jost, J. Mattsson, M. Näslund, B. Smeets, "Cryptography in an all encrypted world", Ericsson Technology Review, vol. 92, December 2015.

[5] Cryptography Fundamentals - Algorithms, http://cryptofundamentals.com/algorithms

[6] D. McGrew "An Interface and Algorithms for Authenticated Encryption", RFC5116, IETF, January 2008.

[7] A. S. Khader, D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol", IEEE 22nd International Conference on Telecommunications (ICT 2015) - Sydney, pp 204-208, June 2015.

[8] A. Langley, M. Hamburg, S. Turner, "Elliptic Curves for Security", RFC7748, IETF, January 2016.

[9] S. Josefsson, I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", RFC8032, IETF, January 2017.

[10] J. Mattsson, "Update of the 3GPP Security Profiles for TLS, IPsec and Certificates", 3GPP SA3 Archives, ETSI, June 2015.

[11] X. Yi, R. Paulet, E. Bertino, „Homomorphic Encryption“ in: Homomorphic Encryption and Applications. SpringerBriefs in Computer Science. Springer, Cham, 2014.

[12] C. Jost, H. Lam, A. Maximov, B. Smeets, "Encryption Performance Improvements of the Paillier Cryptosystem", Ericsson, 2015.

[13] NSA/CSS, "Information Assurance", NSA, February 2017, https://www.nsa.gov/what-we-do/information-assurance/

[14] Electronic Privacy Information Center, Revised U.S. Encryption Export Control Regulations, https://epic.org/crypto/export_controls/regs_1_00.html, January 2000.

[15] Department of Commerce/BIS, "Dual Use Export Licenses", 2016, https://www.bis.doc.gov/index.php/licensing/forms-documents/.../91-cbc-overview

[16] Wassenaar Arrangement, Last updated: 20 Dec 2017, https://www.wassenaar.org/

[17] U.S. Department of Commerce, „Export Control Classification Number (ECCN)“, Bureau of Industry and Security, https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/export-control-classification-number-eccn

[18] EAR, Commerce Control List Supplement No. 1 to Part 774 Category 5 Part 2 - Info. Security, BIS, August 2017.

[19] H.Manaadiar, "What is a HS Code..??", September 2009, https://shippingandfreightresource.com/what-is-a-hs-code/

[20] Ericsson - Conditions and guidelines, https://www.ericsson.com/en/about-us/sourcing/supplier-and-partner-resources/conditions-and-guidelines