

Introduction to Post-Quantum Cryptography training

Dr. Rodica Tirtea, Policy Unit, ENISA

NIS summer school | Heraklion 26/09/2018

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

EXPERTISE

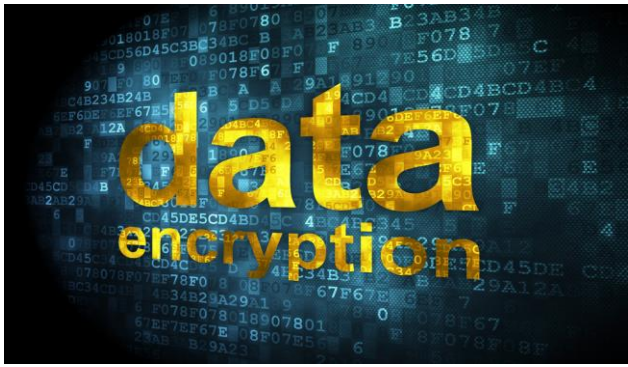
- ✓ Recommendations
- ✓ Independent Advice

Agenda

1	Regulatory measures and requirements for protection of data
2	Past ENISA work on cryptography. A lifecycle perspective on data/information protection
3	Recent activities
4	2017 EU Cybersecurity Strategy & Council Conclusions
5	Overview of the training on **Introduction on Post-Quantum cryptography**

Securing personal data in the context of data protection regulations

Personal data protection requires security protection measures



New GDPR, review of ePrivacy directive, etc.

Personal data breach notification

- ePrivacy directive (2002/58/EC)
  - for the electronic communication sector
- GDPR, extended to other sectors

Appropriate technological protective measures applicable to the notification

- EC Regulation 611/2013 on the measures applicable to the notification
  - Notification flow is different in case of *implemented appropriate technological protection measures*
  - i.e. *notification of a personal data breach to a subscriber or individual concerned shall not be required in such case*, according to art 4, EC Regulation 611/2013
  - ENISA is supporting EC in establishing the indicative list of protective measures
    - Indicative list of appropriate technological protection measures as required by EC Regulation 611/2013

Exceptions for data breaches notification (I)

Telecom sector, Article 4 of ePrivacy Directive

- "In the case of a **personal data breach**, the provider of publicly available electronic communications services shall, without undue delay, **notify the personal data breach to the competent national authority**."
  - Directive 2002/58/EC (12.07.02), OJ L 201, 31.7.2002, p. 37

Commission Regulation No 611/2013 (June, 2013)

- on the measures applicable to the notification of personal data breaches; protective measures
- "unintelligible" -> "encryption"
- Article 4, technological protection measures
  - "*Data shall be considered **unintelligible** if: (a) it **has been securely encrypted with a standardised algorithm** […] or (b) **it has been replaced by its hashed value** calculated with a standardised cryptographic keyed hash function, […]*"

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Exceptions for data breaches notification (II)

GDPR (EU) 679/2016, extending notification to all sectors

- "[…] the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 Hours." (preamble 85 and Article 33, GDPR)

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

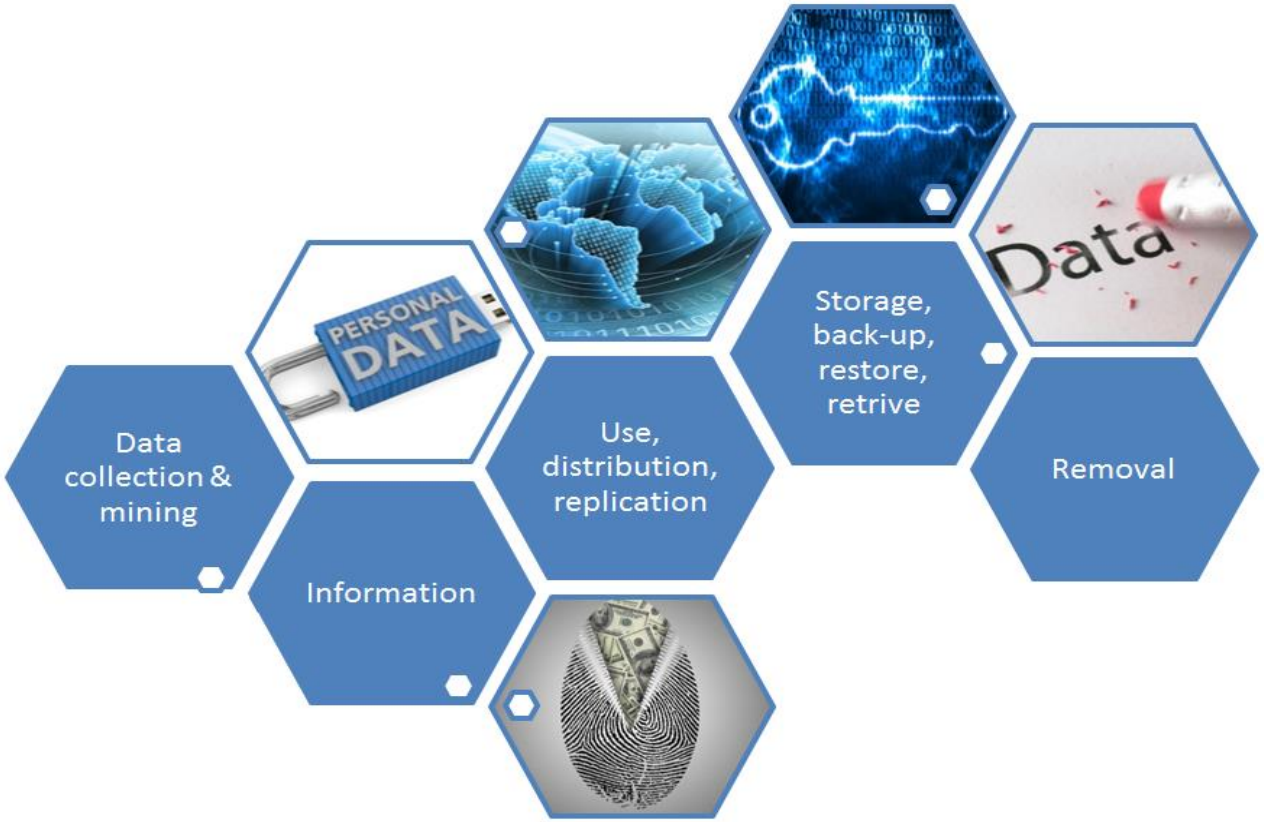
- "The communication […] to the data subject […] shall not be required if […]

a. the controller has implemented appropriate technological and organizational protection measures and those measures were applied to the data affected by the personal data breach, in particular those that render the data unintelligible to any person who is not authorised to access it, such as encryption […]" (Article 34 GDPR)

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

ENISA approach in protection of data / information

A lifecycle perspective



ENISA on crypto (I)

1. The Use of Cryptographic Techniques in Europe, available at: https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe
2. Algorithms, Key Sizes and Parameters Report – 2013, available at: https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report
3. Recommended cryptographic measures - Securing personal data, 2013, available at: https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data
4. Securing personal data in the context of data retention, 2013,available at: https://www.enisa.europa.eu/publications/securing-personal-data-in-the-context-of-data-retention
5. Algorithms, key size and parameters report 2014, available at: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
6. Study on cryptographic protocols, 2014, available at: https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols

ENISA on crypto (II)

- Supporting cooperation and inter-institutional debate
  1. Cooperation with Europol. Europol and ENISA Joint Statement on lawful criminal investigation that respects 21st Century data protection, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection
  2. ENISA's Opinion Paper on Encryption, Strong Encryption Safeguards our Digital Identity, December 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption
  3. Article 14 request
  4. ENISA/DG HOME/EC3 workshop

New/updated perspectives

EU Cybersecurity Strategy 2017 and encryption

JOIN/2017/0450 final, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, section 2.5 A cybersecurity competence network with a European Cybersecurity Research and Competence Centre:

"A particular focus of work by the competence network must be the lack of European capacity on assessing the ***encryption*** *of products and services used by citizens, businesses and governments within the Digital Single Market.* ***Strong encryption is the basis for secure digital identification systems that play a key role in effective cybersecurity*** *[…];* ***it also keeps people's intellectual property secure and enables protecting fundamental rights such as freedom of expression and the protection of personal data, and ensures safe online commerce****. […]"*

JOIN/2017/0450 final, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

Council conclusions on EU Cybersecurity Strategy - JOIN/2017/0450 final

Council Conclusions of 20 November 2017 on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

The Council [emphasis added by ENISA]:

*"17. WELCOMES the confirmation in the Joint Communication that **strong and trusted encryption is highly important** for properly **ensuring human rights and fundamental freedoms** in EU **and for public trust** in the Digital Single Market, while taking into account the need of law enforcement authorities to access data necessary for their investigations and the confirmation that secure digital identification and communication play both a key role in ensuring effective cybersecurity in EU;"*

*42. "WELCOMES the work by EU and its Member States in addressing the challenges posed by systems that allow criminals and terrorists to communicate in ways that competent authorities cannot access, STRESSES that this work has to keep in mind that **strong and trusted encryption is of high importance to cybersecurity and for the trust in the** Digital Single Market and ensuring the respect of human rights and fundamental freedoms;"*

49. "INVITES the EU and its Member States to continue working:

- *[…] to address the challenges posed by anonymising technologies while keeping in mind that **strong and trusted encryption is of high importance to cybersecurity and for the trust** in the Digital Single Market;"*

http://www.consilium.europa.eu/media/31666/st14435en17.pdf

Summary

01 The digital revolution depend on cybersecurity which relies on secure products, services and systems

02 Cryptography, and strong encryption are building blocks for cybersecurity

03 A cybersecurity Agency cannot ignore the cryptography area

04 The Agency needs to anticipate upcoming threats and challenges

Introduction on Post-Quantum Cryptography

Training at NIS Summer School 2018

Introduction on Post-Quantum cryptography
@NIS Summer School, 26-28 September 2018

Day / Slot	Title of presentation	Speaker	Hours
Wednesday, 9:00-11:00	Introduction to Post Quantum Cryptography track at ENISA summer school	Rodica Tirtea	9:00 – 9:10
	Cryptology, cryptography, cryptanalysis. Definitions, meanings, requirements, and current challenges	Tanja Lange	9:10-11:00
Wednesday, 11:30-12:30	Policies in the Quantum era	Nineta Polemi	11:30-12:30
Wednesday, 14:00-15:15	EU investment in quantum computing	Gustav Kalbe (call)	14:00-14:30
	What do quantum computers do?	Daniel J. Bernstein	14:30- 15:15
Wednesday, 15:45-18:00	Introduction to Post Quantum cryptography. Standardisation status	Michael Groves	15:45-17:00
	Challenges and opportunities. Business cases for Quantum key distribution	Bart Preneel	17:00-18:00
Thursday, 9:00-11:00	Lattice based post quantum cryptography	Vadim Lyubashevsky	9:00-10:00
	Practical implementation of lattice-based cryptography	Maire O'Neill	10:00-11:00
Thursday, 11:30-12:30	Case study on PQ identity-based cryptography	Michael Groves	11:30-12:30
Thursday, 14:00-15:15	Hash-based Signatures	Stefan-Lukas Gazdag	14:00-14:45
	Code-based Cryptography (I)	Daniel Loebenberger	14:45-15:15
Thursday, 15:45-18:00	Code-based Cryptography (II)	Daniel Loebenberger	15:45-16:00
	Protocol integration and implementation problems	Stefan-Lukas Gazdag	16:00-17:00
	The libpqcrypto software library for post-quantum cryptography	Daniel J. Bernstein	17:00-18:00
Friday 9:00-11:30	Summary of recommendations	Tanja Lange	9:00-9:30

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu