ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

εκδδα

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ημερίδα Προστασίας Δεδομένων

«ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ: Η ΕΦΑΡΜΟΓΗ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ»

«Ενίσχυση της ασφάλειας δεδομένων στο ΓΚΠΔ: ψευδωνυμοποίηση-κρυπτογράφηση»

Δρ Ευφροσύνη Σιουγλέ
ΕΕΠ, Ελέγκτρια Πληροφορικός

Ασφάλεια επεξεργασίας

- **Άρθρο 32 ΓΚΠΔ**: (…) ο ΥΕ και ο ΕΕ εφαρμόζουν κατάλληλα **τεχνικά και οργανωτικά μέτρα** προκειμένου να διασφαλίζεται το **κατάλληλο επίπεδο ασφάλειας** έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:

  α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων,

  β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

  γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος ασφάλειας λόγω φυσικού ή τεχνικού λόγου,

  δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

- Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι **κίνδυνοι** που απορρέουν από την επεξεργασία (…)

Προστασία δεδομένων ήδη από το σχεδιασμό

- **Άρθρο 25 ΓΚΠΔ:** (…) ο ΥΕ εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας,
- κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση,
- σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία
- κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των ΥΔ

3

Οριοθέτηση εννοιών

- Ψευδωνυμοποίηση (αρ. 4(5)): *η επεξεργασία δεδομένων κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση* ***συμπληρωματικών πληροφοριών****, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες* ***διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα*** *προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε* ***ταυτοποιημένο ή ταυτοποιήσιμο*** *φυσικό πρόσωπο.*

Οριοθέτηση εννοιών

Ψευδωνυμοποίηση: **αντικατάσταση** ενός ή περισσοτέρων αναγνωριστικών (identifiers) με ψευδώνυμα + **προστασία και διαχωρισμός** των συμπληρωματικών πληροφοριών από τα ψευδωνυμοποιημένα δεδομένα

Αναγνωριστικά (identifiers): στοιχεία που επιτρέπουν την, άμεση ή έμμεση, **ταυτοποίηση** του ΥΔ

Συμπληρωματικές πληροφορίες: **αντιστοίχιση/σύνδεση** μεταξύ αναγνωριστικών και ψευδωνύμων

Ψευδωνυμοποιημένα δεδομένα: τα δεδομένα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με **ταυτοποιήσιμο φυσικό πρόσωπο (αιτ. 26 ΓΚΠΔ)**

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Οριοθέτηση εννοιών

Για να **κριθεί** κατά πόσο ένα φυσικό πρόσωπο είναι **ταυτοποιήσιμο**:

- θα πρέπει να λαμβάνονται υπόψη **όλα τα μέσα** τα οποία είναι **ευλόγως πιθανό** ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο **διαχωρισμός του (singling out),**
- είτε από τον **ΥΕ** είτε από **τρίτο,** για την **άμεση ή έμμεση** εξακρίβωση της ταυτότητάς του

Μέσα ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας:

- όλοι **οι αντικειμενικοί παράγοντες**, όπως τα **έξοδα** και ο **χρόνος** για την ταυτοποίηση,
- λαμβανομένων υπόψη της διαθέσιμης **τεχνολογίας** και των **εξελίξεων** αυτής

Οι αρχές της προστασίας δεν θα πρέπει να εφαρμόζονται σε **ανώνυμες πληροφορίες**,

- δηλ. πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο ή
- σε δεδομένα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η **ταυτότητα** του ΥΔ να **μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί**

Η «ευρεία» έννοια του αναγνωριστικού

- Εκτός από τα **αναγνωριστικά** (identifiers), υπάρχουν και τα **οιονεί-αναγνωριστικά** (quasi-identifiers), τα οποία συνδυαστικά δύναται να οδηγήσουν σε ταυτοποίηση του ΥΔ

Όνομα	Ηλικία	Φύλο	Τ.Κ.	Άθλημα
Α1	15	Α	53715	Κολύμβηση
Α2	30	Γ	53715	Τένις
Α3	45	Γ	53703	Μπάσκετ
Α4	60	Α	53703	Στίβος
Α5	35	Γ	53706	Ενόργανη

- Σύμφωνα με έρευνα στις ΗΠΑ 2002, το 87% του πληθυσμού των ΗΠΑ μπορεί ν ταυτοποιηθεί από την τριπλέτα «Ταχ. Κώδικας - ημερομηνία γέννησης – φύλο»
- Τα αναγνωριστικά μας «έξυπνης» κινητής συσκευής: IMSI, IMEI, MAC

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Ψευδωνυμοποίηση: παράδειγμα

Αρχικά δεδομένα

Όνομα: Νικόλαος
Επώνυμο: Παπαδόπουλος
Ηλικία: 35
Φύλο: Άνδρας
Χώρα: Ελλάδα
Αριθμός τηλ.: 6945 153 146
Επάγγελμα: Προγραμματιστής

Συμπληρωματικές προστατευμένες πληροφορίες

Ψευδώνυμο: A50
Όνομα: Νικόλαος
Επώνυμο: Παπαδόπουλος
Ηλικία: 35
Αριθμός τηλ.: 6945 153 146

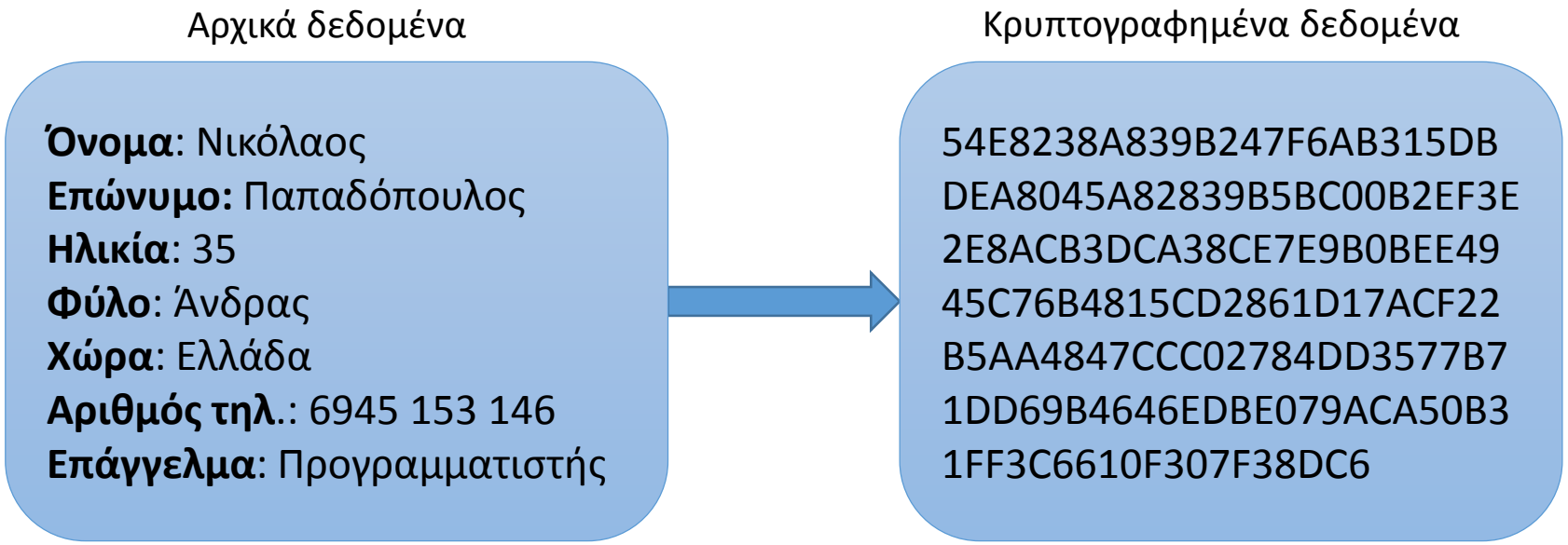
Ψευδωνυμοποιημένα δεδομένα

Ψευδώνυμο: A50
Φύλο: Άνδρας
Χώρα: Ελλάδα
Επάγγελμα: Προγραμματιστής

Κρυπτογράφηση δεδομένων

Κρυπτογράφηση:

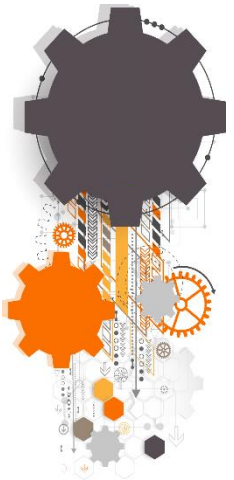
- μετατροπή του συνόλου των δεδομένων σε ακατάληπτη/μη αναγνώσιμη μορφή
- επεξεργασία των δεδομένων μετά από αποκρυπτογράφηση



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Ρόλος ψευδωνυμοποίησης - κρυπτογράφησης στο ΓΚΠΔ

- Κατάλληλα μέτρα για την **ασφάλεια** της επεξεργασίας (αρ. 32(1)) (ψευδ/ση, κρυπ/ση)
- Ψευδωνυμοποίηση: κατάλληλο μέτρο για την προστασία δεδομένων **ήδη από το σχεδιασμό** (αρ. 25(1))
- Μεταξύ των **κατάλληλων εγγυήσεων** για:
  - να κριθεί η **συμβατότητα** άλλου σκοπού με τον αρχικό σκοπό συλλογής των δεδομένων (αρ. 6(4)) (ψευδ/ση, κρυπ/ση)
  - για την επεξεργασία για σκοπούς **αρχειοθέτησης** προς το δημόσιο συμφέρον ή σκοπούς **επιστημονικής ή ιστορικής** έρευνας ή **στατιστικούς** σκοπούς (αρ. 5(1)(β), 89(1)) (ψευδ/ση)
- **Κώδικες δεοντολογίας**: περιλαμβάνεται ο προσδιορισμός της ψευδωνυμοποίησης (αρ. 40(2)(δ))

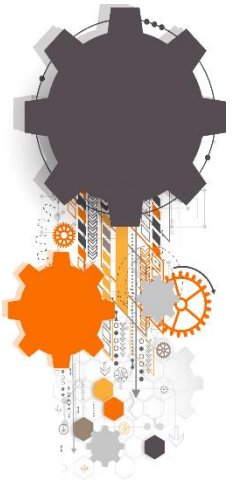


Ρόλος ψευδωνυμοποίησης - κρυπτογράφησης στο ΓΚΠΔ

- **Περιστατικά παραβίασης** – κρυπτογράφηση:
  - Η ανακοίνωση στα ΥΔ **δεν απαιτείται** όταν ο ΥΕ εφάρμοσε μέτρα που καθιστούν **μη κατανοητά** τα δεδομένα όπως η **κρυπτογράφηση** (αρ. 34(3))
- **Περιστατικά παραβίασης** - ψευδωνυμοποίηση:
  - μέτρο που **δύναται να μειώσει** την πιθανότητα ταυτοποίησης των ΥΔ
  - **λαμβάνεται υπόψη** από τον ΥΕ για την εκτίμηση του κινδύνου και την απόφαση ανακοίνωσης στα ΥΔ
- **Εκτίμηση αντικτύπου**:
  - σύνδεση κινδύνου με την έννοια της ενδεχόμενης βλάβης στα ΥΔ: **παράνομη άρση της ψευδωνυμοποίησης** (αιτ. 75)
  - αποτελεσματικότητα της ψευδωνυμοποίησης ως προς τον **υπολειπόμενο κίνδυνο**

Ρόλος ψευδωνυμοποίησης στο ΓΚΠΔ

- **Άρθρο 11**: Όταν ο ΥΕ **μπορεί να αποδείξει** ότι δεν είναι σε θέση **να εξακριβώσει την ταυτότητα** του ΥΔ, ο ΥΕ ενημερώνει σχετικά το ΥΔ, εάν είναι δυνατόν
- Στις περιπτώσεις αυτές, τα άρθρα 15 ως 20 δεν εφαρμόζονται, εκτός εάν το ΥΔ (…) παρέχει συμπληρωματικές πληροφορίες που επιτρέπουν την εξακρίβωση της ταυτότητάς του
- Άρθρα 15-20: δικαιώματα πρόσβασης/διόρθωσης /διαγραφής /περιορισμού επεξεργασίας/φορητότητας δεδομένων
- Στην περίπτωση αυτή:
  - κατάλληλα δομημένες και τεκμηριωμένες **διαδικασίες** από τον ΥΕ και
  - **διαφάνεια** της διαδικασίας ψευδωνυμοποίησης

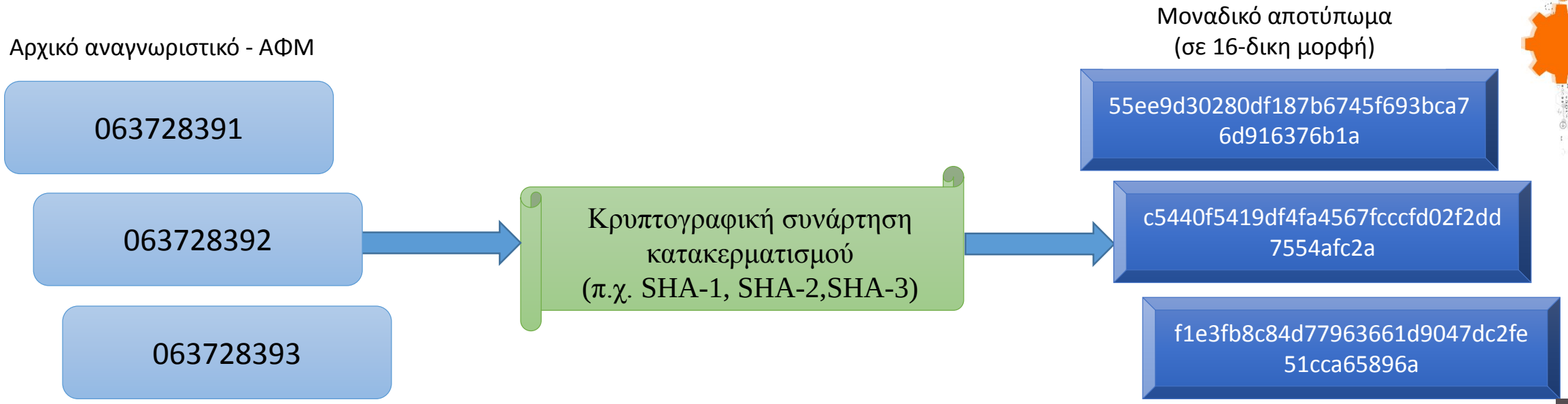


ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Τεχνικές ψευδωνυμοποίησης

Κρυπτογραφική συνάρτηση κατακερματισμού (cryptographic hash function):

- μετασχηματισμός του αρχικού αναγνωριστικού (όπως ΑΦΜ) σε ένα **μοναδικό** ακατάληπτο **αποτύπωμα**/hash value (=**ψευδώνυμο**)
- μαθηματικά **μη αναστρέψιμη** (irreversible) συνάρτηση
- το ίδιο ψευδώνυμο **αντιστοιχίζεται πάντα** στο ίδιο αναγνωριστικό

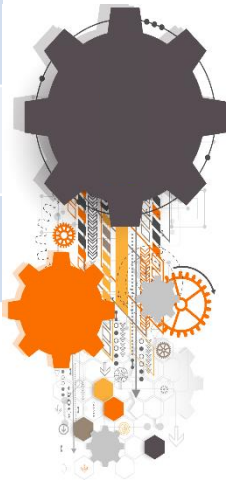


ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Τεχνικές ψευδωνυμοποίησης

- Είναι **ανθεκτική** η τεχνική αυτή σε επιθέσεις **άρσης της ψευδωνυμοποίησης**;
- Γίνεται να επαληθευτεί αν ΥΔ με συγκεκριμένο ΑΦΜ (αρχικό αναγνωριστικό) βρίσκεται σε ψευδωνυμοποιημένη λίστα;
  - υπολογισμός του αποτυπώματος του ΑΦΜ (έστω 063728393) με χρήση της συνάρτησης κατακερματισμού
  - σύγκριση αν το αποτύπωμα ταιριάζει με κάποιο από αυτά της λίστας

Αποτύπωμα	Φύλλο	Ασθένεια	
55ee9d30280df187b6745f693bca76d916376b1a	Α	γρίπη	☒
c5440f5419df4fa4567fcccfd02f2dd7554afc2a	Γ	γαστρεντερίτιδα	☒
2f9123728b8a09fa525f202e5fa497681020db0e	Α	ανεύρυσμα	☑



- Το ΥΔ με ΑΦΜ: 063728393 έχει ανεύρυσμα!

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Τεχνικές ψευδωνυμοποίησης

- **Gravatar:** δωρεάν υπηρεσία που επιτρέπει στους χρήστες να τους ακολουθεί αυτόματα το ίδιο "**avata**r" (εικόνα προφίλ) σε οποιοδήποτε site συμμετέχουν, το οποίο υποστηρίζει Gravatar
- **Προϋπόθεση**: ο χρήστης συμμετέχει στα sites με το **ίδιο email**
- **Avatar:** βασίζεται στο **md5** αποτύπωμα του email και είναι **δημόσια προσβάσιμο**

md5("MyEmailAddress@example.com") =
"f9879d71855b5ff21e4963273a886bfc"

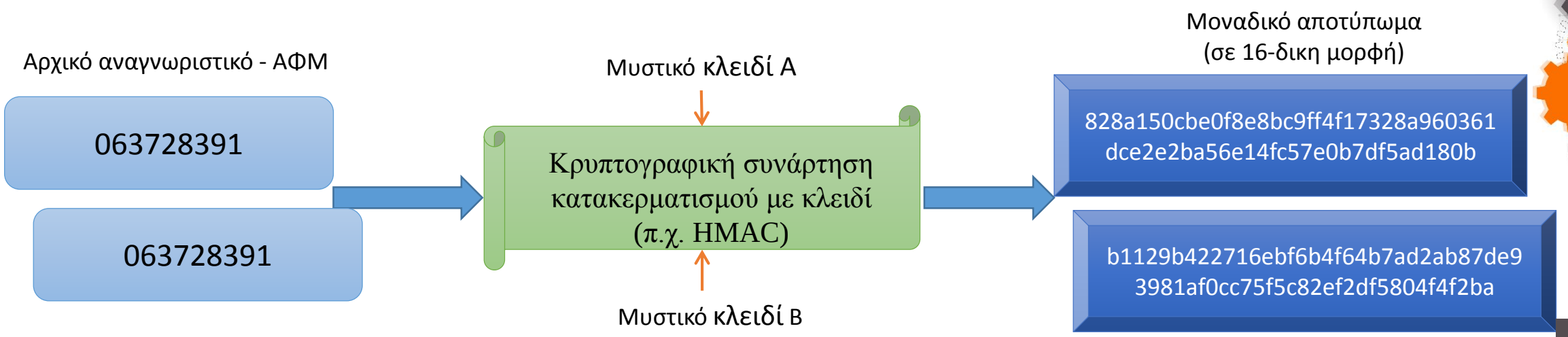
Gravatar URL: https://www.gravatar.com/avatar/HASH

- Από τα αποτυπώματα προσδιορίστηκαν τα emails ανώνυμων σχολιαστών ενός γαλλικού πολιτικού ιστολογίου: επετεύχθη αντιστοίχιση **avatar (=ψευδωνύμου)** → **email**

Τεχνικές ψευδωνυμοποίησης

Κρυπτογραφική συνάρτηση κατακερματισμού με μυστικό «κλειδί» (keyed hash functions):

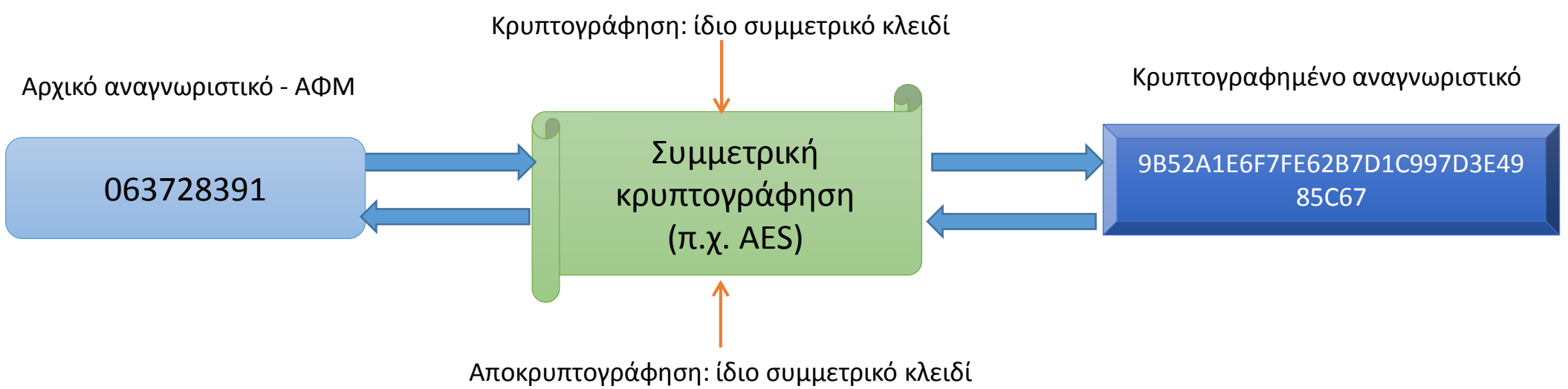
- το ίδιο αναγνωριστικό μπορεί να αντιστοιχηθεί σε πολλαπλά μοναδικά διαφορετικά αποτυπώματα (αναλόγως το «κλειδί») (**unlinkability**)
- ο τρίτος **δεν είναι σε θέση να επαληθεύσει** εάν ένα ψευδώνυμο αντιστοιχεί σε συγκεκριμένο αναγνωριστικό (χωρίς γνώση του «κλειδιού»)
- ασφαλής διαγραφή του «κλειδιού» + συνάρτηση κρυπτογραφικά ισχυρή → υπολογιστικά δύσκολη η άρση της ψευδωνυμοποίησης



Τεχνικές ψευδωνυμοποίησης

Συμμετρική κρυπτογράφηση (symmetric encryption):

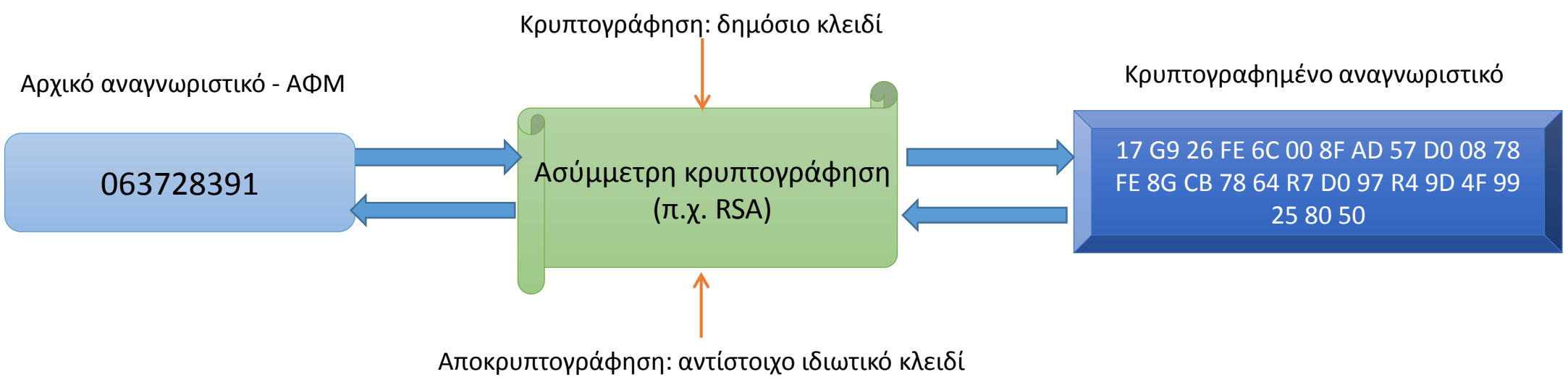
- **ντετερμινιστική (deterministic) μορφή**: κρυπτογράφηση του ίδιου αναγνωριστικού με το ίδιο μυστικό κλειδί παράγει πάντα το ίδιο ψευδώνυμο
- Αποκρυπτογράφηση → ανάκτηση του αρχικού αναγνωριστικού
- Αποτελεσματικότητα της μεθόδου: χρήση σύγχρονων (state-of the art) αλγόριθμων και κλειδιών επαρκούς μήκους



Τεχνικές ψευδωνυμοποίησης

Ασύμμετρη κρυπτογράφηση (asymmetric encryption):

- **Πιθανοτική (probabilistic) μορφή:** παραγωγή διαφορετικού, κάθε φορά, ψευδωνύμου για το ίδιο αναγνωριστικό με εισαγωγή τυχαιότητας (και χρήση του ίδιου δημόσιου κλειδιού)
- Δεν επηρεάζεται η δυνατότητα αποκρυπτογράφησης από τον κάτοχο του ιδιωτικού κλειδιού
- Εφαρμογή σε περιπτώσεις χρήσης **πολλαπλών ψευδωνύμων για το ίδιο ΥΔ**:
  - πχ απόδοση διαφορετικού ψευδώνυμου σε κάθε διαφορετική οικιακή μέτρηση προερχόμενη από έξυπνο μετρητή για τον ίδιο καταναλωτή



Τεχνικές ψευδωνυμοποίησης

- **Άλλες τεχνικές**: masking, scrambling (εφαρμογή συνήθως σε αποθηκευμένα δεδομένα)

- **Masking**: τεχνική απόκρυψης μέρους του αναγνωριστικού με τυχαίους χαρακτήρες ή άλλα δεδομένα

AB 034412 → XX XXXX12

- **Scrambling**: τεχνική ανάμειξης/μετάθεσης των χαρακτήρων/στοιχείων του αναγνωριστικού

First Name	Surname	Age
Alice	Smith	42
Bob	Johnson	21
Dave	Doe	74
Eve	Jackson	44
Grace	Chang	32

Surname is Shuffled

First Name	Surname	Age
Alice	Doe	42
Bob	Jackson	21
Dave	Chang	74
Eve	Smith	44
Grace	Johnson	32

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Συμπεράσματα

- Ο ΓΚΠΔ προκρίνει την **ψευδωνυμοποίηση** και την **κρυπτογράφηση**
- Η ψευδωνυμοποίηση:
  - συνεισφέρει στην **απόκρυψη** των **στοιχείων ταυτοποίησης** του ΥΔ και
  - υποστηρίζει την **ελαχιστοποίηση των δεδομένων** και τη δυνατότητα **μη συνδεσιμότητας (unlinkability)** σε διαφορετικά περιβάλλοντα/χώρους/τομείς επεξεργασίας
- Η ψευδωνυμοποίηση **δεν αποτελεί ανωνυμοποίηση**
  - μπορεί να συνδυαστεί με τεχνικές ανωνυμοποίησης
- Επιλογή της κατάλληλης τεχνικής ψευδωνυμοποίησης: βάσει της μελέτης **εκτίμησης αντικτύπου στην προστασία δεδομένων**
- Βελτίωση αποτελεσματικότητας ψευδωνυμοποίησης: χρήση σύγχρονων τεχνικών κρυπτογράφησης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
εκδδα
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Ευχαριστούμε πολύ για την προσοχή σας