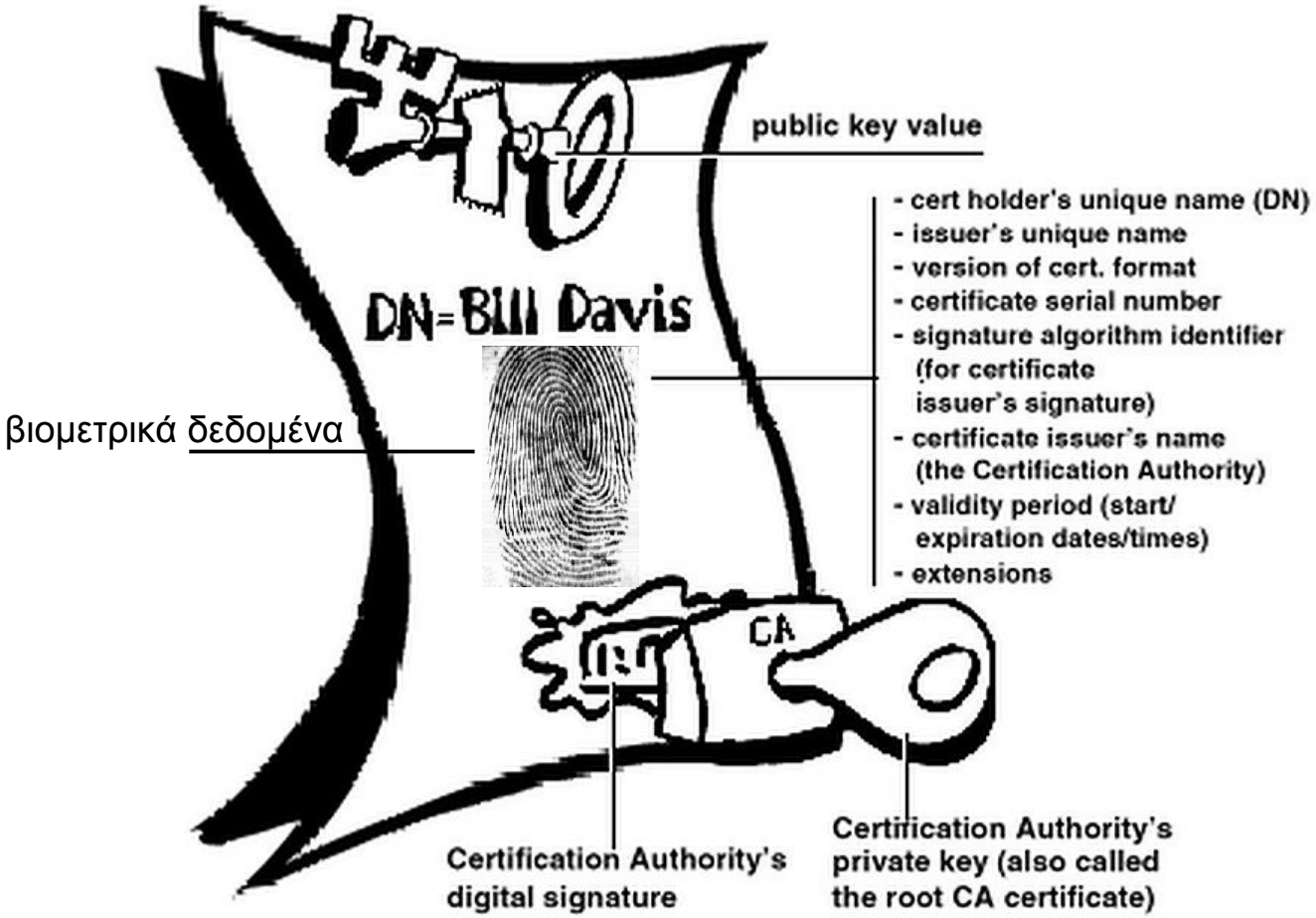
Βιομετρικά κλειδιά, κρυπτογραφία και υποδομή διανομής

του φοιτητή
Παναγιώτη Ματάμη
Αρ. Μητρώου: 001582

επιβλέπων καθηγητής
Ηλιούδης Χρήστος

PKI + βιομετρικά δεδομένα;



- **Υποδομή βιοκρυπτογραφικού κλειδού (BKI)**

Τι είναι Βιομετρία;

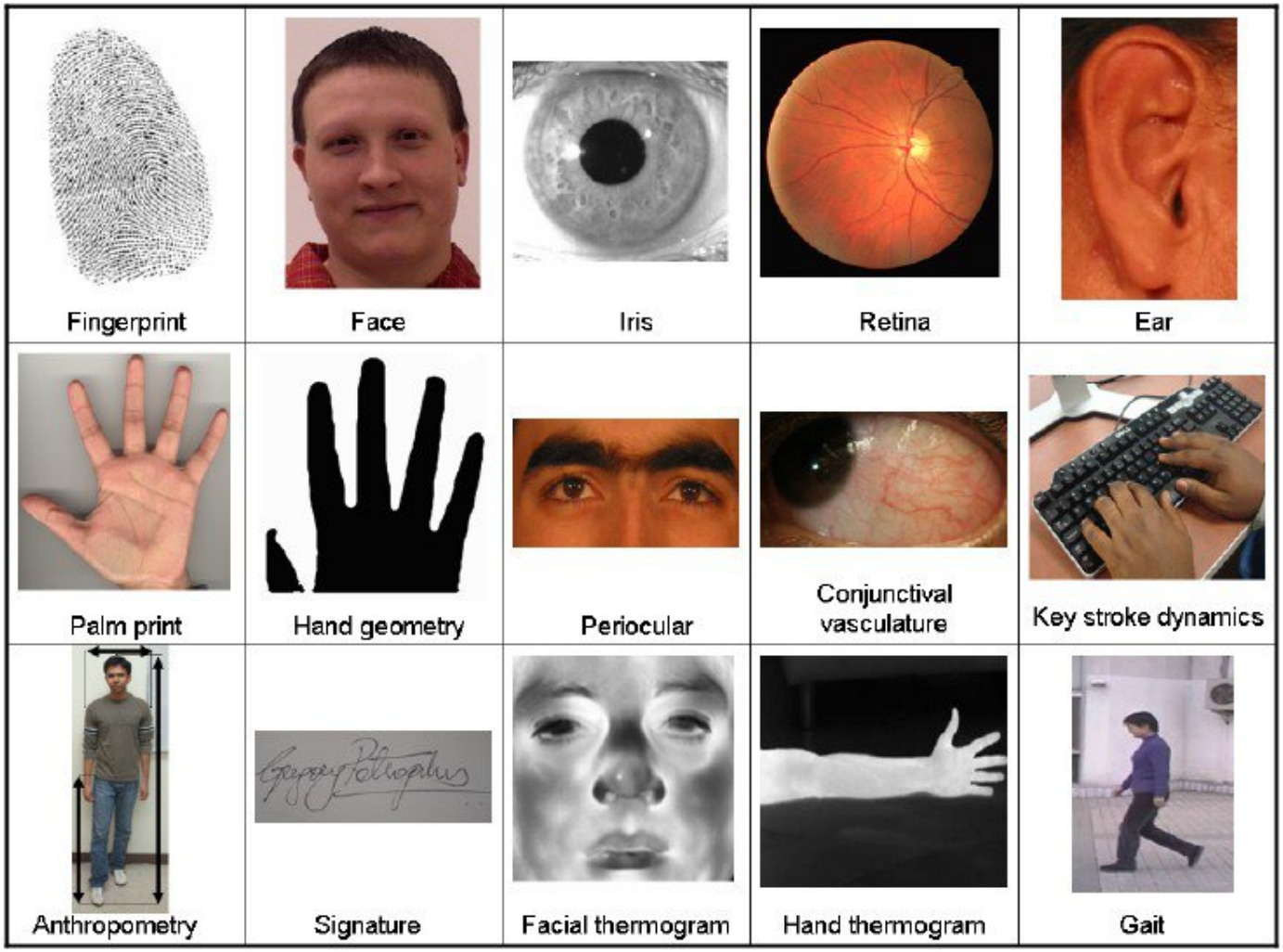
Βιομετρική αναγνώριση ή απλά βιομετρία, ονομάζεται η αναγνώριση ατόμων, με αυτόματο τρόπο, βάσει ανατομικών χαρακτηριστικών και χαρακτηριστικών που έχει η συμπεριφορά τους.

- Δακτυλικά αποτυπώματα
- Αναγνώριση προσώπου
- Ίριδα
- DNA
- Φωνή
- Αποτύπωμα Παλάμης
- Βάδισμα

- Πληκτρολόγηση
- Υπογραφή
- Κερατοειδής
- Γεωμετρία χεριού
- Θερμογράφημα χεριού ή προσώπου
- Τοποθεσία;

καταλληλότητα βιομετρικών στοιχείων

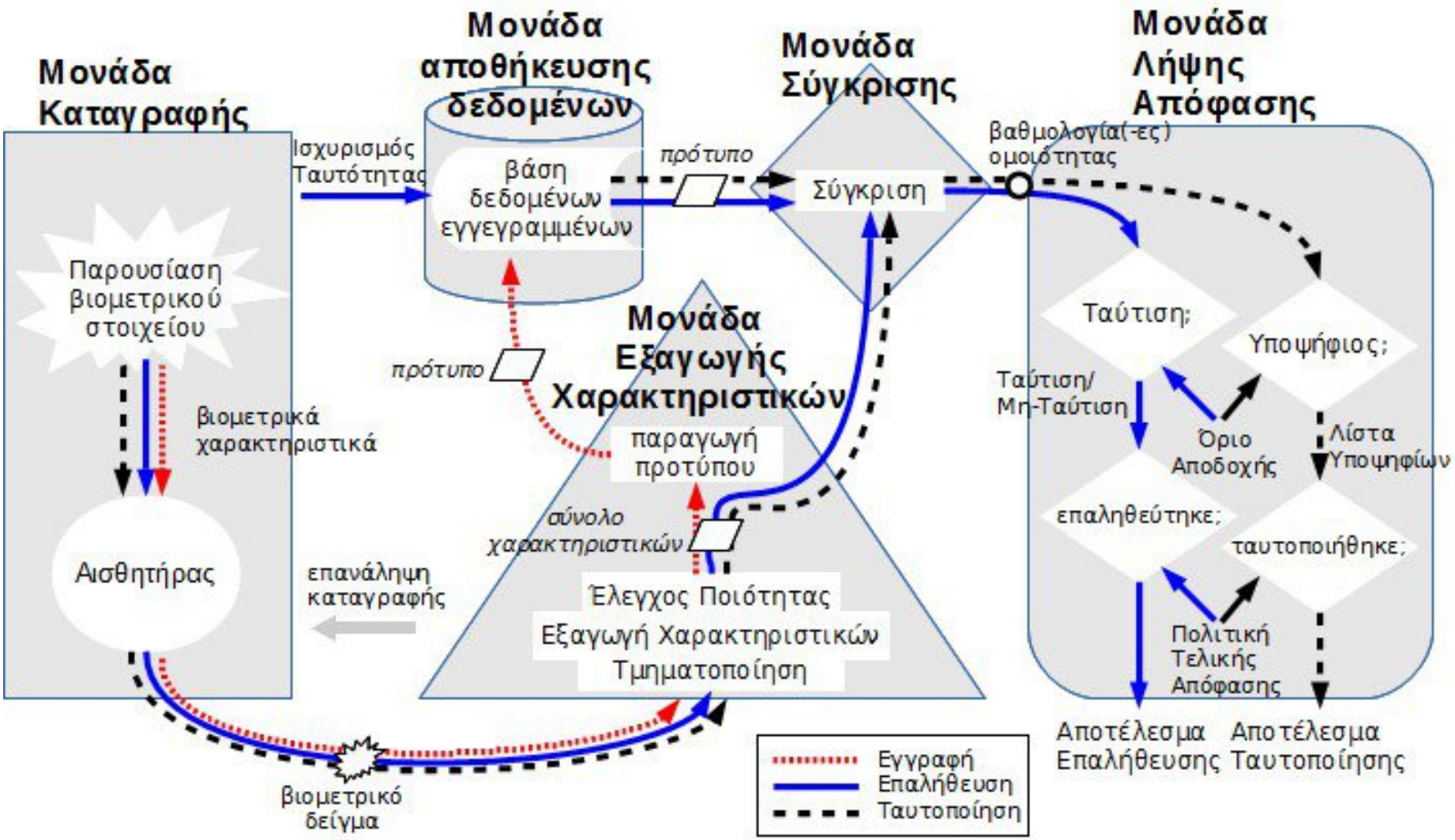
- καθολικότητα
- μοναδικότητα
- μονιμότητα
- μετρησιμότητα
- απόδοση
- αποδοχή
- παραποίηση



Διαφορές μεταξύ βιομετρίας και PIN και κωδικών

- Τα βιομετρικά στοιχεία
  - δεν μεταδίδονται ούτε μοιράζονται.
  - παραμένουν για πάντα.
  - μπορούν να αποκτηθούν χωρίς να το ξέρουμε.
- Τα βιομετρικά δείγματα δεν είναι ακριβώς ίδια κάθε φορά.
- Τα βιομετρικά στοιχεία είναι ίδια για όλες τις εφαρμογές ενώ οι κωδικοί διαφορετικοί για κάθε εφαρμογή.
- Η βιομετρία απαιτεί ειδικά μηχανήματα.
- Η βιομετρία επιτρέπει τον εντοπισμό κάποιου μεταξύ πολλών συστημάτων.
- **Ένα βιομετρικό σύστημα μπορεί να αναγνωρίσει αν κάποιος είναι γνωστός στο σύστημα ή όχι.**

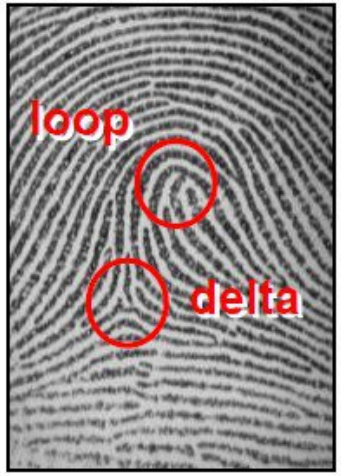
Βιομετρικό Σύστημα

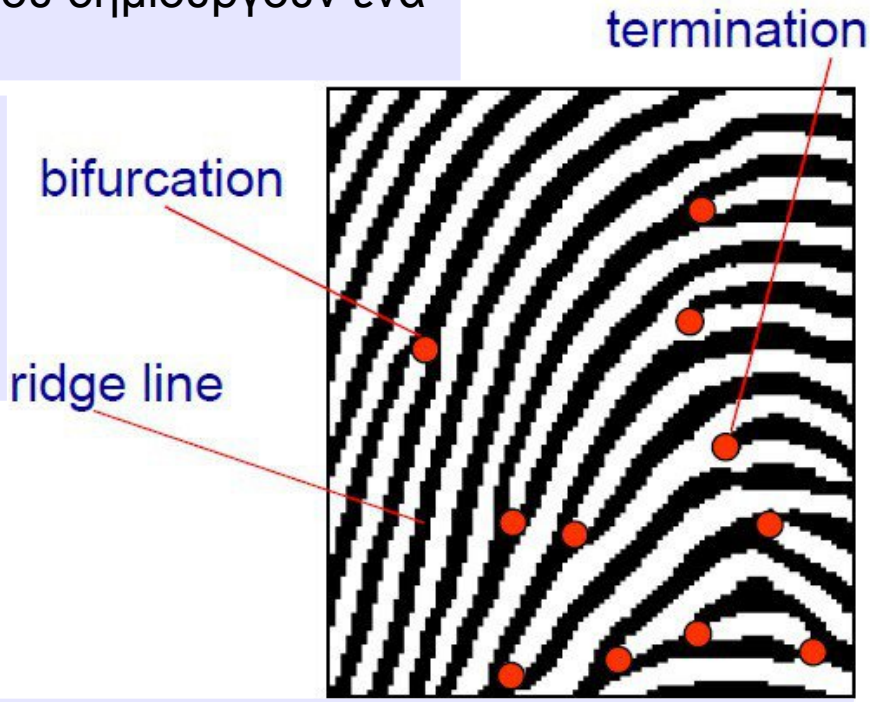


Δακτυλικά αποτυπώματα

Ένα δακτυλικό αποτύπωμα αποτελείται από ένα σύνολο γραμμών (ridge lines), παράλληλων σε μεγάλο βαθμό, που δημιουργούν ένα μοτίβο (ridge pattern)

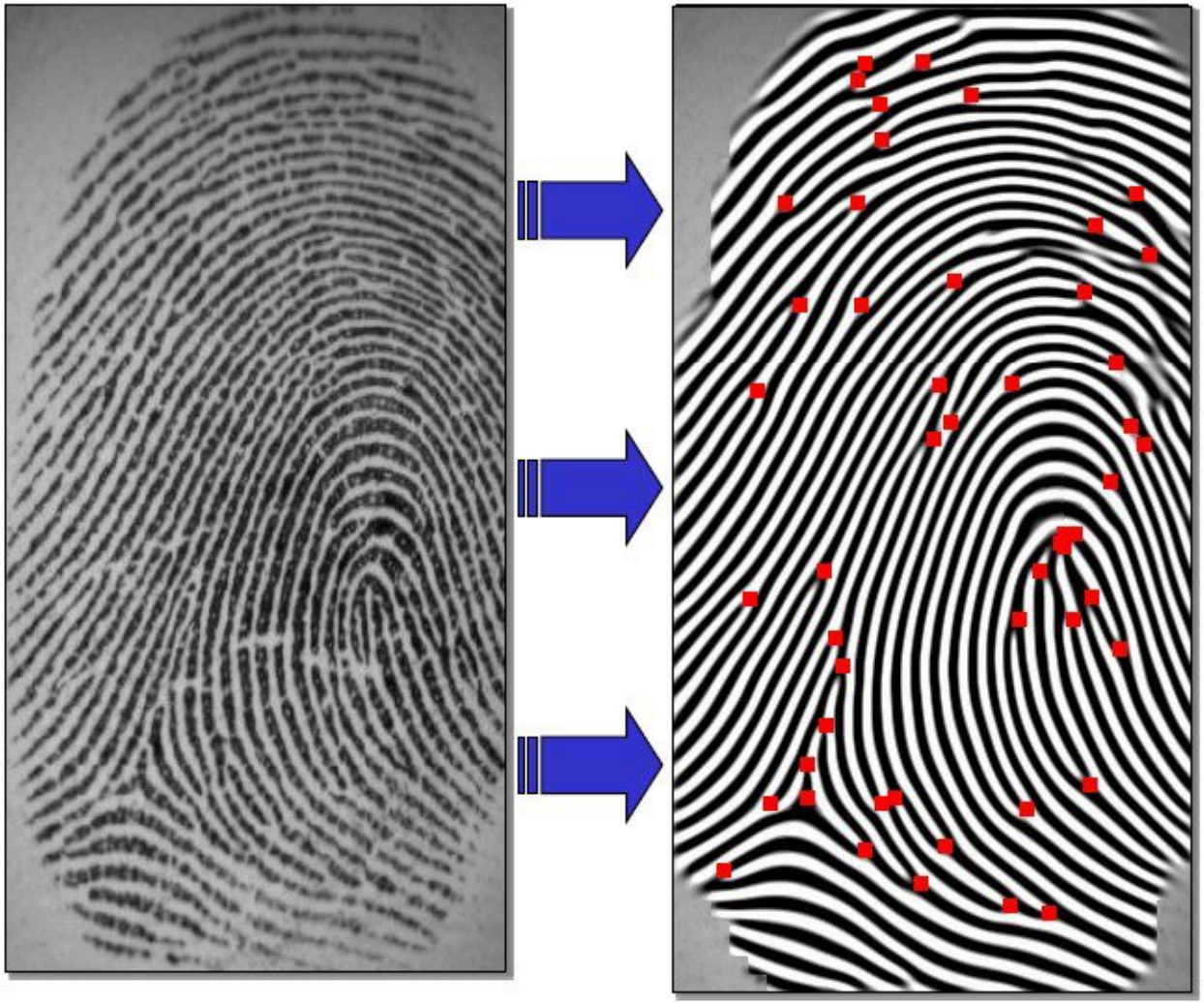
Μερικές φορές οι γραμμές δημιουργούν τοπικές ιδιαιτερότητες (macro-singularities), που αποκαλούνται σπείρα-whorl (O), βρόχος-loop (U) και δέλτα-delta (Δ). Χρησιμοποιούνται συχνά για την κατηγοριοποίηση και ευθυγράμμιση των δακτυλικών αποτυπωμάτων.

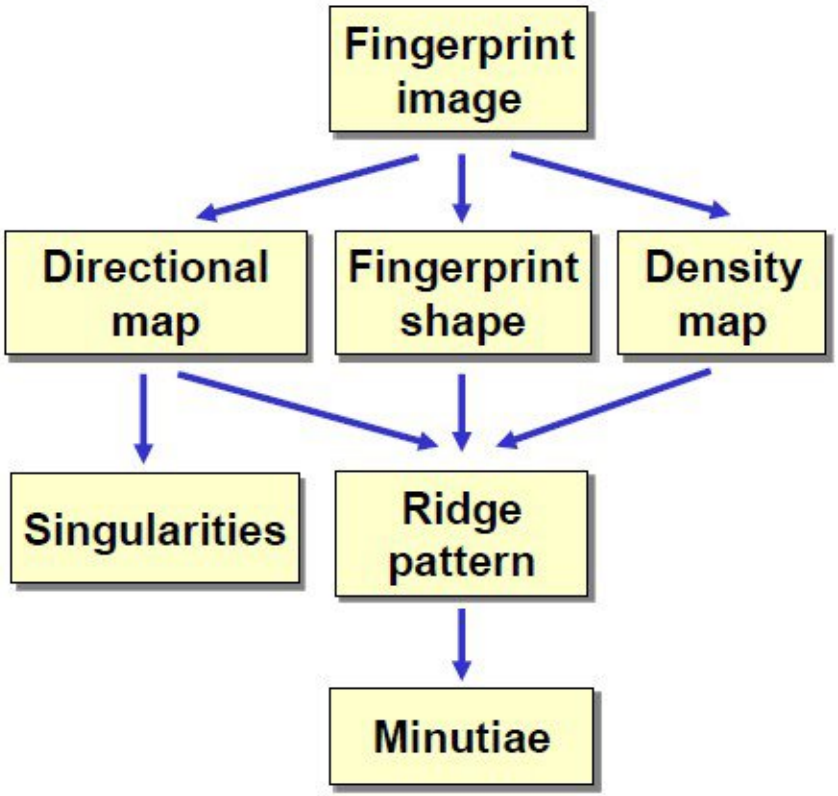




οι μικρολεπτομέρειες (minutiae), ή χαρακτηριστικά Galton, καθορίζονται από τον τερματισμό ή τον διαχωρισμό των γραμμών.

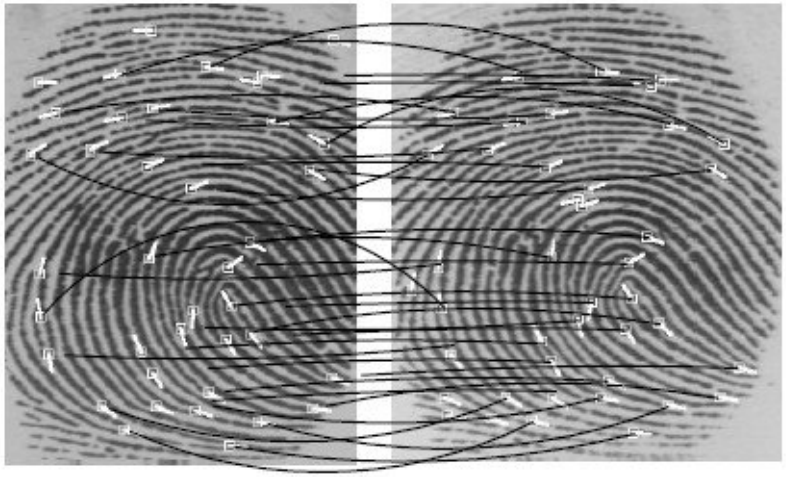
Feature extraction steps

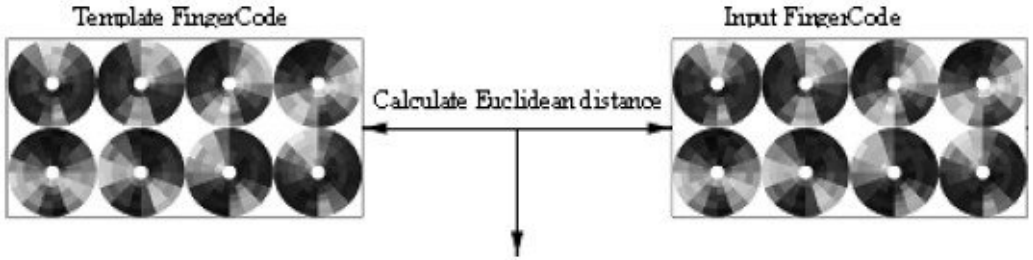




Προσεγγίσεις για τη σύγκριση δακτυλικών αποτυπωμάτων

- Minutiae-based matching
  - The most popular and widely used technique. Minutiae-based matching consists in finding the alignment that results in the maximum number of minutiae pairings.
- Correlation-based matching
  - Two fingerprints are superimposed and the correlation between corresponding pixels is computed for different alignments.
- Ridge feature-based matching
  - Other features of the fingerprint ridge pattern (e.g., *local orientation* and *frequency*, *ridge shape*, *texture information*) may be extracted more reliably than minutiae in *low-quality images*.





Βασικές μετρήσεις απόδοσης

- Δείκτης αποτυχίας εγγραφής (FTE)
- Δείκτης αποτυχίας απόκτησης (FTA)
- Δείκτης λανθασμένης μη-ταύτισης (FNMR)
- Δείκτης λανθασμένης ταύτισης (FMR)

Μετρήσεις απόδοσης ενός συστήματος επαλήθευσης

- Δείκτης λανθασμένων απορρίψεων (FRR)
- Δείκτης λανθασμένων αποδοχών (FAR)
- Δείκτης αυθεντικών αποδοχών (GAR) ή Δείκτης πραγματικών αποδοχών (TAR)
- Γενικευμένος δείκτης λανθασμένων απορρίψεων (GFRR)
- Γενικευμένος δείκτης λανθασμένων αποδοχών (GFAR)

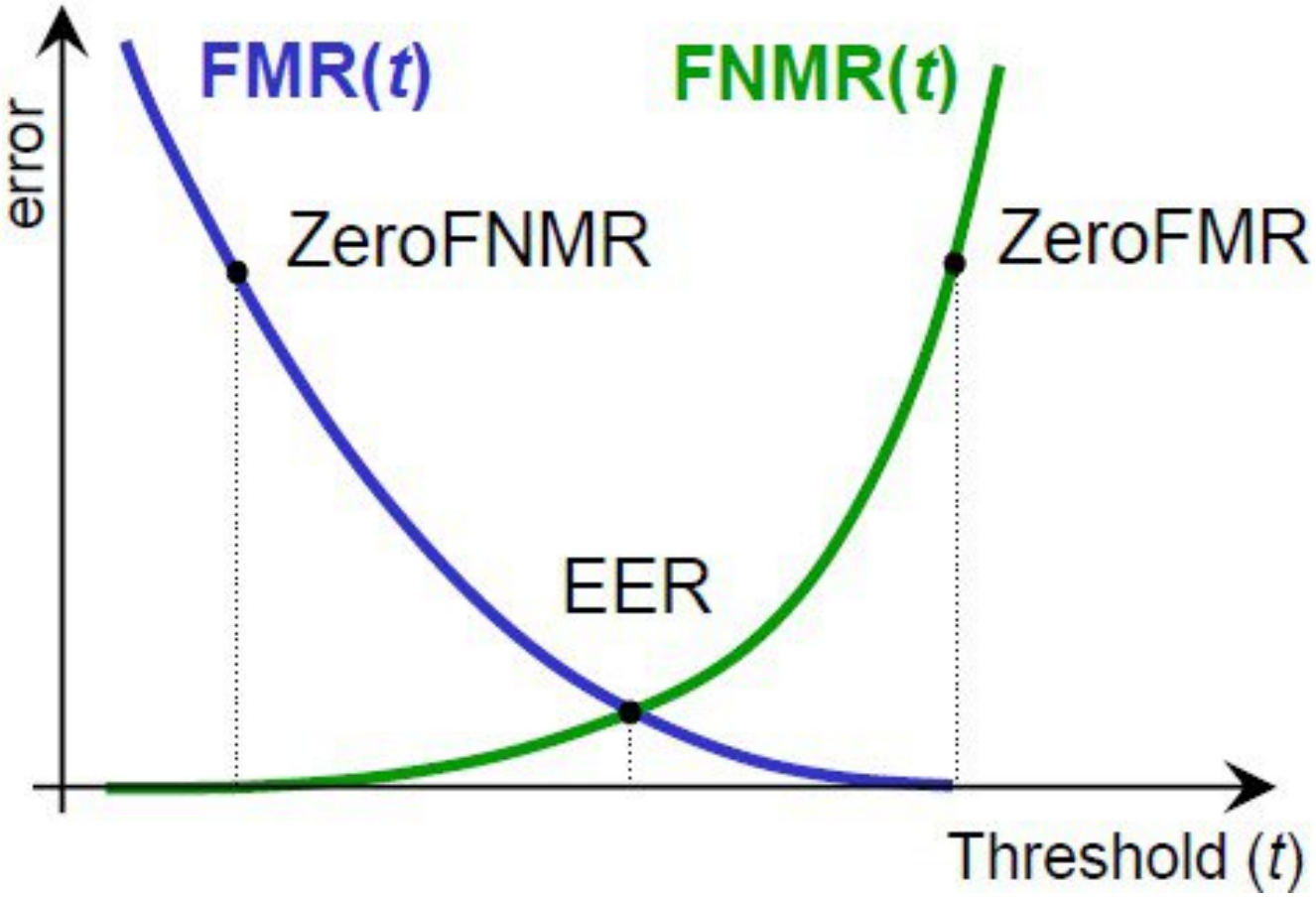
Μετρήσεις απόδοσης ενός συστήματος ταυτοποίησης

- Δείκτης σωστής ταυτοποίησης (CIR) ή δείκτης αληθώς θετικής ταυτοποίησης (TPIR)
- Δείκτης ψευδώς αρνητικής ταυτοποίησης (FNIR)
- Δείκτης ψευδώς θετικής ταυτοποίησης (FPIR)

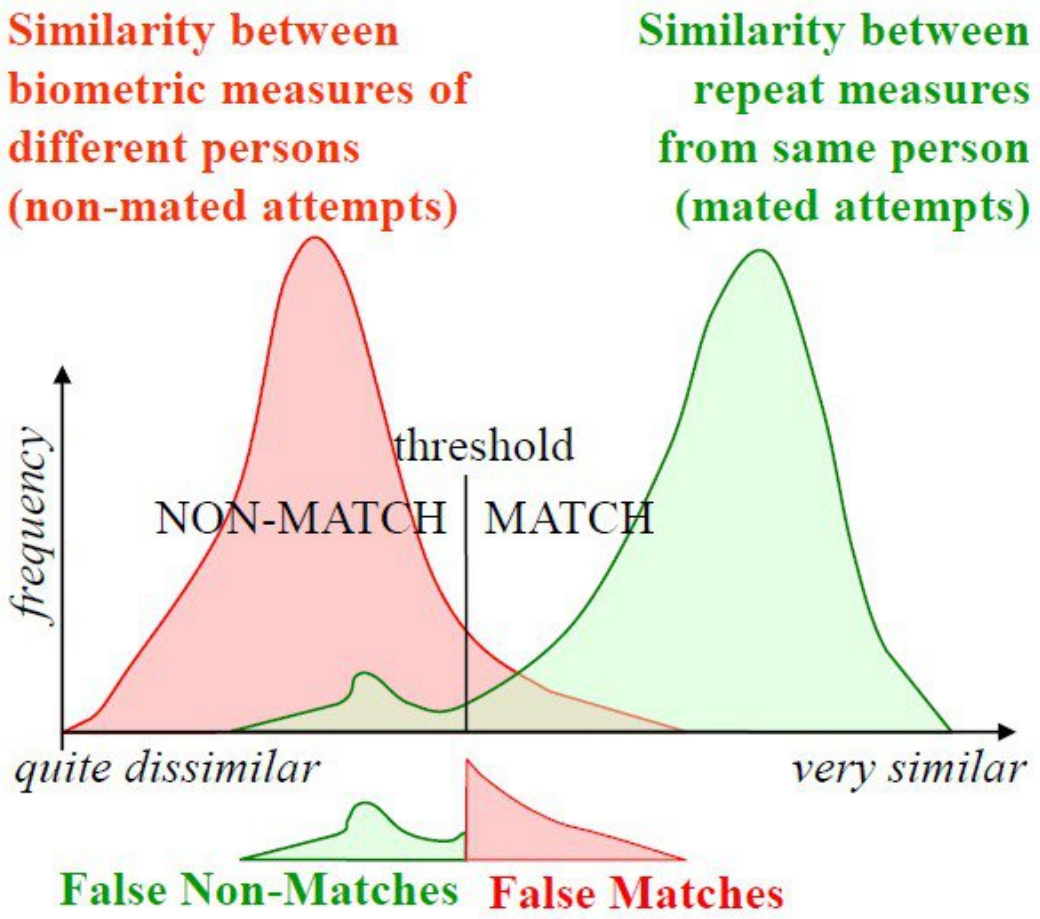
Άλλες μετρήσεις απόδοσης

- Κατανομή Αυθεντικών βαθμολογιών (Genuine score distribution και κατανομή Κακόβουλων βαθμολογιών (Impostor score distribution)
- Δείκτης ισάριθμων Σφαλμάτων – EER (equal error rate)
- EER*
- FMR100
- FMR1000
- ZeroFMR
- ZeroFNMR

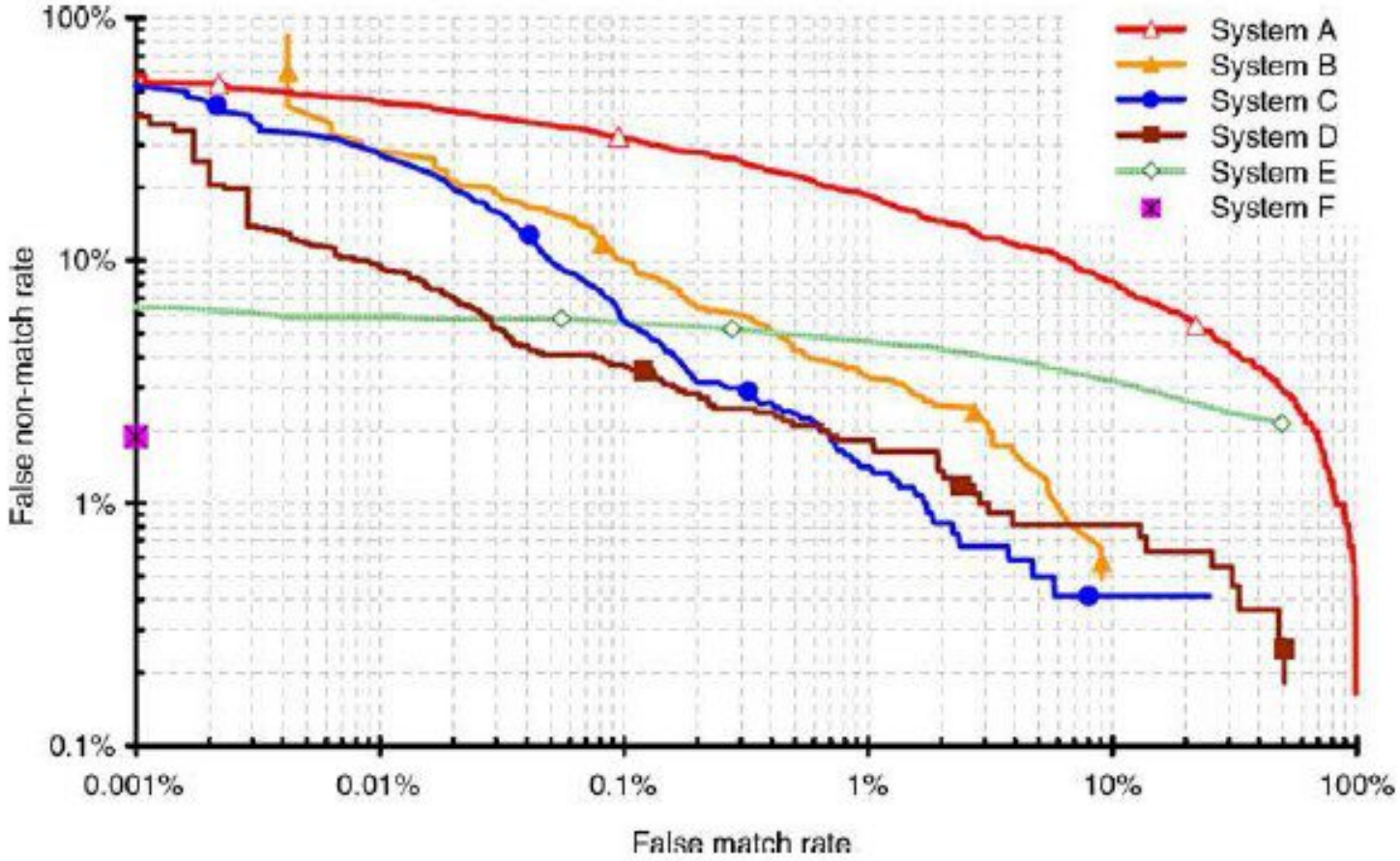
καμπύλες FMR(t) και FNMR(t)



Κατανομή βαθμολογίας Ομοιότητας



Καμπύλη DET


100%
10%
1%
0.1%
False non-match rate
0.001%
0.01%
0.1%
1%
10%
100%
False match rate
System A
System B
System C
System D
System E
System F

Κατηγορίες βιομετρικών εφαρμογών

- Συνεργάσιμοι και μη συνεργάσιμοι χρήστες
- Φανερή ή συγκεκαλυμμένη εφαρμογή
- Εξοικειωμένοι ή μη εξοικειωμένοι χρήστες
- Με επίβλεψη ή χωρίς επίβλεψη
- Ελεγχόμενο περιβάλλον και μη ελεγχόμενο περιβάλλον
- Ανοιχτό ή κλειστό σύστημα

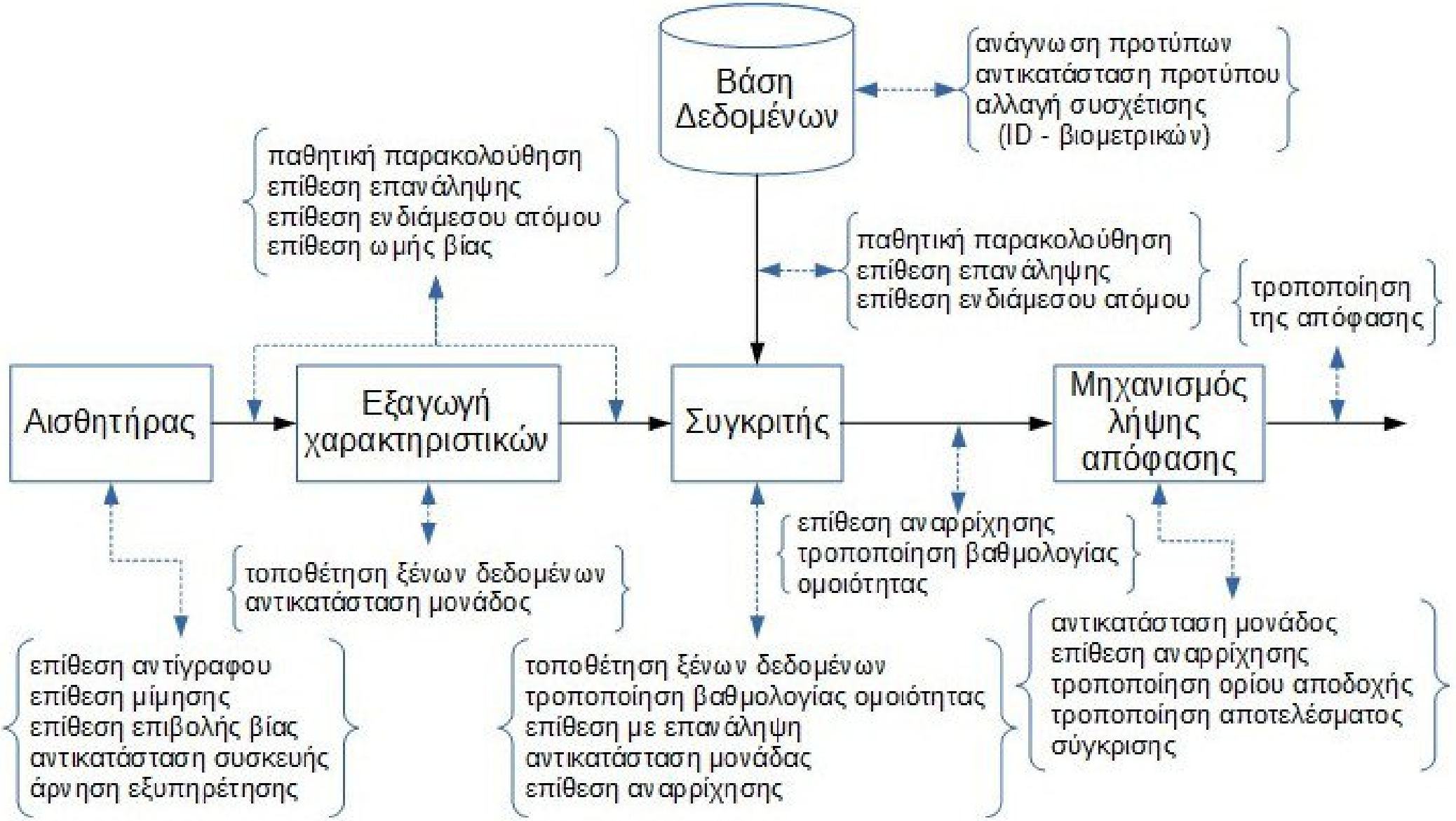
Οι κυριότερες ανησυχίες σχετικά με την χρήση της βιομετρίας

- Βιομετρικά δεδομένα μπορεί να συλλέγονται ή να μοιράζονται, χωρίς την άδεια των χρηστών, χωρίς επαρκή ενημέρωση, ή χωρίς συγκεκριμένο σκοπό.
- Βιομετρικά δεδομένα που έχουν συλλεγεί για συγκεκριμένο σκοπό, μπορεί αργότερα να χρησιμοποιηθούν για κάποιον άλλο σκοπό, μη θεμιτό ή χωρίς εξουσιοδότηση (function creep).
- Όσο εξαπλώνεται η χρήστη της βιομετρίας, αυξάνεται ταυτόχρονα η πιθανότητα να υποκλαπούν τα βιομετρικά μας δεδομένα, καθώς κάποια μέρη είναι πιο ευάλωτα από άλλα.
- Τα βιομετρικά δεδομένα μπορεί να χρησιμοποιηθούν για να αποκαλύψουν το φύλο και την εθνικότητα κάποιου. Ακομα, μπορεί να αποκαλύπτουν λεπτομέρειες για το ιατρικό ιστορικό.

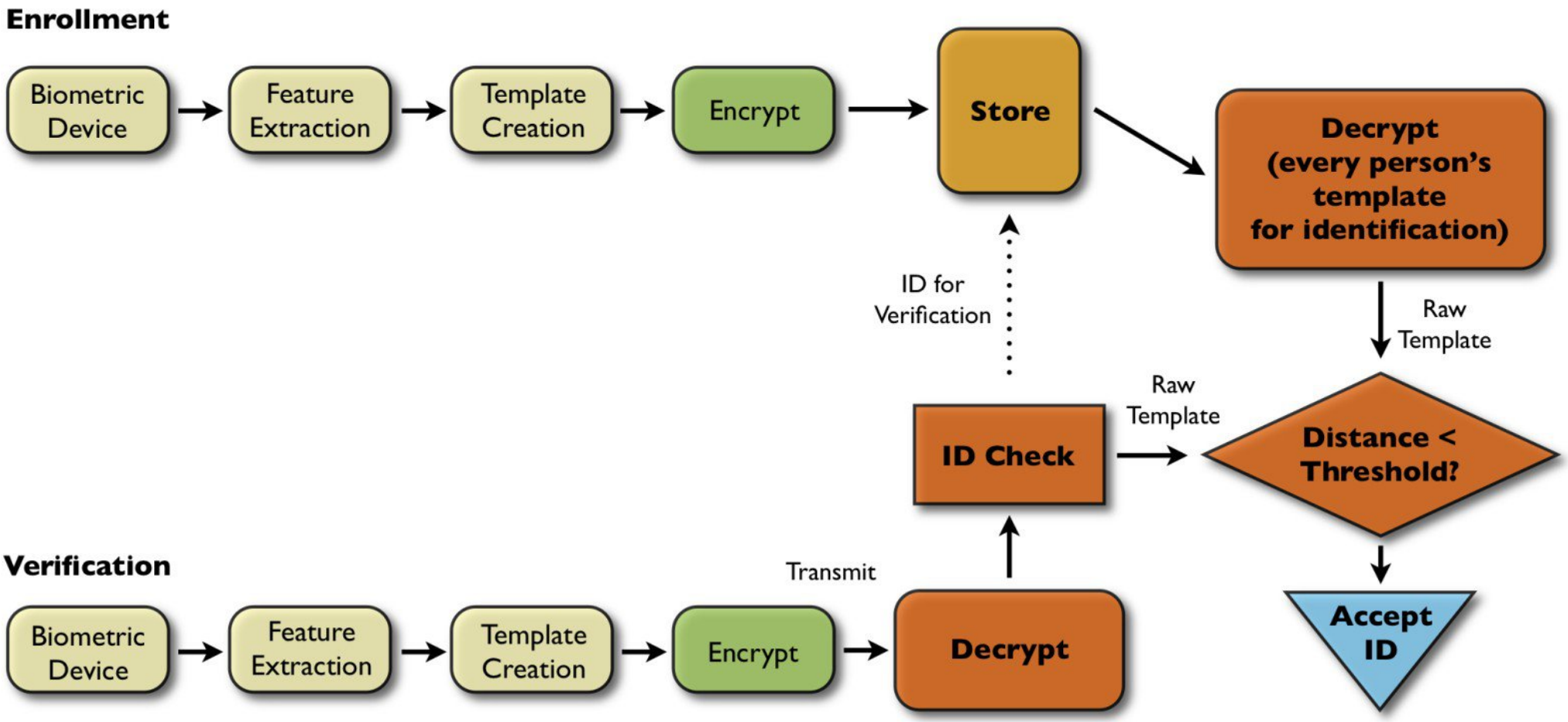
Οι κυριότερες ανησυχίες σχετικά με την χρήση της βιομετρίας (2)

- Η βιομετρία μπορεί να χρησιμοποιηθεί για τον εντοπισμό ή την παρακολούθηση ατόμων.
- Η βιομετρία μπορεί να χρησιμοποιηθεί για την συλλογή προσωπικών πληροφοριών.
- Τα βιομετρικά δεδομένα μπορεί να αποθηκεύονται ή να μεταδίδονται με ακατάλληλο τρόπο.
- Παραβιάζεται το δικαίωμα κάθε ατόμου στην ανωνυμία.
- Θα πρέπει να υπάρχει κάποια ισορροπία ανάμεσα στην χρήση βιομετρίας και την ασφάλεια που απαιτείται.

Τρόποι επίθεσης σε ένα βιομετρικό σύστημα



Η χρήση τυπικής κρυπτογραφίας δεν είναι ασφαλής λύση



Ένας τρόπος προστασίας προτύπων θα πρέπει να πληροί τις παρακάτω ιδιότητες:

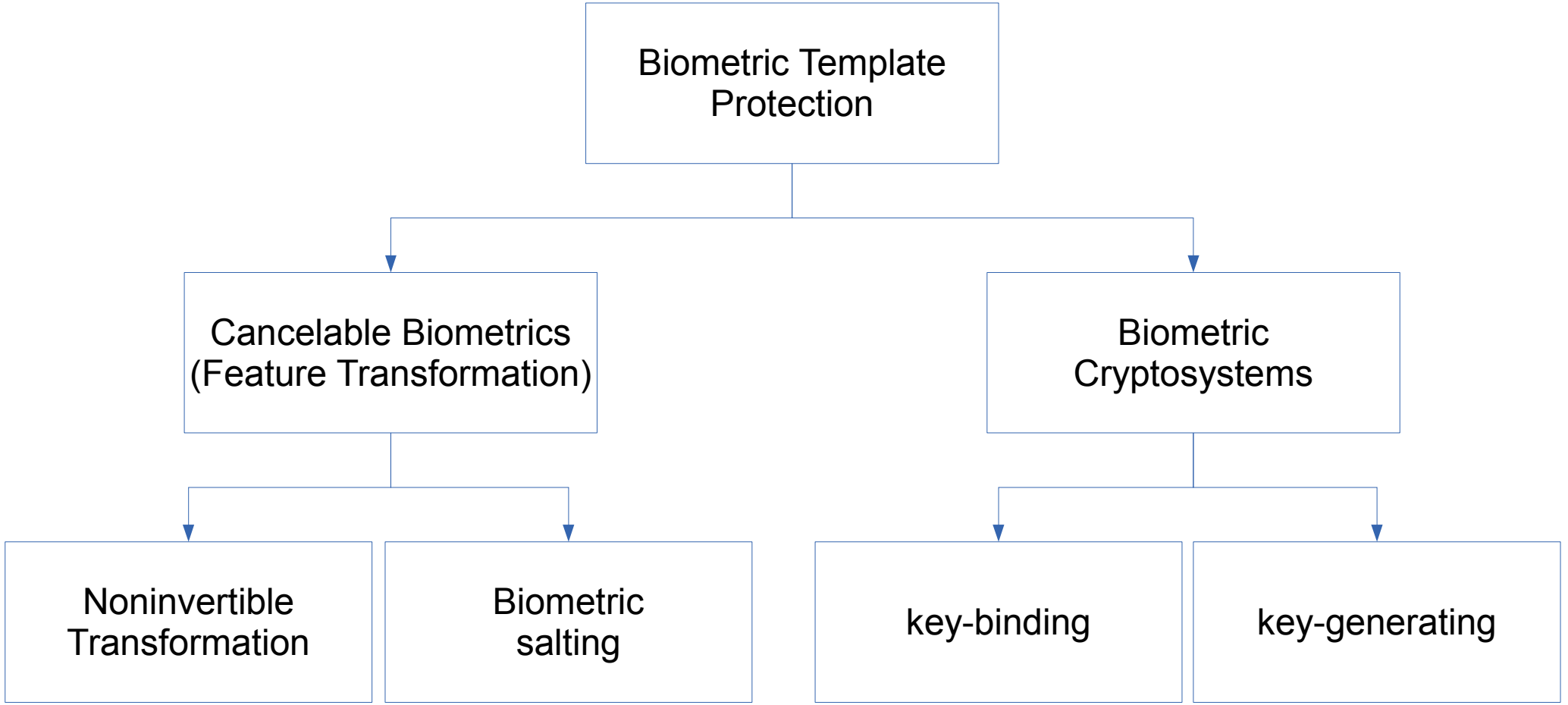
1) Ανανέωση: θα πρέπει να είναι δυνατή η ανάκληση ενός παραβιασμένου πρότυπου και η επανέκδοση ενός νέου βασισμένο στα ίδια βιομετρικά δεδομένα

2) Πολυμορφία: κάθε πρότυπο που παράγεται από ένα βιομετρικό στοιχείο δεν θα πρέπει να ταιριάζει με τα προγενέστερα που δημιουργήθηκαν από τα ίδια βιομετρικά δεδομένα. Αυτή η ιδιότητα απαιτείται για να προστατευθεί η ιδιωτικότητα του χρήστη.

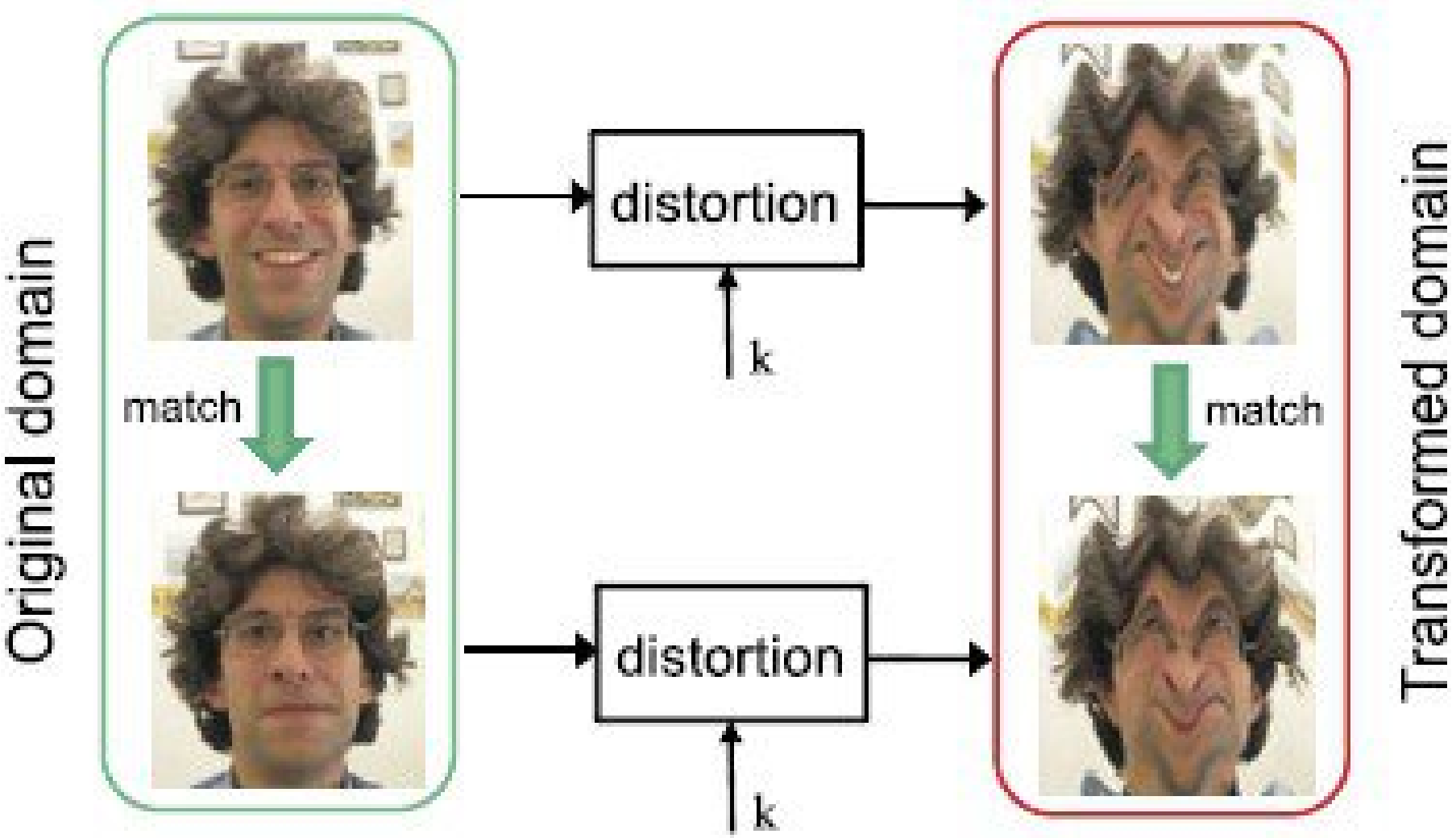
3) Ασφάλεια: θα πρέπει να είναι αδύνατο ή υπολογιστικά πολύ δύσκολο να αποκτηθεί το αρχικό βιομετρικό πρότυπο από αυτό που είναι αποθηκευμένο και προστατευμένο. Αυτή η ιδιότητα χρειάζεται για να αποτρέπει κάποιον κακόβουλο από το να δημιουργεί ψεύτικα βιομετρικά χαρακτηριστικά από κλεμμένα πρότυπα.

4) Απόδοση: Οι δείκτες λαθών της βιομετρικής αναγνώρισης, όπως ο δείκτης λανθασμένης Απόρριψης (False Rejection Rate) ή ο δείκτης λανθασμένης Αποδοχής (False Acceptance Rate) δεν θα πρέπει να χειροτερεύουν σημαντικά με την εφαρμογή του τρόπου προστασίας προτύπων, σε σχέση με την προσέγγιση χωρίς προστασία.

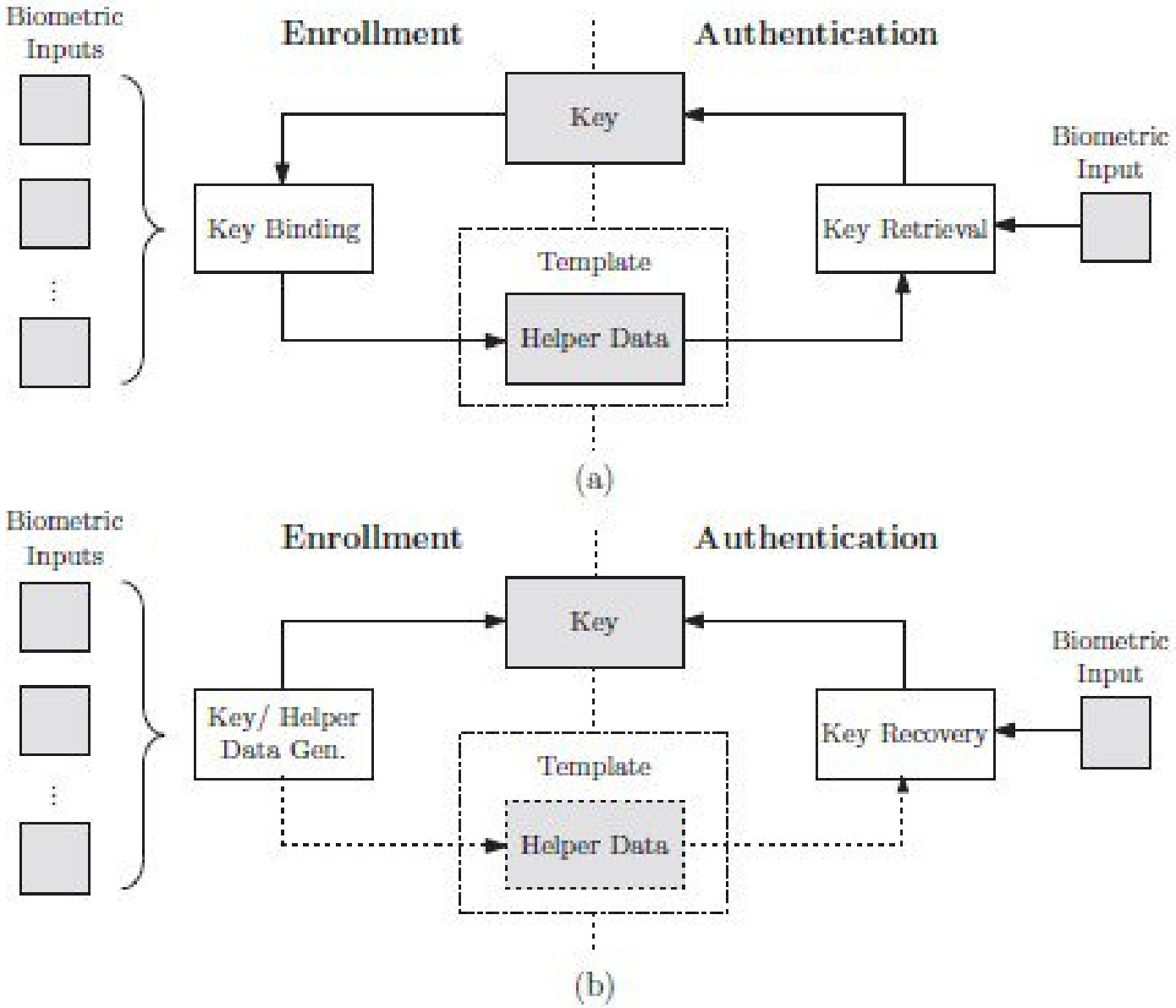
Τεχνολογίες προστασίας βιομετρικών προτύπων



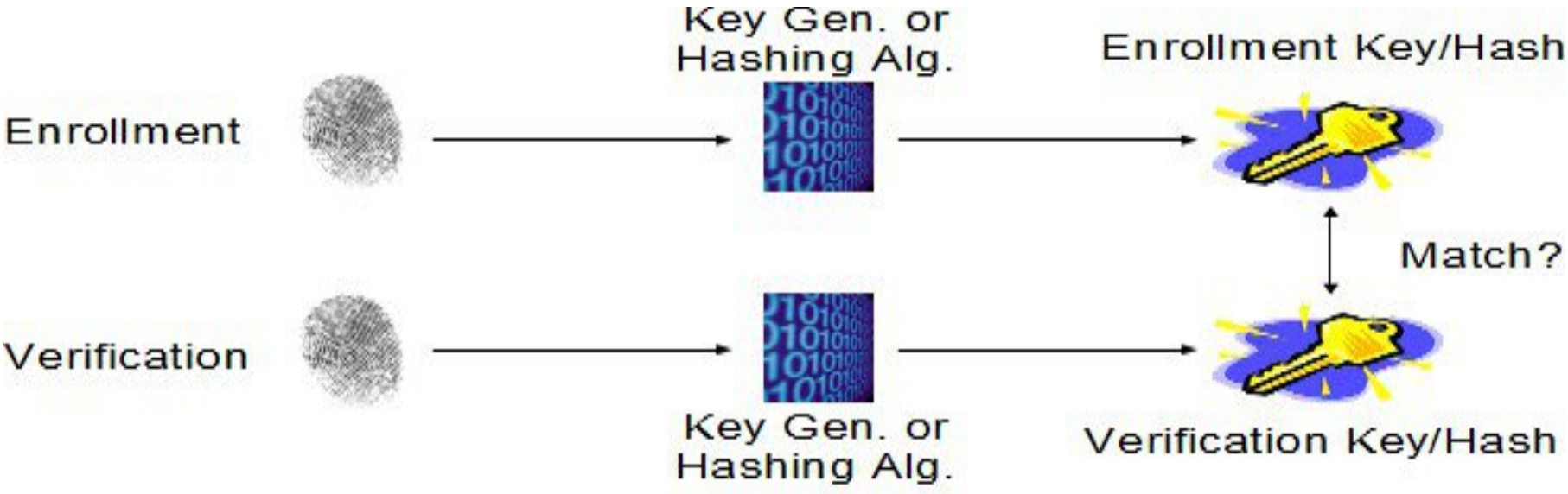
Μετασχηματισμού Χαρακτηριστικών



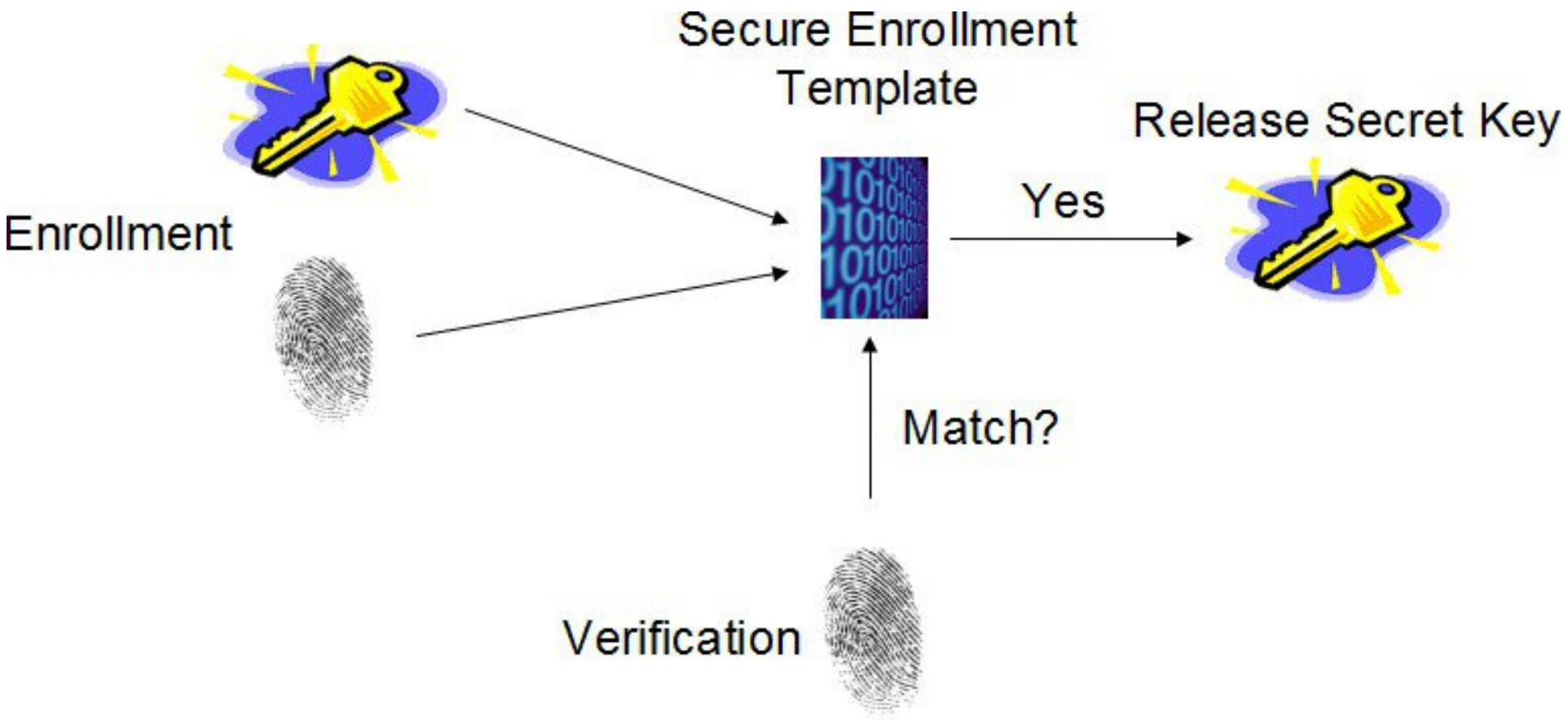
Κρυπτοσυστήματα α) ενσωμάτωσης κλειδιού β) παραγωγής κλειδιού



Παραγωγής Κλειδιού Key-generating



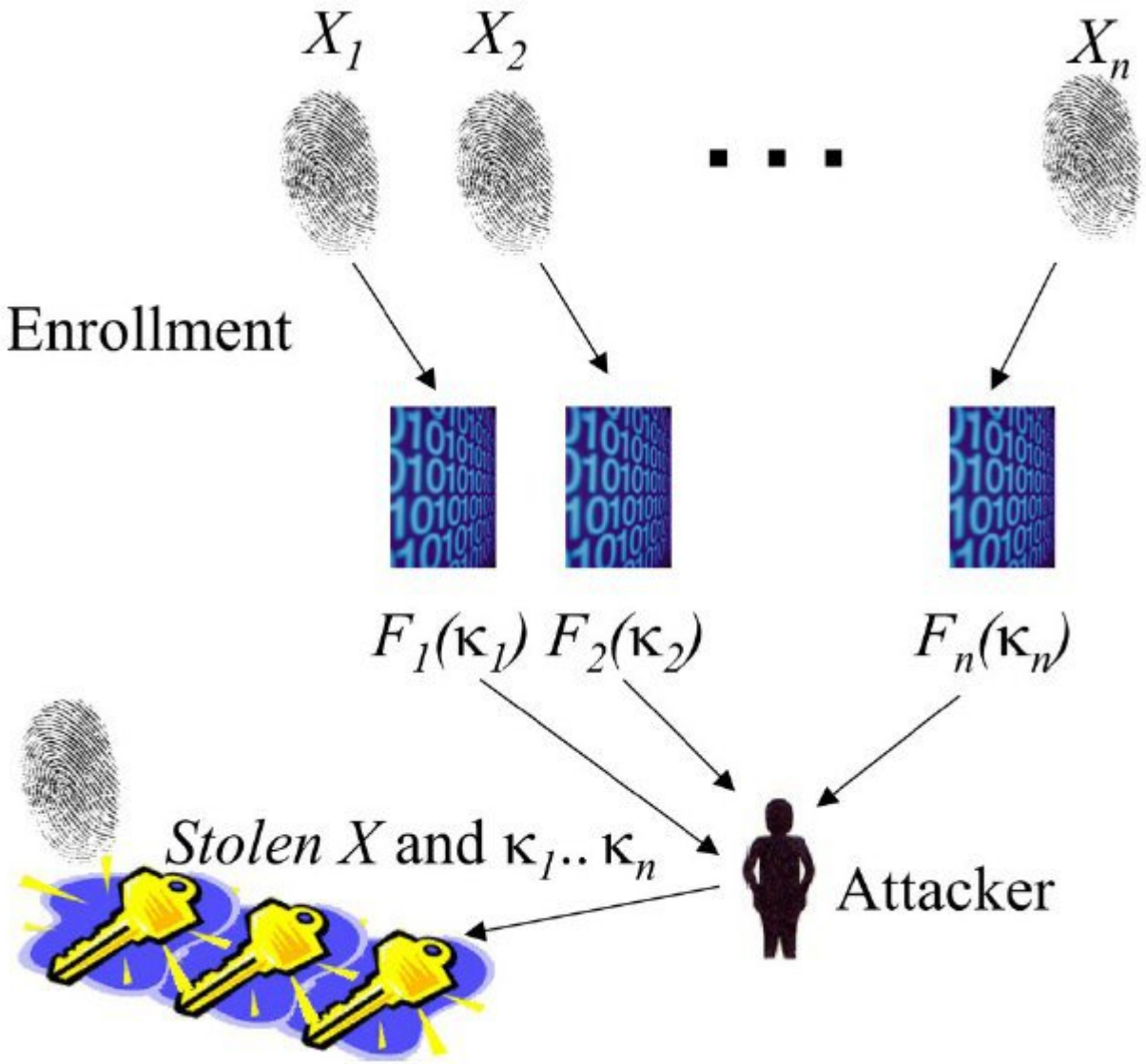
Ενσωμάτωσης Κλειδιού (Key-binding)



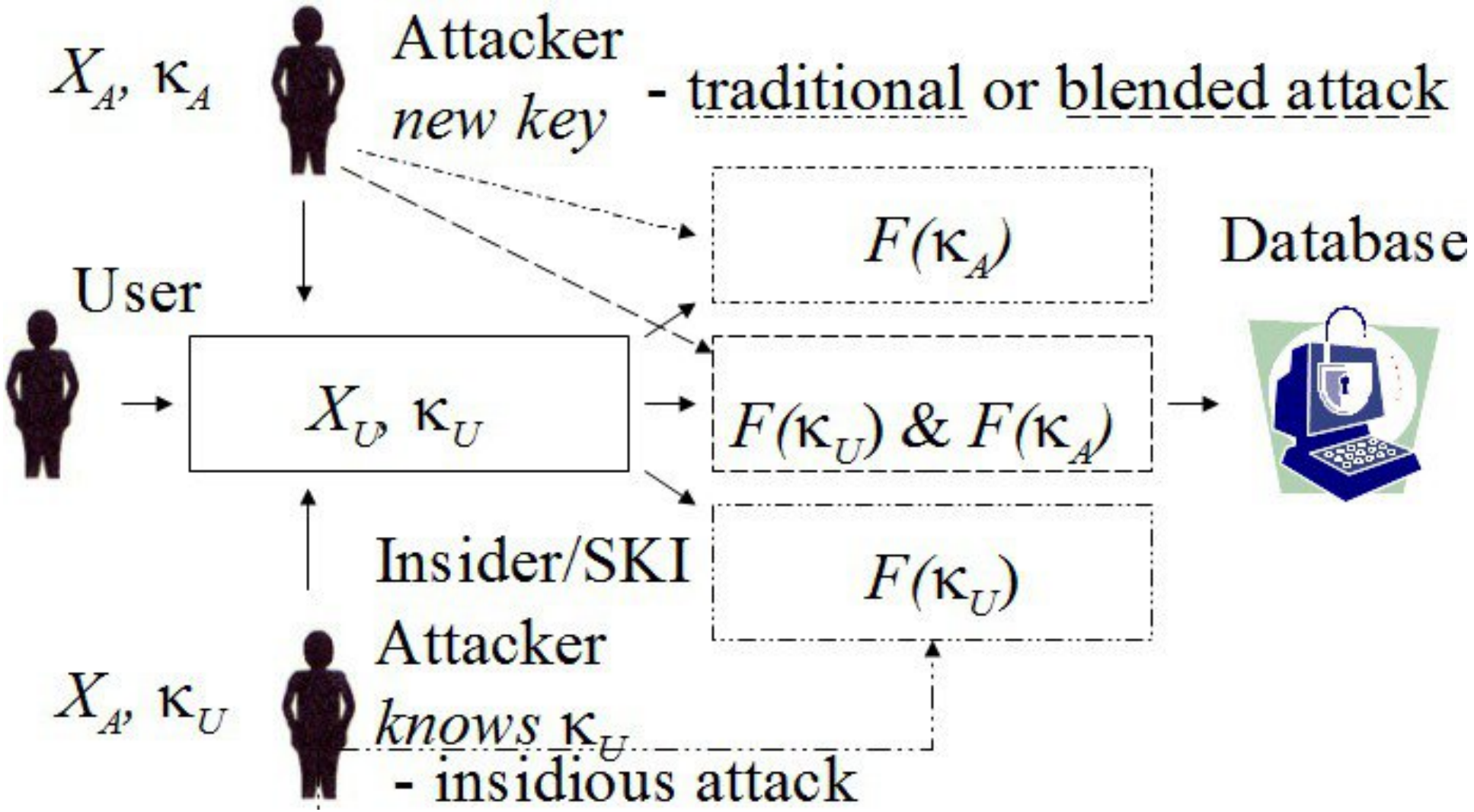
Επιθέσεις κατά τεχνολογιών προστασίας προτύπων

- Επίθεση μέσω Πολλαπλών Εγγραφών (Attack via record multiplicity – ARM)
- Επίθεση ανάμιξης (Blended Substitution Attacks)
- Επίθεση αφανούς ανάμιξης (insidious blending)
- Επίθεση απόκρυφης αντιστροφής κλειδιού (surreptitious key inversion attack)
- Αντίστροφη αναζήτηση πάνω σε ένα πρότυπο μετασχηματισμένων χαρακτηριστικών

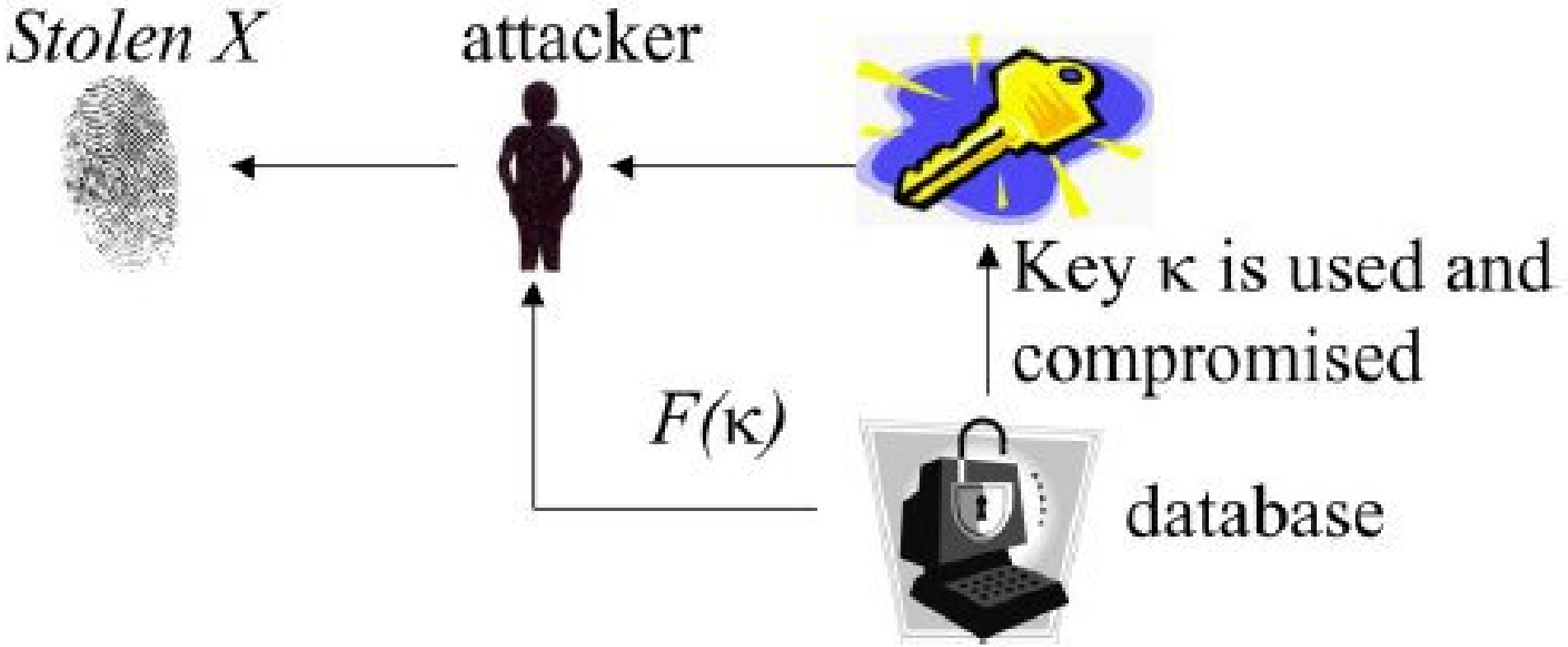
Επίθεση μέσω Πολλαπλών Εγγραφών (ARM)



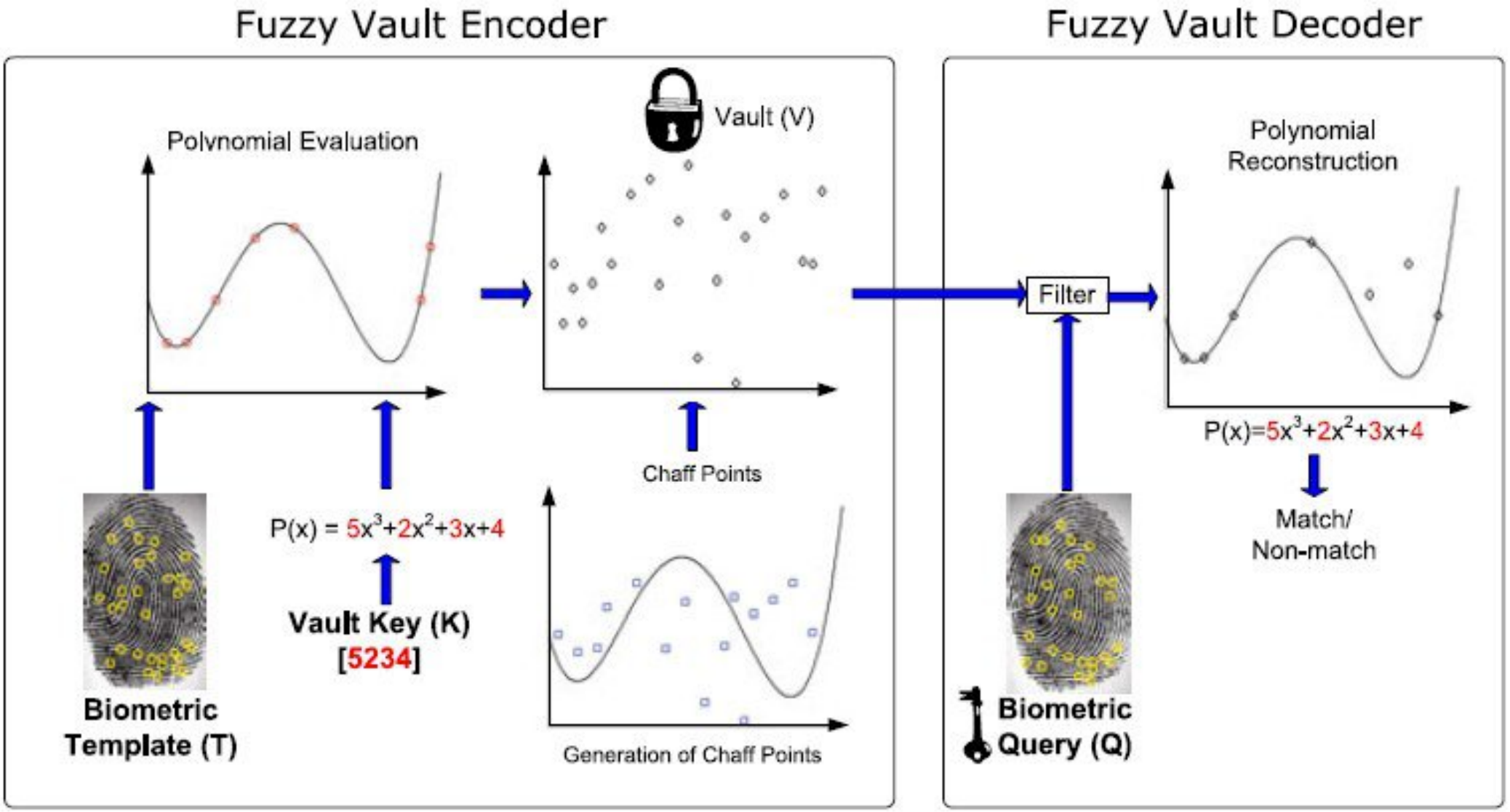
Επίθεση Αντικατάστασης και Επίθεση Ανάμιξης



Επίθεση απόκρυψης αντιστροφής κλειδιού



Fuzzy Vaults



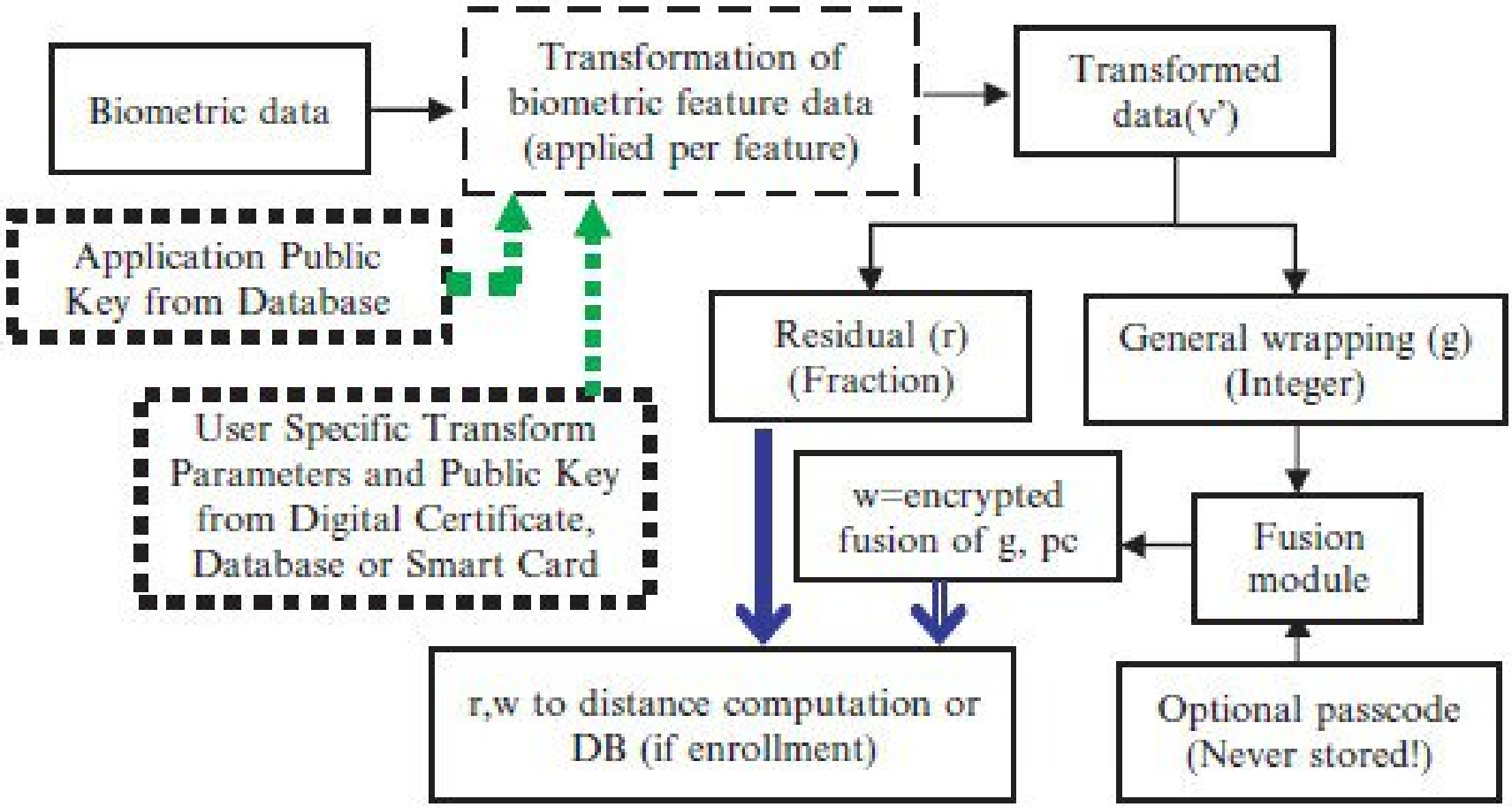
Ασφαλή Biotoken με δυνατότητα ανάκλησης

- Εύρωστη απόσταση/σύγκριση
- Ασφάλεια/δυνατότητα ανάκλησης
- Χωρίζουμε τα δεδομένα σε δύο μέρη:
  - Σταθερό μέρος και Ασταθές
- Το σταθερό μέρος το κρυπτογραφούμε
- Τα δύο μέρη παρέχουν εύρωστη μέτρηση της απόστασης, η οποία δεν έχει επίπτωση στην ακρίβεια σύγκρισης

Ασφαλή Biotoken με δυνατότητα ανάκλησης

- Κάθε τιμή του συνόλου χαρακτηριστικών, μετασχηματίζεται, εφαρμόζοντας μία μετατόπιση και στη συνέχεια γίνεται μεγέθυνση
  $u' = (u - t) * s$
- Στη συνέχεια χωρίζουμε τα δεδομένα σε δύο μέρη, ένα πηλίκο q που πρέπει να ταιριάζει απόλυτα και ένα υπόλοιπο r
- Αφήνουμε το υπόλοιπο χωρίς να το κωδικοποιήσουμε
- Κρυπτογραφούμε το q με ένα δημόσιο κλειδί P

Διαδικασία παραγωγής Biotoken



Ιδιότητα Εμφώλευσης

- Το προστατευμένο πρότυπο w_j επανακωδικοποιείται από κάποια συνάρτηση μετασχηματισμού T

  1η κωδικοποίηση: $w_{j,1}(u', P)$

  2η κωδικοποίηση: $w_{j,2}(w_{j,1}, T_2)$

  n κωδικοποίηση: $w_{j,n}(w_{j,n-1}, T_n)$

- Η εμφώλευση μπορεί να είναι αντιστρέψιμη μέσω των κλειδιών, αλλά κρυπτογραφικά ασφαλής

Πολλαπλές κωδικοποιήσεις

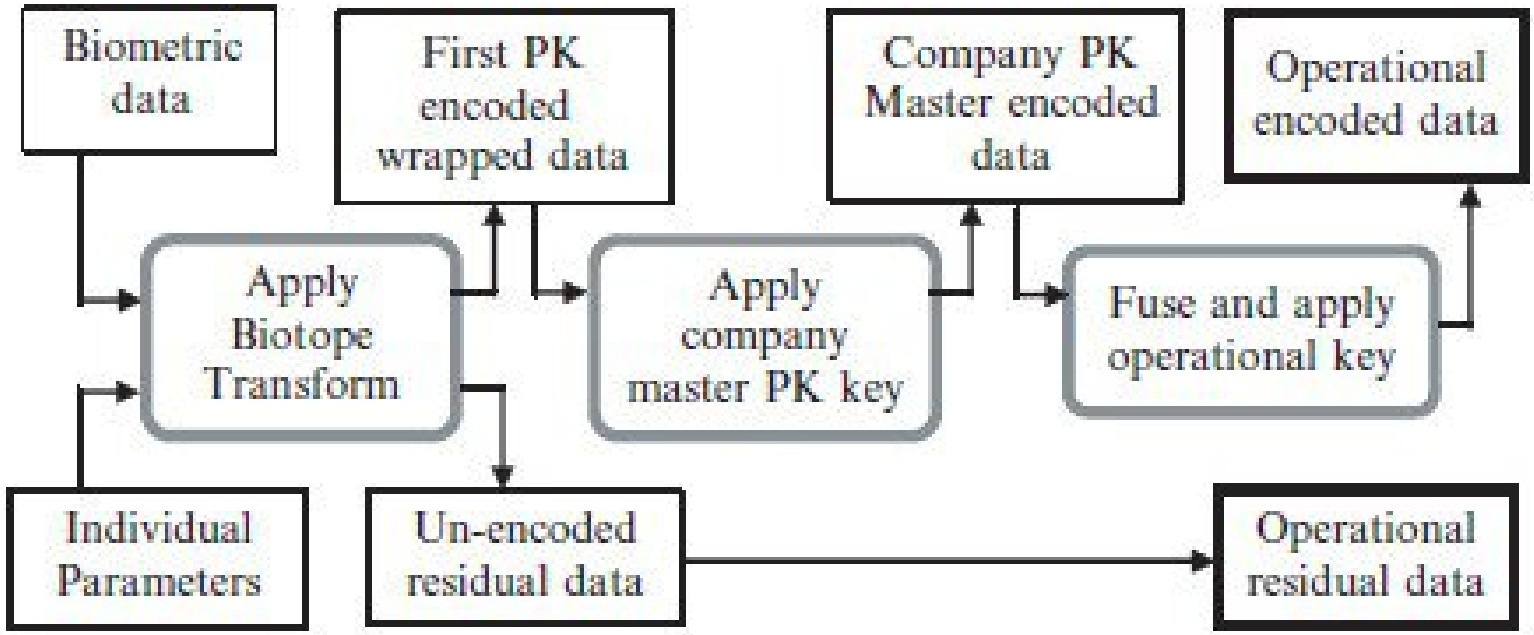
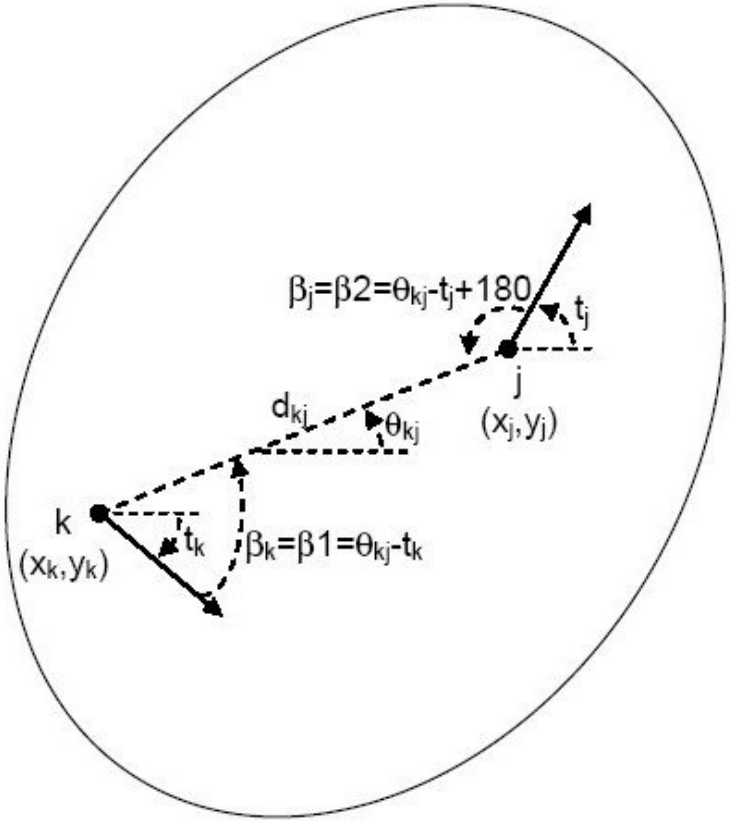


Fig. 22.6. Biotope generation followed by multistep PK encoding to provide easily reissued Biotopes. Data in dotted boxes are not stored.

Minutiae Matching (BOZORTH3)



αρχείο με minutiae
MINDTCT.xyt

```
( x   y   θ   q )
20 600 79 8
111 507 225 6
133 518 214 7
138 494 45 7
158 378 67 16
…
734 384 202 15
734 86 236 35
736 294 34 13
736 280 45 14
```

{dkj, β1, β2, k, j, θkj}

Αντικατοπτριζόμενο modulo

x	21	22	23	24	25	26	27	...	46	47	48	49	50	51
x mod 24	21	22	23	0	1	2	3	...	22	23	0	1	2	3
x rmod 24	21	22	23	24	23	22	21	...	2	1	0	1	2	3

Window size E
x=d%(E*2)
    rmod(d,E)=x if x<E
    rmod(d,E)=(E*2)-x otherwise

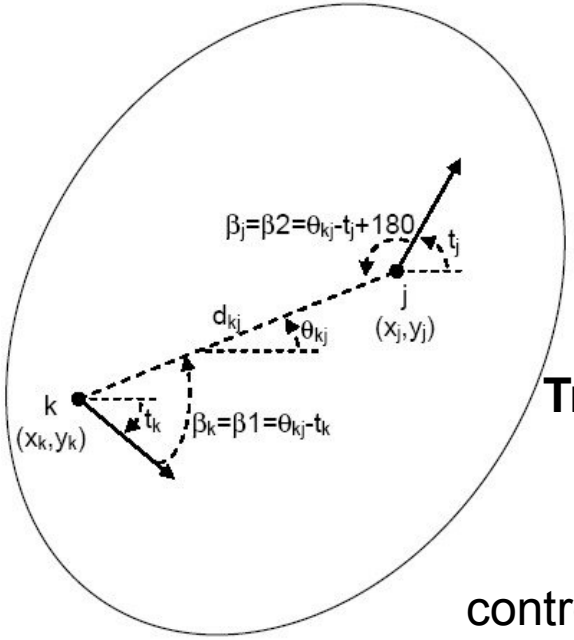
u'=(u-t)*s
r=rmod(u',E)
q=int(u'/E)

Παράδειγμα:
Τιμές κανονικής πράξης modulo:
49 mod 24 = 1
47 mod 24 = 23

Τιμές πράξης rmod:
x = 49%(24*2) = 49mod48 = 1, x<24

x = 47%(24*2) = 47 mod 48 = 47, x>24
άρα (24*2)-x = 48 – 47 = 1

Biotoken βασισμένο στον Bozorth



	distance dkj	angle β1	angle β2	k, j, θkj
	16 bits	9 bits 7bits	9 bits 7 bits	

		u'	u'	u'
Transform	16 bits	16 bits	8 bits 8bits	8 bits 8bits

	control (k,j,θkj)	r	g
row	3 bytes	4 bytes	4 bytes

Παράδειγμα

Αν μετατόπιση **t=20** και πολλαπλασιασμός **s=40** και παράθυρο **E=500**

dkj β1 β2 : 44 150 225

υ' = (44-20)*40 = 24*40 = **960**

x = d%(E*2)

x = 960%1000 = **960**

rmod(d,E)= x αν x < E και rmod(d,E)=(E*2)-x στις υπόλοιπες περιπτώσεις.

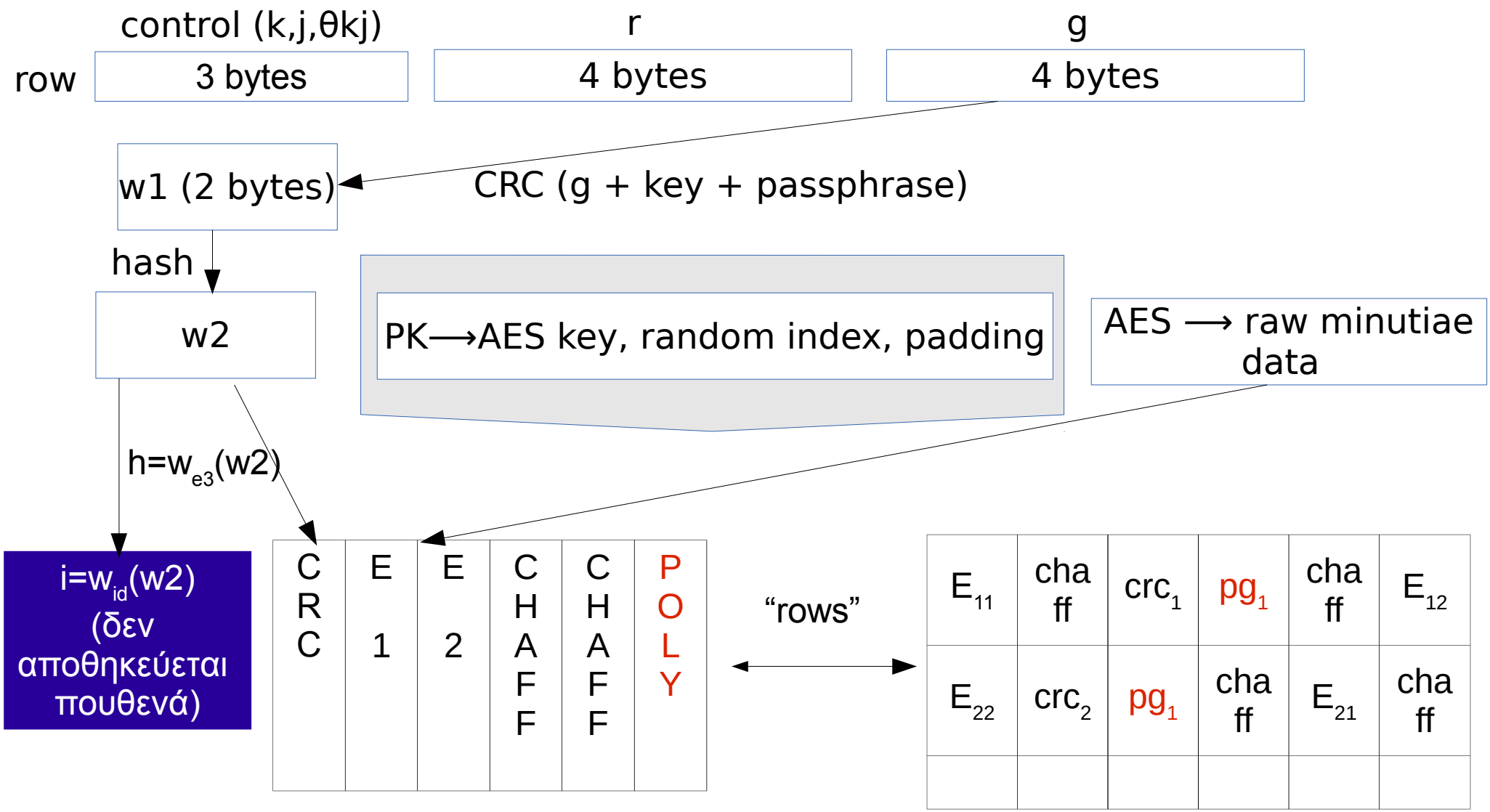
Άρα rmod(d,E)=(E*2)-x=1000-960=40

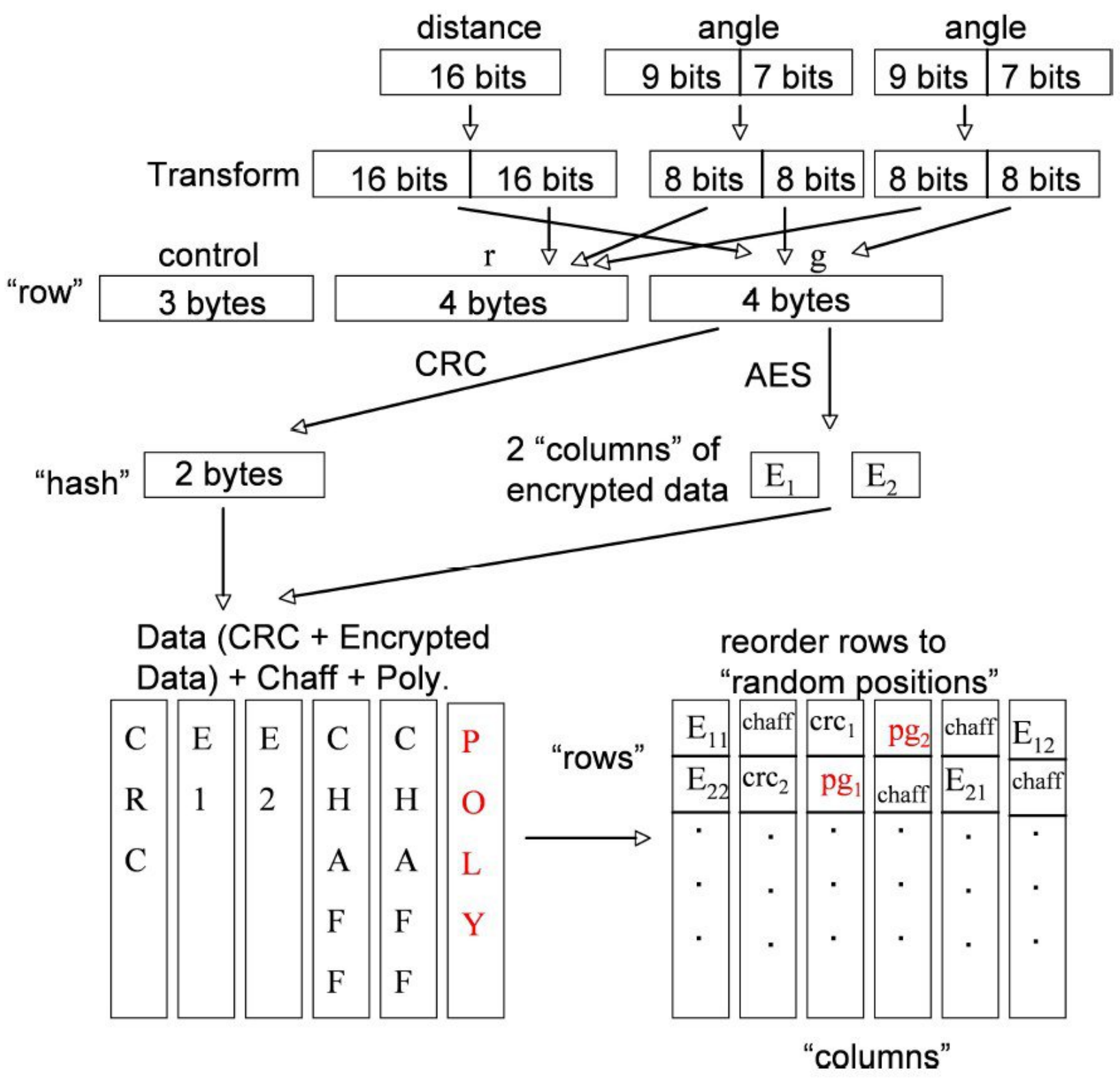
Άρα **q=int(υ'/E)=960/500=1** και **r=40**

Αντίστοιχα για το 150 και το 215 θα είχαμε: q=int(υ'/E)=5200/500=10 και r=200 και q=int(υ'/E)=8200/500=16 και r=200

Transform	**960**	5200	8200
	r	**g**	
row	**40** 200 200	**1** 10 16	

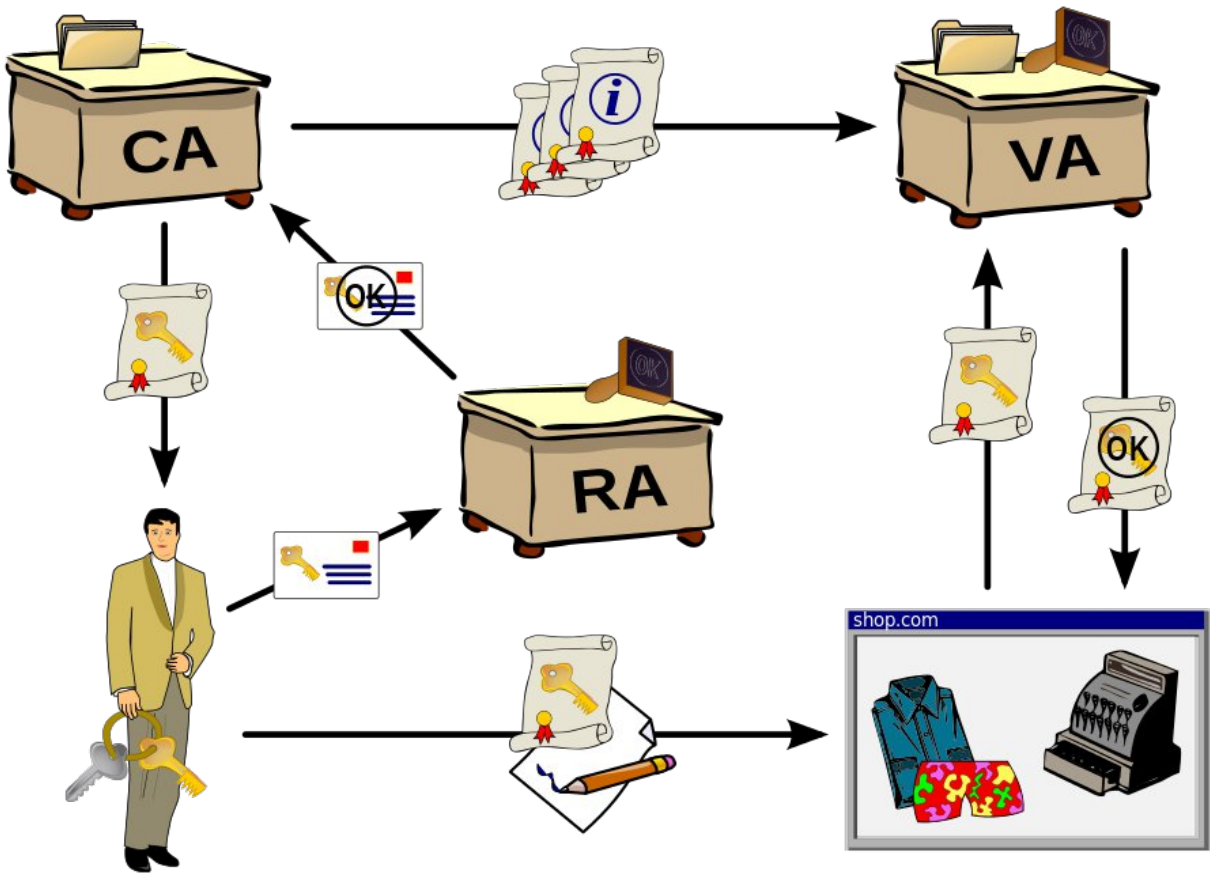
Bipartite Biotoken




distance
angle
angle
16 bits
9 bits
7 bits
9 bits
7 bits
Transform
16 bits
16 bits
8 bits
8 bits
8 bits
8 bits
control
r
g
"row"
3 bytes
4 bytes
4 bytes
CRC
AES
"hash"
2 bytes
2 "columns" of encrypted data
E_1
E_2
Data (CRC + Encrypted Data) + Chaff + Poly.
C R C
E 1
E 2
C H A F F
C H A F F
P O L Y
"rows"
reorder rows to "random positions"
E_{11}
chaff
crc_1
pg_2
chaff
E_{12}
E_{22}
crc_2
pg_1
chaff
E_{21}
chaff
"columns"

Public Key Infrastructure

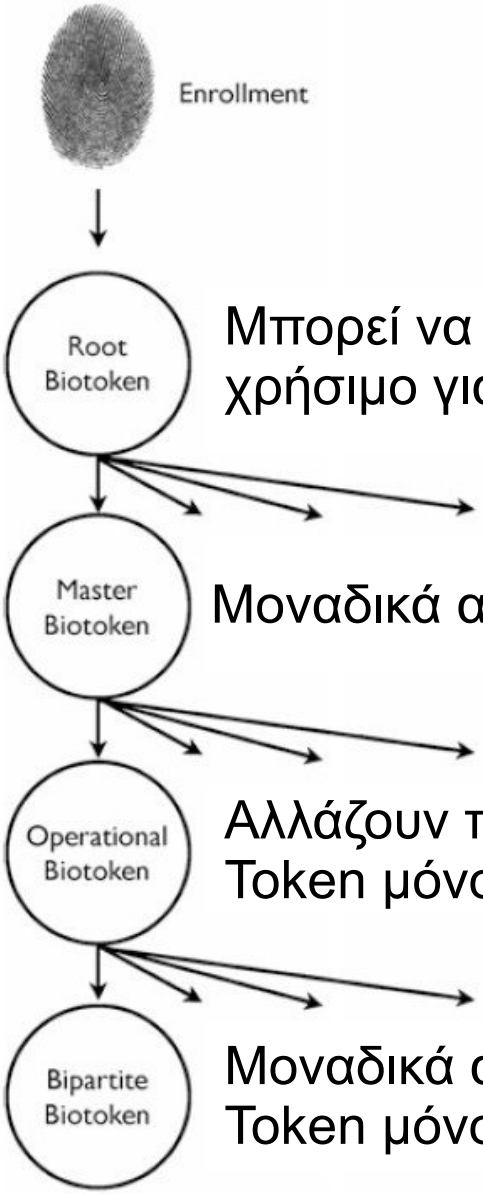
- PKI είναι η υποδομή εκείνη που διαχειρίζεται ψηφιακά πιστοποιητικά (x.509)



Απαιτήσεις μίας υποδομής Βιοκρυπτογραφικού κλειδιού

- Κρυπτογραφικά ασφαλής προστασία των βιομετρικών χαρακτηριστικών
- Δυνατότητα ανάκλησης και επανέκδοσης προτύπων
- Εμφωλευμένες επανακωδικοποιήσεις, που υποστηρίζουν την παραγωγή μίας ιεραρχίας από πρότυπα, ξεκινώντας από ένα βασικό πρότυπο.
- Υποστήριξη δημόσιων προτύπων
- Δυνατότητα ενσωμάτωσης κλειδιού χωρίς την παρέμβαση του ατόμου που σχετίζεται με το πρότυπο

Δέντρο έκδοσης/επανέκδοσης Biotoken



Μπορεί να χρησιμοποιηθεί για έλεγχο διπλοεγγραφών, κάνοντας το χρήσιμο για αναγνώριση και επαλήθευση

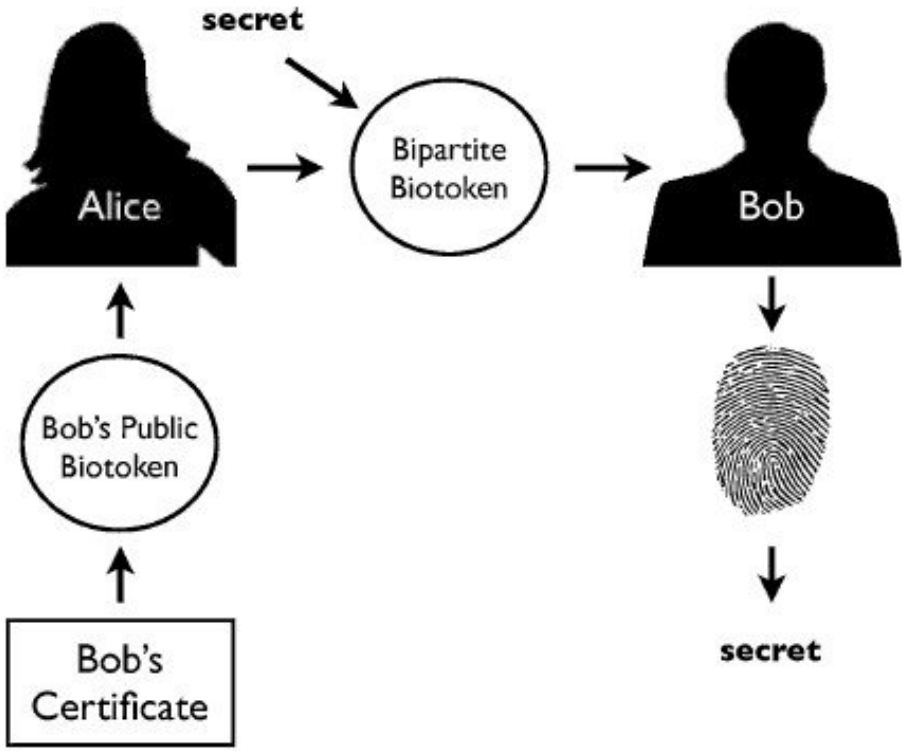
Μοναδικά ανά εφαρμογή/βάση δεδομένων. Token μόνο για επαλήθευση

Αλλάζουν τακτικά όπως πχ υπάρχει ημερομηνία λήξης στις πιστωτικές. Token μόνο για επαλήθευση

Μοναδικά ανά συναλλαγή. Υποστηρίζει ασφαλή απελευθέρωση κλειδιού. Token μόνο για επαλήθευση

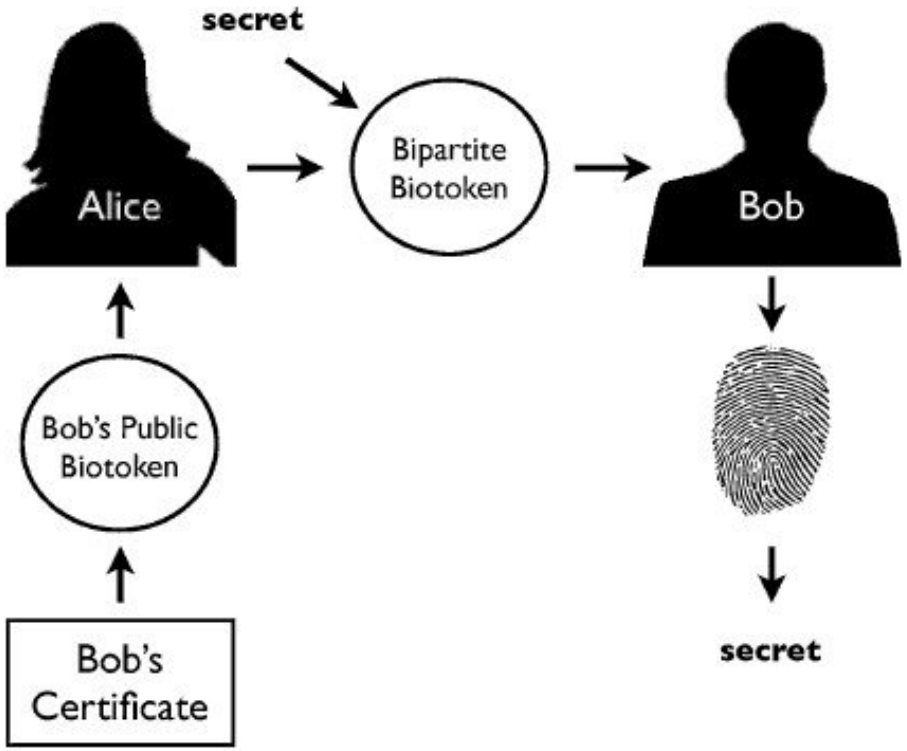
Πλεονέκτημα ενός BKI

- Δυνατότητα να αποθηκεύονται δημόσια biotokens μέσα σε ψηφιακά πιστοποιητικά.
  - Μία οντότητα της υποδομής μπορεί να στείλει μυστικά δεδομένα που μόνο ο ιδιοκτήτης του biotoken μπορεί να ξεκλειδώσει.

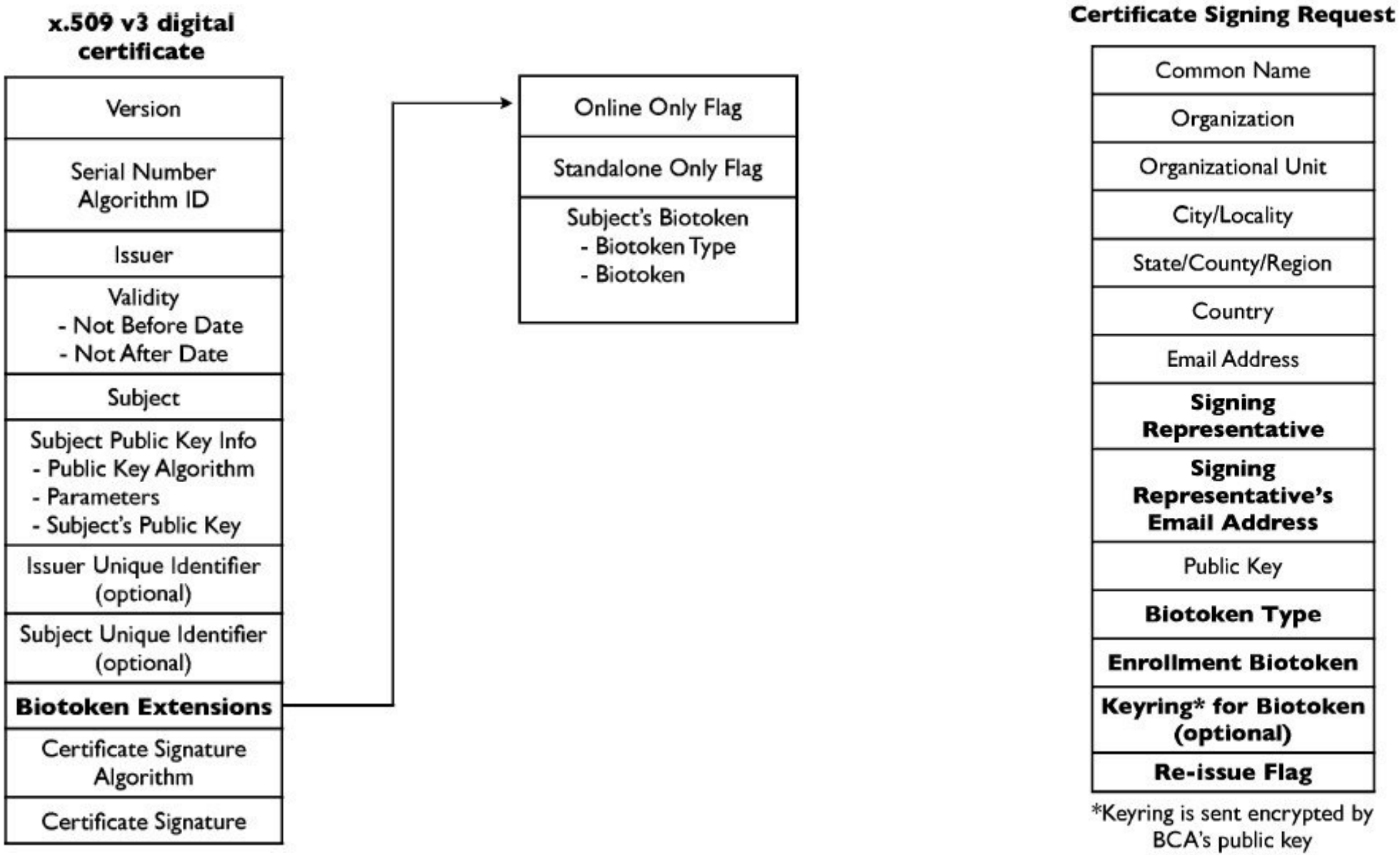


Πλεονέκτημα ενός BKI

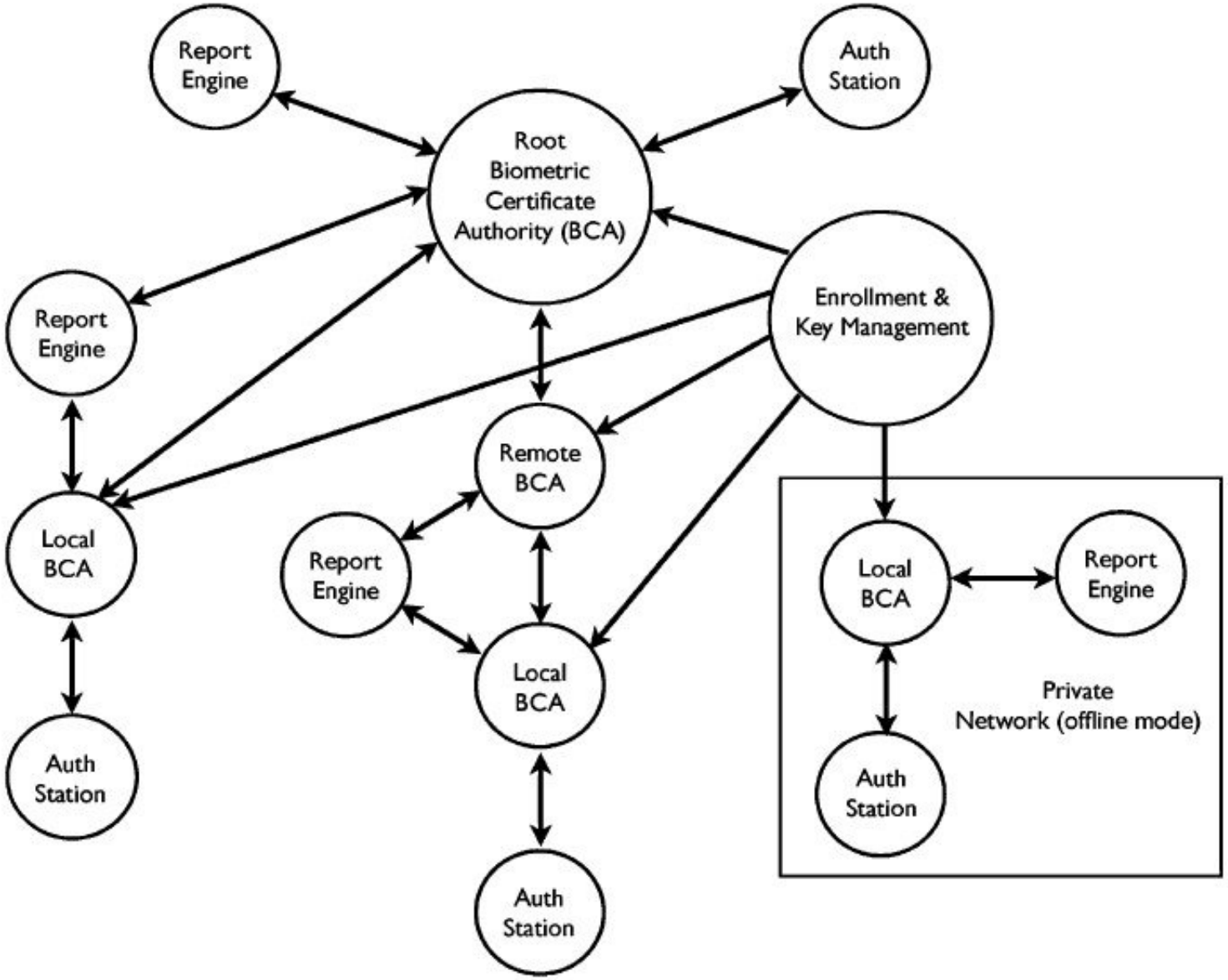
- πρόσθεσε τα biotoken πεδία και τις ημερομηνίες σε ένα x.509v3 πιστοποιητικό
- η BCA εξακριβώνει την ID, εκδίδει και υπογράφει το “root” πιστοποιητικό του χρήστη
- Η BCA παράγει ένα λειτουργικό πιστοποιητικό και το επιστρέφει ή το δημοσιεύει σε ένα ιδιωτικό ή δημόσιο κατάλογο
- Η Αλίκη μπορεί να εντοπίσει το πιστοποιητικό του Βύρωνα και να παράγει ένα νέο πιστοποιητικό συναλλαγής με ενσωματωμένο κλειδί. Υπογράφει το πιστοποιητικό και το στέλνει στον Βύρωνα.
- Ο Βύρων μπορεί να επικυρώσει το μήνυμα, να χρησιμοποιήσει βιομετρία για να εξάγει το κλειδί και να το χρησιμοποιήσει ή να το υπογράψει για να επικυρώσει την συναλλαγή και την ταυτότητα του



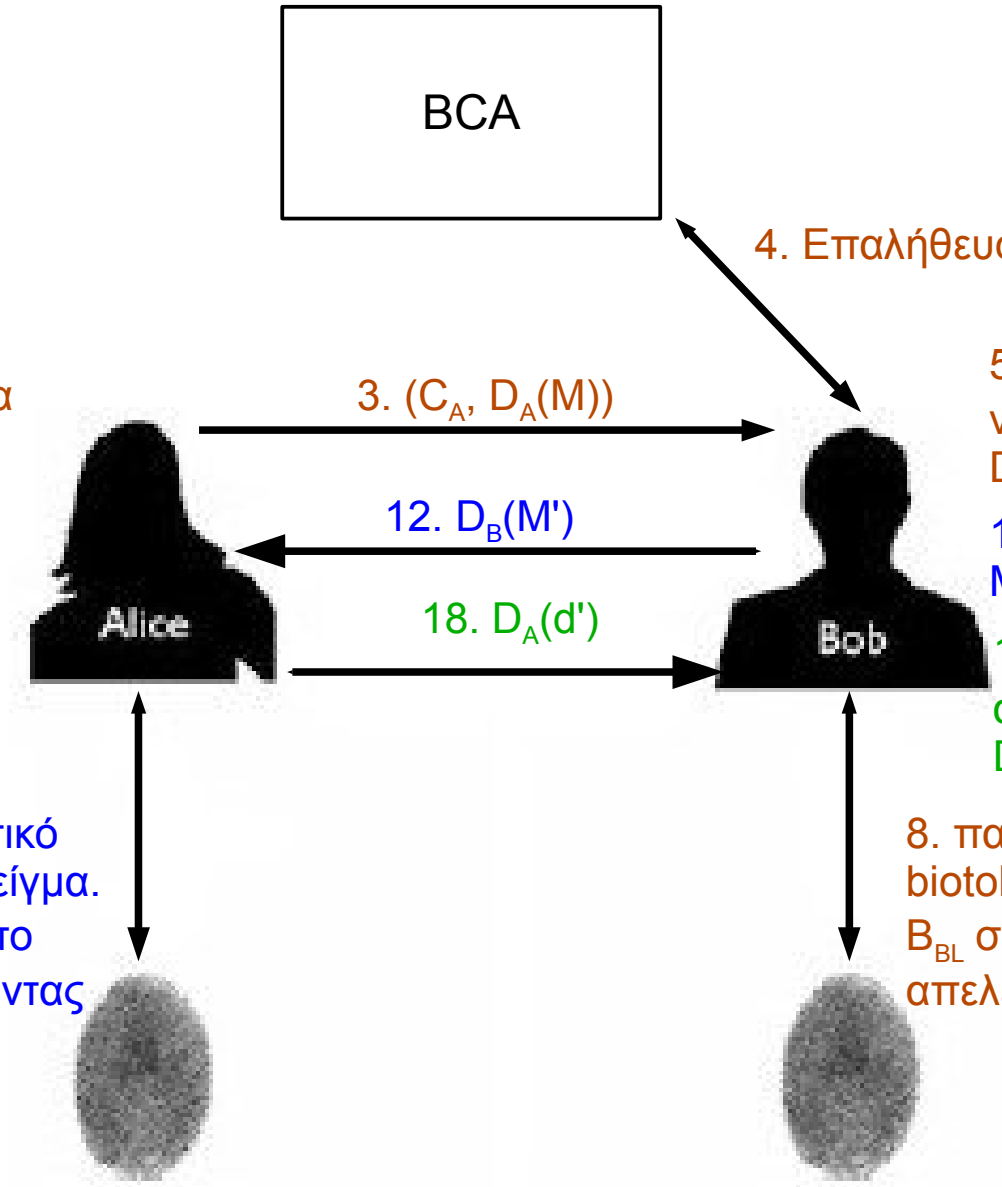
Ψηφιακό πιστοποιητικό με Biotokens



Σχεδιάγραμμα Υποδομής Βιοκρυπτογραφικού Κλειδιού



Πρωτόκολλα επικοινωνίας



1. Η Αλίκη παράγει έναν τυχαίο αριθμό, R_A

2. Η Αλίκη δημιουργεί ένα μήνυμα, M = (T_A, R_A, I_B, $B_{BB}(d)$)

3. (C_A, $D_A(M)$)

4. Επαλήθευση του C_A

5. Χρησιμοποιεί το E_A για να αποκρυπτογραφήσει $D_A(M)$

8. παράγεται ένα τοπικό biotoken B_{BL} από το δείγμα. Το B_{BL} συγκρίνεται με το $B_{BB}(d)$, απελευθερώνοντας το d

11. constructs message M' = (T_B, R_B, I_A, $B_{AB}(d)$)

12. $D_B(M')$

13. Με το E_B αποκρυπτογραφεί το $D_B(M')$

16. παράγεται ένα τοπικό biotoken B_{AL} από το δείγμα. Το B_{AL} συγκρίνεται με το $B_{AB}(d)$, απελευθερώνοντας το d

18. $D_A(d')$

19. Με το E_A αποκρυπτογραφεί το $D_A(d')$

Ανάκληση Πιστοποιητικού

- Σενάριο 1: Χειροκίνητη Επανέκδοση
  - Ο κάτοχος του πιστοποιητικού παράγει ένα νέο ζεύγος κλειδιών δημόσιο-ιδιωτικό και ένα νέο biotoken
- Σενάριο 2: Αυτόματη Επανέκδοση Biotoken
  - Η BCA έχει στην κατοχή της τα κλειδιά των μετασχηματισμών, επαναφέρει το δημόσιο biotoken σε κάποιο κατώτερο επίπεδο, εκδίδει νέα κλειδιά μετασχηματισμού και νέο δημόσιο biotoken
- Σενάριο 3: Αυτόματη Επανέκδοση του Ζεύγους-Κλειδιών
  - Η BCA εκδίδει νέο ζεύγος-κλειδιών, και μεταδίδει το μυστικό κλειδί στον κάτοχο μέσο ενός bipartite biotoken

CRN Message

Certificate Re-issue Notification

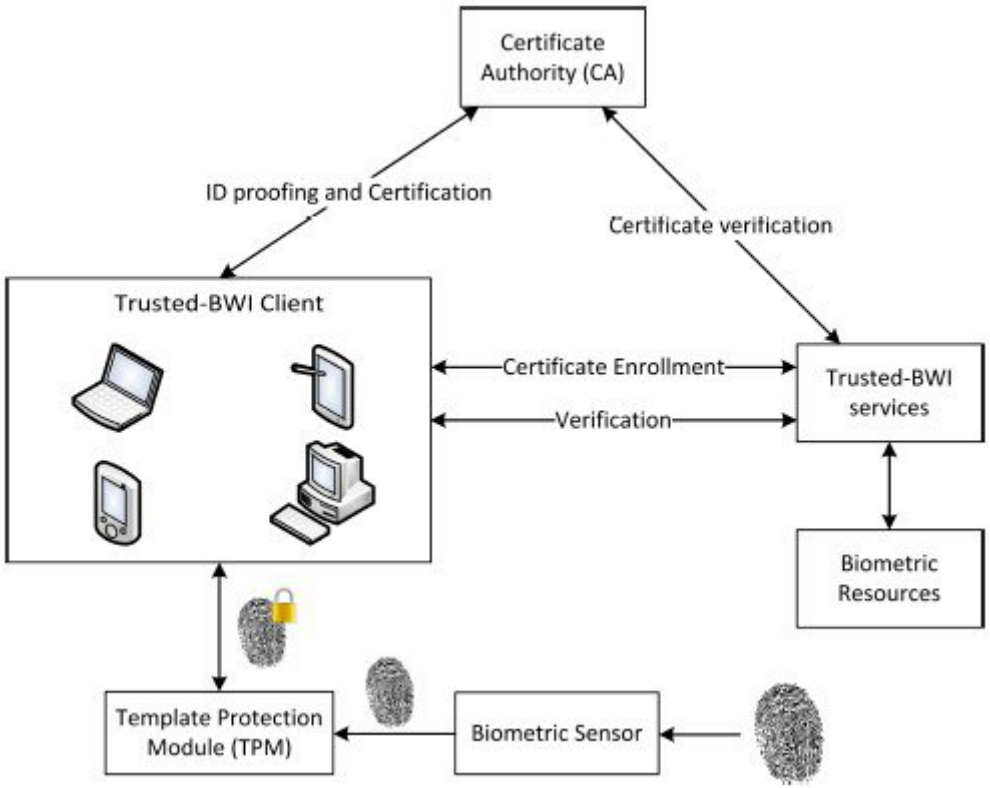
Serial Number
New Serial Number
Biotoken Re-issued Flag
Key-pair Re-issued Flag
Biotoken and Key-pair Revoked Flag
*Keyring for Biotoken (Optional)
Biotoken Type (Optional)
Biotoken (Optional)
Signature

*Keyring is encrypted with the user's public key

Νέες Εφαρμογές

- Αντιμετώπιση επιθέσεων Man-in-the-Middle και Phising
- Bio-Kerberos
- Bio-S/Key
- BKI-enabled LDAP
- Biometric Digital Signatures

Trusted Biometric Web Identities



Certificate Signing Request (CSR)

Version
Common Name
Organization
Organization Unit
Locality
State
Email Address
Signing Representative*
Signing Representative Email Address*
Public Key
Biotoken Type
Biotoken Data*
Biometric Public key*
Signature Algorithm
Signature

Biometric Extension

* Indicates optional fields

Figure 2. Format of Certificate Signing Request (CSR).

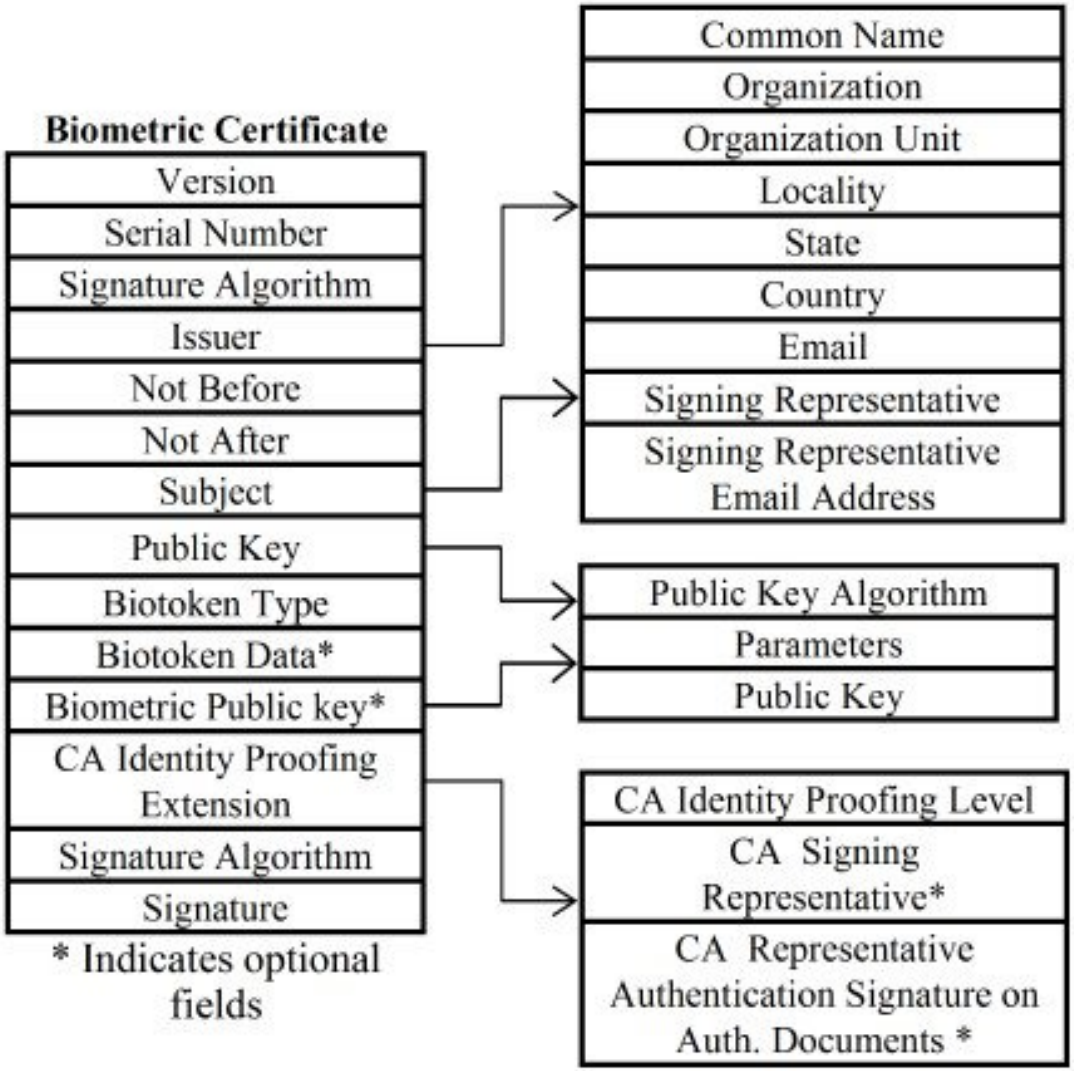
$$\underbrace{DD}_{\text{CA biometric auth. level}} . \underbrace{DD}_{\text{CA documents auth. level}} . \underbrace{DDDD}_{\text{CA reissue auth. level}}$$

Figure 3. Format of the CA Identity proofing level field.

Trusted Biometric Web Identities

No.	CA biometric authentication levels
00	No biometric authentication is used.
10	CA remotely authenticates the user's biotoken using a remote authentication protocol.
20	CA remotely authenticates the user's biometric public key using a remote authentication protocol.
30	CA authenticates, in person, the user's soft biotoken and biometric public key (i.e. using a local challenge and response protocol).
40	CA authenticates, in person, the user's TEE with biometric public key (i.e. by requiring the user to bring in the device with TEE).
50	CA authenticates, in person, the user's hardware biometric public key (i.e. by requiring the user to bring in the secure biometric sensor with hardware trusted module).

No.	CA documents authentication levels
00	No document authentication is used.
10	CA authenticates remotely the user's documents.
20	CA authenticates, in person, the user's documents.



Σύνδεσμοι

- http://icb12.iiitd.ac.in/IrisKeynote-ICB2012.pdf
- http://icb12.iiitd.ac.in/Fingerprint-ICB2012.pdf
- http://atvs.ii.uam.es/icb2013/files/ICB2013_Keynote1.pdf
- http://isp.yale.edu/event/location-tracking-and-biometrics-conference
- http://www.wjscheirer.com/papers/wjs_spb2011_bki.pdf
- http://vast.uccs.edu/~tboult/PAPERS/BTAS13-Trusted-BWI.pdf