Εφαρμογή της τεχνολογίας Distributed Ledger Technology / Blockchain σε συστήματα και διαδικασίες της Δημόσιας Διοίκησης

policy paper



Κείμενο Πολιτικής (Policy Paper) Υπουργείο Ψηφιακής Διακυβέρνησης και Τεχνητής Νοημοσύνης

«Incorporation of new technologies and trends towards Public Administration's advanced services, increase of efficiency and effectiveness, and decrease of systems operating, upgrade and maintenance costs - Introduce DLT / Blockchain»

Έκδοση 1.0 — Ιούλιος 2026

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Ψηφιακής Διακυβέρνησης
και Τεχνητής Νοημοσύνης

Εφαρμογή της τεχνολογίας Distributed Ledger Technology / Blockchain σε συστήματα και διαδικασίες της Δημόσιας Διοίκησης

ΣΥΝΟΨΗ

Η τεχνολογία κατανεμημένου καθολικού (Distributed Ledger Technology — DLT) δεν αποτελεί αυτοτελή στρατηγική ψηφιακού μετασχηματισμού, αλλά επιλεκτικό εργαλείο υποδομής εμπιστοσύνης (trust infrastructure). Η εθνική πολιτική οφείλει επομένως να μετατοπιστεί από τη λογική «υιοθέτησης μιας τεχνολογίας» στη λογική «παροχής υπηρεσιών εμπιστοσύνης»: η Ελλάδα δεν χρειάζεται εθνικό blockchain — χρειάζεται θεσμοθετημένη ικανότητα να εκδίδει, να επαληθεύει και να ανακαλεί ψηφιακές αποδείξεις με διασυνοριακή ισχύ.

ΤΟ ΠΡΟΒΛΗΜΑ

Η διεθνής εμπειρία είναι σαφής και αυστηρή: η συντριπτική πλειονότητα των έργων blockchain στη δημόσια διοίκηση δεν ξεπέρασε το στάδιο της απόδειξης έννοιας (proof of concept).

Το JRC εντόπισε 167 περιπτώσεις χρήσης σε ευρωπαϊκές διοικήσεις, εκ των οποίων ελάχιστες προχώρησαν πέραν του πιλοτικού σταδίου [1].

Ο ΟΟΣΑ έχει τεκμηριώσει ότι η αιτία δεν είναι κατά κύριο λόγο τεχνολογική, αλλά αφορά την αδυναμία τεκμηρίωσης υπεροχής έναντι απλούστερων λύσεων, τον συντονισμό μεταξύ φορέων και τη διαχείριση υπερβολικών προσδοκιών [2].

Η ΕΥΚΑΙΡΙΑ ΚΑΙ ΓΙΑΤΙ ΤΟ 2026 ΕΙΝΑΙ ΔΙΑΦΟΡΕΤΙΚΟ

1. Ο Κανονισμός (ΕΕ) 2024/1183 (eIDAS 2.0) εισάγει τα ηλεκτρονικά καθολικά ως νέα υπηρεσία εμπιστοσύνης με δυνατότητα «εγκεκριμένου» (qualified) καθεστώτος και τεκμήριο ακεραιότητας και χρονολογικής σειράς [3].
2. Η υποχρέωση διάθεσης Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας (EUDI Wallet) έως τον Δεκέμβριο 2026 [4] δημιουργεί άμεση ζήτηση για επαληθεύσιμα διαπιστευτήρια και για μητρώα αξιόπιστων εκδοτών (trust registries) — ακριβώς τλετουργία στην οποία το permissioned DLT προσφέρει τεκμηριωμένη προστιθέμενη αξία.

ΑΝΑΜΕΝΟΜΕΝΟ ΑΠΟΤΕΛΕΣΜΑ (ΩΣ ΠΡΟΣ ΤΟΥΣ ΣΤΟΧΟΥΣ ΤΗΣ ΜΕΤΑΡΡΥΘΜΙΣΗΣ)

Η εξοικονόμηση δεν προκύπτει από την τεχνολογία καθαυτή, αλλά από την κατάργηση επαναλαμβανόμενων επαληθεύσεων και δικαιολογητικών.

Ρεαλιστικός στόχος τριετίας:

↓ 30%

μείωση του αριθμού των διοικητικών επαληθεύσεων που απαιτούν επικοινωνία με τον εκδότη στις στοχευμένες διαδικασίες

και αντικατάσταση διμερών διεπαφών επαλήθευσης με ενιαίο επίπεδο επαλήθευσης.

ΚΟΡΥΦΑΙΕΣ ΣΥΣΤΑΣΕΙΣ

1. **Θεσμοθέτηση υποχρεωτικής «πύλης απόφασης» (decision gate)** πριν από κάθε δοκιμή για DLT: σκορ ≥6/7 στο checklist κριτηρίων αναγκαιότητας (Ενότητα 3.2) και τεκμηριωμένη σύγκριση με τρεις μη-DLT εναλλακτικές.

   Χωρίς αυτό, καμία χρηματοδότηση.

2. **Στρατηγική «EBSI-first»:** αξιοποίηση της Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI) μέσω της συμμετοχής της Ελλάδας στο EUROPEUM-EDIC, αντί ανάπτυξης εθνικού δικτύου DLT.

3. **Δύο και μόνο δύο παραγωγικές προτεραιότητες** για την τριετία: (α) επαληθεύσιμα διαπιστευτήρια δημόσιων εγγράφων μέσω gov.gr Wallet / EUDI Wallet και (β) αγκύρωση ακεραιότητας (notarisation/anchoring) κρίσιμων μητρώων και αρχείων καταγραφής.

4. Απόλυτος κανόνας μηδενικών προσωπικών δεδομένων on-chain, σύμφωνα με τις Κατευθυντήριες Γραμμές 02/2025 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) [5].

5. Ρήτρα λήξης (sunset clause) και στρατηγική εξόδου (exit strategy) ως υποχρεωτικοί συμβατικοί όροι σε κάθε έργο DLT, με προκαθορισμένα κριτήρια διακοπής.

ΒΑΣΙΚΕΣ ΠΗΓΕΣ

[1] JRC (Joint Research Centre), "Blockchain in Public Services – Mapping Study", 2018.
[2] ΘΕCD, "Distributed Ledger Technology (DLT) and Blockchain in Government: Opportunities and Challenges", 2020.
[3] Κανονισμός (ΕΕ) 2024/1183 για την τροποποίηση του Κανονισμού (ΕΕ) αριθ. 910/2014 (eIDAS 2.0).
[4] Κανονισμός (ΕΕ) 2024/1183 (eIDAS 2.0) – Υποχρέωση διάθεσης EUDI Wallet έως 24.12.2026.
[5] European Data Protection Board (EDPB), Guidelines 02/2025 on Blockchain, 2025.



DLT ως ΥΠΟΔΟΜΗ ΕΜΠΙΣΤΟΣΥΝΗΣ: ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ

Από την έκδοση έως την επαλήθευση ψηφιακών αποδείξεων

ΕΚΔΟΣΗ
Ο έμπιστος φορέας εκδίδει ψηφιακό διαπιστευτήριο (credential)

→

ΚΑΤΑΓΡΑΦΗ ΣΤΟ DLT
Καταγράφεται κρυπτογραφικό αποτύπωμα (hash) και μεταδεδομένα (όχι προσωπικά δεδομένα)

→

ΑΠΟΘΗΚΕΥΣΗ ΕΚΤΟΣ ΑΛΥΣΙΔΑΣ
Το έγγραφο/δεδομένα παραμένουν σε ασφαλές σύστημα του εκδότη

→

ΕΠΑΛΗΘΕΥΣΗ
Ο έλεγχος ακεραιότητας και αυθεντικότητας γίνεται μέσω του DLT

→

ΑΝΑΚΛΗΣΗ
Δυνατότητα ανάκλησης και άμεσης ενημέρωσης της κατάστασης

- **ΑΚΕΡΑΙΟΤΗΤΑ** (Integrity)
- **ΜΗ ΑΡΝΗΣΗ** (Non-repudiation)
- **ΧΡΟΝΟΛΟΓΙΚΗ ΣΕΙΡΑ** (Timestamping)
- **ΔΙΑΦΑΝΕΙΑ & ΙΧΝΗΛΑΣΙΜΟΤΗΤΑ** (Transparency & Traceability)

ΠΟΥ ΠΡΟΣΦΕΡΕΙ ΠΡΟΣΤΙΘΕΜΕΝΗ ΑΞΙΑ ΤΟ DLT ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

ΔΥΟ ΠΑΡΑΓΩΓΙΚΕΣ ΠΡΟΤΕΡΑΙΟΤΗΤΕΣ (2026–2028)

1. **ΕΠΑΛΗΘΕΥΣΙΜΑ ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ ΔΗΜΟΣΙΩΝ ΕΓΓΡΑΦΩΝ**
   Έκδοση και επαλήθευση εγγράφων (π.χ. τίτλοι σπουδών, πιστοποιητικά, άδειες, βεβαιώσεις) μέσω EUDI Wallet / gov.gr Wallet



2. **ΑΓΚΥΡΩΣΗ ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΡΙΣΙΜΩΝ ΜΗΤΡΩΩΝ & LOGS**
   Notarisation / anchoring για κρίσιμα μητρώα (κτηματολόγιο, δημοτολόγιο, μητρώο αδειών κ.ά.) και αρχεία καταγραφής συστημάτων



ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΑΜΗΛΗΣ Ή ΜΗΔΕΝΙΚΗΣ ΑΞΙΑΣ

- Αποθήκευση μεγάλων αρχείων ή προσωπικών δεδομένων on-chain
- Εσωτερικές εφαρμογές ενός φορέα χωρίς ανάγκη διαμοιρασμένης εμπιστοσύνης
- Διαδικασίες χωρίς πολλαπλούς, ανεξάρτητους επαληθευτές
- Περιπτώσεις όπου απλές λύσεις (βάσεις δεδομένων, υπογραφές, χρονικές σφραγίδες) επιτυγχάνουν τον ίδιο στόχο

ΣΤΟΧΟΣ: ΛΙΓΕΣ, ΣΤΟΧΕΥΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ ΜΕ ΜΕΤΡΗΣΙΜΟ ΟΦΕΛΟΣ

ΠΛΑΙΣΙΟ ΔΙΑΚΥΒΕΡΝΗΣΗΣ & ΚΡΙΣΙΜΟΙ ΠΥΛΩΝΕΣ ΕΠΙΤΥΧΙΑΣ

1. ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ
Εναρμόνιση με eIDAS 2.0, GDPR, Κατευθυντήριες Γραμμές EDPB, εθνικό νομικό και κανονιστικό πλαίσιο.

2. ΔΙΑΚΥΒΕΡΝΗΣΗ
Κεντρική στρατηγική, σαφείς ρόλοι και αρμοδιότητες, μοντέλο διακυβέρνησης πολλών φορέων.

3. ΤΕΧΝΟΛΟΓΙΑ & ΠΡΟΤΥΠΑ
Χρήση EBSI, ευρωπαϊκών προτύπων (π.χ. W3C Verifiable Credentials), διαλειτουργικότητα by design.

4. ΑΣΦΑΛΕΙΑ & ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ
Μηδενικά προσωπικά δεδομένα on-chain, κρυπτογράφηση, έλεγχοι πρόσβασης, privacy by design.

5. ΟΙΚΟΝΟΜΙΚΗ ΒΙΩΣΙΜΟΤΗΤΑ
Ανάλυση κόστους-οφέλους, βιωσιμότητα, ρήτρα λήξης και στρατηγική εξόδου.

6. ΑΞΙΟΛΟΓΗΣΗ & ΜΕΤΡΗΣΗ
Μετρήσιμοι δείκτες (KPIs), συνεχής αξιολόγηση, προσαρμογή.

-30%

ΚΥΡΙΟΣ ΔΕΙΚΤΗΣ ΕΠΙΤΥΧΙΑΣ
Μείωση διοικητικών επαληθεύσεων που απαιτούν επικοινωνία με τον εκδότη κατά ≥30% στις στοχευμένες διαδικασίες εντός τριετίας

ΜΕΤΡΗΣΙΜΟ ΟΦΕΛΟΣ
Λιγότερες επαληθεύσεις, ταχύτερες διαδικασίες, χαμηλότερο διοικητικό κόστος, αυξημένη εμπιστοσύνη πολιτών και επιχειρήσεων

1. Επιτελική Σύνοψη (Executive Summary)

Η τεχνολογία κατανεμημένου καθολικού (Distributed Ledger Technology — DLT) δεν αποτελεί αυτοτελή στρατηγική ψηφιακού μετασχηματισμού, αλλά επιλεκτικό εργαλείο υποδομής εμπιστοσύνης (trust infrastructure). Η εθνική πολιτική οφείλει επομένως να μετατοπιστεί από τη λογική «υιοθέτησης μιας τεχνολογίας» στη λογική «παροχής υπηρεσιών εμπιστοσύνης»: η Ελλάδα δεν χρειάζεται εθνικό blockchain — χρειάζεται θεσμοθετημένη ικανότητα να εκδίδει, να επαληθεύει και να ανακαλεί ψηφιακές αποδείξεις με διασυνοριακή ισχύ.

Το πρόβλημα. Η διεθνής εμπειρία είναι σαφής και αυστηρή: η συντριπτική πλειονότητα των έργων blockchain στη δημόσια διοίκηση δεν ξεπέρασε το στάδιο της απόδειξης έννοιας (proof of concept). Η καταγραφή του Κοινού Κέντρου Ερευνών της Ευρωπαϊκής Επιτροπής (Joint Research Centre — JRC) εντόπισε 167 περιπτώσεις χρήσης σε ευρωπαϊκές διοικήσεις, εκ των οποίων ελάχιστες προχώρησαν πέραν του πιλοτικού σταδίου [1], ενώ ο ΟΟΣΑ έχει τεκμηριώσει ότι η αιτία δεν είναι κατά κύριο λόγο τεχνολογική, αλλά αφορά την αδυναμία τεκμηρίωσης υπεροχής έναντι απλούστερων λύσεων, τον συντονισμό μεταξύ φορέων και τη διαχείριση υπερβολικών προσδοκιών [2].

Η ευκαιρία (και γιατί το 2026 είναι διαφορετικό). Δύο εξελίξεις μεταβάλλουν ουσιωδώς το πλαίσιο σε σχέση με την περίοδο 2018–2023:

1. Ο Κανονισμός (ΕΕ) 2024/1183 (eIDAS 2.0) εισάγει τα ηλεκτρονικά καθολικά (electronic ledgers) ως *νέα, αυτοτελή υπηρεσία εμπιστοσύνης* με δυνατότητα «εγκεκριμένου» (qualified) καθεστώτος και τεκμήριο ακεραιότητας και χρονολογικής σειράς [3]. Για πρώτη φορά, το DLT αποκτά ρητή νομική βάση και αποδεικτική αξία στο ενωσιακό δίκαιο — παύει να είναι τεχνολογικό πείραμα και γίνεται ρυθμιζόμενη υπηρεσία.
2. Η υποχρέωση διάθεσης Ευρωπαϊκού Πορτοφολιού Ψηφιακής Ταυτότητας (EU Digital Identity Wallet — EUDI Wallet) έως τον Δεκέμβριο 2026 [4] δημιουργεί άμεση, μη αναβαλλόμενη ζήτηση για επαληθεύσιμα διαπιστευτήρια (verifiable credentials) και για μητρώα αξιόπιστων εκδοτών (trust registries) — ακριβώς τη λειτουργία στην οποία το permissioned DLT προσφέρει τεκμηριωμένη προστιθέμενη αξία.

Κορυφαίες συστάσεις (αναλυτικά στην Ενότητα 11):

1. Θεσμοθέτηση υποχρεωτικής «πύλης απόφασης» (decision gate) πριν από κάθε δαπάνη για DLT: σκορ ≥6/7 στο checklist κριτηρίων αναγκαιότητας (Ενότητα 3.2) και τεκμηριωμένη σύγκριση με τρεις μη-DLT εναλλακτικές. Χωρίς αυτό, καμία χρηματοδότηση.
2. Στρατηγική «EBSI-first»: αξιοποίηση της Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (European Blockchain Services Infrastructure — EBSI) μέσω της συμμετοχής της Ελλάδας στο EUROPEUM-EDIC, αντί ανάπτυξης εθνικού δικτύου DLT.
3. Δύο και μόνο δύο παραγωγικές προτεραιότητες για την τριετία: (α) επαληθεύσιμα διαπιστευτήρια δημόσιων εγγράφων μέσω gov.gr Wallet/EUDI Wallet και (β) αγκύρωση ακεραιότητας (notarisation/anchoring) κρίσιμων μητρώων και αρχείων καταγραφής.
4. Απόλυτος κανόνας μηδενικών προσωπικών δεδομένων on-chain, σύμφωνα με τις Κατευθυντήριες Γραμμές 02/2025 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (EDPB) [5].
5. Ρήτρα λήξης (sunset clause) και στρατηγική εξόδου (exit strategy) ως υποχρεωτικοί συμβατικοί όροι σε κάθε έργο DLT, με προκαθορισμένα κριτήρια διακοπής.

Αναμενόμενο αποτέλεσμα ως προς τους στόχους της μεταρρύθμισης. Η εξοικονόμηση δεν προκύπτει από την τεχνολογία καθαυτή, αλλά από την κατάργηση επαναλαμβανόμενων επαληθεύσεων και δικαιολογητικών. Ρεαλιστικός στόχος τριετίας: μείωση του αριθμού των διοικητικών επαληθεύσεων που απαιτούν επικοινωνία με τον εκδότη κατά τουλάχιστον 30% στις στοχευμένες διαδικασίες, και αντικατάσταση διμερών διεπαφών επαλήθευσης με ενιαίο επίπεδο επαλήθευσης.

2. Σκοπός και πλαίσιο πολιτικής

2.1 Σκοπός

Το παρόν κείμενο καθορίζει τη θέση πολιτικής του Υπουργείου Ψηφιακής Διακυβέρνησης για την εισαγωγή τεχνολογιών κατανεμημένου καθολικού (DLT) στη δημόσια διοίκηση. Καθορίζει τις προϋποθέσεις υιοθέτησης, τις αρχιτεκτονικές κατευθύνσεις, το πλαίσιο κανονιστικής συμμόρφωσης και τις προτεραιότητες υλοποίησης για την περίοδο 2026–2030.

Πεδίο εφαρμογής και μεθοδολογία. Οι συστάσεις του παρόντος κειμένου απευθύνονται σε φορείς της Γενικής Κυβέρνησης, σε νομικά πρόσωπα δημοσίου δικαίου και σε φορείς τοπικής αυτοδιοίκησης που εξετάζουν ή υλοποιούν έργα DLT/blockchain, με χρονικό ορίζοντα εφαρμογής την περίοδο 2026–2030. Η ανάλυση βασίζεται σε επεξεργασία δημόσιων στοιχείων, σε νομοθετική και κανονιστική εξέταση του ενωσιακού και εθνικού δικαίου, και σε διεθνή βιβλιογραφική έρευνα με έμφαση στην περίοδο 2024–2026 (τεκμηρίωση στην Ενότητα 4 και στις Πηγές).

2.2 Σύνδεση με τους στόχους της μεταρρύθμισης

Η στρατηγική αξιοποίησης του DLT στην ελληνική δημόσια διοίκηση υπηρετεί έξι στόχους:

1. **Ενίσχυση της αξιοπιστίας και της ακεραιότητας των δημόσιων δεδομένων.**
2. **Αύξηση της διαφάνειας και της λογοδοσίας στις διοικητικές διαδικασίες.**
3. **Βελτίωση της αποδοτικότητας και μείωση του διοικητικού κόστους.**
4. **Ενίσχυση της διαλειτουργικότητας και της συνεργασίας μεταξύ φορέων.**
5. **Υποστήριξη διασυνοριακών ψηφιακών υπηρεσιών στο πλαίσιο της Ευρωπαϊκής Ένωσης.**
6. **Ανάπτυξη θεσμικής και τεχνικής ικανότητας εντός της δημόσιας διοίκησης.**

Η μεταρρύθμιση θέτει τρεις μετρήσιμους στόχους: αύξηση αποδοτικότητας, αύξηση αποτελεσματικότητας και μείωση του κόστους λειτουργίας, αναβάθμισης και συντήρησης συστημάτων. Ο τρίτος στόχος επιβάλλει ιδιαίτερη προσοχή, διότι το DLT δεν μειώνει αυτομάτως το κόστος· αντιθέτως, εισάγει νέες κατηγορίες κόστους (λειτουργία κόμβων, διακυβέρνηση κοινοπραξίας, εξειδικευμένη συντήρηση, κρυπτογραφική διαχείριση κλειδιών).

Πού υπάρχει πραγματική οικονομία. Το DLT μειώνει το κόστος σε ένα και μόνο δομικό σενάριο: όταν αντικαθιστά πολλαπλές διμερείς διασυνδέσεις επαλήθευσης με ένα κοινό επίπεδο. Σε ένα οικοσύστημα N φορέων που πρέπει να επαληθεύουν αμοιβαία δεδομένα, οι απαιτούμενες διμερείς διεπαφές αυξάνονται τετραγωνικά (τάξης N^2), ενώ ένα κοινό επίπεδο επαλήθευσης απαιτεί N συνδέσεις.

> Απλό παράδειγμα. Ένας απόφοιτος ελληνικού πανεπιστημίου που υποβάλλει αίτηση σε γερμανικό εργοδότη. Σήμερα: ο εργοδότης επικοινωνεί με το ίδρυμα, ζητά επικύρωση, μεταφράζει, ενδεχομένως απαιτείται *apostille*. Κόστος: ημέρες, τέλη, ανθρωποώρες σε τρεις χώρες. Με επαληθεύσιμο διαπιστευτήριο αγκυρωμένο σε ευρωπαϊκό μητρώο εμπιστοσύνης: ο εργοδότης επαληθεύει κρυπτογραφικά σε δευτερόλεπτα, χωρίς καμία επικοινωνία με το ίδρυμα. Η εξοικονόμηση δεν είναι στο πανεπιστήμιο· είναι στην κατάργηση της διαδικασίας επαλήθευσης συνολικά.

Πού δεν υπάρχει οικονομία. Όταν υπάρχει ήδη ενιαία, αξιόπιστη κεντρική αρχή (π.χ. ΑΑΔΕ για φορολογικά δεδομένα), η προσθήκη DLT αυξάνει την πολυπλοκότητα χωρίς αντίστοιχο όφελος. Το ίδιο ισχύει όταν το ζητούμενο είναι απλώς η ψηφιοποίηση μιας εσωτερικής ροής.

2.3 Πού βρίσκεται σήμερα η Ελλάδα

Η Ελλάδα διαθέτει ήδη θεσμικά και τεχνικά θεμέλια για στοχευμένη αξιοποίηση DLT, γεγονός που διαφοροποιεί τη σημερινή αφετηρία από εκείνη πολλών άλλων κρατών μελών.

Θεσμικό επίπεδο. Ο Ν.4961/2022 αναγνωρίζει νομικά την τεχνολογία κατανεμημένου καθολικού και τα έξυπνα συμβόλαια (Ενότητα 6.3). **Υποδομές.** Το gov.gr Wallet φιλοξενεί ήδη πλήθος ψηφιακών εγγράφων και έχει διασυνδεθεί με το κυπριακό «Ψηφιακός Πολίτης» από τον Μάιο 2025 (Ενότητα 4.4), ενώ το Κέντρο Διαλειτουργικότητας (ΚΕΔ) παρέχει το υφιστάμενο σημείο ανταλλαγής δεδομένων μεταξύ φορέων (Ενότητα

5.1). **Ευρωπαϊκή συμμετοχή.** Η χώρα συμμετέχει στην European Blockchain Partnership και είναι ιδρυτικό μέλος του EUROPEUM-EDIC που διοικεί το EBSI (Ενότητα 4.2)· η ΕΔΥΤΕ έχει ήδη εμπειρία σε ευρωπαϊκά έργα EBSI [26] και η χώρα διαθέτει από το 2022 υπηρεσία ψηφιακών πιστοποιητικών σπουδών μέσω gov.gr [25]. Η αφετηρία αυτή πρέπει να αξιοποιηθεί άμεσα, πριν εξανεμιστεί το συγκριτικό πλεονέκτημα χρόνου που περιγράφεται στην Ενότητα 4.4.

2.4 Ρητές παραδοχές (assumptions)

#	Παραδοχή	Κίνδυνος αν δεν ισχύει
A1	Η Ελλάδα θα διαθέσει συμμορφούμενο EUDI Wallet εντός του χρονικού πλαισίου του Κανονισμού 2024/1183	Αποσύνδεση των έργων DLT από τη βασική υποδομή ταυτότητας
A2	Το EBSI θα φθάσει σε πλήρη παραγωγική λειτουργία υπό το EUROPEUM-EDIC	Ανάγκη εναλλακτικής εθνικής/διμερούς υποδομής, με αυξημένο κόστος
A3	Τα υφιστάμενα εθνικά μητρώα παραμένουν τα αυθεντικά μητρώα αναφοράς (systems of record)	Νομική αβεβαιότητα ως προς την υπεροχή δεδομένων
A4	Η χρηματοδότηση παραμένει συνδεδεμένη με ορόσημα και όχι με παραδοτέα τεχνολογίας	Υιοθέτηση για λόγους τεχνολογικής μόδας

3. Η αξία και τα όρια του DLT/Blockchain

Το DLT δεν αποτελεί ενιαία τεχνολογική επιλογή, αλλά οικογένεια αρχιτεκτονικών με διαφορετικά χαρακτηριστικά διακυβέρνησης, απόδοσης και κανονιστικής συμμόρφωσης. Οι τρεις βασικές κατηγορίες συνοψίζονται στον πίνακα που ακολουθεί.

Τύπος	Χαρακτηριστικά	Πλεονεκτήματα	Περιορισμοί για δημόσιο τομέα
Δημόσιο (public permissionless)	Πλήρης αποκέντρωση, ανοικτή συμμετοχή (π.χ. Ethereum)	Υψηλή διαφάνεια, ανθεκτικότητα	Περιορισμένος έλεγχος διακυβέρνησης, δυσκολία συμμόρφωσης με GDPR/eIDAS, ζητήματα εμπιστευτικότητας
Ιδιωτικό (private)	Έλεγχος από έναν οργανισμό	Υψηλή απόδοση, πλήρης έλεγχος πρόσβασης	Περιορισμένη αποκέντρωση· συχνά ισοδύναμο συμβατικής βάσης δεδομένων
Συνεργατικό (consortium/permissioned)	Διακυβέρνηση κατανεμημένη μεταξύ αξιόπιστων φορέων	Ελεγχόμενη αποκέντρωση, καλή απόδοση, συμβατότητα με κανονιστικό πλαίσιο	Απαιτεί σαφές πλαίσιο διακυβέρνησης μεταξύ φορέων

Η προτεινόμενη επιλογή για τη δημόσια διοίκηση είναι το συνεργατικό (consortium/permissioned) μοντέλο (βλ. Αρχή 1, Ενότητα 5.1).

3.1 Πού προσφέρει τεκμηριωμένη αξία

Το DLT προσφέρει αξία **αποκλειστικά** όταν συντρέχουν σωρευτικά: (i) πολλαπλοί ανεξάρτητοι φορείς χωρίς πλήρη αμοιβαία εμπιστοσύνη, (ii) ανάγκη αμεταβλητότητας (immutability) και ελεγξιμότητας (auditability), (iii) ανάγκη επαλήθευσης από τρίτους **χωρίς επικοινωνία με τον εκδότη**, (iv) απουσία αποδεκτής κεντρικής αρχής, (v) δυνατότητα τυποποίησης των κανόνων. Οι αρχές αυτές μεταφράζονται σε ένα πρακτικό εργαλείο βαθμολόγησης (Ενότητα 3.2).

3.2 Η υποχρεωτική πύλη απόφασης

Η υιοθέτηση DLT σε νέο έργο δημόσιας διοίκησης προϋποθέτει θετική αξιολόγηση σε ένα δομημένο checklist επτά κριτηρίων αναγκαιότητας, με βαθμολογία 0–7, όπως παρουσιάζεται στον πίνακα που ακολουθεί. **Το παρόν κείμενο πολιτικής καθιστά το εργαλείο αυτό δεσμευτικό** και το ενισχύει με δεύτερο σκέλος:

Ερώτημα αξιολόγησης	Ναι (1)	Όχι (0)
Εμπλέκονται περισσότεροι από δύο ανεξάρτητοι φορείς που δεν εμπιστεύονται πλήρως ο ένας τον άλλον;	☐	☐
Απαιτείται αμετάβλητο ιστορικό καταγραφής (audit trail) για νομικούς ή ελεγκτικούς λόγους;	☐	☐
Είναι ανεπιθύμητη ή μη εφικτή η ύπαρξη κεντρικής αρχής ελέγχου των δεδομένων;	☐	☐
Απαιτείται επαλήθευση δεδομένων από τρίτους χωρίς επικοινωνία με τον εκδότη;	☐	☐
Μπορούν οι διαδικασίες να τυποποιηθούν και να αυτοματοποιηθούν μέσω προκαθορισμένων κανόνων;	☐	☐
Δεν υπάρχει ήδη αξιόπιστη και αποδοτική κεντρική λύση για το ίδιο πρόβλημα;	☐	☐
Τα δεδομένα που θα διαχειριστεί το σύστημα δεν περιλαμβάνουν ευαίσθητα προσωπικά δεδομένα on-chain;	☐	☐

Ερμηνεία αποτελέσματος: Σκορ 6–7 — κατάλληλο, προχωρήστε σε πλήρη σκοπιμότητα· σκορ 4–5 — απαιτείται βαθύτερη ανάλυση εναλλακτικών λύσεων· σκορ 0–3 — η χρήση DLT δεν ενδείκνυται, εξετάστε παραδοσιακές ψηφιακές λύσεις.

Πύλη Α — Αναγκαιότητα. Σκορ ≥6/7 στο checklist κριτηρίων αναγκαιότητας του πίνακα ανωτέρω.

Πύλη Β — Συγκριτική υπεροχή. Τεκμηριωμένη απόρριψη τριών εναλλακτικών, με ποσοτικά στοιχεία:

Εναλλακτική (μη-DLT)	Τι ήδη προσφέρει	Πότε επαρκεί
Εγκεκριμένη ηλεκτρονική σφραγίδα (qualified electronic seal) σε δομημένο έγγραφο	Αυθεντικότητα εκδότη + ακεραιότητα περιεχομένου, επαληθεύσιμη χωρίς επικοινωνία με τον εκδότη	Όταν δεν απαιτείται έλεγχος **κατάστασης/ανάκλησης** ή κοινή ιστορικότητα
Εγκεκριμένη χρονοσφραγίδα (qualified timestamp)	Απόδειξη ύπαρξης δεδομένου σε χρόνο	Όταν αρκεί μεμονωμένη απόδειξη χρόνου, χωρίς κοινό καθολικό
Κέντρο Διαλειτουργικότητας (ΚΕΔ) / API μεταξύ μητρώων	Άντληση αυθεντικών δεδομένων από την πηγή	Όταν οι φορείς εμπιστεύονται την πηγή και η διασύνδεση είναι εφικτή

Κρίσιμη διάκριση για τη χάραξη πολιτικής: η εγκεκριμένη ηλεκτρονική σφραγίδα λύνει ήδη το πρόβλημα της *αυθεντικότητας εγγράφου*. Το DLT προσθέτει αξία κυρίως στα μητρώα εμπιστοσύνης, στην ανάκληση/κατάσταση διαπιστευτηρίων και στο κοινό, μη διαγράψιμο ιστορικό. Έργα που παρουσιάζονται ως «blockchain για ψηφιακά πιστοποιητικά» ενώ αφορούν μόνο υπογραφή εγγράφου, πρέπει να απορρίπτονται.

3.3 Τι δεν λύνει το DLT

- **Ποιότητα εισερχόμενων δεδομένων.** Η αμεταβλητότητα διασφαλίζει ότι ένα λανθασμένο δεδομένο θα παραμείνει λανθασμένο και αναλλοίωτο («oracle problem»). Το DLT εγγυάται *ακεραιότητα*, όχι *ορθότητα*.
- **Ταυτοποίηση.** Απαιτεί ούτως ή άλλως eIDAS-συμβατή ταυτοποίηση.
- **Νομική ισχύ.** Προκύπτει από τον νόμο (Ν.4961/2022, eIDAS 2.0), όχι από το πρωτόκολλο.
- **Οργανωτική δυσλειτουργία.** Η διακυβέρνηση μιας κοινοπραξίας είναι δυσκολότερη από τη λειτουργία μιας βάσης δεδομένων, όχι ευκολότερη.
- **Απόδοση σε πραγματικό χρόνο.** Ακόμη και τα permissioned δίκτυα υστερούν έναντι συμβατικών βάσεων σε φόρτο υψηλής συχνότητας.

4. Διεθνείς και ευρωπαϊκές εξελίξεις (2024–2026)

4.1 eIDAS 2.0: από πείραμα σε ρυθμιζόμενη υπηρεσία εμπιστοσύνης

Ο **Κανονισμός (ΕΕ) 2024/1183** (δημοσίευση 30.04.2024, έναρξη ισχύος 20.05.2024) τροποποιεί τον Κανονισμό 910/2014 και εισάγει το Ευρωπαϊκό Πλαίσιο Ψηφιακής Ταυτότητας [3]. Δύο στοιχεία είναι καθοριστικά για τη δημόσια διοίκηση:

- **Ηλεκτρονικά καθολικά (electronic ledgers).** Θεσπίζεται νέο τμήμα για τα ηλεκτρονικά καθολικά, με ορισμό («αλληλουχία ηλεκτρονικών εγγραφών δεδομένων που διασφαλίζει την ακεραιότητά τους»), νομικά αποτελέσματα και απαιτήσεις για το **εγκεκριμένο** ηλεκτρονικό καθολικό: διαπίστωση προέλευσης εγγραφών, μοναδική διαδοχική χρονολογική σειρά, άμεση ανιχνευσιμότητα κάθε μεταγενέστερης μεταβολής. Το εγκεκριμένο καθολικό μπορεί να παρέχεται από έναν ή περισσότερους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης — δηλαδή και υπό μορφή **permissioned distributed ledger** [3], [6]. *Σημείωση ακρίβειας:* η ακριβής αρίθμηση των άρθρων (Τμήμα 11 του ενοποιημένου Κανονισμού 910/2014) πρέπει να επαληθεύεται στο ενοποιημένο κείμενο του EUR-Lex, καθώς οι δευτερογενείς πηγές παρουσιάζουν αποκλίσεις.
- **Επαληθεύσιμα διαπιστευτήρια και πορτοφόλι.** Κάθε κράτος μέλος υποχρεούται να διαθέσει τουλάχιστον ένα EUDI Wallet έως τα τέλη Δεκεμβρίου 2026 [4]. Τα ηλεκτρονικά διαπιστευτήρια ιδιοτήτων (Electronic Attestations of Attributes — EAA/QEAA) αποτελούν τον φορέα των δημόσιων πιστοποιητικών.

Πρακτική συνέπεια πολιτικής: η ελληνική δημόσια διοίκηση δεν χρειάζεται πλέον να «δικαιολογήσει» νομικά τη χρήση DLT. Χρειάζεται να επιλέξει αν θα λειτουργήσει **ως εκδότης διαπιστευτηρίων**, **ως φορέας μητρώου εμπιστοσύνης**, ή και τα δύο.

4.2 EBSI και EUROPEUM-EDIC: η ευρωπαϊκή υποδομή εισέρχεται σε παραγωγή

Το **EBSI** αποτελεί δίκτυο ομοτίμων κόμβων της Ευρωπαϊκής Σύμπραξης Blockchain (European Blockchain Partnership — EBP: 27 κράτη μέλη, Νορβηγία, Λιχτενστάιν και η Επιτροπή), με αρχικές περιπτώσεις χρήσης τη **συμβολαιογραφική αγκύρωση (notarisation)**, τα **διπλώματα**, την **ευρωπαϊκή ψηφιακή ταυτότητα** και την **αξιόπιστη ανταλλαγή δεδομένων** μεταξύ τελωνειακών και φορολογικών αρχών [7].

Οι εξελίξεις 2024–2026:

- **Μάιος 2024:** σύσταση του **EUROPEUM-EDIC**, ευρωπαϊκής κοινοπραξίας ψηφιακών υποδομών υπό την ηγεσία των κρατών μελών, με εντολή να αναλάβει τη διακυβέρνηση του EBSI και να το οδηγήσει σε παραγωγική λειτουργία. **Η Ελλάδα συγκαταλέγεται στα ιδρυτικά κράτη μέλη**, μαζί με Βέλγιο, Κροατία, Κύπρο, Ιταλία, Λουξεμβούργο, Πολωνία, Πορτογαλία, Ρουμανία, Ισπανία και Σλοβενία [8].
- **2025:** το έργο EBSI-NE ανέπτυξε 18 νέους κόμβους επικύρωσης σε 15 κράτη μέλη και τη Νορβηγία (σύνολο δικτύου ~59 κόμβοι σε πιλοτικό, προπαραγωγικό και παραγωγικό περιβάλλον)· το **παραγωγικού επιπέδου δίκτυο** λειτουργεί με 15 κόμβους επικύρωσης και μηχανισμό συναίνεσης **Proof of Authority**, με απαίτηση συμμόρφωσης κόμβων προς ISO/IEC 27001 ή ισοδύναμο [8].
- **Κατεύθυνση:** το EBSI εξελίσσεται ώστε να πληροί τις προϋποθέσεις **εγκεκριμένου ηλεκτρονικού καθολικού** κατά τον Κανονισμό 2024/1183 [8], [6].

Στρατηγική σημασία για την Ελλάδα: η συμμετοχή στο EUROPEUM-EDIC σημαίνει ότι η χώρα **έχει ήδη πρόσβαση σε παραγωγική, θεσμικά κατοχυρωμένη υποδομή DLT**. Η ανάπτυξη παράλληλου εθνικού δικτύου θα ήταν διπλή δαπάνη χωρίς αντίστοιχο όφελος.

4.3 Πιλότοι Μεγάλης Κλίμακας (Large Scale Pilots): τι έδειξαν

Πιλότος	Περίοδος	Εμβέλεια	Βασικό δίδαγμα
POTENTIAL	04/2023 – 09/2025	140+ οργανισμοί, 19 χώρες + Ουκρανία· 6 περιπτώσεις χρήσης (ηλ. διακυβέρνηση, άνοιγμα τραπεζικού λογαριασμού, εγγραφή SIM/eSIM, ψηφιακή άδεια οδήγησης, εγκεκριμένη ηλ. υπογραφή,	Ταχύτερα προχώρησαν οι χώρες με ισχυρό εθνικό συντονισμό και έγκαιρη εμπλοκή του ιδιωτικού τομέα· απαιτείται αυστηρή,

		ηλ. συνταγογράφηση)· >1.300 δοκιμές, >1.000 επιτυχείς συναλλαγές εκ των οποίων 249 διασυνοριακές	ομοιόμορφη εφαρμογή κοινών προτύπων [9], [10]
EWC (EU Digital Wallet Consortium)	2023 – 2025	Ταξίδια και πληρωμές	Η αποδοχή εξαρτάται από την ψηφιακή ωριμότητα και την εμπιστοσύνη ανά χώρα· οι πολίτες ανησυχούν για συγκεντρωτισμό· κρίσιμα η οικεία σχεδίαση διεπαφής και η λειτουργία εκτός σύνδεσης [9]

4.4 Ετοιμότητα EUDI Wallet: ρεαλιστική εκτίμηση

Παρά την αυστηρή προθεσμία, η ετοιμότητα των κρατών μελών παραμένει άνιση. Δημοσιευμένες αναλύσεις και δηλώσεις παραγόντων της Επιτροπής εντός του 2025–2026 υποδεικνύουν ότι **λιγότερα από το ένα τρίτο των κρατών μελών πληρούν τα κριτήρια ετοιμότητας**, ενώ ορισμένα (π.χ. Κάτω Χώρες) έχουν ήδη σηματοδοτήσει καθυστέρηση [11], [12].

> **Δήλωση αβεβαιότητας.** Οι εκτιμήσεις ετοιμότητας προέρχονται από κλαδικές αναλύσεις και δημοσιογραφικές πηγές, όχι από επίσημη αξιολόγηση της Επιτροπής. Πρέπει να επαληθεύονται μέσω των επίσημων ανακοινώσεων της DG CNECT και της ομάδας συνεργασίας eIDAS.

Συνέπεια πολιτικής: η Ελλάδα διαθέτει **συγκριτικό πλεονέκτημα χρόνου**. Το gov.gr Wallet φιλοξενεί ήδη πλήθος ψηφιακών εγγράφων, και από τον **Μάιο 2025** λειτουργεί η διαλειτουργικότητα με το κυπριακό «Ψηφιακός Πολίτης» — η **πρώτη διασυνοριακή αμοιβαία αναγνώριση ψηφιακών εγγράφων ταυτότητας και άδειας οδήγησης μεταξύ κρατών μελών** [13]. Το πλεονέκτημα αυτό πρέπει να μετατραπεί σε παραγωγικές υπηρεσίες διαπιστευτηρίων, όχι σε νέα πιλοτικά.

4.5 MiCA: οριοθέτηση της συνάφειας

Ο **Κανονισμός (ΕΕ) 2023/1114 (MiCA)** τέθηκε σε πλήρη εφαρμογή στις 30.12.2024 [14]. Στην Ελλάδα, ο **Ν.5193/2025** προσαρμόζει την εθνική νομοθεσία, ορίζει την **Επιτροπή Κεφαλαιαγοράς** ως αρμόδια αρχή για τους παρόχους υπηρεσιών κρυπτοστοιχείων (CASPs) και θεσπίζει κυρώσεις· η Επιτροπή Κεφαλαιαγοράς εξέδωσε την υπ' αριθ. 8/1059/30.07.2025 απόφαση για τη διαδικασία αδειοδότησης [15], [16].

Οριοθέτηση — κρίσιμο για την αποφυγή σύγχυσης: ο MiCA **δεν ρυθμίζει** τη χρήση DLT από τη δημόσια διοίκηση. Ρυθμίζει τα κρυπτοστοιχεία και τους παρόχους σχετικών υπηρεσιών. Έργα δημόσιας διοίκησης που **δεν εκδίδουν μεταβιβάσιμα ψηφιακά περιουσιακά στοιχεία** βρίσκονται εκτός πεδίου εφαρμογής. Η συνάφεια είναι έμμεση αλλά υπαρκτή σε τρία σημεία: (i) οποιαδήποτε μελλοντική **συμβολαιοποίηση (tokenisation)** δημόσιων περιουσιακών στοιχείων ενεργοποιεί σύνθετο ρυθμιστικό καθεστώς και **δεν συνιστάται** στον παρόντα ορίζοντα· (ii) η εποπτική ικανότητα που αναπτύσσεται στην Επιτροπή Κεφαλαιαγοράς αποτελεί εθνικό απόθεμα τεχνογνωσίας· (iii) ο MiCA εδραιώνει την αρχή ότι η ΕΕ ρυθμίζει **χρήσεις**, όχι τεχνολογίες.

4.6 Παραγωγικά έργα κρατών μελών και τι διδάσκουν

Χώρα	Έργο / εξέλιξη	Κατάσταση	Δίδαγμα
Εσθονία	KSI Blockchain σε κρατικά μητρώα (υγεία, κτηματολόγιο, εμπορικό μητρώο, δικαστικές αποφάσεις)· χρονοσφράγιση κάθε ψηφιακής ενέργειας [21]	Παραγωγικό από το 2012	Το πλέον επιτυχημένο μοντέλο είναι αγκύρωση ακεραιότητας, όχι αποθήκευση δεδομένων. Χαμηλό ρίσκο, υψηλή απόδοση.
Ισπανία	ISBE — εθνική υποδομή υπηρεσιών blockchain ευθυγραμμισμένη με EBSI (Hyperledger Besu)· MVP Ιούλιος 2025, τελετή αρχικοποίησης δικτύου Δεκέμβριος 2025	Πρώιμη παραγωγή	Το εθνικό επίπεδο λειτουργεί ως επέκταση, όχι υποκατάστατο του EBSI· ισχυρή σύμπραξη δημόσιου–

			ιδιωτικού (Alastria, Περιφέρεια Μαδρίτης) [17]
Ιταλία	IT Wallet (2024)· N.12/2019 για ισοδυναμία blockchain timestamp και έξυπνες συμβάσεις [23]	Παραγωγικό	Η έγκαιρη νομοθέτηση επιταχύνει την υιοθέτηση· η Ιταλία προχώρησε ταχύτατα στο εθνικό πορτοφόλι
Γερμανία	eWpG (2021) για ηλεκτρονικούς τίτλους· IDunion (SSI) [22]	Παραγωγικό / πιλοτικό	Μοντέλο τροποποίησης υφιστάμενων νόμων αντί νέας νομοθεσίας — εξασφαλίζει νομική συνέχεια
Γαλλία	*Ordonnance* 2017 και νόμος PACTE 2019· συντονισμός του POTENTIAL [24]	Παραγωγικό	Η ηγεσία σε ευρωπαϊκούς πιλότους μεταφράζεται σε επιρροή στα πρότυπα
Ιρλανδία	Αξιολόγηση DLT για το κτηματολόγιο	Εγκαταλείφθηκε — υλοποιήθηκε με συμβατική βάση δεδομένων	Η τεκμηριωμένη απόρριψη είναι επιτυχία πολιτικής, όχι αποτυχία (βλ. γενικά [1], [2])

4.7 Προστασία δεδομένων: το πιο σημαντικό νέο δεδομένο

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) εξέδωσε τις Κατευθυντήριες Γραμμές 02/2025 για την επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω τεχνολογιών blockchain (αρχική έκδοση Απρίλιος 2025, έκδοση 2.0 τον Ιούλιο 2026) [5]. Τα βασικά μηνύματα:

- **Προηγείται το ερώτημα της αναγκαιότητας:** ο υπεύθυνος επεξεργασίας οφείλει να τεκμηριώσει γιατί απαιτείται blockchain και όχι απλούστερη λύση.
- **Προτίμηση ιδιωτικών/permissioned δικτύων** με σαφείς κανόνες ανάγνωσης και εγγραφής, ώστε να είναι δυνατή η **σαφής κατανομή ρόλων** υπευθύνου/εκτελούντος.
- **Η μόνιμη διαθεσιμότητα δεδομένων συναλλαγών συνιστά κίνδυνο** για τα δικαιώματα των υποκειμένων· τα δικαιώματα διαγραφής και διόρθωσης είναι τεχνικά δυσχερή.
- Τα διεθνή δίκτυα δημιουργούν διαβιβάσεις προς τρίτες χώρες — πρόσθετος λόγος αποφυγής δημόσιων δικτύων.
- **Τεχνικά και οργανωτικά μέτρα από το αρχικό στάδιο σχεδιασμού**, με Εκτίμηση Αντικτύπου (DPIA) πριν τον σχεδιασμό, όχι μετά.

Κρίσιμη τεχνική επισήμανση: ο κατακερματισμός (hashing) **δεν συνιστά αυτομάτως ανωνυμοποίηση**. Ένα hash προσωπικού δεδομένου με περιορισμένο χώρο τιμών (π.χ. ΑΦΜ ή ΑΜΚΑ) είναι επιδεκτικό επίθεσης εξαντλητικής αναζήτησης. Απαιτούνται **κλειδωμένοι κατακερματισμοί (keyed hash / HMAC) με διαχείριση και δυνατότητα καταστροφής του κλειδιού**, ή δεσμεύσεις με τυχαιοποίηση (salted commitments).

4.8 Ρυθμιστικό «πειραματικό» πλαίσιο και συσσωρευμένη γνώση

Το **European Blockchain Regulatory Sandbox** (2023–2026) ολοκλήρωσε τρεις κύκλους των 20 περιπτώσεων χρήσης (σύνολο 60), με την τελική έκθεση βέλτιστων πρακτικών να δημοσιεύεται στις **11.02.2026** [18], [19]. Καλύφθηκαν προστασία δεδομένων, κυβερνοασφάλεια, Πράξη για την Τεχνητή Νοημοσύνη και χρηματοπιστωτική ρύθμιση. Αποτελεί άμεσα αξιοποιήσιμη πηγή για την ελληνική δημόσια διοίκηση, χωρίς κόστος.

4.9 Νέες τάσεις με πρακτική σημασία

- Επαληθεύσιμα διαπιστευτήρια και αυτοκυρίαρχη ταυτότητα (Self-Sovereign Identity — SSI): η κυρίαρχη τάση· το DLT υποχωρεί σε ρόλο μητρώου εμπιστοσύνης και κατάστασης ανάκλησης, όχι φορέα δεδομένων.
- **Αποδείξεις μηδενικής γνώσης (zero-knowledge proofs — ZKP) και επιλεκτική αποκάλυψη (selective disclosure):** επιτρέπουν απόδειξη ιδιότητας (π.χ. «άνω των 18») χωρίς αποκάλυψη του δεδομένου.

Αποτελούν τον πλέον υποσχόμενο δρόμο συμβατότητας με GDPR, αλλά η ωριμότητα και η επίδοσή τους σε παραγωγικά περιβάλλοντα παραμένουν υπό αξιολόγηση.

- **Ενεργειακή αποδοτικότητα:** το ζήτημα έχει ουσιωδώς αποδυναμωθεί. Τα permissioned δίκτυα (Proof of Authority, όπως το EBSI) καταναλώνουν ενέργεια συγκρίσιμη με συμβατική υποδομή εξυπηρετητών· η ένσταση της ενεργειακής κατανάλωσης αφορά τα δίκτυα Proof of Work και **δεν αποτελεί πλέον επιχείρημα κατά της χρήσης DLT στον δημόσιο τομέα**.
- **Μετακβαντική κρυπτογραφία (post-quantum cryptography):** οι μακρόβιες αμετάβλητες εγγραφές είναι ευάλωτες σε μελλοντική κρυπταναλυτική πρόοδο. Κάθε σχεδιασμός πρέπει να προβλέπει **κρυπτογραφική ευελιξία (crypto-agility)**.
- Συνδυασμός με ΤΝ και νέφος: το DLT ως επίπεδο προέλευσης και ακεραιότητας δεδομένων (data provenance) για συστήματα ΤΝ αποτελεί αναδυόμενο, αλλά μη ώριμο πεδίο.

5. Πλαίσιο υιοθέτησης για την ελληνική δημόσια διοίκηση

5.1 Πέντε δεσμευτικές αρχιτεκτονικές αρχές

ΑΡΧΗ 1 — Permissioned/consortium κατά κανόνα. Απαγορεύεται η χρήση δημόσιων άδειων δικτύων (public permissionless) για δεδομένα δημόσιας διοίκησης. Εξαίρεση επιτρέπεται μόνο για **αγκύρωση αθροιστικών κρυπτογραφικών αποδείξεων χωρίς κανένα προσωπικό ή ευαίσθητο δεδομένο**, κατόπιν αιτιολογημένης έγκρισης.

ΑΡΧΗ 2 — Αυστηρός διαχωρισμός on-chain/off-chain. On-chain καταγράφονται **αποκλειστικά**: κρυπτογραφικές αποδείξεις (hashes/commitments), χρονοσφραγίδες, αναγνωριστικά κατάστασης και ανάκλησης, μη προσωπικά μεταδεδομένα. Κάθε άλλο δεδομένο παραμένει off-chain, στα υφιστάμενα μητρώα.

ΑΡΧΗ 3 — «EBSI-first». Πρώτη επιλογή είναι η ευρωπαϊκή υποδομή μέσω EUROPEUM-EDIC. Εθνικό δίκτυο DLT εξετάζεται **μόνο** εφόσον τεκμηριωθεί ότι η ευρωπαϊκή υποδομή δεν καλύπτει τη λειτουργική ανάγκη.

ΑΡΧΗ 4 — Το ΚΕΔ παραμένει το σημείο διαλειτουργικότητας. Το DLT **δεν παρακάμπτει** το Κέντρο Διαλειτουργικότητας. Οι υπηρεσίες επαλήθευσης εκτίθενται ως διαδικτυακές υπηρεσίες μέσω ΚΕΔ και καταναλώνονται από το gov.gr, ώστε οι φορείς να μη χρειάζεται να γνωρίζουν την υποκείμενη τεχνολογία.

ΑΡΧΗ 5 — Το DLT δεν είναι μητρώο αναφοράς. Σε περίπτωση απόκλισης, υπερισχύει πάντοτε το θεσμοθετημένο εθνικό μητρώο. Η αρχή αυτή πρέπει να αποτυπώνεται ρητά σε κάθε κανονιστική πράξη και σύμβαση, ώστε να αποφευχθεί νομική αβεβαιότητα.

5.2 Στοίβα αναφοράς (reference stack)

Επίπεδο	Επιλογή	Αιτιολόγηση
Δεδομένα	Εθνικά μητρώα (off-chain)	Παραμένουν αυθεντικά· καμία μετανάστευση δεδομένων
Ταυτότητα / παρουσίαση	gov.gr Wallet → EUDI Wallet	Υποχρέωση Καν. 2024/1183· υφιστάμενη υιοθέτηση από πολίτες
Διαπιστευτήρια	W3C Verifiable Credentials, SD-JWT VC, OpenID4VCI/VP	Ανοικτά πρότυπα· απαίτηση διασυνοριακής διαλειτουργικότητας
Καθολικό	EBSI (permissioned, Proof of Authority)	Θεσμική κατοχύρωση· πορεία προς εγκεκριμένο ηλεκτρονικό καθολικό
Διαλειτουργικότητα	ΚΕΔ / REST APIs	Υφιστάμενη εθνική υποδομή
Παρουσίαση	gov.gr	Ενιαία εμπειρία πολίτη

6. Κανονιστική συμμόρφωση

6.1 GDPR — επιχειρησιακοί κανόνες

Απαίτηση	Επιχειρησιακός κανόνας
Νομιμότητα και αναγκαιότητα	Τεκμηρίωση γιατί απαιτείται DLT — προηγείται κάθε άλλης ανάλυσης (EDPB 02/2025)
Ελαχιστοποίηση	Μηδέν προσωπικά δεδομένα on-chain· χρήση HMAC/salted commitments αντί απλού hash
Δικαίωμα διαγραφής	Υλοποίηση μέσω καταστροφής κλειδιού off-chain (crypto-shredding) και ανάκλησης· τεκμηρίωση των ορίων στη DPIA
Υπεύθυνος επεξεργασίας	Ρητός ορισμός ανά κόμβο· σε κοινοπραξία, συμφωνία από κοινού υπευθύνων (άρθρο 26 GDPR)
Διαβιβάσεις	Απαγόρευση κόμβων εκτός ΕΟΧ χωρίς προηγούμενη αξιολόγηση
Λογοδοσία	DPIA πριν τον σχεδιασμό, διαβούλευση με τον ΥΠΔ, ενημέρωση της ΑΠΔΠΧ όπου απαιτείται

6.2 eIDAS 2.0 και υπηρεσίες εμπιστοσύνης

- Ευθυγράμμιση των εκδιδόμενων διαπιστευτηρίων με τα πρότυπα QEAA/EAA και με τις εκτελεστικές πράξεις του Κανονισμού 2024/1183.
- Δημιουργία **εθνικού μητρώου αξιόπιστων εκδοτών (trust registry)** για δημόσια πιστοποιητικά, διασυνδεδεμένου με τα ευρωπαϊκά μητρώα.
- Μεσοπρόθεσμη αξιολόγηση της δυνατότητας η υπηρεσία αγκύρωσης να λειτουργήσει ως **εγκεκριμένο ηλεκτρονικό καθολικό**, υπό την εποπτεία της αρμόδιας εθνικής αρχής για τις υπηρεσίες εμπιστοσύνης (ΕΕΤΤ).

6.3 Εθνικό πλαίσιο

- **Ν.4961/2022** (ΦΕΚ Α΄146/27.07.2022), Κεφάλαιο Ε΄: αναγνώριση της τεχνολογίας κατανεμημένου καθολικού, ισχύς και απόδειξη των εγγραφών, ορισμός και έννομες συνέπειες των **έξυπνων συμβάσεων (smart contracts)**, σύναψη με εγκεκριμένη ηλεκτρονική υπογραφή ή σφραγίδα [20]. Το πλαίσιο υφίσταται· **το ζητούμενο δεν είναι νέος νόμος αλλά εκτελεστικές κανονιστικές πράξεις και πρότυπα**.
- **Ν.4727/2020** (Ψηφιακή Διακυβέρνηση): έγγραφα, ηλεκτρονικά αντίγραφα, διαλειτουργικότητα μέσω ΚΕΔ — το πλαίσιο εντός του οποίου εντάσσονται οι υπηρεσίες επαλήθευσης.
- **Ν.5193/2025**: προσαρμογή της εθνικής νομοθεσίας στον MiCA· αρμόδια αρχή η Επιτροπή Κεφαλαιαγοράς [15], [16]. (Η ακριβής παραπομπή σε ΦΕΚ πρέπει να επιβεβαιωθεί πριν από κάθε κανονιστική χρήση· η πληροφορία προέρχεται από δευτερογενείς νομικές πηγές.)
- **Ν.4412/2016** (δημόσιες συμβάσεις): πρόβλεψη ανοικτών προτύπων, δικαιωμάτων επί λογισμικού/δεδομένων και στρατηγικής εξόδου ως όρων της σύμβασης.

Κανονιστικό κενό που πρέπει να καλυφθεί. Δεν υφίστανται εκτελεστικές διατάξεις που να ορίζουν: (i) ποια δημόσια έγγραφα εκδίδονται ως επαληθεύσιμα διαπιστευτήρια, (ii) τη διαδικασία ανάκλησης, (iii) την ευθύνη σε περίπτωση σφάλματος επαλήθευσης, (iv) την αποδεικτική ισχύ της αγκύρωσης έναντι του αυθεντικού μητρώου. **Πρόταση: μία υπουργική απόφαση, όχι νέος νόμος.**

7. Διακυβέρνηση και λειτουργικά μοντέλα

7.1 Προτεινόμενο μοντέλο: συνεργατικό με κεντρική πολιτική εποπτεία

Ρόλος	Φορέας	Ευθύνη
Κάτοχος πολιτικής (policy owner)	Υπουργείο Ψηφιακής Διακυβέρνησης	Πύλη απόφασης, πρότυπα, χαρτοφυλάκιο έργων, εκπροσώπηση στο EUROPEUM-EDIC
Φορέας λειτουργίας κόμβου	Αρμόδια Γενική Γραμματεία του ΥΨηΔ, με τεχνική υποστήριξη ΕΔΥΤΕ	Λειτουργία εθνικού κόμβου EBSI, διαθεσιμότητα, ασφάλεια, ISO/IEC 27001
Εκδότες (issuers)	Θεματικοί φορείς (Υπ. Παιδείας/ΑΕΙ, ΑΑΔΕ, ΕΦΚΑ, ΟΤΑ)	Ορθότητα δεδομένων, έκδοση, ανάκληση
Επαληθευτές (verifiers)	Δημόσιοι και ιδιωτικοί αποδέκτες	Έλεγχος εγκυρότητας· καμία αποθήκευση πέραν του αναγκαίου
Προστασία δεδομένων	ΥΠΔ φορέων· εποπτεία ΑΠΔΠΧ	DPIA, δικαιώματα υποκειμένων
Υπηρεσίες εμπιστοσύνης	ΕΕΤΤ	Εποπτεία εγκεκριμένων υπηρεσιών

7.2 Vendor lock-in, ανοικτά πρότυπα και στρατηγική εξόδου

Ο κίνδυνος εγκλωβισμού σε προμηθευτή είναι **ο σοβαρότερος μακροπρόθεσμος κίνδυνος κόστους** και συνδέεται άμεσα με τον στόχο μείωσης δαπανών λειτουργίας και συντήρησης. Υποχρεωτικοί όροι σε κάθε σύμβαση:

1. **Ανοικτά πρότυπα υποχρεωτικά** (W3C VC, SD-JWT VC, OpenID4VCI/VP, ETSI PDL) — απόρριψη ιδιόκτητων μορφότυπων διαπιστευτηρίων.
2. **Πλήρη δικαιώματα του Δημοσίου** επί δεδομένων, σχημάτων, κλειδιών και τεκμηρίωσης.
3. **Τεκμηριωμένη στρατηγική εξόδου** πριν την παραγωγική λειτουργία: διαδικασία εξαγωγής, μορφότυπο, εκτιμώμενο κόστος και χρόνος μετάπτωσης.
4. Μεσεγγύηση πηγαίου κώδικα (source code escrow) για ιδιόκτητα στοιχεία.
5. **Ρήτρα λήξης (sunset clause):** αυτόματη επανεξέταση σε 24 μήνες· εάν δεν επιτευχθούν οι KPI, το έργο τερματίζεται και τα δεδομένα επιστρέφουν στο αυθεντικό μητρώο.

7.3 Λογοδοσία σε κατανεμημένο περιβάλλον

Η βασικότερη νομική ασάφεια των κοινοπρακτικών δικτύων είναι η κατανομή ευθύνης. Απαιτείται **συμφωνία κοινοπραξίας (consortium agreement)** που ορίζει ρητά: κριτήρια εισδοχής/αποβολής κόμβων, διαδικασία αναβαθμίσεων, ευθύνη σε περίπτωση σφάλματος ή διακοπής, μηχανισμό επίλυσης διαφορών και υποχρεώσεις διαθεσιμότητας (SLA).

8. Προτεραιοποιημένες περιπτώσεις χρήσης

Επιλογή βάσει τεσσάρων κριτηρίων: σκορ στο checklist αναγκαιότητας, ευρωπαϊκή ευθυγράμμιση, ρίσκο GDPR, και λόγος δημόσιας αξίας προς κόστος.

UC1 — Επαληθεύσιμα διαπιστευτήρια δημόσιων εγγράφων (Προτεραιότητα 1)

Τι: Έκδοση επιλεγμένων δημόσιων πιστοποιητικών ως επαληθεύσιμα διαπιστευτήρια στο gov.gr/EUDI Wallet, με μητρώο εμπιστοσύνης εκδοτών και μηχανισμό ανάκλησης αγκυρωμένο σε EBSI. **Σειρά υλοποίησης:** (1) ακαδημαϊκοί τίτλοι — υπάρχει ήδη εθνική εμπειρία σε ψηφιακά πιστοποιητικά σπουδών (υπηρεσία gov.gr από το 2022 [25]) και συμμετοχή της ΕΔΥΤΕ σε ευρωπαϊκά έργα EBSI (EBSI-VECTOR, EBSI-NE [26]), σε συνδυασμό

με ώριμο ευρωπαϊκό πλαίσιο· (2) πιστοποιητικά δημοτολογίου/οικογενειακής κατάστασης· (3) βεβαιώσεις ασφαλιστικής/φορολογικής ενημερότητας. **Δημόσια αξία:** κατάργηση δικαιολογητικών, διασυνοριακή αναγνώριση, στήριξη κινητικότητας. **Ρίσκο GDPR:** μεσαίο — αντιμετωπίζεται με επιλεκτική αποκάλυψη και μηδενικά δεδομένα on-chain.

UC2 — Αγκύρωση ακεραιότητας μητρώων και αρχείων καταγραφής (Προτεραιότητα 1)

Τι: Περιοδική καταχώριση κρυπτογραφικών αποδείξεων (Merkle roots) των αλλαγών κρίσιμων μητρώων και των αρχείων ελέγχου σε permissioned καθολικό — το μοντέλο της Εσθονίας. **Δημόσια αξία:** άμεση ανίχνευση μη εξουσιοδοτημένης αλλοίωσης, ενίσχυση ελεγκτικής ικανότητας, αποδεικτική αξία. **Ρίσκο GDPR:** χαμηλό — καμία επεξεργασία προσωπικών δεδομένων στο καθολικό (με ορθή σχεδίαση). **Γιατί πρώτο:** ο υψηλότερος λόγος αξίας/κόστους και το χαμηλότερο νομικό ρίσκο. **Δεν απαιτεί καμία αλλαγή στα υφιστάμενα συστήματα** πέραν προσθήκης εξαγωγής αποδείξεων.

UC3 — Ιχνηλασιμότητα και διαφάνεια δημοσίων συμβάσεων (Προτεραιότητα 2)

Τι: Αγκύρωση των κρίσιμων σταδίων της διαδικασίας (υποβολή, αποσφράγιση, αξιολόγηση, κατακύρωση) των υφιστάμενων συστημάτων (ΕΣΗΔΗΣ/ΚΗΜΔΗΣ), ώστε να δημιουργείται μη τροποποιήσιμο ίχνος ελέγχου. **Δημόσια αξία:** ενίσχυση λογοδοσίας και ελεγκτικού έργου· υποστήριξη ελέγχων ΕΑΔΗΣΥ και Ελεγκτικού Συνεδρίου. **Κρίσιμη επιφύλαξη:** η διεθνής εμπειρία (Εθνική Αρχή κατά της Διαφθοράς της Ιταλίας — ANAC) δείχνει ότι τα οφέλη προκύπτουν **μόνο** όταν συνοδεύονται από οργανωτικές και ελεγκτικές παρεμβάσεις. Η τεχνολογία δεν αντικαθιστά τον έλεγχο. **Δεν αντικαθίσταται το ΕΣΗΔΗΣ.**

UC4 — Διασυνοριακή ιχνηλασιμότητα εφοδιαστικής αλυσίδας και τελωνειακά δεδομένα (Προτεραιότητα 3)

Τι: Συμμετοχή στις ευρωπαϊκές περιπτώσεις χρήσης αξιόπιστης ανταλλαγής δεδομένων μεταξύ τελωνειακών και φορολογικών αρχών (ήδη περιλαμβάνεται στις αρχικές περιπτώσεις χρήσης του EBSI [7]) και σε ιχνηλασιμότητα φαρμάκων. **Γιατί τρίτο:** υψηλή εξάρτηση από ευρωπαϊκό χρονοδιάγραμμα και από τρίτους φορείς· μικρότερη εθνική δυνατότητα ελέγχου του αποτελέσματος.

Μη προτεινόμενα στον παρόντα ορίζοντα

- **Ηλεκτρονική ψηφοφορία σε blockchain:** σοβαρές, μη επιλυμένες ενστάσεις ως προς το απόρρητο και τον έλεγχο· διεθνώς μία μόνο περιορισμένη παραγωγική εφαρμογή. **Δεν συνιστάται.**
- **Συμβολαιοποίηση δημόσιων περιουσιακών στοιχείων:** σύνθετο ρυθμιστικό καθεστώς (MiCA και επόμενα), χωρίς σαφή δημόσια αξία στο παρόν στάδιο.
- **Πλήρη ιατρικά δεδομένα on-chain:** ασύμβατο με GDPR· η διαχείριση συγκατάθεσης μπορεί να εξεταστεί μόνο ως καταγραφή αποδείξεων πρόσβασης, σε μεταγενέστερο στάδιο.

Συγκριτικός πίνακας

Περίπτωση	Ενδεικτικό σκορ checklist	Ρίσκο GDPR	Ευρωπαϊκή ευθυγράμμιση	Ορίζοντας	Επισπεύδων
UC1 Διαπιστευτήρια	6–7	Μεσαίο	Πολύ υψηλή (eIDAS 2.0/EBSI)	12–30 μήνες	ΥΨηΔ + Υπ. Παιδείας
UC2 Αγκύρωση	5–6	Χαμηλό	Υψηλή (notarisation EBSI)	6–18 μήνες	ΥΨηΔ / ΕΔΥΤΕ
UC3 Προμήθειες	5–6	Χαμηλό–μεσαίο	Μεσαία	18–36 μήνες	ΥΨηΔ + ΕΑΔΗΣΥ
UC4 Εφοδιαστική/τελωνεία	5–6	Χαμηλό	Υψηλή	24–48 μήνες	ΑΑΔΕ + ΕΟΦ

Σημείωση: τα σκορ είναι ενδεικτικά και πρέπει να επιβεβαιωθούν από τον επισπεύδοντα φορέα κατά την επίσημη αξιολόγηση.

9. Οδικός χάρτης και δείκτες απόδοσης

9.1 Φάσεις

Φάση 0 — Θεσμική προετοιμασία (0–6 μήνες). Υπουργική απόφαση για την πύλη απόφασης· εκτελεστικές διατάξεις για τα επαληθεύσιμα διαπιστευτήρια· λειτουργία εθνικού κόμβου EBSI σε παραγωγικό επίπεδο· κεντρικό μητρώο έργων DLT της δημόσιας διοίκησης· εκπαίδευση στελεχών· ένταξη στους κύκλους του European Blockchain Sandbox.

Φάση 1 — Ελεγχόμενοι πιλότοι με κριτήρια εξόδου (6–18 μήνες). UC2 (αγκύρωση) σε δύο κρίσιμα μητρώα· UC1 σε ακαδημαϊκούς τίτλους. Κάθε πιλότος ξεκινά με προκαθορισμένα ποσοτικά κριτήρια επιτυχίας και ημερομηνία απόφασης συνέχισης/διακοπής.

Φάση 2 — Παραγωγή και ευθυγράμμιση με EUDI (18–36 μήνες). Παραγωγική λειτουργία UC1 και UC2 εντός του EUDI Wallet· εθνικό μητρώο εμπιστοσύνης· έναρξη UC3.

Φάση 3 — Εδραίωση (36+ μήνες). Αξιολόγηση καθεστώτος εγκεκριμένου ηλεκτρονικού καθολικού· επέκταση σε UC4· άνοιγμα σε ιδιωτικούς επαληθευτές.

9.2 Κριτήρια μετάβασης PoC → παραγωγή (σωρευτικά)

1. **Τεκμηριωμένη υπεροχή** έναντι της βέλτιστης μη-DLT εναλλακτικής, με πραγματικά λειτουργικά δεδομένα του πιλότου.
2. **Επιχειρησιακή ιδιοκτησία:** ορισμένος φορέας ευθύνης, προϋπολογισμός συντήρησης πενταετίας, διαδικασίες υποστήριξης.
3. **Νομική επάρκεια:** ολοκληρωμένη DPIA, κανονιστική πράξη, συμφωνία κοινοπραξίας.
4. **Ασφάλεια:** έλεγχος διείσδυσης, διαχείριση κλειδιών, ISO/IEC 27001 ή ισοδύναμο για τους κόμβους.
5. **Διαλειτουργικότητα:** έκθεση υπηρεσίας μέσω ΚΕΔ· συμμόρφωση με ευρωπαϊκά πρότυπα διαπιστευτηρίων.
6. **Αποδοχή χρηστών:** μετρημένη σε πραγματικές συνθήκες, όχι σε εργαστήριο.
7. **Στρατηγική εξόδου** τεκμηριωμένη και κοστολογημένη.

Ρητή αρχή: η μη συνέχιση ενός πιλότου που τεκμηριώνει ότι η τεχνολογία δεν προσφέρει επαρκές δημόσιο όφελος **δεν συνιστά αποτυχία**, αλλά ορθολογική χρήση δημόσιων πόρων.

9.3 Δείκτες απόδοσης

Κατηγορία	Δείκτης	Μέτρηση	Ενδεικτικός στόχος 24μήνου
Οικονομική	Κόστος ανά επαλήθευση	€ / επαλήθευση	−50% έναντι baseline
Οικονομική	Συνολικό κόστος ιδιοκτησίας (TCO) 5ετίας	€ (DLT vs εναλλακτική)	≤ εναλλακτικής
Λειτουργική	Καταργηθέντα δικαιολογητικά	Αριθμός / %	≥3 κατηγορίες εγγράφων
Λειτουργική	Χρόνος επαλήθευσης	Δευτερόλεπτα	<5 δευτ.
Λειτουργική	Επαληθεύσεις χωρίς επικοινωνία με τον εκδότη	% επί συνόλου	≥30% στις στοχευμένες διαδικασίες
Ποιότητας	Διαθεσιμότητα υπηρεσίας	% uptime	≥99,5%
Ποιότητας	Ικανοποίηση χρηστών	Κλίμακα 1–5	≥4,0
Εμπιστοσύνης	Ανιχνευθείσες αλλοιώσεις	Αριθμός / χρόνος ανίχνευσης	100% ανίχνευση
Εμπιστοσύνης	Κάλυψη ελέγχου	% κρίσιμων μητρώων υπό αγκύρωση	≥3 μητρώα
Ευρωπαϊκή	Διασυνοριακές επαληθεύσεις	Αριθμός/έτος	Μετρήσιμος όγκος >0

Μεθοδολογική προϋπόθεση: κάθε δείκτης απαιτεί **μέτρηση βάσης (baseline) πριν την έναρξη**. Χωρίς baseline, ο δείκτης δεν είναι αξιοποιήσιμος για απόφαση.

10. Κίνδυνοι, αντισταθμίσεις και μέτρα μετριασμού

#	Κίνδυνος	Πιθαν.	Επίπτ.	Μέτρο μετριασμού
K1	Υιοθέτηση χωρίς τεκμηριωμένη ανάγκη («λύση αναζητά πρόβλημα»)	Υψηλή	Υψηλή	Υποχρεωτική πύλη απόφασης· δέσμευση χρηματοδότησης σε ορόσημα
K2	Μη συμμόρφωση με GDPR λόγω δεδομένων on-chain ή αδύναμων hashes	Μεσαία	Πολύ υψηλή	Απόλυτος κανόνας μηδενικών προσωπικών δεδομένων· HMAC με διαχείριση κλειδιού· DPIA πριν τον σχεδιασμό
K3	Εγκλωβισμός σε προμηθευτή και διόγκωση κόστους συντήρησης	Υψηλή	Υψηλή	Ανοικτά πρότυπα· δικαιώματα Δημοσίου· escrow· στρατηγική εξόδου ως όρος σύμβασης
K4	Καθυστέρηση του ευρωπαϊκού χρονοδιαγράμματος (EUDI/EBSI)	Μεσαία	Μεσαία	Σχεδιασμός ώστε τα διαπιστευτήρια να λειτουργούν και εκτός πορτοφολιού· σταδιακή δέσμευση πόρων
K5	Έλλειψη δεξιοτήτων στη δημόσια διοίκηση	Υψηλή	Μεσαία	Στοχευμένη εκπαίδευση· εσωτερική τεχνική ομάδα· συμμετοχή σε ευρωπαϊκά έργα
K6	Αποτυχία διακυβέρνησης κοινοπραξίας (αδράνεια, διαφωνίες)	Μεσαία	Υψηλή	Συμφωνία κοινοπραξίας με μηχανισμό επίλυσης διαφορών και σαφείς κανόνες πλειοψηφίας
K7	Κρυπτογραφική απαξίωση (μετακβαντικός κίνδυνος) σε μακρόβιες εγγραφές	Χαμηλή–μεσαία	Υψηλή	Κρυπτογραφική ευελιξία· σχέδιο επανα-αγκύρωσης· περιορισμός χρόνου ζωής αποδείξεων
K8	Απώλεια/διαρροή κλειδιών εκδότη	Χαμηλή	Πολύ υψηλή	HSM· διαδικασίες εναλλαγής κλειδιών· άμεση ανάκληση· δοκιμές ανάκαμψης
K9	Ψευδής αίσθηση ασφάλειας (σωστά καταγεγραμμένο, λανθασμένο δεδομένο)	Μεσαία	Μεσαία	Έλεγχοι ποιότητας δεδομένων στην πηγή· σαφής επικοινωνία ότι το DLT εγγυάται ακεραιότητα, όχι ορθότητα
K10	Υπερβολικές δημόσιες προσδοκίες και επακόλουθη απαξίωση	Μεσαία	Μεσαία	Συγκρατημένη επικοινωνία· δημοσιοποίηση μετρήσεων και αρνητικών αποτελεσμάτων

Βασικές αντισταθμίσεις (trade-offs)

- **Αποκέντρωση ↔ έλεγχος:** περισσότεροι ανεξάρτητοι κόμβοι αυξάνουν την αξιοπιστία της εγγύησης, αλλά επιβραδύνουν τις αποφάσεις και αυξάνουν το κόστος συντονισμού.
- **Διαφάνεια ↔ ιδιωτικότητα:** κάθε πρόσθετη πληροφορία στο καθολικό αυξάνει την ελεγξιμότητα και ταυτοχρόνως τον κίνδυνο GDPR.
- **Αμεταβλητότητα ↔ διορθωσιμότητα:** η ίδια ιδιότητα που παρέχει αποδεικτική αξία εμποδίζει τη διόρθωση σφαλμάτων.
- **Ταχύτητα υλοποίησης ↔ ευρωπαϊκή ευθυγράμμιση:** εθνική λύση παραδίδεται ταχύτερα, αλλά ενδέχεται να απαιτήσει δαπανηρή αναπροσαρμογή.

Περιορισμοί του παρόντος κειμένου

Οι εκτιμήσεις κόστους/οφέλους δεν στηρίζονται σε πλήρη εθνική κοστολόγηση, η οποία δεν είναι διαθέσιμη. Οι στόχοι KPI είναι **ενδεικτικοί** και πρέπει να βαθμονομηθούν μετά τη μέτρηση βάσης. Η ετοιμότητα των

κρατών μελών για το EUDI Wallet βασίζεται σε κλαδικές αναλύσεις και όχι σε επίσημη αξιολόγηση. Τέλος, η αρίθμηση των άρθρων του eIDAS 2.0 για τα ηλεκτρονικά καθολικά πρέπει να επαληθευθεί στο ενοποιημένο κείμενο.

11. Συστάσεις πολιτικής

Βραχυπρόθεσμα (0–6 μήνες)

Σ1. Θεσμοθέτηση της πύλης απόφασης. Έκδοση υπουργικής απόφασης/εγκυκλίου που καθιστά υποχρεωτική, πριν από κάθε δέσμευση πόρων για DLT, τη συμπλήρωση του checklist (κατώφλι ≥6/7) και τη συγκριτική τεκμηρίωση έναντι τριών μη-DLT εναλλακτικών. *Αρμόδιος:* ΥΨηΔ.

Σ2. Κανόνας μηδενικών προσωπικών δεδομένων on-chain. Έκδοση δεσμευτικής τεχνικής οδηγίας, ευθυγραμμισμένης με τις Κατευθυντήριες Γραμμές EDPB 02/2025, με ρητή απαίτηση HMAC/salted commitments αντί απλού hash και DPIA πριν τον σχεδιασμό. *Αρμόδιος:* ΥΨηΔ σε συνεργασία με ΑΠΔΠΧ.

Σ3. Παραγωγικός εθνικός κόμβος EBSI και ενεργός ρόλος στο EUROPEUM-EDIC. Διασφάλιση λειτουργίας κόμβου παραγωγικού επιπέδου με πιστοποίηση ISO/IEC 27001 και στελέχωση της εθνικής εκπροσώπησης. *Αρμόδιος:* ΥΨηΔ / ΕΔΥΤΕ.

Σ4. Κεντρικό μητρώο έργων DLT. Καταγραφή όλων των υφιστάμενων και σχεδιαζόμενων έργων της δημόσιας διοίκησης, με κατάσταση, κόστος και αποτελέσματα — ώστε να αποφευχθεί ο κατακερματισμός και οι επικαλύψεις. *Αρμόδιος:* ΥΨηΔ.

Σ5. Εκτελεστικές διατάξεις για τα επαληθεύσιμα διαπιστευτήρια. Υπουργική απόφαση βάσει του Ν.4961/2022 και του Ν.4727/2020 που ορίζει κατάλογο εγγράφων, διαδικασία έκδοσης και ανάκλησης, ευθύνη και αποδεικτική ισχύ. **Δεν απαιτείται νέος νόμος.** *Αρμόδιος:* ΥΨηΔ.

Μεσοπρόθεσμα (6–24 μήνες)

Σ6. Υλοποίηση UC2 (αγκύρωση ακεραιότητας) σε δύο κρίσιμα μητρώα. Έργο χαμηλού ρίσκου και υψηλής απόδοσης, κατά το εσθονικό μοντέλο, χωρίς μετάπτωση δεδομένων. *Αρμόδιος:* ΥΨηΔ / ΕΔΥΤΕ + φορείς μητρώων.

Σ7. Υλοποίηση UC1 σε ακαδημαϊκούς τίτλους, με πορεία προς παραγωγή. Αξιοποίηση της εθνικής υπηρεσίας ψηφιακών πτυχίων μέσω gov.gr [25], της συμμετοχής της ΕΔΥΤΕ σε έργα EBSI [26] και της διαλειτουργικότητας gov.gr Wallet – Κύπρος. *Αρμόδιος:* Υπ. Παιδείας + ΥΨηΔ + ΑΕΙ.

Σ8. Εθνικό μητρώο αξιόπιστων εκδοτών (trust registry). Δημιουργία και διασύνδεση με τα ευρωπαϊκά μητρώα, ως προϋπόθεση λειτουργίας του EUDI Wallet. *Αρμόδιος:* ΥΨηΔ, με εποπτεία ΕΕΤΤ.

Σ9. Υποχρεωτικοί συμβατικοί όροι κατά του εγκλωβισμού. Ενσωμάτωση προτύπων όρων (ανοικτά πρότυπα, δικαιώματα Δημοσίου, escrow, στρατηγική εξόδου, sunset clause 24 μηνών) σε όλα τα τεύχη διακήρυξης έργων DLT. *Αρμόδιος:* ΥΨηΔ + ΕΑΔΗΣΥ.

Σ10. Πρόγραμμα ανάπτυξης δεξιοτήτων. Στοχευμένη εκπαίδευση στελεχών σε επαληθεύσιμα διαπιστευτήρια, eIDAS 2.0 και προστασία δεδομένων· σύσταση μικρής μόνιμης τεχνικής ομάδας εντός του Δημοσίου· αξιοποίηση των εκθέσεων του European Blockchain Sandbox. *Αρμόδιος:* ΥΨηΔ + ΕΚΔΔΑ.

Μακροπρόθεσμα (24–48 μήνες)

Σ11. Αξιολόγηση καθεστώτος εγκεκριμένου ηλεκτρονικού καθολικού. Εξέταση της δυνατότητας η εθνική υπηρεσία αγκύρωσης να λάβει καθεστώς εγκεκριμένης υπηρεσίας εμπιστοσύνης κατά τον Κανονισμό 2024/1183, ώστε οι αποδείξεις να αποκτήσουν πλήρη νομική ισχύ σε όλη την ΕΕ. *Αρμόδιος:* ΥΨηΔ + ΕΕΤΤ.

Σ12. Επέκταση σε UC3 και UC4 και άνοιγμα σε ιδιωτικούς επαληθευτές. Μόνο εφόσον τα UC1 και UC2 έχουν επιτύχει τους δείκτες τους. Παράλληλα, θέσπιση διετούς κύκλου δημόσιας αναφοράς αποτελεσμάτων, **συμπεριλαμβανομένων των αρνητικών**, ώστε η εθνική πολιτική να παραμένει τεκμηριωμένη. *Αρμόδιος:* ΥΨηΔ.

12. Πηγές / References

[1] European Commission, Joint Research Centre — *Blockchain for Digital Government* / European landscape on the use of blockchain technology by the public sector. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC115049/blockchain_for_digital_government_online.pdf

[2] OECD (2020), *The Uncertain Promise of Blockchain for Government*, OECD Working Papers on Public Governance No. 43. https://www.oecd.org/en/publications/the-uncertain-promise-of-blockchain-for-government_d031cd67-en.html · Συνοδευτικό σχόλιο OPSI: https://oecd-opsi.org/blog/uncertain-promise-blockchain/

[3] Κανονισμός (ΕΕ) 2024/1183 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για το ευρωπαϊκό πλαίσιο ψηφιακής ταυτότητας (eIDAS 2.0), ΕΕ L, 30.04.2024. Μόνιμος σύνδεσμος (ELI): https://eur-lex.europa.eu/eli/reg/2024/1183/oj · Πλήρες κείμενο: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401183

[4] European Commission, *The European Digital Identity Regulation* (EU Digital Identity Wallet). https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation

[5] European Data Protection Board, *Guidelines 02/2025 on processing of personal data through blockchain technologies* (v2.0). https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202502_blockchain_v2_en.pdf · Ανακοίνωση υιοθέτησης: https://www.edpb.europa.eu/news/news/2025/edpb-adopts-guidelines-processing-personal-data-through-blockchains-and-ready_en

[6] ETSI GR PDL 017 V1.1.1 (2024-07), *Permissioned Distributed Ledger (PDL)*. https://www.etsi.org/deliver/etsi_gr/PDL/001_099/017/01.01.01_60/gr_PDL017v010101p.pdf · Βλ. επίσης EBSI-VECTOR, *Role of EBSI within eIDAS 2.0*: https://www.ebsi-vector.eu/wp-content/uploads/2025/02/Role-of-EBSI-within-eIDAS.pdf

[7] European Commission, *European blockchain services infrastructure (EBSI)*. https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

[8] EBSI / EUROPEUM-EDIC, *About us* και ενημερώσεις δικτύου. https://ec.europa.eu/digital-building-blocks/sites/spaces/EBSI/pages/474513483/About+us · https://ebsi.eu/about-us

[9] European Commission, *What are the Large Scale Pilot Projects*. https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487808/What+are+the+Large+Scale+Pilot+Projects · LSP-EWC: https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/920064565/LSP-EWC

[10] Biometric Update, *EUDI Wallet needs common standards applied rigorously, POTENTIAL pilot finds* (Νοέμβριος 2025). https://www.biometricupdate.com/202511/eudi-wallet-needs-common-standards-applied-rigorously-potential-pilot-finds

[11] Biometric Update, *EU Commission doubtful all member states will be able to launch EUDI wallets this year*. https://www.biometricupdate.com/202604/eu-commission-doubtful-all-member-states-will-be-able-launch-eudi-wallets-this-year

[12] European Commission, *EU Digital Identity Wallet Pilot implementation*. https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

[13] Δημόσιες ανακοινώσεις για τη διαλειτουργικότητα gov.gr Wallet – «Ψηφιακός Πολίτης» (Κύπρος), Μάιος 2025. https://wallet.gov.gr/ · Ενδεικτική κάλυψη: https://gr.euronews.com/2025/05/19/kypros-kai-ellada-mazi-sti-nea-psifiaki-epoxi

[14] European Securities and Markets Authority (ESMA), *Markets in Crypto-Assets Regulation (MiCA)*. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

[15] Επιτροπή Κεφαλαιαγοράς, Απόφαση 8/1059/30.07.2025 — διαδικασία αδειοδότησης παρόχων υπηρεσιών κρυπτοστοιχείων. http://www.hcmc.gr/aweb/files/Cryptos/files/Eng/Submitting_an_application_for%20_CASP_teliko_en.pdf

[16] ΕΥ Ελλάδος, *MiCA Regulation — Authorisation Procedure for Crypto-Asset Service Providers*. https://www.ey.com/en_gr/technical/tax/tax-alerts/mica-regulation-authorisation-procedure-for-crypto-asset-service-providers

[17] Alastria, *ISBE — Blockchain Services Infrastructure of Spain / ISBE Begins Operations*. https://alastria.io/en/proyectos/isbe-blockchain-services-infrastructure-of-spain/ · https://alastria.io/en/isbe-begins-operations-spain-blockchain-infrastructure/

[18] European Commission, *The European Blockchain Sandbox releases the third cohort best practices report* (11.02.2026). https://digital-strategy.ec.europa.eu/en/news/european-blockchain-sandbox-releases-third-cohort-best-practices-report

[19] EU Blockchain Observatory and Forum, *European Blockchain Sandbox* — εκθέσεις βέλτιστων πρακτικών. https://blockchain-observatory.ec.europa.eu/european-blockchain-sandbox_en

[20] Ν.4961/2022 «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις» (ΦΕΚ Α΄146/27.07.2022), Κεφάλαιο Ε΄ (ΤΚΚ και έξυπνες συμβάσεις). Επίσημο κείμενο: Εθνικό Τυπογραφείο, https://www.et.gr · Ενοποιημένο κείμενο: https://www.taxheaven.gr/law/4961/2022 · Ανάλυση: https://www.ey.com/el_gr/technical/tax/tax-alerts/l-4961-2022-the-greek-legal-framework-on-emerging-technologies

[21] e-Estonia, «KSI Blockchain». https://e-estonia.com/solutions/cyber-security/ksi-blockchain/

[22] Gesetz über elektronische Wertpapiere (eWpG), 3 Ιουνίου 2021. https://www.gesetze-im-internet.de/ewpg/

[23] Legge 11 febbraio 2019, n. 12, άρθρο 8-ter (τεχνολογίες βασισμένες σε κατανεμημένα μητρώα και έξυπνες συμβάσεις). https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=0&art.flagTipoArticolo=0&art.codiceRedazionale=19A00934&art.idArticolo=8&art.idSottoArticolo=3&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=2019-02-12&art.progressivo=0

[24] Ordonnance n° 2017-1674 du 8 décembre 2017· κύρωση με το άρθρο 206 του Loi n° 2019-486 (PACTE). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000036171908

[25] Υπουργείο Ψηφιακής Διακυβέρνησης, υπηρεσία «Πιστοποιητικά Σπουδών» μέσω gov.gr. https://ptyxia.gov.gr/universities/ · Ανακοίνωση: https://www.mindigital.gr/archives/7817

[26] ΕΔΥΤΕ (GRNET), έργα EBSI-VECTOR και EBSI-NE. https://grnet.gr/en/business-directory/ebsi-verifiable-credentials-trusted-organisations-registries-ebsi-vector/ · https://grnet.gr/en/business-directory/ebsi-ne-en/

Όλοι οι σύνδεσμοι ελέγχθηκαν κατά τη σύνταξη του παρόντος (Ιούλιος 2026). Όπου η πληροφορία προέρχεται από δευτερογενή πηγή, αυτό δηλώνεται ρητά στο κείμενο.

Παράρτημα Α — Γλωσσάριο όρων (EN ↔ EL)

Αγγλικός όρος	Ελληνική απόδοση	Σύντομη επεξήγηση
Distributed Ledger Technology (DLT)	Τεχνολογία κατανεμημένου καθολικού	Κοινό, αντιγραμμένο σε πολλούς κόμβους αρχείο εγγραφών
Permissioned / consortium blockchain	Blockchain ελεγχόμενης πρόσβασης / συνεργατικό	Συμμετοχή μόνο εξουσιοδοτημένων φορέων
Smart contract	Έξυπνη σύμβαση / συμβόλαιο	Κώδικας που εκτελείται αυτόματα υπό προϋποθέσεις
Verifiable Credential (VC)	Επαληθεύσιμο διαπιστευτήριο	Ψηφιακά υπογεγραμμένη βεβαίωση, επαληθεύσιμη χωρίς τον εκδότη
Self-Sovereign Identity (SSI)	Αυτοκυρίαρχη ταυτότητα	Μοντέλο όπου ο χρήστης ελέγχει τα διαπιστευτήριά του
EU Digital Identity Wallet (EUDI Wallet)	Ευρωπαϊκό Πορτοφόλι Ψηφιακής Ταυτότητας	Εφαρμογή αποθήκευσης/παρουσίασης διαπιστευτηρίων
Trust registry	Μητρώο εμπιστοσύνης	Κατάλογος αναγνωρισμένων εκδοτών
Electronic ledger / qualified electronic ledger	Ηλεκτρονικό καθολικό / εγκεκριμένο ηλεκτρονικό καθολικό	Νέα υπηρεσία εμπιστοσύνης κατά τον Καν. 2024/1183
Notarisation / anchoring	Συμβολαιογραφική αγκύρωση / αγκύρωση	Καταχώριση κρυπτογραφικής απόδειξης δεδομένου
Hash	Κρυπτογραφικό αποτύπωμα	Σταθερού μήκους αποτύπωμα δεδομένου
HMAC / keyed hash	Κλειδωμένο κρυπτογραφικό αποτύπωμα	Hash με μυστικό κλειδί — αποτρέπει εξαντλητική αναζήτηση
Zero-Knowledge Proof (ZKP)	Απόδειξη μηδενικής γνώσης	Απόδειξη ισχυρισμού χωρίς αποκάλυψη του δεδομένου
Selective disclosure	Επιλεκτική αποκάλυψη	Παρουσίαση μόνο των αναγκαίων πεδίων
On-chain / off-chain	Εντός / εκτός καθολικού	Πού αποθηκεύεται το δεδομένο
Proof of Authority (PoA)	Απόδειξη εξουσιοδότησης	Μηχανισμός συναίνεσης με γνωστούς επικυρωτές
Audit trail	Ίχνος ελέγχου	Καταγραφή ενεργειών για ελεγκτικούς σκοπούς
Immutability	Αμεταβλητότητα	Αδυναμία μη ανιχνεύσιμης τροποποίησης
Vendor lock-in	Εγκλωβισμός σε προμηθευτή	Εξάρτηση που δυσχεραίνει τη μετάβαση
DPIA	Εκτίμηση Αντικτύπου Προστασίας Δεδομένων	Υποχρεωτική αξιολόγηση κινδύνων κατά GDPR
Crypto-agility	Κρυπτογραφική ευελιξία	Δυνατότητα αντικατάστασης αλγορίθμων

Παράρτημα Β — Υπόδειγμα Πύλης Απόφασης (Decision Gate)

Μέρος 1 — Checklist αναγκαιότητας (βλ. Ενότητα 3.2, σκορ 0–7). Καταγράφεται σκορ και τεκμηρίωση ανά κριτήριο. *Κατώφλι προώθησης:* ≥6.

Μέρος 2 — Συγκριτική τεκμηρίωση. Για καθεμία από τις εναλλακτικές (εγκεκριμένη ηλεκτρονική σφραγίδα· εγκεκριμένη χρονοσφραγίδα· διασύνδεση μέσω ΚΕΔ): τι δεν καλύπτει και γιατί, με ποσοτικά στοιχεία.

Μέρος 3 — Συμμόρφωση. Κατηγορίες δεδομένων on-chain (πρέπει να είναι μηδενικές ως προς προσωπικά δεδομένα)· κατάσταση DPIA· νομική βάση· ορισμός υπευθύνου επεξεργασίας.

Μέρος 4 — Βιωσιμότητα. Φορέας ιδιοκτησίας· TCO 5ετίας· στρατηγική εξόδου· ημερομηνία επανεξέτασης (sunset).

Μέρος 5 — Μετρήσεις. Baseline ανά KPI· στόχοι· ημερομηνία απόφασης συνέχισης/διακοπής.

Έγκριση: επισπεύδων φορέας → ΥΠΔ → ΥΨηΔ (πολιτική έγκριση).