ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΜΗΧΑΝΙΚΩΝ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΜΕΣΩ ΕΡΕΥΝΑΣ

(ΠΜΣ-ΜΕ.Δ.Μ.Ο.Δ.Ε.)

ΤΙΤΛΟΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Πολιτικές Διαλειτουργικότητας, Ηλεκτρονική Ταυτοποίηση και υπηρεσίες εμπιστοσύνης: Το Ευρωπαϊκό Δίκτυο eIDAS: Τεχνολογική Δομή, Υπηρεσίες και Πολιτικές.

ΕΙΣΗΓΗΤΗΣ: Στασής Αντώνης

ΕΠΙΒΛΕΠΩΝ: Πέτρος Καβάσαλης

Χίος, Δεκέμβριος 2020

UNIVERSITY OF THE AEGEAN

Πίνακας περιεχομένων

Πίνακας περιεχομένων 2
Πίνακά σχημάτων 4
Πρόλογος 5
Ευχαριστίες 6
Περίληψη 7
Executive Summary 11
1 Η διαλειτουργικότητα ως θεμέλιος λίθος για την παροχή ψηφιακών υπηρεσιών 14
1.1 Έννοια της Διαλειτουργικότητας 15
1.2 Τύποι Διαλειτουργικότητας 16
1.3 Διαλειτουργικότητα, Οικονομία και Διοίκηση 19
1.4 Παραδείγματα αποτελεσματικότητας 19
1.5 Αρχές του EIF 2017 20
1.6 Στρατηγική υλοποίησης της διαλειτουργικότητας 22
2 Παροχή Ολοκληρωμένων Διαλειτουργικών Υπηρεσιών 22
2.1 Απαιτήσεις προγραμματισμού διαλειτουργικών ψηφιακών υπηρεσιών 23
2.1.1 Επίδραση του θεσμικού πλαισίου 23
2.1.2 Επίδραση Οργάνωσης και Λειτουργίας Δημόσιας Διοίκησης 24
2.1.3 Στρατηγικές στην υλοποίηση ολοκληρωμένων δημοσίων υπηρεσιών. 25
2.1.4 Οργανωσιακά ζητήματα διαλειτουργικότητας 26
2.2 Ευρωπαϊκή Αρχιτεκτονική Διαλειτουργικότητας 27
2.3 Αναγκαίες Ικανότητες για διαλειτουργικές υπηρεσίες 29
2.4 Περιορισμοί στο σχεδιασμό διαλειτουργικών υπηρεσιών 29
3 Βελτίωση διαδικασιών προγραμματισμού για διαλειτουργικές δημόσιες υπηρεσίες 30
3.1 Διαμόρφωση στρατηγικών στόχων 31
3.2 Στρατηγικός σχεδιασμός 31
3.3 Ανάπτυξη επιχειρησιακού σεναρίου 32
3.4 Διαχείριση έργου – Διαχείριση πόρων 33
3.5 Αξιολόγηση επιδόσεων 33
3.6 Καταγραφή της διαλειτουργικής υπηρεσίας 33
4 Κανονισμός eIDAS – Εκτελεστικές αποφάσεις – Διαλειτουργικότητας σε ζητήματα ηλεκτρονικής ταυτοποίησης 34
4.1 Εκτελεστική απόφαση (ΕΕ) 2015/296 της 24ης Φεβρουαρίου 2015 για τη θέσπιση διαδικαστικών λεπτομερειών της συνεργασίας μεταξύ των κρατών μελών σχετικά με την ηλεκτρονική ταυτοποίηση (European Commission, 2015a), ... 37

4.2 Εκτελεστικός κανονισμός (ΕΕ) 2015/1501 της 8ης Σεπτεμβρίου 2015 για το πλαίσιο διαλειτουργικότητας (eIDAS Node) (European Commission, 2015b),..... 37

4.3 Εκτελεστικός κανονισμός (ΕΕ) 2015/1502 της 8ης Σεπτεμβρίου 2015 σχετικά με τη θέσπιση ελάχιστων τεχνικών προδιαγραφών και διαδικασιών για τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης (Χαμηλό, Βασικό, Υψηλό) (European Commission, 2015c)..... 38

4.4 Εκτελεστική απόφαση (ΕΕ) 2015/1984 της 3ης Νοεμβρίου 2015 για τον καθορισμό των περιστάσεων, των μορφοτύπων και των διαδικασιών κοινοποίησης συστημάτων ταυτοποίησης (European Commission, 2015d) 39

4.5 Εκτελεστικός κανονισμός (ΕΕ) 2015/806 της 22ας Μαΐου 2015 για τη θέσπιση προδιαγραφών σχετικά με τη μορφή του ενωσιακού σήματος εμπιστοσύνης για τις εγκεκριμένες υπηρεσίες εμπιστοσύνης (European Commission, 2015e) 40

4.6 Εκτελεστική απόφαση (ΕΕ) 2015/1505 της 8ης Σεπτεμβρίου 2015 περί καθορισμού των τεχνικών προδιαγραφών και των μορφότυπων των καταλόγων εμπίστευσης (European Commission, 2015f)..... 40

4.7 Εκτελεστική απόφαση (ΕΕ) 2015/1506 της 8ης Σεπτεμβρίου 2015 για τον καθορισμό προδιαγραφών σχετικά με τους μορφότυπους των προηγμένων ηλεκτρονικών υπογραφών και των προηγμένων σφραγίδων που πρέπει να αναγνωρίζονται από φορείς του δημόσιου τομέα (XAdES, CAdES, PAdES) (European Commission, 2015g) 41

4.8 Εκτελεστική απόφαση (ΕΕ) 2016/650 της of 25ης Απριλίου 2016 σχετικά με τον καθορισμό προτύπων για την αξιολόγηση της ασφάλειας των εγκεκριμένων διατάξεων δημιουργίας υπογραφής και σφραγίδας (ISO/IEC 15408, ISO/IEC 18045, EN 419 211) (European Commission, 2016a) 41

5 Ο κόμβος eIDAS ως η κύρια υποδομή διαλειτουργικότητας για διασυνοριακό έλεγχο ταυτότητας (European Commission, 2016b) 42

6 Δομή Διακυβέρνησης του κανονισμού eIDAS σε σχέση με το πρόγραμμα CEF... 44

7 Τομείς Πολιτικής που επηρεάζονται από τον κανονισμό eIDAS 47

8 Ζητήματα έρευνας για τη Διαλειτουργικότητας και τον κανονισμό eIDAS..... 49

8.1 Επικαιροποίηση του Ελληνικού Πλαισίου Διαλειτουργικότητας 50

8.2 Ψηφιακές Δεξιότητες για δημόσιες διαλειτουργικές υπηρεσίες. 53

9 Σχεδιασμός ενός ηλεκτρονικού συστήματος διαχείρισης ακαδημαϊκής ταυτότητας για την κινητικότητα των φοιτητών χρησιμοποιώντας τις τεχνολογίες eIDAS eID και Self-Sovereign Identity 54

9.1 Πολιτικές για έναν Ευρωπαϊκό Εκπαιδευτικό χώρο και τη ψηφιακή ταυτότητα..... 57

9.2 Προσέγγιση για «Διασυνδεδεμένη Ακαδημαϊκή Ταυτότητα» με χρήση τεχνολογιών διαχείρισης ταυτότητας από το χρήστη (Self-Sovereign-Identity -SSI) 61

9.2.1.1 Βασικές Έννοιες 65

9.2.1.2 Βασικοί ρόλοι και εδραίωση εμπιστοσύνης (Trust Anchoring)..... 66

9.2.1.3 Βασικές Λειτουργίες 67

9.2.1.4 Παράδειγμα 69
9.2.2 Θεσμικά και επιχειρησιακά προαπαιτούμενα 69
10 Επίσημες ταυτότητες μίας χρήσεως (Disposable Yet Official Identities -DYOI) για το σχεδιασμό συστημάτων προστασίας της ιδιωτικότητας 70
10.1 Η επαλήθευση ψηφιακού εγγράφου και ο έλεγχος πρόσβασης βάσει διαπιστευτηρίων σε εξωτερικούς και εσωτερικούς χώρους την εποχή του COVID-19 72
10.1.1 Ταυτότητα μίας χρήσης 75
10.1.2 Παρουσίαση VC 77
10.1.3 Bluetooth χαμηλής Ενέργειας (Bluetooth Low Energy -BLE) 79
11 Συμπεράσματα 81
12 Δημοσιεύσεις από την Ερευνητική εργασία 85
13 Βιβλιογραφία – Αναφορές 88

Πίνακά σχημάτων

Σχήμα 1: Ενωσιακό σήμα για εγκεκριμένες υπηρεσίες εμπιστοσύνης 40
Σχήμα 2:Κόμβος eIDAS (European Commission, 2015h) 43
Σχήμα 3: Το οικοσύστημα του eIDAS 45
Σχήμα 4: Δομή Διακυβέρνησης του eIDAS 46
Σχήμα 5: Σχέση eIDAS - Προγράμματος CEF 47
Σχήμα 6: Προτεινόμενη υψηλού επιπέδου αρχιτεκτονική 64
Σχήμα 7: Παράγωγα επαληθεύσιμα διαπιστευτήρια 81

Πρόλογος

Η συγκεκριμένη διπλωματική εργασία έχει ως στόχο να αναδείξει τη σημασία της διαλειτουργικότητας ως πολιτική και στρατηγική επιλογή στην υποστήριξη σύγχρονων ψηφιακών υπηρεσιών, διασφαλίζοντας την επαναχρησιμοποίηση υποδομών, αρχιτεκτονικών, εφαρμογών λογισμικού και επιχειρησιακών διαδικασιών για την κάλυψη αναγκών σε διαφορετικούς τομείς της Δημόσιας Διοίκησης και της Οικονομίας.

Σημαντική προϋπόθεση για την επίτευξη διαλειτουργικότητας αλλά και την ανάπτυξη ψηφιακών υπηρεσιών είναι η δημιουργία κλίματος εμπιστοσύνης και η ύπαρξη μηχανισμών για τη διασφάλιση της ιδιωτικότητας των συναλλασσόμενων.

Ο κανονισμός eIDAS ρυθμίζει το πλαίσιο των υπηρεσιών εμπιστοσύνης, δηλαδή των υπηρεσιών που εξασφαλίζουν το κλίμα εμπιστοσύνης που αναφέρθηκε παραπάνω. Ο κανονισμός eIDAS λειτούργησε καταλυτικά για την ανάπτυξη νέων υπηρεσιών που απαιτούν ένα σύγχρονο πλαίσιο ασφάλειας.

Χαρακτηριστικό παράδειγμα είναι οι διασυνοριακές διαλειτουργικές υπηρεσίες που απαιτούνται για την κινητικότητα των φοιτητών και του ακαδημαϊκού προσωπικού μέσα από την υλοποίηση του προγράμματος Erasmus μεταξύ Ακαδημαϊκών Ιδρυμάτων σε ευρωπαϊκό επίπεδο.

Επίσης η ανάπτυξη της ανέπαφης οικονομίας με αφορμή την πανδημία του Covid-19, έδωσε ώθηση σε νέες λύσεις βασισμένες σε νέες τεχνολογίες όπως θα αναλυθεί στις επόμενες ενότητες της εργασίας.

Τέλος εξαιτίας της σπουδαιότητας του ανθρώπινου δυναμικού στην υλοποίηση όλων αυτών, το ζήτημα των ψηφιακών δεξιοτήτων για την ανάπτυξη ψηφιακών διαλειτουργικών υπηρεσιών καθίσταται σημαντικό κομμάτι του όλου οικοσυστήματος και υπό αυτή έννοια προσεγγίζεται στο πλαίσιο της εργασίας.

Ευχαριστίες

Ιδιαίτερη αναφορά θα πρέπει να γίνει στη τριμελή επιτροπή μου και ιδίως τον επιβλέποντα κ. Πέτρο Καβάσαλη που μου έδωσε την ευκαιρία να ασχοληθώ μες αυτά τα θέματα αιχμής και μου παρείχε καθοδήγηση και στήριξη, φέρνοντας με σε επαφή με πολλούς επιστήμονες και έργα που συνδιαμορφώνουν αυτό τον καινοτομικό χώρο.

Περίληψη

Μία σύγχρονη οικονομία που επιδιώκει να είναι ανταγωνιστική, προσπαθεί να επιτύχει τα μέγιστα δυνατά αποτελέσματα με χρήση των ελάχιστών κατά το δυνατό πόρων. Η δημιουργία κοινών, επαναχρησιμοποιήσιμων υποδομών, υπηρεσιών και διαδικασιών αποτελεί σύγχρονο στρατηγικό στόχο, διότι μία επένδυση σε μία υποδομή που αναπτύσσεται μία φορά, αξιοποιείται σε πολλαπλούς διαφορετικούς επιχειρησιακούς τομείς. Στο πλαίσιο αυτό η διαλειτουργικότητα αποτελεί θεμέλιο λίθο μίας σύγχρονης οικονομίας αλλά και βασικό συστατικό στοιχείο για την αποδοτική και αποτελεσματική λειτουργία της δημόσιας διοίκησης.

Οι πρόσφατες εξελίξεις για τη Δημόσια Υγεία, κυρίως εξαιτίας του Covid-19 προώθησαν έντονα την ανέπαφη οικονομία, δηλαδή την ψηφιοποίηση των υπηρεσιών και των καθημερινών λειτουργιών προκειμένου να είναι εφικτή ή τήρηση των κανόνων κοινωνικής αποστασιοποίησης που επέβαλαν οι συνθήκες της πανδημίας.

Η δημιουργία διαλειτουργικών υπηρεσιών που αξιοποιούν υφιστάμενες υποδομές, υπηρεσίες και ανταλλάσσουν δεδομένα χωρίς να απαιτείται φυσική αλληλεπίδραση μεταξύ των εμπλεκομένων είναι προαπαιτούμενο για την ψηφιοποίηση της Οικονομίας και της Δημόσιας Διοίκησης.

Στο πλαίσιο της εργασίας προτείνεται μία διαδικασία για το στρατηγικό και επιχειρησιακό προγραμματισμό διαλειτουργικών δημοσίων υπηρεσιών αναγνωρίζοντας τις υφιστάμενες αδυναμίες της Ελληνικής Δημόσιας Διοίκησης και των ενεργειών που πρέπει να πραγματοποιηθούν προκειμένου να είναι εφικτή η επιτυχής υλοποίηση αυτών. Βασικά στάδια αυτής της διαδικασίας είναι:

1) Η διαμόρφωση στρατηγικών στόχων
2) Ο στρατηγικός σχεδιασμός
3) Η ανάπτυξη του επιχειρησιακού σεναρίου, με την αναγνώριση και συμπερίληψη ήδη υφιστάμενων διαλειτουργικών υπηρεσιών
4) Η διαχείριση έργου και διαχείριση πόρων
5) Η αξιολόγηση επιδόσεων

6) Η καταγραφή διαλειτουργικής υπηρεσίας σε μητρώο διαλειτουργικών υπηρεσιών

Σε ότι αφορά στην Ελλάδα η υπουργική απόφαση που περιγράφει το Ελληνικό Εθνικό Πλαίσιο Διαλειτουργικότητας (Greek e-GIF) εκδόθηκε το 2012 με τον τίτλο «Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης» (ΦΕΚ 1301/Β'/12-04-2012). Έκτοτε δεν έχει γίνει επικαιροποίηση του πλαισίου με αποτέλεσμα σημαντικές εξελίξεις όπως π.χ. αυτή του κανονισμού eIDAS να μην έχουν ληφθεί υπόψη. Στο πλαίσιο της παρούσας εργασίας προτάθηκαν τα σημεία βελτίωση και επικαιροποίησης, πολλά από τα οποία ενσωματώθηκαν στον νόμο για την Ψηφιακή Διακυβέρνηση (Ν.4727/2020).

Για το ζήτημα των απαραίτητων ψηφιακών δεξιοτήτων αναλύθηκαν τα αντίστοιχα προφίλ τόσο για τους πολίτες όσο και τους επαγγελματίες που αναπτύχθηκαν κατά την τελευταία δεκαετία στην Ευρώπη αναδεικνύοντας τις ψηφιακές δεξιότητες που είναι απαραίτητες για τη διαλειτουργικότητα.

Το ψηφιακό διαλειτουργικό περιβάλλον οφείλει να δημιουργεί ένα κλίμα εμπιστοσύνης, που εδραιώνεται θεσμικά και ουσιαστικά σε αξιόπιστες πηγές που ελέγχονται από δημόσιες αρχές οι οποίες διαφυλάττουν το δημόσιο συμφέρον. Το 2014 εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, ο κανονισμός για τις ηλεκτρονικές υπηρεσίες ταυτοποίησης και εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά. Μια σημαντική πτυχή του κανονισμού eIDAS είναι η αμοιβαία αναγνώριση των εθνικών μέσων ηλεκτρονικής ταυτοποίησης από τα άλλα κράτη μέλη.

Ο σκοπός του κανονισμού eIDAS είναι: i) να διασφαλίσει ότι τα φυσικά πρόσωπα και οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τα εθνικά ηλεκτρονικά αναγνωριστικά τους (π.χ. ηλεκτρονικές ταυτότητες) για να αυθεντικοποιηθούν σε δημόσιες υπηρεσίες που προσφέρονται από άλλες χώρες της ΕΕ και ii) να αυξήσουν την εμπιστοσύνη μεταξύ των ενδιαφερομένων μερών στην εσωτερική αγορά.

Η εφαρμογή του κανονισμού eIDAS είναι ένα ζήτημα που επηρεάζει: α) σε επίπεδο πολιτικής διαφορετικές τομεακές πολιτικές όπως π.χ. για τον ακαδημαϊκό χώρο, την υγεία, τη φορολογία, τα τελωνεία και οριζόντιες

πολιτικές όπως για τη προστασία δεδομένων και τις πολιτοκεντρικές υπηρεσίες, β) σε επιχειρησιακό επίπεδο εμπλέκει διάφορους οργανισμούς όπως την Ευρωπαϊκή Επιτροπή, τον ENISA , το ETSI , τις αρμόδιες αρχές από τα κράτη μέλη, τους μηχανισμούς χρηματοδότησης, όπως το πρόγραμμα CEF Telecom, το πρόγραμμα Horizon και γενικά τα διαρθρωτικά, επενδυτικά ταμεία και το ταμείο ανάπτυξης, γ) σε τεχνικό επίπεδο σαφείς προδιαγραφές, διαφορετικές υλοποιήσεις αναφοράς, δομικά στοιχεία λογισμικού, πλατφόρμες δοκιμών και ελέγχων κ.λπ.

Μια μεγάλη πρόκληση για τον κανονισμό eIDAS είναι να δημιουργηθεί ένα μοντέλο διασφάλισης της ιδιωτικής ζωής που θα σέβεται τις διατάξεις του GDPR, δηλαδή να παρέχει ένα ασφαλές, αξιόπιστο περιβάλλον πληροφοριών που θα εμφανίζει μόνο τα προσωπικά δεδομένα που κάθε φορά απαιτούνται για την παροχή μιας συγκεκριμένης ψηφιακής υπηρεσίας.

Σε αυτή την κατεύθυνση μία πολλά υποσχόμενη τεχνολογία είναι αυτή των Self-Sovereign Identities (SSI) και ειδικότερα των επαληθεύσιμών διαπιστευτηρίων (Verifiable Credentials-VC). Προκειμένου να αυξηθεί το επίπεδο διασφάλισης ποιότητας των πληροφοριών που παρέχονται και να καλυφθεί θεσμικά η τεχνολογία των SSI, προτείνεται στο πλαίσιο της παρούσας εργασίας η διασύνδεση με τα στοιχεία της ηλεκτρονικής ταυτότητα που παρέχονται από τον μηχανισμό του κανονισμού eIDAS.

Στο πλαίσιο της εργασίας αναλύεται ως μελέτη περίπτωσης ο τρόπος εφαρμογής των ανωτέρω στην πολιτική για τον Ευρωπαϊκό Χώρο Εκπαίδευσης και ειδικότερα για την κινητικότητα φοιτητών και ακαδημαϊκού προσωπικού στο πλαίσιο του προγράμματος ERASMUS.

Επιπρόσθετα με αφορμή την απαίτηση ελέγχου διαφόρων εγγράφων που έχουν θεσμοθετηθεί στο πλαίσιο της πανδημίας του Covid-19, προτείνεται βασισμένος στις ίδιες αρχές, ο σχεδιασμός ενός συστήματος διαλειτουργικών υπηρεσιών που προσφέρουν τη δυνατότητα: α) να διαχειρίζεται ο χρήστης άμεσα και να επαληθεύει ένα ευρύ φάσμα πιθανών ψηφιακών εγγράφων, όπως βεβαιώσεις, πιστοποιητικά κλπ. και β) να ελέγχεται η πρόσβαση σε ένα εσωτερικό ή εξωτερικό χώρο, βάσει διαπιστευτηρίων, ειδικά για τις

περιπτώσεις που πραγματοποιείται με παρέμβαση ανθρώπου με χρήση έξυπνων συσκευών ή συσκευών Internet of Things (IoT).

Η προτεινόμενη προσέγγισή επιπρόσθετα αξιοποιεί τις δυνατότητες των τεχνολογιών για ταυτότητες μίας χρήσης (Disposal Identities) για να επιτρέψει την επαλήθευση ενός ψηφιακού εγγράφου και τον έλεγχο πρόσβασης. Προς αυτήν την κατεύθυνση, εισάγεται η έννοια των «παραγώγων» (derivative) επαληθεύσιμων διαπιστευτηρίων (VC) που ισχύουν για περιορισμένο χρόνο και χώρο. Στο ίδιο πλαίσιο προτείνεται και ένα υποσύστημα για το μετασχηματισμό των VC σε μορφή που ένας άνθρωπός ή μία συσκευή να μπορεί να τα ερμηνεύσει και επαληθεύσει.

Με αυτές τις υπηρεσίες αναδεικνύεται η επίδραση του κανονισμού eIDAS στην υλοποίηση πολιτικών για τη δημόσια υγεία, που όμως μπορεί να επεκταθεί σε μία ευρύτερη γκάμα εφαρμογών, όπως αυτές για σημεία ελέγχου αεροδρομίων, σιδηροδρομικών σταθμών, ελέγχων επιβίβασης και πρόσβασης σε φυσικούς χώρους, εφαρμόζοντας του κανόνες κοινωνικής αποστασιοποίησης μεταξύ του ελεγκτή και του υποκειμένου του ελέγχου.

Executive Summary

A modern economy that aims to be competitive, strives to achieve the maximum possible results, using the least possible resources. Toward this direction, a strategic goal is to create common reusable, infrastructure, services and processes, so that the investment of an infrastructure that is developed once, can be utilized in as many as possible different business areas. In this context, interoperability is the cornerstone of a modern economy but also a key component for the efficient and effective operation of public administration. Recent challenges in Public Health, mainly due to Covid-19, have strongly promoted the contactless economy, i.e. the digitization of services and day-to-day operations in order to comply with the rules of social distance imposed by the pandemic measures for the reduction of the pace that Covid-19 is spread.

The creation of interoperable services that utilize existing infrastructure, services and exchange data without requiring physical interaction between stakeholders, is a prerequisite for the digitization of the Economy and Public Administration. In the context of this thesis, a process for the strategic and operational planning of interoperable public services is proposed, recognizing the existing weaknesses of the Greek Public Administration and the actions that must be taken so that the successful implementation to be possible. Important steps of this process are:

1) Formulation of strategic goals
2) Strategic planning
3) Development of the business scenario, with the recognition and inclusion of already existing interoperable services
4) Project management and resource management
5) Performance evaluation
6) The registration of interoperable service in a interoperability service registry

As far as it concerns Greece, the ministerial decision describing the Greek National Interoperability Framework (Greek e-GIF) was issued in 2012 with

the translated title "Greek Framework for the provision of e-Government Services" (Government Gazette 1301/B'/12-04-2012). Afterwards, the framework has not been updated resulting in significant evolutions and provisions such as the ones in the eIDAS Regulation have not been taken into account. In the context of the present thesis, areas for improvement and updating were proposed, many of which were incorporated in the new law on Digital Governance (Law 4727/2020).

The issue of advanced digital skills and the respective profiles for both citizens and professionals has been developed in Europe during the last decade. In this thesis these profiles were analyzed, highlighting the advanced digital skills necessary for interoperability.

The digital interoperable environment must create an trust realm, which is institutionally and substantially based in reliable sources controlled by public authorities that safeguard the public interest. In 2014, the regulation on electronic identification and trust services for electronic transactions in the internal market was approved by the European Parliament and the Council as eIDAS regulation. An important aspect of the eIDAS Regulation is the mutual recognition of national means of electronic identification by other Member States. The purpose of the eIDAS Regulation is: i) to ensure that individuals and businesses can use their national electronic identifiers and credentials (e.g. electronic IDs) to authenticate themselves in public services offered by other EU countries; and ii) increase trust between stakeholders in the internal market.

The implementation of the eIDAS regulation is an issue that affects: a) at policy level different sectoral policies such as academia, health, taxation, customs and horizontal policies, such as data protection and citizen centric services; (b) at operational level various bodies such as ENISA, ETSI, responsible authorities from Member States, funding mechanisms, such as the CEF Telecom program, the Horizon program and in general the Structural, Investment and Development Funds; c) at technical level, clear specifications, different reference implementations, software components, and testing platforms, etc.

A major challenge for eIDAS regulation is to create a model that ensures the privacy and respects the provisions of GDPR, i.e., to provide a secure, reliable information environment that displays only the personal data required at a specific timeframe for the provision of a digital service.

In this regard, a very promising technology is Self-Sovereign Identities (SSI) and particularly the verifiable credentials (Verifiable Credentials-VC). The interconnection of SSI technology with the electronic identity data provided by the eIDAS regulation has been proposed in this thesis in order to increase the level of quality assurance of the information provided.

The way of applying of the above-mentioned proposals in the European Education Area for the mobility of students and academic staff in the context of the ERASMUS program is analyzed as a case study in this thesis.

Additionally, as a solution to the need of checking various documents that have been institutionalized for Covid-19 pandemic, the design of an interoperable system based on the above-mentioned principles has been proposed. This design can provide the user capabilities such as: a) to manage directly and verify a wide range possible digital documents, such as certificates and b) control access to an indoor or outdoor area, based on credentials, especially in cases involving human intervention using smart devices or Internet of Things (IoT) devices.

The proposed approach further leverages the capabilities of Disposal Identities technologies to enable the verification of a digital document and access control. In this direction, the concept of "derivative" verifiable credentials (VC) that are valid for a limited time and space area is introduced. In the same context, a subsystem is proposed for the transformation of VCs in a form that humans or a device can interpret and verify.

These services highlight the impact of the eIDAS regulation on the implementation of public health policies and can be extended to a wider range of applications, such as airport, train station, boarding and on-site access control, applying the rules of social distance between the officials and the subjects of control.

1 Η διαλειτουργικότητα ως θεμέλιος λίθος για την παροχή ψηφιακών υπηρεσιών

Κατά τη διάρκεια της διάσκεψης για την ηλεκτρονική διακυβέρνηση που πραγματοποιήθηκε στο Κομό της Ιταλίας στις 7-8 Ιουλίου 2003 υπό την Ιταλική Προεδρία, οι αρμόδιοι Υπουργοί αναγνώρισαν ότι η διαλειτουργικότητα αποτελεί βασική προϋπόθεση για την ανάπτυξη πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης και ότι το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας αποτελεί απαραίτητη προϋπόθεση[1].

Το 2004 δημοσιεύτηκε η πρώτη έκδοση του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας - EIF (European Commission, 2004). Το 2009, δημιουργήθηκε το Παρατηρητήριο για την Παρακολούθηση της υλοποίησης των Εθνικών Πλαισίων Διαλειτουργικότητας (NIFO- National Interoperability Framework Obserbatory[2,3]) και την αξιολόγηση της συμβατότητας τους με το EIF. Το 2010, η ΕΕ σε ανακοίνωση της δημοσίευσε το πρώτο επίσημο ευρωπαϊκό πλαίσιο διαλειτουργικότητας (European Commission, 2010) και την ευρωπαϊκή στρατηγική διαλειτουργικότητας (European Commission, 2010b), καθορίζοντας τις προτεραιότητες για τη διαλειτουργικότητα. Το 2014, η ΕΕ πρότεινε την πρώτη ευρωπαϊκή αρχιτεκτονική αναφοράς για τη διαλειτουργικότητα[4] και ένα μοντέλο αξιολόγησης ηλεκτρονικών υπηρεσιών σε ότι αφορά την ωριμότητα της διαλειτουργικότητας για να διευκολύνει την εφαρμογή του EIF[5,6]. Το EIF αποτέλεσε υποχρεωτική απαίτηση σε όλες τις δράσεις που χρηματοδοτήθηκαν από τα ευρωπαϊκά διαρθρωτικά ταμεία (European Commission, 2018), ή από άλλα προγράμματα όπως το πρόγραμμα

[1] EIF - European Interoperability Framework for pan-European eGovernment services: https://wayback.archive-it.org/12090/20200212132355/https://ec.europa.eu/idabc/en/document/2319/5644.html

[2] National Interoperability Frameworks Observatory – NIFO,IDABC, 2009 https://wayback.archive-it.org/12090/20200212134102/https://ec.europa.eu/idabc/en/document/7796.html

[3] The National Interoperability Framework Observatory, ISA[2], 2018 https://ec.europa.eu/isa2/solutions/nifo_en

[4]European Interoperability Reference Architecture and Cartography tool https://ec.europa.eu/isa2/solutions/eira_en

[5] Interoperability Maturity Assessment Model https://joinup.ec.europa.eu/collection/imaps-interoperability-maturity-assessment-public-service/solution/imaps

[6]Interoperability Maturity Assessment of a Public Service https://ec.europa.eu/isa2/solutions/imaps_en

Connecting Europe Facility (CEF) [7]. Το EIF αναθεωρήθηκε το 2017 (European Commission, 2017) λαμβάνοντας υπόψη την εμπειρία εφαρμογής της τελευταίας δεκαετίας. Επιπλέον, τα κράτη μέλη της Ευρωπαϊκής Ένωσης εφάρμοσαν πολλές εθνικές δράσεις συμπληρωματικές αυτών που γίνονται σε ευρωπαϊκό επίπεδο. Όλα αυτά τα χρόνια, το κύριο ευρωπαϊκό πρόγραμμα που επικεντρώθηκε στη διαλειτουργικότητα ήταν το Interoperable Solutions for European Public Administrations programme (ISA) και, από το 2016, ο διάδοχός του ISA[2]. Σήμερα τα ζητήματα διαλειτουργικότητας εντάσσονται στο πρόγραμμα Digital Europe Programme[8] της νέας προγραμματικής περιόδου 2021-2027.

Παράλληλα, πολλές τομεακές πρωτοβουλίες προώθησαν τη διαλειτουργικότητα. Οι πιο σημαντικές από αυτές εφαρμόστηκαν σε τομείς όπως: Τελωνεία και Φορολογία, Επιχειρηματική Κινητικότητα, Γεωχωρική Πληροφορία, Δημόσιες Προμήθειες, Ηλεκτρονική Υγεία, Εκπαιδευτικό και Πολιτιστικό Περιεχόμενο, Επαναχρησιμοποίηση πληροφοριών Δημόσιου Τομέα.

Σε ότι αφορά στην Ελλάδα, η θεσμοθέτηση του Ελληνικού Πλαισίου Διαλειτουργικότητας πραγματοποιήθηκε με την υπουργική απόφαση για την κύρωση του Ελληνικού Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης[9]. Η πρακτική εφαρμογή του εν λόγω πλαισίου μέχρι σήμερα δεν έγινε με συστηματικό τρόπο. Παράλληλα υπάρχουν πολλές άλλες νομοθετικές ρυθμίσεις που προβλέπουν τη διαλειτουργικότητα σε συγκεκριμένες εφαρμογές και υπηρεσίες του Δημόσιου τομέα (European Commission 2018b).

1.1 Έννοια της Διαλειτουργικότητας

Η έννοια της διαλειτουργικότητας πρεσβεύει και υποστηρίζει την επαναχρησιμοποίηση διαδικασιών και υπηρεσιών, την ανταλλαγή δεδομένων,

[7] CEF Telecom Work Programme 2018: New Building Blocks and Grant Funding https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/02/07/CEF+Telecom+Work+Programme+2018%3A+New+Building+Blocks+and+Grant+Funding

[8] Digital Europe Programme, https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme

[9] Κύρωση Πλαισίου Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης ΥΑΠ/Φ.40.4/1/989 (ΦΕΚ 1301/Β'/12-04-2012)

το διαμοιρασμό πληροφορίας και γνώσης. Σε ότι αφορά στην ηλεκτρονική διακυβέρνηση τα ανωτέρω πρέπει να υποστηρίζονται από τα πληροφοριακά συστήματα των οργανισμών και των φορέων. Κατά καιρούς έχουν δοθεί πολλοί ορισμοί για τη διαλειτουργικότητα σε ακαδημαϊκό, και διοικητικό επίπεδο. Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας του 2017 ορίζει ως διαλειτουργικότητα:

«την ικανότητα των οργανισμών να αλληλοεπιδρούν προς αμοιβαία επωφελείς στόχους, με την ανταλλαγή πληροφοριών και γνώσεων μεταξύ αυτών των οργανισμών, μέσω των επιχειρησιακών διαδικασιών που υποστηρίζουν, μέσω της ανταλλαγής δεδομένων μεταξύ των συστημάτων Τεχνολογίας Πληροφορικής και Επικοινωνιών.»

1.2 Τύποι Διαλειτουργικότητας

Οι τύποι της διαλειτουργικότητας που έχουν αναδειχθεί σε διοικητικό επίπεδο ως σημαντικοί για την επίτευξη της, είναι οι κάτωθι:

1) **Τεχνική Διαλειτουργικότητα:** Είναι ο πρώτος τύπος διαλειτουργικότητας που εμφανίστηκε στο χώρο της ηλεκτρονικής διακυβέρνησης προκειμένου να αντιμετωπίσει την ανάγκη της ασφαλούς ανταλλαγής δεδομένων σε τεχνικό επίπεδο μεταξύ πληροφοριακών συστημάτων διαφορετικών χωρών και φορέων. Η τεχνική διαλειτουργικότητα επικεντρώνεται σε τεχνικά πρότυπα επικοινωνίας διαφορετικών συστημάτων π.χ. γλώσσα html, αρχεία pdf, jpg, mp3, mp4 κλπ. Η τεχνική διαλειτουργικότητα συνήθως έχει να κάνει με τους κατασκευαστές υλικού και συστημικού λογισμικού κλπ.

Πολύ γρήγορα διαπιστώθηκε ότι η τεχνική διαλειτουργικότητα δεν επαρκεί από μόνη της για την επίτευξη διαλειτουργικότητας. Με την έκδοση του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας το 2004[1] προστέθηκαν άλλοι δύο τύποι:

2) **Σημασιολογική διαλειτουργικότητα:** Έχει να κάνει με τη διακινούμενη πληροφορία και τον τρόπο που αυτή ορίζεται προκειμένου να μπορεί να ερμηνευθεί με τον ίδιο τρόπο μεταξύ διαφορετικών πληροφοριακών

συστημάτων. Η σημασιολογική διαλειτουργικότητα απαιτεί σαφή ορισμό εννοιών και δομών δεδομένων που προϋποθέτει επιχειρησιακή συμφωνία μεταξύ διαφορετικών οργανισμών προκειμένου να αναπαριστούν μία πληροφορία με τον ίδιο τρόπο. Σε ευρωπαϊκό επίπεδο είναι εξαιρετικά σημαντική η πρωτοβουλία του Semantic Interoperability Community (SEMIC[10]) με σημαντικά αποτελέσματα σε βασικά λεξιλόγια (Core Vocabularies) σε διάφορους τομείς. Για παράδειγμα από τα σημαντικότερα προβλήματα της Ελληνικής Δημόσιας Διοίκησης σε ότι αφορά τη διασταύρωση στοιχείων μεταξύ διαφορετικών φορέων είναι το γεγονός ότι δεν υπάρχει σημασιολογική διαλειτουργικότητα π.χ. ένα ακίνητο είναι με διαφορετικό τρόπο είναι ορισμένο στο Εθνικό Κτηματολόγιο (εμπράγματα δικαιώματα), στις Πολεοδομίες (σχετική άδεια δόμησης), στην ΑΑΔΕ (έντυπα Ε9), στη ΔΕΗ (λογαριασμοί ρεύματος) , στους δήμους (ΤΑΠ) ή στις τράπεζες (υποθήκες, δάνεια).

3) **Οργανωσιακή διαλειτουργικότητα:** Αφορά κυρίως στην ευθυγράμμιση των επιχειρησιακών διαδικασιών, των υποχρεώσεων και των προσδοκιών ενός οργανισμού με τις διαδικασίες του άλλου οργανισμού, προκειμένου οι ανταλλασσόμενες πληροφορίες, διαδικασίες και δεδομένα να μπορούν να αξιοποιηθούν. Ενδεικτικό παράδειγμα οργανωσιακής διαλειτουργικότητας είναι π.χ. η επικοινωνία με ηλεκτρονικό ταχυδρομείο μεταξύ δύο φορέων που όμως οι υπάλληλοι του ενός, δεν παρακολουθούν συστηματικά το ηλεκτρονικό τους ταχυδρομείο και δεν απαντούν στα εισερχόμενα μηνύματα, δεδομένου ότι δεν υποχρεούνται από τις εσωτερικές τους διαδικασίες.

Παρόλο που τα τελευταία χρόνια έχουν γίνει βήματα στους ανωτέρω τύπους διαλειτουργικότητας, το αναθεωρημένο EIF εισήγαγε το 2008 ακόμη δύο τύπους που αναλύονται παρακάτω:

[10] Semantic Interoperability Community, https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic

4) **Θεσμική διαλειτουργικότητα:** Συχνά τίθεται το ερώτημα κατά πόσο η ανταλλασσόμενη πληροφορία μπορεί να έχει έννομα αποτελέσματα. Η Θεσμική διαλειτουργικότητα αφορά στη διασφάλιση της συνεργασίας μεταξύ των οργανισμών που λειτουργούν βάσει διαφορετικών νομικών πλαισίων, πολιτικών και στρατηγικών. Αυτό απαιτεί να μην εμποδίζονται οι ολοκληρωμένες ευρωπαϊκές δημόσιες υπηρεσίες εντός και μεταξύ των κρατών μελών και να υπάρχουν σαφείς συμφωνίες για τον τρόπο αντιμετώπισης των διαφορών στη νομοθεσία σε διασυνοριακές υπηρεσίες, συμπεριλαμβανομένης της δυνατότητας θέσπισης νέας νομοθεσίας. Χαρακτηριστικό παράδειγμα είναι έγγραφα που δεν έχουν νομική ισχύ όταν ψηφιοποιηθούν π.χ. εγγυητικές επιστολές. Άλλο παράδειγμα για διασυνοριακές υπηρεσίες είναι η έκδοση άδειας ασκήσεως επαγγέλματος σε κάποιον που έχει ακαδημαϊκό τίτλο σπουδών από άλλη χώρα και απαιτείται έκδοση ισοτιμίας του τίτλου για να μπορεί να έχει έννομη συνέπεια ο τίτλος στη χώρα υποδοχής.
5) **Διοίκηση της διαλειτουργικότητας:** Η διαλειτουργικότητα εξελίσσεται διότι εξελίσσονται τα πρότυπα, οι τεχνολογίες, οι προδιαγραφές, οι ηλεκτρονικές υπηρεσίες, οι εμπλεκόμενοι φορείς, οι στρατηγικοί τους στόχοι. Για το λόγο αυτό απαιτείται ένας μηχανισμός διοίκησης που να επικαιροποιεί τα πλαίσια διαλειτουργικότητας, τις συμφωνίες μεταξύ των συνεργαζόμενων οργανισμών, τις πολιτικές τους ρόλους και τις αρμοδιότητες. Χαρακτηριστικό παράδειγμα είναι η οδηγία inspire που αφορά σε διαλειτουργικότητα Γεωχωρικών δεδομένων.

Η αναθεωρημένη τρίτη έκδοση του EIF έθεσε ένα νέο τύπο διαλειτουργικότητας που αφορά στη Διοίκηση ολοκληρωμένων δημοσίων υπηρεσιών.

6) **Διοίκηση ολοκληρωμένων δημοσίων υπηρεσιών:** Κύριο μέλημα είναι η δημιουργία συμφωνιών διαλειτουργικότητας μεταξύ των εμπλεκομένων φορέων που να θέτουν τις υποχρεώσεις αλλά και τα δικαιώματα των εμπλεκόμενων φορέων. Στο παρελθόν στην Ελλάδα καταργήθηκαν υπηρεσίες όπως βεβαιώσεις του ΙΚΑ από τα ΚΕΠ,

αυτόματες αναρτήσεις φορέων στο πρόγραμμα Διαύγεια, διότι ένας εκ των συνεργαζόμενων φορέων μονομερώς άλλαξες προδιαγραφές ή/και αναβάθμισε τα συστήματα του χωρίς αισθάνεται την υποχρέωση συνεννόησης με τους φορείς που διαλειτουργούσε.

1.3 Διαλειτουργικότητα, Οικονομία και Διοίκηση

Ένας από τους βασικούς στόχους του νέου δημοσίου Μάνατζμεντ είναι η αρχή της αποτελεσματικότητας και οικονομικότητας, δηλαδή της επίτευξης αποτελεσμάτων με το μικρότερο δυνατό κόστος. Οι εν λόγω αρχές έχουν υιοθετηθεί από το σύνολο της ελεύθερης οικονομίας και σε επίπεδο Ψηφιακής Διακυβέρνησης. Αποτέλεσμα αυτών των αρχών είναι, να δίνεται προτεραιότητα στην επαναχρησιμοποίηση υφιστάμενων δεδομένων, λειτουργιών και υπηρεσιών από τους διάφορους οργανισμούς κατά τη δημιουργία νέων ψηφιακών υπηρεσιών. Είναι σαφές ότι η διαλειτουργικότητα συνεισφέρει στην αποτελεσματικότητα της οικονομίας και της δημόσιας διοίκησης αφού οι νέες παρεχόμενες ηλεκτρονικές υπηρεσίες δεν απαιτείται να δημιουργήσουν εκ νέου συστήματα και εφαρμογές που ήδη υπάρχουν. Επίσης δεν απαιτούνται διαδικασίες για τη συντήρηση των δεδομένων που λαμβάνονται με τεχνικές διαλειτουργικότητας, διότι ότι ο αρμόδιος φορέας που τα παρέχει, αναλαμβάνει πλήρως τη συγκεκριμένη ευθύνη και εφαρμόζει τις σχετικές διαδικασίες.

Η διαλειτουργικότητα διασφαλίζει συνεπή δεδομένα μεταξύ των φορέων, μειώνει τα κόστη παροχής μίας υπηρεσίας, διαμοιράζεται το κόστος λειτουργίας των υποδομών και των εφαρμογών που έχει αναπτύξει ένας φορέας.

Όλα αυτά συνεισφέρουν στην αποτελεσματικότητα των προσφερόμενων υπηρεσιών, αλλά και στη διευκόλυνση των πολιτών.

1.4 Παραδείγματα αποτελεσματικότητας

Χαρακτηριστικό παράδειγμα είναι ο νέος κανονισμός για την Ενιαία Ψηφιακή Θύρα (Ευρωπαϊκή Ένωση, 2018)[11] όπου βασίζεται σε μητρώα των κρατών

[11] Regulation on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012, COM(2017) 256 final

μελών χωρίς να δημιουργεί αντίγραφα των δεδομένων αυτών. Στο παρελθόν στην Ελλάδα είχαμε πολλές περιπτώσεις δράσεων που είχαν γίνει στο παρελθόν από πολλούς φορείς για την επικαιροποίηση στοιχείων π.χ. απογραφή ασφαλισμένων για απόδοση ΑΜΚΑ ή υποχρέωση ενημέρωσης των φορολογικών αρχών για αλλαγή ταυτότητας. Σήμερα γίνεται η αντίστοιχη εργασία με άντληση στοιχείων από την αστυνομία ή το δημοτολόγιο.

Άλλο παράδειγμα στο τομέα της υγείας είναι η μεταφορά του συνοπτικού φακέλου υγείας ενός ασθενή από νοσοκομείο σε νοσοκομείο, καθιστώντας τη συνέχιση της θεραπείας σε διαφορετικά νοσοκομεία ευκολότερη χωρίς να απαιτούνται διαδικασίες όπως π.χ. λήψη ιστορικού. Η προσπάθεια για εμπλουτισμό των στοιχείων Ιατρικού φακέλου με όχημα την ηλεκτρονική συνταγογράφηση από την ΗΔΙΚΑ Α.Ε. (Ηλεκτρονικής Διακυβέρνησης Κοινωνικής Ασφάλισης) έχει αυτό το σκοπό.

Παραδείγματα αποτελεσματικών υπηρεσιών με χρήση τεχνικών διαλειτουργικότητας είναι:

1) Κανονισμός eIDAS για την αυθεντικοποίηση των χρηστών (που αποτελεί και το βασικό θέμα διαλειτουργικότητας της παρούσας εργασίας), χωρίς να απαιτούνται ταυτοποιητικά στοιχεία στη χώρα υποδοχής. Αντίστοιχο χαρακτηριστικό παράδειγμα στην Ελλάδα είναι οι κωδικοί του Taxisnet και ο κλειδάριθμος όταν χρησιμοποιείται από άλλες υπηρεσίες.
2) Διαδικτυακή πύλη για Ηλεκτρονική Δικαιοσύνη[12] με τη διαλειτουργική διασύνδεση των Μητρώων Επιχειρήσεων σε όλη την Ευρώπη,
3) N-lex[13] η πύλη της Ευρωπαϊκής Ένωσης για πρόσβαση στην Εθνική Νομοθεσία σε διαλειτουργική διασύνδεση με τα «Εθνικά Τυπογραφεία των Κρατών Μελών».

1.5 Αρχές του EIF 2017

Το αναθεωρημένο EIF του 2017 βασίζεται στις ακόλουθες αρχές:

1) Επικουρικότητα και αναλογικότητα,

[12] https://e-justice.europa.eu/home.do?action=home&plang=el
[13] N-LEX https://n-lex.europa.eu/n-lex/

2) Ανοιχτότητα,
3) Διαφάνεια,
4) Επαναχρησιμοποίηση,
5) Τεχνολογική ουδετερότητα και φορητότητα δεδομένων,
6) Επικέντρωση στο χρήστη,
7) Συμπερίληψη και προσβασιμότητα,
8) Ασφάλεια και προστασία της ιδιωτικής ζωής,
9) Πολυγλωσσία,
10) Διοικητική απλούστευση,
11) Διατήρηση πληροφοριών,
12) Αξιολόγηση της αποτελεσματικότητας και της αποδοτικότητας.

Επιπρόσθετα το νέο EIF αναλύει το εννοιολογικό μοντέλο μίας ολοκληρωμένης δημόσιας υπηρεσίας. Αυτό είναι πολύ σημαντικό, διότι περιγράφει τα δομικά στοιχεία που απαιτούνται για τη σχεδίαση μία τέτοιας υπηρεσίας. Τα δομικά στοιχεία που αναφέρονται είναι:

1) Τα βασικά μητρώα, όπως π.χ. μητρώο πολιτών, ακινήτων, αυτοκινήτων, εταιριών κλπ τα οποία παρέχουν πληροφορίες που απαιτούνται στις δημόσιες υπηρεσίες,
2) Τα ανοιχτά δεδομένα, που ελεύθερα μπορεί κάποιος να τα χρησιμοποιήσει σε μία δημόσια υπηρεσία π.χ. δεδομένα που δίνει η στατιστική υπηρεσία για τον προσδιορισμό των τιμών ζώνης αντικειμενικού προσδιορισμού αξίας ακινήτων,
3) Κατάλογοι υπηρεσιών που μπορούν να χρησιμοποιηθούν και να καταναλωθούν από μία ολοκληρωμένη ψηφιακή δημόσια υπηρεσία. Οι κατάλογοι έχουν προδιαγραφές που επιτρέπουν οι τελικοί χρήστες και οι διάφορες εφαρμογές να αναζητούν τις προς «κατανάλωση» υπηρεσίες.
4) Εξωτερικές υπηρεσίες όπως π.χ. ηλεκτρονικές πληρωμές από τράπεζες, τηλεπικοινωνιακές υπηρεσίες που επιτρέπουν τη χρήση των ηλεκτρονικών δημοσίων υπηρεσιών, πληροφορίες από αισθητήρες π.χ. στην περίπτωση των έξυπνων πόλεων.

5) Ασφάλεια και ιδιωτικότητα που είναι απαραίτητη σε όλες τις συναλλαγές με τη δημόσια διοίκηση.

1.6 Στρατηγική υλοποίησης της διαλειτουργικότητας

Η στρατηγική υλοποίησης της διαλειτουργικότητας έχει ως στόχο να περιγράψει τις προτεραιότητες, τα βασικά εργαλεία που θα εξασφαλίσουν την υλοποίηση των ανωτέρω.

Το πρώτο βασικό στοιχείο είναι η επικαιροποίηση του πλαισίου διαλειτουργικότητας που όπως αναφέρθηκε για το EIF έγινε το 2017.

Επίσης δίνεται έμφαση στα θέματα συντονισμού και συνεργασίας σε όλα τα επίπεδα, στην οργανωσιακή διαλειτουργικότητα με έμφαση στη συνεργασία μεταξύ παρόχων και καταναλωτών υπηρεσιών και δεδομένων.

Επιπρόσθετα αναδεικνύεται η σημασία της συμμετοχής και ευαισθητοποίησης των εμπλεκομένων, η δημιουργία των βασικών υπηρεσιών εμπιστοσύνης όπως π.χ. η αυθεντικοποίηση, η ψηφιακή υπογραφή, καθώς και ενέργειων που υποστηρίζουν τις ασφαλείς ηλεκτρονικές συναλλαγές.

Τα χρηματοδοτικά εργαλεία για την υλοποίηση της στρατηγικής είναι τα προγράμματα HORIZON 2020, το CEF, τα διαρθρωτικά και επενδυτικά ταμεία, το ταμείο ανάπτυξης καθώς και το πρόγραμμα Digital Europe Programme για την νέα προγραμματική περίοδο 2021-2027.

Για τη παρακολούθηση της στρατηγικής υλοποίησης ορίζεται και περιγράφεται μηχανισμός για την παρακολούθηση και τη δημιουργία αναφορών με βάση το πρόγραμμα ISA[2].

2 Παροχή Ολοκληρωμένων Διαλειτουργικών Υπηρεσιών

Η παροχή ολοκληρωμένων Διαλειτουργικών ψηφιακών υπηρεσιών ως δημόσια πολιτική απαιτεί τη συνεργασία μεταξύ διαφορετικών φορέων, μέσω οργάνων της διοίκησης που έχουν τις σχετικές εξουσιοδοτήσεις και μεριμνούν για την τήρηση του υφιστάμενου ρυθμιστικού πλαισίου.

Στόχος της παρούσας ενότητας είναι να αναδείξει τις δυσκολίες του ανωτέρω εγχειρήματος και να προτείνει μία διαδικασία για το στρατηγικό και επιχειρησιακό προγραμματισμό διαλειτουργικών δημοσίων υπηρεσιών

αναγνωρίζοντας τις υφιστάμενες αδυναμίες της Ελληνικής Δημόσιας Διοίκησης και των ενεργειών που πρέπει να πραγματοποιηθούν προκειμένου να είναι εφικτή η επιτυχής υλοποίηση αυτών.

Σήμερα σε Εθνικό επίπεδο δεν υπάρχει κάποια κοινά αποδεκτή μεθοδολογία ή πρακτική που να ενσωματώνει τη διαλειτουργικότητα στις δημόσιες ψηφιακές υπηρεσίες. Για παράδειγμα αν η υλοποίηση μία πολιτικής π.χ. για τη φορολογία βασίζεται στα δεδομένα του φορολογικού ή άλλων μητρώων και στην σημασιολογική ερμηνεία αυτών, τότε οποιαδήποτε νέα υπηρεσία θα έχει ως βάση σχεδιασμού αυτή την αφετηρία. Θεσμικά, οργανωτικά και τεχνολογικά ζητήματα που απαιτούνται για τη διαλειτουργικότητα θα αντιμετωπιστούν στην συνέχεια. Αυτό πρακτικά σημαίνει ότι οι αποφάσεις που θα ληφθούν θα έχουν συγκεκριμένη οπτική, η οποία θα μπορούσε να ήταν διαφορετική αν υπήρχε κάποια άλλη αρχική παραδοχή και υπόθεση.

Η Ελλάδα ως μέλος της Ευρωπαϊκής Ένωσης έχει επηρεαστεί τα τελευταία χρόνια από τις σχετικές πρωτοβουλίες για τη διαλειτουργικότητα, είτε μέσω μηχανισμών συγκριτικής προτυποποίησης π.χ. οι δείκτες για την Ψηφιακή Οικονομία και Κοινωνία (DESI) (European Commission, 2019), είτε μέσω πολιτικών που έχουν το στόχο τον εκσυγχρονισμό της δημόσιας διοίκησης μέσα από πολιτικές για διασυνοριακή διαλειτουργικότητα όπως π.χ. το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Commission, 2017) και η Ενιαία Ψηφιακή Αγορά (European Commission, 2019b).

Η ύπαρξη υποδομής για τη διαλειτουργικότητα αναγνωρίζεται ως ένας από τους βασικούς παράγοντες που διασφαλίζουν τη παροχή ποιοτικών δημόσιων υπηρεσιών (OECD, 2019).

2.1 Απαιτήσεις προγραμματισμού διαλειτουργικών ψηφιακών υπηρεσιών

2.1.1 Επίδραση του θεσμικού πλαισίου

Η νομοθεσία σε ένα κράτος δικαίου είναι βασικό στοιχείο για τη λειτουργία της Δημόσιας Διοίκησης και βασικός καθοδηγητής στο σχεδιασμό και προγραμματισμό των ψηφιακών δημόσιων υπηρεσιών. Οι νομοθετικές πράξεις

θέτουν απαιτήσεις για την εφαρμογή των δημόσιων πολιτικών και την παροχή διαλειτουργικών ψηφιακών υπηρεσιών.

Επιπρόσθετα στη παροχή διαλειτουργικών δημοσίων υπηρεσιών συμμετέχουν διαφορετικοί φορείς που συμβάλουν στην παροχή της υπηρεσίας. Εδώ οι ρόλοι των εμπλεκομένων δεν είναι ισότιμοι αφού είναι εντελώς διαφορετικό ένας φορέας απλά συμμετέχει ως εταίρος, από τον φορέα που είναι επισπεύδων και διαθέτει τα δεδομένα ή τις ψηφιακές διαδικασίες για την παροχή της υπηρεσίας αυτής (Lindquist, 2015). Σε θεσμικό επίπεδο αυτό καθορίζεται από την αρμοδιότητα του κάθε εμπλεκόμενου φορέα που συνήθως προσδιορίζεται σε κάθε παρεχόμενη υπηρεσία.

Παράλληλα οι κανονιστικές αρμοδιότητες που σχετίζονται με την νομοθεσία έχουν διαφορετικά κέντρα αποφάσεων ανάλογα με τον τομέα πολιτικής π.χ. είναι διαφορετικός ο οργανισμός που εισηγείται και παρακολουθεί την εφαρμογή των κανονιστικών πράξεων για την πολιτική του κτηματολογίου και των χρήσεων γης από την πολιτική της αγροτικής παραγωγής και των τροφίμων. Έτσι για παράδειγμα μία υπηρεσία που αφορά επιδοτήσεις καλλιεργειών μετατρέπεται σε διαλειτουργική υπηρεσία που κανονιστικά ρυθμίζεται από δύο κέντρα αποφάσεων.

Επιπρόσθετα οι κανονιστικές ρυθμίσεις σε ένα κράτος δικαίου ξεκινούν από ένα υψηλό επίπεδο αρχών και γενικών απαιτήσεων και φτάνουν μέχρι την παροχή εξειδικευμένων οδηγιών για την εφαρμογή και άσκηση της πολιτικής. Για παράδειγμα το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας – EIF (European Commission, 2017) είναι ένα χαρακτηριστικό κείμενο αρχών και γενικών οδηγιών ενώ η εκτελεστική απόφαση της Ευρωπαϊκής Επιτροπής για το Ευρωπαϊκό Έγγραφο Δημοσίων Συμβάσεων (European Union, 2017) είναι ένα παράδειγμα λεπτομερούς κανονιστικού κειμένου προδιαγραφών.

2.1.2 Επίδραση Οργάνωσης και Λειτουργίας Δημόσιας Διοίκησης

Η Δημόσια Διοίκηση σε ένα Κράτος δικαίου χρηματοδοτείται από το Κράτος και έχει ως στόχο την παραγωγή και υλοποίηση Δημόσιων και Κυβερνητικών πολιτικών. Οι κυβερνητικές πολιτικές εξειδικεύονται σε συγκεκριμένους τομείς όπως π.χ. Οικονομία, Άμυνα, Δικαιοσύνη, Φορολογία, Περιβάλλον, Κοινωνική Ασφάλιση, Υγεία, Έρευνα, Εκπαίδευση, και Εξωτερική πολιτική.

Στην Ελλάδα κάθε διακριτός τομέας πολιτικής ασκείται κατά κύριο λόγο από ένα διακριτό οργανισμό (π.χ. Υπουργεία, Ανεξάρτητες Αρχές, Οργανισμοί Τοπικής Αυτοδιοίκησης). Παράλληλα οι τυπολογίες των αρμοδιοτήτων που έχουν οι φορείς της δημόσιας διοίκησης είναι κανονιστικές, συντονισμού, υλοποίησης, ελέγχου και παροχής υπηρεσιών. Ανάλογα με την τυπολογία των αρμοδιοτήτων εμπλέκονται διαφορετικοί φορείς. Ο βαθμός εκχώρησης αρμοδιοτήτων από την κεντρική διοίκηση σε περιφερειακούς ή αποκεντρωμένους οργανισμούς εξαρτάται σε μεγάλο βαθμό από τον τομέα δημόσιας πολιτικής. Έτσι επιχειρησιακά υπάρχουν πολιτικές που ασκούνται κεντρικά σε επίπεδο Ευρωπαϊκής Ένωσης, ή σε Επίπεδο Κράτους μέλους ή σε περιφερειακό επίπεδο ή σε επίπεδο Δήμου.

Η αρχή της επικουρικότητας γενικά επιτάσσει την άσκηση αρμοδιοτήτων κυρίως σε τοπικό επίπεδο, εντούτοις υπάρχει τάση συγκέντρωσης των αρμοδιοτήτων σε κεντρικό επίπεδο κάτι που τα τελευταία χρόνια διευκολύνεται από την τεχνολογία με την ανάπτυξη του διαδικτύου και των κεντρικών υπολογιστικών υποδομών (π.χ. e-justice portal στην Ευρωπαϊκή Ένωση[12], κανονισμός ΕΕ/2018/1724 για την Ενιαία Ψηφιακή Θύρα (Ευρωπαϊκή Ένωση, 2018). Είναι προφανές ότι ο συγκερασμός των δύο τάσεων μπορεί να επιλυθεί μόνο με διαλειτουργικές υπηρεσίες.

2.1.3 Στρατηγικές στην υλοποίηση ολοκληρωμένων δημοσίων υπηρεσιών

Ο τρόπος υλοποίησης των δημόσιων πολιτικών επηρεάζει την παροχή των ολοκληρωμένων ψηφιακών υπηρεσιών αφού καθορίζει το πλαίσιο και τους κανόνες λήψης των αποφάσεων.

Κάποιος θα μπορούσε να αναγνωρίσει τρείς βασικές στρατηγικές (Kubicek, 2009) υλοποίησης ολοκληρωμένων δημοσίων υπηρεσιών:

Α) Ολοκλήρωση δεδομένων: Η παροχή της υπηρεσίας απαιτεί δεδομένα από διαφορετικά υφιστάμενα συστήματα, αλλά υπάρχει ένα ισχυρό θεσμικό πλαίσιο και πολιτική βούληση που κανονίζει τη λειτουργία τους π.χ. το παράδειγμα της ενοποίηση των ασφαλιστικών ταμείων στον Ενιαίο Φορέα Κοινωνικής Ασφάλισης (www.efka.gov.gr). Η περίπτωση αυτή δεν χαρακτηρίζεται ως διαλειτουργικότητα παρόλα αυτά μπορεί να παρέχει ολοκληρωμένη υπηρεσία,

Β) Έμφαση στην προτυποποίηση (standardization): Είναι κατάλληλο για περιπτώσεις όπου οι οργανισμοί χρησιμοποιούν τα παρόμοια δεδομένα και δομές δεδομένων. Εδώ δίνεται έμφαση στην προτυποποίηση των δεδομένων και εφόσον κάποιος φορέας δεν έχει ακριβώς τα ίδια αναλαμβάνει να μετατρέψει τα δεδομένα στην συμφωνημένη μορφή του προτύπου. Χαρακτηριστικό παράδειγμα είναι ο Διεθνής Τραπεζικός Λογαριασμός (International Bank Account Number - IBAN) όπου όλες οι Τράπεζες κλήθηκαν να μετατρέψουν του λογαριασμούς που είχαν στα εσωτερικά τους συστήματα σε αυτή τη μορφή για την επικοινωνία σε διατραπεζικές εφαρμογές. Στη περίπτωση αυτή πρέπει να υπάρχει είτε προκαθορισμένο πρότυπο ή να υπάρχει θεσμικό πλαίσιο που το περιγράφει.

Γ) Χρήση ενδιάμεσων μηχανισμών: Θεωρητικά αν όλοι οι φορείς ακολουθούσαν τα ίδια πρότυπα η διαλειτουργικότητα θα μπορούσε να επιτευχθεί. Παρόλα αυτά σε πολλές περιπτώσεις είναι πιο οικονομικό να υπάρχουν κεντρικοί μηχανισμοί που να αναλαμβάνουν αυτό το ρόλο για τους φορείς που διαλειτουργούν. Αυτοί οι μηχανισμοί συνήθως συντηρούν κεντρικούς καταλόγους και υπηρεσίες μετατροπής δεδομένων. Αυτό διευκολύνει στη συντήρηση όταν γίνονται αλλαγές. Τέτοιο παράδειγμα είναι το Εθνικό Δημοτολόγιο όπου π.χ. η μεταδημότευση από Δήμο σε Δήμο γίνεται στο κεντρικό σύστημα του Εθνικού Δημοτολογίου και στη συνέχεια ενημερώνει τα συστήματα των Δήμων, διασφαλίζοντας ότι ταυτόχρονα με την εγγραφή σε ένα δήμο θα γίνει η διαγραφή από τον προηγούμενο Δήμο.

Το EIF έχει καθορίσει τα κάτωθι επίπεδα για την ανάπτυξη διαλειτουργικών υπηρεσιών: Θεσμικό, Οργανωσιακό, Σημασιολογικό και Τεχνολογικό. Οι ψηφιακές υπηρεσίες αποτελούν μέρος της λύσης που προκρίνεται για την υλοποίηση των δημόσιων πολιτικών και κατά συνέπεια τα οργανωσιακά και θεσμικά ζητήματα μπορεί να επιβάλλουν διαφορετικές προσεγγίσεις στην υλοποίηση δίνοντας διαφορετικές προτεραιότητα στα επίπεδα του EIF.

2.1.4 Οργανωσιακά ζητήματα διαλειτουργικότητας

Το οργανωσιακό επίπεδο της διαλειτουργικότητας καλείται να συσχετίσει τις επιχειρησιακές διαδικασίες με τις υποδιαδικασίες δεδομένα και αποτελέσματα που μπορούν να επαναχρησιμοποιηθούν για τη κάλυψη συγκεκριμένου

σκοπού. Η πολιτοκεντρική προσέγγιση ανάπτυξης των υπηρεσιών απαιτεί όλες αυτές οι εργασίες να γίνονται από τη σκοπιά του πολίτη – χρήστη των υπηρεσιών. Στο πλαίσιο αυτό θα πρέπει να γίνει εναρμόνιση των επιμέρους διαδικασιών των διαφόρων φορέων προκείμενου αυτές να μπορούν να επαναχρησιμοποιήσουν δεδομένα και διαδικασίες που διαθέτουν άλλοι φορείς.

Στο πλαίσιο αυτό η οργανωσιακή διαλειτουργικότητα πρέπει να απαντήσει τα κάτωθι ερωτήματα:

1) Τι είναι αυτό που χρειάζεται να προτυποποιηθεί; Μήπως υπάρχει κάτι συναφές ήδη διαθέσιμο;
2) Ποιος φορέας θα αναλάβει την εργασία προτυποποίησης;
3) Πως θα λειτουργεί και θα συντηρείται το προς ανάπτυξη πρότυπο;
4) Ποιος θα παρακολουθεί την ορθή υλοποίηση του; Αποτελεί δομικό στοιχείο και άλλων λύσεων;
5) Ποιος θα συντηρήσει το πρότυπο με βάση τις τεχνολογικές αλλαγές και τις νέες ανάγκες και θα αναπτύξει και τις σχετικές αρχιτεκτονικές που θα συμφωνηθούν;

Τα ανωτέρω ζητήματα οργανωσιακής διαλειτουργικότητας διατρέχουν όλα τα άλλα επίπεδα διαλειτουργικότητας όπως αυτά ορίζονται στο EIF.

2.2 Ευρωπαϊκή Αρχιτεκτονική Διαλειτουργικότητας

Η Ευρωπαϊκή Αρχιτεκτονική για τη Διαλειτουργικότητα - European Interoperability Architecture (EIRA, 2019) έχει ως στόχο να καθοδηγήσει τις δημόσιες διοικήσεις στην ανάπτυξη διαλειτουργικών δημοσίων υπηρεσιών. Ειδικότερα η EIRA εισάγει:

1) Κοινή ορολογία για τον καλύτερο συντονισμό,
2) Μία αρχιτεκτονική αναφοράς για τη παροχή ψηφιακών δημόσιων υπηρεσιών,
3) Δομικά αρχιτεκτονικά στοιχεία που είναι ανεξάρτητα από την τεχνολογία και εμπορικά προϊόντα (Architecture Building Blocks),
4) Είναι συμβατή με το EIF και έχει αναπτυχθεί με βάση ένα ευρύτερο ανοιχτό πλαίσιο αρχιτεκτονικής (The Open Group, 2018).

Η EIRA έχει ορίσει δομικά στοιχεία αρχιτεκτονικής (Architecture Building Blocks-ABBs) που μπορούν να επαναχρησιμοποιηθούν σε οποιοδήποτε περιβάλλον προκειμένου να προκύψουν στη συνέχεια δομικά στοιχεία επαναχρησιμοποιούμενων λύσεων (Solution Building Blocks- SBBs).

Ένα από τα βασικά δομικά στοιχεία που έχει προσδιοριστεί στην EIRA είναι αυτό που θέτει κατευθύνσεις για την υλοποίηση των πολιτικών. Στο πλαίσιο αυτό καθορίζονται τέσσερις εναλλακτικές:

Α) Πολιτικές όπου οι αρμοδιότητες ασκούνται σε κεντρικό επίπεδο και ο έλεγχος είναι επίσης σε κεντρικό επίπεδο (π.χ. μητρώο πολιτών – φορολογικό μητρώο). Στις περιπτώσεις αυτές η βαρύτητα δίνεται στη σημασιολογική διαλειτουργικότητα και στα δεδομένα των βασικών μητρώων.

Β) Πολιτικές που έχουμε πολλούς συναρμόδιους φορείς για την υλοποίηση αλλά υπάρχει σαφές θεσμικό πλαίσιο που καθορίζεται κεντρικά. Η προσέγγιση σε αυτή την περίπτωση είναι κανονιστική με έμφαση στις τεχνικές προδιαγραφές π.χ. Πανεπιστήμια (παράρτημα διπλώματος), Νοσοκομεία (φάκελος νοσηλείας ασθενή).

Γ) Πολιτικές όπου αν και οι αρμοδιότητες ασκούνται κεντρικά εν τούτοις το θεσμικό πλαίσιο είναι χαλαρό για κάθε ένα από αυτούς τους οργανισμούς. Σε αυτή τη περίπτωση η προσέγγιση είναι οργανωσιακή μέσα από συμφωνίες διαλειτουργικότητας που ενισχύουν το χαλαρό θεσμικό πλαίσιο π.χ. αναφορές επιχειρηματικότητας Εθνικής Στατιστικής Υπηρεσίας, Τράπεζας Ελλάδας και Υπουργείου Ανάπτυξης – Γενικού Εμπορικού Μητρώου.

Δ) Τέλος έχουμε την περίπτωση όπου έχουμε αποκεντρωμένες αρμοδιότητες και ταυτόχρονα χαλαρό θεσμικό κανονιστικό πλαίσιο. Η προσέγγιση εδώ απαιτεί Πλαίσια Διαλειτουργικότητας, Αρχιτεκτονικές Αναφοράς (π.χ. βλέπε περίπτωση Ευρωπαϊκής Ένωσης) και σέβεται την αρχή της επικουρικότητας.

Η διαλειτουργική δημόσια ψηφιακή υπηρεσία έχει οριστεί σε διοικητικό επίπεδο στο Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Commission, 2017) ως η συγκέντρωση βασικότερων ειδικών τομεακών υπηρεσιών και υπηρεσιών υποδομών οι οποίες παρέχονται μέσα από επαναχρησιμοποιήσιμα

δομικά στοιχεία τα οποία έχουν αναπτυχθεί με ανοιχτά πρότυπα και ανοιχτές τεχνικές προδιαγραφές.

2.3 Αναγκαίες Ικανότητες για διαλειτουργικές υπηρεσίες

Με βάση τα αναφερόμενα στις προηγούμενες ενότητες ένα δημόσιος οργανισμός θα πρέπει να διαθέτει ικανότητες στους κάτωθι τομείς προκειμένου να είναι σε θέση παρέχει διαλειτουργικές υπηρεσίες (Pardo, 2008):

2.3.1 Ικανότητες ανάπτυξης και διαχείρισης πρωτοβουλιών διαλειτουργικότητας

Οι ικανότητες αυτές εξειδικεύονται στα κάτωθι πεδία:

α) Διακυβέρνηση, β)Στρατηγικό σχεδιασμό, γ) Ανάπτυξη επιχειρησιακού σεναρίου, δ) Διαχείριση έργου, ε) Διαχείριση πόρων, στ) Αναγνώριση και εμπλοκή των ενδιαφερομένων μερών, ζ) Ηγεσία, η) Λειτουργικές και τεχνικές αρχιτεκτονικές, θ) Αξιολόγηση επιδόσεων.

2.3.2 Ικανότητες διαμοιρασμού της πληροφορίας

Οι ικανότητες αυτές αναλύονται σε:

α)Ετοιμότητα συνεργασίας (π.χ. χρήση συνεργατικών εργαλείων, ζητήματα εκπαίδευσης, χρηματοδότηση, προσωπικό) , β) Οργανωσιακή συμβατότητα (π.χ. διαδικασίες λήψης απόφασης, επίλυση συγκρούσεων, ανταγωνισμός, κουλτούρα) , γ) Πολιτικές διαχείρισης της πληροφορίας (π.χ. συλλογή, χρήση, διάδοση, αποθήκευση, ιδιωτικότητα, εμπιστευτικότητα, ασφάλεια) δ) Ετοιμότητα για αποδοχή αλλαγών (π.χ. θετικές και αρνητικές συμπεριφορές, εμπιστοσύνη στη χρήση νέων εργαλείων), ε) Γνώση της τεχνολογίας (π.χ. έμπειρο προσωπικό, εκπαίδευση, τεκμηρίωση τεχνολογικών πόρων), στ) Γνώση των απαιτήσεων και διαθέσιμων δεδομένων (π.χ. τεκμηρίωση βάσεων δεδομένων), ζ) Ασφαλές περιβάλλον (π.χ. κατάλληλες πρακτικές για εφαρμογές συστήματα και δίκτυα), η) Τεχνολογική συμβατότητα (π.χ. πρότυπα, εξοπλισμός, λογισμικό).

2.4 Περιορισμοί στο σχεδιασμό διαλειτουργικών υπηρεσιών

Οι διαλειτουργικές υπηρεσίες εξαιτίας του ότι εμπλέκουν διαφορετικούς φορείς λειτουργούν κάτω από σχεδιαστικούς περιορισμούς οι οποίοι θα

πρέπει να αναγνωρίζονται και εξετάζονται έγκαιρα προκειμένου να μην καταστούν μη εφαρμόσιμες μετά την ανάπτυξη και υλοποίηση τους. Συνήθεις περιοχές που δύναται να υπάρχουν περιορισμοί είναι: α) Συνταγματικοί και θεσμικοί περιορισμοί (π.χ. δεν επιτρέπεται να περιλαμβάνονται στοιχεία για το θρήσκευμα κατά την ταυτοποίηση ενός χρήστη), β) περιορισμοί αρμοδιότητας (π.χ. μπορεί ένας φορέας να παρέχει πληροφορίες όταν δεν εμπίπτουν στην αρμοδιότητα του; Παράδειγμα είναι τα στοιχεία οικογενειακής κατάστασης από τη φορολογική δήλωση ή οι υπηρεσίες ενός δήμου που παρέχονται από συστήματα άλλου), γ) περιορισμοί στη συνεργασία (π.χ. μπορεί να μεταδοθεί πληροφορία από ένα εσωτερικό πληροφοριακό σύστημα των Ένοπλων Δυνάμεων που δεν έχει για λόγους ασφάλεια πρόσβαση στο δημόσιο διαδίκτυο;), δ) Οργανωτικοί περιορισμοί (π.χ. διαδικασίες και οι πόροι μπορεί να διαφέρουν τόσο, ώστε να είναι δυσχερής η διαλειτουργικότητα αν δεν προϋπάρξουν δράσεις για προτυποποίηση και εναρμόνιση διαδικασιών και συστημάτων), ε) Περιορισμοί στη πληροφορία (η ποιότητα – κωδικοποίηση της πληροφορίας είναι τέτοια που δεν δίνει επαρκή ασφάλεια στη χρήση της μετά την ανταλλαγή), στ) Διαχειριστικοί περιορισμοί (π.χ. όταν οι συνεργαζόμενοι φορείς έχουν ασυμβίβαστα και ανταγωνιστικά συμφέροντα όπως π.χ. η άσκηση επαγγελματικής δραστηριότητας από το επιμελητήριο ή από τις φορολογικές αρχές), ζ) Περιορισμό κόστους (π.χ. οι συνεργαζόμενοι φορείς δεν έχουν τους πόρους για να κάνουν τις εργασίες που τους αντιστοιχούν), η) Τεχνολογικοί περιορισμοί (π.χ. η ετερογένεια των πληροφοριακών συστημάτων είναι τέτοια που δεν επιτρέπει την ανταλλαγή πληροφοριών μέσα από ανοιχτά πρότυπα), θ) Περιορισμοί επίδοσης (π.χ. τα υφιστάμενα συστήματα δεν μπορούν να εξυπηρετήσουν ικανοποιητικά την πρόσθετη ζήτηση που θα προκύψει).

3 Βελτίωση διαδικασιών προγραμματισμού για διαλειτουργικές δημόσιες υπηρεσίες

Από την ανάλυση των προηγούμενων ενοτήτων καθίσταται σαφές ότι η ανάπτυξη και παροχή διαλειτουργικών ψηφιακών υπηρεσιών είναι ένα σύνθετο ζήτημα που πρέπει να αντιμετωπιστεί σε πολλαπλά επίπεδα και κατά συνέπεια στο προγραμματισμό θα πρέπει να συμπεριληφθούν ειδικές πρόνοιες

για την αντιμετώπιση τους. Επίσης γίνεται η παραδοχή ότι σε εθνικό επίπεδο υπάρχει Πλαίσιο Διαλειτουργικότητας με βασικές αρχές, Κατάλογος Υπηρεσιών, μητρώο διαλειτουργικότητας με τεχνικά στοιχεία για την επαναχρησιμοποιήση των υπηρεσιών, μοντέλα δεδομένων και λίστες προτύπων που πρέπει να χρησιμοποιούνται, να αποφεύγονται ή να απαγορεύονται κλπ.

3.1 Διαμόρφωση στρατηγικών στόχων

Η διαμόρφωση των στρατηγικών στόχων σε ότι αφορά τις διαλειτουργικές υπηρεσίες πρέπει να προκύπτει από συνεργασία μεταξύ των ενδιαφερόμενων φορέων. Δηλαδή θα πρέπει να εντοπιστούν οι ενδιαφερόμενοι φορείς που είτε παρέχουν τα δεδομένα που απαιτούνται, είτε που δυνητικά μπορούν να επαναχρησιμοποιήσουν τα αποτελέσματα της διαλειτουργικής υπηρεσίας που σχεδιάζεται. Δηλαδή η διαμόρφωση των στρατηγικών στόχων πρέπει να είναι κοινή απόφαση που συνήθως εκφράζεται σε επίπεδο Υπουργείων θεσμικά μέσα από μία κοινή Υπουργική Απόφαση ή εφόσον πρόκειται για άλλη μορφή φορέων με προγραμματική συμφωνία ή μνημόνιο συνεργασίας ή σύμβαση.

Το ενδιαφέρον είναι ότι με το άρθρο 47 του νόμου 4623/2019 (ΦΕΚ Α’ 134) τα ανωτέρω θέματα στην Ελλάδα ρυθμίζονται μόνο με απόφαση του Υπουργού Ψηφιακής Διακυβέρνησης.

3.2 Στρατηγικός σχεδιασμός

Για τον προσδιορισμό της στρατηγικής προσέγγισης θα πρέπει να εξεταστούν τα σενάρια που αναφέρονται στην παράγραφο «Στρατηγικές στην υλοποίηση ολοκληρωμένων δημοσίων υπηρεσιών» και να επιλεχθεί το κατάλληλο. Παράλληλα πρέπει να εξεταστούν τα ζητήματα που αναφέρονται στην παράγραφο «Περιορισμοί στο σχεδιασμό διαλειτουργικών υπηρεσιών» προκειμένου να διασφαλιστεί η εφικτότητα του εγχειρήματος και οι προπαρασκευαστικές ενέργειες για την υλοποίηση της υπηρεσίας.

Στη συνέχεια συστήνονται οι ομάδες εργασίες που απαιτούνται για την υλοποίηση της διαλειτουργικής υπηρεσίας. Με το άρθρο 47 του νόμου 4623/2019 (ΦΕΚ Α’ 134) παρέχεται η σχετική εξουσιοδότηση στον Υπουργό Ψηφιακής Διακυβέρνησης.

3.3 Ανάπτυξη επιχειρησιακού σεναρίου

Για τη διαμόρφωση του επιχειρησιακού σεναρίου της διαλειτουργικής υπηρεσίας πρέπει να προσδιοριστούν τα κάτωθι:

i) Οι διαδικασίες που απαιτείται να ακολουθηθούν προκειμένου να παρέχεται η υπηρεσία. Οι διαδικασίες θα πρέπει να ελεγχθούν σε σχέση με τη συμβατότητα τους με τις διαδικασίες των εμπλεκόμενων φορέων αλλά και την πολιτοκεντρική τους προσέγγιση. Σε περίπτωση που υπάρχει ασυμβατότητα θα πρέπει να ακολουθήσει εναρμόνιση των διαδικασιών. Συνίσταται επίσης να προηγηθεί απλούστευση των διαδικασιών λαμβάνοντας υπόψη τις δυνατότητες της ψηφιακής τεχνολογίας,

ii) Ο προσδιορισμός την πληροφορίας που θα ανταλλάσσεται και τυχόν θεσμικές και άλλες πρόνοιες για αυτή, που θα θέσουν πρόσθετες λειτουργικές απαιτήσεις π.χ. ενεργή συγκατάθεση σε ζητήματα ιδιωτικότητας, κρυπτογράφηση για λόγους εμπιστευτικότητας,

iii) Τα σημεία διεπαφών μεταξύ διαφορετικών φορέων και των κοινών υπηρεσιών που απαιτούνται. Στο πλαίσιο αυτό θα πρέπει να ελεγχθεί αν αυτά έχουν ήδη αναλυθεί στην EIRA ως κοινά δομικά στοιχεία αρχιτεκτονικής (π.χ. δομικό στοιχείο ηλεκτρονικής ταυτοποίησης, ψηφιακών υπογραφών, υπηρεσία εμπιστοσύνης) ή/και στο Εθνικό Πλαίσιο Διαλειτουργικότητας (www.e-gif.gov.gr) π.χ. σχήμα δεδομένων για περιγραφή γεωχωρικών δεδομένων και διεύθυνση κατοικίας,

iv) Αν υπάρχουν διαθέσιμες ψηφιακές υπηρεσίες που καλύπτουν έστω μέρος των απαιτήσεων ή τεχνολογικές λύσεις που να είναι συμβατές με τα υφιστάμενα πληροφοριακά συστήματα που θα διαλειτουργήσουν. Εφόσον εντοπιστούν οι υπηρεσίες και λύσεις αυτές επαναχρησιμοποιούνται,

v) Στη συνέχεια όλα τα νέα τμήματα που θα αναπτυχθούν ανατίθενται στους φορείς που διαθέτουν τα πληροφοριακά συστήματα που θα τροποποιηθούν ή σε φορείς που έχουν τη διαθεσιμότητα των πόρων και την τεχνογνωσία να υποστηρίξουν την ανάπτυξη.

vi) Παράλληλα δημιουργούνται σενάρια ελέγχου των απαιτήσεων που έχουν διατυπωθεί από την ανάλυση των διαδικασιών και τον προσδιορισμό των διεπαφών. Με βάση αυτά γίνεται ο σχεδιασμός του νέου στοιχείου που θα αναπτυχθεί και συμφωνείται η αρχιτεκτονική του προκειμένου και αυτό με τη σειρά του να είναι διαλειτουργικό,

vii) Προσδιορίζονται τα παραμετρικά κωδικολόγια που τυχόν θα χρησιμοποιηθούν και εντοπίζονται είτε στο Πλαίσιο Διαλειτουργικότητας ή σε άλλες εργασίες προτυποποίησης π.χ. κωδικοί χωρών, διοικητική διαίρεση της χώρας, κωδικοί επαγγελματικών δραστηριότητων κλπ. Σε περίπτωση μη ύπαρξης σχετικών κωδικολογίων τότε ορίζονται ομάδες συναρμοδίων φορέων για τη διαμόρφωση σχετικών προτάσεων και ένταξη τους στα προς διερεύνηση πρότυπα.

3.4 Διαχείριση έργου – Διαχείριση πόρων

Σε αυτά τα σημεία δεν υπάρχει κάποια ιδιαιτερότητα για τις διαλειτουργικές υπηρεσίες σε σχέση με την συνήθη υλοποίηση ενός έργου ανάπτυξης λογισμικού στο οποίο συμμετέχουν εκπρόσωποι από διάφορους φορείς.

3.5 Αξιολόγηση επιδόσεων

Η αξιολόγηση επιδόσεων θα γίνει από τον κάθε εμπλεκόμενο φορέα αλλά και από την οπτική του τελικού χρήστη των υπηρεσιών όπως έχει ήδη αναφερθεί στην ενότητα «Οργανωσιακά ζητήματα διαλειτουργικότητας» σε σχέση με τα σενάρια ελέγχου που διατυπώθηκαν στην αρχική φάση του σχεδιασμού.

3.6 Καταγραφή της διαλειτουργικής υπηρεσίας

Εφόσον η νέα διαλειτουργική υπηρεσία γίνει αποδεκτή τότε πρέπει να καταχωρηθεί ως νέα υπηρεσία στο κατάλογο των υπηρεσιών. Παράλληλα στο μητρώο διαλειτουργικότητας πρέπει να καταγραφούν τα τεχνικά στοιχεία των επιμέρους διαδικτυακών υπηρεσιών που την αποτελούν. Σε περίπτωση ορισμού νέων δομικών στοιχείων, κωδικολογίων και προτύπων θα πρέπει να ενταχθούν στις σχετικές λίστες προς διερεύνηση. Με το πέρασμα του χρόνου αναμένεται να βελτιωθούν - οριστικοποιηθούν και στη συνέχεια θα καταστούν νέα προτεινόμενα πρότυπα.

Οι διαλειτουργικές ψηφιακές δημόσιες υπηρεσίες απαιτούν συνδυασμό πολλών παραμέτρων για να τεθούν σε λειτουργία. Στη παρούσα ενότητα αναπτύχθηκαν όλες οι παράμετροι πολιτικών που τις επηρεάζουν και έγινε προσαρμογή στην τυπική διαδικασία στρατηγικού σχεδιασμού και προγραμματισμού προκειμένου να αντιμετωπίσει ζητήματα διαλειτουργικότητας με επιτυχία.

Βασικό προαπαιτούμενο είναι να υπάρχει Εθνικό Πλαίσιο Διαλειτουργικότητας που να επικαιροποιείται και εφαρμόζεται κατά την ανάπτυξη των υπηρεσιών. Σε διαφορετική περίπτωση δεν θα είναι δυνατός ο εντοπισμός κοινόχρηστων υπηρεσιών και λύσεων κάτι που αυξάνει την αποδοτικότητα των υπηρεσιών της δημόσιας διοίκησης και συμβάλει έντονα στη παροχή ποιοτικών υπηρεσιών προς του πολίτες και τα ενδιαφερόμενα μέρη.

4 Κανονισμός eIDAS – Εκτελεστικές αποφάσεις – Διαλειτουργικότητας σε ζητήματα ηλεκτρονικής ταυτοποίησης

Το 2014 εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, ο κανονισμός για τις ηλεκτρονικές υπηρεσίες ταυτοποίησης και εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (European Union, 2014). Την 1η Ιουλίου 2016 ο κανονισμός τέθηκε σε ισχύ για την πλειονότητα των διατάξεων του. Μια σημαντική πτυχή του κανονισμού eIDAS είναι η αμοιβαία αναγνώριση των εθνικών μέσων ηλεκτρονικής ταυτοποίησης από τα άλλα κράτη μέλη που κατέστη υποχρεωτική στις 29 Σεπτεμβρίου 2018. Μέσα στο 2020 η Ευρωπαϊκή Επιτροπή ξεκίνησε τη διαδικασία αξιολόγησης προκειμένου να προβεί σε επανεξέταση του κανονισμού λαμβάνοντας υπόψη την μέχρι τώρα εφαρμογή του στην ΕΕ.

Η εφαρμογή του κανονισμού eIDAS είναι ένα ζήτημα που επηρεάζει: α) σε επίπεδο πολιτικής διαφορετικές τομεακές πολιτικές όπως π.χ. για τον ακαδημαϊκό χώρο, την υγεία, τη φορολογία, τα τελωνεία και οριζόντιες πολιτικές όπως για τη προστασία δεδομένων (European Union 2016), τις πολιτοκεντρικές υπηρεσίες (Ευρωπαϊκή Ένωση, 2018), β) σε επιχειρησιακό

επίπεδο εμπλέκει διάφορους οργανισμούς όπως την Ευρωπαϊκή Επιτροπή, τον ENISA[14], το ETSI[15], τις αρμόδιες αρχές από τα κράτη μέλη, τους μηχανισμούς χρηματοδότησης, όπως το πρόγραμμα CEF Telecom[16], το πρόγραμμα Horizon[17] και γενικά τα διαρθρωτικά, επενδυτικά ταμεία και το ταμείο ανάπτυξης, γ) σε τεχνικό επίπεδο σαφείς προδιαγραφές, διαφορετικές υλοποιήσεις αναφοράς δομικών στοιχείων (EIRA, 2019), πλατφόρμες δοκιμών και ελέγχων κ.λπ.

Στο πλαίσιο αυτής της εργασίας θα μελετηθεί συστηματικά η προσέγγιση που υιοθετήθηκε κατά την εφαρμογή του κανονισμού eIDAS συγκριτικά με τις μεθόδους και τις πρακτικές που προτείνονται και χρησιμοποιούνται στις διαλειτουργικές δημόσιες υπηρεσίες που αναφέρθηκαν στις προηγούμενες ενότητες (European Commission, 2017), σε πρακτικές που σχετίζονται με καινοτομία και πρότυπα (Hawkins, 2017), και τις οργανωτικές και πολιτικές προσεγγίσεις για υπηρεσίες δημόσιας διοίκησης (Lindquist, 2015), (Kubicek, 2009).

Ο σκοπός του κανονισμού eIDAS είναι: i) να διασφαλίσει ότι τα φυσικά πρόσωπα και οι επιχειρήσεις μπορούν να χρησιμοποιήσουν τα εθνικά ηλεκτρονικά αναγνωριστικά τους (π.χ. ηλεκτρονικές ταυτότητες) για να αυθεντικοποιηθούν σε δημόσιες υπηρεσίες που προσφέρονται από άλλες χώρες της ΕΕ και ii) να αυξήσουν την εμπιστοσύνη μεταξύ των ενδιαφερομένων μερών στην εσωτερική αγορά.

Ο κανονισμός εισάγει την έννοια της «Εγκεκριμένης Υπηρεσίας Εμπιστοσύνης». Εγκεκριμένες υπηρεσίες εμπιστοσύνης, όπως οι ψηφιακές υπογραφές για φυσικά πρόσωπα, οι ηλεκτρονικές σφραγίδες για νομικά πρόσωπα και δημόσιους οργανισμούς, η ηλεκτρονική χρονοσήμανση, οι ηλεκτρονικές υπηρεσίες συστημένης παράδοσης (π.χ. συστημένη ηλεκτρονική αλληλογραφία), προσφέρονται από εγκεκριμένους παρόχους

[14] European Union Agency for Cyber Security, https://www.enisa.europa.eu/
[15] European Telecommunication Standard Institute, https://www.etsi.org/
[16] Innovation and Networks Executive Agency https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom
[17] Overview of Horizon 2020 projects on "ICT-enabled Public Sector Innovation" https://ec.europa.eu/digital-single-market/en/news/overview-horizon-2020-projects-ict-enabled-public-sector-innovation

υπηρεσιών εμπιστοσύνης που είναι εγγεγραμμένοι σε καταλόγους εμπίστευσης που διατηρούνται από τα κράτη μέλη (π.χ. ΕΕΤΤ για την Ελλάδα).

Επιπρόσθετα, ο κανονισμός καθιερώνει στενή συνεργασία μεταξύ των κρατών μελών για θέματα που σχετίζονται με τη διαλειτουργικότητα, την ασφάλεια, την αξιολόγηση από εκπροσώπους των κρατών μελών σε ομότιμη βάση και την ανταλλαγή πληροφοριών και ορθών πρακτικών σχετικά με τα σχήματα ηλεκτρονικής ταυτοποίησης.

Επιπλέον, ο κανονισμός περιγράφει τη διαδικασία κοινοποίησης στα κράτη μέλη ενός νέου σχήματος – συστήματος ηλεκτρονικής ταυτοποίησης, διευθετεί ζητήματα που σχετίζονται με την ανάκληση και την αναστολή συστημάτων ταυτοποίησης σε περιπτώσεις παραβίασης της ασφάλειας, ορίζει τις ευθύνες του εποπτικού οργάνου που τα κράτη μέλη είναι υποχρεωμένα να ορίσουν (ΕΕΤΤ για την Ελλάδα).

Μία καινοτόμος πρωτοβουλία του κανονισμού είναι η καθιέρωση του σήματος εμπιστοσύνης της ΕΕ, το οποίο θα μπορούσαν να χρησιμοποιήσουν οι εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης που είναι εγγεγραμμένοι στις λίστες - καταλόγους υπηρεσιών εμπιστοσύνης για να δείξουν με απλό, αναγνωρίσιμο και σαφή τρόπο ότι παρέχουν εγκεκριμένες υπηρεσίες εμπιστοσύνης.

Ο κανονισμός τέθηκε σε πλήρη ισχύ τον Σεπτέμβριο του 2018, όπου όλα τα κράτη μέλη υποχρεώθηκαν να αποδεχθούν συστήματα ταυτοποίησης και εγκεκριμένες υπηρεσίες εμπιστοσύνης που συμμορφώνονται με τον κανονισμό eIDAS και παρέχονται από τα άλλα Κράτη Μέλη.

Τα θέματα που χειρίζεται ο κανονισμός eIDAS είναι περίπλοκα και έχει εξουσιοδοτηθεί η Ευρωπαϊκή Επιτροπή να εκδίδει ειδικές εκτελεστικές αποφάσεις για τον καθορισμό των λεπτομερειών του κανονισμού που θα είναι απαραίτητες για την εφαρμογή (eIDAS Observatory, 2015). Η πρώτη εκτελεστική απόφαση της Επιτροπής αφορούσε τη συνεργασία των κρατών μελών και εκδόθηκε στις 24 Φεβρουαρίου 2015.

4.1 Εκτελεστική απόφαση (ΕΕ) 2015/296 της 24ης Φεβρουαρίου 2015 για τη θέσπιση διαδικαστικών λεπτομερειών της συνεργασίας μεταξύ των κρατών μελών σχετικά με την ηλεκτρονική ταυτοποίηση (European Commission, 2015a),

Αυτή η εκτελεστική απόφαση εισήγαγε το Δίκτυο Συνεργασίας των Κρατών Μελών που έχει την εξουσιοδότηση να καθορίσει μεθόδους ανταλλαγής καλών πρακτικών, να εξετάσει τις εξελίξεις στον τομέα της ηλεκτρονικής ταυτοποίησης, να εγκρίνει το σχετικό πλαίσιο διαλειτουργικότητας, να εξετάσει τα έντυπα κοινοποίησης, να γνωμοδοτήσει αναφορικά με τα αποτελέσματα της διαδικασία αξιολόγησης συστημάτων αυθεντικοποίησης που κοινοποιούνται στην ΕΕ κ.λπ.

Η εκτελεστική απόφαση ΕΕ 2015/296 απαιτεί από κάθε κράτος μέλος να ορίσει ένα μοναδικό σημείο επαφής για την επικοινωνία με τα άλλα κράτη μέλη, καθώς και την Ευρωπαϊκή Επιτροπή.

Η απόφαση καθορίζει επίσης τις λεπτομέρειες για τη διαδικασία αξιολόγησης από του εκπροσώπους των Κρατών Μελών των συστημάτων αυθεντικοποίησης και την ανταλλαγή πληροφοριών και ορθών πρακτικών.

4.2 Εκτελεστικός κανονισμός (ΕΕ) 2015/1501 της 8ης Σεπτεμβρίου 2015 για το πλαίσιο διαλειτουργικότητας (eIDAS Node) (European Commission, 2015b),

Αυτή είναι μία από τις σημαντικότερες εκτελεστικές αποφάσεις της Επιτροπής, επειδή περιγράφει την αρχιτεκτονική διαλειτουργικότητας για τον διασυνοριακό έλεγχο ταυτότητας. Το κύριο συστατικό αυτής της αρχιτεκτονικής είναι ο κόμβος eIDAS, δηλαδή το σημείο που έχει τη δυνατότητα να αναλύσει ένα μήνυμα και να αποφασίσει εάν αυτό θα πρέπει να προωθηθεί στον κόμβο eIDAS ενός άλλου κράτους μέλους ή να υποβληθεί σε επεξεργασία από την ίδια χώρα και να μεταφερθεί μέσω συγκεκριμένης διεπαφής στα εθνικά σχήματα ταυτοποίησης που συνδέονται με τον κόμβο. Οι απαιτήσεις για την προστασία της ιδιωτικότητας των δεδομένων, την εμπιστευτικότητα, την ακεραιότητα, του μορφότυπου των μηνυμάτων, την ασφάλεια αναφέρονται σε αφηρημένο επίπεδο στην απόφαση. Αυτή η

απόφαση αντιμετωπίζει επίσης ένα από τα πιο σημαντικά ζητήματα, δηλαδή τα στοιχεία ταυτότητας που θα υποστηρίζονται από τον κόμβο eIDAS. Τα στοιχεία αυτά είναι τόσο για φυσικά όσο και για νομικά πρόσωπα.

Τα υποχρεωτικά στοιχεία των φυσικών προσώπων είναι:

i) τα τρέχοντα οικογενειακά ονόματα,
ii) τα τρέχοντα μικρά ονόματα,
iii) η ημερομηνία γέννησης και
iv) ένα μοναδικό αναγνωριστικό.

Το μοναδικό αναγνωριστικό παράγεται από το κράτος μέλος αποστολής και πρέπει να είναι όσο το δυνατόν πιο σταθερό στο χρόνο.

Ο κόμβος eIDAS δύναται να υποστηρίζει και προαιρετικά στοιχεία, δηλαδή στοιχεία που τα συστήματα ταυτοποίησης των κρατών μελών παρόλο που δεν υποχρεούνται να τα υποστηρίζουν σε πολλές περιπτώσεις το κάνουν και τα οποία μπορεί να είναι χρήσιμα για συγκεκριμένες ηλεκτρονικές υπηρεσίες.

Τα προαιρετικά χαρακτηριστικά είναι:

i) τα ονόματα και τα οικογενειακά ονόματα κατά τη γέννηση
ii) ο τόπος γέννησης,
iii) η τρέχουσα διεύθυνση,
iv) το φύλο.

4.3 Εκτελεστικός κανονισμός (ΕΕ) 2015/1502 της 8ης Σεπτεμβρίου 2015 σχετικά με τη θέσπιση ελάχιστων τεχνικών προδιαγραφών και διαδικασιών για τα επίπεδα διασφάλισης των μέσων ηλεκτρονικής ταυτοποίησης (Χαμηλό, Βασικό, Υψηλό) (European Commission, 2015c)

Διαφορετικές υπηρεσίες απαιτούν διαφορετικό επίπεδο διασφάλισης της εγκυρότητας της ταυτότητας του χρήστη. Για παράδειγμα, μια υπηρεσία που δεν χειρίζεται προσωπικά δεδομένα μπορεί να απαιτεί έλεγχο ταυτότητας μόνο για να επιτρέψει στον χρήστη να δημιουργήσει ένα ειδικό προφίλ χρήστη. Σε αυτήν την περίπτωση μια απλή εγγραφή από τον ίδιο τον χρήστη και ένας έλεγχος ταυτότητας χρησιμοποιώντας ένα όνομα χρήστη και ένα κωδικό πρόσβασης μπορεί να επαρκούν για τις ανάγκες της υπηρεσίας.

Αντίθετα, οι υπηρεσίες που συνήθως χειρίζονται ευαίσθητα προσωπικά δεδομένα απαιτούν να είναι διασφαλισμένες σχετικά με την εγκυρότητα της ταυτότητα του φυσικού προσώπου.

Το επίπεδο διασφάλισης της εγκυρότητας της ταυτότητας εξαρτάται από τις διαδικασίες εγγραφής για την έκδοση και διάθεση των μέσων ταυτοποίησης. Η ηλεκτρονική ταυτοποίηση σημαίνει διαχείριση των μέσων ταυτοποίησης (π.χ. έκδοση, παράδοση, ανάκληση, αντικατάσταση), μηχανισμός ελέγχου ταυτότητας, διαχείριση και οργάνωση (π.χ. πληροφορίες χρήστη, διαχείριση ασφάλειας, τήρηση αρχείων, συμμόρφωση και έλεγχος κ.λπ.). Όσο υψηλότερο είναι το επίπεδο διασφάλισης της εγκυρότητας, απαιτούνται οι πιο περίπλοκες διαδικασίες και ασφαλείς συσκευές.

Σύμφωνα με αυτήν τον εκτελεστικό κανονισμό, ορίζονται τρία επίπεδα αξιοπιστίας: χαμηλό, βασικό και υψηλό. Η προδιαγραφή περιγράφεται αναλυτικά στο παράρτημα του εκτελεστικού κανονισμού.

4.4 Εκτελεστική απόφαση (ΕΕ) 2015/1984 της 3ης Νοεμβρίου 2015 για τον καθορισμό των περιστάσεων, των μορφοτύπων και των διαδικασιών κοινοποίησης συστημάτων ταυτοποίησης (European Commission, 2015d)

Αυτή η εκτελεστική απόφαση καθορίζει το έντυπο «κοινοποίησης» και τις διαδικασίες που πρέπει να ακολουθήσει ένα Κράτος Μέλος προκειμένου να κοινοποιήσει στα άλλα Κράτη Μέλη ένα σύστημα ηλεκτρονικής ταυτοποίησης. Το έντυπο κοινοποίησης παρέχει πληροφορίες σχετικά με πολλά ζητήματα όπως ευθύνη, εγγραφή, διαχείριση μέσων ηλεκτρονικής ταυτοποίησης, διαλειτουργικότητα κλπ. Επιπλέον, εκτός από το έντυπο κοινοποίησης, θα πρέπει επίσης να υποβάλλονται και όλα τα υποστηρικτικά κείμενα.

4.5 Εκτελεστικός κανονισμός (ΕΕ) 2015/806 της 22ας Μαΐου 2015 για τη θέσπιση προδιαγραφών σχετικά με τη μορφή του ενωσιακού σήματος εμπιστοσύνης για τις εγκεκριμένες υπηρεσίες εμπιστοσύνης (European Commission, 2015e)

Αυτός ο εκτελεστικός κανονισμός περιγράφει τα χρώματα, την ορθή χρήση του σήματος εμπιστοσύνης της ΕΕ για τις εγκεκριμένες υπηρεσίες εμπιστοσύνης. Στο παρακάτω σχήμα απεικονίζεται το σήμα εμπιστοσύνης της ΕΕ του εκτελεστικού κανονισμού.

Σχήμα 1: Ενωσιακό σήμα για εγκεκριμένες υπηρεσίες εμπιστοσύνης

4.6 Εκτελεστική απόφαση (ΕΕ) 2015/1505 της 8ης Σεπτεμβρίου 2015 περί καθορισμού των τεχνικών προδιαγραφών και των μορφότυπων των καταλόγων εμπίστευσης (European Commission, 2015f)

Αυτή η απόφαση περιέχει τις τεχνικές προδιαγραφές σχετικά με το κοινό πρότυπο των αξιόπιστων λιστών σύμφωνα με το ETSI TS 119 612 v2.1.1. Κάθε κράτος μέλος πρέπει να δημοσιεύσει αυτήν τη λίστα εμπιστοσύνης σύμφωνα με τις συγκεκριμένες προδιαγραφές σε μηχανογραφημένη και ανθρώπινη μορφή (δηλαδή PDF / A). Η απόφαση καθορίζει επίσης τις απαιτήσεις για τη διατήρηση των αξιόπιστων λιστών σύμφωνα με το ETSI TS 119 612.

4.7 Εκτελεστική απόφαση (ΕΕ) 2015/1506 της 8ης Σεπτεμβρίου 2015 για τον καθορισμό προδιαγραφών σχετικά με τους μορφότυπους των προηγμένων ηλεκτρονικών υπογραφών και των προηγμένων σφραγίδων που πρέπει να αναγνωρίζονται από φορείς του δημόσιου τομέα (XAdES, CAdES, PAdES) (European Commission, 2015g)

Η εκτελεστική απόφαση καθορίζει τις τεχνικές προδιαγραφές προηγμένης ηλεκτρονικής υπογραφής για XML, CMS και PDF σύμφωνα με το XAdES Baseline Profile (European Telecommunications Standards Institute, 2012), CAdES Baseline Profile (European Telecommunications Standards Institute, 2013a), PAdES Baseline Profile (European Telecommunications Standards Institute) , 2013β).
Οι ηλεκτρονικές υπογραφές θα πρέπει να χρησιμοποιούν ένα περίβλημα ασφάλειας σύμφωνα με το βασικό προφίλ Associated Signature Container (European Telecommunications Standards Institute, 2013c). Οι τεχνικές προδιαγραφές για τις ηλεκτρονικές σφραγίδες βασίζονται στα ίδια προφίλ και πρότυπα με αυτά των ηλεκτρονικών υπογραφών.

4.8 Εκτελεστική απόφαση (ΕΕ) 2016/650 της of 25ης Απριλίου 2016 σχετικά με τον καθορισμό προτύπων για την αξιολόγηση της ασφάλειας των εγκεκριμένων διατάξεων δημιουργίας υπογραφής και σφραγίδας (ISO/IEC 15408, ISO/IEC 18045, EN 419 211) (European Commission, 2016a)

Οι Ψηφιακές υπογραφές και οι σφραγίδες θα πρέπει να δημιουργούνται χρησιμοποιώντας εγκεκριμένες διατάξεις και συσκευές που είναι συμβατές με συγκεκριμένα πρότυπα και εφόσον αξιολογηθούν με κοινά κριτήρια για την ασφάλεια της τεχνολογία πληροφοριών (Common criteria for IT security), και τα κατάλληλα προφίλ προστασίας (protection profiles).
Η απόφαση έχει υιοθετήσει το ISO / IEC 15408 για τα κριτήρια αξιολόγησης,

το ISO / IEC 18045 για τη μεθοδολογία αξιολόγησης και το EN 419 211 για τα προφίλ προστασίας.

5 Ο κόμβος eIDAS ως η κύρια υποδομή διαλειτουργικότητας για διασυνοριακό έλεγχο ταυτότητας (European Commission, 2016b)

Ο κόμβος eIDAS που εισήχθη στον εκτελεστικό κανονισμό ΕΕ 2015/1501 για το πλαίσιο διαλειτουργικότητας είναι ένα σύνολο προδιαγραφών για το προφίλ eID - eIDAS και μια υλοποίηση λογισμικού αναφοράς που στοχεύει στη διευκόλυνση της διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων ηλεκτρονικής ταυτοποίησης (eID).

Ο κόμβος eIDAS έχει τις ακόλουθες τεχνικές διεπαφές:

i) **eIDAS-Connector:** δηλ. η διεπαφή μέσω της οποίας οι πάροχοι υπηρεσιών μιας χώρας συνδέονται με τον εθνικό κόμβο eIDAS προκειμένου να είναι διαλειτουργικοί με συστήματα eID από άλλη χώρα. Σε αυτήν την περίπτωση, οι πάροχοι υπηρεσιών είναι τα εξαρτώμενα μέρη που καταναλώνουν τις πληροφορίες eID που παρέχονται από τα κράτη μέλη. Επιπλέον, το eIDAS-Connector μπορεί να παρέχει στον χρήστη τη δυνατότητα να επιλέξει το κράτος μέλος του οποίου θα χρησιμοποιήσει το κοινοποιημένο σύστημα eID. Το τελευταίο διάστημα από την πλευρά της Ευρωπαϊκής Επιτροπής έχει επιτραπεί η χρήση μη κοινοποιημένου συστήματος eID, εφόσον ο πάροχος υπηρεσιών το αποδέχεται.

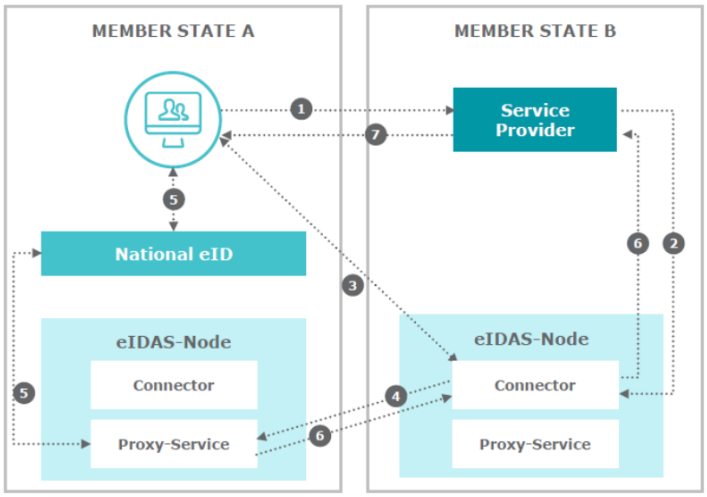
ii) **eIDAS-services:** δηλαδή η διεπαφή της υπηρεσίας διακομιστή μεσολάβησης που θα μεταφέρει το αίτημα στο σύστημα eID.

Η διασύνδεση των εμπιστευόμενων μερών (πάροχοι υπηρεσιών) και των συστημάτων eID με το eIDAS-Connector και eIDAS-services αντιστοίχως αποτελούν μέρος του εθνικού συστήματος των Κράτους Μέλους (ΚΜ) που παραλαμβάνει και του ΚΜ που αποστέλλει αντίστοιχα.

Το γενικό σενάριο που υποστηρίζει ο κόμβος eIDAS είναι το ακόλουθο:

1. Ο χρήστης στο ΚΜ Α ζητά πρόσβαση σε πάροχο υπηρεσιών στο ΚΜ Β.
2. Ο πάροχος υπηρεσιών στο ΚΜ Β στέλνει το αίτημα SAML στον κόμβο eIDAS (Connector).

3. Κατά τη λήψη του αιτήματος, ο σύνδεσμος eIDAS-Node ζητά από τον χρήστη τη χώρα προέλευσης.
4. Όταν η χώρα προέλευσης επιλέγεται από τον χρήστη, το αίτημα SAML προωθείται στην υπηρεσία διακομιστή μεσολάβησης eIDAS-Node του κράτους μέλους του χρήστη.



Σχήμα 2:Κόμβος eIDAS (European Commission, 2015h)

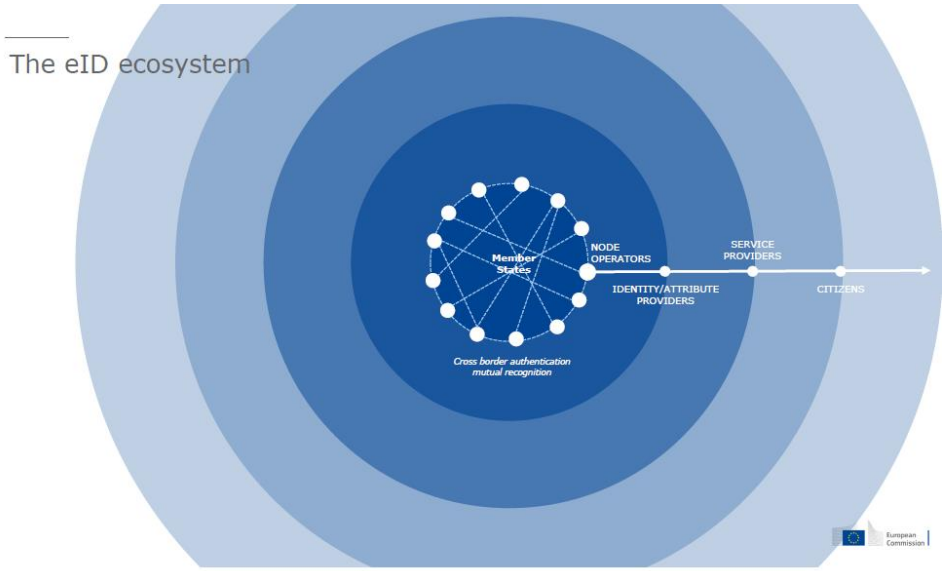
5. Ο χρήστης αυθεντικοποιείται μέσω των διαπιστευτηρίων της ηλεκτρονικής του ταυτότητας. Μόλις αυθεντικοποιηθεί ο χρήστης, τα στοιχεία ταυτότητα προωθούνται στην υπηρεσία διακομιστή μεσολάβησης eIDAS-Node (του κράτους μέλους του χρήστη). Σε αυτό το στάδιο, εάν απαιτείται η συναίνεση του χρήστη μπορεί να παρέχεται αναφορικά με τις πληροφορίες που θα μεταφερθούν.
6. Η υπηρεσία διακομιστή μεσολάβησης eIDAS-Node στέλνει μια δήλωση SAML Assertion στον αιτούντα κόμβο eIDAS-Node του άλλου ΚΜ, ο οποίος προωθεί την απάντηση στον πάροχο υπηρεσιών.
7. Ο πάροχος υπηρεσιών με βάση τα στοιχεία που έλαβε αποφασίζει αν και σε τι θα παρέχει πρόσβαση στον χρήστη.

Ο κόμβος eIDAS, εκτός από το γενικό σενάριο που περιγράφηκε παραπάνω, μπορεί να υποστηρίξει και πρόσθετα σενάρια υπηρεσιών ανάλογα με την κατάσταση του Κράτους Μέλους.

6 Δομή Διακυβέρνησης του κανονισμού eIDAS σε σχέση με το πρόγραμμα CEF

Το παρακάτω σχήμα απεικονίζει το οικοσύστημα του eIDAS που περιλαμβάνει:

1) **Τα Κράτη Μέλη:** Τα πληροφοριακά συστήματα χρησιμοποιούν τις υπηρεσίες ηλεκτρονικής ταυτοποίησης όπως αυτές προσφέρονται από τα Εθνικά Συστήματα και λειτουργούν με βάση την εθνική νομοθεσία του κάθε ΚΜ.
2) **Τους οργανισμούς που λειτουργούν τους κόμβους eIDAS των ΚΜ.** Οι οργανισμοί αυτοί με βάση τις προδιαγραφές και το πρότυπο λογισμικό που έχει παρασχεθεί από την Ευρωπαϊκή Ένωση έχουν αναπτύξει και λειτουργούν τον eIDAS κόμβο του εκάστοτε ΚΜ που ανήκουν και είναι υπεύθυνοι για τη διασύνδεση των εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης και τη διασύνδεση των παρόχων υπηρεσιών στο ίδιο ΚΜ.
3) **Τους Πάροχους υπηρεσιών ηλεκτρονικής ταυτοποίησης και συναφών στοιχείων:** Πρόκειται για οργανισμούς που λειτουργούν με βάση την εθνική νομοθεσία και καλύπτουν τις απαιτήσεις που θέτει ο κανονισμός eIDAS σε επίπεδο διαδικασιών, ασφάλειας και τεχνολογικών προτύπων.
4) **Τους πάροχους υπηρεσιών:** Δηλαδή οργανισμούς που βασίζονται στα δεδομένα που διαθέτουν οι πάροχοι υπηρεσιών ηλεκτρονικής ταυτοποίησης για να παρέχουν τις ηλεκτρονικές τους υπηρεσίες.
5) **Πολίτες:** Είναι οι χρήστες των υπηρεσιών και ταυτόχρονα τα υποκείμενα των δεδομένων που διακινούνται για το σκοπό της ηλεκτρονικής ταυτοποίησης, μετά από δική τους ενεργή συγκατάθεση ή/και απαίτηση.



Σχήμα 3: Το οικοσύστημα του eIDAS

Για τη διακυβέρνηση αυτού του οικοσυστήματος υπάρχουν τα κάτωθι οργανισμοί, όργανα και προγράμματα:

Co-operation network: Πρόκειται για τους εκπροσώπους των ΚΜ που λειτουργούν με βάση την Εκτελεστική απόφαση (ΕΕ) 2015/296 (παράγραφος 4.1),

eIDAS Expert group: Πρόκειται για εμπειρογνώμονες με τεχνική κατάρτιση που συνεισφέρουν στις τεχνικές προδιαγραφές του κανονισμού και ιδίως του eIDAS node και των υπηρεσιών εμπιστοσύνης.

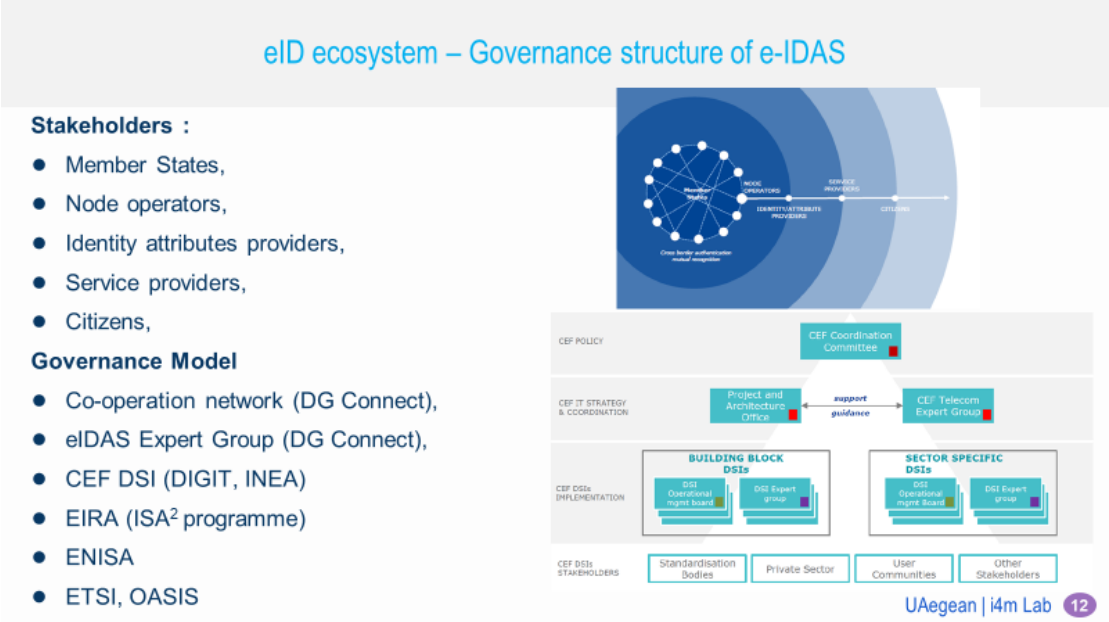
CEF DSI: Αφορά στην υποστήριξη εφαρμογής λύσεων με πρωτότυπο λογισμικό που παρέχονται από το πρόγραμμα CEF και συνεισφέρουν στην υλοποίηση ψηφιακών υπηρεσιών υποδομής (Digital Service Infrastructure) όπως ο κόμβος eIDAS.

EIRA (ISA^2 programme): Οι ανωτέρω λύσεις είναι συμβατές με το EIF και ακολουθούν την πρότυπη αρχιτεκτονική αναφοράς για τη διαλειτουργικότητα που έχει προτείνει το πρόγραμμα ISA^2.

ENISA: Είναι ο οργανισμός της ΕΕ που έχει την αρμοδιότητα παρακολούθησης της υλοποίησης του κανονισμού eIDAS και των υπηρεσιών εμπιστοσύνης από άποψη ασφάλειας και τον εντοπισμό και υποστήριξη των Κρατών μελών

συναφή θέματα π.χ. αναφορά περιστατικών ασφάλειας στο πλαίσιο του κανονισμού (άρθρο 19 του κανονισμού eIDAS).

ETSI OASIS: Οργανισμοί προτυποποίησης ειδικά για θέματα ψηφιακών υπογραφών και υπηρεσιών συστημένης παράδοσης (eDelivery).

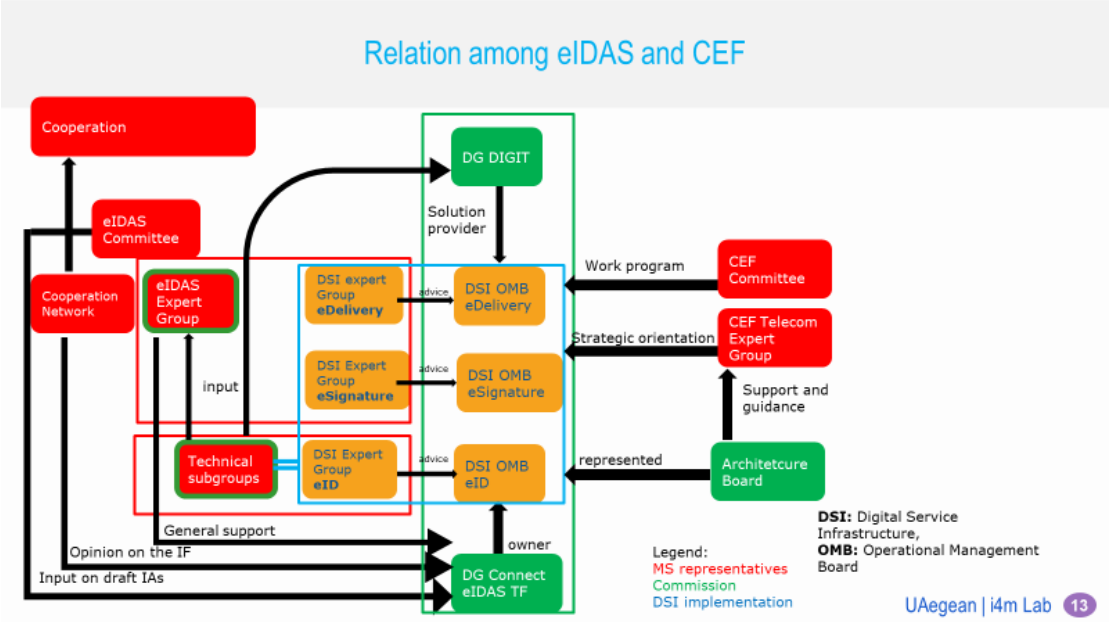


Σχήμα 4: Δομή Διακυβέρνησης του eIDAS

Η σχέση της οργανωτικής δομής της εφαρμογής του κανονισμού eIDAS με την αντίστοιχη του προγράμματος CEF φαίνεται τόσο στο Σχήμα 4 και στο Σχήμα 5. Τα όργανα και οι οργανισμοί διακυβέρνησης του προγράμματος CEF που υποστηρίζει την εφαρμογή του κανονισμού eIDAS εκτείνεται σε τέσσερα επίπεδα:

1) Πολιτικής
2) Στρατηγικής και συντονισμού
3) Υλοποίησης των ψηφιακών υπηρεσιών υποδομής
4) Εμπλοκής όλων των ενδιαφερομένων μερών όπως π.χ. οι οργανισμοί προτυποποίησης, ο ιδιωτικός τομέας, οι κοινότητες χρηστών κλπ.

Η Γενική Διεύθυνση Πληροφορικής της Ευρωπαϊκής Επιτροπής είναι από τους παρόχους τεχνικών λύσεων για τα θέματα του κανονισμού eIDAS αλλά και αρμόδια για θέματα διαλειτουργικότητας μέσω του προγράμματος ISA².



Σχήμα 5: Σχέση eIDAS - Προγράμματος CEF

7 Τομείς Πολιτικής που επηρεάζονται από τον κανονισμό eIDAS

Οι τομείς πολιτικής που έχουν επηρεαστεί από τον κανονισμό eIDAS είναι αφενός οριζόντιες αλλά και τομεακές. Χαρακτηριστικά παραδείγματα τομέων πολιτικής αναφέρονται ακολούθως:

1. Ομοιόμορφη διαχείριση χρηστών και ψηφιακή υπογραφή στους τομείς φορολογίας και τελωνείων ήτοι Uniform User Management & Digital signature in Taxation and Customs -UUM&DS. Χαρακτηριστικό παράδειγμα που ανήκει σε αυτή την κατηγορία είναι η εγγραφή και αναγνώριση οικονομικού φορέα σε διασυνοριακό επίπεδο[18],
2. Ηλεκτρονική υγεία με έμφαση στην αναγνώριση ασθενών και επαγγελματιών υγείας,
3. Οδηγία για τις υπηρεσίες πληρωμών II ((ΕΕ) 2015/2366), καθώς και η 5η οδηγία για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες ((ΕΕ) 2018/843). Για την εφαρμογή αυτή της οδηγίας παίζει σημαντικό ρόλο ο καθορισμός της οικονομική

[18]UUM&DS, https://ec.europa.eu/taxation_customs/sites/taxation/files/2._eo_manual_uumds_0.2_en_.pdf

ταυτότητας που περιλαμβάνει τόσο στοιχεία ταυτότητα όσο και στοιχεία οικονομικής δραστηριότητας,

4. Γενικός κανονισμός για την προστασία δεδομένων (GDPR). Είναι σημαντικό να αναφερθεί ότι αν και το GDPR έχει πολύ ευρύτερο πεδίο εφαρμογής, στον ψηφιακό κόσμο η εφαρμογή συνεπάγεται τη χρήση του πλαισίου eID και eIDAS. Πιο συγκεκριμένα:

I. Στο άρθρο 6 «Νομιμότητα της επεξεργασίας», απαιτείται η ταυτοποίηση του υποκειμένου των δεδομένων, προκειμένου να δοθεί η συγκατάθεση για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους συγκεκριμένους σκοπούς,

II. Στο άρθρο 7 «Προϋποθέσεις για συγκατάθεση», όταν ο υπεύθυνος επεξεργασίας πρέπει να αποθηκεύει την απόκριση του κόμβου eIDAS για να μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των προσωπικών του δεδομένων,

III. Στο άρθρο 15 «Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων» απαιτείται η ταυτοποίηση του υποκειμένου των δεδομένων, προκειμένου να του παραχωρηθεί πρόσβαση στα δεδομένα του,

IV. Στο άρθρο 20 «Δικαίωμα στη φορητότητα των δεδομένων» απαιτείται ταυτοποίηση για τον προσδιορισμό του υποκειμένου των δεδομένων που ζητά φορητότητα δεδομένων.

5. Κανονισμός ενιαίας ψηφιακής θύρας (ΕΕ) 2018/1724 και ειδικά:

I. Στο άρθρο 13 «Διασυνοριακή πρόσβαση σε επιγραμμικές διαδικασίες»,

II. Στο άρθρο 14 «Τεχνικό σύστημα για τη διασυνοριακή αυτοματοποιημένη ανταλλαγή δικαιολογητικών και εφαρμογή της αρχής «μόνον άπαξ»»

III. Στο άρθρο 33 «Προστασία δεδομένων προσωπικού χαρακτήρα»

6. Ευρωπαϊκή Αρχιτεκτονική Αναφοράς για τη Διαλειτουργικότητα eID ABB[19],

[19] EIRA https://joinup.ec.europa.eu/solution/eira/distribution/eira-v300-overview

7. Ακαδημαϊκό eID - Κινητικότητα φοιτητών
8. Self-Sovereign Identity
9. Εμπειρία χρήστη σε διεπαφές του κόμβου eIDAS για την ηλεκτρονική ταυτοποίηση,
10. Ηλεκτρονική υπηρεσία συστημένης παράδοσης (eDelivery)
11. eIDAS και ασφάλεια στον κυβερνοχώρο

Το οικοσύστημα του κανονισμού eIDAS είναι μια προηγμένη εφαρμογή διαλειτουργικών υπηρεσιών. Το κανονιστικό πλαίσιο του eIDAS διαδραματίζει καθοριστικό ρόλο σε βασικές δημόσιες πολιτικές ηλεκτρονικής διακυβέρνησης και σε μεγάλο αριθμό τομέων πολιτικής όπως η υγεία, η εκπαίδευση, οι τραπεζικές υπηρεσίες, τις υπηρεσίες κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Ο κανονισμός eIDAS επιδρά επίσης σε οριζόντιες πολιτικές όπως το GDPR, και ο κανονισμός για την Ενιαία Ψηφιακή Θύρα κλπ.

Το οικοσύστημα eIDAS περιλαμβάνει ένα sui-generis μοντέλο διακυβέρνησης.

Στις επόμενες ενότητες θα εξεταστούν οι επιδράσεις του κανονισμού eIDAS σε συγκεκριμένους τομείς όπως:

1) Η διασυνοριακή κινητικότητα φοιτητών και ακαδημαϊκού προσωπικού στον ακαδημαϊκό χώρο,
2) Σε ζητήματα υγείας και επιπτώσεων όπως αυτή της πανδημίας του Covid-19,
3) Σε ζητήματα ψηφιακών δεξιοτήτων.

Επίσης θα εξεταστούν ειδικές περιπτώσεις για την βελτίωση του υφιστάμενου πλαισίου διαλειτουργικότητας στην Ελλάδα που είναι η γενικότερη πολιτική κάτω από την οποία εντάσσεται και ο κανονισμός eIDAS.

8 Ζητήματα έρευνας για τη Διαλειτουργικότητας και τον κανονισμό eIDAS

Ο κύριος στόχος των ερευνητικών δραστηριοτήτων που αποτυπώνονται στη παρούσα εργασία ήταν η διαλειτουργικότητα σε ευρωπαϊκό και εθνικό επίπεδο στην Ελλάδα. Αναλύθηκαν επίσης οι απαιτούμενες ψηφιακές δεξιότητες σχετικά με τη διαλειτουργικότητα σε υπηρεσίες ηλεκτρονικής

διακυβέρνησης. Τα δομικά στοιχεία του eIDAS για την ηλεκτρονική ταυτοποίησης και τις ψηφιακές υπογραφές συμπεριλαμβάνονται στην ανάλυση της διαλειτουργικότητας. Μελετήθηκαν επίσης οι μελλοντικές τάσεις και η σχέση μεταξύ του κανονισμού eIDAS και της νέα επιστημονικής τάσης για τις ψηφιακές ταυτότητες που ελέγχονται πλήρως από τους χρήστες (Self-Sovereign identities). Παρόλο που από άποψη ασφάλειας και προστασία δεδομένων προσωπικού χαρακτήρα αυτές οι ταυτότητες είναι πολλά υποσχόμενες, εντούτοις ακόμη χρειάζονται αρκετά βήματα σε ότι αφορά στη θεσμοθέτηση τους.

Αυτές εξετάστηκαν τόσο στη περιοχή πολιτικής του ακαδημαϊκού χώρου όσο και σε θέματα υγείας όπως π.χ. η πρόσφατη πανδημία με τον COVID-19.

Τα αποτελέσματα της έρευνας παρουσιάστηκαν σε διεθνή συνέδρια και έγιναν αποδεκτά και σε επιστημονικά περιοδικά. Ενδιαφέρον είχε την πρόσφατη περίοδο η διεξαγωγή των επιστημονικών συνεδρίων με χρήση τηλεδιάσκεψης για λόγους προστασίας των συμμετεχόντων από τον Covid-19.

Τα ζητήματα πολιτικής eIDAS καλύπτουν ένα ευρύ φάσμα διαφορετικών τομέων που δεν είναι δυνατόν στο πλαίσιο αυτής της μεταπτυχιακής εργασίας να αναλυθούν πλήρως στο ίδιο επίπεδο λεπτομέρειας. Ως εκ τούτου, η εργασία επικεντρώθηκε αφενός σε οριζόντιες πολιτικές για τη διαλειτουεργικότητα με έμφαση στην επικαιροποίηση του Ελληνικού Πλαισίου Διαλειτουργικότητας και των Ψηφιακών Δεξιοτήτων σε διαλειτουργικές ηλεκτρονικές υπηρεσίες και αφετέρου σε δύο τομεακές πολιτικές και περιπτώσεις χρήσης που αναδεικνύουν πως ο κανονισμός eIDAS επιδρά σε τομεακές πολιτικές, δηλαδή στον ακαδημαϊκό τομέα και τον τομέα της δημόσιας υγείας, κυρίως εξαιτίας της πρόσφατης Πανδημίας του COVID - 19.

8.1 Επικαιροποίηση του Ελληνικού Πλαισίου Διαλειτουργικότητας

Κατά το πρώτο εξάμηνο του 2019 το ζήτημα της διαλειτουργικότητας τέθηκε ως πρώτη προτεραιότητα από την ελληνική κυβέρνηση.

Όπως αναλύθηκε στην ενότητα 2.2 της παρούσας εργασίας η ύπαρξη πολλών αυτοδιοικούμενων δημόσιων οργανισμών με θεσμικό πλαίσιο που επιτρέπει τη

χαλαρή συνεργασία, επιβάλει την ύπαρξη συμφωνιών διαλειτουρικότητας κάτω από ένα Εθνικό ή/και Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας.

Σε ότι αφορά στην Ελλάδα η υπουργική απόφαση που περιγράφει το Ελληνικό Εθνικό Πλαίσιο Διαλειτουργικότητας (Greek e-GIF) εκδόθηκε το 2012 με τον τίτλο «Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης» (ΦΕΚ 1301 / Β' / 12-04-2012). Έκτοτε δεν έχει γίνει επικαιροποίηση του πλαισίου με αποτέλεσμα σημαντικές εξελίξεις όπως π.χ. αυτή του κανονισμού eIDAS να μην έχουν ληφθεί υπόψη.

Στο πλαίσιο της ερευνητικής εργασίας διαπιστώθηκε ότι σε επίπεδο πολιτικής τα ακόλουθα θέματα θα πρέπει να αντιμετωπιστούν από το Ελληνικό Πλαίσιο Διαλειτουργικότητας (Kalogirou, 2020):

1. Οι έννοιες της ομοσπονδιακής ταυτότητας που εισάγονται με τον κανονισμό eIDAS (EU / 2014/910) πρέπει να συμπεριληφθούν στο Ελληνικό Πλαίσιο Διαλειτουργικότητας. Αυτές οι έννοιες έχουν εισαχθεί στο άρθρο 10 του Ν. 4325/2015 (ΦΕΚ 47 / Α' / 2015) χωρίς να δοθεί έμφαση στη διασυνοριακή διάσταση του κανονισμού eIDAS. Ο πρόσφατος νόμος για την Ψηφιακή Διακυβέρνηση Ν.4727 (ΦΕΚ 184/Α' /23-09-2020) στα άρθρα 24, 25 και στο Κεφάλαιο Θ' ενσωματώνει τις προβλέψεις του κανονισμού eIDAS,
2. Η επαναχρησιμοποίηση πληροφοριών του δημόσιου τομέα που ενσωματώνει την αρχή «ανοιχτά εξ΄ ορισμού δεδομένα» εισήχθη με τον Ν. 4305/2014 και κωδικοποιήθηκε με το νόμο Ψηφιακή Διακυβέρνηση Ν.4727 (ΦΕΚ 184/Α' /23-09-2020) και ιδίως το κεφάλαιο Ι'. Το Ελληνικό Πλαίσιο Διαλειτουργικότητας δεν παρέχει συγκεκριμένες οδηγίες ή συστάσεις για ανοιχτά δεδομένα και ως εκ τούτου θα πρέπει να συμπληρωθεί,
3. Οι έννοιες του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ / 2016/679) και ιδίως οι απαιτήσεις για την παρακολούθηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και το δικαίωμα διαγραφής θέτουν νέες απαιτήσεις στις διαλειτουργικές υπηρεσίες και στο πλαίσιο διαλειτουργικότητας,
4. Ο κανονισμός για την Ενιαία Ψηφιακή Θύρα (ΕΕ / 2018/1724) και ιδίως οι διατάξεις για τη διασυνοριακή πρόσβαση σε διαδικτυακές διαδικασίες, η

αυτόματη ανταλλαγή αποδεικτικών στοιχείων λαμβάνοντας υπόψη την αρχή «Μόνον Άπαξ», θέτει νέες απαιτήσεις στο πλαίσιο διαλειτουργικότητας.

Η διαλειτουργικότητα είναι ένας κρίσιμος παράγοντας για τις ψηφιακές υπηρεσίες του δημόσιου τομέα. Η διαλειτουργικότητα διευκολύνει τις δημόσιες ψηφιακές υπηρεσίες να είναι διαφανείς, γενικευμένες (για χρήση σε περισσότερους από έναν τομείς) και βοηθά ώστε να μπορούν να αλληλεπιδρούν αποτελεσματικά διασυνοριακά με τη χρήση κοινών πλαισίων, προτύπων για την ανταλλαγή πληροφοριών, δεδομένων και διαδικασιών. Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (EIF) παρέχει κατευθυντήριες γραμμές για τις Δημόσιες Διοικήσεις, ώστε να μπορούν να παρέχουν διαλειτουργικές, αποδοτικές και αποτελεσματικές δημόσιες υπηρεσίες σε πολίτες και επιχειρήσεις. Η ευθυγράμμιση του Ελληνικού Πλαισίου Διαλειτουργικότητας με την τρέχουσα έκδοση του EIF, μπορεί να συνεισφέρει ευρύτερα στην ελληνική ψηφιακή διακυβέρνηση και την ψηφιοποίηση. Οι προτάσεις τροποποιήσεων που διατυπώθηκαν στο πλαίσιο αυτή της εργασίας, βασίστηκαν στη μεθοδολογία που χρησιμοποιείται στο EIF για τις αξιολογήσεις των Εθνικών Πλαισίων Διαλειτουργικότητας και στις θεσμικές προβλέψεις και πολιτικές κατευθύνσεις. Στο πλαίσιο της εργασίας διατυπώθηκαν πρακτικές προτάσεις για τη διαμόρφωση και χάραξη πολιτικής για τη διαλειτουργικότητα.

Τα αποτελέσματα της εργασίας έγιναν αποδεκτά για παρουσίαση από το Διεθνές Συνέδριο Θεωρίας και Πρακτικής Ηλεκτρονικής Διακυβέρνησης 2020 “Digital Governance in the Era of Disruptive Technologies and Globalisation” που συνδιοργανώθηκε και από το Πανεπιστήμιο Αιγαίου. Τα αποτελέσματα της εργασίας δημοσιεύτηκαν από το Association for Computing Machinery ACM σε ειδικό τεύχος για το συνέδριο[20],[21].

[20] http://www.icegov.org/track/paper-session-4/
[21] Adapting National Interoperability Frameworks Beyond EIF 3.0: The Case of Greece https://dl.acm.org/doi/10.1145/3428502.3428536

8.2 Ψηφιακές Δεξιότητες για δημόσιες διαλειτουργικές υπηρεσίες.

Οι δημόσιες διοικήσεις επενδύουν πολλά για να βελτιώσουν τις ψηφιακές δεξιότητες του προσωπικού τους σε θέματα νέων τεχνολογιών και διαλειτουργικότητας.

Η δημόσια διοίκηση πρέπει αφενός να αξιολογεί τις υπάρχουσες δημόσιες υπηρεσίες ως προς τη διαλειτουργικότητα και αφετέρου να προσδιορίζει τις απαραίτητες ενέργειες που θα βελτιώσουν την ωριμότητα διαλειτουργικότητας. Σε αυτή την ερευνητική εργασία (Papastylianou, 2020) χρησιμοποιήσαμε το μοντέλο αξιολόγησης ωριμότητας διαλειτουργικότητας της Ευρωπαϊκής Επιτροπής[22] ως βάση για τη δημιουργία ανοιχτού εκπαιδευτικού υλικού για το συγκεκριμένο ζήτημα.

Η ηλεκτρονική ταυτοποίηση, η ηλεκτρονική υπογραφή, η ηλεκτρονική υπηρεσία συστημένης παράδοσης και οι διασυνοριακές υπηρεσίες που ρυθμίζονται από τον κανονισμό eIDAS είναι μεταξύ των κριτηρίων αξιολόγησης που περιλαμβάνονται στο μοντέλο που χρησιμοποιήθηκε. Η εργασία αυτή παρουσιάστηκε στο 8ο Διεθνές Συνέδριο για την Ηλεκτρονική Δημοκρατία τον Δεκέμβριο του 2019 και συμπεριλήφθηκε στα πρακτικά του συνεδρίου “E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age” που δημοσιεύτηκε από το Springer[23]. Επίσης νεότερη έκδοση της εργασίας έχει υποβληθεί και είναι σε διαδικασία αξιολόγησης στο περιοδικό «International Journal of Electronic Governance»[24].

Τα πρόσφατα μέτρα κοινωνικής αποστασιοποίησης που επέβαλε η πανδημία του Covid-19 ενίσχυσαν την ανάγκη για αποδοτικές και αποτελεσματικές διαλειτουργικές ηλεκτρονικές υπηρεσίες. Αποτέλεσμα αυτού είναι οι Δημόσιες Διοικήσεις να επενδύουν στην προσφορά περισσότερων διαλειτουργικών δημόσιων υπηρεσιών και στην υλοποίηση δράσεων που σκοπεύουν να καλύψουν το κενό των ψηφιακών δεξιοτήτων των υπαλλήλων της Δημόσιας Διοίκησης. Το αντικείμενο της εργασίας αυτή ήταν η πολιτική ψηφιακών δεξιοτήτων σε σχέση με τη διαλειτουργικότητα. Αναλύθηκαν τα αντίστοιχα

[22] Interoperability Maturity Model-IMAPS https://joinup.ec.europa.eu/collection/imaps-interoperability-maturity-assessment-public-service/solution/imaps/release/v120
[23] https://link.springer.com/chapter/10.1007/978-3-030-37545-4_6
[24] https://www.inderscience.com/jhome.php?jcode=ijeg

προφίλ τόσο για τους πολίτες όσο και τους επαγγελματίες που αναπτύχθηκαν κατά την τελευταία δεκαετία στην Ευρώπη αναδεικνύοντας τις δεξιότητες για τη διαλειτουργικότητα. Σημαντικές μελέτες περιπτώσεων όπως η Εθνική Ψηφιακή Ακαδημία για τους Πολίτες στην Ελλάδα[25], η Ακαδημία Διαλειτουργικότητας ISA[26] αναλύονται βάσει των προαναφερθέντων πλαισίων. Τέλος, παρουσιάστηκαν πρακτικές εξ' αποστάσεως κατάρτισης από το Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης για τη διαλειτουργικότητα, συμπεριλαμβανομένων πρωτοβουλιών για Open Collaborative Courseware αλλά και της αναδιοργάνωσης των συμβατικών μαθημάτων F2F σε πλήρως διαδικτυακά μαθήματα.

9 Σχεδιασμός ενός ηλεκτρονικού συστήματος διαχείρισης ακαδημαϊκής ταυτότητας για την κινητικότητα των φοιτητών χρησιμοποιώντας τις τεχνολογίες eIDAS eID και Self-Sovereign Identity[27]

Μια μεγάλη πρόκληση για τον κανονισμό eIDAS είναι να δημιουργηθεί ένα μοντέλο διασφάλισης της ιδιωτικής ζωής που θα σέβεται τις διατάξεις του GDPR, δηλαδή να παρέχει ένα ασφαλές, αξιόπιστο περιβάλλον πληροφοριών που θα εμφανίζει μόνο τα προσωπικά δεδομένα που κάθε φορά απαιτούνται για την παροχή μιας συγκεκριμένης ψηφιακής υπηρεσίας. Επιπλέον, σε επίπεδο πολιτικής ο Ευρωπαϊκός Χώρος Εκπαίδευσης (European Educational Area) υποστηρίζει την κινητικότητα των φοιτητών και του ακαδημαϊκού προσωπικού μέσω διαφόρων προγραμμάτων όπως το πρόγραμμα Erasmus. Σε αυτή την κατεύθυνση μία πολλά υποσχόμενη τεχνολογία είναι αυτή των Self-Sovereign Identities (SSI). Προκειμένου να αυξηθεί το επίπεδο διασφάλισης ποιότητας των πληροφοριών που παρέχονται και να καλυφθεί θεσμικά η τεχνολογία των SSI, θα πρέπει να διασυνδέεται με τα στοιχεία της ηλεκτρονικής ταυτότητα που παρέχονται από τον μηχανισμό του κανονισμού eIDAS. Το κομμάτι αυτό της ερευνητικής εργασίας είχε ως στόχο διασυνδέσει

[25] https://nationaldigitalacademy.gov.gr/
[26] https://joinup.ec.europa.eu/collection/digital-skills-public-sector/solution/interoperability-academy
[27] https://www.eunis.org/calendar/eunis-2020-annual-congress/

το eIDAS eID με τεχνολογίες SSI και να προτείνει ένα μοντέλο που μπορεί να εφαρμοστεί στο πλαίσιο της κινητικότητας στο επίπεδο των Ανώτατων Εκπαιδευτικών Ιδρυμάτων (Stasis A., 2020).

Τα ευρωπαϊκά πανεπιστήμια εισέρχονται σε μια φάση έντονης συνεργασίας μεταξύ τους και συμμαχιών για να αντιμετωπίσουν την ανάγκη για κινητικότητα των φοιτητών σε ολόκληρη την Ευρώπη στο πλαίσιο ενός μελλοντικού διασυνοριακού πανεπιστημιακού οργανωτικού μοντέλου (Klobučar, 2019). Επιπλέον, τα πανεπιστήμια συνεργάζονται όλο και περισσότερο με τον ιδιωτικό τομέα, σε διεθνή προγράμματα έρευνας και καινοτομίας, και με τον δημόσιο τομέα σε ζητήματα επαγγελματικών προσόντων που εξαρτώνται από ακαδημαϊκά διπλώματα. Οι ψηφιακές τεχνολογίες είναι κρίσιμης σημασίας για τη δημιουργία και διεύρυνση ενός κοινού Ευρωπαϊκού Χώρου Εκπαίδευσης και Έρευνας που προωθεί τη συνεργασία μεταξύ ομοτίμων ιδρυμάτων και την ανταλλαγή βέλτιστων πρακτικών εκπαίδευσης, κατάρτισης και έρευνας. Ωστόσο, οι ψηφιακές τεχνολογίες είναι αποδοτικότερες όταν διασφαλίζεται η διαλειτουργικότητα τόσο σε επίπεδο τεχνολογικής υποδομής όσο και σε επίπεδο υπηρεσίας. Στο πλαίσιο αυτή της προοπτικής, διάφορες ευρωπαϊκές πολιτικές και πρωτοβουλίες όπως η πρωτοβουλία για την Ευρωπαϊκή Ακαδημαϊκή Ταυτότητα (European Student Card Initiative[28]), η πρωτοβουλία για τη διεκπεραίωση των διαδικασιών του προγράμματος Erasmus χωρίς χρήση χαρτιού (Erasmus Without Paper Network[29]), οι πρωτοβουλίες για εφαρμογές σε κινητό (Erasmus + Mobile App[30]), η συμφωνία για διαδικτυακή μάθηση (Online Learning Agreement[31]), προωθούν την αυτοματοποιημένη ανταλλαγή ακαδημαϊκών δεδομένων μεταξύ των ιδρυμάτων τριτοβάθμιας εκπαίδευσης (ΑΕΙ). Οι παραπάνω πρωτοβουλίες χρηματοδοτούνται από προγράμματα της Ευρωπαϊκής Επιτροπής όπως π.χ. της Γενικής Διεύθυνσης για την Εκπαίδευση και τον Πολιτισμού (DG for Education and Culture), το πρόγραμμα CEF

[28] https://europeanstudentcard.eu/

[29] https://www.erasmuswithoutpaper.eu/ewp-network

[30] https://erasmusapp.eu/

[31] https://www.learning-agreement.eu/start/

Telecom που παρουσιάστηκε στην ενότητα 6. Στόχος είναι να δημιουργηθεί ένα σύστημα ακαδημαϊκής ταυτότητας για του φοιτητές που θα διευκολύνει την κινητικότητα των φοιτητών με βάση τις ακαδημαϊκές τους ταυτότητες και τις ταυτότητες που είναι στο πλαίσιο του κανονισμού eIDAS. Το CEF υποστηρίζει επίσης την υλοποίηση μιας πλατφόρμας υπηρεσιών υποδομής (Core Service Platform[32]) για την προώθηση της κινητικότητας των φοιτητών που θα είναι ολοκληρωμένη με τις υπηρεσίες του κανονισμού eIDAS.

Στο πλαίσιο της ψηφιακής συνεργασίας μεταξύ των ιδρυμάτων τριτοβάθμιας εκπαίδευσης οι διασυνοριακές υπηρεσίες συνεργατικής μάθησης και η παροχή ακαδημαϊκών υπηρεσιών πρέπει να είναι προσβάσιμες από το Διαδίκτυο (είτε για φοιτητές εξ αποστάσεως ή ακόμη και επί τόπου). Σε ένα τέτοιο περιβάλλον η ύπαρξη μία φοιτητικής ψηφιακής ταυτότητα που να λειτουργεί σε διασυνοριακό επίπεδο και να συνδυάζει με συνέπεια τόσο πληροφορίες για το φυσικό πρόσωπο (eIDAS) όσο και πληροφορίες για τις ακαδημαϊκές του ιδιότητες είναι απολύτως απαραίτητη. Σήμερα, τα ακαδημαϊκά συστήματα ταυτότητας μπορεί να είναι αποτελεσματικά σε τοπικό επίπεδο, αλλά είναι κατακερματισμένα σε ευρωπαϊκό επίπεδο, και διαλειτουργούν μόνο μέσα στο δίκτυο του eduGAIN (Torroglosa et al, 2018), δηλαδή ενός ομοσπονδιακού συστήματος διαχείρισης ταυτότητας (Birrell and Schneider, 2013) που επικεντρώνεται μόνο στο ζήτημα της online αυθεντικοποίησης. Κάποιες πιο πρόσφατες, πρωτοβουλίες όπως η Ευρωπαϊκή Κάρτα Φοιτητών[28] και διάφορες μορφές καρτών σε κάποιες πανεπιστημιουπόλεις προσπαθούν να εξασφαλίσουν διευρυμένη αξιοποίηση τους και σε άλλες ψηφιακές υπηρεσίες. Ωστόσο, τα υπάρχοντα συστήματα ακαδημαϊκών ταυτοτήτων ακόμη δεν παρέχουν έναν συστηματικό μηχανισμό για την αναγνώριση εθνικών διαπιστευτηρίων και μέσων αναγνώρισης στο εξωτερικό. Ως αποτέλεσμα, μια ολόκληρη κατηγορία υπηρεσιών (ειδικά, υπηρεσίες που απαιτούν μεταφορά δεδομένων μεταξύ δύο ΑΕΙ ή και τρίτο φορέα) είναι μόνο σε πιλοτική εφαρμογή και δεν μπορούν να αξιοποιηθούν σε παραγωγική βάση, επειδή δεν

32 https://ec.europa.eu/inea/sites/inea/files/eu_student_ecard_call_for_a_core_service_platform_final-v1.0.pdf

είναι σε θέση να επαληθεύσουν διαδικτυακά και με αξιόπιστο τρόπο, τις ταυτότητες των φοιτητών και του ακαδημαϊκού προσωπικού με βάση τα διαπιστευτήρια της χώρας και του ακαδημαϊκού ιδρύματος προέλευσης.

Η εφαρμογή των επιπέδων διασφάλισης ποιότητας για την ηλεκτρονική ταυτοποίηση, όπως έχουν οριστεί από τον κανονισμό eIDAS (ΕΕ / 910/2014) και τον αντίστοιχο εκτελεστικό κανονισμό (ΕΕ / 1502/2015) εφόσον διασυνδεθούν με τα συστήματα ακαδημαϊκής ταυτότητας, μπορούν να έχουν πολλαπλά οφέλη, να διευκολύνουν την κινητικότητα των φοιτητών στο εξωτερικό, να αυξήσουν και βελτιώσουν τις διαθέσιμες διεπιστημονικές και διασυνοριακές ακαδημαϊκές και υποστηρικτικές υπηρεσίες. Αναμένεται επίσης μία τέτοια διασύνδεση θα έχει θετικό αντίκτυπο στη μείωση του διοικητικού βάρους, των εγγραφών και γενικότερα της υποδοχής φοιτητών σε επίπεδο συνεργαζόμενων ΑΕΙ. Ως αποτέλεσμα, η συνδυασμένη και ασφαλής χρήση της ηλεκτρονικής ταυτοποίησης του eIDAS και των ακαδημαϊκών διαπιστευτηρίων γίνεται ο ακρογωνιαίος λίθος της χάραξης πολιτικής της Ευρωπαϊκής Ένωσης. Η ανάπτυξη-εξειδίκευση ενός τομεακού ευρωπαϊκού πλαισίου διαλειτουργικότητας που υποστηρίζει μια αμοιβαία αναγνωρισμένη ακαδημαϊκή ψηφιακή ταυτότητα αποτελεί το επόμενο βήμα. Αναμένουμε από αυτή η νέα μορφή «συνδεδεμένης ταυτότητας» να καταστήσει δυνατή μια διαδικασία ταυτοποίησης για ακαδημαϊκούς σκοπούς με υψηλότερο επίπεδο διασφάλισης ποιότητας που θα αξιοποιεί τα συστήματα eID των χρηστών που υποστηρίζονται από το κράτος μέλος προέλευσης τους.

9.1 Πολιτικές για έναν Ευρωπαϊκό Εκπαιδευτικό χώρο και τη ψηφιακή ταυτότητα

Η ευρωπαϊκή πολιτική «μαθησιακής κινητικότητας», δηλαδή η πολιτική προώθησης της «διακρατικής κινητικότητας με σκοπό την απόκτηση νέων γνώσεων, δεξιοτήτων και ικανοτήτων», απορρέει από τη σύσταση του Συμβουλίου της Ευρωπαϊκής Ένωσης προς τα κράτη μέλη να «δημιουργήσουν ένα θετικό περιβάλλον για υποστήριξη της μαθησιακής κινητικότητας», στο πλαίσιο της πολιτικής «Νεολαία σε κίνηση» του 2011 (European Council, 2011). Μετά από χρόνια επιτυχημένης εφαρμογής του προγράμματος Erasmus για φοιτητές, η έννοια της κινητικότητας επεκτάθηκε ώστε να συμπεριλάβει

προγράμματα κινητικότητας ακαδημαϊκού προσωπικού, συνεργασίες μεταξύ ΑΕΙ, υποτροφίες, πρακτική άσκηση και πολιτιστικές δραστηριότητες. Όλες αυτές οι μορφές συνεργασιών αποτελούν βασικό μέρος της ευρωπαϊκής πολιτικής για τον τομέα της εκπαίδευσης, που καθορίστηκε από το Ευρωπαϊκό Συμβούλιο (European Council, 2019) βάσει της πρότασης της Ευρωπαϊκής Επιτροπής (European Commission, 2018), ως στρατηγικού πλαισίου για τη συνεργασία στην εκπαίδευση και την κατάρτιση και ως ένας κοινός χώρος «στον οποίο η μάθηση, η μελέτη και η έρευνα δεν θα παρεμποδίζονταν από σύνορα». Σε αυτό το πλαίσιο, το Eurydice[33], ένα δίκτυο 43 εθνικών μονάδων που εδρεύουν σε όλες τις 38 χώρες του προγράμματος Erasmus +, έχει αναλάβει τη διεξαγωγή ερευνών και αναφορών σχετικά με τον τρόπο λειτουργίας και εξέλιξης των εθνικών εκπαιδευτικών συστημάτων και τη διεξαγωγή συγκριτικών μελετών για τη διευκόλυνση της διακρατικής κινητικότητας των ΑΕΙ μεταξύ χωρών της ΕΕ, του ΕΟΧ και υποψήφιες προς ένταξη χώρες. Το Eurydice δημοσίευσε πρόσφατα τον πίνακα αποτελεσμάτων για την κινητικότητα της τριτοβάθμιας εκπαίδευσης, προσδιορίζοντας, μεταξύ άλλων, ως βασικά θέματα κινητικότητας: α) την πληροφόρηση και την καθοδήγηση σε φοιτητές και ακαδημαϊκό προσωπικό, β) τη φορητότητα επιχορηγήσεων και δανείων, συμπεριλαμβανομένης της πιστωτικής κινητικότητας για βραχυπρόθεσμες σπουδές και πλήρης- πτυχιακές σπουδές, γ) την αναγνώριση των μαθησιακών αποτελεσμάτων μέσω του Ευρωπαϊκού Συστήματος Μεταφοράς Ακαδημαϊκών Μονάδων (European Credit Transfer and Accumulation System - ECTS) και δ) την αναγνώριση των προσόντων[34].

Όλες οι προαναφερόμενες προτεραιότητες πολιτικής απαιτούν την αυτοματοποιημένη και έγκυρη μεταφορά ακαδημαϊκών δεδομένων μεταξύ των ΑΕΙ, προκειμένου να αποφευχθεί η γραφειοκρατία και να επιτευχθούν οφέλη από το χαμηλότερο κόστος συναλλαγής (χρόνος διεκπεραίωσης και κόστος επεξεργασίας) και ενιαία ταυτοποίηση των φοιτητών και του ακαδημαϊκού προσωπικού σε διάφορες χώρες και ιδρύματα. Στην πράξη, αυτό που

[33] https://eacea.ec.europa.eu/national-policies/eurydice/home_en

[34] https://eacea.ec.europa.eu/national-policies/eurydice/sites/eurydice/files/mobilityscoreboard_2018_19.pdf

απαιτείται είναι: α) η διασύνδεση των πληροφοριακών συστημάτων των ΑΕΙ ώστε να επιτρέπεται η ασφαλής ανταλλαγή και επαλήθευση των δεδομένων των φοιτητών και των ακαδημαϊκών στοιχείων, β) η παροχή απρόσκοπτης πρόσβασης στις διαδικτυακές ακαδημαϊκές υπηρεσίες και εγκαταστάσεις του ΑΕΙ παροχής των υπηρεσιών (συμπεριλαμβανομένης της εγγραφής) για τους φοιτητές και το ακαδημαϊκό προσωπικό που συμμετέχουν σε ένα πρόγραμμα κινητικότητας και, γ) τη δυνατότητα για φοιτητές και ακαδημαϊκό προσωπικό να ταυτοποιηθούν στις υπηρεσίες του ΑΕΙ υποδοχής χρησιμοποιώντας τα εθνικά τους διαπιστευτήρια, με αξιόπιστο τρόπο και σύμφωνα με την αρχή «Μόνον Άπαξ[35]».

Σε αυτό το πλαίσιο, έχουν ενταχθεί αρκετές πρωτοβουλίες για την ανάπτυξη μίας πιλοτικής υπηρεσίας και εφαρμογές που να υλοποιούν βασικές ψηφιακές λειτουργίες για συνεργασία μεταξύ ΑΕΙ. Μεταξύ αυτών, τα έργο ERASMUS Without Paper (EWP) [36] και το έργο EMREX[37]. Το πρώτο αποσκοπεί στη δημιουργία, μιας δημόσιας υποδομής που θα αντικαταστήσει τις συμβατικές έγχαρτες ροές εργασίας για την κινητικότητα των φοιτητών με αντίστοιχες ψηφιακές. Η πλατφόρμα που αναπτύχθηκε αναμένεται να διευκολύνει τα ΑΕΙ στην ανταλλαγή δεδομένων φοιτητών (συμπεριλαμβανομένων διμερών συμφωνιών ΑΕΙ, μαθησιακών συμφωνιών, πιστοποιητικά άφιξης / αναχώρησης κλπ.), χρησιμοποιώντας τη διαλειτουργικότητα και την ασφάλεια του δικτύου EWP. Το δεύτερο έργο, το EMREX, παρέχει μια υποδομή και υπηρεσίες για τη μεταφορά μεγάλων συνόλων δεδομένων, επιτρέποντας έτσι στους φοιτητές να παρέχουν, μέσω του δικτύου EMREX, τα ακαδημαϊκά τους διαπιστευτήρια (συμπεριλαμβανομένων ακαδημαϊκών στοιχείων και βαθμών) διασυνοριακά, στα ΑΕΙ και πιθανούς εργοδότες όταν υποβάλλουν αίτηση για θέση εργασίας.

Οι τρέχουσες πολιτικές και πρωτοβουλίες για την προώθηση της Μαθησιακής κινητικότητας και της έρευνας συμπληρώνονται με μια πολιτική για ψηφιακή

[35] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle

[36] https://www.erasmuswithoutpaper.eu/ewp-network

[37] https://emrex.eu/

πανευρωπαϊκή ταυτότητα, κατ' εφαρμογή του σχεδίου δράσης της Ευρωπαϊκής Επιτροπής του 2018 (European Commission, 2018): «by 2025 all students in Erasmus+ mobility should be able to have their national identity and student status recognized automatically across EU Member States, including access to campus services when arriving abroad». Ο συνδυασμός των δύο ταυτοτήτων, της εθνικής και της φοιτητικής ταυτότητας, απαιτεί τη δημιουργία ενός αξιόπιστου και ασφαλούς συνδέσμου μεταξύ τους, χρησιμοποιώντας τις δυνατότητες και τις διασφαλίσεις που παρέχει η σύγχρονη κρυπτογραφία. Η «συνδεδεμένη ταυτότητα» θα πρέπει, φυσικά, να συγκεντρώνει χαρακτηριστικά τόσο από το eIDAS eID όσο και από την ομοσπονδιακή ταυτότητα του eduGAIN. Αυτό προϋποθέτει την αντιμετώπιση σημαντικών σημασιολογικών ζητήματα και θεμάτων ασφάλειας, διότι θα απαιτηθούν αρκετές επισκέψεις από το ένα σύστημα στο άλλο, γεγονός που καθιστά την εμπειρία του χρήστη προβληματική αφού οι χρήστες ενδεχομένως να είναι απρόθυμοι να υιοθετήσουν μια τόσο περίπλοκη υπηρεσία. Τα τελευταία χρόνια, έχουν γίνει σημαντικές προσπάθειες σε αρκετά έργα για την επίλυση των ανωτέρω θεμάτων (π.χ. εντός του έργου STORK 2.0 αλλά και σε πιο πρόσφατα έργα όπως το ID4U, το ESMO[38] και το MyAcedmeicID[39]), αλλά ακόμη δεν έχει υιοθετηθεί μία κοινά αποδεκτή λύση. Νεότερες πρωτοβουλίες, όπως η Ευρωπαϊκή Κάρτα Φοιτητών (ESC), που έχει πλέον εξελιχθεί για να ενσωματώσει τους κανόνες αναγνώρισης του κανονισμού eIDAS καθώς και νέες μορφές καρτών εντός πανεπιστημιουπόλεων (όπως η φοιτητική κάρτα που προτείνει η European Campus Card Association), υπόσχονται μια καλύτερη εμπειρία χρήστη.

Παρόλη την πρόοδο που έχει σημειωθεί και την πολιτικής ώθηση σε λύσεις συμβατές με τον eIDAS, πολλά ερωτήματα παραμένουν ανοιχτά και θα πρέπει να αποφασιστούν σύντομα. Πώς είναι δυνατή η αναβάθμιση, η μεταρρύθμιση και η προσαρμογή των υφιστάμενων ακαδημαϊκών υποδομών πληροφορικής στην πρόκληση μιας ευρωπαϊκής ψηφιακής ακαδημαϊκής ταυτότητας; Ποιες νέες τεχνολογίες πρέπει να υιοθετηθούν προκειμένου να επιταχυνθεί η

[38] http://www.esmo-project.eu/

[39] https://uni-foundation.eu/project/myacademicid/

διαδρομή ψηφιοποίησης στον τομέα των υπηρεσιών ακαδημαϊκής ταυτότητας, για να υποστηριχθεί αποτελεσματικά η παροχή μιας νέας γενιάς διασυνοριακής μάθησης και ακαδημαϊκών διαδικτυακών υπηρεσιών;

9.2 Προσέγγιση για «Διασυνδεδεμένη Ακαδημαϊκή Ταυτότητα» με χρήση τεχνολογιών διαχείρισης ταυτότητας από το χρήστη (Self-Sovereign-Identity -SSI)

Όπως αναφέρθηκε στις προηγούμενες ενότητες, ένα από τα κύρια προβλήματα για την υλοποίηση μιας διασυνοριακής ακαδημαϊκής ταυτότητας (ειδικά όσον αφορά την κινητικότητα των φοιτητών) είναι ότι είναι κατακερματισμένη. Τα στοιχεία που χαρακτηρίσουν τους σπουδαστές σε ξεχωριστούς παρόχους υπηρεσιών ταυτότητας (identity providers) και ιδιοτήτων (attribute providers) που δεν είναι απαραίτητα διασυνδεδεμένοι μεταξύ τους. Η κατάσταση γίνεται χειρότερη, επειδή κάθε τέτοιο σύστημα χρησιμοποιεί διαφορετικά τοπικά αναγνωριστικά για τον ίδιο φοιτητή, τα οποία τις περισσότερες φορές δεν μπορούν να συσχετιστούν μεταξύ τους. Ακόμη και στις περιπτώσεις που είναι εφικτός ένας βαθμός συσχέτισης (για παράδειγμα συνδυάζοντας το όνομα, το επώνυμο και την ημερομηνία γέννησης ενός φοιτητή σε διαφορετικά πανεπιστήμια), προκύπτει μία αμφιβολία σχετικά με το επίπεδο βεβαιότητας για αυτήν τη νέα διασυνδεδεμένη ταυτότητα. Το eIDAS eID έχει θεωρηθεί ως το συνδετικό στοιχείο που θα συγκολλούσε όλα αυτά τα κομμάτια μαζί, ωστόσο η αξιοποίηση του στον ακαδημαϊκό τομέα είναι μικρή. Αυτό οφείλεται κυρίως στο γεγονός ότι οι υπάρχουσες υποδομές πληροφορικής πρέπει να αναβαθμιστούν προκειμένου να συσχετιστούν τα αναγνωριστικά πανεπιστημίου με τα αναγνωριστικά του eIDAS, κάτι που δεν είναι εύκολο.

Μια απλοϊκή λύση θα ήταν να υλοποιηθεί ένα κεντρικό σύστημα όπου οι φοιτητές θα μπορούσαν να συγκεντρώσουν τα στοιχεία τους και να επιτρέψουν στους παρόχους των υπηρεσιών (SP) να ταυτοποιούν τους χρήστες μέσω αυτού του συστήματος. Ωστόσο, τέτοια συστήματα αποτελούν πόλο έλξης για επιθέσεις κλοπής ταυτότητας. Μια άλλη προσέγγιση θα ήταν να επιτρέπεται στους χρήστες να πραγματοποιούν έλεγχο ταυτότητας μέσω

διάφορων παρόχων ταυτότητας και να "συγκεντρώνουν" τη στιγμή της συναλλαγής όλα τα απαιτούμενα στοιχεία. Ωστόσο, η εμπειρία μας έδειξε ότι αυτό οδηγεί σε πολύ κακή εμπειρία χρήστη και υψηλά ποσοστά εγκατάλειψης των ψηφιακών υπηρεσιών.

Το σύστημα που προτείνεται σε αυτή την εργασία προσπαθεί να αντιμετωπίσει αυτά τα ζητήματα υιοθετώντας το eIDAS eID και διασυνδέοντας το με Self Sovereign Identity (SSI) (Allen, 2016) ως μέσο δημιουργίας ακαδημαϊκών ταυτοτήτων κατάλληλων και αποδεκτών σε διασυνοριακές υπηρεσίες και Ακαδημαϊκά Ιδρυμάτα.

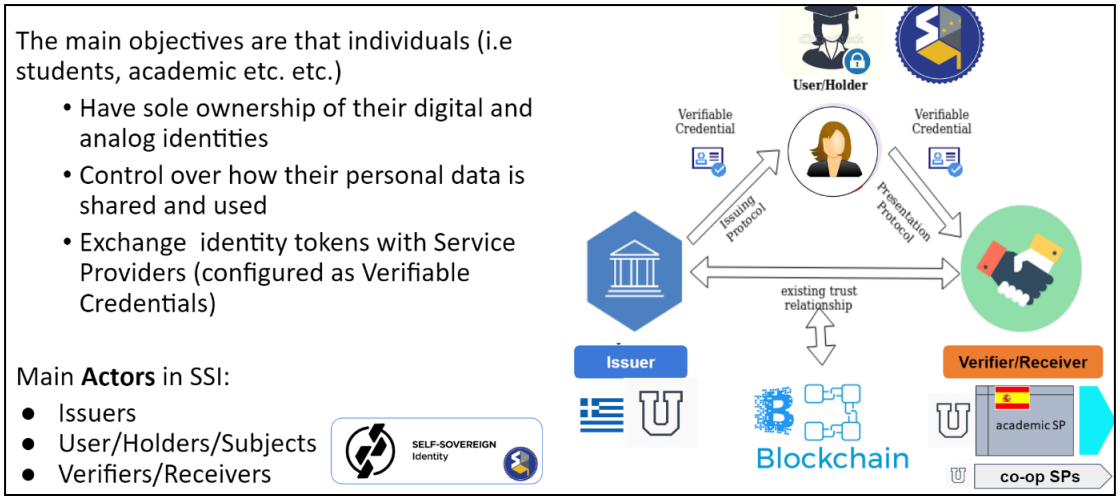
Η τεχνολογία που επιτρέπει τη διαχείριση του κύκλου ζωής της ταυτότητας του χρήστη από τον ίδιο τον χρήστη (Self-Sovereign Identity -SSI) (Mühle et al, 2018), (van Bokkem et al, 2019), (Wang and De Filippi 2020), είναι μια νέα προσέγγιση στην αποκέντρωση της διαχείρισης προσωπικών δεδομένων που δίνει στους χρήστες τον ουσιαστικό έλεγχο των δεδομένων τους. Το SSI βασισμένο σε τεχνολογίες blockchain στοχεύει στη δημιουργία ενός πολύ υψηλότερου επιπέδου εμπιστοσύνης στο διαδίκτυο, βάσει μηχανισμών που επιτρέπουν τον αυτοματοποιημένο και επαληθεύσιμο προσδιορισμό των μερών σε μια συναλλαγή, ενώ ταυτόχρονα μειώνει το κόστος που συνεπάγεται οι τρέχοντες κεντρικοί μηχανισμοί οικοδόμησης εμπιστοσύνης που συνήθως βασίζονται στο Κράτος. Η κατευθυντήρια αρχή του SSI, δηλαδή, διασφαλίζει τον έλεγχο των προσωπικών τους δεδομένων, μέσα από τη χρήση επαληθεύσιμων διαπιστευτηρίων (VC). Ένα VC μπορεί να περιέχει όλες τις πληροφορίες που έχει συμβατικό έγχαρτο πιστοποιητικό, αλλά επιπλέον καθιστά εμφανή τυχόν παραβίαση του καθιστώντας το πιο αξιόπιστο από έγχαρτο πιστοποιητικό, καθώς μπορεί να επαληθευτεί με κρυπτογραφικές μεθόδους. Ένα κρυπτογραφικά αυθεντικό και μη ανακλημένο VC μπορεί να χρησιμοποιηθεί για την αυτόματη επαλήθευση της κυριότητας, της αυθεντικότητας και της μη αποποίησης, καθώς και τον εντοπισμό της εκδούσας αρχής.

Συγκεκριμένα, για τη Διασυνδεδεμένη Ακαδημαϊκή Ταυτότητα προτείνεται η χρήση Επαληθεύσιμων Διαπιστευτηρίων (Verifiable Credentials - VC), όπως

αυτά έχουν προτυποποιηθεί από το W3C[40], για τη διασύνδεση των στοιχείων της ταυτότητας. Τα VC είναι «σφραγισμένα αποδεικτικά στοιχεία» (tamper-evident) διαπιστευτήρια που δεν επιτρέπουν την παραβίαση τους, έχουν αποδεδειγμένο δικαιούχο, ιδιοκτησία και ακεραιότητα που επαληθεύεται με κρυπτογραφικές μεθόδους. Είναι πάντα υπό τον έλεγχο των χρηστών, δεν απαιτούν κεντρικό αποθετήριο και είναι επεκτάσιμα (με άλλα λόγια μπορούν να χρησιμοποιηθούν για να αντιπροσωπεύουν μια διευρυμένη ταυτότητα φοιτητή με πολλά ακαδημαϊκά στοιχεία). Με το νέο αυτό μοντέλο δεδομένων, καταργείται η ανάγκη διαλειτουργικότητας μεταξύ των υφιστάμενων πηγών δεδομένων.

Με λίγα λόγια, το προτεινόμενο σύστημα επιτρέπει στους φοιτητές να δημιουργήσουν τον ιδιωτικό τους χώρο με πληροφορίες ταυτότητας και ακαδημαϊκά στοιχεία από τα ΑΕΙ. Αυτό επιτρέπει στους χρήστες να αποθηκεύουν με ασφάλεια τα στοιχεία της ακαδημαϊκής τους ταυτότητάς τους, καθώς αυτά συλλέγονται από τις διάφορες έγκυρες πηγές, σε μορφή επαληθεύσιμων διαπιστευτηρίων και τα οποία μπορούν να συνδέονται μεταξύ τους. Έτσι, οι φοιτητές μπορούν να δημιουργήσουν μια συνδεδεμένη ταυτότητα συνδυάζοντας τα διάφορα κομμάτια ταυτότητας που προσφέρονται από διαφορετικού παρόχους στοιχείων και ταυτότητας. Επιπλέον, οι υπηρεσίες των ΑΕΙ ή οι τρίτοι πάροχοι υπηρεσιών μπορούν να επαληθεύσουν την αυθεντικότητα των στοιχείων ταυτότητας και των ακαδημαϊκών ιδιοτήτων που παρουσιάζονται από τους φοιτητές χωρίς να χρειάζεται να επικοινωνήσουν με μια κεντρική υπηρεσία που θα λειτουργούσε ως single point of failure για το σύστημα ή θα έπρεπε να διασυνδεθεί και να ενοποιηθεί με πολλαπλούς IdPs / APs. Το παρακάτω σχήμα απεικονίζει το υψηλού επιπέδου σχεδιασμό της προτεινόμενης αρχιτεκτονικής.

[40] https://www.w3.org/TR/vc-data-model/



Σχήμα 6: Προτεινόμενη υψηλού επιπέδου αρχιτεκτονική

Τα βασικά χαρακτηριστικά της προτεινόμενης αρχιτεκτονικής είναι: α) η μετατροπή της ψηφιακής (ομόσπονδης) ταυτότητας σε αξιόπιστες συνδεδεμένες ταυτότητες και β) η εφαρμογή νέων μορφών διαχείρισης ταυτότητας, υπό τον πλήρη έλεγχο του χρήστη, ικανή να διατηρεί και να διαχειρίζεται συνδέσμους μεταξύ των διαφορετικών στοιχείων ταυτότητας ενός χρήστη, που φιλοξενούνται σε διαφορετικούς IdPs και παραδίδονται μέσω διαφορετικών δικτύων (για παράδειγμα eIDAS, eduGAIN) χωρίς να διακυβεύεται η ιδιωτικότητα του χρήστη.

Σε αυτό το πλαίσιο, ο χρήστης (δηλαδή) το Υποκείμενο Δεδομένων «κρατά» ένα «πορτοφόλι» επαληθεύσιμων διαπιστευτηρίων (VC). Κάθε διαπιστευτήριο αποτελείται από έναν αριθμό επικαλούμενων στοιχείων ταυτότητας (identity claims). Κάθε VC είναι ένα κομμάτι πληροφοριών που είναι κρυπτογραφικά αξιόπιστο.

Η προτεινόμενη αρχιτεκτονική επιτρέπει λύσεις, οι οποίες θα φέρουν συγκεκριμένα οφέλη και πραγματικές βελτιώσεις αντιμετωπίζοντας την ανάγκη να διευκολύνουν αποτελεσματικά την (φυσική και εικονική) κινητικότητα των ευρωπαίων φοιτητών σε ολόκληρο τον Ευρωπαϊκό Χώρο Ανώτατης Εκπαίδευσης, βάσει ψηφιακών διαδικασιών που επιτρέπουν την εκτεταμένη διατομεακή - διασυνοριακή χρήση συστημάτων ηλεκτρονικής ταυτοποίησης και ελέγχου ταυτότητας σύμφωνα με τον eIDAS (που ελαχιστοποιεί τους κινδύνους κλοπής ταυτότητας / πλαστοπροσωπίας), την

ικανότητα ανταλλαγής ακαδημαϊκών ιδιοτήτων με τρόπο συμβατό και συμπληρωματικό ως προς τον κανονισμό eIDAS από το δίκτυο eduGAIN, την Ευρωπαϊκή Κάρτα Φοιτητών με εναρμονισμένη προσέγγιση διασυνδεδεμένης ταυτότητας ως βάση για τη διαλειτουργικότητά τους. Αναμένεται τεράστια εξοικονόμηση χρόνου και μετακινήσεων για τους φοιτητές και το ακαδημαϊκό προσωπικό, επιτυγχάνοντας αξιοσημείωτη απλοποίηση σε πολλές διοικητικές διαδικασίες και σημαντική μείωση του χρόνου για την επεξεργασία των δεδομένων σε σύγκριση με τις ίδιες διαδικασίες που βασίζονται σε έγχαρτες διασυνοριακές ροές εργασίας.

Σε τεχνικό επίπεδο ο αντίκτυπος της διασύνδεσης ακαδημαϊκών ιδιοτήτων με το δομικό στοιχείο λογισμικού για το eID που παρέχεται από πρόγραμμα CEF, μπορεί να χρησιμοποιηθεί ως αφετηρία για μια ενιαία ευρωπαϊκή ταυτότητα φοιτητή, καθώς και για την δημιουργία άλλων διασυνδεδεμένων ταυτοτήτων, προσωρινών ή μόνιμων όπως π.χ. το orcID[41] για τους επιστήμονες.

9.2.1.1 Βασικές Έννοιες

Πιο αναλυτικά, οι κύριες τεχνικές έννοιες της αρχιτεκτονικής είναι: Αποκεντρωμένα αναγνωριστικά (Decentralized Identifiers-DID), επαληθεύσιμα διαπιστευτήρια (VC) και επαληθεύσιμες παρουσιάσεις (Verifiable Presentations-VP). Τα DID[42] είναι URI που σχετίζονται με έναν χρήστη, δηλαδή για ένα συγκεκριμένο θέμα και το μέσο για έμπιστες αλληλεπιδράσεις. Είναι υπό τον πλήρη έλεγχο του χρήστη και είναι ανεξάρτητα από οποιοδήποτε κεντρικό μητρώο (όπως για παράδειγμα έναν πάροχο υπηρεσιών ταυτότητας ή τα αρχεία του Πανεπιστημίου). Τα VC είναι μη αξιόπιστα σύνολα δηλώσεων που πραγματοποιούνται από μια οντότητα για άλλη οντότητα. Αυτές οι δηλώσεις δημιουργούνται κρυπτογραφικά. Στο πλαίσιο του ακαδημαϊκού χώρου ένα VC θα μπορούσε να εκδοθεί από ένα Πανεπιστήμιο, το οποίο να επιβεβαιώνει ότι ένα άτομο διαθέτει πτυχίο από αυτό. Οι VP είναι ένα σφραγισμένο αποδεικτικό που κωδικοποιείται με τέτοιο τρόπο ώστε ο δημιουργός του να μπορεί να θεωρηθεί αξιόπιστος μετά από μια

[41] https://orcid.org/

[42] https://www.w3.org/TR/did-core/

διαδικασία κρυπτογραφικής επαλήθευσης. Είναι παρόμοια με τα VC με την κύρια διαφορά τους να είναι ότι τα VP συνήθως περιέχουν δεδομένα που συντίθενται από VC, αλλά δεν περιέχουν τα αρχικά VC. Με αυτόν τον τρόπο οι VP μπορούν να παρουσιαστούν ως απόδειξη της κατοχής δηλώσεων που εκδίδονται από διαφορετικούς εκδότες. Ένας VP μπορεί να εκφράζει δεδομένα από ένα ή περισσότερα VC.

9.2.1.2 Βασικοί ρόλοι και εδραίωση εμπιστοσύνης (Trust Anchoring)

Οι βασικοί ρόλοι του συστήματος είναι ο Χρήστης / Υποκείμενο των δεδομένων, ο Κάτοχος, οι Εκδότες SSI, τα Πορτοφόλια (wallet) / Πράκτορας (agent) για SSI και τέλος οι Καταναλωτές των SSI (ή οι Πάροχοι Υπηρεσιών). Τα Υποκείμενα είναι οι οντότητες με τις οποίες σχετίζεται ένα συγκεκριμένο VC. Ο Κάτοχος δηλώνει το άτομο ή την οντότητα που ελέγχει το ψηφιακό πορτοφόλι ή τον πράκτορα που αποθηκεύει και ελέγχει τη χρήση ενός δεδομένου διαπιστευτηρίου. Ο Κάτοχος μπορεί να είναι ή όχι το Υποκείμενο. Ένας εκδότης SSI είναι μια οντότητα που μπορεί να δημιουργήσει επαληθεύσιμα διαπιστευτήρια σχετικά με τους χρήστες/υποκείμενα, π.χ. το πανεπιστήμιο προέλευσης ή ο πάροχος ταυτότητας. Αυτές οι δηλώσεις εκφράζουν μια πληροφορία που ο εκδότης έχει στην κατοχή του. Έτσι, η εμπιστοσύνη ενός καταναλωτή σε μια τέτοια δήλωση σχετίζεται άμεσα με την εμπιστοσύνη του καταναλωτή στον εκδότη. Τα πορτοφόλια SSI είναι ψηφιακά πορτοφόλια που επιτρέπουν στους χρήστες να κάνουν έλεγχο ταυτότητας χρησιμοποιώντας τις επαληθεύσιμες δηλώσεις που έχουν εκδοθεί και αποθηκευτεί σε αυτά τα VC. Συνήθως υλοποιούνται ως εφαρμογές σε μια κινητή συσκευή. Οι πληροφορίες που εμπεριέχουν ταυτοποιητικά προσωπικά δεδομένα (Personally Identifiable Information) αποθηκεύονται στο πορτοφόλι SSI. Ένας καταναλωτής δηλώνει αν μια οντότητα έχει τη δυνατότητα να λαμβάνει και να επικυρώνει VC από πορτοφόλια χρήστη π.χ. πανεπιστήμιο προορισμού.

Στην προτεινόμενη αρχιτεκτονική η εμπιστοσύνη είναι αποκεντρωμένη. Οι καταναλωτές επαληθεύσιμων δηλώσεων αποφασίζουν ποιους εκδότες θα εμπιστεύονται. Για να διευκολύνουμε τη σχέση εμπιστοσύνης μεταξύ Εκδοτών και Καταναλωτών, αξιοποιούμε το υπάρχον δίκτυο eIDAS για τον εντοπισμό

και την επαλήθευση της ταυτότητας των Εκδοτών στο σύστημα[43]. Επιπλέον, οι καταναλωτές είναι σε θέση ανεξάρτητα: α) να επαληθεύσουν την ταυτότητα των εκδοτών, β) να επικυρώσουν την ίδια την δήλωση και γ) να επικυρώσουν την ιδιοκτησία του χρήστη στο VC.

9.2.1.3 Βασικές Λειτουργίες

Οι κύριες λειτουργίες του πλαισίου σχετίζονται με τη διαχείριση του κύκλου ζωής του VC. Αξίζει πραγματικά να αναφέρουμε τα εξής:

Αρχικοποίηση εκδότη: Οι εκδότες ενός VC δημιουργούν ένα δημόσιο έγγραφο DID. Ένα έγγραφο DID περιέχει πληροφορίες σχετικά με το ποιος είναι ο εκδότης, τα endpoints που χρησιμοποιεί και τα κρυπτογραφικά κλειδιά που χρησιμοποιεί (αυτά τα έγγραφα συνήθως αποθηκεύονται σε ένα κατανεμημένο καθολικό μητρώο (distributed ledger). Στην προτεινόμενη αρχιτεκτονική, οι εκδότες περιλαμβάνουν σε αυτό το έγγραφο DID τα δημόσια κλειδιά που προέρχονται από μια εγκεκριμένη ηλεκτρονική σφραγίδα του κανονισμού eIDAS. Με αυτόν τον τρόπο, η νομική οντότητα πίσω από έναν εκδότη βασίζεται (anchored) στο έμπιστο δίκτυο του eIDAS και έτσι μπορεί εύκολα να εντοπιστεί και επαληθευτεί.

Έκδοση VC: Ο χρήστης αποκτά πρόσβαση σε μια υπηρεσία εκδότη και αποδεικνύει την κυριότητα ενός DID. Στη συνέχεια, ο χρήστης συλλέγει ιδιότητες και στοιχεία από έγκυρες πηγές (π.χ. eIDAS, eduGAIN κ.λπ.) που είναι διασυνδεδεμένες με τον Εκδότη. Τέλος, ο Εκδότης δημιουργεί VC για τον χρήστη που περιέχουν ορισμένες πληροφορίες τις οποίες επιβεβαιώνουν (με βάση τα διαθέσιμα χαρακτηριστικά), συμπεριλαμβάνουν το DID του χρήστη ως αντικείμενο του VC και μεταφέρουν τα VC στο πορτοφόλι του χρήστη. Ένα VC βασικά είναι μια δήλωση, που λέει ότι το Υποκείμενο αυτού του τεκμηρίου έχει ορισμένες ιδιότητες που επιβεβαιώνει ο εκδότης. Επομένως, ο εκδότης είναι η οντότητα εμπιστοσύνης σε αυτό το πλαίσιο και όχι ο χρήστης. Στην περίπτωση της ακαδημαϊκής κοινότητας, ο εκδότης μπορεί να είναι είτε ένα ΑΕΙ είτε μια υπηρεσία διαμεσολάβισης του δικτύου eduGAIN (proxy service).

[43] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

Αυτή η λειτουργικότητα συμμορφώνεται με μια προκαθορισμένη Πολιτική Αρχιτεκτονική Διασύνδεσης που καθορίζει τις υψηλού επιπέδου απαιτήσεις για τη διαχείριση και παροχή μιας αποτελεσματικής Υπηρεσίας Διασύνδεσης. Τα VC συνοδευόμενα από ένα δημόσιο αποκεντρωμένο αναγνωριστικό (DID) γραμμένο από το Εκδότη των διαπιστευτηρίων, κοινοποιούνται ως απόδειξη ενός συνόλου ιδιοτήτων ταυτότητας (που λαμβάνονται από αρμόδιες και έγκυρες πηγές, όπως το eIDAS eID και το eduGAIN κ.λπ.) σε ένα κατανεμημένο καθολικό μητρώο, με χρήση αποκεντρωμένου (Decentralized) PKI.

Αποθήκευση VC: Τα VC αποθηκεύονται με ασφάλεια στο πορτοφόλι των χρηστών, υποθέτοντας ότι ο χρήστης διαθέτει ένα πορτοφόλι SSI ικανό να αποδείξει την κυριότητα των αποκεντρωμένων αναγνωριστικών (DID). Τα VC μεταφέρονται κρυπτογραφημένα και υπογράφονται στο Πορτοφόλι του χρήστη (μια ασφαλής εφαρμογή, συνήθως αποθηκευμένη στην κινητή συσκευή του χρήστη).

Κατανάλωση VC: Οι χρήστες θέλουν να παρουσιάσουν τις ιδιότητες από ένα (σύνολο) VC σε κάποιο Πάροχο Υπηρεσιών (π.χ. AEI προορισμού). Οι χρήστες αλληλεπιδρούν (χρησιμοποιώντας το πορτοφόλι τους) με το AEI, δημιουργώντας, στις περισσότερες περιπτώσεις, μια Επαληθεύσιμη Παρουσίαση (VP) που περιέχει τις απαιτούμενες ιδιότητες βάσει των VC που είναι αποθηκευμένα στο πορτοφόλι τους (ή σε ορισμένες περιπτώσεις μπορεί ακόμη και να μεταφέρουν τα ίδια τα VC). Στη συνέχεια, ο Πάροχος Υπηρεσιών λαμβάνει τα υποβληθέντα δεδομένα και επαληθεύει την εγκυρότητα, την αυθεντικότητα και την κυριότητα του χρήστη πάνω σε αυτά. Στη συνέχεια ο πάροχος παρέχει στο χρήστη πρόσβαση στην υπηρεσία. Η αυθεντικότητα ενός VC μπορεί να επαληθευτεί από ένα δημόσιο κλειδί που σχετίζεται με το DID του εκδότη μέσω μιας διεπαφής υπηρεσίας που παρέχεται σε παρόχους ακαδημαϊκών υπηρεσιών (AEI) και όχι μόνο. Η ιδιοκτησία ενός VC μπορεί επίσης να επαληθευτεί κρυπτογραφικά, με παρόμοιο τρόπο.

9.2.1.4 Παράδειγμα

Για παράδειγμα, ας υποθέσουμε ότι ένας φοιτητής πρέπει να κάνει κράτηση δωματίου σε ξενοδοχείο που προσφέρει ειδικές τιμές σε φοιτητές του Erasmus. Για να ενεργοποιηθεί αυτή η ειδική τιμή:

1. Ο φοιτητής αποκτά πρόσβαση στην υπηρεσία έκδοσης VC του Πανεπιστημίου υποδοχής. Συνδέει το πορτοφόλι SSI του, αυθεντικοποιείται χρησιμοποιώντας τα πανεπιστημιακά διαπιστευτήριά του και λαμβάνει VC που πιστοποιεί την ιδιότητα του ως φοιτητής του προγράμματος Erasmus (αυτό μπορεί να είναι το περιεχόμενο του VC ή να περιέχει πρόσθετες πληροφορίες - δεδομένα).
2. Ο φοιτητής μαθητής έχει πρόσβαση στη σελίδα κράτησης του ξενοδοχείου. Εκεί επιλέγει να ενεργοποιήσει την ειδική έκπτωση και απαιτείται να παρουσιάσει έναν VP που να αποδεικνύει την ιδιότητα του ως φοιτητή του προγράμματος Erasmus.
3. Ο φοιτητής ξεκλειδώνει και συνδέει το πορτοφόλι του με την υπηρεσία του ξενοδοχείου (SP). Στη συνέχεια, το πορτοφόλι δημιουργεί ένα κατάλληλο VP και το υποβάλει στην υπηρεσία του ξενοδοχείου (SP).
4. Το ξενοδοχείο λαμβάνει την VP, την επικυρώνει και επαληθεύει ότι το αντίστοιχο DID ανήκει στο εκδότη πανεπιστήμιο που συμμετέχει στο πρόγραμμα.
5. Η υπηρεσία του ξενοδοχείου (SP) χορηγεί την έκπτωση στον φοιτητή ανάλογα.

9.2.2 Θεσμικά και επιχειρησιακά προαπαιτούμενα

Σήμερα, το επίπεδο διασφάλισης ποιότητας που χαρακτηρίζει τα συστήματα ηλεκτρονικής ταυτοποίησης του eIDAS, πρέπει να επεκταθεί για να αξιολογήσει την ποιότητα της υπηρεσίας διασύνδεσης σε ένα περιβάλλον SSI και επαληθεύσιμων διαπιστευτηρίων. Είναι σημαντικό να αναφερθεί ότι το επίπεδο διασφάλισης ποιότητα των ακαδημαϊκών ιδιοτήτων πρέπει επίσης να επανεξεταστεί και να επανακαθοριστεί με βάση τις αρχές του κανονισμού eIDAS, διαφορετικά η εμπιστοσύνη θα βασίζεται μόνο σε διμερής συμφωνίες μεταξύ των ΑΕΙ. Αυτό ακριβώς γίνεται στις υπηρεσίες έργου EWP και τις υπηρεσίες ESC. Στο πλαίσιο του κανονισμού eIDAS, ο ρόλος του παρόχου

υπηρεσιών ταυτοποίησης είναι ζωτικής σημασίας και είναι υπεύθυνος για τη διαχείριση των διαπιστευτηρίων των χρηστών. Τα επαληθεύσιμα διαπιστευτήρια θα πρέπει να αναγνωρίζονται ως ένας νέος τρόπος ηλεκτρονικής ταυτοποίησης, λαμβάνοντας υπόψη τόσο τεχνικά ζητήματα όσο και ένα σύνολο κανόνων που επιτρέπουν τη χρήση τους. Αυτό θα απαιτήσει την επανεξέταση των εκτελεστικών κανονισμών ΕΕ / 2015/1501, ΕΕ / 2015/1502, ΕΕ/2015/1984 της Ευρωπαϊκής Επιτροπής.

Επιπλέον, θα απαιτηθούν συμπληρωματικές νομικές διατάξεις σε εθνικό επίπεδο, δεδομένου ότι τα εθνικές ηλεκτρονικές ταυτότητες εκδίδονται σύμφωνα με την εθνική νομοθεσία.
Η χρήση επαληθεύσιμων διαπιστευτηρίων θα πρέπει επίσης να επεκταθεί πέραν του νομικού πεδίου του eIDAS, ειδικά όταν πρόκειται για ιδιωτικά ΑΕΙ. Τα ΑΕΙ στο πλαίσιο του eIDAS θα πρέπει να γίνουν εγκεκριμένοι πάροχοι υπηρεσιών εμπιστοσύνης που εκδίδουν επαληθεύσιμες δηλώσεις, δηλαδή εκδότες SSI, που διασυνδέονται με πληροφορίες ταυτότητας, με έμπιστο τρόπο που βασίζεται σε εγκεκριμένα ψηφιακά πιστοποιητικά.
Οι απαιτήσεις του GDPR θα εφαρμοστούν εύκολα σε αυτό το προτεινόμενο πλαίσιο, δεδομένου ότι ο χρήστης είναι ο κάτοχος των δεδομένων και μόνο με τη συγκατάθεσή του τα δεδομένα θα αποκαλυφθούν στον πάροχο υπηρεσιών, δηλαδή το ΑΕΙ προορισμού. Οι επαληθεύσιμες δηλώσεις και διαπιστευτήρια που εκδίδονται από ένα ΑΕΙ πρέπει να θεωρούνται ταυτοποιητικά προσωπικά δεδομένα, καθώς συνδέονται με την ταυτότητα ενός ατόμου, παρόλο που δεν είναι δυνατόν να γίνει αυτός ο συσχετισμός χωρίς τη συγκατάθεση του χρήστη (European Commission, 2020).

10 Επίσημες ταυτότητες μίας χρήσεως (Disposable Yet Official Identities -DYOI) για το σχεδιασμό συστημάτων προστασίας της ιδιωτικότητας

Σε αυτή την ενότητα της ερευνητικής εργασίας εξετάζουμε τη δυνατότητα εφαρμογής των αρχών του κανονισμού eIDAS και του SSI στο χώρο της υγείας και συγκεκριμένα στον σχεδιασμό ενός συστήματος υπηρεσιών που προσφέρουν τη δυνατότητα: α) να διαχειρίζεται ο χρήστης άμεσα και να

επαληθεύει ένα ευρύ φάσμα πιθανών ψηφιακών εγγράφων, όπως βεβαιώσεις, πιστοποιητικά κλπ. και β) για την παροχή ελέγχου πρόσβασης βάσει διαπιστευτηρίων σε εσωτερικούς ή εξωτερικούς χώρους, ειδικά σε περιπτώσεις όπου η επαλήθευση δεν γίνεται από κάποια διαδικτυακή εφαρμογή, αλλά με παρέμβαση του ανθρώπου με χρήση έξυπνων κινητών ή μιας συσκευής Internet of Things (IoT). Τέτοιου τύπου υπηρεσίες ανέδειξαν τη χρησιμότητα τους στην περίοδο της πρόσφατης πανδημίας του Covid-19. Η συγκεκριμένη αρχιτεκτονική προτάθηκε με αφορμή την κάλυψη των έκτακτών αναγκών για τη δημόσια υγεία. Με αυτές τις υπηρεσίες αναδεικνύεται η επίδραση του κανονισμού eIDAS στην υλοποίηση πολιτικών για τη δημόσια υγεία, που όμως μπορεί να επεκταθεί σε μία ευρύτερη γκάμα εφαρμογών, όπως αυτές για σημεία ελέγχου αεροδρομίων, σιδηροδρομικών σταθμών, ελέγχων επιβίβασης και πρόσβασης σε φυσικούς χώρους, εφαρμόζοντας του κανόνες κοινωνικής αποστασιοποίησης μεταξύ του ελεγκτή και του υποκειμένου του ελέγχου. Η προτεινόμενη προσέγγισή αξιοποιεί τις δυνατότητες των τεχνολογιών για ταυτότητες μίας χρήσης (Disposal Identities[44]), των τεχνολογιών Self-Sovereign Identities και των επαληθεύσιμων διαπιστευτηρίων (VC) για να επιτρέψει την επαλήθευση ενός ψηφιακού εγγράφου και τον έλεγχο πρόσβασης. Προς αυτήν την κατεύθυνση, εισάγουμε συγκεκριμένα την έννοια των «παραγώγων» (derivative) επαληθεύσιμων διαπιστευτηρίων δηλαδή, κωδικοποιημένα / με βάση τα στοιχεία από το ευρύτερο πεδίο της εφαρμογής. Ένα παράγωγο VC εγγυάται την εγκυρότητα και την κυριότητα των στοιχείων του, βασισμένο άλλα VC, αλλά η χρηστικότητα του περιορίζεται σε ένα πολύ συγκεκριμένο πλαίσιο (τοπικά και χρονικά) για την αλληλεπίδραση μεταξύ του υποκειμένου και μιας υπηρεσίας Παρόχου. Το παράγωγο VC συνδέεται με ένα συγκεκριμένο αποκεντρωμένο αναγνωριστικό (Pairwise DID).

[44] https://www.disposableidentities.eu/

10.1 Η επαλήθευση ψηφιακού εγγράφου και ο έλεγχος πρόσβασης βάσει διαπιστευτηρίων σε εξωτερικούς και εσωτερικούς χώρους την εποχή του COVID-19[45]

Το τελευταίο διάστημα με αφορμή την πανδημία του COVID-19 τέθηκε έντονα το ζήτημα της διερεύνησης - ιχνηλάτησης των επαφών που είχε κάποιο επιβεβαιωμένο κρούσμα της πανδημίας, προκειμένου να εντοπιστούν πιθανά άλλα κρούσματα που μπορεί να μεταδίδουν τον υιό έστω και αν δεν έχουν κάποια εμφανή συμπτώματα[46]. Στο πλαίσιο αυτό ξεκίνησε μία προσπάθεια για ψηφιακές εφαρμογές που θα μπορούσαν να συνεισφέρουν στην ιχνηλάτηση και παράλληλα ξεκίνησε μία συζήτηση για πιθανά ψηφιακά πιστοποιητικά που θα βεβαιώνουν την κατάσταση του φυσικού προσώπου είτε σε επίπεδο ασθένειας, είτε σε επίπεδο εμβολιασμού. Παράλληλα απαιτήθηκαν πολλαπλά έγγραφα ιδιαίτερα σε συνθήκες απαγόρευσης της κυκλοφορίας που να βεβαιώνουν την αναγκαιότητα μετακίνησης, να συμπληρώνουν τις πληροφορίες των ταξιδιωτικών εγγράφων και να θέτουν πρόσθετες προϋποθέσεις για καθημερινές δραστηριότητες. Η νέα πρόκληση είναι ότι όλα αυτά τα ψηφιακά έγγραφα θα πρέπει να ελέγχονται τηρώντας τους κανόνες κοινωνικής αποστασιοποίησης, απαιτώντας ο ελεγκτής να μην έρχεται σε επαφή με το υποκείμενο του ελέγχου.

Παρόλο που όπως αναφέρεται στο (Crocker, 2020) δεν είναι εφικτό να λύσουμε τα ζητήματα της πανδημίας δημιουργώντας την άριστη εφαρμογή, ωστόσο, καθώς αρκετές χώρες σε όλο τον κόσμο εφαρμόζουν σήμερα στρατηγικές εξόδου από την καθολική απαγόρευση κυκλοφορίας, η χρήση εφαρμογών ιχνηλάτησης περιστατικών του COVID-19 είναι ανάμεσα στις πολιτικές επιλογές που στοχεύουν στην προοδευτική επιστροφή στην ομαλότητα. Η τρέχουσα προσέγγιση για την ψηφιακή ανίχνευση επαφών χρησιμοποιεί τεχνολογίες Bluetooth για τον προσδιορισμό της εγγύτητας επαφών (proximity tracing)[47] οι οποίες μετρούν την ισχύ του σήματος Bluetooth για να προσδιορίσουν εάν δύο έξυπνές συσκευές (π.χ. smartphone) είναι αρκετά κοντά, χωρίς ωστόσο να αποκαλύπτεται η πραγματική ταυτότητα

[45] https://zenodo.org/record/4016977#.X7_fErPQBPY

[46] https://eody.gov.gr/wp-content/uploads/2020/03/covid-19-diaxeirisi-epafon.pdf

[47] Μια απλή προσέγγιση για την ιχνηλάτηση επαφών με χρήση τεχνολογιών προσδιορισμού εγγύτητας μπορεί κάποιος να δει το https://epic.org/privacy/covid/Rivest-Contact-Tracing.pdf,

των ατόμων που έρχονται σε επαφή λόγω της χρήσης εναλλασσόμενων ή προσωρινών αναγνωριστικών όπως π.χ. τα Ephemeral Ids (Hassidim, 2016). Σε γενικές γραμμές, μια εφαρμογή προσδιορισμού εγγύτητας θα πρέπει να ενημερώνει εάν οι χρήστες είχαν έρθει σε επαφή με κάποιο επιβεβαιωμένο κρούσμα. Σε αυτή τη κατεύθυνση είναι σημαντική η πρόσφατη συνεργασία των εταιριών Google και Apple για τη διαλειτουργικότητα μεταξύ συσκευών που έχουν λειτουργικό σύστημα από αυτές[48].

Ανεξάρτητα από τη σημερινή ουσιαστική ή όχι αποτελεσματικότητα των μεθόδων προσδιορισμού εγγύτητας, μπορεί κάποιος να ισχυριστεί ότι οι εφαρμογές ιχνηλάτησης επαφών ανήκουν στο πρώτο κύμα εφαρμογών για τη Δημόσια Υγεία με σκοπό τη μελέτη και παρακολούθηση της εξέλιξης των επιδημιών. Αναμένεται οι επόμενες εφαρμογές να έχουν αυξημένη πολυπλοκότητα και αξιοποιώντας σύγχρονες συσκευές, να αποφέρουν βελτιωμένη απόδοση στην ιχνηλάτηση επαφών (μέσω βελτιστοποιημένου προσδιορισμού της εγγύτητας και παρακολούθησης τοποθεσίας) και να συνδέονται άμεσα με τον ηλεκτρονικό φάκελο υγείας των πολιτών. Τέτοιες εφαρμογές μπορούν παρέχουν λειτουργίες ενημέρωσης του ηλεκτρονικού φακέλου υγείας, εντοπισμού περιοχών με αυξημένο χωρικό κινδύνο, έγκαιρη προειδοποίηση σε περίπτωση πιθανής λοίμωξης, προτάσεις για τη μείωση των κινδύνων μόλυνσης[49], κλπ.

Η McKinsey προβλέπει την άνοδο της «ανέπαφης» οικονομίας και την αύξηση του αυτοματισμού, όπου ακόμη και βασικές εργασίες που απαιτούν ανθρώπινη επαφή θα αυτοματοποιηθούν όσο το δυνατόν περισσότερο. Για πολλούς ανθρώπους, η επιστροφή στην καθημερινότητα περιλαμβάνει την επανεμφάνιση π.χ. πελατών στα καταστήματα, στα περίπτερα του δρόμου που είναι συνηθισμένα μεγάλο μέρος του κόσμου. Παρόλα αυτά η εικόνα δεν θα είναι όπως τη γνωρίζαμε, διότι κάποια από αυτά θα αντικατασταθούν ηλεκτρονικές υπεραγορές χωρίς μετρητά. Ακόμη και οι ασθενείς με

[48] https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/amp/

[49] Στο έργο Covid-Watch έχει γίνει ανάλυση μιας εφαρμογής για κινητά για τη μείωση της εξάπλωσης του COVID-19, που αποτελείται από δύο μέρη, την παρακολούθηση επαφών Bluetooth και τις προτάσεις χρηστών (https://www.covid-watch.org/covid_watch_whitepaper.pdf)

πολύπλοκες ανάγκες που απαιτείται να δουν τους γιατρούς τους προσωπικά θα αλλάξουν (πχ. βλέπε άυλη συνταγογράφηση στην Ελλάδα). Οι τάσεις είναι αδιαμφισβήτητες - και πιθανώς μη αναστρέψιμες[50].

Είναι προφανές ότι όλες αυτές οι υπηρεσίες θέτουν ζητήματα ισορροπίας μεταξύ της προστασίας της δημόσιας υγείας και προστασίας της ιδιωτικότητας των πολιτών[51].

Στόχος αυτού του τμήματος της ερευνητικής εργασίας είναι να προτείνει το σχεδιασμό ενός συστήματος υπηρεσιών που θα παρέχει στις εφαρμογές κινητής τηλεφωνίας υπηρεσίες για την αντιμετώπιση των ανωτέρω ζητημάτων των πανδημιών με τη δυνατότητα: α) να διαχειρίζονται άμεσα και να επαληθεύουν ψηφιακά έγγραφα του COVID-19 (βεβαιώσεις κυκλοφορίας, άδειες εργασίας ή ταξιδιού, πιστοποιητικά εμβολιασμού κ.λπ.) και β) για πραγματοποιούν έλεγχο βάσει διαπιστευτηρίων, ειδικά σε περιπτώσεις όπου το όργανο που επαληθεύει πρέπει να διατηρεί φυσική απόσταση από τον υποκείμενο του ελέγχου.

Ένα τέτοιο σύστημα πρέπει να διέπεται από προδιαγραφές υψηλής ασφάλειας, προκειμένου να υιοθετηθεί και οι υπεύθυνοι χάραξης πολιτικής να μπορέσουν να οργανώσουν με επιτυχία την επιστροφή στην εργασία. Από την άλλη οι επιχειρήσεις θα πρέπει να εφαρμόσουν ανέπαφους τρόπους οργάνωσης και λειτουργίας όπως π.χ. εξ΄ αποστάσεως έλεγχος για πρόσβαση στους χώρους της επιχείρησης, άδειες εργασίας ή ταξιδιού για το προσωπικό με ψηφιακά διαπιστευτήρια που εκδίδονται από υγειονομική αρχή, ανέπαφη επαλήθευση της ταυτότητας του πελάτη στο σημείο παροχής υπηρεσιών και εξυπηρέτησης πελατών κλπ[52].

---

[50] McKinsey, 2020, The future is not what it used to be: Thoughts on the shape of the next normal, https://www.mckinsey.com/featured-insights/leadership/the-future-is-not-what-it-used-to-be-thoughts-on-the-shape-of-the-next-normal

[51] Επισκόπηση των διαφορετικών πρωτοκόλλων διασφάλισης απορρήτου που χρησιμοποιούνται για τον εντοπισμό της έκθεσης COVID-19, https://isc.sans.edu/forums/diary/Privacy+Preserving+Protocols+to+Trace+Covid19+Exposure/26066/

[52] Η ομάδα εργασίας της πρωτοβουλίας Covid-19 Credential Initiative (https://www.covidcreds.com/) έχει περιγράψει αρκετές περιπτώσεις χρήσης ψηφιακών διαπιστευτηρίων για τον COVID-19, https://docs.google.com/document/d/14z7deFUHSI-x60KMLhF2FoxPIbCGmEMEJI0myr4g4dA/edit#.

10.1.1 Ταυτότητα μίας χρήσης

Η προστασία της ιδιωτική ζωή σε ένα τέτοιο περιβάλλον μπορεί να επιτευχθεί με τη χρήση ηλεκτρονικών ταυτοτήτων μίας χρήσης (Disposal Identities), και της επαλήθευσης των στοιχείων τους, δηλαδή στην περίπτωση μας των ψηφιακών εγγράφων για τον COVID-19 με χρήση επαληθεύσιμων διαπιστευτηρίων (Verifiable Credential) (βλέπε ενότητα 9.2). Με χρήση πρόσθετων ασφαλιστικών δικλείδων όπως, η έκδοση διαφορετικών μη συσχετισμένων αποκεντρωμένων αναγνωριστικών (DID) ανά άτομο και αποκεντρωμένους μηχανισμού κρυπτογραφίας, ένα τέτοιο σύστημα μπορεί να παρέχει ισχυρές εγγυήσεις για τη διασφάλιση του απορρήτου ενώ προωθεί τη βιωσιμότητα και την αποτελεσματικότητα στη χρήση.

Οι ταυτότητες μιας χρήσης είναι προσωρινές ταυτότητες που βασίζονται σε ιδιότητες ενσωματωμένες σε ένα έξυπνο συμβόλαιο[53] (smart contract) μεταξύ ενός παραλήπτη και ενός παρόχου μιας υπηρεσίας. Με την αξιοποίηση της αρχιτεκτονικής SSI, οι ταυτότητες μίας χρήσης είναι σε θέση να παρέχουν ανωνυμοποιημένες, σχεδόν σε πραγματικό χρόνο, επαληθεύσιμες και ταυτοποιήσιμες πληροφορίες. Αν οι εν λόγω πληροφορίες έχουν εκδοθεί από τον αρμόδιο φορέα τότε αναφερόμαστε στη χρήση επίσημων ταυτοτήτων μίας χρήσης (DYOI), δηλαδή ενός μοντέλου ταυτοτήτων μίας χρήσης με βάση την αρχιτεκτονική SSI και την υιοθέτηση της αρχής των DID επί των οποίων ένα άτομο έχει κυριότητα και έλεγχο.

Πρακτικά, ένα υποκείμενο δημιουργεί πολλαπλά διαπιστευτήρια «μίας χρήσης» προσανατολισμένα στο σκοπό που τα θέλει, τα οποία συνδέονται με διαφορετικά DID για τα οποία το υποκείμενο έχει την κυριότητα και τον έλεγχο. Ο όρος αποκεντρωμένο αναγνωριστικό (DID) χρησιμοποιείται για να περιγράψει ένα αναγνωριστικό που είναι δημόσια ανιχνεύσιμο χρησιμοποιώντας για παράδειγμα ένα κατανεμημένο καθολικό μητρώο (distributed ledger). Ωστόσο, ο δημόσιος χαρακτήρας ενός DID δεν παρέχει τη διευκολύνει στη συσχέτιση και προσδιορισμό της ταυτότητας του χρήστη. Δηλαδή οι χρήστες των DID δεν απαιτείται να αποκαλύπτουν τίποτα περισσότερο από τα σημεία που βρίσκονται τα DID και τα δημόσια

[53] με τη διευρυμένη έννοια του όρου

κρυπτογραφικά κλειδιά. Συγκεκριμένα, χρησιμοποιώντας Pairwise DID δηλαδή DID που αντιστοιχούν σε ένα VC[54], τα υποκείμενα μπορούν να δημιουργήσουν νέα DID, δυναμικά, και να επικοινωνήσουν με ασφάλεια και ιδιωτικά μία πληροφορία που δεν είναι εφικτό να συσχετιστεί με άλλες πληροφορίες, εξασφαλίζοντας από το σχεδιασμό την ιδιωτικότητα (privacy by design) του υποκειμένου. Μόνο το ίδιο το υποκείμενο μπορεί να κάνει τη συσχέτιση μεταξύ των διαφορετικών DID υπό την κυριότητα τους. Δηλαδή τα DID είναι πλήρως αποσυσχετισμένα.

Οι έννοια των επίσημων ταυτοτήτων μίας χρήσης επιτρέπει να ορίσουμε για συγκεκριμένες χρονικές περιόδους και συγκεκριμένες συνθήκες ταυτοποιητικά στοιχεία που θα βασίζουν την εγκυρότητα τους σε αξιόπιστες πηγές όπως π.χ. η ηλεκτρονική ταυτοποίηση του eIDAS ή άλλα σχήματα ταυτοποίησης. Οι επίσημες ταυτότητες μίας χρήσης υπονοούν, στην πραγματικότητα, ότι:

- Μπορούν να εκδοθούν από μια επίσημη αρχή, αλλά η διαχείριση τους γίνεται πλήρως από το υποκείμενο της ταυτότητας μέσω μιας εφαρμογής πορτοφολιού για έξυπνες συσκευές (π.χ. κινητά) που ανήκουν στους πολίτες και αποθηκεύονται εκεί σε κρυπτογραφημένη μορφή.
- Μπορούν να περιλαμβάνουν επίσημες προσωπικές πληροφορίες π.χ. για την υγεία, για την ιχνηλάτηση επαφών, να περιέχουν δεδομένα τοποθεσίας, που όμως είναι πλήρως αποσυσχετισμένα με τις προσωπικές (επίσημες) ταυτοποιήσιμες πληροφορίες του υποκειμένου (δεδομένα PII) ή το αναγνωριστικό της έξυπνης συσκευής.

Οι επίσημες ταυτότητες μιας χρήσης αποτελούν το βασικό μέρος μιας αρχιτεκτονικής πολλαπλών επιπέδων που επικεντρώνεται σε ψηφιακά έγγραφα και μπορεί να: α) διαχειριστεί την αποθήκευση και την παρουσίαση (για επαλήθευση) ψηφιακών εγγράφων και αδειών σχετικών με το COVID-19, β) παρέχει υποστήριξη για την ενσωμάτωση αποσπασματικών δεδομένων (όπως δεδομένα ιχνηλάτησης επαφών) σε νέα ψηφιακά έγγραφα που

[54] Τα Pairwise DID το W3C τα ονομάζει Peer DIDs στις προδιαγραφές του 2020, https://identity.foundation/peer-did-method-spec/

δημιουργεί και επεξεργάζεται, γ) επιτρέπει την αυτόματη επαλήθευση εγγράφων σε σημεία ελέγχου που βρίσκονται σε οποιοδήποτε χώρο, όπου ένας ελεγκτής με χρήση μιας συσκευής σαρώνει την οθόνη της έξυπνης συσκευής του υποκειμένου που προβάλει π.χ. ένα bar code ή QR code, χωρίς να απαιτείται επαφή μεταξύ ελεγκτή και υποκειμένου, διατηρώντας μια απόσταση ασφαλείας μεταξύ τους.

Ένα τέτοιος μηχανισμός μπορεί να καλύψει αρκετές περιπτώσεις επαλήθευσης εγγράφων και ελέγχου πρόσβασης σε φυσικό χώρο, διασφαλίζοντας παράλληλα την προστασία της ιδιωτικής ζωής του υποκειμένου και τη φυσική ασφάλεια των συμμετεχόντων στη διαδικασία ελέγχου (ελεγκτής και υποκείμενο ελέγχου). Στη συνέχεια θα μας απασχολήσει: α) η επαλήθευση ψηφιακού εγγράφου σε φυσικούς χώρους και εγκαταστάσεις, β) η εξουσιοδότηση πρόσβασης βάσει διαπιστευτηρίων μέσω φορητής έξυπνης συσκευής. Ο προτεινόμενος σχεδιασμός μπορεί να έχει εφαρμογή σε περιπτώσεις διαχείρισης μία κατάστασης για τη Δημόσια Υγεία όπως αυτή του Covid-19, αλλά μπορεί να έχει και ευρύτερη εφαρμογή σε διαφορετικές περιπτώσεις όπως σημεία ελέγχου αεροδρομίων και σιδηροδρομικών σταθμών, θεάτρων, γηπέδων κλπ.

Σε αυτό το επιχειρησιακό μοντέλο λειτουργίας, ο Ελεγκτή - Επαληθευτής είναι είτε ένα φυσικό πρόσωπο που κρατά μία έξυπνη συσκευή (π.χ. ένας υπεύθυνος ελέγχου) είτε μια συσκευή IoT. Και στις δύο περιπτώσεις απαιτούνται μέσα κατάλληλης παρουσίασης που να μπορούν να κατανοηθούν σωστά από τον παραλήπτη / επαληθευτή. Για αυτόν τον λόγο, πρέπει να χρησιμοποιηθεί ένα πρόσθετο επίπεδο επεξεργασίας, προκειμένου η επαλήθευση του SSI-VC να είναι σε θέση να αντιμετωπίσει αυτή την πρόσθετη απαίτηση. Πρακτικά αυτό συνεπάγεται ότι το πρωτότυπο επαληθεύσιμο διαπιστευτήριο που είναι σε ένα ασφαλές κυβερνο-φυσικό VC πρέπει να μετατραπεί σε ένα σε παράγωγο διαπιστευτήριο ανάλογα με το περιβάλλον της χρήσης το οποίο εκ’ προοιμίου είναι προσωρινό και άρα μίας χρήσης.

10.1.2 Παρουσίαση VC

Συγκεκριμένα, το σύστημα για να λειτουργήσει εισάγει μια υπηρεσία μετασχηματισμού του VC στην αρχιτεκτονική. Αυτό το νέο συστατικό της

αρχιτεκτονικής έρχεται σε επαφή με το πορτοφόλι του υποκειμένου για να δημιουργήσει ένα πολύ περιορισμένο (με την έννοια του χρόνου ζωής και του χώρου) ασφαλές διακριτικό. Αυτά τα διακριτικά μπορούν εύκολα να ερμηνευτούν τόσο από ανθρώπους όσο και από μηχανές. Ένα παράδειγμα τέτοιου διακριτικού θα μπορούσε να είναι ένας κωδικός QR, ένας 6ψήφιος αριθμός ή μια λέξη που επιλέγεται από μια προκαθορισμένη λίστα. Είναι σημαντικό να διευκρινιστεί ότι η εγκυρότητα αυτών των διακριτικών επηρεάζεται από το περιβάλλον τους, δηλαδή το πότε και πού χρησιμοποιούνται. Επειδή αυτά εξαρτώνται από το περιβάλλον εφαρμογής, η δημιουργία ενός τέτοιου διακριτικού για συγκεκριμένη λειτουργία από επαληθεύσιμα διαπιστευτήρια είναι πολύ πιο ασφαλές.

Ειδικότερα, όταν ένα υποκείμενο απαιτείται να παρουσιάσει ένα διαπιστευτήριο, η εφαρμογή του πορτοφολιού στην έξυπνη συσκευή του υποκειμένου, λαμβάνει ένα "Αίτημα αποκάλυψης VC" από έναν Ελεγκτή – Επαληθευτή. Στη συνέχεια ζητά από το υποκείμενο να συναινέσει στην αποκάλυψη του κατάλληλου διαπιστευτηρίου. Ο Ελεγκτής-Επαληθευτής επιβεβαιώνει την κυριότητα, την αυθεντικότητα και την εγκυρότητα του διαπιστευτηρίου που αποκάλυψε το υποκείμενο χωρίς να αποκαλύπτονται άλλες πληροφορίες σχετικά με αυτό. Εάν μια διαδικασία απαιτεί συγκεκριμένους τύπους διαπιστευτηρίων, όπως π.χ. διακριτικά βραχυχρόνιας διάρκειας (που περιγράφθηκαν παραπάνω), η έκδοση τους μπορεί να αντιμετωπιστεί με παρόμοιο τρόπο. Η μετατροπή των VC σε ειδικά διακριτικά μπορεί να γίνει από μία διαδικτυακή υπηρεσία, δηλαδή μια υπηρεσία που να μετασχηματίζει τα υπάρχοντα επαληθεύσιμα διαπιστευτήρια (VC) σε ένα κατάλληλο ασφαλές διακριτικό (παράγωγο διαπιστευτήριο) και το επιστρέφει στο πορτοφόλι του υποκειμένου. Με αυτόν τον τρόπο, ένα επαληθεύσιμο διαπιστευτήριο χρησιμοποιείται ως το κλειδί για τη δημιουργία ενός διακριτικού για σκοπούς φυσικής πρόσβασης ή πρόσβασης στον κυβερνοχώρο. Έχοντας λάβει αυτό το διακριτικό, το κινητό πορτοφόλι του υποκειμένου μπορεί να το χρησιμοποιήσει για να το παρουσιάσει σε διάφορες λειτουργίες και σενάρια χρήσης. Η επιβεβαίωση αυτών των διακριτικών πρόσβασης είναι απλή καθώς ο παραλήπτης χρειάζεται μόνο παραπομπή του ληφθέντος διακριτικού σε μια λίστα έγκυρων κωδικών που λαμβάνονται από

την υπηρεσία μετασχηματισμού VC. Οι κωδικοί QR, οι φράσεις/λέξεις (seed phrase[55]) και τα σήματα (πακέτα διαφήμισης - advertising packages) που βγάζουν συσκευές Bluetooth χαμηλής ενέργειας είναι οι πιθανές μορφές παρουσίασης στις οποίες πρέπει να μετασχηματιστούν τα επαληθεύσιμα διαπιστευτήρια, για την αντιμετώπιση των ειδικών αναγκών επαλήθευσης ψηφιακού εγγράφου και ελέγχου πρόσβασης σε φυσικό χώρο βάσει διαπιστευτηρίων.

10.1.3 Bluetooth χαμηλής Ενέργειας (Bluetooth Low Energy -BLE)

Το Bluetooth Low Energy (BLE) είναι μια ασύρματη τεχνολογία που χρησιμοποιείται σε πολλές εφαρμογές του IoT από έξυπνες πόλεις, έξυπνα σπίτια έως ηλεκτρονική υγεία κ.λπ. (Gomez et al, 2012). Ο τρόπος λειτουργίας του BLE είναι μέσω ενός συγκεκριμένου μοντέλου μετάδοσης: όταν είναι ενεργοποιημένη μια περιφερειακή συσκευή BLE, στέλνει περιοδικά πακέτα εκπομπής σε συγκεκριμένα κανάλια μετάδοσης για να υποδείξει σε άλλες συσκευές ότι είναι έτοιμη και έτοιμη να λάβει συνδέσεις (διαφημιστικά πακέτα). Ταυτόχρονα, μια άλλη συσκευή BLE ανιχνεύει τις συχνότητες του περιβάλλοντος χώρου («ακρόαση») για να εντοπίσει τις επερχόμενες δυνατότητα διασύνδεσης.

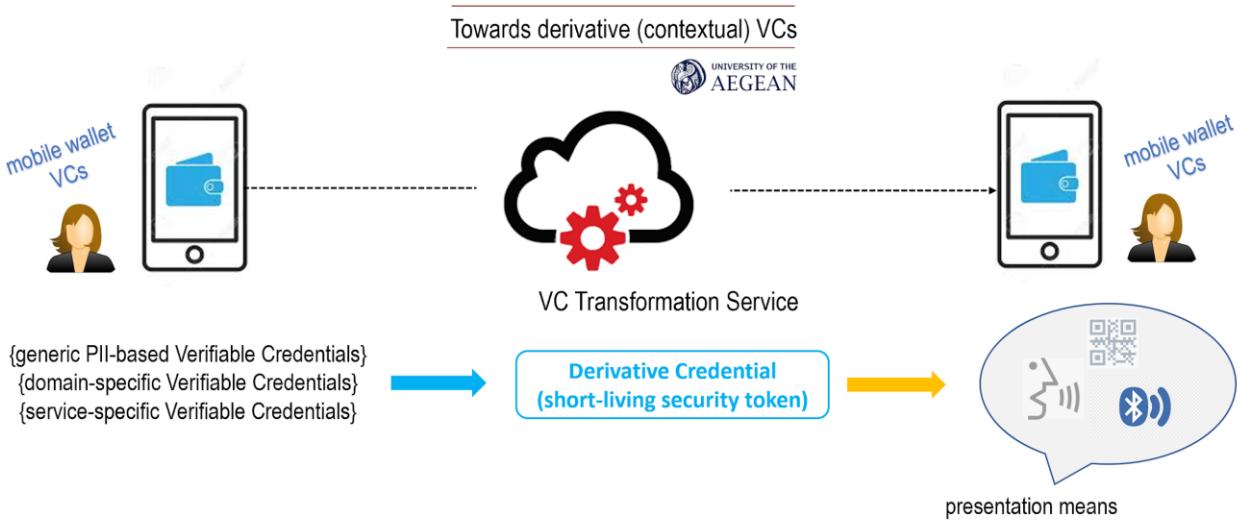
Με βάση τις προδιαγραφές για τα BLE, σχεδιάζουμε μια υπηρεσία ανταλλαγής δεδομένων χωρίς απαίτηση εγκατάστασης επικοινωνίας και διασύνδεση σε επίπεδο εφαρμογής που στέλνει σταματά και περιμένει "stop and waiting":

- Ένα τυπικό πακέτο δεδομένων εκπομπής BLE με μία στατική τιμή (UUID) 16 bytes στο αναγνωριστικό πακέτο του Bluetooth, το οποίο ενημερώνει τον παραλήπτη ότι αυτό το πακέτο εκπομπής χρησιμεύει ως πακέτο για δυαδική μεταφορά δεδομένων μεταξύ των δύο συσκευών.
- Ένα πακέτο μετάδοσης ACK (αναγνώρισης - acknowledgement) με μια συγκεκριμένη στατική τιμή UUID στο αναγνωριστικό πακέτο του Bluetooth, διαφορετική από εκείνη του τυπικού πακέτου BLE για τη μεταφορά δυαδικών δεδομένων, το οποίο ενημερώνει τον αποστολέα ότι αυτό το

[55] https://themerkle.com/what-is-a-mnemonic-seed/

πακέτο μετάδοσης είναι στην πραγματικότητα το πακέτο αναγνώρισης των προηγούμενων επιτυχημένων πακέτων για μετάδοση δεδομένων.

- Τα 2 bytes του πεδίο " Major value " του τυπικού πακέτου εκπομπής είναι η βασική μονάδα μεταφοράς της σχεδιασμένης υπηρεσίας, ενώ τα 2 byte του πεδίου δεδομένων "Minor value" χρησιμοποιούνται για να δηλώσουν ένα προσωρινό αναγνωριστικό περιόδου σύνδεσης (Ephemeral) και έναν αριθμό ακολουθίας για την αναγνώριση των πακέτων εκπομπής που θα ακοκλουθήσουν.
- Μια αντιστοίχιση των bit για την εφαρμογή του βασικού μηχανισμού ελέγχου ροής δεδομένων για το πρωτόκολλο μεταφοράς δεδομένων χωρίς εγκατάσταση διασύνδεσης. Τα 2 byte του πεδίου "Major value" συμπληρώνονται με ακέραιο αριθμό. Αντιστοιχείται στα ίδια bit με το κρυπτογραφημένο κομμάτι δεδομένων των 2 byte που αποθηκεύεται μέσα σε κάθε πακέτο μετάδοσης BLE. Παρομοίως, τα 2 byte του πεδίου " Minor value" συμπληρώνονται με ακέραιο αριθμό. Η δυαδική αναπαράστασή του περιέχει ένα μοναδικό τυχαίο αναγνωριστικό περιόδου σύνδεσης στα πρώτα οκτώ (8) bits και τον αριθμό ακολουθίας κάθε πακέτου συνεδρίας στα οκτώ τελευταία (8) bits.
- Αντίστοιχα, ένα πακέτο εκπομπής BLE ACK (αναγνώριση) μοιράζεται τις ίδιες ακέραιες τιμές των πεδίων Major value και Minor value με το πακέτο δεδομένων BLE του οποίου η λήψη αναγνωρίζεται.



Σχήμα 7: Παράγωγα επαληθεύσιμα διαπιστευτήρια

11 Συμπεράσματα

Μία σύγχρονη οικονομία που επιδιώκει να είναι ανταγωνιστική, προσπαθεί να επιτύχει τα μέγιστα δυνατά αποτελέσματα με χρήση των ελάχιστών κατά το δυνατόν πόρων (αρχή της οικονομικότητας). Υπό αυτή την έννοια η δημιουργία κοινών, επαναχρησιμοποιήσιμων υποδομών, υπηρεσιών και διαδικασιών αποτελεί ένα σύγχρονο στρατηγικό στόχο. Με αυτό το σκεπτικό μία επένδυση σε μία υποδομή που αναπτύσσεται μία φορά πρέπει να αξιοποιείται σε πολλαπλούς διαφορετικούς επιχειρησιακούς τομείς. Στο πλαίσιο αυτό η διαλειτουργικότητα έτσι όπως ορίστηκε στο Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας αποτελεί θεμέλιο λίθο μίας σύγχρονης οικονομίας αλλά και βασικό συστατικό στοιχείο για την αποδοτική και αποτελεσματική λειτουργία της δημόσιας διοίκησης και της οικονομίας.

Οι πρόσφατες εξελίξεις για τη Δημόσια Υγεία, κυρίως εξαιτίας του Covid-19 προώθησαν έντονα την ψηφιοποίηση των υπηρεσιών και των καθημερινών λειτουργιών προκειμένου να είναι εφικτή ή τήρηση των κανόνων κοινωνικής αποστασιοποίησης που επέβαλαν οι συνθήκες της πανδημίας.

Η δημιουργία διαλειτουργικών υπηρεσιών που αξιοποιούν υφιστάμενες υποδομές, υπηρεσίες και ανταλλάσσουν δεδομένα χωρίς να απαιτείται φυσική

αλληλεπίδραση μεταξύ των εμπλεκομένων, είναι προαπαιτούμενο για την ψηφιοποίηση της οικονομίας και της δημόσιας διοίκησης αλλά και απαίτηση για μία ανέπαφη οικονομία.

Το ψηφιακό περιβάλλον οφείλει να δημιουργεί ένα κλίμα εμπιστοσύνης που εδραιώνεται θεσμικά και ουσιαστικά σε αξιόπιστες πηγές που ελέγχονται από δημόσιες αρχές οι οποίες διαφυλάττουν το δημόσιο συμφέρον.

Η εμπιστοσύνη στις ψηφιακές συναλλαγές απαιτεί διαλειτουργικότητα στα ζητήματα ταυτοποίησης των οντοτήτων που συνεργάζονται αλλά και επιβεβαίωσης των ισχυρισμών του καθενός με την αξιοποίηση των πληροφοριών που υπάρχουν σε αρχεία αξιόπιστών και θεσμικών πηγών.

Όλα τα ανωτέρω πρέπει να γίνονται με προστασία της ιδιωτικότητας υπό τον πλήρη έλεγχο του χρήστη, ώστε στο μέλλον να μην δημιουργηθεί κάποιος υπερ-οργανισμός που θα ελέγχει όλα τα δεδομένα των χρηστών - πολιτών.

Η ανάπτυξη των ψηφιακών υπηρεσιών που να καλύπτουν τις ανωτέρω προϋποθέσεις απαιτούν εξειδικευμένες γνώσεις, ψηφιακές δεξιότητες και μεθοδολογίες όπως αναφέρεται στην ενότητα 2 και 8.2 της παρούσας εργασίας που απαιτεί αλληλεπίδραση σε επίπεδο πολιτικών και στρατηγικών επιλογών, θεσμικού πλαισίου και τεχνολογικών υποδομών.

Ο κανονισμός eIDAS δημιούργησε την υποδομή για την εδραίωση της εμπιστοσύνης σε ένα περιβάλλον διαλειτουργικότητας και ψηφιακών συναλλαγών (ενότητα 4 της παρούσας).

Παρόλα αυτά πολύ γρήγορα φάνηκε ότι τα δεδομένα ταυτότητας που εντάσσονται στο πλαίσιο του κανονισμού eIDAS δεν επαρκούν για στοιχειώδεις ψηφιακές συναλλαγές. Η διασυνδεδεμένες ταυτότητες είναι ο τρόπος όπου από τη μία αξιοποιείται το περιβάλλον εμπιστοσύνης του κανονισμού eIDAS αλλά και ειδικές τομεακού χαρακτήρα πληροφορίες που απαιτούνται για τη παροχή των ψηφιακών υπηρεσιών. Στην εν λόγω εργασία (ενότητα 9) διερευνήθηκε ως μελέτη περίπτωσης και προτάθηκε η εφαρμογή των διασυνδεδεμένων ταυτοτήτων στο πλαίσιο των αναγκών των ακαδημαϊκών

ιδρυμάτων αλλά και της ψηφιοποίησης των διαδικασιών προγράμματος Erasmus.

Δομικά στοιχεία της προτεινόμενη λύσης είναι η χρήση τεχνολογιών SSI και επαληθεύσιμων διαπιστευτηρίων που διασφαλίζουν τον πλήρη έλεγχο των ταυτοποιητικών στοιχείων από το ίδιο το χρήστη – φοιτητή και από την άλλη παρέχουν, μετά τη συγκατάθεση του χρήστη, τη δυνατότητα στο παραλήπτη αυτών να επιβεβαίωση την ορθότητας τους με επίσημο τρόπο μέσα από την αξιοποίηση του μηχανισμού εμπιστοσύνης του κανονισμού eIDAS με εγκεκριμένες ψηφιακές σφραγίδες του ακαδημαϊκού ιδρύματος προέλευσης και προηγμένες κρυπτογραφικές μεθόδους.

Η υιοθέτηση των τεχνολογιών SSI (Wang και De Filippi 2020), (van Bokkem et al, 2019) και των επαληθεύσιμων διαπιστευτηρίων για τον σχεδιασμό ενός αποκεντρωμένου πλαισίου διαχείρισης ακαδημαϊκής ταυτότητας ως υπηρεσίας σύνδεσης (Chadwick και Inman 2009), μετατρέπει τις διασυνδεδεμένες ταυτότητες σε αξιόπιστα συνδεδεμένα στοιχεία με χρήση του blockchain.

Τα στοιχεία αυτά μπορούν να διασυνδεθούν μόνο από τον ίδιο το χρήστη δηλαδή στοιχεία ταυτότητας με τα στοιχεία ακαδημαϊκών ιδιοτήτων.

Ειδικότερα λαμβάνοντας υπόψη ότι: α) τα υποχρεωτικά στοιχεία ταυτοποίησης (δηλαδή τα ελάχιστα δεδομένα για την ταυτοποίησης των φυσικών προσώπων) μπορούν να λαμβάνονται αυτόματα μέσω των ισχυρισμών (assertions) που βασίζονται στο πρωτόκολλο SAML που έχει υιοθετήσει ο κανονισμός eIDAS, β) τα Κράτη Μέλη εγγυώνται την αξιοπιστία των δεδομένων που παρέχονται μέσα από το δίκτυο του κανονισμού eIDAS, και γ) οι ακαδημαϊκές ιδιότητες δίνονται με έγκυρο τρόπο από τα Ακαδημαϊκά Ιδρύματα, το δίκτυο eduGAIN, την Ακαδημαϊκή Ταυτότητα (ESC) και το έργο EMPEX, δίνεται η δυνατότητα για ασφαλή διασύνδεση αυτών των δεδομένων και για αυτόματη συμπλήρωση διαδικτυακών φορμών που απαιτούνται π.χ. στο πρόγραμμα Erasmus, αποφεύγοντας χειροκίνητη εισαγωγή δεδομένων και ελαχιστοποιώντας έτσι τον κίνδυνο σφαλμάτων κατά την εισαγωγή προσωπικών ταυτοποιητικών πληροφοριών των φοιτητών στα πληροφοριακά

συστήματα των ΑΕΙ υποδοχής. Μεγαλύτερο όφελος προκύπτει για τους φοιτητές που προέρχονται Κράτη μέλη της ΕΕ και διαθέτουν τις δικές τους εθνικές ταυτότητες. Παραμένει το ζήτημα της θεσμικής αντιστοίχισης του επιπέδου βεβαιότητας για την ποιότητα της πληροφορίας που παρέχεται από τα Ακαδημαϊκά Ιδρύματα με αυτά του κανονισμού eIDAS (Quality Assurance Levels).

Η προτεινόμενη αρχιτεκτονική διασφαλίζει την ιδιωτικότητα αφού επιτρέπει στον χρήστη να διαχειρίζεται το πορτοφόλι των ταυτοποιητικών του στοιχείων, μέσα από μία διεπαφή που παρέχεται, είτε από μία διαδικτυακή υπηρεσία, είτε από την έξυπνη συσκευή του, συνδέοντας υπάρχοντα στοιχεία και δημιουργώντας καινούργια (όπως π.χ. ένα αναγνωριστικό εσωτερικού συστήματος που θα μπορούσε να διασυνδεθεί και να χρησιμοποιηθεί ως Ευρωπαϊκή Ταυτότητα Φοιτητή), ελέγχοντας επίσης ποιες πληροφορίες μπορεί να παραδοθούν και σε ποιον. Τέτοιου τύπου διεπαφές δίνουν τη δυνατότητα στο χρήστη να διαγράφει διασυνδέσεις και δημιουργεί νέες για συγκεκριμένη χρήση (υπο-προφίλ).

Λαμβάνοντας υπόψη αυτό το πλαίσιο σε μια προσπάθεια πανευρωπαϊκή αναγνώριση της ταυτότητας και της κατάστασης των φοιτητών, βασισμένη της αρχή «Μόνον Άπαξ», θα πρέπει να αναπτυχθεί μία νέα ψηφιακή υπηρεσία υποδομής από το πρόγραμμα CEF DSI για την αντιμετώπιση της ανάγκης για μία ενιαία ψηφιακή διασυνδεδεμένη ακαδημαϊκή ταυτότητα, με τη σύνδεση εθνικών ταυτοτήτων και ακαδημαϊκών αναγνωριστικών, σύμφωνα με τις ανάγκες των ΑΕΙ / Υπουργείων / φοιτητών στα Κράτη Μέλη. Αυτό θα συμβάλει στην επίτευξη του στρατηγικού στόχου για ψηφιακή εφαρμογή και εγγραφή σε οποιοδήποτε διαπιστευμένο ΑΕΙ στην Ευρώπη όταν κάποιος μετακινείται στο εξωτερικό για σπουδές, πρακτική άσκηση ή εργασία και αναμένεται να μειώσει τις διοικητικές διαδικασίες που απαιτούνται για την κινητικότητα.

Η ίδια υποδομή – αρχιτεκτονική προτάθηκε και στη μελέτη περίπτωσης της επιβεβαίωσης ψηφιακών εγγράφων που αφορούν την πανδημία του Covid-19. Η προσθήκη εδώ είναι ότι τα επαληθεύσιμα διαπιστευτήρια είναι περιορισμένης διάρκειας χρονικά και στο πλαίσιο συγκεκριμένου χώρου. Αυτό εισάγει την έννοια των ταυτοτήτων μια χρήσης που μετά από την επίτευξη του

σκοπού τους παύουν να ισχύουν και δεν μπορούν να επαναχρησιμοποιηθούν. Αυτό διασφαλίζει ακόμη περισσότερο την ιδιωτικότητα του χρήστη και δεν επιτρέπει το συνδυασμό των πληροφοριών που παρέχει ο χρήστης με άλλες πληροφορίες στο μέλλον.

Η μελέτη περίπτωσης για τους ελεγκτές ψηφιακών πιστοποιητικών για τις ανάγκες μίας πανδημίας αναδεικνύει την ανάγκη για ένα ακόμη δομικό στοιχείο που αναλαμβάνει τη μετατροπή των επαληθεύσιμων διαπιστευτηρίων σε μορφή που να είναι κατανοητή από έναν άνθρωπο ή και μία έξυπνη συσκευή (π.χ. QR code).

Συμπερασματικά η ανάπτυξη διαλειτουργικών υπηρεσιών με επαναχρησιμοποίηση δομικών στοιχείων που έχουν αναπτυχθεί για άλλο σκοπό είναι βασική στρατηγική και ο κανονισμός eIDAS είναι ένα τέτοιο παράδειγμα όπου εκτός από τις υπηρεσίες εμπιστοσύνης που αρχικά στόχευε, πλέον λειτουργεί καταλυτικά για την ανάπτυξη ενός οικοσυστήματος νέων υπηρεσιών τόσο από τη δημόσια διοίκηση όσο και από τον ιδιωτικό τομέα.

Οι σύγχρονες έξυπνες συσκευές πλέον ενσωματώνουν τεχνολογίες για την ασφαλή εκτέλεση των κρυπτογραφικών εργασιών που απαιτούνται σε κατάλληλο περιβάλλον (secure execution engine) ώστε να αποτελούν ένα ασφαλές πορτοφόλι για τον κάτοχο τους και υποκείμενο των δεδομένων.

Στο μέλλον αναμένονται πολλές νέες υπηρεσίες βασισμένες σε αυτές τις αρχές και στο πλαίσιο εμπιστοσύνης του κανονισμού eIDAS.

12 Δημοσιεύσεις από την Ερευνητική εργασία

Στο παρακάτω πίνακα φαίνονται οι επιστημονικές δημοσιεύσεις που προέκυψαν από αυτή την ερευνητική εργασία με χρονολογική σειρά.

Άρθρο	**HM/NIA**	**Διεθνές συνέδριο η περιοδικό**
Blended Learning and Open Courseware for	10-12-2019	E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age,

Promoting Interoperability in Public Services,		https://link.springer.com/chapter/10.1007/978-3-030-37545-4_6
Disposable Yet Official Identities (DYOI) for Privacy-Preserving System Design The case of COVID-19 digital document verification and credential-based access control in ad hoc outdoor and indoor settings (and beyond)	16-09-2020	Data for Policy 2020 5th International Conference https://dataforpolicy.org/data-for-policy-2020/
Adapting national interoperability frameworks beyond EIF 3.0: the case of Greece,	23-09-2020	ICEGOV'20, September 23–25, 2020, Athens, Greece, https://dl.acm.org/doi/10.1145/3428502.3428536
Advanced digital skills towards interoperable e-government services –	11-10-2020	International Journal of Electronic Governance Υποβλήθηκε και είναι υπό αξιολόγηση https://www.inderscience.com/jhome.php?jcode=ijeg

European and Greek case studies		
Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies	11-11-2020	European Journal of Higher Education IT 2020-1 https://www.eunis.org/erai/2020-1/

13 Βιβλιογραφία – Αναφορές

1) European Commission (2004), EIF - European Interoperability Framework for pan-European eGovernment services, European Communities, https://wayback.archive-it.org/12090/20121103055400/http://ec.europa.eu/idabc/en/document/3473.html
2) European Commission (2010), European Interoperability Framework (EIF) for European Public Services, COM(2010) 744 final annex 2, https://ec.europa.eu/isa2/sites/isa/files/isa_annex_ii_eif_en.pdf
3) European Commission (2010b), Towards interoperability for European public services, COM(2010) 744 final, https://eur-lex.europa.eu/resource.html?uri=cellar:f132547a-7d66-4626-8eb6-9f7428394de7.0017.03/DOC_1&format=PDF
4) European Telecommunications Standards Institute, (2012), ETSI Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile ETSI TS 103171 v.2.1.1.
5) European Telecommunications Standards Institute, (2013a), ETSI Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile ETSI TS 103173 v.2.2.1
6) European Telecommunications Standards Institute, (2013b), ETSI Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile ETSI TS 103172 v.2.2.2.
7) European Telecommunications Standards Institute, (2013c), ETSI Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile ETSI TS 103174 v.2.2.1
8) European Union (2014), Regulation (EU) 2014/910 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ECEU 910/2014 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN,
9) eIDAS Observatory (2015), The implementing acts of the eIDAS regulation https://ec.europa.eu/futurium/en/content/eidas-implementing-acts,

10) European Commission (2015a), Commission implementing decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D0296&from=MT,

11) European Commission (2015b), Commission implementing regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R1501,

12) European Commission (2015c), Commission implementing regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN

13) European Commission (2015d), Commission implementing decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_289_R_0007 ,

14) European Commission (2015e), Commission implementing regulation (EU) 2015/806 of 22 May 2015 laying down specifications relating to the form of the EU trust mark for qualified trust services http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R0806&from=EN

15) European Commission (2015f), Commission implementing decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015D1505&from=en

16) European Commission (2015g), Commission implementing decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015D1506

17) European Commission (2015h), Get Started with eID https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Get+Started+eID

18) European Union (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj,

19) European Commission (2016a), Commission implementing decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal markethttp://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016D0650

20) European Commission. (2016b). European Commision-DIGIT, eIDAS-Node Installation, Configuration and Integration Manual, available at https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+version+2.3.1#

21) European Commission (2017), Communication on The European Interoperability Framework- Implementation Strategy COM (2017) 134 Annex

2, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017DC0134,

22) European Union (2017), Commission implementing regulation 2016/7 establishing the standard form for the European Single Procurement Document, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0007,

23) European Commission (2018), The role of eGovernment and Interoperability in the European Semester process, ISA2 Programme, DIGIT, European Union, 2018

24) European Commission (2018b) eGovernment in Greece, ISA^2, https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Greece_2018_0.pdf

25) Ευρωπαϊκή Ένωση (2018), Κανονισμός (ΕΕ) 2018/1724 για τη δημιουργία ενιαίας ψηφιακής θύρας με σκοπό την παροχή πρόσβασης σε πληροφορίες, σε διαδικασίες και σε υπηρεσίες υποστήριξης και επίλυσης προβλημάτων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1024/2012

26) European Comission (2019), The Digital Economy and Society Index (DESI), https://ec.europa.eu/digital-single-market/en/desi,

27) European Comission (2019b), Digital Single Market, https://ec.europa.eu/digital-single-market/en,

28) OECD (2019), Methodological Framework of the Principles of Public Administration, http://www.sigmaweb.org/publications/Methodological-Framework-for-the-Principles-of-Public-Administration-May-2019.pdf,

29) Lindquist E., Wanna J. (2015), Is Implementation only about policy execution? Advice for Public Sector Leaders from the literature', Semantic Scholar, https://www.semanticscholar.org/paper/'Is-Implementation-only-about-policy-execution-for-Lindquist-Wanna/7b4b30eb8f2e4f9f887b86ce96063e2ba997f0d5,

30) Kubicek H., Cimander R. (2009), Three dimensions of organizational interoperability. Insights from recent studies for improving interoperability frame-works, European Journal of ePractice, https://pdfs.semanticscholar.org/e577/473a84b71fda605b04aa64a65d95d96fd596.pdf,

31) EIRA (2019), Public Policy Implementation approach ABB is https://joinup.ec.europa.eu/taxonomy/term/http_e_f_fdata_ceuropa_ceu_fdr8_fPublicPolicyImplementationApproach,

32) The Open Group (2018), The Open Group Architecture Framework (TOGAF® v9.2), https://www.opengroup.org/,
33) Pardo T., Burke B. (2008), Improving Government Interoperability: A capability framework for government managers, ResearchGate, https://www.researchgate.net/publication/237532560,
34) Scholl, H. J., & Klischewski, R. (2007), E-Government Integration and Interoperability: Framing the Research Agenda, Intl Journal of Public Administration, 30: 889–920, 2007, https://www.researchgate.net/publication/232918178
35) Papastylianou A., Stasis A., Rantos K., Kalogirou V., (2020), Blended Learning and Open Courseware for Promoting Interoperability in Public Services, Published in: E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age,
36) Kalogirou V., Stasis A., Charalabidis Y., (2020), Adapting national interoperability frameworks beyond EIF 3.0: the case of Greece, ICEGOV'20, September 23–25, 2020, Athens, Greece, Association for Computing Machinery, ACM, https://dl.acm.org/doi/10.1145/3428502.3428536
37) Stasis A., Triantafyllou N., Georgakopoulos P., Armitt Little. R., Kavassalis P., Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies, European Journal of Higher Education IT 2020-1, ISSN 2519-1764, https://www.eunis.org/erai/2020-1/
38) Klobučar T. (2019), "Facilitating Access to Cross-Border Learning Services and Environments with eIDAS", Learning and Collaboration Technologies. Ubiquitous and Virtual Environments for Learning and Collaboration, International Conference on Human-Computer Interaction pp 329-342, June 2019
39) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
40) Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
41) European Commission (2018), CEF eID Building Block for Banking and Educational Domains, Architectural Solution Document (eStudent) with recommendations, Deliverable March 2018

42) E. Torroglosa, J. Ortiz, A. Skarmeta (2018), "Matching federation identities, the eduGAIN and STORK approach", in Future Generation Computer Systems Volume 80, pp. 126-138, March 2018
43) E. Birrell and F. B. Schneider (2013), "Federated Identity Management Systems: A Privacy-Based Characterization", in IEEE Security & Privacy, vol. 11, no. 5, pp. 36-48, Sept.-Oct. 2013
44) D. van Bokkem et al (2019), "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology", available at https://arxiv.org/pdf/1904.12816.pdf
45) A. Mühle et al (2018), "A survey on essential components of a self-sovereign identity", https://arxiv.org/pdf/1807.06346.pdf
46) F. Wang and P. De Filippi (2020), "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full
47) P. Coelho et al (2018), "Federation of Attribute Providers for User Self-Sovereign Identity", in Journal of Information Systems Engineering & Management, vol. 3 (4), pp.32, 2018
48) S. Pal et al (2019), "On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation", in IEEE Internet of Things Journal, pp.1-1
49) S. Jung (2017). Personal OAuth authorization server and push OAuth for Internet of Things, in International Journal of Distributed Sensor Networks, 13(6), p.155014771771262
50) Q. Stokkink and J. Pouwelse (2018), "Deployment of a Blockchain-Based Self-Sovereign Identity", in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1336-1342
51) Chadwick D. W. and Inman G. (2009), "Attribute Aggregation in Federated Identity Management", in Computer, vol. 42, no. 5, pp. 33-40, May
52) Ferdous M. S. et al (2019), "In Search of Self-Sovereign Identity Leveraging Blockchain Technology", in IEEE Access, vol. 7, pp. 103059-103079
53) Hammudoglu J.S. et al (2017), "Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems", available at https://arxiv.org/abs/1706.03744
54) Lagutin D. et al. (2019), "Enabling Decentralised Identifiers and Verifiable Credentials for Constrained Internet-of-Things Devices using OAuth-based Delegation", in Workshop on Decentralized IoT Systems and Security (DISS), San Diego, CA, available at: https://www.ndss-symposium.org/wp-content/uploads/DISS2019-proceedings-front-matter.pdf

55) Self-ssi.com (2020), “esatus SeLF - Enables Self-Sovereign Identities (SSI) and empowers legacy & SSI-native IT systems”, available at: https://self-ssi.com/en/#aboutus
56) Diebold Z. (2017), «Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain», Master in Computer Science. University of Dublin, Trinity College
57) Palomares A. (2019), “The next Identity Management evolution: Self Sovereign Identity”, Atos, aailable at https://atos.net/en/blog/the-next-identity-management-evolution-self-sovereign-identity
58) Wang J. (2018), “Single Sign-on using OAuth2 and JWT for Distributed Architecture”, available at https://insready.com/en/blog/single-sign-using-oauth2-and-jwt-distributed-architecture
59) Allen C. (2016), “Self-Sovereign Identity Principles”, available at https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-Identity-principles.md
60) European Commission (2020), “SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market”, Dr. Ignacio Alamillo Domingo
61) ETSI (2020), Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services,
62) Kavassalis P., Triantafyllou N., Georgakopoulos P., Stasis A., Kranenburg R., (2020) Disposable Yet Official Identities (DYOI) for Privacy-Preserving System Design. The case of COVID-19 digital document verification and credential-based access control in ad hoc outdoor and indoor settings (and beyond) https://dataforpolicy.org/data-for-policy-2020/
63) Crocker A. et al, 2020, The Challenge of Proximity Apps For COVID-19 Contact Tracing, Electronic Frontier Foundation available at https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing
64) Hassidim A. et al, 2016, Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats to BLE Beacons, available at https://developers.google.com/beacons/eddystone-eid-preprint.pdf
65) Gomez C., Oller J., Paradells J., (2012), Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology, Sensors/MDPI, https://www.mdpi.com/1424-8220/12/9/11734/pdf