ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Προηγμένα Συστήματα Πληροφορικής – Ανάπτυξη Λογισμικού και Τεχνητής Νοημοσύνης

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Εξατομίκευση ταυτότητας με χρήση blockchain.** **Personalized ID using European Blockchain InfraStructure.**
Ονοματεπώνυμο Φοιτητή	**Θεοφυλάκτου Διονυσία**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΣΠ19015**
Επιβλέπων	**Ευάγγελος Σακκόπουλος, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Νοέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

Ευάγγελος Σακκόπουλος Αναπληρωτής Καθηγητής	Ευθύμιος Αλέπης Αναπληρωτής Καθηγητής	Διονύσιος Σωτηρόπουλος Επίκουρος Καθηγητής

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος Εικόνων 4

Κατάλογος Διαγραμμάτων 5

Κατάλογος Πινάκων 6

ΠΕΡΙΛΗΨΗ 7

ABSTRACT 8

1. Εισαγωγή 9

2. Επεξήγηση Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI) 12

2.1 Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials) 12

2.2 Εφαρμογές των επαληθεύσιμων διαπιστευτηρίων**.** 13

2.3 EBSI Use Case Lifecycle 14

3. Λειτουργία των επαληθεύσιμων διαπιστευτηρίων (Verifiable Credentials) 16

3.1 Η λειτουργία των επαληθεύσιμων διαπιστευτηρίων (Verifiable Credentials) 16

3.2 Αποκεντρωμένο αναγνωριστικό W3C (DID) 17

3.3 Μέθοδος Decentralized Identifiers (DID) 18

3.3.1 Λειτουργία της μεθόδου DID για Νομικά Πρόσωπα (LE) 19

3.3.2 Λειτουργία της μεθόδου DID για για φυσικά πρόσωπα (NP) 20

3.4 Έγγραφο DID από τεχνική άποψη 20

3.4.1 Το Δημόσιο ή ιδιωτικό κλειδί και η χρήση του 21

3.4.2 Μητρώο καταχώρισης DID / Επαληθεύσιμο μητρώο DID 21

4. Προσέγγιση της Αυτοκυριαρχικής ταυτότητας (Self-Sovereign Identity) 22

4.1 Οι προσεγγίσεις για την ψηφιακή ταυτότητα 22

4.2 Εθνική Προσέγγιση 22

4.3 Ομοσπονδιακή Προσέγγιση 23

4.4 Προσέγγιση της Αυτοκυριαρχικής ταυτότητας 24

4.5 Διαχείριση ταυτότητας με χρήση πορτοφολιών 25

5. Επεξηγημένα μοντέλα εμπιστοσύνης EBSI 26

5.1 Issuers Trust Montel 26

5.1.1 Το κλασικό μοντέλο εμπιστοσύνης για τους εκδότες 26

5.1.2 Ένα νέο μοντέλο εμπιστοσύνης για τους εκδότες 26

5.1.3 Βασικοί παράγοντες του Μοντέλου Εμπιστοσύνης Εκδοτών της EBSI 27

5.1.3.1 Trusted Accreditation Organisation (TAO) 27

5.1.3.2 EBSI Ledger 27

5.1.3.3 Trusted Issuers (TI) 28
5.2 Trust anchoring 28
5.3 Παραδείγματα Ιεραρχίας 31
5.3.1 Απλή αλυσίδα εμπιστοσύνης με νομικά πρόσωπα που εκπληρώνουν πολλαπλούς ρόλους (Trusted Accreditation AND Attestation Issuers) 32
5.3.2 Ένταξη σε Νομικό Πρόσωπο 33
5.3.3 Διαπίστευση Νομικού Προσώπου - Νομικό Πρόσωπο Ανωτάτου Επιπέδου 33
5.3.4 Νομικά Πρόσωπα Υποεπιπέδου 34
6. OpenID για επαληθεύσιμα διαπιστευτήρια 36
6.1 Το OpenID για τα επαληθεύσιμα διαπιστευτήρια η σημασία τους 36
6.2 Λειτουργία OpenID για τα επαληθεύσιμα διαπιστευτήρια 37
6.2.1 OpenID για επαληθεύσιμη έκδοση διαπιστευτηρίων 37
6.3 Πορτοφόλι και επαληθεύσιμα διαπιστευτήρια 39
6.3.1 Αίτημα Ελέγχου ταυτότητας 39
6.3.2 Επαληθεύσιμη παρουσίαση 40
7. Υλοποίηση λειτουργιών που αφορούν την διαδικασία των επαληθεύσιμων διαπιστευτηρίων ***..... 42***
7.1 DID RESOLVER 43
7.2 SIOP Authentication 45
7.3 Verifiable Credential 54
ΒΙΒΛΙΟΓΡΑΦΊΑ 59
ΑΝΑΦΟΡΈΣ ΕΙΚΟΝΩΝ 60
ΑΝΑΦΟΡΕΣ ΔΙΑΓΡΑΜΜΑΤΩΝ 61

Κατάλογος Εικόνων

Εικόνα 1 Self-sovereign scenario (European Commission,2022)....13
Εικόνα 2 Κατανομή ρόλων στα κράτη μέλη (European Commission,2022)....14
Εικόνα 3 Σενάριο χρήσης διπλωμάτων (European Commission,2022)....15
Εικόνα 4 Μέρη του DID (European Commission,2022)....17
Εικόνα 5 Παράδειγμα Επαληθεύσιμων Διαπιστευτηρίων (European Commission,2022)....18
Εικόνα 6 Δημιουργία DID (European Commission,2022)....19
Εικόνα 7 Παράδειγμα DID document (European Commission,2022)....20
Εικόνα 8 Παράδειγμα Εθνικής Προσέγγισης (European Commission,2022)....23
Εικόνα 9 Παράδειγμα Ομοσπονδιακής Προσέγγισης (European Commission,2022)....23
Εικόνα 10 Τρόπος λειτουργίας Προσέγγιση της Αυτοκυριαρχίας (European Commission,2022)....25
Εικόνα 11 Αίτημα Ελέγχου Ταυτότητας....39
Εικόνα 12 Επαληθεύσιμη Παρουσίαση....41
Εικόνα 13 DID Document....44
Εικόνα 14 Δημιουργία Request....46
Εικόνα 15 Πιστοποίηση Authentication Request....47
Εικόνα 16 Απάντηση Authentication Request....48
Εικόνα 17 Το συμβαλλόμενο μέλος επαληθεύει την απάντηση....50
Εικόνα 18 Access token....51
Εικόνα 19 Πιστοποίηση της απάντηση και λήψη access token....52
Εικόνα 20 Πιστοποίηση access token....53

Κατάλογος Διαγραμμάτων

Διάγραμμα 1 (European Commission,2022)..... 31
Διάγραμμα 2 (European Commission,2022)..... 32
Διάγραμμα 3 (European Commission,2022)..... 33
Διάγραμμα 4 (European Commission,2022)..... 34
Διάγραμμα 5 (European Commission,2022)..... 35

Κατάλογος Πινάκων

Πίνακας 1 Διαφορές Μεθόδων Did 18
Πίνακας 2 Σύγκριση μοντέλων εμπιστοσύνης με το μοντέλο εμπιστοσύνης EBSI 27
Πίνακας 3 Registered on the EBSI ledger 28
Πίνακας 4 Trust anchoring 29

ΠΕΡΙΛΗΨΗ

Η Ευρωπαϊκή Ένωση πρόκειται να εισαγάγει μια Ευρωπαϊκή Ψηφιακή Ταυτότητα που θα είναι διαθέσιμη σε όλους τους πολίτες και τις επιχειρήσεις της ΕΕ. Αυτό θα έχει τεράστιο αντίκτυπο στον τρόπο με τον οποίο οι πολίτες και οι επιχειρήσεις αλληλοεπιδρούν στο διαδίκτυο. Οι μεγάλες εταιρείες τεχνολογίας υπαγορεύουν, επί του παρόντος, τον τρόπο που χρησιμοποιούνται οι ψηφιακές ταυτότητες. Ως αποτέλεσμα, έχουν συγκεντρώσει μεγάλο αριθμό ιδιωτικών δεδομένων από τους χρήστες. Κινήματα όπως το Self-Sovereign Identity στοχεύουν να δώσουν στους χρήστες τον έλεγχο της διαδικτυακής τους ταυτότητας. Το TrustVault είναι το πρώτο πορτοφόλι δεδομένων που δίνει στους χρήστες τον έλεγχο της ταυτότητάς τους και όλων των δεδομένων τους. Το TrustVault επιτρέπει στους χρήστες να αποθηκεύουν όλα τα δεδομένα τους στα smartphone τους και να ελέγχουν με ποιον τα μοιράζονται. Ο χρήστης έχει λεπτομερή έλεγχο πρόσβασης που βασίζεται σε επαληθεύσιμα διαπιστευτήρια του χρήστη. Το EBSI συνδέει το TrustVault με το Ευρωπαϊκό Πλαίσιο Αυτοκυριαρχικής Ταυτότητας που επιτρέπει στους χρήστες να χρησιμοποιούν Επαληθεύσιμα Διαπιστευτήρια από δημόσιους και ιδιωτικούς φορείς στις πολιτικές ελέγχου πρόσβασής τους. Στην παρούσα εργασία περιγράφεται ο τρόπος λειτουργίας της ταυτοποίησης επαληθεύσιμων διαπιστευτηρίων με βάση την τεχνολογία του blockchain που αναπτύσσεται από την Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain. Για το σκοπό αυτών υλοποιήθηκαν μια σειρά από λειτουργίες που αφορούν την διαδικασία των επαληθεύσιμων διαπιστευτηρίων.

ABSTRACT

The European Union is on course to introduce a European Digital Identity that will be available to all EU citizens and businesses. This will have a huge impact on how citizens and businesses interact online. Big Tech companies currently dictate how digital identities are used. As a result, they have amassed vast amounts of private user data. Movements like Self-Sovereign Identity aim to give users control over their online identity. TrustVault is the first data wallet that gives users back control of their identity and all their data. TrustVault allows users to store all their data on their smartphones and control with whom they share it. The user has finegrained access control based on verifiable user attributes. EBSI connects TrustVault to the European Self-Sovereign Identity Framework allowing users to use Verifiable Credentials from public and private institutions in their access control policies. In the present study describes the operation of the identification of verifiable credentials based on the blockchain technology developed by the European Blockchain Services Infrastructure. For this purpose, a series of functions related to the process of verifiable credentials were implemented.

1. Εισαγωγή

Το EBSI (European Blockchain Services Infrastructure- Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain) είναι μια κοινή πρωτοβουλία της Ευρωπαϊκής Επιτροπής και της EBP (European Blockchain Partnership - Ευρωπαϊκή Συνεργασία Blockchain). Το όραμα του EBSI είναι να αξιοποιήσει την τεχνολογία blockchain για να επιταχύνει τη δημιουργία διασυνοριακών υπηρεσιών των δημόσιων διοικήσεων και των συστημάτων τους. Από το 2020, η EBSI αναπτύσσει ένα δίκτυο κατανεμημένων κόμβων σε όλη την Ευρώπη, υποστηρίζοντας εφαρμογές για επιλεγμένες περιπτώσεις χρήσης.

Η τεχνολογία Blockchain βρίσκεται στον πυρήνα του ψηφιακού μέλλοντος της Ευρώπης. Η Ε.Ε. θέλει να ηγηθεί στην καινοτομία του blockchain αξιοποιώντας την ως βάση για σημαντικές πλατφόρμες, εφαρμογές και εταιρείες.

Η τεχνολογία αυτή επιτρέπει σε άτομα και οργανισμούς που ενδέχεται να μην συνδέονται ή να μην εμπιστεύονται ο ένας τον άλλον να συμφωνούν συλλογικά και να καταγράφουν μόνιμα πληροφορίες χωρίς την εξάρτηση από ένα τρίτο μέρος. Η αξιοπιστία των δεδομένων επιτυγχάνεται με τρόπο που δεν ήταν δυνατόν να προκύψει στο παρελθόν. Η τεχνολογία blockchain έχει τη δυνατότητα να φέρει επανάσταση στον τρόπο με τον οποίο μοιραζόμαστε πληροφορίες και πραγματοποιούμε συναλλαγές στο διαδίκτυο.

Για την επίτευξη των στόχων της, η στρατηγική της Ευρωπαϊκής Επιτροπής έχει καθορίσει βασικές προτεραιότητες:

i. Περιβαλλοντική βιωσιμότητα: Η τεχνολογία blockchain πρέπει να είναι βιώσιμη και ενεργειακά αποδοτική.
ii. Προστασία δεδομένων: Η τεχνολογία Blockchain θα πρέπει να είναι συμβατή με τους ισχυρούς κανονισμούς προστασίας δεδομένων και απορρήτου της Ευρώπης και όπου είναι δυνατόν να υποστηρίζεται.

iii. Ψηφιακή Ταυτότητα: Η τεχνολογία Blockchain θα πρέπει να σέβεται και να βελτιώνει το εξελισσόμενο πλαίσιο ψηφιακής ταυτότητας της Ευρώπης. Αυτό περιλαμβάνει τη συμβατότητα με κανονισμούς ηλεκτρονικής υπογραφής, όπως το eIDAS, και την υποστήριξη ενός λογικού, ρεαλιστικού αποκεντρωμένου και αυτοκυριάρχου πλαισίου ταυτότητας.
iv. Κυβερνοασφάλεια: Η τεχνολογία Blockchain θα πρέπει να είναι σε θέση να παρέχει υψηλά επίπεδα ασφάλειας στον κυβερνοχώρο.
v. Διαλειτουργικότητα: Θα πρέπει να εξασφαλίζεται η διαλειτουργικότητα μεταξύ των νέων και των παλαιών συστημάτων.

1.1 Η European Blockchain Partnership (EBP), μια βασική πρωτοβουλία για την ανάπτυξη της στρατηγικής της ΕΕ για το blockchain

Στις 10 Απριλίου 2018, 21 κράτη μέλη και η Νορβηγία συμφώνησαν να υπογράψουν μια Διακήρυξη για τη δημιουργία της Ευρωπαϊκής Συνεργασίας Blockchain (EBP) και να συνεργαστούν για τη δημιουργία μιας Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI) που θα υποστηρίζει την παροχή κοινών διασυνοριακών ψηφιακών υπηρεσιών, με τα υψηλότερα πρότυπα ασφάλειας και ιδιωτικότητας. Έκτοτε, οκτώ ακόμη χώρες έχουν προσχωρήσει στην εταιρική σχέση, ανεβάζοντας τον συνολικό αριθμό των υπογραφόντων σε 30.

Στο μέλλον, όλες οι δημόσιες υπηρεσίες θα χρησιμοποιούν τεχνολογία blockchain. Το Blockchain είναι μια εξαιρετική ευκαιρία για την Ευρώπη και τα κράτη μέλη να επανεξετάσουν τα συστήματα πληροφοριών τους, να προωθήσουν την εμπιστοσύνη των χρηστών και την προστασία των προσωπικών δεδομένων, να βοηθήσουν στη δημιουργία νέων επιχειρηματικών ευκαιριών και να δημιουργήσουν νέους τομείς ηγεσίας, προς όφελος των πολιτών, των δημόσιων υπηρεσιών και των επιχειρήσεων. Η εταιρική σχέση που ξεκίνησε σήμερα δίνει τη δυνατότητα στα κράτη μέλη να συνεργαστούν με την Ευρωπαϊκή Επιτροπή για να μετατρέψουν τις τεράστιες δυνατότητες της τεχνολογίας blockchain σε καλύτερες υπηρεσίες για τους πολίτες

Από τον Απρίλιο του 2018, η Σύμπραξη πραγματοποιεί μηνιαίες συναντήσεις με στόχο την ανάπτυξη μιας αξιόπιστης, ασφαλούς και ανθεκτικής Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI) που πληροί τα υψηλότερα πρότυπα όσον αφορά το απόρρητο, την ασφάλεια στον κυβερνοχώρο, τη διαλειτουργικότητα και την ενεργειακή απόδοση. Η φιλοδοξία της εταιρικής σχέσης είναι να καταστήσει αυτή την αξιόπιστη υποδομή προσβάσιμη για την υποστήριξη ψηφιακών υπηρεσιών που αναπτύσσονται από δημόσιους και τελικά στο μέλλον και ιδιωτικούς φορείς.

Τον Δεκέμβριο του 2019, η Ευρωπαϊκή Επιτροπή ξεκίνησε επίσης μια διαβούλευση ανοιχτής αγοράς για την προετοιμασία της ευρωπαϊκής προ-εμπορικής προμήθειας blockchain που αναζητά νέες, βελτιωμένες λύσεις blockchain για τη μελλοντική εξέλιξη της Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain.

1.2 Η Ευρωπαϊκή Υποδομή Υπηρεσιών Blockchain

Το Πρόγραμμα Ψηφιακής Ευρώπης (DIGITAL) είναι ένα νέο πρόγραμμα χρηματοδότησης της ΕΕ που επικεντρώνεται στην παροχή ψηφιακής τεχνολογίας σε επιχειρήσεις, πολίτες και δημόσιες διοικήσεις.

Η Ευρωπαϊκή Επιτροπή έχει αρχίσει να εξετάζει μια πιο πράσινη Ευρώπη μέσα από το πρίσμα της Ευρωπαϊκής Πράσινης Συμφωνίας. Ταυτόχρονα, ανοίγει συζητήσεις για τη μετάβαση σε έναν πιο ψηφιακό κόσμο μέσω της ψηφιακής μετάβασης. Η ψηφιακή τεχνολογία και οι υποδομές διαδραματίζουν κρίσιμο ρόλο στην ιδιωτική ζωή και στο επιχειρηματικό περιβάλλον.

Το Πρόγραμμα Ψηφιακής Ευρώπης θα παρέχει στρατηγική χρηματοδότηση υποστηρίζοντας έργα σε πέντε βασικούς τομείς δυναμικότητας: στην τεχνητή νοημοσύνη, την ασφάλεια στον κυβερνοχώρο, τις προηγμένες ψηφιακές δεξιότητες και τη διασφάλιση ευρείας χρήσης ψηφιακών τεχνολογιών στην οικονομία και την κοινωνία, μεταξύ άλλων μέσω των Κόμβων Ψηφιακής Καινοτομίας.

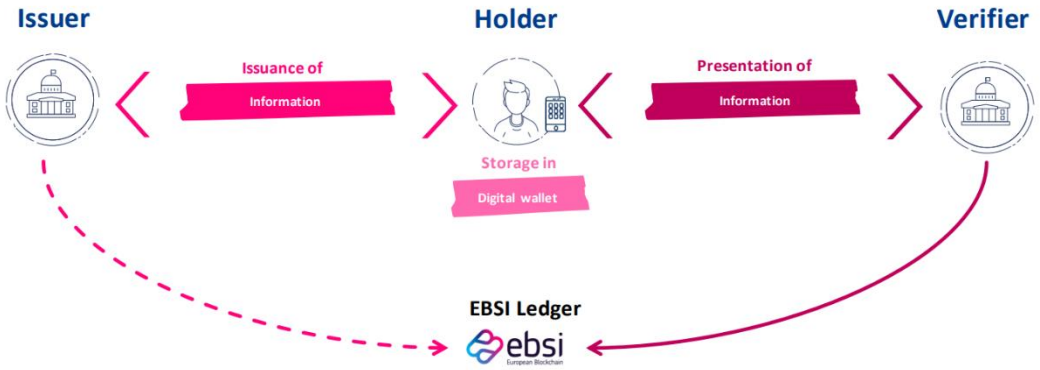
2. *Επεξήγηση Ευρωπαϊκής Υποδομής Υπηρεσιών Blockchain (EBSI)*

Το EBSI είναι ένα δίκτυο blockchain κατανεμημένων κόμβων σε όλη την Ευρώπη για την υποστήριξη σημαντικών εφαρμογών. Όταν τα έγγραφα και οι πληροφορίες κοινοποιούνται στο διαδίκτυο, εξακολουθεί να είναι δύσκολο να επαληθευτεί ότι οι πληροφορίες είναι αυθεντικές. Η μείωση του χρόνου και του κόστους της επαλήθευσης είναι μια πρόκληση που δεν μπορεί να αντιμετωπιστεί μόνο με το blockchain.

2.1 Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials)

Η επαλήθευση εγγράφων και πληροφοριών παραμένει πρόκληση. Στις μέρες μας 110 δισ. ευρώ φέρονται να ξεπλένονται στην Ευρωπαϊκή Ένωση μέσω πλαστογραφημένων εγγράφων, παράνομα και πλαστά προϊόντα διακινούνται και μία στις πέντε ετικέτες στην Ευρώπη είναι ψευδής και επομένως υπάρχει έλλειψη συμμόρφωσης με τους ευρωπαϊκούς κανόνες. Αυτοί είναι οι λόγοι για τους οποίους υπάρχει η ανάγκη για την ανάπτυξη τεχνολογίας που μπορεί να μας βοηθήσει να επαληθεύουμε εύκολα έγγραφα και πληροφορίες.

Οι αυθεντικές πηγές δεδομένων είναι πλέον ψηφιακές και διαδικτυακές, αλλά η πρόσβαση σε πραγματικό χρόνο συχνά δεν είναι δυνατή, αυτό γίνεται από μεσάζοντες. Η επαλήθευση μέσω της πρόσβασης στις αυθεντικές πηγές πληροφοριών είναι συχνά ενδιάμεση (δηλαδή μια οντότητα για λογαριασμό άλλης οντότητας). Στόχος είναι η άμεση επαλήθευση. Ένα νέο μοτίβο για την ανταλλαγή πληροφοριών είναι αυτό που βασίζεται στην αυτοκυριαρχία. Γεγονός που μπορεί να επιτευχθεί με τη



Εικόνα 1 Self-sovereign scenario (European Commission,2022)

χρήση της τεχνολογίας. Η επίτευξη της επαλήθευσης πληροφοριών μεταξύ του πολίτη και μια επιχείρησης ή της κυβέρνησης γίνεται με τα επαληθεύσιμα διαπιστευτήρια που αποτελούν ουσιαστικό αλλά όχι επαρκές στοιχείο για την επίτευξη αυτού του στόχου . Υπάρχουν άλλες δύο προκλήσεις η εμπιστοσύνη στην έκδιδουσα αρχή και η εμπιστοσύνη σε αυτόν που αποδίδει τα επαληθεύσιμα διαπιστευτήρια.

Τα επαληθεύσιμα διαπιστευτήρια γίνονται το πρότυπο επειδή :

i. Έχουν υψηλό επίπεδο βεβαιότητας ότι ο εκδότης είναι αξιόπιστος παράλληλα με τον χρόνο έκδοσης, την ημερομηνία λήξης κ.λπ.
ii. Έχουν υψηλό επίπεδο βεβαιότητας ότι ο κάτοχος είναι αυτός στον οποίο εκδόθηκε το επαληθεύσιμο διαπιστευτήριο.
iii. Οι επαληθευτές έχουν εύκολη πρόσβαση στις πληροφορίες, αλλά ο κάτοχος διατηρεί τον έλεγχο και την ιδιοκτησία των δεδομένων με δυνατότητα μερική αποκάλυψη πληροφοριών.

2.2 Εφαρμογές των επαληθεύσιμων διαπιστευτηρίων.

Η περίπτωση χρήσης του EBSI θα υποστηρίζει διασυνοριακές υπηρεσίες σε πολλούς τομείς, επιλεγμένους από το EBP, όπως :

1. Εντοπισμός και Παρακουλούθηση

Με αποτέλεσμα τη διασφάλιση της ακεραιότητας και παρακολούθησης της εξέλιξης δεδομένων ή εγγράφων, παρακολούθηση προϊόντων στην εφοδιαστική αλυσίδα μέσω του ψηφιακού τους διαβατηρίου

2. Επαληθεύσιμα Διαπιστευτήρια

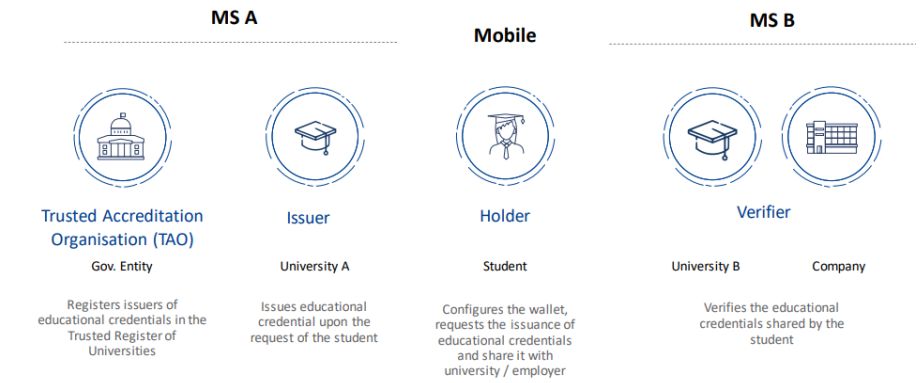
Ο έλεγχος στους πολίτες κατά τη διαχείριση των διαπιστευτήριών τους, όπως διπλώματα ή ανάρτηση πιστοποιητικών για μετακινούμενους εργαζόμενους που συνδέονται με την ψηφιακή τους ταυτότητα, μειώνοντας σημαντικά το κόστος επαλήθευσης και βελτιώνοντας την εμπιστοσύνη της γνησιότητας

3. Εμπιστοσύνη στην ανταλλαγή δεδομένων:

Ενίσχυση της εφαρμογής της πολιτικής της ΕΕ και των διαδικασιών συμμόρφωσης μεταξύ των διοικήσεων π.χ. για διαχείριση αιτήματος ασύλου ή ανταλλαγή ΑΦΜ για εισαγόμενα προϊόντα

4. Διαχείρισης πνευματικής ιδιοκτησίας (Intellectual property (IP) management):

Διευκόλυνση των κατόχων δικαιωμάτων στον έλεγχο και τη διαχείριση της πνευματικής ιδιοκτησίας.



Εικόνα 2 Κατανομή ρόλων στα κράτη μέλη (European Commission,2022)

2.3 EBSI Use Case Lifecycle

Οι περιπτώσεις χρήσης αναπτύσσονται ακολουθώντας τον ακόλουθο κύκλο ζωής.

1. Επιλογή

Οι πιθανές περιπτώσεις χρήσης προτείνονται από τις χώρες EBP, οι οποίες στη συνέχεια επιλέγουν τις πιο υποσχόμενες που θα περάσουν στο επόμενο στάδιο. Διορίζονται σύνεδροι για να καθοδηγούν κάθε περίπτωση χρήσης.

2. Ανάπτυξη

Οι σύνεδροι (Convenors) θα συγκεντρώσουν τις απαιτήσεις και θα διαμορφώσουν τις προδιαγραφές των Περιπτώσεων Χρήσης μαζί με μια ομάδα εμπειρογνωμόνων με βάση τα στοιχεία των MS. Στη συνέχεια, οι προδιαγραφές θα αναπτυχθούν και θα εφαρμοστούν από την τεχνική ομάδα του EBSI.

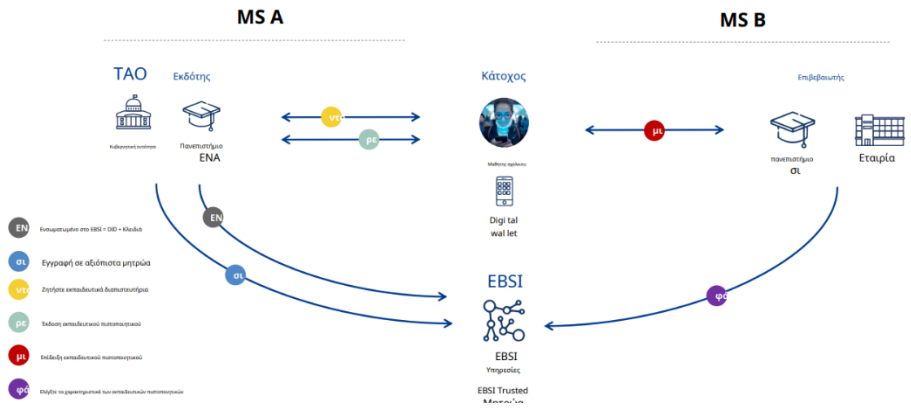
3. Πιλοτικό

Η πρώτη υλοποίηση θα ελεχθεί και θα δοκιμαστεί πιλοτικά από τους συμμετέχοντες των projects της EBP που συμμετέχουν στο Πρόγραμμα Early Adopters. Τα σχόλια που λαμβάνονται από τους πρώτος που θα χρησιμοποιήσουν την εφαρμογή(Early Adopters) ενσωματώνονται στη συνέχεια από την τεχνική ομάδα του EBSI.

4. Υιοθέτηση

Μόλις οι προδιαγραφές και η υλοποίηση φτάσουν σε ένα ορισμένο επίπεδο σταθερότητας, αναπτύσσονται στο παραγωγικό δίκτυο του EBSI και στην συνέχεια η εφαρμογή μπορεί να αναπτυχθεί παραπάνω.

Σήμερα, το EBSI είναι αρκετά προηγμένο στους τομείς της Αυτοκυριαρχίας, της Κοινωνικής Ασφάλισης και των Διπλωμάτων. Στο **μοντέλο ταυτότητας** η περίπτωση χρήσης Self-Sovereign Identity θα αποδείξει ότι το EBSI μπορεί να εφαρμόσει διασυνοριακή επαλήθευση διαπιστευτηρίων ταυτότητας με βάση τον κύκλο ζωής του Verifiable Credential. Αυτό σημαίνει ότι μια επαληθεύσιμη ταυτότητα που εκδίδεται από τη Χώρα Α μπορεί να επαληθευτεί από οποιαδήποτε οντότητα της χώρα Β. Στην **κοινωνική ασφάλιση** (European Social Security Pass) θα αποδείξει ότι το EBSI μπορεί να εφαρμόσει διασυνοριακή επαλήθευση της κάλυψης κοινωνικής ασφάλισης των αποσπασμένων εργαζομένων, δηλαδή επαλήθευση του εγγράφου PDA-1. Αυτό σημαίνει ότι ένας αρμόδιος φορέας κοινωνικής ασφάλισης σε μια χώρα ΕΒΡ εκδίδει το έγγραφο PDA-1 ως επαληθεύσιμη βεβαίωση και ένας επιθεωρητής σε άλλη χώρα ΕΒΡ το επαληθεύει. Τέλος, **στη χρήση διπλωμάτων** το EBSI θα αποδείξει ότι μπορεί να εφαρμόσει διασυνοριακή επαλήθευση των εκπαιδευτικών διαπιστευτηρίων με βάση τον κύκλο ζωής του Επαληθεύσιμου Διαπιστευτηρίου. Αυτό σημαίνει ότι μια επαληθεύσιμη βεβαίωση (όπως ένα δίπλωμα) που εκδίδεται από τη Χώρα Α μπορεί να επαληθευτεί από πανεπιστήμιο ή τρίτο μέρος, π.χ. «εργοδότης» από τη χώρα Β, όπως βλέπουμε στην εικόνα 2.



Εικόνα 3 Σενάριο χρήσης διπλωμάτων (European Commission,2022)

3. *Λειτουργία των επαληθεύσιμων διαπιστευτηρίων (Verifiable Credentials)*

3.1 Η λειτουργία των επαληθεύσιμων διαπιστευτηρίων (Verifiable Credentials)

Βήμα 0.

Οι εκδότες ενσωματώνονται.

i. Καταχώριση αυτο-εκδοθέντων Δημόσιων Κλειδιών και DID (ως μέρος ενός εγγράφου DID) στο EBSI
ii. Διαπίστευση εκδοτών από Αξιόπιστες Αρχές Διαπίστευσης (Trusted Accreditation Authorities - TAOs)
iii. Εγγραφή Εκδοτών στο μητρώο εκδοτών του EBSI

Τα πορτοφόλια ρυθμίζονται.

i. Επιλέγει ένα πορτοφόλι συμβατό με το EBSI
ii. Το Πορτοφόλι δημιουργεί DID, Δημόσια και Ιδιωτικά κλειδιά. Όλα αποτελούν μέρος ενός εγγράφου DID που είναι αποθηκευμένο στο πορτοφόλι.

Δημιουργούνται τα περιβάλλοντα επαληθευτών.

i. Συγκεκριμένη ενσωμάτωση ή ρύθμιση εκτός από τη δημιουργία μιας εφαρμογής επαληθευτή που μπορεί να εκμεταλλευτεί τα API EBSI και να αλληλοεπιδράσει με πορτοφόλια που συμμορφώνονται με το EBSI.

Βήμα 1. Έκδοση ενός επαληθεύσιμου διαπιστευτηρίου το οποίο στη συνέχεια αποθηκεύεται σε ένα πορτοφόλι συμβατό με EBSI.

Τα επαληθεύσιμα διαπιστευτήρια περιέχουν :

A. Μεταδεδομένα διαπιστευτηρίων. Το DID της οντότητας που εκδίδει το διαπιστευτήριο και την κατάσταση του διαπιστευτηρίου (Ημερομηνία έκδοσης, Ημερομηνία λήξης)
B. Αξιώσεις (Claims). Το DID του κατόχου του διαπιστευτηρίου και τις αξιώσεις σχετικά με το θέμα (Τι ισχυρίζεται ο εκδότης για το θέμα).
C. Απόδειξη (υπογραφή του Εκδότη). Η ψηφιακή απόδειξη για να καταστεί προφανής η παραβίαση της διαπιστευτηρίου (Μία ή περισσότερες κρυπτογραφικές αποδείξεις που μπορούν να χρησιμοποιηθούν για την ανίχνευση παραποίησης και την επαλήθευση).

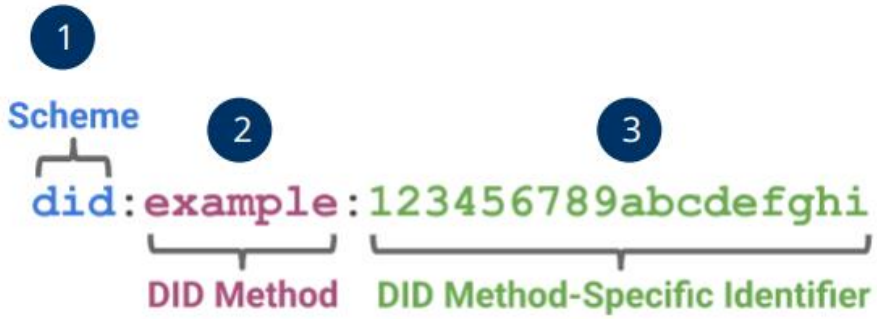
Βήμα 2. Παρουσίαση επαληθεύσιμου διαπιστευτηρίου.

Σημεία ελέγχου:

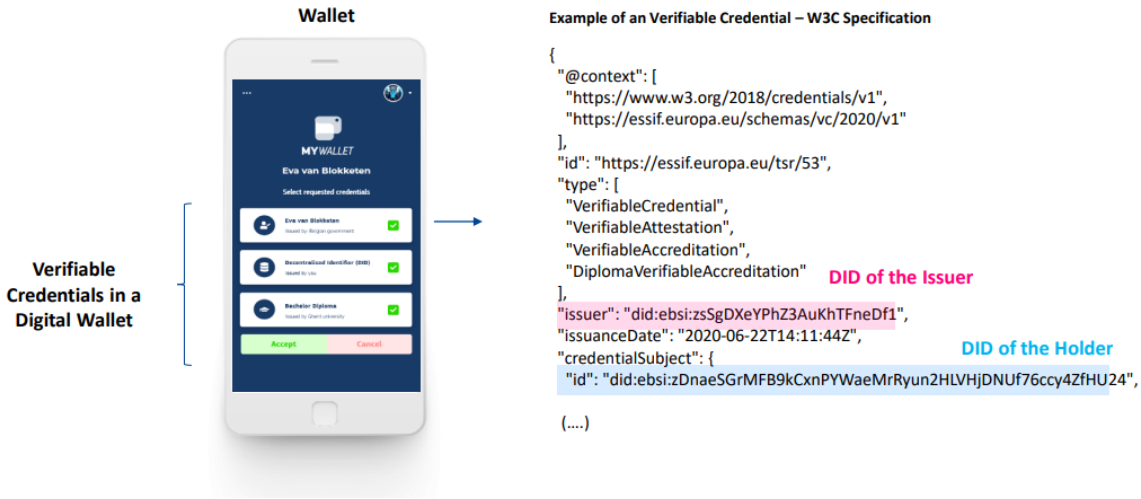
i. **Το DID του κατόχου.** Ελέγχει ότι ο κάτοχος του VC είναι αυτός που το παρουσιάζει.
ii. **Μεταδεδομένα διαπιστευτηρίων.** Ελέγχεται ο χρόνος έκδοσης, εάν έχει λήξει.
iii. **Αξιώσεις (Claims).** Ελέγχονται οι ισχυρισμοί σχετικά με το θέμα.
iv. **Απόδειξη (υπογραφή του Εκδότη).** Ελέγχεται η υπογραφή του εκδότη.
v. **Απόδειξη (υπογραφή κατόχου).** Ελέγχεται η υπογραφή του κατόχου.
vi. **Ελέγχεται η διαπίστευση του εκδότη.**

3.2 Αποκεντρωμένο αναγνωριστικό W3C (DID)

Το DID είναι απλώς μια μεγάλη συμβολοσειρά που δεν παρέχει ουσιαστικές πληροφορίες για μια φυσική ή νομική οντότητα. Τα DID και τα DID Documents δημιουργούνται από τους κατόχους τους με το πορτοφόλι τους ή τα συστήματα back-office τους.



Εικόνα 4 Μέρη του DID (European Commission,2022)



Εικόνα 5 Παράδειγμα Επαληθεύσιμων Διαπιστευτηρίων (European Commission,2022)

Σύμφωνα με το πρότυπο W3C, ένα DID αποτελείται πάντα από τρία μέρη, το πρώτο μέρος είναι πάντα τα τρία γράμματα 'did', το δεύτερο μέρος ορίζει το αναγνωριστικό για τη μέθοδο DID, και το τρίτο μέρος είναι εντελώς μοναδικός τυχαίος αριθμός που ακολουθεί κανόνες παραγωγής για τη συγκεκριμένη μέθοδο. Τα DID χρησιμοποιούνται για τη διασφάλιση της γνησιότητας των εκδοτών και των κατόχων σε έγγραφα επαληθεύσιμα από μηχανή, γνωστά ως Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials - VCs).

3.3 Μέθοδος Decentralized Identifiers (DID)

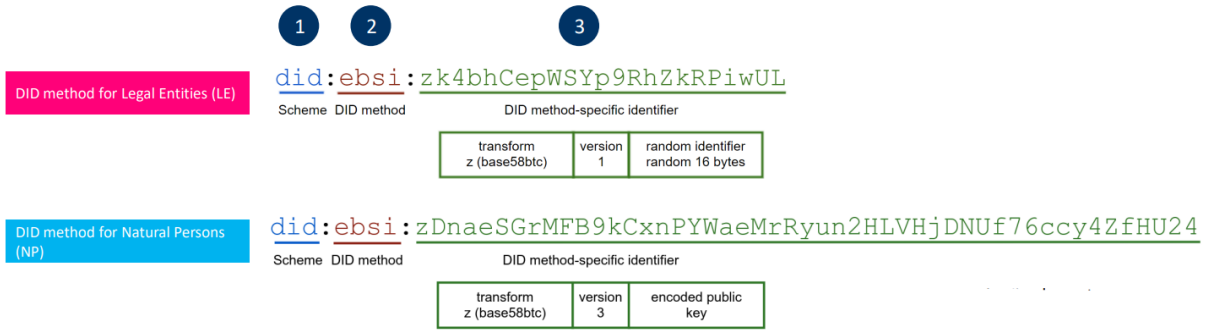
Το EBSI υποστηρίζει 2 διαφορετικές μεθόδους DID. Την Μέθοδος EBSI DID για Νομικά Πρόσωπα (LE), όπου τα έγγραφα είναι αποθηκευμένα στο ψηφιακό καθολικό της EBSI και την μέθοδο EBSI DID για φυσικά πρόσωπα (NP), όπου τα έγγραφα είναι αποθηκευμένα στο πορτοφόλι. Επομένως η μία μέθοδος απευθύνεται σε Νομικά Πρόσωπα (Εκδότες) και η άλλη σε Φυσικά Πρόσωπα (Κάτοχοι).Στον πίνακα 1 καταγράφονται οι βασικές διαφορές των δύο μεθόδων.

Πίνακας 1 Διαφορές Μεθόδων Did

	Προδιαγραφή μεθόδου EBSI DID για Νομικά Πρόσωπα (LE)	**Προδιαγραφή μεθόδου EBSI DID για φυσικά πρόσωπα (NP)**
ΧΡΗΣΗ	Νομικά Πρόσωπα (Εκδότες).	Φυσικά Πρόσωπα
ΔΗΜΙΟΥΡΓΙΑ	DID και DID έγγραφο είναι που δημιουργείται από μια εφαρμογή backoffice ή μια εφαρμογή που μοιάζει με πορτοφόλι.	DID και έγγραφο δημιουργούνται και αποθηκεύονται στο πορτοφόλι.
ΚΑΤΑΓΡΑΦΗ	Το έγγραφο DID καταγράφεται στο ψηφιακό καθολικό της EBSI. Δεν υπάρχει σύζευξη μεταξύ DID και Δημοσίου Κλειδιού,	Έγγραφο DID δεν έχει καταχωρηθεί στο καθολικό του EBSI. Η ιδιοκτησία DID μπορεί να είναι κρυπτογραφικά επαληθεύσιμη επειδή περιέχει

	επιτρέποντας τη συχνή εναλλαγή του κλειδιού από τους εκδότες.	ένα αποτύπωμα JWK του Δημόσιου Κλειδιού – επομένως, εάν ο κάτοχος αποδείξει την κυριότητα του ιδιωτικού κλειδιού, αποδεικνύει την ιδιοκτησία του DID.
ΛΕΙΤΟΥΡΓΙΑ	Οι επαληθευτές ανακτούν το έγγραφο DID από το EBSI για να επιβεβαιώσουν την ιδιοκτησία των DID και να επαληθεύσουν την υπογραφή των επαληθεύσιμων διαπιστευτηρίων χρησιμοποιώντας το δημόσιο κλειδί του Εκδότη για επιβεβαίωση.	Το πορτοφόλι περιλαμβάνει το DID και το έγγραφο DID κατά την παρουσίαση πληροφοριών στους Επαληθευτές ή όταν του ζητείται να επιβεβαιώθει η ιδιοκτησία DID από τους επαληθευτές ή από τους εκδότες

Το DID της EBSI αποτελείται από τρία μέρη και στις δύο μεθόδους, αλλά η μέθοδος DID για φυσικά πρόσωπα (NP) θα χρησιμοποιεί έναν τυποποιημένο τρόπο για τον υπολογισμό του hash ενός δημόσιου κλειδιού.



Εικόνα 6 Δημιουργία DID (European Commission,2022)

3.3.1 Λειτουργία της μεθόδου DID για Νομικά Πρόσωπα (LE)

Ο εκδότης δημιουργεί DID, τα κρυπτογραφικά κλειδιά που σχετίζονται με ένα δεδομένο DID και καταγράφει αυτές τις πληροφορίες στο EBSI με τη μορφή εγγράφου DID. Το έγγραφο DID μπορεί να ανακτηθεί από το EBSI από εκδότες και επαληθευτές χρησιμοποιώντας μια απλή διεύθυνση URL. Η μέθοδος DID (LE) επιτρέπει στους εκδότες να διαχειρίζονται με ευελιξία τα κλειδιά τους και την πρόσβασή τους σε πραγματικό χρόνο από τους επαληθευτές. Η χρήση DID και εγγράφων DID που έχουν καταχωριθεί στο EBSI, όπως ορίζεται στη μέθοδο DID, επιτρέπει στους εκδότες να εναλλάσσουν τα κλειδιά τους, δηλαδή να ενημερώνουν τακτικά τα κρυπτογραφικά τους κλειδιά (π.χ. κάθε δεύτερο μήνα)

χωρίς να επηρεάζουν τους επαληθευτές, καθώς μπορούν εύκολα να ανακτήσουν τη σωστή έκδοση του εγγράφου DID από την EBSI. Αυτό επιτρέπει μια πολύ πιο ομαλή και ασφαλή διαχείριση των κλειδιών σε μεγάλα οικοσυστήματα. Επιπλέον, οι εκδότες μπορούν να έχουν πολλαπλά ενεργά κλειδιά συνδεδεμένα στο DID τους. Η εναλλαγή κλειδιών ελαχιστοποιεί τον αριθμό των επαληθεύσιμων διαπιστευτηρίων που ανακαλούνται λόγω της ανάκλησης των κλειδιών υπογραφής του εκδότη.

3.3.2 Λειτουργία της μεθόδου DID για για φυσικά πρόσωπα (NP)

Το πορτοφόλι δημιουργεί τα κρυπτογραφικά κλειδιά και εξάγει το DID σύμφωνα με το προφίλ του σχήματος DID του EBSI για φυσικά πρόσωπα (NP) κωδικοποιώντας το Δημόσιο Κλειδί. Στη διαδικασία έκδοσης επαληθεύσιμου διαπιστευτηρίου, ο Κάτοχος κοινοποιεί το έγγραφο DID (δημόσιο κλειδί) και αποδεικνύει την κατοχή του DID επιβεβαιώνοντας την κατοχή του αντίστοιχου ιδιωτικού κλειδιού στον επαληθευτή. Στη διαδικασία ανταλλαγής επαληθεύσιμης παρουσίασης, ο κάτοχος κοινοποιεί το έγγραφο DID του (δημόσιο κλειδί) και αποδεικνύει την κατοχή του DID επιβεβαιώνοντας την κατοχή του αντίστοιχου ιδιωτικού κλειδιού στον επαληθευτή.

3.4 Έγγραφο DID από τεχνική άποψη

Κάθε DID αντιστοιχίζεται σε ένα ενιαίο και μοναδικό έγγραφο DID το οποίο μπορεί να εκδοθεί.


```
{
 "@context": "https://w3id.org/did/v1",
 "id": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
 "verificationMethod": [
  {
   "id": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1",
   "type": "EcdsaSecp256k1VerificationKey2019",
   "controller": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
   "publicKeyJwk": {
    "kty": "EC",
    "crv": "secp256k1",
    "x": "n03trG-1sWidluyYQ2gcKrgYE94rMkLIArZCHjv2GpI",
    "y": "6__x_vqe0nBGYf7azbQ1_VvvuCafG5MhhUPNvYp-Mak"
   }
  }
],
 "assertionMethod": [
  "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1"
 ]
}
```


Public key

Reference to Public key

Εικόνα 7 Παράδειγμα DID document (European Commission,2022)

Κάθε αποκεντρωμένο αναγνωριστικό (DID) συσχετίζεται με τα δημόσια κλειδιά που χρησιμοποιούνται από τους επαληθευτές για την επαλήθευση των ηλεκτρονικών υπογραφών σε ένα έγγραφο DID. Ένα έγγραφο DID περιέχει τα κρυπτογραφικά δημόσια κλειδιά που χρησιμοποιούνται για την επαλήθευση των διαπιστευτηρίων. Σύμφωνα με τη μέθοδο DID για Νομικά Πρόσωπα (LE), οι εκδότες πρέπει να διαθέτουν ένα έγγραφο DID αποθηκευμένο στο EBSI το οποίο μπορούν να διαχειρίζονται. Σύμφωνα με τη μέθοδο DID για φυσικά πρόσωπα (NP), οι εκδότες δε διαθέτουν έγγραφο DID στο EBSI. Το έγγραφο DID αποθηκεύεται και μοιράζεται από το πορτοφόλι.

3.4.1 Το Δημόσιο ή ιδιωτικό κλειδί και η χρήση του

Οι ηλεκτρονικές υπογραφές χρησιμοποιούν δημόσια και ιδιωτικά κλειδιά για να εξασφαλιστεί η εμπιστοσύνη μεταξύ των εκδοτών και επαληθευτών, καθώς μεταξύ κατόχων και επαληθευτών. Ένα δημόσιο κλειδί και ένα ιδιωτικό κλειδί σχετίζονται μαθηματικά μεταξύ τους (αλλά δεν σχετίζονται με το DID). Όταν δημιουργούνται, τα επαληθεύσιμα διαπιστευτήρια υπογράφονται από τους εκδότες (χρησιμοποιώντας το ιδιωτικό τους κλειδί) και ελέγχονται από τους επαληθευτές (χρησιμοποιώντας το δημόσιο κλειδί στο έγγραφο DID ενός συγκεκριμένου Εκδότη) για να διασφαλιστεί η ακεραιότητα και η αυθεντικότητά τους. Το ιδιωτικό κλειδί πρέπει να παραμένει μυστικό και να μην μπορεί να μοιραστεί (π.χ. πρέπει να παραμείνει στο πορτοφόλι του Κατόχου). Κατά την κοινή χρήση πληροφοριών, οι επαληθεύσιμες παρουσιάσεις υπογράφονται από τους κατόχους (χρησιμοποιώντας το ιδιωτικό τους κλειδί) και ελέγχονται από τους επαληθευτές (χρησιμοποιώντας το δημόσιο κλειδί στο έγγραφο DID του κατόχου) για να διασφαλιστεί η ακεραιότητα και η αυθεντικότητά τους. Τα ένα ή τα περισσότερα δημόσια κλειδιά που χρησιμοποιούνται από εκδότες και κατόχους δημοσιοποιούνται στο έγγραφο DID χωρίς να μειώνεται η ασφάλεια της διαδικασίας.

3.4.2 Μητρώο καταχώρισης DID / Επαληθεύσιμο μητρώο DID

Η χρήση του DID απαιτεί ένα υποκείμενο σύστημα μητρώου που μπορεί να είναι ένα κατανεμημένο καθολικό, αποκεντρωμένο σύστημα αρχείων, βάση δεδομένων ή οποιαδήποτε άλλη μορφή αξιόπιστης αποθήκευσης δεδομένων. Το EBSI είναι ο καταχωρητής όλων των DID του EBSI. Ο καταχωρητής DID χρησιμοποιείται μόνο στη μέθοδο DID για Νομικά Πρόσωπα (LE) για έγγραφα DID των Εκδοτών.

4. *Προσέγγιση της Αυτοκυριαρχικής ταυτότητας (Self-Sovereign Identity)*

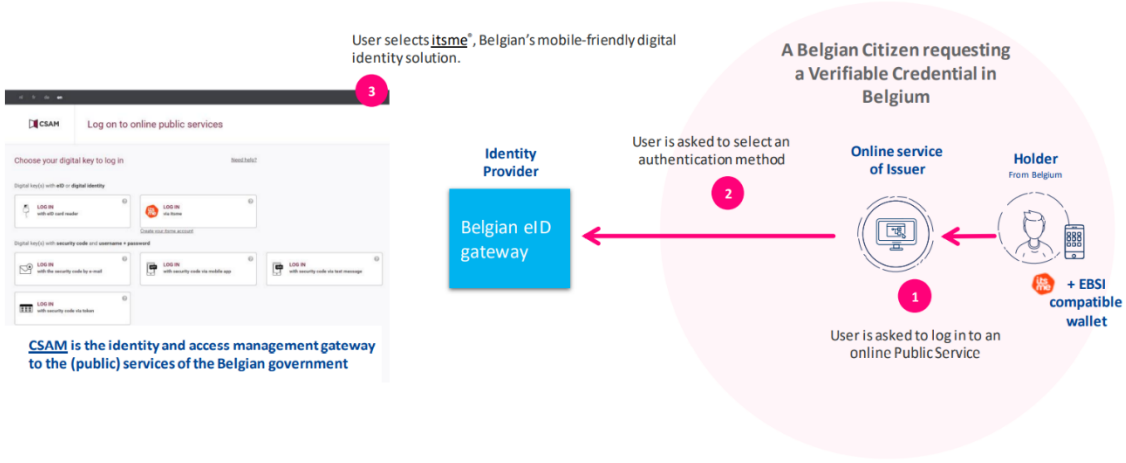
4.1 Οι προσεγγίσεις για την ψηφιακή ταυτότητα

Η Ψηφιακή Ταυτότητα βρίσκεται στο θεμέλιο όλων των άλλων ψηφιακών υπηρεσιών. Η ψηφιακή ταυτότητα του κατόχου μπορεί να επιβεβαιωθεί με διαφορετικούς τρόπους. Οι εφαρμογές που χρησιμοποιούνται από εκδότες και επαληθευτές απαιτούν έλεγχο ταυτότητας και ταυτοποίηση, όπως και στο ίδιο το ψηφιακό πορτοφόλι. Οι διαφορετικές προσεγγίσεις για την ψηφιακή ταυτότητα είναι η Εθνική Προσέγγιση, Ομοσπονδιακή Προσέγγιση και Αυτοκυριαρχική Προσέγγιση Εθνική Προσέγγιση, Ομοσπονδιακή Προσέγγιση και Αυτό-κυριαρχική Προσέγγιση.

4.2 Εθνική Προσέγγιση

Μία κεντρική Αρχή, όπως ένα κράτος, διαχειρίζεται την υπηρεσία εθνικής ταυτότητας και είναι υπεύθυνο για τον έλεγχο ταυτότητας καθώς και την ταυτοποίηση των πολιτών που έχουν πρόσβαση στις Ψηφιακές Υπηρεσίες του. Στην εικόνα 8 περιγράφεται ένα παράδειγμα της ψηφιακής ταυτότητας για από την Βέλγικη Κυβέρνηση. Αρχικά ζητείται από τον χρήστη να συνδεθεί σε μια διαδικτυακή Δημόσια Υπηρεσία, στη συνέχεια ο χρήστης επιλέγει μία μέθοδο αυθεντικότητα και τέλος ο χρήστης χρησιμοποιεί τη βελγική λύση ψηφιακής ταυτότητας που είναι φιλική προς τα κινητά. Το επαληθεύσιμο διαπιστευτήριο εκδίδεται μετά από επιτυχή έλεγχο ταυτότητας, εάν ο Κάτοχος αποδείξει με επιτυχία

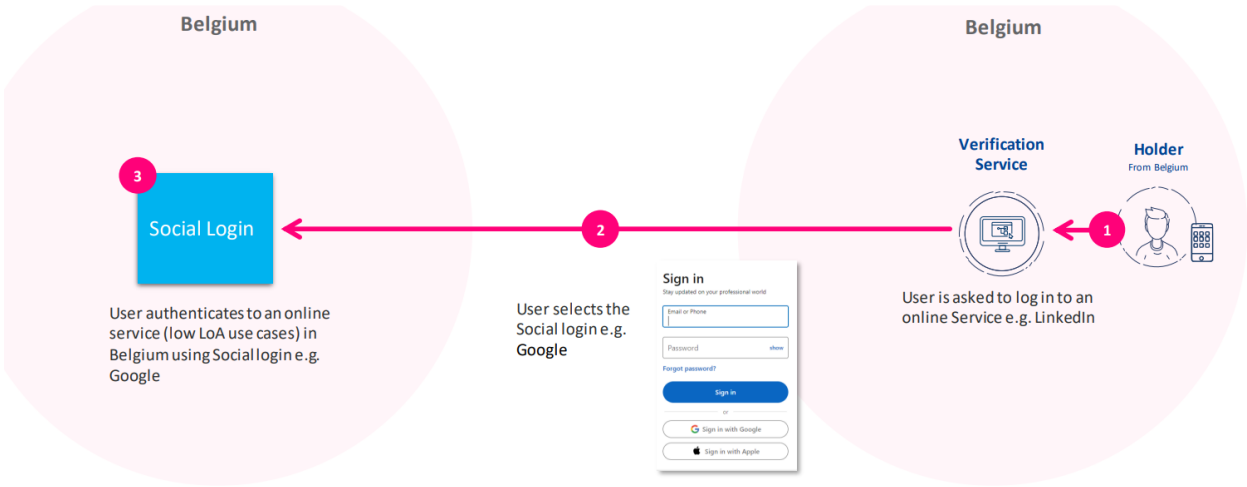
την κυριότητα του DID που παρουσιάστηκε στον Εκδότη. Ένα σημαντικό όφελος για της εθνικής προσέγγισης είναι ότι ο χρήστης μπορεί να επιλέξει το τρόπο αυθεντικοποίησης.



Εικόνα 8 Παράδειγμα Εθνικής Προσέγγισης (European Commission,2022)

4.3 Ομοσπονδιακή Προσέγγιση

Υπάρχουν διάφοροι τρόποι για την Ομοσπονδιακή Προσέγγιση. Για παράδειγμα, ο κανονισμός eIDAS έχει θεσπίσει αμοιβαία αναγνώριση των κοινοποιημένων εθνικών συστημάτων ηλεκτρονικής ταυτοποίησης (eID) διασυνοριακά, δίνοντας τη δυνατότητα στους πολίτες να χρησιμοποιούν τα εθνικά τους eID όταν έχουν πρόσβαση σε διαδικτυακές υπηρεσίες από άλλες ευρωπαϊκές χώρες. Στην εικόνα 9 περιγράφεται ένα παράδειγμα ομοσπονδιακής προσέγγισης, αρχικά ο χρήστης καλείται να συνδεθεί σε μια ηλεκτρονική Υπηρεσία (π.χ. LinkedIn) στη συνέχεια ο χρήστης επιλέγει μια κοινωνική σύνδεση (π.χ Google), τέλος ο χρήστης πραγματοποιεί έλεγχο ταυτότητας χρησιμοποιώντας τη σύνδεση μέσων



Εικόνα 9 Παράδειγμα Ομοσπονδιακής Προσέγγισης (European Commission,2022)

κοινωνικής δικτύωσης π.χ. Google. Όφελος από αυτή την προσέγγιση είναι ότι υπάρχει επιλογή του παρόχου ταυτότητας και μέθοδος αυθεντικότητας.

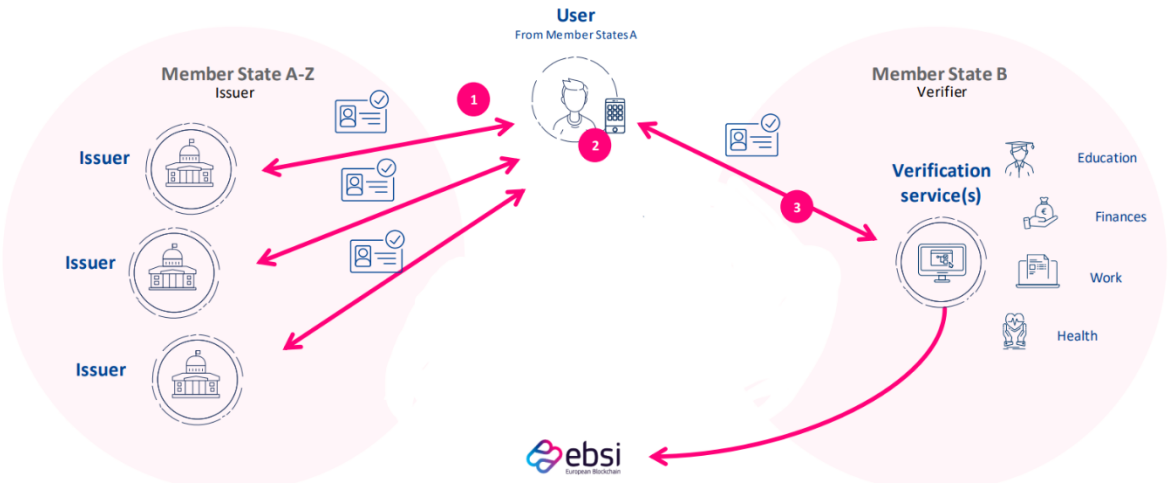
4.4 Προσέγγιση της Αυτοκυριαρχικής ταυτότητας

Η προσέγγιση της αυτοκυριαρχικής ταυτότητας είναι ένα αποκεντρωμένο μοντέλο ψηφιακής ταυτότητας που αναπτύχθηκε για να αντιμετωπίσει τις αδυναμίες των προηγούμενων προσεγγίσεων ταυτότητας στο Διαδίκτυο . Με κεντρικές ταυτότητες, κεντρικά ιδρύματα όπως οι κυβερνήσεις και οι τράπεζες εκδίδουν διαπιστευτήρια που επιτρέπουν στους πολίτες να αλληλοεπιδρούν με τις υπηρεσίες και μεταξύ τους. Στο διαδίκτυο δημιουργείται ένας λογαριασμός με κάθε ιστότοπο, υπηρεσία ή εφαρμογή.

Η άνοδος της τεχνολογίας blockchain ενέπνευσε το μοντέλο αποκεντρωμένης ταυτότητας. Αυτό το μοντέλο δεν βασίζεται σε λογαριασμούς με κεντρικά ιδρύματα ή σε παρόχους ταυτότητας αλλά σε άμεσες σχέσεις μεταξύ των συμβαλλόμενων μελών.

Κανένα μέλος δεν ελέγχει ή κατέχει τη σχέση. Οι χρήστες έχουν τον απόλυτο έλεγχο των δεδομένων ταυτότητάς τους και του τρόπου κοινής χρήσης. Τα συμβαλλόμενα μέλη δημιουργούν ιδιωτικές συνδέσεις ανταλλάσσοντας με ασφάλεια δημόσια κλειδιά, όπου τα blockchain χρησιμεύουν ως αποκεντρωμένες υποδομές δημόσιου κλειδιού. Αυτό το μοντέλο μοιάζει περισσότερο με τον τρόπο με τον οποίο διαχειριζόμαστε την ταυτότητά μας στον πραγματικό κόσμο. Με πορτοφόλια που περιέχουν διαπιστευτήρια που λαμβάνονται από αξιόπιστα μέρη τα οποία μπορούν να παρουσιαστούν σε άλλα μέρη για να ξεκινήσουν μια αλληλεπίδραση.

W3C's επαληθεύσιμα διαπιστευτήρια μπορεί να χρησιμοποιηθούν για τη δημιουργία επαληθεύσιμων αναγνωριστικών που μπορούν να συνδυάζονται εύκολα με άλλα διαπιστευτήρια, ώστε να επεκτείνονται ο αριθμός των χαρακτηριστικών που χρησιμοποιούνται για σκοπούς ελέγχου ταυτότητας και ταυτοποίησης, αλλά και για αντιστοίχιση αρχείων. Το μοντέλο υποστηρίζει επίσης την έκδοση και την παρουσίαση των επαληθεύσιμων βεβαιώσεων. Στην εικόνα 10 περιγράφεται ο τρόπος λειτουργίας της προσέγγισης αυτοκυριαρχίας. Αρχικά ο χρήστης λαμβάνει επαληθεύσιμα αναγνωριστικά που εκδόθηκαν από διαφορετικούς αξιόπιστους εκδότες, στη συνέχεια τα επαληθεύσιμα αναγνωριστικά αποθηκεύονται σε ένα ψηφιακό πορτοφόλι και τέλος ο χρήστης παρουσιάζει το επαληθεύσιμα αναγνωριστικά σε διαφορετικούς επαληθευτές σε διαφορετικά κράτη - μέλη.



Εικόνα 10 Τρόπος λειτουργίας Προσέγγιση της Αυτοκυριαρχίας (European Commission,2022)

Η Προσέγγιση της Αυτό - κυριαρχικής ταυτότητας έχει οφέλη για τον πολίτη την επιλογή παρόχου ταυτότητας, την επιλογή μεθόδου αυθεντικότητας και την επιλογή των δεδομένων που θέλω να αποκαλύψω.

4.5 Διαχείριση ταυτότητας με χρήση πορτοφολιών

Ο χρήστης θα μπορούσε να χρησιμοποιήσει οποιοδήποτε πορτοφόλι για τον έλεγχο ταυτότητας και τη λήψη των διαπιστευτηρίων. Το αποκεντρωμένο μοντέλο δίνει τη δυνατότητα στους κατόχους να επιλέξουν το πορτοφόλι και τα διαπιστευτήριά τους που θα μοιραστούν. Σήμερα 13 πορτοφόλια συμμορφώνονται με τις προδιαγραφές EBSI.

5. *Επεξηγημένα μοντέλα εμπιστοσύνης EBSI*

5.1 Issuers Trust Montel

5.1.1 Το κλασικό μοντέλο εμπιστοσύνης για τους εκδότες

Οι κλασικές λύσεις απαιτούν συχνά από τους επαληθευτές να επικοινωνούν με τους εκδότες προκειμένου να διασφαλίσουν ότι οι πληροφορίες που λαμβάνουν από τους κατόχους είναι αξιόπιστες. Αυτό το μοτίβο ονομάζεται “phoning home”. Στην περίπτωση αυτή δημιουργούνται οι εξής προκλήσεις:

I. Επιβάλλει τεχνικό βάρος στον Εκδότη διαπιστευτηρίων, ο οποίος πρέπει να δημιουργήσει και να διατηρήσει διαθέσιμα API Επαληθευτών και να βεβαιώνει ότι η συνδεσιμότητα είναι διαθέσιμη συνεχώς.
II. Απαιτεί από τον Επαληθευτή να δημιουργεί και να διατηρεί κλήσεις προς όλα αυτά τα API από κάθε Εκδότη διαπιστευτηρίων. Σε ένα ανοιχτό οικοσύστημα διαπιστευτηρίων, αυτό θα μπορούσε να περιλαμβάνει εκατοντάδες ή χιλιάδες ενσωματώσεις για κάθε στηριζόμενο μέρος.
III. Προκαλεί προκλήσεις απορρήτου επειδή παρέχει έναν τρόπο στους εκδότες και τους επαληθευτές να συσχετίσουν τη χρήση ενός διαπιστευτηρίου από έναν κάτοχο ταυτότητας σε όλους τους τομείς.

5.1.2 Ένα νέο μοντέλο εμπιστοσύνης για τους εκδότες

Σύμφωνα με το μοντέλο Επαληθεύσιμων Διαπιστευτηρίων του EBSI, το EBSI δίνει τη δυνατότητα στους Επαληθευτές να εμπιστεύονται τους εκδότες χωρίς “phoning home”. Αντίθετα, οι Επαληθευτές μπορούν να ανακτήσουν τις πληροφορίες που απαιτούνται για την εμπιστοσύνη των Εκδοτών από το καθολικό

του EBSI. Τρία βασικά μοντέλα εμπιστοσύνης εκδοτών επαληθεύσιμων διαπιστευτηρίων, μπορούν να συνδυαστούν. Το Κεντρικό Μοντέλο Εμπιστοσύνης, το Ομοσπονδιακό μοντέλο εμπιστοσύνης και το Μοντέλο Κατανεμημένης Εμπιστοσύνης. Ο Κανονισμός eIDAS εισήγαγε την έννοια του Trusted List. Η εκτελεστική απόφαση (ΕΕ) 2015/1505 καθορίζει τις τεχνικές προδιαγραφές της.[1]

Πίνακας 2 Σύγκριση μοντέλων εμπιστοσύνης με το μοντέλο εμπιστοσύνης EBSI

Το κεντρικό και το ομοσπονδιακό μοντέλο βασίζεται συνήθως σε πιστοποιητικά X.509.	Το μοντέλο κατανεμημένης εμπιστοσύνης της EBSI βασίζεται στο blockchain και στο DID.
Τα μοντέλα αυτά είναι ιεραρχικά και όχι τόσο ευέλικτα καθώς απαιτεί πολλούς ρόλους.	Η χρήση των DID παράλληλα με το blockchain επιτρέπει την αποκέντρωση και μεγαλύτερη ευελιξία. Απαιτούνται μόνο δύο ρόλοι:
Αρχή έκδοσης πιστοποιητικών (Certificate Authority- CA) που αποθηκεύει, εκδίδει και υπογράφει τα ψηφιακά πιστοποιητικά.	Αξιόπιστος Οργανισμός Διαπίστευσης (Trusted Accreditation Organisation- TAO) επαληθεύει, διαπιστεύει και διαχειρίζεται τις οντότητες, δηλαδή τους Αξιόπιστους εκδότες, που εκδίδουν ηλεκτρονικά έγγραφα.
Αρχή Εγγραφής. (Registration Authority-RA) που επαληθεύει την ταυτότητα των οντοτήτων που ζητούν τα ψηφιακά τους πιστοποιητικά να αποθηκευτούν στην ΑΠ.	Αξιόπιστος εκδότης (Trusted Issuer-TI)είναι υπεύθυνος για την έκδοση ορισμένων τύπων ηλεκτρονικών εγγράφων και τη διαχείριση των κλειδιών υπογραφής τους με την υποστήριξη του blockchain. Από τεχνική άποψη, διαχειρίζεται ένα έγγραφο DID.
Αρχή Επικύρωσης(Validation Authority-VA) που μπορεί να παρέχει πληροφορίες για επικύρωση εκ μέρους της ΑΠ.	
Αρχή Διανομής(Validation Authority-VA) που είναι αρμόδια για τη διανομή των πιστοποιητικών.	

5.1.3 Βασικοί παράγοντες του Μοντέλου Εμπιστοσύνης Εκδοτών της EBSI

5.1.3.1 Trusted Accreditation Organisation (TAO)

Οι Trusted Accreditation Organisations (TAO) είναι υπεύθυνοι για τη διαπίστευση Αξιόπιστων Εκδοτών, ενός συγκεκριμένου τομέα, για την έκδοση ορισμένων τύπων επαληθεύσιμων Διαπιστευτηρίων (VC). Για παράδειγμα, στον τομέα της εκπαίδευσης, το Υπουργείο Παιδείας μιας χώρας είναι υπεύθυνο για τη διαπίστευση των Πανεπιστημίων αυτής της χώρας. Οι TAO καταγράφουν επίσης τα αξιόπιστα σχήματα που σχετίζονται με το Επαληθεύσιμο Διαπιστευτήριο, π.χ. Δίπλωμα.

5.1.3.2 EBSI Ledger

EBSI ως το δημόσιο μητρώο εκδοτών, περιέχει τη λίστα των αξιόπιστων νομικών οντοτήτων που είναι διαπιστευμένα από τους TAOs για την έκδοση ορισμένων τύπων διαπιστευτηρίων. Με άλλα λόγια, οι διαπιστευμένες οντότητες γίνονται Αξιόπιστοι Εκδότες μέσω μιας απλής διαδικασίας διαπίστευσης.

[1] https://europa.eu/!GRyHFF

Για παράδειγμα, στον τομέα της εκπαίδευσης, εκτός από τα έγγραφα DID εγγεγραμμένων Πανεπιστημίων, το EBSI διαθέτει στους Επαληθευτές τη διαπίστευση που δόθηκε από ένα TAO, το οποίο είναι επαληθεύσιμο διαπιστευτήριο, και ο σύνδεσμος προς το συσχετισμένο αξιόπιστο σχήμα.

Πίνακας 3 Registered on the EBSI ledger

	Μητρώο Εκδοτών	**Μητρώο αξιόπιστων σχημάτων**
Trusted Accreditation Organisation (TAO)	**Έγγραφο DID and DID του TAO** ➢ **Επαληθεύσιμη εξουσιοδότηση του TAO** ➢ **Επαληθεύσιμη διαπίστευση του TAO** (συμπεριλαμβανομένης της αναφοράς στο DID, την ισχύουσα δικαιοδοσία και τους οργανισμούς τους οποίους επιτρέπεται να διαπιστεύουν τα VC και τα αντίστοιχα σχήματα).	**Σχήμα διαπιστευτηρίων περιγράφει το μοντέλο δεδομένων για:** ➢ **Οργανισμοί στους οποίους επιτρέπεται να διαπιστεύουν** ➢ **Εφαρμοστέα δικαιοδοσία** ➢ **Τύπος επαληθεύσιμου διαπιστευτηρίου**
Trusted Issuers (TI)	➢ **DID και Έγγραφο Αξιόπιστου Εκδότη** ➢ **Επαληθεύσιμη διαπίστευση εκδότη** (συμπεριλαμβανομένης της αναφοράς στο DID, τα VC που επιτρέπεται να εκδίδουν και την ισχύουσα δικαιοδοσία, και το αντίστοιχο σχήμα).	**Επαληθεύσιμο σχήμα διαπιστευτηρίων περιγράφει το μοντέλο δεδομένων για:** Επαληθεύσιμα διαπιστευτήρια που επιτρέπεται να εκδίδουν. Σημείωση: το σχήμα VC προσδιορίζεται σε επίπεδο Χρήσης περίπτωσης/πολιτικής.

5.1.3.3 Trusted Issuers (TI)

Επιπλέον, το EBSI καθιστά επίσης διαθέσιμα τα σχήματα των επαληθεύσιμων διαπιστευτηρίων. Ένα σχήμα υποστηρίζει τη διαδικασία επαλήθευσης και διασφαλίζει ότι οι εκδότες σέβονται τα συμφωνημένα μοντέλα δεδομένων που ορίζονται από κάθε τομέα.

5.2 Trust anchoring

Οι νομικές οντότητες μπορούν να έχουν πολλαπλές διαπιστεύσεις από μεμονωμένες ή πολλαπλές αλυσίδες καταπιστευμάτων. Κάθε διαπίστευση παρέχει στα νομικά πρόσωπα διαφορετικές δυνατότητες.

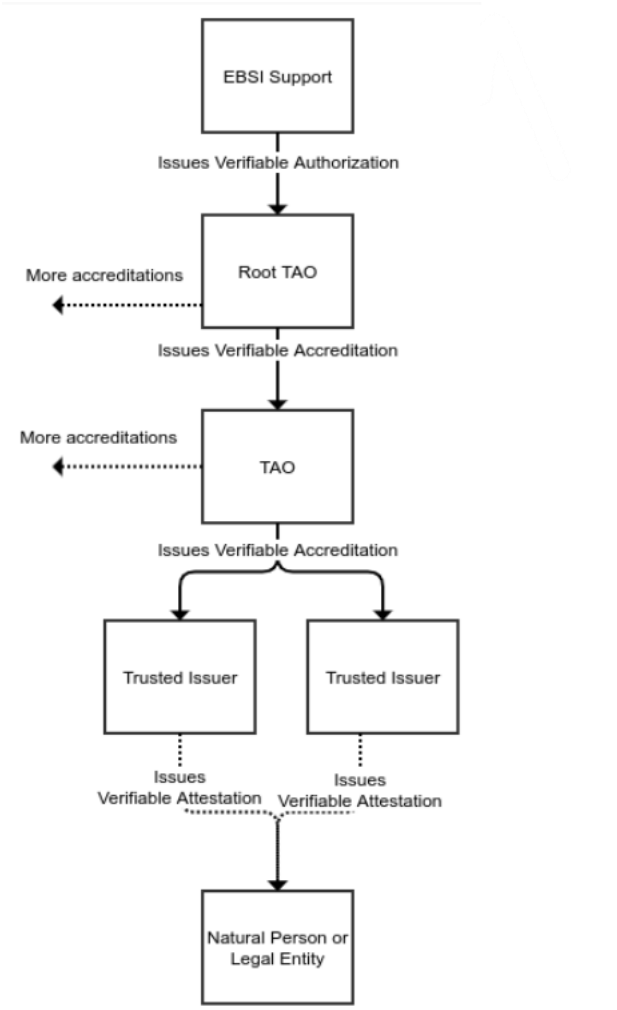
Πίνακας 4 Trust anchoring

Actor (Σύνολο ενεργειών στοιχείων)	Role (Ρόλοι)	Capabilities (Δυνατότητες)	Requirements (Απαιτήσεις)	Description (Περιγραφή)
Εκδότης ελέγχου ταυτότητας περίπτωσης χρήσης EBSI	Αξιόπιστος εκδότης εξουσιοδότησης	Μπορεί να εξουσιοδοτήσει Νομικά Πρόσωπα να δηλωθούν ως Έμπιστος Εκδότης Διαπίστευσης.	Η εξουσιοδότηση νομικής οντότητας εκδότη πρέπει να εγκριθεί από το EBSI ή άλλη αρχή.	
Root TAO **(Root Trusted Accreditation Organization)**	Αξιόπιστος εκδότης Διαπίστευσης	Μπορεί να αυτό-διαπιστευτεί και να εκδώσει Επαληθεύσιμες Διαπιστεύσεις (Διαπιστεύσεις, Βεβαιώσεις και Εξουσιοδοτήσεις) των διαπιστευμένων τύπων για νομικά πρόσωπα.	Πρέπει να έχει: **i.** καταχωρήσει το έγγραφο DID στο μητρώο DID. **ii.** εγγραφεί DID στο Μητρώο Αξιόπιστων Εκδοτών. **iii.** Επαληθεύσιμη Διαπίστευση καταχωρισμένη στο Μητρώο Αξιόπιστων Εκδοτών. **iv.** δώσει τύπους διαπίστευσης εγγεγραμμένους στο Μητρώο αξιόπιστων σχημάτων. **v.** διαπίστευση με συγκεκριμένους τύπους.	Ο πρωταρχικός σκοπός είναι η διαχείριση της αλυσίδας εμπιστοσύνης ώστε να συμμορφώνεται με την περίπτωση χρήσης. Επιτρέπει μια ιεραρχία που μπορεί να συμμορφώνεται με οποιοδήποτε μοντέλο διακυβέρνησης ή διαπίστευσης.

Actor (Σύνολο ενεργειών στοιχείων)	Role (Ρόλοι)	Capabilities (Δυνατότητες)	Requirements (Απαιτήσεις)	Description (Περιγραφή)
AO **(Αξιόπιστος Οργανισμός Διαπίστευσης)**	Αξιόπιστος Εκδότης Διαπίστευσης	Ο Εκδότης Διαπίστευσης Μπορεί να εκδίδει Επαληθεύσιμες Διαπιστεύσεις. (Διαπιστεύσεις, Βεβαιώσεις και Εξουσιοδοτήσεις) των διαπιστευμένων τύπων για νομικά πρόσωπα	Πρέπει να έχει Διαπίστευση για διαπίστευση με συγκεκριμένους τύπους.	Μπορεί να διαπιστεύσει άλλα νομικά πρόσωπα για την επέκταση της αλυσίδας εμπιστοσύνης. Ο πρωταρχικός σκοπός είναι η διαχείριση της αλυσίδας εμπιστοσύνης ώστε να συμμορφώνεται με την περίπτωση χρήσης. Επιτρέπει μια ιεραρχία που μπορεί να συμμορφώνεται με οποιοδήποτε μοντέλο διακυβέρνησης ή διαπίστευσης.
TI (Trusted Issuer)	Αξιόπιστος εκδότης βεβαίωσης	Μπορεί να εκδίδει Επαληθεύσιμες Βεβαιώσεις των διαπιστευμένων τύπων για φυσικά και νομικά πρόσωπα.	Πρέπει να έχει Διαπίστευση για να πιστοποιήσει με συγκεκριμένους τύπους.	Εκδίδει επαληθεύσιμα διαπιστευτήρια για τους τελικούς χρήστες

5.3 Παραδείγματα Ιεραρχίας

Το διάγραμμα 1 δείχνει μια ιεραρχία νομικών οντοτήτων, οι οποίες ενεργούν είτε ως Αξιόπιστος Εκδότης Διαπίστευσης (Root TAO and TAO) είτε ως Trusted Attestation Issuer.



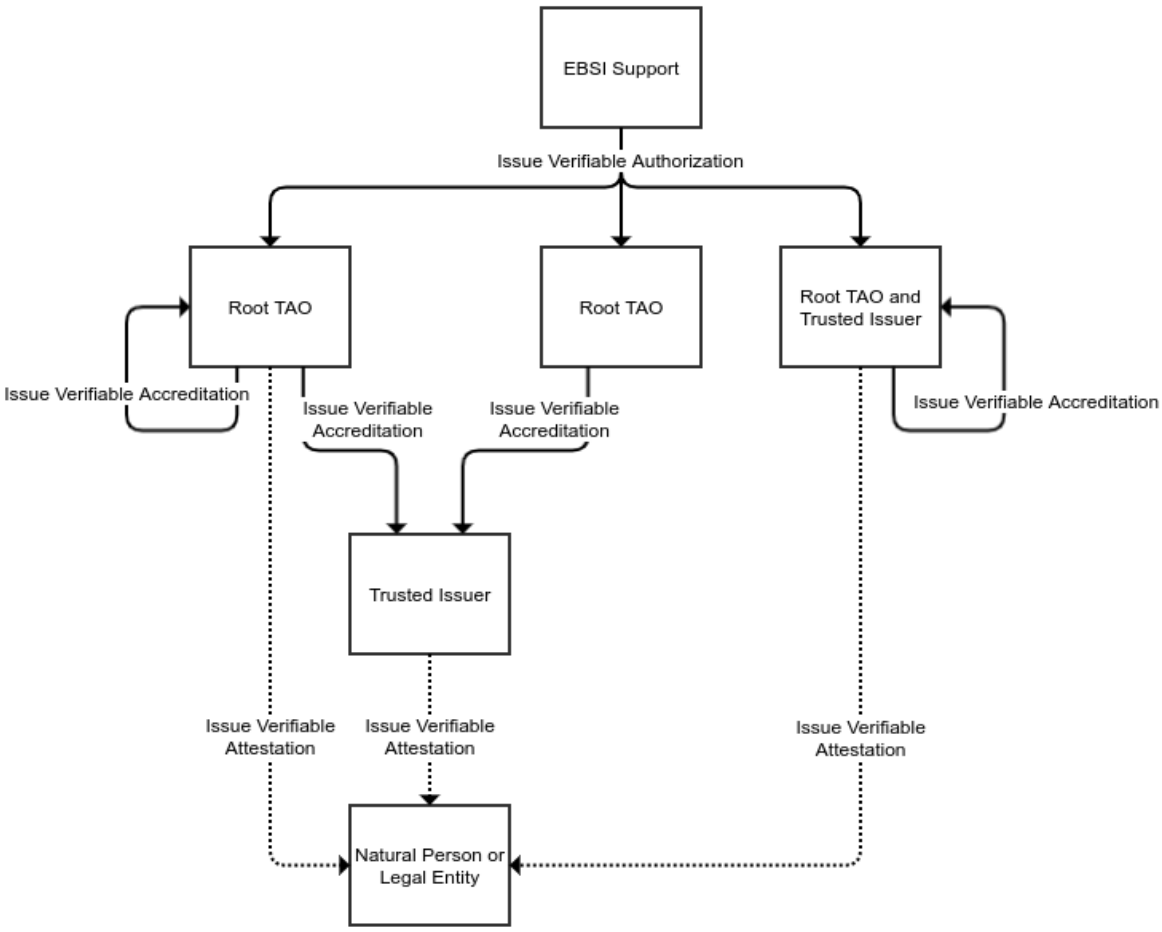
Διάγραμμα 1 (European Commission,2022)

5.3.1 Απλή αλυσίδα εμπιστοσύνης με νομικά πρόσωπα που εκπληρώνουν πολλαπλούς ρόλους (Trusted Accreditation AND Attestation Issuers).

Το διάγραμμα 2 δείχνει πολλούς διαπιστευτές ανώτατου επιπέδου, όπου μια μεμονωμένη νομική οντότητα είναι διαπιστευμένη από δύο μεμονωμένες αλυσίδες εμπιστοσύνης. Ο πιο δεξιός διαπιστευτής ανώτατου επιπέδου είναι αυτόνομος και δεν έχει ιεραρχία. Με άλλα λόγια, μια ενιαία νομική οντότητα μπορεί να εκπληρώσει πολλούς ρόλους:

- Root TAO (Trusted Accreditation Issuer που διαπιστεύει άλλους Trusted Accreditation Issuers)
- TAO (Αξιόπιστος Εκδότης Διαπίστευσης που διαπιστεύει τους Αξιόπιστους Εκδότες Πιστοποιήσεων)
- του αξιόπιστου εκδότη (Εκδότης αξιόπιστης βεβαίωσης που εκδίδει βεβαιώσεις σε φυσικό πρόσωπο ή νομική οντότητα (κάτοχοι)

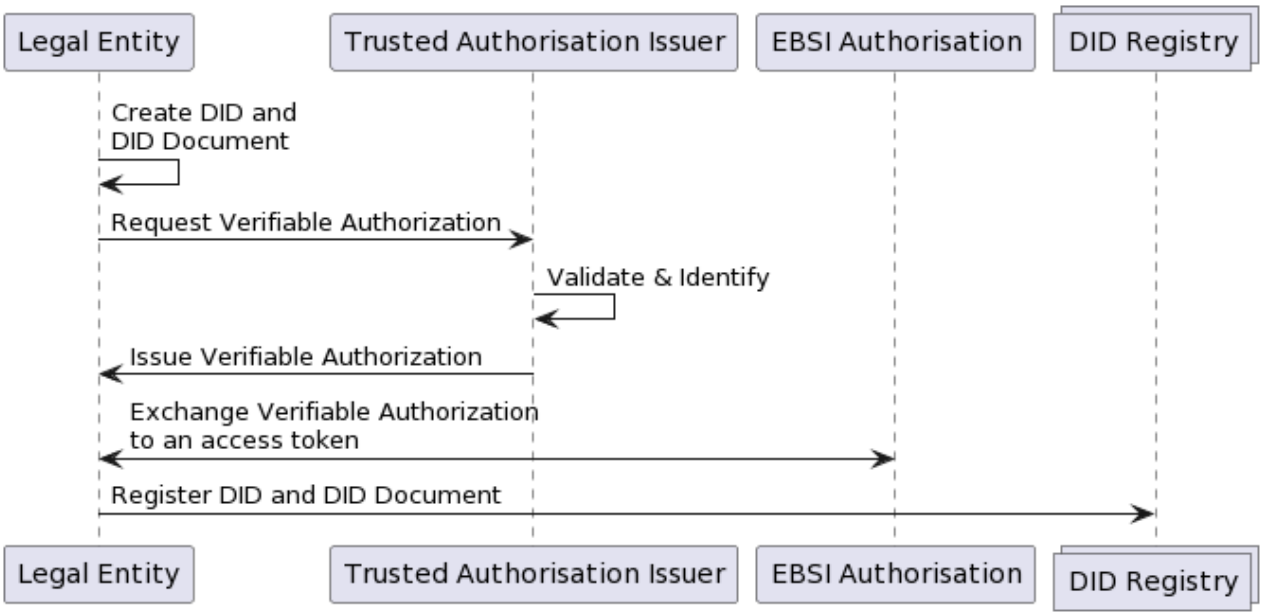
Η σχέση μεταξύ Αξιόπιστων Εκδοτών ορίζεται από την περίπτωση χρήσης και μπορεί να κυμαίνεται από μια απλή λίστα έως μια πολύπλοκη ιεραρχική δομή.



Διάγραμμα 2 (European Commission,2022)

5.3.2 Ένταξη σε Νομικό Πρόσωπο

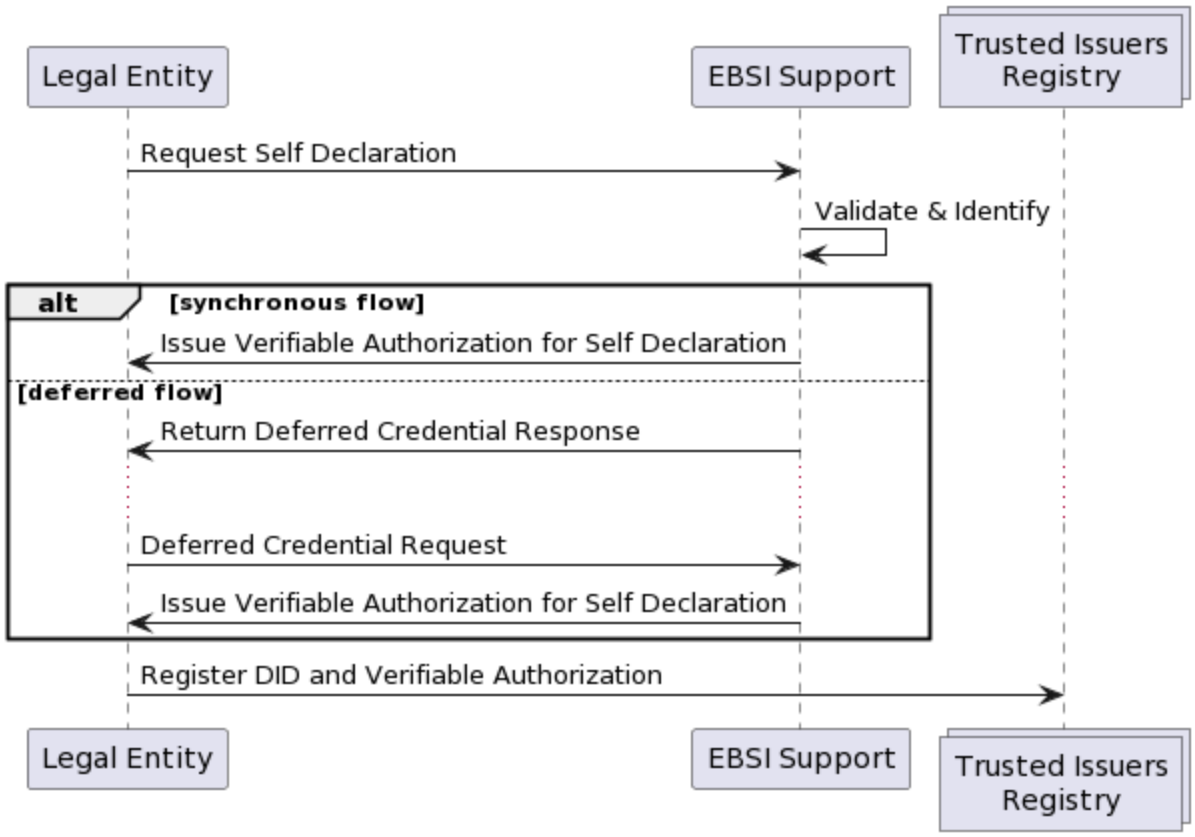
Η είσοδος σε μια νομική οντότητα ή ένα φυσικό πρόσωπο έχει μια μικρή διαφορά στη ροή. Η πρώτη διαφορά είναι το αναγνωριστικό για το EBSI DID Method και η δεύτερη είναι η καταχώριση του εγγράφου DID . Τα νομικά πρόσωπα πρέπει να καταχωρήσουν το DID και το DID Document τους, στο μητρώο DID σύμφωνα με τη μέθοδο DID για Νομικά Πρόσωπα. Αντίθετα, τα φυσικά πρόσωπα δεν καταχωρούν πουθενά το έγγραφο DID. Μια επισκόπηση υψηλού επιπέδου της ενσωμάτωσης μιας νομικής οντότητας παρουσιάζεται στο διάγραμμα 3.



Διάγραμμα 3 (European Commission,2022)

5.3.3 Διαπίστευση Νομικού Προσώπου - Νομικό Πρόσωπο Ανωτάτου Επιπέδου

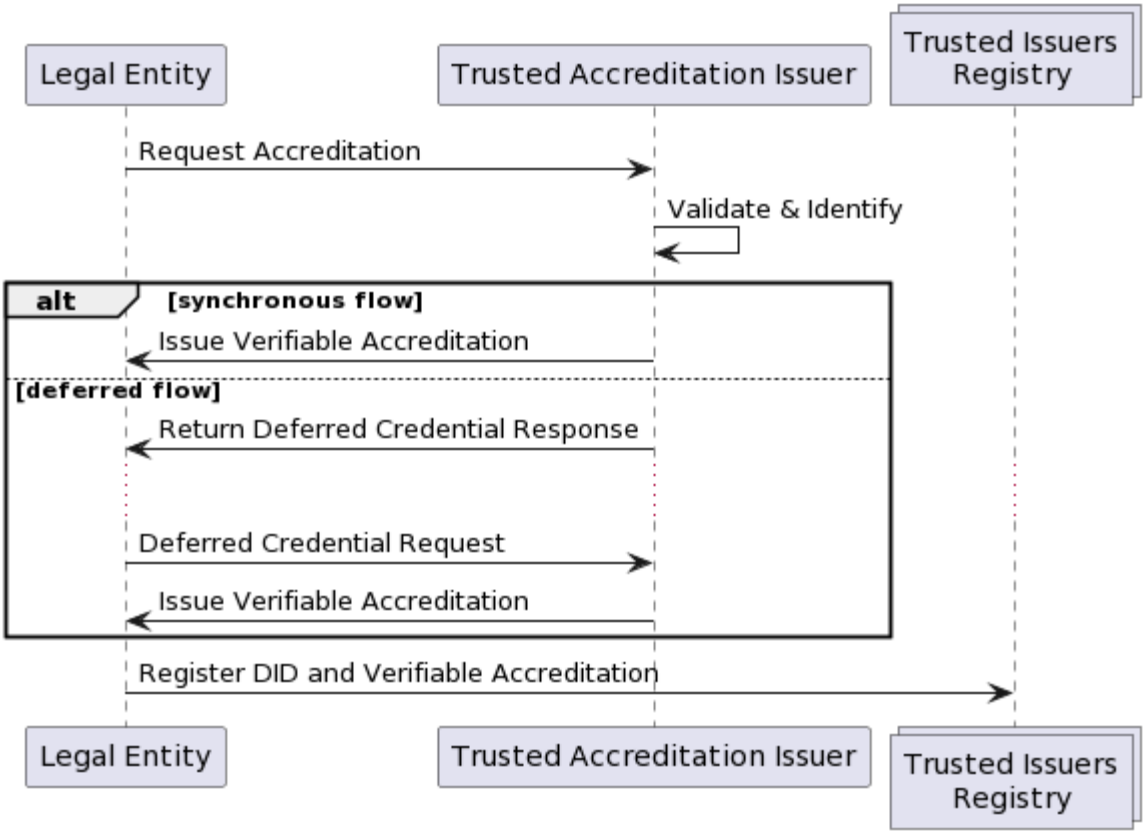
Το σημείο εμπιστοσύνης root ή του ανώτατου επιπέδου (Trusted Accreditation Issuer) λειτουργεί διαφορετικά από τα υπόλοιπα, καθώς το ανώτατο επίπεδο δηλώνεται από μόνο του. Μετά την εγγραφή μητρώο αξιόπιστων εκδοτών (TIR), η νομική οντότητα αυτό-δηλώνεται ως αξιόπιστος εκδότης διαπίστευσης για τα χαρακτηριστικά που ορίζονται στην επαληθεύσιμη εξουσιοδότηση. Η ροή καταλήγει σε μια εγγραφή στο μητρώο αξιόπιστων εκδοτών και στην κατοχή μιας Επαληθεύσιμης Εξουσιοδότησης μιας χρήσης. Η ληφθείσα Επαληθεύσιμη Εξουσιοδότηση δεν χρειάζεται πλέον μετά την εγγραφή, καθώς αποθηκεύεται στο μητρώο (TIR). Μια επισκόπηση παρουσιάζεται στο διάγραμμα 4.



Διάγραμμα 4 (European Commission,2022)

5.3.4 Νομικά Πρόσωπα Υποεπιπέδου

Μια νομική οντότητα μπορεί να έχει πολλαπλές διαπιστεύσεις από την ίδια ή διαφορετικές νομικές οντότητες. Μετά την εγγραφή στο TIR, η νέα διαπίστευση ισούται με τους διαπιστευμένους τύπους που ορίζονται στη συγκεκριμένη διαπίστευση. Η ροή καταλήγει σε μια εγγραφή TIR και στην κατοχή μιας επαληθεύσιμης διαπίστευσης μιας χρήσης. Η ληφθείσα Επαληθεύσιμη Διαπίστευση δεν χρειάζεται πλέον μετά την εγγραφή, καθώς αποθηκεύεται στο TIR. Το νομικό πρόσωπο μπορεί να ζητήσει διαπιστεύσεις για διαπίστευση, βεβαίωση ή εξουσιοδότηση, όπως παρουσιάζεται στο διάγραμμα 5.



Διάγραμμα 5 (European Commission,2022)

6. *OpenID για επαληθεύσιμα διαπιστευτήρια*

6.1 Το OpenID για τα επαληθεύσιμα διαπιστευτήρια η σημασία τους

Τα περισσότερα πρωτόκολλα επιτρέπουν μόνο στους κατόχους να εξουσιοδοτούν επαληθευτές που είναι σε σχέση με τον εκδότη και να έχουν πρόσβαση στις πληροφορίες. Ο κάτοχος, δεν μπορεί να μοιραστεί πληροφορίες με τον επαληθευτή που επιθυμεί. Στο νέο μοντέλο αυτοκυριαρχίας η ανταλλαγή πληροφοριών επιτρέπεται στους κατόχους, και δίνεται η δυνατότητα να μοιράζονται τις πληροφορίες τους με οποιονδήποτε θέλουν. Υπάρχουν τέσσερα πρότυπα για να καταστεί δυνατή η νέα ανταλλαγή πληροφοριών. Καθώς δεν υπάρχει ενιαίο πρωτόκολλο για την ανταλλαγή επαληθεύσιμων διαπιστευτηρίων, υπάρχουν λίγες εναλλακτικές λύσεις.

i. OpenID για Επαληθεύσιμο
Το OpenID Foundation είναι τυποποίηση μιας οικογένειας προδιαγραφών OpenID για επαληθεύσιμα διαπιστευτήρια για αυτοκυρίαρχη έκδοση και παρουσίαση επαληθεύσιμων διαπιστευτηρίων.

ii. Διαπιστευτήρια ISO 18013-5 (mDL)
Το ISO τυποποιεί το 18013-5 για την ανταλλαγή άδειας οδήγησης εκτός σύνδεσης για κινητά και το 23220 (ο OpenID για VC είναι μέρος του προτύπου) για την ηλεκτρονική ανταλλαγή διαπιστευτηρίων.

iii. Πιστοποιητικό Έκδοση και Παρούσα Απόδειξη
Το Hyperledger τυποποιεί τα πρωτόκολλα Issue Credential και Present Proof. (Το πρωτόκολλο υλοποιείται πάνω από το πρωτόκολλο DIDCommmessaging)

iv. WACI

Το DIF τυποποιεί το πρωτόκολλο Αλληλεπίδρασης Πορτοφολιού και Διαπιστευτηρίων (WACI το πρωτόκολλο υλοποιείται πάνω από το πρωτόκολλο DIDCommmessaging) για την έκδοση και παρουσίαση επαληθεύσιμων διαπιστευτηρίων

Το EBSI επέλεξε το OpenID πρωτόκολλο επαληθεύσιμων διαπιστευτηρίων. Το OpenID Foundation είναι τυποποίηση μιας οικογένειας ανοιχτών προδιαγραφών OpenID για επαληθεύσιμα διαπιστευτήρια για το αυτοκυριαρχικό μοντέλο κα την παρουσίαση επαληθεύσιμων διαπιστευτηρίων. Το OpenID είναι ένα ανοιχτό πρότυπο, υψηλού επιπέδου, ωριμότητας, και βασίζονται σε αποδεδειγμένα βιομηχανικά πρότυπα OIDC και OAuth.

- **OAuth και OpenID Connect (OIDC)**
  Πρωτόκολλο που υποστηρίζει την ανταλλαγή διαπιστευτηρίων βάσει εξουσιοδότησης όπου ο κάτοχος εξουσιοδοτεί έναν επαληθευτή (πελάτη) να έχει πρόσβαση σε πληροφορίες για λογαριασμό του.
- **OpenID για VC (OID4VC)**
  Πρωτόκολλο που υποστηρίζει την ανταλλαγή διαπιστευτηρίων αυτοκυριαρχίας όπου ο κάτοχος μπορεί να ελέγχει αυτόνομα την ανταλλαγή διαπιστευτηρίων με όποιον επαληθευτή θέλει.

Το OID4VCs αποτελείται από τρία πρότυπα. Δύο από αυτά χρησιμοποιούνται από το EBSI. Το OpenID για επαληθεύσιμα διαπιστευτήρια (OID4VCs) είναι μια συλλογή τριών προτύπων που επιτρέπουν τον έλεγχο ταυτότητας αυτοτελούς κυριαρχίας και την έκδοση και παρουσίαση επαληθεύσιμων διαπιστευτηρίων. Το EBSI χρησιμοποιεί αυτά για την έκδοση και παρουσίαση VC.

1. **Αυθεντικοποίηση (SIOPv2)**
   Καθορίζει τον τρόπο με τον οποίο οι κάτοχοι μπορούν να πιστοποιήσουν την ταυτότητα με έναν αυτοκυρίαρχο τρόπο. Ο EBSI υποστηρίζει οποιουσδήποτε άλλους ελέγχους ταυτότητας και δεν περιορίζεται στο SIOPv2 για έλεγχο ταυτότητας κατόχου.
2. **Έκδοση OpenID για Επαληθεύσιμο Πιστοποιητικό Έκδοση (OID4VCI)**
   Καθορίζει τα API και τους αντίστοιχους μηχανισμούς εξουσιοδότησης που βασίζονται στο OAuth2 για την έκδοση επαληθεύσιμων διαπιστευτηρίων.
3. **Παρουσίαση OpenID για Επαληθεύσιμο Παρουσιάσεις (OID4VP)**
   Καθορίζει μηχανισμούς πάνω από το OAuth2 για να επιτρέπεται η παρουσίαση αξιώσεων με τη μορφή επαληθεύσιμων διαπιστευτηρίων.

6.2 Λειτουργία OpenID για τα επαληθεύσιμα διαπιστευτήρια

6.2.1 OpenID για επαληθεύσιμη έκδοση διαπιστευτηρίων

6.2.1.1 Η επαληθεύσιμη έκδοση διαπιστευτηρίων αποτελείται από τέσσερις βασικές ενέργειες:

- **Αίτημα VC**

Ένας κάτοχος ξεκινά την έκδοση στον ιστότοπο του εκδότη και το πορτοφόλι λαμβάνει πληροφορίες σχετικά με τον τύπο των επαληθεύσιμων διαπιστευτηρίων που ζητούνται από τον κάτοχο στον ιστότοπο του εκδότη μέσω ενός κωδικού QR ή μιας ανακατεύθυνσης στο πορτοφόλι. Αυτό το βήμα παραλείπεται εάν ο χρήστης ζητήσει VC από το πορτοφόλι. Το Wallet λαμβάνει μεταδεδομένα εκδότη για να μάθει σχετικά με τις υποστηριζόμενες ροές, μορφές, υπογραφές και τελικά σημεία. Το

OID4VCI επεκτείνει τα μεταδεδομένα OAuth2. Το Πορτοφόλι ζητά ένα επαληθεύσιμο διαπιστευτήριο. Το αίτημα εξουσιοδότησης είναι ένα εκτεταμένο αίτημα εξουσιοδότησης OAuth2 όπου το πορτοφόλι μπορεί να καθορίσει τον τύπο και τη μορφή του VC και τον τύπο και τη μορφή υπογραφής.

- **Έλεγχος ταυτότητας**

Ο κάτοχος επαληθεύει την ταυτότητα με τον εκδότη μέσω της μεθόδου ελέγχου ταυτότητας που υποστηρίζεται από τον εκδότη.

- **Έκδοση VC**

Πιστοποιώ την αυθεντικότητα. Μετά από έναν επιτυχημένο έλεγχο ταυτότητας, το πορτοφόλι λαμβάνει έναν κωδικό OAuth2 τον οποίο στέλνει στο τελικό σημείο του διακριτικού OAuth2, λαμβάνει ένα διακριτικό πρόσβασης και μια πρόκληση για να αποδείξει τον έλεγχο του κλειδιού DID. Ο εκδότης επιστρέφει ένα διακριτικό πρόσβασης και μια πρόκληση που καλείται να υπογράψει. Ο κάτοχος πρέπει να υπογράψει την πρόκληση με τα κλειδιά DID της για να αποδείξει τον έλεγχο των κλειδιών DID.

- **Συλλέξτε VC**

Ο εκδότης εκδίδει ένα VC και ειδοποιεί το πορτοφόλι να το παραλάβει.

6.2.1.2 Το OpenID4VCI

Η επαληθεύσιμη έκδοση διαπιστευτηρίων αποτελείται από τέσσερις βασικές ενέργειες:

- **Αίτημα VC**

Ένας μηχανισμός για τον εκδότη να δημοσιεύει μεταδεδομένα σχετικά με υποστηριζόμενους τύπους, μορφές και υπογραφές VC. Μηχανισμοί για την έναρξη της έκδοσης (Μέσω του ιστότοπου του εκδότη και μέσω του πορτοφολιού). Δύο επαληθεύσιμες ροές έκδοσης διαπιστευτηρίων (προεγκεκριμένη ροή και ροή εξουσιοδότησης). Αίτημα εξουσιοδότησης που επιτρέπει στα πορτοφόλια να ζητούν εξουσιοδότηση για να ζητήσουν την έκδοση Επαληθεύσιμων Διαπιστευτηρίων.

- **Έλεγχος ταυτότητας**
- **Έκδοση VC**

Ένα νέο τελικό σημείο προστασίας διαπιστευτηρίων OAuth2 για εκδότες όπου τα πορτοφόλια συλλέγουν τα εκδοθέντα διαπιστευτήρια**.** Ο μηχανισμός δέσμευσης των εκδοθέντων διαπιστευτηρίων σε κρυπτογραφικό κλειδί ή πιστοποιητικό.

- **Συλλέξτε VC**

Ένας μηχανισμός για έγκαιρη ή αναβαλλόμενη έκδοση VC.

6.3 Πορτοφόλι και επαληθεύσιμα διαπιστευτήρια

6.3.1 Αίτημα Ελέγχου ταυτότητας

Μπορούν να ζητηθούν επαληθεύσιμα διαπιστευτήρια βάσει κριτηρίων. Η περιγραφή του αιτήματος ελέγχου ταυτότητας περιλαμβάνει.

- **Μεταδεδομένα αιτήματος ελέγχου ταυτότητας (Authentication request metadata)** Τα μεταδεδομένα αιτήματος ελέγχου ταυτότητας περιέχουν τον τυπικό έλεγχο ταυτότητας OAuth2. Όταν ζητηθούν οι αξιώσεις, το πορτοφόλι να μπορεί να μάθει τα πάντα για τον επαληθευτή (τελικά σημεία, υποστηριζόμενες μορφές, υπογραφές κ.λπ.) και για την προστασία της παρουσίασης.
- **Ορισμός παρουσίασης (Presentation Definition)** Ο ορισμός παρουσίασης είναι μέρος της γλώσσας έκφρασης Presentation Exchange που επιτρέπει την αίτηση ενός ή περισσότερων επαληθεύσιμων διαπιστευτηρίων ανά τύπο διαπιστευτηρίου ή με βάση τα συμφραζόμενα κριτήρια.
- **Περιγραφές εισόδου (Input descriptors)** Οι περιγραφείς εισόδου χρησιμοποιούνται για να ορίσουν ποιες πληροφορίες ζητούνται από τον επαληθευτή. Ο επαληθευτής μπορεί να ζητήσει ένα συγκεκριμένο VC ανά τύπο αναφέροντας το σχήμα JSON (π.χ. στο Μητρώο αξιόπιστων σχημάτων EBSI) ή μπορείτε να ζητήσετε VC καθορίζοντας ποιες αξιώσεις πρέπει να έχουν το VC (π.χ. όνομα, επώνυμο, διεύθυνση).
- **Μορφή (Format)** Η μορφή μπορεί να χρησιμοποιηθεί για τον καθορισμό των απαιτούμενων επαληθεύσιμων διαπιστευτηρίων και παρουσίασης.

Εικόνα 11 Αίτημα Ελέγχου Ταυτότητας

6.3.2 Επαληθεύσιμη παρουσίαση

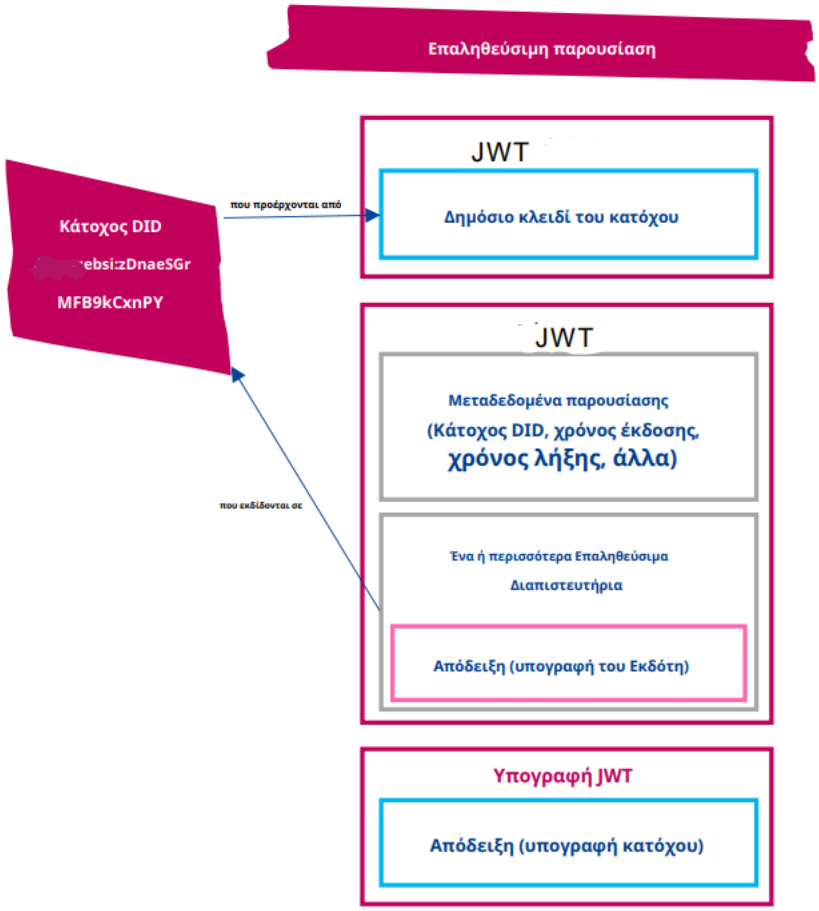
Οι επαληθεύσιμες παρουσιάσεις είναι αυτοεκδοθέντες και αυτοτελείς. Μια επαληθεύσιμη παρουσίαση περιγράφεται στην εικόνα 12 και περιλαμβάνει τα ακόλουθα:

- **Επικεφαλίδα JWT**. Δημόσιο κλειδί στην κεφαλίδα υπάρχει το δημόσιο κλειδί DID του κατόχου που πρέπει να επαληθεύσει την υπογραφή VP.
- **Κύριος Σώμα**

Μεταδεδομένα παρουσίασης: περιέχει πληροφορίες σχετικά με το DID του κατόχου, το οποίο πρέπει να προέρχεται από το δημόσιο κλειδί που είναι κοινόχρηστο στην κεφαλίδα, και άλλες τυπικές αξιώσεις VP. Ένα ή περισσότερα επαληθεύσιμα διαπιστευτήρια είναι ενσωματωμένα στο VP. Τα επαληθεύσιμα διαπιστευτήρια πρέπει να εκδίδονται στο ίδιο DID όπως στα μεταδεδομένα παρουσίασης. Εάν τα VC εκδίδονται σε πολλαπλά DID, ο κάτοχος θα πρέπει να παρουσιάσει πολλαπλές επαληθεύσιμες παρουσιάσεις.

- **Υπογραφή**

Απόδειξη είναι η υπογραφή του κατόχου της Επαληθεύσιμης Παρουσίασης. Το δημόσιο κλειδί στην επικεφαλίδα πρέπει να επαληθεύει την υπογραφή.



Εικόνα 12 Επαληθεύσιμη Παρουσίαση

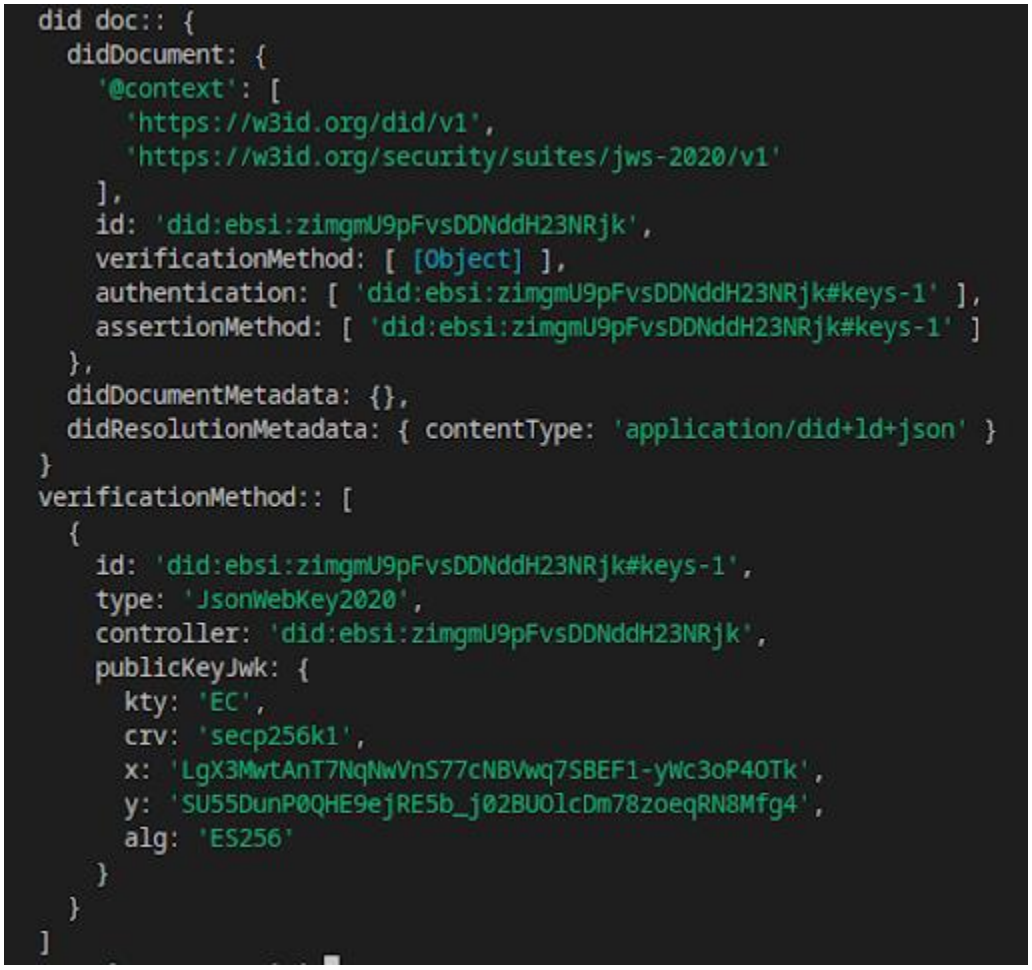
7. Υλοποίηση λειτουργιών που αφορούν την διαδικασία των επαληθεύσιμων διαπιστευτηρίων

Στο παρόν κεφάλαιο παρουσιάζεται η υλοποίηση των διαδικασιών των επαληθεύσιμων διαπιστευτηρίων. Συγκεκριμένα πραγματοποιούμε την ανάκτηση ενός DID document με βάση το αναγνωστικό DID. Στη συνέχεια ο παράγοντας ενός νομικού προσώπου χρησιμοποιεί ένα DID και το επικυρώνει στο μητρώο DID. Το συμβαλλόμενο μέλος χρησιμοποιεί μια εφαρμογή η οποία επικυρώνεται στο μητρώο έμπιστων εφαρμογών (Trusted Apps Registry) . Αυτή η διαδικασία πραγματοποιείται μέσω της υλοποίησης του EBSI SIOP Auth. Για κάθε διαδικασία παρουσιάζεται το αντίστοιχο τμήμα του κώδικα, χωρισμένο σε βήματα και από κάτω δίνεται το αποτέλεσμα του κάθε βήματος που πραγματοποιήθηκε.
Στο τέλος παρουσιάζονται τα τμήματα κώδικα για τη δημιουργία ενός επαληθεύσιμου διαπιστευτηρίου.

7.1 DID RESOLVER

```
import { Resolver } from "did-resolver";

import { getResolver } from "@cef-ebsi/ebsi-did-resolver";

// You must set the address of the DID Registry to be used in order to resolve Legal Entities DID Documents

const resolverConfig = {registry:"https://api.preprod.ebsi.eu/didregistry/v3/identifiers",};

// getResolver will return an object with a key/value pair of {"ebsi": resolver } where resolver is a function used by the generic did resolver.

const ebsiDidResolver = getResolver(resolverConfig);

const didResolver = new Resolver(ebsiDidResolver);

// You can also use ES7 async/await syntax

const doc = await didResolver.resolve("did:ebsi:zub5ZZUfHLLptCduwEy8xRj");
console.log("Doc::",doc);
```

Η βιβλιοθήκη EBSI DID Resolver παρέχει την συνάρτηση resolve() η οποία μας επιστρέφει ένα DID document. Αυτό δε σημαίνει ότι μπορεί να χρησιμοποιηθεί άμεσα αλλά μέσω του did-resolver aggregator. Μπορούμε να χρησιμοποιήσουμε τη μέθοδο getResolver(config) ώστε να γίνει δημιουργία και χρήση της κλάσης Resolver.



Εικόνα 13 DID Document

7.2 SIOP Authentication

Βήμα 0 : Αρχικά δημιουργείται ένα συμβαλλόμενο μέλος.

```
import { RP, Agent, verifyJwtTar, verifyJwtDid } from "@cef-ebsi/siop-auth";
import { calculateJwkThumbprint, exportJWK, generateKeyPair } from
"jose";
const privateKeyRP = (await generateKeyPair("ES256K")).privateKey;
const rp = new RP({
  privateKey: privateKeyRP,
  alg: "ES256K",
  name: "test-appj2",
  kid: "https://api.test.intebsi.xyz/trusted-apps-registry/v3/apps/test-appj2",
  redirectUri: "http://localhost:3000",
  didRegistry: "https://api.test.intebsi.xyz/did-registry/v3/identifiers",
});
```

Βήμα 0: Η δημιουργία ενός παράγοντα για το νομικό πρόσωπο

```
const privateKeyAgent = (await generateKeyPair("ES256K")).privateKey;
const agent = new Agent({
    privateKey: privateKeyAgent,
    alg: "ES256K",
    kid: "did:ebsi:z21oU6xvBhsUQM49nw8KydE6#keys-1",
    siopV2: true,
  });
  console.log("--------------------------------------------------")
  console.log("--------------------------------------------------")
```

Η ροή της επαλήθευσης ακολουθεί τα παρακάτω βήματα, τα οποία περιλαμβάνουν ένα φυσικό πρόσωπο ή μια νομική οντότητα και ένα συμβαλλόμενο μέλος.

Βήμα 1: Το συμβαλλόμενο μέλος δημιουργεί ένα αίτημα επαλήθευσης

```
1. The RP creates an authentication request

 console.log("1. The RP creates an authentication request")

 console.log("--------------------------------------------------")

 console.log("--------------------------------------------------")


 const uri = await rp.createRequest({

  claims: { },

  extraField: "extra data",

 });
```

```
1. The RP creates an authentication request
--------------------------------------------------
--------------------------------------------------
Uri:: openid:///?response_type=id_token&client_id=http%3A%2F%2Flocalhost%3A3000&scope=openid+did_authn&nonce=e962f8cb-7f4a-43a2-a8a9-93ea69a51afb&request=eyJhbGciOiJFUzI1NksiLCJ0eXAiOi
JKV1QiLCJraWQiOiJodHRwczovL2FwaS50ZXN0LmludGVic2kueHl6L3RydXN0ZWQtYXBwcy1yZWdpc3RyeS92My9hcHBzL3Rlc3QtYXBwajIifQ.eyJzY29wZSI6Im9wZW5pZCBkaWRfYXV0aG4iLCJyZXNwb25zZV90eXBlIjoiaWRfdG9rZW
4iLCJyZXNwb25zZV9tb2RlIjoicG9zdCIsImNsaWVudF9pZCI6Imh0dHA6Ly9sb2NhbGhvc3Q6MzAwMCIsInJlZGlyZWN0X3VyaSI6Imh0dHA6Ly9sb2NhbGhvc3Q6MzAwMCIsIm5vbmNlIjoiZTk2MmY4Y2ItN2Y0YS00M2EyLWE4YTktOTNlY
TY5YTUxYWZiIiwiY2xhaW1zIjp7fSwiZXh0cmFGaWVsZCI6ImV4dHJhIGRhdGEiLCJpYXQiOjE2Njk0ODk5NzcsImlzcyI6InRlc3QtYXBwajIiLCJleHAiOjE2Njk0OTAyNzd9.v7PIPSqoWaKXnkVmrUQsYVGpV2Nrt-YTfKlPekRyidv_iDI
rgXiT_TgeXaBGzkZAk1tmO1vqyjqbkUFRtjbGsg
```

Εικόνα 14 Δημιουργία Request

Βήμα 2: Ο παράγοντας του νομικού προσώπου πιστοποιεί το αίτημα επαλήθευσης

```
console.log("2 The agent verifies the authentication request")
console.log("-----------------------------------------------------")
console.log("-----------------------------------------------------")
const urlParams = new URLSearchParams(uri.replace("openid://?", ""));
const { payload: payloadReq } = await verifyJwtTar(urlParams.get("request"), {
 trustedAppsRegistry:
   "https://api.test.intebsi.xyz/trusted-apps-registry/v3/apps",
});
console.log("")
console.log("PayloadReq",payloadReq);
```

```
2 The agent verifies the authentication request
-----------------------------------------------------
-----------------------------------------------------

PayloadReq {
  scope: 'openid did_authn',
  response_type: 'id_token',
  response_mode: 'post',
  client_id: 'http://localhost:3000',
  redirect_uri: 'http://localhost:3000',
  nonce: '33e7518b-b329-4824-809d-d1f548be850d',
  claims: {},
  extraField: 'extra data',
  iat: 1644836701,
  iss: 'test-appj2',
  exp: 1644837001
}
```

Εικόνα 15 Πιστοποίηση Authentication Request

Βήμα 3: Ο παράγοντας του νομικού προσώπου δημιουργεί την απάντηση για το αίτημα επαλήθευσης

```
const alg = "ES256K"

const encryptionKeyPair =
  alg === "EdDSA"
    ? crypto.generateKeyPairSync("x25519")
    : await generateKeyPair(alg);
const publicEncryptionKeyJwk = await exportJWK(encryptionKeyPair.publicKey);
const privateEncryptionKeyJwk = await exportJWK(encryptionKeyPair.privateKey);
const nonce =urlParams.get("nonce");
const { urlEncoded } = await agent.createResponse({
  nonce,
  redirectUri: "http://localhost:3000",
  claims: {
    encryption_key: publicEncryptionKeyJwk,
  },
  extraField: "extra data",
});
console.log("UrlEncoded::",urlEncoded);
```

```
--------------------------------------------------
3 The agent creates an authentication response
--------------------------------------------------
--------------------------------------------------
UrlEncoded:: http://localhost:3000#id_token=eyJhbGciOiJFUzI1NksiLCJ0eXAiOiJKV1QiLCJraWQiOiJkaWQ6ZWJzaTp6MjFvVTZ4dkJoc1VRTTQ5bnc4S3lkRTYja2V5cy0xIn0.eyJhdWQiOiJodHRwOi8vbG9jYWxob3N0OjMwMDAiLCJzdWIiOiI1QVlXSDhBOTNxdF8wUU1uRzdzTXpIenNMUjVjTGhpQTNEWnNUZHhvVG9rIiwic3ViX2p3ayI6eyJrdHkiOiJFQyIsIngiOiI1di1kN3dORTNQMXotR1JMaTZ1dk14blZZUkxlVUp6cmc1SWk4ME5LQWk0IiwieSI6IjBrNnBRWEtNWEU1cGw2WGdSWlMxMEQwTzJCT3JLREpaUENmNTNtYWdkZkEiLCJjcnYiOiJzZWNwMjU2azEifSwibm9uY2UiOiJlOTYyZjhjYi03ZjRhLTQzYTItYThhOS05M2VhNjlhNTFhZmIiLCJjbGFpbXMiOnsiZW5jcnlwdGlvbl9rZXkiOnsia3R5IjoiRUMiLCJ4IjoiaXdtMXJZaUhEVFFtZjFtdzdjNDBmM1lNZERzZzRpM0QxVnFHTFFOdEV5YyIsInkiOiJWZlpHa2J0TFJfMmNvS2w5NU1GT1hqUzhpZTdkY0NlckFZWkFrU0c4X18wIiwiY3J2Ijoic2VjcDI1NmsxIn19LCJleHRyYUZpZWxkIjoiZXh0cmEgZGF0YSIsImlhdCI6MTY2OTQ4OTk3NywiaXNzIjoiaHR0cHM6Ly9zZWxmLWlzc3VlZC5tZS92MiIsImV4cCI6MTY2OTQ5MDI3N30.CsErI3c8m3DG2ilcwtfxbJO9YrUfgdeh4IhW0XeprPV0Q3lLDI0aCAbmPoX7umUZxj3YuhCGBb6twIVoJKM6rA
```

Εικόνα 16 Απάντηση Authentication Request

Βήμα 4: Το συμβαλλόμενο μέλος επαληθεύει την απάντηση.

```
const idTokenAuthResponse = new URLSearchParams(
   urlEncoded.substring(urlEncoded.indexOf("#") + 1)
 ).get("id_token");
 const resVerification = await RP.verifyResponse(
  idTokenAuthResponse,
  async (claims) => {
   if (!claims || !claims.encryption_key)
     throw new Error("no encryption_key found in the claims");
  const { didDocument } = await verifyJwtDid(idTokenAuthResponse, {
   didRegistry: "https://api.test.intebsi.xyz/did-registry/v3/identifiers",
  });
  const did = didDocument?.id ?? "";
   return { ...claims, did };
  }
 );
 console.log("resVerification:",resVerification);
```

```
4 The RP verifies the authentication response It expects a callback to validate custom claims.
-------------------------------------------------
-------------------------------------------------
resVerification: {
  payload: {
    did: 'did:ebsi:z21oU6xvBhsUQM49nw8KydE6',
    aud: 'http://localhost:3000',
    sub: 'ySg9VLABPynDyofayy0bLMiVsh5dlcHX5p6cMMLJapY',
    sub_jwk: {
      kty: 'EC',
      x: '9LvxdmTRiw-Jsx4pbSWlnF3R48Q-wAzHdvkYmWDRu78',
      y: 'P4iNFkyJehOAO9KYHKjqH0zu5CIg5s3JsjMRpfee-fw',
      crv: 'secp256k1'
    },
    nonce: '8f7b3321-84e0-45f4-914c-da7f09c341e1',
    claims: { encryption_key: [Object] },
    extraField: 'extra data',
    iat: 1669495045,
    iss: 'https://self-issued.me/v2',
    exp: 1669495345
  },
  header: {
    alg: 'ES256K',
    typ: 'JWT',
    kid: 'did:ebsi:z21oU6xvBhsUQM49nw8KydE6#keys-1'
  },
  resultClaims: {
    encryption_key: {
      kty: 'EC',
      x: '6n26Yf7ivwfPq12SJofW-zUsNCBoBWiBtQJeUqK1lus',
      y: '-zn8rWZID9byrDRMUAKzd-KEsFvFf76qWlImQ70NmpI',
      crv: 'secp256k1'
    },
    did: 'did:ebsi:z21oU6xvBhsUQM49nw8KydE6'
  }
}
resVerification.payload.claims: {
  encryption_key: {
    kty: 'EC',
    x: '6n26Yf7ivwfPq12SJofW-zUsNCBoBWiBtQJeUqK1lus',
    y: '-zn8rWZID9byrDRMUAKzd-KEsFvFf76qWlImQ70NmpI',
    crv: 'secp256k1'
  }
}
```

Εικόνα 17 Το συμβαλλόμενο μέλος επαληθεύει την απάντηση

Βήμα 5: Το συμβαλλόμενο μέλος δημιουργεί ένα access token

```
const akeAccessToken = await rp.createAccessToken(resVerification);

console.log(akeAccessToken);
```

Εικόνα 18 Access token

Βήμα 6: Ο παράγοντας του νομικού προσώπου πιστοποιεί την απάντηση (με χρήση του AKE protocol format) και λαμβάνει ένα access token.

```
const accessToken = await Agent.verifyAkeResponse(akeAccessToken, {
   nonce,
   privateEncryptionKeyJwk,
   trustedAppsRegistry:
    "https://api.test.intebsi.xyz/trusted-apps-registry/v3/apps",
   alg: "ES256K",
 });
 console.log("accessToken:",accessToken);
```

Εικόνα 19 Πιστοποίηση της απάντηση και λήψη access token.

Βήμα 7: Μία διαφορετική υπηρεσία πιστοποιεί το access token

```
const accessToken2 = await verifyJwtTar(accessToken, {
   trustedAppsRegistry:
    "https://api.test.intebsi.xyz/trusted-apps-registry/v3/apps",
   audience: "ebsi-core-services",
 });
 console.log("accessToken2:",accessToken2);
```

```
7 A different service verifies the access token
------------------------------------------------
------------------------------------------------
accessToken2: {
  payload: {
    scope: 'openid did_authn',
    response_type: 'id_token',
    response_mode: 'post',
    client_id: 'http://localhost:3000',
    redirect_uri: 'http://localhost:3000',
    nonce: '33e7518b-b329-4824-809d-d1f548be850d',
    claims: {},
    extraField: 'extra data',
    iat: 1644836701,
    iss: 'test-appj2',
    exp: 1644837001
  },
  payloadReq: 42,
  id: 1
}
```

Εικόνα 20 Πιστοποίηση access token

7.3 Verifiable Credential

Δημιουργούνται και επαληθεύονται τα επαληθεύσιμα διαπιστευτήρια W3C που είναι συμβατά με το EBSI σε μορφή JWT.

Δημιουργία ενός αντικειμένου EBSIIssuer για την υπογραφή JWT

```
import type { EbsiIssuer } from "@cef-ebsi/verifiable-credential";

const issuer: EbsiIssuer = {

  did: "did:ebsi:zgPs5MVWHwJJb4g9kZvYf3e",

  kid: "did:ebsi:zgPs5MVWHwJJb4g9kZvYf3e#keys-1",

  publicKeyJwk: <JWK>,

  privateKeyJwk: <JWK>,

  alg: "ES256K",

};
```

Δημιουργία ενός επαληθεύσιμου διαπιστευτηρίου. Για να δημιουργηθεί ένα έγκυρο JWT, ο εκδότης πρέπει να είναι εγγεγραμμένος στο Μητρώο Αξιόπιστων Εκδοτών.

```
import { createVerifiableCredentialJwt } from "@cef-ebsi/verifiable-credential";

import type { EbsiVerifiableAttestation } from "@cef-ebsi/verifiable-credential";

const vcPayload: EbsiVerifiableAttestation = {

  "@context": ["https://www.w3.org/2018/credentials/v1"],

  id: "urn:did:123456",

  type: ["VerifiableCredential", "VerifiableAttestation", "VerifiableId"],

  issuer: "did:ebsi:zgPs5MVWHwJJb4g9kZvYf3e",

  issuanceDate: "2021-11-01T00:00:00Z",

  validFrom: "2021-11-01T00:00:00Z",

  credentialSubject: {

    id: "did:ebsi:zYud7H5Wvf9ksRUrmTrFo9D",

    personalIdentifier: "IT/DE/1234",

    familyName: "Castafiori",

    firstName: "Bianca",

    dateOfBirth: "1930-10-01",

  },

  credentialSchema: {

    id: "https://api-test.ebsi.eu/trusted-schemas-registry/v2/schemas/0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49",

    type: "FullJsonSchemaValidator2021",

  },

  expirationDate: "2031-11-30T00:00:00Z",

  issued: "2021-10-30T00:00:00Z",

};
```

Καθορισμός των επιλογών για την επικύρωση του εκδότη και του διαπιστευτηρίου.

```
const options = {
  // EBSI URI Authority ([userinfo "@"] host [":" port])
  ebsiAuthority: "api-test.ebsi.eu",
};
```

Δημιουργία ενός JWT το οποίο έχει υπογραφθεί από τον παραπάνω εκδότη χρησιμοποιώντας τη συνάρτηση createVerifiableCredentialJwt.

```
const vcJwt = await createVerifiableCredentialJwt(vcPayload, issuer, options);
console.log(vcJwt);
//eyJraWQiOiJkaWQ6ZWJzaTp6Z1Bz...j9Pv1HSIR9aPXIVRMGYfjhmQH8oSM03
```

Πιστοποίηση των JWTs. Η πιστοποίηση του JWT στα επαληθεύσιμα διαπιστευτήρια πραγματοποιείται με τη συνάρτηση verifyCredentialJwt.

```
import { verifyCredentialJwt } from "@cef-ebsi/verifiable-credential";

const vcJwt = "eyJraWQiOiJkaWQ6ZWJzaTp6Z1Bz...j9Pv1HSIR9aPXIVRMGYfjhmQH8oSM03g";

const options = {
  // EBSI URI Authority ([userinfo "@"] host [":" port])
  ebsiAuthority: "api-test.ebsi.eu",
};

const verifiedVc = await verifyCredentialJwt(vcJwt, options);

console.log(verifiedVc);

/*
{
  "@context": ["https://www.w3.org/2018/credentials/v1"],
  id: "urn:did:123456",
  type: ["VerifiableCredential", "VerifiableAttestation", "VerifiableId"],
  issuer: "did:ebsi:zgPs5MVWHwJJb4g9kZvYf3e",
  issuanceDate: "2021-11-01T00:00:00Z",
  validFrom: "2021-11-01T00:00:00Z",
  credentialSubject: {
    id: "did:ebsi:zYud7H5Wvf9ksRUrmTrFo9D",
    personalIdentifier: "IT/DE/1234",
    familyName: "Castafiori",
    firstName: "Bianca",
    dateOfBirth: "1930-10-01",
  },
  credentialSchema: {
    id: "https://api-test.ebsi.eu/trusted-schemas-
registry/v2/schemas/0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49",
    type: "FullJsonSchemaValidator2021",
  },
  expirationDate: "2031-11-30T00:00:00Z",
  issued: "2021-10-30T00:00:00Z",
}
*/
```

ΠΑΡΑΡΤΗΜΑ ΕΠΕΞΗΓΗΣΗ ΟΡΩΝ

Αποκεντρωμένο αναγνωριστικό (DID):Ένα φορητό αναγνωριστικό που βασίζεται σε URL, γνωστό και ως DID, που σχετίζεται με μια οντότητα. Αυτά τα αναγνωριστικά χρησιμοποιούνται συχνότερα σε επαληθεύσιμα διαπιστευτήρια και σχετίζονται με θέματα έτσι ώστε ένα επαληθεύσιμο διαπιστευτήριο μπορεί να μεταφερθεί εύκολα από το ένα αποθετήριο σε ένα άλλο χωρίς να απαιτείται επανέκδοση του διαπιστευτηρίου.

Αποκεντρωμένο έγγραφο αναγνώρισης (έγγραφο DID):Αναφέρεται επίσης ως έγγραφο DID, αυτό είναι ένα έγγραφο που περιέχει πληροφορίες που σχετίζονται με ένα συγκεκριμένο αποκεντρωμένο αναγνωριστικό, όπως το σχετικό αποθετήριο και πληροφορίες δημόσιου κλειδιού.

Εκδότης: Ένας ρόλος που μπορεί να εκτελέσει μια οντότητα προβάλλοντας αξιώσεις για ένα ή περισσότερα θέματα, δημιουργώντας ένα επαληθεύσιμο διαπιστευτήριο από αυτές τις αξιώσεις και μεταδίδοντας το επαληθεύσιμο διαπιστευτήριο σε έναν κάτοχο.

Επαληθεύσιμο διαπιστευτήριο (VC): Ένα σύνολο από μία ή περισσότερες αξιώσεις που υποβάλλονται από έναν εκδότη. Ένα επαληθεύσιμο διαπιστευτήριο είναι ένα διαπιστευτήριο με προφανή παραποίηση που έχει συγγραφικό στοιχείο που μπορεί να επαληθευτεί κρυπτογραφικά. Τα επαληθεύσιμα διαπιστευτήρια μπορούν να χρησιμοποιηθούν για τη δημιουργία επαληθεύσιμων παρουσιάσεων, οι οποίες μπορούν επίσης να επαληθευτούν κρυπτογραφικά.

Επαληθεύσιμη παρουσίαση (VP): Δεδομένα που προέρχονται από ένα ή περισσότερα επαληθεύσιμα διαπιστευτήρια, που εκδίδονται από έναν ή περισσότερους εκδότες, τα οποία κοινοποιούνται σε έναν συγκεκριμένο επαληθευτή. Μια επαληθεύσιμη παρουσίαση είναι μια παρουσίαση με προφανή παραβίαση κωδικοποιημένη με τέτοιο τρόπο ώστε να είναι αξιόπιστη η συγγραφή των δεδομένων μετά από μια διαδικασία κρυπτογραφικής επαλήθευσης.

Μητρώο επαληθεύσιμων δεδομένων: Ένας ρόλος που μπορεί να διαδραματίσει ένα σύστημα διαμεσολαβώντας τη δημιουργία και την επαλήθευση αναγνωριστικών, κλειδιών και άλλων σχετικών δεδομένων, όπως επαληθεύσιμα σχήματα διαπιστευτηρίων, μητρώα ανάκλησης, δημόσια κλειδιά εκδότη κ.λπ., τα οποία μπορεί να απαιτούνται για τη χρήση επαληθεύσιμων διαπιστευτηρίων.

Επιβεβαιωτής: Ένας ρόλος που εκτελεί μια οντότητα λαμβάνοντας ένα ή περισσότερα επαληθεύσιμα διαπιστευτήρια, προαιρετικά μέσα σε μια επαληθεύσιμη παρουσίαση για επεξεργασία. Άλλες προδιαγραφές μπορεί να αναφέρονται σε αυτήν την έννοια ως στηριζόμενο μέρος.

Μητρώο αξιόπιστων εκδοτών (TIR): Μητρώο εκδοτών για την εγγραφή των διαπιστεύσεών τους

ΒΙΒΛΙΟΓΡΑΦΊΑ

[1] *Torres Moreno R, Bernal Bernabe J, García Rodríguez J, Kasper Frederiksen T, Stausholm M, Martínez N, Sakkopoulos E, Ponte N, Skarmeta A. The OLYMPUS Architecture—Oblivious Identity Management for Private User-Friendly Services.* Sensors*. 2020; 20(3):945. https://doi.org/10.3390/s20030945*

[2] Piotopoulos, S., & Sakkopoulos, E. (2022, July). On-line enrollment systems for migrants: A case study on the new Greek Certificate of Knowledge Competency for Naturalization. In 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) (pp. 1-4). IEEE.

[3] S. Piotopoulos and E. Sakkopoulos, "Smart eGov Services for Citizenship: Improving Personalized Services," 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA*, 2020, pp. 1-8, doi: 10.1109/IISA50023.2020.9284376*

[4] E. Viennas, Z. -M. Ioannou, G. Pavlidis, G. Tzimas and E. Sakkopoulos, "HappyCruise: An architecture for Personalized Secure Boarding on Cruises," 2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA*, 2020, pp. 1-8, doi: 10.1109/IISA50023.2020.9284375*

[5] Jingxuan Li, Yue Jing, "Establishing an International Engagement Model of Digital Identity Based on Blockchain", Mobile Information Systems, vol. 2022, Article ID 6988211,7 pages,2022. https://doi.org/10.1155/2022/6988211

[6] *EBSI Verifiable Credentials Explained - EBSI Specifications -. (n.d.). https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained*

[7*] Sharif Jacobino, Johan Pouwelse: TrustVault: A privacy-first data wallet for the European Blockchain Services Infrastructure. CoRR abs/2210.02987 (2022)*

[8] GDPR: EUR-Lex - 32016R0679 - EN - EUR-Lex. (n.d.-b). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[9] eIDAS. (n.d.). The Ecosystem. https://www.eid.as/

[10] RFC 7517 - JSON Web Key (JWK). (n.d.). https://datatracker.ietf.org/doc/html/rfc7517

ΑΝΑΦΟΡΈΣ ΕΙΚΟΝΩΝ

Εικόνα 1 Chapter 2, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 2 Chapter 2, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 3 Chapter 2, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 4 Chapter 3, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 5 Chapter 3, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 6 Chapter 3, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 8 Chapter 4, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 9 Chapter 4, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].
Εικόνα 10 Chapter 4, European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/EBSI+Verifiable+Credentials+Explained [Accessed 26 November 2022].

ΑΝΑΦΟΡΕΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

Διάγραμμα 1 European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model++Accreditation+of+Issuers#IssuerstrustmodelAccreditationofIssuers-Issuerstrustmodel-onboardingandaccreditations [Accessed 26 November 2022].
Διάγραμμα 2 European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model++Accreditation+of+Issuers#IssuerstrustmodelAccreditationofIssuers-Issuerstrustmodel-onboardingandaccreditations [Accessed 26 November 2022]
Διάγραμμα 3 European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model++Accreditation+of+Issuers#IssuerstrustmodelAccreditationofIssuers-Issuerstrustmodel-onboardingandaccreditations [Accessed 26 November 2022]
Διάγραμμα 4 European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model++Accreditation+of+Issuers#IssuerstrustmodelAccreditationofIssuers-Issuerstrustmodel-onboardingandaccreditations [Accessed 26 November 2022]
Διάγραμμα 5 European Commission,2022 [Online] Available from: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Issuers+trust+model++Accreditation+of+Issuers#IssuerstrustmodelAccreditationofIssuers-Issuerstrustmodel-onboardingandaccreditations [Accessed 26 November 2022]