Τίτλος έργου: **Διασυνδεδεμένες Έξυπνες Πόλεις για την Ελλάδα 2.0**

Κωδικός: **TAEDR-0536642**

MIS (ΟΠΣ): **5149305**

Παραδοτέο: **Π1.2**

Τίτλος: **Αρχιτεκτονική συστήματος και κυβερνοασφάλεια**

Συμμετέχοντες

Φορέας
Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ)
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ)
Εθνικό Μετσόβιο Πολυτεχνείο (ΕΜΠ)
Πανεπιστήμιο Θεσσαλίας (ΠΘ)
Πανεπιστήμιο Δυτικής Μακεδονίας (ΠΔΜ)
Πανεπιστήμιο Πατρών (ΠΠ)

Περιεχόμενα

Λίστα Εικόνων

Λίστα Πινάκων

Κατάλογος Συντομεύσεων

API	Application Programming Interface
BAE	Business API Ecosystem
BDVA	Big Data Value Association
CEF	Connecting Europe Facility
COSE	CBOR Object Signing and Encryption
CWT	CBOR Web Token
DCAT	Data Catalog Vocabulary
DID	Distributed Identity
DSBA	Data Spaces Business Alliance
DSSC	Data Space Support Center
DSI	Digital Service Infrastructure
EU	European Union
EUDI	European Digital Identity
H2M	Human-to-Machine
IDS	International Data Spaces
IDSA	International Data Spaces Association
IIRA	Industrial Internet Reference Architecture
IoT	Internet of Things
JOSE	JSON Object Signing and Encryption
JWT	JSON Web Token
KWA	Key Wrap Algorithm
M2M	Machine-to-Machine
ML	Machine Learning
MVF	Minimum Viable Framework
OIDC	OpenID Connect
OIDC4VCI	OpenIDConnect for Verifiable Credentials Issuance
OIDC4VP	OpenID Connect for Verifiable Presentations
PDP	Policy Decision Point
PKI	Public Key Infrastructure
RAMI	Reference Architectural Model Industrie
SCRA	Smart City Reference Architecture
VC	Verifiable Credential
VP	Verifiable Presentation
W3C	World Wide Web Consortium
XACML	eXtensible Access Control Markup Language
ΔτΠ	Διαδίκτυο των Πραγμάτων
ΧΔ	Χώρος Δεδομένων

1. Εισαγωγή

1.1 Επισκόπηση του έργου «Διασυνδεδεμένες Έξυπνες Πόλεις για την Ελλάδα 2.0»

Ο βασικός στόχος του έργου είναι η ανάπτυξη μίας καθολικής πλατφόρμας για τη διαχείριση Έξυπνων Πόλεων και η δημιουργία ενός κεντρικού σημείου αναφοράς οικοσυστημάτων του Διαδικτύου των Πραγμάτων (ΔτΠ).

Συγκεκριμένα, από τεχνικής σκοπιάς έχει προχωρήσει η ανάπτυξη μιας πλατφόρμας διαλειτουργικότητας, υλοποιημένη και κατανεμημένη σε πολλαπλά επίπεδα, η οποία εν τέλει θα συγκεντρώσει τεχνολογίες και υπηρεσίες που προέρχονται από το σύνολο των υπαρχόντων κάθετων υλοποιήσεων που βρίσκονται ήδη εν λειτουργία στις μεγαλύτερες πόλεις της Ελλάδας που είχαν ήδη εκδηλώσει το ενδιαφέρον είτε κατά την περίοδο συγγραφής της πρότασης (Τρίκαλα, Πάτρα, Ηράκλειο, Θεσσαλονίκη), ή το έκαναν κατά τη διάρκεια εκτέλεσης του έργου (Αθήνα, Λάρισα, Κοζάνη).

Η πλατφόρμα, μέσω του πλήθους των παρεχόμενων ενοποιημένων υπηρεσιών που θα επιτρέπουν την απευθείας άντληση δεδομένων ετερογενών συστημάτων, αλλά και την οπτικοποίηση του συνόλου της πληροφορίας, θα καθιστά πλέον εφικτή την ανάπτυξη νέων καινοτόμων υπηρεσιών και προϊόντων προστιθέμενης αξίας στο πλαίσιο του προγράμματος Ελλάδα 2.0 και συγκεκριμένα στον τομέα των Έξυπνων Πόλεων.

Με αυτόν τον τρόπο θα τοποθετηθεί ένας ακρογωνιαίος λίθος για την ουσιαστική δικτύωση και ταχύτερη αξιοποίηση των υφιστάμενων υποδομών, για τη δημιουργία σύνθετων προϊόντων και υπηρεσιών με στόχους:

- τη μεταφορά και αξιοποίηση υφιστάμενης τεχνογνωσίας
- τη δημιουργία καινοτόμων εφαρμογών και υπηρεσιών.
- την ενδυνάμωση της επιχειρηματικότητας και ανταγωνιστικότητας.
- την προώθηση της συμμετοχικότητας στη λειτουργία της τοπικής αυτοδιοίκησης
- την προώθηση της σύμπραξης ακαδημαϊκών και ερευνητικών φορέων με τη βιομηχανία.

1.2 Σκοπός και πεδίο εφαρμογής του παραδοτέου

Στο παρόν παραδοτέο θα περιγραφεί αναλυτικά η αρχιτεκτονική του συστήματος της μετα-πλατφόρμας, εστιάζοντας στον τρόπο επικοινωνίας και αλληλεπίδρασης των επιμέρους υποσυστημάτων τόσο σε λογικό όσο και σε φυσικό επίπεδο. Θα αποτυπωθούν οι βασικές δομικές συνιστώσες της πλατφόρμας, οι τεχνολογίες που αξιοποιούνται για τη διασύνδεση και

διαλειτουργικότητα των συστημάτων, καθώς και οι αρχές σχεδιασμού που εξασφαλίζουν την αποδοτικότητα και την επεκτασιμότητα της λύσης.

Επιπλέον, θα εξεταστούν διεξοδικά οι μηχανισμοί ασφαλείας που εφαρμόζονται για τη θωράκιση της πλατφόρμας, εστιάζοντας σε θέματα ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των δεδομένων. Θα παρουσιαστούν οι στρατηγικές προστασίας έναντι κυβερνοαπειλών, οι διαδικασίες διαχείρισης ταυτοτήτων και ελέγχου πρόσβασης, καθώς και τα πρωτόκολλα ασφαλούς επικοινωνίας μεταξύ των υποσυστημάτων.

Παράλληλα, θα αναλυθούν οι πολιτικές ασφάλειας που υιοθετούνται τόσο σε συνολικό επίπεδο όσο και σε επίπεδο επιμέρους δομών, διασφαλίζοντας την αξιόπιστη λειτουργία της πλατφόρμας και την προστασία των χρηστών της. Τέλος, θα παρουσιαστούν βέλτιστες πρακτικές και προτεινόμενες βελτιώσεις για την περαιτέρω ενίσχυση της ασφάλειας και της λειτουργικότητας του συστήματος, λαμβάνοντας υπόψη σύγχρονες τάσεις και τεχνολογικές εξελίξεις στον τομέα των έξυπνων πόλεων και της κυβερνοασφάλειας.

1.3 Δομή του παραδοτέου

Το έγγραφο αποτελεί μια λεπτομερή ανάλυση του σχεδιασμού της αρχιτεκτονικής μιας μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων. Ξεκινά με την εισαγωγή, όπου περιγράφεται ο σκοπός, το πεδίο εφαρμογής και η δομή του παραδοτέου. Στη συνέχεια, αναλύεται η μεθοδολογία σχεδιασμού της αρχιτεκτονικής, περιλαμβάνοντας τη διαδικασία εξαγωγής αρχιτεκτονικής και τη χρήση χώρων δεδομένων, ενώ εξετάζονται συναφείς αρχιτεκτονικές, όπως FIWARE, OpenDEI, GAIA-X και άλλες πρωτοβουλίες δεδομένων. Το τρίτο μέρος εστιάζει στην αρχιτεκτονική της μετα-πλατφόρμας, περιγράφοντας βασικά δομικά στοιχεία, όπως οι υπηρεσίες διακυβέρνησης και αξίας δεδομένων, καθώς και το υποσύστημα διασύνδεσης (connectors). Στη συνέχεια, το τέταρτο μέρος πραγματεύεται ζητήματα κυβερνοασφάλειας, εστιάζοντας στη διαχείριση ταυτοτήτων, την αυθεντικοποίηση και την εξουσιοδότηση. Τέλος, συνοψίζει τα κύρια σημεία και τα συμπεράσματα του εγγράφου.

2. Μεθοδολογία Σχεδιασμού της Αρχιτεκτονικής της Μετά-Πλατφόρμας

Στην ενότητα αυτή εισάγουμε σύντομα τη μεθοδολογία που ακολουθούμε για το σχεδιασμό της αρχιτεκτονικής της μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων.

2.1 Διαδικασία εξαγωγής αρχιτεκτονικής

Η αρχική έκδοση της αρχιτεκτονικής αναπτύχθηκε έχοντας ως οδηγό τις βασικές απαιτήσεις της μετα-πλατφόρμας, όπως αυτές ενσωματώθηκαν στην πρόταση του έργου. Στη συνέχεια, και ύστερα από την εξαγωγή των τελικών απαιτήσεων συστήματος (Παραδοτέο Π1.1), ο αρχικός σχεδιασμός τροποποιήθηκε μέσω αρκετών επαναλήψεων, έτσι ώστε να καταλήξουμε στην τρέχουσα εκδοχή της αρχιτεκτονικής. Η αρχιτεκτονική που αναπτύχθηκε βασίστηκε στην προσέγγιση των *Χώρων Δεδομένων (Data Spaces),* οι οποίοι αποτελούν αποκεντρωμένα δια-λειτουργικά οικοσυστήματα διαμοιρασμού και ανταλλαγής δεδομένων, μέσω ενός πλαισίου εμπιστοσύνης και διαφύλαξης της κυριαρχίας επί των δεδομένων [1].

Διερευνήσαμε διάφορα αρχιτεκτονικά μοντέλα που σχετίζονται με τον σχεδιασμό τόσο πλατφορμών δεδομένων έξυπνων πόλεων όσο και χώρων δεδομένων, όπως επίσης, και με την προσαρμογή υπαρχουσών πλατφορμών έξυπνων πόλεων και την ένταξή τους σε έναν χώρο δεδομένων έξυπνων πόλεων. Το τελευταίο σενάριο θεωρούμε ότι είναι ιδιαίτερα ευθυγραμμισμένο με τους στόχους της μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων του παρόντος έργου, αφού το έργο επιδιώκει τη διαλειτουργικότητα μεταξύ υπαρχουσών καθετοποιημένων υλοποιήσεων έξυπνων πόλεων σε επίπεδο δεδομένων και υπηρεσιών. Ιδιαίτερη έμφαση δόθηκε στο Αρχιτεκτονικό Μοντέλο Αναφοράς (Reference Architecture Model) του International Data Space Association (IDS-RAM)[1] που έχει εισάγει τις θεμελιώδεις έννοιες και τα στοιχεία ενός χώρου δεδομένων, πάνω στα οποία στηρίχθηκαν αρκετά νεότερα αρχιτεκτονικά μοντέλα αλλά και υλοποιήσεις. Το IDS-RAM έχει βασιστεί σε προϋπάρχοντα αρχιτεκτονικά μοντέλα, όπως το Industrial Internet Reference Architecture (IIRA) [2] και το Reference Architectural Model Industrie 4.0 (RAMI 4.0) [3].

2.2 Χώροι Δεδομένων

Ο όρος Χώρος Δεδομένων (ΧΔ) μπορεί να θεωρηθεί ως ένας γενικός όρος που ενσωματώνει πολλές στενά συνδεδεμένες έννοιες που σχετίζονται με την κοινή χρήση δεδομένων σε συνεργατικά περιβάλλοντα. Εμφανίστηκε αρχικά εντός της κοινότητας διαχείρισης δεδομένων και ορίστηκε, στην πιο απλή του μορφή, ως ένα σύνολο συμμετεχόντων που προσφέρουν αποθετήρια δεδομένων σε συνδυασμό με τις σχέσεις μεταξύ τους [4]. Πρόσφατα, οι ΧΔ έχουν κινήσει ιδιαίτερα το ενδιαφέρον

[1] https://docs.internationaldataspaces.org/knowledge-base/ids-ram-4.0

της κοινότητας, με ένα συνεχώς αυξανόμενο αριθμό ευρωπαϊκών πρωτοβουλιών που διερευνούν τη χρησιμότητα και την εφαρμογή του σε διαφορετικούς τομείς και οικοσυστήματα δεδομένων (π.χ. κινητικότητα, έξυπνες πόλεις, εφοδιαστική αλυσίδα, έξυπνα λιμάνια κ.ά.). Η Ευρωπαϊκή Στρατηγική Δεδομένων (European Data Strategy) λειτούργησε ως καταλύτης προς αυτή την κατεύθυνση, αναγνωρίζοντας τη σημασία της προστασίας δεδομένων και της αξιόπιστης κοινής χρήσης. Έτσι, ενθαρρύνεται η δημιουργία μιας ενιαίας αγοράς δεδομένων της ΕΕ που υπόκειται στις ευρωπαϊκές νομικές κατευθυντήριες γραμμές και εγγυάται την κυριαρχία των δεδομένων για τους παραγωγούς και τους καταναλωτές δεδομένων.

Στο πλαίσιο των έξυπνων πόλεων, η λύση των ΧΔ προσφέρει τα εξής πλεονεκτήματα:

- **Διαλειτουργικότητα:** Οι ΧΔ διευκολύνουν την απρόσκοπτη διαλειτουργικότητα μεταξύ διαφορετικών πηγών δεδομένων και συστημάτων σε μια έξυπνη πόλη. Χρησιμοποιώντας τυποποιημένες μορφές δεδομένων και πρωτόκολλα επικοινωνίας, διασφαλίζουν ότι διαφορετικά συστήματα μπορούν να ανταλλάσσουν και να χρησιμοποιούν αποτελεσματικά δεδομένα και υπηρεσίες. Αυτή η διαλειτουργικότητα είναι ζωτικής σημασίας για τη δημιουργία ενός συνεκτικού οικοσυστήματος όπου τα δεδομένα από διάφορους τομείς μπορούν να ενσωματωθούν για να παρέχουν ολοκληρωμένες υπηρεσίες και εφαρμογές προστιθέμενης αξίας.
- **Ενισχυμένη ασφάλεια, ιδιωτικότητα και εμπιστοσύνη:** Η ασφάλεια και ιδιωτικότητα των δεδομένων είναι πρωταρχικής σημασίας στις εφαρμογές της έξυπνης πόλης. Οι ΧΔ ενσωματώνουν ισχυρές μεθόδους ασφάλειας και ιδιωτικότητας, όπως κρυπτογράφηση, έλεγχοι πρόσβασης και χρήσης δεδομένων, τεχνικές ανωνυμοποίησης κ.ά.. Κατά συνέπεια, οι ΧΔ προσφέρουν ένα ασφαλές περιβάλλον για την έμπιστη ανταλλαγή δεδομένων μεταξύ των συμμετεχόντων μερών, διασφαλίζοντας την κυριαρχία στα δεδομένα (data sovereignty).
- **Κλιμακωσιμότητα και ευελιξία:** Η αρχιτεκτονική των ΧΔ είναι εγγενώς επεκτάσιμη και κλιμακώσιμη, επιτρέποντας την απρόσκοπτη προσθήκη νέων πηγών δεδομένων και χρηστών. Αυτή η κλιμακωσιμότητα είναι απαραίτητη για τις έξυπνες πόλεις, οι οποίες είναι δυναμικά περιβάλλοντα με συνεχώς εξελισσόμενες ανάγκες δεδομένων. Οι χώροι δεδομένων μπορούν να προσαρμοστούν στον αυξανόμενο όγκο δεδομένων που προέρχονται από υποδομές Διαδικτύου των Πραγμάτων (IoT), διασφαλίζοντας την αποδοτικότητα και συνάφεια (relevance).
- **Διευκόλυνση καινοτομίας**: Παρέχοντας ένα πλαίσιο ενορχήστρωσης της ανταλλαγής δεδομένων, οι ΧΔ ενισχύουν την καινοτομία και τη συνεργασία μεταξύ διαφόρων ενδιαφερομένων, π.χ. παρόχων υποδομών έξυπνων πόλεων, επιχειρήσεων, ερευνητικών φορέων κ.ά. Το συνεργατικό αυτό οικοσύστημα προωθεί την προώθηση λύσεων έξυπνων πόλεων και περιπτώσεων χρήσης (use cases) καθοδηγούμενων από δεδομένα (data-driven) και βασίζονται σε στοιχεία (evidence-based).

- **Αποτελεσματικότερη λήψη αποφάσεων:** Η πρόσβαση σε ολοκληρωμένα και σε πραγματικού χρόνου δεδομένα μέσω ΧΔ δίνει τη δυνατότητα λήψης τεκμηριωμένων αποφάσεων. Η ενοποίηση δεδομένων από πολλαπλές πηγές παρέχει μια ολιστική άποψη της δυναμικής των αστικών περιβαλλόντων, επιτρέποντας προγνωστικές αναλύσεις και προληπτικές παρεμβάσεις, με χρήση προχωρημένων τεχνικών ανάλυσης δεδομένων και μηχανικής μάθησης. Έτσι, είναι δυνατή η βελτίωση της συνολικής διαχείρισης της πόλης και η ικανοποίηση των πολιτών.

Στον Πίνακα 1 συνοψίζουμε το σκεπτικό ικανοποίησης των βασικών απαιτήσεων της μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων διαμέσου της αρχιτεκτονικής ΧΔ.

Πίνακας 1: Ικανοποίηση βασικών απαιτήσεων μετα-πλατφόρμας μέσω αρχιτεκτονικής Χώρου Δεδομένων.

Βασική απαίτηση	Λύση Χώρου Δεδομένων
Σημασιολογική διαλειτουργικότητα δεδομένων και υπηρεσιών	Η διαλειτουργικότητα είναι στον πυρήνα μιας αρχιτεκτονικής ΧΔ. Ένας ΧΔ πρέπει να προσφέρει ένα συμπαγές πλαίσιο για την αποδοτική ανταλλαγή δεδομένων μεταξύ των συμμετεχόντων, υποστηρίζοντας την αποσύνδεση μεταξύ παραγωγών και καταναλωτών δεδομένων και υπηρεσιών. Η σημασιολογική διαλειτουργικότητα μεταξύ κοινών μοντέλων δεδομένων είναι απαραίτητη, έτσι ώστε όλοι οι συμμετέχοντες να επικοινωνούν με μία κοινή γλώσσα.
Ενοποιημένες Προγραμματιστικές Διεπαφές Εφαρμογών (Application Programming Interaces - APIs) ανταλλαγής και ανάκτησης δεδομένων	Εκτός των κοινών μοντέλων δεδομένων, η διαλειτουργικότητα σε ένα ΧΔ απαιτεί την υιοθέτηση κοινών APIs για την αξιόπιστη ανταλλαγή/διαμοιρασμό δεδομένων.
Πλαίσιο για ασφαλή και έμπιστο διαμοιρασμό δεδομένων	Οι ΧΔ παρέχουν τα τεχνικά μέσα που εγγυώνται ότι οι συμμετέχοντες ενός ΧΔ μπορούν αν εμπιστευτούν ο ένας τον άλλο και να ασκήσουν κυριαρχία στα δεδομένα που μοιράζονται. Συνεπώς, προσφέρουν ένα πλαίσιο εμπιστοσύνης που καλύπτει τις απαιτήσεις για διαχείριση ταυτότητας, πρόσβασης και χρήσης δεδομένων, παρέχοντας μία κλιμακώσιμη και αυτοκυρίαρχη (self-sovereign) λύση, με προσεγγίσεις όπως οι Αποκεντρωμένες Ταυτότητες (Decentralized Identities-DIDs) και τα Επαληθεύσιμα Διαπιστευτήρια (Verifiable Credentials - VCs).

Αποκεντρωμένη αποθήκευση δεδομένων	Ένας ΧΔ υιοθετεί μία προσέγγιση ομοσπονδίας δεδομένων (federated data approach), αποφεύγοντας ένα δεδομενοκεντρικό μοντέλο. Γενικά, τα δεδομένα μένουν αποθηκευμένα στις εγκαταστάσεις/υποδομές των συμμετεχόντων (όχι σε μία κεντρικοποιημένη υποδομή) και ανακτώνται ή/και υφίστανται επεξεργασία (π.χ. ανωνυμοποιούνται, συγκεράζονται κ.ά.) σύμφωνα με τις πολιτικές χρήσης που ορίζει ο παραγωγός των δεδομένων.
Εφαρμογές και υπηρεσίες δεδομένων προστιθέμενης αξίας	Αυτό είναι σύμφωνο με ένα από τα τεχνικά δομικά στοιχεία των ΧΔ, όπως ορίζονται από το έργο OpenDEI[2]. Οι ΧΔ παρέχουν υποστήριξη για τη δημιουργία πολυμερών αγορών, όπου οι συμμετέχοντες μπορούν να δημιουργήσουν αξία από την κοινή χρήση δεδομένων (δηλαδή, τη δημιουργία αλυσίδων αξίας δεδομένων). Για παράδειγμα, εφαρμογές μεγάλων δεδομένων και υπηρεσίες ML μπορούν να προσφερθούν αξιοποιώντας τα δεδομένα που ανταλλάσσονται.
Επαναχρησιμοποίηση καθιερωμένων και τυποποιημένων τεχνολογικών λύσεων	Τα αρχιτεκτονικά μοντέλα ΧΔ δεν προσπαθούν να επανεφεύρουν τον τροχό, αλλά ενθαρρύνουν εγγενώς την υιοθέτηση καθιερωμένων υποκείμενων τεχνολογικών λύσεων, σε όλα τα τεχνικά δομικά στοιχεία (διαλειτουργικότητα δεδομένων, εμπιστοσύνη και κυριαρχία δεδομένων, δημιουργία αξίας δεδομένων).
Οπτικοποίηση ετερογενών δεδομένων προερχόμενων από διαφορετικές πηγές δεδομένων	Αυτό μπορεί να θεωρηθεί ως ειδική περίπτωση υπηρεσίας αξίας δεδομένων. Οι πλούσιες και κατανοητές οπτικοποιήσεις δεδομένων διαδραματίζουν κρίσιμο ρόλο στην προσθήκη αξίας στα δεδομένα που ανταλλάσσονται, βελτιώνοντας την κατανόηση, διευκολύνοντας την ανακάλυψη πληροφοριών, ενισχύοντας την επικοινωνία, υποστηρίζοντας τη λήψη αποφάσεων και επιτρέποντας την δεδομενοκεντρική εξερεύνηση και περιγραφή.

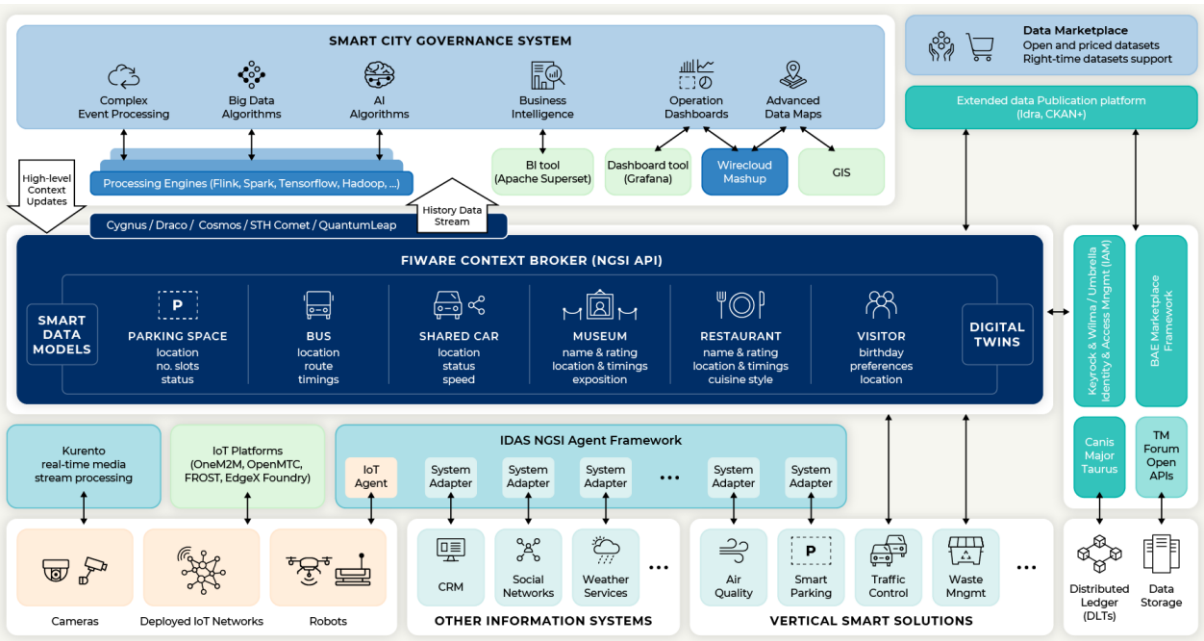
2.3 Σχετικές αρχιτεκτονικές

Στην παρούσα υποενότητα παρουσιάζουμε αρχιτεκτονικές προερχόμενες από ποικίλα έργα/πρωτοβουλίες, οι οποίες είτε αποτελούν καθιερωμένες αρχιτεκτονικές λύσεις έξυπνων πόλεων, είτε είναι περισσότερο προσαρμοσμένες στη φιλοσοφία των Χώρων Δεδομένων.

[2] https://www.opendei.eu/

2.2.1 FIWARE Αρχιτεκτονική Αναφοράς Έξυπνης Πόλης

Η FIWARE Αρχιτεκτονική Αναφοράς Έξυπνης Πόλης (FIWARE Smart City Reference Architecture - FIWARE-SCRA)[3] (Εικόνα 1) παρέχει ένα ολοκληρωμένο πλαίσιο για το σχεδιασμό και την ανάπτυξη λύσεων έξυπνων πόλεων. Αυτή η αρχιτεκτονική αξιοποιεί ανοιχτά πρότυπα και διαλειτουργικά στοιχεία για τη δημιουργία ενός οικοσυστήματος ποικίλων αστικών εφαρμογών. Στον πυρήνα της, όπως συμβαίνει με όλα τα συστήματα που υιοθετούν την αρχιτεκτονική FIWARE, χρησιμοποιεί τον *Context Broker*, ένα δομικό στοιχείο που διαχειρίζεται και διανέμει την πληροφορία πλαισίου (context information) που διακινείται στο σύστημα. Επίσης, επιτρέπει τη διαλειτουργική ανταλλαγή δεδομένων χρησιμοποιώντας διαλειτουργικά μοντέλα δεδομένων (με χρήση των *Smart Data Models*)[4], υποστηρίζει αρραγή διασύνδεση με συσκευές IoT διαμέσου σχετικών προσαρμογέων, γνωστών ως IoT Agents, ενσωματώνει την έννοια του ψηφιακού διδύμου (digital twin) μέσω της ικανότητας διασύνδεσης έξυπνων πλατφορμών που σχηματίζουν ένα σύστημα συστημάτων (system-of-systems) και υποστηρίζει την ενσωμάτωση αγοράς δεδομένων (data marketplace), χρησιμοποιώντας το πλαίσιο *BAE marketplace*[5]. Η αρχιτεκτονική είναι σχεδιασμένη με αρθρωτό τρόπο, επιτρέποντας τη διασύνδεση διαφορετικών και ετερογενών πηγών δεδομένων και υποστηρίζεται από ένα σύνολο στοιχείων, γνωστών ως *Generic Enablers (GEs)*, που προσφέρουν κατά το δοκούν διάφορες λειτουργικότητες, όπως διαχείριση ασφάλειας, αποθήκευση δεδομένων, ανάλυση δεδομένων και οπτικοποίηση δεδομένων.

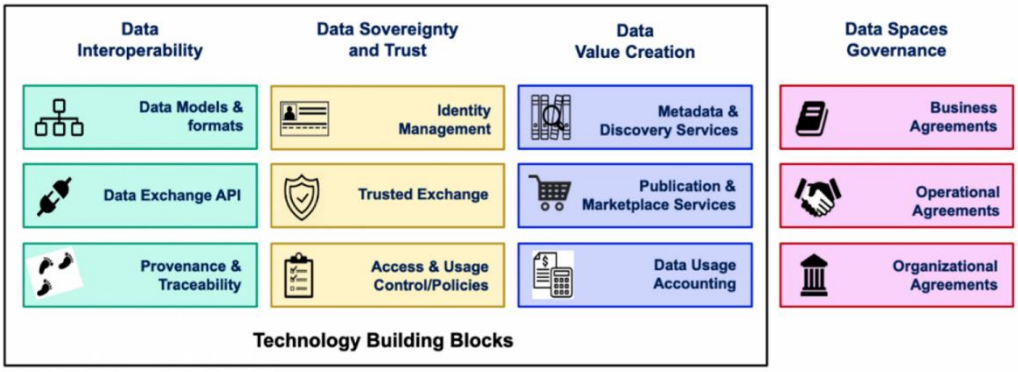


Εικόνα 1: FIWARE Αρχιτεκτονική Αναφοράς Έξυπνης Πόλης

[3] https://www.fiware.org/wp-content/directories/marketing-toolbox/material/FIWAREBrochure_SmartCities.pdf
[4] https://www.fiware.org/smart-data-models/
[5] https://github.com/FIWARE-TMForum/Business-API-Ecosystem

2.3.2 OpenDEI

Το έργο *OpenDEI ("OPEN DEI – Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitizing European Industry")*[6] ανέπτυξε τις βασικές αρχές που απαιτούνται για το σχεδιασμό ενός Χώρου Δεδομένων ανεξάρτητου τομέα (domain-independent). Όπως φαίνεται στην Εικόνα 1, πρότεινε ένα σύνολο από δομικά στοιχεία (building blocks), τα οποία διατρέχουν δύο κατηγορίες, δηλ. (α) οργανωτικά δομικά στοιχεία και (β) τεχνολογικά δομικά στοιχεία. Οι σχεδιαστικές αρχές περιλαμβάνουν την κυριαρχία επί των δεδομένων (data sovereignty), ισότιμους όρους ανταγωνισμού για κοινή χρήση και ανταλλαγή δεδομένων, αποκεντρωμένη ήπια υποδομή (soft infrastructure) και δημόσια-ιδιωτική διακυβέρνηση. Από τεχνικής σκοπιάς, ένα ΧΔ μπορεί να γίνει κατανοητός ως μία συλλογή από τεχνικά στοιχεία που διευκολύνουν τη δυναμική, ασφαλή και αδιάλειπτη ροή δεδομένων μεταξύ μερών. Έτσι τα τεχνολογικά δομικά στοιχεία ανήκουν σε τρεις κατηγορίες: (α) δια-λειτουργικότητα δεδομένων, (β) κυριαρχία και εμπιστοσύνη δεδομένων, και (γ) δημιουργία αξίας δεδομένων. Τα δομικά στοιχεία του OpenDEI παρέχουν ένα αξιόλογο κοινό έδαφος για το σχεδιασμό ΧΔ συγκεκριμένου τομέα και γι' αυτό έχουν υιοθετηθεί από διάφορες άλλες πρωτοβουλίες που ακολούθησαν.



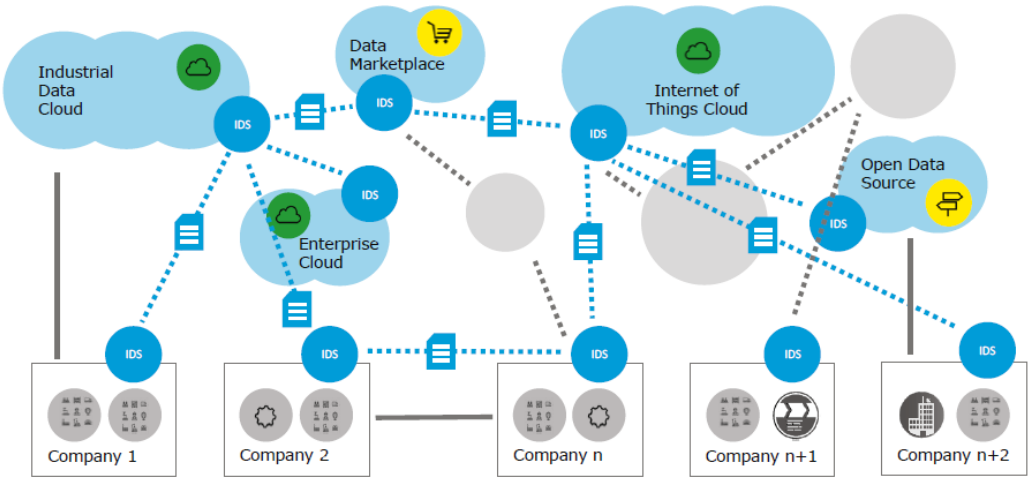
Εικόνα 2: Δομικά στοιχεία χώρου δεδομένων κατά OpenDEI

2.3.3 International Data Spaces

Η πρωτοβουλία *International Data Spaces (IDS)* ενσωματώνει ένα εύρος από υπάρχουσες τεχνολογίες και πρότυπα που έχουν ως στόχο τη δημιουργία ΧΔ σε διάφορα πεδία εφαρμογών. Αυτοί οι ΧΔ διευκολύνουν την τυποποιημένη ανταλλαγή και σύνδεση δεδομένων εντός ενός ασφαλούς και έμπιστου περιβάλλοντος, όπως φαίνεται στην Εικόνα 2. Ο *International Data Spaces Association (IDSA)* είναι ένας μη κερδοσκοπικός οργανισμός που αποσκοπεί στην εγκαθίδρυση της αρχιτεκτονικής του IDS ως καθολικό πρότυπο σε ποικίλους τομείς όπως κινητικότητα, ιατρική φροντίδα κ.ά. Κάποιοι από αυτούς τους τομείς έχουν σχηματίσει συγκεκριμένες κοινότητες, π.χ. IDS-Industrial, με σκοπό την ανάπτυξη

[6] https://www.opendei.eu/

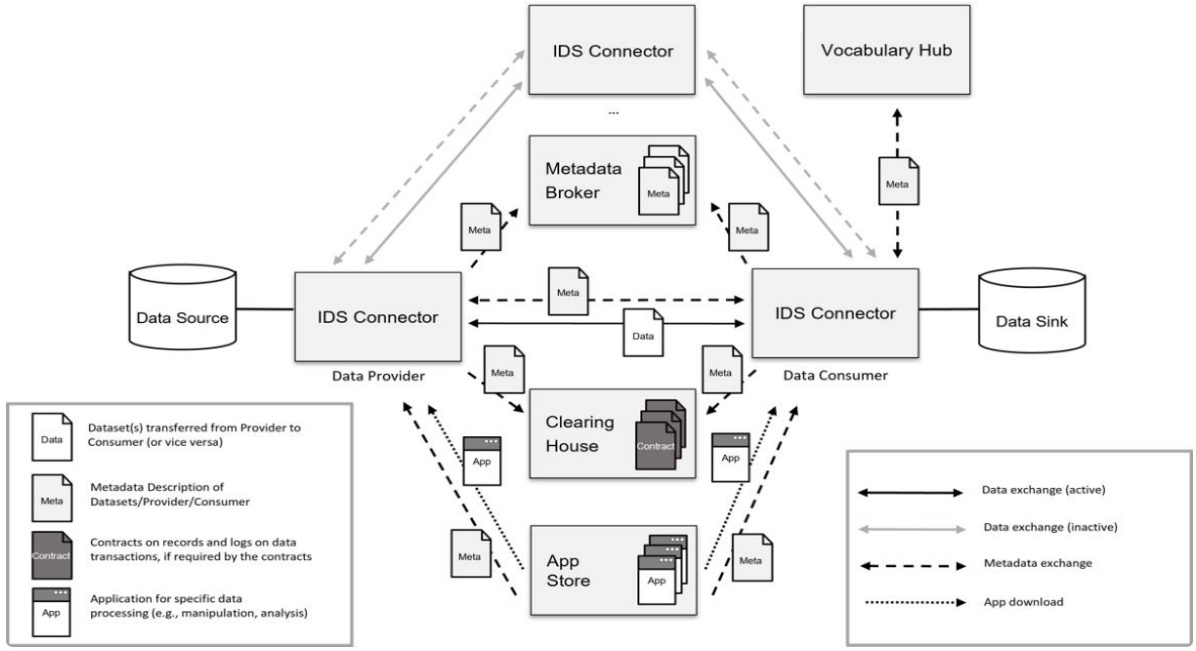
ΧΔ συγκεκριμένου τομέα. Ο IDSA έχει δημοσιεύσει σχετικό Αρχιτεκτονικό Μοντέλο Αναφοράς (Reference Architecture Model - IDS-RAM)[7], το οποίο στοχεύει να παίξει το ρόλο ενός αρχιτεκτονικό περίγραμμα (blueprint) για τη δημιουργία αξιόπιστων συστημάτων δεδομένων που προωθούν την κοινή χρήση δεδομένων. Οι βασικές στρατηγικές απαιτήσεις που επιδιώκει να ικανοποιήσει το IDS-RAM είναι: (α) εμπιστοσύνη, (β) ασφάλεια και κυριαρχία στα δεδομένα, (γ) οικοσύστημα δεδομένων, (δ) τυποποιημένη διαλειτουργικότητα, (ε) εφαρμογές προστιθέμενης αξίας, (στ) αγορά δεδομένων, (ζ) επαναχρησιμοποίηση υπαρχουσών τεχνολογιών και (η) συνεισφορά στην προτυποποίηση των αρχιτεκτονικών λύσεων.



Εικόνα 3: Δομικά στοιχεία χώρου δεδομένων κατά OpenDEI

Το IDS-RAM περιλαμβάνει πέντε επίπεδα αρχιτεκτονικής, δηλ. επιχειρηματικό επίπεδο (business layer), λειτουργικό επίπεδο (functional layer), επίπεδο διεργασιών (process layer), επίπεδο πληροφορίας (information layer) και επίπεδο συστήματος (system layer). Στο επίπεδο συστήματος γίνεται αντιστοίχιση των ρόλων που καθορίζονται στο επιχειρηματικό επίπεδο, σε συγκεκριμένα τεχνικά στοιχεία, τα οποία με τη σειρά τους δομούν μία συμπαγή αρχιτεκτονική δεδομένων και υπηρεσιών. Στην Εικόνα 3 απεικονίζεται η αλληλεπίδραση των βασικών τεχνικών στοιχείων του επιπέδου συστήματος.

[7] https://docs.internationaldataspaces.org/knowledge-base/ids-ram-4.0



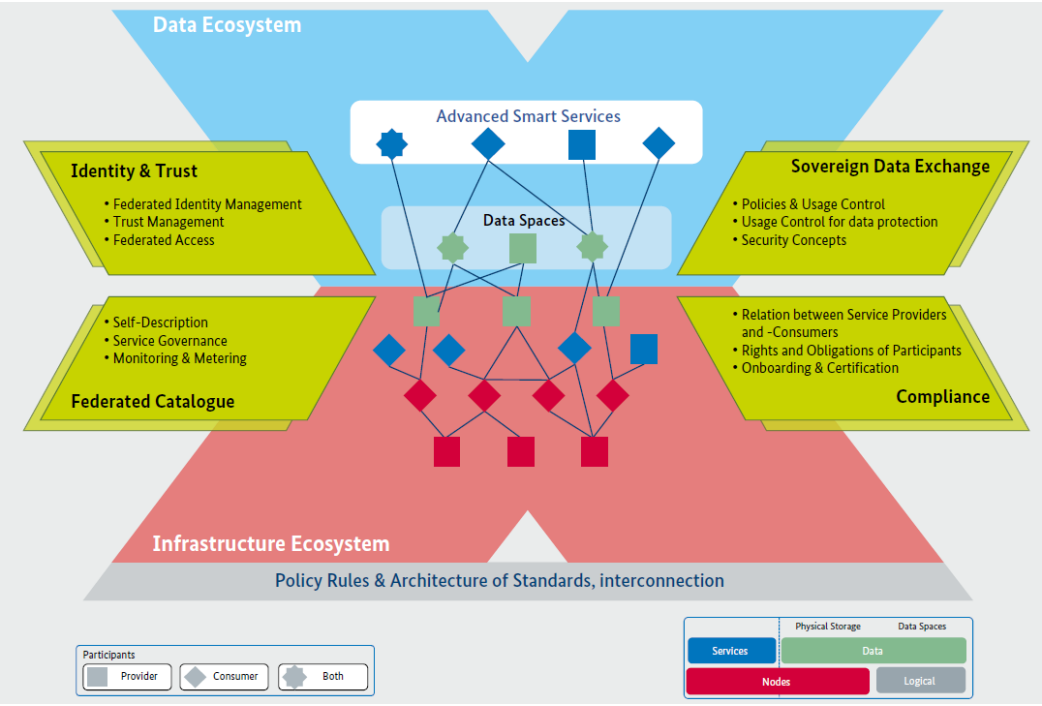
Εικόνα 4: Αλληλεπίδραση τεχνικών στοιχείων επιπέδου συστήματος IDS-RAM.

Το οικοσύστημα του IDS έχει σχεδιαστεί έτσι ώστε να είναι ευέλικτο και να μην περιορίζεται από συγκεκριμένες περιπτώσεις χρήσης ή τομείς. Για την ένταξη στο οικοσύστημα και την τυποποιημένη ανταλλαγή δεδομένων, οι συμμετέχοντες χρειάζονται τον *IDS Connector*, ένα συγκεκριμένο τεχνικό στοιχείο που λειτουργεί ως πύλη εισόδου στο οικοσύστημα, ενσωματώνοντας τις διεπαφές μεταξύ των εσωτερικών συστημάτων των συμμετεχόντων και του IDS οικοσυστήματος. Ο IDS Connector χρησιμοποιείται από όλα τα μέρη, είτε αυτά είναι παραγωγοί είτε καταναλωτές δεδομένων, έτσι ώστε να διασφαλιστεί η ασφαλής και κυρίαρχη ανταλλαγή δεδομένων (εφαρμογή πολιτικών πρόσβασης και χρήσης). Η λειτουργικότητα που παρέχει ένας IDS Connector μπορεί να επεκταθεί μέσω πιστοποιημένων εφαρμογών δεδομένων (*IDS Apps*). Αυτές είναι αυτοτελή, λειτουργικά και επαναχρησιμοποιούμενα τμήματα λογισμικού που παρέχονται με ασφαλή τρόπο από την πλατφόρμα του *IDS App Store*. Οι κατηγορίες των εφαρμογών που παρέχονται από το IDS App Store είναι: (α) *Data App*, δηλ. εφαρμογές επεξεργασίας δεδομένων (π.χ. μετασχηματισμός, καθαρισμός, συγκερασμός κ.ά.), (β) *Adapter App*, δηλ. εφαρμογές προσαρμογής και διασύνδεσης υπαρχόντων πληροφοριακών συστημάτων με τον IDS Connector, έτσι ώστε να γίνουν διαθέσιμα τα δεδομένα των συστημάτων αυτών στο Χώρο Δεδομένων, και (γ) *Control App*, δηλ. εφαρμογές που επιτρέπουν τον έλεγχο του IDS Connector από εξωτερικά συστήματα. Το στοιχείο IDS Metadata Broker είναι εκείνο που αποθηκεύει και διαχειρίζεται μεταδεδομένα σχετικά με τις διαθέσιμες πηγές δεδομένων στο οικοσύστημα, με τη μορφή τυποποιημένων self-descriptions που συντηρούν οι IDS Connectors των συμμετεχόντων. Ουσιαστικά, λειτουργεί ως κατάλογος των διαθέσιμων πηγών δεδομένων, μέσω του οποίου ένα καταναλωτής μπορεί να αναζητήσει τα δεδομένα που επιθυμεί. Το στοιχείο IDS Clearing House παρέχει υπηρεσία εκκαθάρισης και διακανονισμού (clearing and settlement service) στη βάση των

πολιτικών και συμβολαίων χρήσης, με σκοπό την αυτοματοποίηση των πληρωμών μεταξύ παρόχου και καταναλωτή δεδομένων. Επίσης, παρέχει υπηρεσία καταγραφής (logging service) των αλληλεπιδράσεων μεταξύ των μερών του οικοσυστήματος. Το στοιχείο IDS Vocabulary Hub διατηρεί και παρέχει λεξικά που χρησιμοποιούνται από τους συμμετέχοντες για την περιγραφή δεδομένων, υπηρεσιών, συμβολαίων κ.ά., με στόχο την ικανοποίηση της απαίτησης της διαλειτουργικότητας σε ένα Χώρο Δεδομένων.

2.3.4 GAIA-X

Το GAIA-X είναι μια ευρωπαϊκή πρωτοβουλία που στοχεύει στη διευκόλυνση της έμπιστης ανταλλαγής δεδομένων μεταξύ εταίρων σε μια ομοσπονδία, ένα αποκεντρωμένο οικοσύστημα δεδομένων, με έμφαση κυρίως στο επίπεδο των υπηρεσιών. Αποτελεί μία αρχιτεκτονική που υποστηρίζει την ανάπτυξη ΧΔ και διαφέρει από τις παραδοσιακές ευρωπαϊκές υπηρεσίες υπολογιστικού νέφους, παρέχοντας ένα αρχιτεκτονικό πρότυπο για τη διασύνδεση ποικίλων παρόχων υπηρεσιών υπολογιστικού νέφους, το οποίο είναι ευθυγραμμισμένο με το Γενικό Κανονισμό Προστασίας Δεδομένων και την Ευρωπαϊκή Στρατηγική Δεδομένων (European Data Strategy). Όπως φαίνεται στην Εικόνα 4, η υψηλού επιπέδου αρχιτεκτονική του GAIA-X [5] συγκροτείται αδρά από δύο διασυνδεδεμένα οικοσυστήματα, δηλ. ένα οικοσύστημα δεδομένων και ένα οικοσύστημα υποδομής. Το πρώτο προσφέρει χώρους δεδομένων με έξυπνες υπηρεσίες συγκεκριμένης βιομηχανίας (industry-specific), ενώ το δεύτερο συγκροτείται από κόμβους που παρέχουν υπολογιστικούς πόρους.



Εικόνα 5: Υψηλού επιπέδου αρχιτεκτονική GAIA-X.

Οι υπηρεσίες ομοσπονδίας (federation services) που εμπεριέχονται στην αρχιτεκτονική διασφαλίζουν τη διαλειτουργικότητα και την κυριαρχία επί των δεδομένων μέσω διαχείρισης ταυτοτήτων και εμπιστοσύνης, ομόσπονδη υπηρεσία καταλόγου και μηχανισμούς συμμόρφωσης. Η πρωτοβουλία GAIA-X παρέχει ανοιχτές προδιαγραφές και υλοποιήσεις αναφοράς για τη δημιουργία ομοσπονδιών υπαρχουσών υποδομών και όχι μεμονωμένης λειτουργικής υποδομής.

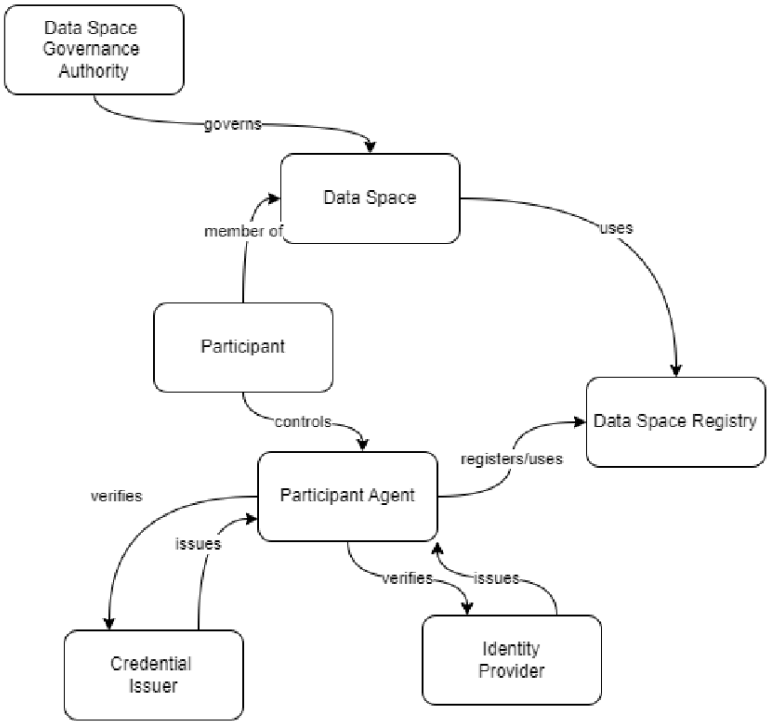
2.3.5 Data Spaces Business Alliance

Οι Big Data Value Association (BDVA), FIWARE Foundation, Gaia-X, και IDSA δημιούργησαν από κοινού το Data Spaces Business Alliance (DSBA)[8] με στόχο την προώθηση της υιοθέτησης των Χώρων Δεδομένων στην Ευρώπη. Ως μέρος αυτής της πρωτοβουλίας, τα μέλη του DSBA αναπτύσσουν ένα κοινό τεχνολογικό πλαίσιο, αντλώντας στοιχεία από υπάρχουσες αρχιτεκτονικές και μοντέλα, και λειτουργώντας συμπληρωματικά σε ήδη υπάρχουσες προδιαγραφές και υλοποιήσεις. Ο σκοπός της σύμπραξης είναι η διασφάλιση της διαλειτουργικότητας και της φορητότητας των λύσεων που αφορούν στους ΧΔ, ευθυγραμμίζοντας τεχνολογικά στοιχεία και μεθόδους διακυβέρνησης. Η προσπάθεια αυτή οδήγησε στην έκδοση ενός εγγράφου τεχνολογικής σύγκλισης (DSBA Technical Convergence document)[9]. Το έντυπο αυτό ενσωματώνει ένα Minimum Viable Framework (MVF) βασισμένο στα τεχνολογικά δομικά στοιχεία του OpenDEI και παρέχει μία αντιστοίχιση των στοιχείων του συστήματος (π.χ. connectors, federated services) με τα δομικά στοιχεία. Επιπλέον, ορίζει τους ρόλους σε ένα Χώρο Δεδομένων, όπως φαίνεται στην Εικόνα 5, και προτείνει ένα πλαίσιο μέσω του οποίου μία υπάρχουσα πλατφόρμα δεδομένων/έξυπνη πλατφόρμα μπορεί να συμμετάσχει σε ένα Χώρο Δεδομένων. Τέλος, δίνει βάρος και εγγυάται την τεχνολογική διαλειτουργικότητα, υιοθετώντας το πρότυπο IDS Communication Protocol[10].

[8] https://data-spaces-business-alliance.eu/

[9] https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf

[10] https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-g/communication/protocols/idscp2

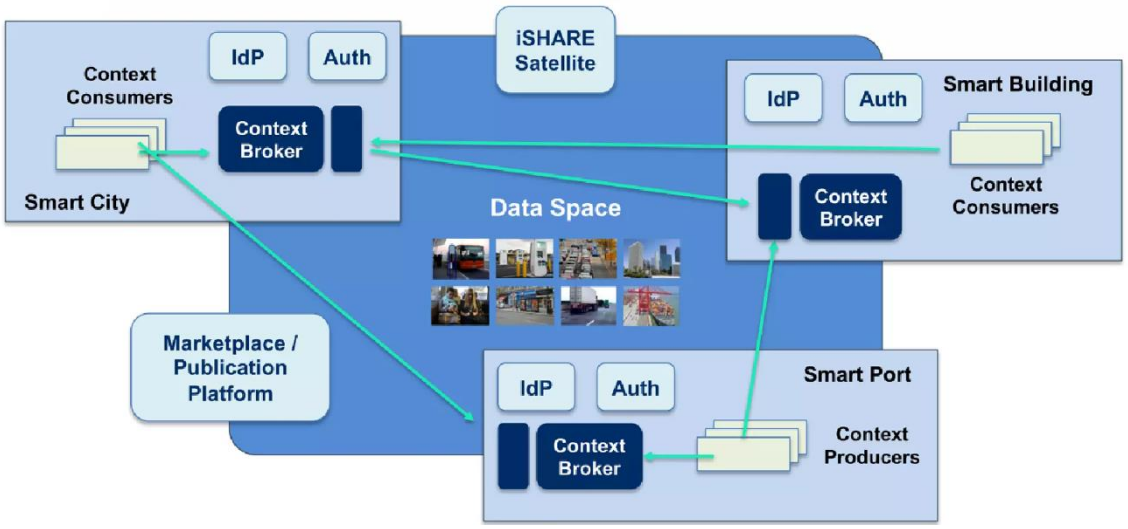


Εικόνα 6: Ρόλοι Χώρου Δεδομένων (DSBA convergence document).

2.3.6 i4Trust

Ο βασικός στόχος του έργου i4Trust[11] (Εικόνα 7) είναι η προώθηση καινοτόμων υπηρεσιών που αφορούν στις αλυσίδες αξίας δεδομένων, μέσω της υποστήριξης ανάπτυξης ΧΔ με τη συμμετοχή μικρομεσαίων επιχειρήσεων και κέντρων ψηφιακής καινοτομίας (Digital Innovation Hubs - DIHs). Για την ανάπτυξη της σχετικής αρχιτεκτονικής αναφοράς, το i4Trust ενσωματώνει καθιερωμένα δομικά στοιχεία από τα πλαίσια FIWARE και iSHARE[12]. Από τη μία πλευρά, το οικοσύστημα του FIWARE παρέχει τα εργαλεία για τη διαλειτουργικότητα σε επίπεδο μοντέλων δεδομένων (Smart Data Models) και APIs (NGSI-LD) (ο FIWARE Context Broker υποστηρίζει την αποτελεσματική ανταλλαγή δεδομένων μεταξύ των μερών), ενώ από την άλλη πλευρά το iSHARE παρέχει το πλαίσιο εμπιστοσύνης, τη διαχείριση ταυτοτήτων και τον έλεγχο πρόσβασης στο ΧΔ. Τόσο κλασικές (OIDC), όσο και αποκεντρωμένες (W3C DID, W3C VC, OIDC4VP) λύσεις διαχείρισης ταυτοτήτων και ελέγχου πρόσβασης είναι δυνατό να χρησιμοποιηθούν.

[11] https://i4trust.org/
[12] https://ishare.eu/

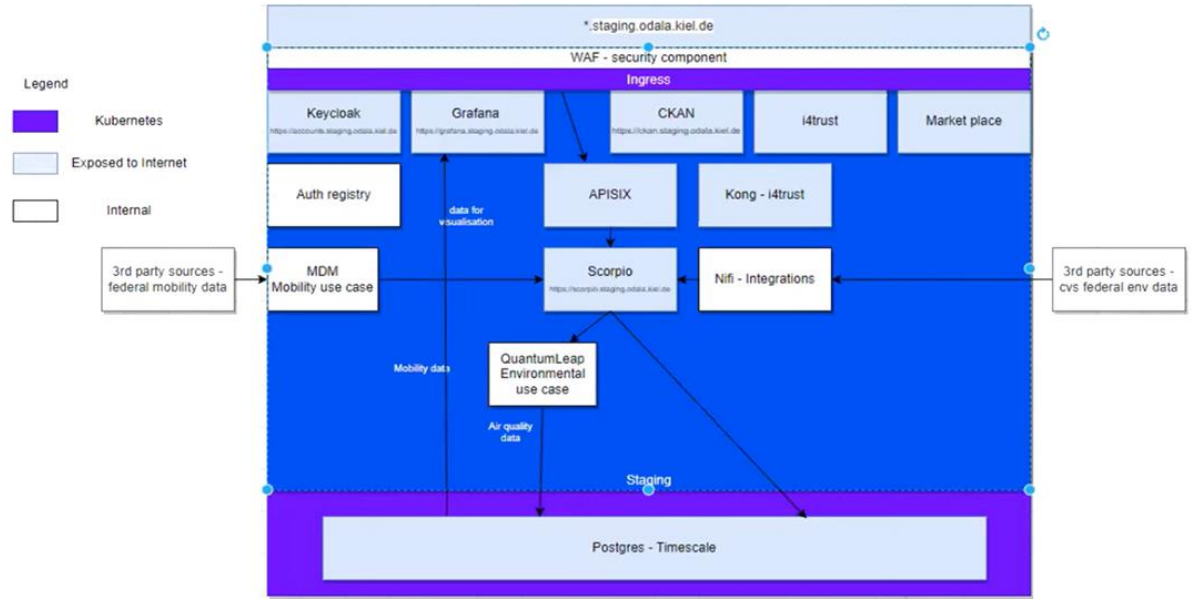


Εικόνα 7: Ανταλλαγή δεδομένων σε ένα Χώρο Δεδομένων βασισμένο στο πλαίσιο i4Trust.

2.3.7 ODALA

Το έργο ODALA[13] ("Collaborative, Secure, and Replicable Open Source Data Lakes for Smart Cities") είναι ένα έργο για τη βελτίωση της διαχείρισης δεδομένων σε πόλεις και περιφέρειες. Ένα σύμπλεγμα εταιρειών και ερευνητικών ινστιτούτων αξιοποιεί τεχνολογίες ανοιχτού κώδικα και ψηφιακού μετασχηματισμού προς όφελος της δημόσια διοίκησης σε πόλεις τεσσάρων ευρωπαϊκών χωρών. Το έργο ODALA υιοθετεί την ευρωπαϊκή Ψηφιακή Υποδομή Υπηρεσιών (Digital Service Infrastructure - DSI) διαμέσου των Connecting Europe Facility (CEF) Building Blocks, ώστε να δημιουργήσει ένα περιβάλλον και αγορά διαμοιρασμού δεδομένων μεταξύ πόλεων και εταιρειών. Το περιβάλλον αυτό, το οποίο χαρακτηρίζεται ως data lake, επιτρέπει στις πόλεις να παρέχουν διαφορετικού τύπου δεδομένα (στατικά, ιστορικά και πραγματικού χρόνου). Η αρχιτεκτονική του έργου ODALA (Εικόνα 8) βασίζεται στο FIWARE-SCRA, ενσωματώνοντας επίσης στοιχεία της αρχιτεκτονικής του i4Trust, ώστε να ευθυγραμμιστεί καλύτερα στη λογική των ΧΔ. Είναι μια αρχιτεκτονική περισσότερο προσαρμοσμένη στην υλοποίηση (implementation-oriented architecture), σχεδιασμένη με bottom-up λογική, βασισμένη δηλ. σε παραδείγματα χρήσης (π.χ. έξυπνη κινητικότητα, επιτήρηση/ανίχνευση περιβάλλοντος κ.ά.).

[13] https://odalaproject.eu/

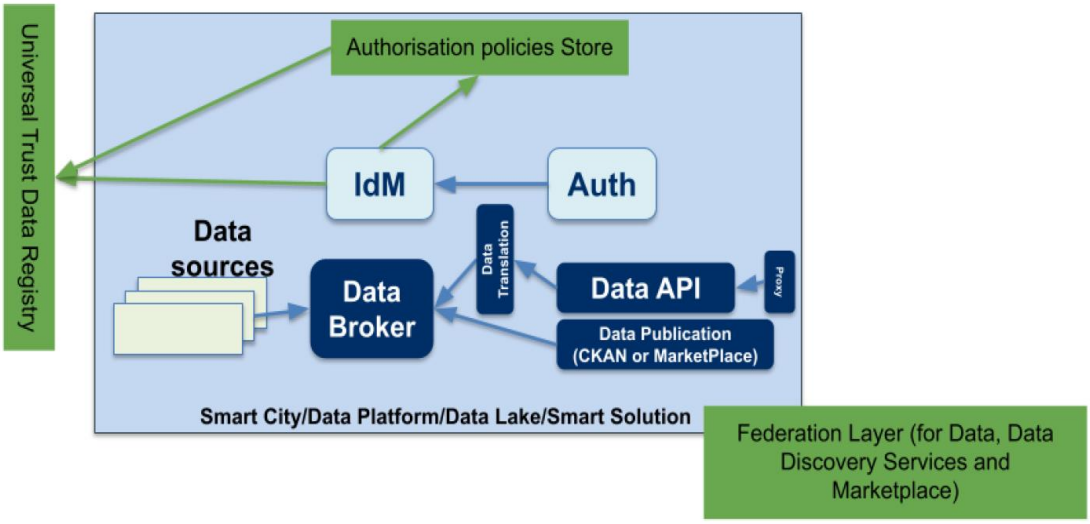


Εικόνα 8: Αρχιτεκτονική ODALA

2.3.8 Data Space for Smart and Sustainable Cities and Communities

Το έργο Data Space for Smart and Sustainable Cities and Communities (DS4SSCC) αποτελεί μία δράση για τη δημιουργία ΧΔ έξυπνων κοινοτήτων και πόλεων. Το αρχιτεκτονικό μοντέλο που προτείνει είναι βασισμένο στις σχεδιαστικές αρχές ενός ΧΔ, όπως αυτές ορίζονται από το Data Space Support Center (DSSC) (διαλειτουργικότητα, κυριαρχία, οικοσύστημα δεδομένων, ασφάλεια, αποκέντρωση) και ενσωματώνει τους μηχανισμούς ελάχιστης διαλειτουργικότητας (Minimum Interoperability Mechanisms) για την υλοποίηση του ΧΔ. Στον πυρήνα του το DS4SSCC επιδιώκει να ορίσει μία αρχιτεκτονική, η οποία επιτρέπει την εξέλιξη μίας πλατφόρμας δεδομένων/έξυπνης πλατφόρμας (data platform/smart platform) σε μορφή που μπορεί να ενσωματωθεί σε ένα ΧΔ (data-space ready). Αφού αναγνωρίζονται τρία επίπεδα ωριμότητας των υπαρχουσών πλατφορμών (greenfield, brownfield, digital twin) και ορίζονται τα βασικά κοινά δομικά στοιχεία τους, περιγράφονται τα συμπληρωματικά στοιχεία που απαιτούνται για το μετασχηματισμό και τη σύνδεσή τους διά μέσου ενός ΧΔ.

Τα στοιχεία με πράσινο χρώμα στην Εικόνα 9 αποτελούν τις οντότητες που καθιστούν εφικτό το μετασχηματισμό μίας πλατφόρμας δεδομένων σε ένα σύστημα έτοιμο προς συμμετοχή σε ΧΔ. Συγκεκριμένα, αυτά είναι: (α) Universal Trust Data Registry, το οποίο αποτελεί το πλαίσιο



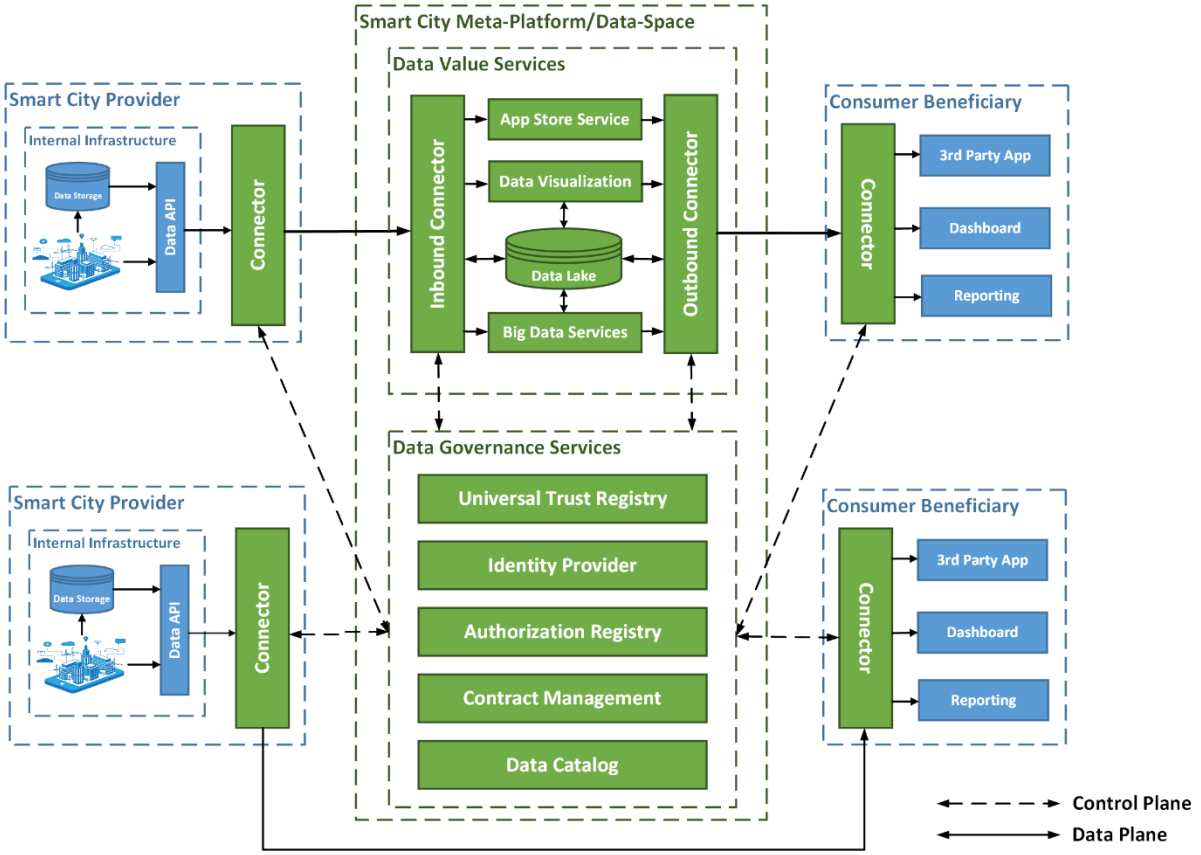
Εικόνα 9: Υψηλού επιπέδου αρχιτεκτονική DS2SSCC.

εμπιστοσύνης που επιτρέπει την ανταλλαγή δεδομένων με ασφαλή τρόπο και ενσωματώνει μηχανισμούς ταυτοποίησης, αυθεντικοποίησης και εξουσιοδότησης τόσο Machine-to-Machine (M2M) όσο και Human-to-Machine (H2M), (β) Authorization Policy Store, το οποίο σχετίζεται στενά με τη διαχείριση ταυτοτήτων σε επίπεδο κάθε συμμετέχοντα και περιλαμβάνει τις πολιτικές πρόσβασης στα δεδομένα, και (γ) Federation Layer, το οποίο περιλαμβάνει όλα εκείνα τα στοιχεία που επιτρέπουν χρήστες από τους διάφορους συμμετέχοντες να αποκτούν πρόσβαση στις υπηρεσίες και τα δεδομένα που προσφέρονται μέσα στο ΧΔ, π.χ. υπηρεσίες καταλόγου, υπηρεσίες αγοράς δεδομένων κ.ά

3. Αρχιτεκτονική μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων

Στην παρούσα ενότητα παρουσιάζουμε την υψηλού επιπέδου αρχιτεκτονική της μετα-πλατφόρμας και αναλύουμε τα επιμέρους αρχιτεκτονικά στοιχεία της. Η μετα-πλατφόρμα σχεδιάστηκε έτσι ώστε να:

- καθιστά εφικτή τη διασύνδεση ετερογενών καθετοποιημένων υπαρχουσών λύσεων έξυπνων πόλεων σε ένα στενά ενσωματωμένο οικοσύστημα,
- διασφαλίζει τη διαλειτουργικότητα σε επίπεδο δεδομένων και υπηρεσιών, διαμέσου της υιοθέτησης κοινών μοντέλων δεδομένων και ενοποιημένων προγραμματιστικών διεπαφών εφαρμογών για την ανάκτηση και την ανταλλαγή δεδομένων,
- παρέχει το πλαίσιο εμπιστοσύνης για τη διασφάλιση της έμπιστης και αυτοκυρίαρχης ανταλλαγής δεδομένων σύμφωνα με σαφώς ορισμένες πολιτικές πρόσβασης και χρήσης των δεδομένων,
- υιοθετεί μία προσέγγιση αποκεντρωμένης αποθήκευσης των διαθέσιμων δεδομένων,
- αξιοποιεί τα ομογενοποιημένα συλλεχθέντα δεδομένα για να παρέχει υπηρεσίες προστιθέμενης αξίας, όπως υπηρεσίες προχωρημένης οπτικοποίησης, ανάλυσης μεγάλων δεδομένων κ.ά.



Εικόνα 10: Υψηλού επιπέδου αρχιτεκτονική μετα-πλατφόρμας έξυπνων πόλεων

Στην Εικόνα 10 απεικονίζεται η υψηλού επιπέδου αρχιτεκτονική της μετα-πλατφόρμας. Με πράσινο χρώμα απεικονίζονται τα στοιχεία που ανήκουν εγγενώς στη μετα-πλατφόρμα (ή Χώρο Δεδομένων), ενώ με μπλε χρώμα απεικονίζονται τα στοιχεία που ανήκουν σε συστήματα που αλληλοεπιδρούν με την μετα-πλατφόρμα, αλλά δεν ανήκουν σε αυτή. Συγκεκριμένα, διακρίνουμε δύο εξωτερικές οντότητες, δηλ. (α) τους παρόχους καθετοποιημένων λύσεων έξυπνων πόλεων (Smart City providers), οι οποίοι διαθέτουν κάποια υπάρχουσα υποδομή έξυπνων πόλεων, από την οποία μπορούν να συλλέξουν και να αποθηκεύσουν σχετικά δεδομένα, τα οποία στη συνέχεια διαθέτουν μέσω κατάλληλου Data API, και (β) τους ωφελούμενους καταναλωτές δεδομένων και υπηρεσιών, οι οποίοι μπορούν να έχουν πρόσβαση στα δεδομένα των παρόχων διαμέσου της πλατφόρμας, με σκοπό τη χρήση τους σε τρίτες εφαρμογές.

Στον πυρήνα της πλατφόρμας υπάρχουν δύο κατηγορίες υπηρεσιών: (α) Υπηρεσίες Διακυβέρνησης Δεδομένων (Data Governance Services), και (β) Υπηρεσίες Αξίας Δεδομένων (Data Value Services). Η διαδικασία ανάκτησης/ανταλλαγής των δεδομένων μεταξύ των συμμετεχόντων μερών καθίσταται εφικτή μέσω του στοιχείου Connector, το οποίο προσφέρει την απαραίτητη τεχνική στοίβα για αυτό το σκοπό. Το στοιχείο Connector χρησιμοποιείται εδώ, όπως ορίζεται στο αρχιτεκτονικό μοντέλο αναφοράς IDS-RAM, και λειτουργεί ως ένας διαμεσολαβητής που παρέχει τις απαραίτητες διεπαφές για τη σύνδεση και επικοινωνία με το οικοσύστημα της μετα-πλατφόρμας, διασφαλίζοντας τη διαλειτουργικότητα και την εμπιστοσύνη στο διαμοιρασμό των δεδομένων.

3.1 Υπηρεσίες Διακυβέρνησης Δεδομένων

Ως Διακυβέρνηση Δεδομένων ορίζουμε το πλαίσιο από διαδικασίες, πολιτικές και μηχανισμούς που αφορούν στη διαχείριση και εποπτεία του κύκλου ζωής των δεδομένων που διακινούνται στο οικοσύστημα της μετα-πλατφόρμας. Η Διακυβέρνηση Δεδομένων αυξάνει τη συνέπεια και την εμπιστοσύνη των δεδομένων που έχουν καταχωρηθεί, βελτιώνοντας την ασφάλειά τους και ελαχιστοποιώντας τον κίνδυνο μη συμμόρφωσης με τους σχετικούς κανονισμούς. Οι Υπηρεσίες Διακυβέρνησης Δεδομένων της πλατφόρμας περιλαμβάνουν, τα παρακάτω στοιχεία:

- **Καθολικό Μητρώο Εμπιστοσύνης (Universal Trust Registry):** Το Καθολικό Μητρώο Εμπιστοσύνης παίζει το ρόλο του πλαισίου εμπιστοσύνης που είναι απαραίτητο για την ασφαλή και έμπιστη ανταλλαγή δεδομένων. Ενσωματώνει ένα πρωτόκολλο αυθεντικοποίησης και εξουσιοδότησης τόσο για M2M, όσο και H2M επικοινωνία, παίζοντας το ρόλο της αρχής εμπιστοσύνης (trust authority). Το μητρώο καταχωρεί τους έμπιστους συμμετέχοντες (trusted participants) του ΧΔ αλλά και τους έμπιστους εκδότες διαπιστευτηρίων (trusted issuers). Μπορεί να υλοποιηθεί είτε βασιζόμενο σε κλασική λύση Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure - PKI), όπου κάθε συμμετέχων διαθέτει ένα ζεύγος ιδιωτικού /

δημοσίου κλειδιού και κατάλληλο ψηφιακό πιστοποιητικό, είτε βασισμένο σε αποκεντρωμένο πλαίσιο εμπιστοσύνης, όπως προτείνεται από το DSBA, συμβατό με την αρχιτεκτονική EUDI Wallet Architecture[14]. Η αποκεντρωμένη λύση μπορεί να χρησιμοποιεί τα τελευταία W3C και OIDC πρότυπα: (α) W3C Decentralized Identifiers (DID)[15] και Verifiable Credentials[16] (VC), (β) OpenIDConnect for Verifiable Credentials Issuance (OIDC4VCI)[17], (γ) OpenIDConnect for Verifiable Presentations (OIDC4VP)[18]. Εν γένει, το Καθολικό Μητρώο Εμπιστοσύνης θα πρέπει να διαθέτει τα παρακάτω στοιχεία/λειτουργικότητες: (α) αποθήκευση ιδιωτικών κλειδιών (περίπτωση PKI), (β) λίστα ανάκλησης (περίπτωση PKI), (γ) λίστα έμπιστων συμμετεχόντων, (δ) λίστα έμπιστων εκδοτών, (ε) κατάλληλα APIs. Υπάρχουσες υλοποιήσεις ενός Καθολικού Μητρώου Εμπιστοσύνης είναι το iSHARE Trust Framework[19] (χρησιμοποιείται στα i4Trust και ODALA) και το GAIA-X Trust Framework[20].

- **Διαχείριση Ταυτότητας (Identity Management):** Η Διαχείριση Ταυτοτήτων είναι απαραίτητη για την αποθήκευση των ταυτοτήτων των χρηστών των συμμετεχόντων μερών, π.χ. αναγνωριστικά χρηστών, email, κωδικοί πρόσβασης κτλ. Δημοφιλείς υλοποιήσεις Διαχείρισης Ταυτότητας είναι ολοκληρωμένες IAM λύσεις, όπως το Keyrock[21] και Keycloak[22].
- **Μητρώο Εξουσιοδότησης (Authorization Registry):** Το Μητρώο Εξουσιοδότησης είναι στενά συνδεδεμένο με το στοιχείο Διαχείριση Ταυτότητας και συντηρεί τις πολιτικές πρόσβασης. Πρακτικά, παίζει το ρόλο του Σημείου Απόφασης Πολιτικών (Policy Decision Point - PDP), σύμφωνα με το eXtensible Access Control Markup Language (XACML), κατά την υλοποίηση του πρωτοκόλλου ελέγχου πρόσβασης στις διαθέσιμες υπηρεσίες και δεδομένα, δηλ. της οντότητας η οποία αποφασίζει αν επιτρέπεται ή όχι η πρόσβαση ενός χρήστη σε συγκεκριμένους πόρους. Μπορεί να παρέχεται ως ενσωματωμένο στη λύση Διαχείρισης Ταυτότητας ή να υφίσταται ως αυτοτελές στοιχείο, π.χ. iSHARE Authorization Registry[23].
- **Διαχείριση Συμβολαίων (Contract Management):** Η Διαχείριση Συμβολαίων είναι υπεύθυνη για τη διατήρηση των συμβολαίων διαμοιρασμού δεδομένων μεταξύ παρόχου και καταναλωτή δεδομένων. Η κατάσταση των συμβολαίων αυτών αποθηκεύεται και ενημερώνεται στο συγκεκριμένο στοιχείο της αρχιτεκτονικής, και αξιοποιείται κατά τα αιτήματα πρόσβασης στα δεδομένα από πλευράς καταναλωτή. Το FIWARE Contract

[14] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
[15] https://www.w3.org/TR/did-core/
[16] https://www.w3.org/TR/vc-data-model-2.0/
[17] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[18] https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
[19] https://ishare.eu/home/about/trust-framework/
[20] https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/
[21] https://keyrock-fiware.github.io/
[22] https://www.keycloak.org/
[23] https://dev.ishare.eu/reference/authorization.html

Management Service[24] είναι μια ενδεικτική υλοποίηση ενός στοιχείου Διαχείρισης Συμβολαίων, το οποίο βασίζεται σε γεγονότα που ορίζονται στο Open TM Forum API[25], για να αποτυπώσει την ανά πάσα στιγμή κατάσταση των συμβολαίων.

- **Κατάλογος Δεδομένων (Data Catalog):** Ο Κατάλογος Δεδομένων είναι απαραίτητος για τη δημοσίευση της μεταπληροφορίας των διαθέσιμων δεδομένων από πλευράς παρόχων, έτσι ώστε να μπορούν να αναζητηθούν και βρεθούν από τους καταναλωτές. Η μεταπληροφορία σχετικά με τα διαθέσιμα σύνολα δεδομένων μπορεί να εκφραστεί διαμέσου κατάλληλων λεξικών, όπως το W3C Data Catalog Vocabulary (DCAT)[26]. Λύσεις, όπως το FIWARE Business API Ecosystem[27] μπορούν να χρησιμοποιηθούν για την υλοποίηση του Καταλόγου Δεδομένων.

3.2 Υπηρεσίες Αξίας Δεδομένων

Ο διαλειτουργικός διαμοιρασμός/ανάκτηση δεδομένων από πολλαπλές ετερογενείς κάθετες υλοποιήσεις Έξυπνων Πόλεων επιτρέπει την ανάπτυξη νέων εφαρμογών και υπηρεσιών που θα συνδυάζουν ή/και συγχωνεύουν τα δεδομένα που αντλούνται. Η συλλογή ομογενοποιημένων δεδομένων από πολλαπλές πηγές χαρακτηρίζεται από μεγάλο όγκο, ταχύτητα και μεταβλητότητα, δημιουργώντας σύνολα δεδομένων που εμπίπτουν στην κατηγορία των μεγάλων δεδομένων. Η μετα-πλατφόρμα διασυνδεδεμένων Έξυπνων Πόλεων σκοπεύει να αξιοποιήσει τα δεδομένα αυτά για την παροχή υπηρεσιών προστιθέμενης αξίας και την υποστήριξη καθοδηγούμενων-από-δεδομένα (data-driven) αποφάσεων σχετικών με την υποδομή Έξυπνων Πόλεων. Αυτός είναι ο ρόλος της ομάδας Υπηρεσιών Αξίας Δεδομένων που συγκροτείται από τα παρακάτω στοιχεία:

- **Υπηρεσία Αποθετηρίου Εφαρμογών (App Store Service):** Η Υπηρεσία Αποθετηρίου Εφαρμογών αποτελεί μια ασφαλή υπηρεσία για το διαμοιρασμό πιστοποιημένων εφαρμογών δεδομένων προς τα συμμετέχοντα μέρη του οικοσυστήματος. Ακολουθεί τη φιλοσοφία του IDS App Store[28], όπως αυτό περιγράφεται στο IDS-RAM. Διαθέτει μητρώο διαθέσιμων εφαρμογών και τη δυνατότητα αναζήτησης εφαρμογών βάσει διαφορετικών κριτηρίων. Επίσης, υποστηρίζει λειτουργίες καταχώρησης, δημοσίευσης, ενημέρωσης και παροχής της εφαρμογής σε συμμετέχοντα που σκοπεύει να την αναπτύξει προς χρήση.
- **Υπηρεσίες Μεγάλων Δεδομένων (Big Data Services):** Οι υπηρεσίες αυτές αφορούν κυρίως σε προχωρημένες υπηρεσίες ανάλυσης μεγάλων δεδομένων. Ιστορικά δεδομένα ή/και

[24] https://github.com/FIWARE/contract-management
[25] https://www.tmforum.org/oda/open-apis/
[26] https://www.w3.org/TR/vocab-dcat-2/
[27] https://github.com/FIWARE-TMForum/Business-API-Ecosystem
[28] https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3_5_0_system_layer/3_5_3_app_store_and_data_apps

δεδομένα πραγματικού χρόνου που αντλούνται ακολουθώντας το μοντέλο δεδομένων της πλατφόρμας μπορούν να αξιοποιηθούν για την ανάλυση δεδομένων χρησιμοποιώντας τεχνικές μηχανικής μάθησης. Ενδεικτικά παραδείγματα τέτοιων υπηρεσιών μπορούν να είναι προβλεπτική εποπτεία υποδομών Έξυπνης Πόλης, πρόβλεψη κυκλοφορίας σε πραγματικό χρόνο, ανάλυση και πρόβλεψη ενεργειακής κατανάλωσης κτιρίων/υποδομών, εποπτεία ποιότητας νερού/εντοπισμός διαρροών στο δίκτυο ύδρευσης κ.ά.

- **Οπτικοποίηση δεδομένων (Data Visualization):** Η μετα-πλατφόρμα διασυνδεδεμένων Έξυπνων Πόλεων σκοπεύει να παρέχει υπηρεσίες προχωρημένων τεχνικών οπτικοποίησης δεδομένων, οι οποίες θα διαδραματίζουν κρίσιμο ρόλο στην προσθήκη αξίας στα δεδομένα που ανταλλάσσονται, βελτιώνοντας την κατανόηση, διευκολύνοντας την ανακάλυψη πληροφοριών, ενισχύοντας την επικοινωνία, υποστηρίζοντας τη λήψη αποφάσεων και επιτρέποντας την δεδομενοκεντρική εξερεύνηση και περιγραφή. Οι υπηρεσίες οπτικοποίησης θα επιτρέπουν τη δυναμική απεικόνιση δεδομένων ΔτΠ του συνόλου των καθετοποιημένων λύσεων που θα συμμετέχουν στο οικοσύστημα, αλλά και των αποτελεσμάτων της ανάλυσης δεδομένων, όπως αυτή υλοποιείται από τις Υπηρεσίες Μεγάλων Δεδομένων της μετα-πλατφόρμας.
- **Λίμνη Δεδομένων (Data Lake):** Η μετα-πλατφόρμα υιοθετεί την προσέγγιση της αποκεντρωμένης ομοσπονδίας δεδομένων, δλδ. τα δεδομένα των παρόχων παραμένουν αποθηκευμένα στην υποδομή τους, από την οποία μπορούν να ανακτηθούν. Παρ' όλα αυτά ενδέχεται κατά περίπτωση να απαιτείται η προσωρινή αποθήκευση δεδομένων από διαφορετικές πηγές ή δεδομένων που έχουν υποστεί προ-επεξεργασία (π.χ. φιλτράρισμα, μετασχηματισμό, συγκερασμό κ.ά.) πριν τη χρήση τους από τις Υπηρεσίες Μεγάλων Δεδομένων ή/και την Οπτικοποίηση Δεδομένων, αλλά και τη διάθεσή τους στους καταναλωτές ωφελούμενους. Η Λίμνη Δεδομένων παίζει το ρόλο του προσωρινού αποθηκευτικού χώρου αυτών των δεδομένων.

3.3 Connectors (Υποσύστημα Διασύνδεσης)

Ο Connector είναι ένα ιδιαίτερα σημαντικό στοιχείο σε ένα οικοσύστημα ΧΔ. Σύμφωνα με το αρχιτεκτονικό μοντέλο IDS-RAM, ο Connector αποτελεί το βασικό τεχνολογικό στοιχείο διαμέσου του οποίου επιτυγχάνεται η διασφάλιση των πολιτικών διακυβέρνησης των δεδομένων, όπως αυτές ορίζονται στα πλαίσια του συγκεκριμένου ΧΔ, αλλά και ο τυποποιημένος διαμοιρασμός των δεδομένων μεταξύ των συμμετεχόντων. Κάθε συμμετέχων στο ΧΔ διαθέτει έναν Connector, ο οποίος παρέχει τις εξής βασικές λειτουργικότητες:

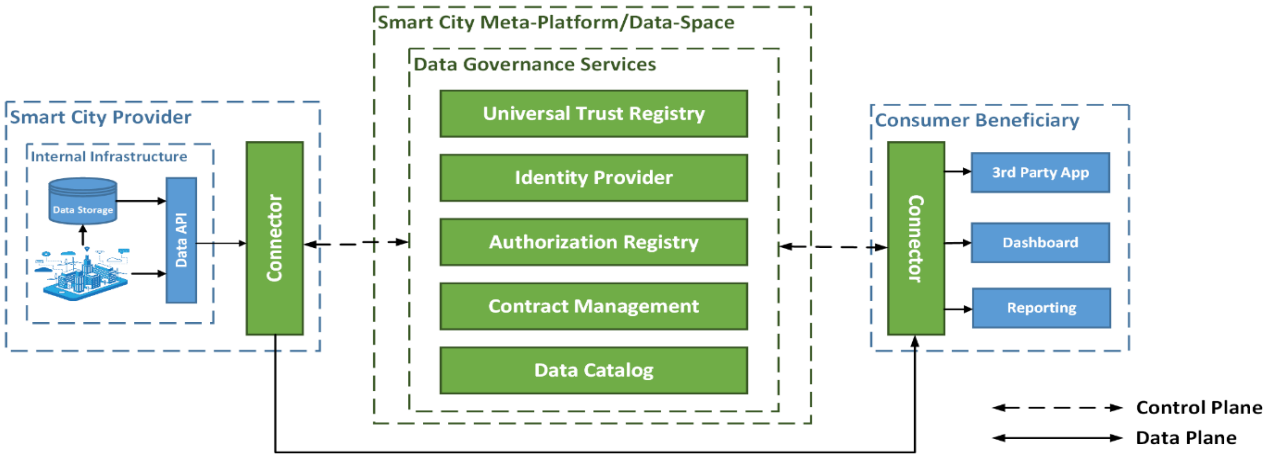
- Ενσωμάτωση (onboarding) του συμμετέχοντα (παραγωγός ή καταναλωτής) στο οικοσύστημα και καταχώρησή του ως έμπιστης οντότητας του ΧΔ.

- Δημοσίευση/ενημέρωση μεταδεδομένων των διαθέσιμων δεδομένων στον κατάλογο δεδομένων του ΧΔ (περίπτωση παρόχου).
- Διαπραγμάτευση συμβολαίου (contract negotiation) μεταξύ παρόχου και καταναλωτή για την πρόσβαση και χρήση παρεχόμενων δεδομένων, βασιζόμενα στις σχετικές πολιτικές.
- Ενορχήστρωση ανταλλαγής/διαμοιρασμού δεδομένων μεταξύ παρόχου και καταναλωτή.
- Προμήθεια και εκτέλεση εφαρμογών δεδομένων από το Αποθετήριο Εφαρμογών Δεδομένων.

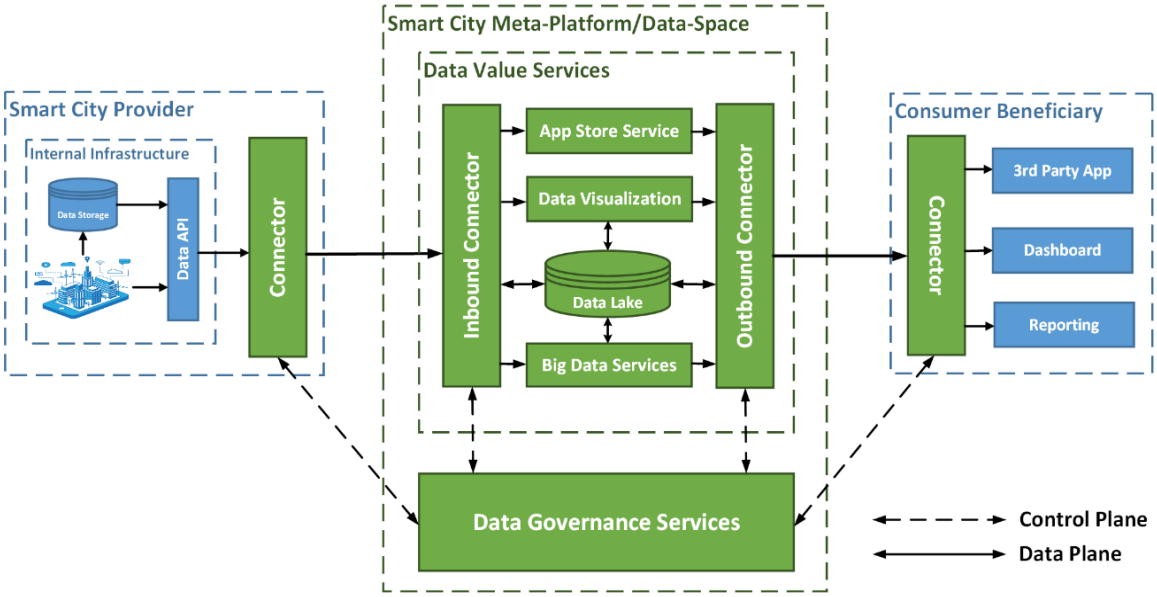
Στην περίπτωση της μετα-πλατφόρμας διασυνδεδεμένων πόλεων του έργου, διακρίνουμε τις εξής κατηγορίες Connectors (Εικόνα 10):

- Connector (καθετοποιημένης λύσης) Έξυπνης Πόλης (παρόχου)
- Connector καταναλωτή / ωφελούμενου
- Connectors μετα-πλατφόρμας σχετικών με την παροχή Υπηρεσιών Αξίας Δεδομένων: (α) Εισερχόμενος Connector (Inbound Connector), για την κατανάλωση δεδομένων από τους παρόχους καθετοποιημένων λύσεων, (β) Εξερχόμενος Connector (Outbound Connector), για την παροχή δεδομένων που παράγονται από τις Υπηρεσίες Αξίας Δεδομένων προς τους ωφελούμενους καταναλωτές. Επισημαίνεται ότι ο διαχωρισμός σε Εισερχόμενο και Εξερχόμενο Connector γίνεται σε λογικό επίπεδο, ενώ σε επίπεδο υλοποίησης είναι δυνατόν να υπάρχει ένας Connector που θα επιτελεί και τους δύο ρόλους.

Όπως φαίνεται στην Εικόνα 10, διακρίνουμε δύο περιπτώσεις ροής δεδομένων από τους παρόχους καθετοποιημένων λύσεων Έξυπνης Πόλης προς τους καταναλωτές ωφελούμενους. Στην πρώτη περίπτωση, η οποία για ευκολία παρουσιάζεται στην Εικόνα 11, τα δεδομένα διαμοιράζονται απ' ευθείας μεταξύ παραγωγού και καταναλωτή. Στη δεύτερη περίπτωση, η οποία απεικονίζεται στη Εικόνα 12, τα δεδομένα διαμοιράζονται διά μέσου της υποδομής της μετα-πλατφόρμας και συγκεκριμένα ύστερα από χρήση των Υπηρεσιών Αξίας Δεδομένων. Σε κάθε περίπτωση, η ενορχήστρωση μεταξύ των Connectors για την προετοιμασία τους διαμοιρασμού γίνεται μέσω των Υπηρεσιών Διακυβέρνησης της μετα-πλατφόρμας (ενσωμάτωση συμμετέχοντα, καταχώριση μεταδεδομένων στον κατάλογο, διαπραγμάτευση συμβολαίων κ.τ.λ.).

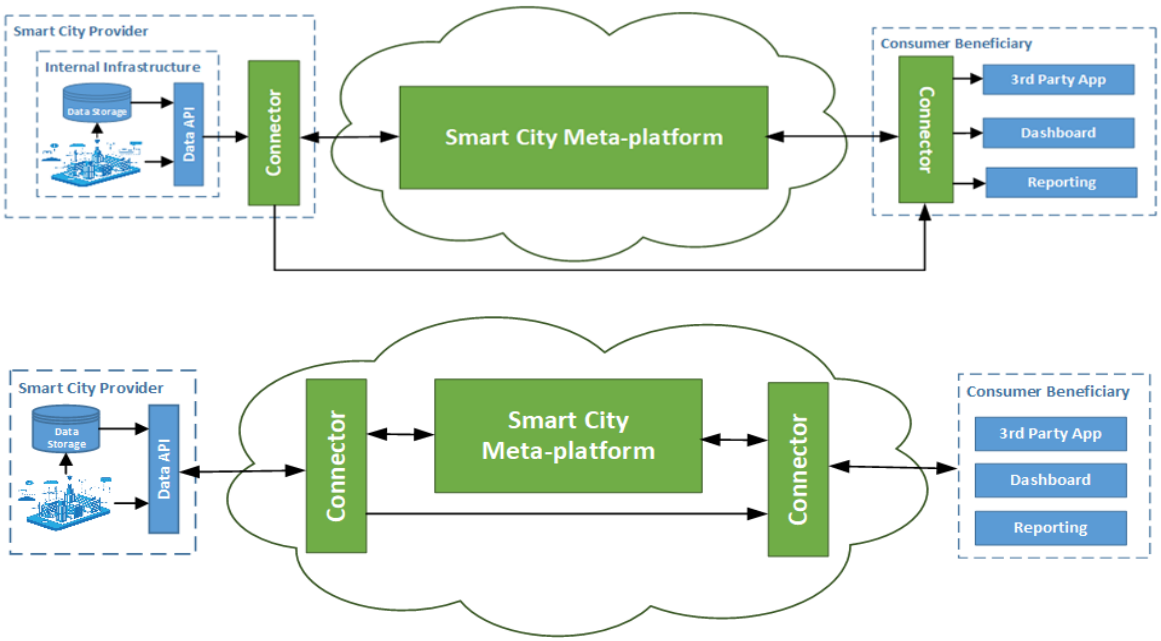


Εικόνα 11: Απ' ευθείας διαμοιρασμός δεδομένων μεταξύ παρόχου και καταναλωτή



Εικόνα 12: Διαμοιρασμός δεδομένων διαμέσου Υπηρεσιών Αξίας Δεδομένων.

Ένας Connector, όπως αναφέρθηκε και παραπάνω, δεν είναι ένα μεμονωμένο στοιχείο λογισμικού, αλλά μια τεχνολογική στοίβα που επιτελεί ένα σύνολο λειτουργικοτήτων για το διαμοιρασμό των δεδομένων. Η ανάπτυξη (deployment) της τεχνολογικής αυτής στοίβας μπορεί να γίνει με δύο διαφορετικούς τρόπους (Εικόνα 13): (α) στις εγκαταστάσεις (on-premises) του παρόχου καθετοποιημένης λύσης ή καταναλωτή ωφελούμενου, (β) σε υποδομή υπολογιστικού νέφους, ως υπηρεσία (Connector-as-a-Service). Η πρώτη λύση προσφέρει μεγαλύτερη ευελιξία και δυνατότητα παραμετροποίησης/ελέγχου της τεχνολογικής στοίβας του Connector, ενώ η δεύτερη μικρότερο διαχειριστικό φόρτο και απαίτηση σε εγκατεστημένους πόρους στις εγκαταστάσεις του συμμετέχοντα.



Εικόνα 13: Τρόποι ανάπτυξης (deployment) Connector: (πάνω) στις εγκαταστάσεις (on-premises), (κάτω) ως-υπηρεσία (as-a-Service)

4. Κυβερνοασφάλεια

4.1 Γενικά

Το τοπίο των απειλών (cyber-threat landscape) επεκτείνεται συνεχώς με πολυάριθμες επιθέσεις, όπως κακόβουλο λογισμικό (malware), άρνηση υπηρεσίας (denial of service), λυτρισμικό (ransomware), κλοπή ταυτότητας (identity theft), κλπ., που συμβαίνουν σε κρίσιμης σημασίας αλλά και άλλες υποδομές με συχνά καταστροφικές συνέπειες. Υπάρχει μία ποικιλία από παράγοντες απειλών (threat agents) όπως κυβερνο-εγκληματίες, εθνικές οντότητες, κλπ., που επιδιώκουν συνεχώς να εντοπίσουν και να εκμεταλλευτούν τα τρωτά σημεία των τεχνολογιών που χρησιμοποιούνται στις διάφορες υποδομές, παρακολουθώντας στενά τις τάσεις της τεχνολογίας και την υιοθέτηση του κύκλου ζωής της (adoption lifecycle). Εν τω μεταξύ, οι πρόσφατες γεωπολιτικές εντάσεις (Πανδημία COVID, πόλεμος στην Ουκρανία, κλπ.), έχουν κάνει την ασφάλεια στον κυβερνοχώρο μέρος του «οπλοστασίου» με εξελιγμένες και επίμονες επιθέσεις, ενώ διάφοροι κυβερνο-εγκληματίες έχουν αυξήσει την εξειδίκευση και επικινδυνότητά τους μέσω λογισμικού για την δημιουργία κυβερνο-επιθέσεων που προσφέρεται ως υπηρεσία (software offered as-a-service) , γεγονός που επιτρέπει την δημιουργία επιθέσεων, οι οποίες είναι δύσκολο να προβλεφθούν αλλά και να εντοπιστούν. Είναι αναπόφευκτο ότι σε κάθε είδος τεχνολογίας, υπάρχει ένα σύνολο τρωτών σημείων (ευπάθειες-vulnerabilities) προς εκμετάλλευση για την δημιουργία επιθέσεων, των οποίων οι συνέπειες είναι συνήθως συνάρτηση του τύπου της ευπάθειας, των δυνατοτήτων των επιτιθέμενων αλλά και της χρονικής στιγμής που έγινε η επίθεση.

Το τοπίο των απειλών αυξάνεται συνεχώς, μετά την ευρεία χρήση τεχνολογιών που σχετίζονται με τα IoT, Edge Computing, Cloud Computing. Τα περιστατικά που σχετίζονται με το Cloud Computing έχουν σχεδόν διπλασιαστεί και οφείλονται συνήθως σε ηλεκτρονικό ψάρεμα (phishing), λυτρισμικό (ransomware) αλλά και τυχαία διαρροή δεδομένων . Επίσης, υπάρχουν ευπάθειες που σχετίζονται με το Edge Computing όσον αφορά την ασφάλεια του δικτύου και θέματα ιδιωτικότητας (privacy). Επιπλέον, η διάδοση των τεχνολογιών IoT είναι αξιοσημείωτη τα τελευταία χρόνια, υποστηρίζοντας πληθώρα εφαρμογών (έξυπνες πόλεις, υγεία, κατασκευαστικός τομέας, κλπ.). Υπολογίζεται ότι ο αριθμός των συσκευών IoT που θα τεθούν σε λειτουργία έως το 2030 θα φτάσει τα 21.1 δισεκατομμύρια δολάρια, με έσοδα 1.5 τρισεκατομμύρια. Η ετερογενής φύση των συσκευών από άποψη λογισμικού και υλικού, με αρκετές από αυτές να υπόκεινται σε σοβαρούς περιορισμούς (επεξεργαστής, μνήμη, αποθήκευση), δημιουργεί νέες προκλήσεις όσον αφορά την ασφάλεια, το απόρρητο και τη διαχείριση δεδομένων. Σύμφωνα με μία πρόσφατη έρευνα του Eclipse Foundation , η δεύτερη μεγαλύτερη ανησυχία των προγραμματιστών λογισμικού (33%) είναι η ασφάλεια. Επιπλέον, σε ευρωπαϊκό επίπεδο, ο νόμος της ΕΕ για την κυβερνοασφάλεια (EU Cybersecurity Act) και η στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο (EU Cybersecurity Strategy) τονίζουν τη σημασία της κυβερνοασφάλειας για την ενίσχυση της συλλογικής ανθεκτικότητας της Ευρώπης έναντι των απειλών στον κυβερνοχώρο.

Η σύγχρονη πραγματικότητα σχετικά με τον κίνδυνο και τις συνέπειες των κυβερνοεπιθέσεων απαιτεί τον σχεδιασμό και την υλοποίηση συστημάτων για τον εντοπισμό και την προστασία από τέτοιου είδους επιθέσεις. Με βάση και τις απαιτήσεις του συστήματος όπως περιεγράφηκαν στο παραδοτέο Π1.1, η αρχιτεκτονική της μετα-πλατφόρμας του έργου, όσον αφορά την κυβερνοασφάλεια, θα αποτελείται από οντότητες για την εξασφάλιση των παρακάτω ιδιοτήτων: (1) Εμπιστευτικότητα (confidentiality), για την προστασία των δεδομένων έναντι κακόβουλων χρηστών, οι οποίοι δεν έχουν δικαίωμα πρόσβασης σ' αυτά τα δεδομένα, (2) Ακεραιότητα (integrity), χαρακτηριστικό το οποίο δεν επιτρέπει σε ενδιάμεσους, μη εξουσιοδοτημένους χρήστες, να αλλάζουν τα δεδομένα που μεταφέρονται, (3) Αυθεντικοποίηση (authentication), χαρακτηριστικό το οποίο επιτρέπει την εξακρίβωση ότι ένας χρήστης (ή μία εφαρμογή) είναι πράγματι αυτός που ισχυρίζεται ότι είναι, ώστε να του δοθεί πρόσβαση σε συγκεκριμένους πόρους του συστήματος, (4) Εξουσιοδότηση (authorisation), χαρακτηριστικό που ελέγχει εάν ένας χρήστης, μετά το στάδιο της αυθεντικοποίησης, έχει δικαίωμα πρόσβασης σε πόρους του συστήματος, (5) Διαθεσιμότητα (availability), ώστε οι υπηρεσίες σχετικές με την επικοινωνία της πλατφόρμας να είναι διαθέσιμες οποιαδήποτε στιγμή στους εξουσιοδοτημένους χρήστες, (6) Μη αποκήρυξη (non-repudiation), ώστε να διασφαλίζεται ότι ο αποστολέας (ή ο παραλήπτης) ενός μηνύματος μπορεί να αποδείξει ότι δεν έστειλε (ή δεν έλαβε) το συγκεκριμένο μήνυμα, και (7) Εμπρόσθια εμπιστευτικότητα (forward secrecy), έτσι ώστε να διασφαλίζεται η μυστικότητα της επικοινωνίας που πραγματοποιήθηκε στο παρελθόν, σε περίπτωση που υποκλαπεί το μυστικό κλειδί του αποστολέα που χρησιμοποιήθηκε γι' αυτή την επικοινωνία.

Για να καταστούν εφικτά όλα τα παραπάνω, το παρών έργο θα σχεδιάσει και υλοποιήσει τις παρακάτω οντότητες: (1) **Σύστημα διαχείρισης ταυτοτήτων** (identity management system), (2) **Σύστημα αυθεντικοποίησης και εξουσιοδότησης** (authentication and authorisation system).

4.2 Σύστημα διαχείρισης ταυτοτήτων

Η διαχείριση ταυτότητας (identity management) γίνεται συνήθως με τη χρήση αναγνωριστικών (IDs) που εκδίδονται από τρίτα μέρη όπως κυβερνητικούς οργανισμούς, μεγάλες εταιρείες πληροφορικής, κ.τ.λ. Ωστόσο, ορισμένοι απ' αυτούς τους τύπους είναι χρήσιμοι μόνο σε συγκεκριμένα περιβάλλοντα (π.χ. χρήση ηλεκτρονικής αλληλογραφίας από συγκεκριμένο πάροχο), ενώ άλλοι μπορούν να χρησιμοποιηθούν για ευρύτερους σκοπούς (πχ Gmail account), όμως μπορούν να αποκαλύψουν προσωπικά δεδομένα σε τρίτους. Εξίσου σημαντικό είναι ότι βρίσκονται εκτός ελέγχου των χρηστών και είναι επίσης επιρρεπείς σε επιθέσεις κλοπής ταυτότητας με σοβαρές συνέπειες (π.χ. πλαστοπροσωπία με στόχο την πραγματοποίηση κυβερνοεπίθεσης εκ των έσω σε έναν οργανισμό). Είναι επομένως σημαντικό να σχεδιαστεί και να υλοποιηθεί μηχανισμός όπου τα υποκείμενα της ταυτότητας (χρήστες, συσκευές, κλπ.) θα έχουν τον πλήρη έλεγχο της ταυτότητάς τους (αυτοκυριαρχία) και θα μπορούν να αποκαλύπτουν μόνο όσες προσωπικές πληροφορίες είναι απαραίτητες. Είναι επίσης

υψίστης σημασίας, τα υποκείμενα να μπορούν να δημιουργούν πολλαπλές ταυτότητες ή να ανακαλούν άλλες παλαιότερες, ώστε να μειωθούν οι κίνδυνοι παραβίασης της ιδιωτικότητά τους. Ταυτόχρονα, η δυνατότητα πολλαπλών ταυτοτήτων που μπορούν να χρησιμοποιούνται από ένα μόνο υποκείμενο, δεν θα πρέπει να αποτελέσει πλεονέκτημα για κακόβουλους χρήστες με σκοπό την παράκαμψη των μέτρων κυβερνοασφάλειας.

Ο οργανισμός W3C έχει προτείνει τη χρήση αποκεντρωμένων ταυτοτήτων (decentralised identities-DIDs)[29], οι οποίοι έχουν σχεδιαστεί ώστε να δίνεται η δυνατότητα σε μεμονωμένα υποκείμενα (πχ χρήστες) ή οργανισμούς να δημιουργούν τα δικά τους DIDs χρησιμοποιώντας συστήματα που εμπιστεύονται. Η μορφή ενός DID δεν είναι αυστηρά καθορισμένη αλλά εξαρτάται από τις ανάγκες κάθε συστήματος (σχετικές με χαρακτηριστικά ασφάλειας) και τους διαθέσιμους πόρους. Για παράδειγμα, μία απλή μορφή DID είναι η did:key[30], όπου περιέχει το δημόσιο κλειδί (public key) ενός υποκειμένου σε κωδικοποιημένη μορφή, ενώ μία πιο σύνθετη είναι η did:peer[31], όπου το DID μπορεί να περιέχει περισσότερες πληροφορίες, όπως για παράδειγμα ένα (κωδικοποιημένο) αρχείο σε μορφή JSON.

4.3 Σύστημα αυθεντικοποίησης και εξουσιοδότησης

Ο ρόλος του συστήματος αυθεντικοποίησης και εξουσιοδότησης είναι να: 1) αυθεντικοποιεί ένα υποκείμενο με βάση το DID του, και 2) να ελέγχει εάν αυτό το υποκείμενο έχει το δικαίωμα πρόσβασης σε πόρους που αιτείται (πχ δεδομένα) και εάν ναι, να παρέχει πρόσβαση με ασφαλή τρόπο σε αυτούς τους πόρους. Για τον σχεδιασμό αυτού του συστήματος, αρχικά, διακρίνουμε τους εξής ρόλους: 1) Issuer, 2) Verifier, και 3) End User. Ο σκοπός του Issuer είναι να εκδίδει τα διαπιστευτήρια που απαιτούνται για την πρόσβαση σε συγκεκριμένους πόρους. Ο Verifier είναι η οντότητα υπεύθυνη για την επαλήθευση των διαπιστευτηρίων, ενώ ο End User είναι το υποκείμενο, το οποίο αιτείται την δημιουργία διαπιστευτηρίων και την παρουσίασή τους αργότερα στον Verifier, ώστε να αποκτήσουν πρόσβαση σε πόρους του συστήματος.

Στα πλαίσια του έργου αυτού, θα χρησιμοποιηθούν τα Verifiable Credentials (VCs-διαπιστευτήρια που μπορούν να επαληθευθούν), όπως τα προτείνει ο οργανισμός W3C[32]. Κάθε VC εκδίδεται μετά από αίτηση ενός End User και περιλαμβάνει πληροφορίες όπως: 1) πληροφορίες σχετικές με το αντικείμενο του VC, 2) το DID του End User, 3) χρόνο εγκυρότητας του VC, 4) τους πόρους στους οποίους μπορεί να έχει πρόσβαση ο End User, κλπ. Σε περίπτωση πολλαπλών διαπιστευτηρίων για έναν End User, μπορούν να ομαδοποιηθούν σε μία δομή που ονομάζεται Verifiable Presentations (VPs-παρουσιάσεις

[29] https://www.w3.org/TR/did-core
[30] https://w3c-ccg.github.io/did-method-key
[31] https://identity.foundation/peer-did-method-spec/index.html
[32] https://www.w3.org/TR/vc-data-model-2.0

που μπορούν να επαληθευθούν). Σημαντική παραδοχή σε ένα τέτοιο σύστημα είναι ότι οι Verifiers εμπιστεύονται τους Issuers, οι οποίοι συνήθως περιγράφονται μέσω ενός δημόσιου κρυπτογραφικού κλειδιού. Για την προστασία της ακεραιότητας και εμπιστευτικότητας ενός VC (ή VP), θα πρέπει να παρθούν κατάλληλα μέτρα, όπως για παράδειγμα, δημιουργία μίας κρυπτογραφικής απόδειξης (cryptographic proof) που αποτελεί μέρος του VC και μπορεί να επαληθευθεί από τον Issuer. Καθώς συνήθως τα VCs αποτελούν μέρος ενός JSON Web Token (JWTs)[33] ή CBOR Web Token (CWT)[34], μπορούν να χρησιμοποιηθούν οι μορφές JOSE[35] ή COSE[36] αντίστοιχα, οι οποίες δίνουν την δυνατότητα ψηφιακής υπογραφής ή/και κρυπτογράφησης των VCs (VPs).

Αναφορικά με την αρχιτεκτονική που παρουσιάστηκε στην Εικόνα 10, ο End User (τελικός χρήστης) αντιστοιχεί στον συμμετέχοντα (παραγωγό ή καταναλωτή) και ο Issuer (εκδότης) μπορεί να αποτελεί μέρος της Διακυβέρνησης Δεδομένων. Σχετικά με τον Verifier (επικυρωτή), υπάρχουν δύο προσεγγίσεις: 1) είναι κεντρικοποιημένος και αποτελεί μέρος της Διακυβέρνησης Δεδομένων, κάτι το οποίο απλοποιεί την υλοποίηση της μετα-πλατφόρμας του έργου, επηρεάζει όμως αρνητικά την ιδιωτικότητα καθώς ο Verifier θα γνωρίζει ποιος End User ζητά πρόσβαση σε ποιους πόρους και πότε, και 2) κάθε πάροχος καθετοποιημένης λύσης να διαθέτει τον δικό του Verifier, κάτι το οποίο ενισχύει την ιδιωτικότητα, αυξάνει όμως την πολυπλοκότητα της υλοποίησης.

Σημαντικό ζήτημα επίσης αποτελεί, στην περίπτωση κρυπτογραφημένων VCs, η γνωστοποίηση στον Verifier του συμμετρικού κλειδιού κρυπτογράφησης που χρησιμοποίηση ο Issuer ώστε να μπορέσει να τα αποκρυπτογραφήσει και έτσι να προσπαθήσει να τα επαληθεύσει. Μία προσέγγιση είναι το JWT (CWT) να περιέχει επίσης: 1) κρυπτογραφημένο αυτό το κλειδί χρησιμοποιώντας έναν Key Wrap Algorithm (KWA)[37], 2) μία αναφορά στο συμμετρικό κλειδί (πχ key id: 4) που χρησιμοποιήθηκε από τον KWA, υποθέτοντας ότι αυτό το κλειδί διανεμήθηκε στον Verifier μέσω ενός μηχανισμού που προηγήθηκε. Έτσι ο Verifier, με βάση την αναφορά στο κλειδί του KWA, θα αναζητήσει το κλειδί αυτό στη βάση δεδομένων του, θα το χρησιμοποιήσει έπειτα για να αποκρυπτογραφήσει το συμμετρικό κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση (μέρους) του JWT (CWT) και έπειτα θα προχωρήσει με την αποκρυπτογράφησή του. Οι μορφές δεδομένων JOSE και COSE αποτελούνται από τμήματα τα οποία κάποια είναι κρυπτογραφημένα (πχ κλειδί για την αποκρυπτογράφηση του JWT) και κάποια άλλα όχι (πχ KWA key id). Τα κρίσιμα μη κρυπτογραφημένα τμήματα θα πρέπει να προστατεύονται έναντι επιθέσεων ακεραιότητας χρησιμοποιώντας κατάλληλο αλγόριθμο

[33] https://datatracker.ietf.org/doc/html/rfc7519

[34] https://datatracker.ietf.org/doc/html/rfc8392

[35] https://datatracker.ietf.org/wg/jose/documents

[36] https://datatracker.ietf.org/doc/html/rfc8152

[37] https://www.ietf.org/rfc/rfc3394.txt

κρυπτογράφησης με πρόσθετα δεδομένα (authenticated encryption algorithm with additional data), όπως για παράδειγμα τον AES-CCM[38].

Καθώς μπορούν να υπάρξουν διαφορετικά είδη VCs που να απαιτούν τη χρήση διαφορετικών για παράδειγμα αλγορίθμων κρυπτογράφησης, ψηφιακής υπογραφής, διαχείρισης των κρυπτογραφικών κλειδιών, κλπ., απαιτείται η χρήση μετα-δεδομένων πριν την δημιουργία ενός VC (και κατ' επέκταση JWT/CWT) όπου ο End User και ο Verifier γνωστοποιούν ο ένας στον άλλο τις λεπτομέρειες αυτές. Μία προσέγγιση που θα μπορούσε να ακολουθηθεί είναι η χρήση μηνυμάτων Credential Offer, Authorization Request και Authorization Response, χρησιμοποιώντας τα πρωτόκολλα OAuth2 και OpenId[39].

[38] https://datatracker.ietf.org/doc/html/rfc6655

[39] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

Σύνοψη

Αυτό το παραδοτέο, Π1.2, αναλύει την μεθοδολογία που ακολουθείται για το σχεδιασμό της αρχιτεκτονικής της μετα-πλατφόρμας διασυνδεδεμένων έξυπνων πόλεων, παρουσιάζει την αρχιτεκτονική της πλατφόρμας σε υψηλό επίπεδο και την αρχιτεκτονική της πλατφόρμας όσον αφορά την κυβερνοασφάλεια.

Η ανάπτυξη της αρχιτεκτονικής έγινε με οδηγό τις τελικές απαιτήσεις της πλατφόρμας (Παραδοτέο Π1.1). Η αρχιτεκτονική που αναπτύχθηκε βασίστηκε στην προσέγγιση των Χώρων Δεδομένων. Κατά την ανάπτυξη αυτής της αρχιτεκτονικής μελετήθηκαν διάφορες καθιερωμένες αρχιτεκτονικές λύσεις από ποικίλα έργα έξυπνων πόλεων.

Στο παραδοτέο Π1.2 παρουσιάζεται η υψηλού επιπέδου αρχιτεκτονική της μετα-πλατφόρμας. Στην αρχιτεκτονική αυτή περιλαμβάνονται στοιχεία/υποσυστήματα τα οποία ανήκουν εγγενώς στην μετα-πλατφόρμα καθώς και στοιχεία/υποσυστήματα που αλληλοεπιδρούν με αυτήν. Η πλατφόρμα περιλαμβάνει δύο κατηγορίες υπηρεσιών: (α) Υπηρεσίες Διακυβέρνησης Δεδομένων και (β) Υπηρεσίες Αξίας Δεδομένων. Η ανταλλαγή δεδομένων μεταξύ των συμμετεχόντων πραγματοποιείται μέσω του στοιχείου Connector, το οποίο, βάσει του αρχιτεκτονικού μοντέλου IDS-RAM, λειτουργεί ως διαμεσολαβητής που διασφαλίζει τη διαλειτουργικότητα και την εμπιστοσύνη.

Με βάση τις απαιτήσεις του συστήματος, όπως περιγράφονται στο παραδοτέο Π1.1, η αρχιτεκτονική του συστήματος όσον αφορά την κυβερνοασφάλεια περιέχει, και θα υλοποιηθούν στο πλαίσιο του έργου, 2 οντότητες: Ένα σύστημα διαχείρισης ταυτοτήτων και ένα σύστημα αυθεντικοποίησης και εξουσιοδότησης/πιστοποιήσης.

Αναφορές

[1] B. Otto, M. ten Hompel, and S. Wrobel, “International Data Spaces,” in Digital Transformation, 2019.

[2] Industrial Internet Consortium, “Industrial Internet Reference Architecture,” Tech. Rep., 2015.

[3] K. Schweichhart, “Reference Architectural Model Industrie 4.0 (RAMI 4.0) - An Introduction,” Plattf. Ind. 4.0, vol. 0, 2016.

[4] M. Franklin, A. Halevy, and D. Maier, “From databases to dataspaces: A new abstraction for information management,” SIGMOD Rec., vol. 34, no. 4, 2005.

[5] A. Braud, G. Fromentoux, B. Radier, and O. Le Grand, “The Road to European Digital Sovereignty with Gaia-X and IDSA,” IEEE Network, vol. 35, no. 2. 2021.