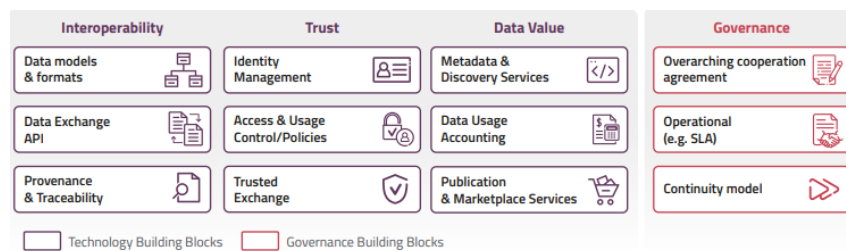


## Περιβάλλον πειραματισμού με Data-Spaces με χρήση FIWARE και i4Trust

### Περιγραφή

Σκοπός της παρούσας διπλωματικής είναι να εξετάσει τη χρήση των τεχνολογικών δομικών στοιχείων των Χώρων Δεδομένων (Data Spaces). Ο όρος “Χώροι Δεδομένων” αναφέρεται σε ένα πλαίσιο για κοινή χρήση, διαχείριση και πρόσβαση σε δεδομένα από διαφορετικούς οργανισμούς ή συστήματα, διατηρώντας παράλληλα τον έλεγχο, την ασφάλεια και τη διακυβέρνηση των δεδομένων<sup>1</sup>. Οι “Χώροι Δεδομένων” επιτρέπουν τη συνεργασία και την ανταλλαγή δεδομένων για χρήση στην οικονομία και στην κοινωνία, **χωρίς** να απαιτείται η **κεντρική αποθήκευσή** τους, ενισχύοντας τη διαλειτουργικότητα και την εμπιστοσύνη μεταξύ των συμμετεχόντων. Βασική προϋπόθεση λειτουργίας τους είναι η ψηφιακή κυριαρχία. Η ψηφιακή κυριαρχία υλοποιείται από ένα σύνολο μηχανισμών που εξασφαλίζουν τον έλεγχο πρόσβασης σε επίπεδο ατομικών δεδομένων. Η ψηφιακή κυριαρχία είναι εξαιρετικά σημαντική σε συνεργαζόμενες συλλογές δεδομένων (όταν δεν υπάρχει μία οντότητα που έχει μοναδικό έλεγχο σε όλα τα δεδομένα). Μια τυπική αναπαράσταση των λειτουργιών φαίνεται στην παρακάτω εικόνα:



Εικόνα 1 Για τη λειτουργία των χώρων δεδομένων τα τεχνολογικά στοιχεία είναι απαραίτητα ενώ τα στοιχεία πολιτικής είναι σημαντικά για την πολιτική της χρήσης τους.

Ο/Η υποψήφιος θα εργαστεί με δύο σύνολα δεδομένων (datasets): α) ζήτησης ενέργειας από νοικοκυριά<sup>2</sup> και περιβαλλοντικά (πραγματικού χρόνου) από τον μετεωρολογικό σταθμό ΕΜΠ<sup>3</sup>. Σε πρώτη φάση θα εγκατασταθεί μια πλατφόρμα ανταλλαγής δεδομένων τύπου FIWARE<sup>4</sup>. Ο/Η υποψήφιος θα χρησιμοποιήσει smart-data models<sup>5</sup> π.χ. κάποιο για την Ενέργεια<sup>6</sup> που αξιοποιεί το σχήμα JSON-LD<sup>7</sup> συμβατό με το πρότυπο NGSIn2/NGSI-LD του ETSI<sup>8,9</sup> και έτοιμα docker images<sup>10</sup> σύμφωνα με οδηγίες από το postman<sup>11,12</sup>. Για τη δημιουργία DataSpaces θα χρησιμοποιηθεί ο συνδυασμός FIWARE με το Fiware Data space Connector<sup>13</sup> και i4Trust<sup>14,15</sup> ώστε να εγκατασταθούν και ρυθμισθούν λειτουργίες και να επιδειχθεί ένας τυπικός κύκλος εκχώρησης πρόσβασης. Συγκεκριμένα, θα δημιουργηθεί ένας οργανισμός στην περιοχή Industrial Area (Energy & Environment) για τη διαχείριση δεδομένων νοικοκυριών ή μιας επιχείρησης και ενός περιβαλλοντικού σταθμού με τις κάτωθι λειτουργίες χρήσης:

- Εισαγωγή/Δημιουργία ενός οργανισμού στο χώρο των δεδομένων (distributed data space authority)
- Καταχώρηση καταναλωτή δεδομένων

<sup>1</sup> <https://gaia-x.eu/what-is-gaia-x/>

<sup>2</sup> <https://github.com/sathanasoulias/Plegma-Dataset>

<sup>3</sup> <https://openmeteo.org/stations/1334/>

<sup>4</sup> <https://www.fiware.org/about-us/>

<sup>5</sup> <https://github.com/smart-data-models>

<sup>6</sup> <https://github.com/smart-data-models/SmartEnergy>

<sup>7</sup> <https://fiware-datamodels.readthedocs.io/en/stable/index.html>

<sup>8</sup> <https://github.com/FIWARE/tutorials.NGSI-LD/blob/master/docs/understanding-@context.md>

<sup>9</sup> <https://forge.etsi.org/rep/cim/NGSI-LD>

<sup>10</sup> <https://github.com/FIWARE/tutorials.Linked-Data>

<sup>11</sup> <https://www.postman.com/fiware/fiware-foundation-ev-s-public-workspace/overview>

<sup>12</sup> <https://www.postman.com/fiware/fiware-foundation-ev-s-public-workspace/documentation/x1yijss/ngsi-lid-linked-data>

<sup>13</sup> <https://github.com/FIWARE/data-space-connector>

<sup>14</sup> <https://github.com/i4Trust/building-blocks>

<sup>15</sup> <https://github.com/i4Trust/training>

- Διαχείριση πρόσβασης (contract management)
- Αλληλεπίδραση υπηρεσιών Human-To-Machine (H2M), Machine-To-Machine (M2M)

Ο έλεγχος πρόσβασης και οι πολιτικές χρήσης είναι τα δύο κύρια θέματα που θα επιδειχθούν στη διπλωματική για να επιβεβαιωθεί η ψηφιακή κυριαρχία των παραγωγών των δεδομένων με χρήση πολιτικών πρόσβασης ως μέρος των όρων και προϋποθέσεων που καθορίζονται κατά τη δημοσίευση δεδομένων. Ένας διακομιστής μεσολάβησης (gateway-API) παίζει το ρόλο του Σημείου Επιβολής Πολιτικής (PEP) και απαιτεί ένα πρόσθετο Policy Decision Point (PDP). Το PDP παρέχει έναν μηχανισμό συμβατότητας για τη χρήση του τελικού σημείου ανάθεσης iShare<sup>16</sup> ως πηγή αξιόπιστων εκδοτών διαπιστευτηρίων. Επιπλέον, το τελικό σημείο ανάθεσης iShare χρησιμοποιείται για την αξιολόγηση των πραγματικών πολιτικών που αναφέρονται από τους ρόλους στα ληφθέντα διαπιστευτήρια.

Ο έλεγχος πρόσβασης δεν μπορεί να συμβεί εάν δεν υπάρχουν ταυτότητες χρηστών. Προς αυτή την κατεύθυνση θα εγκατασταθεί το δομικό στοιχείο Keyrock<sup>17</sup> το οποίο υλοποιεί τον μηχανισμό OAuth που παράγει token για την ελεγχόμενη πρόσβαση<sup>18</sup> σε δεδομένα ή εφαρμογές<sup>19</sup>). Το iSHARE προτείνει<sup>20</sup> ένα μηχανισμό που επιτρέπει στους οργανισμούς να παρέχουν ο ένας στον άλλο πρόσβαση στα δεδομένα τους μέσω συμφωνιών που βελτιώνουν τις συνθήκες για την ανταλλαγή δεδομένων. Το iSHARE χρησιμοποιεί υπογεγραμμένα JSON Web Tokens για την προστασία της ακεραιότητας του περιεχομένου του μηνύματος. Κάθε μέρος μιας συμφωνίας με iSHARE επικυρώνει τις υπογραφές και ερμηνεύει το περιεχόμενο των JWT. Μια τρίτη έμπιστη οντότητα (iSHARE Satellite) διατηρεί τη σωστή λειτουργία του οικοσυστήματος του δικτύου συμμετεχόντων του.

Οι βιβλιοθήκες που θα χρησιμοποιηθούν είναι επέκταση του Kong API-Gateway<sup>21</sup> που έχει ήδη υλοποιηθεί από το FIWARE. Το DSBA-PDP<sup>22</sup>, που χρησιμοποιεί το EBSI Trusted Issuers Registry API<sup>23</sup> για να αξιολογήσει εάν επιτρέπεται σε έναν εκδότη να εκδώσει ορισμένα διαπιστευτήρια, μπορεί να ενσωματωθεί στη ροή<sup>24</sup> με το PEP. Επιπλέον, το Keyrock εφαρμόζει επίσης τις τυπικές λειτουργίες XACML<sup>25</sup> Point Administration Policy (PAP) και Policy Management Point (PMP). Για τον καθορισμό πολιτικών πρόσβασης, το iSHARE φέρνει το μοντέλο δεδομένων αποδεικτικών εκχώρησης<sup>26</sup> (delegation evidence model) που είναι δομημένα σύμφωνα με μια μετάφραση σε JSON του προτύπου XACML.

Ένα ελάχιστο λειτουργικό πορτοφόλι για την αποθήκευση των διαπιστευτηρίων παρέχεται από το VCWallet<sup>27</sup>.

## Υποστήριξη

Η διπλωματική υποστηρίζεται από το Pleiades innovation hub και θα χρηματοδοτηθεί με έπαθλο ολοκλήρωσης για την επιβεβαίωση κατανομής πρόσβασης από δύο υποθετικούς διαφορετικούς οργανισμούς.

Επικοινωνία: Ε. Συκάς (sykas@cn.ntua.gr), Δ. Καλογεράς ([dkalo@noc.ntua.gr](mailto:dkalo@noc.ntua.gr), τηλ. 210-7721863). Η διπλωματική μπορεί να υλοποιηθεί από δύο υποψηφίους

<sup>16</sup> <https://dev.ishare.eu/authorisation-registry-role/delegation-endpoint>

<sup>17</sup> [https://github.com/ging/fiware-idm/blob/master/doc/getting\\_started.md](https://github.com/ging/fiware-idm/blob/master/doc/getting_started.md)

<sup>18</sup> <https://www.postman.com/fiware/fiware-foundation-ev-s-public-workspace/folder/byc06ib/securing-the-orion-context-broker>

<sup>19</sup> <https://www.postman.com/fiware/workspace~b6e7fcf4-ff0c-47cb-ada4-e222ddee5ac/request/Otu51y7/keyrock-obtain-roles-and-domain>

<sup>20</sup> <https://ishareworks.atlassian.net/wiki/spaces/IS/overview>

<sup>21</sup> <https://github.com/Kong/kong>

<sup>22</sup> <https://github.com/FIWARE/dsba-pdp>

<sup>23</sup> <https://hub.ebsi.eu/apis/pilot/trusted-issuers-registry/v5>

<sup>24</sup> <https://github.com/FIWARE/kong-plugins-fiware>

<sup>25</sup> <https://en.wikipedia.org/wiki/XACML>

<sup>26</sup> <https://dev.ishare.eu/reference/delegation-evidence>

<sup>27</sup> <https://github.com/FIWARE/VCWallet>