# ΓΕΩΠΟΝΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών Γενικού Τμήματος

Κατεύθυνση: ΓΕΩΠΛΗΡΟΦΟΡΙΚΗ


## Μεταπτυχιακή Διπλωματική Εργασία

**ΑΣΦΑΛΗΣ ΚΑΙ ΦΙΛΙΚΗ ΣΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ ΔΙΑΛΕΙΤΟΥΡΓΙΚΗ ΠΛΑΤΦΟΡΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑ ΠΑΝΕΥΡΩΠΑΪΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ - ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ**


ΣΤΕΡΓΙΟΣ Γ. ΤΣΙΑΦΟΥΛΗΣ

Επιβλέπων: Αλέξανδρος Β. Σιδερίδης, Καθηγητής



Αθήνα, 2013

# Μεταπτυχιακή Διπλωματική Εργασία

## ΑΣΦΑΛΗΣ ΚΑΙ ΦΙΛΙΚΗ ΣΤΗΝ ΙΔΙΩΤΙΚΟΤΗΤΑ ΔΙΑΛΕΙΤΟΥΡΓΙΚΗ ΠΛΑΤΦΟΡΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΤΑΥΤΟΠΟΙΗΣΗΣ ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΚΑΙ ΛΕΙΤΟΥΡΓΙΑ ΠΑΝΕΥΡΩΠΑΪΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ - ΕΙΔΙΚΑ ΖΗΤΗΜΑΤΑ

ΣΤΕΡΓΙΟΣ Γ. ΤΣΙΑΦΟΥΛΗΣ

Επιβλέπων: Αλέξανδρος Β. Σιδερίδης, Καθηγητής

Μέλη ΕΚ: Κ.Γιαλούρης, Αναπληρωτής Καθηγητής, Κ.Κωστοπούλου, Αναπληρώτρια Καθηγήτρια

# Περίληψη

Τον Μάρτιο του 2000 κατά την σύνοδο κορυφής της Λισαβόνας, οι ηγέτες των κυβερνήσεων της Ευρωπαϊκής Ένωσης (ΕΕ) έθεσαν σαν στόχο την οικονομική ανάπτυξη της οικονομίας της ΕΕ καθώς και την αύξηση και την βελτίωση των θέσεων εργασίας. Η χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην δημόσια διοίκηση του εκάστοτε κράτους μέλους της ΕΕ καθώς και η διασυνοριακή συνεργασία των κρατών μελών σε επίπεδο δημοσίας διοίκησης αλλά και η παροχή υπηρεσιών διευρωπαϊκής ηλεκτρονικής διακυβέρνησης σε πολίτες και επιχειρήσεις, θα συντελέσουν στην επίτευξη του στόχου αυτού.

Στην παρούσα διπλωματική εργασία γίνεται αναφορά στις έννοιες της ηλεκτρονικής διακυβέρνησης, στις βασικότερες υπηρεσίες που προσφέρονται σε ένα περιβάλλον ηλεκτρονικής διακυβέρνησης καθώς και μια ιστορική ανάδρομη στην εξέλιξη των υπηρεσιών αυτών. Ακόμη, εξετάζονται οι λειτουργικές απαιτήσεις για την παροχή υπηρεσιών από το κράτος προς τους πολίτες και τις επιχειρήσεις σε πανευρωπαϊκό επίπεδο ενώ παρουσιάζονται και οι πολιτικές της ΕΕ για την προώθηση τους. Αναφέρονται και αναλύονται επιγραμματικά τα μεγάλης κλίμακας προγράμματα τα οποία συγχρηματοδοτήθηκαν από την ΕΕ για την υλοποίηση και υποστήριξη των διασυνοριακών αυτών υπηρεσιών σε περιβάλλοντα πραγματικής λειτουργίας.

Αναπτύσσονται επίσης τα Ευρωπαϊκά πληροφοριακά συστήματα που σχετίζονται με την ελεύθερη μετακίνηση των πολιτών και την επίτευξη της ενιαίας αγοράς στο χώρο της Ευρώπης όπως το Schengen, VIS, CIS, IMI. Ακόμη περιγράφεται η λειτουργία του μεγάλης κλίμακας πιλοτικό πρόγραμμα STORK το οποίο υλοποίησε και εγκατέστησε μια πλατφόρμα διαλειτουργικότητας για την διασυνοριακή ηλεκτρονική ταυτοποίηση και την παροχή διασυνοριακών υπηρεσιών προς τους πολίτες και τις επιχειρήσεις.

**Λέξεις κλειδιά**: Ηλεκτρονική Διακυβέρνηση, Διαλειτουργικότητα, Ηλεκτρονική Ταυτοποίηση, Διασυνοριακές Υπηρεσίες. Μεγάλης Κλίμακας Πιλοτικά Προγράμματα (LSPs), Schengen, STORK, Ιδιωτικότητα.

# ABSTRACT

In March 2000 at the Lisbon Summit, the leaders of the governments of the European Union set the objective of economic development of the EU economy and the growth with better jobs. The use of Information Technology and Communications (ICT) in the public administration of the Member States of EU and cross-border cooperation at the level of public administration and also the provision of Pan-European eGovernment services to citizens and businesses would help achieve the objective.

This thesis refers to the concepts of electronic governance in basic services offered in an environment of e-government and a historic overview of these services. Also, it examines the functional requirements for the provision of services from government to citizens and businesses across Europe and presents the EU policies that were introduced in order to promote those. The large-scale projects co-financed by the EU that aimed to implement and support cross-border services in real life environments are listed and briefly analyzed.

Also concentrates to the European information systems that are related to the free movement of citizens and the single market act in the space of Europe, such as Schengen, VIS, CIS, and IMI. Furthermore, it also describes the operation of large scale pilot STORK which developed and established an interoperability platform for cross-border e-identification and cross-border services for citizens and businesses.



**Key words**: eGovernment, Interoperability, Electronic Authentication, cross-border services. Large scale pilot schemes (LSPs), Schengen, STORK, Privacy.

# Ευχαριστίες

Η παρούσα Μεταπτυχιακή Διπλωματική Εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος του Γενικού Τμήματος του Γεωπονικού Πανεπιστημίου Αθηνών.

Θα ήθελα να εκφράσω την βαθιά ευγνωμοσύνη μου και την εκτίμηση μου στον Καθηγητή Σιδερίδη Αλέξανδρο, ο οποίος μου έδωσε την δυνατότητα να αναλάβω την εργασία αυτή. Επίσης θα ήθελα να τον ευχαριστήσω για την εμπιστοσύνη που έδειξε στο πρόσωπο μου, την υπομονή του και την ουσιαστική βοήθεια του κατά την εκπόνηση της.

Ευχαριστώ τα μέλη της επιτροπής κρίσης Αναπληρωτή Καθηγητή Γιαλούρη Κωνσταντίνο και Επίκουρη Καθηγήτρια Κωστοπούλου Κωνσταντίνα για το ενδιαφέρον τους και τις εύστοχες υποδείξεις τους.

Ιδιαίτερα θα ήθελα να καταθέσω την ευγνωμοσύνη μου στον Δρα Βασίλειο Ζορκάδη για την καθοδήγηση του και την αμέριστη υποστήριξη του καθ’ όλη την διάρκεια του Μεταπτυχιακού Προγράμματος και ειδικότερα κατά την εκπόνηση της διπλωματικής μου εργασίας.

Ιδιαίτερες ευχαριστίες στην οικογένεια μου η οποία μου στάθηκε όλο αυτό το χρονικό διάστημα.

# Περιεχόμενα

# Κατάλογος Σχημάτων

# Κατάλογος Πινάκων

# Συντομογραφίες

## Λατινικές

| | |
|---|---|
| AP | Attribute Provider |
| CIP | Competitiveness and Innovation Framework Programme |
| CIS | Customs Information System |
| Cot | Circle of Trust |
| EId | Electronic Identification |
| EIS | European Interoperability Strategy |
| EIG | European Interoperability Guidelines |
| EIP | Entrepreneurship and Innovation Programme |
| EIF | European Interoperability Framework |
| EPO | European procedure for Payment Order |
| e-CODEX | Communication via Online Data Exchange |
| EpSOS | European Patients Smart Open Services |
| EHIC | European Health Insurance Card |
| IDA | interchange data between Administrations |
| IDABC | Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens |
| IdP | Identity Provideer |
| IEEP | Intelligent Energy-Europe Programme |
| ICT PSP | Information and Communication Technologies Policy Support Programme |
| IT | transport infrastructure |
| IMI | Internal Market Information System |

| | |
|---|---|
| ISO | International Organization for Standardization |
| HTTP | Hypertext Transfer Protocol |
| MW | Middleware |
| MDSSO | multi-domain SSO |
| NPS | National Proxy Servers |
| NP | National Portals |
| NIMIC | National IMI Coordinator |
| OCSP | Online Certificate Status Protocol |
| *OCSP* | Online Certificate Status Protocol |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PEPS | Pan European Proxy Service |
| PEPPOL | Pan-European Public Procurement Online |
| POM | Project Object Model |
| PSC | Points of Single Contact |
| QAA | Quality of Authentication Assurance |
| LSP | Large Scale Pilot project |
| SPOCS | Simple Procedures Online for Cross- Border Services |
| STORK | Secure idenTity acrOss boRders linked |
| SIS | Schengen information system |
| SEMIC | Semantic Interoperability Community |
| SSO | Single Sign On |
| SAML | Secure Assertion Markup Language |

| | |
|---|---|
| SD | Service Directive |
| SIRENE | Supplementary Information REquest at the National Entries |
| SOAP | Simple Object Access Protocol |
| TAN | Transaction Authentication Number |
| VIS | Visa Information System |
| XML | Extensible Mark-up Language |

## Ελληνικές

| | |
|---|---|
| ΕΕ | Ευρωπαϊκή Ένωση |
| ΕΙΦ | Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας |
| ΕΚΕ | Ενιαία Κέντρα Εξυπηρέτησης |
| ΗΔ | Ηλεκτρονική Διακυβέρνηση |
| ΗΤ | Ηλεκτρονική Ταυτοποίηση |
| ΤΠΕ | Τεχνολογίες Πληροφορικής και Επικοινωνιών |

# ΕΙΣΑΓΩΓΗ

Τον Μάρτιο του 2000, κατά την σύνοδο κορυφής της Λισαβόνας, οι ηγέτες των κυβερνήσεων της Ευρωπαϊκής Ένωσης (ΕΕ) έθεσαν σαν στόχο την οικονομική ανάπτυξη της οικονομίας της ΕΕ καθώς και την αύξηση και την βελτίωση των θέσεων εργασίας οδηγώντας στην βελτίωση της ποιότητας ζωής των πολιτών και σε μεγαλύτερη κοινωνική συνοχή. Η χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην δημόσια διοίκηση έκαστου κράτους μέλους της ΕΕ, καθώς και η διασυνοριακή συνεργασία των κρατών μελών σε επίπεδο δημοσίας διοίκησης, αλλά και η παροχή υπηρεσιών διευρωπαϊκής ηλεκτρονικής διακυβέρνησης σε πολίτες και επιχειρήσεις, θα συντελέσουν στην επίτευξη του στόχου αυτού

Στην παρούσα διπλωματική εργασία γίνεται αναφορά στις έννοιες της ηλεκτρονικής διακυβέρνησης, στις βασικότερες υπηρεσίες που προσφέρονται σε ένα περιβάλλον ηλεκτρονικής διακυβέρνησης καθώς και μια ιστορική ανάδρομη στην εξέλιξη των υπηρεσιών αυτών. Ακόμη, εξετάζονται οι λειτουργικές απαιτήσεις για την παροχή υπηρεσιών από το κράτος προς τους πολίτες και τις επιχειρήσεις και αναπτύσσονται έννοιες των αρχών της διαλειτουργικότητας μεταξύ των συστημάτων των συμμετεχόντων μερών για την παροχή κυβερνητικών υπηρεσιών σε πανευρωπαϊκό επίπεδο. Επίσης, παρουσιάζονται οι πολιτικές της ΕΕ για την προώθηση των κυβερνητικών ηλεκτρονικών υπηρεσιών με την υποστήριξη των ΤΠΕ. Σχετικά μεγάλης κλίμακας προγράμματα τα οποία συγχρηματοδοτήθηκαν από την ΕΕ και σκοπός τους ήταν να υλοποιήσουν πιλοτικά, σε περιβάλλον πραγματικής λειτουργίας, συναφείς υπηρεσίες αναφέρονται και αναλύονται επιγραμματικά. Τα προγράμματα αυτά σχετίζονται κυρίως με την υποστήριξη των μικρομεσαίων επιχειρήσεων αλλά και τη βελτίωση του βιοτικού επίπεδου των πολιτών γενικότερα.

Εκτός των μεγάλης κλίμακας πιλοτικών προγραμμάτων για την παροχή ηλεκτρονικών υπηρεσιών με την χρήση των ΤΠΕ, παρουσιάζεται μια σύντομη ανάλυση ως προς την λειτουργία των βασικότερων ευρωπαϊκών πληροφοριακών συστημάτων. Τα συστήματα αυτά σχετίζονται με την ελεύθερη μετακίνηση των πολιτών και την επίτευξη της Ενιαίας Αγοράς στο χώρο της Ευρώπης και, συνεπώς, έχουν άμεση συνάφεια με την Ηλεκτρονική Ταυτοποίηση (ΗΤ). Ειδικότερα γίνεται μια ιστορική αναδρομή στην καθιέρωση του χώρου Schengen για την ελεύθερη μετακίνηση πολιτών και διακίνησης αγαθών.

Σε συνέχεια των ανωτέρω περιγράφουμε την πορεία της εξέλιξης του πληροφοριακού συστήματος ελέγχου του χώρου της ΕΕ, μέσω του οποίου επικοινωνούν οι δικαστικές και αστυνομικές αρχές των κρατών μελών του χώρου Schengen ανταλλάσοντας πληροφορίες για άτομα στα οποία εκκρεμούν δικαστικά εντάλματα, για άτομα τα έχουν δηλωθεί ως «εξαφανισμένα» καθώς και για κλεμμένα οχήματα. Μέσα στους στόχους του πληροφοριακού αυτού συστήματος είναι και η ενίσχυση των εξωτερικών συνόρων του χώρου Schengen καθώς και η αποτροπή εισόδου στον χώρο επικίνδυνων ουσιών και φορτίων (ναρκωτικά, πυρομαχικά, όπλα).

Ένα ακόμη πληροφοριακό σύστημα στο οποίο αναλύθηκε συνοπτικά ως προς την λειτουργία του, είναι το Πληροφοριακό Σύστημα Ελέγχου Θεωρήσεων VIS (Visa Information System) το όποιο συμβάλλει στην επίτευξη κοινής πολίτικης θεωρήσεων βίζας και στον έλεγχο της εισόδου ανεπιθύμητων ή επικίνδυνων ατόμων στο χώρο της ΕΕ από τρίτες χώρες. Στο ίδιο κεφάλαιο έγινε αναφορά στο πληροφοριακό σύστημα που υποστηρίζει τα ηλεκτρονικά τελωνεία CIS (Customs Information Systems) το όποιο είναι και αυτό ένα πληροφοριακό σύστημα το οποίο αποσκοπεί στην διευκόλυνση της κυκλοφορίας των εμπορευμάτων εντός και εκτός της εσωτερικής αγοράς και στην βελτίωση της ασφάλειας των πολιτών της ΕΕ.

Σε ιδιαίτερο κεφάλαιο περιγράφηκε η λειτουργία του μεγάλης κλίμακας πιλοτικό πρόγραμμα STORK (Secure idenTity acrOss boRders linKed) το οποίο υλοποίησε και εγκατέστησε μια πλατφόρμα διαλειτουργικότητας για την παροχή διασυνοριακών υπηρεσιών προς τους πολίτες και τις επιχειρήσεις. Η χρήση της κλίμακας QAA (Quality

of Authentication Assurance) για την διασφάλιση της αξιοπιστίας της αυθεντικοποίησης καθώς και η προστασία της ιδιωτικότητας της προτεινόμενης πλατφόρμας αυθεντικοποίησης αποτελούν σημαντικά ζητήματα και αναπτύχθηκαν σε ξεχωριστές ενότητες αυτού του κεφαλαίου.

Τέλος, στο τελευταίο κεφάλαιο της διπλωματικής εργασίας αναλύονται τα συμπεράσματα που προκύπτουν από την ενασχόλησή μου με τα θέματα της παροχής ηλεκτρονικών υπηρεσιών σε Ευρωπαϊκό επίπεδο στο πλαίσιο της Μεταπτυχιακής αυτής διατριβής. Στο κεφάλαιο αυτό, παρατίθεται επίσης και η προσωπική μου κριτική για τα Έργα αυτά και ειδικότερα για το Έργο STORK, μέσα από την εμπειρία που έχω αποκομίσει με την συμμετοχή μου στο Ευρωπαϊκό Έργο Μεγάλης Κλίμακας STORK 2.0, το οποίο αποτελεί την συνέχεια του Έργου STORK.

# Κεφάλαιο 1: Εισαγωγικές έννοιες Ηλεκτρονικής Διακυβέρνησης

## 1.1 Ηλεκτρονική Διακυβέρνηση

Τον Μάρτιο του 2000, κατά την σύνοδο κορυφής της Λισαβόνας, οι ηγέτες των κυβερνήσεων της Ευρωπαϊκής Ένωσης (ΕΕ) έθεσαν σαν στρατηγικό στόχο να αναδειχτεί η ΕΕ στην «στην πιο ανταγωνιστική και δυναμική, βασισμένη στη γνώση οικονομία στον κόσμο, ικανή για αειφόρο οικονομική ανάπτυξη με περισσότερες και καλύτερες θέσεις εργασίας και μεγαλύτερη κοινωνική συνοχή». Για να επιτευχθούν οι στόχοι της στρατηγικής αυτής της ΕΕ, η οποία ονομάστηκε «Στρατηγική της Λισαβόνας», θα έπρεπε να ληφθούν κατάλληλες δράσεις και πολιτικές σε διάφορους τομείς όπως αυτών της ενιαίας εσωτερικής αγοράς, της κοινωνίας της πληροφορίας, της έρευνας, της εκπαίδευσης αλλά και σε διαθρωτικές οικονομικές μεταρρυθμίσεις και οικονομικών πολιτικών που θα ευνοούσαν την αειφόρο οικονομική ανάπτυξη και θα δημιουργούσαν νέες θέσεις εργασίας. Οι περισσότεροι από αυτούς τους τομείς βρίσκονται σε αλληλεξάρτηση καθώς για παράδειγμα τα βιώσιμα οικονομικά βοηθούν στην ανάπτυξη και κατά συνέπεια στην δημιουργία νέων θέσεων εργασίας. Επίσης, η χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) στην δημόσια διοίκηση του έκαστου κράτους μέλους της ΕΕ καθώς και η διασυνοριακή συνεργασία των κρατών μελών σε επίπεδο δημοσίας διοίκησης αλλά και η παροχή υπηρεσιών διευρωπαϊκής ηλεκτρονικής διακυβέρνησης σε πολίτες και επιχειρήσεις, θα εξοικονομήσουν κεφάλαια στην ΕΕ ενώ θα δημιουργήσουν παράλληλα νέες θέσεις εργασίας.

Στην ΕΕ η Ηλεκτρονική Διακυβέρνηση (ΗΔ) (e-Government) ορίζεται ως η χρήση των εργαλείων και των συστημάτων που παρέχονται από τις ΤΠΕ με στόχο την βελτίωση των παρεχόμενων υπηρεσιών προς τους πολίτες και τις επιχειρήσεις [15].

Μία αποτελεσματική ΗΔ μπορεί να αποφέρει μεγάλα οφέλη στις κυβερνήσεις αλλά και στις επιχειρήσεις όπως η βελτίωση της αποδοτικότητας, η εξοικονόμηση χρημάτων, η

αύξηση της διαφάνειας και η συμμετοχικότητα των πολιτών στην διοίκηση του κράτους.

Ακόμη, μέσα από την ΗΔ μπορεί να επιτευχτεί ο στόχος της ψηφιακής ενιαίας αγοράς, όπου οι πολίτες όλων των χωρών της ΕΕ θα μπορούν να μετακινούνται ελεύθερα είτε για εργασία είτε για προσωπικούς λόγους και να συναλλάσσονται εύκολα με τις δημόσιες υπηρεσίες εκτός των συνόρων των χωρών τους. Για να υλοποιηθεί αυτό, θα πρέπει οι υπηρεσίες των κρατών μελών της ΕΕ να ανταλλάσουν πληροφορίες με αποδοτικό τρόπο και να συνεργάζονται για την εξυπηρέτηση των πολιτών.

Για την ανάπτυξη και την εφαρμογή της ΗΔ δεν αρκεί η χρήση των ΤΠΕ στην δημόσια διοίκηση καθώς η ΗΔ δεν είναι απλά ο παλιός τρόπος διακυβέρνησης με χρήση ΤΠΕ. Για να αξιοποιηθούν οι δυνατότητες των ΤΠΕ υπάρχει η ανάγκη διαθρωτικών μεταρρυθμίσεων στην διακυβέρνηση των κρατών μελών καθώς και ο συντονισμός μεταξύ των κρατών μελών για την παράλληλη ανάπτυξη της ΗΔ. Μέσα από την εφαρμογή της ΗΔ παρέχονται ηλεκτρονικές υπηρεσίες προς τους πολίτες και τις επιχειρήσεις υψηλότερης ποιότητας με μικρότερο χρονικό και οικονομικό κόστος.

## 1.2 Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης

Οι χώρες μέλη της ΕΕ συμφώνησαν στον χαρακτηρισμό μιας λίστας 20 δημόσιων υπηρεσιών ως δείκτες αξιολόγησης για τον βαθμό ανάπτυξης της ΗΔ [1, 2]. Στον Πίνακας 1 αναφέρονται οι υπηρεσίες αυτές, από τις οποίες οι 12 αφορούν υπηρεσίες προς τους πολίτες και οι υπόλοιπες 8 υπηρεσίες προς επιχειρήσεις. Οι υπηρεσίες αυτές αξιολογούνται ετησίως σε ευρωπαϊκό επίπεδο, βάσει κοινής μεθοδολογίας, παρέχοντας κατά αυτόν τον τρόπο μεταξύ άλλων την δυνατότητα σύγκρισης της προόδου διαφορετικών κρατών στην ανάπτυξη των ίδιων υπηρεσιών.

**Πίνακας 1 Ηλεκτρονικές Δημόσιες Υπηρεσίες**

| **Δημόσιες υπηρεσίες προς τους πολίτες** |
|---|
| **Φόρος εισοδήματος: δήλωση, γνωστοποίηση του οφειλόμενου ποσού** |
| **Υπηρεσίες ευρέσεως εργασίας από αντίστοιχα γραφεία** |
| **Εισφορές κοινωνικής ασφάλισης** |
| **Προσωπικά έγγραφα (διαβατήριο και άδεια οδήγησης)** |
| **Καταχωρίσεις αυτοκινήτων (νέα, μεταχειρισμένα και εισαγόμενα αυτοκίνητα)** |
| **Έκδοση οικοδομικής άδειας** |
| **Δηλώσεις στην αστυνομία (π.χ. σε περίπτωση κλοπής)** |
| **Δημόσιες βιβλιοθήκες (διαθεσιμότητα καταλόγων των εργαλείων, αναζήτηση)** |
| **Πιστοποιητικά (γέννησης, γάμου): αίτηση και παραλαβή** |
| **Εγγραφές στην τριτοβάθμια εκπαίδευση / πανεπιστήμιο** |
| **Αναγγελίες μετακόμισης (αλλαγή διεύθυνσης)** |
| **Υπηρεσίες υγείας (π.χ. διαδραστικές συμβουλές για τη διαθεσιμότητα υπηρεσιών σε διάφορα νοσοκομεία, ραντεβού σε νοσοκομεία)** |
| **Δημόσιες υπηρεσίες για επιχειρήσεις** |
| **Κοινωνική ασφάλιση των εργαζομένων** |
| **Φόρος εταιρειών: δήλωση, γνωστοποίηση** |
| **ΦΠΑ: δήλωση, γνωστοποίηση** |
| **Καταχώριση νέας εταιρείας** |
| **Υποβολή δεδομένων σε στατιστικές υπηρεσίες** |
| **Οι τελωνειακές διασαφήσεις** |
| **Περιβάλλον που σχετίζονται με τις άδειες (συμπεριλαμβανομένης της υποβολής εκθέσεων)** |
| **Δημόσιες συμβάσεις** |

Για να μπορέσει όμως να αξιολογηθεί το επίπεδο και η ποιότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών ορίστηκαν για τις υπηρεσίες αυτές 4 σταθμισμένα επίπεδα ωριμότητας [2, 3].

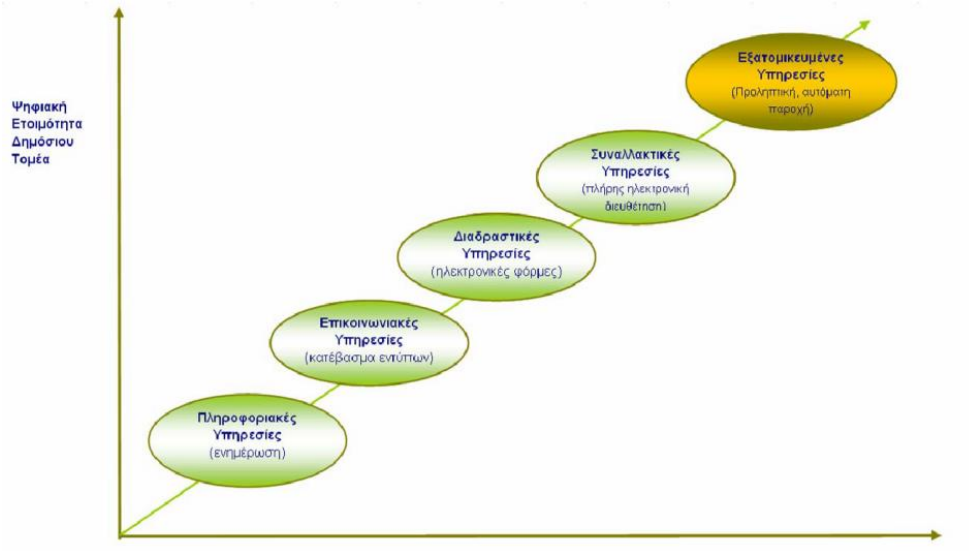
1. **Πληροφόρηση (Information):** Οι υπηρεσίες παρέχουν μόνο ηλεκτρονική πληροφόρηση. Οι χρήστες μπορούν να αναγνώσουν ή και να κατεβάσουν στον υπολογιστή τους τις πληροφορίες αυτές.
2. **Αλληλεπίδραση (One-way Interaction)**: Φόρμες αιτήσεων διατίθενται ηλεκτρονικά. Οι χρήστες μπορούν να ενημερωθούν για τον τρόπο διεκπεραίωσης των διαδικασιών, να κατεβάσουν στον υπολογιστή τους τα αντίστοιχα, να τυπώσουν και να τα χρησιμοποιήσουν στις συναλλαγές τους με

τους φορείς. Η διαδικασία της εξυπηρέτησης ξεκινά με την παρουσίαση στον φορέα των αιτήσεων σε έγχαρτη μορφή.

3. **Αμφίδρομη Αλληλεπίδραση (Two-way Interaction):** Είναι δυνατή η υλοποίηση κάποιων μεμονωμένων υπηρεσιών μεταξύ της διοίκησης και πολιτών ή και επιχείρησης. Η διαδικασία της συναλλαγής περιλαμβάνει κάποιο μηχανισμό ταυτοποίησης και προστασίας των δεδομένων που αποστέλλει ο χρήστης. Η διαδικασία μπορεί να ξεκινήσει ηλεκτρονικά αλλά ολοκληρώνεται με μη ηλεκτρονικό τρόπο .
4. **Συναλλαγή (Transaction):** Υπάρχει η δυνατότητα πλήρους υποκατάστασης της αντίστοιχης μη ηλεκτρονικής υπηρεσίας. Η παροχή των υπηρεσιών προς τους πολίτες και τις επιχειρήσεις είναι πλήρως αυτοματοποιημένες.
5. **Προσωποποίηση(Personalisation):** Είναι προληπτική και στοχευμένη παροχή υπηρεσιών. Κατά την προληπτική παροχή υπηρεσιών το κράτος προχωρά σε δράσεις μέσω τον οποίων βελτιώνει την παροχή της υπηρεσίας και την φιλικότητα της προς τον χρήστη. Επίσης παρέχει αυτόματα κάποιες υπηρεσίες προς τον πολίτη χωρίς αυτός να τις ζητήσει.

Το στάδιο 5 προστέθηκε στην ετήσια αναφορά του 2007 για την εξέλιξη των 20 βασικών υπηρεσιών. Το νέο επίπεδο ΗΔ έχει εφαρμογή μόνο σε εννιά (9) από τις 20 βασικές υπηρεσίες.

Στο σχήμα 1 φαίνονται τα πέντε επίπεδα παροχής υπηρεσιών στην ΗΔ.




**Σχήμα 1 :Επίπεδα Ολοκλήρωσης Υπηρεσιών ΗΔ [2]**

Οι υπηρεσίες ΗΔ χωρίζονται σε τρεις κατηγορίες ανάλογα με το ποιος τις παρέχει και σε ποιους απευθύνονται. Οι υπηρεσίες αυτές παρέχονται από τη Δημόσια Διοίκηση προς πολίτες, επιχειρήσεις ή εργαζομένους ή ανάμεσα σε φορείς της Διοίκησης από τη Δημόσια Διοίκηση προς άλλα μέρη [1] :

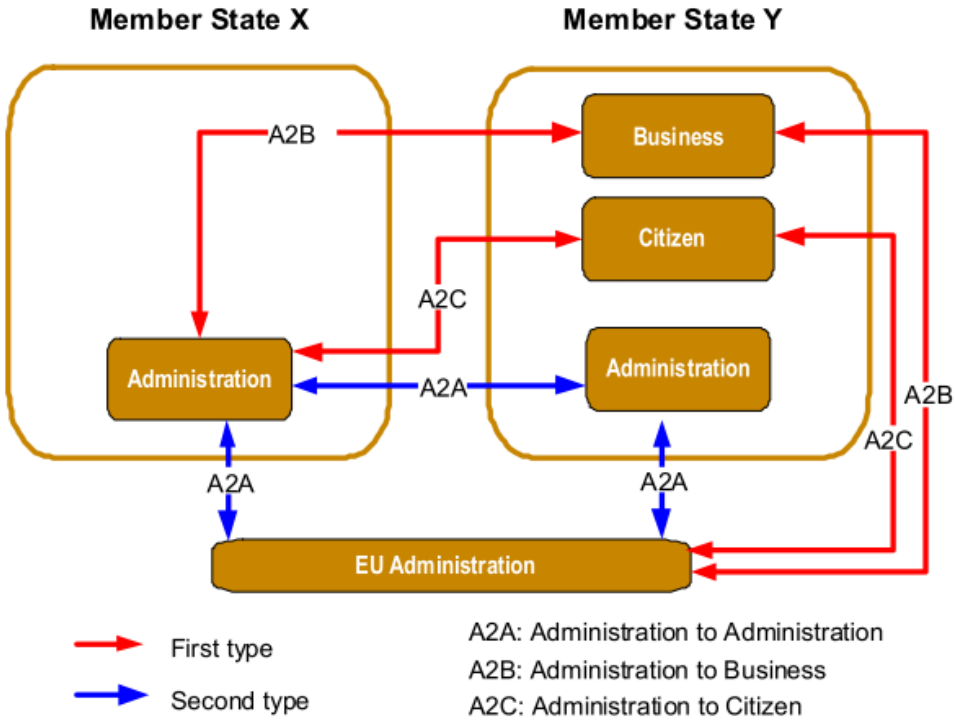
• G2C (Government to Citizen): Στην κατηγορία αυτή περιλαμβάνονται όλες εκείνες οι υπηρεσίες οι οποίες παρέχονται από τους φορείς της Δημόσιας Διοίκησης προς πολίτες.

• G2B (Government to Business): Στην κατηγορία αυτή ανήκουν όλες οι υπηρεσίες που παρέχονται από τους κρατικούς φορείς και απευθύνονται σε επιχειρήσεις.

• G2G (Government to Government): Η κατηγορία αυτή αναφέρεται στα διάφορα είδη υπηρεσιών που πραγματοποιούνται μεταξύ των φορέων της Δημόσιας Διοίκησης.

Στόχος της ΕΕ είναι οι υπηρεσίες των δημοσίων διοικήσεων των κρατών μελών να παρέχονται σε διασυνοριακό επίπεδο ενισχύοντας την ενιαία αγορά. Για να μπορέσει

ένα φυσικό ή νομικό πρόσωπο ενός κράτους να απολάβει τις υπηρεσίες που προσφέρονται σε ένα δεύτερο κράτος, θα πρέπει οι οργανισμοί των διοικήσεων και τα αντίστοιχα πληροφοριακά συστήματα τους να έχουν την δυνατότητα αλληλεπίδρασης μεταξύ τους. Στο σχήμα 2 απεικονίζονται οι αλληλεπιδράσεις που απαιτούνται για την παροχή δημοσίων υπηρεσιών από ένα κράτος Χ σε νομικά και φυσικά πρόσωπα κάποιου άλλου κράτους Υ αλλά και μεταξύ των δημοσίων διοικήσεων των δύο χωρών .




**Σχήμα 2: Αλληλεπιδράσεις για την παροχή δημόσιων υπηρεσιών σε διασυνοριακό επίπεδο [1]**

Ο πρώτος τύπος αφορά την άμεση αλληλεπίδραση μεταξύ επιχειρήσεων ή πολιτών από ένα κράτος μέλος Χ και δημόσιες διοικήσεις σε άλλο κράτος μέλος Υ καθώς και / ή την διοίκηση της ΕΕ ( Administration to Business (A2B) και Administration to Citizens (A2C)) που παρέχουν τη δημόσια υπηρεσία για τις επιχειρήσεις και τους πολίτες.

Ο δεύτερος τύπος αφορά την αλληλεπίδραση μεταξύ των διοικήσεων διαφόρων κρατών μελών της ΕΕ ή των διοικήσεων τους (Administration to Administration (A2A)).

Μέσω αυτού του τύπου αλληλεπίδραση μπορεί να υποστηριχτούν οι διοικήσεις για την παροχή υπηρεσιών προς τις επιχειρήσεις ή τους πολίτες (A2B, A2C).

Στο σχήμα 3 αναφέρονται μερικές από τις υπηρεσίες οι οποίες αντιστοιχούν στις ανάλογες αλληλεπιδράσεις μεταξύ των διοικήσεων, των πολιτών και των επιχειρήσεων.

| Sector/Area | Service |
|---|---|
| Business development (A2B, A2A) | Start-up of a company<br>Public procurement<br>Registration of patents, trademarks, designs<br>Consumer protection, labelling, packaging |
| Certificates and licenses (A2C) | Birth and marriage certificates<br>Driving licences<br>Passports, visas<br>Residence and working permits<br>Car registration |
| Education (A2C) | Enrolment in schools and universities<br>Study grants |
| Taxes for citizens (A2C) | Online Tax |

| Sector/Area | Service |
|---|---|
| Social security (A2C) | Information service for social security systems<br>Unemployment benefits<br>Child allowances<br>Pensions<br>Public health insurance |
| Supply of statistical data (A2B, A2A) | Tax for businesses<br>VAT refunding<br>Information on tax incentives<br>Declaration of excise goods |
| Work (A2C) | Recognition of qualifications and diplomas<br>Job search |
| Customs (A2C, A2B, A2A) | Information on Customs duties<br>Customs declarations |

**Σχήμα 3: Παραδείγματα δημοσίων υπηρεσιών [1]**

## 1.3 Εξέλιξη και μέλλον Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

Με σκοπό να υλοποιηθούν οι στόχοι της «Στρατηγικής της Λισαβόνας », εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο το σχέδιο δράσεων eEurope (action plans) που σκοπός του ήταν η τόνωση των παρεχόμενων ηλεκτρονικών υπηρεσιών από τις κυβερνήσεις των κρατών μελών καθώς και η ανάπτυξη της παραγωγικότητας σε όλες τις μορφές της οικονομίας. Το 2003 συμφωνήθηκαν τα βήματα που πρέπει να γίνουν για την υλοποίηση των στόχων της eEurope μέσα από ένα σχέδιο δράσεων το οποίο ονομάστηκε eEurope2005. Σύμφωνα με το eEurope2005 [4], η Ευρώπη έως το 2005 θα έπρεπε να παρέχει τις παρακάτω σύγχρονες δικτυακές δημόσιες υπηρεσίες :

- όσον αφορά την ΗΔ
    - υπηρεσίες ηλεκτρονικής μάθησης (e- learning)και
    - ηλεκτρονικές υπηρεσίες υγείας (e-health),
- ένα δυναμικό περιβάλλον για το ηλεκτρονικό επιχειρείν (e-bussiness)
- ασφαλής υποδομές πληροφοριών
- δυναμικό περιβάλλον για το ηλεκτρονικό επιχειρείν (e-business),
- ασφαλής υποδομή πληροφοριών,
- μαζική διάθεση ευρυζωνικής πρόσβασης σε ανταγωνιστικές τιμές,
- συγκριτική αξιολόγηση της προόδου και διάδοση ορθών πρακτικών.

Το 1995 είχε ξεκινήσει το πρόγραμμα IDA (Interchange Data between Administrations) [5], το οποίο αποσκοπούσε στην διευκόλυνση της ανάπτυξης και της επιχειρησιακής εφαρμογής δικτύων τηλεματικής για την ανταλλαγή δεδομένων μεταξύ δημόσιων διοικήσεων σε πανευρωπαϊκό επίπεδο. Το πρόγραμμα χωρίστηκε σε δυο φάσεις: στο IDA I και το IDA II. Κατά την πρώτη φάση το πρόγραμμα συνέβαλε στην υλοποίηση μεγάλων δικτύων τηλεματικής τα οποία είχαν εφαρμογή σε τομείς όπως η απασχόληση, ο ανταγωνισμός, η υγεία, η γεωργία και η στατιστική. Η δεύτερη φάση του προγράμματος, το IDA II, ξεκίνησε το 1999 και επικεντρώθηκε προς την αγορά και την διαλειτουργικότητα με σκοπό την βελτίωση της παροχής δημόσιων υπηρεσιών προς τους πολίτες και τις επιχειρήσεις. Το IDA και IDA II διαδέχτηκε το πρόγραμμα IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens) [1], το οποίο ξεκίνησε το 2005 και ολοκληρώθηκε το 2009. Αποτελώντας την συνέχεια του IDAII, χρησιμοποίησε τις δυνατότητες που προσφέρουν οι ΤΠΕ για την υποστήριξη της παροχής διασυνοριακών δημόσιων υπηρεσιών προς τους πολίτες και τις επιχειρήσεις αποσκοπώντας στην βελτίωση της αποτελεσματικότητας και της συνεργασίας μεταξύ των δημοσίων υπηρεσιών των χωρών της ΕΕ και στην βελτίωση του βιοτικού επιπέδου των πολιτών στον χώρο της ΕΕ. Για να μπορέσουν οι πολίτες και οι επιχειρήσεις να απολαμβάνουν τις δημόσιες υπηρεσίες που προσφέρονται μέσα από την ΗΔ, θα πρέπει τα

πληροφοριακά συστήματα όλων των εμπλεκομένων να ακολουθούν κάποια κοινά τεχνικά πρότυπα έτσι ώστε να μπορούν να συνδέονται μεταξύ τους και να ανταλλάσουν πληροφορίες.

Μετά την έγκριση του eEurope 2005, η Ευρωπαϊκή Επιτροπή κλήθηκε "*να εκδώσει ένα συμφωνημένο πλαίσιο διαλειτουργικότητας για την υποστήριξη της παροχής πανευρωπαϊκών υπηρεσιών ηλεκτρονικής διακυβέρνησης για τους πολίτες και τις επιχειρήσεις*"[4]. Στο πλαίσιο αυτό θα αναφέρονταν όλες εκείνες οι πληροφορίες καθώς και οι τεχνικές πολιτικές και προδιαγραφές που κρίνονται απαραίτητες για την διασύνδεση των πληροφοριακών συστημάτων των δημοσίων διοικήσεων όλων των κρατών της ΕΕ. Το σχέδιο δράσης προέβλεπε επίσης ότι, το πλαίσιο «*θα πρέπει να βασίζεται σε ανοικτά πρότυπα και να ενθαρρύνεται η χρήση του λογισμικού ανοικτού κώδικα*» [4]. Το παραγόμενο έγγραφο θα καθόριζε το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας EIF (European Interoperability Framework) [6] πάνω στο οποίο θα βασίζονταν η παροχή πανευρωπαϊκών υπηρεσιών ΗΔ και θα αποτελούσε το έγγραφο αναφοράς για το πρόγραμμα IDABC.

Το σχέδιο δράσης eEurope2005 διαδέχτηκε το πρόγραμμα δράσης i2010 [7] μέσα από το οποίο καθορίστηκαν οι γενικές πολιτικές κατευθύνσεις για την κοινωνία της πληροφορίας και τα μέσα ενημέρωσης. Επιδίωξη της στρατηγικής i2010 ήταν η ώθηση της ευρωπαϊκής πρωτοπορίας στις ΤΠΕ και η αξιοποίηση των οφελών της Κοινωνίας της Πληροφορίας υπέρ της ευρωπαϊκής οικονομικής ανάπτυξης και της απασχόλησης. Για να επιτευχτεί η επιδίωξη αυτή ορίστηκαν τρεις στόχοι προτεραιότητας που θα έπρεπε να υλοποιηθούν μέχρι το 2010 για τις ευρωπαϊκές πολιτικές στους τομείς της κοινωνίας της πληροφορίας και των μέσων ενημέρωσης:

- Η ολοκλήρωση ενός ενιαίου ευρωπαϊκού χώρου πληροφοριών,
- Η ενίσχυση της καινοτομίας και των επενδύσεων στην έρευνα για τις ΤΠΕ και
- Η ολοκλήρωση της δημιουργίας μιας κοινωνίας της πληροφορίας και των μέσων ενημέρωσης με βάση την κοινωνική ένταξη.

Το 2010 προτάθηκε μια νέα πολιτική στρατηγική για την ΕΕ με τίτλο «Europe 2020[1]» με στόχο την αύξηση της απασχόλησης, την τόνωση της παραγωγικότητας και την ενίσχυση της κοινωνικής συνοχής στην Ευρώπη. Μια από τις επτά πρωτοβουλίες που προτείνονται μέσα από την στρατηγική αυτή είναι το νέο Ψηφιακό Θεματολόγιο για την Ευρώπη (Digital Agenda). Οι δράσεις που απαιτούνται στο πλαίσιο του Ψηφιακού Θεματολογίου είναι:

- Υλοποίηση της ενιαίας ψηφιακής αγοράς
- Αύξηση της διαλειτουργικότητας και των προτύπων
- Εδραίωση της εμπιστοσύνης και της ασφάλειας στο διαδίκτυο
- Προώθηση της ταχείας και υπερταχείας πρόσβασης στο διαδίκτυο για όλους
- Επένδυση στην έρευνα και την καινοτομία
- Βελτίωση του *ψηφιακού γραμματισμού*, των δεξιοτήτων και της κοινωνικής ένταξης
- Οφέλη για την κοινωνία χάρη στην έξυπνη αξιοποίηση της τεχνολογίας.

Μέρος της Ψηφιακής Ατζέντας 2020[2] υλοποιείται από το σχέδιο δράσης «The European eGovernment Action Plan 2011-2015»[8] το οποίο στοχεύει στην αξιοποίηση των ΤΠΕ για την προώθηση έξυπνων, βιώσιμων και καινοτόμων ευρωπαϊκών κυβερνήσεων. Σε αυτό το σχέδιο δράσης καθορίζονται οι παρακάτω 4 πολιτικές προτεραιότητες για όλες τις Ευρωπαϊκές δημόσιες διοικήσεις για τα επόμενα 5 χρόνια:

- Οι πολίτες και οι επιχειρήσεις απολαμβάνουν υπηρεσίες ΗΔ που έχουν σχεδιαστεί γύρω από τις ανάγκες τους καθώς και αυξημένη πρόσβαση σε δημόσιες πληροφορίες, ενισχυμένη διαφάνεια και κατάλληλα μέσα για τη συμμετοχή των ενδιαφερομένων σε διαδικασίες χάραξης πολιτικής.

[1] http://ec.europa.eu/europe2020/index_en.htm
[2] http://ec.europa.eu/digital-agenda/

- Η κινητικότητα στην Ενιαία Αγορά[3] (Single Market) ενισχύεται από αδιάλειπτες υπηρεσίες ΗΔ για τη σύσταση και τη λειτουργία επιχειρήσεων καθώς και τη φοίτηση, την εργασία, την κατοίκιση και τη συνταξιοδότηση οπουδήποτε στην Ευρωπαϊκή Ένωση,
- Οι δημόσιες υπηρεσίες είναι αποδοτικές και αποτελεσματικές μέσω μιας συνεχούς προσπάθειας για την χρησιμοποίηση της ΗΔ στοχεύοντας στη μείωση του διοικητικού φόρτου, στη βελτίωση των οργανωτικών διαδικασιών και την προώθηση της αειφόρου οικονομίας χαμηλών εκπομπών άνθρακα,
- Η εφαρμογή των προτεραιοτήτων της πολιτικής έχει καταστεί δυνατή με τη δημιουργία των κατάλληλων βασικών εργαλείων και με την εφαρμογή των απαραίτητων νομικών και τεχνικών προϋποθέσεων.

Ειδικότερα, για την παροχή των υπηρεσιών προς τις επιχειρήσεις θα πρέπει αυτές να μπορούν να προσφέρουν τις υπηρεσίες τους και να πουλούν τα προϊόντα τους σε ολόκληρη την Ευρώπη μέσω εύκολων στην χρήση ηλεκτρονικών δημόσιων συμβάσεων [9] (*e-procurment*[4]) και μέσα από την αποδοτική εφαρμογή των υπηρεσιών που προσφέρονται από τα ενιαία κέντρα εξυπηρέτησης των κρατών για την αλληλεπίδραση των επιχειρήσεων με την δημόσια διοίκηση. Ακόμη, σε πολλές από τις παρεχόμενες υπηρεσίες είναι απαραίτητο να ταυτοποιηθεί και να αυθεντικοποιηθεί το φυσικό ή το νομικό πρόσωπο στο οποίο πρόκειται να παραδοθεί η υπηρεσία. Για τις διασυνοριακές υπηρεσίες θα πρέπει να χρησιμοποιούνται μέθοδοι ηλεκτρονικής ταυτοποίησης και αυθεντικοποίησης πιο αποδοτικοί και ασφαλείς από αυτές της χρήσης κωδικών που συνηθίζεται έως τώρα. Για τους σκοπούς αυτούς τα κράτη μέλη θα πρέπει να αναπτύξουν διασυνοριακές υπηρεσίες βασιζόμενες στα αποτελέσματα των Μεγάλης Κλίμακας διασυνοριακών Πιλοτικών προγραμμάτων LSPs (Large Scale Pilots) SPOCS (Simple Procedures Online for Cross- border Services), PEPPOL ((Pan-European Public Procurement Online), STORK (Secure Identity Across Borders Linked eID),e-CODEX

[3] http://ec.europa.eu/internal_market/top_layer/index_en.htm
[4] http://ec.europa.eu/internal_market/publicprocurement/e-procurement/

(justice Communication via Online Data EXhange), epSOS (Smart Open Services for european patients).

Ακόμη, μέσα από το σχέδιο δράσης 2011-2015 τα κράτη μέλη θα πρέπει να έχουν συμμορφώσει τα εθνικά πλαίσια διαλειτουργικότητάς τους σύμφωνα με τις συστάσεις που παρέχονται από το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας [1].

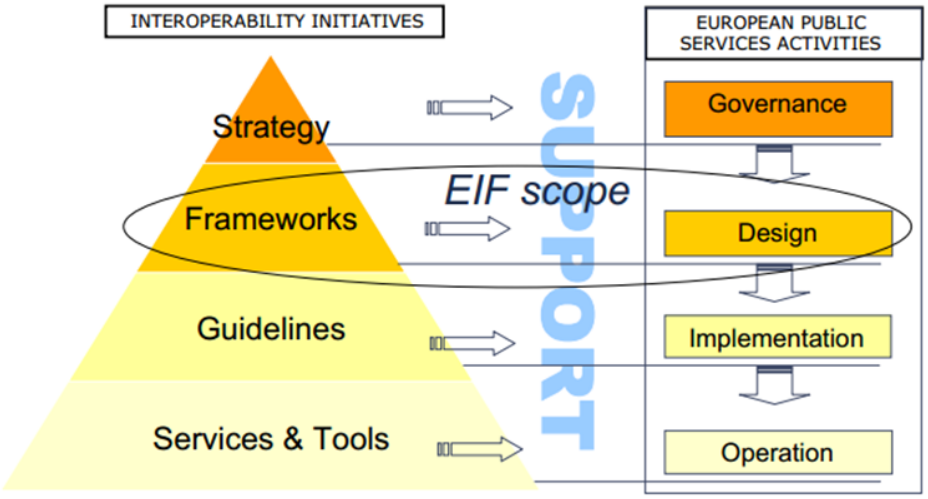
# Κεφάλαιο 2: Διαλειτουργικότητα Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης

## 2.1 Διαλειτουργικότητα

Το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας είναι μια από μια σειρά πρωτοβουλιών διαλειτουργικότητας που σκοπό έχουν την εγκαθίδρυση Ευρωπαϊκών δημόσιων υπηρεσιών. Στο σχήμα 4 διακρίνονται οι σχέσεις μεταξύ αυτών των πρωτοβουλιών οι οποίες είναι:

- η Ευρωπαϊκή Στρατηγική Διαλειτουργικότητας (European Interoperability Strategy (EIS))[5],
- το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας (European Interoperability Framework (EIF))[6],
- οι Ευρωπαϊκές Οδηγίες Διαλειτουργικότητας (European Interoperability Guidelines),
- οι Ευρωπαϊκές Υπηρεσίες και τα Εργαλεία Διαλειτουργικότητας για την θέσπιση Ευρωπαϊκών δημόσιων υπηρεσιών.

[5] http://ec.europa.eu/idabc/en/document/7772.html
[6] http://ec.europa.eu/idabc/en/document/2319/5644.html



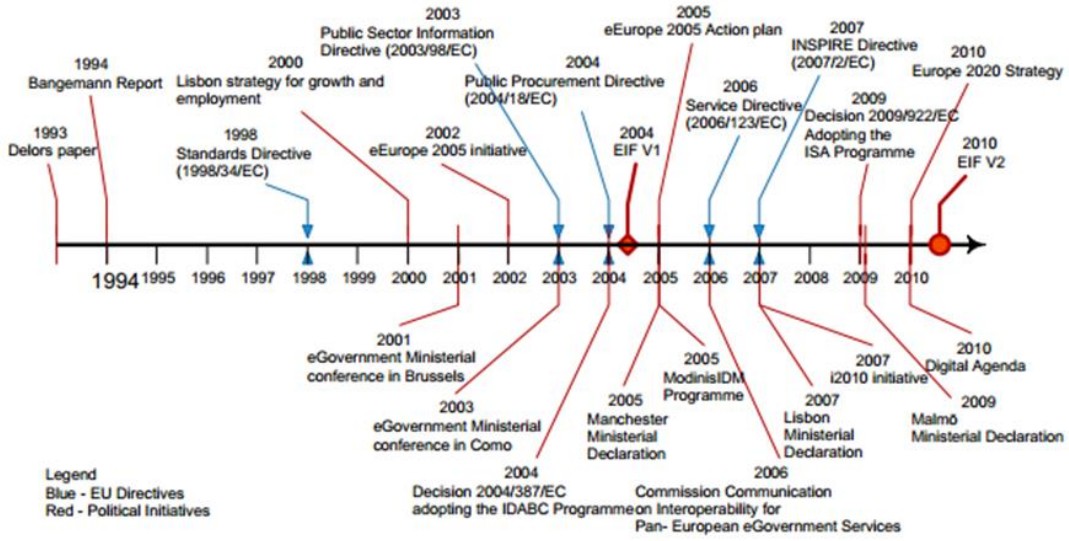

**Σχήμα 4: Πρωτοβουλίες διαλειτουργικότητας για την εγκαθίδρυση Ευρωπαϊκών δημόσιων υπηρεσιών**

Η Ευρωπαϊκή Στρατηγική Διαλειτουργικότητας (European Interoperability Strategy-EIS)[10] παρέχει τη βάση για ένα οργανωτικό, οικονομικό και επιχειρησιακό πλαίσιο για την υποστήριξη της διασυνοριακής και / ή την διατομεακή διαλειτουργικότητα. Το EIS καθοδηγεί το EFI και όλων των άλλων σχετικών προσπαθειών, καθορίζοντας τις στρατηγικές προτεραιότητες και τους στόχους. Ο σκοπός του EFI είναι να βοηθήσει στο σχεδιασμό ευρωπαϊκών δημόσιων υπηρεσιών. Οι Ευρωπαϊκές Οδηγίες για την διαλειτουργικότητα βοηθούν στην ανάπτυξη ευρωπαϊκών υπηρεσιών και εργαλείων που υποστηρίζουν την παροχή Ευρωπαϊκών δημόσιων υπηρεσιών

Η Διαλειτουργικότητα σύμφωνα με το άρθρο 2 της απόφασης 922/2009 της ΕΕ [11], ορίζεται ως εξής:

«*Διαλειτουργικότητα, στο πλαίσιο των ευρωπαϊκών δημόσιων υπηρεσιών, είναι η ικανότητα ανόμοιων και διαφορετικών οργανισμών να αλληλεπιδρούν προς αμοιβαίο όφελος και συμφωνημένων κοινών στόχων, όπου περιλαμβάνουν την ανταλλαγή πληροφοριών και γνώσεων μεταξύ των οργανισμών, μέσω των επιχειρηματικών διαδικασιών που υποστηρίζουν, μέσω της ανταλλαγής δεδομένων μεταξύ των αντίστοιχων συστημάτων τους ΤΠΕ*».

Η επίτευξη διασυνοριακής διαλειτουργικότητας αποτελεί πολιτική προτεραιότητα στις ευρωπαϊκές πρωτοβουλίες για τις δημόσιες υπηρεσίες. Η παροχή αδιάλειπτων διασυνοριακών δημόσιων υπηρεσιών (για τις οποίες η διαλειτουργικότητα αποτελεί προϋπόθεση) μπορεί να έχει μεγάλο αντίκτυπο στις επιχειρήσεις και τους πολίτες. Οι πρωτοβουλίες της ΕΕ, εμφανίζονται στο σχήμα 5 αντικατοπτρίζουν την υποστήριξη που παρέχεται σε πολιτικό επίπεδο από την ΕΕ, σε χρονική κλίμακα, για τη διαλειτουργικότητα μεταξύ των δημοσίων διοικήσεων.




**Σχήμα 5: Απεικόνιση σε χρονική κλίμακα των πρωτοβουλιών της ΕΕ για την διαλειτουργικότητα**

## 2.2 Αρχές Διαλειτουργικότητας

Το σχέδιο δράσης eEurope 2005 [4], καθώς και οι αποφάσεις του Κοινοβουλίου, του Συμβουλίου και της Επιτροπής της ΕΕ που αναφέρονται παραπάνω, έχουν υιοθετήσει και προωθήσει μια σειρά από γενικές αρχές που πρέπει να τηρούνται για τις υπηρεσίες ΗΔ που έχουν συσταθεί σε πανευρωπαϊκό επίπεδο. Κατά συνέπεια, οι παρατηρήσεις

και οι συστάσεις του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας πρέπει να ορίζονται με βάση τις ακόλουθες αρχές [1]:

### 2.2.1 Προσβασιμότητα

Υπάρχει η ανάγκη να διασφαλιστεί ότι η ΗΔ δημιουργεί ίσες ευκαιρίες για όλους μέσω ανοικτών, χωρίς αποκλεισμούς ηλεκτρονικών υπηρεσιών οι οποίες είναι προσιτές στο κοινό χωρίς διακρίσεις. Ο σχεδιασμός των διεπαφών πρέπει να ακολουθεί κάποιες γενικές αποδεκτές από όλους αρχές προκειμένου να εξασφαλιστεί η πρόσβαση των ατόμων με αναπηρία και να προσφέρουν υποστήριξη σε μια γλώσσα κατανοητή από τον χρήστη. Ο Κατευθυντήριος Οδηγός για την Προσβασιμότητα (Web Accessibility Guidelines) ο οποίος συστάθηκε από την Πρωτοβουλία Διαδικτυακής Πρόσβασης (Web Access Initiative), της Κοινοπραξίας του Παγκόσμιου Ιστού (Word Wide Web Consortium ) θα πρέπει επίσης να λαμβάνεται υπόψη.

### 2.2.2 Πολυγλωσσία

Στις προσφερόμενες υπηρεσίες στην Ευρώπη χρησιμοποιούνται μια μεγάλη ποικιλία από γλώσσες. Στο επίπεδο παρουσίασης (front office και ιστοσελίδες στο Διαδίκτυο - το επίπεδο στο οποίο οι πολίτες και οι επιχειρήσεις να αλληλεπιδρούν με τις διοικήσεις), η γλώσσα είναι σαφώς ένας σημαντικός παράγοντας για την αποτελεσματική υλοποίηση των διευρωπαϊκών υπηρεσιών ΗΔ.

Στο επίπεδο back-office, οι βασικές αρχιτεκτονικές θα πρέπει να είναι γλωσσικά ουδέτερες, έτσι ώστε η πολυγλωσσία να μην αποτελεί εμπόδιο για την παροχή υπηρεσιών ΗΔ. Αν ουδετερότητα δεν είναι εφικτή (π.χ. σε XML-συστήματα), θα πρέπει να προβλεφθούν διατάξεις για τη διευκόλυνση των μηχανισμών μετάφρασης.

### 2.2.3 Ασφάλεια

Γενικότερα, η αξιόπιστη ανταλλαγή πληροφοριών πραγματοποιείται σύμφωνα με μια καθιερωμένη πολιτική ασφαλείας. Αυτό επιτυγχάνεται με τη διεξαγωγή κατάλληλων

ενεργειών αξιολόγησης κινδύνου πριν από τον τελικό καθορισμό και υλοποίηση των υπηρεσιών και των κατάλληλων μέτρων ασφαλείας. Η αρχή αυτή ισχύει εξίσου και για την ανταλλαγή πληροφοριών σε πανευρωπαϊκό επίπεδο. Στην περίπτωση αυτή, οι διοικήσεις των κρατών μελών θα πρέπει να εξετάσουν τη δική της πολιτική ασφαλείας τους και να καταλήξουν σε συμφωνία σχετικά με μια κοινή πολιτική για την ασφάλεια σε πανευρωπαϊκό επίπεδο. Ειδικότερα, για την ταξινόμηση εγγράφων σε επίπεδο ΕΕ και των σχετικών μέτρων ασφαλείας, εφαρμόζεται το άρθρο 13 του Συμβουλίου Ασφαλείας[12].

Από τη πλευρά των χρηστών, οι λειτουργίες που σχετίζονται με την ασφάλεια (ταυτοποίηση, έλεγχος ταυτότητας, μη-αποκήρυξη, εμπιστευτικότητα), θα πρέπει να παρέχουν ένα μέγιστο επίπεδο διαφάνειας και παρέχουν το συμφωνημένο επίπεδο ασφάλειας.

### 2.2.4 Προστασία Προσωπικών Δεδομένων

Οι Πανευρωπαϊκές υπηρεσίες ΗΔ θα πρέπει να διασφαλίζουν ένα ενιαίο επίπεδο προστασίας των προσωπικών δεδομένων, συμπεριλαμβανομένων μέτρων κατά τα οποία τα άτομα έχουν το δικαίωμα να επιλέγουν εάν τα δεδομένα τους μπορούν να χρησιμοποιηθούν για σκοπούς άλλους από αυτούς για τους οποίους τα δεδομένα είχαν αρχικά δοθεί. Πρέπει επίσης να παρέχονται σε κάθε ενδιαφερόμενο πληροφορίες σχετικά με την επεξεργασία των δεδομένων. Γενικότερα, οι εργασίες για τη διαλειτουργικότητα θα πρέπει να συνάδουν με τους μηχανισμούς που ήδη εφαρμόζονται από την οδηγία 95/46/ΕΚ 16 (ιδίως το άρθρο 29)[13]. Ακόμη, όταν είναι εφικτό θα πρέπει να εφαρμόζονται τεχνολογίες που σέβονται και ενισχύουν την ιδιωτικότητα.

### 2.2.5 Επικουρικότητα

Η καθοδήγηση που παρέχεται από το Ευρωπαϊκό πλαίσιο διαλειτουργικότητας αφορά μόνο το πανευρωπαϊκό επίπεδο των υπηρεσιών. Σύμφωνα με την αρχή της

επικουρικότητας, η καθοδήγηση δεν επηρεάζει την εσωτερική λειτουργία των διοικήσεων και των θεσμικών οργάνων της ΕΕ. Κάθε κράτος μέλος και όργανο της ΕΕ θα πρέπει να λαμβάνει τα αναγκαία μέτρα για να διασφαλίζεται η διαλειτουργικότητα σε πανευρωπαϊκό επίπεδο.

### 2.2.6 Χρήση ανοικτών προτύπων

Η καθοδήγηση για την επίτευξη της διαλειτουργικότητας στο πλαίσιο των πανευρωπαϊκών υπηρεσιών ΗΔ, θα πρέπει να επικεντρωθεί σε ανοικτά πρότυπα.

Για να χαρακτηριστεί ένα πρότυπο «ανοικτό» θα πρέπει οι προδιαγραφές και τα έγγραφα που το συνοδεύουν να ικανοποιούν τα παρακάτω ελάχιστα χαρακτηριστικά:

- Το πρότυπο υιοθετήθηκε και θα συντηρείται από μια μη- κερδοσκοπική οργάνωση, και η συνεχή ανάπτυξη βασίζεται σε ανοικτή διαδικασία λήψης αποφάσεων η οποία είναι προσιτή σε όλους τους ενδιαφερόμενους.
- Το πρότυπο έχει δημοσιευθεί και το τυποποιημένο έγγραφο προδιαγραφών είναι διαθέσιμο είτε ελεύθερα είτε έναντι συμβολικού αντιτίμου. Θα πρέπει να επιτρέπεται σε όλους η αντιγραφή του, η διανομή του και η χρησιμοποίηση του ελεύθερα είτε έναντι συμβολικού αντιτίμου.
- Η πνευματική ιδιοκτησία - δηλαδή τα διπλώματα ευρεσιτεχνίας που ενδεχομένως υπάρχουν – και αφορούν είτε ολόκληρο το πρότυπο είτε τμήματα γίνεται αμετάκλητα διαθέσιμη σε ατελώς βάση.
- Δεν υπάρχουν περιορισμοί σχετικά με την περαιτέρω χρήση των πρότυπων.

## 2.3 Επίπεδα και Είδη Διαλειτουργικότητας

Σύμφωνα με το Ευρωπαϊκό Πλαίσιο Διαλειτουργικότητας, στην ΗΔ η διαλειτουργικότητα αναλύεται σε τέσσερα επίπεδα: την νομική διαλειτουργικότητα (legal interoperability), την οργανωσιακή διαλειτουργικότητα (organizational

interoperability), την σημασιολογική διαλειτουργικότητα (semantic interoperability) και την τεχνική διαλειτουργικότητα (technical interoperability) [1, 6].

### 2.3.1 Οργανωσιακή Διαλειτουργικότητα

Αυτή η πτυχή της διαλειτουργικότητας σχετίζεται με τον καθορισμό στόχων, την μοντελοποίηση των διαδικασιών και την επίτευξη συνεργασίας των διοικήσεων που επιθυμούν να ανταλλάξουν πληροφορίες και οι οποίοι ενδέχεται να έχουν διαφορετικές εσωτερικές δομές και διαδικασίες. Επιπλέον, η οργανωσιακή διαλειτουργικότητα στοχεύει στο να ανταπεξέλθει στις απαιτήσεις των χρηστών, καθιστώντας τις υπηρεσίες διαθέσιμες, εύκολα αναγνωρίσιμες, προσβάσιμες και προσανατολισμένες προς τον χρήστη. Οι δημόσιες διοικήσεις των κρατών θα πρέπει να τεκμηριώσουν τις επιχειρηματικές διαδικασίες τους και να συμφωνήσουν για το πώς αυτές οι διαδικασίες θα μπορέσουν να αλληλεπιδράσουν διασυνοριακά με σκοπό την προσφορά μιας Ευρωπαϊκής δημόσιας υπηρεσίας [1].

### 2.3.2 Σημασιολογική Διαλειτουργικότητα

Αυτή η πτυχή της διαλειτουργικότητας σχετίζεται με τη διασφάλιση της απόδοσης, της κατανόησης της, της ακριβής σημασίας και της διατήρησης των ανταλλασσόμενων πληροφοριών σε όλες τις αλληλεπιδράσεις μεταξύ των εμπλεκομένων μερών . Μέσω της σημασιολογικής διαλειτουργικότητας των συστημάτων δίνεται η δυνατότητα στους οργανισμούς να λαμβάνουν και να συνδυάζουν πληροφορίες από διαφορετικές πηγές πληροφόρησης αλλά και να τις επεξεργάζονται με ουσιαστικό τρόπο. Επιτυγχάνεται με τον ορισμό ενός κοινού λεξιλογίου εννοιών και ορολογιών για τα συστήματα και τις υπηρεσίες. Η σημασιολογική διαλειτουργικότητα αποτελεί συνεπώς προϋπόθεση για την front-end πολύγλωσση παροχή υπηρεσιών προς το χρήστη. Η επίτευξη της σημασιολογικής διαλειτουργικότητας σε επίπεδο ΕΕ είναι ένα σχετικά καινούργιο έργο και κάτι το οποίο δεν έχει επιτευχτεί μέχρι τώρα σε αυτό το εύρος.

Ως σημείο εκκίνησης για την επίτευξη του έργου αυτού, είναι η δημιουργία ειδικών δομών δεδομένων και αντικειμένων ανά τομέα διοίκησης (sector specific) τα οποία θα

μπορούν να αναφέρονται ως αγαθά (assets) σημασιολογικής διαλειτουργικότητας. Όταν ολοκληρωθεί η δημιουργία τους, οι συνεργαζόμενοι φορείς θα πρέπει να συμφωνήσουν στις έννοιες των πληροφοριών που ανταλλάσσονται. Αυτό αποτελεί μία σημαντική πρόκληση λόγω των διαφορετικών γλωσσικών, πολιτιστικών, νομικών, διοικητικών και περιβαλλόντων των διαφόρων κρατών μελών. Επιπλέον, η πολυγλωσσία στην ΕΕ προσθέτει ακόμη περισσότερη πολυπλοκότητα στο εγχείρημα αυτό[14].

Σύμφωνα με το Ευρωπαϊκό πλαίσιο διαλειτουργικότητας, η σημασιολογική διαλειτουργικότητα περιλαμβάνει τις ακόλουθες έννοιες [1]:

- Τη *σημασιολογική* διαλειτουργικότητα η οποία είναι σχετική με την έννοια των αντικειμένων των δεδομένων και τις σχέσεις μεταξύ αυτών. Περιλαμβάνει την ανάπτυξη λεξιλογίου για την περιγραφή των ανταλλαγών δεδομένων, και εξασφαλίζει ότι τα αντικείμενα είναι κατανοητά με τον ίδια έννοια από τα μέρη που ανταλλάσσουν τα δεδομένα .
- Τη *συντακτική* διαλειτουργικότητα η οποία περιγράφει την ακριβή μορφή των πληροφοριών που ανταλλάσσονται σε σχέση με τη γραμματική, τη μορφή και σχήματα τους.

Η επίτευξη σημασιολογικής διαλειτουργικότητας σε ευρωπαϊκό επίπεδο απαιτεί τουλάχιστον:

- συμφωνημένες διαδικασίες και μεθοδολογίες για την ανάπτυξη σημασιολογικών αγαθών διαλειτουργικότητας.
- συμφωνίες εξειδικευμένες για κάθε τομέα διοίκησης και αλλά και διατομεακές ανάμεσα στις κοινότητες για τη χρήση των σημασιολογικών αγαθών διαλειτουργικότητας σε ευρωπαϊκό επίπεδο.

Λόγω της πολυπλοκότητας του έργου της επίτευξη της σημασιολογικής διαλειτουργικότητας σε επίπεδο ΕΕ και του μεγάλου αριθμού των ενδιαφερομένων

μερών, θα χρειαστεί μια συντονισμένη ομαδική προσπάθεια για την εναρμόνιση των διαδικασιών και μεθοδολογιών.

Για την επίτευξη της σημασιολογικής διαλειτουργικότητας έχουν ξεκινήσει πολλές πρωτοβουλίες, τόσο σε εθνικό όσο και σε κοινοτικό επίπεδο. Η πρωτοβουλία της ΕΕ για τη σημασιολογική διαλειτουργικότητα (SEMIC) [15] έχει ως στόχο να θέσει τα θεμέλια της σημασιολογικής διαλειτουργικότητας για τις ευρωπαϊκές δημόσιες υπηρεσίες, σε όλους τους τομείς και σε στενή συνεργασία με τις εθνικές πρωτοβουλίες. Παρέχονται επίσης, υπηρεσίες καθοδήγησης για τα στάδια του σχεδιασμού και της υλοποίησης, καθώς και μια web-based πλατφόρμα για τη συνεργασία και την ανταλλαγή λύσεων σε προβλήματα σημασιολογικής διαλειτουργικότητας.

### 2.2.3 Τεχνική Διαλειτουργικότητα

Αυτή η πτυχή της διαλειτουργικότητας καλύπτει τα τεχνικά ζητήματα της διασύνδεσης των συστημάτων πληροφορικής και των υπηρεσιών. Περιλαμβάνει ζητήματα όπως: τις προδιαγραφές των διεπαφών, τις τεχνικές προδιαγραφές των υποδομών και του λογισμικού για την αποθήκευση, ενσωμάτωση, μεταφορά, παρουσίαση και ασφάλεια των δεδομένων και των υπηρεσιών [16].

# Κεφάλαιο 3: Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ευρωπαϊκή Ένωση

## 3.1 Πολιτικές Υποστήριξης ΤΠΕ- Πρόγραμμα Ανταγωνιστικότητας και Καινοτομίας

Μέσα από την έγκριση του στρατηγικού πλαισίου*, i2010 [7]- Ευρωπαϊκή κοινωνία της πληροφορίας για την ανάπτυξη και την απασχόληση* - προωθείται μια ανοικτή και ανταγωνιστική ψηφιακή οικονομία και υπογραμμίζονται οι ΤΠΕ ως κινητήρια δύναμη για την κοινωνικής ένταξη και την ποιότητα της ζωής. Ως βασικό στοιχείο της ανανεωμένης συμφωνίας της Λισσαβόνας για την ανάπτυξη και την απασχόληση, η στρατηγική i2010 χτίζει μια ολοκληρωμένη προσέγγιση για την κοινωνία της πληροφορίας και των πολιτικών για τα οπτικοακουστικά μέσα ενημέρωσης στην ΕΕ.

Βασιζόμενη σε μια διεξοδική ανάλυση των προκλήσεων της κοινωνίας της πληροφορίας και στην ευρεία διαβούλευση των ενδιαφερομένων μερών στην περίπτωση προηγούμενων πρωτοβουλιών και μέσων, η στρατηγική που προτείνεται στο *i2010* προτείνει τρεις προτεραιότητες για την ευρωπαϊκή κοινωνία της πληροφορίας και τα μέσα επικοινωνίας[7] :

i. Την ολοκλήρωση του ενιαίου Ευρωπαϊκού Χώρου της Πληροφορικής (Single European Information Space) που προωθεί την ανοιχτή και ανταγωνιστική εσωτερική αγορά για την κοινωνία της πληροφορίας και τα μέσα ενημέρωσης
ii. Την ενίσχυση της καινοτομίας και των επενδύσεων στην έρευνα των ΤΠΕ με στόχο την προώθηση της ανάπτυξης περισσότερων και καλύτερων θέσεων εργασίας
iii. Την επίτευξη μιας Ευρωπαϊκής Κοινωνίας της Πληροφορίας (Inclusive European Information Society) που είναι συμβατή με την αειφόρο ανάπτυξη και η όποια δίνει προτεραιότητα στη βελτίωση των δημόσιων υπηρεσιών και της ποιότητας ζωής.

Για την επίτευξη αυτών των προτεραιοτήτων, έχουν δρομολογηθεί ένα σύνολο δράσεων. Αυτές περιλαμβάνουν: ρυθμιστικές ενέργειες (actions), ενέργειες συντονισμού των πολιτικών, και χρηματοδοτικά εργαλεία σε κοινοτικό επίπεδο. Το ICT PSP (μέσα από το πρόγραμμα CIP)[7] ήταν ένα από τα κύρια χρηματοοικονομικά εργαλεία της στρατηγικής του i2010.

Το Πρόγραμμα Ανταγωνιστικότητας και Καινοτομίας (CIP)[8] είχε εγκριθεί στις 24 Οκτωβρίου 2006 με την απόφαση αριθ. 1639/2006/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[17]. Η χρονική περίοδος λειτουργίας του CIP ήταν από το 2007 έως το 2013 και είχε συνολικό προϋπολογισμό € 3621 εκατομμύρια. Η ICT PSP [18]στόχευε στην τόνωση της καινοτομίας και της ανταγωνιστικότητας μέσω της ευρύτερης αφομοίωσης και βέλτιστης χρήσης των ΤΠΕ από τους πολίτες, τις κυβερνήσεις και τις επιχειρήσεις και ειδικότερα τις Μικρομεσαίες Επιχειρήσεις (SMEs) και να βοηθήσει στην ανάπτυξη της κοινωνίας της πληροφορίας. Το κοινοτικό αυτό πρόγραμμα οργανώθηκε γύρω από τρία πολυετή ειδικά προγράμματα:

1. Το Πρόγραμμα για την Επιχειρηματικότητα και την Καινοτομία (Entrepreneurship and Innovation Programme (EIP))
2. Το Πρόγραμμα Στήριξης της Πολιτικής των ΤΠΕ (Information and Communication Technologies Policy Support Programme (ICT PSP 2011))
3. Το Πρόγραμμα για την Ευφυή Ενέργεια-Ευρώπη (Intelligent Energy-Europe Programme (IEEP)).

Μεταξύ του 2007 και του 2010, η Ευρωπαϊκή Επιτροπή έχει χρηματοδοτήσει 132 έργα (projects) στο πλαίσιο των CIP ICT PSP [9]στρατηγικών προτεραιοτήτων, οι όποιες έχουν αντιμετωπίσει θέματα όπως: αποτελεσματική και διαλειτουργική ΗΔ (e-Goverment), φιλικές προς το χρήστη (user friendly) διοικήσεις, προσβασιμότητα, γήρανση, αειφόρες και διαλειτουργικές υπηρεσίες υγείας, ενεργειακής απόδοσης και αειφορίας στις

[7] http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm
[8] http://ec.europa.eu/cip/
[9] http://ec.europa.eu/information_society/apps/projects/index.cfm?menu=secondary&prog_id=IPSP

αστικές περιοχές, ΤΠΕ για μια οικονομία χαμηλών εκπομπών διοξειδίου του άνθρακα και έξυπνης κινητικότητας, ψηφιακές βιβλιοθήκες, πολύγλωσσες ιστοσελίδες, πληροφορίες του δημόσιου τομέα, ανάπτυξη και ασφάλεια του Διαδικτύου, ανοικτές καινοτόμες υπηρεσίες στις "έξυπνες" πόλεις.

Οι στόχοι του CIP ICT PSP επιδιώκονται μέσα από τρία εργαλεία υλοποίησης [18]:

- Πιλοτικό Α : Βασίζεται στις πρωτοβουλίες των κρατών μελών ή των σχετιζόμενων χωρών για να εξασφαλιστεί η πανευρωπαϊκή διαλειτουργικότητα των βασισμένων στις ΤΠΕ λύσεων. Τα Μεγάλης Κλίμακας Πιλοτικά έργα (Large Scale Pilots projects (LSPs)) εμπίπτουν στην κατηγορία αυτή και εμπλέκονται σε αυτά τουλάχιστον έξι κράτη μέλη, με δυνατότητα για περαιτέρω επέκταση τους σε όλα τα κράτη μέλη
- Πιλοτικό Β (επιχειρησιακό πιλοτικό): Στοχεύει στην τόνωση της αφομοίωσης των καινοτόμων υπηρεσιών και των προϊόντων που βασίζονται στις ΤΠΕ. Οι συμμετέχοντες στο πιλοτικό είναι δημόσιες αρχές, πάροχοι υπηρεσιών, φορείς και χρήστες του βιομηχανικού κλάδου.
- Θεματικά Δίκτυα: Εξασφάλιση ενός φόρουμ για τα ενδιαφερόμενα μέρη για την ανταλλαγή εμπειριών και την επίτευξη συναίνεσης σχετικά με την εφαρμογή πολιτικής για τις ΤΠΕ.

Οι δράσεις του πιλοτικού Α βοηθούν να εξασφαλιστεί η πανευρωπαϊκή διαλειτουργικότητα των λύσεων βασισμένων στις ΤΠΕ οι όποιες έχουν ήδη ξεκινήσει ή είναι ήδη σε λειτουργία στα κράτη μέλη. Επίσης θα βοηθήσουν να εξασφαλιστεί διασυνοριακή πρόσβαση σε αυτές τις υπηρεσίες και να αποφευχθεί ο κατακερματισμός της αγοράς των καινοτόμων υπηρεσιών και προϊόντων.

Οι δράσεις του πιλοτικού Β θα στηρίξουν την εφαρμογή και την υιοθέτηση των νέων καινοτόμων λύσεων που βασίζονται στις ΤΠΕ. Τα θεματικά δίκτυα θα υποστηρίξουν την ανταλλαγή εμπειριών και την επίτευξη συναίνεσης σχετικά με την εφαρμογή πολιτικής για τις ΤΠΕ.Στον πίνακα 2 παρουσιάζονται οι υπηρεσίες που ανακοινώθηκαν στην πρόσκληση για υποβολή προτάσεων για την υλοποίηση τους μέσα από το CIP ICT PSP το 2007.

**Πίνακας 2: Υπηρεσίες που περιλαμβάνονται στην πρόσκληση του CIP ICT PSP 2007**

| Themes and objectives | | Funding Instrument | Intended number of proposals to be funded |
|---|---|---|---|
| **Call for proposals** | | | |
| ***Theme 1 : Efficient and interoperable eGovernment services*** | | | |
| **1.1:** | **Enabling EU-wide public eProcurement** | ***Pilot Type A*** | 1 |
| **1.2:** | **Towards pan-European recognition of electronic IDs (eIDs)** | ***Pilot Type A*** | 1 |
| 1.3: | Innovative solutions for inclusive and efficient eGovernment | *Pilot Type B* | several |
| 1.4: | Experience sharing and consensus building in the uptake of innovative eGovernment services | *Thematic Network* | 3 |
| ***Theme 2 : ICT for accessibility, ageing and social integration*** | | | |
| 2.1: | ***Accessible digital Audiovisual (AV) systems*** | *Pilot Type B* | 1 |
| 2.2: | ICT for ageing | *Pilot Type B* | several |
| 2.3: | Experience sharing and consensus building in ICT for inclusion | *Thematic Network* | 3 |
| ***Theme 3: ICT for sustainable and interoperable health services*** | | | |
| **3.1:** | **EU wide implementation of eHealth services to support continuity of care: patient's summary and ePrescription** | ***Pilot Type A*** | 1 |
| 3.2: | Experience sharing and consensus building in eHealth | *Thematic Network* | 2 |
| ***Other themes and horizontal actions*** | | | |
| 4.1: | Experience sharing on ICT initiatives for SMEs | *Thematic Network* | up to 4 |
| 4.2: | Supporting sustainable growth | *Thematic Network* | 2 |
| 4.3: | Intelligent cars | *Thematic Network* | 1 |
| 4.4: | Privacy protection infrastructure | *Thematic Network* | 1 |

Τα βασικότερα από τα έργα (project) του CIP ICT PSP που ανέλαβαν να υλοποιήσουν υπηρεσίες που αφορούν την ΗΔ και τις δημόσιες υπηρεσίες αλλά και τις υπηρεσίες υγείας είναι τα παρακάτω (βλεπ. πίνακα 3):

**Πίνακας 3: Έργα του CIP ICT PSP για την ΗΔ, τις δημόσιες υπηρεσίες και τις υπηρεσίες υγείας**

| | |
|---|---|
| **ADD ME!** | **Activating Drivers for Digital eMpowerment in Europe** |
| **CEMSDI** | Civil-servants Empowerment for Multi-media Service Delivery ICT-enabled |
| **DIEGO** | Highly scalable Deployment model" of Inclusive E-Government |
| **e-CODEX** | e-CODEX: Justice Communication via Online Data Exchange |
| **ECRN** | European Civil Register Network |
| **EGOS** | e-Guidance and e-Government Services |
| **EGOV4U** | eGovernment for You |
| **iSAC6+** | A Unique European Citizens' Attention Service |
| **PEPPOL** | One step further towards cross-border public eProcurement in Europe |
| **RURAL-INCLUSION** | e-Government Lowering Administrative Burdens for Rural Businesses |
| **SPOCS** | Next generation Points of Single Contact |
| **epSOS** | Smart Open Services for European Patients |
| **STORK** | Secure Identity Across Borders Linked eID - easier access to public services across the EU |

### 3.1.1 Μεγάλης Κλίμακας Πιλοτικά Έργα (LSP)

Το υψηλό και αυξανόμενο ενδιαφέρον που δείχνουν τα ενδιαφερόμενα μέρη για τις πρωτοβουλίες που αναφερθήκαν παραπάνω και ιδιαίτερα οι δημόσιες αρχές από

διάφορες χώρες της ΕΕ οι οποίες και συμμετέχουν ενεργά σε πιλοτικά προγράμματα, είναι ένα θεμελιώδες βήμα προς την κατεύθυνση της λύσης των θεμάτων διαλειτουργικότητας και την ανάπτυξη πανευρωπαϊκών υπηρεσιών προς όφελος των επιχειρήσεων και των πολιτών. Τα έργα που για την υλοποίηση των υπηρεσιών βασιστήκαν σε υφιστάμενες τεχνικές λύσεις και υποδομές, και διασύνδεσανε τα συστήματα των κρατών μελών, έτσι ώστε να μπορούν να «μιλήσουν μεταξύ τους». Αυτό συμβάλλει στην ενίσχυση της εσωτερικής αγοράς και την ενίσχυση της ανταγωνιστικότητας της Ευρώπης μέσω μιας προσέγγισης από κάτω προς τα πάνω (bottom-up). Τα μεγάλης κλίμακας πιλοτικά έργα STORK[10], PEPPOL[11], SPOCS[12], epSOS[13] και e-CODEX [14] , είναι πέντε παραδείγματα σημαντικών πρωτοβουλιών που αναλήφθηκαν τα τελευταία χρόνια σε αυτό το πεδίο:

- Το STORK στόχευε στο να καταστήσει εφικτή τη διασυνοριακή ηλεκτρονική αναγνώριση, επιτρέποντας στους πολίτες και τις επιχειρήσεις να έχουν πρόσβαση υπηρεσίες ΗΔ σε κάθε κράτος μέλος στην οποία ζουν ή ταξιδεύουν.
- Το PEPPOL στόχευε στο να καταστήσει ευκολότερο για τις επιχειρήσεις να υποβάλουν προσφορές για συμβάσεις του δημόσιου τομέα οπουδήποτε στην ΕΕ με ένα απλούστερο και πιο αποτελεσματικό τρόπο. Το SPOCS να εγκαταστήσει Εθνικά Κέντρα Ενιαίας Επαφής (Points of Single Contact), π.χ. Υπηρεσίες μιας Στάσης (one -stop shops) για να διευκολύνει την επικοινωνία μεταξύ των επιχειρήσεων και των εθνικών δημόσιων διοικήσεων αλλά και να υποστηρίξει την ολοκλήρωση των διοικητικών διαδικασιών με ηλεκτρονικό τρόπο.
- Το epSOS στόχευε στο να καταστήσει ευκολότερο για τους ανθρώπους να λαμβάνουν ιατρική βοήθεια οπουδήποτε στην ΕΕ με την άρση των γλωσσικών, διοικητικών και τεχνικών εμποδίων.

[10] https://www.eid-stork.eu/index.php
[11] http://www.peppol.eu/
[12] http://www.eu-spocs.eu/
[13] http://www.epsos.eu/
[14] http://www.e-codex.eu/home.html

- Το eCODEX στόχευε στη βελτίωση της διασυνοριακής ανταλλαγής πληροφοριών που αφορούν δικαστικές διαδικασίες, στις οποίες εμπλέκονται πολίτες, επιχειρήσεις και κυβερνήσεις, με ένα ασφαλές, προσιτό και βιώσιμο τρόπο βελτιώνοντας παράλληλα την διαλειτουργικότητα μεταξύ των νομικών αρχών των κρατών της ΕΕ.

Τα πιλοτικά έργα εκτελέστηκαν σε μεγάλη έκταση από τα κράτη μέλη της ΕΕ και ανάπτυξαν πρακτικές λύσεις δοκιμασμένες σε πραγματικές περιπτώσεις χρήσης κυβερνητικών (δημόσιων) υπηρεσιών σε την όλη την Ευρώπη. Αυτές οι πρακτικές λύσεις θα βοηθήσουν στο να καταστήσουν τις κυβερνητικές διασυνοριακές υπηρεσίες πραγματικότητα. Θα διασφαλίσουν ώστε οι δημόσιες αρχές των διαφόρων χωρών της ΕΕ να μπορούν να «μιλήσουν ο ένας στον άλλο» ψηφιακά παρά τις διαφορετικές εθνικές τεχνικές ιδιαιτερότητες και τις γλώσσες. Τέλος, οι λύσεις αυτές θα καταργήσουν τα ψηφιακά σύνορα στην Ευρώπη και θα θέσουν τα θεμέλια για τη μελλοντική ευρωπαϊκή ανάπτυξη και ανταγωνιστικότητα

#### *3.1.1.1 e-CODEX (Communication via Online Data Exchange)*

Το e-CODEX είναι μια λειτουργία η οποία παρέχει έναν ευκολότερο (ψηφιακό) τρόπο για την ανταλλαγή νομικών πληροφοριών μεταξύ των χωρών της ΕΕ , μειώνοντας την γραφειοκρατία και προωθώντας την διαλειτουργικότητα στον χώρο των νομικών υπηρεσιών μεταξύ των χωρών της ΕΕ.

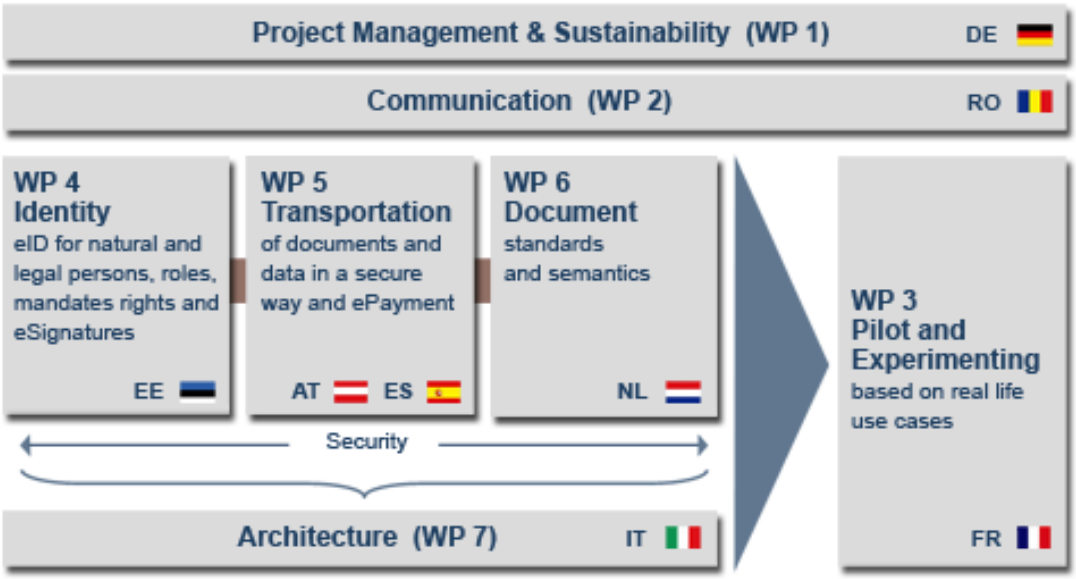
Ο στόχος του έργου είναι να συμβάλει στην υλοποίηση του Ευρωπαϊκού Νομικού Πλαισίου και στο Ευρωπαϊκό σχέδιο δράσης για την ηλεκτρονική δικαιοσύνη ( e-Justice) με σεβασμό στην αρχή της επικουρικότητας. Ακόμη, να συμβάλλει στην επίτευξη της διαλειτουργικότητας μεταξύ υφιστάμενων εθνικών δικαστικών συστημάτων και να ενεργοποιήσει όλα τα κράτη μέλη να συνεργαστούν για την επίτευξη ενός πιο αποτελεσματικού δικαστικού συστήματος στην Ευρώπη. Παράλληλα, στοχεύει στην βελτίωση της αποτελεσματικότητας και της αποδοτικότητας της επεξεργασίας του

αυξανόμενου αριθμού των διασυνοριακών νομικών ενεργειών και ιδανικότερα αυτών που σχετίζονται με αστικές, ποινικές και εμπορικές υποθέσεις. Στοχεύει επίσης να συμβάλλει στον εκσυγχρονισμό των δικαστικών συστημάτων στην Ευρώπη και να αυξήσει την συνεργασία μεταξύ αυτών.

**Το έργο e-CODEX αποτελείται από 7 πακέτα εργασίας [19]:**

- Πακέτο Εργασίας 1: Διαχείριση και Βιωσιμότητα του έργου (Project administration and sustainability)
- Πακέτο Εργασίας 2: Επικοινωνία (Communication)
- Πακέτο Εργασίας 3: Πιλοτικά προγράμματα και Πειραματισμός (Pilot and Experimenting)
- Πακέτο Εργασίας 4: Ηλεκτρονική υπογραφή και ηλεκτρονική ταυτοποίηση (e-Signature and e-Identity)
- Πακέτο Εργασίας 5: Ηλεκτρονική παράδοση εγγράφων και ηλεκτρονικές Πληρωμές (e-Delivery and e-Payment)
- Πακέτο Εργασίας 6: Έγγραφα και Σημασιολογία (Documents and Semantics)
- Πακέτο Εργασίας 7: Αρχιτεκτονική (Architecture)

Στο σχήμα 6 απεικονίζονται τα πακέτα εργασίας και η μεταξύ τους σχέσεις.




**Σχήμα 6: Τα πακέτα εργασίας του e-CODEX [19]**

Το πακέτο εργασίας 3 περιλαμβάνει 4 πιλοτικά προγράμματα που θα υποστηρίξουν τις πραγματικές περιπτώσεις χρήσης του χώρου του e-Justice π.χ. να στραφεί νομικά κάποιος κατά κάποιον σε άλλο κράτος μέλος ή να γίνει ανταλλαγή δεδομένων σε διασυνοριακές υποθέσεις μεταξύ των δικαστικών αρχών. Τα πιλοτικά προγράμματα που πρόκειται να αναπτυχθούν στο έργο είναι:

- Μικρής έκτασης Αγωγές (Small Claims)
- Ευρωπαϊκή διαδικασία για Διαταγή Πληρωμών (The European procedure for Payment Order (EPO))
- Ευρωπαϊκό Ένταλμα Σύλληψης (The European Arrest Warrant)
- Ασφαλή διασυνοριακή ανταλλαγή ευαίσθητων δικαστικών δεδομένων (Secure cross-border exchange of sensitive juducial data)
- Αμοιβαία Αναγνώριση Οικονομικών Προστίμων (Mutual Recognition of Financial Penalties)

Τα πιλοτικά αυτά εμπλέκουν ένα ευρύ φάσμα τεχνολογιών συμπεριλαμβανομένων των μορφών και προτύπων (formats and standards) για τα έγγραφα, την ασφάλεια των πληροφοριών, την ασφαλή ηλεκτρονική ταυτοποίηση, τις ψηφιακές υπογραφές, την

παράδοση εγγράφων με ηλεκτρονικό τρόπο (e-delivery) και τις τεχνολογίες σημασιολογίας.

#### *3.1.1.2 epSOS (European Patients Smart Open Services (e-health))*

Το epSOS έχει ως στόχο να σχεδιάσει, να κατασκευάσει και να αξιολογήσει μια υποδομή υπηρεσιών η οποία θα αναδεικνύει τη διασυνοριακή διαλειτουργικότητα μεταξύ των συστημάτων των ηλεκτρονικών μητρώων υγείας στην Ευρώπη [20].

Μέσα από το epSOS θα επιχειρηθεί να γίνει εφικτή η προσφορά αδιάλειπτης υγειονομικής περίθαλψης προς τους ευρωπαίους πολίτες. Οι βασικοί στόχοι είναι η βελτίωση της ποιότητας και ασφάλειας της υγειονομικής περίθαλψης των πολιτών όταν ταξιδεύουν σε κάποια άλλη Ευρωπαϊκή χώρα. Επιπλέον, γίνεται προσπάθεια για την ανάπτυξη ενός πρακτικού πλαισίου ηλεκτρονικής υγείας και υποδομών ΤΠΕ που θα επιτρέπουν την ασφαλή πρόσβαση των ασθενών σε πληροφορίες για την υγεία μεταξύ των διαφόρων ευρωπαϊκών συστημάτων υγειονομικής περίθαλψης. Το epSOS μπορεί να συμβάλλει σημαντικά στην ασφάλεια των ασθενών από τη μείωση της συχνότητας των ιατρικών σφαλμάτων και δυνατότητα γρήγορης πρόσβασης σε έγγραφα τεκμηρίωσης (documentation). Σε καταστάσεις έκτακτης ανάγκης, αυτή η τεκμηρίωση παρέχει στο ιατρικό προσωπικό σωτήριες πληροφορίες για τους ασθενείς και να μειώσει την άσκοπη μερικές φορές επανάληψη διαγνωστικών διαδικασιών

Το έργο χωρίζεται σε δύο φάσεις σε κάθε μία από τις οποίες θα υλοποιηθούν οι παρακάτω υπηρεσίες:

Στην πρώτη φάση:

- Συνοπτικό Ιατρικό Ιστορικό Ασθενούς (Patient Summary): πρόσβαση σε σημαντικά ιατρικά δεδομένα για την θεραπεία των ασθενών.
- Διασυνοριακή χρήση των Ηλεκτρονικών Συνταγών (Συστήματα ηλεκτρονικής συνταγογράφησης)

Το Συνοπτικό Ιατρικό Ιστορικό Ασθενούς στα πλαίσια του epSOS αναφέρεται σε ένα σύνολο στοιχείων που περιέχει:

- γενικές πληροφορίες για τον ασθενή (π.χ. όνομα, ηλικία)
- ένα ιατρικό φάκελο που αποτελείται από τα πιο σημαντικά κλινικά δεδομένα του ασθενή (π.χ. αλλεργίες, τρέχοντα ιατρικά προβλήματα, ιατρικά εμφυτεύματα, μεγάλες χειρουργικές επεμβάσεις κατά τη διάρκεια των τελευταίων έξι μηνών κλπ.)
- ένα φαρμακευτικό φάκελο όπου αναγράφονται όλα τα τρέχοντα φάρμακα που αφορούν τον ασθενή

Οι υπηρεσίες Ηλεκτρονικών Συνταγών (ePrescription and eDispensation) αφορούν τη συνταγογράφηση των φαρμάκων μέσω χρήσης λογισμικού και την ηλεκτρονική διαβίβαση της συνταγής από το Παραπέμποντα (επαγγελματία υγειονομικής περίθαλψης), στο Διανεμητή (π.χ., φαρμακείο), όπου η συνταγή ανακτάται ηλεκτρονικά, το φάρμακο χορηγείται στον ασθενή (eDispensation), και οι πληροφορίες σχετικά με το χορηγούμενο φάρμακο διαβιβάζονται ηλεκτρονικά. Η διαλειτουργικότητα μεταξύ των εθνικών συστημάτων είναι αναγκαία στην περίπτωση ενός ασθενή χρειάζεται κάποιο φάρμακο το οποίο έχει ήδη συνταγογραφηθεί στη χώρα καταγωγής του και πάει σε μια άλλη χώρα. Σε αυτή την περίπτωση ο φαρμακοποιός πρέπει να είναι να έχει ηλεκτρονική πρόσβαση στη συνταγή, και όταν το φάρμακο χορηγηθεί, το σύστημα υγειονομικής περίθαλψης της χώρας του ασθενούς θα πρέπει να ενημερώνεται σχετικά με τα διανεμημένο φάρμακο.

Σε μια δεύτερη φάση (φάση της διεύρυνσης epSOS) θα υλοποιηθούν οι παρακάτω υπηρεσίες:

- Ενσωμάτωση των υπηρεσιών του ενιαίου Ευρωπαϊκού Αριθμού Έκτακτης Ανάγκης ( EU-wide Emergency Number) 112
- Ενσωμάτωση της Ευρωπαϊκής Κάρτας Ασφάλισης Ασθένειας (European Health Insurance Card (EHIC))
- Πρόσβαση των Ασθενών στα δεδομένα τους

#### *3.1.1.3 STORK (Secure idenTity acrOss boRders linked)*

Η διασυνοριακή αυθεντικοποίηση χρηστών θα εφαρμοστεί και θα δοκιμαστεί από το έργο με τη βοήθεια πέντε πιλοτικών έργων που θα χρησιμοποιήσουν τις υπάρχουσες κυβερνητικές υπηρεσίες σε κράτη μέλη της ΕΕ. Στην συνέχεια θα συνδεθούν με την πλατφόρμα επιπλέον πάροχοι υπηρεσιών αυξάνοντας έτσι τον αριθμό των διασυνοριακών υπηρεσιών που προσφέρονται στους ευρωπαίους χρήστες [21].

Ο ρόλος της πλατφόρμας STORK είναι να αναγνωρίσει έναν χρήστη που βρίσκεται σε μια σύνοδο με κάποιο φορέα παροχής υπηρεσιών και να αποστείλει τα δεδομένα του σε αυτή την υπηρεσία. Εάν ο πάροχος υπηρεσιών ζητήσει επιπλέον δεδομένα , ο χρήστης έχει τον έλεγχο της αποστολής των δεδομένα αυτών. Η ρητή συγκατάθεση του ιδιοκτήτη των δεδομένων δηλαδή του χρήστη, απαιτείται πάντοτε πριν από την αποστολή των δεδομένων του στο φορέα παροχής υπηρεσιών. Αυτή η προσέγγιση με επίκεντρο τον χρήστη (user centric approach) υιοθετήθηκε για να καλύψει τις νομικές απαιτήσεις από τις διάφορες χώρες οι οποίες συμμετείχαν στο έργο και υποχρέωναν στην λήψη σαφών μέτρων για την διασφάλιση και τον σεβασμό των θεμελιωδών δικαιωμάτων των πολιτών, όπως η προστασία της ιδιωτική τους ζωής.

Υπάρχουν διαφορετικές προσεγγίσεις για την εφαρμογή της ηλεκτρονικής ταυτοποίησης στις διάφορες χώρες της ΕΕ. Οι περισσότερες χώρες έχουν ήδη αναπτύξει εθνικές ηλεκτρονικές κάρτες του πολίτη, ενώ κάποιες άλλες χρησιμοποιούν απλούστερες μεθόδους οι οποίες βασίζονται στην χρήση ονόματος και κωδικού πρόσβασης και σε κάποιες περιπτώσεις με την σύγχρονη χρήση κάποιου επιπλέον μηχανισμού ταυτοποίησης. Στόχος του STORK δεν είναι να αντικαταστήσει τις ταυτότητες αυτές, αλλά να συνδέσει όλες αυτές τις διαφορετικές προσεγγίσεις ταυτοποίησης με διαφάνεια και με τρόπο τέτοιο ώστε να μπορούν οι χρήστες να υποβάλουν τα πιστοποιημένα προσωπικά τους δεδομένα σε διοικήσεις άλλων χωρών.

Το έργο STORK δοκίμασε την πλατφόρμα διαλειτουργικότητας μέσω της εφαρμογής πέντε πιλοτικών προγραμμάτων, τα οποία μέσα από την πλατφόρμα του STORK

ενσωματώθηκαν σε ήδη υπάρχουσες εφαρμογές και δοκιμάστηκαν σε πραγματικές συνθήκες λειτουργίας.

Τα πιλοτικά προγράμματα μέσα από τα οποία έγιναν δοκιμάστηκε η λειτουργία και η διαλειτουρικότητα της πλατφόρμας του STORK σε πραγματικές συνθήκες παρείχαν τις παρακάτω υπηρεσίες:

- Cross-border Authentication Platform for Electronic Services
- Λειτουργία διασυνοριακών ηλεκτρονικών υπηρεσιών σε διάφορα κράτη μέλη μέσω των εθνικών πυλών τους.
- Ασφαλέστερη συνομιλία μέσω διαδικτύου (safer chat): Προώθηση της ασφαλούς χρήσης του Διαδικτύου από τα παιδιά και τους νέους
- Κινητικότητα φοιτητών (Student mobility): Διευκόλυνση των πολιτών που θέλουν να σπουδάσουν σε άλλο κράτος μέλος
- Παράδοση Εγγράφων (eDelivery): Ανάπτυξη διασυνοριακών μηχανισμών για ασφαλείς online παράδοση των εγγράφων
- Αλλαγή Διεύθυνση (Change of Address): Παροχή βοήθειας στους πολίτες της ΕΕ κυκλοφορούν και να εγκατασταθούν σε άλλες χώρες της ΕΕ
- European Commission Authentication Service (ECAS): Ενσωμάτωση του STORK με την Υπηρεσία Αυθεντικοποίησης της Ευρωπαϊκής Επιτροπής για πρόσβαση στις εφαρμογές της Ευρωπαϊκής Επιτροπής.

Το STORK ολοκληρώθηκε με επιτυχία το 2011. Το 2012 ως συνέχεια του STORK και με στόχο την αύξηση του αριθμού των παρεχόμενων υπηρεσιών μέσω της ήδη πλέον εγκαθιδρυμένης και δοκιμασμένης πλατφόρμας διασυνοριακής ταυτοποίησης ξεκίνησε το πιλοτικό έργο STORK 2. Το STORK 2 θα παρέχει υπηρεσίες Ηλεκτρονικής Τραπεζικής (e-banking), αναγνώρισης επαγγελματικών και ακαδημαϊκών προσόντων (job and academic qualifications), ηλεκτρονικής μάθησης (e-learning) καθώς και υπηρεσίες προς τις επιχειρήσεις και ηλεκτρονικές παροχές για την υγεία (e-health).

### *3.1.1.4 PEPPOL (Pan-European Public Procurement Online)*

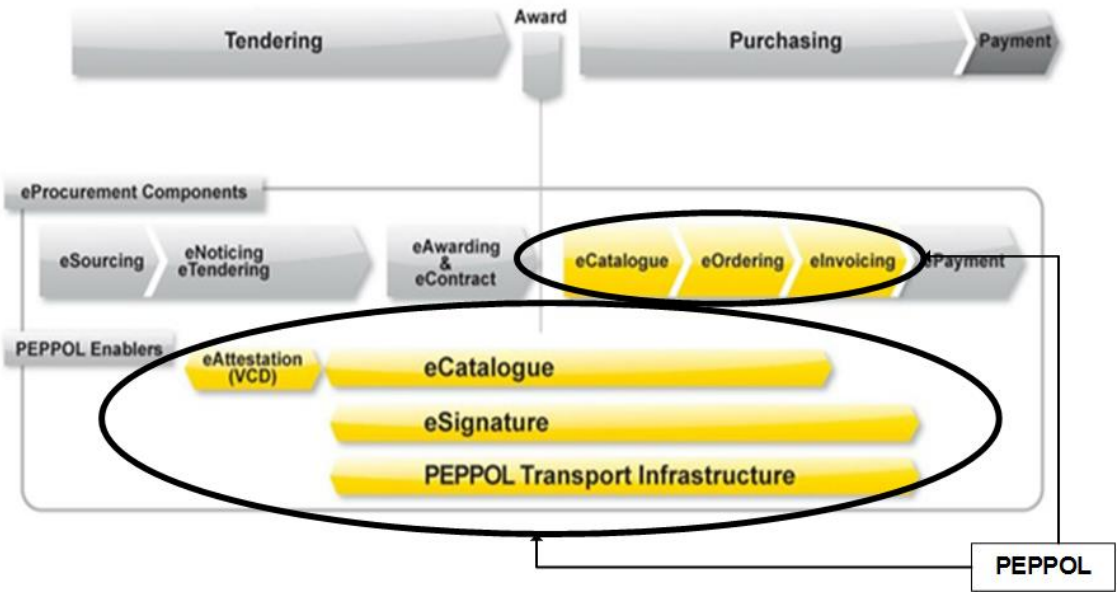
Το PEPPOL παρέχει πρόσβαση στην βασιζόμενη σε πρότυπα πληροφοριακής υποδομής ή επικοινωνίας του (IT transport infrastructure), από συγκεκριμένα σημεία πρόσβασης, παρέχοντας υπηρεσίες για τις ηλεκτρονικές δημόσιες συμβάσεις οι οποίες είναι σε τυποποιημένη ηλεκτρονική μορφή. Το PEPPOL στοχεύει στην παροχή της δυνατότητας στις επιχειρήσεις να επικοινωνούν ηλεκτρονικά με οποιοδήποτε θεσμικό όργανο της κυβέρνησης για ότι σχετίζεται με τις διαδικασίες σύναψης δημοσίων συμβάσεων καθώς και στην αύξηση της αποτελεσματικότητας και της μείωσης του κόστους των συμβάσεων. Μέσω συμφωνίας σχετικά με τις προδιαγραφές για τις διασυνοριακές διαδικασίες δημόσιων συμβάσεων, το πιλοτικό έργο της Ευρωπαϊκής Επιτροπής PEPPOL έχει σκοπό να συμβάλει στην ανάπτυξη μίας πανευρωπαϊκής πληροφοριακής υποδομής βασιζόμενη σε πρότυπα. Το PEPPOL θα στηριχτεί πάνω στα υφιστάμενα εθνικά πληροφοριακά συστήματα ηλεκτρονικών προμηθειών και με τη χρήση των ΤΠΕ θα δώσει την δυνατότητα σε αυτά να επικοινωνούν μεταξύ τους.

Το PEPPOL διευκολύνει τις διαδικασίες πριν και μετά την ανάθεση (pre-award, post-award) μιας προσφοράς με τυποποιημένα εργαλεία εστιάζοντας στις πιο πολύπλοκες διαδικασίες των ηλεκτρονικών συμβάσεων. Στο σχήμα 7 απεικονίζονται οι διαδικασίες των ηλεκτρονικών συμβάσεων και επισημαίνονται οι διαδικασίες στις οποίες εστιάζει το PEPPOL. Στην προ-ανάθεση φάση, το έργο PEPPOL υποστηρίζει τη διαδικασία της δημόσιας σύμβασης με:

- Την επικύρωση των Ηλεκτρονικών Υπογραφών (e-Signature) που βασίζονται σε ηλεκτρονικά πιστοποιητικά τα οποία εκδίδονται από τις αρμόδιες αρχές
- Έναν Εικονικό Φακέλο Εταιρείας (Virtual Company Dossier) για την υποβολή τυποποιημένων πληροφοριών της εταιρείας (αποδείξεις, πιστοποιητικά και βεβαιώσεις)
- Έναν Ηλεκτρονικό Κατάλογο (e-Catalogue) για την υποβολή προσφορών σχετικά με προϊόντα και υπηρεσίες σε τυποποιημένη μορφή

Στην μετά-ανάθεση φάση, το έργο PEPPOL υποστηρίζει τη διαδικασία της δημόσιας σύμβασης με [22]:

- Τον Ηλεκτρονικό Κατάλογο (e-Catalogue) για την ανταλλαγή πληροφοριών σχετικά με τα αγαθά και τις υπηρεσίες που προσφέρονται στο πλαίσιο της σύμβασης
- Τις Ηλεκτρονικές Παραγγελίες και την Ηλεκτρονική Τιμολόγηση (eOrders και eInvoicing) παρέχοντας στον αγοραστή και τους προμηθευτές καθορισμένες διαδικασίες με σκοπό να μπορούν να μοιραστούν κοινές επιχειρηματικές πληροφορίες.
- Την Υποδομή Μεταφορών (Transport Infrastructure), τη βάση όλων των μετά την ανάθεση υπηρεσιών που παρέχονται από το PEPPOL, η οποία βασίζεται σε κοινές, συμβατές με τα εθνικά πρότυπα τεχνολογίες πληροφοριών και διασύνδεει τις κοινότητες των ηλεκτρονικών συμβάσεων (e-Procurement communities).




**Σχήμα 7: Ανάλυση των δομικών στοιχείων των Ηλεκτρονικών Συμβάσεων και απεικόνιση των εργαλείων του PEPPOL**

#### *3.1.1.5 SPOCS (Simple Procedures Online for Cross- Border Services)*

Το πρόγραμμα SPOCS επικεντρώνεται στην ανάπτυξη της επόμενης γενιάς πυλών (portals) των Ενιαίων Κέντρων Εξυπηρέτησης (Point of Single Contact) τα οποία κάθε ευρωπαϊκή χώρα έχει εγκατεστημένα, μέσω της υλοποίησης και διάθεσης υψηλού αντίκτυπου διασυνοριακών ηλεκτρονικών διαδικασιών.

Τα Ενιαία Κέντρα Εξυπηρέτησης (ΕΚΕ) δημιουργήθηκαν με σκοπό να εφαρμοστεί η κοινοτική Οδηγία για τις Υπηρεσίες (Service Directive) στην ενιαία αγορά[15] [23]. Η Οδηγία για τις Υπηρεσίες εγκρίθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο στις 12 Δεκεμβρίου 2006. Έπρεπε να υιοθετηθεί και να μεταφερθεί πλήρως από τα κράτη μέλη στα εθνικά τους συστήματα μέχρι τις 28 Δεκεμβρίου 2009. Η κοινοτική οδηγία για τις υπηρεσίες απαιτεί μεταξύ άλλων όλες οι απαιτούμενες διαδικασίες που αφορούν την ίδρυση μιας επιχείρησης και την παροχή υπηρεσιών σε κάποια άλλη χώρα της ΕΕ να γίνονται εξολοκλήρου ηλεκτρονικά μέσω διαδικτύου. Ο στόχος της Οδηγίας για τις Υπηρεσίες είναι να απελευθερώσει τις ανεκμετάλλευτο δυναμικό της αγοράς των προσφερόμενων υπηρεσιών στην Ευρώπη, με την άρση των νομικών και διοικητικών εμποδίων στις συναλλαγές στον τομέα των υπηρεσιών. Τα μέτρα απλούστευσης που προβλέπονται από την οδηγία στοχεύουν να αυξήσουν σημαντικά τη διάρκεια ζωής των Μικρομεσαίων Επιχειρήσεων και τη διαφάνεια γύρω από αυτές και τους καταναλωτές κατά την παροχή την κατανάλωση υπηρεσιών στην ενιαία αγορά (Single Market).

Τα οφέλη που αναμένεται να προκύψουν μέσα από την υλοποίηση του προγράμματος SPOCS είναι η μείωση της γραφειοκρατίας, η αύξηση της διαφάνειας, η απλοποίηση και ο εκσυγχρονισμός των διοικητικών υπηρεσιών. Ακόμη, θα προσφέρει νέες επιχειρηματικές ευκαιρίες στον δημόσιο τομέα και θα προωθήσει καινοτόμα προϊόντα πληροφορικής τα οποία θα βασίζονται στα ανοικτά πρότυπα.

[15] http://ec.europa.eu/internal_market/services/services-dir/index_en.htm

Ο στόχος του έργου SPOCS είναι να δημιουργήσει μία πλατφόρμα διαλειτουργικότητας διευκολύνοντας τους παρόχους υπηρεσιών να αιτούνται και να συναλλάσσονται μέσω των ενιαίων κέντρων εξυπηρέτησης τα οποία έχουν δημιουργηθεί για τις επιχειρήσεις από τα κράτη μέλη της ΕΕ. Μέσα από το έργο θα αναπτυχθούν τα κατάλληλα δομικά στοιχεία (building blocks) για την υλοποίηση της πλατφόρμας αυτής. Στην συνέχεια θα πρέπει να εξακριβωθεί και να δειχτεί ότι τα δομικά στοιχεία που αναπτύσσονται μέσα από το πρόγραμμα SPOCS και τα οποία συνθέτουν αυτό το πλαίσιο διαλειτουργικότητας είναι όντως λειτουργικά στο πραγματικό περιβάλλον δραστηριοποίησης των επιχειρήσεων. Τα δομικά στοιχεία που συνθέτουν τη πλατφόρμα αυτή σχετίζονται με τις ηλεκτρονικές διαδικασίες που προσφέρονται από τα Ενιαία Κέντρα Εξυπηρέτησης και είναι τα εξής [24]:

1. Πληροφόρηση (Syndication): σχετίζεται με την ενημέρωση του τελικού χρήστη του ΕΚΕ σχετικά με τα απαραίτητα έγγραφα που πρέπει να υποβληθούν.

2. Ηλεκτρονικές Υπηρεσίες (eServices): αφορά την βελτίωση των παρεχόμενων ηλεκτρονικών υπηρεσιών

3. Ηλεκτρονική Ασφάλεια (eSafe): αφορά την ασφαλή αποθήκευση και ανάκτηση εγγράφων από τον πάροχο υπηρεσιών

4. Ηλεκτρονική Παράδοση (eDelivery): σχετίζεται με την ανταλλαγή εγγράφων με ασύγχρονο τρόπο.

5. Ηλεκτρονικά Έγγραφα (eDocuments): αφορά στην παρουσίαση, υπογραφή και ανταλλαγή ηλεκτρονικών εγγράφων

Η διαδικασία που ακολουθείται από το SPOCS ώστε να φτάσει στο στάδιο της δοκιμής σε πραγματικό περιβάλλον είναι η παρακάτω:

1) Καθορισμός των δομικών στοιχείων του SPOCS (Syndication, eDocuments, eDelivery, eSafe και eServices).
2) Κατασκευή των δομικών στοιχείων με βάση τις προδιαγραφές τους.
3) Ανάπτυξη αυτών στις χώρες που συμμετέχουν στο πιλοτικό πρόγραμμα.

4) Αξιολόγηση των αποτελεσμάτων και προσαρμογή των προδιαγραφών και των παραγόμενων μονάδων λογισμικού όπου αυτό είναι απαραίτητο.
5) Κλιμάκωση και Διατήρηση (Scaling and Sustaining) των δομικών στοιχείων του πιλοτικού.

**Το πιλοτικό έργο χωρίζεται στα ακόλουθα πακέτα εργασιών:**

- Πακέτο Εργασίας 1: Διάθεση Πληροφοριών (Content Syndication), ζητήματα πολυγλωσσίας και λεξιλόγιο
- Πακέτο Εργασίας 2: Ηλεκτρονικά Έγγραφα (eDocuments)
- Πακέτο Εργασίας 3: Διαλειτουργική Παράδοση, eSafe, ασφαλείς και διαλειτουργικές συναλλαγές και αποδείξεις παραλαβής.
- Πακέτο Εργασίας 4 : Καταλόγοι Διαλειτουργικών Ηλεκτρονικών Υπηρεσιών (eServices)
- Πακέτο Εργασίας 5: Πειραματισμός
- Πακέτο Εργασίας 6: Αύξηση της Ευαισθητοποίησης, διάδοση, εμπλοκή των ενδιαφερομένων ομάδων και καλλιέργεια κοινοτήτων πρακτικής.
- Πακέτο Εργασίας 7: Διαχείριση / Διοίκηση του Έργου

Μέσα από το πακέτο εργασίας 5 θα γίνουν οι δοκιμές σε πραγματικό περιβάλλον. Για το σκοπό αυτό έχουν οριστεί να προσφερθούν διασυνοριακά οι εξής υπηρεσίες:

- Μεσιτικού Γραφείου (Real Estate)
- Τουριστικού Πράκτορα (Travel Agent)
- Εργολάβου Οικοδομών (Master Builder)
- Αρχιτέκτονα (Architect).

Στο σχήμα 8 απεικονίζονται τα πακέτα εργασίας καθώς και η μεταξύ τους σχέση.


**Σχήμα 8: Ανάλυση του έργου SPOCS στα πακέτα εργασίας**

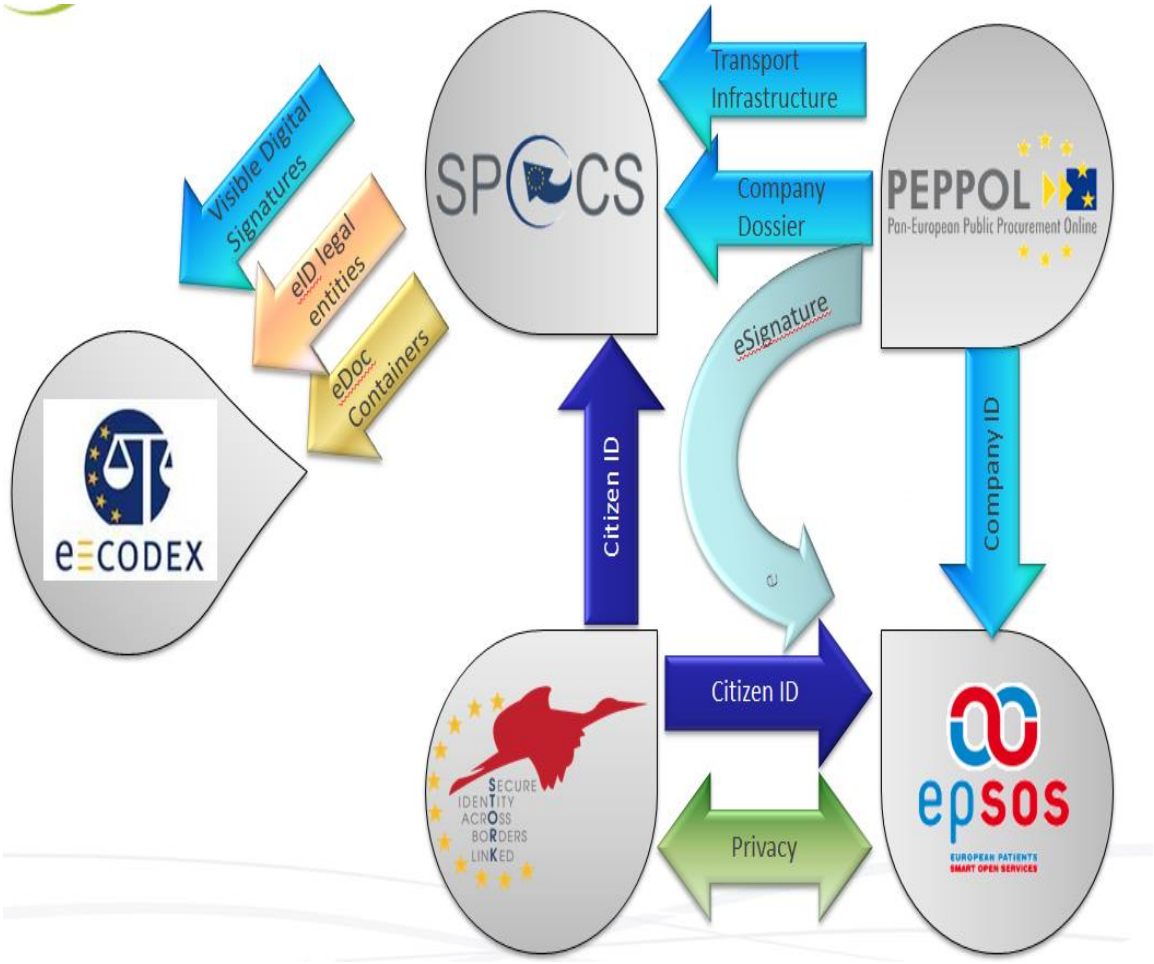
### *3.1.1.6 Συνεργασία/αλληλεπίδραση LSPs*

Τα πέντε παραπάνω προγράμματα σχετίζονται μεταξύ τους και ανταλλάσουν πληροφορίες αλλά και δομικά στοιχεία. Στον παρακάτω πίνακα 4 απεικονίζονται τα δομικά στοιχεία που είναι απαραίτητα για την παροχή των προαναφερόμενων διασυνοριακών υπηρεσιών και τα προγράμματα τα οποία ασχολούνται με αυτά.

**Πίνακας 4: Συσχέτιση δομικών στοιχείων και πιλοτικών έργων**

| Υπηρεσία | Σχετιζόμενο Πιλοτικό Έργο |
|---|---|
| **e-ID** | STORK, STORK 2.0 |
| **e-Signatures** | PEPPOL |
| **e-Documents** | PEPPOL, SPOCS |
| **e-Delivery** | PEPPOL, SPOCS, e-CODEX |
| **Privacy** | epSOS |

Όπως είναι εμφανές, από τα πέντε αυτά μεγάλα πιλοτικά έργα, το έργο STORK είναι αυτό το οποίο παρέχει αποκλειστικά τις υπηρεσίες ηλεκτρονικής ταυτοποίησης αλλά και ιδιωτικότητας σε συνεργασία με το epSOS. Όσον αφορά τις υπόλοιπες υπηρεσίες το PEPPOL είναι αυτό το οποίο παρέχει τις απαιτούμενες υπηρεσίες ηλεκτρονικής υπογραφής, ενώ σε μαζί με τα SPOCS ασχολείται με τις υπηρεσίες των ηλεκτρονικών εγγράφων και ηλεκτρονικής παράδοσης. Η υπηρεσία ηλεκτρονικής παράδοσης εγγράφων παρέχεται από τα έργα PEPPOL, SPOCS και e-CODEX. Η συνεργασία και αλληλεπίδραση των έργων απεικονίζεται στο σχήμα 9.




**Σχήμα 9: Αλληλεπίδραση μεταξύ των LSPs**

## 3.2 Σύστημα Πληροφόρησης για την Εσωτερική Αγορά

Η Ευρωπαϊκή Επιτροπή χρηματοδότησε μέσω του προγράμματος IDABC το σύστημα Πληροφόρησης για την Εσωτερική Αγορά IMI (Internal Market Information) το οποίο και ανέπτυξε σε συνεργασία με τα κράτη μέλη. Μετά την ολοκλήρωση του IBAC τον Δεκέμβριο του 2009, την χρηματοδότηση του έργου ανέλαβε το πρόγραμμα ISA[16]. Αρχικά, υιοθετήθηκε από τα κράτη μέλη με την απόφαση 2008/49/ΕΚ («κανονισμός IMI») και στην συνέχεια από τον κανονισμό με 1024/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου [25]. Στόχος της πρωτοβουλίας αυτής είναι να βοηθήσει τα κράτη μέλη κατά την πρακτική εφαρμογή των απαιτήσεων ανταλλαγής πληροφοριών, οι οποίες καθορίζονται στις πράξεις της ΕΕ, παρέχοντας έναν κεντρικό μηχανισμό επικοινωνίας που να διευκολύνει τη διασυνοριακή ανταλλαγή πληροφοριών. Συγκεκριμένα, το IMI βοηθά τις αρμόδιες αρχές να εντοπίζουν την ομόλογη αρχή άλλου κράτους μέλους, να διαχειρίζονται την ανταλλαγή πληροφοριών, συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα, βάσει απλών και ενοποιημένων διαδικασιών και να υπερβαίνουν τα γλωσσικά εμπόδια με τη βοήθεια προκαθορισμένων και εκ των προτέρων μεταφρασμένων ροών εργασίας. Είναι ένα από τα βασικά εργαλεία της ενιαίας αγοράς και συμπράττει στην εφαρμογή της Ευρωπαϊκής οδηγίας 2005/36/EC (Professional Qualifications Directive (2005/36/EC))[26] για την αναγνώριση των επαγγελματικών προσόντων καθώς και της οδηγίας για τις υπηρεσίες 2006/123/EC (Service Directive)[23].

Το IMI το χρησιμοποιούν εθνικές, περιφερειακές και τοπικές αρχές στην ΕΕ, την Ισλανδία, το Λιχτενστάιν και τη Νορβηγία, οι οποίες είναι αρμόδιες για τη νομοθεσία που υποστηρίζει η εφαρμογή. Σε κάθε κράτος που χρησιμοποιεί το IMI έχει οριστεί ένας εθνικός συντονιστής NIMIC (National IMI Coordinator) ο οποίος ανήκει σε κάποιο εθνικό υπουργείο και είναι υπεύθυνος για την ομαλή λειτουργία του σε εθνικό επίπεδο. Οι τελικοί χρήστες της εφαρμογής είναι οι αρμόδιες αρχές ή φορείς του

[16] http://ec.europa.eu/isa/

δημοσίου που εμπλέκονται στην εφαρμογή της νομοθεσίας της ενιαίας αγοράς. Στο IMI μπορούν να καταχωρίζονται μόνο αυτές οι αρχές και η καταχώρισή τους θα πρέπει να εγκρίνεται από συντονιστή IMI.

Το IMI βοηθά τους χρήστες:

- Να βρουν τη σωστή αρχή με την οποία θα επικοινωνήσουν σε άλλο κράτος μέλος και
- Να επικοινωνήσουν μαζί της χρησιμοποιώντας τυποποιημένες προμεταφρασμένες ομάδες ερωτήσεων και απαντήσεων.

Οπότε, αν μια Ελληνική Αρχή χρειάζεται πληροφορίες από έναν Ιταλικό φορέα μπορεί να επιλέξει μια ερώτηση στα Ελληνικά. Η Ιταλική Αρχή θα δει την ερώτηση και τις προτεινόμενες απαντήσεις της στα Ιταλικά, η Ελληνική αρχή όμως θα λάβει την απάντησή της στα Ελληνικά.

Επειδή τα κράτη μέλη συνεργάστηκαν για τη διαμόρφωση του συστήματος, το IMI εξασφαλίζει ομοιόμορφες μεθόδους εργασίας που έχουν συμφωνηθεί από όλα τα κράτη μέλη της ΕΕ. Ωστόσο, σε περίπτωση που προκύψουν διαφορές, μπορούν να παρέμβουν οι εθνικοί συντονιστές IMI για την επίλυση του προβλήματος.

Υπεύθυνη για την συντήρηση και την ανάπτυξη του εργαλείου αλλά και για τις υπηρεσίας βοήθειας και την εκπαίδευση των χρηστών, είναι η Ευρωπαϊκή Επιτροπή. Ακόμη, στα καθήκοντά της περιλαμβάνεται και η διαχείριση και υποστήριξη του δικτύου των συντονιστών IMI καθώς και η προώθηση της περαιτέρω επέκτασης του IMI. Επιπλέον, όταν υπάρχει δυνατότητα, η Ευρωπαϊκή Επιτροπή οφείλει παρέχει στους χρήστες του IMI κάθε πρόσθετη μεταφραστική λειτουργικότητα που ανταποκρίνεται στις ανάγκες τους, είναι συμβατή με τις απαιτήσεις ασφάλειας και εμπιστευτικότητας για την ανταλλαγή πληροφοριών στο IMI και μπορεί να παρασχεθεί σε λογικό κόστος.

# Κεφάλαιο 4: Πανευρωπαϊκά Πληροφοριακά Συστήματα Ειδικού Σκοπού

Η τεχνολογία μπορεί να διαδραματίσει καίριο ρόλο στη βελτίωση και την ενίσχυση των εξωτερικών συνόρων αλλά και την καλύτερη εμπορική συνεργασία μεταξύ των χωρών μελών τη ΕΕ. Κατά τα τελευταία χρόνια, η ΕΕ έχει αναπτύξει μεγάλης κλίμακας πληροφοριακά συστήματα για τη συλλογή, επεξεργασία και ανταλλαγή πληροφοριών σχετικά με τη διαχείριση των εξωτερικών συνόρων και τις εμπορικές συναλλαγές. Το πληροφορικό σύστημα Schengen (Schengen Information System (SIS))[27], το οποίο πήρε το όνομα του από μία μικρή επαρχιακή πόλη του Λουξεμβρούργου, το Σύστημα Πληροφοριών για τις Θεωρήσεις (Visa Information System (VIS))[28] και το Πληροφοριακό Σύστημα Τελωνείων ηλεκτρονικά τελωνεία (Customs Information System (CIS))[29], τα οποία υποστηρίζονται από την εφαρμογή αντίστοιχων κοινών πολιτικών της ΕΕ, είναι μερικά από αυτά τα εργαλεία.

## 4.1 Schengen information system

### 4.1.1 Πληροφοριακό Σύστημα Schengen (SIS)

Τον Ιούνιο του 1984, το Ευρωπαϊκό Συμβούλιο ανακοίνωσε ότι θα έπρεπε να καταργηθούν η αστυνόμευση και οι τελωνειακές διατυπώσεις για τα αγαθά και τα άτομα που διασχίζουν ενδοκοινοτικά σύνορα. Τρεις εβδομάδες αργότερα, στις 13 Ιουλίου 1984, η Γερμανία και η Γαλλία σύναψαν μια συμφωνία προς την κατεύθυνση αυτήν. Στις 14 Ιουνίου 1985, τρείς χώρες ακόμη το Βέλγιο, το Λουξεμβούργο και η Ολλανδία ακολούθησαν την Γερμανία και την Γαλλία στις προσπάθειες τους για κατάργηση των συνόρων. Οι πέντε αυτές χώρες υπέγραψαν στο Schengen (Σένγκεν), συμφωνία για την σταδιακή κατάργηση των ελέγχων στα κοινά τους σύνορα. Η κατάργηση των ελέγχων αναφερόταν και σε πρόσωπα και σε αγαθά[30] .

Η κατάργηση των ελέγχων στα πρόσωπα θα ήταν μια σημαντική πρόοδος για την ελεύθερη μετακίνηση των πολιτών που ορίζεται από την οδηγία για την επίτευξη της Ενιαίας Αγοράς (Internal Market). Ακόμη, η συμφωνία αυτή σχετιζόταν με την εγκαθίδρυση μιας κοινής πολιτικής ασφάλειας στην ΕΕ και εδραίωσης σχέσεων εμπιστοσύνης μεταξύ των κρατών μελών.

Στις 19 Ιουνίου το 1990 υπογράφηκε από τα πέντε κράτη τα οποία είχαν υπογράψει και την σχετική συμφωνία η Σύμβαση για την εφαρμογής της Συμφωνίας Schengen η οποία άρχισε να ισχύει το 1995 και επέτρεψε την κατάργηση των ελέγχων στα εσωτερικά σύνορα μεταξύ των χωρών που την είχαν υπογράψει. Με τη σύμβαση αυτή δημιουργήθηκαν ενιαία εξωτερικά σύνορα, όπου πραγματοποιούνται έλεγχοι εισόδου στον χώρο Schengen, σύμφωνα με τις ίδιες διαδικασίες και με κοινούς κανόνες.

Παρά την κατάργηση των ελέγχων στα εσωτερικά σύνορα του χώρου του Σένγκεν, επιτρέπεται ο έλεγχος κάθε ατόμου ή αγαθού για το οποίο υπάρχουν κάποιες υποψίες, όπως συμβαίνει εσωτερικά και σε κάθε κράτος. Επίσης, σε εξαιρετικές περιπτώσεις όπου κινδυνεύει η δημόσια τάξη και ασφάλεια, επιτρέπεται σε κάποιο κράτος να επαναφέρει τους συνοριακούς ελέγχους για κάποιο συγκεκριμένο χρονικό διάστημα. Στην σύμβαση για την εφαρμογή της συμφωνίας Schengen με σκοπό την ενίσχυση της ασφάλειας, ορίστηκαν μεταξύ άλλων συμπληρωματικά μέτρα τα οποία αφορούσαν[30-32]:

- Την ενίσχυση και την εναρμόνιση των ελέγχων των εξωτερικών συνόρων, και της εναρμόνισης της πολιτικής θεωρήσεων βραχείας διαμονής
- Της ουσιαστικής αμοιβαίας δικαστικής συνδρομής σε ποινικές υποθέσεις
- Τα μέτρα πρόληψης για τα ναρκωτικά, καθώς και για τα πυροβόλα όπλα και πυρομαχικά
- Την ενίσχυση της αστυνομικής συνεργασίας, συμπεριλαμβανομένου ενός κοινού πληροφοριακού συστήματος-του Συστήματος Πληροφοριών Σένγκεν (Schengen Information System- SIS).

Κατόπιν, ο χώρος Schengen επεκτάθηκε και συμπεριέλαβε και άλλα κράτη μέλη της ΕΕ, καθώς και τα τέσσερα κράτη μέλη της Ευρωπαϊκής Ζώνης Ελευθέρων Συναλλαγών EFTA (European Free Trade Association)[17]. Το Ηνωμένο Βασίλειο, η Κύπρος και η Ιρλανδία είναι τρία από τα κράτη μέλη της ΕΕ τα οποία δεν συμμετέχουν στον χώρο Schengen ενώ η Βουλγαρία και η Ρουμανία βρίσκονται σε διαδικασίες διαπραγμάτευσης για την είσοδο τους. Τα 26 κράτη μέλη του χώρου Schengen παρουσιάζονται στον πίνακα 5 μαζί με την χρονολογία εισόδου τους.

Πίνακας 5: Κράτη που συμμετέχουν στον χώρο Schengen ή βρίσκονται υπό ένταξη

| **ΚΡΑΤΗ ΜΕΛΗ ΤΗΣ ΕΕ ΠΟΥ ΣΥΜΜΕΤΕΧΟΥΝ ΣΤΟΝ ΧΩΡΟ ΣΕΝΓΚΕΝ** |
|---|
| |
| 1995: Βέλγιο – Γαλλία – Γερμανία – Λουξεμβούργο – Κάτω Χώρες – Πορτογαλία – Ισπανία |
| 1997: Αυστρία – Ιταλία |
| 2000: Ελλάδα |
| 2001: Δανία – Φινλανδία – Σουηδία |
| 2007: Εσθονία – Λετονία – Λιθουανία – Μάλτα – Ουγγαρία – Πολωνία – Σλοβακία – Σλοβενία – Τσεχική Δημοκρατία |
| |
| **ΚΡΑΤΗ ΕΚΤΟΣ ΤΗΣ ΕΕ ΠΟΥ ΣΥΜΜΕΤΕΧΟΥΝ ΣΤΟΝ ΧΩΡΟ ΣΕΝΓΚΕΝ (μέλη της EFTA)** |
| 2001: Ισλανδία – Νορβηγία |
| 2008: Ελβετία |
| 2011: Λιχτενστάιν |
| |
| **ΚΡΑΤΗ ΜΕΛΗ ΤΗΣ ΕΕ ΠΟΥ ΒΡΙΣΚΟΝΤΑΙ ΣΕ ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΣΧΩΡΗΣΗΣ ΣΤΟΝ ΧΩΡΟ ΣΕΝΓΚΕΝ** |
| Βουλγαρία – Ρουμανία |
| |
| **ΚΡΑΤΗ ΜΕΛΗ ΤΗΣ ΕΕ ΠΟΥ ΔΕΝ ΣΥΜΜΕΤΕΧΟΥΝ ΣΤΟΝ ΧΩΡΟ ΣΕΝΓΚΕΝ** |
| Ηνωμένο Βασίλειο – Ιρλανδία – Κύπρος |

Η κατάργηση των συστηματικών ελέγχων στα εσωτερικά σύνορα των κρατών του χώρου Schengen οδήγησε στην ανάγκη συστηματικής ανταλλαγής πληροφοριών μεταξύ των αστυνομικών αρχών των κρατών μέσω του πληροφοριακού συστήματος SIS με σκοπό την επίτευξη της ασφάλειας μέσα στα κράτη αυτά.

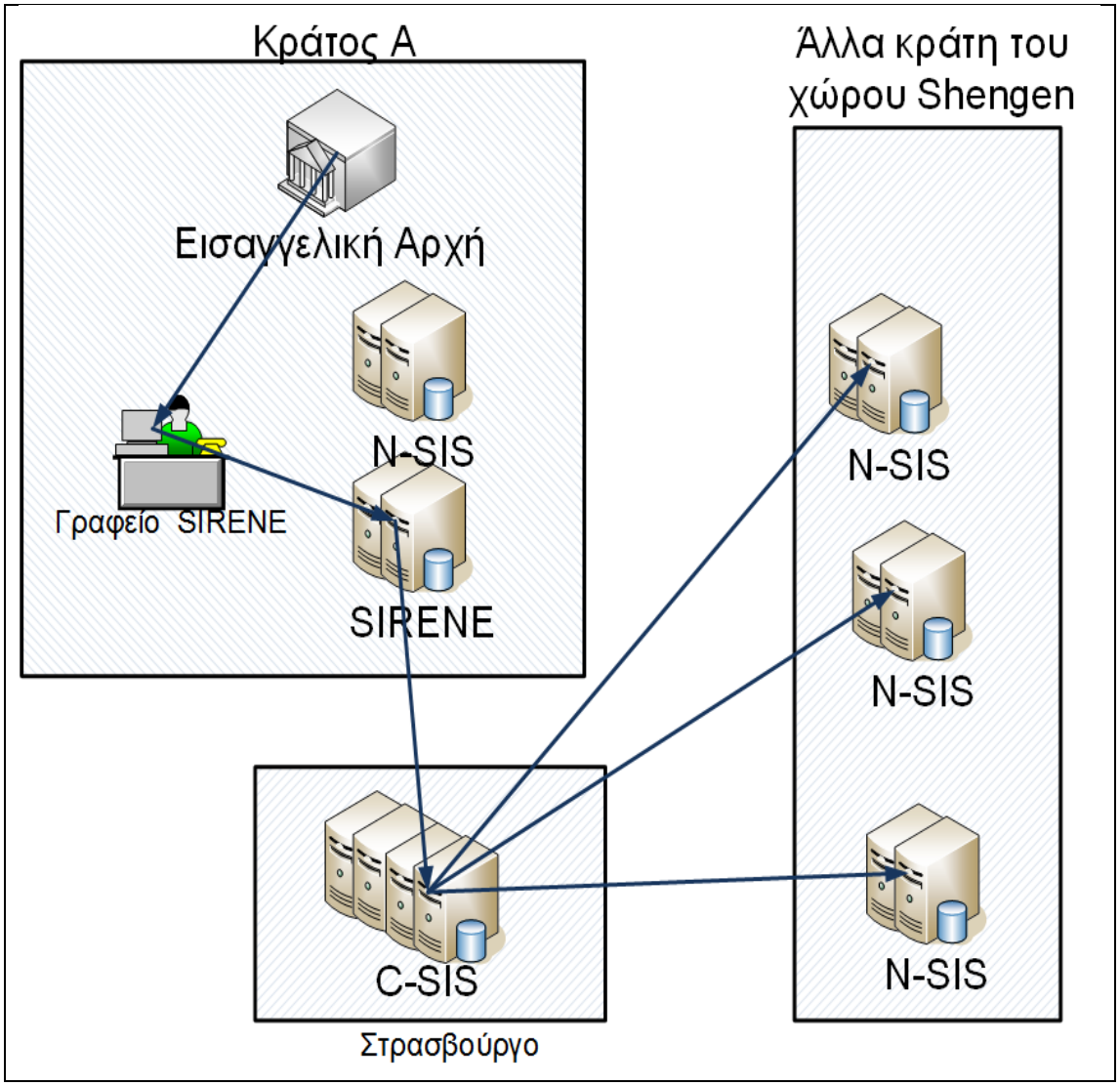
Αρχικά το SIS υλοποιήθηκε για να καλύψει τις ανάγκες για 18 κράτη μέλη. Αποτελείται από πανομοιότυπα εθνικά πληροφοριακά συστήματα (N-SISs) και το κεντρικό

[17] http://www.efta.int/

πληροφοριακό σύστημα SIS (C-SISs). Το C-SISs εδρεύει στη πόλη Στρασβούργο της Γαλλίας και παρέχει την τεχνική υποστήριξη και τροφοδοτεί με πληροφορίες τα N-SISs των κρατών μελών. Ακόμη, φροντίζει ώστε τα N-SIS να είναι πάντα ενημερωμένα (up-to-date) και διασφαλίζει ότι όλα τα N-SIS έχουν τις ίδιες πληροφορίες. Το κόστος λειτουργίας του μοιράζεται μεταξύ των κρατών μελών [31].

Κάθε κράτος μέλος του χώρου Schengen, οφείλει να συγκροτήσει μια υπηρεσία η οποία είναι υπεύθυνη για την ομαλή λειτουργία του N-SIS του κράτους και για την συμμόρφωση τους με τις διατάξεις της σύμβασης Schengen. Οι υπηρεσίες αυτές ονομάζονται S.I.RE.N.E, από τα αρχικά των λέξεων Supplementary Information REquest at the National Entries (Αίτηση Συμπληρωματικών Πληροφοριών για Εθνικές Καταχωρίσεις). Οι υπηρεσίες αυτές είναι υπεύθυνες και για την έκδοση νέων προειδοποιήσεων προς το C-SIS ενώ το προσωπικό της φροντίζει για όλες τις πτυχές επικοινωνίας που σχετίζονται με το SIS. Επιπλέον φροντίζει για την ανταλλαγή πληροφοριών, την μετάφραση όπου χρειάζεται, την αξιολόγηση και την επικύρωση των υποχρεωτικών πληροφοριών καθώς και για την αποθήκευση των απαραίτητων δεδομένων. Το C-SIS λαμβάνει πληροφορίες από τα γραφεία SIRENE και ενημερώνει τα N-SIS των υπόλοιπων κρατών μελών. Στο σχήμα 10 απεικονίζεται η βασική λειτουργία του SIS[32] . Μια εισαγγελική αρχή ελέγχει κατά πόσο για κάποιο άτομο το οποίο έχει διατελέσει κάποιο αδίκημα πληρούνται οι προϋποθέσεις για να αιτηθεί καταχώρηση νέου αιτήματος συναγερμού για αυτό το άτομο στο SIRENE. Αφού διαπιστωθεί ότι πληρούνται οι προϋποθέσεις και πρέπει να εκδοθεί αίτημα συναγερμού, αποστέλλει το αντίστοιχο αίτημα στο αρμόδιο για την λειτουργία του SIRENE γραφείο. Ο αρμόδιος υπάλληλος, μετά από πολύ σύντομες διαδικασίες ελέγχου και αφού διαπιστώσει ότι δεν υπάρχει κάποιο πρόβλημα στην διαδικασία, αποστέλλει το αίτημα για νέα καταχώρηση στο κεντρικό C-SIS. Το C-SIS ενημερώνει όλα τα N-SIS των υπόλοιπων κρατών για τον καινούργιο συναγερμό. Όταν κατά τον έλεγχο ενός ατόμου που διενεργείται από κάποιον αστυνομικό σε κάποια από τα υπόλοιπα κράτη μέλη διαπιστωθεί ότι υπάρχει ένταλμα για σύλληψη του, ο αστυνομικός συλλαμβάνει το άτομο αυτό και ενημερώνει το γραφείο SIRENE του κράτους του. Στην συνέχεια το

γραφείο αυτό έρχεται σε επικοινωνία και ενημερώνει το γραφείο SIRENE του κράτους από το οποίο εκδόθηκε ο συναγερμός και ζήτα οδηγίες για τις περαιτέρω ενέργειες[31]. Αφού λάβει τις οδηγίες αυτές ενημερώνει τον αστυνομικό.




**Σχήμα 10: Διαδικασία ενημέρωσης και λειτουργία του SIS**

### 4.1.2 SIS II

Ήδη από τον Οκτώβριο του 1997, η Εκτελεστική Επιτροπή (Executive Committee) της συνθήκης Schengen είχε πάρει την απόφαση ότι θα πρέπει να υλοποιηθεί μία νέα γενιά SIS με εκσυγχρονισμένες τεχνολογίες πληροφοριών, περισσότερες αρμοδιότητες και με την προσθήκη επιπλέον αποδοτικών μονάδων, απόφαση η οποία είχε χαρακτηριστεί ως εμπιστευτική και απόρρητη [32]. Το 1999 η Επιτροπή αυτή αντικαταστάθηκε από το αντίστοιχο Συμβούλιο. Στο Συμβούλιο αυτό συμμετέχουν οι Υπουργοί εσωτερικών όλων των κρατών του χώρου Schengen με την διαφορά ότι τα κράτη τα οποία δεν είναι μέλη της ΕΕ έχουν γνώμη για την διαμόρφωση αποφάσεων αλλά όχι για την λήψη αυτών. Το 2000 ανακοινώθηκε από το συμβούλιο η απόφαση για την ανάγκη υλοποίησης νέας γενιάς SIS όπως αυτή είχε οριστεί τρία χρόνια νωρίτερα [32].

Το Συμβούλιο εξουσιοδότησε και όρισε την Ευρωπαϊκή Επιτροπή αρμόδια για την μελέτη της κατασκευής του SIS II, το οποίο θα αποτελούσε την δεύτερη γενιά SIS. Οι προτάσεις που υποβλήθηκαν από την ΕΕ οδηγούσαν σε ένα σύστημα πολύ πιο πολύπλοκο και εξεζητημένο και με πολύ περισσότερες αρμοδιότητες και ικανότητες από ότι το SIS. Κατά συνέπεια, υπήρξαν φόβοι ότι η ΕΕ είναι οδεύει προς ένα χώρο ασφάλειας, αλλά χωρίς ελευθερία και τη δικαιοσύνη, με τις ατομικές ελευθερίες και ειδικότερα την προστασία των δεδομένων να βρίσκονται σε κίνδυνο[31].

Οι λόγοι για τους οποίους θεωρήθηκε απαραίτητη και υποστηρίχτηκε από την ΕΕ η δημιουργία του SIS II ήταν από τη μία τα προβλήματα χωρητικότητας που θα προέκυπταν λόγω των πρόσφατων και μελλοντικών διευρύνσεων της ΕΕ και από την άλλη η ανάγκη για τεχνολογικό εκσυγχρονισμό του συστήματος.

Το 2005, εκτιμήθηκε ότι το SIS II θα ολοκληρωνόταν και θα λειτουργούσε το 2007. Επιπλέον, είχε προβλεφθεί ότι η Ελβετία θα συμμετείχε απευθείας στο πληροφοριακό SIS II, αντί να συμμετέχει αρχικά στη παλιότερη γενιά του SIS. Αντίθετα, η πρόθεση των παλαιών κρατών μελών της ΕΕ ήταν να περιοριστεί η συμμετοχή των δέκα νέων κρατών μελών της ΕΕ στο SIS II, αποφεύγοντας με αυτόν τον τρόπο τη μετακίνηση των εξωτερικών συνόρων προς την Ανατολική Europe [32].

Σύμφωνα με το [32] πίσω από τις επίσημες δηλώσεις για τους λόγους για τη δημιουργία ενός SIS II κρυβόταν η επιθυμία να καθιερωθεί ένα σύστημα πληροφοριών το οποίο επιτρέπει την αποθήκευση περισσότερων κατηγοριών δεδομένων, με μεγαλύτερες δυνατότητες διασύνδεσης (interlinking), και ευρύτερη πρόσβαση των αρχών. Ακόμη στο ίδιο άρθρο υποστηρίζεται ότι η Ευρωπαϊκή Επιτροπή και το Συμβούλιο στην πλειοψηφία τους προσπάθησαν να προωθήσουν αυτό το έργο γρήγορα μέσω νομοθετικών διαδικασιών.

Τα θέματα που ανέκυψαν σχετικά με τις ελευθερίες του ατόμου και την προστασία των προσωπικών δεδομένων οδήγησε στην αμφισβήτηση της περαιτέρω ανάπτυξης του SIS. Το Ευρωπαϊκό Κοινοβούλιο, οι φορείς προστασίας δεδομένων, καθώς και μη κυβερνητικές οργανώσεις προειδοποιούσαν για την εισαγωγή ενός νέου πληροφοριακού συστήματος χωρίς να έχει προηγηθεί κάποια σχετική σαφής συμφωνία για τον σκοπό του συστήματος αυτού. Κάτω από αυτές τις συνθήκες υπήρξε μεγάλη καθυστέρηση στην πρόοδο για την ολοκλήρωση του έργου SIS II.

### 4.1.3 SISone4all

Οι καθυστερήσεις στην υλοποίηση του SIS II, το πρόβλημα της χωρητικότητας που εμφανίστηκε, οι φόβοι για την μη έγκαιρη ολοκλήρωση και καθιέρωση του SIS II αλλά και οι πιέσεις από τα προς ένταξη στον χώρο του Schengen μέλη, οδήγησαν στην εξεύρεση μιας λύσης η οποία θα έλυνε προσωρινά το πρόβλημα. Η λύση δόθηκε μέσα από το πληροφοριακό σύστημα «SISone4all»[32].

Η υλοποίηση του «SISone4all» χρησιμοποιούσε την ήδη υπάρχουσα λύση του SIS. Για να αντιμετωπιστεί το πρόβλημα της χωρητικότητας τα κράτη μέλη του Schengen πρόσφεραν ένα κλώνο του δικού τους N-SIS στις υπό ένταξη χώρες. Για παράδειγμα η Ελβετία έλαβε ένα κλώνο από την Πορτογαλία επιτρέποντάς την να συμμετέχει στο σύστημα και να επικοινωνεί με το C-SIS με την ίδια ποιότητα με την Πορτογαλία όπως και να έχει πρόσβαση στα ίδια δεδομένα. Με αυτό τον τρόπο ξεπεράστηκε το πρόβλημα της χωρητικότητας επιτρέποντας όλο και περισσότερες χώρες να γίνουν

μέλη του χώρου Schengen. Τον Νοέμβριο του 2007 το συμβούλιο αποφάσισε την ενσωμάτωση των υποένταξη κρατών του 2004 στον χώρο του Σέγκεν με εξαίρεση την Κύπρο. Η ολοκλήρωση του SIS II και η λειτουργία του υπολογίζεται το πρώτο τετράμηνο του 2013 [30].

Στα πλαίσια της ενίσχυσης των εξωτερικών συνόρων του χώρου Schengen δημιουργήθηκε ο «Ευρωπαϊκός Οργανισμός για τη Διαχείριση της Επιχειρησιακής Συνεργασίας για Εξωτερικά Σύνορα των κρατών μελών της ΕΕ»[33]. Στα πλαίσια του οργανισμού αυτού, τον Ιανουάριο του 2005 ανέλαβε καθήκοντα η υπηρεσία "*FRONTEX*"[18] .

Η Frontex εδρεύει στην πόλη Βαρσοβία της Πολωνίας και στηρίζει τα κράτη μέλη στην καθημερινή εφαρμογή των διατάξεων για τον έλεγχο των συνόρων. Μεταξύ των άλλων μέτρων, έχει την δυνατότητα αποστολής ειδικών τεχνικού προσωπικού στους συνοριακούς σταθμούς για την παροχή κατάρτισης στους εθνικούς φορείς οι οποίοι είναι υπεύθυνοι για την εκπαίδευση των δυνάμεων ελέγχου των συνόρων των χωρών. Η βασικές επιχειρηματικές δραστηριότητες της Frontex είναι η διεξαγωγή μελετών ανάλυσης κινδύνου, η αξιολόγηση απειλών, ο εντοπισμός τρωτών σημείων και ο υπολογισμός των συνεπειών σε τέτοιες περιπτώσεις.

### 4.1.4 Πλεονεκτήματα SIS

Το SIS είναι το βασικό στοιχείο της συνεργασίας Schengen. Παρέχει πληροφορίες σχετικά με τα πρόσωπα για τα οποία υπάρχει ένταλμα σύλληψης ή είναι εξαφανισμένα και αναζητούνται καθώς και για αντικείμενα όπως κλεμμένα αυτοκίνητα. Η ανταλλαγή πληροφοριών στο SIS είναι πιο αποτελεσματική την ανταλλαγή που συμβαίνει στην συμφωνία INTERPOL. Τα C-SIS δεδομένα παραδίδονται χωρίς καθυστέρηση. Οι αξιωματικοί που διαχειρίζονται τους σταθμούς SIRENE εισάγουν τα δεδομένα στη γλώσσα τους, και οι πληροφορίες στη συνέχεια μετατρέπονται σε έναν ψηφιακό κωδικό αριθμό ο οποίος αυτόματα μετατρέπεται εκ νέου στη γλώσσα του αιτούντος

[18] http://www.frontex.europa.eu/

μέλους του Schengen. Η τυποποίηση στην μέθοδο εισαγωγής δεδομένων εξασφαλίζει την ποιότητα των δεδομένων. Το SIS επιτρέπει την πρόσβαση 24 ώρες σε μία πολύ μεγάλη βάση δεδομένων. Ήδη από την 1η Ιανουαρίου 2004, το SIS περιείχε 11,7 εκατομμύρια στοιχεία δεδομένων [32]. Επιπλέον, οι διατάξεις Schengen είναι νομικά δεσμευτικές πράγμα το οποίο δεν ισχύει για όλες τις διατάξεις της συμφωνίας INTERPOL[19].

## 4.2 Πληροφοριακό Σύστημα Θεωρήσεων (VIS)

Το Πληροφοριακό Σύστημα Θεωρήσεων VIS (Visa Information System) αποβλέπει στην καλύτερη εφαρμογή της κοινής πολιτικής θεωρήσεων, της προξενικής συνεργασίας και της διαβούλευσης μεταξύ των κεντρικών προξενικών αρχών, διευκολύνοντας την ανταλλαγή δεδομένων που αφορούν αιτήσεις θεωρήσεων και σχετικών αποφάσεων μεταξύ των κρατών μελών. Σκοπός του VIS είναι να διευκολυνθούν οι διαδικασίες υποβολής των αιτήσεων θεώρησης καθώς και να ενισχυθεί η καταπολέμηση της απάτης και οι έλεγχοι στα εξωτερικά σημεία συνοριακής διέλευσης αλλά και στο έδαφος των κρατών μελών. Ακόμη, να παρεμποδιστεί η δόλια πρακτική της «άγρας θεωρήσεων» (visa shopping) δηλαδή της περαιτέρω υποβολής αιτήσεων θεώρησης σε άλλα κράτη μέλη της ΕΕ, όταν η πρώτη αίτηση έχει απορριφθεί [34]. Ακόμη το VIS ενδυναμώνει τους μηχανισμούς εντοπισμών προσώπων που δεν πληρούν ή έπαψαν να πληρούν πλέον τους όρους εισόδου, παραμονής ή κατοίκισης στο έδαφος των κρατών μελών συμβάλλοντας με αυτό τον τρόπο στην εφαρμογή του κανονισμού (ΕΚ) αριθ. 343/2003 του Συμβουλίου, της 18ης Φεβρουαρίου 2003 ο οποίος καθορίζει τη θέσπιση κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης ασύλου που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας, καθώς επίσης και να συμβάλει στην αποτροπή των απειλών κατά της εσωτερικής ασφάλειας των κρατών μελών [28].

[19] http://www.interpol.int/

Μέσα από το VIS παρέχεται η δυνατότητα σε όλα τα κράτη που ανήκουν στην συνθήκη Schengen να ανταλλάζουν δεδομένα θεωρήσεων (visa data). Το σύστημα αποτελείται από το κεντρικό πληροφοριακό σύστημα και από μια υποδομή μέσω της οποίας διενεργείται η επικοινωνία του κεντρικού αυτού πληροφοριακού συστήματος με τα επιμέρους εθνικά.

Το VIS συνδέει τα προξενεία που βρίσκονται σε τρίτες χώρες (χώρες εκτός ΕΕ) και όλα τα εξωτερικά σημεία συνοριακής διέλευσης των κρατών Schengen. Επεξεργάζεται δεδομένα και αποφάσεις που αφορούν αιτήσεις για θεωρήσεις βραχείας διαμονής ή διέλευσης από την περιοχή Schegen. Το σύστημα μπορεί να εκτελέσει τα βιομετρικές αντιστοιχίσεις, κυρίως δακτυλικών αποτυπωμάτων, για λόγους ταυτοποίησης και επαλήθευσης [34]. Το σύστημα συμβάλει στην :

- **Διευκόλυνση των ελέγχων και την έκδοση των θεωρήσεων**: VIS επιτρέπει στους συνοριοφύλακες να βεβαιωθούν ότι η θεώρηση που παρουσιάζεται από κάποιο πρόσωπο ανήκει νόμιμα σε αυτό και να εντοπίσουν άτομα που βρίσκονται στο έδαφος χωρών Schengen χωρίς ή με πλαστά έγγραφα. Οι έλεγχοι για την επιβεβαίωση της ταυτότητας του κατόχου γίνονται με μεγαλύτερη ακρίβεια και ταχύτητα με τη χρήση βιομετρικών στοιχείων. Το σύστημα επίσης διευκολύνει τη διαδικασία έκδοσης θεωρήσεων, ιδίως για τους συχνούς ταξιδιώτες.
- **Καταπολέμηση καταχρήσεων**: Παρότι η μεγάλη πλειοψηφία των κατόχων θεωρήσεων ακολουθούν τους κανόνες, μπορεί παρουσιαστούν και περιπτώσεις καταχρήσεων. Το VIS συμβάλει στην καταπολέμηση και την πρόληψη δόλιων συμπεριφορών, όπως για παράδειγμα αυτή της άγρας θεωρήσεων "visa shopping".
- **Προστασία των ταξιδιωτών**: Η βιομετρική τεχνολογία επιτρέπει την ανίχνευση των ταξιδιωτών που χρησιμοποιούν ταξιδιωτικά έγγραφα άλλου ατόμου και προστατεύει τους ταξιδιώτες.

- **Παροχή βοήθειας στις αιτήσεις ασύλου**: Το VIS καθιστά ευκολότερο να καθοριστεί ποιο κράτος της ΕΕ είναι υπεύθυνο για την εξέταση αιτήσεων ασύλου και άλλων σχετικών αιτήσεων.
- **Ενίσχυση της ασφάλειας**: Το VIS βοηθά στην πρόληψη, την ανίχνευση και στη διερεύνηση τρομοκρατικών πράξεων και άλλων σοβαρών αξιόποινων πράξεων.

Κατά την υποβολή αιτήσεων θεώρησης λαμβάνονται από τα πρόσωπα που υποβάλλουν την αίτηση 10 δακτυλικά αποτυπώματα και μια ψηφιακή φωτογραφία. Αυτά τα βιομετρικά δεδομένα, μαζί με τα στοιχεία που παρέχονται στο έντυπο της αίτησης θεώρησης καταγράφονται σε μια ασφαλή κεντρική βάση δεδομένων. Η λήψη των δακτυλικών αποτυπωμάτων δεν απαιτείται από παιδιά κάτω των 12 ετών. Ακόμη οι συχνοί ταξιδιώτες δεν είναι απαραίτητο να δίνουν τα δακτυλικά τους αποτυπώματα κάθε φορά που κάνουν αίτηση για νέα θεώρηση καθώς τα αποτυπώματα τους αποθηκεύονται στην κεντρική αυτή βάση δεδομένων και έχουν ισχύ για 5 χρόνια.

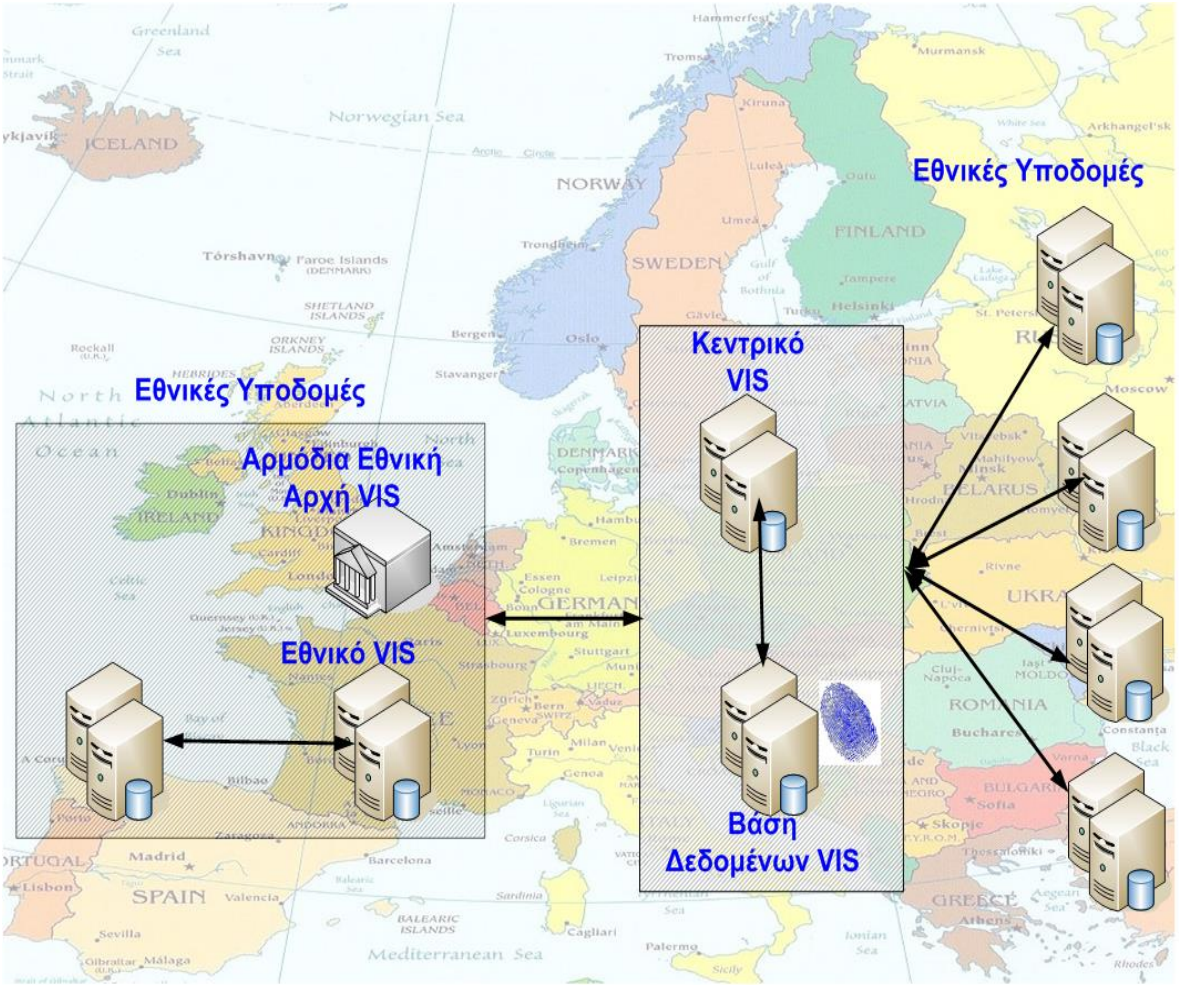
Πρόσβαση στο VIS μπορούν να έχουν οι αρμόδιες αρχές για την εξέταση αιτήσεων και την παροχή θεωρήσεων καθώς και των αποφάσεων που σχετίζονται με αυτές καθώς και οι αρχές οι οποίες είναι αρμόδιες για την διενέργεια ελέγχων στα εξωτερικά σύνορα του χώρου Schengen καθώς και εντός των εθνικών εδαφών. Ακόμη οι αρχές οι οποίες είναι αρμόδιες για την παροχή ασύλου έχουν την δυνατότητα διενέργειας αναζητήσεων μέσα από το VIS με σκοπό τον εντοπισμό του κράτους το οποίο είναι αρμόδιο για την χορήγηση ασύλου. Σε ξεχωριστές με σκοπό την πρόληψη, εξακρίβωση και διερεύνηση τρομοκρατικών και άλλων ποινικών αδικημάτων περιπτώσεις παρέχεται πρόσβαση στα αποθηκευμένα δεδομένα του VIS στις εθνικές αρχές και στην Europol[20].

Το κύριο Κεντρικό πληροφοριακό σύστημα VIS έχει εγκατασταθεί στο Στρασβούργο (Γαλλία) και έχει την τεχνική εποπτεία και διοίκηση. Ένα εφεδρικό Κεντρικό VIS βρίσκεται στο Sankt Johann im Pongau (Αυστρία), το οποίο έχει την δυνατότητα να διενεργήσει όλες τις λειτουργίες του κύριου κεντρικού VIS σε περίπτωση αυτό υποστεί

[20] http://www.interpol.int/

κάποια βλάβη. Το VIS συνδέεται με το εθνικό σύστημα κάθε κράτους μέλους μέσω της εθνικής διεπαφής στο συγκεκριμένο κράτος μέλος. Στο σχήμα 11 απεικονίζεται σχηματικά η σχέση μεταξύ του κεντρικού VIS με τις εθνικές υποδομές και η μεταξύ τους επικοινωνία.

Κάθε κράτος μέλος είναι αρμόδιο για την ανάπτυξη του εθνικού συστήματος του και την προσαρμογή του στο VIS, τη διαχείριση, τη διοργάνωση, τη λειτουργία και τη συντήρηση του εθνικού τους συστήματος. Επίσης κάθε κράτος μέλος είναι υπεύθυνο για τον ορισμό μιας εθνικής αρχής η οποία έχει την αρμόδια της παροχής πρόσβασης στις αρμόδιες αρχές. Το προσωπικό των αρχών αυτών που έχουν πρόσβαση στο VIS, πριν λάβει την εξουσιοδότηση πρόσβασης στο VIS και της επεξεργασίας δεδομένων VIS εκπαιδεύεται κατάλληλα στην ασφάλεια και τους κανόνες προστασίας των δεδομένων και ενημερώνεται για τις συναφείς αξιόποινες πράξεις και ποινές.




**Σχήμα 11: Σχηματική απεικόνιση της λειτουργίας του VIS**

## 4.3 Πληροφοριακό Σύστημα Τελωνίων (CIS)

Το Συμβούλιο της Ευρώπης εξέδωσε το 1997 την οδηγία 515/97 [35] με την οποία όριζε την αμοιβαία συνδρομή και συνεργασία μεταξύ των διοικητικών αρχών των κρατών μελών με την Ευρωπαϊκή Επιτροπή για να εξασφαλιστεί η ορθή εφαρμογή του νόμου περί τελωνειακών και γεωργικών ρυθμίσεων. Η οδηγία αυτή οδήγησε στην δημιουργία ενός ενιαίου Πληροφοριακό Σύστημα Τελωνίων (CIS - Customs information System) το οποίο συνδέει όλα τα τελωνεία των κρατών μελών της ΕΕ. Αυτό το κοινό δίκτυο υπολογιστών που ενώνει τις τελωνιακές αρχές έχει την μορφή μιας κεντρικής βάσης δεδομένων η οποία είναι προσβάσιμη μέσω τερματικών σε κάθε κράτος μέλος της ΕΕ. Επιτρέπει την άμεση ανταλλαγή δεδομένων και πληροφοριών και βοηθάει στην πρόληψη, διερεύνηση και δίωξη παραβάσεων των κοινοτικών τελωνείων και των γεωργικών ρυθμίσεων. Ακόμη, παρέχει την δυνατότητα συστηματικής ή περιστασιακής ανταλλαγής δεδομένων σχετικά με τα αγαθά που διακινούνται μεταξύ της Ευρώπης και τρίτων χωρών.

Το CIS διέπεται από αυστηρούς και συγκεκριμένους κανόνες λειτουργίας. Ένας από τους περιορισμούς που τίθενται για την λειτουργία του είναι ο περιορισμός των δεδομένων τα οποία μπορούν να εισάγονται στο σύστημα. Τα δεδομένα θα πρέπει να σχετίζονται με [36, 37]:

- αγαθά
- μεταφορικά μέσα
- επιχειρήσεις
- ανθρώπους
- τις τάσεις των απατών
- Διαθέσιμες αρμοδιότητες
- Κατακρατήσεις, κατασχέσεις ή δημεύσεις αγαθών
- Κατακρατήσεις, κατασχέσεις ή δημεύσεις μετρητών.

Στο CIS μπορούν να εισαχθούν και προσωπικά στοιχεία (personal data) τα οποία όμως περιγράφονται λεπτομερώς σε ένα περιορισμένο προκαθορισμένο κατάλογο. Τα προσωπικά στοιχεία κάποιου ατόμου εισάγονται μόνο εάν υπάρχουν σοβαρές ενδείξεις ότι ο άτομο αυτό έχει παραβιάσει, παραβιάζει ή θα παραβιάσει τους τελωνειακούς ή γεωργικούς κανονισμούς. Κάθε πρόσωπο έχει δικαίωμα πρόσβασης στα δεδομένα που το αφορούν για να ελέγξει ότι είναι ακριβή και σε τι επεξεργασία υπόκεινται.

Τα δεδομένα του CIS είναι εμπιστευτικά και μπορούν να αναπαραχθούν για τεχνικούς λόγους. Με την έγκριση της αρχής που τα εισήγαγε, τα προσωπικά δεδομένα μπορούν

να μεταδοθούν σε συστήματα διαχείρισης κινδύνου που χρησιμοποιούνται για τελωνειακούς ελέγχους σε εθνικό επίπεδο ή σε συστήματα επιχειρησιακής ανάλυσης που χρησιμοποιούνται σε κοινοτικό επίπεδο.

Πρόσβαση στα δεδομένα του πληροφοριακού συστήματος των τελωνείων μπορούν να έχουν μόνο οι αρχές που ορίζονται από τα κράτη μέλη και την Ευρωπαϊκή Επιτροπή. Αυτές οι αρχές ορίζονται από την Επιτροπή μετά από μια λίστα που στέλνεται σε αυτήν με λεπτομερείς όρους σχετικά με την πρόσβαση της κάθε Αρχής.

Το πρώτο σύστημα για την ηλεκτρονική υποβολή τελωνιακών διασαφήσεων ήταν το NCTS (New Computerised Transit System) το οποίο λειτούργησε για πρώτη φορά το 1997. Το Ευρωπαϊκό Κοινοβούλιο το 2008 εξέδωσε την απόφαση 70/2008/ΕΚ [38] με την οποία υποχρέωνε την Επιτροπή να εκπονήσει και να αναπροσαρμόζει ένα Πολυετές Στρατηγικό Σχέδιο MASP (Multi – Annual Strategic Plan) για τα ηλεκτρονικά τελωνειακά συστήματα. Η απόφαση κυρίως στόχευε [37, 39]:

- Να δεσμευτούν οι ενδιαφερόμενοι φορείς για την εφαρμογή πανευρωπαϊκών διαλειτουργικών και προσβάσιμων ηλεκτρονικών τελωνειακών συστημάτων
- Να καθοριστούν οι στόχοι, η στρατηγική και ο μηχανισμός συντονισμού για τα ηλεκτρονικά τελωνειακά συστήματα
- Να καθοριστούν οι κοινοτικές και εθνικές συνιστώσες των συστημάτων καθώς και οι σχετικές αρμοδιότητες και τα καθήκοντα
- Να δημιουργηθεί ένα πλαίσιο παρακολούθησης και υποβολής για την πρωτοβουλία ηλεκτρονικών τελωνείων.

Το όραμα και οι στόχοι του MASP είναι [36, 39] :

• Ο έλεγχος και η δευκόλυνση της κυκλοφορίας των εμπορευμάτων εντός και εκτός της εσωτερικής αγοράς μέσω αποτελεσματικών διαδικασιών εισαγωγής και εξαγωγής

• Η αύξηση της ανταγωνιστικότητας του ευρωπαϊκού εμπορίου μέσω της μείωσης των διοικητικών δαπανών και της βελτίωσης του χρόνου εκτελωνισμού

•Η βελτίωση της ασφάλειας και της προστασίας των πολιτών σε σχέση με την μεταφορά επικίνδυνων και παράνομων εμπορευμάτων

• Η προστασία των οικονομικών συμφερόντων της ΕΕ και των κρατών μελών της

• Η συμβολή στην καταπολέμηση του διεθνούς εγκλήματος και της τρομοκρατίας με την γρήγορη παροχή κατάλληλων πληροφοριών όσον αφορά τη διεθνή αλυσίδα εφοδιασμού

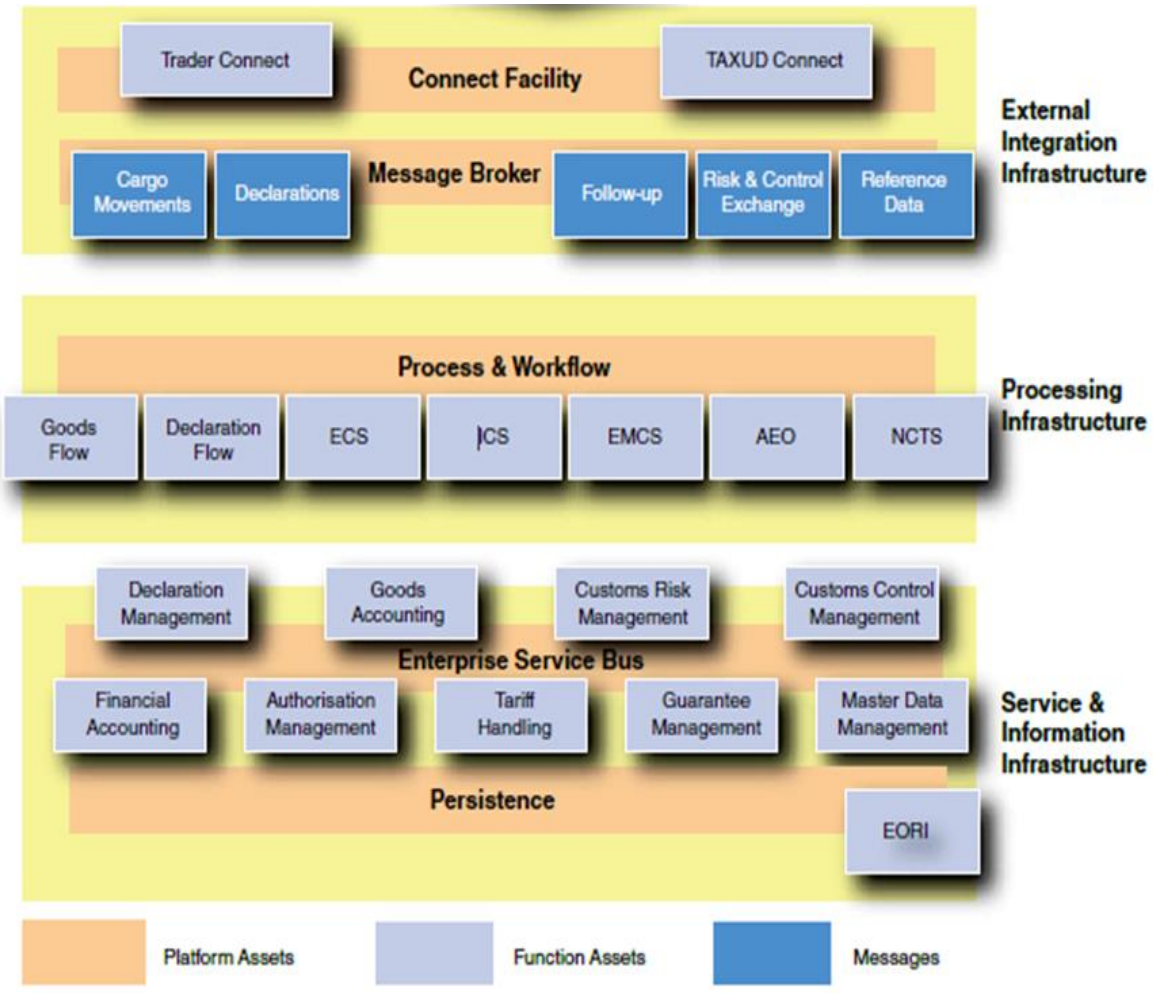
• Η απρόσκοπτη ροή και ανταλλαγής δεδομένων μεταξύ των χωρών εξαγωγής και εισαγωγής.

Το CIS αποτελείται από ένα πλήθος συστημάτων τα οποία απεικονίζονται στο σχήμα 12. Τα κυριότερα από τα συστήματα από τα οποία αποτελείται είναι [36] :

- Νέο Μηχανογραφημένο Σύστημα Διαμετακόμισης-NCTS (New Computerized Transit System). Το NCTS είναι μηχανογραφικό σύστημα διαχείρισης και παρακολούθησης της Κοινοτικής/Κοινής Διαμετακόμισης (καθεστώς Τ1/Τ2) καθώς και κινήσεων Διαμετακόμισης υπό το καθεστώς TIR, εντός της ΕΕ και των χωρών της Ευρωπαϊκής Ζώνης Ελευθέρων Συναλλαγών (ΕΖΕΣ). Περιλαμβάνει υποχρεωτικές ηλεκτρονικές συναλλαγές μεταξύ συναλλασσομένων και Τελωνείων.
- Σύστημα Ελέγχου Εξαγωγών-ECS (Export Control System). Σύστημα ανταλλαγής πληροφοριών Ενιαίων Διοικητικών Εγγράφων (ΕΔΕ) εξαγωγής μεταξύ των συναλλασσομένων, του τελωνείου εξαγωγής και του τελωνείου εξόδου με στόχο τη βεβαίωση εξόδου των εμπορευμάτων.
- Σύστημα Ελέγχου Εξαγωγών-ECS (Export Control System). Σύστημα ανταλλαγής πληροφοριών ΕΔΕ εξαγωγής μεταξύ των συναλλασσομένων, του τελωνείου εξαγωγής και του τελωνείου εξόδου με στόχο τη βεβαίωση εξόδου των εμπορευμάτων.
- Σύστημα Ελέγχου Εισαγωγών-ICS (Import Control System) Το Σύστημα Ελέγχου Εισαγωγών αποτελεί το πρώτο στάδιο του Αυτοματοποιημένου Συστήματος Εισαγωγών AIS (Automated Import System). Το ICS υποστηρίζει την ηλεκτρονική υποβολή, διαχείριση και επεξεργασία των Συνοπτικών Διασαφήσεων Εισόδου. Επιπλέον, υποστηρίζει τα αποτελέσματα ανάλυσης κινδύνου για την ασφάλεια και προστασία μέσω της ηλεκτρονικής επικοινωνίας και ανταλλαγής σχετικών μηνυμάτων μεταξύ Ελληνικών και ευρωπαϊκών αρχών.
- Σύστημα Παρακολούθησης και Ελέγχου Ειδικών Φόρων Κατανάλωσης- EMCS (Excise Movement and Control System). Το EMCS είναι ένα Ηλεκτρονικό Σύστημα Παρακολούθησης και Ελέγχου της ενδοκοινοτικής διακίνησης των προϊόντων που υπόκεινται σε ειδικό φόρο κατανάλωσης (Ε.Φ.Κ.) (ενεργειακά, καπνικά & αλκοολούχα προϊόντα) υπό καθεστώς αναστολής των φόρων. Το Σύστημα αυτό θα επιτρέπει την παρακολούθηση σε πραγματικό χρόνο της

διακίνηση των προϊόντων Ε.Φ.Κ. και να διενεργούν τους αναγκαίους ελέγχους, απλοποιώντας τις διαδικασίες. στον τομέα αυτό.

Προκειμένου να εξασφαλιστεί η απρόσκοπτη ροή δεδομένων μεταξύ των υφιστάμενων κοινοτικών τελωνειακών συστημάτων, όπως του NCTS, συμπεριλαμβανομένων των CCN / CSI, των νέων συστημάτων, όπως η ECS / AES, ICS / AIS, καθώς και του συστήματος ελέγχου της κυκλοφορίας των ειδικών προϊόντων (EMCS), θα πρέπει να υπάρχει μεταξύ τους διαλειτουργικότητα. Θα πρέπει επίσης να έχουν την δυνατότητα να ενσωματώνουν υφιστάμενες και νέες βάσεις δεδομένων, όπως το TARIC, Quota, EBTI, και άλλα συστήματα αναφοράς που συνδέονται με την κυκλοφορία των εμπορευμάτων.




**Σχήμα 12: Σχηματική αναπαράσταση λειτουργικών μονάδων ηλεκτρονικού τελωνίου**

# Κεφάλαιο 5: Ηλεκτρονική Ταυτοποίηση

## 5.1 Μια γενική προσέγγιση για την Διασυνοριακή Ηλεκτρονική Ταυτοποίηση

Ένα από τα βασικά εργαλεία για την επίτευξη διασυνοριακής διαλειτουργικότητας μεταξύ των υπηρεσιών που προσφέρονται στην Ευρωπαϊκή Ψηφιακή Ενιαία Αγορά είναι η καθιέρωση αξιόπιστων ηλεκτρονικών ταυτοτήτων. Για την ανάπτυξη 'value-added' διασυνοριακών υπηρεσιών, δηλαδή υπηρεσιών οι οποίες θα προσθέσουν κάτι καινούργιο στον χώρο των υπηρεσίων προς τους πολίτες, είναι καίριας σημασίας η ύπαρξη ενός μηχανισμού ελέγχου της αυθεντικότητας της ταυτότητας ενός χρήστη με κάποιο ικανοποιητικό επίπεδο ασφάλειας. Η έλλειψη διασυνοριακής διαλειτουργικότητας των εθνικών συστημάτων ηλεκτρονικής ταυτότητας εμποδίζει στους ευρωπαίους χρήστες την πρόσβαση στις ηλεκτρονικές υπηρεσίες άλλων κρατών μελών με συνέπεια να μην μπορούν να επωφεληθούν πλήρως από την ενιαία ψηφιακή αγορά. Οι πολίτες της Ευρώπης θα πρέπει να είναι σε θέση να σπουδάζουν, να εργάζονται, να διαμένουν, να λαμβάνουν υγειονομική περίθαλψη και συνταξιοδοτούνται οπουδήποτε στην Ευρωπαϊκή Ένωση (ΕΕ). Οι επιχειρηματίες θα πρέπει να είναι σε θέση να μπορούν να δημιουργήσουν και να λειτουργήσουν ομαλά μια επιχείρηση οπουδήποτε και σε κάθε κράτος μέλος.

Για την υλοποίηση ενός βιώσιμου μοντέλου Ηλεκτρονικής Ταυτοποίησης (ΗΤ) θα πρέπει να ληφθούν υπόψη οι προοπτικές, οι ανάγκες και τις προσδοκίες των βασικών ενδιαφερόμενων μερών (key stakeholders). Τα βασικά ενδιαφερόμενα μέρη μπορούν να διακριθούν στους: παρόχους των υπηρεσιών (service providers), στους παρόχους ταυτότητας (identity providers), στους παρόχους χαρακτηριστικών (attribute providers) και στους τελικούς χρήστες.

Υπάρχουν πολλά οφέλη τα οποία οδηγούνται από τις βασικές τάσεις της εποχής μας στο πεδίο της παροχής ηλεκτρονικών υπηρεσιών. Οι παρατηρούμενες βασικές τάσεις και προκλήσεις της σημερινής εποχής σε ότι αφορά την ΗΤ για παρόχους υπηρεσιών είναι οι παρακάτω:

• Υπάρχει μια σημαντική αύξηση των προσφερόμενων δικτυακών υπηρεσιών τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Κάθε πάροχος υπηρεσιών αναζητεί τρόπους για την ταυτοποίηση των τελικών του χρηστών.

• Κάθε πάροχος υπηρεσιών πρέπει να βρει έναν τρόπο για να καταχωρήσει, να ταυτοποιήσει και να αυθεντικοποιήσει τους τελικούς του χρήστες. Όταν αυτό όμως γίνεται μόνο σε εθνικό επίπεδο ενδέχεται να οδηγήσει σε ένα διάσπαρτο μη διαλειτουργικό διασυνοριακό πεδίο ηλεκτρονικής ταυτοποίησης.

- Οι πάροχοι υπηρεσιών πρέπει είτε να δημιουργήσουν το δικό τους σύστημα ή να βασιστούν σε συστήματα που έχουν κατασκευαστεί από άλλους παρόχους επιβαρύνοντας τους πρώτους με περιττά έξοδα, ενώ προκύπτουν και ζητήματα για τους σχετικούς όρους και τις προϋποθέσεις που αφορούν συνεργασίες σε αυτό το επίπεδο .
- Μια άλλη σημαντική πρόκληση για όλους τους παρόχους υπηρεσιών είναι η αυξανόμενη ζήτηση για ταυτοποίηση μέσω κινητών τηλεφώνων (mobile eId).

Τα οφέλη που θα προκύψουν από την δημιουργία ενός ενιαίου Ευρωπαϊκού συστήματος ΗΤ για τους παρόχους υπηρεσιών σχετίζονται με το γεγονός ότι[40]:

- Θα έχουν πρόσβαση σε ένα μεγάλο αριθμό Ευρωπαίων καταναλωτών στους οποίους θα είναι σε θέση να προσφέρουν τις υπηρεσίες τους μέσα από το ευρύτερο πλαίσιο των διασυνοριακών υπηρεσιών.
- Θα γνωρίζουν ότι οι προ-εγγεγραμμένοι καταναλωτές τους είναι εξοπλισμένοι με πιστοποιημένες συσκευές (tokens) ΗΤ.
- Θα μπορούν να μειώσουν το κόστος τους για την εγγραφή των χρηστών τους και την αυθεντικοποίηση τους.
- Θα είναι σε θέση να αποφύγουν νομικές αβεβαιότητες (legal uncertainty), ενδεχόμενες επιβαρύνσεις και απάτες κατά την παροχή των υπηρεσιών τους διασυνοριακά.

- Θα παραχθούν και θα προσφερθούν στα ενδιαφερόμενα μέρη κοινές προδιαγραφές, πρότυπα και δομικά στοιχεία τα οποία θα συντελέσουν στην υλοποίηση καλύτερων και διαλειτουργικών προϊόντων και υπηρεσιών.

Κατά τα τελευταία χρόνια τα κράτη μέλη της ΕΕ έχουν εκδώσει όλο και περισσότερα ηλεκτρονικά αναγνώσιμα έγγραφα ταυτότητας (eID documents) για τους πολίτες τους για διαφορετικούς σκοπούς και εφαρμογές. Οι λύσεις αυτές έχουν σχεδιαστεί για να είναι όσο το δυνατόν περισσότερο αποτελεσματικές αλλά και λειτουργικές σε σχέση με τις εθνικές απαιτήσεις και τις διαθέσιμες ή σχεδιαζόμενες υποδομές.

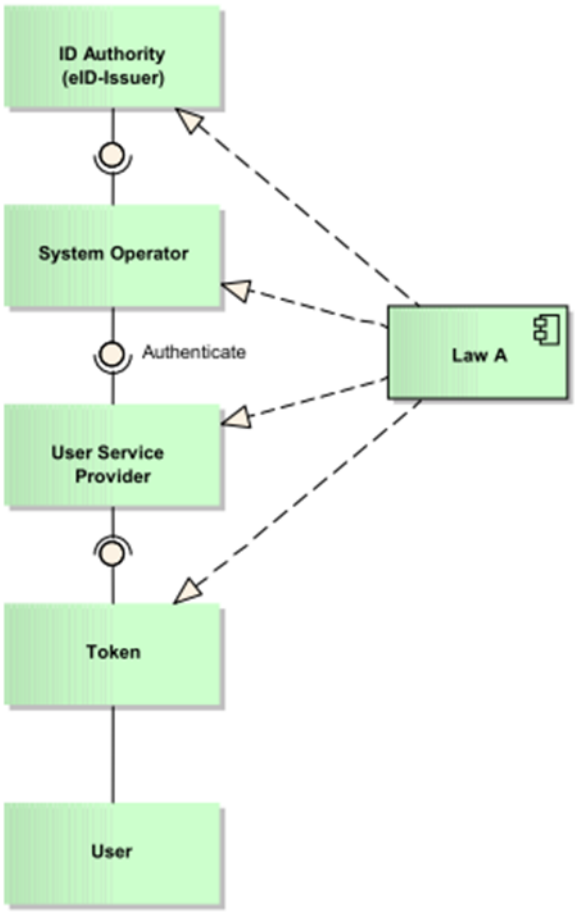
Οι στόχοι αυτών των συστημάτων είναι σε γενικές γραμμές οι ίδιοι για όλα τα κράτη μέλη και σχετίζονται με[41] :

- διαχείριση ταυτοτήτων,
- βελτίωση της διοικητικής αποτελεσματικότητας,
- βελτίωση της προσβασιμότητας και της φιλικότητα προς τον χρήστη,
- μείωση της κατάχρησης και της απάτης και,
- μείωση των εξόδων.

Η βελτίωση της διαλειτουργικότητας της ΗΤκαι της επαλήθευσης της ταυτότητας είναι ευρωπαϊκό καθήκον αλλά και καθήκον του κάθε κράτους μέλους. Σημαντικές προσπάθειες έχουν γίνει μέσα από διάφορα προγράμματα για να αντιμετωπιστούν οι προκλήσεις της πανευρωπαϊκής διαλειτουργικότητας στην ΗΤκαι να αξιολογηθούν οι σκοπιμότητες των διαφορετικών προσεγγίσεων.

Για την επίτευξη της διαλειτουργικότητας σε ότι αφορά την ΗΤ το ελάχιστο που απαιτείται είναι η σύναψη μίας σύμβασης σχετικής με τα δικαιώματα και τις υποχρεώσεις των συμμετεχόντων μερών αλλά και των περιορισμών που αφορούν την επεξεργασία και αποθήκευση των δεδομένων. Σε αυτό μπορεί να συμβάλλει σε μεγάλο βαθμό η Ευρωπαϊκή νομοθεσία, η οποία μπορεί να θέσει τα θεμέλια για την καθιέρωση εθνικών νομοθεσιών με στόχο την υποστήριξη των διασυνοριακών εφαρμογών.

Ο θεμέλιος λίθος κάθε υπηρεσίας ΗΔ, ηλεκτρονικής υγείας ή οποιασδήποτε άλλης υπηρεσίας που εμπλέκει προσωπικά δεδομένα είναι η εμπιστοσύνη στην αυθεντικότητα (trust in the authenticity) όλων των συμμετεχόντων και των δεδομένων που παρέχονται. Δεδομένου ότι οι περισσότερες από αυτές τις υπηρεσίες χειρίζονται εμπιστευτικά δεδομένα, η εμπιστευτικότητα πρέπει να προστατεύεται και σε ένα διασυνοριακό σενάριο. Ακόμη, μερικές υπηρεσίες απαιτούν υψηλή διαθεσιμότητα μέσα από τις οποίες ο πολίτης δεν επιτρέπεται να υφίσταται αδικαιολόγητες καθυστερήσεις.




**Σχήμα 13: Εγχώριο σύστημα ηλεκτρονικής ταυτοποίησης [41]**

Στο σχήμα 13 απεικονίζεται ένα σύστημα ΗΤ το οποίο έχει σχεδιαστεί για να παρέχει υπηρεσίες σε εθνικό επίπεδο (εγχώριο σύστημα). Σε κάθε σύστημα που περιλαμβάνει ηλεκτρονικό έλεγχο ταυτότητας, έχει εκχωρηθεί στον χρήστη μια ηλεκτρονική ταυτότητα (eID). Η ηλεκτρονική αυτή ταυτότητα μπορεί να χρησιμοποιεί για να ταυτοποιήσει τον χρήστη κάποιο μοναδικό αριθμό, όπως τον αριθμό ασφάλισης υγείας ή τον αριθμό μητρώου πολιτών. Η αρχή ταυτοποίησης (eID Athority) συσχετίζει και εισάγει στο σύστημα την ηλεκτρονική ταυτότητα του χρήστη. Η αρχή ταυτοποίησης εκδίδει επίσης μία ειδική διάταξη (Token). Ένα token είναι μια συσκευή, π.χ., μία έξυπνη κάρτα, η οποία αντιπροσωπεύει την ταυτότητα του χρήστη. Παραδείγματα είναι μια κάρτα ασφάλισης υγείας ή μια κάρτα εθνική ταυτότητα. Το token μπορεί να περιέχει δεδομένα για την ταυτότητα του ατόμου και άλλα δεδομένα σε ηλεκτρονική μορφή[41].

Μια δυνητικά ξεχωριστή οντότητα στο σύστημα είναι ο διαχειριστής του συστήματος (System Operator) (π.χ. μια εταιρεία ασφάλισης υγείας ή μια υπηρεσία μητρώου πολιτών). Αυτός διαχειρίζεται το σύστημα ΗΤ και διεκπεραιώνει οποιεσδήποτε διαδικασίες αυθεντικοποίησης που αφορούν το σύστημα, συνήθως με τη μορφή κεντρικής υποστήριξης (backend).

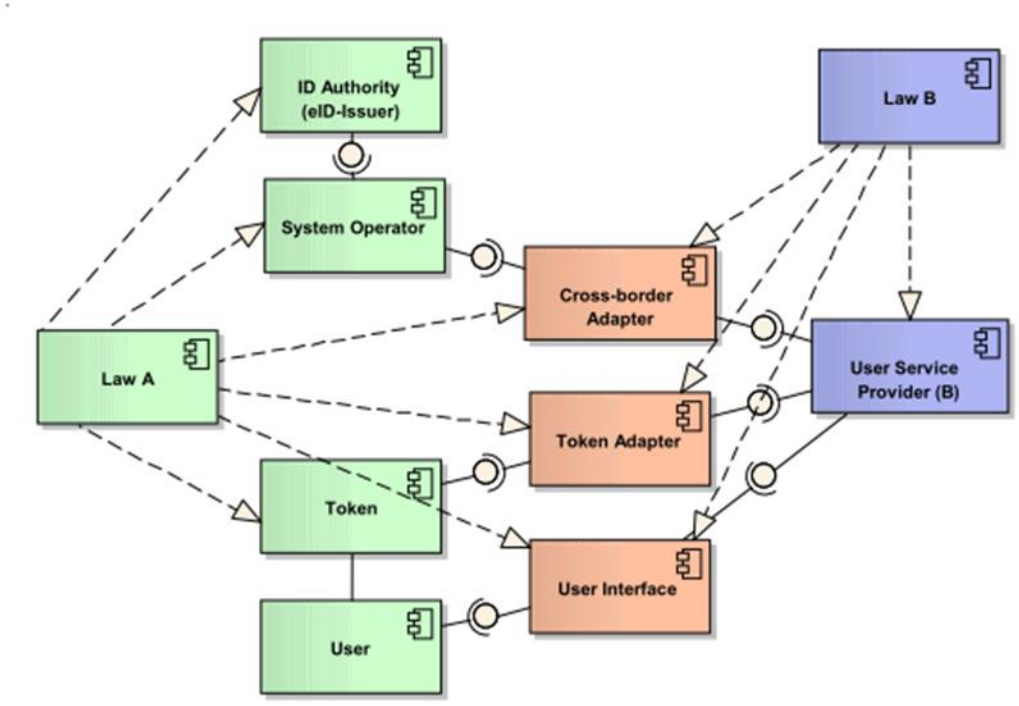
Ο πάροχος υπηρεσιών (Service Provider) των χρηστών (π.χ., ένας γιατρός ή ένα γραφείο καταχώρισης οχημάτων) αλληλεπιδρά με το χρήστη (User) και το token του χρήστη. Αυτός παρέχει μια υπηρεσία στο χρήστη που συνδέεται με την εφαρμογή που παρέχεται από το διαχειριστή του συστήματος. Οι νόμοι, οι κανονισμοί ή οι συμβάσεις που διέπουν την παροχή αυτής της υπηρεσίας απαιτούν από τον πάροχο υπηρεσιών τον έλεγχο της ταυτότητας του χρήστη μέσω του token του χρήστη διαμέσου του διαχειριστή του συστήματος. Όλο αυτό το σύστημα, οι συμμετέχοντες, τα συστατικά του και τις διαδικασίες διέπονται από το ίδιο σύνολο των νόμων και των κανονισμών (Law A). Αυτοί οι νόμοι αφορούν γενικούς κανονισμούς σχετικά με τον χειρισμό των προσωπικών δεδομένων (π.χ., με βάση την Οδηγία Προστασίας Δεδομένων 95/46/ΕΚ [13]) αλλά και συγκεκριμένες διατάξεις σχετικά με την εφαρμογή, τις υπηρεσίες ή τα token.

Ενώ υπάρχει ένα ευρύ φάσμα πιθανών (και υφιστάμενων) τεχνικών λύσεων αλλά και παραλλαγών που αφορούν τα tokens και την ηλεκτρονική αυθεντικοποίηση, η γενική αρχή είναι η ίδια για όλα τα εν λόγω συστήματα. Όλα αυτά τα συστήματα:

• είναι ομοιογενή όσον αφορά την τεχνολογία,

• διέπονται από ένα ενιαίο σύνολο νόμων,

• «γνωρίζουν» όλους τους συμμετέχοντες του συστήματος, που σημαίνει ότι είναι «κλειστά» για τους μη συμμετέχοντες στο σύστημα.




**Σχήμα 14 : Διασυνοριακό σύστημα HT [41]**

Για να αξιοποιηθεί μια εφαρμογή διασυνοριακά ή να χρησιμοποιηθεί μια υπηρεσία που παρέχεται με την χρήση κάποιου token εκτός των συνόρων του κράτους στο οποίο ανήκει ο πάροχος υπηρεσιών, το μοντέλο HT που λειτουργεί σε εθνικό επίπεδο πρέπει να επεκταθεί.

Η μεγάλη διαφορά της διασυνοριακής ταυτοποίησης σε σχέση με αυτήν που λειτουργεί σε εθνικό επίπεδο, είναι το γεγονός ότι ο πάροχος υπηρεσιών (B) είναι στην πραγματικότητα ένας πάροχος υπηρεσιών από ένα άλλο σύστημα που διέπεται από διαφορετικούς νόμους (L B) και κανόνες για την λειτουργία των επιχειρήσεων από αυτούς που διέπουν τους εγχώριους παρόχους υπηρεσιών. Επιπλέον, το άλλο σύστημα μπορεί να χρησιμοποιεί διαφορετική τεχνολογία και να μην υπάρχει συμβατότητα μεταξύ αυτών[41].

Επίσης, σημαντικό είναι το γεγονός ότι ο πάροχος υπηρεσιών (B) συνήθως δεν είναι «γνωστός» στον διαχειριστή του συστήματος (System Operator), με την έννοια ότι συχνά δεν υπάρχει άμεση συμφωνία (contractual agreement) και δεν υπάρχουν σαφείς νομικές διατάξεις που διέπουν τη σχέση τους. Ακόμη, οι νόμοι που διέπουν τη λειτουργία του φορέα παροχής υπηρεσιών (B) και του διαχειριστή συστήματος είναι διαφορετικοί, κάτι το οποίο μπορεί να προκαλέσει πλήθος προβλημάτων που σχετίζονται με την προστασία των δεδομένων και με θέματα ασφάλειας[41].

Προκειμένου να επιτευχθεί συμβατότητα μεταξύ των δύο συστημάτων έτσι ώστε ένας χρήστης του πρώτου συστήματος να μπορεί να λάβει υπηρεσίες από το δεύτερο σύστημα, πρέπει να προστεθούν στο σύστημα ειδικοί προσαρμογείς[40]. Ένας διασυνοριακός προσαρμογέας αναλαμβάνει στην πραγματικότητα να προωθήσει (proxying) μια ηλεκτρονική αίτηση ελέγχου ταυτότητας από τον τοπικό πάροχο υπηρεσιών (B) διασυνοριακά μεταξύ των χωρών αλλά και των συστημάτων στον ανάλογο διαχειριστή του συστήματος. Στην διαδικασία αυτή μπορεί να περιλαμβάνεται η μετάφραση της μορφής των δεδομένων και των κανόνων των επιχειρήσεων όπου αυτό είναι απαραίτητο. Ο διασυνοριακός προσαρμογέας μπορεί να υλοποιηθεί με μια σειρά από τρόπους όπως για παράδειγμα με τη χρήση Εθνικών Υπηρεσιών Μεσολάβησης (National Proxy Servers), Εθνικών Πυλών (National Portals) ή με την χρήση κάποιας εφαρμογής διαμεσολάβησης μεταξύ των δύο συστημάτων (middleware). Για κάθε ένα διασυνοριακό σύστημα πρέπει να βρίσκεται η καταλληλότερη λύση για την υλοποίηση του. Η εξεύρεση της ιδανικής λύσης δεν είναι

τόσο τεχνολογικό ζήτημα όσο ζητημάτων που σχετίζονται με τους νόμους και τις συμβάσεις- συμφωνίες που συνάπτονται μεταξύ των συστημάτων.

Ο προσαρμογέας για τα token ( token adapter) είναι το δεύτερο στοιχείο που σχετίζεται ειδικά με τη διασυνοριακή λύση του συστήματος. Το κύριο καθήκον του είναι η διασύνδεση ενός token από μια χώρα με τον πάροχο υπηρεσιών χρήστη από μια άλλη χώρα. Είναι υπεύθυνος για την λειτουργία της συμβατότητας του token με τα συστήματα του παρόχου υπηρεσιών χρήστη. Μπορεί να θεωρηθεί ως μια επέκταση των πληροφοριακών συστημάτων του τοπικού φορέα παροχής υπηρεσιών.

Συγκρίνοντας το γενικό μοντέλο ενός διασυνοριακού συστήματος ελέγχου ταυτότητας με το εγχώριο σύστημα είναι εμφανείς κάποιες αλλαγές στις γενικές αρχές του σχεδιασμού του συστήματος και οι οποίες σχετίζονται με κάθε είδους αξιολόγηση της ασφάλειας του συστήματος. Ένα διασυνοριακό σύστημα:

• είναι ετερογενές όσον αφορά στην τεχνολογία,

• διέπεται από δύο ξεχωριστά και εν μέρει τουλάχιστον διαφορετικά σύνολα νόμων,

«δεν γνωρίζει» όλους τους συμμετέχοντες του συστήματος, δηλαδή είναι δυνητικά ανοικτό και σε μη συμμετέχοντες.

## 5.2 Προστασία Ιδιωτικότητας (privacy)

### 5.2.1 Θέματα Ασφάλειας στην Διασυνοριακή Ταυτοποίηση

Τα διεθνή πρότυπα για την αξιολόγηση της ασφάλειας των πληροφοριών και πληροφοριακών συστημάτων διαχείρισης της ασφάλειας που αναφέρονται στα πρότυπα ISO της οικογένειας ISO 2700x. Τα πρότυπα αυτά παρέχουν θεμελιώδεις απαιτήσεις ασφάλειας, αν και αυτές περιγράφονται σε γενικές γραμμές. Η γερμανική Ομοσπονδιακή Υπηρεσία για την Ασφάλεια Πληροφορικής BSI (Bundesamt für Sicherheit in der Informationstechnik) έχει δημοσιεύσει μια σειρά από γερμανικά πρότυπα BSI 100 έως BSI 1 100-4 [42-44]. Αυτά είναι συμβατά με τα πρότυπα ISO 2700x αλλά πλεονεκτούν στην πρακτικότητα τους και στην παροχή πιο λεπτομερών

οδηγιών για τον τρόπο αξιολόγησης ζητημάτων ασφάλειας και της δημιουργίας ενός κατάλληλου συστήματος διαχείρισης της ασφάλειας και των μέτρων ασφαλείας.

Ο βασικότερο σημείο σε κάθε αξιολόγηση ασφάλειας, σύμφωνα με τη μεθοδολογία που περιγράφεται στο BSI 100-2 IT-(Grundschutz Methodology) είναι ο ορισμός των αγαθών ή περιουσιακών στοιχείων (assets) που πρέπει να προστατευθούν και οι απαιτήσεις για την προστασία των εν λόγω περιουσιακών στοιχείων. Ως αγαθά αναφέρονται όλα δεδομένα τα οποία αξίζουν προστασία, καθώς και για τα συστήματα που τα επεξεργάζονται, τα αποθηκεύουν και τα μεταφέρουν. Για κάθε αγαθό έχει εκχωρηθεί κάποια απαίτηση προστασίας για τις τρεις βασικές αξίες της προστασίας: της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας[41]. Στον σχήμα 15 περιγράφονται οι βασικές αξίες προστασίας και οι κατηγορίες των απαιτήσεων προστασίας.

| Protection requirement categories[3] | | |
|---|---|---|
| **ENISA** | **BSI-100-2** | **Description** |
| Low | Normal | The impact of any loss or damage is limited and calculable. |
| Medium | High | The impact of any loss or damage may be considerable. |
| High | Very High | The impact of any loss or damage can attain catastrophic proportions. |

| Basic protection values according to ISO/IEC 27002 [27] | |
|---|---|
| Confidentiality | ensuring that information is accessible only to those authorised to have access |
| Integrity | safeguarding the accuracy and completeness of information and processing methods |
| Availability | ensuring that authorised users have access to information and associated assets when required |

**Σχήμα 15: Βασικές αξίες και απαιτήσεις προστασίας δεδομένων**

Για να οριστούν οι απαιτήσεις για την προστασία ενός περιουσιακού στοιχείου, αξιολογούνται τα ακόλουθα σενάρια ζημιών:

- παραβίαση των νόμων, των κανονισμών ή των συμβάσεων,

•μείωση της δυνατότητας του πληροφοριακού αυτοπροσδιορισμού (informational self-determination)[21],

• βλάβες από φυσικά αίτια,

• μειωμένη άσκηση καθηκόντων,

• αρνητικές εσωτερικές ή εξωτερικές επιδράσεις, δηλαδή, η μείωση της υπόληψης και της εμπιστοσύνης,

• οικονομικές συνέπειες.

Ένα απλό περιστατικό απώλειας ή ζημίας μπορεί να έχει αντίκτυπο σε διάφορα σενάρια ζημιών (π.χ. μία απάτη συνήθως παραβιάζει νόμους ή συμβάσεις και έχει οικονομικές συνέπειες). Κατά γενικό κανόνα, η οδηγία BSI 100-2 ακολουθεί την «αρχή του μεγαλύτερου» (maximum principal), δηλαδή εάν διάφορα σενάρια βλάβης αποδίδονται σε διαφορετικές κατηγορίες απαιτήσεων προστασίας για οποιαδήποτε αξία προστασίας, λαμβάνεται υπόψη η υψηλότερη κατηγορία.

### 5.2.2 Προσωπικά Δεδομένα

Τα δεδομένα που σχετίζονται άμεσα με την ταυτότητα ενός προσώπου θα πρέπει να θεωρούνται ως αγαθά που είναι άξια προστασίας σε κάθε περίπτωση. Με τα δεδομένα προσωπικού χαρακτήρα, η κύρια ανησυχία είναι η εμπιστευτικότητα δεδομένου ότι η χρήση των προσωπικών δεδομένων περιορίζεται από την οδηγία για την προστασία των δεδομένων (95/46/ΕΚ). Η κατηγορία ανάγκης προστασίας εξαρτάται σε μεγάλο βαθμό από την εφαρμογή και την ποσότητα και το είδος των προσωπικών δεδομένων που μεταδίδονται μέσα από ένα διασυνοριακό σύστημα. Είναι προφανές ότι το όνομα, η διεύθυνση και η ημερομηνία γέννησης ενός ατόμου είναι λιγότερο κρίσιμα από κάποια άλλα δεδομένα προσωπικού χαρακτήρα, όπως η οικονομική κατάσταση, το ποινικό ή ιατρικό ιστορικό. Στο σχήμα 16 περιγράφονται οι απαιτήσεις ασφάλειας που αφορούν τα προσωπικά δεδομένα, καθώς και τα βασικότερα σενάρια βλαβών.

[21] “The right of the individual to decide what information about himself should be communicated to others and under what circumstances” The Right to Privacy" (Warren and Brandeis,1970)

| Personal data | | Personal data: yes |
|---|---|---|
| **Protection requirements** | | **Rationale** |
| Confidentiality | At least 'medium' | Due to the Data Protection Directive and the laws of Member States, any personal data is restricted in usage and distribution. |
| Integrity | At least 'low' | Impact of any loss of integrity is limited and calculable. |
| Availability | At least 'low' | Only has limited or no impact if system is not available for several days. |
| **Major damage scenarios:** | | |
| Confidentiality: abuse of personal data for non-system purposes | | |
| Confidentiality: misuse of person-related data has effect on social or financial standing | | |
| Integrity: identity theft | | |
| Integrity: impaired performance of duties due to false data | | |
| Integrity: falsification of person-related data has effect on social or financial standing | | |
| Availability: impaired performance of duties | | |
| Availability: increased cost of performance of duties | | |
| Availability: unavailability of service has effects on social or financial standing of individual | | |

**Σχήμα 16: Απαιτήσεις προστασίας προσωπικών δεδομένων**

### 5.2.3 Γενικές Απειλές (Generic Threats)

Κατά τον σχεδιασμό οποιουδήποτε συστήματος διασυνοριακής ταυτοποίησης θα πρέπει να λαμβάνονται υπόψη οι παρακάτω τεχνικοί κίνδυνοι (technical security risks) που αφορούν την ασφάλεια του συστήματος[41]:

•Η χρήση διαφορετικών τύπων διαπιστευτηρίων με διαφορετική αξιοπιστία μπορεί να οδηγήσει σε παραποιημένα δεδομένα προσωπικού χαρακτήρα και αναξιόπιστα tokens.

•Tokens με διαφορετικά επίπεδα ασφάλειας διαφέρουν στην αξιοπιστία τους.

•Μη έμπιστοι πάροχοι υπηρεσιών ή διασυνοριακοί προσαρμογείς μπορεί να οδηγήσουν σε ανάκληση και κακή χρήση δεδομένων προσωπικού χαρακτήρα καθώς και σε αποθήκευση τους για προσωπικό όφελος.

•Διαφορετικές τεχνικές υποδομές και διαφορετικά πρωτόκολλα αυθεντικοποίησης αυξάνουν τον αριθμό των τρωτών σημείων της ασφάλειας λόγω των διαφορετικών τους επιπέδων ασφάλειας.

•Οι επιθέσεις «Man-in-the-middle», όπου ένας επιτιθέμενος εισάγει τον εαυτό του μεταξύ του υπολογιστή ή του τερματικού του χρήστη κάπου στο δίκτυο κατά την διαδικασία αυθεντικοποίησης και θέτει τον εαυτό του ως πάροχο υπηρεσιών στο διαχειριστή του συστήματος και το αντίστροφο είναι δυνητικά πιο εύκολες.

•Παράνομος εντοπισμός της θέσης ή της συμπεριφοράς του χρήστη, όπου ο εισβολέας μπορεί να δημιουργήσει ένα προφίλ για τον χρήση χρησιμοποιώντας για παράδειγμα την θέση του αναγνώστη της ηλεκτρονικής ταυτότητας, τον χρόνο χρήσης, κλπ.

•Επιθέσεις που σχετίζονται με τη διαθεσιμότητα της διασυνοριακής διαδικασίας αυθεντικοποίησης με τη δημιουργία αυξημένου αριθμού πλαστών αιτήσεων ελέγχου ταυτότητας που μπορεί να επιφέρουν κατάσταση άρνησης παροχής υπηρεσιών (denial of service attack).

•Τα πρόσθετα συστήματα που εμπλέκονται στην διασυνοριακή διαδικασία ελέγχου ταυτότητας μπορεί να μην είναι αξιόπιστα.

## 5.3 Προκλήσεις για την Διασυνοριακή Ταυτοποίηση

Η επέκταση ενός εθνικού συστήματος ΗΤ έτσι ώστε να επιτρέπει την διασυνοριακή ΗΤ χρηστών σε συνεργασία με κάποιον πάροχο υπηρεσιών ο οποίος δεν ανήκει στο ίδιο κράτος, θέτει μια σειρά νομικών και τεχνικών προκλήσεων κάποιες από τις οποίες περιγράφονται παρακάτω. Οι προκλήσεις αυτές πρέπει να αντιμετωπιστούν και να ξεπεραστούν με επιτυχία ώστε να επιτευχτεί η διασυνοριακή διαλειτουργικότητα:

- Μπορεί να υπάρχουν διαφορετικοί τύποι διαπιστευτηρίων που συνδέουν την ταυτότητα του χρήστη με ένα token. Έτσι, μέθοδοι βιομετρικής επαλήθευσης όπως για παράδειγμα τα δακτυλικά αποτυπώματα, μπορεί να δημιουργήσουν

σοβαρά προβλήματα όσον αφορά την τεχνολογία του συστήματος και την ασφάλεια του.

- Η αξιοπιστία των διαπιστευτηρίων μπορεί να διαφέρει. Αυτό μπορεί να δημιουργήσει προβλήματα που σχετίζονται με τη διαχείριση των διαφορετικών επιπέδων αξιοπιστίας αλλά και με νομικά ζητήματα.
- Υπάρχουν και χρησιμοποιούνται ευρεία φάσματα διαφορετικών tokens:
    1. Ηλεκτρονικά και μη ηλεκτρονικά tokens με διαφορετικά επίπεδα ασφάλειας
    2. Tokens με διαφορετικά επίπεδα εγκυρότητας.
    3. Tokens από προηγούμενα και / ή συναφή συστήματα
    4. Tokens που λειτουργούν με διαφορετικά σύνολα δεδομένων
    5. Tokens που έχουν εκδοθεί από διαφορετικούς φορείς του συστήματος ή για λογαριασμό των κυβερνήσεων

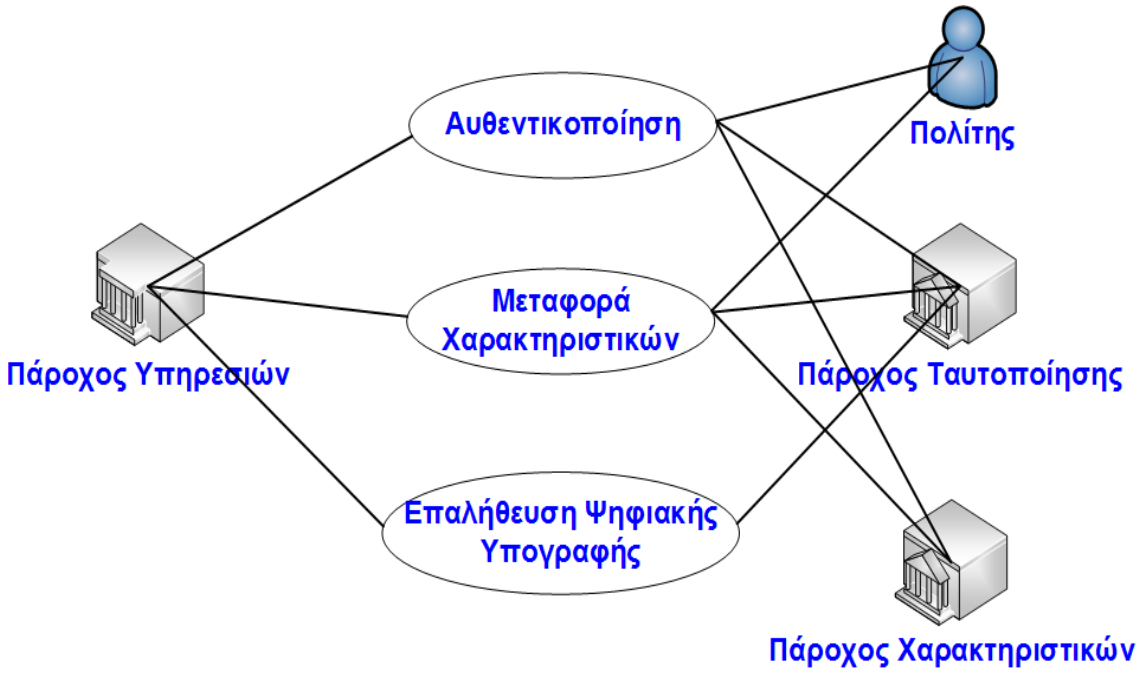
Ακόμη και εντός ενός εσωτερικού εθνικού συστήματος μπορεί να χρησιμοποιείται ένας μεγάλος αριθμός από διαφορετικά tokens,για το σύνολο των οποίων ενδέχεται να απαιτείται η υποστήριξη τους σε ένα διασυνοριακό σενάριο.

- Χρησιμοποιούνται διαφορετικές τεχνικές υποδομές και εξοπλισμός σε κάθε κράτος. Αν και αυτό φαίνεται να είναι κυρίως ένα τεχνολογικό ζήτημα, οι οικονομικές συνέπειες που προκύπτουν για την υποστήριξη αυτών των τεχνολογιών μπορεί να αποδειχθούν το μεγαλύτερο πρόβλημα.
- Έχουν ακολουθηθεί διαφορετικά πρωτόκολλα και διαδικασίες ελέγχου ταυτότητας. Αυτό δεν είναι μόνο ένα τεχνολογικό πρόβλημα, αλλά μπορεί να είναι και ένα νομικό ζήτημα.
- Διαφορετικά σύνολα των δεδομένων προσωπικού χαρακτήρα προέρχονται από διαφορετικές χώρες. Αφορά τεχνολογικά ζητήματα όπως η μορφή και η χρήση των αναγνωριστικών.

- Η αποδοχή και εμπιστοσύνη των δεδομένων προσωπικού χαρακτήρα που προέρχονται από μια ξένη χώρα. Αυτό αφορά κυρίως νομικά ζητήματα και ζητήματα εμπιστοσύνης καθώς και το γεγονός ότι ένας πάροχος υπηρεσιών πρέπει να αποδεχθεί τον διαχειριστή του συστήματος του άλλου κράτους ως μία διαπιστευμένη αρχή.
- Μπορεί να απαιτηθεί έλεγχος της γνησιότητας ενός ξένου token. Ενδέχεται να χρειαστεί να υλοποιηθούν διαδικασίες μέσα από τις οποίες να ελέγχεται η γνησιότητα των ξένων token πριν από την διαδικασία της ΗΤ.
- Μπορεί να απαιτηθεί έλεγχος της άδειας των ξένων φορέων παροχής υπηρεσιών. Πριν από την απάντηση μιας αίτησης ελέγχου ταυτότητας, ο διαχειριστής του συστήματος πρέπει να βεβαιωθεί ότι ο πάροχος υπηρεσιών που δημιουργεί το αίτημα έχει την αρμοδιότητα να εκτελέσει αυτή την αίτηση ελέγχου ταυτότητας

# Κεφάλαιο 6 ΑΝΑΛΥΣΗ ΑΠΑΙΤΗΣΕΩΝ & ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΛΕΙΤΟΥΡΓΙΚΩΝ ΥΠΟΔΟΜΩΝ ΗΤ

## 6.1 Γενικές Απαιτήσεις Διαλειτουργικών Υποδομών ΗΤ




Σχήμα 17: Διαδικασίες ΗΤ

Τα κυριότερα μέρη που συμμετέχουν σε μια διαδικασία ΗΤ είναι:

- Ο πολίτης ο οποίος αιτείται πρόσβασης σε κάποιο προστατευμένο πόρο ή υπηρεσία.
- Ο πάροχος υπηρεσιών (service provider) ο οποίος είναι αυτός που προσφέρει την υπηρεσία καθώς και
- Ο πάροχος ταυτοποίησης (identity provider) ο οποίος πιστοποιεί ηλεκτρονικά την ταυτότητα του πολίτη.

Στην διαδικασία μπορεί να λαμβάνει μέρος και ένας ή περισσότεροι πάροχοι χαρακτηριστικών για την μεταφορά προς τον πάροχο υπηρεσιών κάποιων επιπλέον χαρακτηριστικών του πολίτη. Σε πολλές περιπτώσεις η λειτουργία του παρόχου χαρακτηριστικών υλοποιείται από τον πάροχο ταυτοποίησης.

Οι επιμέρους διαδικασίες που συντελούν για την ΗΤ είναι η αυθεντικοποίηση και η μεταφορά των χαρακτηριστικών. Σε ορισμένες περιπτώσεις παροχής υπηρεσιών είναι απαραίτητη και η επαλήθευση της ψηφιακής υπογραφής του πολίτη.

**1. Αυθεντικοποίηση και Ταυτοποίηση (Authentication and Identification):** είναι η διαδικασία επαλήθευσης της ταυτότητας ενός συγκεκριμένου χρήστη. Αυτό επιτυγχάνεται ζητώντας από τον χρήστη πληροφορίες που αποδεικνύουν την ταυτότητά του. Μετά την ολοκλήρωση της διαδικασίας επαλήθευσης της ταυτότητας του, επιτρέπεται η πρόσβαση του χρήστη σε προνομιακά δεδομένα. Συνήθως αυτή η διαδικασία τελειώνει με έναν πλήρως ταυτοποιημένο χρήστη, που σημαίνει ότι ηλεκτρονικό αναγνωριστικό του (eID) μεταφέρεται στο φορέα παροχής υπηρεσιών (SP), και αυτός ο SP αναγνωρίζει τον χρήστη αυτόν με οποιαδήποτε σχέση μπορεί να έχει ο χρήστης τον SP (πελάτης, μαθητής, συνεργάτη κλπ) .

**2. Μεταφορά Χαρακτηριστικών (Attribute Transfer):** είναι η διαδικασία που επιτρέπει σε έναν φορέα παροχής υπηρεσιών να αποκτήσει πρόσβαση σε επιπλέον χαρακτηριστικά διαφορετικά από εκείνα που απαιτούνται για το βασικό έλεγχο της ταυτότητας μέσω κάποιου παρόχου χαρακτηριστικών (AP). Αυτή η διαδικασία προϋποθέτει έναν πλήρως ταυτοποιημένο χρήστη αλλά για λόγους προστασίας προσωπικών δεδομένων, το eID του δεν αναγνωρίζεται από τον SP ως γνωστό. Σε μία τέτοια περίπτωση ο χρήστης θα πρέπει να ταυτοποιηθεί για δεύτερη φορά από τον πάροχο ταυτοποίησης και να δώσει την συγκατάθεση του για την μεταφορά των επιπλέον χαρακτηριστικών. Τα χαρακτηριστικά που μπορεί να ζητηθούν είναι οποιοσδήποτε συνδυασμός τύπων δεδομένων. Η συγκατάθεση αυτή του χρήστη για την μεταφορά των δεδομένων του εφαρμόζεται σύμφωνα με τις νομικές απαιτήσεις για την προστασία των δεδομένων του κάθε κράτους μέλους.

**3. Επικύρωση Πιστοποιητικού (Certificate validation):** είναι η διαδικασία μέσα από την οποία δίνεται η δυνατότητα σε έναν πάροχο υπηρεσιών (SP) να ελέγξει την ψηφιακή υπογραφή κάποιου χρήστη.

## 6.2 Εναλλακτικές Αρχιτεκτονικές Διαλειτουργικών υποδομών ΗΤ (PEPS, Middleware)

Μετά την ανάπτυξη των μοντέλων της διαλειτουργικότητας και του οδικού χάρτη για την ΗΤ που παρουσιάστηκαν από το σχέδιο δράσης eEurope 2005, το πρόγραμμα IDABC ανέλαβε μέσα από το σχέδιο δράσης i2010, να αναλύσει τις απαιτήσεις διαλειτουργικότητας για την διασυνοριακή ηλεκτρονική ταυτοποίηση.

Κατά την ανάλυση αυτή θα έπρεπε να επισημανθούν οι απαιτούμενες λειτουργίες διαλειτουργικότητας για την επίτευξη της ΗΤ, να προταθούν λύσεις οι οποίες θα βασιζόταν στις ήδη υπάρχουσες τεχνολογίες και να προταθούν οι κοινές προδιαγραφές για την διασυνοριακή ΗΤ στην ΕΕ. Το IDABC είχε την υποστήριξη ομάδας εμπειρογνωμόνων και χρησιμοποίησε τα αποτελέσματα προηγούμενων δράσεων της ΕΕ για την ηλεκτρονική ταυτοποίηση. Μερικές από τις δράσεις αυτές ήταν η μελέτη *Modinis*[22] για την διαχείριση της ταυτοποίησης στην ΗΔ (Study on ID Management in eGovernment), το έργο *GUIDE*[23] (Gentle user interfaces for elderly people), FIDIS[24]( Future of Identity in the Information Society) and *PRIME*[25] (Privacy and Identity Management for Europe), καθώς και τα αποτελέσματα των εργασιών της ομάδας *Porvoo Group*[26] .

Ένα μοντέλο που προτάθηκε από το IDABC ήταν η εγκαθίδρυση εθνικών πυλών, που ονομάστηκαν Πανευρωπαϊκοί Διακομιστές Υπηρεσιών PEPS (Pan European Proxy Service) [45]. Οι κύριοι στόχοι αυτών των πυλών είναι:

[22] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi
[23] http://www.guide-project.eu/
[24] http://www.fidis.net/
[25] https://www.prime-project.eu/
[26] http://www.fineid.fi/default.aspx?id=539

• Να αποκρύψουν τα εθνικά εσωτερικά προβλήματα των συστημάτων από τα άλλα κράτη μέλη.

• Να είναι ένας σύνδεσμος εμπιστοσύνης, ο οποίος να επιτρέπει την αξιοποίηση του εθνικού κύκλο εμπιστοσύνης της Ευρώπη (circle of trust).

Επιπλέον, αυτές οι πύλες θα εγγυώνται την επεκτασιμότητα, καθώς οποιαδήποτε αλλαγή εσωτερικά σε ένα κράτος μέλος θα επηρεάζει μόνο τη δική του πύλη.

Ένα ακόμη μοντέλο HT το οποίο είχε εφαρμογή στην Γερμανία και την Αυστρία είναι το μοντέλο Middleware (MW). Το μοντέλο αυτό είναι περισσότερο προσανατολισμένο προς τον χρήστη έχοντας ο ίδιος στην κατοχή του τα διαπιστευτήρια για την ταυτοποίηση του. Για να μπορέσει όμως σε ένα διασυνοριακό σενάριο ένας πάροχος ταυτοποίησης από ένα άλλο κράτος να προσφέρει την υπηρεσία του, θα πρέπει να εγκαταστήσει έναν κατάλληλο διακομιστή στο δικό του επιχειρησιακό περιβάλλον [46].

Ορισμένες χώρες διέκριναν κάποια προβλήματα στην υιοθέτηση μιας λύσης με τη χρήση PEPS, είτε νομικά είτε αξιοπιστίας και ασφάλειας καθώς και προβλήματα συμβατότητας με τις εθνικές τους πύλες στις περιπτώσεις που αυτές υλοποιούνταν μέσω της αποκεντρωμένης αρχιτεκτονικής Middleware. Κατά την αποκεντρωμένη αρχιτεκτονική ο κάθε πάροχος υπηρεσιών έχει εγκατεστημένο λογισμικό (μερικές φορές αναφέρεται ως SPware), το οποίο αλληλεπιδρά με τα διαπιστευτήρια του χρήστη μέσω κάποιου ενδιάμεσου λογισμικού εγκατεστημένου στον υπολογιστή του χρήστη.

Η άμεση επικοινωνία μεταξύ των παρόχων υπηρεσιών και των χρηστών χρησιμοποιώντας απευθείας τα ειδικά SPwares του εκάστοτε κράτους μέλους δημιουργεί προβλήματα επεκτασιμότητας του συστήματος αλλά και προβλήματα εμπιστοσύνης σε ένα διασυνοριακό σενάριο:

- Πρώτα απ ‘όλα, εμφανίζονται προβλήματα που αφορούν την επεκτασιμότητα και την βιωσιμότητα του συστήματος, καθώς θα πρέπει όλοι οι πάροχοι υπηρεσιών να υποστηρίζουν έναν μεγάλο και διαρκώς αυξανόμενο αριθμό

διεπαφών SPware από κάθε χώρα, με όλες τις αντίστοιχες συνέπειες συντήρησης που αυτό επιφέρει.

- Επίσης, θα πρέπει να όλοι οι πάροχοι υπηρεσιών να ενημερώνουν τις λίστες στις οποίες αποθηκεύουν τους έμπιστους (ID) τους διακομιστές, κάθε φορά που ένας νέος πάροχος ID αναγνωρίζεται σε οποιαδήποτε από αυτές τις χώρες που χρησιμοποιούν την αρχιτεκτονική Middleware.

Για να αντιμετωπιστούν αυτά τα προβλήματα, ενσωματώθηκε ένα αφαιρετικό επίπεδο πάνω από τα SPwares το οποίο επιτρέπει τους SP να υποστηρίζουν οποιοδήποτε αριθμό SPwares χρησιμοποιώντας μια ενιαία διεπαφή και προσθέτοντας στο σύστημα μία μόνο συνιστώσα, η οποία ονομάστηκε εικονικός πάροχος ταυτότητας (Virtual IDP), ή V-IDP. Ο V-IDP έχει τους ίδιους στόχους με έναν PEPS, δηλαδή αποσκοπεί στο να κρύψει τα εσωτερικά εθνικά προβλήματα από τα άλλα κράτη μέλη και να είναι ένας σύνδεσμος εμπιστοσύνης που να επιτρέπει την ενδυνάμωση του κύκλου εμπιστοσύνης των κρατών μελών στην Ευρώπη. Η κύρια διαφορά είναι το σημείο στο οποίο υλοποιούνται τα δύο συστήματα: πρέπει να βρίσκεται όσο το δυνατόν πλησιέστερα προς τον πάροχο υπηρεσιών επιτρέποντας με αυτόν τον τρόπο μία «end-to-end» επικοινωνία μεταξύ του παρόχου υπηρεσιών και του χρήστη, αλλά να επιτρέπει επίσης και την χρήση των εθνικών πυλών της κάθε χώρας.

Τα δύο μοντέλα διαλειτουργικότητας Middleware (MW) και Pan-European Proxy Service (PEPS) διερευνηθήκαν και λειτούργησαν πιλοτικά μέσα από το πρόγραμμα STORK, το οποίο συνδύασε τα μοντέλα αυτά με όλους τους δυνατούς τρόπους (MW => MW, PEPS => PEPS, MW => PEPS, PEPS => MW). Οι κοινές προδιαγραφές των προτεινόμενων μοντέλων διαλειτουργικότητας έχουν σχεδιαστεί με τέτοιο τρόπο ώστε τα βασικά συστήματα τους να λειτουργούν με τα ίδια πρωτόκολλα, ανεξάρτητα από το μοντέλο ή συνδυασμούς αυτών.

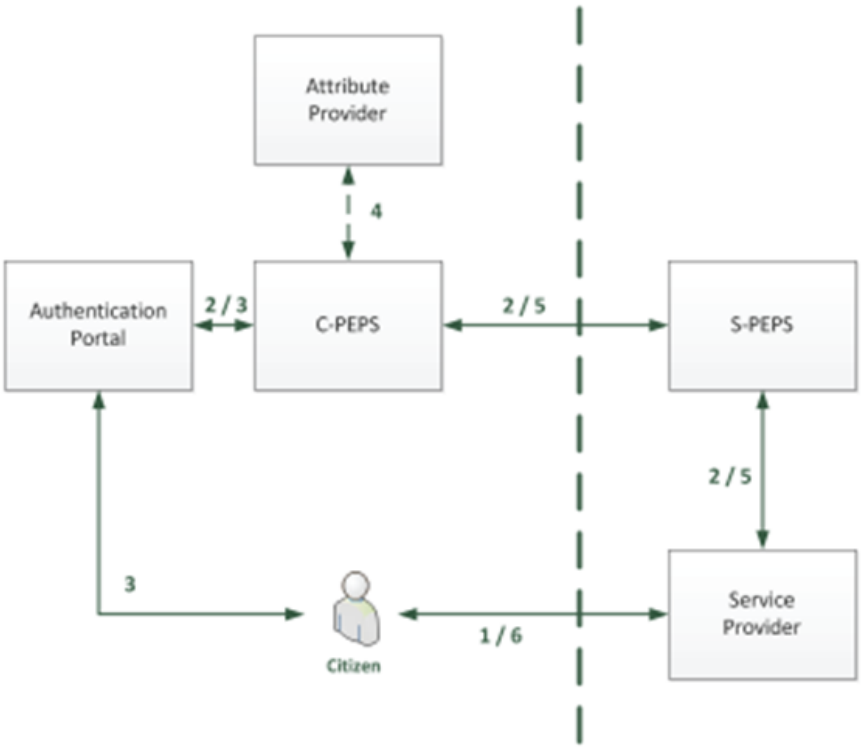
Στις παρακάτω υποενότητες περιγράφονται και στην συνέχεια συγκρίνονται τα δύο αυτά αρχιτεκτονικά μοντέλα.

### 6.2.1 Πανευρωπαϊκός Διακομιστής Υπηρεσιών (PEPS)

Σε αντίθεση με το προσανατολισμένο προς τον χρήστη μοντέλο MW, το μοντέλο της διαλειτουργικότητας PEPS χρησιμοποιεί μια προσέγγιση βασισμένη στην ύπαρξη μιας ομοσπονδίας διαμεσολαβητών. Σύμφωνα με το [47], κάθε ευρωπαϊκό πλαίσιο διαλειτουργικότητας πρέπει να εκτελεί μια σειρά από βασικές λειτουργίες. Σε αυτές συμπεριλαμβάνονται ο προσδιορισμός ενός τοπικού παρόχου ταυτότητας, η ανάκτηση των χαρακτηριστικών ταυτότητας και η μεταφορά αυτών των χαρακτηριστικών σε ένα αξιόπιστο φορέα παροχής υπηρεσιών διασυνοριακά. Μια υπηρεσία η οποία υλοποιεί τις παραπάνω λειτουργίες ονομάζεται Πανευρωπαϊκός Διακομιστής Υπηρεσιών PEPS (Pan-European Proxy Service). Ένας PEPS μπορεί να θεωρηθεί ως μια ενιαία πύλη, η οποία από τη μια πλευρά κρύβει τις πολυπλοκότητες των επιμέρους εθνικών υποδομών και από την άλλη πλευρά υλοποιεί το πρωτόκολλο διασυνοριακής επικοινωνίας. Το σχήμα 18 απεικονίζει η λογική της διασυνοριακής διαδικασίας ελέγχου ταυτότητας μέσα από την αρχιτεκτονική PEPS. Η ροή των δεδομένων μεταξύ των εμπλεκόμενων φορέων στην πραγματικότητα υλοποιείται μέσω του φυλλομετρητή του χρήστη. Ως εκ τούτου, το πρωτόκολλο ελέγχου ταυτότητας STORK έχει σχεδιαστεί με τέτοιο τρόπο ώστε τα δεδομένα ταυτότητας μεταξύ των διαφόρων φορέων να ανταλλάσσονται και να διαβιβάζονται χρησιμοποιώντας εντολές τύπου HTTPs POSTs που πραγματοποιούνται από το πρόγραμμα περιήγησης του χρήστη.

Στο σχήμα 18 εξετάζεται το σενάριο όπου ο χρήστης από το κράτος μέλος Α θέλει να αυθεντικοποιηθεί σε έναν φορέα παροχής υπηρεσιών που εδρεύει στο κράτος μέλος Β. Στο σενάριο αυτό, τόσο κράτος μέλος που εδρεύει ο πάροχος υπηρεσιών όσο και το κράτος μέλος από το οποίο προέρχεται ο χρήστης χρησιμοποιούνε την αρχιτεκτονική PEPS. Το κομμάτι του PEPS του κράτους μέλους Α ονομάζεται C-PEPS (Citizens- PEPS) το οποίο αναφέρεται στην χώρα προέλευσης του πολίτη ενώ το κομμάτι του PEPS του κράτους μέλους Β ονομάζεται S-PEPS (Service Provider PEPS) που αναφέρεται στην χώρα προέλευσης του πάροχου υπηρεσιών. Τα C-PEPS και οι S-PEPS έχουν μια σχέση εμπιστοσύνης μεταξύ τους. Το ίδιο ισχύει και μεταξύ των S-PEPS και του παρόχου υπηρεσιών. Η διαδικασία επαλήθευσης ταυτότητας είναι η εξής:

- Ο χρήστης επιθυμεί να αποκτήσει πρόσβαση σε ένα προστατευμένο πόρο του παρόχου υπηρεσιών (1),
- ο πάροχος υπηρεσιών προωθεί την διαδικασία αυθεντικοποίησης στο αντίστοιχο S-PEPS,
- Το S-PEPS προωθεί με την σειρά του τη διαδικασία ελέγχου ταυτότητας στο αντίστοιχο C-PEPS (2) της χώρας προέλευσης του χρήστη.
- Η αυθεντικοποίηση του χρήστη πραγματοποιείται στο C-PEPS ή σε κάποιον άλλον εθνικό πάροχο ταυτότητας πίσω από αυτό(3).
- Το C-PEPS μπορεί να ανακτήσει επίσης πρόσθετες πληροφορίες ταυτότητας από κάποιον πάροχο χαρακτηριστικών (4).
- Η αυθεντικοποίηση της ταυτότητας του χρήστη και των πληροφοριών της ταυτότητάς του, μεταφέρονται από το C-PEPS πίσω στο S-PEPS (5)
- Το S-PEPS προωθεί τελικά τις πληροφορίες αυτές στον αιτούμενο πάροχο υπηρεσιών (5).
- Ο χρήστης έχει πλέον πρόσβαση στον πόρο που ζήτησε.




**Σχήμα 18: Λογικό διάγραμμα λειτουργίας PEPS στο STORK [46]**

Ένας PEPS μιας χώρας συνδέει την εθνική υποδομή της ηλεκτρονικής ταυτότητας της χώρας με τους παρόχους υπηρεσιών εκτός αυτής, καθώς και τους εθνικούς φορείς παροχής υπηρεσιών της με υποδομές διαχείρισης ηλεκτρονικής ταυτότητας άλλων χωρών. Στην λειτουργία ενός τέτοιου μοντέλου HT, ο χρήστης παίζει σημαντικό ρόλο καθώς χωρίς τη συμμετοχή του δεν υπάρχει κανένας τρόπος ανταλλαγής δεδομένων.

Κατά την επικοινωνία δύο PEPSes ο ένας έχει το ρόλο του S-PEPS, προκειμένου να παρακολουθεί και να εκτελεί τις αιτήσεις των παρόχων υπηρεσιών από τη χώρα όπου προέρχονται, και ο άλλος έχει το ρόλο του C-PEPS, ο όποιος φροντίζει για την διεπαφή με τον πολίτη στη χώρα προέλευσής του. Ακόμη, στον τελευταίο αυτό ρόλο

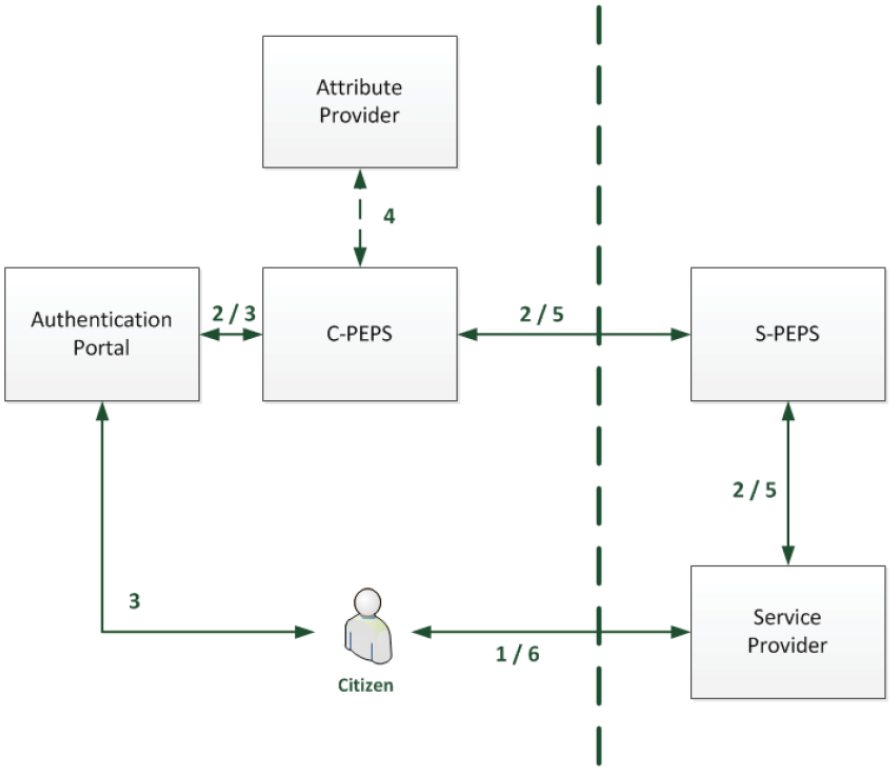
προστίθεται και η φροντίδα για την διεπαφή με τον πάροχο ταυτότητας καθώς και με ενδεχόμενους πρόσθετους παρόχους χαρακτηριστικών ταυτότητας.

Αξίζει να σημειωθεί τα ενδιάμεσα βήματα ανακατεύθυνσης από τον πάροχο υπηρεσίων προς τον C PEPS διάμεσου του φυλλομετρητή του χρήστη και μέσω του S-PEPS παρότι γίνονται δύο φορές, αυτά είναι διαφανή για τον χρήστη. Οι ρόλοι, S-PEPS και C-PEPS μπορούν επίσης να εντοπιστούν και στη δομή του λογισμικού PEPS αλλά και στους υποδοχείς των ερωτημάτων. Υπό κανονικές συνθήκες σε μια διασυνοριακή συναλλαγή, ένας PEPS θα αναλάβει μόνο έναν από τους παραπάνω ρόλους. Μόνο στην περίπτωση όπου η χώρα του παρόχου υπηρεσιών και η χώρα προέλευσης πολιτών είναι η ίδια ο PEPS θα αναλάβει και τους δύο ρόλους. Αλλά καθώς αυτό το σενάριο δεν είναι διασυνοριακό είναι εκτός του πεδίου εφαρμογής του STORK και σε είναι πιθανό σε ορισμένες χώρες να μην μπορέσει να λειτουργήσει.

### 6.2.2 Αρχιτεκτονική Middleware (MW)

Το σχήμα 19 απεικονίζει η αρχιτεκτονική Middleware (MW). Αυτή η αρχιτεκτονική είναι προσανατολισμένη προς τον χρήστη (user-centric) καθώς τα δεδομένα της ταυτότητάς του αποθηκεύονται ή προσπελαύνονται συνήθως με tokens τα οποία είναι στην αποκλειστική κατοχή του χρήστη, όπως για παράδειγμα μια έξυπνη κάρτα ή ένα κινητό τηλέφωνο. Η επικοινωνία με το token συνήθως παρέχεται μέσω ενός πελάτη MW ο οποίος επιτρέπει στον χρήστη να επιβεβαιώσει τη διαδικασία ελέγχου ταυτότητας με έναν Προσωπικό Αριθμό Αναγνώρισης (PIN) ή Αριθμό Συναλλαγής (TAN)[46, 48].

Στην αρχιτεκτονική MW, οι πάροχοι υπηρεσιών για να μπορέσουν να υποστηρίξουν την διασυνοριακή αυθεντικοποίηση, πρέπει να εγκαταστήσουν έναν διακομιστή MW στο περιβάλλον λειτουργίας τους. Αυτό το λογισμικό θα είναι υπεύθυνο για το χειρισμό της διαδικασίας ελέγχου ταυτότητας μεταξύ του χρήστη και του MW πελάτη. Ως εκ τούτου, το κομμάτι του MW που αφορά τους παρόχους υπηρεσιών (server-side MW) πρέπει να είναι σε θέση να πραγματοποιεί τους μηχανισμούς ελέγχου ταυτότητας για όλους τους τύπους tokens που υποστηρίζει και για κάθε χώρα.




**Σχήμα 19 : Μοντέλο MW [46]**

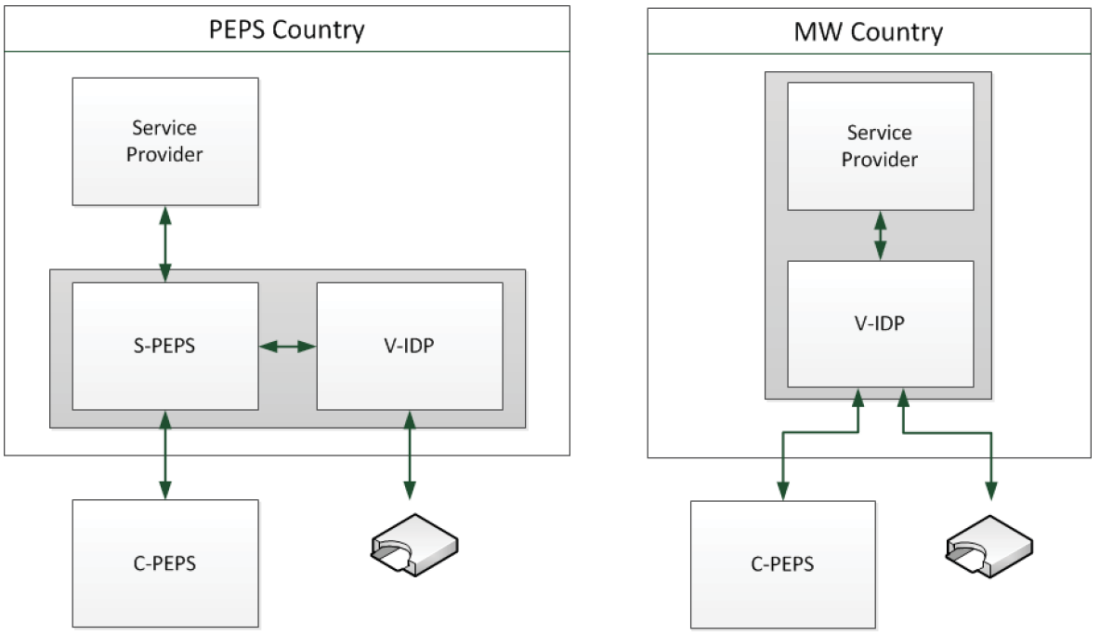
Ωστόσο, η διαφύλαξη της ιδιωτικής ζωής είναι μια σημαντική πτυχή και στα δύο μοντέλα. Για να είναι συμβατά τα δύο μοντέλα με την Οδηγία της ΕΕ για την προστασία των δεδομένων (95/46/EC) και στις δύο περιμένουν οι χρήστες πρέπει να δώσουν τη συγκατάθεσή τους για την χρησιμοποίηση των δεδομένων τους στο εξωτερικό.

### 6.2.3 Συνδυάζοντας τα δύο μοντέλα

Παρότι οι δύο αρχιτεκτονικές MW και PEPS έχουν εντελώς διαφορετικά μοντέλα λειτουργίας, μπορούν να συνδυαστούν, όπως προαναφέρθηκε, με την έννοια του εικονικού παρόχου αυθεντικοποίησης V-IDP, ο οποίος απεικονίζεται στο σχήμα 21. Ένας V-IDP είναι ένας διακομιστής MW ο οποίος περιλαμβάνει μια διεπαφή PEPS, έτσι ώστε οι δύο αρχιτεκτονικές να μπορούν να επικοινωνούν μεταξύ τους. Αυτό είναι

εφικτό δεδομένου ότι τα βασικά λειτουργικά συστατικά λειτουργούν κάτω από τα ίδια πρωτόκολλα και στις δύο αρχιτεκτονικές[46, 48].

Σύμφωνα με το σχήμα 20, μια χώρα που χρησιμοποιεί την αρχιτεκτονική PEPS μπορεί να εγκαταστήσει τον V-IDP στο περιβάλλον του S-PEPS έτσι ώστε οι χρήστες από χώρες που χρησιμοποιούν την λογική του PEPS να προωθούνται στους εθνικούς τους PEPS ενώ οι χρήστες που προέρχονται από χώρες που χρησιμοποιούν MW λογική να μπορούν να αυθεντικοποιηθούν άμεσα στον V-IDP. Τα δεδομένα από την αυθεντικοποίηση και στις δύο περιπτώσεις επιστρέφουν στην συνέχεια πίσω στο φορέα παροχής υπηρεσιών μέσα από την ίδια διεπαφή. Σε μια χώρα middleware ένας πάροχος υπηρεσιών μπορεί να εγκαταστήσει το V-IDP, έτσι ώστε οι χρήστες από χώρες με PEPS να προωθούνται στους εθνικούς τους PEPS και οι χρήστες από χώρες MW να μπορούν να αυθεντικοποιούνται άμεσα στον V-IDP. Με αυτόν τον τρόπο τόσο μπορούν να υλοποιηθούν και οι δύο συνδυασμοί MW-PEPS και PEPS-MW.




**Σχήμα 20: Θέση εικονικού παρόχου αυθεντικοποίησης V-IdP [46]**

### 6.2.4 Σύγκριση μοντέλων

Συγκρίνοντας το μοντέλο MW και το μοντέλο PEPS, διακρίνονται αρκετές διαφορές. Στο μοντέλο MW οι ξένοι χρήστες αυθεντικοποιούνται επικοινωνώντας απευθείας με τον πάροχο υπηρεσιών. Δεν υπάρχουν μεσάζοντες μεταξύ του χρήστη και του παρόχου υπηρεσιών, κάτι το οποίο επιτρέπει την εφαρμογή μεθόδων ασφάλειας end-to-end. Δεδομένου ότι τα στοιχεία ταυτότητας ανακτώνται από eID του χρήστη, ο χρήστης παραμένει ο κάτοχος των δεδομένων ενώ ο πάροχος υπηρεσιών είναι υπεύθυνος για την επεξεργασία των δεδομένων (data controller). Έτσι, το μοντέλο αυτό είναι προσανατολισμένο στο χρήστη (user centric). Αν και το μοντέλο αυτό παρέχει έναν υψηλό βαθμό προστασίας της ιδιωτικής ζωής και ασφάλειας, το μεγαλύτερο μειονέκτημα του είναι η εξάρτησή του από την διαρκή συντήρηση των eID tokens[49].

Σε αντίθεση με το μοντέλο MW, το μοντέλο PEPS περιλαμβάνει τρίτους. Από την στιγμή που τα C-PEPS και S-PEPS μεσολαβούν μεταξύ της πηγής των δεδομένων ταυτότητας του χρήστη και του παρόχου υπηρεσιών, ένα PEPS γίνεται αναπόφευκτα ένας επεξεργαστής και διαχειριστής δεδομένων ταυτότητας (identity data processor and controller). Σε αντίθεση με το μοντέλο MW, υπάρχει μια μετατόπιση ευθύνης από τον πάροχο υπηρεσιών προς τα PEPS. Επιπλέον, η end- to end ασφάλεια του MW αντικαθίσταται από τις σχέσεις εμπιστοσύνης του μοντέλου PEPS. Ακόμη και αν το μοντέλο αυτό αποτελεί έναν καλό τρόπο απόκρυψης της πολυπλοκότητας των εθνικών υποδομών ταυτότητας, ο βαθμός προστασίας της ιδιωτικής ζωής και ασφάλειας δεν είναι ο ίδιος με το μοντέλο MW [49].

Η προστασία της ιδιωτικής ζωής είναι μια σημαντική πτυχή και στα δύο μοντέλα. Για να είναι συμβατά με την οδηγία προστασίας δεδομένων της ΕΕ (Συμβούλιο της Ευρωπαϊκής Ένωσης, 1995) και στα δύο μοντέλα χρήστες πρέπει να δώσουν τη συγκατάθεσή τους για την χρήση των δεδομένων τους στο εξωτερικό[41].

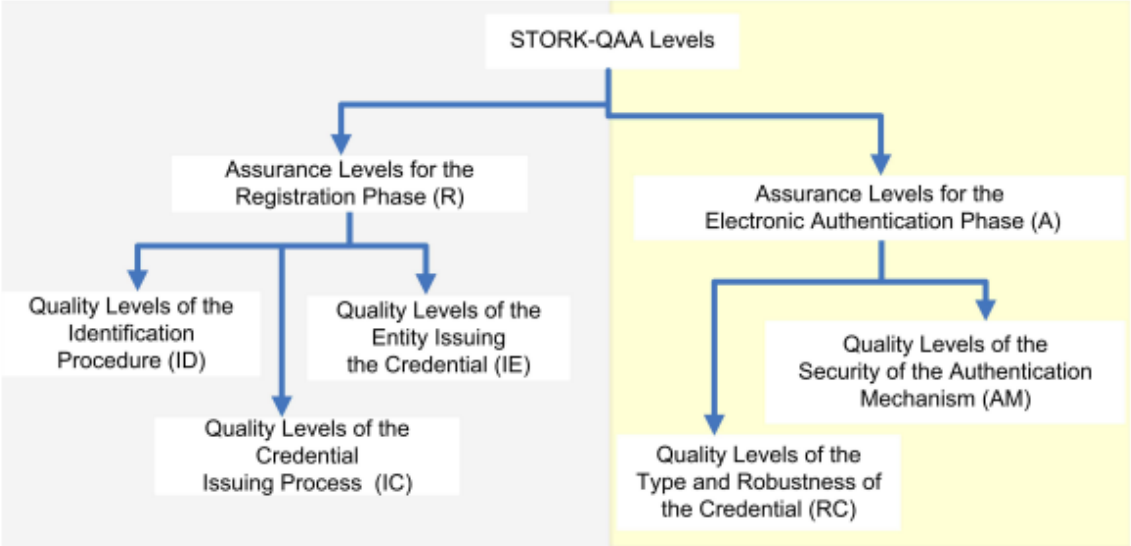
## 6.4 Επιβεβαίωση αυθεντικότητας (QAA)

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο οι κυβερνήσεις τον κρατών εδώ και αρκετά χρόνια είναι υποχρεωμένες να δίνουν την δυνατότητα στους πολίτες να έχουν ηλεκτρονική πρόσβαση στην διοίκηση. Έτσι, σε κάθε κράτος μέλος έχουν εφαρμοστεί ορισμένοι μηχανισμοί για να δοθεί η πρόσβαση αυτή. Κάποια χρησιμοποιούν απλά το παραδοσιακό σχήμα όνομα χρήστη / κωδικός χρήστη, άλλα χρησιμοποιούν αυτό το σχήμα αλλά το έχουν ενισχυθεί με κωδικούς μίας χρήσης (one time password) που παράγονται από συγκεκριμένες συσκευές ή αποστέλλονται στον πολίτη μέσω SMS. Σε αρκετές χώρες επίσης, χρησιμοποιούνται οι Υποδομές Δημόσιου Κλειδιού PKI (Public Key Infrastructure) για την παραγωγή ψηφιακών πιστοποιητικών και την υλοποίηση των εν λόγω πιστοποιητικών σε ασφαλή κρυπτογραφικά τσιπς (crypto- chips) που βρίσκονται στην κάρτα του πολίτη.

Εκτός από την πληθώρα των διαφορετικών tokens που υπάρχουν στα κράτη μέλη, διαφέρουν και οι διαδικασίες απόκτησης τους. Σε ορισμένες περιπτώσεις μπορεί να αποκτηθεί με μια απλή επίσκεψη σε μια ιστοσελίδα στην οποία ο πολίτης καλείται να πληκτρολογήσετε ορισμένα από τα δεδομένα του, ενώ σε άλλες περιπτώσεις απαιτείται ο πολίτης να επισκεφθεί ένα γραφείο εγγραφής το οποίο μπορεί να είναι μια δημόσια υπηρεσία, πριν από την έκδοση διαπιστευτηρίων του. Ακόμη, σε ορισμένες χώρες δίνεται η πρόσβαση στις διοικητικές υπηρεσίες μόνο με τις κυβερνητικές ηλεκτρονικές ταυτότητες ενώ σε άλλα κράτη και μέσω ηλεκτρονικών ταυτοτήτων που εκδίδονται από ιδιωτικούς οργανισμούς, κυρίως από τις τράπεζες [50].

Είναι κατανοητό ότι όλοι αυτοί οι διαφορετικοί τύποι tokens δεν παρέχουν τον ίδιο βαθμό αξιοπιστίας. Κάποια tokens παρέχουν καλύτερη αυθεντικοποίηση σε σύγκριση με κάποια άλλα. Σαν συνέπεια, ορισμένες πύλες δεν θα μπορούσαν να επιτρέψουν την πρόσβαση σε χρήστες με κάποια από αυτά τα tokens καθώς η ποιότητα της αξιοπιστίας της αυθεντικοποίησης που παρέχουν θα θεωρούταν ανεπαρκής για τους κινδύνους που συνδέονται με τη χρήση της εφαρμογής. Για το λόγο αυτό, το έργο STORK έχει ορίσει την κλίμακα της Ποιότητας της Αξιοπιστίας της Αυθεντικοποίησης QAA (Quality

of Authentication Assurance ), η οποία εκφράζει την ποιότητα αυτή σε μια κλίμακα από τον αριθμό 1 έως 4, όπως φαίνεται και στον πίνακα 6 . Για τον προσδιορισμό του αριθμού αυτού λαμβάνονται υπόψη και οι 7 επισημασμένοι παράγοντες που φαίνονται και στο σχήμα 21 τόσο κατά την καταγραφή και τη διαδικασία έκδοσης των token, όσο και την ποιότητα των ίδιων των διαπιστευτηρίων [51].




**Σχήμα 21 : Παράγοντες που επηρεάζουν το επίπεδο αξιοπιστίας της αυθεντικοποίησης (QAA) [51]**

Τα επίπεδα QAA ορίζονται λαμβάνοντας υπόψη τους οργανωτικούς και τεχνικούς παράγοντες που χαρακτηρίζουν τη διαδικασία της αυθεντικοποίησης [51]. Οι παράγοντες αυτοί αφορούν τόσο η φάση της καταχώρισης όσο και την (διαδικτυακή) ηλεκτρονική φάση της αυθεντικοποίησης, οι οποίες είναι δύο φάσεις που συνθέτουν τη διαδικασία της αυθεντικοποίησης.

Οργανωτικοί παράγοντες, που αφορούν τη φάση της καταχώρισης, είναι οι εξής:

- Η ποιότητα της διαδικασίας αναγνώρισης (IC).
- Η ποιότητα της έκδοσης των διαπιστευτηρίων.
- Η ποιότητα του φορέα που εκδίδει το πιστοποιητικό.

Τεχνικοί παράγοντες, οι οποίοι αφορούν την ηλεκτρονική φάση ελέγχου ταυτότητας, περιλαμβάνουν:

• Το είδος και την ευρωστία (robustness) των διαπιστευτηρίων.

•Τα χαρακτηριστικά ασφαλείας του μηχανισμού αυθεντικοποίησης κατά την απομακρυσμένη αυθεντικοποίηση.

Κάθε επίπεδο διασφάλισης περιγράφει το βαθμό με τον οποίο ένας τρίτος συμβαλλόμενος σε μια ηλεκτρονική συναλλαγή μπορεί να είναι βέβαιος ότι οι πληροφορίες ταυτότητας που παρουσιάζονται αντιπροσωπεύουν πραγματικότητα την οντότητα που αναφέρεται στις πληροφορίες ταυτότητας. Οι πάροχοι υπηρεσιών θα πρέπει να διαχειριστούν τον κίνδυνο της παροχής μιας υπηρεσίας σε λάθος πολίτη ή χρήστη (εξαιτίας μίας man-in-the-middle επίθεσης, ή λόγω μη ασφαλών διαδικασίων έκδοσης διαπιστευτηρίων, κλεμμένων κωδικών πρόσβασης και ούτω καθεξής). Θα πρέπει να αναλύσουν τους κινδύνους αυτούς και να αποδώσουν μέσα από ένα επίπεδο ποιότητας της αξιοπιστίας της αυθεντικοποίησης.

### 6.4.1 Επίπεδα QAA

Σε γενικές γραμμές, τα επίπεδα αυτά QAA μπορούν να ταξινομηθούν από τα μέσα που χρησιμοποιούνται και τις διαδικασίες μέσω των οποίων διανέμονται: Έξυπνες κάρτες με PKI συνήθως σημαίνουν λύσεις υψηλού επιπέδου, χρήση ψηφιακών πιστοποιητικών θεωρούνται ως λύσεις μεσαίου επιπέδου ενώ λύσεις που βασίζονται στο σχήμα όνομα χρήστη / κωδικός πρόσβασης χαρακτηρίζονται συνήθως χαμηλού επιπέδου. Για παράδειγμα, από την πλευρά των διαδικασιών, ένα ψηφιακό πιστοποιητικό μέσω του Internet χωρίς φυσική παρουσία του ιδιοκτήτη και χωρίς τη χρήση αναγνωρισμένων υπογραφών παρέχει λιγότερη διασφάλιση από έναν σχήμα όνομα χρήστη / κωδικός πρόσβασης που λαμβάνονται μέσω επιβεβαίωσης με φυσική παρουσίας του χρήστη από την κυβέρνηση.

**Πίνακας 6 : Επίπεδα QAA**

| STORK QAA level | Description |
|---|---|
| **1** | **Καθόλου ή ελάχιστη αξιοπιστία** |
| **2** | **Χαμηλή αξιοπιστία** |
| **3** | **Σημαντική αξιοπιστία** |
| **4** | **Υψηλή αξιοπιστία** |

Τα τέσσερα επίπεδα που ορίζονται στο STORK είναι παρόμοια με την "IDABC έκθεση για τα επίπεδα ελέγχου ταυτότητας"[50]. Είναι επίσης αρκετά συμβατά με το "πλαίσιο αξιοπιστίας αυθεντικοποίησης Liberty"[27][52]. Μια τεσσάρων επιπέδων κλίμακα χρησιμοποιείται για να διατηρήσει την πολυπλοκότητα και το κόστος για τη διατήρηση τόσο των πληροφοριών της αυθεντικοποίησης και της συναφούς υποδομής σε διαχειρήσιμα επίπεδα. Αντίθετα, προσφέρει επαρκή αναλυτικότητα να αντιστοιχιστούν οι διαφορετικές επιχειρησιακές απαιτήσεις με τους πιθανούς μηχανισμούς προστασίας με αποτέλεσμα την πλήρη κάλυψη των κινδύνων. Ένας μεγαλύτερος αριθμός επιπέδων δεν θα ήταν επιθυμητός, δεδομένου ότι μπορεί να οδηγήσει σε ασαφή διάκριση μεταξύ των επιπέδων και μπορεί να θέσει σε κίνδυνο την αξιοπιστία του πλαισίου της διαλειτουργικότητας. Ομοίως, πάρα πολλά επίπεδα αξιοπιστίας της αυθεντικοποίησης μπορούν να μπερδέψουν τον χρήστη και κατά συνέπεια θα μπορούσε να μειώσει την εμπιστοσύνη του στο πλαίσιο της αυθεντικοποίησης και των εφαρμογών που χρησιμοποιούν το πλαίσιο.

Τα επίπεδα STORK QAA ορίζονται ανάλογα με τη σοβαρότητα των επιπτώσεων των ζημιών που μπορεί να προκύψουν από την υπεξαίρεση της ταυτότητας ενός προσώπου. Όσο πιο σοβαρές είναι οι πιθανές συνέπειες τόσο μεγαλύτερο είναι το επίπεδο αξιοπιστίας της δηλούμενης ταυτότητας που απαιτείται από την πλευρά του φορέα παροχής υπηρεσιών κατά την διάρκεια μιας συναλλαγής [51].

[27] http://www.projectliberty.org/

**STORK QAA επίπεδο 1:** είναι το χαμηλότερο επίπεδο διασφάλισης. Εξασφαλίζει είτε ελάχιστη εμπιστοσύνη για την δηλούμενη ταυτότητα ή ακόμη και καθόλου εμπιστοσύνη. Τα διαπιστευτήρια της ταυτοποίησης γίνονται αποδεκτά χωρίς καμία μορφή ελέγχου. Εάν ο συνδρομητής παρέχει μια διεύθυνση e-mail, ο μόνος έλεγχος που γίνεται είναι η επαλήθευση της ορθότητας της διεύθυνσης e-mail. Αυτό το επίπεδο είναι κατάλληλο, αν οι αρνητικές συνέπειες που προκύπτουν από την εσφαλμένη ταυτότητα έχουν πολύ χαμηλή ή αμελητέα επίπτωση.

**STORK QAA επίπεδο 2**: χρησιμοποιείται από υπηρεσίες στις οποίες η ζημία από την υπεξαίρεση της ταυτότητας ενός πολίτη στον «πραγματικό κόσμο», έχει χαμηλό αντίκτυπο. Ακόμα και αν δεν είναι υποχρεωτική η φυσική παρουσία των αιτούντων κατά τη διάρκεια της εγγραφής, η ταυτότητες τους θα πρέπει να επικυρωθούν στον «πραγματικό κόσμο» και να τους χορηγηθεί κάποιο token από κάποιον φορέα που έχει συνάψει σχετική συμφωνία με την κυβέρνηση. Τα tokens της ταυτοποίησης πρέπει να παραδίδονται στους χρήστες με εγγυήσεις ασφάλειας. Κατά τη διάρκεια της ΗΤ πρέπει να χρησιμοποιούνται αξιόπιστα πρωτόκολλα ελέγχου ταυτότητας.

**STORK QAA Επίπεδο 3**: χρησιμοποιείται από υπηρεσίες στις οποίες μπορεί να προκληθούν σημαντικές ζημιές σε περίπτωση κατάχρησης μιας ταυτότητας. Η καταχώρηση μιας ταυτότητας σε επεξεργασία με μεθόδους που σαφώς και με ένα υψηλό επίπεδο βεβαιότητας προσδιορισμό του ενάγοντα. Οι πάροχοι ταυτοτήτων (identity providers) είναι διαπιστευμένοι και εποπτεύονται από την κυβέρνηση. Τα διαπιστευτήρια που παραδίδονται στους χρήστες είναι το λιγότερο ψηφιακά πιστοποιητικά ή πιστοποιητικά σε μορφή hardware. Οι μηχανισμοί αυθεντικοποίησης που χρησιμοποιούνται κατά την απομακρυσμένη φάση αυθεντικοποίησης είναι πολύ «ισχυροί».

**STORK QAA Επίπεδο 4**: είναι το υψηλότερο επίπεδο αξιοπιστίας και απευθύνεται σε εκείνες τις υπηρεσίες στις όποιες η ζημιά που θα προκληθεί σε περίπτωση κακής χρήσης της ταυτότητας κάποιου χρήστη μπορεί να έχει

μεγάλο αντίκτυπο. Η εγγραφή απαιτεί τουλάχιστον μία φορά (δηλαδή, την πρώτη φορά της αίτησης, αλλά όχι για μεταγενέστερη ανανέωση) είτε η φυσική παρουσία του αιτούντος ή μια φυσική συνάντηση με τον αιτούντα. Για παράδειγμα μπορεί να γίνει η αίτηση για την χορήγηση της ταυτότητας ηλεκτρονικά, αλλά να ζητηθεί να γίνει η παραλαβή στο σπίτι, όπου και θα παραδοθεί μετά από φυσική εξακρίβωση της ταυτότητας του αιτούντος. Εναλλακτικά, στην περίπτωση της on-line εγγραφής, δίνεται η μπορεί να εξακριβωθεί/ επικυρωθεί η ταυτότητα του αιτούντος με τη χρήση αξιόπιστων ηλεκτρονικών υπογραφών. Σύμφωνα με το παράρτημα ΙΙ της Οδηγίας 1999/93/ΕΚ [53] για τις ηλεκτρονικές υπογραφές οι λεπτομέρειες για την επαλήθευση της ταυτότητας με ηλεκτρονική υπογραφή παρέχονται από το εθνικό δίκαιο κάθε χώρας. Ως εκ τούτου, το επίπεδο 4 παρέχεται μόνο εφόσον πληρούνται οι εθνικές νομικές προϋποθέσεις για την έκδοση αναγνωρισμένων πιστοποιητικών (qualified certificate). Επιπλέον, σύμφωνα με το παράρτημα ΙΙ της οδηγίας για τις ηλεκτρονικές υπογραφές, ο πάροχος της ταυτότητας πρέπει να είναι ένας πιστοποιημένος φορέας. Ακόμη, σύμφωνα με το παράρτημα Ι της ίδια οδηγίας, τα πιστοποιητικά είναι σε μορφή hardware (hard certificates). Κατά την διαδικασία της αυθεντικοποίησης χρησιμοποιούνται οι πιο ισχυροί μηχανισμοί ελέγχου αυθεντικοποίησης.

### 6.4.2 Παράγοντες που επηρεάζουν την Ποιότητα Αξιοπιστίας και Αυθεντικοποίησης (QAA)

Όπως περιγράφεται και στο σχήμα 21 κάθε επίπεδο STORK QAA αντιπροσωπεύεται από ένα σύνολο οργανωτικών (ID, IC, και IE) και τεχνικών (RC και AM) παραγόντων και των επιμέρους αυτών επιπέδων ποιότητας. Η χαμηλότερη τιμή από τις τιμές των επιμέρους επιπέδων ποιότητας καθορίζει τελικά το συνολικό επίπεδο STORK QAA.

#### *6.4.2.1 Οργανωτικοί παράγοντες*

Όσον αφορά τους οργανωτικούς παράγοντες και ειδικότερα την ποιότητα της διαδικασίας αναγνώρισης, αυτή αποτελείται από τρείς ανεξάρτητες πτυχές οι όποιες διαβαθμίζονται ανάλογα:

- την φυσική παρουσία του αιτούντος στη διαδικασία της ταυτοποίησης του,
- την ποιότητα των δηλούμενων χαρακτηριστικών (assertions) που αφορούν την ταυτότητα του αιτούντος,
- την ποιότητα της επικύρωσης αυτών των χαρακτηριστικών.

Η επιβολή φυσικής παρουσίας κατά την διαδικασία της ταυτοποίησης του χρήστη προσδίδει υψηλότερο βαθμό ποιότητας αξιοπιστίας από την περίπτωση της μη επιβεβλημένης φυσικής παρουσίας. Παρόμοια, η ύπαρξη μεταξύ των δηλούμενων χαρακτηριστικών κάποιου μοναδικού χαρακτηριστικού ταυτότητας του χρηστή, όπως για παράδειγμα ο αριθμός ταυτότητας του ή ο αριθμός κοινωνικής ασφάλισης, προσδίδουν επίσης υψηλότερο επίπεδο αξιοπιστίας από τις περιπτώσεις εκείνες όπου η ταυτοποίηση του χρήστη δεν μπορεί να γίνει με μοναδικό τρόπο. Η διαδικασία της επικύρωσης των παραπάνω χαρακτηριστικών μπορεί να χωριστεί στις παρακάτω περιπτώσεις [51]:

1. Η επικύρωση περιορίζεται στην επαλήθευση μιας ηλεκτρονικής διεύθυνσης, εάν αυτό παρέχεται. Διαφορετικά, δεν γίνεται κανένας έλεγχος.
2. Η επικύρωση γίνεται από τη διασταύρωση των παρεχόμενων χαρακτηριστικών με μια επίσημη υπηρεσία παροχής ταυτοτήτων ή μιας βάσης δεδομένων ταυτότητας από μια ουδέτερη και αξιόπιστη πηγή, όπως για παράδειγμα μια τράπεζα, έναν οργανισμό ασφάλισης ή κάποια κυβερνητική υπηρεσία.
3. Για την επικύρωση απαιτείται η υπογραφή των χαρακτηριστικών με μία απλή ψηφιακή υπογραφή (non-qualified digital signature).
4. Για την επικύρωση απαιτείται η προσκόμιση ενός επίσημου κυβερνητικού έγγραφου (πχ δελτίο ταυτότητας, διαβατήριο ή άδεια οδήγησης), το οποίο περιέχει την φωτογραφία του αιτούντος και / ή την υπογραφή του .

5. Για την επικύρωση απαιτείται η υπογραφή των χαρακτηριστικών με ψηφιακή υπογραφή η οποία είναι εγκεκριμένη από έναν Πιστοποιημένο Πάροχο Υπηρεσιών, πριν από την έκδοση των διαπιστευτηρίων ή του σχετικού token.

Η ποιότητα της έκδοσης των διαπιστευτηρίων αξιολογείται μέσω της ποιότητας του φορέα που εκδίδει τα πιστοποιητικά ταυτότητας (πιστοποιητικά, κωδικοί πρόσβασης, tokens). Ένας τέτοιος φορέας θα μπορούσε για παράδειγμα να είναι ένας παραδοσιακός ή ηλεκτρονικός πάροχος ταυτότητας ή μια αρχή έκδοσης πιστοποιητικών (Certificate Athority). Ενώ οι εκδότες των παραδοσιακών εγγράφων ταυτότητας (π.χ. διαβατήρια και οι ταυτότητες) είναι συνήθως δημόσιοι κυβερνητικοί φορείς, οι εκδότες ψηφιακών ταυτοτήτων μπορεί να είναι είτε φορείς του δημόσιου τομέα ή σε κάποια τρίτη οντότητα. Ο ρόλος της αρχής πιστοποίησης και του παρόχου ταυτότητας συνήθως εκτελείται από την ίδια φυσική οντότητα, η οποία καλείται πάροχος υπηρεσιών πιστοποίησης. Γίνεται μια διάκριση μεταξύ των φορέων που είναι πιστοποιημένοι και εκείνων που δεν είναι σύμφωνα με τα όσα αναφέρονται στο Παράρτημα ΙΙ της Οδηγίας 1999/93/ΕΚ [53]. Μόνο οι πιστοποιημένοι φορείς μπορούν να προσφέρουν το υψηλότερο επίπεδο αξιοπιστίας.

Επίσης, όσο αφορά τους μη πιστοποιημένους φορείς, γίνεται διάκριση μεταξύ αυτών οι οποίοι εφαρμόζουν μηχανισμούς που έχουν εγκριθεί, επιβλέπονται ή είναι διαπιστευμένοι από την κυβέρνηση και τους φορείς που δεν χρησιμοποιούν τέτοιους μηχανισμούς (π.χ. τράπεζες).

Πιστοποιημένοι φορείς είναι εκείνοι οι όποιοι πληρούν τις απαιτήσεις του Παραρτήματος ΙΙ της Οδηγίας 1999/93/ΕΚ. Ένας πιστοποιημένος φορέας επιτρέπεται επίσης, να προσφέρει αναγνωρισμένα πιστοποιητικά ακολουθώντας τους περιορισμούς που εκφράζονται στο Παράρτημα Ι της ίδιας οδηγίας. Για την αξιολόγηση των φορέων αλλά και γενικότερα των διαδικασιών καταχώρισης, λαμβάνεται υπόψη και οι προδιαγραφές που αναλύονται στο έγγραφο «Απαιτήσεις της πολιτικής για τις αρχές πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά δημόσιου κλειδιού» (ETSI TS 102 042) [54]

#### *6.4.2.2 Τύποι και ανθεκτικότητα διαπιστευτηρίων*

Όσο αφορά στους τεχνικούς παράγοντες και ειδικότερα αυτόν που αφορά τα προσφερόμενα επίπεδα ασφάλειας των διαφορετικών τύπων των διαπιστευτηρίων, ο πρώτος παράγοντας που επηρεάζει την ποιότητα την ποιότητα της αξιοπιστίας της αυθεντικοποίησης είναι ο τύπος του token. Οι τύποι των token στο STORK έχουν ως εξής [51]:

- **Όνομα χρήστη / Κωδικός πρόσβασης ή PIN**: είναι μια σειρά χαρακτήρων, που θα πρέπει να απομνημονευτούν και να κρατηθούν μυστικοί από τον αιτούντα. Αυτό το είδος του token χρησιμοποιείται σε πολλά κράτη μέλη, ιδίως για τις υπηρεσίες χαμηλού κινδύνου. Συχνά, ένα συγκεκριμένος συνδυασμός όνομα χρήστη / κωδικός πρόσβασης, ή τον κωδικός PIN, συνδέεται και επιτρέπει τη χρήση με ένα συγκεκριμένο σύνολο υπηρεσιών. Το τμήμα του συνδυασμού «όνομα χρήστη» μπορεί είτε να επιλεγεί από τον αιτούντα ή να παραχθεί από τον πάροχο ταυτότητας. Δεδομένου ότι το όνομα χρήστη είναι δημόσιο, δεν έχει αντίκτυπο στο επίπεδο αυθεντικοποίησης. Όμως, για το τμήμα «κωδικός πρόσβασης» ή το PIN το επίπεδο αυθεντικοποίησης επηρεάζεται ανάλογα με το αν έχει επιλεγεί από τον αιτούντα ή έχει δημιουργηθεί αυτόματα.
- **Λίστα Κωδικών**: Είναι ένα προσωπική λίστα κωδικών την οποία έχει στην κατοχή του ο αιτών. Μια τέτοια λίστα συχνά περιέχει κωδικούς PIN οι οποίοι συνδυάζονται με ένα σταθερό κωδικό πρόσβασης ή το PIN στο πλαίσιο του συστήματος αυθεντικοποίησης.
- **Συσκευή παραγωγής κωδικών μιας χρήσης**: Είναι μια προσωπική συσκευή που δημιουργεί κωδικούς (one-time password) οι οποίοι ισχύουν για μία μόνο συνεδρία αυθεντικοποίησης. Σε ορισμένες περιπτώσεις, οι κωδικοί μιας χρήσης παράγονται ως χρονοσημάνσεις «timestamp», χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης που

συνδυάζει την τρέχουσα ώρα και ένα μυστικό αριθμό (secret seed) που είναι αποθηκευμένος στη συσκευή. Σε άλλες περιπτώσεις, μια ειδική συσκευή ανάγνωσης συνδυάζει ένα συμμετρικό κλειδί που είναι αποθηκευμένο σε μια προσωπική συσκευή (π.χ., μια κάρτα) με κάτι άλλο, το οποίο για παράδειγμα μπορεί να είναι τρέχουσα ώρα, μία γεννήτρια αριθμών που βρίσκεται στη συσκευή ανάγνωσης.

- **Ψηφιακό πιστοποιητικό (**soft certificate**):** είναι ένα κρυπτογραφικό κλειδί το οποίο είναι συνήθως αποθηκευμένο σε ένα δίσκο, USB stick ή κάποιο άλλο μέσο. Η αυθεντικοποίηση επιτυγχάνεται αποδεικνύοντας την κατοχή και τον έλεγχο του κλειδιού. Συνήθως, το ψηφιακό πιστοποιητικό κρυπτογραφείται με ένα κλειδί που προέρχεται από έναν κωδικό πρόσβασης ο οποίος είναι γνωστός μόνο στον χρήστη ο οποίος και είναι απαραίτητος για την ενεργοποίηση του πιστοποιητικού.
- **Ειδικευμένο ψηφιακό πιστοποιητικό** (Qualified Soft certificate ): είναι ένα ψηφιακό πιστοποιητικό του οποίου τα τεχνικά χαρακτηριστικά είναι σύμφωνα με τις απαιτήσεις που ορίζονται στο Παράρτημα I της Οδηγίας 1999/93/ΕΚ [53] . Παρόλο που υπάρχουν διαφορές κατά την μεταφορά της οδηγίας στις εθνικές νομοθεσίες, υπάρχει κοινό έδαφος για το πώς δημιουργούνται τα πιστοποιητικά και για τα έννομα αποτελέσματά τους. Στα πιστοποιητικά αυτά συμπεριλαμβάνονται και αυτά που εκδίδονται με τις ίδιες διαδικασίες από τις κυβερνήσεις σε εθνικό επίπεδο.
- **Υλικό πιστοποιητικό (**Hard Certificate**)**: είναι μια έξυπνη κάρτα ή κάποιο παρόμοιο μέσο, που περιέχει ένα προστατευμένο κρυπτογραφικό κλειδί. Η αυθεντικοποίηση επιτυγχάνεται αποδεικνύοντας την κατοχή της συσκευής και τον έλεγχο του κλειδιού.
- **Ειδικευμένο υλικό πιστοποιητικό** (Qualified Hard Certificate): είναι ένα υλικό πιστοποιητικό του οποίου τα τεχνικά χαρακτηριστικά είναι σύμφωνα με τις απαιτήσεις που καθορίζονται στο παράρτημα I της οδηγίας 1999/93/ΕΚ [53] .

Τα επιμέρους επίπεδα αξιοπιστίας για τους διαφορετικούς τύπους token φαίνονται στο σχήμα 22

| Requirements | Quality Levels of the Type and Robustness of the Credential | | | |
|---|---|---|---|---|
| | RC1 | RC2 | RC3 | RC4 |
| Password or PIN-based token, chosen by the claimant or automatically generated but not conform common guidelines for strong passwords or PINs (e.g. insufficient length, no mixture of characters, reused, etc.) and therefore vulnerable to guessing or dictionary attacks. | • | | | |
| Password or PIN-based token, chosen by the claimant or automatically generated but conform common guidelines for strong passwords or PINs (e.g. sufficient length, mixture of characters, not reused, etc.) and therefore not vulnerable to guessing or dictionary attacks. | • | • | | |
| Soft certificates or one-time password device token. | • | • | • | |
| Qualified Soft certificates according to Annex I of Directive 1999/93/EC. | • | • | • | |
| Hard certificates. | • | • | • | |
| Qualified Hard certificates according to Annex I of Directive 1999/93/EC. | • | • | • | • |

**Σχήμα 22: Επίπεδα αξιοπιστίας token αυθεντικοποίησης [51]**

### *6.4.2.3 Ασφάλεια των μηχανισμών αυθεντικοποίησης*

Το επίπεδο αξιοπιστίας που μπορεί να τεθεί σε ένα απομακρυσμένο μηχανισμό αυθεντικοποίησης εξαρτάται από την ευρωστία (robustness) της ασφάλειας του. Η ευρωστία των μηχανισμών αυθεντικοποίησης εδώ κρίνεται σε σχέση με την πιο σοβαρή απειλή που αφορά την αυθεντικοποίηση που είναι η κλοπή της ταυτότητας. Στις περισσότερες περιπτώσεις, ένας εγκληματίας πρέπει να αποκτήσει προσωπικά στοιχεία ή έγγραφα που σχετίζονται με ένα άτομο, προκειμένου να μπορέσει να τον υποδυθεί. Αυτό μπορεί να γίνει με διάφορους τρόπους, μεταξύ των οποίων, για

παράδειγμα, μέσω της ανάκτησης πληροφοριών από κάποιον αποσυρμένο υπολογιστή οποίος είναι εκτεθειμένος χωρίς να έχουν γίνει οι απαραίτητες ενέργειες απομάκρυνσης προσωπικών στοιχειών , ή προβαίνοντας σε έρευνα για το θύμα στα μητρώα της κυβέρνησης ή στις μηχανές αναζήτησης στο διαδίκτυο και στις δημόσιες υπηρεσίες, ή ακόμη και μέσα από την περιήγηση σε κοινωνικά δίκτυα (π.χ., το MySpace και το Facebook) ανακτώντας προσωπικά στοιχεία τα οποία έχουν καταχωρηθεί από τους ίδιους τους χρήστες [50] .

Στο STORK η ανάλυση των επιπέδων διασφάλισης του απομακρυσμένου ελέγχου ταυτότητας επικεντρώνονται στις απειλές που προέρχονται από τις επιθέσεις που κατευθύνονται μόνο προς το ίδιο το πρωτόκολλο αυθεντικοποίησης. Σε αυτή την περίπτωση η ταυτότητα ενός χρήστη μπορεί να κλαπεί μέσα από μία σειρά επιθέσεων εναντίον της διαδικασίας απομακρυσμένης αυθεντικοποίησης. Παρακάτω αναλύονται οι τύποι τέτοιων επιθέσεων [41, 51, 55]

1. **Εικασία (guessing):** είναι μια απλή επίθεση, όπου ένας κακόβουλος χρήστης προσπαθεί να μαντέψει ένα μυστικό (secret) που χρησιμοποιείται κατά την επικοινωνία (π.χ. ένα κλειδί κρυπτογράφησης ή ένα PIN). Αυτή η επίθεση επιφέρει αποτελέσματα σε περιπτώσεις όπου το μυστικό είναι αδύναμο. Για παράδειγμα, έναν απλό κωδικός πρόσβασης μπορεί εύκολα κάποιος να τον μαντέψει χρησιμοποιώντας ειδικά λεξικά που περιέχουν πιθανούς κωδικούς (λεξικογραφικές επιθέσεις).
2. **Υποκλοπές** (Eavesdropping): είναι μια επίθεση που συνίσταται στην παρακολούθηση των μηνυμάτων που περνούν μέσα από ένα κανάλι επικοινωνίας, το οποίο για παράδειγμα μπορεί να χρησιμοποιείται από ένα πρωτόκολλο αυθεντικοποίησης. Τα μηνύματα αυτά συνήθως αποθηκεύονται για την μετέπειτα εκτέλεση κάποιων off-line αναλύσεων των πληροφοριών, και χρησιμοποιούνται για την εκτέλεση διαδοχικών επιθέσεων
3. **Πειρατεία** (Hijacking): είναι μια επίθεση που συνίσταται στην ανάληψη μιας ήδη πιστοποιημένης συνεδρίας από έναν εισβολέα με σκοπό να μάθουν ευαίσθητες πληροφορίες.

4. **Επανάληψη** (Replay): είναι μια μορφή επίθεσης, όπου ένα κακόβουλος χρήστης επαναλαμβάνει ή καθυστερεί μηνύματα που προηγουμένως έχουν διακοπεί και υποκλαπεί, προκειμένου να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες.
5. **Man-in-the-middle** είναι μια ενεργητικής μορφής υποκλοπών κατά τις οποίες ο επιτιθέμενος δημιουργεί ανεξάρτητες συνδέσεις με τα θύματα και τα μεταξύ τους ανταλλασσόμενα μηνύματα, κάνοντάς τους να πιστεύουν ότι μιλούν απευθείας ο ένας στον άλλο σε μια ιδιωτική σύνδεση, ενώ στην πραγματικότητα η όλη συνομιλία ελέγχεται από τον εισβολέα. Ο εισβολέας είναι σε θέση να παρακολουθεί όλα τα μηνύματα μεταξύ των δύο θυμάτων ενώ μπορεί να εισάγει και νέα μηνύματα. Υπάρχει άμεση σχέση μεταξύ του επιπέδου αξιοπιστίας του πρωτοκόλλου αυθεντικοποίησης και της ευρωστίας έναντι αυτού του είδους των επιθέσεων.

Σε κάθε περίπτωση η ευρωστία είναι μια ιδιότητα που μπορεί να αξιολογηθεί μόνο σε σχέση με την τρέχουσα κατάσταση της τεχνολογίας. Οι επιθέσεις και οι άμυνες εξελίσσονται ταυτόχρονα μέσα στο χρόνο. Έτσι στον παρακάτω πίνακα κατατάσσονται οι απομακρυσμένες διαδικασίες αυθεντικοποίησης σχετικά με την αποδεδειγμένη (στην τρέχουσα τεχνολογία και γνώση) ασφάλεια τους ή την αποδεδειγμένη έλλειψη ασφάλειας έναντι των προαναφερθεισών επιθέσεων. Αποδεδειγμένη ανασφάλεια σημαίνει ότι είναι γνωστό ότι το πρωτόκολλο είναι ευάλωτο στην επίθεση. Ο όρος «αποδεδειγμένη ασφάλεια» δεν είναι μπορεί να οριστεί τόσο ξεκάθαρα. Μπορεί να αναφέρεται στην «de facto» ευρωστία όπως για παράδειγμα στην περίπτωση μηχανισμών που έχουν χρησιμοποιηθεί για αρκετό χρονικό διάστημα χωρίς να έχει αναφερθεί καμία επίθεση. Εναλλακτικά, ο όρος «αποδεδειγμένη ασφάλεια» μπορεί να ορίζεται και ως «τυπικά ασφαλής», όταν έχουν πραγματοποιηθεί μελέτες και δοκιμές για την ασφάλεια του μηχανισμού με θετικά αποτελέσματα [51] .

Πρέπει να σημειωθεί ότι ορισμένα είδη επιθέσεων, όπως οι πειρατείες και οι «man-in-the-middle» επιθέσεις, είναι πολύ δύσκολο να ανιχνευθούν. Ακόμη, όταν λέμε ότι ένας μηχανισμός προσφέρει προστασία (ή ισχυρή προστασία) απέναντι σε μια επίθεση,

εννοούμε ότι σε σχέση με την τρέχουσα τεχνολογία, ο μηχανισμός αυτός χρησιμοποιεί άμυνες οι όποιες είναι αναγνωρισμένες ότι είναι εύρωστες ενάντια στην συγκεκριμένη επίθεση. Έτσι, για παράδειγμα η χρησιμοποίηση τυχαίων κωδικών πρόσβασης μεγαλύτερων των 8 χαρακτήρων και με το αλφαριθμητικούς χαρακτήρες είναι γνωστό ότι είναι μία εύρωστη τεχνική ενάντια σε λεξικογραφικές επιθέσεις και σε επιθέσεις εικασίας.

Αυτό αφήνει να εννοηθεί ότι μόνο το 4$^{ο}$ επίπεδο μπορεί να περιγραφεί από την τυπική έννοια της ασφάλειας. Για τα υπόλοιπα επίπεδα πρέπει να γίνει μια αυτοαξιολόγηση. Η αυτοαξιολόγηση αυτή μπορεί να γίνει μέσα από τις διαδικασίες και την καθοδήγηση που περιγράφονται από τον οργανισμό Κοινών Κριτηρίων για τις Τεχνολογίες της Πληροφορικής (Common Criteria for Information Technology) για τα επίπεδα διασφάλισης αξιοπιστίας [56].

Στο σχήμα 23 συνοψίζονται οι απαιτήσεις για τα επίπεδα διασφάλισης αξιοπιστίας που σχετίζονται με τον μηχανισμό αυθεντικοποίησης.

| Requirements | Quality Levels of the Security of the Authentication Mechanism | | | |
|---|---|---|---|---|
| | AM1 | AM2 | AM3 | AM4 |
| Authentication mechanisms that offer little or no protection against the above-mentioned attacks. | • | | | |
| Secure authentication mechanisms that offer some protection against the above-mentioned attacks. | • | • | | |
| Secure authentication mechanisms that offer protection against most of the above-mentioned attacks. | • | • | • | |
| Recognized secure authentication mechanisms that offer protection against all of the above-mentioned attacks. Comparable with EAL4+ or higher of the Common Criteria. | • | • | • | • |

**Σχήμα 23: Απαιτήσεις μηχανισμών αυθεντικοποίησης για τα επίπεδα διασφάλισης αξιοπιστίας**

Συνδυάζοντας τα δεδομένα των σχημάτων 22 και 23 δύο παραπάνω πίνακες και ακολουθώντας τον κανόνα ότι πάντα υπερισχύει το χαμηλότερο επίπεδο εμπιστοσύνης, μπορούν να προσδιοριστούν τα επίπεδα εμπιστοσύνης για την φάση της ηλεκτρονικής αυθεντικοποίησης. Τα επίπεδα διασφάλισης αξιοπιστίας που προκύπτουν από τα παραπάνω φαίνονται στο παρακάτω σχήμα 24.

| Aspects relevant for electronic authentication | Quality assurance levels for electronic authentication phase | | | |
|---|---|---|---|---|
| | **EA1** | **EA2** | **EA3** | **EA4** |
| Type and Robustness of Identity Token (Table 9) | RC1 | RC2 | RC3 | RC4 |
| Security of Authentication Mechanism (Table 10) | AM1 - 3 | AM1 - 3 | AM1 - 3 | AM4 |

**Σχήμα 24: Τελικά επίπεδα αξιοπιστίας για την φάση της ηλεκτρονικής αυθεντικοποίησης [51]**

Συνδυάζοντας όλα τα παραπάνω που αναφέρθηκαν είναι δυνατή η δημιουργία ενός μοντέλου με την βοήθεια του οποίου μπορεί να γίνει η αξιολόγηση της ποιότητας των παρεχόμενων υπηρεσιών αυθεντικοποίησης. Κάθε κράτος ακολουθώντας τις απαιτήσεις που προδιαγράφονται στο μοντέλο αυτό θα πρέπει να αξιολογήσει και να αντιστοιχίσει τις παρεχόμενες σε εθνικό επίπεδο λύσεις αυθεντικοποίησης που παρέχει με το κατάλληλο STORK QAA επίπεδο. Η ασφάλεια της υποδομής του STORK βασίζεται στην δημιουργία ενός κύκλου εμπιστοσύνης (circle of trust). Κάθε κράτος αποθηκεύει στις υποδομές τους τα απαιτούμενα χαρακτηριστικά των υπόλοιπων κρατών (πιστοποιητικά που χρησιμοποιούνται για υπογραφές, τις ηλεκτρονικές διευθύνσεις που δέχονται τα αιτήματα κλπ). Για να είναι ασφαλής αυτός ο κύκλος εμπιστοσύνης, θα πρέπει κάθε κράτος να ικανοποιεί τις απαραίτητες προδιαγραφές ασφάλειας να

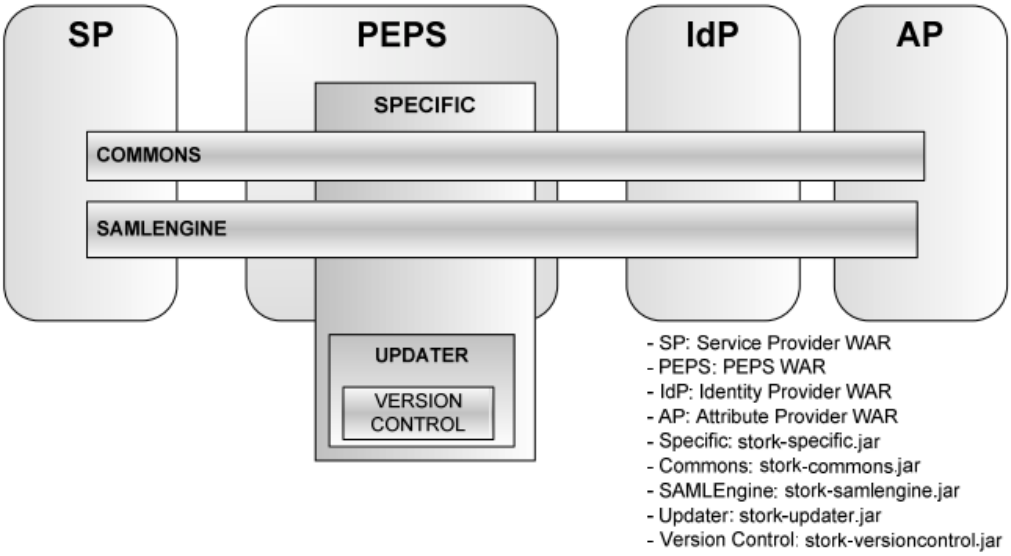
αυτοαξιολογηθεί σύμφωνα με τα παραπάνω και να δηλώνει το STORK QAA επίπεδο το οποίο ικανοποιεί.

# Κεφάλαιο 7: Θέματα Υλοποίησης και Εγκατάστασης PEPS

## 7.1 Ανάλυση Συστήματος

Το σύστημα αποτελείται από εννέα (9) μονάδες λογισμικού, αυτές των Παρόχου Υπηρεσιών (SP), Παρόχου Ταυτότητας (IdP), Παρόχου χαρακτηριστικών (AP), του Μηχανισμού SAML, του PEPS, των Κοινών Μονάδων (Commons), της μονάδας Αναβάθμισης (Updater) και της μονάδας Ελέγχου Έκδοσης (Version Control). Στο σχήμα 25 φαίνονται οι αλληλεξαρτήσεις μεταξύ των μονάδων λογισμικού.

Στις υποενότητες που ακολουθούν, θα αναλυθούν οι μονάδες λογισμικού που αφορούν και επιτελούν τις κύριες λειτουργίες του PEPS ενώ θα γίνει μία συνοπτική αναφορά στις μονάδες λογισμικού που αφορούν τους πάροχους υπηρεσιών, χαρακτηριστικών και ταυτότητας.




**Σχήμα 25: Αλληλεξαρτήσεις μονάδων λογισμικού PEPS [57]**

### 7.1.1 Μονάδα για την υλοποίηση του PEPS

Σε κάθε PEPS υλοποιούνται 2 ρόλοι [58]: αυτός που μεριμνά για αιτήματα των παρόχων υπηρεσιών και αυτός ο όποιος βρίσκεται στην χώρα που εκδόθηκε η ταυτότητα του πολίτη που θα χρησιμοποιηθεί στην διαδικασία της αυθεντικοποίησης. Η εθνικότητα του εκδότη της ταυτότητας μπορεί να διαφέρει από την εθνικότητα του πολίτη.

Κάθε αίτημα που λαμβάνεται, ο πρώτος το προωθεί στο συνεργαζόμενο PEPS, και ο δεύτερος επιλύει τα αιτήματα που υποβλήθηκαν από το συνεργαζόμενο PEPS. Κάθε PEPS μπορεί να περιλαμβάνει και λειτουργίες που αφορούν ειδικά το κάθε κράτος μέλος, οι οποίες είναι συνήθως οι διεπαφές με τους τοπικούς παρόχους ταυτότητας και χαρακτηριστικών. Οι διεπαφές με τους παρόχους υπηρεσιών (SPS) μπορεί επίσης να είναι διαφορετικές σε κάθε χώρα. Όμως η επικοινωνία μεταξύ των PEPSes και οι κοινές λειτουργίες τους είναι τυποποιημένες**.**

Η διαδικασία αυθεντικοποίησης πραγματοποιείται χρησιμοποιώντας ως πύλη εξόδου για κάθε μήνυμα το οποίο χρειάζεται να ανταλλαχτεί μεταξύ των δύο οντοτήτων του STORK, το διαδικτυακό πρόγραμμα περιήγησης του χρήστη. Ως εκ τούτου, η αίτηση αυθεντικοποίησης που προέρχεται από έναν πάροχο υπηρεσιών και πρέπει να σταλεί στο S-PEPS, θα αποσταλεί μέσω του διαδικτυακού προγράμματος περιήγησης του χρήστη. Κατά τον ίδιο τρόπο, το S-PEPS θα ανακατευθύνει (αν χρειαστεί) την αίτηση αυθεντικοποίησης (ως SAML AuthnRequest) στο C-PEPS μέσω του ίδιου προγράμματος. Ορισμένοι Ευρωπαϊκοί κανονισμοί για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων, έχουν υποχρεώσει το STORK να χρησιμοποιεί αυτό το μηχανισμό για την αποστολή των πληροφοριών των χρηστών μεταξύ των μελών της υποδομής STORK. Η απαίτηση αυτή υποστηρίζεται από το προφίλ ανακατεύθυνσης του OASIS SAML HTTP.

Ένα S-PEPS μπορεί ακόμη να ζητήσει από ένα C-PEPS την επικύρωση κάποιου πιστοποιητικού που χρησιμοποιείται για την αυθεντικοποίηση ενός χρήστη, έτσι ώστε να γνωρίζει ότι αυτό το πιστοποιητικό είναι έγκυρο και ότι δεν έχει ανακληθεί. Τα αιτήματα επιβεβαίωσης γίνονται μέσα από το πρωτόκολλο *OCSP* (Online Certificate Status Protocol).

Οι αποκρίσεις στα αιτήματα *OCSP* των S-PEPS, δημιουργούνται είτε από τα C-PEPS είτε από τον εθνικό πάροχο ταυτοποίησης (IdP) κάθε κράτους. Σε κάθε περίπτωση, το C-PEPS πρέπει να υπογράψει το μήνυμα απόκρισης πριν την αποστολή του στο S-PEPS. Ως εκ τούτου, η απόκριση OCSP δημιουργείται έξω από το C-PEPS, η υπογραφή του εθνικού IdP πρέπει να αντικατασταθεί από την υπογραφή που χρησιμοποιείται από το C-PEPS. Σε διαφορετική περίπτωση το S-PEPS δεν θα είναι σε θέση να «εμπιστευτεί» την απάντηση λόγω των περιορισμών για την δημιουργία του κύκλου εμπιστοσύνης μεταξύ των PEPS [58] .

### 7.1.2 SAML

Η διαδικασία αυθεντικοποίησης του STORK γίνεται σύμφωνα με το πρότυπο SAML (Secure Assertion Markup Language). Το πρότυπο OASIS (SAML) καθορίζει ένα πλαίσιο το οποίο είναι βασισμένο σε XML γλώσσα με σκοπό την περιγραφή και την ανταλλαγή πληροφοριών ασφάλειας. Οι πληροφορίες ασφάλειας εκφράζονται με τη μορφή των ισχυρισμών SAML (assertions) τους οποίους οι εφαρμογές μπορούν να εμπιστευτούν [59]. Το πρότυπο OASIS SAML καθορίζει τους ακριβείς κανόνες σύνταξης και υποβολής των αιτήσεων, τη δημιουργία, την επικοινωνία, και την χρήση αυτών των ισχυρισμών SAML.

Ένα από τα κύρια πλεονεκτήματα του πρότυπου SAML είναι το ότι βασίζεται στην γλώσσα XML προσδίδοντας στο πρότυπο επεκτασιμότητα, κάτι το οποίο το καθιστά πολύ ευέλικτο. Δύο συναλλασσόμενα μέρη (federation partners) έχουν την δυνατότητα να ανταλλάξουν οποιοδήποτε χαρακτηριστικό ταυτότητας θέλουν μέσα από το ωφέλιμο φορτίο (payload) των ισχυρισμών SAML, αρκεί τα χαρακτηριστικά αυτά να μπορούν να αναπαρασταθούν σε γλώσσα XML.

Ακόμη, το πρότυπο SAML χαρακτηρίζεται από την διαλειτουργικότητα του, πλεονεκτώντας έτσι σε σχέση με τους αποκλειστικούς μηχανισμούς Single Sign On (SSO) οι οποίοι απαιτούν από τον πάροχο ταυτότητας (IdP) και παροχής υπηρεσιών (SP) να χρησιμοποιούν την ίδια εφαρμογή λογισμικού. Σε αντίθεση με τους μηχανισμούς SSO

όπου κάθε νέα σύνδεση απαιτεί δυνητικά μια νέα και διαφορετική εφαρμογή λογισμικού, το SAML μπορεί να υποστηρίξει συνδέσεις SSO με πολλά διαφορετικά συναλλασσόμενα μέρη (federation partners) [60] .

Σε επιχειρησιακό επίπεδο, το SAML μπορεί να χρησιμοποιηθεί σε διαδικτυακές υπηρεσίες αυθεντικοποίησης απλοποιώντας τις διαδικασίας που εμπλέκονται σε αυτές. Οι πιο σημαντικοί λόγοι που επιλέχτηκε το πρότυπο αυτό από το STORK είναι η δυνατότητες που έχει στην παροχή υπηρεσιών SSO, στην παροχή υπηρεσιών «ταυτότητας ομοσπονδίας» αλλά και στην επαναχρησιμοποίηση των λειτουργιών του από άλλα πρότυπα [59, 60]:

- **Single Sign-On**: Υπάρχουν διάφορα προϊόντα στο εμπόριο τα οποία στοχεύουν στην παροχή διαδικτυακών υπηρεσιών SSO. Τα προϊόντα αυτά συνήθως χρησιμοποιούν τα *cookies* του προγράμματος περιήγησης του χρήστη για να διατηρήσουν της πληροφορίες που αφορούν την αυθεντικοποίηση του, ώστε να μην απαιτείται επανέλεγχος της ταυτότητας του (re-authentication) κάθε φορά που ο χρήστης συνδέεται στο σύστημα. Ωστόσο, δεδομένου ότι τα cookies δεν μεταδίδονται μεταξύ τομέων DNS, οι πληροφορίες αυθεντικοποίησης για κάποιο τομέα δεν μπορούν να διατεθούν σε κάποιον άλλον. Για να ξεπεραστεί αυτό το πρόβλημα, χρησιμοποιούνται μηχανισμοί *multi-domain SSO* (MDSSO) οι οποίοι αναλαμβάνουν την μεταφορά των πληροφοριών αυθεντικοποίησης των χρηστών από τον έναν τομέα στον άλλον. Και σε αυτήν την λύση όμως συναντώνται προβλήματα τα οποία έχουν οφείλονται στην ετερογένεια των συστημάτων μεταξύ των συναλλασσόμενων μερών. Με την χρήση του SAML μπορεί να ξεπεραστεί το πρόβλημα MDSSO καθώς ορίζει ένα πρότυπο γραμματικής και πρωτοκόλλου για την μεταφορά των πληροφοριών αυθεντικοποίησης από τον έναν τομέα στον άλλον μέσω του προγράμματος περιήγησης του χρήστη και το οποίο είναι ανεξάρτητο των συστημάτων που επικοινωνούν.
- **Ταυτότητα Ομοσπονδίας (**Federated identity**)**: Κατά την υλοποίηση διαδικτυακών υπηρεσιών σε ένα συνεργατικό περιβάλλον με κοινούς χρήστες, τα συστήματα θα

πρέπει να είναι σε θέση να κατανοούν τη σύνταξη του πρωτοκόλλου και των σχετικών σημασιολογιών που εμπλέκονται κατά την ανταλλαγή των πληροφοριών αυθεντικοποίησης, αλλά επίσης πρέπει να γνωρίζον και σε ποίον χρήστη αναφέρονται οι πληροφορίες αυτές. Οι χρήστες συχνά έχουν μεμονωμένες τοπικές ταυτότητες μέσα στο πλαίσιο των τομέων ασφάλειας του καθενός από τα συναλλασσόμενα μέρη με το οποίο αλληλεπιδρούν. Η Ταυτότητα της ομοσπονδίας παρέχει την δυνατότητα στα συναλλασσόμενα μέρη να συμφωνήσουν και να δημιουργήσουν ένα κοινό αναγνωριστικό (identifier) με το οποίο θα αναφέρονται στο χρήστη προκειμένου να μοιράζονται πληροφορίες για αυτόν. Ο χρήστης λέγεται ότι έχει μια ταυτότητα ομοσπονδίας όταν τα συναλλασσόμενα μέρη έχουν δημιουργήσει μια τέτοια συμφωνία σχετικά με το πώς θα αναφέρονται στο χρήστη. Αυτού του είδους η συμφωνία μπορεί να βοηθήσει στη μείωση του κόστους διαχείρισης ταυτοτήτων καθώς δεν είναι απαραίτητο συλλέγονται και να διατηρούνται τα δεδομένα που σχετίζονται με την ταυτότητα των χρηστών (π.χ. κωδικούς πρόσβασης, χαρακτηριστικά ταυτότητας) για κάθε υπηρεσία ξεχωριστά.

- **Διαδικτυακές υπηρεσίες και άλλα πρότυπα** (Web Services): Το SAML επιτρέπει την χρήση των ασφαλών ισχυρισμών (security assertions) που προτείνονται από το πρότυπο και σε άλλα πρότυπα ή υπηρεσίες αυθεντικοποίησης. Έτσι η ευελιξία και η προσαρμοστικότητα (modularity) του SAML επιτρέπει τα μηνύματα που ανταλλάσσονται και περιγράφονται σε αυτό να χρησιμοποιηθούν και εκτός του πλαισίου που περιγράφεται σε αυτό.

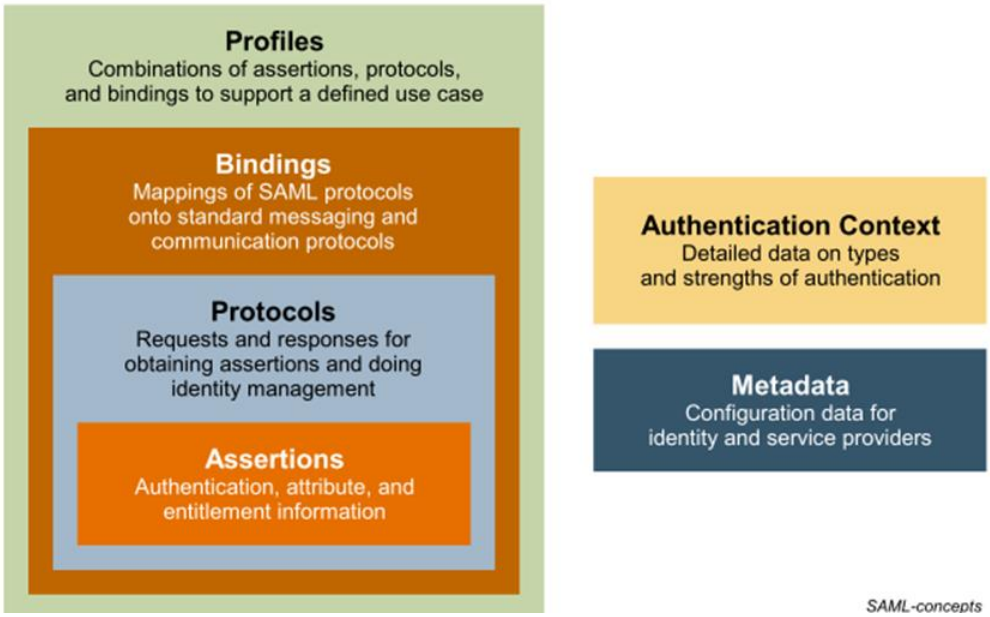
#### *7.1.2.1 Λειτουργία SAML*

Το πρότυπο SAML αποτελείται από μία σειρά δομικών στοιχείων τα οποία και σχηματίζουν μία ενιαία δομή (building block) μέσω της οποίας μπορεί να υποστηριχτούν διάφορες περιπτώσεις χρήσης. Τα δομικά στοιχεία επιτρέπουν τη μεταφορά των πληροφοριών της ταυτότητας, της αυθεντικοποίησης, των χαρακτηριστικών και των εξουσιοδοτήσεων μεταξύ των αυτόνομων οργανισμών που έχουν μια εδραιωμένη σχέση εμπιστοσύνης.

Στις προδιαγραφές του πυρήνα SAML ορίζεται η δομή και το περιεχόμενο των μηνυμάτων των ισχυρισμών και του πρωτοκόλλου που χρησιμοποιείται για τη μεταφορά αυτών των πληροφοριών Στο σχήμα 26 απεικονίζονται τα κυριότερα δομικά στοιχεία του SAML και η μεταξύ τους σχέση.

Οι ισχυρισμοί SAML μεταφέρουν δηλώσεις (statements) από ένα συναλλασσόμενο μέρος (asserting party ) το οποίο υποστηρίζει ότι είναι έγκυρες. Η έγκυρη δομή και το περιεχόμενο ενός ισχυρισμού ορίζονται μέσα στο XML σχήμα των SAML ισχυρισμών. Οι ισχυρισμοί συνήθως δημιουργούνται ως απόκριση σε αίτημα κάποιου από τα συμβαλλόμενα μέρη, αν και σε ορισμένες περιπτώσεις οι ισχυρισμοί αυτοί μπορεί να σταλούν στα συναλλασσόμενα μέρη χωρίς να έχει προηγηθεί σχετικό αίτημα. Για την υλοποίηση των SAML αιτημάτων και αποκρίσεων χρησιμοποιούνται τα μηνύματα πρωτοκόλλου SAML. Η δομή και τα περιεχόμενα των μηνυμάτων αυτών καθορίζονται από ένα πρωτόκολλο βασισμένο σε XML [60]. Ο τρόπος με τον οποίο τα χαμηλότερου επιπέδου πρωτόκολλα επικοινωνίας ή ανταλλαγής μηνυμάτων (όπως το HTTP ή το SOAP) χρησιμοποιούνται για να μεταφέρουν τα μηνύματα του πρωτοκόλλου SAML μεταξύ των συναλλασσομένων μερών ορίζεται από το επίπεδο δομικό στοιχείο *Bindings*.

Στη συνέχεια, ορίζεται το προφίλ SAML με τρόπο τέτοιο ώστε να εξυπηρετηθεί μια συγκεκριμένη περίπτωση χρήσης. Για παράδειγμα, ορίζεται ένα προφίλ που να ικανοποιεί την περίπτωση χρήσης SSO μέσα από ένα πρόγραμμα περιήγησης. Τα προφίλ συνήθως περιγράφουν τους περιορισμούς σχετικά με το περιεχόμενο των ισχυρισμών, των πρωτοκόλλων και των bindings του SAML για την επίτευξη μιας περίπτωσης χρήσης με διαλειτουργικό τρόπο. Ακόμη, υπάρχουν προφίλ χαρακτηριστικών μέσα από τα οποία ορίζονται οι τρόποι με τους οποίους μπορεί να γίνει μεταφορά χαρακτηριστικών, χρησιμοποιώντας τους ισχυρισμούς SAML.




**Σχήμα 26 : Βασικά στοιχεία του SAML [60]**

Δύο ακόμη έννοιες είναι χρήσιμες για την οικοδόμηση και την ανάπτυξη ενός περιβάλλοντος SAML: τα *μεταδεδομένα* και το *περιεχόμενο αυθεντικοποίησης* (authentication contex)

• Τα *μεταδεδομένα* ορίζουν ένα τρόπο με τον οποίο μπορούν να δηλωθούν και να μοιραστούν πληροφορίες και ρυθμίσεις παραμέτρων μεταξύ των συναλλασσόμενων μερών. Για παράδειγμα, με την χρήση εγγράφων μεταδεδομένων σε XML μορφή, μία οντότητα μπορεί να δηλώσει τους ρόλους που υποστηρίζει σε μια περίπτωση χρήσης (IDP, SP, κλπ), τις πληροφορίες ταυτότητας που χρησιμοποιεί ή ακόμα και πληροφορίες σχετικά με το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και την ψηφιακή υπογραφή.

• Σε ορισμένες περιπτώσεις, ένας πάροχος υπηρεσιών ενδέχεται να χρειάζεται λεπτομερείς πληροφορίες σχετικά με τον τύπο και το επίπεδο αξιοπιστίας της αυθεντικοποίησης που ένας χρήστης χρησιμοποιεί για την αυθεντικοποίηση του σε κάποιον πάροχο ταυτότητας. Ένα *πλαίσιο αυθεντικοποίησης* SAML χρησιμοποιείται (ή γίνεται αναφορά σε αυτό) μέσα από δηλώσεις ισχυρισμών αυθεντικοποίησης του

SAML για να μεταφέρει τις πληροφορίες αυτές. Ένας πάροχος υπηρεσιών μπορεί επίσης να συμπεριλάβει ένα πλαίσιο ελέγχου ταυτότητας σε ένα αίτημα προς έναν IdP και να ζητήσει για τον χρήστη να επαληθεύεται μέσα από ένα συγκεκριμένο σύνολο απαιτήσεων αυθεντικοποίησης. Υπάρχει ένα γενικό σχήμα XML που καθορίζει τους μηχανισμούς για τη δημιουργία δηλώσεων μέσα από πλαίσια αυθεντικοποίησης και ένα σύνολο κλάσεων πλαισίου αυθεντικοποίησης ορισμένα μέσω του SAML με ξεχωριστά XML σχήμα για το καθένα, που περιγράφουν τις πιο συχνά χρησιμοποιούμενες μεθόδους αυθεντικοποίησης.

#### *7.1.2.2 Ιδιωτικότητα στο SAML*

Όσο αφορά την ιδιωτικότητα, το SAML παρέχει μια σειρά από μηχανισμούς που υποστηρίζουν την προστασία της ιδιωτικότητας [60] .

- Υποστηρίζει τη δημιουργία ψευδωνύμων μεταξύ ενός παρόχου ταυτότητας και ενός παρόχου υπηρεσιών. Τέτοια ψευδωνύμα δεν επιτρέπουν την μη επιθυμητή συσχέτιση των χαρακτηριστικών των χρηστών μεταξύ των παρόχων υπηρεσιών, κάτι το οποίο θα ήταν εφικτό ο πάροχος ταυτότητας παρείχε το ίδιο αναγνωριστικό για έναν χρήστη σε κάθε φορέα παροχής υπηρεσιών (global identifier).
- Υποστηρίζει μίας χρήσης ή παροδικής αναγνώρισης αναγνωριστικά. Με αυτόν τον τρόπο εξασφαλίζεται ότι κάθε φορά που ένα συγκεκριμένος χρήστης αποκτά πρόσβαση σε ένα πάροχο υπηρεσιών μέσω μιας υπηρεσίας single sign-on από κάποιον πάροχο ταυτότητας, ο πάροχος υπηρεσιών δεν είναι σε θέση να τον αναγνωρίσει ως το ίδιο άτομο το οποίο του είχε παρέχει κάποια υπηρεσία στο παρελθόν
- Παρέχει μηχανισμούς πλαισίου αυθεντικοποίησης που επιτρέπουν στο χρήστη να αυθεντικοποιούνται με επαρκή (αλλά όχι περισσότερο από όσο είναι απαραίτητο) επίπεδο αξιοπιστίας, ανάλογα με τον πόρο στον οποίο προσπαθεί να αποκτήσει πρόσβαση σε κάποιο πάροχο υπηρεσιών

- Δίνει την δυνατότητα της διατύπωσης του απαιτούμενο γεγονότος για συναίνεση του χρήστη σε ορισμένες πράξεις μεταξύ των παρόχων.

### 7.1.3 Κύκλος εμπιστοσύνης (Circle of trust)

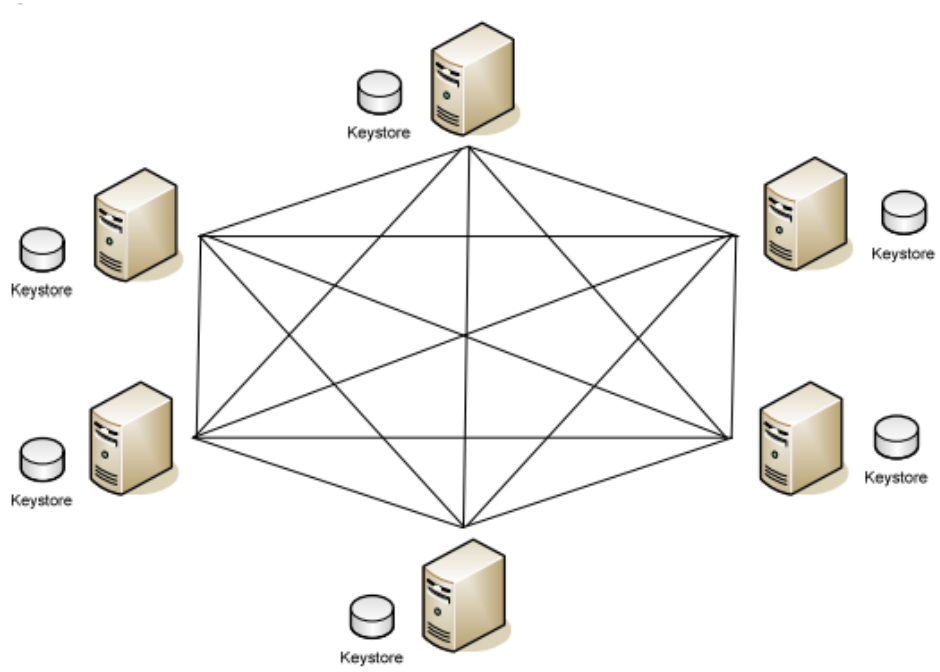
Όπως αναφέρθηκε και στο κεφάλαιο 6, η ασφάλεια της υποδομής του STORK βασίζεται στην δημιουργία ενός κύκλου εμπιστοσύνης. Η υλοποίηση αυτού του κύκλου εμπιστοσύνης σε επίπεδο λογισμικού γίνεται μέσα από την διασύνδεση των PEPSes μέσα από μια αρχιτεκτονική πλέγματος (Mesh architecture) και την ανταλλαγή μηνυμάτων ασφάλειας σύμφωνα με το πρότυπο SAML.

Όπως φαίνεται και στο σχήμα 27 κάθε PEPS διαχειρίζεται αρχεία καταγραφής *java keystore*. Σε ένα αρχείο keystore αποθηκεύονται κρυπτογραφικά μέσα, όπως κλειδιά κρυπτογράφησης και ψηφιακά πιστοποιητικά, ενώ συνήθως προστατεύονται και από κάποιο κωδικό. Η χρήση τέτοιων αρχείων επιτρέπει σε μια οντότητα να δημιουργεί σχέσης εμπιστοσύνης με τρίτους συμπεριλαμβάνοντας τα πιστοποιητικά τους (ή τα πιστοποιητικά της αντίστοιχης Αρχής Πιστοποίησης (CA authority)) στο δικό τους αρχείο keystore. Με αυτόν τον τρόπο μια οντότητα μπορεί να εμπιστευτεί μια άλλη είτε άμεσα (στην περίπτωση όπου έχει αποθηκευμένο το πιστοποιητικό της) είτε έμμεσα (στην περίπτωση που έχει αποθηκευμένο το πιστοποιητικό της αντίστοιχης Αρχής Πιστοποίησης). Κάθε PEPS διαχειρίζεται τρία τέτοια αρχεία keystore δύο εκ των οποίων επικεντρώνονται στην υλοποίηση του κύκλου εμπιστοσύνης (CoT) που αναφέρθηκε προηγουμένως, ενώ το τρίτο χρησιμοποιείται για την αποθήκευση κρυπτογραφικού υλικού, όπως για παράδειγμα τα ιδιωτικά κλειδιά των PEPSes.

Οι τύποι των μηνυμάτων που ανταλλάσσονται μεταξύ των PEPS μπορεί να είναι:

- Αίτημα SAML το οποίο αποστέλλεται από κάποιον «SAML αιτούντα» (*requester*) προς έναν «SAML αποκριτή» (*responder*).
- Αίτημα απόκρισης SAML το οποίο αποστέλλεται από κάποιον SAML αποκριτή προς έναν SAML αιτούντα.

- Αίτημα OCSP το οποίο αποστέλλεται από έναν OCSP αιτούντα προς έναν OCSP αποκριτή (responder).
- Αίτημα απόκρισης OCSP το οποίο αποστέλλεται από κάποιον OCSP αποκριτή προς έναν OCSP αιτούντα.




**Σχήμα 27 : Κύκλος Εμπιστοσύνης με αρχιτεκτονική πλέγματος [61]**

Κάθε PEPS συμπεριφέρεται σαν *requester* και *responder*. Όταν η παρεχόμενη υπηρεσία είναι υπηρεσία αυθεντικοποίησης ο τύπος των μηνυμάτων που ανταλλάσσονται αφορούν κάποιο SAML token, ενώ όταν η υπηρεσία είναι υπηρεσία επικύρωσης πιστοποιητικού τότε αφορούν κάποιο μήνυμα OCSP.

Κάθε μήνυμα που ανταλλάσσεται πρέπει να προστατεύεται από πιθανές επιθέσεις όπως αυτές των μη εξουσιοδοτημένων τροποποιήσεων, των επιθέσεων με παραποίηση ταυτότητας (identity masquerading attacks) και των υποκλοπών (eavesdropping). Για τον λόγω αυτό κάθε μήνυμα πρέπει να υπογράφεται ψηφιακά από τον αποστολέα χρησιμοποιώντας μεθόδους ασύμμετρης κρυπτογραφίας.

Προκειμένου να αποφευχθεί η ανάπτυξη μίας *adhoc PKI* λειτουργίας για την έκδοση και διαχείριση των πιστοποιητικών που θα πρέπει να χρησιμοποιηθούν από κάθε PEPS, η αρχιτεκτονική πλέγματος υλοποιεί έναν νοητό κύκλο άμεσης εμπιστοσύνης μεταξύ των PEPSes. Αυτό επιτυγχάνεται με την δημιουργία και τη διανομή των keystores που περιέχουν τα πιστοποιητικά κάθε PEPS στους κόμβους του κύκλου εμπιστοσύνης. Επιπλέον, κάθε πιστοποιητικό PEPS θα πρέπει να είναι ένα *self-signed* πιστοποιητικό. Για τους παραπάνω λόγους έχει δημιουργηθεί ένα έμπιστο κοινό keystore για να χρησιμοποιείται από όλους τους PEPS [61] .

Όπως προαναφέρθηκε, έχουν υλοποιηθεί τρία keystores, δύο εκ των οποίων σχετίζονται με την δημιουργία του κύκλου εμπιστοσύνης το τρίτο με την αποθήκευση του κρυπτογραφικού υλικού. Τα αρχεία αυτά είναι σε τυπική μορφή *Java KeyStore (JKS)*. Αναλυτικότερα είναι τα [61] :

- **STORKTrustedKeyStore.jks:** Σε αυτό το αρχείο αποθηκεύονται τα self-signed πιστοποιητικά του κάθε PEPS και χρησιμοποιούνται για την υπογραφή των SAML tokens και των OCSP αιτημάτων. Το πιστοποιητικό που χρησιμοποιείται για την υπογραφή των αιτημάτων και των αποκρίσεων SAML καθώς και των αιτημάτων OCSP, μπορεί να είναι το ίδιο καθώς δεν απαιτείται κάποια επιπλέον επέκταση ή πληροφορία για τον διαχωρισμό αυτών. Έτσι μπορεί να χρησιμοποιηθεί για την προστασία των μηνυμάτων και στις δύο περιπτώσεις.
- **STORKOCSPRespondersTrustedKeyStore.jks:** Σε αυτό το αρχείο αποθηκεύονται τα self-signed πιστοποιητικά του κάθε PEPS τα οποία χρησιμοποιούνται για την υπογραφή των OCSP αποκρίσεων. Στα πιστοποιητικά που περιέχονται σε αυτό το αρχείο θα πρέπει να περιλαμβάνουν την επέκταση για το κλειδί id-kp-OCSPSigning OID του αναγνωριστικού του αντικειμένου (object identifier OID).
- **STORKOwnKeyStore.jks:** Τα δύο παραπάνω αρχεία περιλαμβάνουν μόνο τα ψηφιακά πιστοποιητικά αλλά όχι τα ιδιωτικά κλειδιά. Στο αρχείο αυτό περιέχονται τα δύο self-signed πιστοποιητικά τα οποία περιέχονται και στα παραπάνω αρχεία καθώς και τα αντίστοιχα κλειδιά του κάθε PEPS. Το ένα κλειδί χρησιμοποιείται από τα PEPS για την υπογραφή των OCSP αποκρίσεων

που αποστέλλονται σε άλλα PEPS. Το δεύτερο κλειδί χρησιμοποιείται για την υπογραφή των SAML αιτημάτων και αποκρίσεων.

### 7.1.4 Μονάδες για την υλοποίηση του πρωτοκόλλου SAML

Στο σχήμα 28 απεικονίζεται η λειτουργία του μηχανισμού αυθεντικοποίησης. Καθώς, το πρωτόκολλο SAML είναι αυτό που χρησιμοποιείται για την αυθεντικοποίηση των χρηστών, ο μηχανισμός αυτός ονομάζεται και μηχανισμός SAML (SAMLENGINE). Στις παρακάτω παραγράφους επεξηγούνται τα επιμέρους μέρη του μηχανισμού[62].

Το επίπεδο αυθεντικοποίησης είναι υπεύθυνο για την εφαρμογή της επιχειρησιακής λογικής της υπηρεσίας αυθεντικοποίησης των PEPSes, τόσο για το C-PEPS και το S-PEPS. Κάτω από αυτό το επίπεδο, η λειτουργία χωρίζεται στα κοινά και τα ειδικά μέρη.

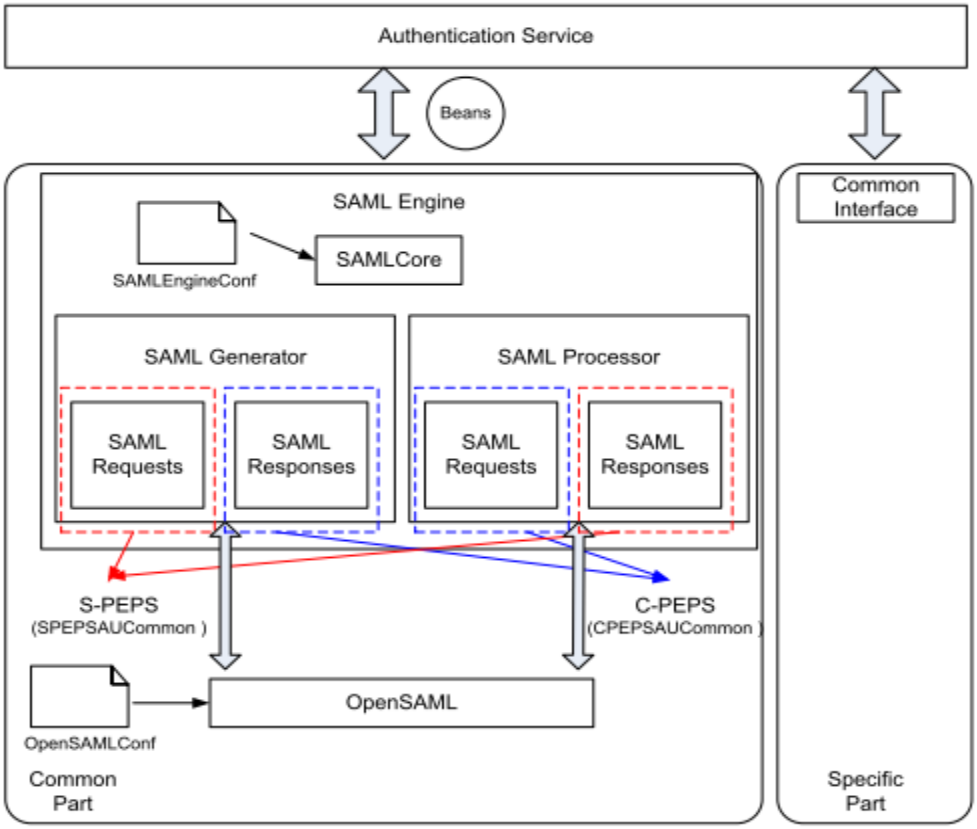
Η μονάδα λογισμικού του μηχανισμού SAML (SAML Engine) είναι υπεύθυνη για την διεκπεραίωση αιτημάτων (S-PEPS) και αποκρίσεων (C-PEPS) των SAML μηνυμάτων. Οι ρυθμίσεις για αυτήν την μονάδα γίνονται μέσω της υπομονάδας του πυρήνα SAML (SAML CORE). Η υπομονάδα του πυρήνα SAML διαχωρίζεται στις κάτωθι υποενότητες:

- **Γεννήτρια SAML**: Είναι το κομμάτι του μηχανισμού το οποίο είναι υπεύθυνο για τη δημιουργία SAML token τα οποία μπορεί να είναι είτε αιτήματα αυθεντικοποίησης (ή παροχής χαρακτηριστικών) SAML είτε αποκρίσεις SAML (SAML Assertions) σε ερωτήματα αυθεντικοποίησης ή παροχής χαρακτηριστικών.
- **Επεξεργαστής SAML**: Είναι το κομμάτι του μηχανισμού το οποίο είναι υπεύθυνο για την επικύρωση και την επεξεργασία των παραπάνω SAML tokens.

Η λειτουργίες των S-PEPS καλύπτονται από τις επιμέρους λειτουργίες της υπομονάδας της γεννήτριας SAML για την παραγωγή αιτημάτων (SAML request) και τις λειτουργίες της υπομονάδας του επεξεργαστή SAML για την απόκριση στα αιτήματα SAML (responses). Δηλαδή, το S-PEPS δημιουργεί αιτήματα και επεξεργάζεται τις αποκρίσεις σε αυτά.

Η λειτουργίες των C-PEPS καλύπτονται από τις επιμέρους λειτουργίες της υπομονάδας του επεξεργαστή SAML για την δημιουργία αιτημάτων SAML και τις επιμέρους λειτουργίες της υπομονάδας της γεννήτριας SAML για την απόκριση σε αιτήματα SAML. Δηλαδή, το C-PEPS επεξεργάζεται αιτήματα και δημιουργεί αποκρίσεις για αιτήματα.

Οι σχετικές SAML πληροφορίες που παράγονται, μεταφέρονται από το επίπεδο του μηχανισμού SAML στο επίπεδο αυθεντικοποίησης μέσα από ένα επίπεδο υπηρεσιών μέσω των αντίστοιχων κλάσεων λογισμικού (Beans).




**Σχήμα 28 : Σχηματική αναπαράσταση του μηχανισμού SAML [61]**

### 7.1.5 Μονάδες για την υλοποίηση της επικύρωσης των PEPS (ValidationPEPS)

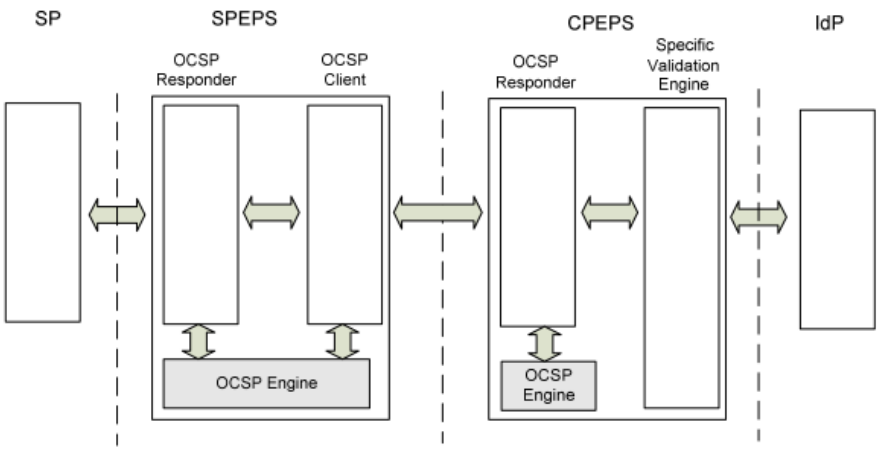
Ο μηχανισμός OCSP είναι υπεύθυνος για την υλοποίηση των διαδικασιών (όπως την έκδοση, τη δημιουργία, κτλ.) που αφορούν τα μηνύματα OCSP, τόσο για τα αιτήματα OCSP όσο για τις αποκρίσεις OCSP. Η αρχιτεκτονική μέσω της οποίας υλοποιείται η υπηρεσία επικύρωσης των PEPSes, παρουσιάζεται στο σχήμα 29, όπου ένας πάροχος υπηρεσιών αιτείται την επικύρωση ενός PEPS κατά την διαδικασία της

αυθεντικοποίησης. Το μοντέλο υλοποίησης του μηχανισμού επικύρωσης φαίνεται στο σχήμα 30.

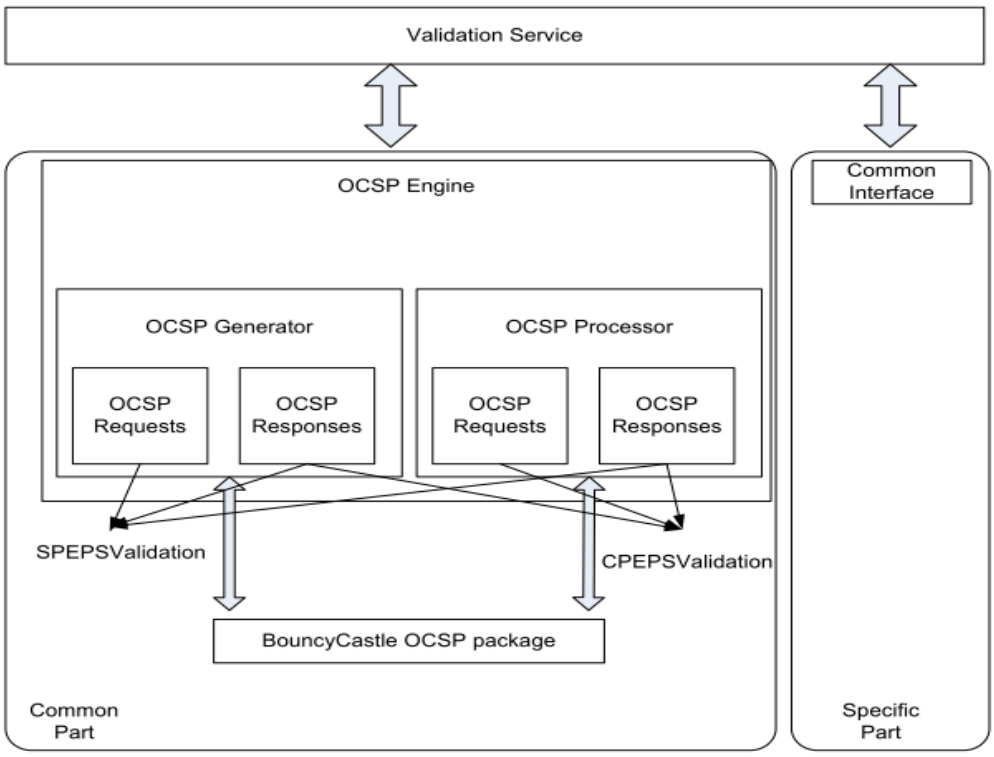
Η λειτουργίες των S-PEPS καλύπτονται από τις υπομονάδες αιτημάτων OCSP και αποκρίσεων OCSP της γεννήτριας OCSP καθώς και από την υπομονάδα αποκρίσεων OCSP του επεξεργαστή OCSP. Δηλαδή, το S-PEPS δημιουργεί OCSP αιτήματα, επεξεργάζεται OCSP αποκρίσεις και δημιουργεί αποκρίσεις OCSP [61].

Η λειτουργίες των C-PEPS καλύπτονται από τις υπομονάδες αιτημάτων OCSP και αποκρίσεων OCSP του επεξεργαστή καθώς και από την υπομονάδα αποκρίσεων OCSP της γεννήτριας OCSP. Δηλαδή, το C-PEPS επεξεργάζεται τις αιτήσεις που λαμβάνει από το S-PEPS και τις αποκρίσεις λαμβάνει από τον συγκεκριμένο μηχανισμό επικύρωσης (Specific Validation Engine) και δημιουργεί τις OCSP αποκρίσεις που πρέπει να σταλούν πίσω στο S-PEPS.

Η μηχανισμός OCSP διαχειρίζεται τα αντικείμενα OCSP μέσω της βιβλιοθήκης BouncyCastle OCSP. Αυτή η βιβλιοθήκη περιέχει διάφορες κλάσεις που μπορούν οι οποίες μπορούν να χρησιμοποιηθούν από τον μηχανισμό OCSP, όπως της BasicOCSPResp (για την δημιουργία των βασικών μηνυμάτων απόκρισης OCSP), της OCSPReqGenerator για την δημιουργία των αιτημάτων OCSP ή της OCSPRespGenerator για την παραγωγή αποκρίσεων OCSP [61] .




Σχήμα 29: Αρχιτεκτονική επικύρωσης PEPS [61]




Σχήμα 30 : Μηχανισμός επικύρωσης PEPS [61]

### 7.1.6 Μονάδες λογισμικού κοινών και εξειδικευμένων λειτουργιών (Commons & Specific)

Οι μονάδες *Commons* και *Specific* αφορούν η πρώτη τις κοινές απαιτήσεις και προδιαγραφές ενώ η δεύτερη τις εξειδικευμένες απαιτήσεις και προδιαγραφές που θέλει κάθε κράτος να υλοποιήσει ξεχωριστά.

Έτσι στην δομική μονάδα Commons περιέχονται αρχεία όπως αυτά που ορίζουν το μέγιστο μέγεθος των παραμέτρων, τα μηνύματα λάθους, την υλοποίηση της κλάσης για το άθροισμα ελέγχου (hash class) ή αν η επικύρωση του πιστοποιητικού του PEPS είναι ενεργή.

Στην δομική μονάδα *Specific* περιέχονται όλες εκείνες οι ειδικές ρυθμίσεις που καλύπτουν τις ιδιαιτερότητες της λειτουργίας του PEPS κάθε κράτους. Μερικές από αυτές είναι η κανονικοποίηση (*Normalization*), η παραγωγή χαρακτηριστικών (*derivation*), η επικύρωση τιμών των χαρακτηριστικών (*validation*) και η παραγωγή ψηφιακής υπογραφής (*Signature Creator*) [61] .

Η λειτουργία της κανονικοποίησης χρησιμοποιείται για να μεταφράσει τα ονόματα από τις τοπικές ρυθμίσεις των PEPS στην μορφή που ορίζεται από το STORK, και αντίστροφα. Η παραγωγή χαρακτηριστικών χρησιμοποιείται για την μετάφραση κάποιον συγκεκριμένων χαρακτηριστικών τα οποία δεν μπορούν να αποσταλούν απευθείας στον πάροχο ταυτότητας, σε κάποιο άλλο χαρακτηριστικό πριν από την αποστολή. Μέσω της επικύρωσης των τιμών των χαρακτηριστικών ορίζονται οι τιμές των χαρακτηριστικών εκείνων, οι οποίες πρέπει να επικυρώνονται πριν από την δημιουργία της απάντησης από το C-PEPS προς το S-PEPS.

### 7.1.7 Μονάδες υλοποίησης παρόχου υπηρεσιών και ταυτότητας (SP & IdP)

Μέσα από τις μονάδες λογισμικού του STORK παρέχονται και αυτές οι οποίες υλοποιούν τον ρόλο του παρόχου υπηρεσιών και του παρόχου ταυτοποίησης ενώ για δοκιμαστικούς σκοπούς παρέχονται και ολοκληρωμένες διεπαφές.

Κάθε πάροχος υπηρεσιών πρέπει να υλοποιήσει την δικιά του διεπαφή συμπεριλαμβάνοντας σε αυτήν τις βασικές συναρτήσεις που ορίζονται από το STORK για την επικοινωνία με τις υπόλοιπες δομικές μονάδες του συστήματος. Ειδικότερα για τον πάροχο ταυτότητας δίνονται δύο επιλογές: η εσωτερική και η εξωτερική.

Υπάρχουν δύο διαφορετικοί μηχανισμοί αυθεντικοποίησης: εσωτερικός (internal) και εξωτερικός (external) [61]:

- Κατά την αυθεντικοποίηση που χρησιμοποιείται ο εξωτερικός μηχανισμός, η εφαρμογή ανακατευθύνει την αίτηση αυθεντικοποίησης σε ένα πάροχο ταυτότητας (IdP) ο οποίος την χειρίζεται και στη συνέχεια αφού το απαντητικό του μήνυμα μετατραπεί στην κατάλληλη μορφή στέλνεται στο πάροχο υπηρεσιών. Η ανακατεύθυνση της αίτησης καθώς και η μετατροπή του μηνύματος γίνονται από κλάσεις της μονάδας Specific.
- Κατά την αυθεντικοποίηση όπου χρησιμοποιείται ο εσωτερικός μηχανισμός η αίτηση αυθεντικοποίησης διεκπεραιώνεται εσωτερικά στο C-PEPS.

Όσο αφορά την παροχή χαρακτηριστικών αυτή υλοποιείται με τρείς τρόπους: εσωτερικά , εξωτερικά και διαμέσω του παρόχου ταυτότητας.

- Σύμφωνα με τον «εξωτερικό» τρόπο το αίτημα παροχής χαρακτηριστικών ανακατευθύνεται σε έναν ή περισσότερους παρόχους χαρακτηριστικών (AP) οι οποίοι διεκπεραιώνουν το αίτημα και απαντούν στο C-PEPS. Η ανακατεύθυνση της αίτησης υλοποιείται όπως και στην περίπτωση της εξωτερικής αυθεντικοποίησης από κλάσεις της μονάδας Specific.
- Κατά τον εσωτερικό τρόπο, το αίτημα διεκπεραιώνεται απευθείας στο C-PEPS.
- Τα χαρακτηριστικά μπορούν ακόμη να χορηγηθούν και από τον πάροχο ταυτότητας. Σε αυτήν την περίπτωση δεν είναι απαραίτητη η ύπαρξη του παρόχου χαρακτηριστικών.

### 7.1.8 Μονάδα αναβάθμισης και ελέγχου έκδοσης συστήματος (Updater & Version Control)

Ο έλεγχος έκδοσης (version control) είναι ένα πρόγραμμα το οποίο στην ουσία εξασφαλίζει ότι τα PEPS όλων των κρατών έχουν την ίδια έκδοση λογισμικού. Εκτελείται σε καθημερινή βάση και εξάγει από το λογισμικό το αριθμό έκδοσης του, από τα αρχεία παραμετροποιήσεων την ημερομηνία της τελευταίας τροποποίησης τους και δημοσιοποιεί τα στοιχεία αυτά μέσα από ένα XML αρχείο στα υπόλοιπους εταίρους του STORK

Με αυτό τον τρόπο όλοι οι εταίροι του STORK μπορούν να γνωρίζουν πότε έχουν γίνει οι αλλαγές. Τα αρχεία ελέγχου όλων των εταίρων μεταφορτώνονται σε καθημερινή βάση και συντίθεται από αυτά ένα παρόμοιο με το παλιό, νέο αρχείο ελέγχου έκδοσης το οποίο και κοινοποιείται στους παρόχους υπηρεσιών μέσα στην ίδια χώρα. Αυτό το αρχείο περιέχει για το εθνικό PEPS την ίδια περιγραφή με το προηγούμενο αρχείο και επιπλέον μια σύνοψη των διαθέσιμων δεδομένων και QAA για κάθε άλλη χώρα. Ένα πρόγραμμα ενημέρωσης για την λειτουργία της «επιλογής χωρών» (*country selector updater*) κατεβάζει αυτό το αρχείο κάθε μέρα και ενημερώνει των επιλογέα χώρων του κάθε παρόχου υπηρεσιών, λαμβάνοντας υπόψη τα χαρακτηριστικά και το QAA επίπεδο που απαιτείται από την υπηρεσία, καθώς και τις χώρες οι οποίες πρέπει να εξαιρεθούν. Με αυτό τον τρόπο, οι νέες χώρες περιλαμβάνονται αυτόματα σε όλους τους «επιλογείς χώρων» όλων των παρόχων υπηρεσιών μόλις κάποιος εθνικός κόμβος STORK περιλάβει τη χώρα αυτή [61] .

Από την άλλη πλευρά, αυτή λειτουργία του έλεγχου έκδοσης δημοσιεύει τα στοιχεία έκδοσης κάθε εγκατάστασης, επιτρέποντας έτσι τον εθνικό φορέα που διαχειρίζεται τα PEPS να ελέγξει αν έχουν εγκατασταθεί τα αναγκαία *patches* και να αποφασίσει αν κάποιο νέο μπορεί να εγκατασταθεί.

### 7.1.9 Διαδικασία Αυθεντικοποίησης

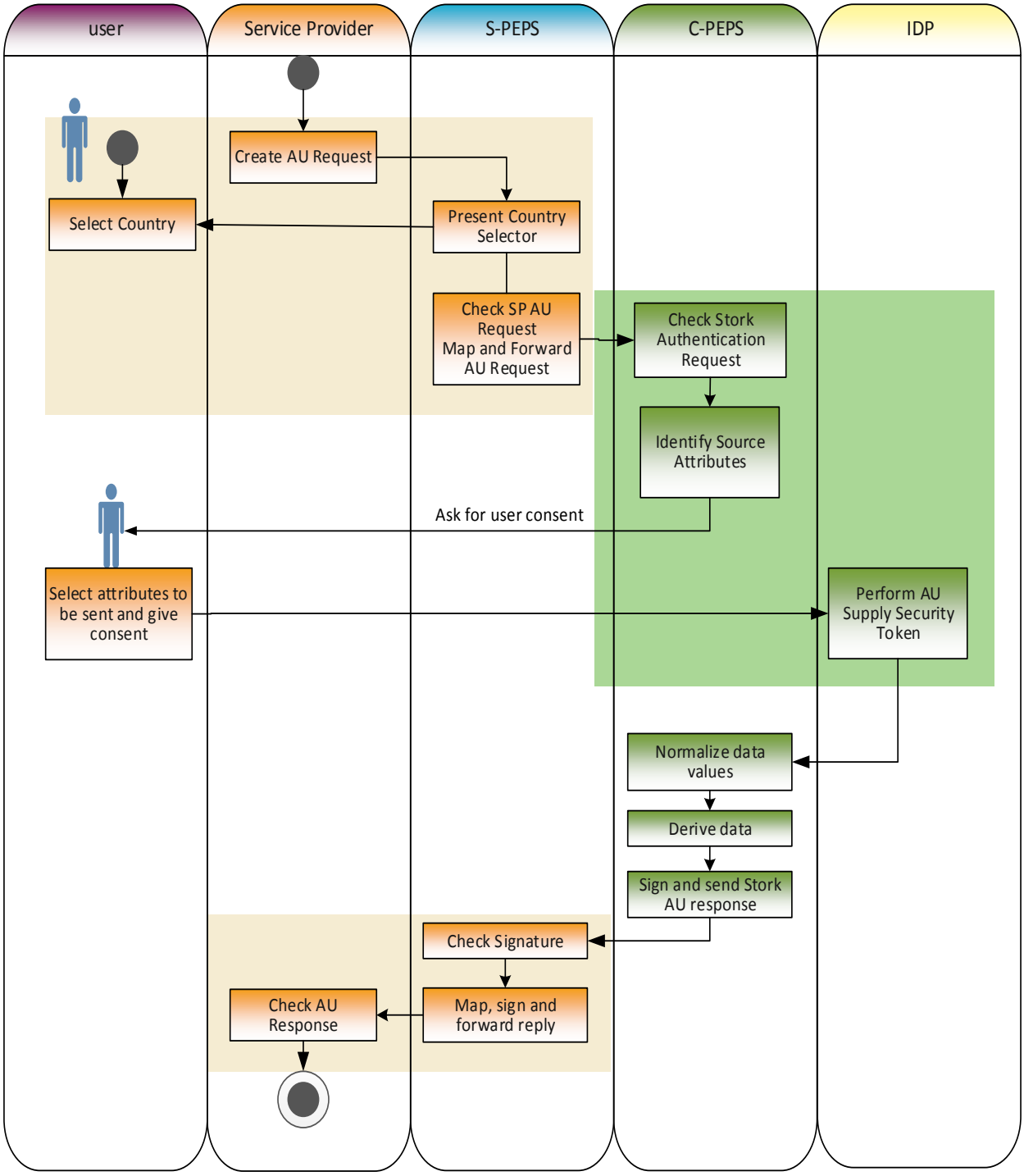
Για να αποκτήσει πρόσβαση ένας χρήστης σε κάποια ηλεκτρονική υπηρεσία που προσφέρεται από ή μέσα σε κάποιο κράτος μέλος της ΕΕ, θα πρέπει να παρουσιάσει την ηλεκτρονική του ταυτότητα μέσω του υπολογιστή που χρησιμοποιεί. Μέσω της διαλειτουργικής πλατφόρμας του STORK η οποία είναι προσβάσιμη από οποιοδήποτε διαδικτυακό φυλλομετρητή, προσφέρεται η δυνατότητα στον πάροχο μίας υπηρεσίας της επικύρωσης της ηλεκτρονικής ταυτότητας του χρήστη και μετά από την συγκατάθεση του τελευταίου, της μεταφοράς των δεδομένων της ταυτότητας στον πάροχο που προσφέρει την ηλεκτρονική υπηρεσία.

Κατά την τυπική διαδικασία αυθεντικοποίησης με την χρήση της πλατφόρμας του STORK, ο χρήστης επιλέγει μια ηλεκτρονική υπηρεσία που προσφέρεται από έναν πάροχο υπηρεσιών και ο οποίος υποστηρίζεται από την πλατφόρμα του STORK. Εφόσον ο χρήστης επιλέξει να αυθεντικοποιηθεί μέσω της ηλεκτρονικής του ταυτότητας ή κάποιας ισοδύναμης ταυτότητας η οποία αναγνωρίζεται από το STORK, ο πάροχος ζητάει από αυτόν να επιλέξει την χώρα από την οποία θέλει να αυθεντικοποιηθεί, δηλαδή την χώρα έκδοσης της ταυτότητας του. Αφού επιλέξει μέσα από μία λίστα χωρών αυτήν στην οποία θέλει να αυθεντικοποιηθεί, γίνεται ανακατεύθυνση του αιτήματος του για αυθεντικοποίηση μέσα από την πλατφόρμα του STORK προς το αντίστοιχο PEPS και πιο συγκεκριμένα προς το S-PEPS της χώρας αυτής.

Μετά από κάποιους ελέγχους που αφορούν την προέλευση του αιτήματος, την εγκυρότητα του καθώς και την ορθή σύνταξη του από το S-PEPS, το μήνυμα αυθεντικοποίησης υπογράφεται ψηφιακά και αποστέλλεται προς το C-PEPS. Το C-PEPS με την σειρά του ελέγχει την σύνταξη του μηνύματος , το περιεχόμενο του και αν προέρχεται από κάποιον έγκυρο και έμπιστο κόμβο. Ελέγχεται η πηγή των αιτούμενων χαρακτηριστικών και αποστέλλει ανάλογο μήνυμα προς τον πάροχο ταυτότητας αφού όμως πρώτα ενημερώσει τον χρήστη για τα ζητούμενα χαρακτηριστικά και ζητήσει την συγκατάθεση του για την ενέργεια αυτή. Ο πάροχος ταυτότητας αυθεντικοποιεί τον χρήστη και αποστέλλει τις απαιτούμενες πληροφορίες στο C-PEPS. Στο C-PEPS γίνεται η κανονικοποίηση των δεδομένων, όπως για παράδειγμα η μεταφορά της

κωδικοποίησης των δεδομένων από την μορφή του STORK στην μορφή που ζητείται από την χώρα προέλευσης του αιτήματος. Επιπλέον από τα δεδομένα που μεταφέρθηκαν γίνεται και η παραγωγή νέων χαρακτηριστικών. Ένα τέτοιο παραγόμενο χαρακτηριστικό μπορεί να είναι αυτό το οποίο εκφράζει αν ο χρήστης είναι πάνω από μία ζητούμενη ηλικία (isAgeOver()).

Στο σχήμα 31 παρουσιάζεται το διάγραμμα δραστηριοτήτων της τυπικής διαδικασίας αυθεντικοποίησης. Στο διάγραμμα αυτό παραλείπεται ο σχεδιασμός των ανακατευθύνσεων που δρομολογούνται κατά την ανταλλαγή μηνυμάτων SAML. Ο πίνακας 7 επεξηγεί της διαδικασίες που υλοποιούνται από το κάθε συναλλασσόμενο μέρος.




**Σχήμα 31: Διάγραμμα δραστηριοτήτων διαδικασίας αυθεντικοποίησης**

Πίνακας 7: Επιμέρους διαδικασίες αυθεντικοποίησης

| | |
|---|---|
| **Sp** | **Create AU Request**<br><br>Ο χρήστης έχει επιλέξει μια υπηρεσία η οποία απαιτεί αυθεντικοποίηση. Ο πάροχος υπηρεσιών στέλνει ένα αίτημα για Αυθεντικοποίηση Χρήστη (AU request) στο S-PEPS. Το αίτημα περιλαμβάνει το απαιτούμενο επίπεδο QAA, τα υποχρεωτικά και προαιρετικά ζητούμενα χαρακτηριστικά και κάποια ταυτότητα του SP. |
| **S-PEPS** | **Present country selector**<br><br>Το S-PEPS παρέχει κάποιο κώδικα ο οποίος ενσωματώνεται στην ιστοσελίδα του S-PEPS από όπου ο χρήστης μπορεί να επιλέξει την εθνικότητα της ταυτότητας του. Η ιστοσελίδα περιέχει της σημαίες των κρατών κάθε χώρας που συμμετέχει στο STORK μαζί με το όνομα της χώρας που απεικονίζει στην γλώσσα της κάθε χώρας. |
| **User** | **Select country**<br><br>Όταν ένας πολίτης επιλέγει μια χώρα, μια αίτηση αυθεντικοποίησης αποστέλλεται στον S-PEPS. Το αίτημα θα περιλαμβάνει: το επίπεδο αυθεντικοποίησης QAA, τα υποχρεωτικά και προαιρετικά χαρακτηριστικά, το αναγνωριστικό του SP και την χώρα της ταυτότητας του χρήστη. |
| **S-PEPS** | **Check SP AU Request**<br><br>Το S-PEPS λαμβάνει το αίτημα αυθεντικοποίησης του χρήστη και ελέγχει το αίτημα ως προς την προέλευση, τη μορφή και το περιεχόμενο του.<br><br>***Έλεγχος προέλευσης***<br><br>Κάθε χώρα εφαρμόζει τοπικές πολιτικές ελέγχου για τον προσδιορισμό των SP που μπορούν να έχουν πρόσβαση στα PEPS τους. Τα PEPS εκτελούν ορισμένους ελέγχους για να επιβεβαιωθεί ότι ο SP μπορεί να ζητήσει έλεγχο |

| | |
|---|---|
| | ταυτότητας σε αυτό PEPS.<br><br>Π.χ. Μπορεί να ελέγχει τον τομέα από τον οποίο προέρχεται το αίτημα του ώστε να επιβεβαιώσει ότι προέρχεται από την χώρα του.<br><br>- ελέγχει τον αριθμό των αιτήσεων για τα τελευταία 60 δευτερόλεπτα: Εάν ο αριθμός αυτός υπερβαίνει μια μέγιστη τιμή, το εισερχόμενο αίτημα απορρίπτεται (για την αποφυγή επιθέσεων τύπου DoS).<br><br>***Έλεγχος περιεχομένου***<br><br>Το περιεχόμενο του αιτήματος ελέγχεται για την εγκυρότητα του και τη μορφή του:<br><br>- Εάν η μορφή είναι εσφαλμένη η αίτηση απορρίπτεται.<br><br>- πρέπει να προσδιορίζεται το επίπεδο QAA καθώς και η εθνικότητα της ταυτότητας του χρήστη.<br><br>***Προσδιορισμός προορισμού***<br><br>Ο κωδικός της χώρας περιλαμβάνεται στην αίτηση αυθεντικοποίησης. Αν δεν αναγνωρίζεται, η αίτηση απορρίπτεται. Με τον κωδικό της χώρας καθορίζεται ο προορισμός, δηλαδή το PEPS, του αιτήματος αυθεντικοποίησης. |
| **Sp** | **Map and Forward AU Request**<br><br>***Αντιστοίχιση χαρακτηριστικών***<br><br>Τα χαρακτηριστικά μεταφράζονται σύμφωνα με τους όρους του STORK. Μόνο ορισμένα χαρακτηριστικά μπορούν να ζητηθούν.<br><br>Π.χ. μια χώρα μπορεί να επιτρέπει να ζητείται το χαρακτηριστικό *moradaTexto* (διεύθυνση στα πορτογαλικά), το οποίο όμως μεταφράζεται |

| | |
|---|---|
| | σε *textResidenceAddress* πρέπει να μεταφραστεί στο STORK σε *textResidenceAddress.* Η μετάφραση γίνεται από μια ειδική λειτουργία (specific functionality).<br><br>***Αποστολή αιτήματος αυθεντικοποίησης*.**<br><br>Το S-PEPS χρησιμοποιεί τις πληροφορίες που έχουν συγκεντρωθεί για να προετοιμάσει το αίτημα της αυθεντικοποίησης του χρήστη προς το C-PEPS.<br><br>Το πακέτο δεδομένων της αίτησης υπογράφεται από τον S-PEPS και αποστέλλεται στο C-PEPS |
| **C-PEPS** | **Check STORK AU Request**<br><br>Το C-PEPS παραλαμβάνει και ελέγχει την αίτηση αυθεντικοποίησης του χρήστη.<br><br>***Έλεγχος προέλευσης***<br><br>Γίνεται ο έλεγχος για το αν η αίτηση προέρχεται από ένα έμπιστο PEPS. Εάν όχι, το αίτημα απορρίπτεται. |
| **C-PEPS** | **Identify source attributes**<br><br>Εάν το S-PEPS είναι αξιόπιστο το C-PEPS εξάγει τις παραμέτρους αιτήματος από την αίτηση αυθεντικοποίησης του χρήστη.<br><br>**Έλεγχος του περιεχομένου και της μορφή της αίτησης.**<br><br>Εάν η μορφή είναι εσφαλμένη η αίτηση απορρίπτεται.<br><br>Έλεγχος περιεχομένου: Γίνεται αντιστοίχιση των αιτούμενων χαρακτηριστικών με τα χαρακτηριστικά των κρατών μελών. |

| | |
|---|---|
| | **Έλεγχος πληρότητας**<br><br>Γίνεται έλεγχος αν για κάθε ένα από τα αντιστοιχισμένα υποχρεωτικά χαρακτηριστικά υπάρχει κάποιο εθνικό διαπιστευτήριο (κάρτα, πιστοποιητικό, κλπ.) ή κάποιος πάροχος Χαρακτηριστικών που μπορεί να δώσει τα αιτούμενα χαρακτηριστικά.<br><br>Στην συνέχεια γίνεται ο ίδιος έλεγχος και για τα προαιρετικά χαρακτηριστικά. |
| **C-PEPS** | **Normalise data values**<br><br>Γίνεται η κανονικοποίηση των δεδομένων. Αυτή η λειτουργία Η εξομάλυνση των δεδομένων που είναι ειδικό για κάθε χώρα. Αυτή η λειτουργία μετατρέπει την εθνική κωδικοποίηση και μορφοποίηση των δεδομένων κάθε χώρας στην κωδικοποίηση και μορφή του STORK.<br><br>Π.χ. το φύλο μπορεί σε εθνικό επίπεδο να αναφέρεται ως M (ännlich) και W (eiblich), ενώ στο STORK χρησιμοποιείται η κωδικοποίηση M(ale) και F(emale).<br><br>Στην συνέχεια, γίνεται η αντιστοίχηση των τιμών των χαρακτηριστικών και των δεδομένων. Τα χαρακτηριστικά που λήφθηκαν αντιστοιχίζονται με τα χαρακτηριστικά που ζητήθηκαν από τον πάροχο υπηρεσιών μέσω του S-PEPS. |
| **C-PEPS** | **Derive data**<br><br>Τα χαρακτηριστικά που λήφθηκαν από το C-PEPS χρησιμοποιούνται για την δημιουργία δεδομένων όπου χρειάζεται. |
| **C-PEPS** | **Sign and send STORK AU Response**<br><br>Το C-PEPS υπογράφει και αποστέλλει ένα μήνυμα (assertion) που περιέχει όλα τα δεδομένα τα οποία έχουν συλλεχτεί από το S-PEPS |

| | |
|---|---|
| **S-PEPS** | **Check signature**<br><br>Γίνεται έλεγχος και επικύρωση του μηνύματος (assertion) από το S-PEPS. Ένα το μήνυμα προέρχεται από κάποιο έμπιστο PEPS η διαδικασία συνεχίζεται, διαφορετικά απορρίπτεται το αίτημα. |
| **S-PEPS** | **Map, sign and forward reply**<br><br>Εάν το μήνυμα είναι έγκυρο, το S-PEPS εξάγει το περιεχόμενο του.<br><br>**Map the attributes**<br><br>Προσδιορίζεται για κάθε χαρακτηριστικό που λήφθηκε μέσω του STORK ποιο είναι το αντίστοιχο χαρακτηριστικό στον πάροχο υπηρεσιών.<br><br>**Build, sign and send response to the SP**<br><br>*Δημιουργείται* (*Build*) το μήνυμα απόκρισης με τα αντιστοιχισμένα χαρακτηριστικά.<br><br>*Υπογράφεται* (*Sign*) και προωθείται το μήνυμα απόκρισης στον πάροχο υπηρεσιών. |
| **SP** | **Check AU Response**<br><br>Ο πάροχος υπηρεσιών ελέγχει την προέλευση και το περιεχόμενο του μηνύματος απόκρισης, επικυρώνει το μήνυμα (assertion) και παρέχει πρόσβαση στην αιτούμενη υπηρεσία εάν θεωρήσει το μήνυμα έμπιστο. |

Σε κάθε περίπτωση πριν μεταφερθούν τα δεδομένα, πρέπει να ζητηθεί η συγκατάθεση του χρήστη. Εξαρτάται την από την υλοποίηση του συστήματος της κάθε χώρας αν το αίτημα αυτό θα γίνει πριν ζητηθούν τα δεδομένα ή πριν αποσταλούν. Επιπλέον, ο χρήστης θα πρέπει να είναι σε θέση να απορρίψει την μεταφορά των προαιρετικών χαρακτηριστικών. Ακόμη, τα δεδομένα που περιέχονται στην απόκριση του αιτήματος αυθεντικοποίησης πρέπει να διατηρηθούν εμπιστευτικά, ενώ πρέπει να διασφαλίζεται η προέλευση και η ακεραιότητα των μηνυμάτων αυθεντικοποίησης που ανταλλάσσονται με την χρήση κατάλληλης ψηφιακής υπογραφής.

## 7.2 Εγκατάσταση και Παραμετροποίηση του Συστήματος

Το σύστημα παρέχεται από την ΕΕ μέσω της ιστοσελίδας *Joinup* ( http://joinup.ec.europa.eu/software/stork/release/10-ms ) σε μορφή επιμέρους μονάδων λογισμικού. Για την ανάπτυξη του συστήματος χρησιμοποιήθηκε το «ανοικτού» κώδικα λογισμικό διαχείρισης έργων *Apache Maven*[28]. Το Maven βασίζεται στην έννοια του μοντέλου αντικειμένου έργου (project object model (POM)), και μέσω αυτού μπορεί να γίνει η διαχείριση και η κατασκευή ενός έργου βασισμένου σε γλώσσα JAVA καθώς και η υποβολή εκθέσεων και τεκμηρίωσης του. Επίσης, ο server που χρησιμοποιήθηκε είναι ο *Apache Tomcat* 5[29] .

Για την εγκατάσταση του συστήματος και την παραμετροποίηση του ακολουθήθηκαν οι οδηγίες που δίνονται στο αντίστοιχο έγγραφο του STORK [57] και τα βήματα για την εγκατάσταση του συστήματος περιγράφονται στον **π**ίνακα 8 :

**Πίνακας 8: Βήματα εγκατάστασης συστήματος PEPS**

| |
|---|
| 1. **Έγινε η εισαγωγή της μεταβλητής του συστήματος** |
| [1] $TOMCAT_HOME →/home/user/apps/apache-tomcat-5.5.28 |
| 2. **Στα αρχεία *keystore* χρησιμοποιήθηκαν τα παραδείγματα τα οποία διατίθενται μαζί με το πακέτο εγκατάστασης. Ελέγχθηκε ότι παρακάτω ιδιότητες των *keystores* ανταποκρίνονται στις διαδρομές που ορίζονται.** |
| [1] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-PEPS\src\main\config\embedded\SignModule_CPEPS.xml ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο του CPEPS “storkKeystore.jks”; |
| [2] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-PEPS\src\main\config\embedded\SignModule_SPEPS_CPEPS.xml |
| [3] ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο του SPEPS |

[28] http://maven.apache.org/
[29] http://tomcat.apache.org/

| |
|---|
| “storkKeystore.jks”; |
| [4] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-PEPS\src\main\config\embedded\SignModule_SP_SPEPS. ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο του SPEPS “storkKeystore.jks”; |
| [5] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-SP\src\main\resources\SignModule_SP.xml ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο του SP “storkKeystore.jks”; |
| [6] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-IdP\src\main\resources\SignModule_IdP.xml ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο του IdP “storkKeystore.jks”; |
| [7] Οι ιδιότητες του “keystorePath” στο αρχείο STORK-Specific\src\main\config\embedded\SignModule_Specific.xml ανταποκρίνεται στην διαδρομή που βρίσκεται το αρχείο τουSpecific “storkKeystore.jks”. |
| 3. **Έγινε η μεταφόρτωση της βιβλιοθήκης SAML από την διεύθυνση http://mvnrepository.com/artifact/org.opensaml/opensaml/2.5.1-1** |
| 4. **Αποσυμπιέστηκε το συμπιεσμένο αρχείο OpenSAML και αντιγράφηκαν οι ακόλουθες βιβλιοθήκες στον φάκελο common/ endorsed του διακομιστή. Δηλαδή, στην διεύθυνση** |
| $TOMCAT_HOME/common/endorsed |
| Αντιγράφηκαν τα αρχεία jar της βιβλιοθήκης OpenSAML |
| [1] endorsed\xml-apis-2.9.1.jar |
| [2] endorsed\resolver-2.9.1.jar |
| [3] endorsed\serializer-2.9.1.jar |

| |
|---|
| [4] endorsed\xalan-2.7.1.jar |
| [5] endorsed\xercesImpl-2.9.1.jar |
| 5. **Στο φάκελο *src* του έργου *project* src , δημιουργήθηκε ένας φάκελος:** |
| main\resources. |
| Για να ενεργοποιηθεί η δυνατότητα καταγραφών για τις διαδικτυακές εφαρμογές, στο φάκελο αυτό δημιουργήθηκε ένα XML αρχείο με την ονομασία *log4j.xml* με το ακόλουθο περιεχόμενο: |

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE log4j:configuration SYSTEM "log4j.dtd">
<log4j:configuration xmlns:log4j="http://jakarta.apache.org/log4j/">
 <appender name="MainLogger" class="org.apache.log4j.ConsoleAppender">
  <layout class="org.apache.log4j.PatternLayout">
   <param name="ConversionPattern" value="%d (ABSOLUTE) %5p %c (_1 ) [%M]:%L - %m%n" />
  </layout>
 </appender>
 <logger name="org.opensaml">
  <level value="ERROR" />
 </logger>
 <logger name="eu.stork">
  <level value="trace" />
 </logger>
 <root>
  <priority value="info" />
  <appender-ref ref="MainLogger" />
 </root>
</log4j:configuration>
```

6. **Για να ενεργοποιηθεί η δυνατότητα καταγραφών των επικοινωνιών μεταξύ των S-PEPS και C-PEPS προστέθηκαν στο προηγούμενο αρχείο οι γραμμές:**

```
<appender name="StorkLogger" class="org.apache.log4j.RollingFileAppender">
   <param name="Threshold" value="INFO" />
   <param name="File" value=" /opt/storklogs/server.log" />
   <param name="Append" value="true" />
   <param name="MaxFileSize" value="500KB" />
   <param name="MaxBackupIndex" value="1" />
   <!-- Rollover at midnight each day -->
   <param name="DatePattern" value="'.'yyyy-MM-dd" />
   <layout class="org.apache.log4j.PatternLayout">
     <!-- The default pattern: Date Priority [Category] Message\n -->
     <param name="ConversionPattern" value="%d %-5p [%c] %m%n" />
   </layout>
 </appender>
```

And:

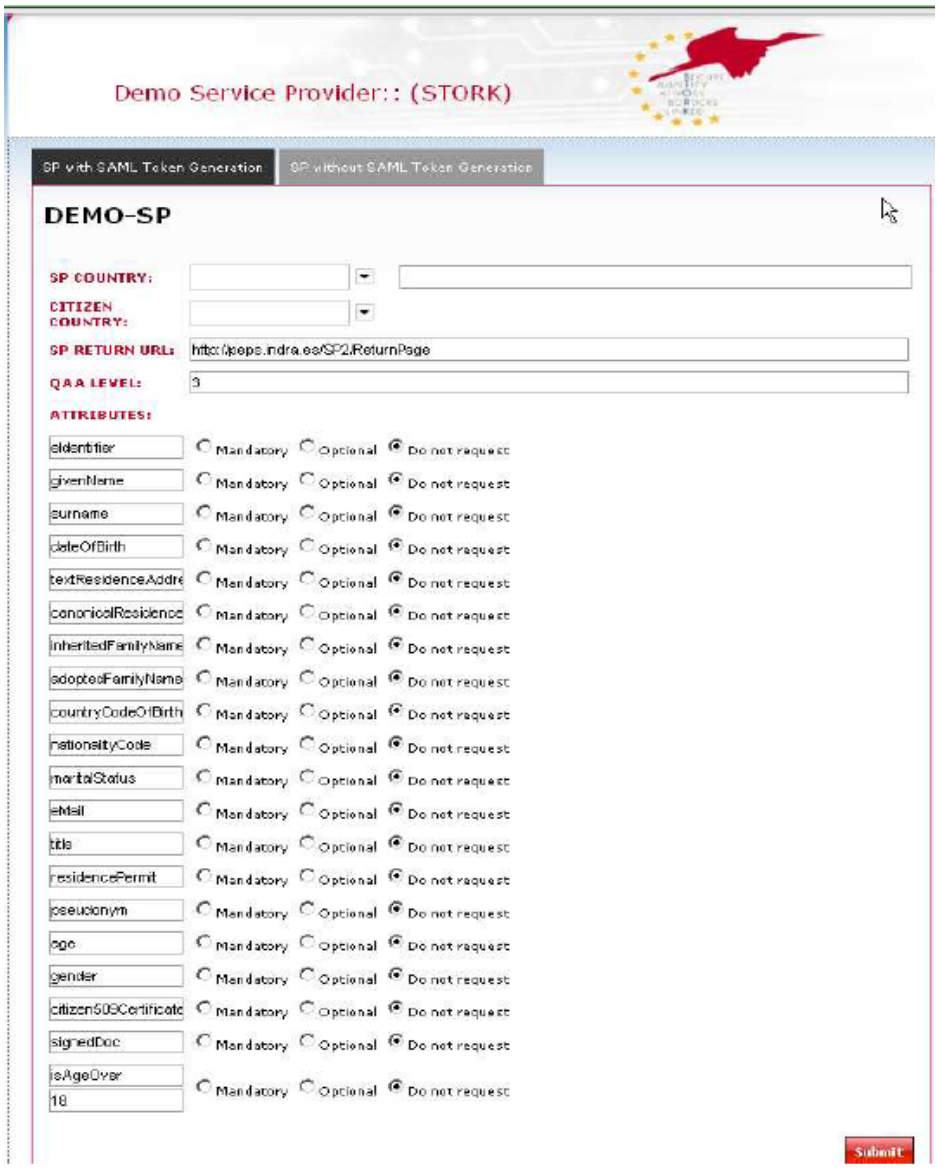
```
<logger name="eu.stork.communication.requests">
   <level value="info" />
   <appender-ref ref="StorkLogger" />
 </logger>
 <logger name="eu.stork.communication.responses">
   <level value="info" />
   <appender-ref ref="StorkLogger" />
 </logger>
```

7. **Ενεργοποιήθηκαν τα *cookies* του διακομιστή τροποποιώντας το αρχείο**

| |
|---|
| **$TOMCAT_HOME\conf\context.xml και αλλάζοντας την ετικέτα "*Context*" σε:** |
| <Context cookies="true"> If you want cookies enabled |
| 8. **Στο αρχείο *hosts* του συστήματος του διακομιστή προστέθηκαν οι ακόλουθες γραμμές**: |
| • *127.0.0.1 sp* |
| • *127.0.0.1 peps* |
| • *127.0.0.1 ap1* |
| • *127.0.0.1 idp* |
| 9. **Τροποποιήθηκε το αρχείο παραμέτρων του Tomcat και αλλάχτηκε η θύρα ακρόασης (listening port) σε 8888.** |
| 10. **Έγινε μεταγλώττιση (compiling) εγκατάσταση και ανάπτυξη των έργων (projects) με την βοήθεια της κονσόλας (command promt),με την παρακάτω σειρά:** |
| [1] Μέσα από τον φάκελο STORK-Commons folder δόθηκε η εντολή: |
| • **mvn clean install –P embedded** |
| [2] Μέσα από τον φάκελο STORK-SAMLEngine folder δόθηκε η εντολή: |
| • **mvn clean install** |
| [3] Μέσα από τον φάκελο STORK-Specific folder δόθηκε η εντολή: |
| • **mvn clean install –P embedded** |
| [4] Μέσα από τον φάκελο STORK-PEPS folder δόθηκε η εντολή: |
| • **mvn clean package –P embedded** |
| • **copy target\PEPS.war** |

| |
|---|
| **$TOMCAT_HOME\webapps\PEPS.war** |
| [5] Μέσα από τον φάκελο STORK-SP folder δόθηκε η εντολή: |
| • **mvn clean package –P embedded** |
| • **copy target\SP.war $TOMCAT_HOME\webapps\SP.war** |
| [6] Μέσα από τον φάκελο STORK-IdP folder δόθηκε η εντολή: |
| • **mvn clean package –P embedded** |
| • **copy target\IdP.war $TOMCAT_HOME\webapps\IdP.war** |
| [7] Μέσα από τον φάκελο STORK-AP folder δόθηκε η εντολή: |
| • **mvn clean package –P embedded** |
| • **copy target\AP.war $TOMCAT_HOME\webapps\AP.war** |
| 11. **Τέλος, έγινε η εκκίνηση του διακομιστή Tomcat** |

Μετά την επιτυχή εγκατάσταση του συστήματος την πληκτρολόγηση της διεύθυνσης (http://127.0.0.1:8888 /SP) σε έναν οποιονδήποτε διαδικτυακό φυλλομετρητή εμφανίζεται η δοκιμαστική του παρόχου υπηρεσιών σελίδα που απεικονίζεται στο σχήμα 32. Η ιστοσελίδα αυτή παρέχεται για τον δοκιμαστικό έλεγχο της λειτουργίας του συστήματος. Μέσα από την ιστοσελίδα ο χρήστης μπορεί να επιλέξει την χώρα στην οποία θέλει να αυθεντικοποιηθεί, την χώρα στην οποία ανήκει ο SP το επιθυμητό επίπεδο QAA καθώς και να επιλέξει ποια από τα χαρακτηριστικά θα ζητηθούν ως υποχρεωτικά, ποια προαιρετικά και ποια από αυτά να μην ζητηθούν.




**Σχήμα 32 : Δοκιμαστική σελίδα παρόχου υπηρεσιών**

## 7.3 Ασφάλεια και Προστασία της Ιδιωτικότητας στο έργο STORK

### 7.3.1 Αξιολόγηση PEPS (Pan European Proxy Service)

Για την αξιολόγηση της διασυνοριακής πλατφόρμας αυθεντικοποίησης που υλοποιήθηκε στο έργο STORK κλήθηκε η ομάδα εργασίας του άρθρου 29[30] [49] για την προστασία των δεδομένων (Article 29 Data Protection Working Party) να συγγράψει σχετική αναφορά και να προτείνει σε περίπτωση που χρειάζεται επιπλέον μέτρα για την προστασία των δεδομένων. Η ομάδα αυτή έχει συσταθεί μέσα από την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου [13] και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των εν λόγω δεδομένων. Ο ρόλος της ομάδας αυτής είναι συμβουλευτικός και ενεργεί ανεξάρτητα. Ακόμη, ο οργανισμός ENISA συνέταξε αναφορά σχετική με το παρεχόμενο επίπεδο ασφάλειας της πλατφόρμας. Η ασφάλεια βασίζεται όπως προαναφέρθηκε στον «κύκλο εμπιστοσύνης» μεταξύ των PEPS και στην αντιστοίχιση των παρόχων και των προσφερόμενων υπηρεσιών στα οριζόμενα επίπεδα QAA.

Η οδηγία για την προστασία των δεδομένων (1995/46/ΕΚ) [13] σχετίζεται άμεσα με το έργο STORK καθώς τα περισσότερα από τα δεδομένα που ανταλλάσσονται μεταξύ των πολιτών και της δημόσιας διοίκησης θεωρούνται δεδομένα προσωπικού χαρακτήρα. Αυτό σημαίνει ότι τα προσωπικά δεδομένα (συμπεριλαμβανομένων των χαρακτηριστικών που ζητούνται) μπορούν να επεξεργαστούν μόνο εάν πληρούνται οι απαιτήσεις του άρθρου 7 της οδηγίας.

***Χρήση και Ανταλλαγή εθνικών αναγνωριστικών αριθμών***

Η χρήση των εθνικών αριθμών αναγνώρισης από ορισμένα κράτη μέλη (όπως η Εσθονία, τη Γερμανία και τις Κάτω Χώρες) παρουσιάζει μια πρόκληση. Στο άρθρο 8 προβλέπεται ότι τα κράτη μέλη καθορίζουν τους όρους για τη χρήση των εθνικών αριθμών αναγνώρισης και άλλων αναγνωριστικών. Στις περισσότερες χώρες, η χρήση των αριθμών αυτών είναι περιορισμένη και ρυθμίζεται από το νόμο. Πρακτικά αυτό

[30] http://ec.europa.eu/justice/data-protection/article-29/

σημαίνει ότι δεν επιτρέπεται οι αναγνωριστικοί αριθμοί να υπόκεινται σε επεξεργασία στις διασυνοριακές αλληλεπιδράσεις της ΗΔ, στις οποίες περιλαμβάνεται και η αποθήκευση αυτών. Ειδικότερα, σε ορισμένα κράτη μέλη όπως η Γερμανία, δεν επιτρέπεται η χρήση αυτών των μόνιμων (μοναδικών) αριθμών αναγνώρισης (identifiers) [49] .

Καθώς οι (εθνικοί) αναγνωριστικοί αριθμοί ταυτότητας δεν μπορούν να χρησιμοποιηθούν σε διασυνοριακές συναλλαγές μεταξύ των κρατών μελών, υπάρχουν δύο σημαντικές νομικές συνέπειες :

- Στην νομιμότητα (legal status) των ψηφιακών πιστοποιητικών που χρησιμοποιούνται για την αυθεντικοποίηση καθώς αν δεν επιτρέπεται να πιστοποιηθούν τα χαρακτηριστικά είναι πολύ δύσκολο να προσδιοριστεί ποιος αιτείται την υπηρεσία.
- Στην χρήση των αναγνωριστικών αριθμών στα κράτη μέλη καθώς δεν υπάρχει κοινό νομικό πλαίσιο για ολόκληρη την Ευρωπαϊκή Ένωση.

Για τα πιστοποιητικά που χρησιμοποιούνται στο πλαίσιο των πιλοτικών εφαρμογών του STORK (που μπορεί να περιλαμβάνονται εθνικοί αριθμοί ταυτότητας), η λύση που προτάθηκε από το STORK είναι η χρήση των αδιαφανών (opaque) (πχ. αδόμητων με καμία εννοιολογική έννοια) και παροδικών αναγνωριστικών με τα ακόλουθα χαρακτηριστικά [50]:

- Αδιαφανή και παροδικά αναγνωριστικά (π.χ. μονόδρομη κρυπτογράφηση)
- Αναγνωριστικά βασισμένα στις συνεδρίες ( Session –based)
- Αναγνωριστικά βασισμένα στις υπηρεσίες:

Κάθε πάροχος υπηρεσιών (SP) έχει το δικό του μοναδικό αναγνωριστικό. Στη συνέχεια, ο χρήστης κρατάει ένα ειδικό αναγνωριστικό για κάθε υπηρεσία χωρίς να χρειάζεται να μοιράζεται τα αναγνωριστικά αυτά μεταξύ των υπηρεσιών. Αυτό επιτυγχάνεται με την παραγωγή αναγνωριστικών από τους εθνικούς αριθμούς αναγνώρισης, χωρίς όμως να γίνεται οποιαδήποτε αποθήκευση αυτών των "αντιστοιχίσεων".

Έτσι υπάρχει διαφορετικό αναγνωριστικό για κάθε υπηρεσία ενώ ο αρχικός αριθμός δεν μπορεί να ανακτηθεί παρά μόνο από τον αρμόδιο κυβερνητικό φορέα.

***Υλοποίηση προτύπου διαχείρισης ταυτότητας user centric και user consent***

Το STORK είναι εξ ολοκλήρου προσανατολισμένο προς τον χρήστη (user centric) και αποσκοπεί στην παροχή όλων εκείνων των εργαλείων που απαιτούνται για την εκπλήρωση των αναγκών κάθε κράτους μέλους. Η προτεινόμενη user centric λύση βασίζεται στην συγκατάθεση του χρήστη, καθώς αυτή είναι η πιο γενική περίπτωση νόμιμης διασυνοριακής επεξεργασίας δεδομένων και εξασφαλίζει ότι τα άτομα έχουν τον πλήρη έλεγχο για τον τρόπο που λαμβάνονται και χρησιμοποιούνται τα προσωπικά τους δεδομένα. Η προτεινόμενη λύση προσφέρει τις ακόλουθες δυνατότητες:

- Η δήλωση απορρήτου είναι διαθέσιμη στο επίπεδο διεπαφής του χρήστη.
- Σε κάθε περίπτωση για να συνεχιστεί και να ολοκληρωθεί μία διαδικασία θα πρέπει ο χρήστης να δώσει την συγκατάθεση του και σε ορισμένες περιπτώσεις θα πρέπει ακόμη και να υπογράψει ψηφιακά την συγκατάθεση του.
- Η επιβεβαίωση της συγκατάθεσης γίνεται στα PEPS και παρέχεται πριν την έξοδο των χαρακτηριστικών από τη χώρα.

***Διαχειριστής και επεξεργαστής δεδομένων* (Data controller / Data processor)**

Ένα από τα θέματα που απασχόλησαν την ομάδα του άρθρου Article 29 [49] είναι ο διαχωρισμός των ρόλων του επεξεργαστή δεδομένων (data processor) και του διαχειριστή δεδομένων (data controller) κατά την επεξεργασία και μεταφορά των δεδομένων μέσα από την πλατφόρμα του Stork. Ο διαχωρισμός αυτός είναι σημαντικός ώστε να μπορέσουν να αποδοθούν οι ανάλογες ευθύνες στους φορείς οι οποίοι εμπλέκονται στις διαδικασίες συλλογής, επεξεργασίας, αποθήκευσης και μεταφοράς των δεδομένων αλλά και να οριστούν οι αρμόδιες εποπτικές αρχές.

Στο μοντέλο PEPS μπορεί να θεωρηθεί ότι ο PEPS είναι ο διαχειριστής των δεδομένων. Επεξεργάζεται προσωπικά δεδομένα και τα προωθεί προς άλλους PEPS ενώ διαχειρίζεται και τις αποκρίσεις αυτών.

Παρά το γεγονός ότι ο PEPS είναι μια υπηρεσία η οποία παρέχεται σε διαφορετικούς φορείς παροχής υπηρεσιών, αυτοί δεν έχουν τον έλεγχο για το ότι συμβαίνει στο PEPS. Ένας πάροχος υπηρεσιών μπορεί μόνο είτε να αποδεχθεί είτε να απορρίψει την προσφορά του παρόχου PEPS.

Από την άλλη πλευρά, μπορεί να υποστηριχτεί ότι ο φορέας παροχής υπηρεσιών (SP), ως υπεύθυνος των υπηρεσιών που παρέχονται στον πολίτη επιλέγει να χρησιμοποιήσει τις υπηρεσίες ενός PEPS και ως εκ τούτου ο PEPS είναι ο μόνος επεξεργαστής δεδομένων και ο οποίος ενεργεί για λογαριασμό του παρόχου υπηρεσιών (SP). Η ερμηνεία αυτή έχει ένα πρακτικό μειονέκτημα από την άποψη του στόχου της μείωσης του διοικητικού φόρτου.

Εάν ένας PEPS θεωρηθεί ως επεξεργαστής αυτό δημιουργεί ένα σημαντικό αριθμό διαχειριστών (controllers) αυτού του PEPS (όλων αυτών που χρησιμοποιούν αυτό PEPS). Κατά συνέπεια, όλα αυτοί οι διαχειριστές θα πρέπει να ενημερώνουν τα PEPS για κάθε περίπτωση όπου υπάρχει επεξεργασία δεδομένων.

Η ομάδα του Άρθρου 29, δεν αποφάνθηκε για τον ορισμό αυτών των ρόλων στους PEPS και στους παρόχους υπηρεσιών καθώς δεν υπήρξε συμφωνία μεταξύ των μελών της ομάδας, οπότε και παραμένει ανοικτό το θέμα. Συνεπώς, οι διαχειριστές των δεδομένων οι οποίοι χρησιμοποιούν τους PEPS καθώς και οι φορείς οι οποίοι παρέχουν τις υπηρεσίες των PEPS θα πρέπει να αποφασίζουν από μόνοι τους αν έχουν τον ρόλο του επεξεργαστή ή του διαχειριστή δεδομένων ακολουθώντας την Οδηγία 95/46 και να επικοινωνούν με την Αρχή Προστασίας Προσωπικών Δεδομένων ώστε να γίνει η επιβεβαίωση του ισχυρισμού τους.

***Ασφάλεια δεδομένων***

Σύμφωνα με τις δηλώσεις των εμπλεκόμενων μερών στο έργο STORK έχουν καθοριστεί οι ελάχιστες κοινές απαιτήσεις ασφάλειας και έχει υλοποιηθεί ασφάλεια *end-to-end*. Το τεχνικό πρότυπο των εργαλείων διαλειτουργικότητας είναι σε πολλές περιπτώσεις υψηλότερο από τα πρότυπα που χρησιμοποιούνται σε τοπικό επίπεδο για την

πρόσβαση σε υπηρεσίες ΗΔ. Επιπλέον, χρησιμοποιούνται υψηλών προδιαγραφών και ασφάλειας τεχνικές κρυπτογράφησης (Segmented technical encryption) όπως SSL, SAML [50].

Ωστόσο, όλη η επικοινωνία δρομολογείται μέσω του προγράμματος περιήγησης των χρηστών και ως εκ τούτου ο κίνδυνος μιας επίθεσης *man in the middle* πρέπει να λαμβάνεται υπόψη στο μοντέλο PEPS, λόγω της μετα-ανακατεύθυνσης μέσω του προγράμματος περιήγησης των χρηστών. Ακόμη πρέπει επίσης να λαμβάνεται μέριμνα για την αντιμετώπιση των κινδύνων που συναντώνται συγκεντρωτικές αρχιτεκτονικές (*centralised architecture*) όπως αυτή του μοντέλου PEPS, όπου υπάρχουν πολύ περισσότερες συναλλαγές επεξεργασίας από ότι θα έπρεπε για κάθε αίτηση. STORK θα πρέπει να εφαρμόσει μια συνεχή παρακολούθηση του συστήματος για να βεβαιωθείτε ότι είναι σε θέση να ανακαλύψουν και να αντιμετωπίσει τους κινδύνους που προκύπτουν κατά τη διάρκεια των συναλλαγών.

Θα πρέπει να τονιστεί ότι η διαφάνεια των χαρακτηριστικών ασφαλείας του κάθε συστήματος ΗΤ βασίζεται στην αυτο-αξιολόγηση του κάθε κράτους μέλους η οποία βασίζεται στο πρότυπο που έχει οριστεί από το STORK.

Δεν υπάρχει καμία πιστοποίηση από τρίτους (third-party certification) που παρέχει πρόσθετες εγγυήσεις για τα μέτρα ασφαλείας του κάθε συστήματος ώστε να βοηθηθούν τα υπόλοιπα κράτη μέλη οι πάροχοι υπηρεσιών να καθορίσουν την πολιτική τους έναντι αυτών των συστημάτων.

Σύμφωνα με την ομάδα του άρθρου 29, σε μία διασυνοριακή πλατφόρμα μεταφοράς δεδομένων δεν αρκεί η αυτό-αξιολόγηση του παρεχόμενου επιπέδου ασφαλείας . Θα ήταν ωφέλιμο να οριστούν τα ελάχιστα εκείνα κοινά πρότυπα ασφάλειας για την επεξεργασία των δεδομένων, πέρα από αυτά που ορίζονται και υλοποιούνται από την βασική υποδομή του STORK και τα οποία θα πρέπει να ακολουθούνται από τους συμμετέχοντες το STORK .

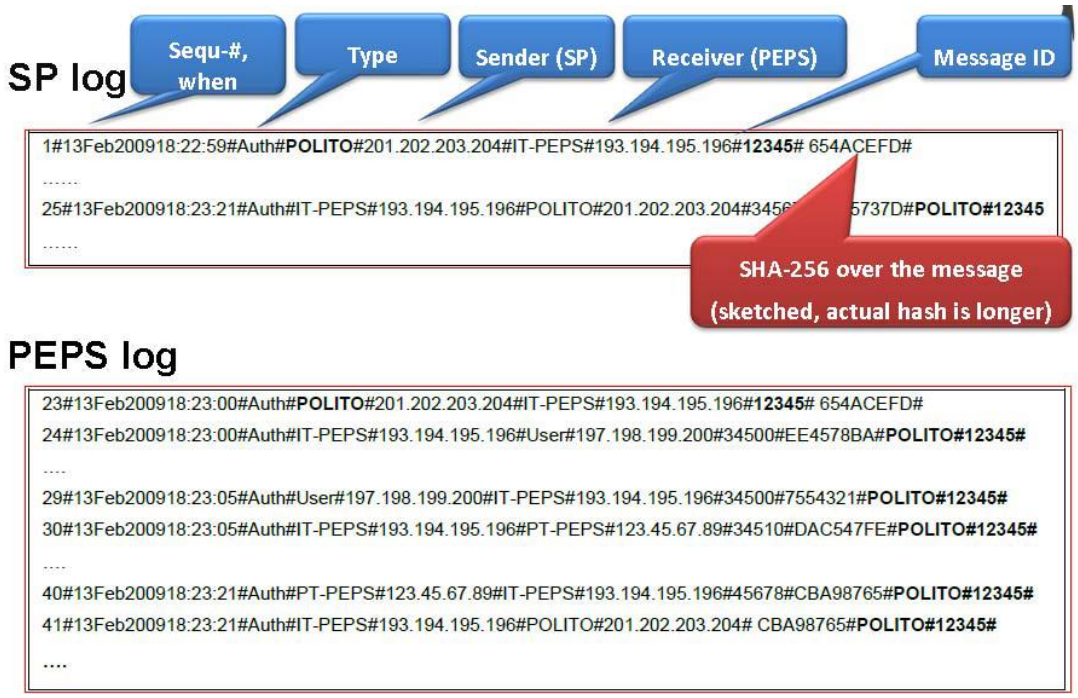
Ακόμη, υπάρχει η ανάγκη για την δημιουργία ενός οδηγού ο οποίος θα καθοδηγεί του παρόχους υπηρεσιών να επιλέξουν ένα από τα τέσσερα επίπεδα Διασφάλισης της

Ποιότητας Αυθεντικοποίησης (QAA), τα οποία προσφέρονται μέσα από το STORK ανάλογα με την υπηρεσία την οποία προσφέρουν. Για παράδειγμα ένας πάροχος ο οποίος προσφέρει Ιατρικές υπηρεσίες και ζητά ή μεταφέρει ιατρικά δεδομένα, θα πρέπει να επιλέγει το επίπεδο QAA 4.

***Αρχεία καταγραφής***

Για να είναι εφικτή η ιχνηλασιμότητα των ηλεκτρονικών αυθεντικοποίησεων διατηρείται ένα ελεγκτικό άθροισμα που παράγεται από μία συνάρτηση κατακερματισμού (hush function) και εφαρμόζεται στα αποθηκευμένα στοιχεία του χρήστη μαζί με κάποια δεδομένα τα οποία αποτελούν την ταυτότητα της συναλλαγής

Μέσω αυτού του ελεγκτικού αθροίσματος είναι δυνατή η ανακατασκευή της συναλλαγής αλλά μόνο με την συμμετοχή του χρήστη και του παρόχου υπηρεσιών. Αυτή είναι μια πολύ ασφαλής τεχνική η οποία καθιστά σχεδόν αδύνατη την άντληση προσωπικών δεδομένων τα οποία κρυπτογραφούνται με τον τρόπο αυτόν. Προτείνεται παρ’ όλα αυτά από την ομάδα του Άρθρου 29 ο ορισμός από το STORK περιόδων διαγραφής των αρχείων καταγραφής [49].




**Σχήμα: 33 Στιγμιότυπα από αρχεία καταγραφής [49]**

***Τήρηση της Αρχής της αναλογικότητας (Selective disclosure)***

Ο πάροχος υπηρεσιών τα δεδομένα ορίζει τα δεδομένα τα οποία ζητά ως υποχρεωτικά και προαιρετικά. Ο χρήστης αποφασίζει ποια από αυτά θα στείλει και ποια όχι. Το STORK και ο πάροχος υπηρεσίων δεν συνδιαλέγονται σχετικά με το ποια χαρακτηριστικά θα ζητηθούν ως υποχρεωτικά, για να είναι πιο πιθανό ότι ο πάροχος υπηρεσιών θα ζητήσει μόνο τα δεδομένα τα οποία είναι απαραίτητα για την προσφερόμενη υπηρεσία είναι απαραίτητη η παροχή οδηγιών και συγκεκριμένων συστάσεων για την επίτευξη των αρχών της αναλογικότητας και της ελαχιστοποίησης των ζητούμενων δεδομένων από αυτούς.

***Αποκάλυψη δεδομένων και αποθήκευση***

Κατά την πλήρη ανάπτυξη της αρχιτεκτονικής STORK δεν υπάρχουν δεδομένα τα οποία μεταδίδονται σε άλλα μέρη εκτός από το πάροχο υπηρεσιών.

Οι PEPS δεν αποθηκεύουν χαρακτηριστικά και κατά συνέπεια δεν αποθηκεύονται δεδομένα προσωπικού χαρακτήρα. Μόλις ολοκληρωθεί μια συναλλαγή από τους PEPS,

τα δεδομένα διαγράφονται από τη μνήμη. Όπως προαναφέρθηκε τα μόνα αρχεία που αποθηκεύονται αφορούν τα κρυπτογραφημένα δεδομένα της συναλλαγής που καταγράφονται στα αρχεία καταγραφής και μπορούν να ανασυντεθούν μόνο με την συμμετοχή του χρήστη.

# Κεφάλαιο 8: Ανασκόπηση – Συμπεράσματα

Η μείωση της γραφειοκρατίας και εύκολη πρόσβαση των πολιτών και των επιχειρήσεων σε υπηρεσίες της δημόσιας διοίκησης θα συνεισφέρουν στην ανάπτυξη και θα οδηγήσουν στην δημιουργία νέων θέσεων εργασίας. Η χρήση των εργαλείων που προσφέρονται από τις ΤΠΕ από την διοίκηση κάθε κράτους μέλους προσφέρει δυνατότητες για την βελτίωση των παρεχόμενων υπηρεσιών. Περαιτέρω, η παροχή τέτοιων υπηρεσιών σε διασυνοριακό επίπεδο θα διευκολύνει την επίτευξη του στόχου της «ενιαίας αγοράς» όπου οι πολίτες όλων των χωρών της ΕΕ θα μπορούν να μετακινούνται και να συναλλάσσονται εύκολα και αποδοτικά με τις δημόσιες υπηρεσίες εκτός των συνόρων των χωρών τους.

Η διαλειτουργικότητα μεταξύ των δημόσιων διοικήσεων των κρατών μελών αποτελεί προϋπόθεση για την παροχή των διασυνοριακών υπηρεσιών. Η προσβασιμότητα, η πολυγλωσσία, η ασφάλεια, η επικουρικότητα, η χρήση ανοικτών προτύπων και η προστασία των προσωπικών δεδομένων αποτελούν τις αρχές πάνω στις οποίες βασίστηκε η σύνταξη του Ευρωπαϊκού Πλαισίου Διαλειτουργικότητας. Η διαλειτουργικότητα των δημοσίων διοικήσεων δεν αφορά μόνο την τεχνική διαλειτουργικότητα αλλά και την την νομική διαλειτουργικότητα, την οργανωσιακή διαλειτουργικότητα καθώς και την σημασιολογική διαλειτουργικότητα.

Μια σειρά από μεγάλης κλίμακας πιλοτικά προγράμματα υποστηρίχτηκαν από το πρόγραμμα της ανταγωνιστικότητας και της καινοτομίας και τις πολιτικές υποστήριξης των ΤΠΕ. Στόχος των πολιτικών αυτών ήταν η τόνωση της καινοτομίας και της ανταγωνιστικότητας μέσω της ευρύτερης αφομοίωσης και βέλτιστης χρήσης των ΤΠΕ από τους πολίτες, τις κυβερνήσεις και τις επιχειρήσεις και ειδικότερα τις Μικρομεσαίες Επιχειρήσεις (SMEs).

Τα πιλοτικά αυτά προγράμματα επικεντρώθηκαν στην παροχή βασικών υπηρεσιών προς τους πολίτες και τις επιχειρήσεις με ηλεκτρονικό τρόπο, σε διασυνοριακό επίπεδο κάνοντας χρήση και συνδέοντας διαλειτουργικά υφιστάμενες υποδομές των κρατών

μελών. Το epSOS, το eCODEX, το PEPPOL και το STORK είναι από τα βασικότερα πιλοτικά προγράμματα έχοντας ως στόχο την παροχή διασυνοριακών υπηρεσιών δικαστικών αρχών, υπηρεσιών υγείας, δημόσιων συμβάσεων και ΗΤ αντίστοιχα.

Για την βελτίωση της ασφάλεια σε μία ενιαία Ευρώπη χωρίς εσωτερικά σύνορα αλλά και για την διευκόλυνση των μετακινήσεων των πολιτών και της διακίνησης αγαθών τέθηκαν σε λειτουργία ειδικά πληροφοριακά συστήματα. Τα πληροφοριακά συστήματα Schengen (SIS), θεωρήσεων (VIS) και τελωνείων (CIS) είναι τα σημαντικότερα από αυτά. Η άμεση και διαρκής ενημέρωση των βάσεων δεδομένων των συστημάτων αυτών είναι ένα από τα κυριότερα πλεονεκτήματα τους παρέχοντας έγκαιρη πληροφόρηση στις ελεγκτικές αρχές.

Η παροχή της δυνατότητας στους πολίτες για ηλεκτρονική αυθεντικοποίηση πέραν των συνόρων είναι ένα από τα βασικά εργαλεία για την απολαβή των διασυνοριακών υπηρεσιών που προσφέρονται στην Ευρωπαϊκή Ψηφιακή Ενιαία Αγορά . Για τον σκοπό αυτό είναι αναγκαία η ύπαρξη μίας κοινής πλατφόρμας διαλειτουργικότητας η οποία θα «κρύβει» τις ιδιαιτερότητες των συστημάτων του κάθε κράτους και επιτρέπει στα συστήματα αυτά να επικοινωνούν και να ανταλλάσουν πληροφορίες. Το μεγάλης κλίμακας πιλοτικό πρόγραμμα STORK υλοποίησε και εγκατέστησε μια πλατφόρμα διαλειτουργικότητας για την παροχή διασυνοριακών υπηρεσιών προς τους πολίτες και τις επιχειρήσεις. Ένα σημαντικό ζήτημα το οποίο ανέλυσε και υλοποίησε μέσα από την πλατφόρμα αυτή είναι η διασυνοριακή ΗΤ των πολιτών με τρόπο ασφαλή και φιλικό προς την ιδιωτικότητα . Η χρήση της κλίμακας QAA για την διασφάλιση της αξιοπιστίας της αυθεντικοποίησης, η επικεντρωμένη στο χρήστη (user centric) πολιτική που ακολουθήθηκε με τον χρηστή να έχει τον πλήρη έλεγχο για την αποστολή και διακίνηση των δεδομένων του παρέχει τις απαιτούμενες εγγυήσεις ασφάλειας και προστασίας της ιδιωτικότητας .

Παρ’ όλα αυτά, είναι αναγκαία η ύπαρξη ενός οδηγού ο οποίος θα παρέχει στους παρόχους υπηρεσιών την απαραίτητη γνώση και μεθοδολογία με τρόπο απλό και κατανοητό, ώστε να μπορούν να κρίνουν και να επιλέγουν το καταλληλότερο επίπεδο ασφάλειας QAA για τις παρεχόμενες υπηρεσίες τους.

Ειδικότερα για τους παρόχους ταυτοποίησης και χαρακτηριστικών είναι επιβεβλημένη η παρουσία ενός κεντρικού φορέα ο οποίος θα εποπτεύει τους παρόχους αυτούς σχετικά με την τήρηση των απαραίτητων κανονισμών και προδιαγραφών για την διασφάλιση της προστασίας της ιδιωτικότητας των πολιτών καθώς και για την ασφάλεια στις μεταξύ τους συναλλαγές.

Η χρήση των ΤΠΕ μπορούν να οδηγήσουν στην βελτίωση του βιοτικού επιπέδου των πολιτών, στην υποστήριξη των μικρομεσαίων επιχειρήσεων και στην οικονομική ανάπτυξη της Ευρώπης. Η μετακίνηση των πολιτών και η απολαβή των δημόσιων υπηρεσιών που παρέχονται από οποιαδήποτε κράτος συμπεριλαμβάνοντας την διαμονή και την εύρεση εργασίας αλλά και την ενισχυμένη παροχή ασφάλειας μέσα από τα αντίστοιχα πληροφοριακά συστήματα μπορεί να συνεισφέρει στην επίτευξη του στόχου για την «Ενιαία Ευρώπη».

Όσον αφορά τα θέματα προστασίας της ιδιωτικότητας είναι σημαντικό να τονιστεί ότι τα δεδομένα υπόκεινται στους κανονισμούς και την νομοθεσία της χώρας στην οποία στέλνονται . Ο χρήστης θα πρέπει να ενημερώνεται κάθε φορά που δίνει την συγκατάθεσή του για τη μεταφορά των χαρακτηριστικών του, ενώ θα πρέπει να του παρέχεται και η δυνατότητα άμεσης πρόσβασης στην σχετική νομοθεσία της χώρας αυτής. Η συγκατάθεση του χρήστη για την μεταφορά των χαρακτηριστικών είναι μια διαδικασία η οποία είναι σύμφωνη με την Ευρωπαϊκή νομοθεσία για την προστασία της ιδιωτικότητας, αλλά η πληροφόρηση του χρήστη για τους ενδεχόμενους κινδύνους που μπορούν να προκύψουν με την συγκατάθεσή του είναι ανεπαρκής. Η ανάπτυξη μιας διαδικασίας, η οποία θα διαχειρίζεται θέματα ιδιωτικότητας και θα ενημερώνει τον χρήστη για την προοριζόμενη χρήση των δεδομένων του και τους ενδεχόμενους κινδύνους που σχετίζονται με θέματα ιδωτικότητας, κάθε φορά που δίνει την συγκατάθεση του για την μεταφορά των χαρακτηριστικών του, θα βελτίωνε την διασυνοριακή ΗΤ σε ότι αφορά στην προστασία της ιδιωτικότητας και θα ενίσχυε την εμπιστοσύνη των χρηστών για την χρήση των διασυνοριακών υπηρεσιών που παρέχονται με την χρήση της ΗΤ.

Η έλλειψη χρηστών για τις προσφερόμενες διασυνοριακές υπηρεσίες, η προσέλκυση νέων χρηστών και η διατήρηση και βελτίωση των υπηρεσιών που υλοποιούνται μέσα από τα Πιλοτικά Έργα Μεγάλης Κλίμακας της ΕΕ, είναι από τα σημαντικότερα προβλήματα που αντιμετωπίζουν τα Έργα αυτά. Η διαφήμιση και διάδοση των παρεχόμενων υπηρεσιών, η ενίσχυση της εμπιστοσύνης των πολιτών και η παροχή κινήτρων για την χρήση των υπηρεσιών κατά την περίοδο ανάπτυξης των έργων αλλά και μετά την ολοκλήρωση τους, είναι μερικές από τις ενέργειες, οι οποίες θα πρέπει να ενισχυθούν και να βελτιωθούν .

Όσον αφορά το έργο STORK, η ύπαρξη και χρήση των δύο διαφορετικών αρχιτεκτονικών PEPS και MW αυξάνει την πολυπλοκότητα της πλατφόρμας και δημιουργεί προβλήματα διαλειτουργικότητας. Προτείνεται στο μέλλον να γίνει αξιολόγηση των δύο διαφορετικών τεχνικών και να υλοποιηθεί η πλατφόρμα διασυνοριακής ΗΤ μέσα σε ένα ομογενές περιβάλλον με κοινή αρχιτεκτονική για όλες τις συμμετέχουσες χώρες. Η ομοιογένεια αυτή θα βελτίωνε την διαλειτουργικότητα, θα ενίσχυε την ασφάλεια της πλατφόρμας και θα καθιστούσε πιο εύκολη την συντήρηση και ενημέρωση της. Ένα ακόμη πρόβλημα που διαπιστώθηκε είναι η δυσκολία της εγκατάστασης του απαραίτητου λογισμικού για την ανάπτυξη της πλατφόρμας σε επίπεδο SP αλλά και σε επίπεδο εθνικού PEPS. Εκτός από την δυσκολία εγκατάστασής τους αλλά και την έλλειψη τεχνικής υποστήριξης, εντοπίστηκαν πολλά σφάλματα κατά την ανάπτυξη των δομικών στοιχείων του λογισμικού τα οποία αφορούσαν κυρίως σε ασυμβατότητες με τις ενημερωμένες εκδόσεις λογισμικού υποστήριξης της γλώσσας Java, των βιβλιοθηκών του SAML και του λογισμικού διαχείρισης ανάπτυξης εφαρμογών Apache Maven. Παρατηρήθηκε επίσης ότι ενώ οι δικτυακοί τόποι όπου ήταν αποθηκευμένες επιμέρους μονάδες λογισμικού (repositories) άλλαξαν, τα αρχεία XML, τα οποία περιλάμβαναν τις διευθύνσεις αυτές, δεν επικαιροποιήθηκαν. Αποτέλεσμα αυτής της μη επικαιροποίησης είναι η αδυναμία αυτόματης εύρεσης και εγκατάστασης απαραίτητων επιμέρους μονάδων λογισμικού που οδηγεί σε επίπονες διαδικασίες αποσφαλμάτωσης του κώδικα, την αναζήτηση,

εύρεση και εγκατάσταση των μονάδων αυτών χειροκίνητα, κάτι το οποίο δημιουργεί νέες ασυμβατότητες με τις υπόλοιπες μονάδες λογισμικού.

Έχει γίνει μεγάλη προσπάθεια από την ΕΕ για την αξιοποίηση των ΤΠΕ από τις Δημόσιες Διοικήσεις και την παροχή δημόσιων υπηρεσιών χρήσιμων προς τους πολίτες και τις επιχειρήσεις οι οποίες να είναι προσβάσιμες από όλους, διασυνοριακά, με τρόπο απλό και άμεσο, μειώνοντας από την μία το κόστος παροχής τους και βελτιώνοντας από την άλλη το βιοτικό επίπεδο στην ΕΕ, καθιστώντας το όραμα της ενιαίας ψηφιακής Ευρώπης πραγματικότητα. Δυστυχώς όμως, φαίνεται ότι η γραφειοκρατία σε επίπεδο ΕΕ καθυστερεί την υλοποίηση έργων που προσφέρουν τις υπηρεσίες αυτές, ενώ είναι σχεδόν αδύνατη η παρακολούθηση των αναγκών των πολιτών και η προσαρμογή των έργων στις ανάγκες αυτών. Θα βοηθούσε πολύ να ορίζονταν οι υπηρεσίες που προτείνονται σε κάθε έργο σύμφωνα με τις πραγματικές ανάγκες των πολιτών, να απλοποιηθούν και να επιταχυνθούν οι διαδικασίες για την υλοποίηση των έργων έτσι ώστε να μπορούν αυτά να ακολουθούν τις εξελίξεις σε τεχνολογικό επίπεδο, αλλά και να ανταποκρίνονται στις διαφορετικές συνθήκες και τις απαιτήσεις που διαμορφώνονται μέσα στον χρόνο. Η προσφορά προς τους πολίτες και τις επιχειρήσεις των υπηρεσιών που αυτοί χρειάζονται και ζητούν, θα συνέβαλλε και στην επίλυση του προβλήματος της έλλειψης χρηστών των υπηρεσιών που παρατηρείται και αποτελεί ένα από τα σημαντικότερα μειονεκτήματα των έργων.

# Βιβλιογραφικές Αναφορές


1. IDABC and EIF, *European Interoperability Framework for Pan-European eGoverment Services*, 2004: Belgium.

2. Βέργη, Ε. and Θ. Παππάς, *Εξέλιξη των 20 βασικών υπηρεσιών Ηλεκτρονικής Διακυβέρνησης στην Ελλάδα*, Παρατηρητήριο για την Κοινωνία της Πληροφορίας, 2007.

3. Wauters, P., *Benchmarking e-government policy within the e-Europe programme.* Aslib Proceedings, 2006. **58**(5): p. 389 - 403.

4. Commision of the European Communities, *eEurope 2005: An information society for all*, 2002: Brussels.

5. Interchange of Data between Administrations (IDA), *Linking up Europe: the Importance of Interoperability for eGovernment Service.* 2003.

6. ISA, *EUROPEAN INTEROPERABILITY FRAMEWORK FOR EUROPEAN PUBLIC SERVICES* 2010, EUROPEAN COMMISSION

7. Commision of the European Communities, *i2010 – A European Information Society for growth and employment*, 2005.

8. European Commission, *The European eGovernment Action Plan 2011-2015 -Harnessing ICT to promote smart, sustainable & innovative Government* in *ICT for Goverment and Public Services*2010: Brussels.

9. European Commission. (2012). e-procurment, from http://ec.europa.eu/internal_market/publicprocurement/e-procurement/

10. European Commission, *Towards interoperability for European public services* T.C. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Editor 2010: Brussels.

11. European Parliament and Council, *DECISION No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA), Official Journal of the European Union, 3/10/2009 L260 p.0020-0027*, 3/10/2009. p. 7.

12. European Commission, *2011/292/EU Council Decision of 31 March 2011 on the security rules for protecting EU classified information, Official Journal L 141 , 27/05/2011 P. 0017 - 0065*, 2011.

13. European Parliament, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of*

*personal data and on the free movement of such data* in *Official Journal L 281* 23/11/1995. p. 20.

14. Tamara Almarabeh, A.A., *A General Framework for E-Government: Definition Maturity Challenges, Opportunities, and Success* European Journal of Scientific Research 2010. **39**: p. 29-42

15. European Commision Joinup. *Semantic Interoperability Community (SEMIC)*. [cited 2013 25 March]; Available from: https://joinup.ec.europa.eu/community/semic/description.

16. PLANET – ΕΠΙΣΕΥ - ATC. (2008). Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ Α.Ε.

17. European Parliament and Council, *DECISION No 1639/2006/EC of European Parliament and Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007 to 2013), Official Journal of the European Union 9/11/2006 L 310 σ. 015-040*, 2006.

18. ICT PSP Work Programme 2007 Competitiveness and Innovation Framework Programme (CIP) ICT Policy Support Programme.

19. European Union, *e-codex*. 2013 [cited 2013; Available from: http://www.e-codex.eu/home.html.

20. European Union, *epSOS*. [cited 2013; Available from: http://www.epsos.eu/.

21. European Union, *STORK*. [cited 2013; Available from: https://www.eid-stork.eu/.

22. European Union, *PEPPOL*. [cited 2013; Available from: http://www.peppol.eu.

23. European Parliament and Council, *DIRECTIVE 2006/123/EC European Parliament and Council of 12 December 2006 on services in the internal market, Official Journal of the European Union 27.12.2006, L 376 p.0036-0068*, 2006.

24. European Union, *SPOCS*. Available from: http://www.eu-spocs.eu/.

25. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 1024/2012 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 25ης Οκτωβρίου 2012 σχετικά με τη διοικητική συνεργασία μέσω του Συστήματος Πληροφόρησης για την Εσωτερική Αγορά και την κατάργηση της απόφασης 2008/49/ΕΚ («κανονισμός ΙΜΙ»), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 14/11/2012 L 316 σ. 001-011*, 2012.

26. European Parliament and Council of the European Union, *DIRECTIVE 2005/36/EC of European Parliament and Council of 7 September 2005 on the recognition of professional qualifications, Official Journal of the European Union 30/9/2005 L 255 p.22 - 142*, 30/9/2005. p. 121.

27. European Union. *Free movement of persons, asylum and immigration*. 2013]; Available from:

http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm.

28. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, *ΚΑΝΟΝΙΣΜΟΣ (ΕΚ) αριθ. 767/2008 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 9ης Ιουλίου 2008 για το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) και την ανταλλαγή δεδομένων μεταξύ κρατών μελών για τις θεωρήσεις μικρής διάρκειας (κανονισμός VIS), Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 13/8/2008, L 218 σ. 0060-0081*, 2008, Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.

29. European Union and Council, *Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Official Journal L 082 , 22/03/1997 P. 0001 - 0016*, 1997: Summaries of EU Legislation.

30. European Union, *Second generation Schengen Information System (SIS II)* 2013 2013; Available from: http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l33020_en.htm.

31. Karanja S K, *The Schengen Information System in Austria: An Essential Tool in Day to Day Police and Border Control Work?* The Journal of Information Law & Technology (JILT), 2002.

32. Planzer Simon, *Data Protection in the Schengen Information System (January 1, 2008)*. SICHERHEIT ALS WIRTSCHAFTLICHES, RECHTLICHES UND KULTURELLES PHÄNOMEN,, 2008.

33. European Union and Council, *COUNCIL REGULATION (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Official Journal of the European Union 25/11/2004 , L 349 p.001-011*.

34. Rahmun F., *National Preparations towards the Operation of the European Visa Information System (VIS)* in *IBPC 2012*. 2012. NIST.

35. European Union and Council, *COUNCIL REGULATION (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, Official Journal L 082 , 22/03/1997 P. 0001 - 0016*, 1997.

36. IBM Corporation, *Implementing e-Customs in Europe: An IBM point of view*, in *Customs, Borders and Revenue Management Solutions*2008: NY USA.

37. European Commision Directorate-General for Taxation and Customs Union, *Electronic Customs Multi-Annual Strategic Plan 2012 Yearly revision (MASP Rev 11.0)*, 2012.

38. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, *ΑΠΟΦΑΣΗ αριθ. 70/2008/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου της 15ης Ιανουαρίου 2008 για ένα περιβάλλον χωρίς χαρτί για τα τελωνεία και τις εμπορικές επιχειρήσεις, Επίσημη Εφημερίδα αριθ. L 023 της 26/01/2008 σ. 0021 - 0026*, 2008.

39. HM Revenue & Customs (HMRC), *RIA : The Multi-Annual Strategic Plan (MASP)* 2005.

40. ISA, *STORK sustainability study* I.S.a.M. Directorate-General, Editor 2011 European Commission

41. ENISA, *Security Issues in Cross-border Electronic Authentication* in *Risk Assessment Report* 2010.

42. Informationstechnik, B.f.S.i.d., *BSI 100-1 Infomation Security Management Systems (ISMS)*, 2008.

43. Informationstechnik, B.f.S.i.d., *BSI100-2 IT-Grundschutz Methodology.*, 2008.

44. Informationstechnik, B.f.S.i.d., *BSI Standard 100-3 Risk Analysis based on IT-Grundschutz* 2008.

45. IDABC, *Common specifications for eID interoperability in the eGovernment context* in *eID Interoperability for PEGS* 2007.

46. Arne Tauber, Thomas Zefferer & Bernd Zwattendorfer, *Approaching the Challenge of eID Interoperability: An Austrian Perspective .* European Journal of ePractice, 2012. **14**.

47. Hans Graux & Jarkko Majava, *Common specifications for eID interoperability in the eGovernment context.* 2007.

48. Herbert Leitold, Reinhard Posch & Hollosi Arno, *Security Architecture of the Austrian Citizen Card Concept*. in *18th Annual Computer Security Applications Conference (ACSAC 2002)*. 2002.

49. Article 29 Data Protection Working Party, *Written Report on STORK project*, 2011.

50. ENISA, *Mapping security services to authentication levels Reflecting on STORK QAA levels.* 2011.

51. STORK e-ID Consortium, *WP2: STORK Deliverable D2.3 Quality authenticator scheme*, 3/3/2009.

52. Project, L.A., *Liberty Identity Assurance Framework*.

53. Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, *ΟΔΗΓΙΑ 1999/93/ΕΚ του Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, 19/1/2000 L 13 σ. 012-020*, 2000.

54. European Telecommunications Standards, *ETSI TS102 042 V1.3.4 Policy requirements for certification authorities issuing public key certificates*, in *Technical Specification* 2007 p. .

55. ENISA, *Privacy and Security Risks when Authenticating on the Internet with European eID Cards* in *Risk Assessment Report* 2009.

56. CCRA Management Committee, *Common Criteria for Information Technology Security Evaluation*. 2012 [cited 2013; Available from: http://www.commoncriteriaportal.org/cc/.

57. STORK e-ID Consortium, *WP 5.8: STORK Deliverable PEPS Installation, Configuration and Integration Manual* 2011.

58. STORK e-ID Consortium, *WP 5.1: STORK Deliverable D5.8.2.a Software Architecture Design*, 8/9/2009.

59. STORK-eID Consortium *STORK Work Item 3.2.1 SAML* 2010.

60. OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, 2008.

61. STORK e-ID Consortium, *WP 5.1: STORK Deliverable D5.8.1.c Software Design.* 8/9/2009.

62. STORK e-ID Consortium, *WP 5.1: STORK Deliverable D5.8.2c Software Design*, 2010.