ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Ανάλυση ευπαθειών σε υποδομές τρίτων παρόχων στον τραπεζικό τομέα: Ελλείψεις και λύσεις

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της/του

Σταματάκης Εμμανουήλ – icsdm323015

Επιβλέπων : Γεώργιος Στεργιόπουλος

Μέλη εξεταστικής επιτροπής: Λίλιαν Μήτρου και Μαρία Καρύδα

Σάμος, [Ιούνιος 2025]

© 2025
του/της
ΣΤΑΜΑΤΑΚΗΣ ΕΜΜΑΝΟΥΗΛ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Πίνακας περιεχομένων

1

Εισαγωγή

1.1 Σκοπός και Στόχοι

Σκοπός της παρούσας εργασίας αποτελεί η διερεύνηση και ανάλυση των ευπαθειών που προκύπτουν από τη χρήση υποδομών τρίτων παρόχων (Third Party Providers - TPPs) στον τραπεζικό τομέα, καθώς και την καταγραφή των ελλείψεων και την πρόταση λύσεων για την ενίσχυση της ασφάλειας και της συμμόρφωσης με τα κανονιστικά και τεχνικά πρότυπα. Η ραγδαία ανάπτυξη των ψηφιακών υπηρεσιών πληρωμών και η ενσωμάτωση των TPPs στο χρηματοοικονομικό οικοσύστημα, μέσω κανονιστικών απαιτήσεων όπως το PSD2 και το Open Banking, έχουν δημιουργήσει νέες προκλήσεις και κινδύνους για την ασφάλεια των τραπεζικών συστημάτων και των προσωπικών δεδομένων των πελατών. Πιο συγκεκριμένα παρακάτω παρουσιάζονται περιληπτικά οι κύριοι στόχοι της παρούσας εργασίας:

- Η αποτύπωση του ρόλου και της σημασίας των τρίτων παρόχων στο σύγχρονο τραπεζικό περιβάλλον.
- Η ανάλυση των κυριότερων ευπαθειών και απειλών που σχετίζονται με τη διασύνδεση τραπεζών και TPPs, τόσο σε τεχνικό όσο και σε κανονιστικό επίπεδο.
- Η συγκριτική αξιολόγηση των υφιστάμενων ρυθμιστικών και τεχνικών πλαισίων (όπως PSD2, EBA Guidelines, PCI DSS, Berlin Group, SWIFT CSCF) ως προς την επάρκεια και την αποτελεσματικότητά τους στην αντιμετώπιση των κινδύνων.
- Η ανάδειξη των ελλείψεων και των προκλήσεων που αντιμετωπίζουν οι τράπεζες και οι TPPs, ειδικά σε θέματα διαλειτουργικότητας, διακυβέρνησης, συμμόρφωσης και τεχνικής υλοποίησης.

- Η παρουσίαση προτάσεων για την ενίσχυση της ασφάλειας, τη βελτίωση της διαχείρισης κινδύνων και την αποτελεσματικότερη συμμόρφωση με τα διεθνή πρότυπα.

1.2 Η σημασία των Τρίτων Παρόχων Υπηρεσιών Πληρωμών στο σύγχρονο χρηματοοικονομικό οικοσύστημα

Οι Τρίτων Παρόχων Υπηρεσιών Πληρωμών (Third Party Providers – TPPs), αξιοποιώντας κανονιστικά πλαίσια όπως η οδηγία PSD2 και τα πρότυπα του Open Banking, έχουν διευρύνει το φάσμα των χρηματοοικονομικών υπηρεσιών, προσφέροντας καινοτόμες λύσεις που ενισχύουν την καινοτομία και την εμπειρία του τελικού χρήστη. Πιο συγκεκριμένα, η ενσωμάτωση των TPPs στο τραπεζικό οικοσύστημα έχει πολλαπλά οφέλη όπως για παράδειγμα την ενισχύει του ανταγωνισμού μεταξύ των τραπεζών οδηγώντας σε καλύτερες υπηρεσίες και χαμηλότερο κόστος για τους καταναλωτές. Παράλληλα, προωθείτε η ανάπτυξη καινοτόμων λύσεων καθώς οι TPPs αναπτύσσουν νέες εφαρμογές και υπηρεσίες που βασίζονται στη διασύνδεση με τραπεζικά δεδομένα μέσω ασφαλών APIs. Επιπλέον, η δυνατότητα ενοποίησης πληροφοριών και η ευκολία στις συναλλαγές βελτιώνουν σημαντικά την εμπειρία του χρήστη, προσφέροντας μεγαλύτερη διαφάνεια και κεντρικοποιημένο έλεγχο στα οικονομικά του δεδομένα. Παρόλα αυτά, η αυξανόμενη εξάρτηση από τρίτους παρόχους δημιουργεί και νέες προκλήσεις, κυρίως σε θέματα ασφάλειας, προστασίας προσωπικών δεδομένων και διακυβέρνησης. Για τον λόγο αυτό δημιουργείται και η ανάγκη για ισχυρούς μηχανισμούς ταυτοποίησης (SCA), ασφαλή κανάλια επικοινωνίας και σαφείς ρυθμιστικές απαιτήσεις προκειμένου να διασφαλιστεί η εμπιστοσύνη των χρηστών και η ομαλή λειτουργία του χρηματοοικονομικού οικοσυστήματος.

1.3 Ορισμοί και εννοιολογικό πλαίσιο

Ακρωνύμια	Περιγραφή
Τρίτοι Πάροχοι Υπηρεσιών Πληρωμών (Third Party Providers – TPPs)	Οι τρίτοι πάροχοι υπηρεσιών πληρωμών, ορίζονται ως οι οντότητες που έχουν εξουσιοδοτηθεί από μία αρμόδια εποπτική αρχή για να έχουν πρόσβαση σε τραπεζικά δεδομένα με την χρήση διεπαφών (APIs) ή να πραγματοποιούν πληρωμές για λογαριασμό πελατών κατόπιν ρητής συγκατάθεσης του πελάτη όπως ορίζεται αντίστοιχα σε κανονισμούς και πρότυπα όπως το PSD2 και το Open Banking.
Πάροχοι Υπηρεσιών Πληροφόρησης Λογαριασμού (Account Information Service Providers – AISPs)	Οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού αποτελούν μία υποκατηγορία των τρίτων παρόχων, οι οποίοι κατόπιν ρητής συγκατάθεσης του πελάτη, μπορούν να έχουν πρόσβαση στις τραπεζικές πληροφορίες του λογαριασμού τους με την χρήση σαφών ορισμένων και ασφαλών APIs. Επιπρόσθετα, οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού, έχουν πρόσβαση μόνο για ανάγνωση στα στοιχεία των λογαριασμών, με σκοπό την συγκέντρωση και συνολική απεικόνιση στοιχείων λογαριασμών από πολλαπλές πηγές σε μια μόνο εφαρμογή, παρέχοντας στους χρήστες μία ενοποιημένη παρουσίαση των οικονομικών τους δεδομένων.

Πάροχοι Υπηρεσιών Εκκίνησης Πληρωμών (Payment Initiation Service Providers – PISPs)	Οι πάροχοι υπηρεσιών εκκίνησης πληρωμών αποτελούν μία υποκατηγορία των τρίτων παρόχων, οι οποίοι είναι εξουσιοδοτημένοι για την εκκίνηση πληρωμών από τον λογαριασμό ενός χρήστη κατόπιν σχετικής συγκατάθεσής του. Για την πραγματοποίηση των πληρωμών οι πάροχοι υπηρεσιών εκκίνησης πληρωμών χρησιμοποιούν ασφαλή APIs για την πρόσβαση στον τραπεζικό λογαριασμό του χρήστη με την χρήση ισχυρής αυθεντικοποίηση σε σχέση με τις παραδοσιακές μεθόδους πραγματοποίησης πληρωμών οι οποίες απαιτούσαν την χρησιμοποίηση από τον χρήστη χρεωστικών ή πιστωτικών καρτών.
Πάροχοι Υπηρεσιών Έκδοσης Καρτών (Card-Based Payment Instrument Issuers – CBPIIs)	Οι πάροχοι υπηρεσιών έκδοσης καρτών αποτελούν υποκατηγορία των τρίτων παρόχων, οι οποίοι είναι υπεύθυνοι για την έκδοση χρεωστικών ή πιστωτικών καρτών, παρέχοντας παράλληλα υπηρεσίες που σχετίζονται με την χρήση τους.
PSD2 (Payment Services Directive 2)	Η οδηγία 2015/2366 (PSD2) του Ευρωπαϊκού Κοινοβουλίου, αποτελεί ένα θεμελιώδες κανονιστικό πλαίσιο που αφορά τις υπηρεσίες πληρωμών στην Ευρωπαϊκή Ένωση. Πιο συγκεκριμένα, το PSD2, θέτει ως κύριους στόχους την ενίσχυση της ασφαλείας, της καινοτομίας και του ανταγωνισμού στον τομέα των πληρωμών διασφαλίζοντας παράλληλα τα στοιχεία των καταναλωτών. Οι βασικές κατευθυντήριες οδηγίες που περιλαμβάνονται στην οδηγία είναι περιληπτικά οι παρακάτω: • Χρήση ισχυρής ταυτοποίησης πελάτη (strong customer authentication – SCA) για την διασφάλιση της ασφαλής πρόσβασης στους τραπεζικούς λογαριασμούς και την εκτέλεση πληρωμών για λογαριασμό ενός πελάτη (κατόπιν σχετικής συγκατάθεσης) • Ρύθμιση της πρόσβασης των τρίτων παρόχων υπηρεσιών πληρωμών σε τραπεζικούς λογαριασμούς μέσω της χρήσης ασφαλών διεπαφών APIs • Την ενίσχυση της διαφάνειας και της πληροφόρησης των καταναλωτών σχετικά με τις χρεώσεις και τους όρους των υπηρεσιών πληρωμών. • Την καθιέρωση κανόνων για την ασφάλεια των συναλλαγών και την προστασία των δεδομένων των χρηστών.
Open Banking	Το Open Banking αποτελεί ένα πλαίσιο το οποίο έχει ως κύριο σκοπό την ασφαλή ανταλλαγή τραπεζικών δεδομένων με εξουσιοδοτημένους τρίτους παρόχους μέσω ασφαλών APIs, καθιστώντας δυνατή την παροχή καινοτόμων χρηματοοικονομικών υπηρεσιών ενισχύοντας παράλληλα τον έλεγχο των πελατών στα δεδομένα που διαμοιράζονται διασφαλίζοντας με αυτό τον τρόπο την προστασία της ιδιωτικότητας.
APIs (Application Programming Interfaces)	Τα APIs αποτελούν ένα σύνολο κανόνων και πρωτοκόλλων που επιτρέπουν σε διαφορετικά λογισμικά συστήματα να επικοινωνούν και να ανταλλάσσουν δεδομένα μεταξύ τους. Στο πλαίσιο των τραπεζικών και χρηματοοικονομικών υπηρεσιών, τα APIs επιτρέπουν την ασφαλή και τυποποιημένη πρόσβαση σε χρηματοοικονομικά δεδομένα και υπηρεσίες διευκολύνοντας με αυτό τον τρόπο την ασφαλή ανταλλαγή πληροφοριών μεταξύ των τραπεζών και των τρίτων παρόχων
Ισχυρή Επαλήθευση Ταυτότητας Πελάτη (Strong Customer Authentication - SCA)	Η ισχυρή επαλήθευση ταυτότητας πελάτη, είναι μία διαδικασία ασφαλείας που επαληθεύει την ταυτότητα ενός χρήστη όπως απαιτείται από κανονισμούς όπως το PSD2 για την ενίσχυση της ασφάλειας των ηλεκτρονικών πληρωμών και την μείωση της πιθανότητας

	απάτης, χρησιμοποιώντας τουλάχιστον δύο από τα παρακάτω ανεξάρτητα στοιχεία επαλήθευσης: • Κάτι που μόνο ο χρήστης γνωρίζει (π.χ. κωδικός πρόσβασης, PIN). • Κάτι που μόνο ο χρήστης κατέχει (π.χ. κινητό τηλέφωνο, token). • Κάτι που είναι ο χρήστης (π.χ. βιομετρικά χαρακτηριστικά).
Ρυθμιστικά Τεχνικά Πρότυπα (Regulatory Technical Standards -RTS)	Τα Ρυθμιστικά Τεχνικά Πρότυπα (RTS) είναι τεχνικές απαιτήσεις και προδιαγραφές που έχουν αναπτυχθεί από τις ευρωπαϊκές εποπτικές αρχές (ESA) όπως η Ευρωπαϊκή Αρχή Τραπεζών (EBA) με σκοπό την διασφάλιση της ομοιόμορφης εφαρμογής των κανονισμών που έχουν αναπτυχθεί στην Ευρωπαϊκή Ένωση σε όλα τα κράτη μέλη της.
Ελαχιστοποίηση χρήσης δεδομένων (Data Minimization)	Η ελαχιστοποίηση χρήσης των δεδομένων είναι μία βασική αρχή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) η οποία ορίζει την συλλογή και επεξεργασία μόνο των δεδομένων που είναι απολύτως απαραίτητη για την επίτευξη ενός συγκεκριμένου σκοπού ή της παροχής μίας υπηρεσίας
Privacy by Design	Η έννοια του Privacy by Design απαιτεί την ενσωμάτωση των αρχών προστασίας δεδομένων σε όλα τα στάδια του σχεδιασμού και της ανάπτυξης νέων προϊόντων και υπηρεσιών με κύριο σκοπό την υλοποίηση προληπτικών μέτρων για την προστασία της ιδιωτικότητας από την αρχική φάση του σχεδιασμού.
Κανονισμοί Υπηρεσιών Πληρωμών (Payment Service Regulations - PSRs)	Οι Κανονισμοί Υπηρεσιών Πληρωμών αποτελούν το νομικό πλαίσιο του Ηνωμένου Βασιλείου που ενσωματώνει και προσαρμόζει την ευρωπαϊκή οδηγία PSD2 στο εθνικό δίκαιο καθορίζοντας απαιτήσεις για την ασφάλεια, τη διαφάνεια, την προστασία των καταναλωτών και την πρόσβαση στα συστήματα πληρωμών. Μετά το Brexit, οι Κανονισμοί Υπηρεσιών Πληρωμών διασφαλίζουν τη συνέχεια της ρύθμισης των υπηρεσιών πληρωμών στο Ηνωμένο Βασίλειο, ενώ παράλληλα επιτρέπουν την προσαρμογή των κανόνων στις ιδιαιτερότητες της βρετανικής αγοράς καλύπτοντας θέματα όπως η αδειοδότηση των παρόχων, η ασφάλεια των συναλλαγών, η διαφάνεια των χρεώσεων και η προστασία των δεδομένων των χρηστών.
Berlin Group	Το Berlin Group είναι ένας πανευρωπαϊκός συνασπισμός που αποτελείται από τράπεζες και άλλους παρόχους υπηρεσιών πληρωμών με κύριο σκοπό την εναρμόνιση των προτύπων και των πρακτικών στον τομέα των πληρωμών, ιδίως στο πλαίσιο εφαρμογής του Open Banking και του PSD2, προκειμένου να διευκολυνθεί η διαλειτουργικότητα και η καινοτομία.
Society for Worldwide Interbank Financial Telecommunication - SWIFT	Το Society for Worldwide Interbank Financial Telecommunication (SWIFT) είναι ένα παγκόσμιο δίκτυο επικοινωνίας που χρησιμοποιείται από χιλιάδες χρηματοπιστωτικά ιδρύματα σε όλο τον κόσμο για την ασφαλή ανταλλαγή πληροφοριών σχετικά με χρηματοοικονομικές συναλλαγές, όπως μεταφορές χρημάτων. Επιπρόσθετα από το Swift, έχει αναπτυχθεί το SWIFT CSCF (Customer Security Controls Framework) το οποίο αποτελεί ένα πλαίσιο ελέγχου ασφάλειας πελατών της SWIFT καθορίζοντας υποχρεωτικά και συμβουλευτικά controls για την προστασία των διατραπεζικών συναλλαγών και την ενίσχυση της ανθεκτικότητας των χρηματοοικονομικών υποδομών.
EBA Guidelines (European Banking Authority Guidelines)	Οι Κατευθυντήριες Γραμμές της Ευρωπαϊκής Αρχής Τραπεζών (EBA Guidelines) είναι οδηγίες που εκδίδονται από την EBA με σκοπό την παροχή οδηγιών και την προώθηση της συνεκτικής εφαρμογής της ευρωπαϊκής νομοθεσίας στον τραπεζικό τομέα. Τα EBA

	Guidelines καλύπτουν ένα ευρύ φάσμα θεμάτων, όπως η διαχείριση κινδύνων, η εποπτεία των τραπεζών, η προστασία των καταναλωτών και η ασφάλεια των πληρωμών.
Payment Card Industry Data Security Standard - PCI DSS	Το Payment Card Industry Data Security Standard (PCI DSS) είναι ένα σύνολο απαιτήσεων ασφαλείας που έχουν σχεδιαστεί για να διασφαλίζουν ότι όλες οι εταιρείες που επεξεργάζονται, αποθηκεύουν ή μεταδίδουν πληροφορίες πιστωτικών καρτών διατηρούν ένα ασφαλές περιβάλλον. Το PCI DSS εφαρμόζεται σε όλους τους οργανισμούς, ανεξαρτήτως μεγέθους ή τοποθεσίας, που εμπλέκονται σε συναλλαγές με πιστωτικές κάρτες.
Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System - ISMS)	Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), όπως ορίζεται από το πρότυπο ISO/IEC 27001:2022, αποτελεί το σύνολο των πολιτικών, διαδικασιών και τεχνικών μέτρων που εφαρμόζονται για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

2

Βιβλιογραφική Ανασκόπηση – Ρυθμιστικά και Τεχνικά Πλαίσια Κυβερνοασφάλειας για TPPs

2.1 Επισκόπηση Κανονιστικών και Τεχνολογικών Εξελίξεων

Στην συγκεκριμένη παράγραφο, θα παραθέσουμε το σύνολο των κανονισμών, οδηγιών και προτύπων τα οποία αφορούν τρίτους παρόχους προμήθειας υπηρεσιών πληρωμών και έχουν σχεδιαστεί για την διασφάλιση της ασφάλειας των συναλλαγών, της διαφάνειας κα της προστασίας των καταναλωτών. Για παράδειγμα, θα αναλύσουμε Ευρωπαϊκούς Κανονισμούς όπως το PSD2 (Payment Service Directive 2) το οποίο επικεντρώνεται κυρίως στην ασφαλή πιστοποίηση της ταυτότητας των πελατών καθώς επίσης και σε παγκόσμια πρότυπα όπως το PCI DSS v4.0 (Payment Card Industry Data Security Standard) το οποίο εστιάζει στην προστασία των καρτικών δεδομένων (για παράδειγμα CVV, αριθμός κάρτας, όνομα κατόχου κτλ.). Πιο συγκεκριμένα:

2.2 Οδηγία PSD2 (Payment Services Directive 2)

2.2.1 Εισαγωγή

Σε συνέχεια των ραγδαίων εξελίξεων στον τομέα τον πληρωμών και πιο συγκεκριμένα στην εξάπλωση των τεχνολογιών με επίκεντρο τα δεδομένα, η Ευρωπαϊκή Ένωση (ΕΕ) υιοθέτησε τη δεύτερη αναθεωρημένη οδηγία για τις υπηρεσίες πληρωμών (Payment Services Directive 2) – *The European parliament and the council of the European Union, 2015 [1]* στις 25 Νοεμβρίου 2015, η οποία παρέχει το νομοκανονιστικό πλαίσιο για την ανάπτυξη και βελτίωση των ηλεκτρονικών πληρωμών εντός της Ευρωπαϊκής Ένωσης. Η οδηγία PSD2, αποτελεί μία κομβική οδηγία η οποία δημιουργήθηκε με σαφής στόχους για την ενίσχυση των μηχανισμών ασφαλείας που σχετίζονται με τις ηλεκτρονικές πληρωμές, την προαγωγή της καινοτομίας και την ενίσχυση του ανταγωνισμού στον τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Third Party Payment Service Providers – TPSPs). Πιο συγκεκριμένα, η οδηγία αποσκοπεί στην αποτελεσματική διασύνδεση των συστημάτων πληρωμών, απλοποιώντας με αυτό τον τρόπο τις διαδικασίες πληρωμών και

ενισχύοντας την ασφάλειά τους, καλλιεργώντας παράλληλα ένα περιβάλλον που ευνοεί την καινοτομία και την ανταγωνιστική ισότητα στον χρηματοοικονομικό κλάδο – *European Central Bank, 2018 [2]*. Με αυτό τον τρόπο η οδηγία PSD2, όχι μόνο επεκτείνει τις θεμελιώδεις ρυθμιστικές αρχές οι οποίες είχαν καθοριστεί στην αρχική έκδοση PSD με έτος δημοσίευσης το 2007 – *The European parliament and the council of the European Union, 2007* [3], αλλά επιπρόσθετα τις βελτιώνει προκειμένου να ανταποκρίνονται στις προκλήσεις που παρουσιάζονται στο συνεχώς εξελισσόμενο τομέα των ψηφιακών πληρωμών. Σε μια σημαντική διαφορά από τον προκάτοχό της, η οδηγία PSD2 επεκτείνει το ρυθμιστικό πλαίσιο για τις διαδικτυακές πληρωμές προκειμένου να συμπεριλάβει στο πεδίο εφαρμογής της νέους παρόχους παροχής υπηρεσιών. Πιο συγκεκριμένα, η PSD2 εισάγει δύο (2) νέες κατηγορίες υπηρεσιών: 1) υπηρεσίες πληροφοριών λογαριασμού (Account Information Services - AIS) και υπηρεσίες εκκίνησης πληρωμών (Payment Initiation Services – PIS). Πιο συγκεκριμένα, οι πάροχοι υπηρεσιών εκκίνησης πληρωμών (Payment Initiation Service Providers – PISPs) όπως οι Paypal, Sofort, Ideal και Tikkie, έχουν πλέον την αδειοδότηση να εκκινούν εντολές πληρωμών απευθείας από τον τραπεζικό λογαριασμό ενός χρήστη κατόπιν σχετικής συγκατάθεσής του. Ομοίως, οι πάροχοι υπηρεσιών πληροφοριών λογαριασμού (Account Information Service Providers - AISPs) όπως οι εταιρίες Moneybox, Spiir, Trustly και Fintonic έχουν την εξουσιοδότηση να συγκεντρώνουν και να παρουσιάζουν ενοποιημένα οικονομικά δεδομένα που συλλέγονται από έναν ή περισσότερους τραπεζικούς λογαριασμούς ενός χρήστη πάντα κατόπιν σχετικής συγκατάθεσης. Η ουσιαστική αλλαγή που επήλθε στον τρόπο λειτουργίας των AISPs, PISPs βάση PSD2, έγκειται στην επίσημη θέσπιση των παραπάνω οντοτήτων καθώς και στην δημιουργία ενός νομοκανονιστικού πλαισίου καθορίζοντας τον τρόπο λειτουργίας τους στην αγορά των ηλεκτρονικών πληρωμών. Επιπρόσθετα, οι προαναφερόμενοι τρίτοι πάροχοι (TPPs) υποχρεούνται να διασφαλίζουν την ασφαλή πρόσβαση στις πληροφορίες των λογαριασμών πληρωμής καθώς και στην διασφάλιση της προστασίας των προσωπικών δεδομένων των χρηστών - *Khakan Najaf, 2021 [4]*. Με τον τρόπο αυτό η PSD2 νομιμοποιεί τον ρόλο των TPPs με την απαιτούμενη εποπτεία από ρυθμιστικές αρχές, διευκολύνοντας την προαγωγή ενός πιο ανταγωνιστικού περιβάλλοντος ηλεκτρονικών πληρωμών διασφαλίζοντας παράλληλα την ασφάλεια των συναλλαγών και το απόρρητο των δεδομένων.

2.2.2 Επισκόπηση Οδηγίας

Η Αναθεωρημένη οδηγία του PSD2 για τις υπηρεσίες πληρωμών αποσκοπεί στην:

- Μείωση του ποσοστού απάτης στον χρηματοοικονομικό κλάδο χωρίς αρνητική επίδραση στην εμπειρία των πελατών αυξάνοντας παράλληλα την εμπιστοσύνη τους.
- Ανάπτυξη ταυτοποίησης πελατών (2-factor authentication). Πιο συγκεκριμένα, το PSD2 απαιτεί την χρήση ισχυρών μέτρων ελέγχου ταυτοποίησης των πελατών (Strong Customer Authentication – SCA) για όλες τις ευρωπαϊκές ηλεκτρονικές συναλλαγές με ισχύ από τις 31 Δεκεμβρίου 2020
- Διεύρυνση του πεδίου εφαρμογής της οδηγίας συμπεριλαμβάνοντας επιπρόσθετους τρίτους παρόχους (TPPs) με κύριο σκοπό την ανάπτυξη της καινοτομίας και του ανταγωνισμού στον τομέα των πληρωμών
- Αύξηση της διαφάνειας και της σαφής οριοθέτησης των ευθυνών στις συμφωνίες αδειοδότησης που αφορούν εφαρμογές ηλεκτρονικών συναλλαγών

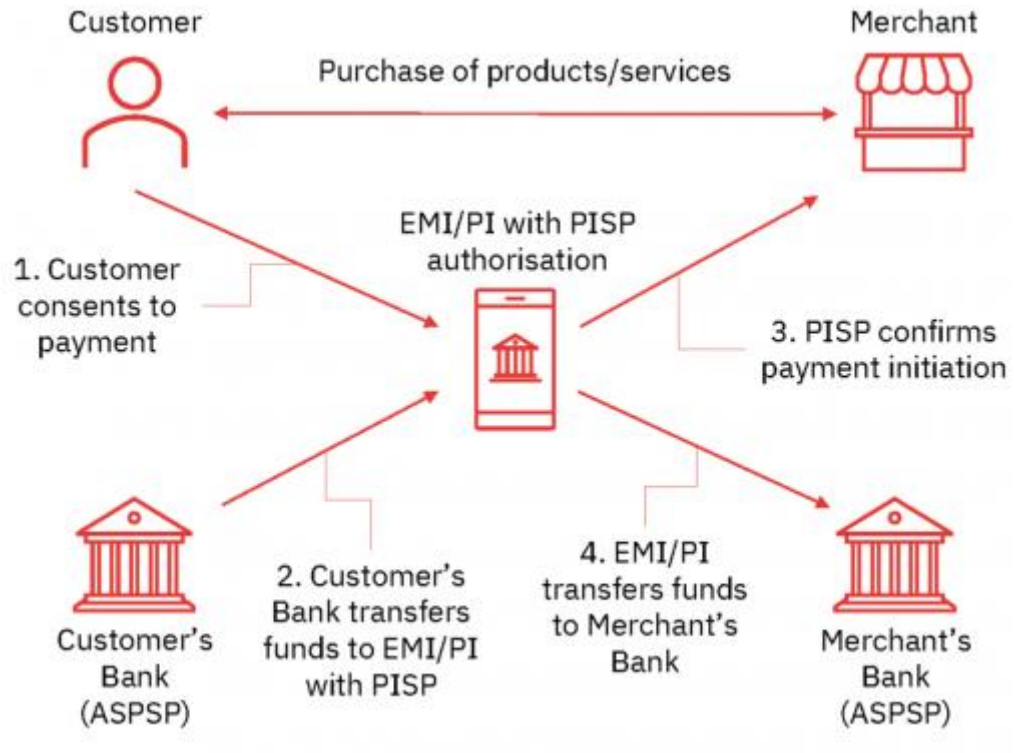
- Μείωση της ευθύνης των καταναλωτών για μη εξουσιοδοτημένες πληρωμές και θέσπιση δικαιώματος επιστροφής χρημάτων για τις άμεσες χρεώσεις σε ευρώ
- Διασφάλιση ότι όταν ολοκληρώνεται μια συναλλαγή, οι εκδότες καρτών καθιστούν διαθέσιμα όλα τα τραπεζικά κεφάλαια
- Απαγόρευση χρέωσης πρόσθετων τελών για πληρωμές που πραγματοποιούνται με πιστωτικές ή χρεωστικές κάρτες είτε σε φυσικό κατάστημα είτε διαδικτυακά.
- Βελτίωση της διαδικασίας υποβολής παραπόνων και ανάπτυξη πρακτικών ανάλυσης και επίλυσης τους από τις τράπεζες

Επιπλέον, η οδηγία PSD2 για την διευκόλυνση της ενσωμάτωσης των νεοεισερχόμενων στον κλάδο των πληρωμών, απαιτεί από τις τράπεζες να παρέχουν τα APIs τους (Application Programming Interface – API) σε όσους τα ζητούν με σκοπό οι πελάτες να έχουν την δυνατότητα να ενοποιήσουν τις πληροφορίες των διαφόρων λογαριασμών τους και την δυνατότητα πληρωμής από μία μόνο συσκευή παρέχοντας με αυτό τον τρόπο καλύτερο έλεγχο και ευκολία στην χρήση. Η παραπάνω απαίτηση αποτελεί μια ριζική αλλαγή στα πλαίσια της θέσπισης του όρου Open Banking η οποία θέτει ως στόχο την αύξηση του ανταγωνισμού και της ανάπτυξης καινοτόμων λύσεων στην Ευρωπαϊκή Ένωση – *J.P.Morgan, 2018 [5]*. Το Open Banking Service Directive προσφέρει στις τράπεζες ένα ενιαίο και τυποποιημένο μέσο αναφοράς για την μοναδική αναγνώριση των τρίτων παρόχων που έχουν πρόσβαση στα APIs τους τους ρόλους και τις υπηρεσίες που είναι εξουσιοδοτημένου να εκτελούν για λογαριασμό των πελατών τους. Επιπρόσθετα, στα πλαίσια του Open Banking Service Directive έχει δημιουργηθεί ένας κατάλογος για την βοήθεια των TPPs και των παρόχων υπηρεσιών πληρωμών εξυπηρέτησης λογαριασμών (Account Servicing Payment Services Providers - ASPSPs) στην κατανόηση των υποχρεώσεων τους δημιουργώντας με αυτό τον τρόπο ένα πλαίσιο εμπιστοσύνης και ασφαλής ανταλλαγής χρηματοοικονομικών πληροφοριών μεταξύ τους – *Open Banking Europe, 2017 [6]*.

Ένας ακόμα σημαντικός στόχος της οδηγίας PSD2 αφορά την διασφάλιση της προστασίας των πελατών κατά την διάρκεια των ηλεκτρονικών πληρωμών τους. Πιο συγκεκριμένα, οι πάροχοι υπηρεσιών πληρωμών (Payment Service Providers – PSPs) πρέπει να συμμορφώνονται με τις απαιτήσεις οι οποίες σχετίζονται με την ισχυρή πιστοποίηση ταυτότητας πελατών (Strong Customer Authentication – SCA) κατά την διάρκεια επεξεργασίας πληρωμών ή παροχής υπηρεσιών που σχετίζονται με πληρωμές για λογαριασμό των πελατών – *European Commission, 2017 [7]*. Επιπρόσθετα, η οδηγία PSD2 απαιτεί έλεγχο ταυτοποίησης πολλαπλών παραγόντων (Multi Factor Authentication – MFA) το οποίο επιτυγχάνεται με την χρήση APIs συνδυαστικά με πιστοποιητικά συμμόρφωσης κατά PSD2. Για την πραγματοποίηση έμπιστων συναλλαγών στο διαδίκτυο, αυτά τα πιστοποιητικά είναι τα SSL (Secure Sockets Layer), TLS (Transport Layer Security) τα οποία κρυπτογραφούν ευαίσθητα δεδομένα και πιστοποιούν τόσο τις τράπεζες όσο και τους TPPs. Επιπλέον όλοι οι PSPs συμπεριλαμβανομένων των τραπεζών και των TPPs οφείλουν να αποδεικνύουν ότι έχουν εφαρμόσει μέτρα ασφαλείας για την διασφάλιση της εγκυρότητας των πληρωμών. Τέλος, σε ετήσια βάση, οι PSPs πρέπει να αξιολογούν τους λειτουργικούς τους κινδύνους και τους κινδύνους ασφαλείας καθώς και τα μέτρα ασφαλείας που έχουν εφαρμόσει – *Sectigo, 2021 [8]*.

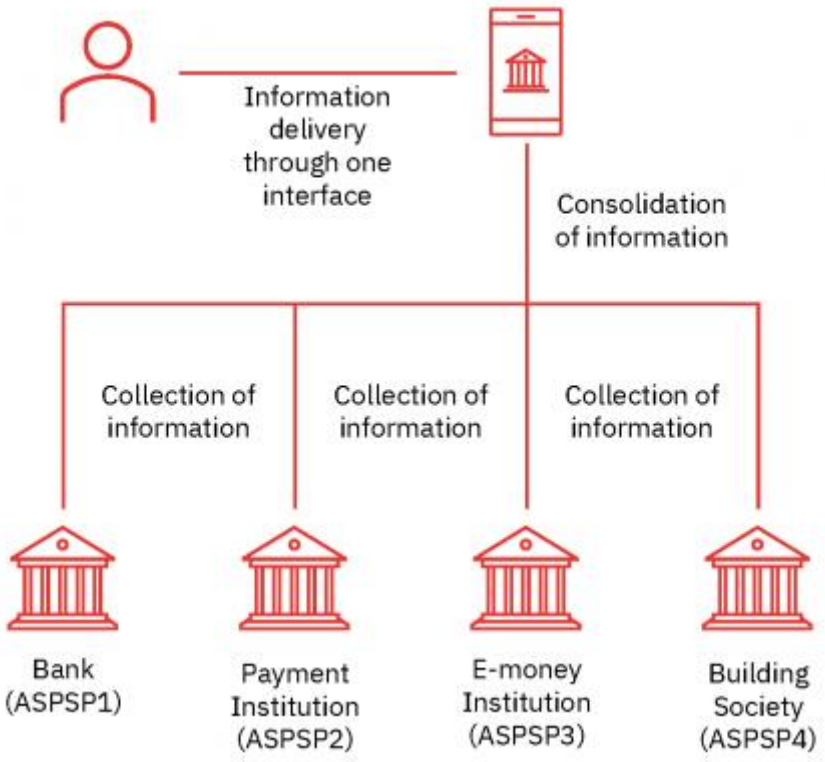
Τέλος παρακάτω θα παρουσιάσουμε τις νέες κατηγορίες παρόχων υπηρεσιών πληρωμών (Payment Service Providers – PSPs). Πιο συγκεκριμένα:

1. **Πάροχοι υπηρεσιών εκκίνησης πληρωμών (Payment Initiation Service Providers – PISPs):** Στην συγκεκριμένη κατηγορία περιλαμβάνονται πάροχοι υπηρεσιών οι οποίες είναι εξουσιοδοτημένοι να δρομολογούν πληρωμές για λογαριασμό ενός πελάτη χωρίς να απαιτείται από τον χρήστη να συνδεθεί στο online banking του. Ένα παράδειγμα χρήσης αποτελεί η αυτόματη μεταφορά χρημάτων στον λογαριασμό ενός πελάτη.



Εικόνα 1: Payment Initiation Service Providers (PISPs) – *PSPLab [9]*

2. **Πάροχοι υπηρεσιών πληροφοριών λογαριασμού (Account Information Service Providers - AISPs):** Στην συγκεκριμένη κατηγορία περιλαμβάνονται πάροχοι υπηρεσιών οι οποίοι έχουν πρόσβαση στα τραπεζικά δεδομένα ενός πελάτη με την χρήση ενός API και μπορούν να εμφανίζουν πληροφορίες λογαριασμού. Πιο συγκεκριμένα, η πρόσβαση στα δεδομένα λογαριασμού, γίνεται μόνο με το δικαίωμα «read-only» το οποίο συνεπάγεται ότι οι πάροχοι αυτής της κατηγορίας δεν μπορούν να πραγματοποιήσουν χρηματικές κινήσεις. Ένα ενδεικτικό παράδειγμα αποτελεί η συγκέντρωση πληροφοριών από πολλούς λογαριασμούς σε μία ενιαία εφαρμογή, δίνοντας την δυνατότητα στον πελάτη ανά πάσα στιγμή να μπορεί να έχει μία συνολική εικόνα των διαθέσιμων λογαριασμών του καθώς και του υπολοίπου που υπάρχει στον κάθε έναν.



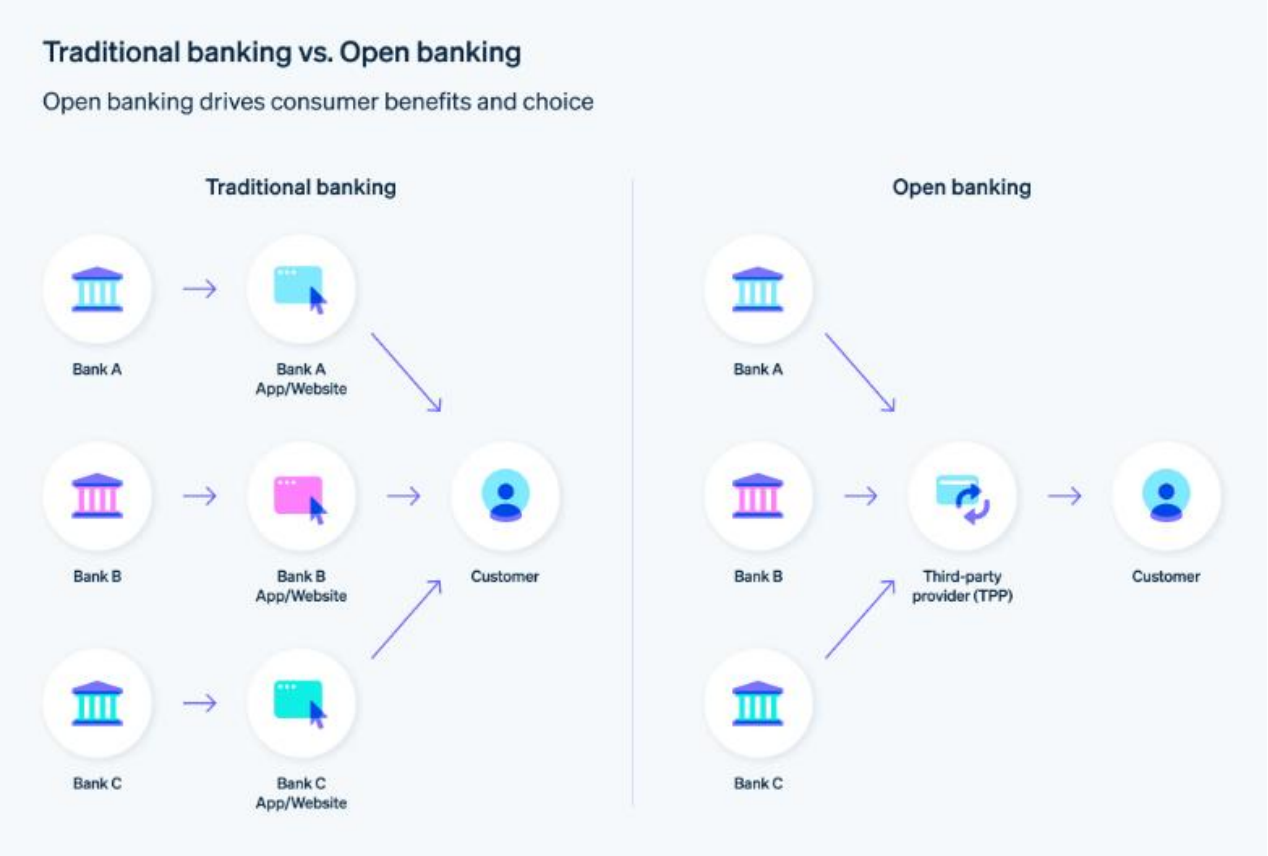
Εικόνα 2: Account Information Service Providers (AISPs) – *PSPLab* [10]

3. **Πάροχοι έκδοσης καρτών (Card-based payment instrument issuing providers - CBPIIP):** Αποτελείται από τους παρόχους που έχουν την δυνατότητα έκδοσης μέσων πληρωμής ή παρέχουν υπηρεσίες συναλλαγών – *Roqqett Blog [11].*
4. **Πάροχοι υπηρεσιών εξυπηρέτησης λογαριασμών (Account Servicing PSP – ASPSP):** οι συγκεκριμένοι πάροχοι εξυπηρετούν την παροχή των νέων υπηρεσιών και χρησιμοποιούνται από τους παραπάνω TPPs για να αποκτήσουν πρόσβαση σε λογαριασμούς ή δεδομένα πελατών – *TrueLayer, 2022 [12].*

2.3 Πρότυπα Open Banking και Εφαρμογές

2.3.1 Εισαγωγή

Με τον ορισμό Open Banking, αναφερόμαστε στα πρότυπα που έχουν οριστεί κατά κύριο λόγο στον χρηματοοικονομικό τομέα και επιτρέπουν τον διαμοιρασμό με ασφάλεια τραπεζικών δεδομένων με εξουσιοδοτημένους τρίτους παρόχους (TPPs) μέσω της χρήσης APIs (Application Programming Interfaces) – *Stripe, 2025 [13].*



Εικόνα 3: Traditional Banking vs Open Banking – *Stripe, 2025 [13]*

Πιο συγκεκριμένα , το Open Banking πρωτοεμφανίστηκε τον Ιανουάριο του 2018 στο Ηνωμένο Βασίλειο ως κανονιστική απαίτηση από την αρχή Ανταγωνισμού και Αγορών (Competition and Markets Authority – CMA) απαιτώντας από τις εννέα μεγαλύτερες τράπεζες την τυποποίηση των APIs καθώς και την δημιουργία ενός καταλόγου με τους εξουσιοδοτημένους τρίτους παρόχους – *Stripe, 2024 [14]*. Στην συνέχεια το Open Banking εφαρμόστηκε και στην Ευρωπαϊκή Ένωση αποτελούμενο μέρος της οδηγίας PSD2 (Payment Service Directive 2), η οποία απαιτεί από όλους τους παρόχους υπηρεσιών πληρωμών (PSPs) την υλοποίηση τεχνικών για την ασφαλή ανταλλαγή δεδομένων καθώς και τον σχεδιασμό APIs -*TrueLayer [15]*. Επιπρόσθετα, μία σημαντική θεμελιώδη αρχή των προτύπων Open Banking, αποτελεί ο καθορισμός τεσσάρων (4) σημαντικών στρατηγιών απαιτήσεων όπως ορίστηκαν από τους Cortet, Rijks, & Nijland το 2016 και παραθέτονται παρακάτω - *Canadian Center of Science and Education, 2018 [16]:*

- **Συμμόρφωση** (εξασφάλιση συμμόρφωση με το άνοιγμα μόνο των υποχρεωτικών δεδομένων),
- **Ανταγωνισμός** (ανταγωνισμός για την εγγύτητα με τους πελάτες μέσω ιδιόκτητων διεπαφών),
- **Επέκταση** (προσφορά νέων υπηρεσιών και API σε τρίτους παρόχους),

- και **Δημιουργία Εσόδων** (ενεργή αναζήτηση νέων πηγών εσόδων μέσω της ανοικτής τραπεζικής).

2.3.2 Επισκόπηση Προτύπου

Αναφορικά με την δυνατότητα των τρίτων παρόχων (TPPs) να προσφέρουν υπηρεσίες πληρωμών, τα πρότυπα του Open Banking απαιτούν την εξουσιοδότηση των TPPs από μια εθνική ρυθμιστική αρχή καθώς επίσης την υλοποίηση ισχυρών μέτρων ασφαλείας για την πρόσβαση σε καρτικά δεδομένα πελατών κατόπιν σχετικής συγκατάθεση από την πλευρά τους - *Investopedia, 2024 [17]*. Πιο συγκεκριμένα, αναφορικά με τα πρότυπα Open Banking, σύμφωνα με τις απαιτήσεις που έχουν οριστεί από την Open Banking Implementation Entity (OBIE) για την Αγγλία καθώς και το ευρωπαϊκό PSD2, καθορίζονται οι παρακάτω κανόνες για τους τρίτους παρόχους – *McKinsey&Company, 2017 [18]*. Πιο συγκεκριμένα:

- **Κατηγοριοποίηση τρίτων παρόχων:** Οι τρίτοι πάροχοι διαχωρίζονται σε δύο (2) βασικές κατηγορίες τους παρόχους υπηρεσιών πληροφοριών λογαριασμού (Account Information Service Providers – AISPs) οι οποίοι αποκτούν κατόπιν συγκατάθεσης του πελάτη πρόσβαση στις πληροφορίες λογαριασμού τους για την παροχή υπηρεσιών όπως προϋπολογισμό και ανάλυση κινήσεων καθώς επίσης και τους παρόχους υπηρεσιών εκκίνησης πληρωμών (Payment Initiation Service Providers – PISPs) οι οποίοι έχουν την δυνατότητα κατόπιν συγκατάθεσης του πελάτη να πραγματοποιούν πληρωμές από τον λογαριασμό του όπως πάγιες εντολές.
- **Εγγραφή τρίτων παρόχων:** Οι τρίτοι πάροχοι πρέπει να είναι εξουσιοδοτημένοι και εγγεγραμμένοι στον κατάλογο εξουσιοδοτημένων τρίτων παρόχων από μία αρμόδια αρχή όπως για παράδειγμα την Financial Authority στην Αγγλία ή την Εθνική Ρυθμιστική Αρχή στην Ευρωπαϊκή Ένωση
- **Ασφάλεια προσωπικών δεδομένων πελατών:** Οι τρίτοι πάροχοι είναι υπόχρεοι στην χρησιμοποίηση ισχυρών μέτρων ελέγχου ταυτοποίησης πελατών (Strong Customer Authentication – SCA) για την πρόσβαση σε δεδομένα και κατ' επέκταση την έναρξη πληρωμών με την χρήση μόνο των απολύτως απαραίτητων δεδομένων
- **Χρήση προτυποποιημένων API:** Οι τράπεζες οφείλουν να παρέχουν τυποποιημένα APIs στους τρίτους παρόχους για την πρόσβαση σε δεδομένα και την έναρξη πληρωμών από τους λογαριασμούς των πελατών τους καθώς επίσης και οι τρίτοι πάροχοι υποχρεούνται να συμμορφώνονται με κανονιστικές απαιτήσεις που σχετίζονται με την προστασία των προσωπικών δεδομένων όπως το GDPR (General Data Protection Regulation).

2.4 Κανονισμοί Πληρωμών του Ηνωμένου Βασιλείου (PSRs)

2.4.1 Εισαγωγή

Η Ρυθμιστική Αρχή Συστημάτων Πληρωμών (Payment Service Regulator – PSR) αποτελεί μια ανεξάρτητη οικονομική αρχή του Ηνωμένου Βασιλείου που ιδρύθηκε με σκοπό την διασφάλιση της ορθής λειτουργίας των συστημάτων πληρωμών. Το PSR δημιουργήθηκε την 1η Απριλίου του 2015 βάση του νόμου Financial Services (Banking Reform) Act 2013 ως θυγατρική του Financial Conduct Authority διαθέτοντας παρόλα αυτά δικό της αυτόνομο διοικητικό συμβούλιο, προϋπολογισμό και εξουσιοδοτήσεις – *PSR [19].* Οι κύριοι στόχοι της ρυθμιστικής αρχής είναι επιγραμματικά – *PSR [20]:*

- Η διασφάλιση ότι τα συστήματα πληρωμών λειτουργούν και αναπτύσσονται με κύριο μέλημα την διασφάλιση των συμφερόντων και την προστασία των πελατών
- Η προώθηση του υγιούς ανταγωνισμού μεταξύ των τραπεζών, των παρόχων υπηρεσιών πληρωμών (Payment Service Providers - PSPs) και των προμηθευτών υποδομών
- Η ανάπτυξη καινοτόμων συστημάτων πληρωμών, ιδίως στην υποδομή που χρησιμοποιείται για τη λειτουργία των συστημάτων αυτών

2.4.2 Επισκόπηση Νομικού πλαισίου

Πιο συγκεκριμένα, η Αγγλία το 2017 κοινοποίησε το νομικό πλαίσιο Payment Services Regulations 2017 (2017 No. 752) – *UK Governance Legislation, 2017 [21]*, το οποίο βασίστηκε κατά κύριο λόγο στην ευρωπαϊκή οδηγίας PSD2 (Payment Service Directive 2 - Directive (EU) 2015/2366) και εφαρμόζεται από την Αρχή Χρηματοοικονομικής Συμπεριφοράς (Financial Conduct Authority – FCA). Πιο συγκεκριμένα, το νομικό πλαίσιο ορίζει για τους τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Payment Servicer Providers – PSPs) τις παρακάτω απαιτήσεις:

1. **Εγγραφή τρίτων παρόχων και εξουσιοδότηση λειτουργίας:** Οι TPPs οφείλουν να εγγραφούν στον κατάλογο τρίτων παρόχων που έχει οριστεί από την FCA προκειμένου να είναι εξουσιοδοτημένοι και να μπορούν να λάβουν την σχετική άδεια λειτουργίας όπως απεικονίζεται στο Part 2 (Registration), σελ.13 του πλαισίου PSR 2017 και πιο συγκεκριμένα στις απαιτήσεις 4-19 του αναφερόμενου κεφαλαίου. Οι αιτήσεις πρέπει να περιλαμβάνουν μεταξύ άλλων επιχειρηματικά πλάνα του οργανισμού, στρατηγικές διακυβέρνησης και διαδικασίες που είναι σε ισχύ και σχετίζονται με την διαδικασία αποζημίωσης ενός πελάτη όπως αναφέρονται στο Regulation 5 (Application for authorisation as a payment institution or variation of an existing authorisation) στην σελ. 14, Regulation 13 Application for registration as a small payment institution or variation of an existing registration) στην σελ. 21, Regulation 17 (Application for registration as an account information service provider or variation of an existing registration) στην σελ.24 και το Schedule 2 (Information to be included in or with an application for authorisation) στην σελ. 113 του πλαισίου PSR 2017. Τέλος, οι AISPs και οι PISPs οφείλουν να διαθέτουν ασφάλιση επαγγελματικής ευθύνης ή ανάλογη εγγύηση για την διασφάλιση των υποχρεώσεών τους

όπως ορίζεται στα πεδία Regulation 6(7)(e) (Conditions for authorisation as a payment institution) στη σελ. 15 και Regulation 18(4) (Conditions for registration as an account information service provider) σελ. 24 του πλαισίου PSR 2017.

2. **Σαφή Οργανωτική Δομή των τρίτων παρόχων:** Οι τρίτοι πάροχοι πρέπει να είναι σε θέση να μπορούν να πιστοποιήσουν ανά πάσα στιγμή ότι έχουν σαφώς καθορισμένη οργανωτική δομή, μεθόδους διαχείρισης κινδύνων καθώς και ότι εκτελούν ανά τακτά χρονικά διαστήματα εσωτερικούς ελέγχους όπως ζητείται στα πεδία Regulation 6(6) (Conditions for authorisation as a payment institution) στη σελ. 15 του πλαισίου PSR 2017. Επιπρόσθετα, τα διευθυντικά στελέχη των οργανισμών πρέπει να διαθέτουν πιστοποιήσεις που να βεβαιώνουν ότι διαθέτουν τις κατάλληλες γνώσεις και εμπειρία για την εκτέλεση του κρίσιμου ρόλου τους όπως απεικονίζεται στα πεδία Regulation 6(7)(b) (Conditions for authorisation as a payment institution) στη σελ. 15 και Regulation 14(7) (Conditions for registration as a small payment institution) στη σελ. 21 του πλαισίου PSR 2017.
3. **Διασφάλιση των κεφαλαίων των χρηστών:** Οι TPPs πρέπει να διασφαλίζουν τα χρηματικά κεφάλαια των χρηστών χρησιμοποιώντας δικλείδες ασφαλείας προστατεύοντάς τα σε περίπτωση ύποπτης ενέργειας όπως παρουσιάζεται στο Regulation 23 (Safeguarding requirements) στη σελ. 26 του πλαισίου PSR 2017.
4. **Τακτική υποβολή αναφορών:** Οι TPPs οφείλουν να ενημερώνουν την FCA σε τακτικά χρονικά διαστήματα και πιο συγκεκριμένα για κάθε ουσιαστική αλλαγή στην επιχειρησιακή τους δραστηριότητα, διοικητικές αλλαγές και λειτουργίες του οργανισμού όπως απεικονίζετε στο πεδίο Regulation 20 (Duty to notify changes) στη σελ. 25 και Regulation 37 (Duty to notify change in circumstance) στη σελ. 39 του πλαισίου PSR 2017 .
5. **Έλεγχος Outsourcing υπηρεσιών:** Στην περίπτωση που οι TPPs κάνουν outsource σημαντικές λειτουργίες (όπως IT systems) τότε πρέπει να εξασφαλίζουν ότι δεν επηρεάζονται οι εσωτερικοί έλεγχοί τους καθώς και η δυνατότητα πιθανού ελέγχου από την FCA όπως προσδιορίζεται στο Regulation 25 (Outsourcing) στη σελ. 33 του πλαισίου PSR 2017.
6. **Συμμόρφωση με κανονισμούς Anti-Money Laundering (AML):** Οι TPPs οφείλουν να συμμορφώνονται με τις απαιτήσεις που ορίζονται σε AML κανονισμούς και να είναι εγγεγραμμένοι στα σχετικά μητρώα όπως αναφέρεται στα σημεία Regulation 6(8) (Conditions for authorisation as a payment institution) στη σελ. 15 και Regulation 14(11) (Conditions for registration as a small payment institution) στη σελ. 22 του πλαισίου PSR 2017.
7. **Προστασία των καταναλωτών και ανάπτυξη διαύλων επικοινωνίας:** Οι τρίτοι πάροχοι πρέπει να ενεργούν λαμβάνοντας πρωτίστως τα συμφέροντα των καταναλωτών με την παροχή σαφώς καθορισμένων πληροφοριών και οδηγιών καθώς και κατάλληλο χειρισμό πιθανών παραπόνων από την πλευρά τους καθώς επίσης οφείλουν να παρέχουν επαρκές πληροφορίες σε περίπτωση αναγνώρισης μη εγκεκριμένων συναλλαγών όπως ορίζεται στα τμήματα Regulations 73-79 (Unauthorised payment transactions) στις σελ. 61-64 και Regulations 91-95 (Non-execution or defective or late execution of transactions, liability for charges and interest and right of recourse) στις σελ. 71-73 του πλαισίου PSR 2017.
8. **Συμμόρφωση με τις συνεχώς αναπτυσσόμενες απαιτήσεις που ορίζει η FCA:** Οι TPPs οφείλουν να συμμορφώνονται συνεχώς με τις απαιτήσεις που ορίζονται από την FCA καθώς

έχει το δικαίωμα να τροποποιήσει ή ακόμα και να ανακαλέσει άδειες λειτουργίας λόγω μη συμμόρφωσης ενός οργανισμού με το πλαίσιο που έχει ορίσει όπως παρουσιάζεται στα πεδία Regulations 7-12 (Imposition of requirements, Variation etc. at request of authorised payment institution, Determination of application for authorisation or variation of authorisation, Cancellation of authorisation, Request for cancellation of authorisation, Variation of authorisation on FCA's own initiative) στις σελ. 17-19 του πλαισίου PSR 2017. Πιο συγκεκριμένα για τους AISPS ορίζεται στα πεδία Regulation 18(3) (Conditions for registration as an account information service provider) στη σελ. 24 και Regulation 18(4) (Conditions for registration as an account information service provider) στη σελ. 24 του πλαισίου PSR 2017 ότι πρέπει να παρέχουν ρητά μόνο υπηρεσίες πληροφόρησης λογαριασμού και όχι άλλες υπηρεσίες εκτός και αν υπάρχει ξεχωριστή άδεια που να το επιτρέπει. Αντίστοιχα για τους PISPs ορίζεται ότι πρέπει να διαθέτουν ασφάλιση για την κάλυψη των ευθυνών από μη εξουσιοδοτημένες συναλλαγές καθώς και να έχουν υλοποιήσει μέτρα για την ασφαλή επικοινωνία και πιστοποίηση ταυτότητας όπως παρουσιάζονται στο πεδίο Regulation 6(7)(e) (Conditions for authorisation as a payment institution) στη σελ.15 και Regulation 100 (Secure communication and authentication) στη σελ. 75 του πλαισίου PSR 2017.

Τέλος, το PSR σε συνεργασία με την αρχή Ανταγωνισμού και Αγορών (Competition and Markets Authority – CMA) και την Αρχή Χρηματοοικονομικής Συμπεριφοράς (Financial Conduct Authority - FCA) ήταν αρμόδιες για την επίβλεψη υιοθέτησης από τους οργανισμούς των Open Banking Standards καθορίζοντας επίσης για την βοήθειά τους την «General Direction 3» που απαιτεί από τίς εννέα (9) μεγαλύτερες τράπεζες της Αγγλίας να παρέχουν ασφαλή APIs access για τους *TPPs – Payment Systems Regulator, 2020 [22]*. Πιο συγκεκριμένα, η οδηγία εφαρμόζεται σε όλους τους φορείς που χρησιμοποιούν συστήματα πληρωμών και διατραπεζικά συστήματα πληρωμών που εμπίπτουν στο Regulation 103 of the PSRs 2017. Κύριος σκοπός είναι να διασφαλίσει άρτια και ασφαλή πρόσβαση στα συστήματα πληρωμών για τους PSPs, συμπεριλαμβανομένων των τρίτων παρόχων.

2.5 Τεχνικά Πρότυπα και Οδηγίες της Ευρωπαϊκής Αρχής Τραπεζών (EBA)

2.5.1 Εισαγωγή

Η Ευρωπαϊκή Αρχή Τραπεζών (European Banking Authority - EBA) είναι μια ανεξάρτητη αρχή της Ευρωπαϊκής Ένωσης με κύριο σκοπό την εξασφάλιση της συμμόρφωσης του τραπεζικού τομέα με κανονιστικά πλαίσια (όπως το PSD2) με κύριο στόχο την διατήρηση της χρηματοπιστωτικής σταθερότητας και την διασφάλιση της ακεραιότητας, της αποτελεσματικότητας και της ορθής λειτουργείας του τραπεζικού τομέα. Για την επίτευξη των προαναφερόμενων στόχων, έχουν κοινοποιηθεί ένα σύνολο Ρυθμιστικών Τεχνικών Προτύπων (Regulatory Technical Standards – RTS), Τεχνικών Προτύπων Υλοποίησης (Implementing Technical Standards – ITS) και οδηγιών (Guidelines) τα οποία αναπτύχθηκαν για την διασφάλιση της συμμόρφωσης με τις απαιτήσεις του PSD2 – *European Banking Authority [23]*.

2.5.2 Επισκόπηση Προτύπων και Οδηγιών

Τα σημαντικότερα RTS και Guidelines, τα οποία μία χρηματοπιστωτική οντότητα οφείλει να καλύπτει κατ' ελάχιστο προκειμένου να συμμορφωθεί με το πρότυπο PSD2 παρουσιάζονται περιληπτικά παρακάτω:

a. Το κανονιστικό τεχνικό πρότυπο (RTS) EBA/RTS/2017/02 – *European Banking Authority, 2017 [24]*, καθορίζει τις απαιτήσεις για την ισχυρή ταυτοποίηση πελάτη (Strong Customer Authentication – SCA) και την κοινή και ασφαλή επικοινωνία (Common Secure Communication – CSC) σύμφωνα με το άρθρο 98 της αναθεωρημένης οδηγίας PSD2. Τα κύρια θέματα που το συγκεκριμένο RTS προσπαθεί να καλύψει και αναλύονται σε μεγαλύτερη ακρίβεια παρακάτω είναι:

    - Πότε απαιτείται να χρησιμοποιείται SCA και υπό ποιες περιπτώσεις μπορεί να εξαιρεθεί η χρήση του
    - Μέτρα προστασίας για την εξασφάλιση της ακεραιότητας των credentials των χρηστών
    - Πρότυπα για την ασφαλή επικοινωνίας μεταξύ των παρόχων υπηρεσιών πληρωμών (PSPs) συμπεριλαμβανομένων των AISPs και των PISPs
    - Υποχρεώσεις προς τους ASPSPs για τις μεθόδους παροχής πρόσβασης στους TPPs

Πιο συγκεκριμένα, το RTS ορίζει για τους τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Payment Servicer Providers – PSPs) τις παρακάτω απαιτήσεις:

1. **Διασφάλιση ασφαλής πρόσβασης και επικοινωνίας:** Οι ASPSPs οφείλουν να παρέχουν τουλάχιστον μία ασφαλή διεπαφή (είτε API είτε διεπαφή πελάτη) που επιτρέπει στους AISPs και στους PISPs να ταυτοποιούνται και να επικοινωνούν με ασφάλεια για να έχουν πρόσβαση σε πληροφορίες λογαριασμών ή να πραγματοποιούν πληρωμές κατόπιν σχετικής εξουσιοδότησης όπως παρουσιάζεται στο Άρθρο 27, σελ. 32. Επιπρόσθετα, οι TPPs πρέπει να χρησιμοποιούν πιστοποιητικά που πληρούν τις απαιτήσεις για την ταυτοποίηση όπως ορίζονται από το eIDAS σύμφωνα με το Άρθρο 29 στην σελ. 34. Τέλος, όλες οι επικοινωνίες θα πρέπει να κρυπτογραφούνται με την χρήση ισχυρών και γνωστών τεχνικών κρυπτογράφησης όπως απαιτείται στο Άρθρο 30, σελ. 35.
2. **Μέτρα Αυθεντικοποίησης και χρήσης SCA:** Οι TPPs οφείλουν να βασίζονται στις διαδικασίες αυθεντικοποίησης που ορίζονται από τους ASPSPs στον χρήστη όπως παρουσιάζεται στο Άρθρο 27 παράγραφο 3 στην σελ. 32. Επίσης αναφορικά με την χρήση του SCA, ορίζεται στο Άρθρο 4, σελ. 19 η χρήση του στις περιπτώσεις που ένας χρήστης έχει πρόσβαση στον ηλεκτρονικό λογαριασμό του, εκκινεί μια πληρωμή ή σχετίζεται με ενέργεια που μπορεί να αποτελεί απάτη. Επιπρόσθετα, η χρήση SCA μπορεί να εξαιρεθείς στις παρακάτω περιπτώσεις:

- Πραγματοποίηση πρόσβαση μόνο στο υπόλοιπο λογαριασμού ή στις συναλλαγές που πραγματοποιήθηκαν τις τελευταίες 90 ημέρες σύμφωνα με το Άρθρο 10, σελ.22
- Πραγματοποίηση ανέπαφων πληρωμών μικρής χρηματικής αξίας σύμφωνα με το Άρθρο 11, σελ. 23
- Πληρωμές σε αυτόματα τερματικά που χρησιμοποιούνται στα μέσα μαζικής μεταφοράς καθώς και σε χώρους στάθμευσης όπως απεικονίζεται στο Άρθρο 12, σελ.23
- Συναλλαγές με αξιόπιστους δικαιούχους καθώς και επαναλαμβανόμενες πληρωμές σύμφωνα με το Άρθρο 13, σελ.23
- Μεταφορές μεταξύ λογαριασμών του ίδιου δικαιούχου σύμφωνα με το Άρθρο 14, σελ.24
- Online συναλλαγές χαμηλής αξίας όπως ορίζεται στο Άρθρο 15, σελ. 24
- Συναλλαγές που έχουν κατηγοριοποιηθεί ως χαμηλού κινδύνου κατόπιν πραγματοποίησης ανάλυσης κινδύνου συναλλαγών (Transaction Risk Analysis – TRA) σύμφωνα με το Άρθρο 16, σελ.24
- Οι τρίτοι πάροχοι υπηρεσιών πληρωμών (TPPs) οφείλουν να διασφαλίζουν ότι έχουν πρόσβαση μόνο σε πληροφορίες για τις οποίες ο χρήστης έχει δώσει τη ρητή συγκατάθεσή του όπως ορίζεται στο Άρθρο 31 Παράγραφος 3, σελ. 36

3. **Επιτρεπόμενη επεξεργασία και ασφάλεια δεδομένων:** Οι TPPs δεν πρέπει να αποθηκεύουν ή να έχουν πρόσβαση σε ευαίσθητα δεδομένα πληρωμών, εκτός εάν αυτό είναι απαραίτητο για την παροχή των υπηρεσιών τους και πάντοτε κατόπιν σχετικής συγκατάθεσης από τον χρήστη όπως παρουσιάζεται στο Άρθρο 31 Παράγραφο 1, σελ.36. Επιπρόσθετα, σε περίπτωση παραβίασης των credentials ενός χρήστη, οι τρίτοι πάροχοι υπηρεσιών πληρωμών οφείλουν να ενημερώνουν τον χρήστη άμεσα όπως ορίζεται στο Άρθρο 30 Παράγραφο 5, σελ. 35
4. **Ορθή χρήση APIs και μεγιστοποίηση αποδοτικότητας:** Στην περίπτωση που οι ASPSPs προσφέρουν διεπαφή API, οι τεχνικές προδιαγραφές πρέπει να είναι καταγεγραμμένες και διαθέσιμες σε ε εξουσιοδοτημένους TPPs όπως ορίζεται στο Άρθρο 27 Παράγραφο 4, σελ.32. Επιπρόσθετα, οι ASPSPs οφείλουν να παρέχουν μία δοκιμαστική εγκατάσταση στους TPPs για να δοκιμάζουν το λογισμικό τους καθώς και τις εφαρμογές τους όπως απαιτείται στο Άρθρο 27 Παράγραφο 6, σελ. 33
5. **Παρακολούθηση και αναφορά μη εξουσιοδοτημένων συναλλαγών:** Οι TPPs που εμπίπτουν στις εξαιρέσεις χρήσης SCA, οφείλουν να παρακολουθούν και να καταγράφουν περιστατικά που σχετίζονται με μη εξουσιοδοτημένες συναλλαγές, την μέση αξία των συναλλαγών καθώς και ποιες περιπτώσεις εξαιρέσεων χρήσης SCA εμπίπτει η κάθε συναλλαγή προκειμένου να είναι σε θέση να τα διαθέσει στις αρχές κατόπιν σχετικού αιτήματος σύμφωνα με το Άρθρο 17, σελ. 25

b. Το τελικό report EBA/RTS/2022/03 [25], το οποίο σχετίζεται με την τροποποίηση των κανονιστικών τεχνικών προτύπων (RTS) για την ισχυρή ταυτοποίηση του πελάτη (Strong Customer Authentication – SCA) και των κοινών και ασφαλή ανοιχτών προτύπων επικοινωνίας (Common and Secure Open Standards for Communication – CSC), τα οποία δημοσιεύθηκαν

από την εθνική αρχή Τραπεζών (EBA) στις 5 Απριλίου του 2022 με στόχο την τροποποίηση στον Commission Delegated Regulation (EU) 2018/389, ο οποίος συμπληρώνει την οδηγία υπηρεσιών πληρωμών (PSD2). Πιο συγκεκριμένα, το συγκεκριμένο έγγραφό δημιουργήθηκε για να διευθέτηση ένα κύριο θέμα που είχε δημιουργηθεί στα πλαίσια εφαρμογής των απαιτήσεων του PSD2, το οποίο απαιτούσε από τους παρόχους υπηρεσιών πληρωμών (Payment Service Providers – PSPs) να εφαρμόζουν SCA κάθε φορά που ένας χρήστης υπηρεσιών πληρωμών (Payment Service Users – PSU) είχε πρόσβαση στον λογαριασμό πληρωμών του διαδικτυακά, είτε απευθείας είτε μέσω ενός παρόχου υπηρεσιών πληροφοριών λογαριασμού (AISP). Ο λόγος αποτελούσε ότι τα προγενέστερα RTS, επέτρεπαν στους PSPs να εξαιρούν την χρήση SCA για την πρόσβαση στο υπόλοιπο των λογαριασμών των πελατών καθώς και στις πρόσφατες συναλλαγές, υπό την προϋπόθεση ότι το SCA εφαρμοζόταν κατά την πρώτη πρόσβαση και τουλάχιστον κάθε 90 μέρες μετέπειτα. Η παραπάνω εξαίρεση ήταν προαιρετική με αποτέλεσμα την ασυνέπεια στην εφαρμογή της καθώς και την δημιουργία παραπόνων από την πλευρά των πελατών. Για τον λόγο αυτό οι κύριες τροποποιήσεις που εφαρμόζονται στο συγκεκριμένο RTS είναι οι παρακάτω:

1. **Υποχρεωτική εξαίρεση από την εφαρμογή SCA των AISPs:** Η τροποποίηση εισάγει υποχρεωτική εξαίρεση από την χρήση SCA για τις περιπτώσεις όπου η πρόσβαση γίνεται μέσω AISP, υπό την προϋπόθεση ότι πληρούνται οι προϋποθέσεις που απεικονίζονται στο Article 10α, σελ. 17-18 με σχετική αναφορά στο Article 2
2. **Προαιρετική εξαίρεση για άμεση πρόσβαση:** Δίνεται η δυνατότητα προαιρετικής εξαίρεσης όταν ο πελάτης έχει άμεση πρόσβαση στις πληροφορίες του λογαριασμού του μέσω ενός παρόχου υπηρεσιών πληρωμών που διαχειρίζεται τον λογαριασμό του όπως αναφέρεται στο Article 10, σελ. 17
3. **Παράταση της περιόδου ανανέωσης των SCA:** Η περίοδος ανανέωσης των SCA παρατείνεται από της 90 ημέρες στις 180 ημέρες, τόσο για την άμεση πρόσβαση όσο και για την πρόσβαση μέσω AISPs όπως παρουσιάζεται στο Article 10 paragraph 2 bullet b και το Article 10a paragraph 2 bullet b
4. **Δικλείδες Ασφαλείας με την χρήση SCA:** Οι ASPs μπορούν να εξακολουθούν να απαιτούν την χρήση SCA ανά πάσα στιγμή και κυρίως αν υπάρχουν υποψίες για μη εξουσιοδοτημένη ή κακόβουλή πρόσβαση όπως αναφέρεται στο Article 10a paragraph 3 στην σελ. 18

c) Το συμβουλευτικό έγγραφο EBA-CP-2017-04 [26] που δημιουργήθηκε τον Μάιο του 2017 από την Ευρωπαϊκή Αρχή Τραπεζών (EBA), εμπεριέχει οδηγίες προς τους παρόχους υπηρεσιών πληρωμών (PSPs) σχετικά με την διαχείριση των λειτουργικών κινδύνων και των κινδύνων ασφαλείας όπως απαιτείται από το Άρθρο 95 της αναθεωρημένης οδηγίας PSD2. Οι απεικονιζόμενες οδηγίες που παρουσιάζονται, επικεντρώνονται σε 8 βασικές κατηγορίες γύρω από τους τρόπους διαχείρισης των λειτουργικών κινδύνων και των κινδύνων ασφαλείας για τους PSPs. Πιο συγκεκριμένα:

1. **Διακυβέρνηση:** Οι PSPs οφείλουν να θεσπίζουν ένα ολοκληρωμένο πλαίσιο διαχείρισης κινδύνων, εγκεκριμένο από το Board of Directors, το οποίο θα περιλαμβάνει μέτρα ασφαλείας για την διαχείριση των κινδύνων. Στο συγκεκριμένο πλαίσιο, θα πρέπει να απεικονίζονται επίσης ξεκάθαρα ρόλοι και αρμοδιότητες καθώς και η περιοδικότητα της αξιολόγησης του πλαισίου για τυχόν αλλαγές βάση του συνεχώς εξελισσόμενου πεδίου απειλών στον κυβερνοχώρο όπως παρουσιάζεται στο Guideline 1, σελ. 18
2. **Αξιολόγηση Κινδύνων:** Οι PSPs υποχρεούνται να αναγνωρίζουν, να ταξινομούν και να αξιολογούν σε τακτικά χρονικά διαστήματα τις επιχειρησιακές τους λειτουργίες, τις διαδικασίες τους και τα assets τους εστιάζοντας στην κρισιμότητα και τις αλληλεξαρτήσεις. Επιπρόσθετα, τα δικαιώματα πρόσβασης οφείλουν να διαχειρίζονται με βάση την αρχή need-to-know και να επαναξιολογούνται ανά τακτικά χρονικά διαστήματα όπως παρουσιάζονται στο Guideline 2, σελ. 18-19
3. **Προστασία:** Οι PSPs οφείλουν να εφαρμόζουν προληπτικά μέτρα ασφαλείας, συμπεριλαμβανομένων μίας προσέγγισης βασισμένης στην αρχή defense-in-depth με την προστασία των ευαίσθητων δεδομένων και την χρήση ισχυρών ελέγχων πρόσβασης. Επιπρόσθετα, δίνεται έμφαση στην ελαχιστοποίηση χρήσης των δεδομένων καθώς επίσης και στην συνεχή ενημέρωση λογισμικού όπως παρουσιάζεται στο Guideline 3, σελ. 19-20
4. **Ανίχνευση:** Οι PSPs πρέπει να διαθέτουν μηχανισμούς συνεχούς παρακολούθησης και ανίχνευσης ανώμαλων δραστηριοτήτων και περιστατικών ασφαλείας, συμπεριλαμβανομένων μηχανισμών ανίχνευσης εισβολών (IDS) και αναφοράς στην ανώτερη διοίκηση όπως παρουσιάζεται στο Guideline 4, σελ 20-21.
5. **Επιχειρησιακή Συνέχεια:** Οι PSPs πρέπει να διαθέτουν μεθόδους διαχείρισης επιχειρησιακής συνέχειας και σχέδια ανάκαμψης σε έκτακτη ανάγκη προκειμένου να εξασφαλίσουν τη συνεχή παροχή υπηρεσιών πληρωμών κατά τη διάρκεια ενός περιστατικού, τα οποία θα δοκιμάζονται σε τακτά χρονικά διαστήματα σε διάφορα σενάρια με την χρήση μηχανισμών επικοινωνίας τόσο εσωτερικά όσο και εξωτερικά του οργανισμού σε περιπτώσεις κρίσεων όπως παρουσιάζεται στο Guideline 5, σελ. 21-22
6. **Δοκιμές μέτρων ασφαλείας**: Τα μέτρα ασφαλείας δοκιμάζονται συνεχώς, συμπεριλαμβανομένων vulnerability scans και penetration tests και κυρίως μετά από σημαντικές αλλαγές ή περιστατικά ασφαλείας. Οι παραπάνω έλεγχοι πραγματοποιούνται με την χρήση εξωτερικού ανεξάρτητου συνεργάτη για την αξιοπιστία και αμεροληψία των αποτελεσμάτων όπως απεικονίζεται στο Guideline 6, σελ. 22-23
7. **Συνεχής Ενημέρωση για την εξέλιξη των απειλών και συνεχής εκπαίδευση:** Οι PSPs πρέπει να παρακολουθούν το τοπίο των απειλών, να συμμετέχουν στην ανταλλαγή πληροφοριών και να διασφαλίζουν ότι το προσωπικό είναι εκπαιδευμένο και ενήμερο για τους συνεχώς εξελισσόμενους κινδύνους ασφαλείας όπως παρουσιάζεται στο Guideline 7, σελ. 23-24
8. **Διαχείριση σχέσεων με τους χρήστες υπηρεσιών πληρωμών (PSUs):** Οι PSPs οφείλουν να ενισχύουν την ευαισθητοποίηση των χρηστών σχετικά με τους κινδύνους ασφάλειας και να παρέχουν σαφείς οδηγίες προκειμένου οι χρήστες να μπορούν να ορίζουν ειδοποιήσεις και να δημιουργούν ασφαλείς διαύλους επικοινωνίας και αναφοράς περιστατικών όπως παρουσιάζεται στο Guideline 8, σελ. 24-25.

Πιο συγκεκριμένα, το παραπάνω πρότυπο ορίζει για τους τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Payment Servicer Providers – PSPs) τις παρακάτω απαιτήσεις:

1. **Δημιουργία πλαισίου διαχείριση κινδύνων:** Οι TPPs οφείλουν να θεσπίσουν και να διατηρούν ένα πλαίσιο διαχείρισης κινδύνων που να καλύπτει όλες τις υπηρεσίες πληρωμών που παρέχουν, συμπεριλαμβανομένων εκείνων που αφορούν την πρόσβαση σε λογαριασμούς χρηστών καθώς και σε άλλα χρηματοοικονομικά ιδρύματα όπως παρουσιάζεται στο Guideline 1.1-1.3, σελ. 17-18.
2. **Όροι συμβάσεων με τρίτους:** Εάν οι TPPs αναθέτουν σε τρίτους παρόχους οποιοδήποτε μέρος των υπηρεσιών πληρωμών τους, τότε οφείλουν να διασφαλίζουν ότι τα security objectives και τα controls περιλαμβάνονται στις συμβάσεις και ότι η συμμόρφωση με αυτά παρακολουθείται ανά τακτά χρονικά διαστήματα Guideline 1.7-1.8, σελ. 18
3. **Έλεγχος προσβάσεων και προστασία δεδομένων:** Οι TPPs πρέπει να εφαρμόζουν αυστηρούς ελέγχους πρόσβασης προκειμένου να προστατεύουν τα ευαίσθητα δεδομένα πληρωμών και να διασφαλίζουν την ελαχιστοποίηση των δεδομένων που απαιτούνται για την παροχή των υπηρεσιών τους, ιδίως όταν διαχειρίζονται credentials χρηστών ή πραγματοποιούν πληρωμές για λογαριασμό χρηστών σύμφωνα με το Guideline 3.3-3.7, σελ. 19-20
4. **Ανίχνευση και αναφορά περιστατικών:** Οι TPPs πρέπει να διαθέτουν μηχανισμούς για την ανίχνευση, ταξινόμηση και αναφορά περιστατικών ασφάλειας, τόσο εσωτερικά όσο και στις αρμόδιες αρχές, όπως απαιτείται από το PSD2 και σύμφωνα με το Guideline 4.1-4.6, σελ. 20-21
5. **Πραγματοποίηση συνεχών δοκιμών και βελτιοποιήσεων:** Οι TPPs υποχρεούνται να δοκιμάζουν τακτικά τα μέτρα ασφαλείας τους προκειμένου να προσαρμόζονται συνεχώς στις νέες απειλές και να διασφαλίζουν την ανεξάρτητη επικυρωποίηση της ορθής λειτουργίας των ελέγχων ασφαλείας τους σύμφωνα με το Guideline 6.1-6.6, σελ. 22-23
6. **Οδηγίες επικοινωνίας χρηστών:** Οι TPPs πρέπει να παρέχουν σαφείς πληροφορίες στους χρήστες σχετικά με τους κινδύνους ασφάλειας, τις διαδικασίες αναφοράς περιστατικών καθώς και τα κανάλια επικοινωνίας όπως παρουσιάζεται στο Guideline 8.1-8.10, σελ. 24-25

2.6 Πρότυπο PCI DSS v4.0

2.6.1 Εισαγωγή

Το πρότυπο PCI DSS v4.0 (Payment Card Industry Data Security Standard) αποτελεί ένα παγκόσμιο σύνολο απαιτήσεων με κύριο σκοπό την προστασία των καρτικών δεδομένων και την ενίσχυση της προστασίας των συστημάτων πληρωμών από απάτες και παραβιάσεις – *PCI Security Standards Council [27]*. Το πρότυπο, αποτελείται από 12 βασικά requirements στα οποία περιλαμβάνουν υποενότητες μαζί με τα σχετικά testing procedures και οδηγίες εφαρμογής - *Arthur B. Cooper Jr, 2023 [28]*. Το PCI DSS v4.0 κυκλοφόρησε το 2024 και αντικατέστησε το προηγούμενο version του

προτύπου (PCI DSS v3.2) – *PCI Security Standards Council, 2022 [29]*, προσαρμοζόμενο με μεγαλύτερη ακρίβεια στην αντιμετώπιση των συνεχών εξελισσόμενων απειλών και τεχνολογιών στο χρηματοοικονομικό τομέα απαιτώντας παράλληλα από τους οργανισμούς την αναθεώρηση του τρόπου αναγνώρισης ρίσκων για την συμμόρφωση με το πρότυπο - Journal of Theoretical and Applied Information Technology, 2024 [30]. Τέλος, το συγκεκριμένο πρότυπο ισχύει για όλες τις χρηματοοικονομικές οντότητες που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν καρτικά δεδομένα συμπεριλαμβανομένων παρόχων υπηρεσιών και τρίτων παρόχων παροχής υπηρεσιών πληρωμών.

2.6.2 Επισκόπηση Προτύπων και Οδηγιών

Πιο συγκεκριμένα, το πρότυπο PCI DSS v4.0 – PCI Security Standards Council, 2022 [31] ορίζει για τους τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Payment Servicer Providers – PSPs) τις παρακάτω απαιτήσεις:

- Οι πάροχοι υπηρεσιών πρέπει πλέον να τεκμηριώνουν και να επιβεβαιώνουν το πεδίο εφαρμογής του PCI DSS τουλάχιστον κάθε έξι μήνες και μετά από σημαντικές αλλαγές (Requirement 12.5.2.1) και να επανεξετάζουν τον αντίκτυπο των οργανωτικών αλλαγών στο πεδίο εφαρμογής του PCI DSS (Requirement 12.5.3).
- Οι πάροχοι υπηρεσιών οφείλουν να χρησιμοποιούν Intrusion-detection/prevention τεχνικές για τον εντοπισμό καναλιών επικοινωνίας κακόβουλου λογισμικού (Requirement 11.5.1.1) και να υποστηρίζουν τους πελάτες στην πραγματοποίηση εξωτερικών penetration tests (Requirement 11.4.7).
- Τήρηση καταλόγου όλων των TPSPs με πρόσβαση σε καρτικά δεδομένα όπως ορίζεται στο Requirement 12.8.1 καθώς επίσης απαιτείται και η υπογραφή συμφωνιών που θα ορίζουν ξεκάθαρα τις αρμοδιότητες τόσο των TPSPs όσο και των οργανισμών ως προς την προστασία των πελατειακών στοιχείων (Requirement 12.8.2).
- Σύμφωνα με τα Requirements 12.8.4 και 12.9 οι TPSPs πρέπει να πιστοποιούν σε ετήσια βάση την συμμόρφωσή τους με την παροχή του σχετικού αποδεικτικού AoC (Attestation of Completion).
- Απαιτείται η χρήση MFA (multi factor authentication – MFA) όχι μόνο για την πρόσβαση των διαχειριστών (admins) στο περιβάλλον διαχείρισης καρτικών δεδομένων (cardholder data environment – CDE) αλλά και για όλους τους χρήστες απλούς και αναβαθμισμένων δικαιωμάτων (privileged) συμπεριλαμβανομένων των εξωτερικών συνεργατών. Με τον συγκεκριμένο τρόπο ένας οργανισμός μπορεί να διασφαλίσει ότι οι TPSPs που έχουν πρόσβαση σε συστήματα με ευαίσθητα δεδομένα, εφαρμόζουν ισχυρά μέτρα ταυτοποίησης.
- Διατήρηση ενός μητρώου ευθυνών που να απεικονίζει ποιες απαιτήσεις PCI DSS διαχειρίζεται κάθε TPSP, ποιες διαχειρίζεται ο οργανισμός και ποιες είναι κοινές σύμφωνα με το Requirement 12.8.5.

2.7 Berlin Group και πρότυπα NextGenPSD2 / OpenFinance API

2.7.1 Εισαγωγή

Το Berlin Group είναι μια ευρωπαϊκή πρωτοβουλία που επικεντρώνεται στη δημιουργία ανοικτών και κοινών προτύπων για τις χρηματοπιστωτικές υπηρεσίες, ιδίως στον τομέα των πληρωμών λαμβάνοντας υπόψιν την οδηγία της Ευρωπαϊκής Ένωσης για τις υπηρεσίες πληρωμών (PSD2), η οποία επιβάλλει στις τράπεζες (ASPSPs - Account Servicing Payment Service Providers) να παρέχουν πρόσβαση σε λογαριασμούς πελατών σε αδειοδοτημένους τρίτους παρόχους (TPPs) κατόπιν συγκατάθεσης του πελάτη. Το Berlin Group ιδρύθηκε το 2004 και αποτελεί έναν πανευρωπαϊκό συνασπισμό τραπεζών, σχημάτων πληρωμών και παρόχων υπηρεσιών πληρωμών με πρωταρχικό στόχο την διευκόλυνση της διαλειτουργικότητας και την εναρμόνιση στην ευρωπαϊκή αγορά πληρωμών. Πιο συγκεκριμένα, ο παραπάνω στόχος μπορεί να επιτευχθεί με την ανάπτυξη ανοικτών και τυποποιημένων τεχνικών προδιαγραφών που επιτρέπουν την ασφαλή και αποτελεσματική επικοινωνία μεταξύ διαφορετικών χρηματοπιστωτικών ιδρυμάτων και τρίτων παρόχων *The Berlin Group [32]*. Το πιο γνωστό έργο του Berlin Group είναι η ανάπτυξη του πλαισίου NextGenPSD2, το οποίο παρέχει ένα τυποποιημένο API (Application Programming Interface) για την πρόσβαση σε τραπεζικούς λογαριασμούς, όπως απαιτείται από την αναθεωρημένη οδηγία της ΕΕ για τις υπηρεσίες πληρωμών (PSD2). Αυτό το πρότυπο API έχει υιοθετηθεί ευρέως σε όλη την Ευρώπη και υποστηρίζει υπηρεσίες όπως πληροφορίες λογαριασμού και αυτοματοποιημένη έναρξη πληρωμών. Τέλος, το Berlin Group έχει δημιουργήσει και άλλα πρότυπα και best practices που σχετίζονται με την επεξεργασία πληρωμών, την ασφάλεια και τη συμμόρφωση τα οποία παρουσιάζονται λεπτομερώς παρακάτω:

2.7.2 Επισκόπηση Προτύπων

- Open Finance API Framework - *The Berlin Group,2024* [33]

Το συγκεκριμένο Framework, παρέχει ένα ολοκληρωμένο μοντέλο δεδομένων και code lists για το openFinance API, το οποίο αποτελεί την εξέλιξη του Berlin Group's NextGenPSD2 XS2A και απαιτεί από τους τρίτους παρόχους υπηρεσιών πληρωμών τα παρακάτω:

1. **Κατανόηση και Χρήση προκαθορισμένων κατηγοριών δεδομένων:** Οι TPPs πρέπει να χρησιμοποιούν τους τύπους δεδομένων που απεικονίζονται στο Section 2 για όλες τις αλληλεπιδράσεις με τις τράπεζες. Πιο συγκεκριμένα:

    - **Εντολές για πρόσβαση σε λογαριασμούς κατόπιν σχετικής συγκατάθεσης:** Οι TPPs πρέπει να διαμορφώνουν τα αιτήματα συγκατάθεσης χρησιμοποιώντας τους τύπους AccountAccess, AccountAccessRights όπως παρουσιάζεται στο Section 2.1–2.6 στις σελ. 4–7
    - **Εντολές για διαχείριση στοιχείων λογαριασμού και κάρτας:** Οι TPPs πρέπει να χειρίζονται τα δεδομένα λογαριασμού καθώς και τα καρτικά δεδομένα χρησιμοποιώντας τους τύπους AccountDetails,

CardAccountDetails όπως παρουσιάζονται στο Section 2.7, σελ.8 και Section 2.36, σελ. 27

- **Εντολές έναρξη πληρωμών:** Τα αιτήματα πληρωμής πρέπει να χρησιμοποιούν τους σωστούς τύπους δεδομένων πληρωμής, όπως PaymentProductJSON, PaymentProductXML τα οποία απεικονίζονται στα Sections 2.93–2.95, σελ. 75–77.
- **Εντολές αυθεντικοποίησης και SCA:** Οι TPPs πρέπει να υποστηρίζουν τα μέτρα αυθεντικοποίησης που ορίζονται στο Section 2.32–2.33, σελ. 24–25, συμπεριλαμβανομένων των μεθόδων SCA όπως SMS_OTP, CHIP_OTP, PHOTO_OTP

2. **Διαχωρισμός δικαιωμάτων πρόσβασης:** Οι TPPs πρέπει να καθορίζουν και να διαχειρίζονται τα δικαιώματα πρόσβασης για λογαριασμούς, κάρτες και δάνεια σύμφωνα με το Section 2.1-2.6, σελ. 4-7
3. **Χειρισμός σφαλμάτων:** Οι TPPs πρέπει να ερμηνεύουν και να χειρίζονται τις πληροφορίες σφάλματος χρησιμοποιώντας τους τύπους ErrorInformation και ClientMessageInformation όπως ορίζεται στο Section 2.44, σελ. 34 και Section 2.52, σελ. 38.
4. **Απαιτήσεις ασφάλειας και SCA:** Οι TPPs πρέπει να υποστηρίζουν την υπογραφή μηνυμάτων, τη διαχείριση πιστοποιητικών και τις προσεγγίσεις SCA, όπως ορίζεται στο ParametersAPISecurity σύμφωνα με το Section 2.73, σελ. 53. Επιπρόσθετα, όπως παρουσιάζεται στο Section 2.73, σελ. τα APIs υποστηρίζουν πολλαπλές προσεγγίσεις SCA όπως Redirect, Embedded, OAuth2, Decoupled και τα οποία οι TPPs θα πρέπει να είναι σε θέση να χειρίζονται με την χρήση κρυπτογράφησης.

- NextGen PSD2 Framework - *The Berlin Group, 2025* [34, 35]

Το NextGenPSD2, είναι μια πρωτοβουλία του Berlin Group, με στόχο τη δημιουργία ενός εναρμονισμένου, ανοιχτού και πανευρωπαϊκού προτύπου API για την ασφαλή και αποτελεσματική πρόσβαση σε τραπεζικούς λογαριασμούς σύμφωνα με την αναθεωρημένη οδηγία PSD2. Το πλαίσιο έχει σχεδιαστεί για να προωθήσει την καινοτομία και να απλοποιήσει τη συμμόρφωση για όλους τους οργανισμούς στο πεδίο εφαρμογής του, συμπεριλαμβανομένων των τραπεζών (ASPSPs), των TPPs και των τελικών χρηστών. Πιο συγκεκριμένα το framework NextGen PSD2 απαιτεί από τους παρόχους:

1. **Υιοθέτηση του τυποποιημένου API:** Οι TPPs πρέπει να χρησιμοποιούν το API NextGenPSD2 για να έχουν πρόσβαση σε πληροφορίες λογαριασμών, να πραγματοποιούν πληρωμές σε όλες τις συμμορφούμενες τράπεζες στην Ευρώπη όπως απεικονίζεται στο Κεφάλαιο "one implementation framework for all" στη σελίδα 2, ενότητα "With standardised API"
2. **Ασφάλεια και ταυτοποίηση:** Οι TPPs υποχρεούνται να χρησιμοποιούν πιστοποιητικά eIDAS QWAC για την ταυτοποίηση σε επίπεδο TLS και, προαιρετικά, πιστοποιητικά QSEAL σε επίπεδο εφαρμογής, εάν απαιτείται από τον ASPSP. Επιπρόσθετα, όλες οι επικοινωνίες πρέπει να διασφαλίζονται με την χρήση TLS 1.2 ή νεότερη όπως αναφέρεται

στο Κεφάλαιο "QWACS eIDAS certificates at TLS level" και "QSEALS eIDAS certificates at application level (at ASPSP discretion)" στη σελίδα 4, ενότητα "Security Features"

3. **Υποστήριξη βασικών υπηρεσιών: Οι TPPs πρέπει να υποστηρίζουν τις ακόλουθες υπηρεσίες σύμφωνα με την ενότητα *"NextGenPSD2 Core services"* στη σελίδα 3:**

    i. **AIS (Account Information Service):** Διαχείριση συγκατάθεσης, στοιχεία λογαριασμών και πραγματοποίηση συναλλαγών.
    ii. **PIS (Payment Initiation Service):** Έναρξη/ακύρωση πληρωμών.
    iii. **PIIS (Funds Confirmation Service):** Επιβεβαίωση διαθεσιμότητας funds.

4. **Μορφές δεδομένων και πρωτόκολλα:** Οι TPPs πρέπει να χρησιμοποιούν REST API με υποστήριξη HAL. Επιπρόσθετα, τα δεδομένα πρέπει να ανταλλάσσονται σε μορφές JSON ή XML, με βάση τα πρότυπα ISO 20022 σύμφωνα με την ενότητα *"REST with HAL support"*, *"JSON & XML"*, *"ISO 20022"* που απεικοίζεται στην σελίδα 3, ενότητα "Technical Characteristics".
5. **Ισχυρή επαλήθευση ταυτότητας πελάτη (SCA):** Οι TPPs πρέπει να υποστηρίζουν μηχανισμούς SCA όπως απαιτείται από τον ASPSP, συμπεριλαμβανομένων OAuth2/redirect μηχανισμών και decoupled και embedded τα οποία αναφέρονται στην Ενότητα *"Authorisation Protocol: OAuth2/redirect, decoupled, embedded"* στην σελίδα 3
6. **Τεκμηρίωση και συμμόρφωση:** Οι TPPs πρέπει να ακολουθούν τις τεχνικές προδιαγραφές και την καταγραφή σύμφωνα με τις οδηγίες του Berlin Group για την εφαρμογή των οδηγιών και τη συμμόρφωση όπως παρουσιάζεται στο κεφάλαιο *"Technical specifications available at https://www.berlin-group.org/psd2-access-to-bank-accounts"* στην σελίδα 4.

2.8 Πλαίσιο Ασφάλειας SWIFT (CSCF)

2.8.1 Εισαγωγή

Ένα ακόμα πρότυπο άξιο αναφοράς, είναι το SWIFT (Society for Worldwide Interbank Financial Telecommunication) το οποίο αποτελεί ένα παγκόσμιο δίκτυο ανταλλαγής μηνυμάτων που χρησιμοποιείται από τράπεζες και χρηματοπιστωτικά ιδρύματα για την ασφαλή αποστολή και λήψη πληροφοριών αναφορικά με χρηματοοικονομικές συναλλαγές. Πιο συγκεκριμένα, το SWIFT παρέχει controls για την παραμετροποίηση της SWIFT υποδομή τα οποία επιτρέπουν την ασφαλή ανταλλαγή μηνυμάτων πληρωμών μεταξύ των χρηματοπιστωτικών ιδρυμάτων σε όλο τον κόσμο - *Swift [36]*. Επιπρόσθετα, το "Swift Customer Security Controls Framework v2024" (CSCF v2024) – *Swift, 2024 [37]* είναι το επίσημο πλαίσιο ασφάλειας για όλους τους χρήστες του Swift, συμπεριλαμβανομένων τραπεζών, χρηματοπιστωτικών ιδρυμάτων και τρίτων παρόχων υπηρεσιών πληρωμών. Το πρότυπο, καθορίζει μια σειρά υποχρεωτικών και συμβουλευτικών controls για την προστασία του Swift περιβάλλοντος από απειλές στον κυβερνοχώρο, απάτες και μη εξουσιοδοτημένη πρόσβαση. Το πλαίσιο αποτελεί μέρος του ευρύτερου Προγράμματος Ασφάλειας Πελατών του Swift (CSP), το οποίο αποσκοπεί στη διασφάλιση ενός ασφαλούς

χρηματοοικονομικού οικοσυστήματος, απαιτώντας από όλους τους χρήστες να εφαρμόζουν βασικά μέτρα ασφαλείας και να πιστοποιούν τη συμμόρφωσή τους σε αυτά σε ετήσια βάση. Το CSCF είναι δομημένο γύρω από τρεις κύριους πυλώνες: 1) προστασία του περιβάλλοντος, 2) επίγνωση και περιορισμός της πρόσβασης, καθώς και 3) ανίχνευση και αντιμετώπιση. Τέλος, βασίζεται σε πρότυπα όπως το NIST, ISO 27000 και PCI-DSS και ενημερώνεται σε ετήσια βάση για να αντιμετωπίζει τις εξελισσόμενες απειλές στον κυβερνοχώρο και τις νέες τεχνολογίες.

2.8.2 Επισκόπηση πλαισίου

Πιο συγκεκριμένα, το πλαίσιο ορίζει για τους τρίτους παρόχους παροχής υπηρεσιών πληρωμών (Payment Servicer Providers – PSPs) τις παρακάτω απαιτήσεις:

1. **Outsourced Critical Activity Protection (Control 2.8):** το συγκεκριμένο control, είναι υποχρεωτικό για όλους τους τύπους αρχιτεκτονικής (A1, A2, A3, A4, B) και απαιτεί όταν κρίσιμες δραστηριότητες που σχετίζονται με το Swift ανατίθενται σε εξωτερικούς συνεργάτες, ο οργανισμός οφείλει να διασφαλίζει ότι ο πάροχος υπηρεσιών προστατεύει τις κρίσιμες δραστηριότητες με τα ίδια security controls βάση CSCF με αυτά που θα απαιτούνταν αν η δραστηριότητα διαχειριζόταν εσωτερικά. Επιπρόσθετα, πρέπει να υπάρχουν συμφωνίες SLA και συμφωνίες NDA με τους τρίτους παρόχους καθώς επίσης θα πρέπει να διενεργείται και έναrisk assessment στον πάροχο κατά την έναρξη του έργου και ανά τακτά χρονικά διαστήματα.
2. **Attestation and Compliance:** Όλοι οι οργανισμοί, συμπεριλαμβανομένων εκείνων που χρησιμοποιούν τρίτους παρόχους, πρέπει να πιστοποιούν τη συμμόρφωση με τους υποχρεωτικούς ελέγχους ετησίως μέσω της εφαρμογής KYC Security Attestation (KYC-SA). Επιπρόσθετα, οι οργανισμοί πρέπει να δηλώνουν τον τύπο της αρχιτεκτονικής τους και να διασφαλίζουν ότι καλύπτονται όλα τα controls που εμπίπτουν στο πεδίο εφαρμογής, συμπεριλαμβανομένων εκείνων που διαχειρίζονται τρίτοι
3. **Πραγματοποίηση τεχνικών ελέγχων:** Τα controls Vulnerability Scanning (2.7), System Hardening (2.3), Security Updates (2.2) και Physical Security (3.1) ισχύουν και για τα περιβάλλοντα που έχουν ανατεθεί σε εξωτερικό συνεργάτη και απαιτούν από τους οργανισμούς να διασφαλίζουν ότι οι τρίτοι εφαρμόζουν τα μέτρα ασφαλείας που απεικονίζονται στο CSCF. Αντίστοιχα, στα controls Logical Access Control (5.1), Multi-Factor Authentication (4.2), και Logging and Monitoring (6.4) πρέπει να εφαρμόζονται σε όλα τα συστήματα που σχετίζονται με το Swift, συμπεριλαμβανομένων εκείνων που διαχειρίζονται από τρίτους παρόχους.

3

Συγκριτική Ανάλυση Κανονισμών και Τεχνικών Πλαισίων

3.1 Συγκριτικός Πίνακας Κανονισμών και Τεχνικών Απαιτήσεων

Η ανάλυση των κανονιστικών και τεχνικών πλαισίων που διέπουν τη λειτουργία των Τρίτων Παρόχων Υπηρεσιών Πληρωμών (TPPs) στον τραπεζικό τομέα αναδεικνύει σημαντικές ομοιότητες αλλά και διαφορές ως προς τις απαιτήσεις ασφάλειας, συμμόρφωσης και διακυβέρνησης. Στο πλαίσιο αυτό, ο συγκριτικός πίνακας που ακολουθεί συνοψίζει τα βασικά χαρακτηριστικά και τις απαιτήσεις των κυριότερων κανονισμών και προτύπων που εφαρμόζονται στον ευρωπαϊκό και βρετανικό χώρο, όπως η οδηγία PSD2, τα EBA Guidelines, το πρότυπο PCI DSS v4.0 και άλλα.

Πλαίσιο/ Κανονισμός	Ισχυρή Αυθεντικοποίηση (SCA)	Ασφαλή APIs & Κανάλια	Αναφορά Περιστατικών & Συμμόρφωση	Προστασία Δεδομένων & Ιχνηλασιμότητα	Μηχανισμοί Πιστοποίησης & Τεχνική Εποπτεία
PSD2	Απαιτεί την εφαρμογή ισχυρής ταυτοποίησης πελάτη (SCA) για όλες τις ηλεκτρονικές συναλλαγές, με εξαίρεσή του μόνο σε χαμηλού κινδύνου συναλλαγές και τη χρήση αυθεντικοποίησης MFA	Υποχρεώνει τη χρήση ασφαλών APIs με κρυπτογράφηση και πιστοποιητικών eIDAS για την ανταλλαγή δεδομένων	Επιβάλλει την υποχρεωτική αναφορά περιστατικών ασφαλείας και την διενέργεια τακτικών ελέγχων	Απαιτεί ρητή συγκατάθεση του χρήστη για την επεξεργασία δεδομένων, ελαχιστοποι-ώντας έτσι τα συλλεγόμενων δεδομένων καθώς επίσης απαιτεί και την καταγραφή των προσβάσεων	Προβλέπει ετήσιες αξιολογήσεις και ανεξάρτητους ελέγχους για τη συμμόρφωση με τα Regulatory Technical Standards (RTS)
EBA Guidelines/RTS	Απαιτεί την εφαρμογή SCA και MFA, τη διαχείριση credentials	Προβλέπει τη χρήση ασφαλών APIs και	Απαιτεί την υποχρεωτική αναφορά	Εστιάζει στην ελαχιστοποίηση των συλλεγόμενων	Απαιτεί την συνεχή αξιολόγηση, την πραγματοποίηση

	και την τακτική αξιολόγηση κινδύνων	κρυπτογράφη-σης, καθώς και συγκεκριμένες τεχνικές προδιαγραφές για την επικοινωνία	περιστατικών ασφαλείας και τη διαχείριση των λειτουργικών κινδύνων	δεδομένων καθώς και στην προστασία τους λαμβάνοντας πάντα υπόψιν την συγκατάθεσή του χρήστη για τις παρεχόμενες υπηρεσίες	ανεξάρτητων εξωτερικών ελέγχων και την πλήρη συμμόρφωση με τους κανονισμούς
Open Banking Standard	Απαιτεί την υλοποίηση SCA μέσω OAuth2, embedded ή decoupled μηχανισμών και την υποχρεωτική ταυτοποίηση των χρηστών	Προβλέπει τη χρήση τυποποιημένων APIs καθώς και την χρησιμοποίηση ασφαλών καναλιών επικοινωνίας με την χρήση κρυπτογράφησης	Επιβάλλει την καταγραφή και την διαχείριση σφαλμάτων, καθώς και τη συμμόρφωση με το GDPR	Απαιτεί ρητή συγκατάθεση του χρήστη, με διαχωρισμό των καθημερινών και των privileged δικαιωμάτων πρόσβασης	Απαιτεί εγγραφή σε μητρώα καθώς επίσης και την πραγματοποίηση penetration tests και συμμόρφωση με τα πρότυπα του OBIE.
PCI DSS v4.0	Απαιτεί τη χρήση MFA για όλους τους χρήστες και διαχειριστές, καθώς και αυστηρό έλεγχο πρόσβασης στα συστήματα	Προβλέπει τη χρήση ασφαλών καναλιών επικοινωνίας, τεχνικών ανίχνευσης εισβολών και τακτικών penetration tests	Υποχρεώνει στην καταγραφή και αναφορά περιστατικών ασφαλείας, στη διατήρηση αρχείων και σε τακτικούς ελέγχους	Εστιάζει στην ελαχιστοποίηση και προστασία των καρτικών δεδομένων και στην καταγραφή των ευθυνών κάθε εμπλεκόμενου	Απαιτεί ετήσια πιστοποίηση, με την συμπλήρωση και κατάθεση του Attestation of Compliance (AoC) καθώς και την πραγματοποίηση εξωτερικών ελέγχων.
Berlin Group	Απαιτεί την υποστήριξη SCA μέσω OAuth2, embedded ή decoupled μηχανισμών και τη χρήση πιστοποιητικών eIDAS QWAC/QSEAL	Προβλέπει τη χρήση τυποποιημένων APIs με την υλοποίηση υποχρεωτικής κρυπτογράφησης και ανταλλαγής δεδομένων σε μορφές	Υποχρεώνει στην καταγραφή και διαχείριση σφαλμάτων	Απαιτεί ρητή συγκατάθεση του χρήστη και διαχωρισμό των δικαιωμάτων πρόσβασης	Απαιτεί συμμόρφωση με τεχνικές προδιαγραφές καθώς και το ISO 20022

		REST/JSON/XML			
SWIFT CSCF	Απαιτεί τη χρήση MFA για την πρόσβαση σε συστήματα με τον αυστηρό έλεγχο ταυτότητας	Προβλέπει υποχρεωτική κρυπτογράφηση, system hardening και τακτικό vulnerability scanning	Υποχρεώνει σε ετήσια αναφορά συμμόρφωσης (KYC-SA) και την ύπαρξη SLAs με τρίτους παρόχους	Απαιτεί την λεπτομερή καταγραφή των προσβάσεων και την πραγματοποίηση risk assessment	Προβλέπει ετήσια πιστοποίηση καθώς και την πραγματοποίηση τεχνικών ελέγχων.
PSR	Απαιτεί την εφαρμογή SCA/MFA και συμμόρφωση με το πλαίσιο PSD2, καθώς και αυστηρό έλεγχο ταυτοποίησης	Προβλέπει τη χρήση ασφαλών APIs και συμμόρφωση με τα πρότυπα του Open Banking	Υποχρεώνει σε αναφορά περιστατικών ασφαλείας στην FCA και τακτική ενημέρωση των αρχών για κάθε ουσιαστική αλλαγή	Εστιάζει στην προστασία των κεφαλαίων των χρηστών, στη συμμόρφωση με το GDPR και στη διαφάνεια προς τους καταναλωτές	Απαιτεί εγγραφή και αδειοδότηση από την FCA, καθώς και τακτικούς εσωτερικούς και εξωτερικούς ελέγχους.

3.2 Συγκρίσεις ανά τομέα:

3.2.1 Ισχυρή Αυθεντικοποίηση (SCA)

Η ισχυρή ταυτοποίηση πελάτη (Strong Customer Authentication – SCA) είναι μία απαίτηση ασφαλείας της αναθεωρημένης οδηγίας PSD2 που έχει ως κύριο στόχο την αύξηση της ασφάλειας των ηλεκτρονικών πληρωμών μειώνοντας ταυτόχρονα όσο το δυνατόν περισσότερο την δυνατότητα ηλεκτρονικών απατών. Το SCA όπως ορίζεται στο άρθρο 4(30) του PSD2, είναι ένα multi factor authentication το οποίο βασίζεται στη χρήση δύο ή περισσότερων διαπιστευτηρίων για την αυθεντικοποίηση του χρήστη και την πραγματοποίηση συναλλαγών όπως παρουσιάζεται στο παρακάτω διάγραμμα:

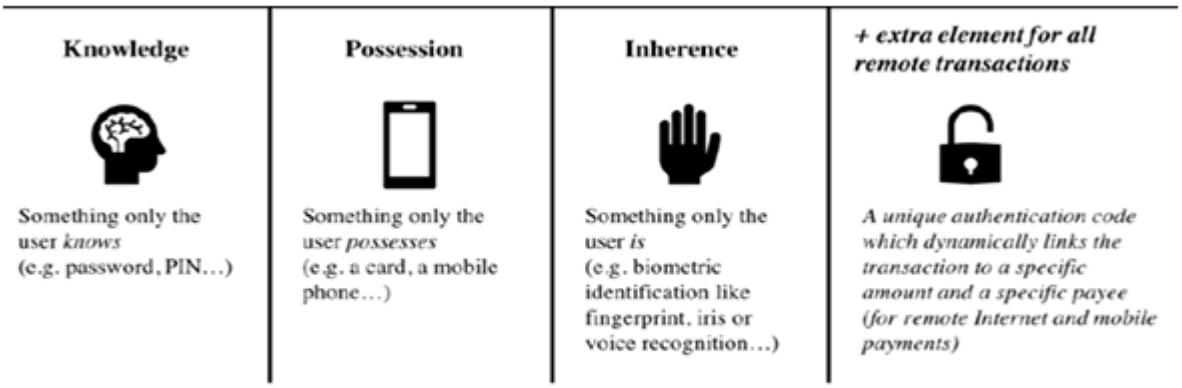


Figure 3. Factors for strong customer authentication. Source: Eide&Hallum (2018)

Εικόνα 4: (SCA) - *Journal of Process Management, 2020 [38]*

Τα παραπάνω στοιχεία είναι ανεξάρτητα, το οποίο σημαίνει ότι η παραβίαση ενός διαπιστευτηρίου δεν θέτει σε κίνδυνο την αξιοπιστία των άλλων διασφαλίζοντας με αυτόν τον τρόπο την εμπιστευτικότητα. Απαιτώντας την πολυπαραγοντική επαλήθευση ταυτότητας, το SCA προσθέτει ένα επιπλέον επίπεδο ασφάλειας στις ηλεκτρονικές συναλλαγές, διασφαλίζοντας ότι μόνο ο νόμιμος κάτοχος της κάρτας μπορεί να πραγματοποιεί αγορές αυξάνοντας με αυτόν τον τρόπο την προστασία τόσο των καταναλωτών όσο και των επιχειρήσεων από κακόβουλες ενέργειες.

3.2.2 Ασφαλή APIs και κανάλια επικοινωνίας

Με τον όρο ασφαλή APIs και κανάλια επικοινωνίας αναφερόμαστε στη χρήση ισχυρών μέτρων ασφαλείας για την προστασία της ανταλλαγής δεδομένων μεταξύ διαφορετικών εφαρμογών λογισμικού και συστημάτων. Πιο συγκεκριμένα μερικά μέτρα προστασίας μπορεί να είναι η εφαρμογή πρωτοκόλλων όπως HTTPS, κρυπτογράφηση όπως SSL/TLS και ισχυρές μεθόδους ελέγχου ταυτότητας, ώστε να διασφαλίζεται ότι τα δεδομένα που μεταδίδονται μέσω API παραμένουν εμπιστευτικά και δεν μπορούν να υποκλαπούν ή να παραποιηθούν από μη εξουσιοδοτημένους χρήστες. Αντίστοιχα για την διασφάλιση της ακεραιότητας των APIs μπορούν να εφαρμοστούν μέτρα όπως έλεγχος πρόσβασης, επικύρωση στοιχείων εισόδου και τακτικές δοκιμές ασφαλείας για την πρόληψη ευπαθειών και επιθέσεων, όπως data breaches ή επιθέσεις man-in-the-middle. Με τις παραπάνω μεθόδους, οι οργανισμοί μπορούν να προστατεύουν ευαίσθητες πληροφορίες διατηρώντας παράλληλα την εμπιστοσύνη των χρηστών και την συμμόρφωσή τους με κανονιστικές απαιτήσεις. - *Journal of Computing and Information Technology, 2024 [39]*

3.2.3 Αναφορές περιστατικών και διακυβέρνηση συμμόρφωσης

Η αναφορά περιστατικών και η διακυβέρνηση συμμόρφωσης αναφέρονται στις δομημένες διαδικασίες και πολιτικές που χρησιμοποιεί ένας οργανισμός για τον εντοπισμό, την καταγραφή και την αντιμετώπιση περιστατικών ασφαλείας, διασφαλίζοντας παράλληλα τη συμμόρφωση με τις νομικές και κανονιστικές απαιτήσεις. Πιο συγκεκριμένα, τα κύρια στοιχεία που πρέπει να καλύπτονται είναι η άμεση ανίχνευση και αναφορά παραβιάσεων ή ύποπτων δραστηριοτήτων, η καταγραφή αρχείου με τα περιστατικά ασφαλείας και η αναφορά των βημάτων αντιμετώπισης που πρέπει να ακολουθηθούν σε περίπτωση κάποιου incident. Με τον όρο διακυβέρνηση συμμόρφωσης έχουμε ως κύριο σκοπό την διασφάλιση ότι οι παραπάνω πολιτικές, διαδικασίες, κλπ είναι σύμφωνες με διεθνή και ευρωπαϊκά πρότυπα όπως το GDPR και το PCI DSS, απαιτώντας παράλληλα των καθορισμό σαφών ορισμένων ρόλων και αρμοδιοτήτων. Η αποτελεσματική αναφορά περιστατικών και η διακυβέρνηση συμμόρφωσης βοηθούν έναν οργανισμό να ελαχιστοποιεί τους κινδύνους ασφαλείας, προστατεύοντας παράλληλα ευαίσθητα δεδομένα εξασφαλίζοντας παράλληλα την συμμόρφωση με διεθνής πρότυπα αυξάνοντας έτσι την εμπιστοσύνη των πελατών τους – *vcomply [40]*

3.2.4 Συγκατάθεση, ελαχιστοποίηση δεδομένων και ιχνηλασιμότητα

Η συγκατάθεση, η ελαχιστοποίηση των δεδομένων και η ιχνηλασιμότητα είναι βασικές αρχές της προστασίας των δεδομένων και της ιδιωτικής ζωής. Πιο συγκεκριμένα, η συγκατάθεση αναφέρεται στην απόκτηση ρητής άδειας από ένα άτομο πριν από τη συλλογή, την επεξεργασία ή την κοινοποίηση των προσωπικών τους δεδομένων το οποίο θα πρέπει να υλοποιείται με την ελαχιστοποίηση συλλογής προσωπικών δεδομένων μόνο σε όσα είναι απαραίτητα για την παροχή των συμφωνημένων υπηρεσιών. Τέλος, η ιχνηλασιμότητα διασφαλίζει ότι οι δραστηριότητες επεξεργασίας δεδομένων μπορούν να παρακολουθούνται και να ελέγχονται, παρέχοντας ένα σαφές αρχείο του τρόπου με τον οποίο χειρίζονται τα δεδομένα από τη συλλογή έως τη διαγραφή τους. Με τις παραπάνω πρακτικές, ένας οργανισμός μπορεί να ενισχύσει τη διαφάνεια, την προστασία της ιδιωτικότητας και την διασφάλιση ενός πλαισίου ορθής διαχείρισης των δεδομένων εντός ενός οργανισμού. – *usercentrics [41]*

3.2.5 Μηχανισμοί πιστοποίησης και τεχνική εποπτεία

Οι μηχανισμοί πιστοποίησης και η τεχνική εποπτεία αποτελούν βασικά στοιχεία ενός ισχυρού πλαισίου ασφάλειας και συμμόρφωσης με κανονιστικές απαιτήσεις. Πιο συγκεκριμένα, οι μηχανισμοί πιστοποίησης περιλαμβάνουν τη χρήση αναγνωρισμένων προτύπων και ανεξάρτητων αξιολογήσεων για την πιστοποίηση ότι τα συστήματα, οι διαδικασίες και τα συστήματα ενός οργανισμού πληρούν τις απαραίτητες απαιτήσεις ασφάλειας και απορρήτου. Για παραδείγματα, το πρότυπο ISO/IEC 27001:2022 απαιτεί την δημιουργία ενός ασφαλούς Information Security Management System (ISMS) και το PCI DSS αντίστοιχα ορίζει απαιτήσεις για την προστασία των καρτικών δεδομένων κατά την διάρκεια διαδικτυακών πληρωμών. Η τεχνική εποπτεία αναφέρεται στη συνεχή παρακολούθηση και αξιολόγηση των συστημάτων μέσω

αυτοματοποιημένων εργαλείων, εσωτερικών επιθεωρήσεων και ανεξάρτητων εξωτερικών, με σκοπό τη διασφάλιση της συνεχούς συμμόρφωσης και τον εντοπισμό πιθανών τρωτών σημείων ή αποκλίσεων από τα καθιερωμένα πρότυπα. Οι προαναφερόμενες πρακτικές εξασφαλίζουν σε ένα οργανισμό την διατήρηση της εμπιστοσύνης με τους πελάτες και τις ρυθμιστικές αρχές, αποδεικνύοντας τη δέσμευσή τους για τη διατήρηση υψηλών επιπέδων ασφαλείας και την ακεραιότητα της λειτουργίας των συστημάτων τους.- GDPR Learning Hub *[42]*

3.3 Συγκλίσεις και αποκλίσεις μεταξύ ΕΕ και Ηνωμένου Βασιλείου

Η σχέση μεταξύ της Ευρωπαϊκής Ένωσης και του Ηνωμένου Βασιλείου διαταράχτηκε ειδικά μετά το Brexit που πραγματοποιήθηκε τον Ιανουάριο του 2020, επηρεάζοντας μεταξύ άλλων και τους τομείς των χρηματοπιστωτικών απαιτήσεων, της απαιτήσεις προστασίας των δεδομένων καθώς και τους εποπτικούς φορείς. Πιο συγκεκριμένα, η ΕΕ και το Ηνωμένο Βασίλειο, συνεχίζουν να μοιράζονται πολλές θεμελιώδεις αρχές και ρυθμιστικά πλαίσια όπως για παράδειγμα τον ευρωπαϊκό Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) τον οποίο έχει διατηρήσει και προσαρμόσει στα δικά της μέτρα η Αγγλία, εξασφαλίζοντας με αυτό τον τρόπο υψηλό επίπεδο προστασίας δεδομένων και διευκόλυνση της ανταλλαγής δεδομένων μεταξύ των δύο περιοχών. Επιπρόσθετα, η Αγγλία έχει υιοθετήσει και συνεχίζει να ευθυγραμμίζεται με βασικά πρότυπα της ΕΕ, όπως το PSD2 για τις υπηρεσίες πληρωμών, τα Open Banking Standards και τεχνικά πλαίσια ασφαλείας όπως το PCI DSS και το SWIFT. Τέλος ένα κύριο μέλημα και των δύο είναι η χρήση ισχυρής ταυτοποίησης πελάτη SCA), η ασφάλεια των APIs και η τυποποιημένη διαδικασία αναφορά περιστατικών, εξασφαλίζοντας έτσι την προστασία των καταναλωτών. Παρόλο τα πρότυπα που αναλύσαμε παραπάνω και εξακολουθούν να υλοποιούνται από κοινού τόσο στην Αγγλία όσο και στην ΕΕ, έχουν διαπιστωθεί και αρκετές αποκλίσεις καθώς το Ηνωμένο Βασίλειο είναι στην διαδικασία δημιουργίας δικού της αυτόνομου εποπτικού μηχανισμού. Πιο συγκεκριμένα, το Ηνωμένο Βασίλειο έχει πλέον την ευελιξία να προσαρμόζεται ή να αποκλίνει από τους κανόνες της ΕΕ, ώστε να ανταποκρίνεται καλύτερα στους δικούς του στόχους σε επίπεδο αγοράς και υλοποίησης μέτρων ασφαλείας. Ένα σημαντικό παράδειγμα, αποτελεί ότι ενώ στην ΕΕ συνεχίζεται να αναπτύσσονται και να εφαρμόζονται EBA Guidelines και Berlin Group standards για τις πανευρωπαϊκές πληρωμές, το Ηνωμένο Βασίλειο έχει επιλέξει να μην εφαρμόσει τα παραπάνω ορίζοντας αυτόνομα χρονοδιαγράμματα. Επιπρόσθετα, το UK's Open Banking standard, παρόλο που αρχικά είχε βασιστεί πάνω στο PSD2, έχει εξελιχθεί με την χρήση αυτόνομών προτ΄πων διακυβέρνισης και τεχνικών προτύπων. Με τον παραπάνω διαχωρισμό μπορεί πλέον το Ηνωμένο Βασίλειο να διαπραγματεύεται τις δικές του διεθνείς συμφωνίες μεταφοράς δεδομένων και να εισάγει νέες κανονιστικές απαιτήσεις ή εποπτικές πρακτικές διαφορετικές από τις αντίστοιχες της ΕΕ. – *UK in A changing Europe, 2025 [43]*

3.4 Προκλήσεις εναρμόνισης και διαλειτουργικότητας

Η εναρμόνιση και η διαλειτουργικότητα αποτελούν θεμελιώδεις προϋποθέσεις για την ομαλή λειτουργία του σύγχρονου χρηματοοικονομικού οικοσυστήματος, ειδικά στο πλαίσιο της ενσωμάτωσης των Τρίτων Παρόχων Υπηρεσιών Πληρωμών (TPPs) στις τραπεζικές υποδομές. Παρά την ύπαρξη κοινών κανονιστικών πλαισίων, όπως το PSD2, τα EBA Guidelines, το Open Banking και τα τεχνικά πρότυπα Berlin Group, η πρακτική εφαρμογή τους παρουσιάζει σημαντικές δυσκολίες και προκλήσεις. Μία από τις βασικότερες προκλήσεις αφορά τις αποκλίσεις στην υλοποίηση των τεχνικών προτύπων και των APIs μεταξύ διαφορετικών τραπεζών και TPPs. Για παράδειγμα, ενώ το Berlin Group NextGenPSD2 API έχει υιοθετηθεί ευρέως στην Ευρώπη, κάθε τράπεζα μπορεί να εφαρμόζει διαφορετικές εκδοχές ή να προσθέτει επιπλέον παραμέτρους, με αποτέλεσμα οι TPPs να χρειάζεται να προσαρμόζουν τα συστήματά τους ξεχωριστά για κάθε οργανισμό. Αυτό αυξάνει το κόστος ανάπτυξης και συντήρησης, ενώ συχνά οδηγεί σε καθυστερήσεις στην υλοποίηση νέων υπηρεσιών. Αντίστοιχα, στο Ηνωμένο Βασίλειο, το Open Banking Standard έχει δώσει έμφαση στη διαλειτουργικότητα μέσω τυποποιημένων APIs, ωστόσο και εκεί παρατηρούνται διαφορές στην υλοποίηση μεταξύ των μεγάλων τραπεζών (CMA9) και των μικρότερων ιδρυμάτων. Επιπρόσθετα, ένα άλλο χαρακτηριστικό πρόβλημα παρουσιάζεται στην διαχείριση της ισχυρής ταυτοποίησης πελάτη (SCA). Παρότι το PSD2 ορίζει συγκεκριμένες απαιτήσεις για το SCA, ο τρόπος με τον οποίο υλοποιείται (π.χ. μέσω SMS OTP, mobile app push notifications, hardware tokens) διαφέρει σημαντικά μεταξύ τραπεζών και χωρών. Αυτό δημιουργεί εμπόδια τόσο για τους τελικούς χρήστες, που συχνά αντιμετωπίζουν διαφορετικές εμπειρίες ανάλογα με τον πάροχο, όσο και για τους TPPs που καλούνται να υποστηρίξουν πολλαπλές μεθόδους ταυτοποίησης. Επιπλέον, η κατάσταση περιπλέκεται ακόμα περισσότερο από τις διαφορές μεταξύ των ευρωπαϊκών και βρετανικών προτύπων, ειδικά μετά το Brexit. Ενώ η Ευρωπαϊκή Ένωση και το Ηνωμένο Βασίλειο διατηρούν κοινές βασικές αρχές (όπως το GDPR και το PSD2), το Ηνωμένο Βασίλειο έχει πλέον τη δυνατότητα να προσαρμόζει ή να αποκλίνει από τα ευρωπαϊκά πρότυπα, εισάγοντας δικές του τεχνικές και εποπτικές απαιτήσεις. Για παράδειγμα, το UK Open Banking Standard έχει εξελιχθεί με αυτόνομους κανόνες διακυβέρνησης και τεχνικές προδιαγραφές, ενώ παράλληλα το Ηνωμένο Βασίλειο έχει τη δυνατότητα να διαπραγματεύεται ξεχωριστές διεθνείς συμφωνίες μεταφοράς δεδομένων. Αυτό έχει ως αποτέλεσμα την εμφάνιση διαφορετικών χρονοδιαγραμμάτων υλοποίησης, διαφορετικών μηχανισμών διακυβέρνησης και τεχνικών προδιαγραφών, γεγονός που δυσχεραίνει την πλήρη διαλειτουργικότητα μεταξύ των συστημάτων. Επιπρόσθετα, σε διεθνές επίπεδο, η έλλειψη παγκόσμιων προτύπων για το Open Banking και τις υπηρεσίες πληρωμών αποτελεί σημαντικό εμπόδιο καθώς για παράδειγμα, στις ΗΠΑ δεν υπάρχει ενιαίο κανονιστικό πλαίσιο για το Open Banking, με αποτέλεσμα κάθε τράπεζα ή πάροχος να εφαρμόζει δικά του APIs και διαδικασίες, γεγονός που περιορίζει τη διαλειτουργικότητα και την καινοτομία. Επιπλέον, η ανάγκη για συνεχή συμμόρφωση με πολλαπλά και συχνά μεταβαλλόμενα πρότυπα (όπως PCI DSS, SWIFT CSCF, EBA Guidelines) απαιτεί από τους οργανισμούς σημαντικούς πόρους για την παρακολούθηση, την υλοποίηση και τον έλεγχο των απαιτήσεων. Η έλλειψη ενιαίας εποπτείας και η απουσία πλήρους εναρμόνισης οδηγούν σε αυξημένο λειτουργικό και κανονιστικό κόστος, ενώ παράλληλα ενισχύουν τον κίνδυνο για κενά ασφάλειας και ασυνέπειες στη διαχείριση των δεδομένων. Τέλος, η διαλειτουργικότητα δεν αφορά μόνο τα τεχνικά συστήματα, αλλά και τις επιχειρησιακές διαδικασίες και τα μοντέλα διακυβέρνησης. Η έλλειψη κοινών προτύπων για τη διαχείριση περιστατικών ασφαλείας, την ανταλλαγή πληροφοριών και την πιστοποίηση των TPPs μπορεί να οδηγήσει σε καθυστερήσεις στην απόκριση σε περιστατικά και σε μειωμένη εμπιστοσύνη των χρηστών.

4

Επιπτώσεις στην Κυβερνοασφάλεια και τη Διακυβέρνηση Πληρωμών

4.1 Αντιστοίχιση κανονιστικών απαιτήσεων με μηχανισμούς ασφαλείας

#	Security Mechanism / Control Area	PSD2/ UK PSR	PCI DSS v4.0	Open Banking (OBIE v3.1 / FAPI)	EBA ICT-&-Security GL 2019/04 (plus Outsourcing GL 2019/02)	SWIFT CSP (Mandatory Controls)
1	Strong Customer Authentication (MFA) & unique IDs	Dir. 2015/2366 Art 97; RTS Arts 4-10. UK PSR Reg 98(3)	Req 8.4–8.6	OBIE Security Profile §2.3; FAPI §5; OAuth 2.0 + OIDC; OBWAC certs	§5.8.3 (Access Control)	2.4 (MFA for users), 2.3 (password policy)
2	Dynamic Linking / Transaction integrity	RTS Arts 5-7 (link payee + amount)	Req 3.4.2 (hashing & integrity of CHD)	FAPI §7 (JWS request/response signing)	§5.8.4 (Data integrity)	Messages inherently signed; complements Segregated Zone 1
3	Encryption of data in transit	RTS Art 35 (CSC via secure channels)	Req 4.2.1 (TLS 1.2+), Req 12.3.3 (crypto inventory)	OBIE mandates mTLS (OBWAC); FAPI §8	§5.8.4 (b)	1.1, 1.2 (segmented secure zone with encrypted channels)

4	Encryption / tokenisation of data at rest	Dir. Art 95(1)(a) high-level requirement	Req 3.5–3.7 (AES-256 or better, key mgmt)	Data at rest encrypted as per OBIE Security Profile §3	§5.8.4 (a); Outsourcing GL §13(f)	3.1 (protect SWIFT-related data)
5	Network segmentation & secure zones	RTS Art 22 (risk-based exemptions need network protections)	Req 1.2.7 (segmentation), Req 1.3.1 (DMZ)	OBIE requires separate API gateway tier	§5.9.3 (network architecture)	1.1, 1.2 (SWIFT zone isolation & firewalls)
6	Secure API gateway / certificate-based auth	RTS Arts 30-36 (Common Secure Comm.)	— (outside PCI scope unless API handles CHD)	OBIE API Gateway + OBWAC/X-509 mutual certs; OIDC dynamic registration	§5.9.3	1.1 (segmentation) + 2.1 (restrict Internet access)
7	Malware / endpoint protection	RTS Art 9(3)(d) (device compromise checks)	Req 5.2–5.4 (AV/EDR)	OBIE Security §2.6 (TPP endpoints hygiene)	§5.10.2 (Protective measures)	2.7 (Malware protection)
8	Patch & vulnerability management	RTS Art 12 (security updates)	Req 6.3.1–6.3.3 (vuln mgmt), Req 11.3 (scans), Req 11.6 (pentest)	OBIE change mgmt §2.8	§5.10.3 & §5.11 (Vuln mgmt + testing)	3.2 (applicable security updates)
9	Logging, monitoring & anomaly detection	RTS Art 18 (logging for audit) & Art 34 (TPP monitoring)	Req 10.2–10.7 (log retention, SIEM)	OBIE Event & Audit Framework	§5.12.1 (Logging & monitoring)	4.2 (log security events), 6.4 (anomaly detection)
10	Incident response & regulatory reporting	Dir. Art 96; RTS Art 33; UK PSR Regs 99-100	Req 12.10 (IR plan)	OBIE §2.9 (major incident comms)	§5.12.2 (Incident mgmt); Outsourcing §13(k)	5.4 (IR plans)
11	Secure SDLC & code review	RTS Art 9(2) (secure design)	Req 6.2, 6.4, 6.5 (SDLC, SAST/DAST)	OBIE §2.7 (secure code)	§5.10.5 (Change & project mgmt)	6.5 (system hardening includes secure build)

12	Physical security	Dir. Art 95(1)(c) (protect devices & data)	Req 9.1–9.5	— (handled by banks)	§5.9.2	7.1 (secure locations)
13	Third-party / outsourcing controls	Dir. Art 19(6), 34(1)	Req 12.8 (service-provider mgmt)	OBIE: TPP onboarding criteria	EBA Outsourcing GL 2019/02 (entire); ICT §5.13	8.1 (critical service provider security)
14	Customer awareness & training	Dir. Art 94(2) PSD2	Req 12.6	OBIE §4 (customer education)	§5.14 (Awareness)	3.4 (security awareness)

4.2 Ενσωμάτωση σε ISMS και πλαισίωση βάσει ISO 27001 / NIST 800-53

Η αποτελεσματική διαχείριση της ασφάλειας πληροφοριών στις υποδομές τρίτων παρόχων στον τραπεζικό τομέα προϋποθέτει την υιοθέτηση ενός ολοκληρωμένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS - Information Security Management System). Το ISMS αποτελεί το θεμέλιο για τη συστηματική προσέγγιση στην προστασία των δεδομένων, τη διαχείριση κινδύνων και τη συμμόρφωση με κανονιστικά πλαίσια, όπως το ISO/IEC 27001 και το NIST SP 800-53. Πιο συγκεκριμένα, η ενσωμάτωση των απαιτήσεων των PSD2, EBA Guidelines, Open Banking, PCI DSS και άλλων προτύπων σε ένα ISMS διασφαλίζει ότι οι πολιτικές, οι διαδικασίες και οι τεχνικοί έλεγχοι που εφαρμόζονται είναι εναρμονισμένοι με τις διεθνείς βέλτιστες πρακτικές. Το ISMS, σύμφωνα με το ISO 27001, περιλαμβάνει τη διαχείριση κινδύνων, τον καθορισμό ρόλων και αρμοδιοτήτων, την εφαρμογή ελέγχων πρόσβασης, την προστασία δεδομένων, την ανίχνευση και αναφορά περιστατικών, καθώς και τη συνεχή βελτίωση μέσω τακτικών ελέγχων και αναθεωρήσεων – *ISO/IEC, 2022 [44]*. Για παράδειγμα, η απαίτηση για ισχυρή αυθεντικοποίηση (SCA) και ασφαλή APIs μπορεί να ενσωματωθεί στο ISMS μέσω συγκεκριμένων ελέγχων πρόσβασης (Access Control), τεχνικών μέτρων (π.χ. κρυπτογράφηση, MFA) και διαδικασιών διαχείρισης ταυτοτήτων. Παράλληλα, η διαχείριση περιστατικών ασφαλείας και η συμμόρφωση με το GDPR εντάσσονται στις διαδικασίες διαχείρισης συμβάντων και προστασίας δεδομένων του ISMS. Με λίγα λόγια το ISO/IEC 27001 αποτελεί το διεθνές πρότυπο για τη διαχείριση της ασφάλειας πληροφοριών και παρέχει ένα δομημένο πλαίσιο για την ανάπτυξη, υλοποίηση, παρακολούθηση και συνεχή βελτίωση του ISMS. Το πρότυπο απαιτεί την εκτίμηση και αντιμετώπιση κινδύνων, την εφαρμογή ελέγχων (controls) που περιγράφονται στο ISO/IEC 27002, και την τεκμηρίωση όλων των διαδικασιών. Ενδεικτικά, το ISO 27001 καλύπτει περιοχές όπως:

- Πολιτικές ασφάλειας πληροφοριών
- Οργάνωση της ασφάλειας
- Διαχείριση περιουσιακών στοιχείων (assets)
- Έλεγχος πρόσβασης
- Κρυπτογράφηση
- Φυσική και περιβαλλοντική ασφάλεια
- Ασφάλεια λειτουργιών
- Ασφάλεια επικοινωνιών
- Απόκριση σε περιστατικά
- Συμμόρφωση με νομικές και κανονιστικές απαιτήσεις

Αντίστοιχα, το NIST Special Publication 800-53 – NIST, 2020 [45] είναι ένα από τα πιο αναγνωρισμένα πλαίσια ασφάλειας πληροφοριών διεθνώς, ιδιαίτερα στον δημόσιο τομέα και σε οργανισμούς που δραστηριοποιούνται στις ΗΠΑ. Το πλαίσιο αυτό παρέχει ένα εκτενές σύνολο ελέγχων (security controls) που καλύπτουν τομείς όπως:

- Πρόσβαση και ταυτοποίηση (Access Control, Identification and Authentication)
- Διαχείριση κινδύνων (Risk Assessment)
- Προστασία δεδομένων (System and Communications Protection)
- Ανίχνευση και απόκριση σε περιστατικά (Incident Response)
- Συνεχής παρακολούθηση και αξιολόγηση (Continuous Monitoring)

4.3 Κενά υλοποίησης σε μικρές έναντι μεγάλων TPPs

Η υλοποίηση των κανονιστικών και τεχνικών απαιτήσεων από τους Τρίτους Παρόχους Υπηρεσιών Πληρωμών (TPPs) παρουσιάζει σημαντικές διαφοροποιήσεις ανάλογα με το μέγεθος, τους διαθέσιμους πόρους και το επίπεδο ωριμότητας κάθε οργανισμού. Τα κενά υλοποίησης μεταξύ μικρών και μεγάλων TPPs αποτελούν κρίσιμο παράγοντα για τη συνολική ασφάλεια του χρηματοοικονομικού οικοσυστήματος. Πιο συγκεκριμένα παρακάτω παρουσιάζονται κάποιες κατηγορίες στα οποία έχουν αναγνωριστεί κενά υλοποίησης βάση του μεγέθους του TPP. Πιο συγκεκριμένα:

1. Διαθεσιμότητα πόρων και τεχνογνωσίας

Οι μεγάλοι TPPs, συχνά πολυεθνικές ή θυγατρικές μεγάλων τραπεζικών ομίλων, διαθέτουν σημαντικούς οικονομικούς και ανθρώπινους πόρους, εξειδικευμένα τμήματα ασφάλειας και πρόσβαση σε προηγμένες τεχνολογίες. Αυτό τους επιτρέπει να υλοποιούν ολοκληρωμένα Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), να πραγματοποιούν τακτικούς ελέγχους (penetration tests, vulnerability assessments), να επενδύουν σε αυτοματοποιημένα

εργαλεία παρακολούθησης και να διατηρούν πιστοποιήσεις όπως ISO 27001, PCI DSS ή SWIFT CSCF.

Αντίθετα, οι μικροί TPPs συχνά λειτουργούν με περιορισμένο προσωπικό και προϋπολογισμό, με αποτέλεσμα να δυσκολεύονται να καλύψουν το πλήρες φάσμα των απαιτήσεων. Η έλλειψη εξειδικευμένων στελεχών ασφάλειας, η αδυναμία επένδυσης σε σύγχρονα εργαλεία και η εξάρτηση από εξωτερικούς συνεργάτες (outsourcing) δημιουργούν κενά στην υλοποίηση και αυξάνουν τον λειτουργικό κίνδυνο.

2. Εφαρμογή τεχνικών προτύπων και διαλειτουργικότητα

Οι μεγάλοι TPPs έχουν τη δυνατότητα να υιοθετούν άμεσα τα τελευταία τεχνικά πρότυπα (π.χ. NextGenPSD2, Open Banking APIs, eIDAS QWAC/QSEAL certificates) και να διασφαλίζουν τη διαλειτουργικότητα με πολλαπλές τράπεζες και συστήματα. Επίσης, μπορούν να συμμετέχουν ενεργά σε διεθνή fora και ομάδες εργασίας, επηρεάζοντας την εξέλιξη των προτύπων.

Αντίθετα, οι μικροί TPPs συχνά περιορίζονται σε βασικές υλοποιήσεις, με ελάχιστη προσαρμογή στις ιδιαιτερότητες κάθε τραπεζικού API, και δυσκολεύονται να παρακολουθήσουν τις συνεχείς αλλαγές στα πρότυπα. Αυτό οδηγεί σε αυξημένο κίνδυνο ασυμβατότητας, σφαλμάτων και καθυστερήσεων στην παροχή υπηρεσιών.

3. Διαχείριση κινδύνων και συμμόρφωση

Οι μεγάλοι TPPs εφαρμόζουν δομημένα πλαίσια διαχείρισης κινδύνων, με τακτική αξιολόγηση, καταγραφή και αντιμετώπιση απειλών, καθώς και πλήρη τεκμηρίωση για σκοπούς ελέγχου και πιστοποίησης. Διαθέτουν εξειδικευμένες ομάδες για τη συμμόρφωση με το PSD2, το GDPR, το PCI DSS και άλλους κανονισμούς, ενώ συχνά συνεργάζονται με εξωτερικούς ελεγκτές και νομικούς συμβούλους.

Οι μικροί TPPs, λόγω περιορισμένων πόρων, συχνά υιοθετούν ad hoc πρακτικές, με ελλιπή τεκμηρίωση, ανεπαρκή παρακολούθηση περιστατικών και αδυναμία άμεσης ανταπόκρισης σε νέες κανονιστικές απαιτήσεις. Αυτό μπορεί να οδηγήσει σε παραβιάσεις, πρόστιμα ή ακόμα και απώλεια άδειας λειτουργίας.

4. Ενημέρωση, εκπαίδευση και κουλτούρα ασφάλειας

Οι μεγάλοι TPPs επενδύουν σε συνεχή εκπαίδευση του προσωπικού, awareness campaigns και ασκήσεις προσομοίωσης περιστατικών (cyber drills), ενισχύοντας την κουλτούρα ασφάλειας σε όλα τα επίπεδα του οργανισμού.

Αντίθετα, στους μικρούς TPPs η εκπαίδευση περιορίζεται συχνά σε βασικά θέματα, με αποτέλεσμα το προσωπικό να μην είναι επαρκώς προετοιμασμένο για την αντιμετώπιση σύγχρονων απειλών (π.χ. phishing, social engineering).

5. Παραδείγματα και πρακτικές συνέπειες

Ένα χαρακτηριστικό παράδειγμα αποτελεί η υλοποίηση του Strong Customer Authentication (SCA) και των μηχανισμών OAuth2/Redirect στα APIs. Οι Μεγάλοι TPPs μπορούν να υποστηρίξουν πολλαπλές μεθόδους SCA (SMS OTP, mobile app, biometrics), ενώ οι μικροί

συχνά περιορίζονται σε μία ή δύο επιλογές, αυξάνοντας τον κίνδυνο αποτυχίας ταυτοποίησης ή κακής εμπειρίας χρήστη.

Επιπλέον, στην περίπτωση περιστατικών ασφαλείας, οι μεγάλοι TPPs διαθέτουν οργανωμένες ομάδες incident response και πλατφόρμες SIEM, ενώ οι μικροί βασίζονται σε χειροκίνητες διαδικασίες, με αποτέλεσμα καθυστερήσεις στην ανίχνευση και αναφορά.

6. Ρυθμιστικές απαιτήσεις και εποπτεία

Οι μεγάλοι TPPs είναι συχνά αντικείμενο αυστηρότερης εποπτείας από τις ρυθμιστικές αρχές (π.χ. FCA, EBA), με τακτικούς ελέγχους και υποχρέωση για ανεξάρτητες πιστοποιήσεις. Οι μικροί TPPs, αν και υπόκεινται στις ίδιες βασικές απαιτήσεις, συχνά λαμβάνουν εξατομικευμένη καθοδήγηση ή απολαμβάνουν μεταβατικές περιόδους συμμόρφωσης, γεγονός που μπορεί να δημιουργήσει ανισορροπίες στην αγορά.

4.4 Ρυθμιστικός και εποπτικός έλεγχος στον χρηματοοικονομικό τομέα

Ο ρυθμιστικός και εποπτικός έλεγχος στον χρηματοοικονομικό τομέα βασίζεται σε ένα πλέγμα ευρωπαϊκών και διεθνών προτύπων, οδηγιών και κανονισμών. Κάθε πλαίσιο ορίζει συγκεκριμένη συχνότητα ελέγχων και καθορίζει τους αρμόδιους φορείς που επιβλέπουν τη συμμόρφωση όπως παρουσιάζεται παρακάτω:

- **PSD2 (Payment Services Directive 2) & RTS (Regulatory Technical Standards):** Τακτικοί έλεγχοι συμμόρφωσης (συνήθως ετήσιοι ή όποτε ζητηθεί από την εποπτική αρχή) με την υποχρεωτική αναφορά περιστατικών ασφαλείας εντός 4 ωρών από την ανίχνευση τους. Οι αρμόδιοι φορείς για τον έλεγχο είναι οι εθνικές εποπτικές αρχές (π.χ. Τράπεζα της Ελλάδος, FCA στο Ηνωμένο Βασίλειο), υπό την καθοδήγηση της Ευρωπαϊκής Αρχής Τραπεζών (EBA).
- **EBA Guidelines (Οδηγίες της Ευρωπαϊκής Αρχής Τραπεζών):** Ετήσια αξιολόγηση συμμόρφωσης και τακτική αναφορά περιστατικών. Επίσης απαιτείται πραγματοποίηση εσωτερικών και εξωτερικών ελέγχων ανάλογα με το risk profile του οργανισμού. Οι αρμόδιοι φορείς για τον έλεγχο είναι η εθνικές εποπτικές αρχές, με συντονισμό και guidance από την EBA.
- **Open Banking Standard (Ηνωμένο Βασίλειο & ΕΕ):** Ετήσια πιστοποίηση συμμόρφωσης με τα πρότυπα του OBIE (Open Banking Implementation Entity) και πραγματοποίηση τακτικών διενεργειών penetration tests και ετήσια αναφορά συμμόρφωσης. Οι αρμόδιοι φορείς για τον έλεγχο είναι οι OBIE (για το Ηνωμένο Βασίλειο), FCA (Financial Conduct Authority) και PSR (Payment Systems Regulator).
- **PCI DSS v4.0 (Payment Card Industry Data Security Standard):** Ετήσια πιστοποίηση (Attestation of Compliance - AoC) από εξωτερικό Qualified Security Assessor (QSA) και πραγματοποίηση τακτικών vulnerability scans (τουλάχιστον τριμηνιαία) και penetration tests (τουλάχιστον ετησίως). Οι αρμόδιοι φορείς για τον έλεγχο είναι οι PCI Security

Standards Council (όπως ορίζει το πλαίσιο), οι εξωτερικοί QSA, οι εσωτερικές ομάδες ασφάλειας, καθώς και οι ίδιες οι τράπεζες/πάροχοι καρτών.

- **Berlin Group / NextGenPSD2 / OpenFinance API:** Τακτική συμμόρφωση με τις τεχνικές προδιαγραφές και ετήσια αναθεώρηση των APIs. Επίσης απαιτείται πραγματοποίηση penetration tests και vulnerability assessments τουλάχιστον ετησίως ή μετά από σημαντικές αλλαγές. Οι αρμόδιοι φορείς για τον έλεγχο είναι οι εθνικές εποπτικές αρχές, Berlin Group (ως consortium για τα πρότυπα), τράπεζες και TPPs μέσω self-assessment.
- **SWIFT CSCF (Customer Security Controls Framework):** Ετήσια πιστοποίηση συμμόρφωσης (KYC Security Attestation) και ετήσιοι τεχνικοί έλεγχοι (penetration tests, vulnerability scans). Οι αρμόδιοι φορείς για τον έλεγχο είναι οι SWIFT (ως οργανισμός), εξωτερικοί auditors και εσωτερικές ομάδες ασφάλειας.
- **ISO/IEC 27001 (Information Security Management System):** Ετήσιοι εσωτερικοί έλεγχοι ISMS, τριετής κύκλος εξωτερικής πιστοποίησης από διαπιστευμένους φορείς (Certification Bodies) με την επανεξέταση των πολιτικών και των διαδικασιών τουλάχιστον ετησίως. Οι αρμόδιοι φορείς για τον έλεγχο είναι οι διαπιστευμένοι φορείς πιστοποίησης (π.χ. TÜV, BSI, Lloyd’s Register).

5

Συμπεράσματα και Μελλοντικές Κατευθύνσεις Έρευνας

5.1 Συνοπτικά ευρήματα της συγκριτικής ανάλυσης

Η συγκριτική ανάλυση των κανονιστικών και τεχνικών πλαισίων που διέπουν τη λειτουργία των Τρίτων Παρόχων Υπηρεσιών Πληρωμών (TPPs) στον τραπεζικό τομέα ανέδειξε σημαντικές ομοιότητες αλλά και κρίσιμες διαφορές ως προς τις απαιτήσεις ασφάλειας, συμμόρφωσης και διακυβέρνησης. Αρχικά, διαπιστώθηκε ότι τα βασικά ευρωπαϊκά πρότυπα (PSD2, EBA Guidelines, Berlin Group, PCI DSS, SWIFT CSCF) και τα αντίστοιχα βρετανικά (Open Banking Standard, PSRs) έχουν ως κοινό στόχο την ενίσχυση της ασφάλειας, της διαφάνειας και της προστασίας των καταναλωτών. Όλα τα πλαίσια απαιτούν ισχυρή ταυτοποίηση πελάτη (SCA), χρήση ασφαλών APIs, καταγραφή και αναφορά περιστατικών ασφαλείας, καθώς και τακτικούς ελέγχους συμμόρφωσης. Ωστόσο, η ανάλυση ανέδειξε σημαντικές αποκλίσεις στην πρακτική εφαρμογή των προτύπων, κυρίως λόγω διαφορών στη ρυθμιστική προσέγγιση μεταξύ ΕΕ και Ηνωμένου Βασιλείου, αλλά και λόγω της πολυπλοκότητας των τεχνικών προδιαγραφών. Για παράδειγμα, ενώ το Berlin Group NextGenPSD2 API έχει υιοθετηθεί ευρέως στην Ευρώπη, κάθε τράπεζα μπορεί να εφαρμόζει διαφορετικές εκδοχές, αυξάνοντας το κόστος και τη δυσκολία διαλειτουργικότητας για τους TPPs. Αντίστοιχα, στο Ηνωμένο Βασίλειο, το Open Banking Standard έχει εξελιχθεί με αυτόνομους κανόνες διακυβέρνησης και τεχνικές προδιαγραφές, οδηγώντας σε περαιτέρω διαφοροποιήσεις μετά το Brexit. Ένα ακόμη βασικό εύρημα αφορά τις προκλήσεις εναρμόνισης και διαλειτουργικότητας. Παρά την ύπαρξη κοινών αρχών, η υλοποίηση των τεχνικών προτύπων και των μηχανισμών SCA διαφέρει σημαντικά μεταξύ τραπεζών, χωρών και TPPs, δημιουργώντας εμπόδια τόσο για τους τελικούς χρήστες όσο και για τους παρόχους. Η ανάγκη για συνεχή συμμόρφωση με πολλαπλά και συχνά μεταβαλλόμενα πρότυπα (όπως PCI DSS, SWIFT CSCF, EBA Guidelines) απαιτεί σημαντικούς πόρους και αυξάνει το λειτουργικό και κανονιστικό κόστος. Επιπλέον, η ανάλυση ανέδειξε ότι οι μικρότεροι TPPs αντιμετωπίζουν μεγαλύτερες δυσκολίες στην υλοποίηση των απαιτήσεων, λόγω περιορισμένων πόρων και τεχνικής τεχνογνωσίας, σε σύγκριση με τους μεγάλους παρόχους που διαθέτουν εξειδικευμένες ομάδες και μεγαλύτερη διαπραγματευτική ισχύ. Αυτό οδηγεί σε ανισότητες στην αγορά και αυξάνει τον κίνδυνο για κενά ασφάλειας. Τέλος, διαπιστώθηκε ότι η έλλειψη ενιαίας εποπτείας και η απουσία πλήρους εναρμόνισης οδηγούν σε αυξημένο ρίσκο για ασυνέπειες στη διαχείριση των δεδομένων και στην απόκριση σε περιστατικά ασφαλείας. Η διαλειτουργικότητα δεν αφορά μόνο τα τεχνικά συστήματα, αλλά και τις επιχειρησιακές διαδικασίες και τα μοντέλα διακυβέρνησης, με αποτέλεσμα να απαιτείται συνεχής συνεργασία μεταξύ ρυθμιστικών αρχών, τραπεζών και TPPs. Συνοψίζοντας, η συγκριτική ανάλυση καταδεικνύει την ανάγκη για

περαιτέρω εναρμόνιση, ενίσχυση της διαλειτουργικότητας και υιοθέτηση κοινών πρακτικών, ώστε να διασφαλιστεί η ασφάλεια, η καινοτομία και η εμπιστοσύνη στο σύγχρονο χρηματοοικονομικό οικοσύστημα.

Βιβλιογραφία

PSD2:

1. The European Parliament and the Council of the European Union (2015). "Payment Services Directive 2 (PSD2)" - Directive (EU) 2015/ of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
2. European Central Bank (2018). "The revised Payment Services Directive (PSD2) and the transition to stronger payments security" - https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html
3. The European Parliament and the Council of the European Union (2007). "Payment Service Directive (PSD)" - Directive (EU) 2007/64 of the European Parliament and of the Council of 13 November 2007on pay
4. Khakan N (2021). "Fintech firms and banks sustainability: Why cybersecurity risk matters?" - Fintech firms and banks sustainability: Why cybersecurity risk matters?
5. J.P.Morgan (2018). "The Second Payments Services Directive: A Catalyst for Innovation" - https://www.jpmorgan.com/insights/payments/payments-optimization/psd2?queryID=5c44d067556735de1d29ef92f8d99fc4
6. Open Banking Europe (2017). "Open Banking Europe - providing collaborative services to support PSD2 Access to Account (XS2A), in partnership with the financial industry" - https://www.openbankingeurope.eu/media/1175/preta-obe-mg-001-002-psd2-xs2a-registration-passporting-guide.pdf
7. European Commission (2017). "Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments" - https://ec.europa.eu/commission/presscorner/detail/en/memo_17_4961
8. Sectigo (2021). "The PSD2 Regulation Explained" - https://www.sectigo.com/resource-library/the-revised-payment-services-directive-psd2-explained
9. PSPLab. "Examples of Payment Initiation Service Providers (PISPs)" - http://psplab.com/services/pi-emi-authorisation/payment-initiation-service-provider-pisp-license/
10. PSPLab. What is the purpose of AISP (the difference between PISPs and AISPs)?" - https://psplab.com/services/pi-emi-authorisation/account-information-service-provider-aisp/
11. Roqqett Blog. "The Role of Card Based Payment Instrument Issuer in the Payment Ecosystem" - https://www.roqqett.com/blog/the-role-of-card-based-payment-instrument-issuer-in-the-payment-ecosystem
12. TrueLayer (2022). "What is an Account Servicing Payment Service Provider (ASPSP)?" - https://truelayer.com/blog/product/what-is-an-aspsp/

Open Banking Standards:

13. Stripe (2025). "What is open banking and how does it work?" - https://stripe.com/en-gr/resources/more/open-banking-explained
14. Stripe (2024). "Open banking regulation explained: A guide" - https://stripe.com/en-gr/resources/more/open-banking-regulation-explained-a-guide
15. TrueLayer. "Open banking around the world" - https://truelayer.com/reports/open-banking-guide/open-banking-around-the-world/
16. Canadian Center of Science and Education (2018). "Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future" - https://iris.unibocconi.it/retrieve/e31e10d3-725c-31fb-e053-1705fe0a5b99/76769-288169-1-SM.pdf
17. Investopedia (2024). "Open Banking: Definition, How It Works, and Risks" - https://www.investopedia.com/terms/o/open-banking.asp
18. McKinsey&Company (2017). "Data sharing and open banking" - https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/Data%20sharing%20and%20open%20banking/Data-sharing-and-open-banking.pdf

Κανονισμοί Πληρωμών του Ηνωμένου Βασιλείου (PSRs):

19. Payment Systems Regulator. "PSR Governance" - https://www.psr.org.uk/about-us/psr-governance/
20. Payment Systems Regulator. "The PSR purpose" - https://www.psr.org.uk/about-us/the-psr-purpose/
21. UK Statutory Instruments (2017). "The Payment Services Regulations 2017" - https://www.legislation.gov.uk/uksi/2017/752/data.pdf
22. Payment Systems Regulator (2020). "PSR General Directive 3" - https://www.psr.org.uk/media/za1cpqbl/psr-general-direction-3-march-2020.pdf

Τεχνικά Πρότυπα και Οδηγίες της Ευρωπαϊκής Αρχής Τραπεζών (EBA):

23. European Banking Authority. "EBA at a glance" - https://www.eba.europa.eu/eba-glance
24. European Banking Authority (2017). "Draft Guidelines on the security measures for operational and security risks of payment services under PSD2" - https://www.eba.europa.eu/sites/default/files/documents/10180/1836621/48750923-ed18-4940-91c7-9436c92b050c/Consultation%20Paper%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20of%20payment%20services%20under%20PSD2%20%28EBA-CP-2017-04%29.pdf
25. European Banking Authority (2017). "Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)" - https://www.eba.europa.eu/sites/default/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1

26. European Banking Authority (2017). "Draft Guidelines on the security measures for operational and security risks of payment services under PSD2" - https://www.eba.europa.eu/sites/default/files/documents/10180/1836621/48750923-ed18-4940-91c7-9436c92b050c/Consultation%20Paper%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20of%20payment%20services%20under%20PSD2%20%28EBA-CP-2017-04%29.pdf

PCI DSS v4.0:

27. PCI Security Standards Council. "PCI Data Security Standard (PCI DSS)" - https://www.pcisecuritystandards.org/standards/pci-dss/
28. Arthur B. Cooper Jr (2023). "The Definitive Guide to PCI DSS Version 4" - https://link.springer.com/content/pdf/10.1007/978-1-4842-9288-4.pdf
29. PCI Security Standards Council (2022). "PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2" - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf
30. Journal of Theoretical and Applied Information Technology (2024). "STRENGTHENING PAYMENT CARD DATA SECURITY: A STUDY ON COMPLIANCE ENHANCEMENT AND RISK MITIGATION THROUGH MFA IMPLEMENTATION UNDER PCI DSS 4.0" - https://www.jatit.org/volumes/Vol102No9/31Vol102No9.pdf
31. PCI Security Standards Council (2022). "PCI DSS:v4.0" - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Berlin Group και πρότυπα NextGenPSD2 / OpenFinance API

32. The Berlin Group. "About Berlin Group" - https://www.berlin-group.org/
33. The Berlin Group (2024). "openFinance API Framework" - https://c2914bdb-1b7a-4d22-b792-c58ac5d6648e.usrfiles.com/ugd/c2914b_0334ae21752c4b1d8b5646b68a4fcb3f.pdf
34. The Berlin Group. "A European Standard for PSD2 XS2A- General Introduction Paper" - https://www.berlin-group.org/_files/ugd/c2914b_ee83f2dd159b4c709e9d8a949aefd863.pdf
35. The Berlin Group (2025). "NextGenPSD2 Framework - Implementation Guidelines" - https://c2914bdb-1b7a-4d22-b792-c58ac5d6648e.usrfiles.com/ugd/c2914b_30e44ea1db1e4bed94c5607c78dee5c0.pdf

Πλαίσιο Ασφάλειας SWIFT (CSCF)

36. Swift. "What is SWIFT" - https://www.swift.com/about-us/discover-swift
37. Swift (2024). "Customer Security Controls Framework v2024" - https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/53.0/CSCF_v2024_20231017.pdf

General

38. (JPMNT) Journal of Process Management (2020). "PSD2 INFLUENCE ON DIGITAL BANKING TRANSFORMATION - BANKS' PERSPECTIVE " - 2334-735X2004001P.pdf

39. Journal of Computing and Information Technology (2024). "The Role of SSL/TLS in Securing API Communications: Strategies for Effective Implementation" - https://universe-publisher.com/index.php/jcit/article/view/20/20

40. Vcomply. "Compliance Incident Management" - https://www.v-comply.com/compliance-incident-management/

41. Usercentrics. "Essential guide to data minimization for GDPR compliance" - https://usercentrics.com/knowledge-hub/data-minimization/

42. GDPR Learning Hub. "Certification and certification mechanisms" - https://gdprlearninghub.com/certification-and-certification-mechanisms/

43. UK in a changing Europe (2025). "Regulating After BREXIT" - https://media.ukandeu.ac.uk/wp-content/uploads/2025/05/Regulating-after-Brexit-Embargoed-13-May.pdf

44. ISO/IEC (2022). "ISO/IEC 27001:2022Information security, cybersecurity and privacy protection — Information security management systems — Requirements" - https://www.iso.org/standard/27001

45. NIST (2020). "NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations" - https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final