ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ένα Πρόσθετο Πελάτη Ηλεκτρονικής Αλληλογραφίας για Προστασία Διαρροής Δεδομένων (An Email Client Add-on for Data leakage protection)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της/του

Σπυρίδων Στόγιου

Επιβλέπων : Αναπλ. Καθηγητής Κυριάκος Κρητικός

Μέλη εξεταστικής επιτροπής: Καθηγήτρια Μαρία Καρύδα, Αναπλ. Καθηγήτρια Ελισάβετ Κωνσταντίνου

Σάμος, 27/10/2025

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του Προπτυχιακού Προγράμματος Σπουδών του Τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου. Αντικείμενό της είναι η ανάπτυξη ενός προσθέτου (add-on) για το Gmail, το οποίο ενσωματώνει μηχανισμούς πρόληψης διαρροής δεδομένων (Data Leakage Prevention) και κρυπτογράφησης, με στόχο την ενίσχυση της ασφάλειας και της ιδιωτικότητας στην ηλεκτρονική επικοινωνία. Η εργασία συνδυάζει θεωρητική ανάλυση και πρακτική υλοποίηση, προσφέροντας μια σύγχρονη, επεκτάσιμη λύση για την προστασία ευαίσθητων πληροφοριών.

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον Καθηγητή Κυριάκο Κρητικό για την πολύτιμη καθοδήγηση, την υποστήριξη και τις ουσιαστικές του παρατηρήσεις κατά τη διάρκεια της εκπόνησης της εργασίας. Ευχαριστώ, επίσης, την οικογένειά μου και τους φίλους μου για τη συνεχή στήριξη και ενθάρρυνση καθ’ όλη τη διάρκεια των σπουδών μου.

του/της

Στόγιου Σπυρίδων

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

AAA	Authentication, Authorization, Accounting
API	Application Programming Interface
CASB	Cloud Access Security Broker
CCPA	California Consumer Privacy Act
DLP/S	Data Loss Prevention / Systems
DNS	Domain Name System
DRM	Digital Rights Management
EDR	Endpoint Detection and Response
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
Gmail	Google Mail
HIPAA	Health Insurance Portability and Accountability Act
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IAM	Identity and Access Management
IDM	Indexed Document Matching
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IRM	Information Rights Management
JSON	JavaScript Object Notation
KMS	Key Management System
MFA	Multi-Factor Authentication
ML	Machine Learning
MUA	Mail User Agent
OCR	Optical Character Recognition
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
REST	Representational State Transfer
RSA	Rivest–Shamir–Adleman
SaaS	Software as a Service
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
UI	User Interface
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network

Περίληψη

Η παρούσα διπλωματική εργασία εστιάζει στην ανάπτυξη ενός προσθέτου (add-on) για το πρόγραμμα πελάτη ηλεκτρονικής αλληλογραφίας Gmail, με κύριο στόχο την πρόληψη διαρροής προσωπικών και ευαίσθητων δεδομένων κατά τη σύνταξη και αποστολή ηλεκτρονικών μηνυμάτων. Το προτεινόμενο σύστημα αναλύει το περιεχόμενο των μηνυμάτων και τους παραλήπτες, προκειμένου να εντοπίζει πιθανές παραβιάσεις πολιτικών ασφάλειας και να υποστηρίζει τον χρήστη στη λήψη ασφαλών αποφάσεων πριν την αποστολή.

Πιο συγκεκριμένα, το πρόσθετο παρέχει λειτουργίες που περιλαμβάνουν: την ανίχνευση ευαίσθητων πληροφοριών στο κείμενο και στο θέμα, την αξιολόγηση των παραληπτών ανάλογα με το αν περιλαμβάνονται στις αποθηκευμένες επαφές του χρήστη, την εμφάνιση ειδοποιήσεων και προειδοποιήσεων για πιθανά περιστατικά διαρροής, καθώς και την κρυπτογράφηση και αποκρυπτογράφηση περιεχομένου μέσω μηχανισμού PGP. Επιπλέον, ενσωματώνει σύστημα διαχείρισης επαφών και δημοσίων κλειδιών, υποστηρίζοντας τη δημιουργία, αποθήκευση και διαμοίραση κλειδιών, καθώς και τη δυνατότητα αποκλεισμού ή απεμπλοκής αποστολέων.

Η διεπαφή χρήσης του προσθέτου σχεδιάζεται με έμφαση στην ευχρηστία και στην παροχή άμεσης πληροφόρησης, μέσω σαφών προειδοποιήσεων και κατάλληλων μηνυμάτων σφάλματος που αντικατοπτρίζουν τον βαθμό επικινδυνότητας κάθε περίπτωσης. Με αυτόν τον τρόπο, ο χρήστης διατηρεί τον πλήρη έλεγχο της αποστολής των μηνυμάτων του, ενώ ταυτόχρονα ενισχύεται η προστασία προσωπικών και εμπιστευτικών πληροφοριών στο περιβάλλον του Gmail.

Λέξεις-κλειδιά: Gmail, Πρόσθετο, Ασφάλεια Ηλεκτρονικής Αλληλογραφίας, Πρόληψη Διαρροής Δεδομένων, Κρυπτογράφηση, Προσωπικά Δεδομένα, Ιδιωτικότητα, Επίπεδο Εμπιστοσύνης.

Abstract

This thesis focuses on the development of an add-on for the Gmail email client, aiming to prevent the leakage of personal and sensitive data during the composition and sending of emails. The proposed system analyzes the message content and recipients to identify potential security policy violations and assist the user in making safe decisions before sending.

More specifically, the add-on provides functionalities such as detecting sensitive information in the message body and subject, evaluating recipients based on whether they are included in the user's stored contacts, displaying alerts and warnings for possible data leakage incidents, and enabling encryption and decryption of message content through a PGP mechanism. Furthermore, it integrates a contact and public key management system that supports the creation, storage, and sharing of keys, as well as the blocking or unblocking of senders.

The add-on's user interface is designed with a focus on usability and immediate feedback, providing clear warnings and informative error messages that reflect the risk level of each situation. In this way, the user retains full control over email transmission, while simultaneously enhancing the protection of personal and confidential information within the Gmail environment.

Keywords: *Gmail, Add-on, Email Security, Data Leakage Prevention, Encryption, Personal Data, Privacy, Trust Level.*

1

Εισαγωγή

1.1 Χρήση και Προκλήσεις Ασφάλειας στα Email

Η εκτεταμένη χρήση του ηλεκτρονικού ταχυδρομείου έχει εγείρει σοβαρές ανησυχίες σχετικά με την ασφάλεια και την προστασία των προσωπικών δεδομένων [1]. Ένα κρίσιμο ζήτημα που προκύπτει είναι το ενδεχόμενο διαρροής πληροφοριών, είτε λόγω λάθους, όπως η αποστολή ενός μηνύματος σε μη εξουσιοδοτημένους παραλήπτες, είτε, ακόμα χειρότερα, λόγω απόρροιας της χρήσης τεχνικών κοινωνικής μηχανικής [2].

Οι επιθέσεις κοινωνικής μηχανικής αποτελούν σοβαρή απειλή για την ασφάλεια των πληροφοριών, καθώς εκμεταλλεύονται ανθρώπινα λάθη και ψυχολογικούς παράγοντες για να παραπλανήσουν τα άτομα και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα τους (ή των οργανισμών στους οποίους αυτά εργάζονται) [2]. Οι επιτιθέμενοι χρησιμοποιούν τεχνικές, όπως η προσποίηση και η δημιουργία ψεύτικων προφίλ, για να παραπλανήσουν υπαλλήλους και να παρακάμψουν ακόμη και τα πιο ισχυρά συστήματα ασφαλείας [2]. Αυτό καθιστά την κοινωνική μηχανική μια από τις μεγαλύτερες προκλήσεις στην κυβερνοασφάλεια [1] .

Οι διαρροές πληροφοριών που προκύπτουν από τέτοιες τεχνικές μπορούν να προκαλέσουν σημαντική ζημιά τόσο σε ιδιώτες όσο και σε επιχειρήσεις. Ένα μόνο περιστατικό διαρροής μέσω email μπορεί να οδηγήσει σε ακριβές νομικές συνέπειες, να βλάψει τη φήμη ενός οργανισμού, να επηρεάσει κρίσιμες διαπραγματεύσεις και να προκαλέσει σοβαρές οικονομικές απώλειες [3] .

1.2 Παραδοσιακά και Σύγχρονα Μέσα Ασφάλειας

Παραδοσιακά, η προστασία των εμπιστευτικών δεδομένων επιτυγχανόταν μέσω πολιτικών και κλασικών τεχνικών ασφαλείας, όπως τα τείχη προστασίας (firewalls), τα εικονικά ιδιωτικά δίκτυα (VPNs) και τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) [4]. Αν και τα IPS διαθέτουν προληπτικές δυνατότητες, τα περισσότερα από αυτά τα συστήματα βασίζονται σε κανόνες που απαιτούν εκ των προτέρων καθορισμό και δεν έχουν σχεδιαστεί με επίκεντρο τα ίδια τα ευαίσθητα δεδομένα και το ενδεχόμενο διαρροής τους. Συνεπώς, ενδέχεται να είναι ανεπαρκή για την πρόληψη διαρροών, καθώς τα ευαίσθητα δεδομένα μπορεί να εμφανιστούν σε ποικίλες μορφές και να διακινηθούν μέσω καναλιών που δεν καλύπτονται πλήρως από τους προκαθορισμένους κανόνες αυτών των συστημάτων [4].

Στο πλαίσιο των παραδοσιακών μηχανισμών ασφάλειας, τα συστήματα IDS και IPS αποτελούν βασικά εργαλεία για την ανίχνευση και την αποτροπή επιθέσεων σε δίκτυα και πληροφοριακά συστήματα. Η σύγκρισή τους αναδεικνύει τη μετάβαση από την παθητική παρακολούθηση προς πιο ενεργές μορφές πρόληψης, προετοιμάζοντας το έδαφος για σύγχρονες λύσεις όπως τα DLPS [1].

Τα IDS (Intrusion Detection Systems) παρακολουθούν τη δραστηριότητα του δικτύου ή του συστήματος για να ανιχνεύουν ύποπτες κινήσεις και πιθανές παραβιάσεις ασφαλείας. Ωστόσο, δεν λαμβάνουν ενεργά μέτρα για να σταματήσουν την επίθεση, αλλά ειδοποιούν τους διαχειριστές ασφαλείας, οι οποίοι με τη σειρά τους θα αναλάβουν την εκτέλεση των απαραίτητων ενεργειών αναχαίτισης ή μετρίασης των επιθέσεων [4]. Τα IDS, επομένως, έχουν κυρίως ανιχνευτικό ρόλο και δεν παρεμβαίνουν στην εξέλιξη της επίθεσης.

Αντίθετα, τα IPS (Intrusion Prevention Systems) έχουν την ικανότητα να μπλοκάρουν ή να αποτρέπουν μια επίθεση σε πραγματικό χρόνο, προτού αυτή προκαλέσει ζημιά [4]. Επομένως, ένα IPS λειτουργεί ως ένα προληπτικό σύστημα που παρεμβαίνει αυτόματα, αποτρέποντας την εξέλιξη της επίθεσης και προστατεύοντας άμεσα το δίκτυο.

Για τον παραπάνω λόγο, τα τελευταία χρόνια έχουν εισαχθεί τα Συστήματα Πρόληψης Διαρροής Δεδομένων (Data Loss Prevention Systems – DLPS) ως εξειδικευμένοι μηχανισμοί για την ανίχνευση και πρόληψη διαρροής εμπιστευτικών πληροφοριών σε όλα τα στάδια της διαχείρισής τους – κατά τη χρήση των εμπιστευτικών πληροφοριών, κατά τη μετάδοσή τους και όταν αυτές είναι αποθηκευμένες [1]. Τα DLPS επεκτείνουν τις δυνατότητες των IDS και IPS, επικεντρώνοντας την ανάλυσή τους όχι μόνο στη ροή της δικτυακής κίνησης αλλά και στο ίδιο το περιεχόμενο των δεδομένων, προκειμένου να ανιχνεύσουν ευαίσθητες πληροφορίες και να αποτρέψουν τη διαρροή τους [1], [3].

1.3 Προτεινόμενη Λύση Διπλωματικής

Το ηλεκτρονικό ταχυδρομείο αποτελεί ένα από τα πιο διαδεδομένα και κρίσιμα κανάλια επικοινωνίας τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο. Επειδή συχνά περιέχει εμπιστευτικές πληροφορίες, γίνεται κύριος στόχος για επιθέσεις και διαρροές δεδομένων [2], [3]. Επιπλέον, το email λειτουργεί συχνά ως το πρώτο επίπεδο επίθεσης σε τεχνικές κοινωνικής μηχανικής, όπου οι επιτιθέμενοι χρησιμοποιούν εξαπάτηση, όπως επιθέσεις phishing, για να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή να παραπλανήσουν τους χρήστες [5]. Η έμφυτη ευπάθεια των email σε ανθρώπινα λάθη, όπως η λανθασμένη αποστολή σε μη εξουσιοδοτημένους παραλήπτες, ή η εκμετάλλευση μέσω κακόβουλων συνδέσμων και συνημμένων, καθιστά επιτακτική την ανάγκη για εξειδικευμένες λύσεις πρόληψης διαρροών (DLP) ακριβώς στο σημείο δημιουργίας και αποστολής των μηνυμάτων [1]. Η επιλογή μας να εστιάσουμε στην προστασία δεδομένων για το Gmail ανταποκρίνεται σε αυτήν την ανάγκη, καθώς στοχεύουμε στην αποτροπή ακούσιων και σκόπιμων διαρροών πληροφοριών σε ένα από τα πιο ευάλωτα αλλά και συχνά χρησιμοποιούμενα κανάλια επικοινωνίας [3], [6], [7].

Στην παρούσα εργασία, παρουσιάζουμε έναν μηχανισμό πρόληψης διαρροής δεδομένων μέσω ενός προσθέτου που αναπτύσσεται ειδικά για το Gmail, έναν από τους πιο διαδεδομένους πελάτες ηλεκτρονικής αλληλογραφίας παγκοσμίως, με περίπου 2,5 δισεκατομμύρια ενεργούς χρήστες [6]. Η επιλογή του Gmail δεν έγινε μόνο λόγω της μεγάλης βάσης χρηστών του, η οποία αυξάνει τις πιθανότητες διαρροών δεδομένων, αλλά και εξαιτίας των ευέλικτων δυνατοτήτων που προσφέρει μέσω του Google Apps Script, επιτρέποντας την ανάπτυξη προσαρμοσμένων προσθέτων [8]. Επιπλέον, η ανάγκη για μια DLP λύση στη διαχείριση της ηλεκτρονικής αλληλογραφίας είναι επιτακτική, καθώς το ηλ. ταχυδρομείο αποτελεί ένα από τα βασικά και πιο ευάλωτα κανάλια μέσω των οποίων διακινούνται ευαίσθητες πληροφορίες [1], [3]. Πλήθος περιστατικών διαρροής δεδομένων οφείλεται είτε σε ανθρώπινο λάθος κατά την αποστολή, είτε σε ανεπαρκή έλεγχο των παραληπτών ή των συνημμένων, είτε σε επιθέσεις κοινωνικής μηχανικής [5].

Η προτεινόμενη λύση στοχεύει στην προστασία των δεδομένων του χρήστη μέσω της ανίχνευσης ευαίσθητων πληροφοριών στο περιεχόμενο των μηνυμάτων προς αποστολή, της ταξινόμησης των συνημμένων αρχείων με βάση τον βαθμό διαρροής πληροφορίας, καθώς και της αξιολόγησης των παραληπτών με βάση το επίπεδο εμπιστοσύνης τους και την ικανότητά τους στη διαχείριση κρυπτογραφημένων δεδομένων. Το πρόσθετο προστατεύει τα ευαίσθητα δεδομένα κατά την αποστολή τους μέσω ηλεκτρονικού ταχυδρομείου, παρέχοντας κάποιες βασικές δυνατότητες:

- Αυτόματη ανίχνευση ευαίσθητων πληροφοριών στο περιεχόμενο των μηνυμάτων.
- Ταξινόμηση και προστασία των συνημμένων αρχείων.
- Αξιολόγηση παραληπτών με βάση το επίπεδο εμπιστοσύνης τους και την ικανότητά τους να διαχειρίζονται κρυπτογραφημένα δεδομένα.
- Αυτοματοποίηση προληπτικών ενεργειών, όπως η κρυπτογράφηση, το μπλοκάρισμα ή η διαγραφή μηνυμάτων.

Μέσω αυτών των λειτουργιών, επιτυγχάνεται έγκαιρη ανίχνευση και αποτροπή πιθανών περιστατικών διαρροής πριν αυτά συμβούν .

Επιπλέον, το πρόσθετο διαθέτει έναν ευέλικτο μηχανισμό κανόνων, επιτρέποντας στον χρήστη να προσαρμόζει πλήρως τη λειτουργία του ανάλογα με τις προσωπικές ή επαγγελματικές ανάγκες ασφαλείας. Ο ευέλικτος αυτός μηχανισμός επιτρέπει την αυτοματοποίηση των προληπτικών ενεργειών, καθώς εφαρμόζει προκαθορισμένες συνθήκες και ενέργειες που ενεργοποιούνται αυτόματα όταν εντοπίζονται συγκεκριμένα μοτίβα ή τύποι ευαίσθητων δεδομένων. Έτσι, λειτουργίες όπως η κρυπτογράφηση, η ειδοποίηση ή ο αποκλεισμός αποστολής εκτελούνται δυναμικά, βάσει των καθορισμένων κανόνων, χωρίς την ανάγκη χειροκίνητης παρέμβασης. Η παραμετροποίηση του συστήματος είναι πλήρως δυναμική, επιτρέποντας τη δημιουργία, τροποποίηση και διαγραφή κανόνων και προφίλ πολιτικής ασφαλείας. Κάθε προφίλ πολιτικής αποτελεί μια συλλογή κανόνων με κοινό σκοπό ή επίπεδο προστασίας, επιτρέποντας στον χρήστη να εφαρμόζει διαφορετικές πολιτικές ασφάλειας ανάλογα με το πλαίσιο χρήσης ή τον τύπο επικοινωνίας.

Το πρόσθετο έχει σχεδιαστεί με γνώμονα την υψηλή απόδοση, ώστε να μην επιβαρύνει τη λειτουργία του Gmail, εξασφαλίζοντας ομαλή εμπειρία χρήστη κατά τη σύνταξη και αποστολή μηνυμάτων. Παράλληλα, η επεκτασιμότητα της λύσης επιτρέπει την προσθήκη νέων ενεργειών και λειτουργιών στο μέλλον, προσαρμοζόμενη στις εξελισσόμενες ανάγκες ασφάλειας. Αν και η τρέχουσα υλοποίηση βασίζεται στο οικοσύστημα του Gmail μέσω Google Apps Script, η κεντρική φιλοσοφία και οι μηχανισμοί λειτουργίας του προσθέτου μπορούν να αξιοποιηθούν ως βάση για πιθανή ανάπτυξη αντίστοιχων λύσεων και σε άλλες πλατφόρμες ηλεκτρονικής αλληλογραφίας, εφόσον το επιτρέπουν τα αντίστοιχα APIs ή εργαλεία ενσωμάτωσης. Έτσι, ο έλεγχος ασφαλείας ενσωματώνεται απρόσκοπτα στην καθημερινή ροή εργασίας του χρήστη.

1.4 Δομή και Περιεχόμενο της διπλωματικής

Η παρούσα διπλωματική εργασία αποτελείται από επτά κεφάλαια. Στο Κεφάλαιο 1 παρουσιάζεται το αντικείμενο, το υπόβαθρο και η αναγκαιότητα της έρευνας, καθώς και η προτεινόμενη λύση και η συνολική δομή της εργασίας. Το Κεφάλαιο 2 περιλαμβάνει την ανάλυση του θεωρητικού υποβάθρου και των σχετικών εννοιών που συνδέονται με την ασφάλεια δεδομένων, όπως η προστασία της ιδιωτικότητας, οι τεχνικές κοινωνικής μηχανικής, τα συστήματα πρόληψης διαρροής δεδομένων (DLPS) και η ασφάλεια στην ηλεκτρονική αλληλογραφία. Στο Κεφάλαιο 3 παρουσιάζονται οι σχετικές εργασίες και μελέτες που έχουν δημοσιευθεί γύρω από το αντικείμενο της πρόληψης διαρροής δεδομένων και της ασφάλειας email, αναδεικνύοντας τα πλεονεκτήματα και τις ελλείψεις των υπαρχουσών προσεγγίσεων. Το Κεφάλαιο 4 επικεντρώνεται στην ανάπτυξη της προτεινόμενης λύσης, περιγράφοντας αναλυτικά τις απαιτήσεις του συστήματος, τη διαδικασία σχεδίασης και υλοποίησης, καθώς και την αρχιτεκτονική και τις βασικές λειτουργικές ενότητες του προσθέτου. Το Κεφάλαιο 5 παρουσιάζει τη διαδικασία εγκατάστασης και επίδειξης της εφαρμογής, περιλαμβάνοντας οδηγίες παραμετροποίησης και παραδείγματα χρήσης του προσθέτου στο περιβάλλον του Gmail. Το Κεφάλαιο 6 αφορά την αποτίμηση της λύσης, όπου παρουσιάζονται τα αποτελέσματα της ποσοτικής και ποιοτικής αξιολόγησης, οι δείκτες απόδοσης και η αξιοπιστία του συστήματος. Τέλος, στο Κεφάλαιο 7 παρατίθενται τα συμπεράσματα της εργασίας, συνοψίζονται τα κύρια ευρήματα και προτείνονται κατευθύνσεις για μελλοντική έρευνα και περαιτέρω ανάπτυξη του συστήματος.

2

Υπόβαθρο

Το κεφάλαιο αυτό παρουσιάζει το θεωρητικό και τεχνολογικό υπόβαθρο που υποστηρίζει την ανάπτυξη της προτεινόμενης λύσης. Στόχος του είναι να εισαγάγει τον αναγνώστη στις βασικές έννοιες που σχετίζονται με την προστασία δεδομένων και την ασφάλεια πληροφοριών, προσφέροντας το απαραίτητο πλαίσιο κατανόησης για τη συνέχεια της εργασίας. Αρχικά, αναλύονται οι θεμελιώδεις αρχές της προστασίας ιδιωτικότητας και προσωπικών δεδομένων, καθώς και το ισχύον κανονιστικό πλαίσιο (ενότητα 2.1). Στη συνέχεια, εξετάζονται οι τεχνικές κοινωνικής μηχανικής και οι μορφές επιθέσεων που στοχεύουν στη χειραγώγηση χρηστών (ενότητα 2.2), ενώ ακολουθεί η παρουσίαση των Συστημάτων Πρόληψης Διαρροής Δεδομένων (Data Loss Prevention Systems – DLPS), με έμφαση στις μεθόδους λειτουργίας και τα είδη αυτών των συστημάτων (ενότητα 2.3). Τέλος, παρουσιάζονται οι αρχές λειτουργίας της ηλεκτρονικής αλληλογραφίας, τα σχετικά πρωτόκολλα και τα επίπεδα ασφάλειας που τη διέπουν (ενότητα 2.4). Μέσω αυτής της δομής, ο αναγνώστης αποκτά ολοκληρωμένη εικόνα του θεωρητικού πλαισίου, ώστε να μπορεί να κατανοήσει πληρέστερα τη σχεδίαση και την υλοποίηση της προτεινόμενης λύσης στα επόμενα κεφάλαια.

2.1 Ιδιωτικότητα Δεδομένων

2.1.1 Ορισμός και Σημασία της Ιδιωτικότητας Δεδομένων

Η ιδιωτικότητα των δεδομένων, γνωστή και ως προστασία προσωπικών δεδομένων, αναφέρεται στο δικαίωμα κάθε ατόμου να ελέγχει τις προσωπικές του πληροφορίες και να καθορίζει πώς, πότε και σε ποιο βαθμό αυτές διαμοιράζονται ή χρησιμοποιούνται [9]. Με την εκρηκτική αύξηση της χρήσης διαδικτυακών υπηρεσιών και της ψηφιακής αλληλεπίδρασης [3], [5], η ιδιωτικότητα των δεδομένων έχει αποκτήσει κεντρική σημασία τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο [1]. Η ανάγκη για διασφάλιση των προσωπικών δεδομένων είναι πλέον πιο επιτακτική από ποτέ, καθώς η έλλειψη προστασίας μπορεί να οδηγήσει σε κατάχρηση, απάτη και απώλεια εμπιστοσύνης των χρηστών στα ψηφιακά συστήματα και τους οργανισμούς που διαχειρίζονται τα δεδομένα τους [1], [5].

2.1.2 Τύποι Δεδομένων που Θεωρούνται Ιδιωτικά

Σήμερα, τα δεδομένα που θεωρούνται ιδιωτικά περιλαμβάνουν διάφορους τύπους ευαίσθητων πληροφοριών [9]:

1. **Προσωπικά Αναγνωριστικά Στοιχεία (PII):** Αυτά περιλαμβάνουν πληροφορίες που μπορούν να αναγνωρίσουν άμεσα ή έμμεσα ένα άτομο, όπως το όνομα, η διεύθυνση, ο αριθμός τηλεφώνου, ο αριθμός ταυτότητας ή διαβατηρίου και η διεύθυνση ηλεκτρονικού ταχυδρομείου [10]. Τα PII είναι θεμελιώδους σημασίας για την προστασία της ιδιωτικότητας, καθώς οποιαδήποτε διαρροή ή μη εξουσιοδοτημένη πρόσβαση σε αυτά μπορεί να θέσει το άτομο σε κίνδυνο κλοπής ταυτότητας και άλλων επιθέσεων [11].
2. **Ευαίσθητα Προσωπικά Δεδομένα:** Αυτή η κατηγορία περιλαμβάνει δεδομένα που απαιτούν αυστηρότερη προστασία, όπως ιατρικά αρχεία, βιομετρικά δεδομένα και οικονομικές πληροφορίες. Στο πλαίσιο του GDPR, οι "ειδικές κατηγορίες" προσωπικών δεδομένων περιλαμβάνουν, πέρα από τα ανωτέρω, δεδομένα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικές πεποιθήσεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συνδικαλιστική ιδιότητα, καθώς και γενετικά δεδομένα, βιομετρικά δεδομένα για σκοπούς ταυτοποίησης, δεδομένα υγείας και δεδομένα που αφορούν τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό [12]. Τα ευαίσθητα δεδομένα μπορούν να έχουν σοβαρές συνέπειες αν διαρρεύσουν, για παράδειγμα μέσω κακόβουλων επιθέσεων ή αδυναμιών ασφαλείας. Ενδεικτικά, η διαρροή ιατρικών δεδομένων μπορεί να οδηγήσει σε διακριτική μεταχείριση ή στιγματισμό [13] (π.χ. αποκάλυψη διάγνωσης/αναπηρίας), η υποκλοπή βιομετρικών στοιχείων να προκαλέσει μη αναστρέψιμο κίνδυνο πλαστοπροσωπίας [14] (π.χ. δακτυλικά αποτυπώματα/αναγνώριση προσώπου που δεν "αλλάζουν"), ενώ η έκθεση οικονομικών πληροφοριών να επιφέρει κλοπή ταυτότητας και οικονομική απάτη [15] (π.χ. μη εξουσιοδοτημένες συναλλαγές, άνοιγμα πιστωτικών γραμμών). Επιπλέον, μπορεί να υπάρξει βλάβη φήμης, απώλεια ευκαιριών εργασίας ή και εκβιασμός, ιδίως όταν αποκαλύπτονται στοιχεία που άπτονται της ιδιωτικής ζωής ή επαγγελματικού απορρήτου

[16]. Δεδομένης της ευαίσθητης φύσης τους, η διαχείρισή τους ρυθμίζεται από αυστηρές νομοθεσίες, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)[17], που επιβάλλει αυστηρά μέτρα διασφάλισης και έλεγχο πρόσβασης [17], [18].

3. **Δεδομένα Συμπεριφοράς και Τρόπου Ζωής**: Αυτά τα δεδομένα περιλαμβάνουν τις συνήθειες, τις προτιμήσεις και τις αλληλεπιδράσεις των ατόμων στο διαδίκτυο, όπως το ιστορικό περιήγησης, οι αναζητήσεις και οι ηλεκτρονικές αγορές [19]. Οι πληροφορίες αυτές χρησιμοποιούνται συχνά από διαφημιστικές και αναλυτικές εταιρείες για την κατανόηση των καταναλωτικών προτύπων [19], ωστόσο η κατάχρησή τους ενδέχεται να παραβιάσει την ιδιωτικότητα των χρηστών με τους εξής τρόπους: (i) δημιουργία λεπτομερών προφίλ και αυτοματοποιημένη λήψη αποφάσεων/στοχευμένη διαφήμιση (profiling/ADM) [20] , (ii) επαναπροσδιορισμός ταυτότητας μέσω συσχέτισης φαινομενικά «ανωνυμοποιημένων» συνόλων (de-anonymization) [21] , (iii) διαρκής ιχνηλάτηση και συσχέτιση συσκευών/λογαριασμών (cookie syncing, cross-device tracking, geofencing) [22] , (iv) διακριτική τιμολόγηση ή αποκλεισμός υπηρεσιών βάσει προφίλ, δηλαδή διαφορετικές τιμές/προσφορές ή όροι πρόσβασης με βάση το προφίλ που προκύπτει από τα δεδομένα συμπεριφοράς (π.χ. υψηλότερη τιμή/ασφάλιστρο ή λιγότερες εκπτώσεις σε «χαμηλής πιστότητας» προφίλ, απόρριψη/περιορισμός υπηρεσίας ή καθυστέρηση παράδοσης σε προφίλ που εκλαμβάνονται ως «υψηλού ρίσκου», εμφάνιση διαφορετικού καταλόγου προϊόντων/διαθεσιμότητας ή αποκλεισμός περιοχών—digital redlining) [23] , (v) δευτερογενής χρήση/κοινοποίηση σε τρίτους χωρίς επαρκή νομική βάση ή διαφάνεια, και (vi) αυξημένος κίνδυνος παραβίασης ασφάλειας λόγω υπερσυγκέντρωσης και μακράς διατήρησης δεδομένων [24].
4. **Δεδομένα Τοποθεσίας και Παρακολούθησης**: Αυτά τα δεδομένα προέρχονται κυρίως από κινητές συσκευές και GPS, καταγράφοντας τη γεωγραφική τοποθεσία ενός ατόμου σε πραγματικό χρόνο [25]. Οι πληροφορίες τοποθεσίας μπορούν να αποκαλύψουν ευαίσθητες πτυχές της ζωής του ατόμου (π.χ. επισκέψεις σε νοσοκομεία/κλινικές, χώρους λατρείας ή πολιτικές συγκεντρώσεις, καθώς και τακτικές διαδρομές μεταξύ κατοικίας – εργασίας – σχολείου) και γι' αυτό απαιτούν ιδιαίτερη προσοχή όσον αφορά τη διαχείριση και την προστασία τους [25], [26].
5. **Επαγγελματικά και Εμπορικά Μυστικά:** Στον επιχειρηματικό τομέα, τα δεδομένα που αφορούν επιχειρηματικές δραστηριότητες, όπως οι πελάτες, τα εμπορικά σχέδια και οι στρατηγικές μιας εταιρείας, θεωρούνται ιδιωτικά. Η διαρροή αυτών των πληροφοριών μπορεί να πλήξει την ανταγωνιστικότητα μιας επιχείρησης και να προκαλέσει οικονομική ζημιά, καθώς και βλάβη στη φήμη της [27].
6. **Δεδομένα Εκπαίδευσης και Εργασίας:** Βαθμοί, πτυχία, ιστορικά εγγραφών, αξιολογήσεις, στοιχεία φοιτητικής/υπηρεσιακής κατάστασης, στοιχεία μισθοδοσίας και αξιολογήσεις απόδοσης. Αποτελούν **προσωπικά δεδομένα** και, όπου αποκαλύπτουν ειδικές κατηγορίες (π.χ. συνδικαλιστική ιδιότητα), υπάγονται στο αυστηρότερο καθεστώς του GDPR [17].
7. **Δεδομένα Ανηλίκων**: Προσωπικά δεδομένα παιδιών [28] απολαμβάνουν ειδικής προστασίας η επεξεργασία τους διέπεται από αυστηρότερες προϋποθέσεις (π.χ. συγκατάθεση γονέα/κηδεμόνα για υπηρεσίες κοινωνίας της πληροφορίας, ηλικιακά όρια

13–16 ανά κράτος-μέλος [29], αυξημένη διαφύλαξη). Παραδείγματα: σχολικές εγγραφές, φωτογραφίες/βίντεο σχολικών δράσεων, μαθητικοί λογαριασμοί e-learning, δεδομένα γεωεντοπισμού σχολικών διαδρομών.

8. **Δεδομένα Πελατών/Συναλλαγών:** Στοιχεία πελατών, ιστορικά αγορών, συνδρομές, παράπονα/αιτήματα υποστήριξης, δεδομένα CRM (π.χ. στοιχεία τιμολόγησης/αποστολής, προτιμήσεις προϊόντων, loyalty IDs, αρχεία επικοινωνίας με support, tokens πληρωμών). Πρόκειται για προσωπικά δεδομένα που εμπίπτουν στο γενικό πλαίσιο του GDPR και, ανάλογα με το περιεχόμενο, μπορεί να ενεργοποιούν πρόσθετες υποχρεώσεις (π.χ. διαφάνεια, ελαχιστοποίηση, περιορισμός σκοπού) [17].
9. **Κυβερνητικά/Διοικητικά Δεδομένα:** Επίσημα αναγνωριστικά και έγγραφα που εκδίδονται από δημόσιες αρχές (π.χ. ΑΔΤ, ΑΦΜ, διαβατήριο, άδεια οδήγησης, άδειες διαμονής/εργασίας, πιστοποιητικά γέννησης/γάμου). Θεωρούνται προσωπικά δεδομένα σε αρκετές έννομες τάξεις η επεξεργασία εθνικών αναγνωριστικών διέπεται από ειδικούς κανόνες· ειδική κατηγορία αποτελεί και η επεξεργασία δεδομένων ποινικών καταδικών/αδικημάτων που υπόκειται σε πρόσθετους περιορισμούς [17].

2.1.3 Κανονιστικό Πλαίσιο για την Προστασία της Ιδιωτικότητας Δεδομένων

Η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων έχει αναδειχθεί σε έναν από τους πλέον κρίσιμους άξονες της ψηφιακής εποχής. Η αυξανόμενη συλλογή, αποθήκευση και ανάλυση προσωπικών δεδομένων τόσο από ιδιωτικούς όσο και από δημόσιους οργανισμούς, καθιστά απαραίτητη την ύπαρξη ενός ισχυρού νομικού και κανονιστικού πλαισίου που να διασφαλίζει τα θεμελιώδη δικαιώματα των πολιτών. Στο επίκεντρο αυτής της προσπάθειας βρίσκονται κανονισμοί, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, ο οποίος έχει θέσει τις βάσεις για ένα εναρμονισμένο νομικό περιβάλλον προστασίας δεδομένων εντός της ΕΕ [17].

Ο GDPR ορίζει τις αρχές της διαφάνειας, της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού, υποχρεώνοντας τους υπεύθυνους επεξεργασίας να λαμβάνουν κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας[17]. Παράλληλα, προσφέρει στους πολίτες αυξημένα δικαιώματα, όπως η πρόσβαση στα δεδομένα τους, η διόρθωση, η διαγραφή (δικαίωμα στη λήθη), καθώς και η φορητότητα των δεδομένων τους, δηλαδή το δικαίωμα να λαμβάνουν τα δεδομένα τους σε δομημένη και αναγνώσιμη μορφή και να τα μεταφέρουν σε άλλον πάροχο υπηρεσιών χωρίς περιορισμούς [17]. Ο κανονισμός συνοδεύεται από αυστηρές κυρώσεις για παραβιάσεις, ενισχύοντας την υποχρέωση συμμόρφωσης για τις επιχειρήσεις [17].

Ανάλογες νομοθεσίες έχουν θεσπιστεί και σε άλλες περιοχές του κόσμου, όπως ο California Consumer Privacy Act (CCPA) στις Ηνωμένες Πολιτείες [30], ο οποίος επικεντρώνεται στο δικαίωμα των καταναλωτών να γνωρίζουν πώς χρησιμοποιούνται τα προσωπικά τους δεδομένα, καθώς και να επιλέγουν αν αυτά θα πωληθούν ή όχι σε τρίτους. Στο διεθνές επίπεδο, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) έχει διαμορφώσει κατευθυντήριες γραμμές για την προστασία της ιδιωτικότητας και τις ροές δεδομένων διασυνοριακά [31].

Η θεσμική κατοχύρωση της ιδιωτικότητας συνδυάζεται με τη διαρκώς αυξανόμενη ανάγκη για τεχνολογικά μέσα συμμόρφωσης. Η έννοια της «ενσωματωμένης και εκ προεπιλογής προστασίας της ιδιωτικότητας» (privacy by design & by default), την οποία εισάγει ο GDPR,

ενθαρρύνει την ανάπτυξη συστημάτων και εφαρμογών που έχουν την προστασία της ιδιωτικότητας στο επίκεντρο της αρχιτεκτονικής τους, ήδη από τη φάση του σχεδιασμού.

Η ανάγκη για προστασία της ιδιωτικότητας δεν είναι μόνο νομική, αλλά και κοινωνική, οικονομική και τεχνολογική. Οι διεθνείς και ευρωπαϊκοί κανονισμοί επιδιώκουν να δημιουργήσουν ένα συνεκτικό και αξιόπιστο πλαίσιο που προστατεύει τον πολίτη απέναντι στις αυξανόμενες απειλές που συνεπάγεται η ψηφιακή εποχή. Η πολυπλοκότητα των ροών δεδομένων, η χρήση τεχνητής νοημοσύνης[32] και οι απαιτήσεις της σύγχρονης επιχειρηματικότητας καθιστούν αναγκαία τη διαρκή αναθεώρηση και προσαρμογή του νομικού πλαισίου. Παράλληλα, η συμμόρφωση με τους κανόνες προστασίας της ιδιωτικότητας γίνεται όλο και πιο δύσκολη υπόθεση για τις επιχειρήσεις, κάτι που απαιτεί την εφαρμογή προηγμένων λύσεων τεχνολογικής υποστήριξης.

Η προστασία της ιδιωτικότητας αποτελεί πυλώνα της ψηφιακής εμπιστοσύνης. Η ύπαρξη ισχυρού νομικού πλαισίου, όπως ο GDPR και ο CCPA, διαμορφώνει ένα ασφαλές περιβάλλον για την επεξεργασία δεδομένων, δίνοντας έμφαση στα δικαιώματα των υποκειμένων των δεδομένων. Ωστόσο, για να είναι αποτελεσματική αυτή η προστασία, απαιτείται συνεργασία μεταξύ νομικής συμμόρφωσης καθώς και τεχνολογικής και οργανωτικής υποστήριξης.

Τα Συστήματα Πρόληψης Διαρροής Δεδομένων (DLPS) παίζουν καθοριστικό ρόλο στην εφαρμογή των νομικών απαιτήσεων, καθώς μπορούν να εντοπίζουν και να αποτρέπουν την παράνομη ή ακούσια διαρροή ευαίσθητων δεδομένων[1]. Η ενσωμάτωσή τους ενισχύει τη συμμόρφωση με κανονισμούς όπως ο GDPR, καθώς επιτρέπουν την παρακολούθηση, την καταγραφή και τον έλεγχο των δεδομένων σε πραγματικό χρόνο. Επιπλέον, διευκολύνουν τη λογοδοσία (accountability) και τη διαφάνεια, στοιχεία που αποτελούν θεμελιώδεις αρχές κάθε σύγχρονου κανονιστικού πλαισίου προστασίας προσωπικών δεδομένων.

2.2 Κοινωνική Μηχανική

2.2.1 Ορισμός

Η κοινωνική μηχανική (social engineering) είναι ένα είδος επίθεσης στον τομέα της κυβερνοασφάλειας που εκμεταλλεύεται ανθρώπινες αδυναμίες, όπως η εμπιστοσύνη, η περιέργεια ή η άγνοια, και ειδικότερα τον ψυχολογικό παράγοντα με στόχο την πρόσβαση σε ευαίσθητες πληροφορίες ή την εκτέλεση μη εξουσιοδοτημένων ενεργειών. Οι επιτιθέμενοι βασίζονται σε τεχνικές εξαπάτησης, αντί να χρησιμοποιούν αποκλειστικά τεχνολογικά εργαλεία, και συχνά καταφέρνουν να επιτύχουν τους στόχους τους χωρίς να χρειάζεται να παραβιάσουν άμεσα κάποιο σύστημα ασφαλείας [33].

2.2.2 Στάδια Επιθέσεων Κοινωνικής Μηχανικής

Οι επιθέσεις κοινωνικής μηχανικής συνήθως ακολουθούν συγκεκριμένα στάδια για την επίτευξη του στόχου τους:

1. **Συλλογή Πληροφοριών (Reconnaissance):**
   Σε αυτό το αρχικό στάδιο, ο επιτιθέμενος συγκεντρώνει όσο το δυνατόν περισσότερες πληροφορίες για το θύμα. Οι πηγές μπορεί να περιλαμβάνουν δημόσια διαθέσιμα δεδομένα, μέσα κοινωνικής δικτύωσης, ιστοσελίδες εταιρειών ή ακόμα και φυσική παρατήρηση. Σκοπός είναι η χαρτογράφηση του στόχου και η αναγνώριση πιθανών ευπαθειών [34] .

2. **Δημιουργία Σεναρίου (Pretext Development):**
   Αφού αποκτηθούν οι απαραίτητες πληροφορίες, ο επιτιθέμενος δημιουργεί ένα πειστικό «σενάριο» ή πρόσχημα. Το σενάριο αυτό καθορίζει τη στρατηγική προσέγγισης και τη μορφή της επίθεσης, π.χ. υποδυόμενος κάποιον από το τμήμα IT ή έναν συνεργάτη [34].

3. **Αρχική Επαφή (Initial Contact):**
   Σε αυτό το στάδιο πραγματοποιείται η πρώτη αλληλεπίδραση με το θύμα. Ο επιτιθέμενος εφαρμόζει το σενάριο και επιδιώκει να κερδίσει την εμπιστοσύνη του θύματος, π.χ. μέσω email, τηλεφωνικής κλήσης ή φυσικής παρουσίας. Η επιτυχία του σταδίου εξαρτάται σε μεγάλο βαθμό από την πειστικότητα και τον ψυχολογικό χειρισμό [34].

4. **Χειραγώγηση και Εκμετάλλευση (Manipulation and Exploitation):**
   Αφού έχει δημιουργηθεί εμπιστοσύνη, ο επιτιθέμενος χειραγωγεί το θύμα ώστε να αποκαλύψει ευαίσθητες πληροφορίες ή να εκτελέσει κάποια ενέργεια (π.χ. άνοιγμα συνημμένου αρχείου ή μεταφορά χρημάτων). Τεχνικές όπως το baiting, το phishing και το pretexting εφαρμόζονται σε αυτό το στάδιο [34].

5. **Επίτευξη Στόχου (Goal Accomplishment):**
   Ο επιτιθέμενος ολοκληρώνει την ενέργεια για την οποία σχεδιάστηκε η επίθεση: απόκτηση πρόσβασης σε σύστημα, συλλογή διαπιστευτηρίων, μεταφορά εμπιστευτικών αρχείων κ.ά. [34].

6. **Κάλυψη Ιχνών και Αποχώρηση (Exit and Cover Tracks):**
   Τέλος, ο επιτιθέμενος φροντίζει να καλύψει τα ίχνη του, ώστε να μην εντοπιστεί εύκολα. Αυτό μπορεί να περιλαμβάνει διαγραφή ψηφιακών αρχείων, αλλοίωση λογιστικών στοιχείων ή αποφυγή περαιτέρω επικοινωνίας με το θύμα [34].

Η γνώση αυτών των σταδίων είναι κρίσιμη για τον σχεδιασμό κατάλληλων μέτρων προστασίας και την εκπαίδευση των χρηστών στην αναγνώριση και αποφυγή τέτοιων τεχνικών εξαπάτησης.

2.2.3 Είδη Επιθέσεων Κοινωνικής Μηχανικής

- **Phishing (Ηλεκτρονικό Ψάρεμα):** Αυτή η τεχνική περιλαμβάνει την αποστολή παραπλανητικών email που φαίνονται να προέρχονται από αξιόπιστες πηγές, όπως τράπεζες ή γνωστούς οργανισμούς, και στοχεύει στην απόκτηση προσωπικών δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού. Η απόκτηση των δεδομένων επιτυγχάνεται συνήθως μέσω συνδέσμων που οδηγούν τον χρήστη σε πλαστές ιστοσελίδες, όπου καλείται να καταχωρήσει ευαίσθητες πληροφορίες (π.χ. στοιχεία σύνδεσης ή τραπεζικούς λογαριασμούς). Από την άλλη, η εγκατάσταση κακόβουλου λογισμικού επιτυγχάνεται μέσω μολυσμένων συνημμένων αρχείων, τα οποία ενεργοποιούνται όταν ο χρήστης τα ανοίξει, δίνοντας στον επιτιθέμενο τη δυνατότητα πρόσβασης στο σύστημά του. Το phishing είναι η πιο κοινή και αναγνωρισμένη μορφή κοινωνικής μηχανικής [35],[36].
    - Παράδειγμα: Ένα email που φαίνεται να προέρχεται από «την τράπεζά σας» σας ενημερώνει για ύποπτη δραστηριότητα στο λογαριασμό σας και σας καλεί να κάνετε άμεσα σύνδεση μέσω ενός επισυναπτόμενου συνδέσμου. Ο σύνδεσμος οδηγεί σε ιστοσελίδα-απομίμηση της πραγματικής και καταγράφει τα στοιχεία σας. Παράλληλα, το email περιέχει ένα δήθεν "απόσπασμα συναλλαγών" σε μορφή αρχείου PDF που, αν ανοιχτεί, εγκαθιστά κακόβουλο λογισμικό.
- **Spear Phishing και Whaling:** Το spear phishing είναι μια εξειδικευμένη μορφή phishing που επικεντρώνεται σε συγκεκριμένα άτομα ή ομάδες. Αυτή η μορφή είναι προσωποποιημένη και πιο πειστική, καθώς περιλαμβάνει πληροφορίες σχετικές με τον στόχο. Το whaling, από την άλλη, στοχεύει στελέχη υψηλού επιπέδου, όπως διευθυντές, οπότε μπορεί να έχει καταστροφικές συνέπειες για μια επιχείρηση, λόγω των αυξημένων δικαιωμάτων που έχουν αυτά τα στελέχη στον οργανισμό τους και στα συστήματά του [35],[36].
    - Παράδειγμα: Ένας διευθυντής οικονομικών λαμβάνει ένα email που φαίνεται να προέρχεται από τον CEO της εταιρείας και του ζητά να εγκρίνει επειγόντως μια μεταφορά χρημάτων σε έναν συνεργάτη. Το email περιλαμβάνει ρεαλιστικές λεπτομέρειες για την εταιρεία και τον συνεργάτη καθώς και για το λόγο μεταφοράς των χρημάτων, καθιστώντας το εξαιρετικά πειστικό. Στην πραγματικότητα, ο αποστολέας είναι ένας επιτιθέμενος που έχει συγκεντρώσει πληροφορίες από δημόσιες πηγές και μέσα κοινωνικής δικτύωσης για να κάνει το μήνυμά του πιο πειστικό και προσωποποιημένο.
- **Pretexting (Προσποίηση):** Η τεχνική του pretexting βασίζεται στη δημιουργία ενός πειστικού και προσχεδιασμένου σεναρίου από τον επιτιθέμενο, το οποίο περιλαμβάνει την υιοθέτηση μιας ψεύτικης ταυτότητας. Ο επιτιθέμενος παρουσιάζεται ως αξιόπιστο πρόσωπο (για παράδειγμα, ως υπάλληλος τεχνικής υποστήριξης, δημόσιος λειτουργός ή πελάτης) με σκοπό να αποκτήσει την εμπιστοσύνη του θύματος. Το σενάριο είναι μελετημένο ώστε να φαίνεται απολύτως ρεαλιστικό και συνεπές με την εκάστοτε κατάσταση, προκειμένου να μην προκαλεί υποψίες. Μέσω αυτής της διαδικασίας, ο επιτιθέμενος καταφέρνει να οδηγήσει το θύμα στην αποκάλυψη ευαίσθητων πληροφοριών ή στη λήψη ενεργειών που εξυπηρετούν τους σκοπούς του [35],[36].

  - Παράδειγμα: Ένας επιτιθέμενος καλεί έναν υπάλληλο εταιρείας, προσποιούμενος τον τεχνικό υποστήριξης του τμήματος IT, και του ζητά να επιβεβαιώσει το όνομα χρήστη και τον κωδικό του για να "διορθώσει" ένα υποτιθέμενο τεχνικό πρόβλημα. Ο υπάλληλος, θεωρώντας την κλήση νόμιμη, αποκαλύπτει τα στοιχεία του, δίνοντας έτσι στον επιτιθέμενο την ευκαιρεία να διεισδύσει στο σύστημα της εταιρείας.

- **Baiting (Δελέασμα):** Οι επιτιθέμενοι χρησιμοποιούν φυσικά ή ηλεκτρονικά «δέλεαρ» για να προσελκύσουν το θύμα και να το παραπλανήσουν να εγκαταστήσει κακόβουλο λογισμικό ή να αποκαλύψει προσωπικές πληροφορίες. Τα φυσικά δέλεαρ μπορεί να περιλαμβάνουν, για παράδειγμα, την εγκατάλειψη USB sticks σε δημόσιους χώρους (π.χ. έξω από γραφεία ή πανεπιστήμια) με την ελπίδα ότι κάποιος θα τα συνδέσει στον υπολογιστή του ώστε να πραγματοποιηθεί η εγκατάσταση κακόβουλου λογισμικού. Τα ηλεκτρονικά δέλεαρ συνήθως παρουσιάζονται ως ελκυστικές προσφορές στο διαδίκτυο – όπως δωρεάν μουσική, ταινίες, λογισμικό ή πρόσβαση σε «αποκλειστικό περιεχόμενο» – και οδηγούν το χρήστη να κάνει κλικ σε συνδέσμους που περιέχουν κακόβουλο κώδικα (πχ. για την αναπαραγωγή του περιεχομένου) ή ψεύτικες φόρμες υποβολής προσωπικών δεδομένων [35].
  - Παράδειγμα: Ένα θύμα βλέπει μια διαδικτυακή διαφήμιση που υπόσχεται δωρεάν λήψη ενός δημοφιλούς προγράμματος. Με το που κάνει κλικ και εγκαθιστά την εφαρμογή, ενεργοποιείται λογισμικό καταγραφής πληκτρολογήσεων που συλλέγει τους κωδικούς πρόσβασής του για λογαριασμούς σε εταιρικά ή εμπορικά συστήματα ή υπηρεσίες.
- **Quid Pro Quo (Ανταλλαγή):** Το quid pro quo αποτελεί τεχνική κοινωνικής μηχανικής κατά την οποία ο επιτιθέμενος υπόσχεται κάποιο όφελος ή υπηρεσία με αντάλλαγμα την αποκάλυψη προσωπικών ή ευαίσθητων πληροφοριών. Η επίθεση αυτή διαφέρει από το pretexting, καθώς εδώ υπάρχει ρητή ανταλλαγή – δηλαδή, το θύμα «κερδίζει» κάτι χειροπιαστό, το οποίο οδηγεί στην παράδοση των πληροφοριών. Η μορφή του οφέλους μπορεί να είναι τεχνική υποστήριξη, έκπτωση, πρόσβαση σε λογισμικό ή άλλο πλεονέκτημα [35].
  - Παράδειγμα: Ένας επιτιθέμενος αποστέλλει email σε υπαλλήλους μιας εταιρείας, προσφέροντάς τους δωρεάν πρόσβαση σε λογισμικό που «βελτιώνει την απόδοση του υπολογιστή» ή παρέχει «premium εργαλεία για την εργασία τους». Για να αποκτήσουν το λογισμικό, οι υπάλληλοι πρέπει να εισαγάγουν τα εταιρικά τους διαπιστευτήρια σε μια φόρμα εγγραφής. Στην πραγματικότητα, ο επιτιθέμενος χρησιμοποιεί αυτή την ανταλλαγή για να υποκλέψει τους κωδικούς πρόσβασης.
- **Dumpster Diving (Έρευνα σε Απορρίμματα):** Η τεχνική dumpster diving αναφέρεται στην πρακτική κατά την οποία ο επιτιθέμενος ερευνά τα φυσικά απορρίμματα ενός οργανισμού ή ατόμου με σκοπό τον εντοπισμό εμπιστευτικών ή χρήσιμων πληροφοριών. Συχνά, στα σκουπίδια καταλήγουν έγγραφα που περιέχουν ευαίσθητα δεδομένα, όπως εσωτερική αλληλογραφία, χειρόγραφες σημειώσεις, πρόχειρα έγγραφα, παλιά τιμολόγια ή ακόμη και λίστες με κωδικούς.Η επίθεση αυτή εκμεταλλεύεται την ελλιπή καταστροφή

φυσικών εγγράφων και θεωρείται απλή αλλά εξαιρετικά επικίνδυνη, ιδίως σε περιβάλλοντα όπου δεν υπάρχουν αυστηρές πολιτικές απόρριψης εγγράφων[35],[36].

- Παράδειγμα: Ένας επιτιθέμενος εισέρχεται στον χώρο με τους κάδους απορριμμάτων ενός οργανισμού και εντοπίζει απορριμμένα έγγραφα με εκτυπωμένους αριθμούς λογαριασμών πελατών και σημειώσεις με κωδικούς πρόσβασης που είχαν γραφτεί πρόχειρα από εργαζόμενους.

- **Shoulder Surfing:** Το shoulder surfing αποτελεί μια τεχνική κοινωνικής μηχανικής κατά την οποία ο επιτιθέμενος παρακολουθεί διακριτικά τις ενέργειες του θύματος, από μικρή απόσταση, προκειμένου να υποκλέψει ευαίσθητες πληροφορίες. Η επίθεση αυτή βασίζεται στην οπτική παρακολούθηση και μπορεί να πραγματοποιηθεί είτε σε φυσικά περιβάλλοντα (π.χ. σε δημόσιους χώρους, μέσα μαζικής μεταφοράς, καφετέριες), είτε μέσω καμερών ασφαλείας ή κινητών τηλεφώνων [35],[36].
  - Παράδειγμα: Ένας επιτιθέμενος κάθεται πίσω από έναν χρήστη στο μετρό και παρακολουθεί ενώ αυτός πληκτρολογεί τα διαπιστευτήρια του σε μια τραπεζική εφαρμογή. Με τον τρόπο αυτό, ο επιτιθέμενος απομνημονεύει ή καταγράφει την πληροφορία, χωρίς να χρειαστεί καμία τεχνική παρέμβαση.
- **Vishing (Voice Phishing):** Το vishing αποτελεί μια μορφή κοινωνικής μηχανικής κατά την οποία ο επιτιθέμενος επιχειρεί να εξαπατήσει το θύμα μέσω τηλεφωνικής επικοινωνίας, προσποιούμενος ότι εκπροσωπεί έναν αξιόπιστο φορέα (όπως μια τράπεζα, μια υπηρεσία τεχνικής υποστήριξης ή έναν δημόσιο οργανισμό). Στόχος της επίθεσης είναι η απόσπαση ευαίσθητων πληροφοριών, όπως δεδομένα ταυτοποίησης, τραπεζικά στοιχεία, ή διαπιστευτήρια πρόσβασης.Η επιτυχία του vishing βασίζεται στην αξιοποίηση του ψυχολογικού παράγοντα, όπως είναι η αίσθηση του επείγοντος, ο φόβος απώλειας, ή η επίκληση στην αυθεντία [35],[36].
  - Παράδειγμα: Ο επιτιθέμενος καλεί τον χρήστη ισχυριζόμενος ότι είναι υπάλληλος της τράπεζάς του και ότι έχει εντοπιστεί ύποπτη δραστηριότητα στον λογαριασμό του. Ζητά επιτακτικά επιβεβαίωση των στοιχείων ταυτοποίησης ή/και του κωδικού μίας χρήσης (OTP), με σκοπό να αποκτήσει πρόσβαση στον λογαριασμό.
- **Angler Phishing:** Το angler phishing αποτελεί μια σύγχρονη παραλλαγή του phishing που εκμεταλλεύεται τις πλατφόρμες κοινωνικής δικτύωσης. Σε αυτές τις επιθέσεις, ο επιτιθέμενος δημιουργεί έναν ψεύτικο λογαριασμό, συνήθως προσποιούμενος ότι είναι υπάλληλος εξυπηρέτησης πελατών ή επίσημος λογαριασμός εταιρείας, με σκοπό να εξαπατήσει τους χρήστες και να αποσπάσει ευαίσθητες πληροφορίες ή να τους οδηγήσει σε κακόβουλους συνδέσμους. Η αποτελεσματικότητα της τεχνικής οφείλεται στο γεγονός ότι πολλές εταιρείες χρησιμοποιούν πραγματικά τα κοινωνικά δίκτυα για υποστήριξη, επομένως η ψεύτικη οντότητα που δημιουργεί ο επιτιθέμενος φαίνεται πειστική [35],[36].
  - Παράδειγμα: Ένας χρήστης δημοσιεύει ένα παράπονο στο Twitter προς μια τράπεζα. Ένας ψεύτικος λογαριασμός, που μοιάζει με τον επίσημο της τράπεζας, απαντά και στέλνει έναν σύνδεσμο υποστήριξης, ο οποίος ζητά τα διαπιστευτήρια σύνδεσης του χρήστη σε μία παραπλανητική ιστοσελίδα.

- **Tailgating (Ακολουθία χωρίς εξουσιοδότηση):**Το tailgating είναι μια μορφή κοινωνικής μηχανικής που αφορά τη φυσική πρόσβαση σε προστατευμένες περιοχές. Ο επιτιθέμενος εισέρχεται σε έναν ασφαλή χώρο ακολουθώντας στενά έναν εξουσιοδοτημένο υπάλληλο, χωρίς να διαθέτει τις απαραίτητες άδειες ή κάρτα πρόσβασης. Η τεχνική βασίζεται συχνά στην εκμετάλλευση της ευγένειας ή της απροσεξίας του προσωπικού ασφαλείας ή των υπαλλήλων. Η επιτυχία αυτής της μεθόδου εξαρτάται από την κοινωνική πίεση: σπάνια ένας εργαζόμενος θα αμφισβητήσει κάποιον που φαίνεται "φυσιολογικός" ή φέρει εξοπλισμό που θυμίζει τεχνικό [35],[36].
    - Παράδειγμα: Ένας επιτιθέμενος ντυμένος ως τεχνικός δικτύου ακολουθεί έναν υπάλληλο σε μια πόρτα ασφαλείας χωρίς να χρησιμοποιήσει κάρτα πρόσβασης. Ο υπάλληλος τον αφήνει να περάσει, πιστεύοντας ότι ανήκει στο προσωπικό.
- **Scareware:** Το scareware είναι μια τεχνική κοινωνικής μηχανικής που εκμεταλλεύεται τον φόβο του χρήστη προκειμένου να τον παραπλανήσει ώστε να εγκαταστήσει κακόβουλο λογισμικό ή να προβεί σε ανεπιθύμητες ενέργειες. Συνήθως εμφανίζεται με τη μορφή ψευδών προειδοποιήσεων για ιούς ή προβλήματα ασφαλείας, οι οποίες ισχυρίζονται ότι ο υπολογιστής είναι "μολυσμένος" και προτείνουν τη λήψη ενός "λογισμικού προστασίας". Το υποτιθέμενο προστατευτικό λογισμικό είναι στην πραγματικότητα κακόβουλο και μπορεί να εγκαταστήσει spyware, trojans, ransomware ή άλλα είδη κακόβουλου λογισμικού που έχουν τη δυνατότητα εκτέλεσης διαφόρων επικίνδυνων ενεργειών (πχ. κρυπτογράφηση δεδομένων χρήστη, παρακολούθηση πληκτρολόγησης, κλπ.) [35],[36].
    - Παράδειγμα: Ο χρήστης βλέπει ένα αναδυόμενο παράθυρο στον φυλλομετρητή του που αναγράφει: "Το σύστημά σας είναι μολυσμένο με 5 ιούς! Κάντε κλικ εδώ για να τους αφαιρέσετε." Εφόσον αυτός πατήσει το σύνδεσμο, ξεκινά η εγκατάσταση του κακόβουλου λογισμικού.
- **Multimedia Masquerading:** Η επίθεση multimedia masquerading βασίζεται στη χρήση πολυμέσων (όπως βίντεο, εικόνες, έγγραφα ή παρουσιάσεις) που φαίνονται νόμιμα και ακίνδυνα, αλλά στην πραγματικότητα κρύβουν κακόβουλο περιεχόμενο ή οδηγούν το θύμα σε παραπλανητικές ενέργειες. Συχνά, οι επιτιθέμενοι αξιοποιούν ψευδείς προελεύσεις και τίτλους αρχείων που τραβούν το ενδιαφέρον του θύματος (π.χ. "Λίστα Μισθοδοσίας.pdf" ή "Video από τη χθεσινή συνάντηση.mp4"), προκειμένου να το παρασύρουν να τα ανοίξει ή να ενεργοποιήσει μακροεντολές. Υπάρχουν δύο εναλλακτικές μεθόδους για την επίθεση αυτή: (α) η κατάληψη του αρχείου είναι παραπλανητική και το αρχείο είναι διαφορετικής μορφής από την αναμενόμενη (πχ. .exe αρχείο αντί για .mp4) και (β) το αρχείο είναι όντως πολυμεσικό αλλά περιλαμβάνει κακόβουλο payload[35],[36].
    - Παράδειγμα: Ένας υπάλληλος λαμβάνει ένα email με συνημμένο αρχείο που ονομάζεται "Έκθεση Εσόδων 2024.pptx". Το αρχείο περιέχει κακόβουλες μακροεντολές που ενεργοποιούνται μόλις ανοίξει, επιτρέποντας την εγκατάσταση λογισμικού καταγραφής πληκτρολογήσεων (keylogger) στον υπολογιστή του.
- **Popup Windows (Αναδυόμενα Παράθυρα):**Οι επιθέσεις μέσω popup windows βασίζονται στη δημιουργία παραπλανητικών αναδυόμενων παραθύρων που εμφανίζονται κατά την περιήγηση σε ιστοσελίδες. Αυτά τα παράθυρα μιμούνται νόμιμα μηνύματα ασφαλείας, ειδοποιήσεις συστημάτων ή προτροπές εγκατάστασης λογισμικού. Στόχος

είναι να εξαπατήσουν το χρήστη ώστε να προβεί σε επιβλαβείς ενέργειες, όπως το κατέβασμα ψεύτικου αντιβιοτικού (antivirus), την εισαγωγή προσωπικών δεδομένων ή την παροχή απομακρυσμένης πρόσβασης [35],[36].

- Παράδειγμα: Κατά την πλοήγηση σε ένα blog, εμφανίζεται ένα popup που μοιάζει με φόρμα σύνδεσης Google, ζητώντας από τον χρήστη να εισαγάγει τα στοιχεία του για να συνεχίσει να βλέπει το περιεχόμενο. Το παράθυρο είναι σχεδιασμένο ώστε να μοιάζει απόλυτα αυθεντικό. Εφόσον ο χρήστης εισάγει τα διαπιστευτήρια, αυτά αποστέλλονται στον επιτιθέμενο, ο οποίος αποκτά πρόσβαση στον λογαριασμό του.

2.2.4 Επιπτώσεις των Επιθέσεων Κοινωνικής Μηχανικής

Οι επιθέσεις κοινωνικής μηχανικής έχουν σοβαρές επιπτώσεις στην ασφάλεια των οργανισμών και των χρηστών, οδηγώντας συχνά σε:

- **Διαρροή Προσωπικών Δεδομένων:** Οι χρήστες παραπλανώνται και αποκαλύπτουν κωδικούς πρόσβασης, οικονομικά στοιχεία ή άλλες ευαίσθητες πληροφορίες, καθιστώντας τους ευάλωτους σε περαιτέρω κακόβουλες ενέργειες [36].
- **Οικονομικές Ζημιές:** Οι επιχειρήσεις ενδέχεται να υποστούν οικονομική ζημιά από μια επίθεση κοινωνικής μηχανικής με πολλαπλούς τρόπους [36]. Για παράδειγμα, σε περίπτωση διαρροής δεδομένων, ενδέχεται να αντιμετωπίσουν πρόστιμα και κυρώσεις από ρυθμιστικές αρχές (όπως βάσει του GDPR [17]), να χρειαστεί να καλύψουν κόστος αποκατάστασης και ενίσχυσης της ασφάλειας, καθώς και απώλεια εσόδων από πελάτες που χάνουν την εμπιστοσύνη τους. Επιπλέον, η κλοπή ταυτότητας υψηλόβαθμων στελεχών μπορεί να οδηγήσει σε μη εξουσιοδοτημένες τραπεζικές συναλλαγές, υποκλοπή στρατηγικών αποφάσεων, ή διαρροή ευαίσθητων οικονομικών πληροφοριών, προκαλώντας σοβαρές οικονομικές συνέπειες, όπως πτώση της μετοχής (σε εισηγμένες εταιρείες), καταγγελίες συμβολαίων ή διαρροή εμπορικών μυστικών σε ανταγωνιστές [36].
- **Απώλεια Εμπιστοσύνης:** Οι επιθέσεις κοινωνικής μηχανικής, όταν γίνονται ευρέως γνωστές, πλήττουν την εμπιστοσύνη των πελατών και μπορεί να βλάψουν σοβαρά τη φήμη μιας επιχείρησης, μειώνοντας την αξιοπιστία της και το πελατολόγιό της [36].
- **Νομικές και Ρυθμιστικές Συνέπειες:** Η παραβίαση δεδομένων μπορεί να επιφέρει κυρώσεις από αρχές προστασίας προσωπικών δεδομένων, όπως πρόστιμα λόγω παραβίασης του GDPR ή άλλων νομοθεσιών [17].
- **Διασπορά Ψευδών Πληροφοριών:** Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν παραπλανητικό περιεχόμενο για να πλήξουν την αξιοπιστία ενός οργανισμού ή ατόμου, διαδίδοντας παραπληροφόρηση [35].
- **Σαμποτάζ και Αποδιοργάνωση Λειτουργιών:** Μέσω κοινωνικής μηχανικής, μπορεί να προκληθεί διακοπή επιχειρησιακών λειτουργιών και υπηρεσιών (π.χ. απενεργοποίηση κρίσιμων συστημάτων, εσωτερική σύγχυση, καθυστερήσεις στη λειτουργία, διακοπή εκτέλεσης υπηρεσιών) [36].

- **Μόλυνση με Κακόβουλο Λογισμικό:** Η επίθεση μπορεί να οδηγήσει στην εγκατάσταση malware, όπως keyloggers, trojans ή spyware, που υποκλέπτουν ή αλλοιώνουν ή καταστρέφουν δεδομένα [35]. Μάλιστα, αν η καταστροφή δεδομένων είναι ολοκληρωτική, τότε η επιχειρησιακή λειτουργία αναχαιτίζεται και υπάρχει κίνδυνος ακόμη και ύπαρξης για την επιχείρηση
- **Απώλεια Δεδομένων μέσω Ransomware:** Ειδικές μορφές κοινωνικής μηχανικής, όπως phishing, μπορούν να λειτουργήσουν ως πύλη για ransomware, προκαλώντας την πλήρη απώλεια πρόσβασης σε κρίσιμα δεδομένα [35].
- **Κατασκοπεία:** Οι επιθέσεις μπορεί να έχουν ως στόχο την απόκτηση εμπιστευτικών πληροφοριών (π.χ. εμπορικών μυστικών ή κρατικών εγγράφων) για σκοπούς κατασκοπείας [35].

Αυτές οι επιπτώσεις καθιστούν σαφές ότι η προστασία από τις επιθέσεις κοινωνικής μηχανικής είναι κρίσιμη για τη διατήρηση της ασφάλειας και της φήμης των οργανισμών και των χρηστών τους.

2.2.5 Μέτρα Αντιμετώπισης των Επιθέσεων Κοινωνικής Μηχανικής

Η αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής απαιτεί την υιοθέτηση συνδυαστικών στρατηγικών που περιλαμβάνουν τεχνολογικά, οργανωτικά και εκπαιδευτικά μέτρα. Δεδομένου ότι οι επιθέσεις στοχεύουν κυρίως στον ανθρώπινο παράγοντα, είναι σημαντικό να εφαρμοστούν λύσεις που ενισχύουν την εγρήγορση, την πρόληψη και την αντίδραση τόσο σε ατομικό όσο και σε οργανωσιακό επίπεδο:

- **Εκπαίδευση Χρηστών:** Η εκπαίδευση των εργαζομένων και των χρηστών σχετικά με τις μεθόδους κοινωνικής μηχανικής και τους κινδύνους που αυτές ενέχουν είναι απαραίτητη για την πρόληψη. Η ευαισθητοποίηση σχετικά με τις τεχνικές εξαπάτησης μπορεί να βοηθήσει τους χρήστες να αναγνωρίζουν ύποπτες δραστηριότητες και να αποφεύγουν πιθανές παγίδες [35], [37].
- **Εφαρμογή Τεχνολογικών Λύσεων:** Η χρήση τεχνολογικών μηχανισμών συμβάλλει σημαντικά στην ανίχνευση και αποτροπή επιθέσεων κοινωνικής μηχανικής. Εργαλεία όπως τα Συστήματα Πρόληψης Διαρροής Δεδομένων (Data Loss Prevention Systems - DLPS)[1] μπορούν να εντοπίζουν και να αποτρέπουν την αποστολή ευαίσθητων δεδομένων σε μη εξουσιοδοτημένους παραλήπτες μέσω email ή άλλων καναλιών επικοινωνίας, μειώνοντας έτσι τον κίνδυνο διαρροής πληροφοριών [35]. Εκτός από τα Συστήματα Πρόληψης Διαρροής Δεδομένων (DLPS), υπάρχουν και άλλα τεχνικά μέτρα που μπορούν να ενισχύσουν την ασφάλεια των πληροφοριακών συστημάτων:
    - **Sandboxing**: Απομονώνει και εκτελεί ύποπτα συνημμένα ή εφαρμογές σε ελεγχόμενο περιβάλλον ώστε να διαπιστωθεί αν είναι κακόβουλα, χωρίς να διακινδυνεύει το υπόλοιπο σύστημα [35].
    - **Monitoring**: Η συνεχής παρακολούθηση της δραστηριότητας στα δίκτυα και τα emails βοηθά στον έγκαιρο εντοπισμό ύποπτων συμπεριφορών και ανωμαλιών [35], [37].
    - **Integrity Checking**: Ελέγχει την ακεραιότητα κρίσιμων αρχείων ή συστημάτων ώστε να ανιχνευθούν μη εξουσιοδοτημένες μεταβολές που μπορεί να σχετίζονται με επίθεση και να αποκατασταθούν [35],[37].

- **Scenario-based Detection**: Εφαρμόζονται συμπεριφορικοί κανόνες ασφαλείας που καλύπτουν γνωστά μοτίβα πολύπλοκων επιθέσεων και λογαριάζουν το τρέχων περιβάλλον (context) ώστε να επιτύχουν την ταχύτερη αναγνώριση ύποπτης δραστηριότητας [35].
- **ML/DL/HL-based Detection**: Η αξιοποίηση τεχνικών μηχανικής, βαθιάς ή υβριδικής μάθησης προσφέρει δυνατότητα αυτόματης ανίχνευσης πολύπλοκων επιθέσεων που δεν είναι άμεσα ορατές, οι οποίες μπορούν να περιλαμβάνουν, συνήθως στην αρχή τους, την εφαρμογή μεθόδων κοινωνικής μηχανικής [35], [37].
- **AAA (Authentication, Authorization, Accounting)**: Η εφαρμογή ισχυρών μηχανισμών ταυτοποίησης, εξουσιοδότησης και καταγραφής ενεργειών ενισχύει τον έλεγχο πρόσβασης και επιτρέπει την ανίχνευση και απόδοση ευθύνης για κακόβουλες ενέργειες. Ένα σύστημα AAA προλαμβάνει επιθέσεις κοινωνικής μηχανικής, ιδιαίτερα μέσω μηχανισμών πολυπαραγοντικής αυθεντικοποίησης, τις ανιχνεύει μέσω ανάλυσης καταγεγραμμένων ενεργειών, καθώς και μετριάζει τις επιπτώσεις τους μέσω σωστά ρυθμισμένων κανόνων και πολιτικών πρόσβασης [35].

- **Ενίσχυση των Πρωτοκόλλων Ασφάλειας:** Η χρήση πολυπαραγοντικής ταυτοποίησης (MFA) και η αυστηρή παρακολούθηση των δικαιωμάτων πρόσβασης συμβάλλουν στην ενίσχυση της ασφάλειας των συστημάτων. Με αυτόν τον τρόπο, μειώνεται η πιθανότητα μη εξουσιοδοτημένης πρόσβασης και αυξάνεται η προστασία απέναντι σε επιθέσεις που βασίζονται στην κοινωνική μηχανική [35].
- **Πολιτικές Ασφαλείας και Έλεγχος Διαδικασιών**: Η καθιέρωση αυστηρών πολιτικών ασφαλείας και η τυποποίηση των διαδικασιών πρόσβασης και διαχείρισης δεδομένων ενισχύουν την ανθεκτικότητα των οργανισμών [35]. Παραδείγματα περιλαμβάνουν πολιτικές αποδοχής νέων πελατών, διαδικασίες επιβεβαίωσης ταυτότητας μέσω τηλεφώνου ή email, και εσωτερικά πρωτόκολλα για την κοινοποίηση ευαίσθητων πληροφοριών. Ο τακτικός έλεγχος της συμμόρφωσης με αυτές τις πολιτικές βοηθά στον εντοπισμό αδυναμιών και στην προσαρμογή των μηχανισμών προστασίας.

Η κοινωνική μηχανική παραμένει μια από τις πιο επικίνδυνες μορφές επιθέσεων, καθώς εκμεταλλεύεται τις ανθρώπινες αδυναμίες – έναν τομέα όπου η τεχνολογία από μόνη της δεν επαρκεί. Ο συνδυασμός τεχνικών λύσεων, εκπαιδευτικών προγραμμάτων και οργανωτικών πολιτικών προσφέρει την πιο ολοκληρωμένη προσέγγιση για την αποτροπή και τη διαχείριση τέτοιων απειλών.

2.3 Συστήματα DLPS (Data Loss Prevention Systems)

2.3.1 Ορισμός και Σκοπός

Τα Συστήματα Πρόληψης Διαρροής Δεδομένων (DLPS) είναι εξειδικευμένα εργαλεία ασφαλείας που εντοπίζουν, παρακολουθούν και ελέγχουν τη μεταφορά ευαίσθητων πληροφοριών για να αποτρέψουν τη μη εξουσιοδοτημένη πρόσβαση, χρήση ή διαρροή τους [1], [3]. Η εφαρμογή τους εκτείνεται σε δεδομένα που βρίσκονται σε διαφορετικές φάσεις [38]:

- **Δεδομένα σε χρήση (data-in-use):** Κατά την πρόσβαση ή επεξεργασία δεδομένων από χρήστες ή προγράμματα [39], [40].
- **Δεδομένα σε μεταφορά (data-in-motion):** Κατά τη μετάδοση πληροφοριών μέσω δικτύων [40].
- **Δεδομένα σε αποθήκευση (data-at-rest):** Κατά την αποθήκευση δεδομένων σε βάσεις δεδομένων ή συσκευές [40].

Τα DLPS είναι απαραίτητα για οργανισμούς που διαχειρίζονται εμπιστευτικές πληροφορίες, όπως ιατρικά αρχεία, οικονομικά δεδομένα και δεδομένα πελατών, διασφαλίζοντας τη συμμόρφωση με διεθνείς κανονισμούς, όπως ο GDPR [17] και το HIPAA [41].

2.3.2 Λειτουργικότητες και Βασικά Χαρακτηριστικά

Οι βασικές λειτουργικότητες των DLPS περιλαμβάνουν:

- **Ανίχνευση περιεχομένου & ταξινόμηση:** Χρησιμοποιούν τεχνολογίες, όπως data fingerprinting[42], κανονικές εκφράσεις, OCR/ML[1], [42], για να εντοπίζουν ευαίσθητα δεδομένα και να τα ταξινομούν[43] σε κατηγορίες ευαισθησίας/κρισιμότητας (π.χ. *Δημόσιο, Εσωτερικό, Εμπιστευτικό, Περιορισμένο*) και τύπους δεδομένων (π.χ. *PII, οικονομικά*), ώστε να εφαρμόζονται οι κατάλληλες πολιτικές.
    - Παράδειγμα: Ένα PDF με ΑΦΜ/ΑΜΚΑ ανιχνεύεται και επισημαίνεται ως «Εμπιστευτικό», προσθέτοντας ετικέτα/label και ενεργοποιώντας αυτόματα κανόνα κρυπτογράφησης πριν από την αποστολή του (πχ. μέσω email).
- **Ανάλυση συμφραζομένων & μοτίβων χρήσης:** Λαμβάνουν υπόψη πληροφορίες, όπως ο αποδέκτης, η γεωγραφική τοποθεσία και η ώρα αποστολής, καθώς και τα συνηθισμένα μοτίβα χρήσης/συμπεριφοράς [37] (τυπικός όγκος/συχνότητα αποστολών, συνήθεις παραλήπτες/τομείς, ώρες εργασίας, «γνωστές» συσκευές/δίκτυα), ώστε να εντοπίζονται αποκλίσεις που αυξάνουν τον κίνδυνο διαρροής [1], [44], [45].
    - Παράδειγμα**:** Χρήστης που συνήθως στέλνει μικρά έγγραφα μόνο σε εσωτερικούς παραλήπτες, επιχειρεί νύχτα από νέα συσκευή να αποστείλει αρχείο 200 MB με PII σε προσωπικό Gmail, με πολλούς εξωτερικούς παραλήπτες σε BCC(*Blind Carbon Copy* – κρυφοί παραλήπτες). Σε αυτή την περίπτωση, το DLPS θα το επισημάνει ως απόκλιση από το καθιερωμένο μοτίβο και θα ενεργοποιήσει κανόνα μπλοκαρίσματος του μηνύματος ή κρυπτογράφησης του περιεχομένου του.

- **Διαχείριση πρόσβασης:** Εφαρμογή πολιτικών και κανόνων πρόσβασης που περιορίζουν την πρόσβαση σε ευαίσθητες πληροφορίες μόνο σε εξουσιοδοτημένους χρήστες [1], [37], [44].
    - Παράδειγμα: Πρόσβαση σε φάκελο «Εμπιστευτικό–HR» μόνο από την ομάδα HR· κάθε εξαίρεση απαιτεί έγκριση προϊσταμένου.
- **Κρυπτογράφηση & απόκρυψη δεδομένων:** Υποστηρίζουν κρυπτογράφηση τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση, διασφαλίζοντας ότι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να αποκτήσουν πρόσβαση[46]. Επιπλέον, μπορεί να εφαρμόζεται data masking (στατικό ή δυναμικό) για να εμφανίζονται μόνο τμήματα των πεδίων ή ισοδύναμα tokens αντί για πραγματικές τιμές, π.χ. partial masking[1], tokenization ή format-preserving τεχνικές, ώστε να μειώνεται η έκθεση χωρίς να χάνεται η λειτουργικότητα [37], [47].
    - Παράδειγμα: Αυτόματη κρυπτογράφηση S/MIME πριν την αποστολή email που περιέχει IBAN και απόκρυψη των τελευταίων ψηφίων στο σώμα/συνημμένο· επιπλέον, δυναμικό masking αριθμού κάρτας ως 4111 11** **** 1111 ή email ως user*****@example.com, και αντικατάσταση ΑΜΚΑ με token για σκοπούς αναφορών/analytics.
- **Ειδοποιήσεις και μπλοκάρισμα:** Παρέχουν δυνατότητες ειδοποίησης ή ακόμα και αποκλεισμού ενεργειών όταν εντοπίζονται παραβάσεις πολιτικών [1], [37], [48].
    - Παράδειγμα**:** Προειδοποιητικό banner «Εντοπίστηκαν PII στο συνημμένο» με επιλογές: κρυπτογράφηση/καραντίνα/ακύρωση. Όταν το ρίσκο είναι υψηλό, εφαρμόζεται hard block (“σκληρό μπλοκάρισμα”).
- **Παρακολούθηση δεδομένων:** Συνεχής επιτήρηση σε χρήση, μεταφορά και αποθήκευση μέσω endpoint agents [37], email/web gateways και σαρωτών αποθετηρίων[1], [40], [49].
    - Παράδειγμα**:** Μπλοκάρισμα αντιγραφής αρχείου με PII σε USB και καραντίνα εξερχόμενου email που περιέχει το ίδιο αρχείο.
- **Συμμόρφωση με κανονισμούς:** Χαρτογράφηση πολιτικών σε GDPR/ISO/NIST/PCI, εφαρμογή ελαχιστοποίησης/διατήρησης και πλήρη audit trails[49].
    - Παράδειγμα**:** Αυτόματη απόδειξη (report) ότι όλα τα emails με PII κρυπτογραφήθηκαν, σύμφωνα με πολιτική ασφάλειας.
- **Παραγωγή αναφορών:** Dashboards [50] και εξαγώγιμες αναφορές για τάσεις, κατηγορίες παραβιάσεων, ψευδώς θετικά/αρνητικά και χρόνους απόκρισης [51].
    - Παράδειγμα**:** Μηνιαία αναφορά «Top 5 κανόνες DLP» και θερμικός χάρτης παραβιάσεων ανά τμήμα.
- **Δυνατότητα ανάλυσης δεδομένων:** Στατιστική ανάλυση (analytics) για tuning κανόνων, risk scoring (αξιολόγηση ρίσκου) και μείωση ψευδών συναγερμών.
    - Παράδειγμα**:** Ρύθμιση ορίων ανίχνευσης ώστε τα ψευδώς θετικά σε τιμολόγια να μειωθούν κατά 40%.
- **Ενοποίηση με οικοσύστημα ασφάλειας:** Διασύνδεση με SIEM/SOAR, IAM/IDP, KMS/PKI, EDR/MDM, CASB [44]και ticketing για ολιστική ανταπόκριση.

- Παράδειγμα**:** Σήμα DLP αποστέλλεται στο SIEM, ανοίγει αυτόματα ticket στο ServiceNow και ενεργοποιεί κρυπτογράφηση μέσω KMS.

- **Προστασία από απειλές:** Συνδυασμός DLP με anti-malware/sandboxing[1], [44], απογύμνωση μακροεντολών και ανίχνευση αιχμών (spikes) εξαγωγής δεδομένων.
    - Παράδειγμα**:** Απόρριψη συνημμένου Office με κακόβουλες μακρο-εντολές και μπλοκάρισμα ασυνήθιστου όγκου αποστολών σε εξωτερικό FTP.

2.3.3 Αρχιτεκτονικές DLPS

Σε μια «κλασική» αρχιτεκτονική DLPS, τα παρακάτω συστατικά συνεργάζονται για να καλύψουν δεδομένα σε χρήση, σε μεταφορά και σε αποθήκευση, από την ανακάλυψη/ταξινόμηση έως την επιβολή πολιτικών και την αναφορά [37]. Τα συστατικά αυτά αποτελούν ένα πρότυπο αρχιτεκτονικό blueprint για συστήματα DLPS.

(α) Μηχανή πολιτικών (Policy Engine).

Καρδιά του DLPS: ερμηνεύει κανόνες/πολιτικές και αποφασίζει ενέργειες (block, κρυπτογράφηση, masking, καραντίνα, ειδοποίηση) με προτεραιότητες/εξαιρέσεις και ιεραρχίες πολιτικών [37].

(β) Ανακάλυψη & ταξινόμηση δεδομένων (Data Discovery & Classification).

Σάρωση αποθετηρίων για data-at-rest, αναγνώριση ευαίσθητου περιεχομένου (regex, fingerprinting, dictionaries, ML) και παροχή ετικετών/βαθμών ευαισθησίας που τροφοδοτούν τη μηχανή πολιτικών [37], [42].

(γ) Παρακολούθηση & ανάλυση δεδομένων (Data-in-Motion / Data-in-Use Monitoring).

Έλεγχοι σε data-in-motion (email/web uploads) και data-in-use [37] (copy/paste, εκτύπωση, screen capture) με ταιριάσματα μοτίβων, έλεγχο περιεχομένου και ανάλυση συμφραζομένων (ποιος/τι/πότε/από πού/προς ποιον).

(δ) Παρακολούθηση δικτύου (Network Monitoring/Gateway Controls).

Έλεγχοι σε πύλες (email/web) και στο δίκτυο (SMTP/HTTP/FTP), με επιβολή πολιτικών πριν την έξοδο δεδομένων [37] (π.χ. φραγή αποστολής PII σε μη έμπιστο domain).

(ε) Απόκριση σε συμβάντα & διαχείρισή τους (Incident Response & Case Management).

Κεντρική διαχείριση περιστατικών: ειδοποιήσεις, καραντίνα/ακύρωση αποστολής, ανάθεση/workflow, τεκμηρίωση και ολοκλήρωση με SIEM/SOAR [37].

(στ) Κρυπτογράφηση & διαχείριση δικαιωμάτων (Encryption & IRM/DRM).

Αυτόματη ενεργοποίηση κρυπτογράφησης (σε μεταφορά/αποθήκευση ή end-to-end όπου υποστηρίζεται) και Information Rights Management (διαχείριση δικαιωμάτων) για έλεγχο χρήσης μετά τη διανομή (άνοιγμα/προώθηση/εκτύπωση, λήξη/ανάκληση) [37].

(ζ) Παραγωγή αναφορών & αναλυτικών (Reporting & Analytics).

Dashboards, KPI/τάσεις, audit trails για συμμόρφωση/λογοδοσία και συνεχή βελτίωση πολιτικών [51].

(η) Κεντρικοποιημένη διαχείριση & APIs (Centralized Admin & Integrations).

Ενιαία κονσόλα πολιτικών, κλειδιών, ενοποίησης με καταλόγους (AD/IdP) και APIs/Connectors προς SIEM, CASB, MDM/EDR, email gateways [37], ticketing.

(θ) Πράκτορες και συνδετήρες (Agents & Cloud Connectors).

Endpoint agents (πράκτορες τελικών σημειών) για data-in-use, cloud connectors (συνδέσεις με νέφος) για SaaS/IaaS (π.χ. email/drive/share), και gateway components (συστατικά πυλών) για email/web—κάλυψη on-prem (επιτόπιων), cloud και υβριδικών περιβαλλόντων [37].

Ροή υψηλού επιπέδου: Πράκτορες/πύλες → Συλλογή περιεχομένου & συμφραζομένων & ετικετών δεδομένων → Μηχανή πολιτικών (απόφαση) → Επιβολή (block/crypto/masking/notify) → Καταγραφή → Αναφορές/Analytics → Βελτιστοποίηση πολιτικών.

Ροή εκπαίδευσης και προσαρμογής πολιτικών: Αποτελέσματα αναφορών/Analytics → Αναγνώριση μοτίβων → Αναθεώρηση κανόνων → Ενημέρωση μηχανής πολιτικών → Νέα εφαρμογή πολιτικών στο σύστημα.

Ροή ταξινόμησης και ετικετοποίησης δεδομένων: Ανίχνευση περιεχομένου → Ανάλυση ευαισθησίας → Αντιστοίχιση με πρότυπα (PII, PHI, IP) → Ανάθεση ετικέτας (π.χ. Confidential/Internal/Public) → Ενημέρωση μηχανής πολιτικών.

Ροή ολοκλήρωσης με συστήματα ασφάλειας:DLPS → Ενοποίηση συμβάντων ασφάλειας → Αυτόματη απόκριση ή ειδοποίηση → Ανατροφοδότηση πολιτικών.

Ο παρακάτω πίνακας συνοψίζει τα προαναφερόμενα συστατικά, καλύπτοντας τον ρόλο τους, τη φάση των δεδομένων που υποστηρίζουν, την τυπική θέση που καταλαμβάνουν στο σύστημα και τις ενδεικτικές ενέργειες που μπορούν να πραγματοποιήσουν.

Πίνακας 1. Σύνοψη συστατικών DLPS.

Συστατικό	**Ρόλος**	**Καλύπτει**	**Τυπική θέση**	**Ενδεικτικές ενέργειες**
Μηχανή πολιτικών (Policy Engine)	Εφαρμόζει κανόνες & αποφασίζει ενέργειες βάσει περιεχομένου/συμφραζομένων/παραληπτών	AR/IM/IU	Κεντρικός server / cloud	Block/allow, κρυπτογράφηση, masking, καραντίνα, ειδοποίηση
Ανακάλυψη & ταξινόμηση (Discovery & Classification)	Σαρώνει αποθετήρια, εντοπίζει ευαίσθητα δεδομένα και αποδίδει βαθμούς	AR	File shares, endpoints, SaaS storage	Regex, fingerprinting, ML tagging
Παρακολούθηση & ανάλυση	Ελέγχει ροές/χρήσεις δεδομένων	IM/IU	Email/Web	Έλεγχος περιεχομένου,

δεδομένων (Data Monitoring)	με pattern & context analysis		gateways, endpoints	context risk scoring, προειδοποιήσεις
Παρακολούθηση δικτύου (Network/Gateway Controls)	Επιβάλλει πολιτικές πριν την έξοδο των δεδομένων στο δίκτυο	IM	Secure email/web gateways	Φραγές αποστολής, απομάσκιση (unmasking)/αφαίρεση συνημμένων
Απόκριση σε συμβάντα (IR & Case Mgmt)	Καταγραφή, workflow, διερεύνηση & κλιμάκωση περιστατικών	AR/IM/IU	SOC / SIEM-SOAR ολοκλήρωση	Καραντίνα, rollback/recall, ειδοποιήσεις, ticketing
Κρυπτογράφηση & δικαιώματα (Encryption & IRM/DRM)	Προστατεύει περιεχόμενο και ελέγχει χρήσεις μετά τη διανομή	AR/IM	Gateways, clients, key mgmt services	S/MIME/PGP, at-rest crypto, rights (view/print/forward), expiry
Αναφορές & analytics (Reporting & Analytics)*	KPIs, τάσεις, audit trails για συμμόρφωση & βελτίωση πολιτικών	AR/IM/IU	Κονσόλα αναφορών	Dashboards, εξαγωγές για audits
Κεντρική διαχείριση & APIs (Admin & Integrations)*	Ενιαία ρύθμιση πολιτικών/κλειδιών και ενοποίηση με τρίτα συστήματα	AR/IM/IU	Κεντρικός server / cloud	AD/IdP sync, SIEM/CASB/MDM/EDR connectors
Πράκτορες & cloud connectors (Agents & Connectors)	Κάλυψη endpoints & SaaS με τοπικούς/νεφιακούς ελέγχους	IU/AR/IM	Endpoints, SaaS/IaaS, gateways	Endpoint agent, API-based cloud scans

AR = at rest (σε αποθήκευση), IM = in motion (σε μεταφορά), IU = in use (σε χρήση).

** Σημείωση για «Αναφορές & Analytics» και «Κεντρική διαχείριση & APIs»:Λειτουργούν ως control-plane (δεν «πιάνουν» τα δεδομένα απευθείας όπως οι πράκτορες/gateways) ενώ τα υπόλοιπα είναι data-plane.Δηλαδή τα control-plane δεν επιβάλλουν πολιτικές στα δεδομένα, αλλά ενοποιούν ορατότητα, διακυβέρνηση και ενορχήστρωση σε όλα τα σημεία επιβολής. Τα δύο αυτά υποσυστήματα «σκεπάζουν» όλο το DLPS. Το Reporting & Analytics συγκεντρώνει και ενοποιεί συμβάντα/μετρήσεις από endpoints, gateways/δίκτυο και cloud αποθετήρια, παράγοντας KPIs, τάσεις και ίχνη ελέγχου. Η Κεντρική διαχείριση & APIs διανέμει πολιτικές, κλειδιά και ρυθμίσεις στα σημεία επιβολής και ενοποιεί το DLPS με τρίτα συστήματα (AD/IdP, SIEM, CASB, MDM/EDR) μέσω APIs. Επειδή εξυπηρετούν και τα τρία στάδια δεδομένων (σε αποθήκευση, σε μεταφορά, σε χρήση), επισημαίνονται ως AR/IM/IU.*

2.3.4 Πλεονεκτήματα DLPS

Τα συστήματα DLPS παρέχουν πολλαπλά οφέλη, όπως:

- **Αποτροπή διαρροών & μη εξουσιοδοτημένης πρόσβασης:** Προλαμβάνουν όχι μόνο τη διαρροή δεδομένων αλλά και τη μη εξουσιοδοτημένη πρόσβαση/χρήση τους [1], μέσω ανίχνευσης περιεχομένου–συμφραζομένων και real-time επιβολής πολιτικών (RBAC/ABAC), κρυπτογράφησης και διαχείρισης δικαιωμάτων (IRM) [37].
- **Ενίσχυση Συμμόρφωσης:** Διευκολύνουν συμμόρφωση με GDPR, HIPAA/PCI κ.λπ., μειώνοντας νομικούς κινδύνους [37].
- **Μείωση Ανθρώπινου Λάθους:** Εντοπίζουν και διορθώνουν λάθη χρηστών [37] (π.χ. λάθος παραλήπτης/συνημμένο [1]).
- **Προστασία Πνευματικής Ιδιοκτησίας (IP):** Διασφαλίζουν source code, σχέδια, R&D κ.ά. από μη εξουσιοδοτημένη διαρροή [37].
- **Μετρίαση Επιχειρησιακών Κινδύνων:** Μειώνουν πιθανότητα/αντίκτυπο περιστατικών με ελέγχους και στοχευμένες πολιτικές.
- **Ενισχυμένη Ορατότητα στη Χρήση Δεδομένων:** Κεντρικά logs/dashboards, συνεχής παρακολούθηση & μετρικές.
- **Βελτιωμένη Διαχείριση & Ταξινόμηση Δεδομένων:** Ετικετοθέτηση ευαισθησίας & κανόνες χειρισμού/διατήρησης [1], [37].
- **Προστασία από Εσωτερικές Απειλές:** Καλύπτει insiders (κακόβουλους/ακούσιους) και ανωμαλίες εξαγωγής [37].
- **Υποστήριξη Απομακρυσμένης Εργασίας:** Επιβολή πολιτικών εκτός εταιρικού δικτύου και σε SaaS [37].
- **Εξοικονόμηση Κόστους:** Μείωση κόστους περιστατικών & προστίμων μη συμμόρφωσης [37].
- **Προσωποποίηση & Κλιμακωσιμότητα:** Παραμετροποιήσιμοι κανόνες/έλεγχοι και οριζόντια κλιμάκωση [1].
- **Ανίχνευση & Απόκριση σε Πραγματικό Χρόνο:** Inline αποφάσεις (Alert/Block/Encrypt/Redact/Quarantine) και αυτοματοποίηση IR(Incident Response) [1], [37].
- **Κάλυψη Πολλαπλών Περιβαλλόντων:** Ενιαίες πολιτικές σε on-prem, cloud, hybrid, mobile περιβάλλοντα [37].
- **Ενίσχυση Κουλτούρας Ασφάλειας:** Εκπαιδευτικά banners/εξηγήσεις στη ροή εργασίας και έλεγχοι awareness [37].

2.3.5 Παραδείγματα Εμπορικών Λύσεων

- **Symantec Data Loss Prevention:** Παρέχει προστασία μέσω ανίχνευσης περιεχομένου και εφαρμογής πολιτικών αποκλεισμού σε περιβάλλοντα υπολογιστικού νέφους (cloud). Στην πράξη, η πλατφόρμα διαχειρίζεται κεντρικά πολιτικές/συμβάντα μέσω του Enforce Platform και καλύπτει discovery/monitoring/protection σε endpoints, email/web και cloud εφαρμογές[52]. Ξεχωρίζει για Exact Data Matching (EDM Ακριβής Αντιστοίχιση Δεδομένων) και Indexed Document Matching [53](IDM Αντιστοίχιση Εγγράφων μέσω Δακτυλικού Αποτυπώματος, fingerprinting) για δομημένα/αδόμητα δεδομένα, με υποστήριξη OCR(Optical Character Recognition Οπτική Αναγνώριση Χαρακτήρων) και δυνατότητες μεταφοράς των δεικτών (indexes) και σε CloudSOC (Cloud Security Operations Center πλατφόρμα ασφάλειας για υπηρεσίες cloud) για έλεγχο SaaS [54].
- **McAfee Total Protection for Data Loss Prevention:** Εστιάζει στην ανάλυση περιεχομένου και στη δυνατότητα προσαρμογής των πολιτικών. Αποτελεί σουίτα (Discover/Monitor/Prevent/Endpoint) που διαχειρίζεται κεντρικά μέσω ePolicy Orchestrator (ePO)· στους σταθμούς εργασίας ελέγχει καναλιακές ενέργειες (email, web, clipboard/εκτυπώσεις, removable media) και προσφέρει user coaching (π.χ. προτροπές για κρυπτογράφηση/μπλοκάρισμα) ώστε να μειώνει τα ακούσια λάθη. Περιλαμβάνει επίσης Device Control (έλεγχο συσκευών) και έτοιμες αναφορές/χειρισμό περιστατικών [55].
- **Forcepoint DLP:** Συνδυάζει ανάλυση συμπεριφοράς και δεδομένων για την ανίχνευση και αποτροπή απειλών. Παρέχει εκτενή βιβλιοθήκη classifiers (ταξινομητών) & regulatory templates (κανονιστικά μοτίβα), fingerprinting και ML, με ενιαία επιβολή πολιτικών σε endpoint, δίκτυο (email/web) και cloud. Περιλαμβάνει Discovery για δεδομένα at-rest (on-prem & cloud) και Network DLP για email/web/FTP, με OCR για δεδομένα μέσα σε εικόνες, και διαφορετικές άδειες χρήσης (IP Protection / Compliance) ανά περίπτωση χρήσης (use case) [56].
- **Trend Micro Integrated DLP:** Εστιάζει στη διαχείριση ευαίσθητων δεδομένων μέσω λύσεων υπολογιστικού νέφους και τελικών σημείων. Το Apex One ενσωματώνει DLP agent με πολιτικές ανά κανάλι και Device Control (π.χ. USB), ενώ το Email Security ελέγχει subject/body/attachments σε εξερχόμενα. Η κεντρική εικόνα/αναφορές παρέχονται από το Apex Central, με κανόνες/templetes, προτεραιότητες και διεργασίες logging των περιστατικών [57].

2.3.6 Προκλήσεις και Περιορισμοί

Τα DLPS αντιμετωπίζουν τις ακόλουθες προκλήσεις:

- **Αναδυόμενες Απειλές:** Η συνεχής εξέλιξη των απειλών απαιτεί τακτική ενημέρωση των κανόνων ασφαλείας. Το τοπίο αλλάζει συνεχώς (νέες τεχνικές εξαγωγής, νέοι φορείς απειλής), άρα οι πολιτικές/ανιχνευτές του DLP θέλουν διαρκή ανανέωση και tuning αλλιώς δημιουργούνται «τυφλά σημεία» [7], [37], [44].
- **Περιορισμοί Ανίχνευσης σε Κρυπτογραφημένα ή Αποκρυμμένα Δεδομένα:** Η αυξανόμενη χρήση τεχνικών κρυπτογράφησης (TLS, E2E, password-protected ή προστατευμένα αρχεία) και απόκρυψης δεδομένων (steganography, ενσωμάτωση σε εικόνες) δυσχεραίνει σημαντικά την επιθεώρηση περιεχομένου και την ανίχνευση διαρροών.Για την αντιμετώπιση των περιορισμών αυτών απαιτούνται προηγμένες μέθοδοι, όπως OCR (Optical Character Recognition – Οπτική Αναγνώριση Χαρακτήρων) ή deep content inspection, καθώς και μετατόπιση των ελέγχων στο endpoint (data-in-use) ή μέσω API επιπέδου για cloud εφαρμογές (SaaS) [1], [37], [40].
- **Ανθρώπινος Παράγοντας:** Χωρίς εκπαίδευση/ευαισθητοποίηση, οι χρήστες παρακάμπτουν πολιτικές (π.χ. shadow IT) ή κάνουν λάθη (λάθος παραλήπτης, λάθος συνημμένο), μειώνοντας την αποτελεσματικότητα του DLP [7], [44].
- **Υψηλό Κόστος Εφαρμογής:** Τα DLPS συχνά απαιτούν σημαντικούς πόρους για την αρχική εγκατάσταση και συντήρησή τους. Απαιτούνται άδειες, υποδομές (agents/gateways), αρχική ταξινόμηση δεδομένων και ενσωματώσεις (SIEM/SOAR/IDP/KMS), καθώς και συνεχιζόμενη συντήρηση [36], [37], [39].
- **Πολυπλοκότητα Υλοποίησης:** Η κάλυψη πολλών καναλιών (endpoint, email, web, cloud) και περιβαλλόντων (on-prem, hybrid, mobile) αυξάνει την αρχιτεκτονική πολυπλοκότητα και τον κίνδυνο ασυνέπειας πολιτικών [1], [37].
- **Ανακρίβεια Ανίχνευσης/Ταξινόμησης:** Οι γενικοί κανόνες παράγουν πολλά false positives, ενώ η έξυπνη «παραλλαγή» (obfuscation) οδηγεί σε false negatives· απαιτείται συνεχής ρύθμιση και τεχνικές EDM/IDM/OCR [1], [37], [48].
- **Αρνητική Επίδραση στην Παραγωγικότητα:** Υπερβολικά περιοριστικές πολιτικές (π.χ. block σε νόμιμα uploads) προκαλούν τριβές με τις καθημερινές λειτουργίες και τις ανάγκες της επιχείρησης και οδηγούν σε παρακάμψεις από τους χρήστες [40].
- **Δυσκολία Κλιμάκωσης:** Όσο αυξάνονται χρήστες/ροές/τύποι αρχείων, οι έλεγχοι deep inspection (OCR, fingerprinting) πιέζουν επιδόσεις/κόστη· χρειάζεται ελαστική αρχιτεκτονική και ιεράρχηση ελέγχων [37], [58].
- **Ανίχνευση Εξεζητημένων Εσωτερικών Απειλών:** Οι κακόβουλοι/«έμπειροι» insiders χρησιμοποιούν σταδιακή εξαγωγή, αποσπασματικά κανάλια ή κρυπτογράφηση· χρειάζεται συνδυασμός content+context+συμπεριφοράς (usage patterns) [37], [44].
- **Δυσκολία στη Μοντελοποίηση Πολιτικών:** Η μετατροπή νομικών/επιχειρησιακών απαιτήσεων σε τεχνικούς κανόνες (ποιοι τύποι δεδομένων, ποια όρια, ποιες εξαιρέσεις) είναι επίπονη και απαιτεί κύκλο δοκιμών/βελτιώσεων [45].

- **Περιορισμένη Κάλυψη Cloud/SaaS & Endpoints:** Ανομοιογενή APIs και «SaaS sprawl» δημιουργούν κενά ορατότητας· χρειάζεται συνδυασμός endpoint agents, email/web gateways και connectors ανά υπηρεσία [37], [39], [51].
- **Υψηλές Απαιτήσεις Συντήρησης & Πόρων:** Συνεχές ενημερωμένο taxonomy (ταξονομία/κατηγοριοποίηση) [36] , ανανέωση υπογραφών/προτύπων συμμόρφωσης, αναθεώρηση πολιτικών και διαχείριση περιστατικών απαιτούν ώριμες διαδικασίες/ομάδες.
- **Ζητήματα Ιδιωτικότητας (Monitoring Εργαζομένων):** Η παρακολούθηση χρήσης ICT πρέπει να σέβεται αναλογικότητα/διαφάνεια/ελαχιστοποίηση η αδιαφανής παρακολούθηση δημιουργεί νομικούς/ηθικούς κινδύνους [17].
- **Έλλειψη Κατανόησης Real-time Συμφραζομένων:** Πολλά DLP εστιάζουν στο περιεχόμενο, χωρίς πλούσια context signals (συσκευή, τοποθεσία, ρίσκο συνεδρίας), δυσκολεύοντας σωστές αποφάσεις σε πραγματικό χρόνο [44].
- **Κλείδωμα σε Πάροχο (Vendor Lock-in):** Μη φορητές πολιτικές/ταξινομήσεις και διαφορετικά formats καθιστούν δύσκολη τη μετεγκατάσταση σε άλλο προμηθευτή· απαιτείται πρόνοια για διαλειτουργικότητα/φορητότητα [37].

2.3.7 DLPS και Email Clients

Τα συστήματα πρόληψης διαρροής δεδομένων (DLPS) έχουν ιδιαίτερη σημασία όταν ενσωματώνονται σε πελάτες ηλ. αλληλογραφίας (email clients), καθώς το ηλεκτρονικό ταχυδρομείο αποτελεί ένα από τα πιο διαδεδομένα μέσα επικοινωνίας τόσο σε προσωπικό όσο και σε επαγγελματικό επίπεδο. Η ενσωμάτωση DLPS σε email clients μπορεί να διασφαλίσει την προστασία ευαίσθητων δεδομένων από ακούσιες ή σκόπιμες διαρροές [2].

2.3.7.1 Ρόλος του DLPS στους Email Clients

Οι email clients, όπως το Gmail, το Outlook και το Thunderbird, έχουν εξελιχθεί ώστε να ενσωματώνουν βασικές δυνατότητες ασφαλείας (π.χ. TLS/S/MIME, spam/phishing φίλτρα). Η ενσωμάτωση ενός DLPS σε αυτούς επεκτείνει ουσιαστικά τη λειτουργικότητά τους, προσθέτοντας:

- **Ανίχνευση ευαίσθητων πληροφοριών** στο σώμα/θέμα/συνημμένα και εμφάνιση policy tips/ειδοποιήσεων πριν την αποστολή (με δυνατότητα «block with override» όπου ταιριάζει) [59], [60].
- **Αξιολόγηση παραληπτών και συμφραζομένων** (εσωτερικοί/εξωτερικοί, domain/χώρα, μέγεθος/τύπος συνημμένων, ώρα/συσκευή) και εφαρμογή ενεργειών, όπως μπλοκάρισμα, καραντίνα ή τροποποίηση [59], [61].
- **Αυτόματες ειδοποιήσεις & alerts** για πιθανά περιστατικά διαρροής πριν την αποστολή (π.χ. ύπαρξη PII/ευαίσθητων) [50].
- **Εφαρμογή πολιτικών** αποτροπής αποστολής μη εξουσιοδοτημένων μηνυμάτων (π.χ. Απόρριψη/Καραντίνα/Τροποποίηση/Αφαίρεση συνημμένων) [59], [61].
- **Κρυπτογράφηση μηνυμάτων & συνημμένων** (π.χ. S/MIME, OME) βάσει πολιτικής/περιεχομένου και απαίτηση ασφαλούς μεταφοράς (TLS) [62].

- **Διαχείριση δικαιωμάτων** (IRM/Sensitivity Labels): περιορισμοί σε προώθηση/εκτύπωση/λήψη, λήξη πρόσβασης, υδατογραφήματα [63].
- **Ανίχνευση & μπλοκάρισμα** ύποπτης εξαγωγής (π.χ. μαζικές αποστολές σε άγνωστους εξωτερικούς χρήστες, ασυνήθιστα μεγάλα συνημμένα, υπερβολικό BCC, αποστολές εκτός ωραρίου) [44], [50].
- **Αφαίρεση/τροποποίηση** περιεχομένου πριν την αποστολή με συναίνεση χρήστη: redaction/masking ευαίσθητων πεδίων, αφαίρεση συνημμένων, αντικατάσταση με ασφαλές σύνδεσμο (link) [59], [61].
- **Ενισχυμένη ορατότητα & αναφορές** καταγραφή συμβάντων DLP, dashboards/στατιστικά, eDiscovery/αρχειοθέτηση (π.χ. Vault, Activity Explorer) [38], [50].
- **Ενοποίηση με το οικοσύστημα ασφάλειας** SIEM/SOAR για αυτοματοποίηση απόκρισης, CASB για SaaS, KMS/HSM για κλειδιά, IAM/IdP για RBAC/ABAC [64].
- **Απρόσκοπτη ενσωμάτωση στην εμπειρία χρήστη** tips/προτάσεις μέσα στο παράθυρο σύνταξης χωρίς διακοπή ροής (compose/reply) [59], [60].

Σημείωση για το υπό ανάπτυξη Gmail add-on: αξιοποιούνται οι native πολιτικές του Gmail Admin (Attachment/Content Compliance για reject/quarantine/modify/remove, require TLS) σε συνδυασμό με S/MIME και διακριτικές policy tips ώστε να μην επιβαρύνεται η εμπειρία χρήστη.

2.3.7.2 Οφέλη της Ενσωμάτωσης DLPS σε Email Clients

Η ενσωμάτωση μηχανισμών DLP απευθείας μέσα στον email client μεταφέρει τον έλεγχο εκεί όπου τα δεδομένα δημιουργούνται και αποστέλλονται (data-in-use, data-in-motion). Έτσι, η επιβολή πολιτικών γίνεται προληπτικά πριν φύγει το μήνυμα, συνδυάζοντας ανάλυση περιεχομένου με συμφραζόμενα (παραλήπτες, συσκευή, τοποθεσία, ώρα) και παρέχοντας ενιαία ορατότητα/συμμόρφωση χωρίς να διαταράσσεται η καθημερινή ροή εργασίας.

Τα βασικά οφέλη συνοψίζονται ως εξής:

- **Πρόληψη διαρροών & μη εξουσιοδοτημένης πρόσβασης:** Προ-αποστολική ανίχνευση ευαίσθητου περιεχομένου, εφαρμογή κανόνων ανά παραλήπτη/τομέα/συσκευή και επιβολή προστατευτικών ενεργειών (block, quarantine, hold-for-review, κρυπτογράφηση), ώστε να αποτραπεί τόσο η τυχαία όσο και η σκόπιμη εκροή [44].
- **Συμμόρφωση με κανονισμούς & πολιτικές:** Ενοποιημένοι κανόνες, labeling/ταξινόμησης και αρχειοθέτησης/eDiscovery διευκολύνουν την τεκμηρίωση συμμόρφωσης (π.χ. GDPR), μειώνοντας νομικούς κινδύνους και έκθεση σε πρόστιμα [17].
- **Ενισχυμένη ορατότητα & ιχνηλασιμότητα:** Κεντρική καταγραφή συμβάντων DLP, dashboards/αναφορές, Activity Explorer και εξαγωγή logs σε SIEM παρέχουν πλήρη εικόνα για ροές δεδομένων και παραβιάσεις [50].

- **Κρυπτογράφηση & διαχείριση δικαιωμάτων (IRM):** Αυτόματη κρυπτογράφηση μηνυμάτων/συνημμένων (π.χ. S/MIME/OME) και περιορισμοί χρήσης (no forward/print, expiry, υδατογραφήματα) για έλεγχο μετά την αποστολή [62].
- **Προστασία πνευματικής ιδιοκτησίας & επιχειρησιακών μυστικών:** Ταξινόμηση/σφράγιση εμπιστευτικών εγγράφων, πολιτικές διαμοιρασμού και αποτροπή εξαγωγής IP σε μη εγκεκριμένους προορισμούς [4].
- **Μετρίαση insider risk & κοινωνικής μηχανικής:** Συνδυασμός περιεχομένου-συμφραζομένων-μοτίβων χρήσης, προειδοποιήσεις (policy tips) και ελεγχόμενα overrides (επιτρέπουν στον χρήστη να παρακάμψει προσωρινά έναν κανόνα ασφαλείας, με καταγραφή και αιτιολόγηση της ενέργειας) μειώνουν ακούσιες «αστοχίες» και εντοπίζουν ύποπτη συμπεριφορά [44], [60].
- **Καλύτερη διαχείριση & ταξινόμηση δεδομένων:** Εφαρμογή labels/ευαισθησίας, πρότυπα αναγνώρισης και content inspection βοηθούν να ξέρουμε τι είναι κρίσιμο και πώς πρέπει να διακινείται μέσω email [4], [63].
- **Υποστήριξη απομακρυσμένης εργασίας & BYOD :** Ενιαίες πολιτικές για προστασία δεδομένων ανεξαρτήτως τοποθεσίας/συσκευής, επιβολή ασφαλών καναλιών (TLS) και έλεγχος συνημμένων/συνδέσμων πριν βγουν εκτός οργανισμού[44].
- **Ανίχνευση & απόκριση σε πραγματικό χρόνο:** Alerts, auto-quarantine και ενοποίηση με SOAR για γρήγορη αντιμετώπιση περιστατικών που ξεκινούν από το email [45], [60].
- **Ενοποίηση με το οικοσύστημα ασφάλειας:** Διασύνδεση με SIEM/SOAR, CASB και KMS/HSM για ενιαίες πολιτικές, καλύτερη ορατότητα σε SaaS και ασφαλή διαχείριση κλειδιών[64].
- **Θετική εμπειρία χρήστη & κουλτούρα ασφάλειας:** Ενσωμάτωση στον email client με διακριτικά hints/προτάσεις, ώστε ο χρήστης να «μαθαίνει» σωστές συμπεριφορές χωρίς να διαταράσσεται η ροή του[60].
- **Μείωση κόστους συμβάντων & λειτουργικής επιβάρυνσης:** Λιγότερα περιστατικά εκροής, αυτοματοποιημένοι έλεγχοι και στοχευμένες αναφορές περιορίζουν κόστος διερεύνησης, αποκατάστασης και μη συμμόρφωσης[44].

**BYOD(Bring Your Own Device): πολιτική που επιτρέπει στους εργαζόμενους να χρησιμοποιούν προσωπικές συσκευές για πρόσβαση σε εταιρικά δεδομένα, με εφαρμογή των ίδιων κανόνων ασφάλειας όπως στα εταιρικά συστήματα.*

2.3.8 Συμπεράσματα σχετικά με τα DLPS

Τα Συστήματα Πρόληψης Διαρροής Δεδομένων (DLPS) αποτελούν κρίσιμο πυλώνα για τη διασφάλιση της ασφάλειας δεδομένων, ιδιαίτερα σε ένα συνεχώς εξελισσόμενο ψηφιακό περιβάλλον, όπου η διαχείριση ευαίσθητων πληροφοριών είναι ζωτικής σημασίας. Τα DLPS, με τις πολυδιάστατες δυνατότητές τους, όπως η ανίχνευση περιεχομένου, η ανάλυση συμφραζομένων, η κρυπτογράφηση δεδομένων και η εφαρμογή πολιτικών ασφαλείας, παρέχουν μια ολοκληρωμένη λύση για την αποτροπή διαρροών και μη εξουσιοδοτημένης πρόσβασης σε όλα τα επίπεδα: κατά τη χρήση, τη μεταφορά και την αποθήκευση δεδομένων. Παράλληλα, διευκολύνουν τη συμμόρφωση με κανονιστικά πλαίσια, όπως τον GDPR, μειώνοντας τους νομικούς κινδύνους και ενισχύοντας την εμπιστοσύνη των χρηστών.

Η συνεχής ανάπτυξη και εξέλιξη των DLPS είναι απαραίτητη για την αντιμετώπιση των σύγχρονων απειλών, όπως οι επιθέσεις κοινωνικής μηχανικής και η εκμετάλλευση ανθρώπινων λαθών. Η δυνατότητά τους να προσαρμόζονται στις ανάγκες κάθε οργανισμού, σε συνδυασμό με την ευελιξία εφαρμογής τους σε διάφορους τομείς, τα καθιστά απαραίτητα εργαλεία για την προστασία της ακεραιότητας και της εμπιστευτικότητας των πληροφοριών.

Παρά τα πλεονεκτήματά τους, τα DLPS συστήματα αντιμετωπίζουν προκλήσεις, όπως η δυσκολία ανάλυσης κρυπτογραφημένων/στεγανοποιημένων δεδομένων και η ανάγκη συνεχούς αναβάθμισης των κανόνων ασφαλείας για την αντιμετώπιση νέων μορφών απειλών. Ωστόσο, η επένδυση στην εφαρμογή τους μπορεί να προσφέρει μακροπρόθεσμα οφέλη, μειώνοντας τους κινδύνους διαρροής και αυξάνοντας τη συνολική ασφάλεια. Η ανάπτυξη εργαλείων DLPS, όπως το προτεινόμενο πρόσθετο για το Gmail, ενισχύει την πρακτική εφαρμογή αυτών των συστημάτων, καθιστώντας την προστασία δεδομένων πιο προσιτή και ευέλικτη. Η εστίαση των προσπαθειών σχεδιασμού, ανάπτυξης και συνεχούς βελτίωσης των DLPS πρέπει να παραμένει στις ίδιες τις δυνατότητές τους και στην εξέλιξη των μηχανισμών τους, ώστε να προσφέρουν συνεχή κάλυψη έναντι των απειλών και να ανταποκρίνονται στις αυξανόμενες απαιτήσεις ασφάλειας. Σε έναν κόσμο όπου οι διαρροές δεδομένων μπορούν να προκαλέσουν σοβαρές επιπτώσεις, τα DLPS αποτελούν αναγκαία και ανεκτίμητα εργαλεία για την προστασία των πληροφοριών.

2.4 Επικοινωνία μέσω Email

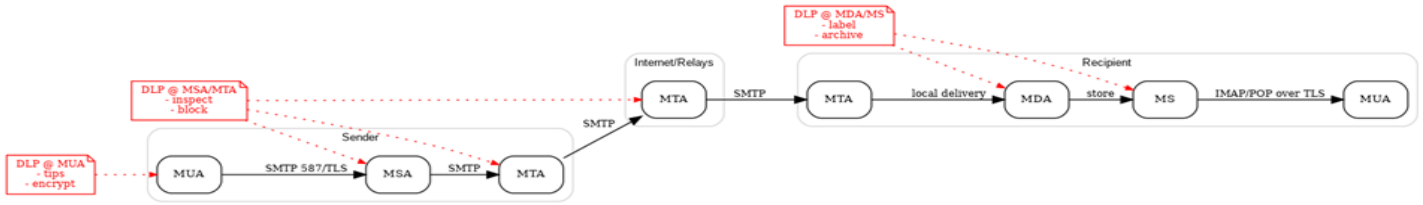
Το ηλεκτρονικό ταχυδρομείο είναι το κύριο μέσο ψηφιακής επικοινωνίας για προσωπικές και επαγγελματικές συναλλαγές και ταυτόχρονα ένα από τα πιο ευάλωτα κανάλια σε απειλές και επιθέσεις. Εξαιτίας της σημασίας του, έχουν αναπτυχθεί διάφορα πρωτόκολλα και τεχνολογίες για να εξασφαλίσουν την ασφάλεια των μηνυμάτων και να διασφαλίσουν ότι οι ευαίσθητες πληροφορίες παραμένουν προστατευμένες.

2.4.1 Συστατικά του Συστήματος Email

Η αρχιτεκτονική του Internet Mail διακρίνει **λογικούς ρόλους/συστατικά** που συνεργάζονται για τη σύνταξη, την υποβολή, τη διαβίβαση, την παράδοση και την πρόσβαση στα μηνύματα. Τα βασικά συστατικά είναι τα εξής [65]:

- **Message User Agent (MUA):** Η εφαρμογή του χρήστη (π.χ. Gmail στο web, Outlook, Thunderbird) με την οποία συντάσσει, στέλνει και διαβάζει email. Ο MUA παράγει/καταναλώνει μηνύματα και δεν κάνει δρομολόγηση. Στο πλαίσιο DLP, εδώ μπορούν να μπουν policy tips/προειδοποιήσεις και client-side έλεγχοι πριν την αποστολή [65].
- **Mail Submission Agent (MSA):** Η υπηρεσία που **παραλαμβάνει προς υποβολή** ένα έτοιμο μήνυμα από τον MUA (συνήθως στην θύρα 587) και ελέγχει συμμόρφωση με πολιτικές/πρότυπα (π.χ. επικύρωση envelope, authentication, rewrite headers αν απαιτείται). Από εδώ αρχίζει η «επίσημη» διακίνηση μηνύματος στο δίκτυο [65], [66].
- **Message Transfer Agent (MTA):** Η «μηχανή μεταφοράς» που **διαβιβάζει hop-by-hop** τα μηνύματα μεταξύ τομέων με SMTP, μέχρι να φτάσουν στον εξυπηρετητή του παραλήπτη (ή σε επόμενο ενδιάμεσο). Οι MTA μπορούν να αλυσοδένονται (π.χ. μεταγωγές, relays, gateways) [65], [67].
- **Mail Delivery Agent (MDA):** Η συνιστώσα που **παραδίδει** το μήνυμα από τον τελικό MTA στον **Message Store (MS)** του παραλήπτη/θυρίδας (π.χ. τοπικό mailbox, maildir, server store), εφαρμόζοντας τελευταίους κανόνες ταξινόμησης/φιλτραρίσματος [65].
- **Message Store (MS):** Το υποσύστημα **αποθήκευσης** όπου διατηρούνται τα εισερχόμενα/φακελωμένα μηνύματα, από όπου στη συνέχεια οι MUA τα ανακτούν μέσω πρωτοκόλλων πρόσβασης [65].
- **Πρωτόκολλα πρόσβασης (IMAP/POP):** Ο MUA συνδέεται στο MS για ανάγνωση/διαχείριση αλληλογραφίας μέσω **IMAP4rev1** (συγχρονισμός φακέλων, flags) ή **POP3** (λήψη/τοπική διαχείριση) [68], [69].

<u>Σημείωση ορολογίας</u>: ο προγενέστερος όρος Mail Access Agent (MAA) απαντάται ως γενίκευση των υπηρεσιών πρόσβασης στα σύγχρονα κείμενα των RFC η πρόσβαση περιγράφεται μέσω IMAP/POP προς τον Message Store και όχι ως ξεχωριστός «agent»[65] .



Εικόνα 1. Ροή άκρου-σε-άκρο στη λειτουργία του συστήματος email.

**Εικόνα 1: απεικόνιση των βασικών συστατικών και ενδεικτικών σημείων εφαρμογής DLP ελέγχων κατά τη διακίνηση των μηνυμάτων. Προσαρμογή και σύνθεση βάσει των Figures 1–3 του RFC 5598: Internet Mail Architecture (IETF, 2009[65]).*

Πώς συνεργάζονται (άκρο-σε-άκρο ροή):

1. Ο MUA συντάσσει το μήνυμα και το υποβάλλει στον MSA.
2. Ο MSA το επικυρώνει/κανονικοποιεί και το προωθεί σε MTA.
3. Ένα ή περισσότερα MTA το διαβιβάζουν SMTP hop-by-hop μέχρι τον τομέα του παραλήπτη.
4. Ο τελικός MTA το παραδίδει μέσω MDA στον Message Store.
5. Ο παραλήπτης, μέσω MUA, προσπελαύνει το MS με IMAP/POP για να διαβάσει/διαχειριστεί το μήνυμα.

Τα συστατικά του συστήματος email λειτουργούν συνδυαστικά για τη μεταφορά, αποθήκευση και διαχείριση των μηνυμάτων. Κάθε τμήμα παίζει σημαντικό ρόλο στην εξασφάλιση της αποτελεσματικής επικοινωνίας και συμβάλλει στην ενίσχυση της ασφάλειας των μηνυμάτων, δημιουργώντας μια βασική υποδομή για την προστασία των δεδομένων κατά τη μεταφορά τους [65], [67], [68].

2.4.2 Πρωτόκολλα Επικοινωνίας και Επίπεδα Ασφαλείας

Για την ασφαλή μετάδοση και πρόσβαση στα μηνύματα, χρησιμοποιούνται βασικά πρωτόκολλα:

- **SMTP (Simple Mail Transfer Protocol):** Είναι το βασικό πρωτόκολλο για την αποστολή email. Η ασφάλεια επιτυγχάνεται με STARTTLS, το οποίο αναβαθμίζει τη σύνδεση σε TLS ώστε τα δεδομένα να είναι κρυπτογραφημένα (παρέχεται εμπιστευτικότητα). Όταν ο εξυπηρετητής ελέγχει σωστά το πιστοποιητικό (αλυσίδα εμπιστοσύνης και όνομα κεντρικού), το TLS συμβάλλει και στην αυθεντικότητα του αντισυμβαλλόμενου, μειώνοντας τον κίνδυνο επιθέσεων «άνθρωπος-στη-μέση» (Man-in-the-Middle) [70], [71].
- **IMAP (Internet Message Access Protocol) και POP3 (Post Office Protocol v3).** Τα δύο πρωτόκολλα χρησιμοποιούνται από τον πελάτη email για πρόσβαση στα μηνύματα που έχουν ήδη παραδοθεί στον διακομιστή. Το IMAP συγχρονίζει φακέλους/κατάσταση στο server (π.χ. αναγνωσμένα, ετικέτες) και ενδείκνυται όταν θέλουμε την ίδια εικόνα αλληλογραφίας σε πολλές συσκευές. Το POP3 είναι πιο απλό: συνήθως «κατεβάζει» τα μηνύματα στον υπολογιστή/κινητό και (παραδοσιακά) μπορεί να τα αφαιρεί από τον server. Και τα δύο μπορούν να χρησιμοποιούν TLS ώστε η πρόσβαση να γίνεται με

ασφάλεια. Σε αντίθεση με αυτά, το SMTP αφορά τη διακίνηση/αποστολή μηνυμάτων μεταξύ συστημάτων [68], [69], [72].

- **Μηχανισμοί επαλήθευσης αποστολέα και ακεραιότητας (anti-spoofing).**
  SPF: το domain του αποστολέα δημοσιεύει στο DNS ποιοι διακομιστές επιτρέπεται να στέλνουν email «εκ μέρους του». Ο παραλήπτης ελέγχει αν το εισερχόμενο μήνυμα προήλθε από επιτρεπόμενη διεύθυνση. Μειώνει το spoofing στο επίπεδο διεύθυνσης αποστολής [73].
  DKIM: ο αποστολέας «υπογράφει» κρυπτογραφικά τμήματα του μηνύματος (headers/σώμα) και ο παραλήπτης επαληθεύει την υπογραφή με το δημόσιο κλειδί από το DNS. Έτσι διασφαλίζονται η ακεραιότητα του περιεχομένου και η σύνδεσή του με συγκεκριμένο domain [74].
  DMARC: συνδυάζει SPF/DKIM και ελέγχει αν «ευθυγραμμίζονται» με το From: που βλέπει ο χρήστης. Ο domain ιδιοκτήτης δηλώνει πολιτική (none/quarantine/reject) και ζητά αναφορές για τα αποτελέσματα (εφαρμογής της πολιτικής από τον server). Μειώνει δραστικά τις πλαστογραφήσεις αποστολέα [75].
- **End-to-End Κρυπτογράφηση (E2E).**
  Η end-to-end κρυπτογράφηση προστατεύει το περιεχόμενο του email από τη στιγμή που δημιουργείται έως τη στιγμή που παραλαμβάνεται, εξασφαλίζοντας ότι μόνο ο αποστολέας και ο παραλήπτης μπορούν να το διαβάσουν. Σε αντίθεση με το TLS/STARTTLS, που προστατεύει μόνο το κανάλι μεταφοράς, η E2E κρυπτογράφηση θωρακίζει το ίδιο το περιεχόμενο του μηνύματος.

  S/MIME (Secure/Multipurpose Internet Mail Extensions) βασίζεται σε ψηφιακά πιστοποιητικά (X.509) και χρησιμοποιεί ασύμμετρη κρυπτογράφηση για την προστασία και την υπογραφή των email. Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη, ενώ η ψηφιακή υπογραφή εγγυάται την ακεραιότητα και την αυθεντικότητα του περιεχομένου. Υποστηρίζεται ευρέως σε εταιρικά περιβάλλοντα (π.χ. Outlook, Exchange) και απαιτεί ύπαρξη Public Key Infrastructure (PKI) [76], [77].

  OpenPGP (Pretty Good Privacy) παρέχει επίσης end-to-end κρυπτογράφηση με χρήση δημόσιων και ιδιωτικών κλειδιών, αλλά βασίζεται σε αποκεντρωμένο μοντέλο εμπιστοσύνης (Web of Trust) αντί για κεντρική αρχή πιστοποίησης. Ο χρήστης δημιουργεί το δικό του ζεύγος κλειδιών και ανταλλάσσει το δημόσιο κλειδί με τους παραλήπτες. Η υπογραφή εγγυάται την αυθεντικότητα, ενώ η κρυπτογράφηση προστατεύει το περιεχόμενο καθ’ όλη τη διαδρομή του μηνύματος [78], [79].

Συνοψίζοντας, τα βασικά πρωτόκολλα επικοινωνίας (SMTP για αποστολή, IMAP/POP3 για πρόσβαση) σε συνδυασμό με τους μηχανισμούς ασφάλειας (TLS/STARTTLS για κρυπτογράφηση καναλιού και SPF/DKIM/DMARC για επαλήθευση και ακεραιότητα) συγκροτούν μια στιβαρή «γραμμή άμυνας» για το email. Η κρυπτογράφηση μειώνει τον κίνδυνο υποκλοπής, ενώ ο έλεγχος ταυτότητας και η ευθυγράμμιση domain περιορίζουν πλαστογραφήσεις και καταχρήσεις του πεδίου From:. Όταν αυτά εφαρμόζονται ορθά και συνδυάζονται με πρόσθετες πρακτικές (π.χ. ισχυρή πιστοποίηση χρηστών, τακτική παρακολούθηση αναφορών αποτυχιών, σωστή διαχείριση πιστοποιητικών), ενισχύουν ουσιαστικά την εμπιστευτικότητα και την ακεραιότητα της επικοινωνίας. Για ιδιαίτερα ευαίσθητο περιεχόμενο, η end-to-end κρυπτογράφηση (π.χ. S/MIME/PGP) προσφέρει επιπλέον θωράκιση πάνω από την ασφάλεια μεταφοράς. Τέλος, η σύζευξη αυτών των πρωτοκόλλων με μηχανισμούς DLP και οργανωτικές πολιτικές συμπληρώνει την άμυνα σε βάθος, διασφαλίζοντας ότι τόσο τα κανάλια μετάδοσης όσο και το ίδιο το περιεχόμενο προστατεύονται αποτελεσματικά.

2.4.3 Πελάτες Email και Βασικά Χαρακτηριστικά Ασφαλείας

Διάφοροι δημοφιλείς πελάτες email εφαρμόζουν τα παραπάνω πρωτόκολλα και τεχνολογίες για την προστασία των χρηστών τους. Οι δυνατότητες ποικίλλουν ανά πλατφόρμα, αλλά συνήθως περιλαμβάνουν ασφαλή μεταφορά (TLS/STARTTLS), μηχανισμούς επαλήθευσης αποστολέα (SPF/DKIM/DMARC), φίλτρα phishing/malware και, όπου υποστηρίζεται, κρυπτογράφηση από άκρο σε άκρο (S/MIME ή/και OpenPGP):

- **Gmail:** Το Gmail χρησιμοποιεί STARTTLS/TLS για την κρυπτογράφηση των μηνυμάτων κατά τη μεταφορά και διαθέτει εξελιγμένα φίλτρα spam/anti-malware, έλεγχο συνδέσμων και συνημμένων πριν την παράδοση και εμφανείς προειδοποιήσεις για ύποπτα μηνύματα [80]. Υποστηρίζει μηχανισμούς επαλήθευσης αποστολέα SPF, DKIM και DMARC, μειώνοντας δραστικά το spoofing και τις επιθέσεις phishing [81], [82], [83]. Επιπλέον, σε περιβάλλοντα Google Workspace διατίθεται Hosted S/MIME για κρυπτογράφηση/υπογραφή end-to-end όπου απαιτείται [84].
- **Outlook:** Πέρα από την ασφαλή μεταφορά (STARTTLS σε SMTP) και την κρυπτογραφημένη πρόσβαση (IMAPS/SMTPS/POPS), το Outlook διαθέτει ισχυρά φίλτρα ανεπιθύμητης αλληλογραφίας/κακόβουλου περιεχομένου και αξιοποιεί τους μηχανισμούς επαλήθευσης αποστολέα SPF, DKIM και DMARC (στο οικοσύστημα Exchange/Microsoft 365) για περιορισμό spoofing/phishing[85]. Υποστηρίζει επίσης S/MIME για κρυπτογράφηση και ψηφιακή υπογραφή email [86].
- **Mozilla Thunderbird:** Ανοιχτού κώδικα πελάτης email που υποστηρίζει όλο το φάσμα των μηχανισμών ασφάλειας: ασφαλή πρόσβαση/μεταφορά (STARTTLS/TLS σε IMAP/POP/SMTP), ενσωματωμένο OpenPGP (PGP) και S/MIME — το τελευταίο λειτουργεί όταν εγκατασταθούν τα προσωπικά πιστοποιητικά του χρήστη από έμπιστη CA[87], [88]. Και οι δύο επιλογές παρέχουν end-to-end κρυπτογράφηση και ψηφιακή υπογραφή (το S/MIME στηρίζεται σε πιστοποιητικά X.509, το OpenPGP σε ζεύγη δημόσιου/ιδιωτικού κλειδιού). Επιπλέον, διαθέτει προσαρμοστικά φίλτρα ανεπιθύμητης αλληλογραφίας και βασικές δικλείδες ,όπως προειδοποιήσεις για ύποπτους συνδέσμους,

αποκλεισμό αυτόματης φόρτωσης εξωτερικών εικόνων και έλεγχο υπογραφής/πιστοποιητικών στα μηνύματα, κατά phishing/κακόβουλων συνημμένων[89].

Οι δημοφιλείς πελάτες email, όπως το Gmail, το Outlook και το Thunderbird, προσφέρουν ενσωματωμένα εργαλεία ασφάλειας που μειώνουν τις απειλές για τα δεδομένα των χρηστών. Αυτές οι πλατφόρμες εφαρμόζουν ισχυρά πρωτόκολλα κρυπτογράφησης, φίλτρα ανεπιθύμητης αλληλογραφίας και προστασία από phishing, προσφέροντας ασφαλέστερη εμπειρία χρήσης.

Συνολικά, παρέχουν ασφαλή μεταφορά με TLS/STARTTLS, φίλτρα spam/phishing και υποστήριξη SPF/DKIM/DMARC για μείωση πιθανότητας spoofing. Η βασική διαφορά είναι στην end-to-end κρυπτογράφηση: το Thunderbird υποστηρίζει εγγενώς OpenPGP και S/MIME, το Outlook (ιδίως σε desktop) S/MIME με εγκατεστημένα πιστοποιητικά, ενώ το Gmail διαθέτει S/MIME κυρίως στο Google Workspace. Το OpenPGP δεν είναι εγγενές σε Gmail/Outlook, αλλά μπορεί να προστεθεί με εργαλεία τρίτων (π.χ. FlowCrypt, Gpg4win/GpgOL). Έτσι, για «έτοιμη» E2E κρυπτογράφηση το Thunderbird υπερέχει, ενώ Gmail/Outlook καλύπτουν επιχειρησιακά σενάρια μέσω S/MIME και σχετικών πολιτικών.

Πίνακας 2. Συγκριτική παρουσίαση χαρακτηριστικών ασφάλειας των δημοφιλέστερων πελατών email.

Δυνατότητα	**Gmail**	**Outlook**	**Thunderbird**
Ασφαλής μεταφορά (TLS/STARTTLS) σε SMTP/IMAP/POP	✓	✓	✓
SPF / DKIM / DMARC (anti-spoofing)	✓	✓	~ (εξαρτάται από server/πρόσθετα προβολής)
Φίλτρα spam/phishing & anti-malware	✓	✓	✓
S/MIME (ενσωματωμένο)	~ (κυρίως **Google Workspace**/Hosted S/MIME)	✓ (ιδίως **desktop**/M365 με πιστοποιητικά)	✓
OpenPGP/PGP (ενσωματωμένο)	×	×	✓

OpenPGP μέσω πρόσθετων	~ (π.χ. **FlowCrypt**[1])	~ (π.χ. **Gpg4win/GpgOL**[2])	– (δεν χρειάζεται, είναι εγγενές)
Έλεγχος/προειδοποιήσεις για συνδέσμους & συνημμένα	✓	✓	~ (βασικές προειδοποιήσεις)
Διαχείριση κλειδιών/πιστοποιητικών για E2E	~ (admin-managed σε Workspace)	✓ (ενσωμάτωση με Windows cert store / M365)	✓ (ενσωματωμένος OpenPGP Key Manager & S/MIME)
Οργανωσιακή κρυπτογράφηση/πολιτικές	~ (Hosted S/MIME, Workspace policies)	✓ (π.χ. **OME**/Purview, M365 policies[3])	~ (κυρίως μέσω server-side πολιτικών /πρόσθετων)

✓ = Υποστηρίζεται εγγενώς , ~ = Υποστηρίζεται υπό προϋποθέσεις/μερικώς,
× = Δεν υποστηρίζεται εγγενώς, – = Μη εφαρμόσιμο/δεν χρειάζεται.

[1] FlowCrypt επέκταση ανοιχτού κώδικα για Gmail και άλλους πελάτες email, που προσφέρει υποστήριξη OpenPGP για end-to-end κρυπτογράφηση και ψηφιακές υπογραφές.

[2] Gpg4win / GpgOL σουίτα εργαλείων ανοιχτού κώδικα για Windows, που ενσωματώνει το πρωτόκολλο OpenPGP στο Outlook μέσω του πρόσθετου GpgOL, επιτρέποντας κρυπτογράφηση, υπογραφές και διαχείριση κλειδιών

[3] Microsoft Office Message Encryption (OME) αποτελεί υπηρεσία κρυπτογράφησης του οικοσυστήματος Microsoft 365, βασισμένη στο Azure Rights Management και το Microsoft Purview Information Protection, η οποία επιτρέπει την αποστολή και λήψη προστατευμένων μηνυμάτων μέσω Outlook ή browser. Οι Microsoft 365 DLP Policies, που διαχειρίζονται κεντρικά μέσω Microsoft Purview, ορίζουν κανόνες για την ανίχνευση και αυτόματη προστασία ευαίσθητων δεδομένων (π.χ. PII, οικονομικά στοιχεία), ενεργοποιώντας ενέργειες όπως μπλοκάρισμα, ειδοποίηση ή κρυπτογράφηση μέσω OME.

2.4.4 Συμπεράσματα σχετικά με την επικοινωνία μέσω Email

Η επικοινωνία μέσω email αποτελεί βασικό μέσο ανταλλαγής πληροφοριών, ωστόσο οι εγγενείς απειλές απαιτούν τη χρήση ισχυρών μέτρων ασφάλειας. Παρά το γεγονός ότι οι δημοφιλείς πελάτες email, όπως το Gmail και το Outlook, παρέχουν βασικές λειτουργίες προστασίας, όπως κρυπτογράφηση, φίλτρα ανεπιθύμητης αλληλογραφίας και μέτρα κατά των επιθέσεων phishing, αυτά τα χαρακτηριστικά μπορεί να μην επαρκούν από μόνα τους. Για την πλήρη προστασία από σύγχρονες και εξελιγμένες επιθέσεις, συστήνεται η χρήση επιπλέον εργαλείων ασφαλείας, όπως συστήματα πρόληψης διαρροής δεδομένων (DLPS), προηγμένες μέθοδοι ταυτοποίησης, και εκπαίδευση των χρηστών σχετικά με τις απειλές, ώστε να ενισχυθεί η συνολική ασφάλεια στην επικοινωνία μέσω email.

3

Σχετικές Εργασίες

3.1 Ερευνητικές προσεγγίσεις σε συστήματα DLPS (γενικά)

Η βιβλιογραφία κατηγοριοποιεί τα DLPS ανά κατάσταση δεδομένων—data-in-motion, data-at-rest, data-in-use—και προτείνει τεχνικές, όπως content inspection (regex, fingerprinting, dictionaries), ανάλυση συμφραζομένων/κινδύνου (ποιος/τι/πότε/πού/προς ποιον), καθώς και ML/NLP για αναγνώριση μοτίβων και μείωση ψευδώς θετικών. Παράλληλα, εξετάζονται ζητήματα κάλυψης καναλιών (email, web, cloud, endpoint) και εκφραστικότητας πολιτικών, με έμφαση στη συμμόρφωση και την απόδοση σε πραγματικά περιβάλλοντα [1], [90]. Η ανάγκη για DLPS εντείνεται από σύγχρονες απειλές (phishing, εξαγωγή δεδομένων, insider) όπως καταγράφονται στα ετήσια Threat Landscape (σύνολο των υπαρκτών και αναδυόμενων απειλών που στοχεύουν ένα σύστημα, οργανισμό ή δίκτυο σε μια δεδομένη χρονική περίοδο) [91].

3.2 DLPS για ηλεκτρονική αλληλογραφία: μορφές και ρόλοι

Παρακάτω συνοψίζουμε τις μορφές που μπορεί να πάρει ένα DLPS και τον ρόλο που μπορεί να επιτελέσει σε ένα σύστημα στο οποίο ενσωματώνεται ή με το οποίο διαλειτουργεί.

(α) Πρόσθετα στον email client (MUA add-ons): Ο έλεγχος γίνεται πριν την αποστολή (pre-send), πολύ κοντά στον χρήστη. Τα πρόσθετα «βλέπουν» περιεχόμενο/συνημμένα/παραλήπτες, εφαρμόζουν πολιτικές (π.χ. προειδοποίηση, μπλοκάρισμα, αυτόματη κρυπτογράφηση/masking) και περιορίζουν ανθρώπινα λάθη [3], [92].

Πλεονέκτημα: ισχυρά συμφραζόμενα και καλή εμπειρία χρήστη (UX), αφού ο έλεγχος ενσωματώνεται ομαλά στη ροή σύνταξης του email.

Πρόκληση: ασφάλεια/δικαιώματα των ίδιων των add-ons.Τα add-ons λειτουργούν εντός του περιβάλλοντος του email client, άρα μπορούν να έχουν πρόσβαση σε ευαίσθητα δεδομένα (σώμα μηνύματος, επαφές, συνημμένα). Εάν δεν ελεγχθούν σωστά ή εγκατασταθούν από μη αξιόπιστες πηγές, ενδέχεται να αποτελέσουν δυνητικό φορέα διαρροής ή κακόβουλης ενέργειας[93].

(β) Email gateways (Secure Email Gateways με DLP): Οι πύλες αυτές λειτουργούν ενδιάμεσα στο SMTP και επιβάλλουν πολιτικές κεντρικά για όλους (inspection, καραντίνα, αφαίρεση/κρυπτογράφηση συνημμένων, έτοιμα templates συμμόρφωσης). Συχνά συνδυάζονται με Antivirus (AV) και Advanced Threat Protection (ATP) (μηχανισμοί προστασίας από κακόβουλο λογισμικό και προηγμένες απειλές), sandboxing (τεχνική απομόνωσης ύποπτου περιεχομένου σε εικονικό περιβάλλον),IRM (Information Rights Management) και S/MIME (Secure/Multipurpose Internet Mail Extensions) ροές, για την προστασία της επικοινωνίας [1], [91] .

Πλεονεκτήματα: Παρέχουν κεντρική διαχείριση πολιτικών, καθολική προστασία ανεξαρτήτως συσκευής ή χρήστη, ευκολία ελέγχου συμμόρφωσης και ισχυρή ανίχνευση απειλών προτού τα μηνύματα φτάσουν στους παραλήπτες. Επιτρέπουν επίσης ορατότητα και καταγραφή όλης της εισερχόμενης και εξερχόμενης ροής, διευκολύνοντας τον εντοπισμό περιστατικών ασφάλειας και τη δημιουργία αναφορών.

Προκλήσεις: Η κρυπτογράφηση TLS ή end-to-end μπορεί να δυσχεράνει την επιθεώρηση περιεχομένου, απαιτώντας πρόσθετους μηχανισμούς αποκρυπτογράφησης ή συνεργασία με τελικά σημεία (endpoints). Επίσης, η επεξεργασία μεγάλου όγκου μηνυμάτων αυξάνει τις απαιτήσεις σε latency και υπολογιστικούς πόρους. Τέλος, η υπερβολικά επιθετική πολιτική DLP μπορεί να οδηγήσει σε ψευδώς θετικά (false positives) ή σε εμπόδια στη ροή εργασίας, επηρεάζοντας την παραγωγικότητα.

(γ) CASB (Cloud Access Security Broker): Για SaaS email (π.χ. Google Workspace, Microsoft 365) οι μεσίτες αυτοί παρέχουν API-based έλεγχο σε data-at-rest (retrospective scans, καραντίνα, relabeling/IRM) και inline proxy για web ροές (π.χ. masking/tokenization) με ενιαίες πολιτικές multi-cloud [94].

Πλεονεκτήματα: Παρέχουν ορατότητα και έλεγχο σε cloud εφαρμογές τρίτων, ανεξάρτητα από το πού βρίσκονται οι χρήστες ή τα δεδομένα. Ενισχύουν τη συμμόρφωση με κανονιστικά πλαίσια (GDPR) [17] και επιτρέπουν προηγμένες πολιτικές DLP σε SaaS πλατφόρμες που διαφορετικά δεν προσφέρουν granular ελέγχους. Επιπλέον, μειώνουν τον κίνδυνο shadow IT [94], αναγνωρίζοντας μη εγκεκριμένες cloud υπηρεσίες [49], [55].

Προκλήσεις: Η εξάρτηση από APIs συνεπάγεται καθυστέρηση (latency) ή περιορισμούς σε πραγματικό χρόνο, ενώ τα inline proxies ενδέχεται να επηρεάζουν την απόδοση ή τη διαθεσιμότητα υπηρεσιών. Επίσης, η διαχείριση πολλαπλών cloud providers αυξάνει την

πολυπλοκότητα πολιτικών και απαιτεί προσεκτική ενοποίηση ταυτοτήτων και ρόλων (IdP integration) για να αποφευχθούν κενά ασφάλειας[95].

Συνολικά, ο συνδυασμός add-on (pre-send), gateway (inline) και CASB (SaaS) δίνει την πληρέστερη κάλυψη: το add-on προλαβαίνει ανθρώπινα λάθη με πλούσια συμφραζόμενα, το gateway επιβάλλει κεντρικά κανόνες σε όλο τον οργανισμό, και το CASB προσφέρει ορατότητα/πολιτικές σε data-at-rest και multi-cloud. Το προτεινόμενο πρόσθετο για Gmail έρχεται να ενισχύσει ακριβώς το πρώτο σημείο άμυνας (τη στιγμή της σύνταξης), με πολιτικές content+context, δυναμική κρυπτογράφηση/IRM και φιλική διεπαφή (policy tips/προειδοποιήσεις)· παράλληλα, η αρχιτεκτονική του μπορεί να συνεργαστεί με gateway/CASB για ενιαία διακυβέρνηση και αναφορές συμμόρφωσης [1], [3], [91].

Ο **Πίνακας 3** που ακολουθεί συνοψίζει συγκριτικά τα βασικά χαρακτηριστικά, τα δυνατά σημεία και τις προκλήσεις των τριών αυτών προσεγγίσεων DLPS για email.

Πίνακας 3. Συγκριτικός πίνακας μορφών DLP για email

Μορφή	**Δυνατά σημεία**	**Περιορισμοί / Προκλήσεις**
Πρόσθετο στον client (MUA add-on)	Pre-send έλεγχος πολύ κοντά στον χρήστη· πλούσια συμφραζόμενα (παραλήπτες/συσκευή/ώρα)· policy tips & καθοδήγηση πριν «φύγει» το email· μείωση ανθρώπινων λαθών (λάθος παραλήπτης/συνημμένο)· δυνατότητα trigger για κρυπτογράφηση/IRM την ώρα της σύνταξης.	Εξάρτηση από συγκεκριμένο client/έκδοση/OS· ζητήματα ασφάλειας/δικαιωμάτων add-ons· ορατότητα μόνο όταν χρησιμοποιείται ο υποστηριζόμενος client· πιο δύσκολη κεντρικοποίηση αν δεν υπάρχει admin κονσόλα· πιθανή ετερογένεια εμπειρίας ανά συσκευή**.**
Email Gateway (Secure Email Gateway με DLP)	Κεντρική, ομοιόμορφη επιβολή πολιτικών για όλους τους χρήστες/clients· καραντίνα/approval workflows· encryption at gateway, απογύμνωση/αφαίρεση ευαίσθητων συνημμένων· έτοιμα compliance templates· ενοποίηση με AV/ATP/sandboxing/IRM.	Δυσκολία επιθεώρησης end-to-end κρυπτογραφημένου περιεχομένου (S/MIME/PGP)· πιθανές παρακάμψεις (π.χ. προσωπικοί λογαριασμοί, εναλλακτικά κανάλια)· ανάγκη για προσεκτικό tuning (latency/false positives)· εξάρτηση από SMTP ροές.
CASB (Cloud Access Security Broker) για SaaS email	API-based έλεγχος data-at-rest (retrospective scans, καραντίνα, re-labeling/IRM)· inline proxy για web ροές (masking/tokenization)· multi-cloud governance & ορατότητα· εντοπισμός shadow IT· ενοποίηση με	Όρια API/καθυστερήσεις & εξάρτηση από τα capabilities του παρόχου SaaS καλύπτει μόνο ροές που «βλέπει» το CASB (π.χ. web/proxy ή με agents)· deployment complexity (agents/proxies)· πιθανός αντίκτυπος

	labels/IRM/SIEM.	στην UX σε αυστηρά modes.

Επιλέγεται συχνά συνδυασμός: add-on (πρόληψη λαθών pre-send) + gateway (κεντρική επιβολή inline) + CASB (ορατότητα/πολιτικές σε SaaS & data-at-rest).

3.3 Εμπορικές & OSS λύσεις DLP για email

Στην πράξη, πολλές υλοποιήσεις εστιάζουν κατευθείαν στο κανάλι της ηλ. αλληλογραφίας—είτε ως gateway, είτε ως δυνατότητα του οικοσυστήματος (SaaS), είτε με πρόσθετα.

- **Google Workspace / Gmail DLP[4]:** Κανόνες περιεχομένου και συμφραζομένων για εξερχόμενα μηνύματα/συνημμένα, έτοιμα πρότυπα (π.χ. PCI/PII/PHI), ενέργειες όπως μπλοκάρισμα/καραντίνα/notification και ενσωμάτωση με confidential mode / IRM σε enterprise εκδόσεις [51].
- **Microsoft Purview DLP (Exchange Online/Outlook)[5]:** Πολιτικές DLP με Policy Tips στον client (πριν σταλεί), αναγνώριση ευαίσθητων τύπων δεδομένων, προαιρετική αυτόματη κρυπτογράφηση/IRM (MSIP/Sensitivity Labels) και κεντρική αναφορά συμμόρφωσης [38].
- **Proofpoint Email DLP / Email Protection[6]:** Κανόνες content+context με "smart identifiers"[7], καραντίνα/approval workflows, encryption, και reporting για συμμόρφωση· συχνά σε συνδυασμό με αξιολόγηση ρίσκου χρήστη [96].
- **Forcepoint Email Security (DLP)[8]:** Ενιαία πολιτική DLP με έτοιμα compliance templates, contextual/risk-adaptive έλεγχο και ισχυρή ενοποίηση με το υπόλοιπο οικοσύστημα DLP της πλατφόρμας [97].

[4] Google Workspace / Gmail DLP Κανόνες περιεχομένου και συμφραζομένων για εξερχόμενα μηνύματα και συνημμένα, με πρότυπα ευαισθησίας και ενέργειες όπως μπλοκάρισμα, καραντίνα ή ειδοποίηση.

[5] Microsoft Purview DLP (Exchange Online / Outlook) :Πολιτικές DLP που εντοπίζουν ευαίσθητα δεδομένα σε email, εφαρμόζουν *Policy Tips* πριν την αποστολή και ενεργοποιούν ενέργειες όπως μπλοκάρισμα ή αυτόματη κρυπτογράφηση, με κεντρική διαχείριση μέσω Purview Compliance Portal.

[6] Proofpoint Email DLP / Email Protection : Λύση προστασίας email με DLP κανόνες περιεχομένου και συμφραζομένων (*content + context filtering*), καραντίνα, encryption και μηχανισμούς συμμόρφωσης για αποτροπή διαρροών δεδομένων.

[7] Ο όρος "smart identifiers" αναφέρεται σε έξυπνους αναγνωριστές προτύπων δεδομένων, δηλαδή μηχανισμούς που αναγνωρίζουν λέξεις-κλειδιά ή δομές δεδομένων λαμβάνοντας υπόψη το συμφραζόμενο (context). Με αυτό τον τρόπο μειώνονται τα ψευδώς θετικά αποτελέσματα και αυξάνεται η ακρίβεια του εντοπισμού ευαίσθητης πληροφορίας.

[8] Forcepoint Email Security (DLP) : Λύση προστασίας email με ενιαίες πολιτικές DLP, contextual και risk-adaptive ελέγχους, καθώς και έτοιμα compliance templates για ενσωμάτωση σε επιχειρησιακά περιβάλλοντα.

- **Mimecast / Cisco Secure Email / Trend Micro Email Security[9]:** Αντίστοιχες δυνατότητες DLP σε gateway (policies, dictionaries, quarantine, optional encryption) και ολοκλήρωση με AV/ATP/sandboxing [98], [99], [100].
- **OSS «δομικά στοιχεία» (όχι πλήρες DLP)[10]:** Αναφέρεται σε εργαλεία ανοιχτού κώδικα που μπορούν να χρησιμοποιηθούν ως βασικά συστατικά (building blocks) για απλούς DLP ελέγχους, χωρίς να αποτελούν ολοκληρωμένες λύσεις. Το Rspamd, για παράδειγμα, εφαρμόζει κανόνες περιεχομένου και συνημμένων, ενώ τα Milter-based φίλτρα είναι επεκτάσεις που συνεργάζονται με mail servers (όπως Postfix ή Sendmail) και επιτρέπουν παρεμβολή στη ροή SMTP για έλεγχο ή απόρριψη μηνυμάτων. Παρότι μπορούν να καλύψουν βασικές ανάγκες, υστερούν σε διοικητική ωριμότητα (policy tips, workflows, compliance reports) σε σχέση με τις εμπορικές λύσεις [101].

Για την καλύτερη κατανόηση των υπαρχουσών προσεγγίσεων στον χώρο της πρόληψης διαρροής δεδομένων μέσω ηλεκτρονικής αλληλογραφίας, παρατίθεται στη συνέχεια ένας συγκριτικός πίνακας (Πίνακας 4) που συνοψίζει τις βασικότερες διαθέσιμες λύσεις Email-DLP. Ο πίνακας παρουσιάζει με συνοπτικό τρόπο τα χαρακτηριστικά, τον τρόπο ενσωμάτωσης, τις κύριες λειτουργίες και τις ιδιαιτερότητες κάθε λύσης, καλύπτοντας τόσο εμπορικές πλατφόρμες όσο και ανοικτού κώδικα υποδομές. Μέσω αυτής της συνοπτικής αποτύπωσης καθίσταται ευκολότερη η αξιολόγηση των διαφορών ανάμεσα σε SaaS-ενσωματωμένες, gateway και client-based υλοποιήσεις, καθώς και η κατανόηση του επιπέδου ελέγχου και παραμετροποίησης που προσφέρουν στον τελικό χρήστη ή στον διαχειριστή ασφαλείας.

[9] Mimecast / Cisco Secure Email / Trend Micro Email Security — Λύσεις επιπέδου gateway που προσφέρουν DLP πολιτικές, dictionaries, καραντίνα και προαιρετική κρυπτογράφηση, σε συνδυασμό με μηχανισμούς antivirus, ATP και sandboxing.

[10] Rspamd / Postfix Milter — Εργαλεία ανοιχτού κώδικα που λειτουργούν ως δομικά στοιχεία για βασικούς DLP ελέγχους σε mail servers, επιτρέποντας παρεμβολή στη ροή SMTP μέσω Milter interfaces για φιλτράρισμα, επισήμανση ή απόρριψη μηνυμάτων.

Πίνακας 4. Συνοπτική σύγκριση λύσεων Email-DLP.

Λύση / Κατηγορία	**Τύπος / Ενσωμάτωση**	**Κύριες Δυνατότητες**	**Ιδιαιτερότητες / Εστίαση**
Google Workspace / Gmail DLP	Ενσωματωμένη σε SaaS (Gmail)	Κανόνες περιεχομένου & συμφραζομένων, πρότυπα PCI/PII/PHI, μπλοκάρισμα, καραντίνα, ειδοποιήσεις, confidential mode / IRM.	Υλοποίηση πολύ κοντά στον χρήστη, καλό integration με Google services.
Microsoft Purview DLP (Exchange Online / Outlook)	SaaS / Client (Microsoft 365).	Πολιτικές DLP, Policy Tips πριν την αποστολή, αναγνώριση ευαίσθητων δεδομένων, αυτόματη κρυπτογράφηση/IRM, αναφορές συμμόρφωσης.	Ισχυρή ενοποίηση με Outlook, καλή εμπειρία χρήστη στο email.
Proofpoint Email DLP / Email Protection	Gateway / Cloud πλατφόρμα.	Κανόνες content+context, smart identifiers, καραντίνα, workflows, encryption, reporting.	Εστίαση στη συμμόρφωση και στον κίνδυνο χρήστη.
Forcepoint Email Security (DLP)	Gateway / Ολοκληρωμένη πλατφόρμα.	Ενιαία πολιτική DLP, compliance templates, contextual & risk-adaptive έλεγχος.	Κεντρική διαχείριση υψηλή ενοποίηση με DLP οικοσύστημα.
Mimecast / Cisco Secure Email / Trend Micro Email Security	Gateway λύσεις.	Policies, dictionaries, quarantine, optional encryption, sandboxing, AV/ATP.	Αντίστοιχα χαρακτηριστικά DLP με έμφαση στη gateway προστασία.
OSS "δομικά στοιχεία" (Rspamd, Postfix, Sendmail)	Mail server / Open-source.	Κανόνες περιεχομένου/συνημμένων, Milter φίλτρα για έλεγχο SMTP.	Βασική DLP λειτουργία χωρίς advanced policy tips ή reporting.

Παρατηρώντας τις λύσεις του Πίνακα 4, διαφαίνεται ότι δεν υπάρχει μια "καλύτερη" λύση με απόλυτους όρους, αλλά κάθε κατηγορία καλύπτει διαφορετικές ανάγκες και επίπεδα ωριμότητας οργανισμών. Οι εταιρικές πλατφόρμες SaaS, όπως οι Google Workspace DLP και Microsoft Purview DLP, υπερέχουν σε ολοκλήρωση, αυτοματοποίηση και συμβατότητα με το υπόλοιπο οικοσύστημα των υπηρεσιών τους. Είναι ιδανικές για οργανισμούς που διαθέτουν ήδη ενιαίο περιβάλλον cloud και δίνουν έμφαση στη συμμόρφωση (compliance) και στην εμπειρία του τελικού χρήστη. Ωστόσο, παρουσιάζουν περιορισμένες δυνατότητες παραμετροποίησης και εξάρτηση από τον πάροχο, ενώ συχνά προϋποθέτουν επιχειρησιακές άδειες υψηλού κόστους.

Αντίθετα, οι gateway λύσεις (Proofpoint, Forcepoint, Mimecast κ.ά.) απευθύνονται σε περιβάλλοντα όπου απαιτείται κεντρική πολιτική ελέγχου, διασύνδεση με υφιστάμενες υποδομές ασφαλείας και εκτεταμένη δυνατότητα ανάλυσης και αναφορών. Εντούτοις, λειτουργούν κυρίως εκτός του πεδίου αλληλεπίδρασης του χρήστη, με αποτέλεσμα η ενημέρωση ή η εκπαίδευση του αποστολέα να είναι έμμεση ή καθυστερημένη (π.χ. ειδοποίηση μετά τον έλεγχο).

Οι ανοιχτού κώδικα λύσεις, όπως το Rspamd ή το Postfix, παρέχουν μεγαλύτερη ευελιξία προσαρμογής και πειραματισμού, όμως απαιτούν τεχνική εξειδίκευση και συντήρηση, κάτι που τις καθιστά λιγότερο κατάλληλες για τελικούς χρήστες ή μικρούς οργανισμούς. Παρόλα αυτά, μπορούν να αποτελέσουν βάση για ερευνητικά έργα ή για ανάπτυξη προσαρμοσμένων DLP μηχανισμών, όπως η λύση που παρουσιάζεται στην παρούσα εργασία.

Συνολικά, οι πιο "ώριμες" εμπορικές λύσεις προσφέρουν υψηλή αξιοπιστία και συμμόρφωση, ενώ οι ελαφρύτερες ή ανοιχτού κώδικα προσεγγίσεις δίνουν περισσότερη αυτονομία και δυνατότητα καινοτομίας. Η προτεινόμενη προσέγγιση του eMailSec επιδιώκει να συνδυάσει τα πλεονεκτήματα των δύο κόσμων παρέχοντας μηχανισμούς πρόληψης διαρροής δεδομένων εντός του ίδιου του περιβάλλοντος του χρήστη, με διαφάνεια και αλληλεπιδραστικότητα που δεν συναντάται εύκολα σε παραδοσιακές DLP λύσεις.

3.4 Συγκριτική σύνθεση & σύνδεση με το προτεινόμενο σύστημα

Στις προηγούμενες ενότητες αναλύθηκαν οι κύριες κατηγορίες και αρχιτεκτονικές υλοποιήσεις των συστημάτων πρόληψης διαρροής δεδομένων (DLPS) για ηλεκτρονική αλληλογραφία, συμπεριλαμβανομένων των λύσεων add-on (MUA-based), gateway (inline) και CASB (SaaS).Στην παρούσα ενότητα επιχειρείται η συγκριτική αποτίμηση των υπαρχόντων προσθέτων DLP για email, με στόχο να αναδειχθεί η καινοτομία και διαφοροποίηση του προτεινόμενου συστήματος eMailSec σε σχέση με τις υπάρχουσες λύσεις.

Η σύγκριση εστιάζει σε τρία αντιπροσωπευτικά παραδείγματα: το Microsoft Outlook DLP Add-in, το Mozilla Thunderbird DLP Extension, και το Google Workspace / Gmail DLP, τα οποία καλύπτουν τις κυριότερες προσεγγίσεις DLP για email σε επίπεδο client ή SaaS.

Η αξιολόγηση βασίζεται σε εννέα κριτήρια που συνοψίζονται στον ακόλουθο πίνακα, τα οποία επιλέχθηκαν ώστε να αποτυπώνουν τόσο τις τεχνικές όσο και τις λειτουργικές πτυχές των λύσεων:

- **Ενσωμάτωση με το περιβάλλον χρήστη (UI):** ο βαθμός στον οποίο το πρόσθετο ή η υπηρεσία DLP εντάσσεται ομαλά στη ροή εργασίας του χρήστη.
- **Έλεγχος ευαίσθητου περιεχομένου:** η δυνατότητα αναγνώρισης ευαίσθητων δεδομένων (PII, οικονομικά, διαπιστευτήρια) και ο τρόπος υλοποίησης (regex, context).
- **Έλεγχος παραληπτών και επαφών:** η ύπαρξη μηχανισμών αξιολόγησης ή φίλτρων ανάλογα με το αν ο παραλήπτης είναι trusted, unknown ή blocked.
- **Ενέργειες πρόληψης (actions):** το φάσμα ενεργειών που μπορεί να εκτελέσει το σύστημα (π.χ. block, encrypt, redact, notify).
- **Κρυπτογράφηση / PGP υποστήριξη:** η ύπαρξη ή όχι μηχανισμών δημιουργίας και διαχείρισης κλειδιών ή ενσωμάτωσης OpenPGP/S-MIME.
- **Προσαρμοστικότητα πολιτικών:** το επίπεδο ευελιξίας στις πολιτικές DLP (user-based ή admin-based).
- **Αλληλεπίδραση με τον χρήστη (UX):** ο βαθμός διαδραστικότητας, καθοδήγησης και ανατροφοδότησης προς τον χρήστη.
- **Υποστήριξη / Επεκτασιμότητα:** οι τεχνικές δυνατότητες διασύνδεσης και επέκτασης (APIs, εξωτερικές υπηρεσίες).
- **Κεντρικοποιημένη διαχείριση και προσανατολισμός:** η ύπαρξη admin console και ο στρατηγικός προσανατολισμός (user-centric ή enterprise DLP).

Πίνακας 5.Συγκριτική αξιολόγηση μεταξύ του eMailSec και DLP λύσεων.

Κριτήριο	**eMailSec (Gmail Add-on)**	**Microsoft Outlook DLP Add-in**	**Mozilla Thunderbird DLP Extension**	**Google Workspace / Gmail DLP**
Ενσωμάτωση με περιβάλλον χρήστη	Πλήρης ενσωμάτωση στο Gmail UI μέσω Google Apps Script (CardService). Παρέχει άμεση προεπισκόπηση κινδύνων και προειδοποιήσεις πριν την αποστολή.	Εμφάνιση Policy Tips μέσα στο Outlook· βαθιά ενοποίηση με το Purview DLP [2].	Περιορισμένη οπτική ενσωμάτωση· εμφανίζει alerts μέσω pop-up ή toolbar [3].	Ενσωμάτωση στο Gmail Web UI· οι πολιτικές DLP εφαρμόζονται pre-send σε επίπεδο SaaS [1].

Έλεγχος ευαίσθητου περιεχομένου	Προηγμένη regex + context-aware ανάλυση (AFM, AMKA, IBAN, PII, credentials κ.ά.) σε subject, body και attachments.	Ανάλυση με έτοιμα templates (PII, PCI, HIPAA) ανίχνευση μέσω Purview policies.	Ανίχνευση με βασικά regex patterns.	Ανάλυση περιεχομένου/συνημμένων και συμφραζομένων με έτοιμα compliance templates (PCI/PII/PHI).
Έλεγχος παραληπτών & επαφών	Εσωτερική διαχείριση επαφών με κατηγορίες (trusted, unknown, blocked) και blacklist.	Έλεγχος βάσει domain policy· όχι ανά χρήστη.	Δεν υποστηρίζεται.	Πολιτικές σε επίπεδο domain και group — όχι ανά χρήστη .
Ενέργειες πρόληψης (actions)	Block, encrypt, redact, notify, recipient deletion — όλα pre-send με διαδραστικό UI.	Block ή warn μέσω Policy Tips.	Μόνο warn/block.	Block, quarantine ή notify βάσει DLP rules· encryption σε confidential mode.
Κρυπτογράφηση / PGP υποστήριξη	Ενσωματωμένη OpenPGP/RSA δημιουργία & διαχείριση κλειδιών, υπογραφές (.sig), upload σε keyserver, αποθήκευση σε PropertiesService.	Υποστηρίζει S/MIME και IRM· απαιτεί enterprise license.	Υποστήριξη PGP με Enigmail add-on.	Confidential Mode & IRM· χωρίς PGP.

Συμπεράσματα

Το **eMailSec** (Gmail Add-on) υπερέχει έναντι των υπαρχόντων MUA-based λύσεων διότι:

- Παρέχει pre-send ανάλυση περιεχομένου, παραληπτών και συμφραζομένων σε επίπεδο χρήστη.
- Υποστηρίζει PGP/RSA key management και τοπική προσαρμογή πολιτικών, χωρίς admin εξάρτηση.
- Ενσωματώνει privacy-by-design αρχιτεκτονική και αρθρωτή (modular) επεκτασιμότητα μέσω Node.js API.
- Εστιάζει στη συμπεριφορική καθοδήγηση χρήστη και στη μείωση ανθρωπίνων λαθών μέσω ενεργών συναγερμών (alerts).

4

Ανάπτυξη Συστήματος

4.1 Μοντέλο ανάπτυξης

Για την ανάπτυξη του προσθέτου DLPS για το Gmail, ακολουθήθηκε το μοντέλο καταρράκτη. Το μοντέλο καταρράκτη είναι μια γραμμική και σειριακή μεθοδολογία ανάπτυξης λογισμικού, στην οποία κάθε στάδιο της διαδικασίας εκτελείται με αυστηρή σειρά [102]. Σε αυτό το μοντέλο, για να προχωρήσουμε από ένα στάδιο στο επόμενο, απαιτείται η ολοκλήρωση του προηγούμενου, διασφαλίζοντας έτσι τη σταδιακή εξέλιξη και τη συνεπή δομή της ανάπτυξης.

Στην περίπτωση αυτή, ξεκινήσαμε με την **ανάλυση απαιτήσεων** (δείτε Ενότητα 4.2), καταγράφοντας τις λειτουργίες και τα χαρακτηριστικά που πρέπει να προσφέρει το πρόσθετο για την προστασία των ευαίσθητων δεδομένων. Στη συνέχεια, προχωρήσαμε στη **σχεδίαση του συστήματος** (δείτε Ενότητα 4.3), όπου καθορίσαμε την αρχιτεκτονική και τον τρόπο λειτουργίας του προσθέτου για να ανταποκρίνεται στις απαιτήσεις που τέθηκαν για αυτό. Έπειτα, ακολούθησε η **υλοποίηση** (δείτε Ενότητα 4.4), κατά την οποία αναπτύχθηκε ο κώδικας για την υλοποίηση των καθορισμένων λειτουργιών του συστήματος. Το τελευταίο στάδιο περιλάμβανε την επικύρωση του προσθέτου (**δοκιμή και αξιολόγηση)** (δείτε Ενότητα 6) για να διασφαλιστεί η λειτουργικότητα και η συμμόρφωση με τις απαιτήσεις που καθορίστηκαν στην αρχή.

Η λειτουργικότητα και η συμμόρφωση της εφαρμογής με τις απαιτήσεις που καθορίστηκαν στο Κεφάλαιο 4.2 αποτυπώνονται μέσω της ανάλυσης της Ενότητας 4.5 (Ικανοποίηση Απαιτήσεων). Η επίδειξη της τελικής μορφής του προσθέτου περιγράφεται αναλυτικά στο Κεφάλαιο 5 (Εγκατάσταση & Επίδειξη), ενώ η αποτίμηση της απόδοσης και της αποτελεσματικότητας του συστήματος παρουσιάζεται συγκεντρωτικά στο Κεφάλαιο 6 (Αποτίμηση Λύσης).

Αυτό το μοντέλο που ακολουθήσαμε επιλέχθηκε με σκοπό να διασφαλίσει την επιτυχή ολοκλήρωση κάθε σταδίου προτού προχωρήσουμε στο επόμενο, μειώνοντας τον κίνδυνο σφαλμάτων και επιτρέποντας μια σαφή κατανόηση της προόδου και των απαιτήσεων του έργου.

4.2 Ανάλυση Απαιτήσεων

4.2.1 Λειτουργικές Απαιτήσεις

Οι λειτουργικές απαιτήσεις καθορίζουν τις συγκεκριμένες δυνατότητες που πρέπει να έχει το πρόσθετο για να διασφαλίζει την προστασία από διαρροές δεδομένων.

1. **Ανίχνευση ευαίσθητων πληροφοριών στο περιεχόμενο του μηνύματος.**
    - Το πρόσθετο πρέπει να εντοπίζει ευαίσθητα ή προσωπικά δεδομένα που περιέχονται στο κείμενο του email (π.χ., αριθμοί ταυτότητας, τηλέφωνα, διευθύνσεις, οικονομικές πληροφορίες).
    - Δυνατότητα αναγνώρισης όλων των τύπων ιδιωτικών/ευαίσθητων δεδομένων (προκαθορισμένα προστατεύονται όλα), με ευελιξία παραμετροποίησης από τον χρήστη ανά κατηγορία.
2. **Ταξινόμηση συνημμένων αρχείων.**
    - Δυνατότητα σάρωσης των συνημμένων και κατάταξής τους με βάση το επίπεδο ιδιωτικότητας (π.χ., αν περιέχουν προσωπικά ή εμπιστευτικά δεδομένα).
3. **Αξιολόγηση παραληπτών.**
    - Το πρόσθετο θα πρέπει να μπορεί να αξιολογεί τους παραλήπτες του email με δύο βασικές διαστάσεις: **(α)** το επίπεδο εμπιστευτικότητάς τους και **(β)** τις δυνατότητες κρυπτογράφησης που έχουν.
4. **Αντιστοίχιση περιεχομένου σε θέματα (topics).**
    - Δυνατότητα ταξινόμησης δεδομένων μέσα σε κάθε μήνυμα και γενικής ταξινόμησης των μηνυμάτων βάσει θέματος, ώστε να ενισχύεται η ακρίβεια στην ανίχνευση ευαίσθητων πληροφοριών.
5. **Εφαρμογή κανόνων διαχείρισης περιεχομένου.**

    - Το σύστημα θα πρέπει να ενσωματώνει ένα πρότυπο σύνολο κανόνων διαχείρισης περιεχομένου που προκαθορισμένα θα ισχύει. Το πρότυπο σύνολο αυτό θα αφορά το προκαθορισμένο προφίλ.
    - Ο χρήστης θα μπορεί να ορίζει ένα προφίλ (κανόνων διαχείρισης περιεχομένου) ως το ενεργό προφίλ, δηλαδή το προφίλ με βάση το οποίο θα στηρίζεται η λειτουργία του πρόσθετου για την διαχείριση των email μηνυμάτων (προς αποστολή).

        I. Ορισμός ενεργού προφίλ κανόνων διαχείρισης περιεχομένου, με δυνατότητα είτε αποκλειστικής ενεργοποίησης (ένα τη φορά) είτε ταυτόχρονης ενεργοποίησης πολλαπλών προφίλ, ανάλογα με το περιεχόμενο και τον σχεδιασμό των κανόνων.

- Ο χρήστης πρέπει να μπορεί να δημιουργεί, να επεξεργάζεται και να διαγράφει κανόνες διαχείρισης περιεχομένου είτε για ένα νέο προφίλ είτε για υπάρχοντα, όπως είναι το προκαθορισμένο.

    I. Κάθε κανόνας προσδιορίζει μια απλή ή σύνθετη συνθήκη και τις δράσεις που θα πρέπει να πραγματοποιηθούν όταν η συνθήκη αυτή ικανοποιείται.

    II. Οι σύνθετες συνθήκες προκύπτουν εφαρμόζοντας λογικούς τελεστές (λογική σύζευξη, διάζευξη ή άρνηση) πάνω σε άλλες συνθήκες.

    III. Μια απλή συνθήκη θα πρέπει να αφορά είτε το περιεχόμενο του μηνύματος, είτε τα συνημμένα του, είτε το θέμα του μηνύματος είτε τον παραλήπτη. Ουσιαστικά, θα μπορεί να ελέγχεται αν το περιεχόμενο ή κάποιο συνημμένο εμπεριέχει ευαίσθητα δεδομένα και ποιου τύπου, το όνομα του θέματος του μηνύματος, το επίπεδο εμπιστευτικότητας του παραλήπτη και οι ικανότητες κρυπτογράφησής του.

6. **Δυνατές ενέργειες**: το σύστημα θα μπορεί να προσδιορίζει διάφορες δράσεις ως προς την διαχείριση περιεχομένου σε κανόνες, όπως τις εξής:

- <u>Κρυπτογράφηση περιεχομένου και συνημμένων:</u>

    I. Η δυνατότητα πλήρους ή μερικής κρυπτογράφησης του περιεχομένου του email και των συνημμένων αρχείων πριν την αποστολή.
    II. Υποστήριξη διαφορετικών επιπέδων κρυπτογράφησης ανάλογα με την ευαισθησία των δεδομένων και τις ανάγκες του χρήστη.
    III. Το σύστημα θα πρέπει να μπορεί να παράγει, να διαχειρίζεται και να επαληθεύει κλειδιά κρυπτογράφησης, διασφαλίζοντας ότι είναι ισχυρά και κατάλληλα για ασφαλή χρήση.

- <u>Ειδοποιήσεις χρήστη:</u>

    I. Παροχή ειδοποιήσεων και μηνυμάτων κινδύνου όταν ανιχνεύονται πιθανές διαρροές δεδομένων.

        - Θα πρέπει να προσδιορίζεται ακριβώς ποιο είναι το ζήτημα σε αυτή την περίπτωση (πχ. ύπαρξη συγκεκριμένου τύπου ευαίσθητων δεδομένων στο περιεχόμενο ή στα συνημμένα του μηνύματος) καθώς και σε ποια δράση ή δράσεις θα προχωρήσει το σύστημα για την αντιμετώπιση του ζητήματος (θα μπορούσε να αναφέρεται και ο κανόνας που έχει ενεργοποιηθεί για λόγους ενημέρωσης αλλά ακόμα και αποσφαλμάτωσης κανόνων).

- Μπλοκάρισμα αποστολής μηνυμάτων:

    I. Το σύστημα θα πρέπει να μπλοκάρει την αποστολή ενός μηνύματος (πχ. διότι ο παραλήπτης δεν πληροί τα κριτήρια ασφαλείας).

        - Σε αυτή την περίπτωση, το μήνυμα μπορεί να αποθηκεύεται σε κάποιο ειδικό φάκελο ώστε να μπορεί να έχει πρόσβαση σε αυτό ο χρήστης όποτε το επιθυμήσει.

- Αφαίρεση συνημμένου:
    I. Αν το συνημμένο εμπεριέχει ευαίσθητα δεδομένα, θα μπορεί απλώς να διαγράφεται από το μήνυμα πριν αυτό αποσταλλεί.
- Διαγραφή μηνύματος:
    I. Ανάλογα με την κρισιμότητα του περιεχομένου ενός μηνύματος θα μπορούσε αυτό να διαγράφεται αντί απλώς να μπλοκαριστεί.

- Χειρωνακτική αντιμετώπιση:

    I. Η δράση αυτή αφήνει την τελική επιλογή στον ίδιο τον χρήστη, ο οποίος μπορεί να αποφασίσει και να προχωρήσει στην αποστολή, κρυπτογράφηση ή και διαγραφή του μηνύματος.
        - Σε αυτή την περίπτωση, το σύστημα θα ρωτά τον χρήστη τι θέλει να κάνει με αυτό το μήνυμα και έπειτα θα προχωρά στην ενέργεια που του προτείνει ο χρήστης.
        - Η δράση αυτή έχει νόημα όταν συνδυάζεται με αυτή της ειδοποίησης χρήστη.

4.2.2 Μη Λειτουργικές Απαιτήσεις

Οι μη λειτουργικές απαιτήσεις αφορούν την ποιότητα, την απόδοση, την ευχρηστία και την ασφάλεια του προσθέτου, εξασφαλίζοντας ότι η εμπειρία του χρήστη θα είναι (πάντοτε) θετική.

1. **Ασφάλεια:**

    - Το πρόσθετο πρέπει να χρησιμοποιεί ασφαλείς μεθόδους κρυπτογράφησης για την προστασία των δεδομένων και να είναι σύμφωνο με τα πρότυπα ασφάλειας.

        I. Οφείλει να ενσωματώνει τουλάχιστον έναν αποδεδειγμένα ασφαλή αλγόριθμο κρυπτογράφησης (π.χ. RSA ή AES), διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών.

2. **Απόδοση:**

    - Η λειτουργία του προσθέτου δεν πρέπει να επηρεάζει γενικά την απόδοση του προγράμματος πελάτη email.
    - Το πρόσθετο πρέπει να είναι ελαφρύ και να μη δημιουργεί καθυστερήσεις κατά τη σύνταξη ή την αποστολή των μηνυμάτων, διατηρώντας χαμηλό χρόνο επεξεργασίας κατά την ανάλυση περιεχομένου και την κρυπτογράφηση.

- Οι λειτουργίες διαχείρισης προφίλ και κανόνων διαχείρισης περιεχομένου θα πρέπει να γίνονται άμεσα με αποδοτικό τρόπο χωρίς οποιαδήποτε καθυστέρηση.

3. **Ευχρηστία:**

- Η διεπαφή χρήστη πρέπει να είναι φιλική και κατανοητή, με ξεκάθαρες ειδοποιήσεις και μηνύματα που καθοδηγούν τον χρήστη κατά τη λήψη αποφάσεων αλλά και κατά τη διαχείριση των προφίλ και των κανόνων διαχείρισης περιεχομένου.
- Τα μηνύματα κινδύνου/ειδοποίησης πρέπει να είναι περιεκτικά και να αναφέρεται με σαφήνεια το επίπεδο κινδύνου, ώστε να βοηθούν τον χρήστη να κατανοήσει τους λόγους για τυχόν μπλοκάρισμα ή κρυπτογράφηση των μηνυμάτων email..
- Αντιστοίχως, τα μηνύματα σφάλματος θα πρέπει να είναι περιεκτικά και σαφή, προσδιορίζοντας με ακρίβεια το λόγο του σφάλματος και προτείνοντας, όπου είναι δυνατό, τον τρόπο επίλυσής του.

4. **Επεκτασιμότητα:**

- Το πρόσθετο θα πρέπει να είναι σχεδιασμένο με τρόπο που να επιτρέπει εύκολη επέκταση στο μέλλον, ώστε να υποστηρίζει:

  I. επιπλέον email πλατφόρμες ή νέες δυνατότητες ανάλυσης και ασφάλειας,
  II. νέα είδη ευαίσθητων δεδομένων που δεν καλύπτονται στην τρέχουσα έκδοση,
  III. νέες δράσεις στο πλαίσιο των κανόνων διαχείρισης περιεχομένου.

Με αυτόν τον τρόπο διασφαλίζεται ότι το πρόσθετο μπορεί να προσαρμοστεί σε μελλοντικές ανάγκες και τεχνολογικές εξελίξεις, χωρίς εκτεταμένες αλλαγές στη βασική του αρχιτεκτονική.

5. **Προσαρμοστικότητα:**

- Ο χρήστης θα πρέπει να μπορεί να προσαρμόζει τους κανόνες ασφαλείας και τις ρυθμίσεις ανάλογα με τις ανάγκες του, επιτρέποντας έτσι μεγαλύτερο έλεγχο στην αποστολή των δεδομένων του.

6. **Φορητότητα:**

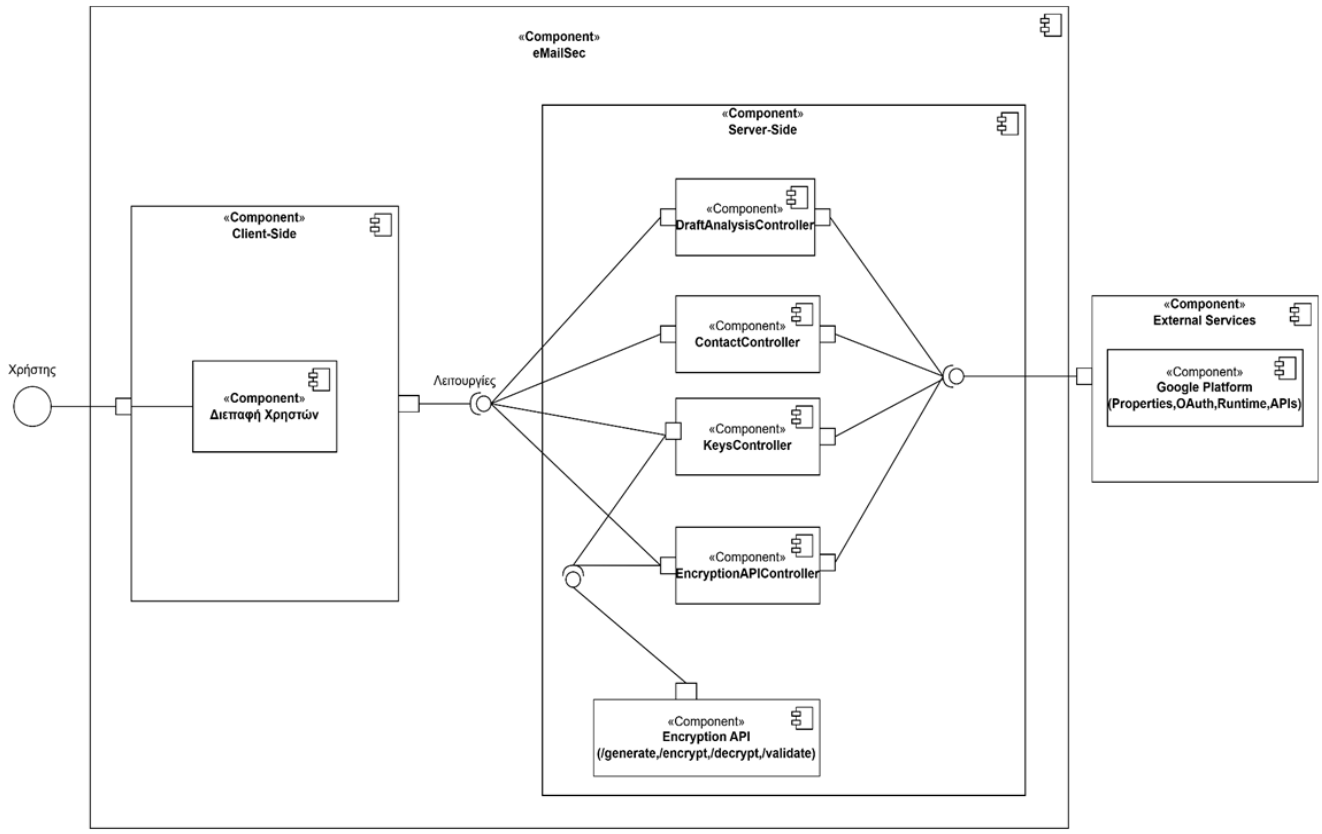
- Το πρόσθετο θα πρέπει να είναι προσβάσιμο και να λειτουργεί ομαλά σε όλες τις συσκευές που υποστηρίζουν την εκτέλεση του Gmail (υπολογιστής, tablet, κινητό) και αντίστοιχα σε όλα τα λειτουργικά συστήματα (Windows, macOS, iOS, Android), χωρίς να απαιτείται ξεχωριστή εγκατάσταση ανά συσκευή, διατηρώντας έτσι συνεπή εμπειρία χρήστη και απόδοση.

4.3 Σχεδίαση

Η σχεδίαση του συστήματος αποτελεί το ενδιάμεσο στάδιο ανάμεσα στην ανάλυση απαιτήσεων και την υλοποίηση. Στόχος είναι η αποτύπωση της δομής και της λειτουργικότητας/συμπεριφοράς του προσθέτου για το Gmail με τρόπο σαφή, ώστε να καθοδηγήσει την υλοποίησή του και να διασφαλίσει ότι όλες οι απαιτήσεις αυτού του έργου λογισμικού ικανοποιούνται.

4.3.1 Διάγραμμα Αρχιτεκτονικής / Συστατικών (Component Diagram)

Το παρόν διάγραμμα αποτυπώνει την αρχιτεκτονική οργάνωση του συστήματος eMailSec και τις σχέσεις μεταξύ των βασικών συστατικών (components) του. Στόχος είναι η απεικόνιση της πολυεπίπεδης δομής του συστήματος και των μεταξύ τους ροών δεδομένων και λειτουργιών, ώστε να κατανοηθεί η διασύνδεση ανάμεσα στα επιμέρους τμήματα λογισμικού.



Εικόνα 2. Διάγραμμα Συστατικών του συστήματος eMailSec.

Όπως φαίνεται και από το διάγραμμα, η αρχιτεκτονική του συστήματος διακρίνεται στα ακόλουθα τρία επίπεδα: Client-Side, Server-Side και External Services, τα οποία συνεργάζονται για την παροχή των υπηρεσιών ανάλυσης, ασφάλειας και κρυπτογράφησης ηλεκτρονικής αλληλογραφίας: **Client-Side**, **Server-Side** και **External Services**.

- **Client-Side:**

  Αντιπροσωπεύει το **Gmail Add-on**, μέσω του οποίου ο χρήστης αλληλεπιδρά με το σύστημα. Περιλαμβάνει το component **Διεπαφή Χρηστών (User Interface)**, υπεύθυνο για την εμφάνιση του περιβάλλοντος σύνθεσης email, την προβολή ειδοποιήσεων ασφαλείας και την ενεργοποίηση λειτουργιών, όπως η σάρωση περιεχομένου και η κρυπτογράφηση.

  Το backend εκθέτει τη διεπαφή Λειτουργίες (UserActions), μέσω της οποίας το περιβάλλον χρήστη (UI) καλεί τις αντίστοιχες μεθόδους, ανάλογα με τις ενέργειες ή τα αιτήματα του χρήστη.

- **Server-Side:**

  Αποτελεί τον βασικό πυρήνα της επιχειρησιακής λογικής και υλοποιείται στο περιβάλλον **Google Apps Script**. Περιλαμβάνει τα ακόλουθα συστατικά:

  - **DraftAnalysisController:** Ανιχνεύει ευαίσθητο περιεχόμενο στα προσχέδια email.
  - **ContactController:** Διαχειρίζεται τις αποθηκευμένες επαφές, κατηγορίες και επίπεδα εμπιστοσύνης.
  - **KeysController:** Δημιουργεί, αποθηκεύει και διανέμει κλειδιά PGP.
  - **EncryptionAPIController:** Αναλαμβάνει την επικοινωνία με το υποσύστημα **Encryption API**.
  - **Encryption API:** Υλοποιεί τις λειτουργίες κρυπτογράφησης, αποκρυπτογράφησης καθώς και δημιουργίας και επικύρωσης κλειδιών μέσω των endpoints `/generate`, `/encrypt`, `/decrypt`, και `/validate`.

  Οι επιμέρους controllers εκθέτουν το **interface Λειτουργίες**, ενώ παράλληλα καταναλώνουν υπηρεσίες της πλατφόρμας Google. Η σχεδίαση αυτή εξασφαλίζει **χαλαρή σύζευξη (loose coupling)** και επεκτασιμότητα.

- **External Services:**

  Περιλαμβάνει αποκλειστικά την Google Platform, η οποία παρέχει το OAuth 2.0 για έλεγχο ταυτότητας, το PropertiesService για αποθήκευση ρυθμίσεων και επαφών, το Gmail Runtime όπου επιτρέπει την αλληλεπίδραση του προσθέτου με το περιβάλλον του Gmail και τα Google Cloud APIs τα οποία προσφέρουν το σύνολο των διεπαφών που παρέχουν πρόσβαση στις υπηρεσίες του Google Cloud Platform.

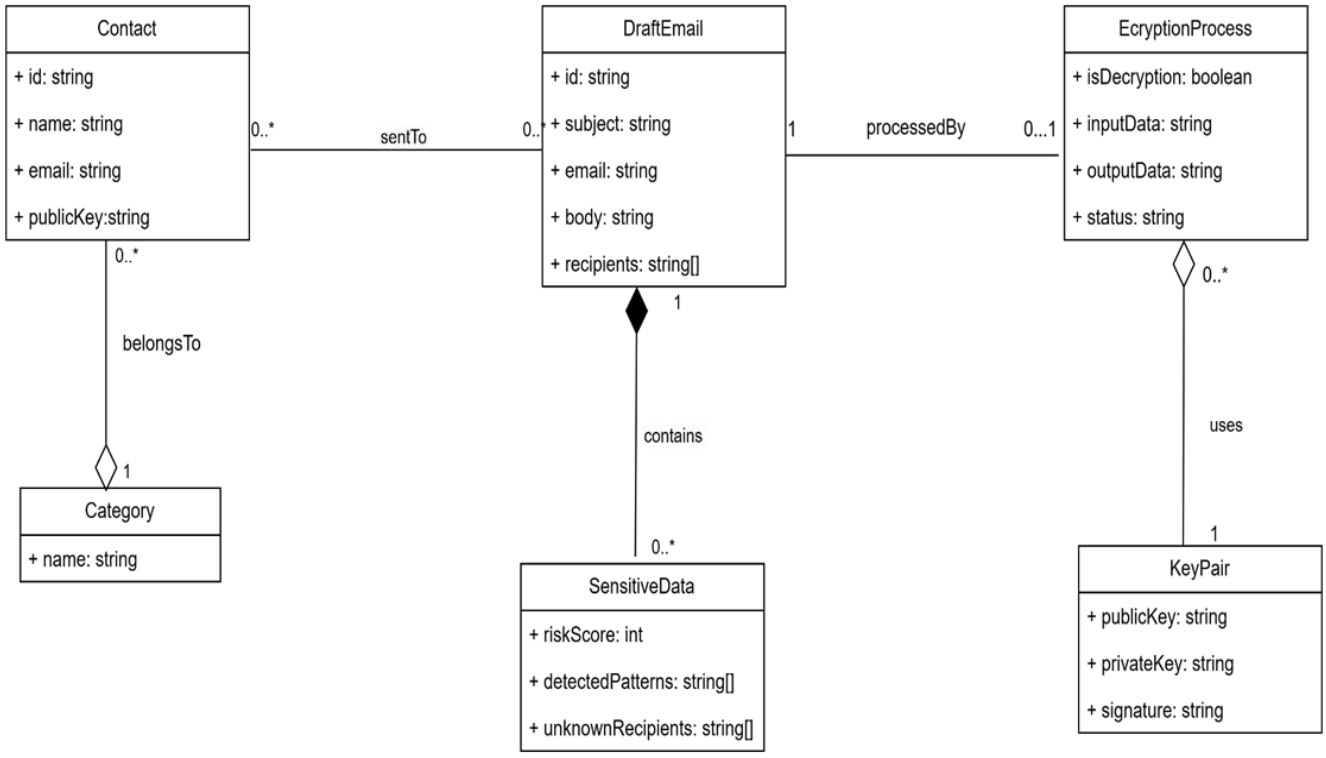
Η συνολική αρχιτεκτονική απεικονίζει τη ροή επικοινωνίας από τον **χρήστη (Client-Side)** προς το **Server-Side**, καθώς και την αλληλεπίδραση του συστήματος με την **Google Platform** για την ασφαλή επεξεργασία και προστασία των δεδομένων ηλεκτρονικής αλληλογραφίας.

4.3.2 Διάγραμμα Κλάσεων (Class Diagram)

Στην παρούσα ενότητα παρουσιάζεται το εννοιολογικό μοντέλο δεδομένων του συστήματος eMailSec, το οποίο αποτυπώνει τις βασικές πληροφοριακές οντότητες που χρησιμοποιούνται από το πρόσθετο και τον τρόπο με τον οποίο συνδέονται μεταξύ τους. Το διάγραμμα έχει τη μορφή UML class diagram, ωστόσο οι απεικονιζόμενες οντότητες αντιστοιχούν σε λογικές δομές δεδομένων (data structures), καθώς η υλοποίηση βασίζεται σε Google Apps Script και Node.js, τα οποία χρησιμοποιούν συναρτήσεις και αντικείμενα JSON για την αναπαράσταση πληροφορίας.

Η δομή δεδομένων περιλαμβάνει οντότητες, όπως Contact, Category, DraftEmail, SensitiveData, KeyPair και EncryptionProcess, που αποτυπώνουν αντίστοιχα τις επαφές του χρήστη, τις κατηγορίες ασφάλειας, τα πρόχειρα μηνύματα, τα αποτελέσματα ανάλυσης ευαίσθητων δεδομένων, τα ζεύγη κλειδιών και τις διαδικασίες κρυπτογράφησης. Οι συσχετίσεις μεταξύ των οντοτήτων εκφράζουν τον τρόπο με τον οποίο διακινείται και συνδέεται η πληροφορία μέσα στο σύστημα για παράδειγμα, κάθε πρόχειρο email (DraftEmail) συνδέεται με μία αναφορά σάρωσης (SensitiveData), ενώ κάθε επαφή (Contact) μπορεί να ανήκει σε μία κατηγορία (Category) ή να διαθέτει αποθηκευμένο δημόσιο κλειδί (public key).

Συνολικά, το διάγραμμα αποτυπώνει τη λογική αρχιτεκτονική των δεδομένων του eMailSec, διευκολύνοντας την κατανόηση της ροής πληροφορίας ανάμεσα στα υποσυστήματα ανάλυσης, ασφάλειας και διαχείρισης χρηστών. Παρότι δεν αντιπροσωπεύει πραγματικές κλάσεις κώδικα, αποδίδει με ακρίβεια τη δομή και τη σημασιολογία των δεδομένων που επεξεργάζεται η εφαρμογή.



Εικόνα 3. Εννοιολογικό διάγραμμα δεδομένων (UML class-style) του eMailSec.

4.3.3 Διάγραμμα Περιβάλλοντος (Context Diagram)

Το διάγραμμα περιβάλλοντος (context diagram) αποτελεί ένα από τα βασικά εργαλεία μοντελοποίησης κατά τη φάση της ανάλυσης ενός πληροφοριακού συστήματος. Στόχος του είναι να οριοθετήσει με σαφήνεια τα όρια του υπό ανάπτυξη συστήματος και να παρουσιάσει με απλό και κατανοητό τρόπο τις εξωτερικές οντότητες με τις οποίες αυτό αλληλεπιδρά, καθώς και τις βασικές ροές δεδομένων που ανταλλάσσονται.

Σε αντίθεση με πιο λεπτομερή διαγράμματα, το context diagram ακολουθεί την προσέγγιση του «μαύρου κουτιού» (black box): το σύστημα τοποθετείται στο κέντρο του διαγράμματος ως ενιαία οντότητα, χωρίς ανάλυση της εσωτερικής του δομής, ενώ γύρω του απεικονίζονται οι εξωτερικοί παράγοντες με τους οποίους επικοινωνεί. Με αυτόν τον τρόπο, ο αναγνώστης μπορεί να κατανοήσει εύκολα το λειτουργικό πλαίσιο στο οποίο εντάσσεται η λύση, χωρίς να απαιτείται γνώση των τεχνικών λεπτομερειών της υλοποίησης.

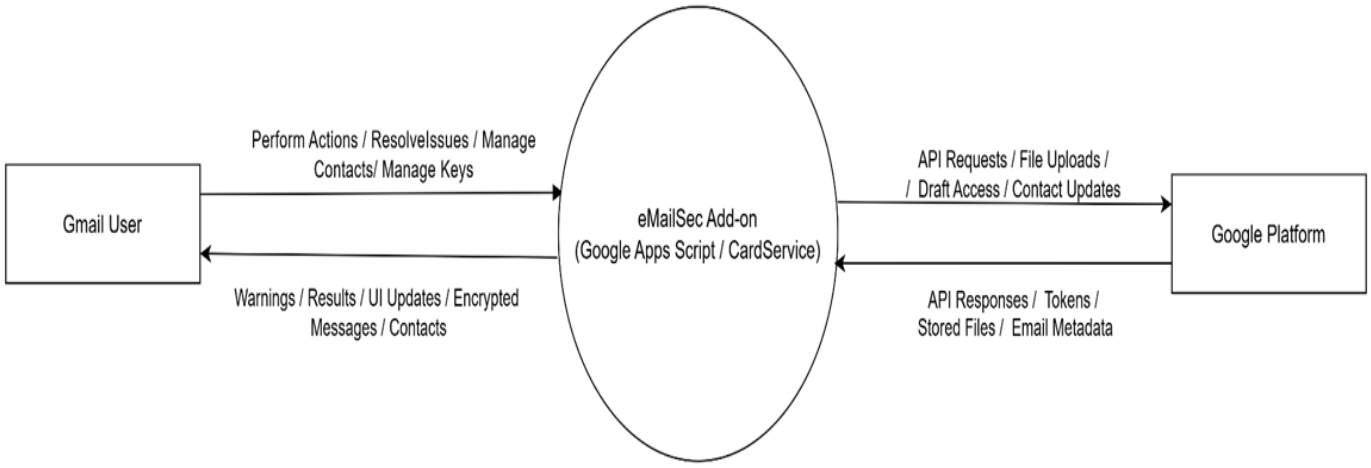
Στην περίπτωση της παρούσας διπλωματικής εργασίας, στο κέντρο του διαγράμματος βρίσκεται το eMailSec Add-on, ένα πρόσθετο για το Gmail που έχει αναπτυχθεί σε Google Apps

Script και παρέχει λειτουργίες ασφάλειας, όπως σάρωση περιεχομένου, εντοπισμό ευαίσθητων δεδομένων, διαχείριση επαφών, καθώς και κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων.

Ο τελικός χρήστης (Gmail User) αλληλεπιδρά με το πρόσθετο μέσω του Gmail Web UI, εκτελώντας ενέργειες όπως Perform Actions, Resolve Issues, Manage Contacts και Manage Keys, ενώ λαμβάνει ειδοποιήσεις, αποτελέσματα ανάλυσης και ενημερώσεις ασφαλείας.

Η εξωτερική οντότητα Google Platform λειτουργεί ως ενιαίο σύστημα που συγκεντρώνει όλες τις υπηρεσίες της Google με τις οποίες συνεργάζεται το πρόσθετο. Μέσω αυτής πραγματοποιούνται API Requests για ανάγνωση drafts, αποθήκευση αρχείων και ενημέρωση επαφών, καθώς και ανταλλαγή tokens και metadata για την ταυτοποίηση, τη διαχείριση χρηστών και την αποθήκευση δεδομένων. Αντίστοιχα, η πλατφόρμα επιστρέφει API Responses, tokens, email metadata και αρχεία αποθήκευσης, υποστηρίζοντας την ασφαλή εκτέλεση των λειτουργιών του συστήματος.

Η συγκεκριμένη απεικόνιση επιτρέπει στον αναγνώστη να έχει μια καθαρή, υψηλού επιπέδου εικόνα του eMailSec: ποια είναι τα όριά του, με ποιες εξωτερικές οντότητες αλληλεπιδρά (Gmail User και Google Platform) και ποιες ροές δεδομένων αποτελούν κρίσιμα σημεία για την ασφάλεια, την απόδοση και την επεκτασιμότητα της εφαρμογής.



Εικόνα 4. Διάγραμμα Περιβάλλοντος (Context diagram)

4.3.4 Διαγράμματα περιπτώσεων χρήσης (Use Case Diagrams)

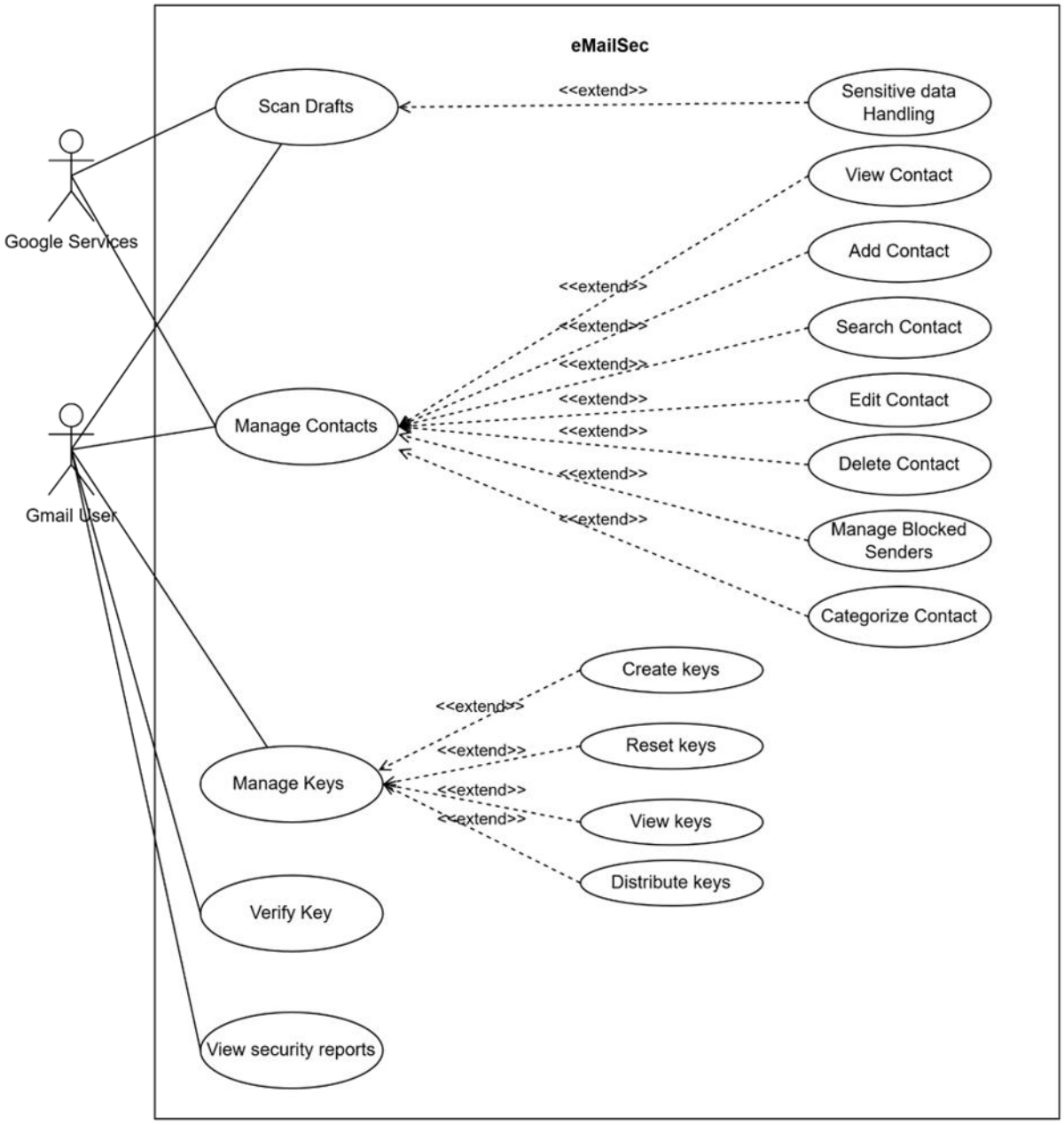
Τα διαγράμματα περιπτώσεων χρήσης (UML Use Case Diagrams) αποτυπώνουν σε υψηλό επίπεδο τον τρόπο με τον οποίο εξωτερικοί ρόλοι (actors) αλληλεπιδρούν με ένα σύστημα και ποιοι λειτουργικοί στόχοι (use cases) επιδιώκονται, με έμφαση στην εξωτερικά ορατή συμπεριφορά και όχι στις λεπτομέρειες υλοποίησης. Αποτελούν βασικό τεχνούργημα της σχεδίασης, καθώς συμπυκνώνουν τις λειτουργικές απαιτήσεις σε μια συνοπτική, εύληπτη όψη που ευθυγραμμίζει αναλυτές, ενδιαφερόμενους και ομάδα ανάπτυξης [103], [104].Τυπικά, το διάγραμμα περιλαμβάνει τα όρια του συστήματος (system boundary), εντός των οποίων τοποθετούνται οι περιπτώσεις χρήσης ως οβάλ (ελλειπτικά) σχήματα με περιγραφικούς τίτλους, και εκτός των οποίων βρίσκονται οι actors — άνθρωποι ή γειτονικά/εξωτερικά συστήματα που εκκινούν ή συμμετέχουν στα σενάρια.

Οι συσχετίσεις actor–use case (απλές γραμμές) δηλώνουν συμμετοχή/εκκίνηση, ενώ οι σχέσεις «include» και «extend» προσφέρουν μηχανισμούς δόμησης: η include μοντελοποιεί υποχρεωτικές, επαναχρησιμοποιούμενες υπο-περιπτώσεις που «αποσπώνται» από βασικές περιπτώσεις, ενώ η extend εισάγει προαιρετικές ή υπό όρους επεκτάσεις της βασικής ροής σε συγκεκριμένα σημεία επέκτασης [104], [105], [106]. Όπου απαιτείται, χρησιμοποιείται και γενίκευση για ρόλους ή use cases, ώστε να δηλωθεί εξειδίκευση συμπεριφοράς.

Σε μεθοδολογικό επίπεδο, ένα use case θεωρείται πλήρες όταν οδηγεί σε παρατηρήσιμο αποτέλεσμα αξίας για τον actor και διαθέτει σαφές νόημα σε επιχειρησιακούς όρους. Η ονοματοδοσία πρέπει να είναι προσανατολισμένη στη δράση (π.χ. Scan Drafts, Encrypt Email), ενώ η επιλογή των σχέσεων include/extend οφείλει να ακολουθεί την πρόθεση μοντελοποίησης και όχι αισθητικές ή εργονομικές σκοπιμότητες του διαγράμματος [106], [107]. Ένα συνοπτικό διάγραμμα με λίγους αλλά αντιπροσωπευτικούς στόχους είναι προτιμότερο από έναν «χάρτη» υπερφόρτωσης.

Ως παραδοτέο της ανάλυσης, το διάγραμμα περιπτώσεων χρήσης λειτουργεί ως γέφυρα από τη συνοπτική απεικόνιση στόχων προς την αναλυτική τεκμηρίωση κάθε περίπτωσης.

Εφαρμογή στο παρόν σύστημα: Για το σύστημα eMailSec, ο κύριος actor είναι ο Gmail User, ενώ τα διαγράμματα ομαδοποιούνται ανά UI context (Home, Open Mail, Compose) ώστε να καθίσταται σαφές ποιοι στόχοι είναι διαθέσιμοι σε κάθε κατάσταση χρήσης της εφαρμογής. Στις αντίστοιχες όψεις, οι σχέσεις include αποτυπώνουν υποχρεωτικές επιμέρους αλληλεπιδράσεις (π.χ. επιμέρους έλεγχοι κατά τη σάρωση), ενώ οι extend καταγράφουν υπό όρους ροές (π.χ. εμφάνιση προειδοποιήσεων ή κλήση διαδικασιών επίλυσης όταν εντοπίζονται ευρήματα). Οι πλήρεις προδιαγραφές των περιπτώσεων χρήσης παρατίθενται αμέσως μετά σε δομημένους πίνακες (τίτλος, πρωτεύων actor,σκοπός, προϋποθέσεις, μετα-συνθήκες , βασική ροή, εναλλακτικές/εξαιρέσεις).

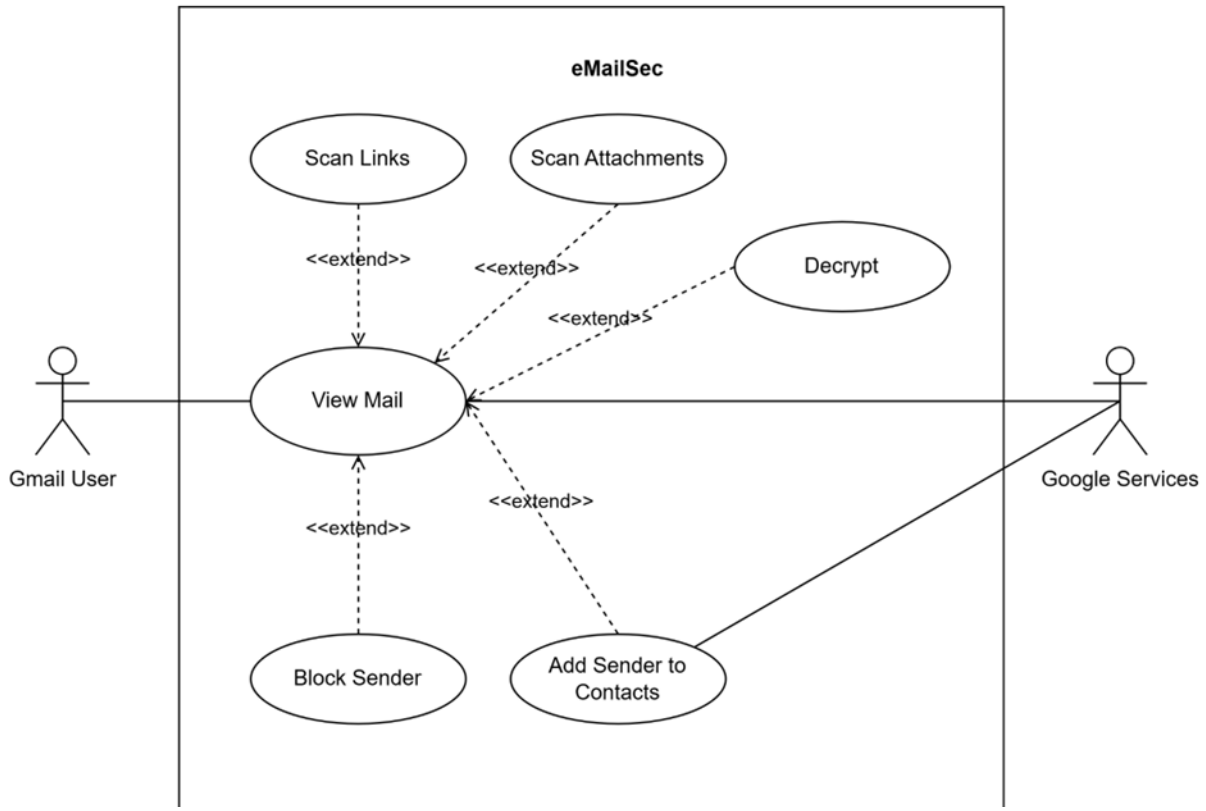


Εικόνα 5. Διάγραμμα Περιπτώσεων Χρήσης - Home page.

Το διάγραμμα παρουσιάζει τη βασική αλληλεπίδραση του Gmail User με το πρόσθετο eMailSec όταν ανοίγει την αρχική κάρτα (Home) του προσθέτου. Ο χρήστης έχει τέσσερις κύριες επιλογές: Scan Drafts, Manage Contacts, Manage Keys και View Security Reports. Με την επιλογή Scan Drafts εκτελείται έλεγχος των προχείρων για πιθανά ζητήματα ο έλεγχος περιλαμβάνει ανάλυση παραληπτών, θέματος, σώματος και συνδέσμων, ενώ —εφόσον υπάρχουν— επεκτείνεται και στα

συνημμένα. Εφόσον εντοπιστούν ευαίσθητα δεδομένα ή κίνδυνοι, ενεργοποιείται ροή προειδοποίησης/επίλυσης ώστε ο χρήστης να λάβει δράση πριν την αποστολή. Η επιλογή Manage Contacts δίνει τη δυνατότητα προβολής, αναζήτησης, προσθήκης, επεξεργασίας και διαγραφής επαφών, καθώς και οργάνωσης σε κατηγορίες ή διαχείρισης αποκλεισμένων αποστολέων (blocked senders). Στο Manage Keys ο χρήστης δημιουργεί ή επαναφέρει ζεύγη κλειδιών, διανέμει το δημόσιο κλειδί (μαζί με υπογραφή) και μπορεί να αποθηκεύσει δημόσιο κλειδί του και την υπογραφή του κλειδίου στο Drive.Στο Verify Key ο χρήστης επαληθεύει τα κλειδιά που έλαβε απο άλλους χρήστες αλλα. Τέλος, το View Security Reports παρέχει συγκεντρωτικά στοιχεία δραστηριότητας (π.χ. πλήθος ελέγχων, ευρήματα, τελευταίος έλεγχος), προσφέροντας συνοπτική εικόνα της κατάστασης ασφαλείας.

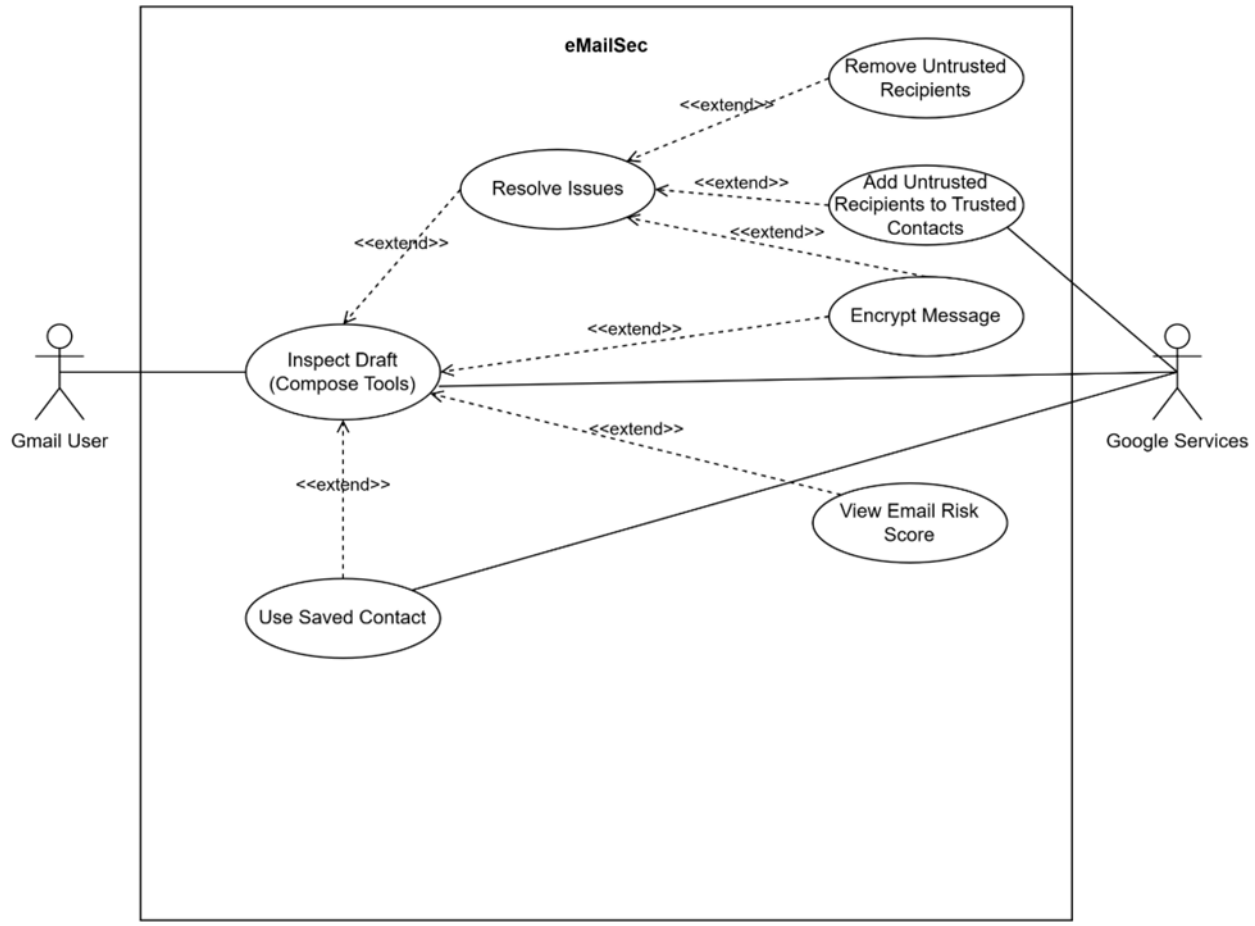
Σκόπιμα το διάγραμμα κρατήθηκε σε απλοποιημένη μορφή ώστε να είναι άμεσα κατανοητό: αποτυπώνει τους στόχους/λειτουργίες που βλέπει ο χρήστης στο Home και τις ουσιώδεις σχέσεις μεταξύ τους (υποχρεωτικά βήματα έναντι προαιρετικών επεκτάσεων), χωρίς να επιβαρύνεται με λεπτομέρειες διεπαφής ή ροές οθονών. Για παράδειγμα, ο έλεγχος Scan Drafts μπορεί να εκκινεί αυτόματα όταν ανοίγει/αλλάζει ένα πρόχειρο ή χειροκίνητα με “Rescan”, όμως και οι δύο τρόποι αφορούν το ίδιο use case και τεκμηριώνονται κειμενικά στα triggers της αντίστοιχης προδιαγραφής.



Εικόνα 6. Διάγραμμα Περιπτώσεων Χρήσης - View email.

Η περίπτωση χρήσης View Mail αντιπροσωπεύει τη βασική ροή που εκτελείται κάθε φορά που ο χρήστης ανοίγει ένα μήνυμα στο Gmail και ενεργοποιείται το πάνελ του eMailSec. Κατά την προβολή του μηνύματος, ο χρήστης μπορεί προαιρετικά να εκτελέσει επιπλέον ενέργειες, όπως σάρωση συνδέσμων (Scan Links), σάρωση συνημμένων αρχείων (Scan Attachments), αποκρυπτογράφηση περιεχομένου (Decrypt), προσθήκη του αποστολέα στις επαφές (Add Sender to Contacts) ή αποκλεισμό αποστολέα (Block Sender). Οι ενέργειες αυτές έχουν μοντελοποιηθεί ως επεκτάσεις (extend) της βασικής περίπτωσης χρήσης, καθώς εκτελούνται μόνο εφόσον το ζητήσει ο χρήστης. Ο Gmail User συνδέεται μόνο με τη βασική περίπτωση, ώστε να καταδεικνύεται ότι όλες οι υπόλοιπες λειτουργίες εκτελούνται στο πλαίσιο αυτής της αλληλεπίδρασης.

Η λειτουργία του διαγράμματος υποστηρίζεται από το Google Services, το οποίο λειτουργεί ως εξωτερική οντότητα και παρέχει στο eMailSec τις απαραίτητες διεπαφές για την ανάγνωση και επεξεργασία των δεδομένων των μηνυμάτων, των αποστολέων και των συνημμένων αρχείων. Οι υπηρεσίες της Google δεν εκκινούν οι ίδιες τις περιπτώσεις χρήσης, αλλά παίζουν έναν υποστηρικτικό ρόλο, επιτρέποντας στο πρόσθετο να υλοποιεί τις ενέργειες ασφάλειας και διαχείρισης εντός του περιβάλλοντος του Gmail.



Εικόνα 7. Διάγραμμα Περιπτώσεων Χρήσης - Compose menu.

Στο παραπάνω διάγραμμα, η Inspect Draft (Compose Tools) αποτελεί τη βασική περίπτωση χρήσης: κάθε φορά που ο χρήστης συντάσσει ή ανοίγει ένα πρόχειρο και εμφανίζεται το πάνελ του eMailSec, το σύστημα συλλέγει αυτόματα τα στοιχεία του πρόχειρου (παραλήπτες, θέμα, σώμα) και εκτελεί ελέγχους εμπιστοσύνης παραληπτών και ανίχνευσης ευαίσθητου περιεχομένου μέσω των υπηρεσιών Google Services.

Οι προαιρετικές ή υπό όρους ροές αποδίδονται ως extend της βασικής περίπτωσης:

- Η **Resolve Issues** ενεργοποιείται μόνο εφόσον εντοπιστούν προβλήματα, παρέχοντας καθοδηγούμενη επίλυση πριν την αποστολή. Στο εσωτερικό της, οι υποπεριπτώσεις **Remove Untrusted Recipients** και **Add Untrusted Recipients to Trusted Contacts** επιτρέπουν στον χρήστη να αφαιρέσει μη έμπιστους παραλήπτες ή να τους προσθέσει στις έμπιστες επαφές, αντίστοιχα.
- Η **Encrypt Message** μπορεί να ενεργοποιηθεί ανεξάρτητα από τον χρήστη, για την κρυπτογράφηση του μηνύματος πριν την αποστολή, αλλά και εντός της **Resolve Issues** όταν το μήνυμα περιέχει ευαίσθητο περιεχόμενο που απαιτεί προστασία. Η διαδικασία κρυπτογράφησης εκτελείται μέσω του Node.js Encryption API, το οποίο λειτουργεί ως ένας υποστηρικτικός μηχανισμός ασφαλείας.
- Η **View Email Risk Score** παρέχει τη δυνατότητα προβολής του συνολικού σκορ κινδύνου και επεξήγησης των παραγόντων που το διαμόρφωσαν.
- Η **Use Saved Contact**, υποστηριζόμενη επίσης από τις υπηρεσίες Google Services, επιτρέπει την εισαγωγή αποθηκευμένων ή έμπιστων επαφών κατά τη σύνταξη.

Ο Gmail User συνδέεται απευθείας μόνο με τη βασική περίπτωση χρήσης, ώστε να αποδίδεται καθαρά ότι όλες οι παραπάνω ενέργειες λαμβάνουν χώρα εντός του ίδιου context σύνταξης μηνύματος και ενεργοποιούνται προαιρετικά ή υπό συνθήκη. Το διάγραμμα παραμένει απλοποιημένο για να αναδεικνύει ποια τμήματα εκτελούνται πάντα αυτόματα και ποια ενεργοποιούνται από τον χρήστη, χωρίς να επιβαρύνεται με επιπλέον λεπτομέρειες διεπαφής.

4.3.5 Αναλυτική Περιγραφή Περιπτώσεων Χρήσης

Παρακάτω παρατίθενται οι πίνακες Αναλυτικής Περιγραφής Περιπτώσεων Χρήσης, οι οποίοι συμπληρώνουν τα διαγράμματα use case δίνοντας τυποποιημένη, επιχειρησιακή αποτύπωση κάθε λειτουργίας του συστήματος. Για κάθε περίπτωση χρήσης καταγράφονται: ο Τίτλος και η Γενική Περιγραφή (σκοπός/πεδίο εφαρμογής), οι Δρώντες (ποιοι αλληλεπιδρούν), οι Προ-συνθήκες και οι Μετά-συνθήκες (κατάσταση πριν/μετά την εκτέλεση), το Αποτέλεσμα (παρατηρήσιμο output), το Βασικό μονοπάτι (τυπική επιτυχής ροή βημάτων) και το Μονοπάτι Εξαίρεσης (αποκλίσεις/σφάλματα/εναλλακτικές), καθώς και ο Στόχος που αποσαφηνίζει το επιχειρησιακό όφελος. Η μορφή αυτή καθιστά τις απαιτήσεις ελέγξιμες και ανιχνεύσιμες: από την υψηλού επιπέδου πρόθεση του χρήστη μέχρι συγκεκριμένα βήματα υλοποίησης και κριτήρια αποδοχής. Με άλλα λόγια, οι πίνακες μεταφράζουν το «τι κάνει» το σύστημα σε ρητό «πώς, πότε και υπό

ποιες προϋποθέσεις το κάνει», ώστε η τεκμηρίωση να είναι συνεπής, σαφής και άμεσα εφαρμόσιμη.

UI context: Home

Πίνακας 6. Περίπτωση χρήσης - Scan Drafts

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Scan Drafts
Γενική Περιγραφή	Από την αρχική κάρτα (Home) ο χρήστης ζητά έλεγχο όλων των drafts του για ευαίσθητα δεδομένα, ύποπτους συνδέσμους και μη έμπιστους παραλήπτες. Το σύστημα συγκεντρώνει τα ευρήματα και εμφανίζει λίστα «Flagged Drafts».
Δρώντες	Gmail User
Προ – συνθήκες	(α) Εγκατεστημένο/εξουσιοδοτημένο eMailSec με κατάλληλα OAuth scopes, (β) Πρόσβαση στο Gmail Drafts, (γ) Διαθέσιμη σύνδεση**.**
Μετά – συνθήκες	Επικαιροποιημένος πίνακας ευρημάτων/στατιστικών. Αποθηκεύεται (τοπικά) η τελευταία ώρα/ημερομηνία σάρωσης.
Στόχος	Προληπτικός έλεγχος όλων των προχείρων (drafts), πριν προκύψει αποστολή με κίνδυνο/διαρροή.
Αποτέλεσμα	Προβάλλεται λίστα Flagged Drafts με σύνοψη ευρημάτων ή μήνυμα «No issues found». Παρέχεται σύνδεσμος Open Drafts Folder ή Review & Resolve.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Scan Drafts. 2) Το σύστημα απαριθμεί όλα τα drafts. 3) Για κάθε draft συλλέγει recipients/subject/body/(αν υπάρχουν) attachments. 4) Εκτελεί ελέγχους: (i) Recipients trust, (ii) Sensitive content 5) Συγκεντρώνει τα ευρήματα. 6) Εμφανίζει Flagged Drafts με δυνατότητα μετάβασης σε συγκεκριμένο draft για επίλυση.
Μονοπάτι Εξαίρεσης	E1: Δεν υπάρχουν drafts → ενημέρωση χρήστη. E2: Σφάλμα API/δίκτυο → μήνυμα και επιλογή Retry. E3: Ανεπαρκή δικαιώματα πρόσβασης (δηλαδή χωρίς την αντίστοιχη εξουσιοδότηση από τον χρήστη) → οδηγίες re-auth.

Πίνακας 7. Περίπτωση χρήσης - Manage Contacts

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Manage Contacts
Γενική Περιγραφή	Διαχείριση αποθηκευμένων επαφών (trusted) και κατηγοριών (επαφών), καθώς και προαιρετική διαχείριση blocked senders. Περιλαμβάνει προβολή/αναζήτηση/προσθήκη/ενημέρωση/διαγραφή επαφών και κατηγοριών, με δυνατότητα συσχέτισης κρυπτογραφικής ταυτότητας ανά επαφή: αποθήκευση Public Key (.asc), Signature (.sig), έλεγχος/επαλήθευση υπογραφής και επισήμανση Verification Status (Verified/Unverified).
Δρώντες	Gmail User
Προ – συνθήκες	(α) Διαθέσιμη αποθήκη επαφών/ρυθμίσεων (π.χ. PropertiesService), (β) εγκατεστημένο/εξουσιοδοτημένο eMailSec, (γ) για επαλήθευση: διαθέσιμα .asc και .sig από την επαφή.
Μετά – συνθήκες	Οι αλλαγές σε στοιχεία, κατηγορίες και κρυπτογραφική ταυτότητα επαφών έχουν αποθηκευτεί. Η κατάσταση εμπιστοσύνης (Trusted/Blocked, Verified/Unverified) ενημερώνει τους ελέγχους σε Home/Open Mail/Compose.
Στόχος	Εμπλουτισμός του καταλόγου επαφών με επαληθευμένες κρυπτογραφικές ταυτότητες, ώστε οι έλεγχοι ασφαλείας και οι λειτουργίες κρυπτογράφησης να βασίζονται σε αξιόπιστους συντελεστές (μείωση spoofing/MITM).
Αποτέλεσμα	Ενημερωμένη λίστα επαφών, σωστή κατηγοριοποίηση, ενημερωμένη blocklist και - όπου δόθηκαν δεδομένα - επαληθευμένο δημόσιο κλειδί και υπογραφή της επαφής.
Βασικό μονοπάτι	1) Ο χρήστης ανοίγει Open Contacts από το Home. 2) Προβολή λίστας/κατηγοριών & αναζήτησης. 3) Επιλογή Details σε επαφή ή Add New Contact. 4) Επεξεργασία στοιχείων (όνομα, email, κατηγορία Trusted/Blocked κ.λπ.). 5) (Προαιρετικά) Προσθήκη κρυπτογραφικής ταυτότητας επαφής: επικόλληση Public Key (.asc) και Signature (.sig). 6) Επιλογή Verify για έλεγχο γνησιότητας (*κλήση της Verify Public*

	Key). 7) Εμφάνιση αποτελέσματος: Valid → αποθήκευση κλειδιού/υπογραφής & Verification Status = Verified. Invalid → ενημέρωση, διατήρηση Unverified (ο χρήστης μπορεί να απορρίψει/αντικαταστήσει στοιχεία). 8) Αποθήκευση επαφής/Ενημέρωση επαφής.
Μονοπάτι Εξαίρεσης	E1: Ελλιπή πεδία κλειδιού/υπογραφής → μήνυμα "Provide both .asc and .sig". E2: Μη έγκυρη μορφή → αποτυχία parsing, οδηγία επανυποβολής. E3: Invalid/Non-matching signature → σήμανση Unverified και πρόταση "request new key/signature". E4: Διπλότυπο email → πρόταση ενημέρωσης αντί νέας καταχώρισης. E5: Μη έγκυρο email → απόρριψη με αιτιολόγηση. E6: Προστατευμένη κατηγορία (μη διαγράψιμη) → ενημέρωση του χρήστη για μη εφικτή διαγραφή.

Πίνακας 8. Περίπτωση χρήσης - Manage Keys.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Manage Keys
Γενική Περιγραφή	Διαχείριση ζευγών κλειδιών (PGP/RSA): Δημιουργία / Επαναφορά κλειδιών, Διανομή Δημόσιου Κλειδιού (με υπογραφή), Επαλήθευση Δημόσιου Κλειδιού & Υπογραφής, Αποθήκευση στο Google Drive.
Δρώντες	Gmail User
Προ – συνθήκες	Διαθέσιμες κρυπτογραφικές λειτουργίες/αποθήκευση κλειδιών, κατάλληλα scopes (όπου απαιτείται για Drive).
Μετά – συνθήκες	Επικαιροποιημένα κλειδιά/υπογραφές, διαθέσιμο δημόσιο κλειδί για διανομή, προαιρετικά backup στο Drive.
Στόχος	Εξασφάλιση έγκυρου/διαθέσιμου κρυπτογραφικού υλικού για κρυπτογράφηση/αποκρυπτογράφηση και εμπιστοσύνη κλειδιών τρίτων.
Αποτέλεσμα	Νέα/επικαιροποιημένα κλειδιά, επιτυχής επαλήθευση τρίτων κλειδιών, αντιγραφή/αποθήκευση δημόσιου κλειδιού.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Manage. 2) Προβάλλεται τρέχον δημόσιο κλειδί. 3)

	Επιλογές: Reset Keys (με επιβεβαίωση), Distribute My Public Key (αντιγραφή/αποστολή), Verify Public Key + Signature (επικόλληση .asc/.sig → αποτέλεσμα), Save to Google Drive (δημιουργία αρχείου).
Μονοπάτι Εξαίρεσης	E1: Αποτυχία δημιουργίας/αποθήκευσης κλειδιού → ενημέρωση/δοκίμασε ξανά. E2: Αποτυχία επαλήθευσης υπογραφής → σαφές μήνυμα μη γνησιότητας. E3: Σφάλμα στις άδειες του Drive(δεν έχουν δοθεί οι αδειες απο το χρήστη) → οδηγίες επανεξουσιοδότησης.

Πίνακας 9. Περίπτωση χρήσης - Verify Public Key.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Verify Public Key
Γενική Περιγραφή	Ο χρήστης επαληθεύει τη γνησιότητα και ακεραιότητα ενός δημόσιου κλειδιού που έλαβε. Επικολλά το ASCII-armored δημόσιο κλειδί (.asc) και την αποσυνδεδεμένη ψηφιακή υπογραφή του (.sig) και πατά Verify Now. Το σύστημα ελέγχει την υπογραφή επάνω στο περιεχόμενο του κλειδιού και εμφανίζει σαφές αποτέλεσμα (έγκυρη/άκυρη).
Δρώντες	Gmail User
Προ – συνθήκες	(α) Διαθέσιμα το δημόσιο κλειδί (.asc) και η αντίστοιχη υπογραφή (.sig) από τον αποστολέα, (β) ενεργό eMailSec με πρόσβαση στις κρυπτογραφικές συναρτήσεις.
Μετά – συνθήκες	Εμφανίζεται αποτέλεσμα επαλήθευσης (valid/invalid) και προαιρετικά προτείνονται επόμενα βήματα (π.χ. αποθήκευση/εισαγωγή επαφής ως verified). Δεν αλλάζει κάτι στο draft ή σε άλλα δεδομένα, εκτός αν ο χρήστης επιλέξει σχετική ενέργεια.
Στόχος	Να επιβεβαιωθεί πριν από τη χρήση ότι το δημόσιο κλειδί που μοιράστηκε ένας αποστολέας είναι πράγματι αυθεντικό και δεν έχει αλλοιωθεί, μειώνοντας τον κίνδυνο spoofing/man-in-the-middle**.**
Αποτέλεσμα	Μήνυμα π.χ. “Signature valid — key is authentic and untampered” ή “Invalid signature — key

	may be altered or not signed by the expected party.”
Βασικό μονοπάτι	1) Από το Home επιλέγεται Verify Key (ή: Home → Manage Keys → Verify). 2) Επικόλληση Public Key (.asc). 3) Επικόλληση Signature (.sig). 4) Κανονικοποίηση/ανάλυση armored κειμένου και φόρτωση υπογραφής. 5) Κρυπτογραφικός έλεγχος της υπογραφής πάνω στο περιεχόμενο του κλειδιού. 6) Εμφάνιση αποτελέσματος· προαιρετικά κουμπί για αποθήκευση/συσχέτιση με επαφή.
Μονοπάτι Εξαίρεσης	E1: Λείπει κάποιο πεδίο → μήνυμα “Please provide both .asc and .sig”. E2: Μη έγκυρη μορφή (.asc/.sig) → αποτυχία parsing με οδηγία επανυποβολής. E3: Invalid/Non-matching signature → εμφανίζεται αποτυχία επαλήθευσης. E4: Μη υποστηριζόμενος αλγόριθμος→ ενημέρωση του χρήστη για αποτυχία διαδικασίας επαλήθευσης .

Πίνακας 10. Περίπτωση χρήσης - View Security Reports.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	View Security Reports
Γενική Περιγραφή	Επισκόπηση βασικών μετρικών ασφάλειας του eMailSec: συνολικοί έλεγχοι emails με ευαίσθητα δεδομένα, πλήθος ευαίσθητων λέξεων/ευρημάτων, Last scan (ημερομηνία/ώρα).
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec, (β) Υπάρχουν αποθηκευμένα δεδομένα σάρωσης/στατιστικών.
Μετά – συνθήκες	(Καμία αλλαγή στο σύστημα)· ο χρήστης έχει ενημερωθεί για την τρέχουσα εικόνα ρίσκου.
Στόχος	Γρήγορη κατάσταση ασφάλειας & τεκμηρίωση για λήψη αποφάσεων/προτεραιοτήτων.
Αποτέλεσμα	Προβολή καρτέλας Security Activity Reports με ενημερωμένα μεγέθη.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει View Reports. 2) Το σύστημα ανακτά/υπολογίζει μετρικές. 3) Εμφανίζει Total emails scanned, Emails with sensitive data, Total sensitive words found, Last

	scan (date/time).
Μονοπάτι Εξαίρεσης	E1: Μη διαθέσιμα δεδομένα → μήνυμα και πρόταση Scan Drafts/εκκίνηση σάρωσης. E2: Σφάλμα ανάκτησης → ενημέρωση & προσπάθεια ξανά.

UI context: Open mail

Πίνακας 11. Περίπτωση χρήσης - View mail.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	View mail
Γενική Περιγραφή	Ο χρήστης ανοίγει ένα μήνυμα στο Gmail και προβάλλει το πάνελ eMailSec. Το σύστημα εμφανίζει βασικά στοιχεία μηνύματος και αξιολογεί την εμπιστοσύνη του αποστολέα και την κατάσταση κρυπτογράφησης. Παρέχει επιλογές ενεργειών (Scan Links/Attachments, Decrypt, Add to Contacts, Block).
Δρώντες	Gmail User
Προ – συνθήκες	α) Ανοικτό email (thread/messageId διαθέσιμο), (β) εγκατεστημένο & εξουσιοδοτημένο eMailSec (OAuth scopes), (γ) πρόσβαση στο σώμα/headers/attachments του μηνύματος.
Μετά – συνθήκες	Έχει παρουσιαστεί η τρέχουσα κατάσταση ασφάλειας του μηνύματος και οι διαθέσιμες ενέργειες.
Στόχος	Γρήγορη εικόνα ασφάλειας για το συγκεκριμένο email και διάθεση στοχευμένων ενεργειών.
Αποτέλεσμα	Εμφάνιση λεπτομερειών (Subject/From/Date/Preview) και ενδείξεων: “sender not in Safe Contacts”, “message encrypted?” κ.λπ., με ενεργά κουμπιά ενεργειών.
Βασικό μονοπάτι	1) Ο χρήστης ανοίγει το πάνελ σε ανοικτό email. 2) Συλλογή στοιχείων μηνύματος (αποστολέας, ημερομηνία, θέμα, σύνοψη). 3) Αξιολόγηση αποστολέα & κατάστασης κρυπτογράφησης (Saved/Trusted/Unknown, PGP). 4) Προβολή κατάστασης & διαθέσιμων ενεργειών (Scan Links, Scan Attachments, Decrypt, Add Sender to Contacts, Block Sender).

Μονοπάτι Εξαίρεσης	E1: Μη προσβάσιμο περιεχόμενο/σφάλμα API → μήνυμα και επιλογή επανάληψης. E2: Ελλιπή scopes → οδηγίες re-auth.

Πίνακας 12. Περίπτωση χρήσης - Scan Links.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Scan Links
Γενική Περιγραφή	Έλεγχος όλων των URL του μηνύματος για ύποπτα χαρακτηριστικά (μορφολογία, ομογραφία, ύποπτα TLD, γνωστές λίστες/κανόνες).
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Ανοικτό email, πρόσβαση στο σώμα/HTML.
Μετά – συνθήκες	Παράγονται ευρήματα/προειδοποιήσεις για συνδέσμους (ή καμία εύρεση).
Στόχος	Εντοπισμός/ελαχιστοποίηση phishing & κακόβουλων ανακατευθύνσεων.
Αποτέλεσμα	Αναφορά συνδέσμων με ένδειξη ασφαλείας/κινδύνου και προτάσεις δράσης.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Scan Links. 2) Εξαγωγή & κανονικοποίηση URL. 3) Έλεγχοι βάσει κανόνων/λιστών. 4) Εμφάνιση αποτελεσμάτων (OK/Warning) και (αν χρειάζεται) μετάβαση σε Resolve Issues.
Μονοπάτι Εξαίρεσης	E1: Δεν βρέθηκαν σύνδεσμοι → μήνυμα “No links found”. E2: Σφάλμα ανάλυσης/δικτύου → ενημέρωση & retry.

Πίνακας 13. Περίπτωση χρήσης - Scan Attachments.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Scan Attachments
Γενική Περιγραφή	Έλεγχος μεταδεδομένων και περιεχομένου συνημμένων για πιθανές απειλές.

Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β)Υπάρχουν συνημμένα στο email και επιτρέπεται πρόσβαση στα μεταδεδομένα/περιεχόμενο.
Μετά – συνθήκες	Παράγεται αναφορά ευρημάτων/προειδοποιήσεων ανά συνημμένο.
Στόχος	Μείωση ρίσκου από κακόβουλα ή ευαίσθητα συνημμένα.
Αποτέλεσμα	Ενημέρωση για πιθανούς κινδύνους (τύπος αρχείου).
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Scan Attachments. 2) Ανάκτηση λίστας/μεγεθών/τύπων. 3) Παρουσίαση αποτελεσμάτων & επιλογές δράσης (π.χ. αποθήκευση/αποφυγή λήψης, κ.λ.π.).
Μονοπάτι Εξαίρεσης	E1: Δεν υπάρχουν συνημμένα → μήνυμα. E2: Σφάλμα πρόσβασης → retry.

Πίνακας 14. Περίπτωση χρήσης - Decrypt Email.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Decrypt Email.
Γενική Περιγραφή	Απόπειρα αποκρυπτογράφησης PGP-κρυπτογραφημένου μηνύματος με διαθέσιμα ιδιωτικά κλειδιά/φράση.
Δρώντες	Gmail User.
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Το email είναι PGP-encrypted και υπάρχουν/είναι διαθέσιμα τα απαιτούμενα κλειδιά.
Μετά – συνθήκες	Προβάλλεται αποκρυπτογραφημένο περιεχόμενο ή ενημέρωση αποτυχίας/έλλειψης κλειδιών.
Στόχος	Ανάγνωση περιεχομένου που προστατεύεται με κρυπτογράφηση.
Αποτέλεσμα	Πρόσβαση στο πραγματικό περιεχόμενο (αν επιτυχής), ή καθοδήγηση για Manage Keys**.**
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Decrypt. 2) Το σύστημα αναζητά κατάλληλο ιδιωτικό κλειδί/φράση. 3) Εκτελείται αποκρυπτογράφηση. 4) Προβάλλεται

	το αποτέλεσμα (ή σώζεται προσωρινά για προβολή).
Μονοπάτι Εξαίρεσης	E1: Δεν βρέθηκε συμβατό κλειδί/λάθος φράση → οδηγία για Manage Keys/Import/Verify. E2: Σφάλμα αποκρυπτογράφησης → ενημέρωση & retry.

Πίνακας 15. Περίπτωση χρήσης - Add Sender to Contacts.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Add Sender to Contacts
Γενική Περιγραφή	Αποθήκευση/ενημέρωση του αποστολέα του email στις trusted επαφές, με αντιστοίχιση σε κατηγορία.
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Προβάλλεται ο αποστολέας του τρέχοντος email. Υπάρχει πρόσβαση στο αποθετήριο επαφών.
Μετά – συνθήκες	Δημιουργημένη/ενημερωμένη επαφή, διαθέσιμη στους ελέγχους εμπιστοσύνης.
Στόχος	Μείωση “Unknown sender” ειδοποιήσεων & βελτίωση εμπιστοσύνης.
Αποτέλεσμα	Ο αποστολέας χαρακτηρίζεται ως γνωστή/έμπιστη επαφή.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Add Sender to Contacts. 2) Έλεγχος αν υπάρχει ήδη επαφή. 3) Δημιουργία ή ενημέρωση στοιχείων. 4) Επιλογή/αντιστοίχιση κατηγορίας. 5) Επιβεβαίωση.
Μονοπάτι Εξαίρεσης	E1: Μη έγκυρο email/διπλότυπο → κατάλληλο μήνυμα & πρόταση ενημέρωσης. E2: Ακύρωση χρήστη → καμία αλλαγή**.**

Πίνακας 16. Περίπτωση χρήσης - Block Sender.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Block Sender
Γενική Περιγραφή	Προσθήκη του αποστολέα σε blocklist του eMailSec (και προαιρετικά δημιουργία φίλτρου

	απόρριψης/αρχειοθέτησης στο Gmail).
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Προβάλλεται ο αποστολέας του τρέχοντος email.
Μετά – συνθήκες	Ο αποστολέας εμφανίζεται ως «μπλοκαρισμένος» σε μελλοντικούς ελέγχους.
Στόχος	Μόνιμος αποκλεισμός ενοχλητικών/κακόβουλων αποστολέων και μείωση ρίσκου.
Αποτέλεσμα	Επιτυχής προσθήκη σε blocklist (με δυνατότητα αναίρεσης).
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει Block Sender. 2) Προβολή επιβεβαίωσης. 3) Προσθήκη στην blocklist (προαιρετικά: δημιουργία φίλτρου Gmail). 4) Μήνυμα ολοκλήρωσης.
Μονοπάτι Εξαίρεσης	E1: Ο αποστολέας είναι ήδη σε blocklist → ενημέρωση του χρήστη πως η ενέργεια απέτυχε για αυτό τον λόγο. E2: Ακύρωση χρήστη → καμία αλλαγή.

UI context: Compose/Draft

Πίνακας 17. Περίπτωση χρήσης - Inspect Draft.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Inspect Draft
Γενική Περιγραφή	Ο χρήστης ανοίγει/συντάσσει ένα πρόχειρο email και εμφανίζει το πάνελ eMailSec. Το σύστημα συλλέγει τα στοιχεία του draft και εκτελεί ελέγχους παραληπτών και περιεχομένου. Προβάλλει συνοπτικά αν βρέθηκαν ζητήματα ή ένδειξη “No sensitive data detected”**.**
Δρώντες	Gmail User
Προ – συνθήκες	(α) Υπάρχει ανοιχτό draft (new/reply/forward) στο Gmail, (β) eMailSec είναι εγκατεστημένο και εξουσιοδοτημένο (OAuth scopes), (γ) πρόσβαση στο ενεργό draft/thread.
Μετά – συνθήκες	Η κατάσταση ασφαλείας του draft έχει ενημερωθεί (ευρήματα/καθαρό). Τυχόν αλλαγές

	που έκανε ο χρήστης (π.χ. σε παραλήπτες) έχουν αποθηκευτεί.
Στόχος	Άμεση ορατότητα της κατάστασης ασφαλείας του πρόχειρου πριν την αποστολή.
Αποτέλεσμα	Εμφανίζεται στο πάνελ είτε Warning/Notice με κουμπί Resolve Issues είτε πράσινη ένδειξη No sensitive data detected, μαζί με προαιρετικές ενέργειες**.**
Βασικό μονοπάτι	1) Ανάκτηση recipients/subject/body/(υπάρχουν;)attachments. 2) Έλεγχος παραληπτών (Saved/Trusted/Unknown/Blocked). 3) Ανάλυση subject & body για ευαίσθητα μοτίβα/λέξεις. 4) Αν δεν βρεθούν ευρήματα → εμφάνιση "No sensitive data detected". 5) Διαθέσιμα κουμπιά: Encryption Options, Use Saved Contact, View Email Risk Score.
Μονοπάτι Εξαίρεσης	Ε1: Εντοπίζονται Unknown recipients ή ευαίσθητο περιεχόμενο → προβάλλεται Security Notice/Warning και κουμπί Resolve Issues. Ε2: Σφάλμα πρόσβασης στο draft → ενημέρωση και επανάληψη. Ε3: Απουσία απαιτούμενων scopes → οδηγίες επαναεξουσιοδότησης .

Πίνακας 18. Περίπτωση χρήσης - Resolve Issues.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Resolve Issues
Γενική Περιγραφή	Καθοδηγούμενη επίλυση των ευρημάτων (παραλήπτες/περιεχόμενο) πριν την αποστολή.
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Έχουν εντοπιστεί ευρήματα στο draft και ο χρήστης επέλεξε Resolve Issues.
Μετά – συνθήκες	Το πρόχειρο έχει ενημερωθεί (παραλήπτες, περιεχόμενο ή πολιτικές), έχει πραγματοποιηθεί αυτόματα νέος έλεγχος (scan) και η ένδειξη έχει ανανεωθεί.
Στόχος	Να λυθούν τα προβλήματα που εμποδίζουν ασφαλή αποστολή.
Αποτέλεσμα	Μηδενισμός ή μείωση ευρημάτων/ρίσκου, ή

	συνειδητή αποδοχή ρίσκου όπου επιτρέπεται από πολιτική.
Βασικό μονοπάτι	1) Display Findings Summary (πάντα). 2) Αν υπάρχουν Unknown recipients → προβάλλεται ενότητα Unknown Recipients Check με επιλογές: Remove Unknown Recipients ή Add to Trusted Contacts. 3) Αν υπάρχει Sensitive content → Subject & Body Check με Take Action (διόρθωση/απόκρυψη ή κλήση Encryption Options). 4) Ο χρήστης εφαρμόζει ενέργειες και πατά Re-scan. 5) Επιστροφή στο compose menu με ενημερωμένη κατάσταση.
Μονοπάτι Εξαίρεσης	E1: Ακύρωση από τον χρήστη → επιστροφή στο compose menu χωρίς αλλαγές. E2: Σφάλμα κατά την εκτέλεση ή την αποθήκευση αλλαγών → εμφάνιση ενημερωτικού μηνύματος και δυνατότητα επανάληψης της ενέργειας.

Πίνακας 19. Περίπτωση χρήσης - Encryption Options.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Encryption Options
Γενική Περιγραφή	Ρυθμίσεις και εφαρμογή κρυπτογράφησης/υπογραφής στο εξερχόμενο email.
Δρώντες	Gmail User
Προ – συνθήκες	Ο χρήστης επέλεξε Encryption Options από το compose menu ή οδηγήθηκε εδώ μέσω Resolve Issues → Take Action.
Μετά – συνθήκες	Έχει διαμορφωθεί/εφαρμοστεί πολιτική κρυπτογράφησης (και προαιρετική υπογραφή).
Στόχος	Εμπιστευτικότητα/ακεραιότητα περιεχομένου σύμφωνα με πολιτικές ασφαλείας.
Αποτέλεσμα	Το draft ενημερώνεται (PGP), και οι ρυθμίσεις αποθηκεύονται.
Βασικό μονοπάτι	1) Επιλογή τρόπου: Provide recipient's public key ή Request key. 2) Εισαγωγή/έλεγχος κλειδιών (και .sig όπου ισχύει). 3) Επιλογή πολιτικής (encrypt subject/body/attachments, sign). 4) Εφαρμογή και επιστροφή στο compose menu με re-scan.

Μονοπάτι Εξαίρεσης	E1: Αποτυχία επαλήθευσης/εύρεσης κλειδιού → ενημέρωση, πρόταση Import/Verify Key.

Πίνακας 20. Περίπτωση χρήσης - Use Saved Contact.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	Use Saved Contact
Γενική Περιγραφή	Γρήγορη εισαγωγή/αντικατάσταση παραληπτών από τις αποθηκευμένες/έμπιστες επαφές.
Δρώντες	Gmail User
Προ – συνθήκες	(α) Ενεργό eMailSec. (β) Υπάρχει διαθέσιμη λίστα επαφών/κατηγοριών του χρήστη.
Μετά – συνθήκες	Οι παραλήπτες του draft έχουν ενημερωθεί και γίνεται re-scan.
Στόχος	Ταχεία επιλογή ασφαλών παραληπτών και μείωση λαθών διευθύνσεων.
Αποτέλεσμα	Μείωση άγνωστων παραληπτών, ευθυγράμμιση με trusted contacts.
Βασικό μονοπάτι	1) Άνοιγμα καταλόγου επαφών. 2) Αναζήτηση/φίλτρα/κατηγορία. 3) Επιλογή επαφής και εισαγωγή σε To/CC/Bcc. 4) Re-scan στο compose menu.
Μονοπάτι Εξαίρεσης	E1: Αποτυχία αναζήτησης (π.χ. σφάλμα ανάκτησης δεδομένων) → εμφάνιση μηνύματος σφάλματος και δυνατότητα επανάληψης της αναζήτησης. E2: Ακύρωση επιλογής → καμία αλλαγή.

Πίνακας 21. Περίπτωση χρήσης - View Email Risk Score.

Πεδίο	**Περιγραφή**
Τίτλος Περίπτωσης Χρήσης	View Email Risk Score
Γενική Περιγραφή	Προβολή συνολικού σκορ ρίσκου του τρέχοντος draft και ανάλυση συνεισφορών (recipients, content, links, attachments).
Δρώντες	Gmail User

Προ – συνθήκες	(α) Ενεργό eMailSec. (β)Υπάρχει πρόσφατο αποτέλεσμα scan.
Μετά – συνθήκες	Ο χρήστης λαμβάνει τεκμηριωμένη εικόνα ρίσκου και ενδεχόμενες συστάσεις δράσης.
Αποτέλεσμα	Απόφαση για αποστολή/διόρθωση/κρυπτογράφηση με βάση διαφάνεια κριτηρίων.
Βασικό μονοπάτι	1) Ο χρήστης επιλέγει την ενέργεια “View Score” 2) Το σύστημα εμφανίζει το συνολικό σκορ και τους επιμέρους δείκτες κινδύνου
Μονοπάτι Εξαίρεσης	E1: Σφάλμα υπολογισμού → ενημέρωση & retry.
Στόχος	Διαφάνεια και υποστήριξη απόφασης πριν την αποστολή.

4.4 Υλοποίηση

4.4.1 Επιλογή Gmail ως Βάση Υλοποίησης

Η επιλογή του Gmail ως πλατφόρμα για την ανάπτυξη του πρόσθετου DLPS έγινε λόγω:

- **Ευρείας διάδοσης**: εκατομμύρια ενεργοί χρήστες, που καθιστούν το Gmail ιδανικό για ανάπτυξη λύσεων με ευρύ αντίκτυπο.

- **Υποστήριξης Add-ons μέσω Google Apps Script**: παρέχεται ευέλικτο περιβάλλον για ανάπτυξη επεκτάσεων με πρόσβαση στο UI και στα APIs του Gmail.

- **Χρήση ενσωματωμένων χαρακτηριστικών ασφάλειας**: κρυπτογράφηση TLS κατά τη μεταφορά, πρωτόκολλα SPF/DKIM/DMARC για επαλήθευση αποστολέων και ισχυρό spam/phishing φίλτρο παρέχονται ως υλοποιημένες λειτουργίες προς ενσωμάτωση.

- **Επεκτασιμότητας**: δυνατότητα ενσωμάτωσης τρίτων εργαλείων ασφαλείας και αξιοποίησης υπηρεσιών, όπως Google Vault.

Τα παραπάνω στοιχεία καθιστούν το Gmail μια ασφαλή και ευέλικτη βάση πάνω στην οποία το eMailSec προσθέτει εξειδικευμένες λειτουργίες προστασίας περιεχομένου (ανίχνευση ευαίσθητων δεδομένων, εφαρμογή πολιτικών, κρυπτογράφηση/υπογραφή).

4.4.2 Υλοποίηση Αρχιτεκτονικής Συστήματος

Στην ενότητα 4.3 παρουσιάστηκε η συνολική αρχιτεκτονική του eMailSec, όπου διακρίνονται τρία κύρια επίπεδα: Client-Side, Server-Side και External Services, καθώς και οι βασικοί controllers του backend (DraftAnalysisController, ContactController, KeysController, EncryptionAPIController). Οι controllers αυτοί ορίζουν τις λειτουργίες και τους μηχανισμούς επικοινωνίας μεταξύ του περιβάλλοντος χρήστη και των εσωτερικών ή εξωτερικών υπηρεσιών, αποτελώντας την "καρδιά" του συστήματος.

Η παρούσα ενότητα περιγράφει την υλοποίηση της αρχιτεκτονικής αυτής, η οποία ακολουθεί πολυεπίπεδη (Layered) δομή με στοιχεία Ports & Adapters. Σε έναν βαθμό, η αρχιτεκτονική μπορεί να θεωρηθεί εξαγωνική (Hexagonal), καθώς η επιχειρησιακή λογική παραμένει ανεξάρτητη από τις τεχνολογίες αποθήκευσης και από το εξωτερικό Encryption API. Με άλλα λόγια, αν το σύστημα χρησιμοποιούσε διαφορετικό αποθηκευτικό μηχανισμό ή διαφορετικό πάροχο κρυπτογράφησης, η λειτουργία του θα παρέμενε αναλλοίωτη. Αυτό το χαρακτηριστικό ευθυγραμμίζεται με την αρχή της "αντιστροφής εξαρτήσεων" (Dependency Inversion) που θεμελιώνει την εξαγωνική αρχιτεκτονική[108], [109].

4.4.2.1 Layered Architecture

Η πολυεπίπεδη αρχιτεκτονική χωρίζει το σύστημα σε διαφορετικά στρώματα, καθένα από τα οποία έχει συγκεκριμένο ρόλο:

- Το **Presentation Layer** αναλαμβάνει την αλληλεπίδραση με τον χρήστη - ανήκει στο Client-Side.

- Το **Application Layer** περιλαμβάνει την επιχειρησιακή λογική - ανήκει στο Server-Side.

- Το **Data Layer** είναι υπεύθυνο για την αποθήκευση και ανάκτηση δεδομένων - ανήκει στο Server-Side.

- Το **External Services Layer** ενσωματώνει λειτουργίες από εξωτερικά συστήματα ή APIs - ανήκει στα External Services.

Ο διαχωρισμός αυτός επιτρέπει σε κάθε στρώμα να εξελίσσεται ανεξάρτητα, ενώ οι αλλαγές σε ένα επίπεδο έχουν περιορισμένο αντίκτυπο στα υπόλοιπα [110].

4.4.2.2 Ports & Adapters (Hexagonal Architecture)

Η αρχιτεκτονική Ports & Adapters (Hexagonal) προτείνει ότι ο πυρήνας της εφαρμογής (domain logic) πρέπει να είναι ανεξάρτητος από συγκεκριμένες τεχνολογίες [109]. Αυτό επιτυγχάνεται με:

- **Ports (θύρες):** διεπαφές που ορίζουν πώς η επιχειρησιακή λογική επικοινωνεί με τον έξω κόσμο.

- **Adapters (προσαρμογείς):** συγκεκριμένες υλοποιήσεις των ports που συνδέουν την εφαρμογή με εξωτερικά συστήματα (UI, αποθήκευση, APIs).

Στο eMailSec, οι θύρες καταναλώνονται από το **Application Layer**, όπου οι **controllers** λειτουργούν ως «application adapters»: λαμβάνουν τις ενέργειες του χρήστη από τη διεπαφή (UI), τις μετασχηματίζουν σε κλήσεις προς τα αντίστοιχα ports και εκτελούν τη ροή λογικής χωρίς να εξαρτώνται από τον εκάστοτε αποθηκευτικό μηχανισμό ή τον πάροχο κρυπτογράφησης.

4.4.2.3 Εφαρμογή στο Add-on

Στο παρόν σύστημα η αρχιτεκτονική εφαρμόζεται ως εξής:

1. **Presentation Layer (Gmail Add-on UI)**
    - Υλοποιείται με το **Google Apps Script CardService στο client-side**.
    - Παρουσιάζει δυναμικές κάρτες στον χρήστη με λειτουργίες όπως:
        - Σάρωση προσχεδίων (drafts) για ευαίσθητα δεδομένα.
        - Επίλυση προβλημάτων παραληπτών/περιεχομένου.
        - Κρυπτογράφηση/αποκρυπτογράφηση μηνυμάτων.
        - Διαχείριση επαφών (προσθήκη, διαγραφή, κατηγοριοποίηση, blocklist).
        - Διαχείριση δημόσιων/ιδιωτικών κλειδιών και υπογραφών.
        - Προβολή δείκτη επικινδυνότητας (risk score).
2. **Application / Service Layer (Λογική Εφαρμογής)**

    Το επίπεδο αυτό δεν λειτουργεί ως ανεξάρτητο RESTful API, αλλά ως εσωτερικό επίπεδο λογικής εφαρμογής του Gmail Add-on. Οι συναρτήσεις του εκτελούνται εντός του περιβάλλοντος του Google Apps Script και καλούνται απευθείας από το UI (CardService actions).
    - Περιλαμβάνει functions στο Google Apps Script που υλοποιούν (Πίνακας 22):
        - Έλεγχο παραληπτών (trusted, untrusted, blocked).
        - Ανίχνευση ευαίσθητων δεδομένων με regex.
        - Υπολογισμό κινδύνου (risk scoring).
        - Διαχείριση επαφών, κατηγοριών και λιστών αποκλεισμού (προσθήκη, διαγραφή, ενημέρωση, αναζήτηση και μεταφορά επαφών μεταξύ κατηγοριών).

    - Διαχείριση κλειδιών (δημιουργία, χρήση, επαλήθευση).
    - Διασύνδεση με το Node.js backend για λειτουργίες κρυπτογράφησης.
- Ορίζονται τα **Ports**:
    - CryptoPort → κρυπτογράφηση/υπογραφές.
    - ContactsPort → διαχείριση επαφών.
    - KeysPort → διαχείριση κλειδιών.
    - PoliciesPort → εφαρμογή κανόνων DLP.

Η υλοποίηση βασίζεται σε **controllers**, οι οποίοι ομαδοποιούν συναρτήσεις με κοινές ευθύνες και συνδέονται με τα αντίστοιχα ports.

Πίνακας 22. Αντιστοιχία controller με ports και κύριες συναρτήσεις.

Controller	**Κύριες Συναρτήσεις**	**Ports που χρησιμοποιούνται**	**Περιγραφή**
DraftAnalysisController	scanDraft(), resolveIssues()	PoliciesPort, ContactsPort	Ανιχνεύει ευαίσθητα δεδομένα με regex και αξιολογεί παραλήπτες βάσει εμπιστοσύνης.
ContactController	addContact(), updateContact(), deleteContact(), searchContacts(), moveCategories()	ContactsPort	Διαχειρίζεται τις επαφές, τις κατηγορίες και τις λίστες αποκλεισμού.
KeysController	generateKeys(), showKeys(), uploadPublicKey(), downloadPublicKey()	KeysPort, CryptoPort	Δημιουργεί και διανέμει δημόσια/ιδιωτικά κλειδιά, δημιουργεί υπογραφές.
EncryptionAPIController	encrypt(), decrypt(), validateSignature()	CryptoPort	Επικοινωνεί με το Encryption API (Node.js) για τις λειτουργίες κρυπτογράφησης/αποκρυπτογράφησης.

3. **Data Layer (Αποθήκευση)**
    - Υλοποιείται με το **Google PropertiesService**.
    - Αποθηκεύει: επαφές, κατηγορίες, trusted/blocked senders, δημόσια/ιδιωτικά κλειδιά, υπογραφές, ρυθμίσεις και patterns.

4. **External Services Layer (Εξωτερικές Υπηρεσίες)**

    Η **Google Cloud Platform** παρέχει τις απαραίτητες υπηρεσίες που καταναλώνουν οι controllers για τη σωστή λειτουργία του συστήματος:

    - **DraftAnalysisController** → αξιοποιεί Gmail Runtime (πρόσβαση σε draft/metadata όπου επιτρέπεται) και PropertiesService (patterns, ρυθμίσεις) για ανίχνευση & risk.
    - **ContactController** → στηρίζεται στο PropertiesService για CRUD επαφών, κατηγοριών και blocked λιστών.
    - **KeysController** → χρησιμοποιεί PropertiesService για ασφαλή αποθήκευση public/private keys και .sig εντός του λογαριασμού χρήστη.
    - **EncryptionAPIController** → καλύπτεται από τις δυνατότητες ταυτοποίησης/εξουσιοδότησης του OAuth 2.0 και τη ροή με Gmail Runtime (ενώ οι καθαρά κρυπτογραφικές πράξεις δεν παρέχονται από GCP στο πλαίσιο του Apps Script και υλοποιούνται εκτός του παρόντος επιπέδου).

Με αυτόν τον τρόπο, το **External Services Layer** αντιστοιχεί λειτουργικά σε **όλους τους controllers**, παρέχοντας αυθεντικοποίηση/εξουσιοδότηση, πρόσβαση στο περιβάλλον του Gmail και ενσωματωμένη αποθήκευση μικρού όγκου δεδομένων — με **μοναδική εξαίρεση** τις καθαρά κρυπτογραφικές πράξεις[11], οι οποίες δεν καλύπτονται από Apps Script.

[11] *Για τις καθαρά κρυπτογραφικές λειτουργίες (δημιουργία/ανανέωση κλειδιών, κρυπτογράφηση/αποκρυπτογράφηση, υπογραφή/επαλήθευση), οι EncryptionAPIController και KeysController αξιοποιούν ένα τρίτο εξωτερικό component, το Node.js Encryption API, στο οποίο γίνεται κλήση μέσω UrlFetchApp (endpoints: /generate, /encrypt, /decrypt, /validate). Το API αυτό παρέχει τις απαιτούμενες υπηρεσίες που δεν υποστηρίζονται εγγενώς από το Apps Script, ενώ η αυθεντικοποίηση/εξουσιοδότηση του προσθέτου παραμένει στη Google Cloud Platform.*

4.4.2.4 Αιτιολόγηση της επιλογής αρχιτεκτονικής

Η συγκεκριμένη προσέγγιση επιλέχθηκε επειδή:

- **Διαχωρίζει ρόλους** (UI, λογική, αποθήκευση, εξωτερικές υπηρεσίες).
- **Εξασφαλίζει επεκτασιμότητα** (προσθήκη νέων λειτουργιών χωρίς αλλαγές στον πυρήνα).
- **Ενισχύει την ασφάλεια** (ιδιωτικά κλειδιά φυλάσσονται στο PropertiesService).

Διευκολύνει τη δοκιμασιμότητα (μέσω Ports μπορούν να δοκιμαστούν σενάρια με mock adapters επιτρέποντας την δοκιμή των συστατικών του συστήματος σε απομόνωση, πριν προχωρήσουμε στις δοκιμές ενοποίησης και συστήματος όπου ελέγχονται ενοποιημένα μέρη ή όλο το σύστημα).

4.4.3 Επαναχρησιμοποιούμενες Βιβλιοθήκες και Εργαλεία Ανάπτυξης

Η υλοποίηση του eMailSec στηρίχθηκε σε ένα σύνολο έτοιμων βιβλιοθηκών και εργαλείων ανάπτυξης, τόσο στο επίπεδο του Gmail Add-on (frontend), όσο και στο backend (Node.js API). Η αξιοποίησή τους επιτρέπει την επαναχρησιμοποίηση δοκιμασμένων λειτουργιών, τη μείωση πολυπλοκότητας, καθώς και τη διασφάλιση ασφάλειας και αξιοπιστίας.

4.4.3.1 Ενσωματωμένες Υπηρεσίες (Built-in Services) του Google Apps Script

Η πλατφόρμα **Google Apps Script** παρέχει ενσωματωμένα modules, τα οποία αξιοποιήθηκαν εκτενώς στην υλοποίηση του πρόσθετου:

- **GmailApp** – Παρέχει πρόσβαση σε πρόχειρα (drafts), σώμα μηνύματος, παραλήπτες και μεταδεδομένα.
- **CardService** – Δημιουργεί δυναμικές κάρτες διεπαφής (UI) μέσα στο περιβάλλον του Gmail με κουμπιά, ενότητες και φόρμες.
- **PropertiesService** – Χρησιμοποιείται για την αποθήκευση μικρού όγκου δεδομένων, όπως επαφές, κατηγορίες, ρυθμίσεις και κλειδιά, σε JSON μορφή.
- **UrlFetchApp** – Επιτρέπει ασφαλή επικοινωνία με εξωτερικά APIs (όπως το Node.js backend).
- **Logger** – Παρέχει καταγραφή γεγονότων και debugging πληροφοριών για εσωτερική χρήση.

Οι υπηρεσίες αυτές επιτρέπουν τη δημιουργία ενός πλήρως λειτουργικού πρόσθετου χωρίς εξωτερικές εξαρτήσεις στην πλευρά του Gmail.

4.4.3.2 Ενεργοποιημένη Προηγμένη Υπηρεσία (Advanced Service) Gmail API v1

Για την πρόσβαση σε πιο εξειδικευμένες λειτουργίες, ενεργοποιήθηκε η **Gmail Advanced Service (v1)** στο περιβάλλον του Apps Script.
Η υπηρεσία αυτή επιτρέπει:

- Ανάγνωση και επεξεργασία μεταδεδομένων email (messageId, labels, threadId).
- Δημιουργία, αποστολή και τροποποίηση μηνυμάτων μέσω των endpoints του Gmail API.
- Ενσωμάτωση με λειτουργίες labels, spam filters και ρυθμίσεων χρηστών.

Η ενεργοποίησή της τεκμηριώνεται στο manifest (αρχείο ρυθμίσεων του Google Apps Script ονομάζεται appsscript.json) και συνοδεύεται από το αντίστοιχο OAuth scope (https://www.googleapis.com/auth/gmail.modify). Η ρύθμιση "**Identifier: Gmail – Version: v1**" επιτρέπει την απευθείας χρήση της ως Gmail.Users.Messages εντός του σεναρίου.

4.4.3.3 Βιβλιοθήκες Backend (Node.js)

Η υλοποίηση του Encryption API αναπτύχθηκε σε Node.js με χρήση του Express framework, παρέχοντας RESTful API endpoints που εξυπηρετούν τις λειτουργίες του προσθέτου. Το API καλείται από τον EncryptionController μέσω της μεθόδου UrlFetchApp, η οποία επιτρέπει την ασφαλή επικοινωνία του Google Apps Script με εξωτερικές διαδικτυακές υπηρεσίες.

Οι βασικές βιβλιοθήκες είναι:

- **express** – Υλοποίηση και δρομολόγηση των endpoints (/generate, /verify, /encrypt, /decrypt).
- **cors** – Ενεργοποιεί ελεγχόμενο Cross-Origin Resource Sharing ώστε να επιτρέπονται αιτήματα από το Apps Script.
- **openpgp** – Κεντρική βιβλιοθήκη για δημιουργία, υπογραφή και αποκρυπτογράφηση PGP/RSA κλειδιών και μηνυμάτων.
- **crypto** – Χρησιμοποιείται για βασικές λειτουργίες ασύμμετρης κρυπτογράφησης και hashing.
- **express.json / express.urlencoded** – Ενσωματωμένα middlewares για parsing JSON και URL-encoded δεδομένων.

Κάθε endpoint έχει σαφή ρόλο:

- **/generate** → Δημιουργεί ζεύγος PGP κλειδιών (public/private) και detached signature του public key.
- **/verify** → Επαληθεύει την εγκυρότητα υπογραφής του public key.
- **/encrypt** → Κρυπτογραφεί απλό κείμενο με παρεχόμενο δημόσιο κλειδί.
- **/decrypt** → Αποκρυπτογραφεί μήνυμα με ιδιωτικό κλειδί και passphrase.

Η χρήση του **openpgp** σε armored μορφή (ASCII-armored) εξασφαλίζει πλήρη συμβατότητα με OpenPGP πρότυπα και ευκολία διαμοιρασμού.

4.4.3.4 Εργαλεία Ανάπτυξης και Δοκιμών

Για την ανάπτυξη και συντήρηση χρησιμοποιήθηκαν τα ακόλουθα εργαλεία:

- **Google Apps Script IDE**: Ολοκληρωμένο περιβάλλον συγγραφής και debugging για το Gmail Add-on.
- **Render**: Φιλοξενία του Node.js server (Encryption API) με δημόσιο HTTPS endpoint για επικοινωνία με το Add-on.
- **GitHub:** Διαχείριση εκδόσεων και συνεργατική ανάπτυξη.
- **Google Drive:** Αποθήκευση λογότυπου, πολιτικών.

4.4.3.5 Πλεονεκτήματα Επαναχρησιμοποίησης και Ασφάλειας

Η επιλογή βιβλιοθηκών και εργαλείων έγινε με γνώμονα:

- **Αξιοπιστία και συντήρηση**: όλες οι βιβλιοθήκες είναι ενεργά υποστηριζόμενες και ανοιχτού κώδικα.
- **Επαναχρησιμοποίηση**: οι ίδιες συναρτήσεις χρησιμοποιούνται σε πολλαπλές ροές (π.χ. UrlFetchApp για όλες τις κλήσεις backend).
- **Ασφάλεια**: αξιοποίηση των OAuth scopes του Gmail, HTTPS επικοινωνίας και αποθήκευση ιδιωτικών κλειδιών μόνο στο PropertiesService.
- **Επεκτασιμότητα**: δυνατότητα προσθήκης νέων endpoints ή modules χωρίς αλλαγή στη βασική αρχιτεκτονική.

4.4.4 Δομή και Οργάνωση Κώδικα

Στην παρούσα ενότητα παρουσιάζεται η **οργάνωση του κώδικα** με τη βοήθεια ενός **διαγράμματος πακέτων (package diagram)**. Το διάγραμμα πακέτων αποτελεί στοιχείο της UML και χρησιμοποιείται για την απεικόνιση της λογικής ομαδοποίησης και των εξαρτήσεων μεταξύ διαφορετικών τμημάτων ενός έργου λογισμικού. Κάθε πακέτο λειτουργεί ως μηχανισμός συγκέντρωσης συναφών στοιχείων (όπως συναρτήσεις, κλάσεις ή modules) σε μία ενιαία ενότητα, ενώ παράλληλα προσφέρει έναν διακριτό χώρο ονομάτων, εξασφαλίζοντας τη μοναδικότητα των αναγνωριστικών. Με αυτόν τον τρόπο, το διάγραμμα πακέτων διευκολύνει την κατανόηση της δομής του συστήματος και απεικονίζει την πολυεπίπεδη αρχιτεκτονική του. Οι εξαρτήσεις μεταξύ πακέτων αποδίδονται με βέλη, τα οποία αναπαριστούν τον τρόπο επικοινωνίας και τη ροή δεδομένων μεταξύ των επιπέδων.

Η υλοποίηση του προσθέτου πραγματοποιήθηκε κυρίως με **Google Apps Script** (server-side JavaScript στο V8 runtime) για το Gmail Add-on και το UI (CardService). Οι λειτουργίες

κρυπτογράφησης και οι πιο σύνθετες εργασίες RSA/PGP υλοποιούνται σε ξεχωριστό **Node.js (Express)** backend (Encryption API), το οποίο παρέχει endpoints (π.χ. /generate, /decrypt) που καλούνται από το Add-on.

Ο κώδικας είναι οργανωμένος σε ανεξάρτητες συναρτήσεις, ακολουθώντας την **αρχή της ενιαίας ευθύνης (Single Responsibility)**:

- **Handlers/entry points** για Compose και Actions.
- **Builders** για το UI (κάθε κάρτα κατασκευάζεται από dedicated function).
- **Modules** για διαχείριση επαφών και κλειδιών (CRUD).
- **Ρουτίνες ανάλυσης/σάρωσης** που βασίζονται σε εκτεταμένα regex patterns για ευαίσθητα δεδομένα.
- **Λειτουργίες Gmail API** για διαχείριση drafts και φίλτρων.

Τα μόνιμα δεδομένα μικρού όγκου (επαφές, κατηγορίες, δημόσια/ιδιωτικά κλειδιά, ρυθμίσεις) αποθηκεύονται στο **PropertiesService** (ενσωματωμένη υπηρεσία της Google Apps Script για αποθήκευση δεδομένων σε μορφή key–value ανά χρήστη) με σειριοποίηση JSON, ενώ τα email και τα drafts παραμένουν στο ίδιο το Gmail.

Η **modular δομή** της υλοποίησης επιτρέπει εύκολη συντήρηση και επεκτασιμότητα, με δυνατότητα προσθήκης νέων κανόνων ανίχνευσης, ενσωμάτωσης επιπλέον keyservers ή βελτίωσης του αλγορίθμου scoring. Η Εικόνα 8 αποτυπώνει, μέσω UML διαγράμματος πακέτων, τη λογική ομαδοποίηση των κύριων ενοτήτων της υλοποίησης του eMailSec, τις μεταξύ τους σχέσεις και εξαρτήσεις, συνοψίζοντας την οργάνωση του κώδικα Το σύστημα οργανώνεται σε τέσσερα βασικά πακέτα:

- **Gmail add-on (eMailSec):** περιλαμβάνει το UI (CardService builders), τις **Compose/Read actions**, τα **SensitivePatterns (Regex)** και το **Storage (PropertiesService)**.

- **Google Apps Script Services:** παρέχει τα APIs **GmailApp/DriveApp**, **CardService**, **PropertiesService** και **UrlFetchApp** που χρησιμοποιεί το Add-on.

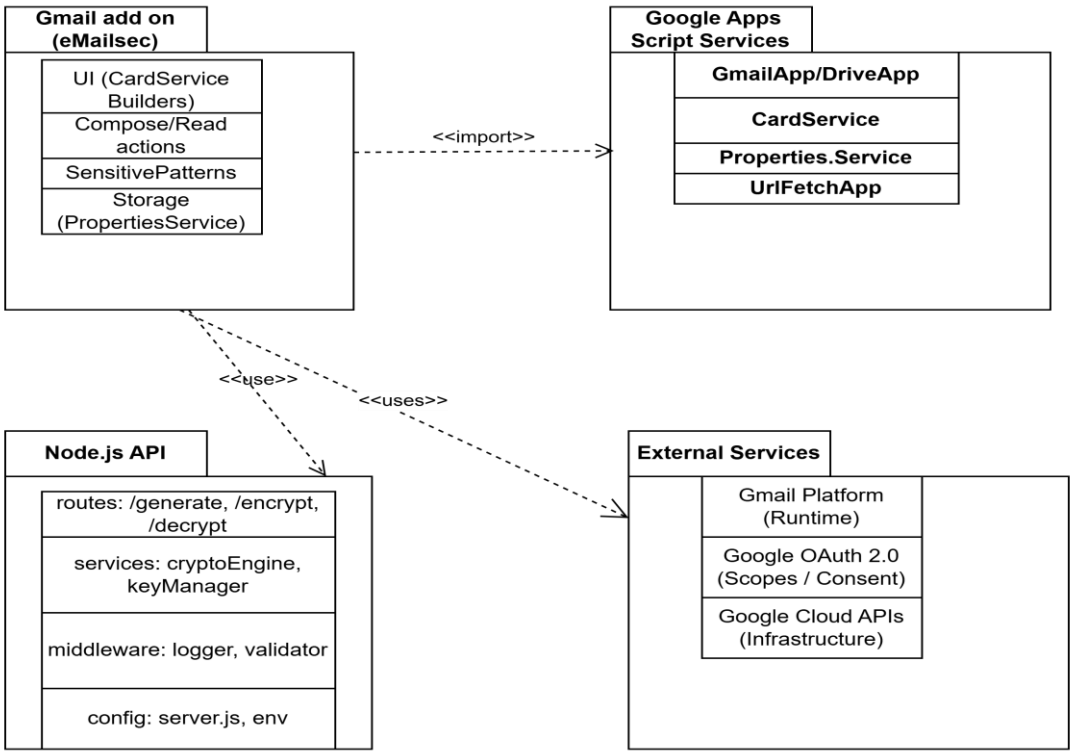
- **Node.js API:** υλοποιεί το backend κρυπτογράφησης/αποκρυπτογράφησης με routes (/generate, /encrypt, /decrypt), services (cryptoEngine, keyManager), middleware (logger, validator) και config (server.js, env).

- **External Services:** αναπαριστά την υποδομή της Google (**Gmail Platform – Runtime**, **Google OAuth 2.0 – Scopes/Consent**, **Google Cloud APIs**).

Οι εξαρτήσεις αποδίδονται με UML stereotypes:

- Το **Gmail Add-on** έχει σχέση **«imports»** με το **Google Apps Script Services** (εισαγωγή και πλήρη χρήση των APIs) και **«uses»** με το **Node.js API** (κλήση backend για κρυπτογράφηση/αποκρυπτογράφηση).
- Το **Gmail Add-on** έχει επίσης σχέση **«uses»** προς τα **External Services**, καθώς εξαρτάται από το Gmail runtime και τη διαδικασία OAuth για την εκτέλεσή του.

Η πολυεπίπεδη αυτή οργάνωση ακολουθεί αρχές καθαρού διαχωρισμού ευθυνών (Separation of Concerns) και χαμηλής σύζευξης (Low Coupling), επιτρέποντας μελλοντική συντήρηση, επέκταση και ευκολία debugging.



Εικόνα 8. Διάγραμμα πακέτων του συστήματος.

4.4.5 Υλοποίηση UI και Βασική Δομή

Η διεπαφή χρήστη του eMailSec αναπτύχθηκε εξ ολοκλήρου με τη χρήση του Google Apps Script CardService, το οποίο παρέχει εγγενείς μεθόδους για τη δημιουργία προσαρμοσμένων καρτών διεπαφής (cards) μέσα στο περιβάλλον του Gmail. Η προσέγγιση αυτή επιλέχθηκε λόγω της πλήρους ενσωμάτωσης στο οικοσύστημα των Google Add-ons, της απλότητας στη συντήρηση και της ασφάλειας που προσφέρει, καθώς όλες οι ενέργειες εκτελούνται μέσω εξουσιοδοτημένων APIs.

Η βασική δομή του UI ακολουθεί τη λογική του card-based design, όπου κάθε κάρτα αντιστοιχεί σε μία λειτουργική ενότητα της εφαρμογής (π.χ. ανάλυση προσχεδίου, διαχείριση επαφών, διαχείριση κλειδιών, επίλυση προβλημάτων). Κάθε κάρτα περιλαμβάνει sections και widgets (όπως text blocks, κουμπιά ενεργειών, πεδία εισαγωγής και εικονίδια), τα οποία δημιουργούνται δυναμικά μέσω του CardService.newCardBuilder().

Η πλοήγηση μεταξύ των καρτών υλοποιείται μέσω του CardService.Navigation, επιτρέποντας την εναλλαγή περιεχομένου χωρίς ανανέωση σελίδας. Οι ενέργειες των χρηστών (π.χ. “Scan”, “Encrypt”, “Manage Contacts”) ενεργοποιούν συναρτήσεις Apps Script με onClickAction, οι οποίες διαχειρίζονται τη ροή δεδομένων και ενημερώνουν το UI με νέα δυναμικά στοιχεία.

Η επικοινωνία με το κρυπτογραφικό μέρος του backend πραγματοποιείται μέσω της υπηρεσίας UrlFetchApp, η οποία αποστέλλει HTTPS αιτήματα προς το Node.js API. Τα αποτελέσματα (π.χ. κρυπτογραφημένο μήνυμα, επαλήθευση υπογραφής, νέα κλειδιά) επιστρέφονται σε μορφή JSON και προβάλλονται στο UI με κατάλληλα στοιχεία ενημέρωσης (π.χ. labels ή dialogs).

Η αποθήκευση κατάστασης και ρυθμίσεων γίνεται με χρήση του PropertiesService.getUserProperties(), όπου αποθηκεύονται επαφές, κατηγορίες, δημόσια/ιδιωτικά κλειδιά και υπογραφές. Έτσι, κάθε χρήστης διατηρεί το δικό του ασφαλές περιβάλλον χωρίς εξωτερική βάση δεδομένων.

Συνολικά, το UI του eMailSec είναι αρθρωτό, δυναμικό και ασφαλές, με δομή που υποστηρίζει εύκολη επεκτασιμότητα. Ο σχεδιασμός του εστιάζει στη λειτουργικότητα, στη σαφή παρουσίαση των ευρημάτων και στη δυνατότητα άμεσης αλληλεπίδρασης με τις λειτουργίες ασφάλειας του πρόσθετου.

4.4.6 Ανίχνευση Ευαίσθητων Δεδομένων σε Επίπεδο Κώδικα

Για την ανίχνευση ευαίσθητων δεδομένων, ο κώδικας εκτελεί έλεγχο στο περιεχόμενο του τρέχοντος προσχεδίου (draft) του Gmail. Αρχικά ανακτάται το κείμενο του email (subject και body) και εφαρμόζονται κανονικές εκφράσεις (regex) για κάθε τύπο πληροφορίας, όπως διευθύνσεις email, αριθμοί τηλεφώνου, ΑΦΜ, ΑΜΚΑ και IBAN.

Όταν εντοπιστεί πιθανό ταίριασμα, καλούνται βοηθητικές συναρτήσεις (helper functions) που παίζουν τον ρόλο validators, επαληθεύοντας τη μορφή του δεδομένου και φιλτράροντας τυχόν λανθασμένα αποτελέσματα. Για παράδειγμα:

- **Αν εντοπιστεί IBAN**, γίνεται έλεγχος μήκους και προθέματος χώρας (*π.χ. GR*) καθώς και έλεγχος εγκυρότητας ψηφίων.

Παράδειγμα: Ελληνικό IBAN

/\bGR\d{2}\s?[\dA-Z]{4}\s?[\dA-Z]{4}\s?[\dA-Z]{4}\s?[\dA-Z]{4}\s?[\dA-Z]{4}\s?[\dA-Z]{3}\b/i

Αναζητά συμβολοσειρές που:

- ξεκινούν με το πρόθεμα **GR(**Δύο αλφαβητικοί χαρακτήρες που δηλώνουν τον κωδικό χώρας (Ελλάδα)**)**,
- ακολουθούνται από **δύο ψηφία** ,
- και στη συνέχεια περιλαμβάνουν **23 αλφαριθμητικούς χαρακτήρες**, επιτρέποντας **προαιρετικά κενά** ανά τετράδα για τη συνήθη μορφοποίηση του IBAN.

Με αυτόν τον τρόπο, το regex εντοπίζει σωστά παραδείγματα όπως:
GR16 0110 1250 0000 0001 2300 695 ή GR1601 10125000000012300695,

- **Για ΑΜΚΑ**, γίνεται έλεγχος ημερομηνίας γέννησης στα πρώτα 6 ψηφία, ώστε να διαπιστωθεί ότι αντιστοιχούν σε λογική και έγκυρη ημερομηνία (π.χ. απορρίπτονται περιπτώσεις όπως *11/00/2034* ή *32/15/1999*).

Παράδειγμα ΑΜΚΑ:

*/(?:A[\s.]*M[\s.]*K[\s.]*A[\s.]*|AMKA)[\s\u00A0]*[:=\-—]?\s*((?:\d[\s\-]*){11})(?!\d)/iu*

Χρησιμοποιείται για την **ανίχνευση αριθμών ΑΜΚΑ**. Αναγνωρίζει τόσο τη μορφή **«ΑΜΚΑ»**, επιτρέποντας **ενδιάμεσα κενά, τελείες ή σύμβολα** ανάμεσα στα γράμματα (π.χ. *Α.Μ.Κ.Α.*, *Α Μ Κ Α*). Ακολουθεί προαιρετικά **διάστημα ή σημεία στίξης** (όπως :, -, =), και στη συνέχεια **έντεκα ψηφία**, που αποτελούν τον αριθμό ΑΜΚΑ.

Η έκφραση αυτή καλύπτει τις πιο συνηθισμένες μορφές γραφής, όπως: ΑΜΚΑ: 01019912345, Α.Μ.Κ.Α 01019912345 ή ΑΜΚΑ-01019912345, εξασφαλίζοντας **ακριβή αναγνώριση** του αριθμού ανεξάρτητα από τη μορφοποίηση.

```
/**  Απλή λογική — 11 ψηφία + έγκυρη ημερομηνία DDMMYY */
function isPlausibleAMKA(val) {
  const n = String(val).replace(/\D/g, '');       // Αφαίρεση μη αριθμητικών χαρακτήρων
  if (n.length !== 11) return false;               // Ο ΑΜΚΑ πρέπει να έχει 11 ψηφία
  const dd = Number(n.slice(0, 2));              // Ημέρα
  const mm = Number(n.slice(2, 4));              // Μήνας
  const yy = Number(n.slice(4, 6));              // Έτος
  // Αποδεκτό εύρος ημερομηνίας: 1900–2099
 const year = yy >= 30 ? 1900 + yy : 2000 + yy;   // Χρήση pivot=30
  const date = new Date(year, mm - 1, dd);
  const validDate = date.getFullYear() === year &&  date.getMonth() === mm - 1 && date.getDate() === dd;
  return validDate;        // Επιστρέφει true μόνο αν η ημερομηνία είναι έγκυρη
}
```

- **Για αριθμούς τηλεφώνου**, ελέγχεται αν αντιστοιχούν σε έγκυρη μορφή κινητού και άρα δεν ανήκουν σε ακολουθίες τυχαίων ψηφίων.

Παράδειγμα κινητού :

```
/\b69\d{8}\b/, /\b2\d{2}[ ]?\d{6}\b/,/\+30\s?2\d{2}\s?\d{6}\b/,
```

Οι έλεγχοι αυτοί επιτρέπουν στο σύστημα να ξεχωρίζει έγκυρα από ψευδή ευρήματα και να επιστρέφει πιο ακριβή αποτελέσματα, αποφεύγοντας περιπτώσεις όπου η απλή χρήση regex θα παρήγαγε ψευδώς θετικά.

Αφού ολοκληρωθεί η διαδικασία ανίχνευσης και επαλήθευσης των ευαίσθητων δεδομένων, ο κώδικας υπολογίζει το **risk score** με βάση το πλήθος και το είδος των ευρημάτων που εντοπίστηκαν (στο subject και στο body), καθώς και τα χαρακτηριστικά των παραληπτών (αν είναι άγνωστοι ή αποκλεισμένοι). Κάθε παράγοντας διαθέτει ένα **προκαθορισμένο βάρος**, το οποίο προστίθεται στη συνολική βαθμολογία έτσι, όσο περισσότερα ευαίσθητα δεδομένα ή επικίνδυνοι παραλήπτες εντοπίζονται, τόσο υψηλότερο είναι το τελικό ρίσκο. Με αυτό τον τρόπο, το σύστημα μετατρέπει τα αποτελέσματα της ανίχνευσης σε μια **μετρήσιμη εκτίμηση κινδύνου**, που βοηθά τον χρήστη να αξιολογήσει τη σοβαρότητα του μηνύματος πριν την αποστολή.

Σε μαθηματικό επίπεδο, ο υπολογισμός του **risk score** βασίζεται σε ένα σύνολο **μεταβλητών–βαρών** που εκφράζουν τη συμβολή κάθε παράγοντα κινδύνου στη συνολική βαθμολογία. Κάθε κατηγορία (subject, body, άγνωστοι παραλήπτες, αποκλεισμένοι παραλήπτες) έχει τη δική της **βασική τιμή (base weight)** και **πρόσθετο βάρος ανά εύρημα ή παραλήπτη (per-hit weight)**. Ο συνολικός κίνδυνος προκύπτει από το **άθροισμα** όλων αυτών των επιμέρους τιμών:

RiskScore = SubjectPart + BodyPart + UnknownRecipientsPart + BonusPart

και κάθε μέρος υπολογίζεται ως εξής:

1. **Μέρος θέματος (SubjectPart)**
   Ενεργοποιείται μόνο αν βρεθεί ευαίσθητο δεδομένο στο subject.

   - Βασική τιμή: **SUBJECT_BASE = 40**
   - Πρόσθετο ανά εύρημα: **SUBJECT_PER_HIT = 6**
   - Ανώτατο πρόσθετο από hits subject: **30**

   - Άρα: **SubjectPart = 40 + min(αριθμός_subject_hits × 6, 30)**

2. **Μέρος σώματος (BodyPart)**
   Ενεργοποιείται μόνο αν βρεθεί ευαίσθητο δεδομένο στο body.

   - Βασική τιμή: **BODY_BASE = 30**
   - Πρόσθετο ανά εύρημα: **BODY_PER_HIT = 4**
   - Ανώτατο πρόσθετο από hits body: **30**

   - Άρα: **BodyPart = 30 + min(αριθμός_body_hits × 4, 30)**

3. **Μέρος άγνωστων παραληπτών (UnknownRecipientsPart)**
   Ενεργοποιείται μόνο αν υπάρχει έστω ένας παραλήπτης που δεν είναι στις αποθηκευμένες/έμπιστες επαφές.

   - Βασική τιμή: **UNKNOWN_BASE = 15**
   - Πρόσθετο ανά άγνωστο: **UNKNOWN_PER_EMAIL = 5**
   - Ανώτατο από άγνωστους: **UNKNOWN_CAP = 30**

   - Άρα: **UnknownRecipientsPart = min(15 + αριθμός_άγνωστων × 5, 30)**

4. **BonusPart**
    - Αν υπάρχουν ευρήματα **και** στο subject **και** στο body:
        - **BonusPart = BOTH_BONUS = 8**
    - Αλλιώς:
        - **BonusPart = 0**

Άρα αν τα βάλουμε όλα μαζί:

RiskScore = [40 + min(S_hits × 6, όριο 30)] + [30 + min(B_hits × 4, όριο 30)] + [min(15 + U × 5, όριο 30)] + (8 ή 0)

όπου:

- **S_hits** = πόσα ευρήματα βρέθηκαν στο subject
- **B_hits** = πόσα ευρήματα βρέθηκαν στο body
- **U** = πόσοι άγνωστοι παραλήπτες βρέθηκαν

Ειδική περίπτωση (blocked):
αν μέσα στους παραλήπτες υπάρχει διεύθυνση που είναι στη λίστα αποκλεισμένων, τότε μετά τον παραπάνω υπολογισμό το σύστημα ορίζει:

- **RiskScore = max(RiskScore, 85)**
  δηλαδή το σκορ ανεβαίνει τουλάχιστον στο 85 για να θεωρηθεί "υψηλό".

Το αποτέλεσμα **κανονικοποιείται στο εύρος 0–100**. Όσο περισσότερα ευρήματα ή ύποπτοι παραλήπτες εντοπίζονται, τόσο αυξάνεται αθροιστικά το τελικό **Risk Score**, αποτυπώνοντας ποσοτικά τον βαθμό επικινδυνότητας του email.

Για δοκιμαστικούς σκοπούς στο Κεφάλαιο 6 (Ενότητα 6.3), εκτελέστηκαν οι συναρτήσεις του συστήματος που καλούν τους μηχανισμούς ανίχνευσης ευαίσθητων δεδομένων, εφαρμόζοντας τα αντίστοιχα **regex** και τους **validators**. Στόχος ήταν να επαληθευτεί ότι ο κώδικας εντοπίζει σωστά τα δεδομένα σε πραγματικά δείγματα κειμένου και ότι οι βοηθητικοί έλεγχοι (όπως το checksum ή ο έλεγχος ημερομηνίας) λειτουργούν ορθά, αποτρέποντας την εμφάνιση ψευδώς θετικών αποτελεσμάτων.

4.5 Ικανοποίηση Απαιτήσεων

Σε αυτήν την ενότητα εξετάζεται σε ποιον βαθμό η υλοποιημένη εφαρμογή ικανοποιεί τις λειτουργικές και μη λειτουργικές απαιτήσεις που ορίστηκαν στην Ενότητα 4.2. Η αξιολόγηση παρουσιάζεται μέσα από πίνακα ιχνηλασιμότητας (Requirements Traceability Matrix – RTM), όπου κάθε απαίτηση αντιστοιχίζεται με την υλοποίηση και βαθμολογείται με ποσοστό κάλυψης (0–100%). Επιπλέον, καταγράφονται οι πρόσθετες λειτουργίες που ενσωματώθηκαν, παρότι δεν είχαν προβλεφθεί ρητά στο στάδιο της ανάλυσης.

4.5.1 Λειτουργικές Απαιτήσεις

Πίνακας 23. Λειτουργικές Απαιτήσεις.

ID	**Απαίτηση**	**Υλοποίηση / Κάλυψη**	**Ποσοστό κάλυψης**	**Σχόλια / Αιτιολόγηση**
FR1	Ανίχνευση ευαίσθητων πληροφοριών (subject/body)	Regex patterns, auto-scan σε Compose, Resolve Issues	100%	Πλήρης κάλυψη με pattern-based scanning.
FR2	Αναγνώριση τύπων βάσει προτιμήσεων χρήστη	-	0%	Δεν υπάρχουν user-defined preferences για τύπους δεδομένων.
FR3	Ταξινόμηση συνημμένων κατά ιδιωτικότητα	-	0%	Δεν υλοποιείται κατάταξη attachments· μόνο ένδειξη προβλήματος στο draft.
FR4	Αξιολόγηση παραληπτών (εμπιστοσύνη + δυνατότητα crypto)	Resolve Issues, cross-check με contacts/keys	100%	Αν λείπει safe contact ή key → προβάλλεται πρόβλημα.
FR5	Αντιστοίχιση σε θέματα (topics)	Μερική ένδειξη/σήμανση προβλήματος	40%	Δεν γίνεται θεματική ταξινόμηση· μόνο alerts για περιεχόμενο.
FR6	Διαχείριση κανόνων (create/edit/delete contacts)	Προκαθορισμένοι κανόνες	0%	Δεν επιτρέπει τη δημιουργία/διαχείριση custom κανόνων από τον χρήστη.
FR7	Ορισμός ενεργού προφίλ	Υλοποιημένο	100%	Active profile flag στο PropertiesService.

FR8	Σύνθετες συνθήκες (AND/OR/NOT)	–	0%	Δεν υποστηρίζεται σύνθεση κανόνων με λογικούς τελεστές.
FR9	Κρυπτογράφηση περιεχομένου/συνημμένων	Node.js API (CryptoPort), Encrypt UI	100%	OpenPGP-style ροές κρυπτογράφησης.
FR10	Διαφορετικά επίπεδα κρυπτογράφησης	Επιλογή κλειδιού (όχι επίπεδα)	50%	Δεν υπάρχουν granular “levels”, μόνο επιλογή κλειδιού.
FR11	Ειδοποιήσεις χρήστη (alerts/warnings)	Alert/Resolve Issues cards	100%	Δυναμικά μηνύματα ανά εύρημα.
FR12	Μπλοκάρισμα αποστολής	Ενημέρωση μόνο	30%	Δεν γίνεται hard block· παρέχεται warning/προτροπή.
FR13	Αφαίρεση συνημμένου	-	0%	Δεν υποστηρίζεται remove attachment από το add-on.
FR14	Διαγραφή μηνύματος	-	0%	Δεν υπάρχει δυνατότητα delete draft από το add-on.
FR15	Χειρωνακτική αντιμετώπιση (override)	Υλοποιημένο	100%	Επιλογές “Take actions” / “Encrypt” / “Delete recipients”.
FR16	Διαχείριση ασφαλών επαφών (safe contacts)	Contacts UI, κατηγορίες, αποθήκευση σε PropertiesService	100%	Προβολή/προσθήκη/ενημέρωση/διαγραφή, ομαδοποίηση ανά category.
FR17	Συσχέτιση/διαχείριση κλειδιών ανά επαφή	Keys UI + αποθήκευση public/private, αποστολή public key & .sig	100%	Public/Private keys και detached signatures ανά επαφή/χρήστη.
FR18	Validate παραλήπτη ως προς ύπαρξη κλειδιού(Σε περίπτωση που ο χρήστης θέλει να	Resolve Issues: ελέγχει αν υπάρχει public key	100%	Αν δεν υπάρχει key → πρόβλημα & οδηγός ενεργειών (request/provide)

	στείλει κρυπτογραφημένο μήνυμα ή που θέλει να το κρυπτογραφίσει επειδή βρέθηκε ευαίσθητο περιεχόμενο)			
FR19	Επικύρωση/επαλήθευση κλειδιού & υπογραφής	Verify Public Key Signature flow	100%	Επαλήθευση γνησιότητας public key (detached signature verify).
FR20	Αποθήκευση κλειδιού επαφής μετά από επιτυχή επικύρωση (validate & store)	Μετά το verify, το public key αποθηκεύεται στο PropertiesService για την αντίστοιχη επαφή	100%	Πλήρης κύκλος: validate → αποθήκευση στο contact → διαθέσιμο για future encryption.

4.5.2 Μη Λειτουργικές Απαιτήσεις

Πίνακας 24. Μη Λειτουργικές Απαιτήσεις.

ID	**Απαίτηση**	**Υλοποίηση / Κάλυψη**	**Ποσοστό κάλυψης**	**Σχόλια / Αιτιολόγηση**
NFR1	Ασφάλεια (ασφαλείς μέθοδοι crypto, αποθήκευση, πρότυπα).	PGP-style crypto μέσω Node.js API, private keys σε PropertiesService, HTTPS επικοινωνία.	90%	Τα ιδιωτικά κλειδιά δεν διαμοιράζονται, πλήρης συμμόρφωση με ασφάλεια.Για επαγγελματική ανάπτυξη θα πρέπει να χρησιμοποιηθεί μια πιο ασφαλής λύση (Google Cloud Secret Manager αντι για PropertiesService).
NFR2	Απόδοση (lightweight, χωρίς καθυστερήσεις).	Apps Script functions, optimized regex, async API calls.	85%	Σε μεγάλα μηνύματα/attachments ενδέχεται ύπαρξη μικρής καθυστέρησης. (Ενότητα 6.4

				Ταχύτητα απόκρισης)
NFR3	Ευχρηστία (φιλικό UI, σαφείς ειδοποιήσεις).	CardService UI, structured alerts, user-friendly μηνύματα.	100%	Το UI είναι consistent με Gmail add-on guidelines.
NFR4	Επεκτασιμότητα (νέες δυνατότητες/AI).	Layered + Ports & Adapters αρχιτεκτονική, modular functions.	90%	Υποστηρίζει νέα features εύκολα· AI δεν έχει ενσωματωθεί ακόμα.
NFR5	Προσαρμοστικότητα (ρυθμιζόμενοι κανόνες).	Profiles & policies editable.	0%	Ο χρήστης δεν μπορεί να φτιάξει πλήρως custom κανόνες.
NFR6	**Φορητότητα** (λειτουργία σε όλες τις συσκευές).	Cloud-based Gmail Add-on, συμβατό με desktop, mobile, OS-agnostic.	100%	Δεν απαιτείται εγκατάσταση, λειτουργεί σε όλα τα Gmail clients.

5

Εγκατάσταση & Επίδειξη

5.1 Εγκατάσταση από πλευράς χρήστη (Gmail Add-on)

Η ενότητα αυτή περιγράφει πώς ένας τελικός χρήστης εγκαθιστά και ενεργοποιεί ένα πρόσθετο (add-on) στο Gmail. Οι οδηγίες ισχύουν για εγκατάσταση από το Google Workspace Marketplace (δημόσια διάθεση) και για ιδιωτική εγκατάσταση μέσω συνδέσμου (private/test).

5.1.1 Προϋποθέσεις

- Ενεργός λογαριασμός Google (Gmail ή Google Workspace).
- Πρόσβαση στο Gmail από σύγχρονο φυλλομετρητή (Chrome, Firefox, Edge, Safari).
- Σε εταιρικούς/σχολικούς λογαριασμούς: ενδέχεται να απαιτείται έγκριση από τον διαχειριστή (admin policy).

5.1.2 Εγκατάσταση μέσω Google Workspace Marketplace (δημόσιο listing)

1. **Άνοιγμα Marketplace**

    - Από το Gmail (δεξί sidebar) επιλέγουμε **Get add-ons / Λήψη προσθέτων**, ή
    - Μετάβαση στο Google Workspace Marketplace και αναζήτηση του προσθέτου με το όνομά του (eMailSec).

2. **Εμφάνιση & Έλεγχος Σελίδας Προσθέτου**
    - Έλεγχος περιγραφής, εκδότη, δικαιωμάτων (permissions) και αξιολογήσεων.
3. **Εγκατάσταση**
    - Επιλογή **Install / Εγκατάσταση → Continue / Συνέχεια** → επιλογή λογαριασμού.
    - Αποδοχή των ζητούμενων δικαιωμάτων.
4. **Ολοκλήρωση**
    - Επιστροφή στο Gmail και **ανανέωση** της σελίδας. Το εικονίδιο του προσθέτου εμφανίζεται στο **δεξί sidebar**.
    - Σε κινητά (Android/iOS), τα add-ons εμφανίζονται κατά την προβολή ενός email, στο κάτω μέρος της οθόνης.

Η παραπάνω διαδικασία περιγράφει τη γενική μέθοδο εγκατάστασης που ακολουθείται για όλα τα πρόσθετα (add-ons) του Gmail μέσω του Google Workspace Marketplace. Στο πλαίσιο της παρούσας εργασίας, η διαδικασία αυτή θεωρείται πως είναι ακόμη θεωρητική διότι ισχύει σε περίπτωση δημοσίευσης του προσθέτου στο Marketplace. Όμως, επί του παρόντος, το πρόσθετο eMailSec δεν έχει δημοσιευθεί δημόσια, αλλά εγκαθίσταται ιδιωτικά (δείτε επόμενη ενότητα 5.1.3) μέσω συνδέσμου ή με απευθείας εκτέλεση από το περιβάλλον του Google Apps Script (developer mode).

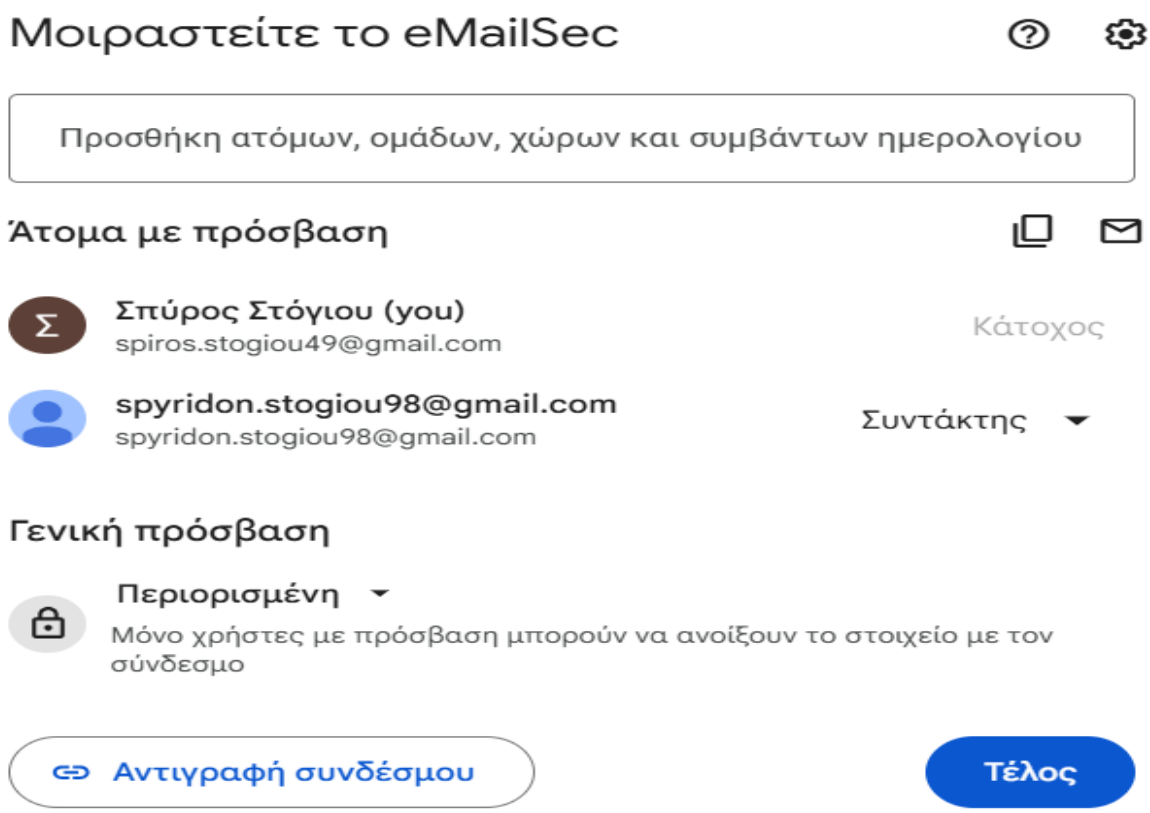
Ο κώδικας του Encryption API αποθηκεύεται online στο GitLab, το οποίο λειτουργεί ως αποθετήριο του έργου. Το Render, από την άλλη, αποτελεί το περιβάλλον εκτέλεσης (runtime environment) του API: ανακτά αυτόματα τον κώδικα από το GitLab και τον εκτελεί σε cloud server. Με αυτό τον τρόπο, το Node.js backend παραμένει συνεχώς ενεργό και προσβάσιμο μέσω δημόσιων HTTPS endpoints, τα οποία χρησιμοποιεί το Gmail Add-on για να πραγματοποιεί τις απαιτούμενες κλήσεις (όπως δημιουργία, κρυπτογράφηση ή αποκρυπτογράφηση κλειδιών). Συνεπώς, ο τελικός χρήστης δεν χρειάζεται να εγκαταστήσει ή να εκτελέσει το API τοπικά, καθώς αρκεί η εγκατάσταση του προσθέτου στο Gmail.

5.1.3 Ιδιωτική εγκατάσταση μέσω κοινοποίησης έργου (private/test)

Σε περιπτώσεις πιλοτικής χρήσης, όπως στο πλαίσιο ακαδημαϊκής εργασίας, η εγκατάσταση του προσθέτου πραγματοποιείται σε **δοκιμαστική λειτουργία (testing mode)**. Η πρόσβαση επιτρέπεται μόνο στους χρήστες που έχουν δηλωθεί ως **δοκιμαστές (test users)** από τον δημιουργό.

Η διαδικασία έχει ως εξής:

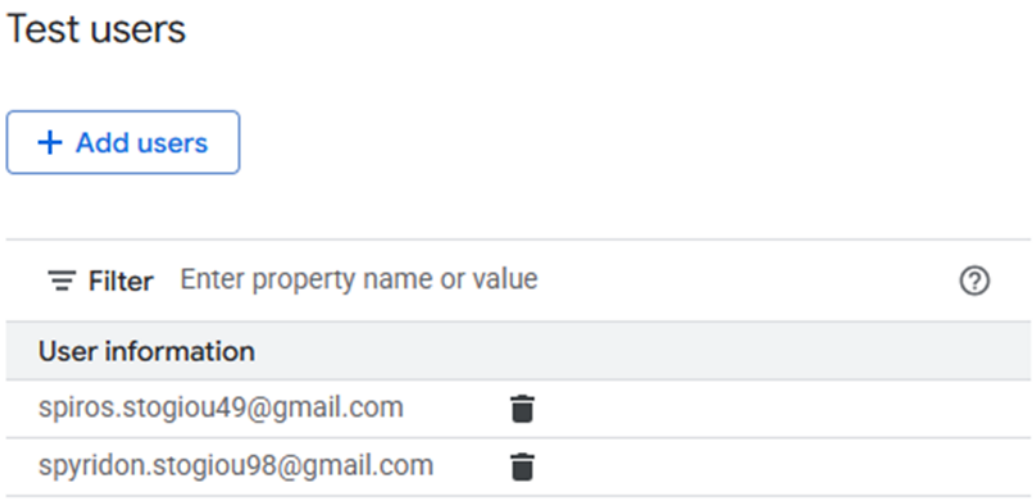
- Ο δημιουργός μεταβαίνει στο έργο του στο script.google.com, επιλέγει **Κοινοποίηση (Share)** και προσθέτει τις διευθύνσεις Gmail των δοκιμαστών με δικαιώματα **Επεξεργαστή (Editor)**.



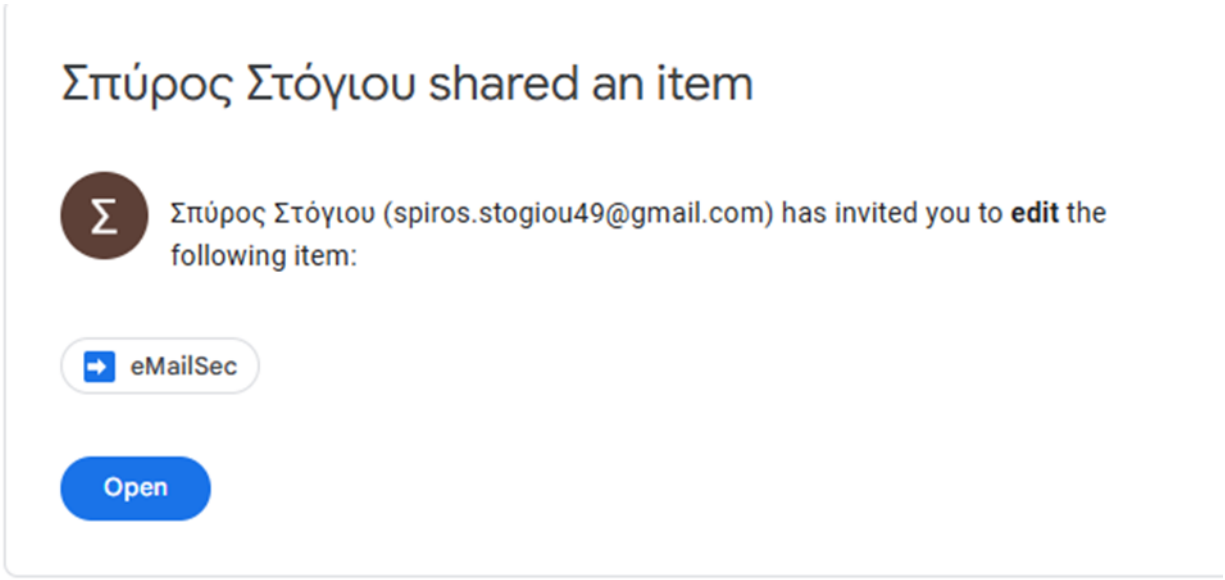
Εικόνα 9. Κοινοποίηση (Share) του eMailSec.

- Παράλληλα, οι ίδιες διευθύνσεις προστίθενται και στη λίστα **Test users** του *Google Cloud Console* (**Google Cloud Console → OAuth consent screen → Audience → Test users**) (βλ. Εικόνα 10).
- Οι δοκιμαστές ανοίγουν την πρόσκληση κοινοποίησης (βλ. Εικόνα 11), εισέρχονται στο έργο Apps Script και επιλέγουν **Deploy → Test deployments → Εγκατάσταση (Install)**.
- Μετά την αποδοχή των ζητούμενων δικαιωμάτων (consent screen), ανανεώνουν το Gmail και το εικονίδιο του προσθέτου εμφανίζεται στο δεξί sidebar.

*Σημείωση: Μετά το πέρας της δοκιμής συνιστάται η **αφαίρεση των δικαιωμάτων Editor** για λόγους ασφάλειας. Σε εταιρικούς ή σχολικούς λογαριασμούς μπορεί να απαιτηθεί έγκριση από τον διαχειριστή (admin policy).*



Εικόνα 10. Προσθήκη δοκιμαστών (Test users) .



Εικόνα 11. Πρόσκληση κοινοποίησης του έργου eMailSec.

Τι θα δει ο χρήστης στα δικαιώματα (ενδεικτικά)

- «Εκτέλεση του προσθέτου στο Gmail σας».
- «Προβολή του περιβάλλοντος μηνύματος/σύνταξης ώστε να παρέχει λειτουργίες».
- «Ανάγνωση βασικών πληροφοριών λογαριασμού (διεύθυνση email)».

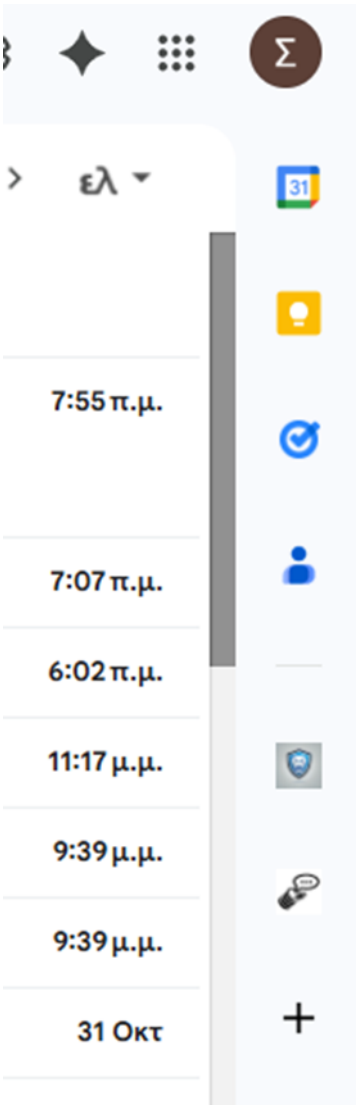
*Τα δικαιώματα πρέπει να είναι **τα ελάχιστα δυνατά** (least privilege). Αν δεν υπάρχει εμπιστοσύνη στο πρόσθετο/εκδότη, ο χρήστης δεν προχωρά.*

5.1.4 Πρώτη χρήση και έλεγχος ορθής εγκατάστασης

Μετά την ολοκλήρωση της εγκατάστασης και την αποδοχή των απαιτούμενων δικαιωμάτων, ο χρήστης μπορεί να ενεργοποιήσει και να ελέγξει τη σωστή λειτουργία του προσθέτου ως εξής:

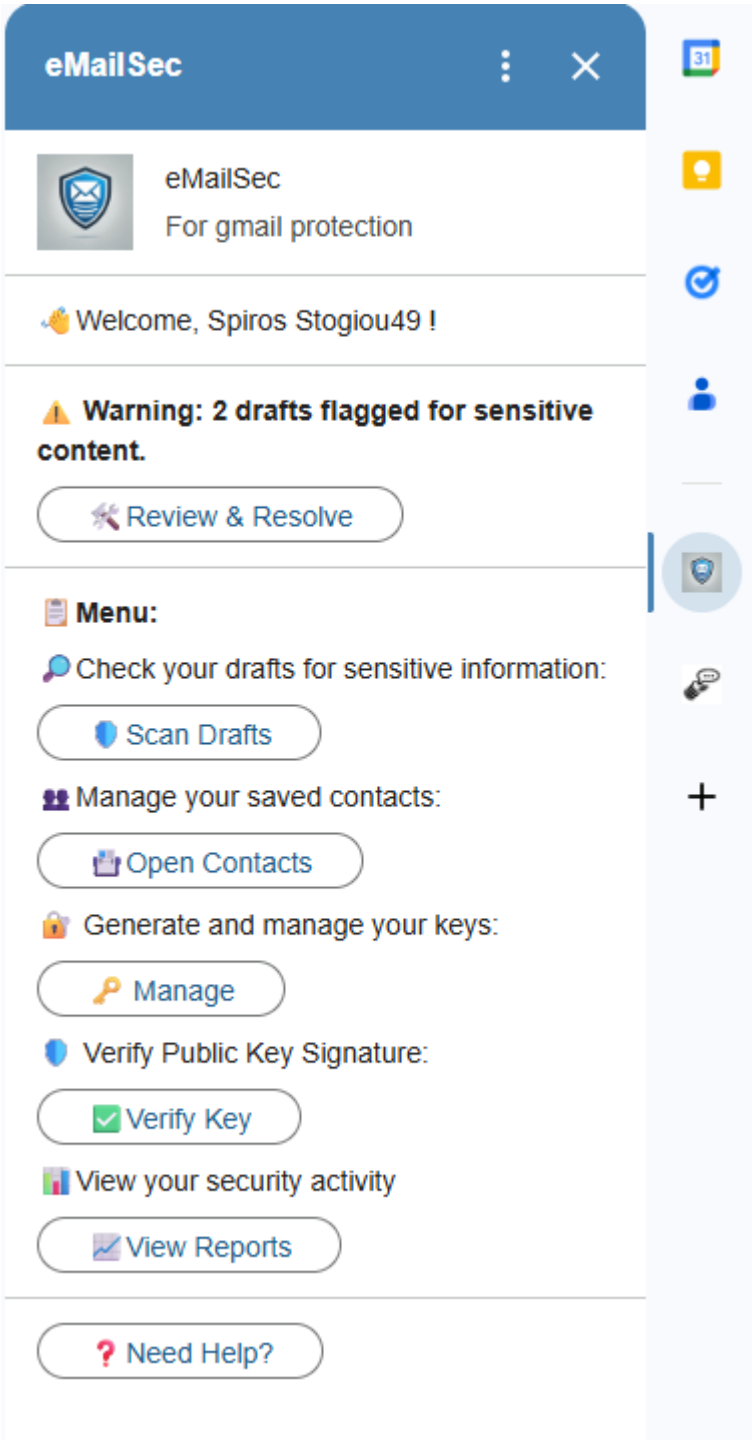
Άνοιγμα του προσθέτου:

- Το εικονίδιο του *eMailSec* εμφανίζεται στο δεξί sidebar του Gmail, μαζί με τα υπόλοιπα add-ons (βλ. Εικόνα 12).



Εικόνα 12. Sidebar του Gmail.

- Με κλικ στο εικονίδιο, φορτώνεται η αρχική κάρτα του προσθέτου μέσω *Google Apps Script CardService* (βλ. Εικόνα 13).



Εικόνα 13. Κεντρικό μενού.

Χρήση στο περιβάλλον "Σύνταξη" (Compose):

- Κατά τη δημιουργία νέου email, το πρόσθετο ενεργοποιεί τις ενέργειες *compose-actions*, επιτρέποντας λειτουργίες, όπως έλεγχο παραληπτών, ανίχνευση ευαίσθητων δεδομένων και κρυπτογράφηση (βλ. Εικόνα 15).

Χρήση σε ανοιχτό μήνυμα:

- Κατά την προβολή ενός email, το πρόσθετο μπορεί να προσφέρει contextual ενέργειες (βλ. Εικόνα 31).

Έλεγχος ορθής εγκατάστασης:

- Το πρόσθετο ανοίγει χωρίς σφάλματα και φορτώνει την αρχική του οθόνη.
- Οι βασικές λειτουργίες είναι διαθέσιμες και εκτελούνται κανονικά (π.χ. σάρωση drafts, ενέργειες κουμπιών, φόρτωση UI).
- Εφόσον όλα λειτουργούν όπως αναμένεται, η εγκατάσταση θεωρείται επιτυχής.

Σημείωση: Αν το πρόσθετο δεν εμφανιστεί στο sidebar, ο χρήστης μπορεί να ανανεώσει τη σελίδα του Gmail ή να ελέγξει τις ρυθμίσεις Manage add-ons.

5.1.5 Συχνά ζητήματα & επίλυση

- **Δεν βλέπω το πρόσθετο**: Κάντε **Refresh** στο Gmail· ελέγξτε ότι ολοκληρώθηκε η εγκατάσταση.
- **Μήνυμα «Authorization required»**: Ακολουθήστε την εξουσιοδότηση μέχρι τέλους και αποδεχτείτε τα permissions.
- **Εταιρικός λογαριασμός — μπλοκάρεται η εγκατάσταση**: Απαιτείται έγκριση από **διαχειριστή** (Google Admin Console).
- **Σε κινητό δεν εμφανίζεται**: Ενημερώστε την εφαρμογή Gmail και ανοίξτε ένα email (τα add-ons εμφανίζονται μέσα στην προβολή μηνύματος).

Με την ολοκληρωμένη εφαρμογή των οδηγιών της τρέχουσας ενότητας (5.1), ο αναγνώστης γνωρίζει πώς να εγκαθιστά στο Gmail το πρόσθετό μας. Στην επόμενη ενότητα (5.2), παρουσιάζεται η επίδειξη λειτουργιών του συγκεκριμένου προσθέτου.

5.2 Επίδειξη της εφαρμογής

Η ενότητα αυτή παρουσιάζει, μέσα από **τρεις χαρακτηριστικές περιπτώσεις χρήσης**, τον τρόπο με τον οποίο το πρόσθετο **eMailSec** λειτουργεί στο περιβάλλον του Gmail, επιδεικνύοντας στην πράξη τις δυνατότητές του σε πραγματικά σενάρια. Στόχος είναι να αναδειχθεί πώς το σύστημα παρεμβαίνει **κατά τη στιγμή που δημιουργείται ο κίνδυνος διαρροής δεδομένων** —δηλαδή τη στιγμή της σύνταξης και αποστολής ενός email— ώστε να εντοπίζει ευαίσθητο περιεχόμενο, να προειδοποιεί τον χρήστη και, όπου απαιτείται, να εφαρμόζει **προληπτικές ενέργειες**, όπως κρυπτογράφηση, αποκλεισμό αποστολής ή προσθήκη εμπιστευμένων επαφών. Η παρουσίαση των σεναρίων έχει **προοδευτική δομή**, ξεκινώντας από βασικές λειτουργίες ανίχνευσης και προειδοποίησης και καταλήγοντας σε πιο σύνθετες ενέργειες που αφορούν τη διαχείριση επαφών και κρυπτογραφικών κλειδιών. Συγκεκριμένα:

- **Αποστολή μηνύματος με ευαίσθητο περιεχόμενο και μη εμπιστευμένους παραλήπτες:** Το σενάριο αυτό δείχνει την **DLP λειτουργικότητα** του συστήματος, δηλαδή την ανίχνευση ευαίσθητων δεδομένων, τον **έλεγχο** και τις ενέργειες που μπορεί να εκτελέσει ο χρήστης (Ενότητα 5.2.1).

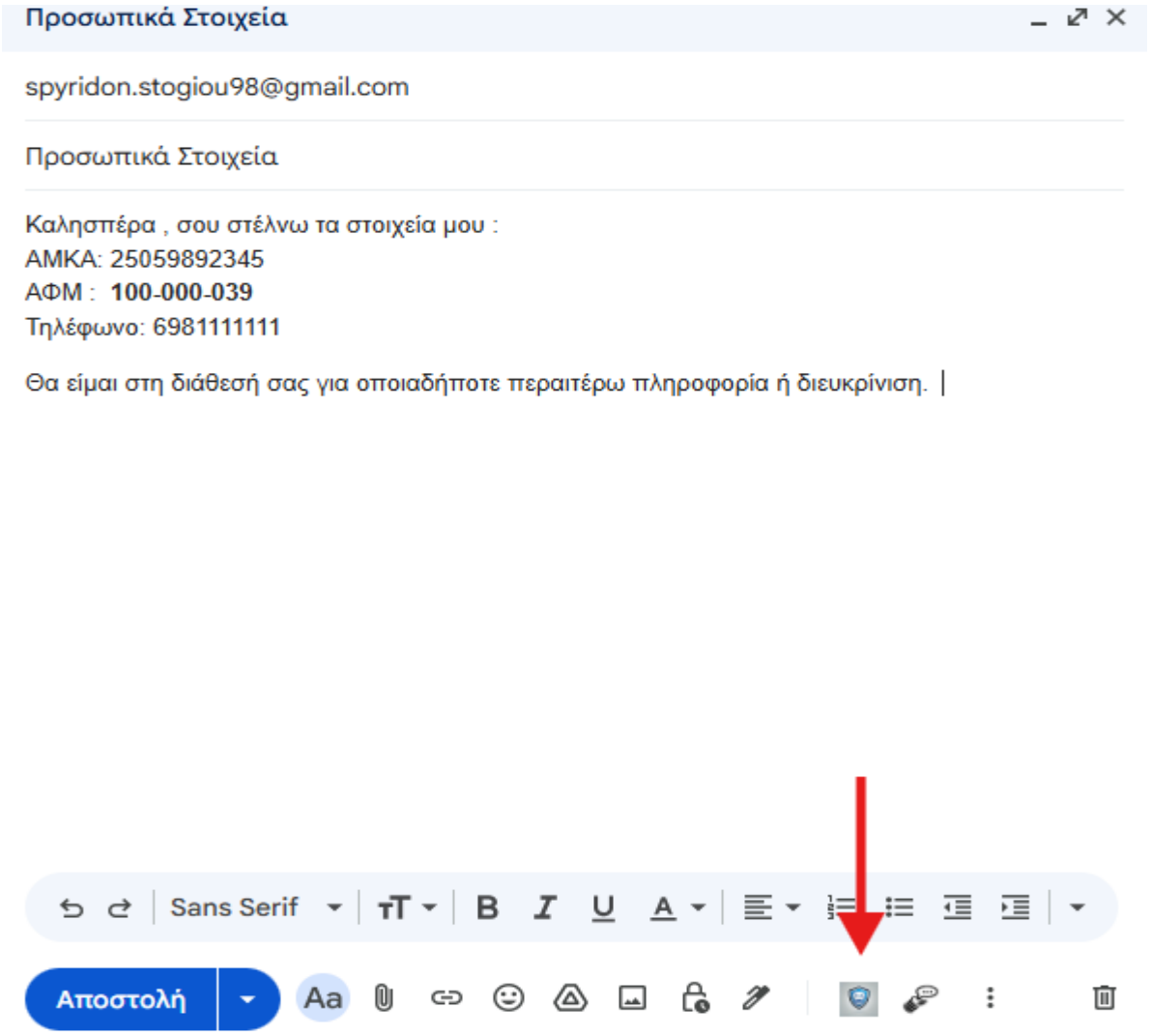
- **Δημιουργία ομάδας επαφών και ενημέρωση επαφής:** Παρουσιάζει τη λειτουργία **διαχείρισης επαφών** του add-on, με δυνατότητα ομαδοποίησης, ενημέρωσης και αποθήκευσης μέσω του μηχανισμού **PropertiesService**, καλύπτοντας το σκέλος της **Contact Management** διεπαφής (Ενότητα 5.2.2).

- **Δημιουργία και αποθήκευση ζεύγους κλειδιών & αποκρυπτογράφηση μηνύματος:** Επικεντρώνεται στο **υποσύστημα Key Management** του eMailSec και στη διαδικασία **PGP/RSA κρυπτογράφησης και αποκρυπτογράφησης**. (Ενότητα 5.2.3)

Κάθε σενάριο περιγράφεται βήμα προς βήμα, με αναφορά στις ενέργειες του χρήστη και στην απόκριση του συστήματος, συνοδευόμενο από **ενδεικτικά στιγμιότυπα οθόνης και επεξηγητικά σχόλια**. Με αυτόν τον τρόπο, ο αναγνώστης αποκτά σαφή εικόνα της λειτουργίας του προσθέτου και της **ολοκληρωμένης DLP εμπειρίας** που προσφέρει.

5.2.1 Αποστολή μηνύματος με ευαίσθητο περιεχόμενο και μη εμπιστευμένους παραλήπτες

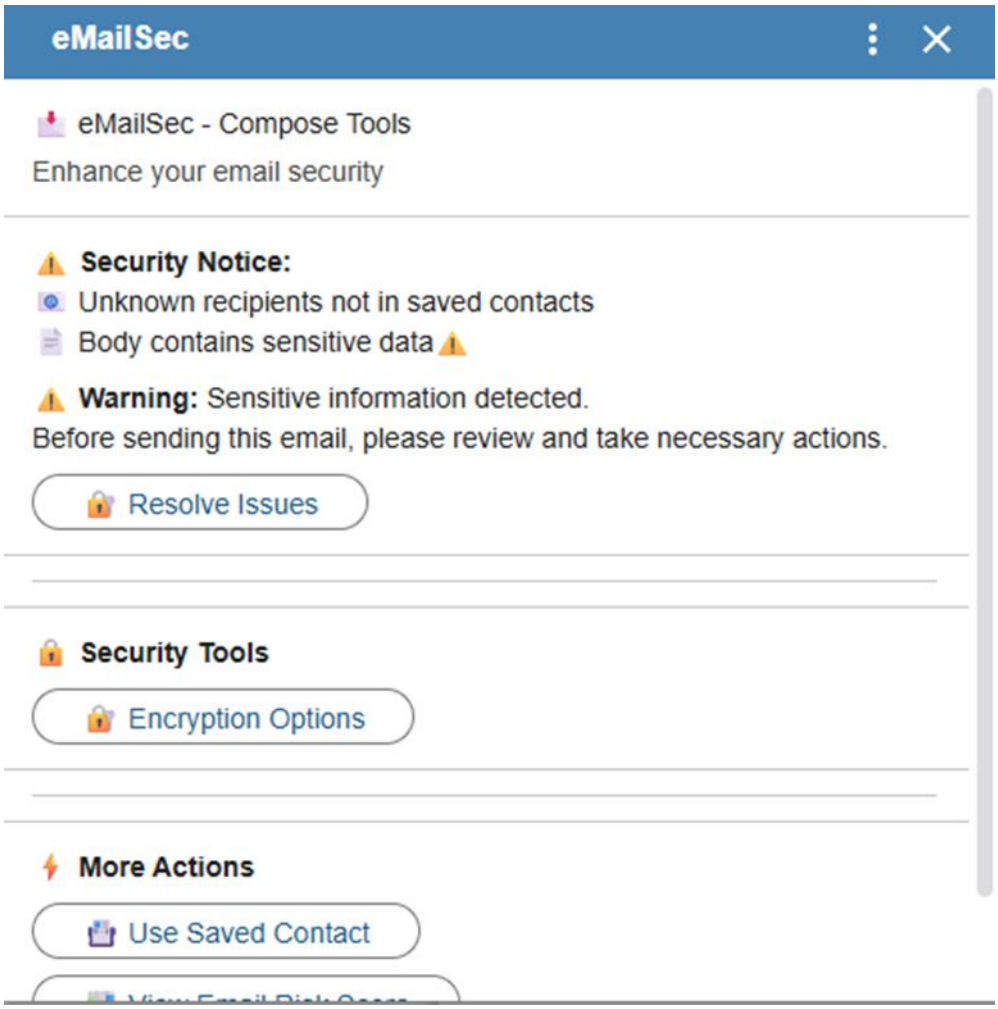
Αρχικά, ο χρήστης συντάσσει το μήνυμά του στο περιβάλλον του Gmail, εισάγοντας το θέμα, το σώμα και τους παραλήπτες. Το περιεχόμενο του email περιλαμβάνει ευαίσθητα προσωπικά δεδομένα, ενώ ένας από τους παραλήπτες δεν βρίσκεται στη λίστα των εμπιστευμένων επαφών (trusted contacts). Αφού ολοκληρώσει τη σύνταξη, ο χρήστης επιλέγει να πραγματοποιήσει έλεγχο ασφάλειας πριν την αποστολή, πατώντας το εικονίδιο του eMailSec που βρίσκεται στο κάτω μενού του παραθύρου σύνταξης (βλ. Εικόνα 14). Η ενέργεια αυτή ενεργοποιεί το πρόσθετο και ανοίγει το παράθυρό του (add-on panel), ξεκινώντας τη διαδικασία ελέγχου.



Εικόνα 14. Σύνταξη email και πρόσθετο eMailSec.

Μετά την ενεργοποίηση του προσθέτου, εμφανίζεται το **κύριο compose πάνελ του eMailSec** (βλ. Εικόνα 15), το οποίο προβάλλει συνοπτικά την **αρχική εκτίμηση του κινδύνου** για το μήνυμα.Το σύστημα ελέγχει αυτόματα τους παραλήπτες, το θέμα και το σώμα του email, και **ενημερώνει τον χρήστη** για τυχόν προβλήματα που εντοπίστηκαν. Στην περίπτωση του συγκεκριμένου σεναρίου, η αναφορά υποδεικνύει:

- την **ύπαρξη μη εμπιστευμένου παραλήπτη**, και
- τον **εντοπισμό ευαίσθητου περιεχομένου** στο σώμα του μηνύματος.



Εικόνα 15. Πάνελ του eMailSec.

Στο κάτω μέρος του πάνελ εμφανίζεται η επιλογή **"Resolve Issues"**, η οποία επιτρέπει στον χρήστη να προχωρήσει σε λεπτομερή ανάλυση των προβλημάτων.Με την επιλογή αυτή, ο χρήστης μεταφέρεται σε **αναλυτική κάρτα ελέγχου** (βλ. Εικόνα 16) όπου παρουσιάζονται **οι συγκεκριμένες θέσεις των προβλημάτων** τόσο οι παραλήπτες που κρίνονται μη εμπιστευμένοι, όσο και τα σημεία του κειμένου που περιέχουν ευαίσθητα δεδομένα.

Η κάρτα χωρίζεται σε δύο κύριες ενότητες:

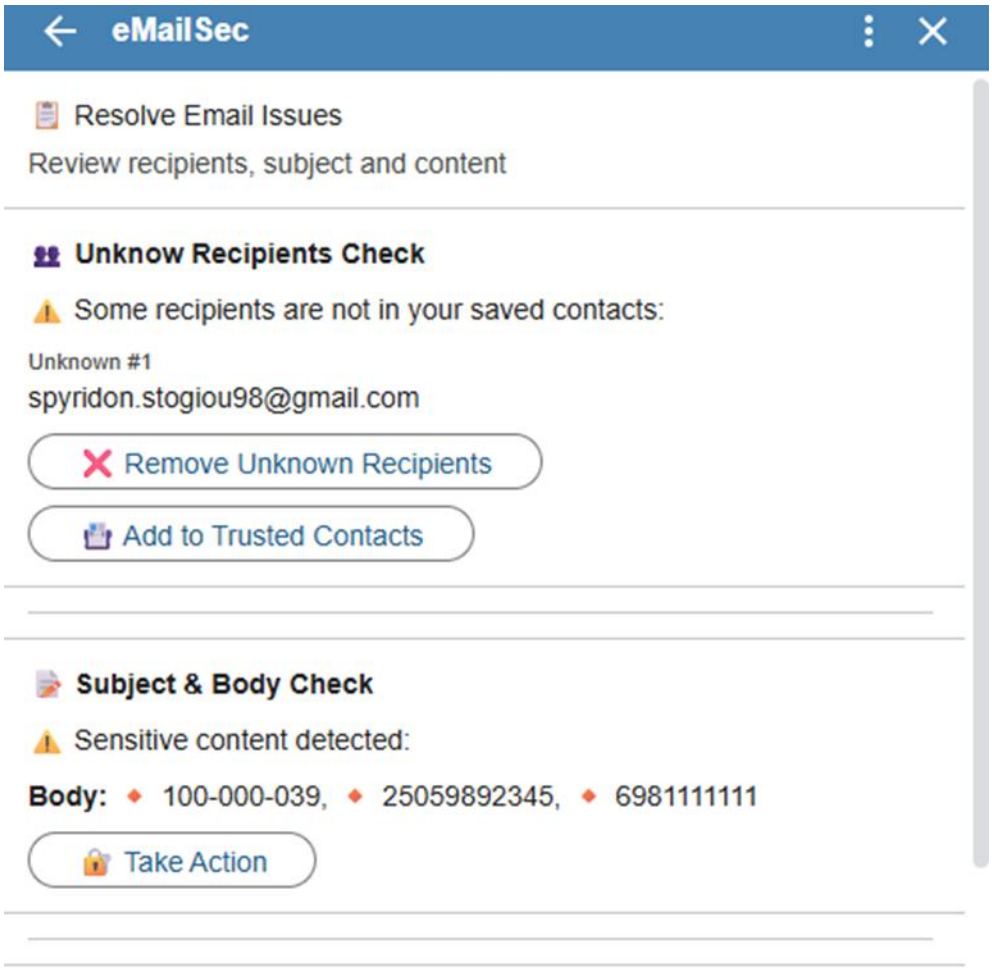
1. **Unknown Recipients Check** – Εμφανίζει όλους τους παραλήπτες που δεν βρίσκονται στη λίστα εμπιστευμένων επαφών. Για κάθε άγνωστο παραλήπτη, το πρόσθετο παρέχει δύο επιλογές:

    - **Remove Unknown Recipients**, για την άμεση αφαίρεση του παραλήπτη από το πεδίο «Προς», και

- **Add to Trusted Contacts**, για την προσθήκη του στη λίστα εμπιστευμένων επαφών (trusted list) μέσω του υποσυστήματος διαχείρισης επαφών.

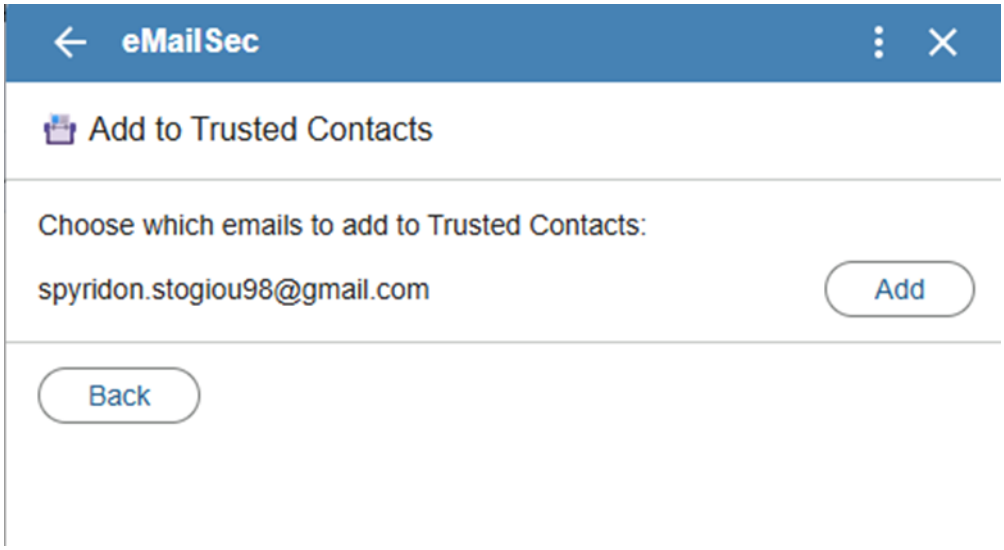
2. **Subject & Body Check** – Εμφανίζει τα σημεία του περιεχομένου όπου εντοπίστηκε ευαίσθητη πληροφορία. Το eMailSec επισημαίνει με ακρίβεια τις φράσεις ή τους αριθμούς που αντιστοιχούν σε **μοτίβα προσωπικών δεδομένων**, επιτρέποντας στον χρήστη να λάβει μέτρα πριν την αποστολή.
   Μέσω της επιλογής **"Take Action"**, ο χρήστης μπορεί να προχωρήσει σε **κρυπτογράφηση (Encrypt)** του περιεχομένου.

Η παρουσίαση των προβλημάτων σε διακριτές ενότητες ενισχύει τη **διαφάνεια και καθοδήγηση** προς τον τελικό χρήστη, προσφέροντας άμεση κατανόηση των κινδύνων και πρακτικές επιλογές για την αντιμετώπισή τους.



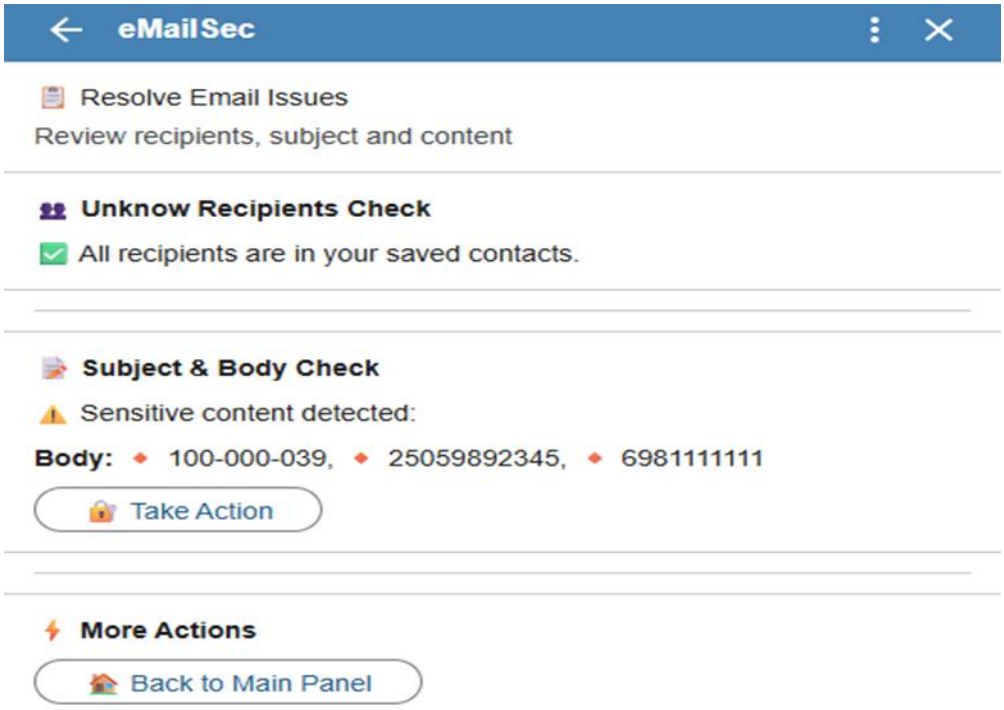
Εικόνα 16. Η αναλυτική κάρτα του eMailSec.

Αφού ο χρήστης ενημερωθεί για τα προβλήματα που εντοπίστηκαν, επιλέγει να **προσθέσει τον άγνωστο παραλήπτη στις εμπιστευμένες επαφές** μέσω του κουμπιού **"Add to Trusted Contacts"**. Ανοίγει νέο παράθυρο στο περιβάλλον του eMailSec (βλ. Εικόνα 17), στο οποίο προβάλλεται η λίστα με τις διευθύνσεις email που μπορούν να προστεθούν στις **εμπιστευμένες επαφές**. Ο χρήστης επιλέγει τη διεύθυνση του παραλήπτη και πατά το κουμπί **"Add"** για να επιβεβαιώσει την προσθήκη.



Εικόνα 17. Παράθυρο προσθήκης παραλήπτη.

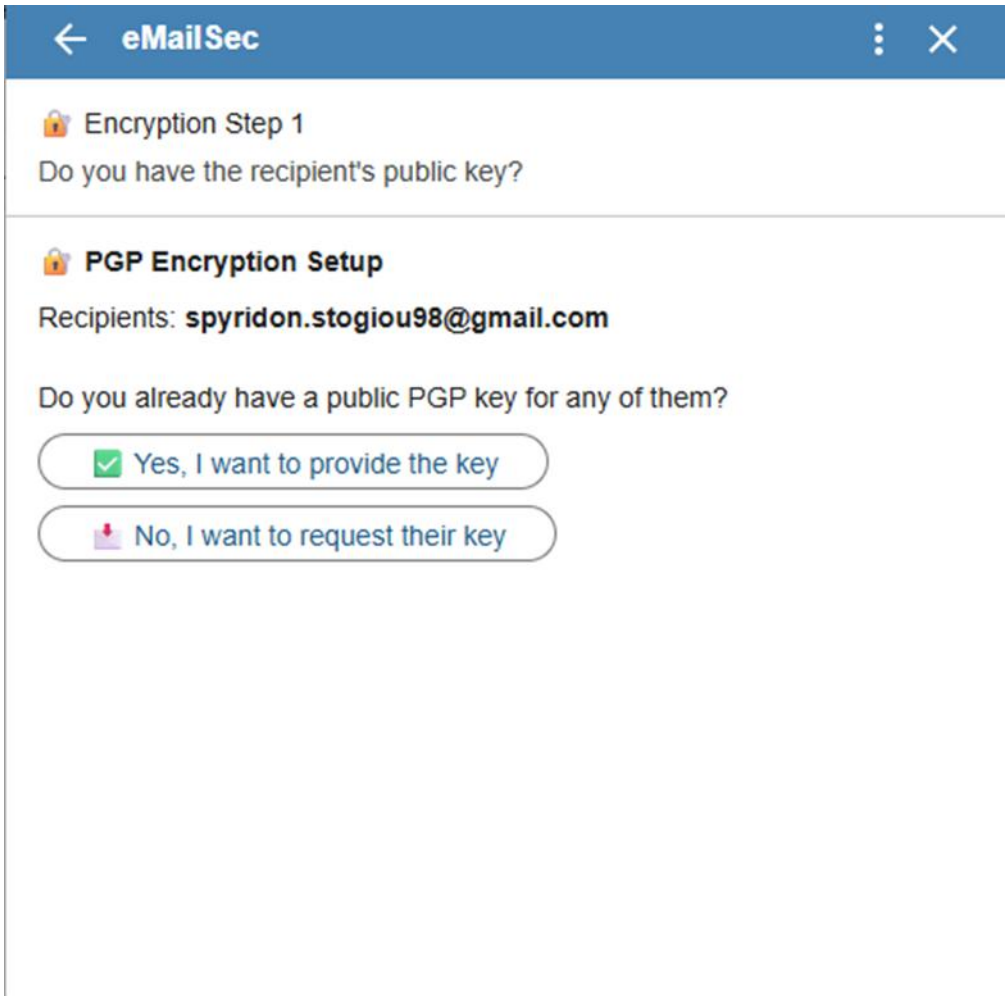
Στην συνέχεια, το eMailSec ενημερώνει εκ νέου την κάρτα επίλυσης προβλημάτων, όπου πλέον απομένει μόνο το θέμα του **ευαίσθητου περιεχομένου** στο σώμα του μηνύματος (βλ Εικόνα 18).



Εικόνα 18. Κάρτα επίλυσης προβλημάτων χωρίς άγνωστους παραλήπτες.

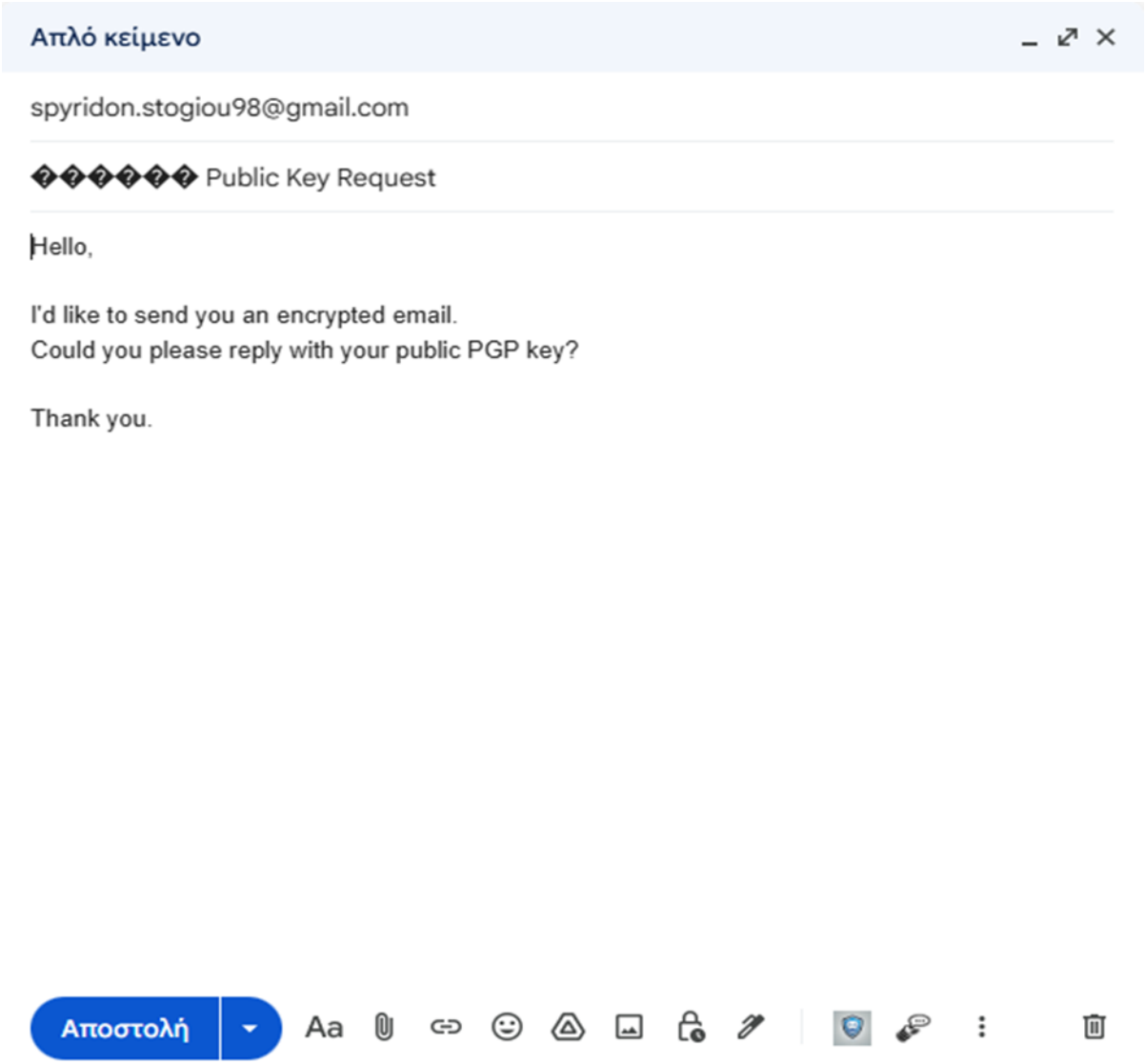
Για να αντιμετωπίσει το ζήτημα, ο χρήστης επιλέγει το κουμπί **"Take Action"**, προκειμένου να καθορίσει τον τρόπο διαχείρισης των ευαίσθητων δεδομένων πριν την αποστολή. Η ενέργεια αυτή ανοίγει τη **διαδικασία κρυπτογράφησης (PGP Encryption Setup)** (βλ. Εικόνα 19), η οποία ξεκινά με το ερώτημα εάν ο χρήστης διαθέτει ήδη το **δημόσιο κλειδί (public key)** του παραλήπτη.
Στην οθόνη εμφανίζονται δύο επιλογές:

- ✅ **"Yes, I want to provide the key"**, εφόσον ο χρήστης έχει ήδη αποθηκευμένο το δημόσιο κλειδί του παραλήπτη και επιθυμεί να το χρησιμοποιήσει για την κρυπτογράφηση, ή
- 📩 **"No, I want to request their key"**, εάν χρειάζεται να αποστείλει **αίτημα λήψης δημόσιου κλειδιού** προς τον συγκεκριμένο παραλήπτη.



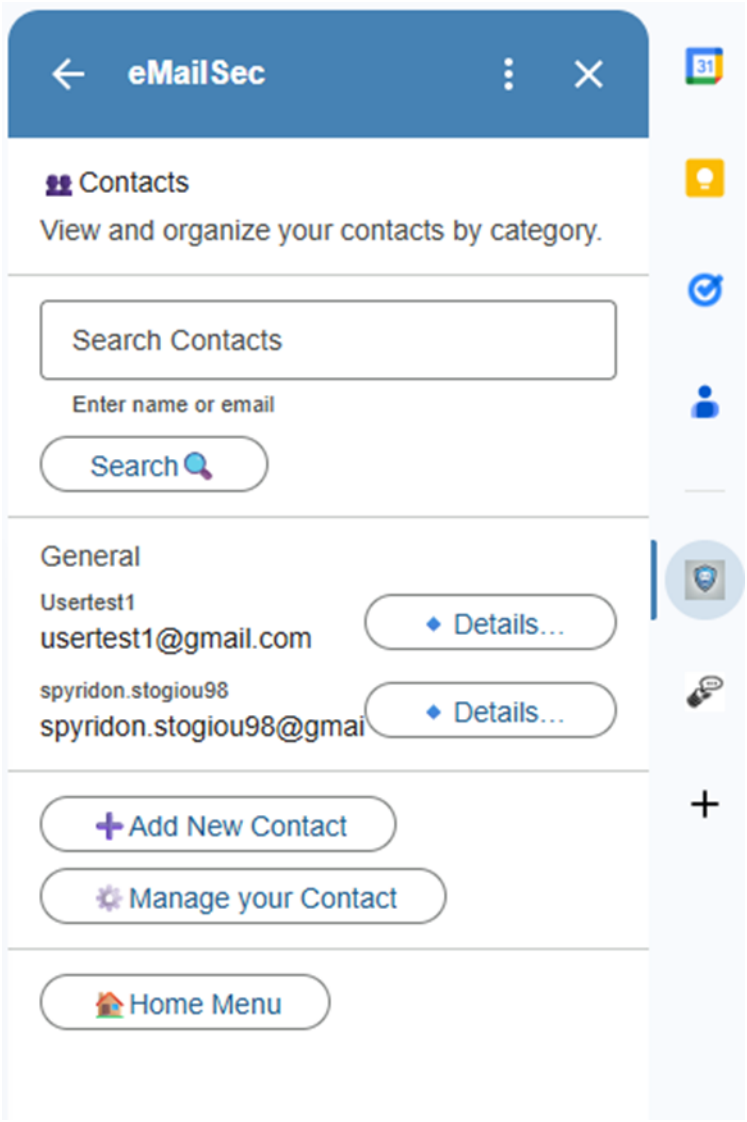
Εικόνα 19. Ο χρήστης επιλέγει "Take Action" .

Στην παρούσα περίπτωση, ο χρήστης επιλέγει την επιλογή **"No, I want to request their key"** ώστε να αποστείλει **αίτημα λήψης δημόσιου κλειδιού** προς τον συγκεκριμένο παραλήπτη (βλ. Εικόνα 20). Με την επιλογή αυτή, το eMailSec προετοιμάζει ένα draft μηνύματος που ο χρήστης μπορεί να αλλάξει εφόσον το επιθυμεί και έπειτα να το στείλει στον παραλήπτη, ζητώντας του να μοιραστεί το δημόσιο PGP κλειδί του. Η ενέργεια αυτή αποτελεί κρίσιμο στάδιο στη διαδικασία **επαλήθευσης ταυτότητας και ασφαλούς ανταλλαγής κλειδιών**, προτού προχωρήσει η κρυπτογράφηση και η τελική αποστολή του email.



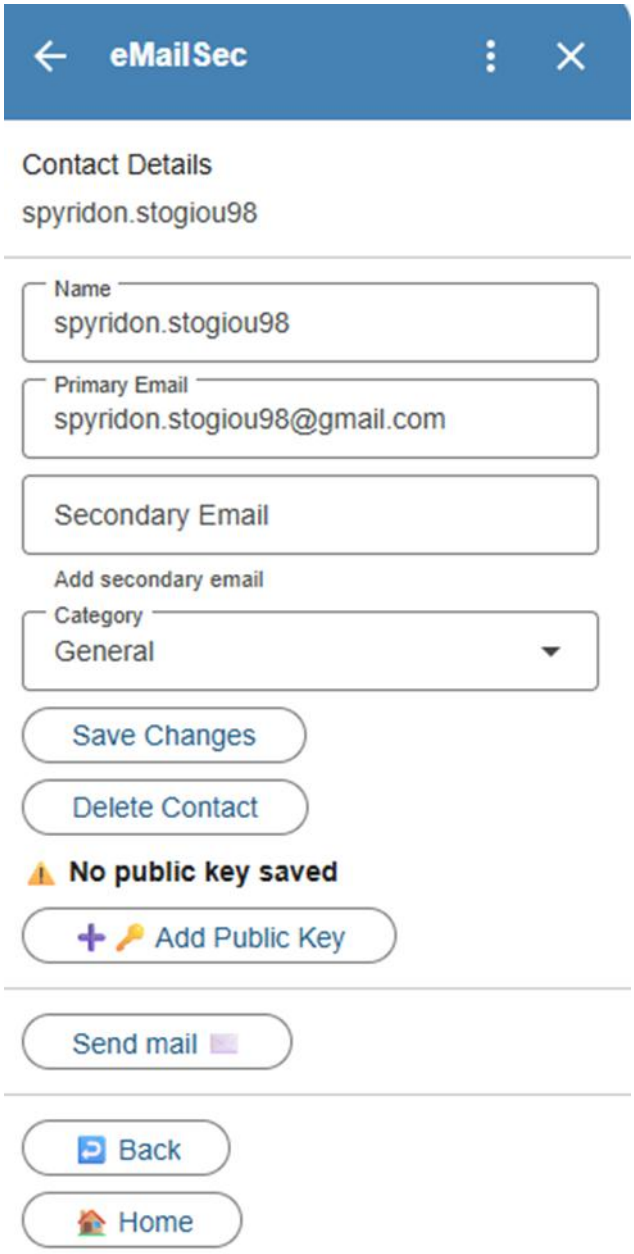
Εικόνα 20. Αίτημα λήψης δημόσιου κλειδιού.

Αφού ο παραλήπτης αποστείλει το **δημόσιο PGP κλειδί** του και τη **σχετική υπογραφή (.sig)** μέσω email, ο χρήστης προχωρά στην προσθήκη τους στο σύστημα επαφών του eMailSec, ώστε να μπορεί στο εξής να πραγματοποιεί **ασφαλείς, κρυπτογραφημένες αποστολές**. Για τον σκοπό αυτό, ο χρήστης ανοίγει το **μενού επαφών (Open Contacts)** (βλ. Εικόνα 21), εντοπίζει τη συγκεκριμένη επαφή και επιλέγει την ενέργεια **"Details"**.



Εικόνα 21. Μενού επαφών (Contacts).

Στην κάρτα πληροφοριών της επαφής εμφανίζεται η επιλογή **"Add Public Key"**, μέσω της οποίας μπορεί να επισυνάψει τα αρχεία που έλαβε (βλ. Εικόνα 22).



Εικόνα 22. Λεπτομέρειες επαφής.

Το σύστημα ζητά από τον χρήστη να εισαγάγει:

- το **δημόσιο κλειδί (public key)** του παραλήπτη και
- την αντίστοιχη **υπογραφή (.sig)** που το συνοδεύει.

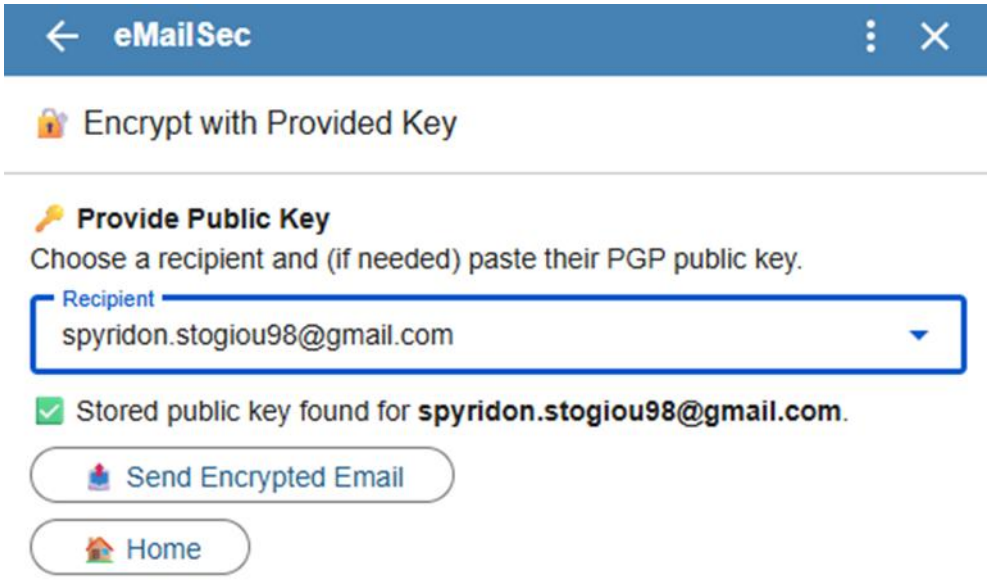
Αφού τα στοιχεία αυτά καταχωρηθούν, το eMailSec εκτελεί **έλεγχο εγκυρότητας (validate)**, επαληθεύοντας ότι η υπογραφή αντιστοιχεί πράγματι στο δηλωμένο δημόσιο κλειδί (βλ. Εικόνα 23).

Εικόνα 23. Προσθήκη κλειδιού στην επαφή.

Μόνο εφόσον η επαλήθευση ολοκληρωθεί επιτυχώς, το κλειδί αποθηκεύεται μόνιμα στην καρτέλα της συγκεκριμένης επαφής, καθιστώντας τη διαθέσιμη για μελλοντική χρήση σε διαδικασίες κρυπτογράφησης (βλ. Εικόνα 24).

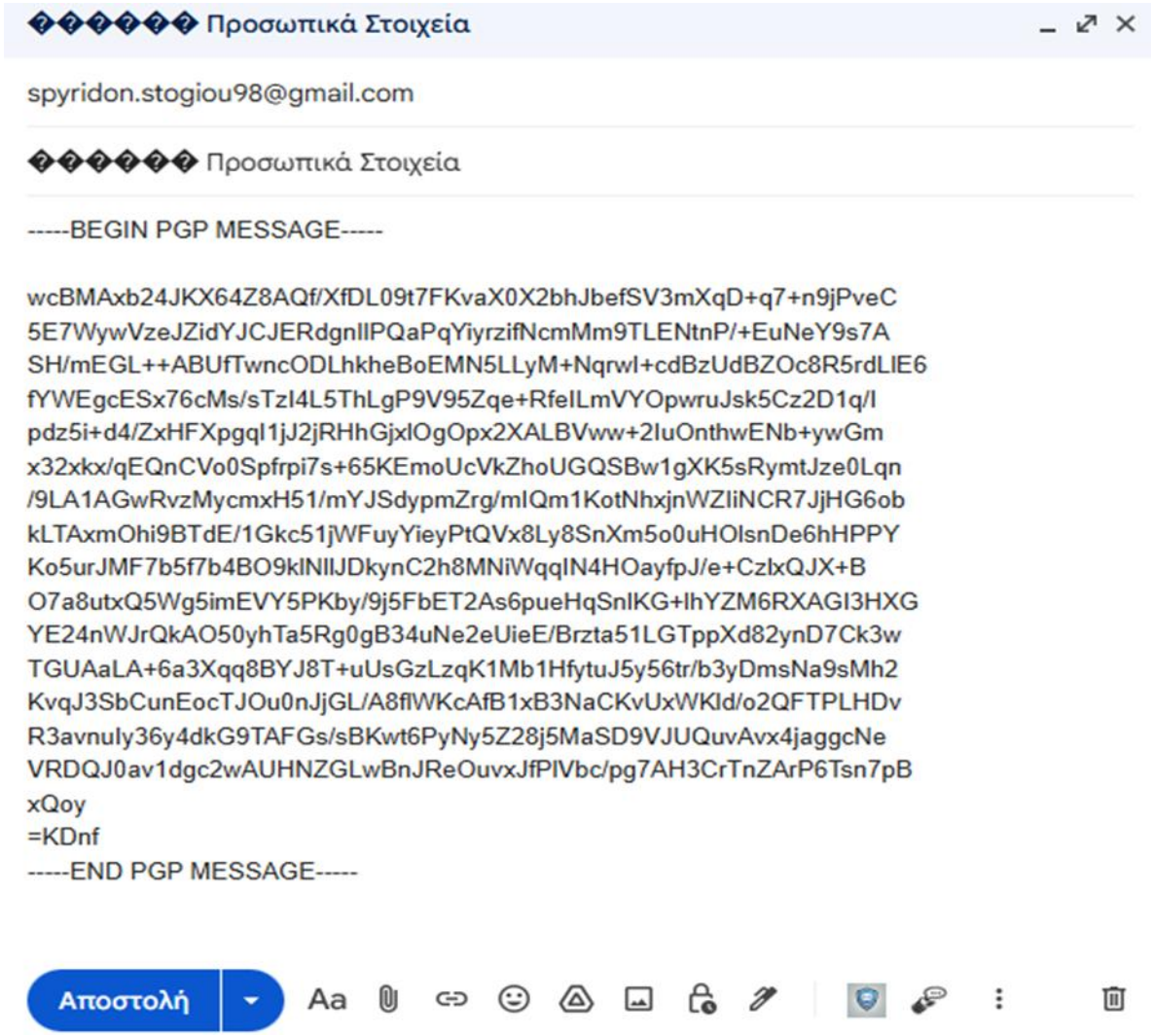
Εικόνα 24. Αποθηκευμένο κλειδί στην επαφή.

Ο χρήστης μπορεί να συνεχίσει τη διαδικασία κρυπτογράφησης του μηνύματος. Επανερχόμενος στην καρτέλα επίλυσης προβλημάτων (Resolve Issues), επιλέγει εκ νέου το κουμπί "Take Action", το οποίο ενεργοποιεί το βήμα "Encrypt with Provided Key" (βλ. Εικόνα 19). Στην οθόνη εμφανίζεται η λίστα με τους παραλήπτες για τους οποίους υπάρχουν αποθηκευμένα δημόσια κλειδιά. Ο χρήστης επιλέγει τον επιθυμητό παραλήπτη και πατά το κουμπί "Send Encrypted Email", ώστε το σύστημα να ξεκινήσει την κρυπτογράφηση του περιεχομένου χρησιμοποιώντας το αντίστοιχο δημόσιο κλειδί (Public PGP Key) (βλ. Εικόνα 25).



Εικόνα 25. Αυτόματη εισαγωγή κλειδιού από τις επαφές.

Τέλος, η διαδικασία ολοκληρώνεται με τη δημιουργία ενός πρόχειρου μηνύματος (encrypted draft), στο οποίο το αρχικό κείμενο έχει αντικατασταθεί από το κρυπτογραφημένο περιεχόμενο τύπου PGP MESSAGE (βλ. Εικόνα 26), το οποίο έπειτα μπορεί να σταλεί από τον χρήστη.



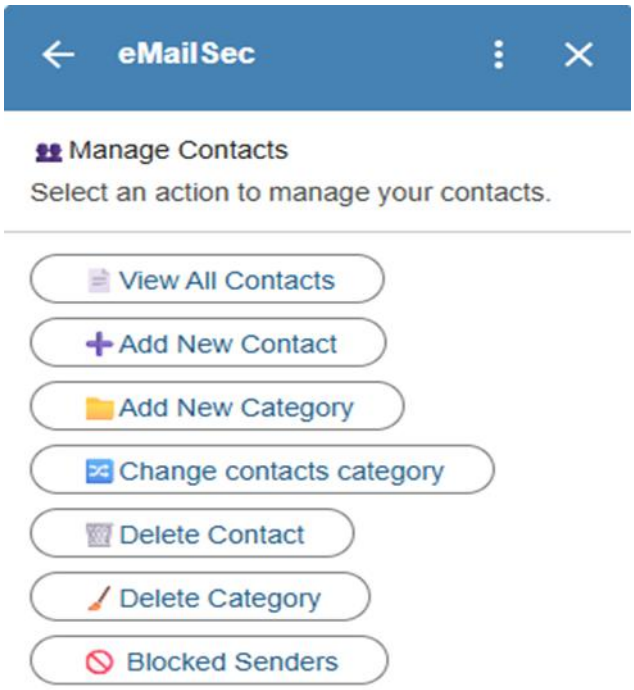
Εικόνα 26. Κρυπτογραφημένο μήνυμα.

Με αυτόν τον τρόπο, το eMailSec ολοκληρώνει τον πλήρη κύκλο προστασίας: **ανίχνευση– προειδοποίηση – επίλυση – επαλήθευση – κρυπτογράφηση – αποστολή.**

5.2.2 Δημιουργία ομάδας επαφών και ενημέρωση επαφής.

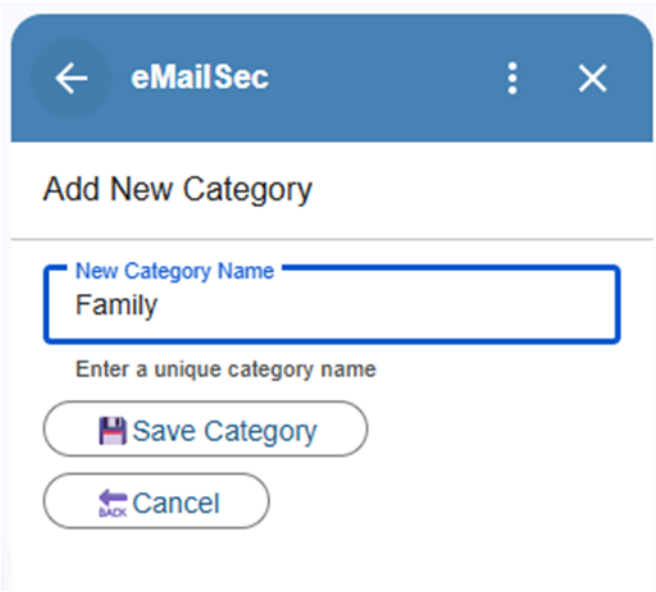
Το δεύτερο σενάριο χρήσης επικεντρώνεται στη λειτουργικότητα **διαχείρισης επαφών (Contact Management)** του προσθέτου eMailSec, η οποία επιτρέπει στον χρήστη να οργανώνει, ενημερώνει και κατηγοριοποιεί τις έμπιστες επαφές του. Η δυνατότητα αυτή είναι κρίσιμη για τη **βελτιστοποίηση της ασφάλειας των επικοινωνιών**, καθώς υποστηρίζει την ομαδοποίηση παραληπτών και τη διατήρηση ενημερωμένων στοιχείων, όπως δημόσια κλειδιά, διευθύνσεις email και κατηγορίες εμπιστοσύνης. Από το κύριο μενού του eMailSec (βλ. Εικόνα 13), ο χρήστης επιλέγει την ενότητα **"Open Contacts"**, μέσω της οποίας εμφανίζεται η πλήρης λίστα των αποθηκευμένων επαφών και κατηγοριών (βλ. Εικόνα 21). Ο χρήστης επιλέγει τη λειτουργία **"Manage your Contacts"**, μέσω της οποίας μπορεί να οργανώσει και να διαχειριστεί το σύνολο των αποθηκευμένων επαφών του.
Στην οθόνη εμφανίζεται το **κύριο μενού ενεργειών** (βλ. Εικόνα 27), που περιλαμβάνει επιλογές όπως:

- **View All Contacts**, για προβολή όλων των επαφών,
- **Add New Contact**, για προσθήκη νέας επαφής,
- **Add New Category**, για δημιουργία νέας κατηγορίας/ομάδας,
- **Change Contacts Category**, για μετακίνηση επαφών μεταξύ κατηγοριών,
- καθώς και λειτουργίες **Delete Contact**, **Delete Category** και **Blocked Senders** για πλήρη διαχείριση.



Εικόνα 27. Manage Contacts.

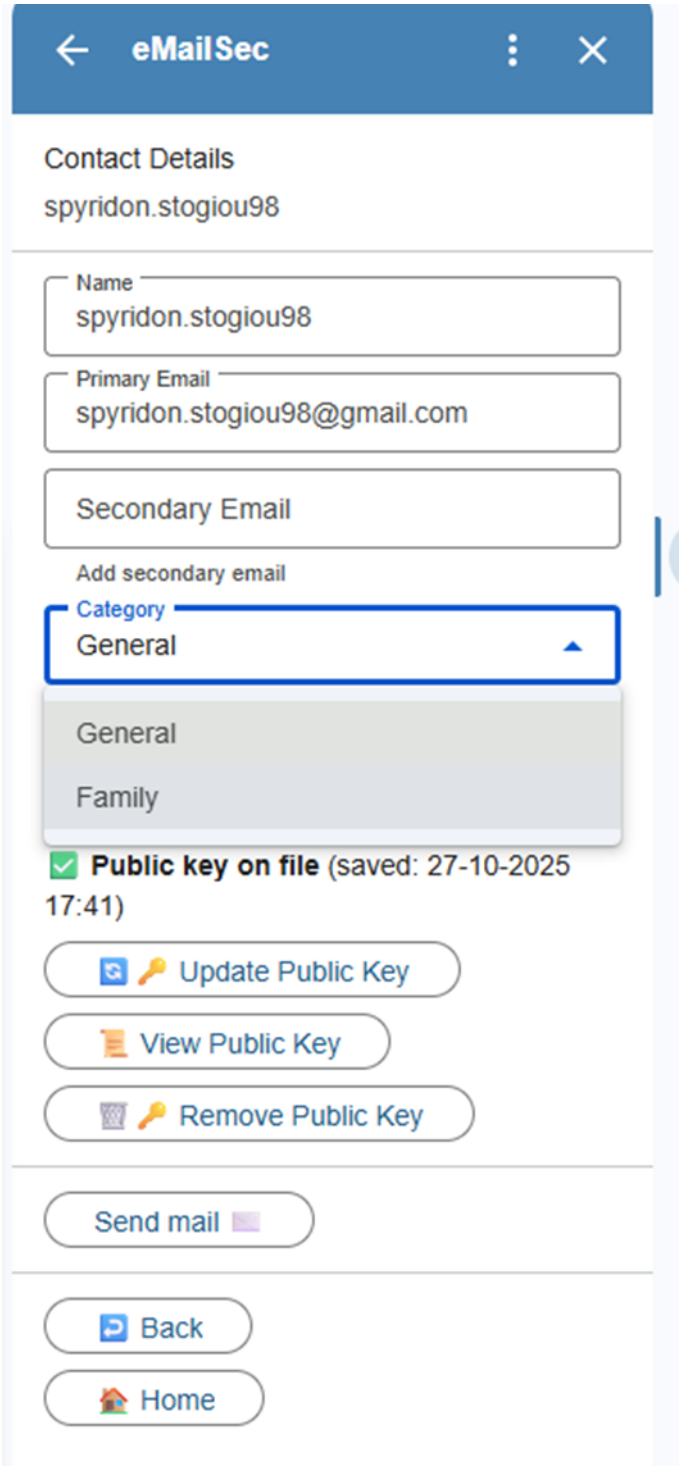
Στο συγκεκριμένο σενάριο, ο χρήστης επιλέγει την επιλογή "Add New Category", προκειμένου να δημιουργήσει μια νέα ομάδα επαφών με το όνομα Family, στην οποία θα μπορεί να ταξινομεί τους παραλήπτες που ανήκουν στην οικογένεια του (βλ. Εικόνα 28).



Εικόνα 28. Νέα κατηγορία επαφών.

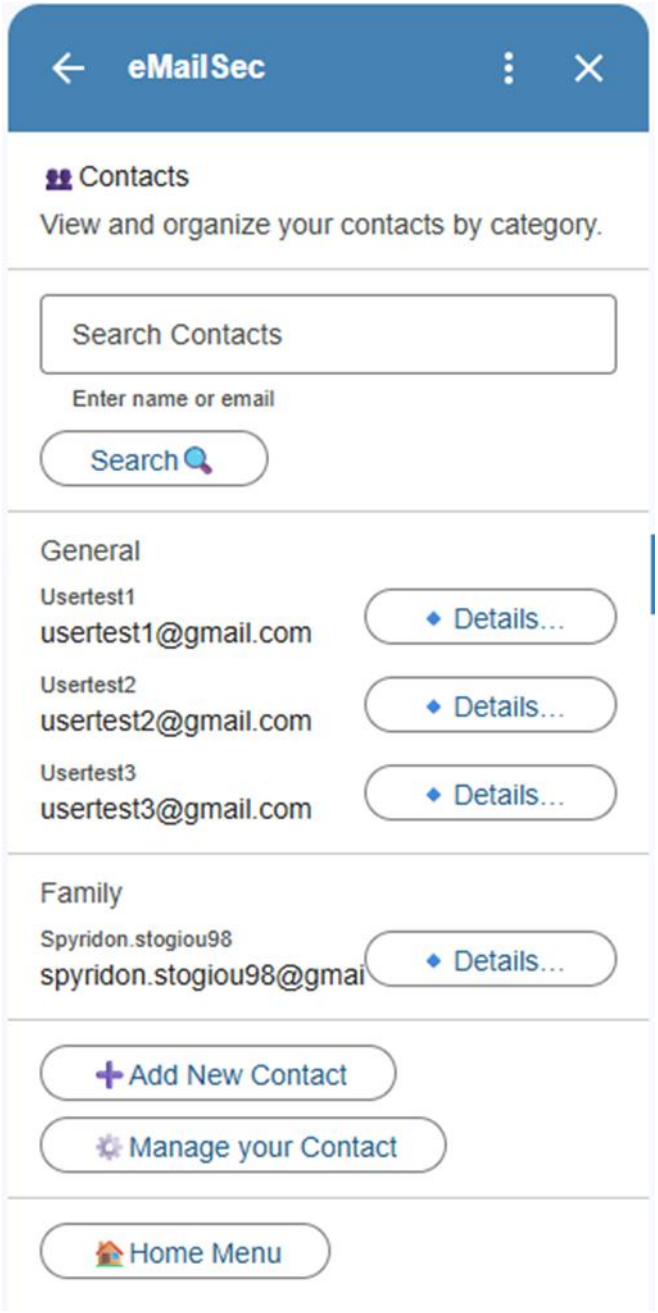
Αφού έχει δημιουργηθεί η νέα κατηγορία επαφών ο χρήστης επιστρέφει αυτόματα στο **κύριο μενού ενεργειών** (βλ. Εικόνα 27), μετά πηγαίνει πίσω στη λίστα των αποθηκευμένων επαφών και εντοπίζει τη συγκεκριμένη επαφή που προστέθηκε προηγουμένως (*Εικόνα 21)*. Με την επιλογή **"Details"**, ανοίγει η **κάρτα πληροφοριών της επαφής**, η οποία περιλαμβάνει τα βασικά πεδία (όνομα, κύρια διεύθυνση email, δευτερεύουσα διεύθυνση, κατηγορία) (βλ. Εικόνα 22).

Από το πεδίο **"Category"**, ο χρήστης επιλέγει τη νέα κατηγορία **"Family"**, προκειμένου να μεταφέρει την επαφή στη συγκεκριμένη ομάδα (βλ. Εικόνα 29). Στη συνέχεια πατά το κουμπί **"Save Changes"** ώστε η τροποποίηση να καταχωρηθεί και να αποθηκευτεί. Τέλος, μετά την αποθήκευση, το eMailSec ενημερώνει αυτόματα τη λίστα επαφών.



Εικόνα 29. Αλλαγή κατηγορίας επαφή.

Η συγκεκριμένη επαφή εμφανίζεται πλέον κάτω από τη νέα κατηγορία **"Family"**, επιβεβαιώνοντας ότι η μεταφορά ολοκληρώθηκε με επιτυχία (βλ. Εικόνα 30).



Εικόνα 30. Ενημερωμένη λίστα επαφών.

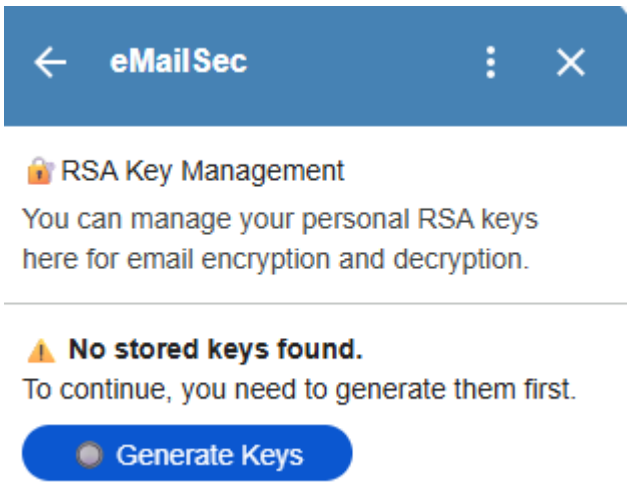
5.2.3 Δημιουργία και αποθήκευση ζεύγους κλειδιών & αποκρυπτογράφηση μηνύματος:

Δημιουργία και αποθήκευση ζεύγους κλειδιών

Στην Ενότητα 5.2 ζητήθηκε από τον χρήστη spyridon.stogiou98@gmail.com να αποστείλει το δημόσιο κλειδί του.

Για την αποστολή του κλειδιού ακολουθούνται τα βήματα:

Κατά το πρώτο άνοιγμα της καρτέλας **Key Management** (από το κεντρικό μενού βλ Εικόνα 13), ο χρήστης πρέπει να δημιουργήσει το ζεύγος κλειδιών (public + private) προκειμένου να χρησιμοποιήσει τις λειτουργίες κρυπτογράφησης/αποκρυπτογράφησης του eMailSec (βλ. Εικόνα 31).

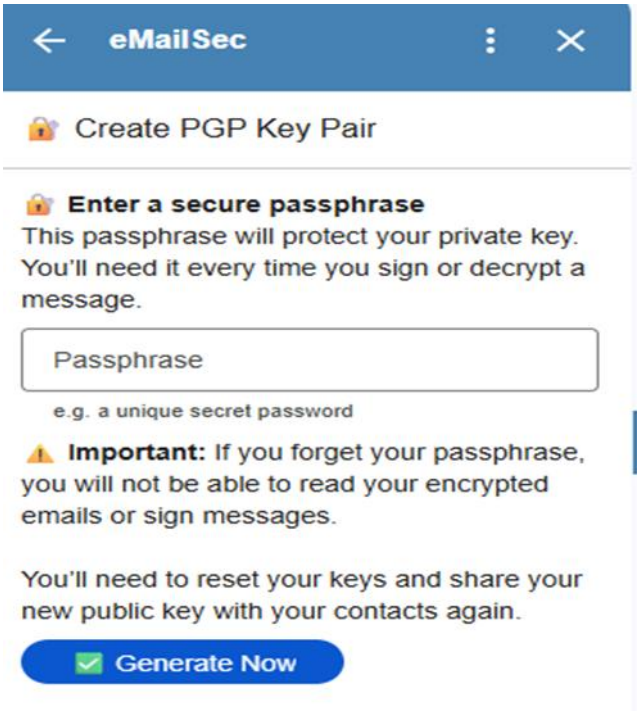


Εικόνα 31. Πρώτο άνοιγμα της καρτέλας Key Management.

Η ροή είναι η εξής:

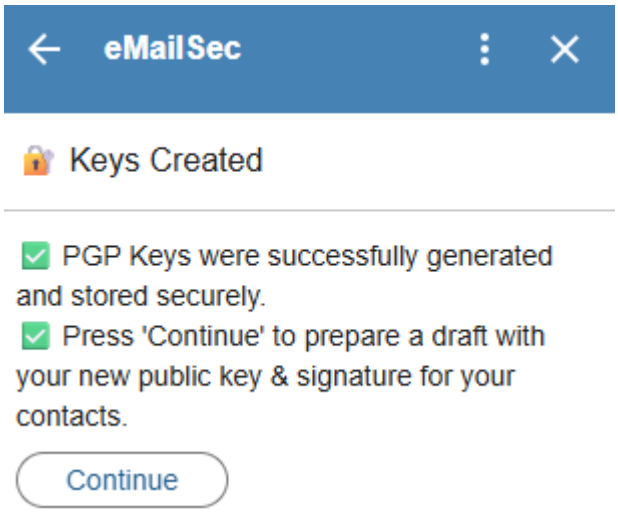
Βασική ροή

1. **Generate Keys**: ο χρήστης επιλέγει «Generate Keys» και το σύστημα δημιουργεί το ζεύγος κλειδιών (PGP).
2. **Εισαγωγή passphrase**: πριν την αποθήκευση, το σύστημα ζητά από τον χρήστη να εισάγει ένα **passphrase** (κωδική φράση). Το passphrase χρησιμοποιείται για την τοπική/εσωτερική κρυπτογράφηση του ιδιωτικού κλειδιού (βλ. Εικόνα 32).



Εικόνα 32. Εισαγωγή passphrase.

3. **Αποθήκευση σε User Properties** — τα παραγόμενα κλειδιά (δημόσιο + ιδιωτικό) αποθηκεύονται **στα UserProperties** του χρήστη και εμφανίζεται μήνυμα επιτυχίας δημιουργίας κλειδιών (βλ. Εικόνα 33).



Εικόνα 33. Μήνυμα επιτυχίας δημιουργίας κλειδιών .

Η αποθήκευση γίνεται με τρόπο που:

- το **ιδιωτικό κλειδί** δεν αποθηκεύεται σε απλό κείμενο αλλά **προστατεύεται** με το passphrase πριν την αποθήκευση,
- το **δημόσιο κλειδί** αποθηκεύεται ώστε να μπορεί να δοθεί ως συνημμένο ή να ανέβει σε keyserver εφόσον το επιθυμεί ο χρήστης.

Η χρήση των UserProperties θεωρείται κατάλληλη για την περίπτωση αυτή διότι ο χώρος αποθήκευσης είναι συνδεδεμένος με τον λογαριασμό Google του χρήστη και προστατεύεται από την υποδομή της Google.

Γιατί ζητάμε passphrase

- Το passphrase προστατεύει το ιδιωτικό κλειδί σε περίπτωση που κάποιος αποκτήσει πρόσβαση στα UserProperties: χωρίς το σωστό passphrase, το ιδιωτικό κλειδί είναι άχρηστο. Σημειώνουμε πως το passphrase λειτουργεί ως συμμετρικό κλειδί κρυπτογράφησης.

- Κατά τη **λήψη** ενός κρυπτογραφημένου email, όταν χρειάζεται να γίνει αποκρυπτογράφηση, το σύστημα **ζητά από τον χρήστη** να εισάγει προσωρινά το passphrase. Με αυτόν τον τρόπο:

    - το ιδιωτικό κλειδί **αποκρυπτογραφείται στο περιβάλλον του add-on** και χρησιμοποιείται για την αποκρυπτογράφηση,

    - ο χρήστης **δεν χρειάζεται** να παρέχει ή να μεταφέρει το ιδιωτικό κλειδί χειροκίνητα σε άλλη θέση, μειώνοντας τον κίνδυνο διαρροής.

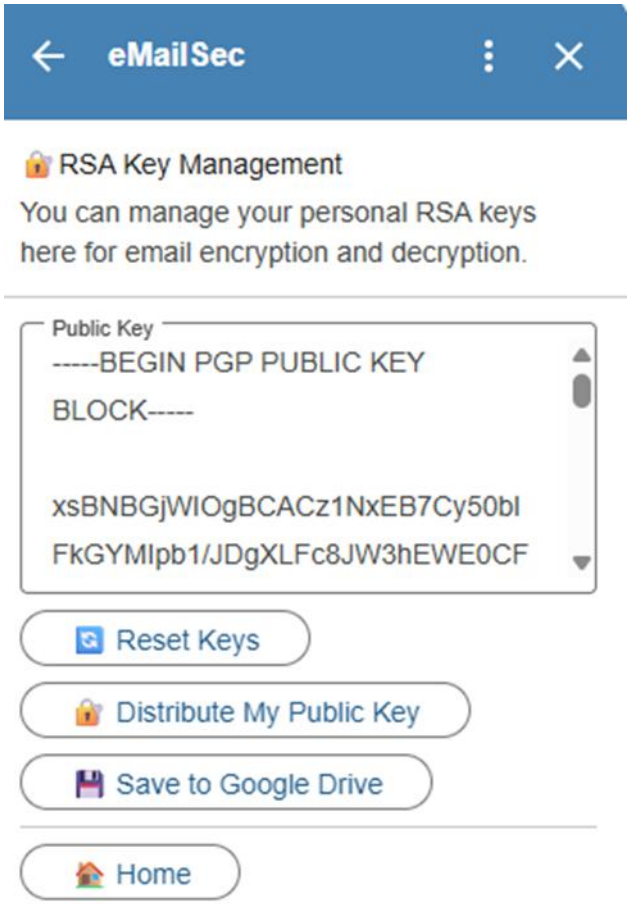
Πλεονεκτήματα ασφάλειας

- Ο χρήστης δεν βλέπει/χειρίζεται άμεσα το ιδιωτικό του κλειδί — αυτό παραμένει κρυπτογραφημένο και αποθηκευμένο με ασφάλεια.

- Αποφεύγεται η αποθήκευση του ιδιωτικού κλειδιού σε μη ασφαλείς τοποθεσίες ή η αποστολή του μέσω δικτύου.

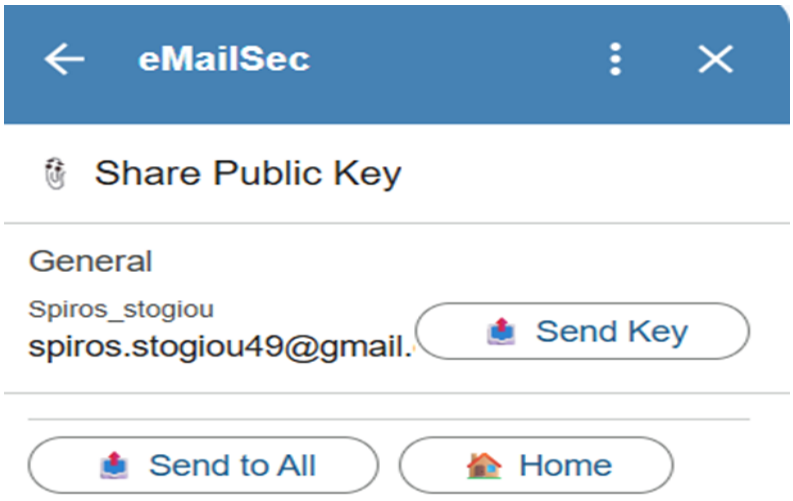
- Η απαίτηση passphrase παρέχει πρόσθετη προστασία σε περίπτωση μη εξουσιοδοτημένης πρόσβασης στο λογαριασμό.

Ο χρήστης μετα την δημιουργία κλειδιών μεταφέρεται αυτόματα στην αρχική καρτα του Key Management (οπου τώρα έχει κλειδιά) και μπορεί ανά πάσα στιγμή να **ανανεώσει** ή **διαγράψει** τα αποθηκευμένα κλειδιά από την ίδια καρτέλα (βλ. Εικόνα 34).



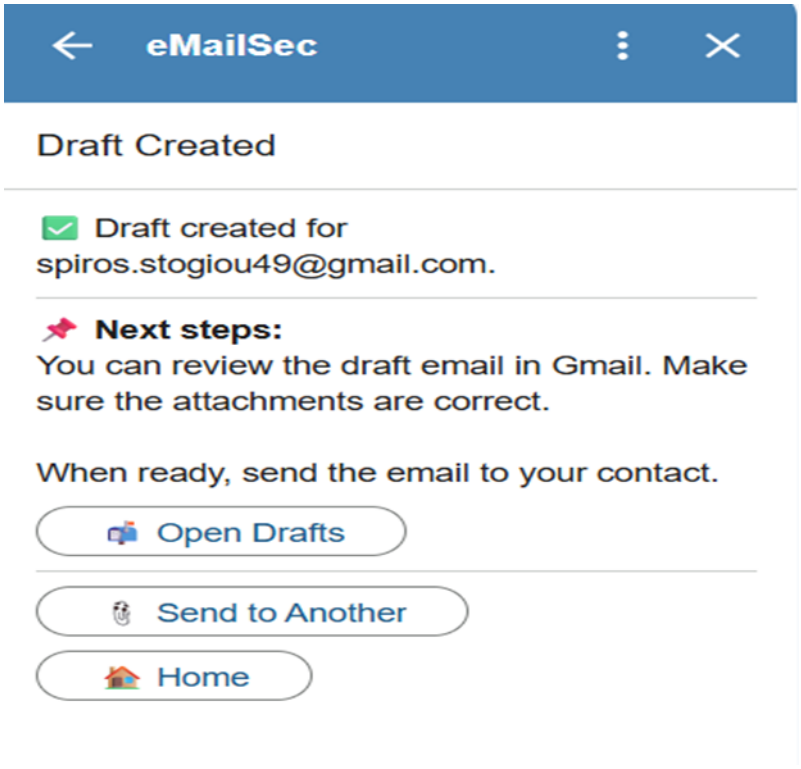
Εικόνα 34. Κάρτα διαχείρισης κλειδιού.

Ο χρήστης στην συνέχεια επιλέγει απο την κάρτα διαχείρισης κλειδιου (βλ. Εικόνα 34) την επιλογή Distribute My Public Key. Εκεί εμφανιζονται οι αποθηκευμένες επαφές του και επιλέγει την επαφή προς διανομή του δημόσιου κλειδιού του (στην περίπτωση μας τον χρήστη spiros.stogiou49@gmail.com) (βλ. Εικόνα 35).



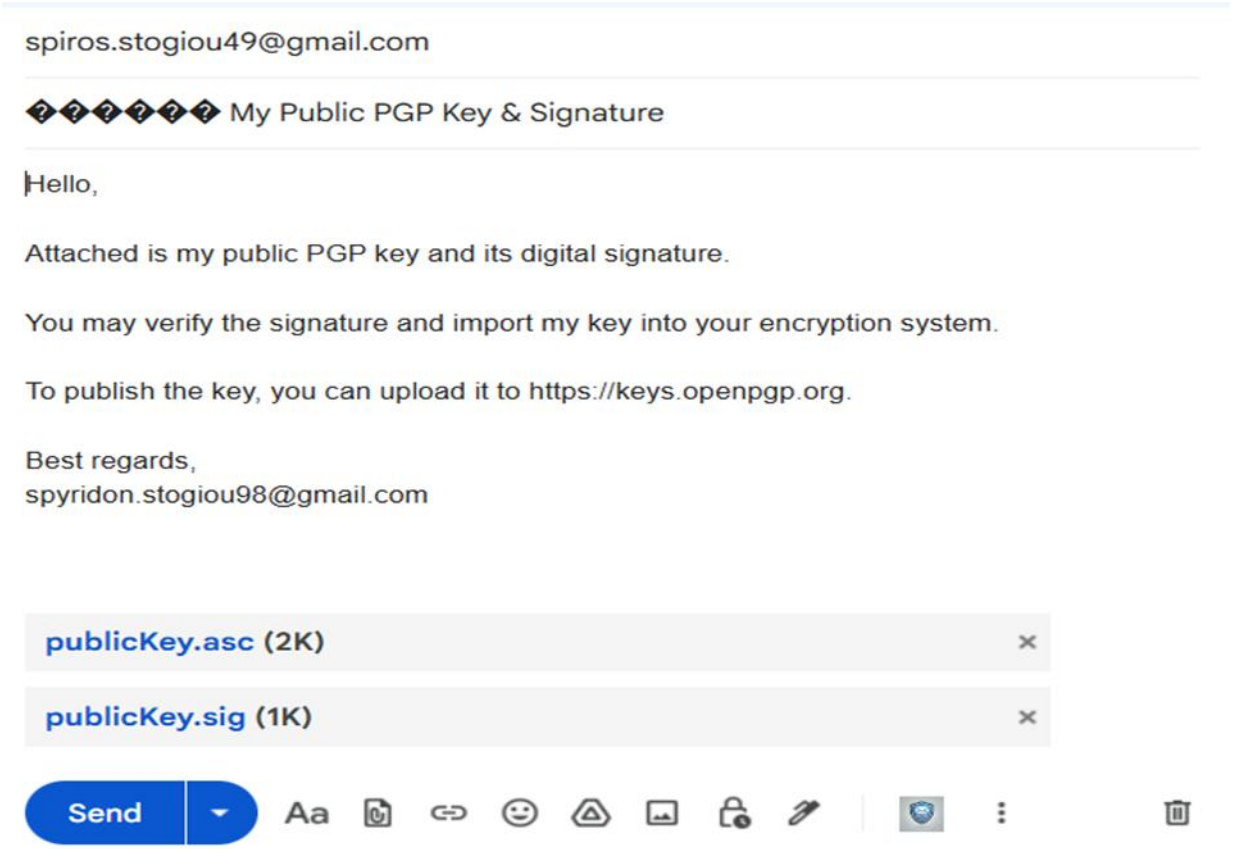
Εικόνα 35. Shere Public Key.

Επιλέγει το Send Key και τότε εμφανίζεται μήνυμα ότι δημιουργήθηκε το draft με το κλειδί και την υπογραφή (βλ. Εικόνα 36).



Εικόνα 36. Μήνυμα επιτυχίας δημιουργίας draft για διαμοιρασμό κλειδιού.

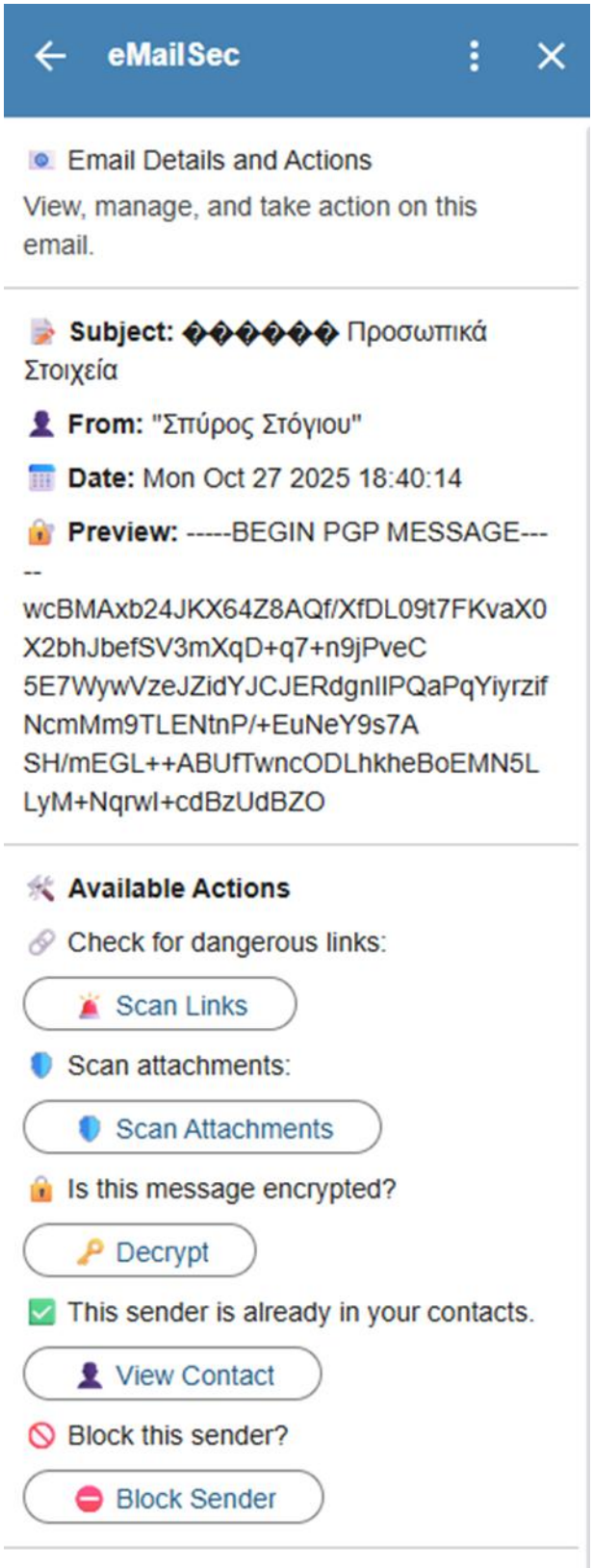
Ο χρήστης ανοίγει τα draft και στέλνει το κλειδί του και την υπογραφή του στον spiros.stogiou49@gmail.com (βλ. Εικόνα 37).



Εικόνα 37. Draft για αποστολή κλειδιών και υπογραφής.

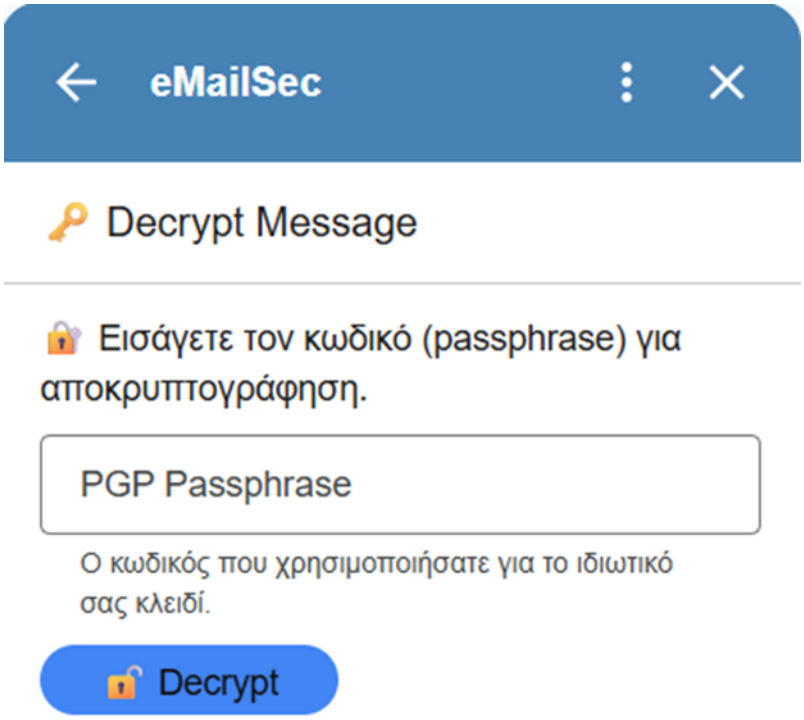
Αποκρυπτογράφηση μηνύματος

Αφου έχει στείλει το κλειδί του, ο χρήστης περιμένει κρυπτογραφημένο μύνυμα (βλ. Εικόνα 26). Μετά τη λήψη του κρυπτογραφημένου email, ο παραλήπτης ανοίγει το μήνυμα στο Gmail και ενεργοποιεί το πρόσθετο **eMailSec** από το δεξί πάνελ, προκειμένου να προβεί σε **αποκρυπτογράφηση** (βλ. Εικόνα 38).



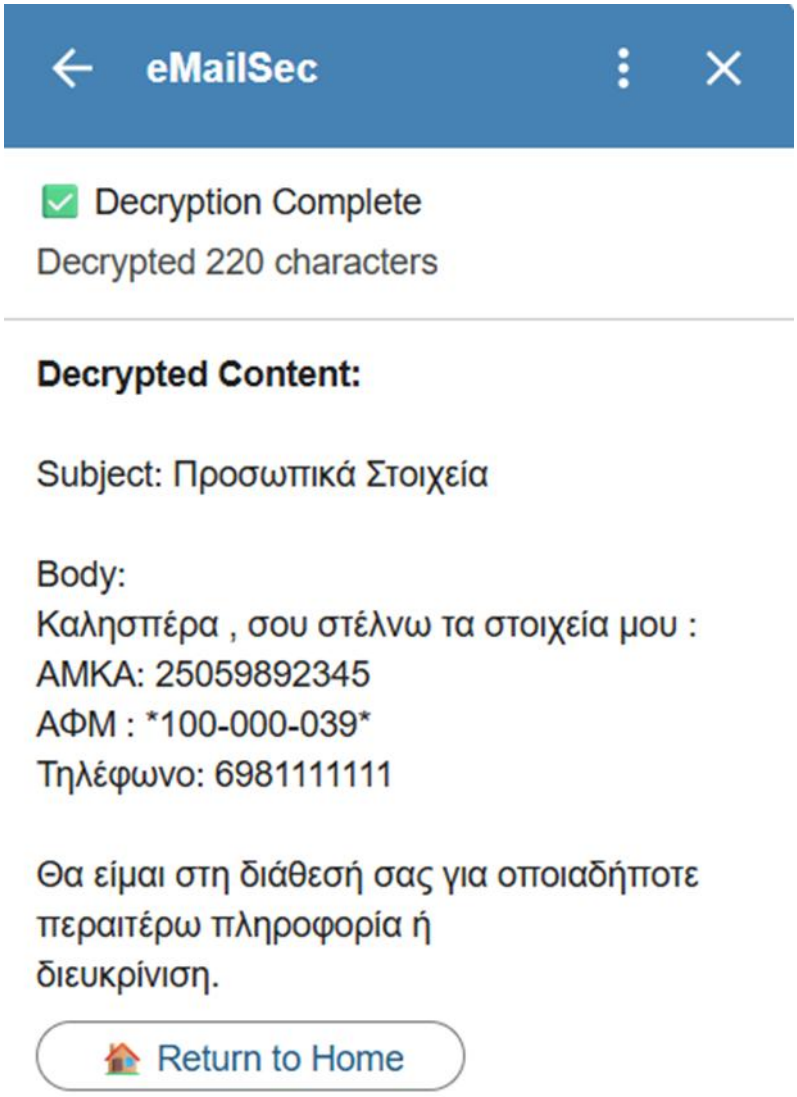
Εικόνα 38. Πάνελ Open Mail του eMailSec.

Ο χρήστης επιλέγει το κουμπί **"Decrypt"**, με αποτέλεσμα το πρόσθετο να ζητήσει το **passphrase** που αντιστοιχεί στο αποθηκευμένο ιδιωτικό κλειδί του χρήστη (βλ. Εικόνα 39). Μόλις αυτό επαληθευτεί, το eMailSec χρησιμοποιεί το ιδιωτικό κλειδί (private key) για να αποκρυπτογραφήσει το περιεχόμενο του μηνύματος μέσω του ασφαλούς backend API.



Εικόνα 39. Εισαγωγή του passphrase.

Το αποτέλεσμα της διαδικασίας προβάλλεται απευθείας μέσα στο Gmail, με το αρχικό κείμενο να αντικαθιστά το κρυπτογραφημένο περιεχόμενο, καθιστώντας έτσι το μήνυμα πλήρως αναγνώσιμο (βλ. Εικόνα 40).



Εικόνα 40. Προβολή του κρυπτογραφημένου μηνύματος.

Στην παρούσα ενότητα παρουσιάστηκαν και δοκιμάστηκαν οι βασικές λειτουργίες του eMailSec —πώς παρεμβαίνει στο στάδιο της σύνταξης, πώς εντοπίζει και επισημαίνει ευαίσθητο περιεχόμενο, πώς διαχειρίζεται παραλήπτες και έμπιστες επαφές, καθώς και οι ροές δημιουργίας/αποθήκευσης κλειδιών και κρυπτογράφησης/αποκρυπτογράφησης. Καλύψαμε το μεγαλύτερο μέρος της διεπαφής χρήστη και των κρίσιμων σεναρίων χρήσης (Alerting, Resolve Issues, Manage Contacts, Key Management, Send Encrypted Mail, Decrypt/Verify), μαζί με τα κύρια σημεία ασφάλειας και ιδιωτικότητας που υποστηρίζουν τις λειτουργίες αυτές.

6

Αποτίμηση Λύσης

Η αποτίμηση της λύσης αποτελεί κρίσιμο στάδιο για την τεκμηρίωση του βαθμού στον οποίο το πρόσθετο μας για το Gmail επιτυγχάνει τον βασικό του σκοπό, δηλαδή την ενίσχυση της ασφάλειας και την αποτροπή διαρροής ευαίσθητων πληροφοριών. Η αξιολόγηση περιλαμβάνει τόσο **ποσοτική** όσο και **ποιοτική** ανάλυση, συνδυάζοντας μετρήσιμα δεδομένα με την εμπειρία των χρηστών. Με αυτόν τον τρόπο διασφαλίζεται ότι το σύστημα αξιολογείται σφαιρικά, όχι μόνο ως προς την τεχνική του απόδοση, αλλά και ως προς τη χρηστικότητα και την αποτελεσματικότητα στην πραγματική χρήση.

6.1 Στόχοι Αποτίμησης

Η αποτίμηση στοχεύει:

- Στην εξέταση της ακρίβειας του μηχανισμού εντοπισμού ευαίσθητων δεδομένων.
- Στην αξιολόγηση της ταχύτητας απόκρισης και της αποδοτικότητας του συστήματος.
- Στην εκτίμηση της εμπειρίας χρήστη και της χρηστικότητας του UI.
- Στον έλεγχο του βαθμού στον οποίο το πρόσθετο ενσωματώνεται ομαλά στη ροή χρήσης του Gmail.
- Στην εκτίμηση της συμβολής του προσθέτου στη μείωση κινδύνου διαρροής δεδομένων.

6.2 Μεθοδολογία

6.2.1 Προσέγγιση

Η αποτίμηση βασίστηκε σε δύο κύριες προσεγγίσεις, οι οποίες είναι ευρέως αποδεκτές στη βιβλιογραφία για την αξιολόγηση συστημάτων πληροφορικής:

1. Ποσοτική αποτίμηση: Η ποσοτική αποτίμηση περιλαμβάνει τη χρήση μετρήσιμων δεικτών απόδοσης και αποτελεσματικότητας, οι οποίοι χρησιμοποιήθηκαν για την αξιολόγηση τόσο της ακρίβειας ανίχνευσης ευαίσθητων δεδομένων, όσο και της ταχύτητας του συστήματος κατά την εκτέλεση βασικών λειτουργιών. Οι σημαντικότεροι δείκτες είναι:

    - **Precision (Ακρίβεια):** μετρά το ποσοστό των σωστών ευρημάτων σε σχέση με όλα τα ευρήματα που επέστρεψε το σύστημα. Ένας υψηλός δείκτης Precision σημαίνει ότι το σύστημα παράγει λίγα false positives [111].

    - **Recall (Ανάκληση):** δείχνει το ποσοστό των πραγματικών ευαίσθητων δεδομένων που εντόπισε το σύστημα. Ένας υψηλός δείκτης Recall σημαίνει ότι δεν χάνονται κρίσιμα δεδομένα (λιγότερα false negatives) [111].

    - **F1-score:** είναι ο αρμονικός μέσος όρος των Precision και Recall, παρέχοντας έναν συνολικό δείκτη ισορροπίας ανάμεσα στην ακρίβεια και την πληρότητα/ανάκληση [112].

    - **Χρόνος εκτέλεσης (Execution Time)**: ο ελάχιστος, μέγιστος και μέσος χρόνος ολοκλήρωσης βασικών λειτουργιών (ανίχνευση, κρυπτογράφηση, αποκρυπτογράφηση).

2. **Ποιοτική αποτίμηση**: αφορά την εμπειρία των χρηστών και τη χρηστικότητα του συστήματος. Εξετάζονται ο βαθμός κατανόησης των προειδοποιήσεων, η ευκολία χρήσης του UI και ο βαθμός στον οποίο το πρόσθετο υποστηρίζει τη ροή εργασίας χωρίς να επιβαρύνει τον χρήστη [113].

Η συνδυαστική αυτή μεθοδολογία επιτρέπει την κάλυψη τόσο των τεχνικών όσο και των ανθρώπινων παραμέτρων, παρέχοντας μια πλήρη εικόνα της αποτελεσματικότητας της λύσης.

6.2.2 Input για τις δοκιμές

Για την αξιολόγηση της ακρίβειας του συστήματος κατασκευάστηκε ένα **golden set** που περιλαμβάνει 52 δείγματα, στα οποία έχουν οριστεί εκ των προτέρων τα αναμενόμενα θετικά και αρνητικά αποτελέσματα. Κάθε εγγραφή του συνόλου έχει τη μορφή:

["Όνομα test","Κείμενο προς έλεγχο",expectedEmail,expectedAFM_AMKA, expectedPhone,expectedIBAN]

Όπου τα expectedEmail, expectedAFM_AMKA, expectedPhone, expectedIBAN είναι λογικές (boolean) μεταβλητές με τιμές true/false που δηλώνουν αν αναμένεται το κείμενο να περιέχει τα αντίστοιχα ευαίσθητα δεδομένα.

Παράδειγμα εγγραφής:

["AMKA valid","AMKA: 01019912345",false,true,false,false]

Στο συγκεκριμένο παράδειγμα, η μεταβλητή expectedAFM_AMKA έχει τιμή true, δηλώνοντας ότι το κείμενο περιέχει έναν έγκυρο αριθμό ΑΜΚΑ που πρέπει να αναγνωριστεί από το σύστημα. Όλες οι υπόλοιπες κατηγορίες (expectedEmail, expectedPhone, expectedIBAN) έχουν τιμή false, αφού το δείγμα δεν περιλαμβάνει στοιχεία άλλων τύπων.

Με αυτόν τον τρόπο ορίζεται για κάθε δοκιμαστικό κείμενο ποια κατηγορία ευαίσθητων δεδομένων θα πρέπει να αναγνωριστεί από το σύστημα. Τα δείγματα καλύπτουν όλες τις βασικές κατηγορίες που υποστηρίζει η υλοποίηση, δηλαδή **διευθύνσεις ηλεκτρονικού ταχυδρομείου (Email)**, **ΑΦΜ/ΑΜΚΑ**, **τηλεφωνικούς αριθμούς** και **IBAN/οικονομικά δεδομένα**, όπου κάθε δείγμα αντιστοιχεί σε μία και μόνο περίπτωση ώστε να αξιολογείται μεμονωμένα η ικανότητα αναγνώρισης του συστήματος ανά κατηγορία ευαίσθητων δεδομένων.

Κατά την εκτέλεση των δοκιμών, τα αποτελέσματα κατηγοριοποιήθηκαν σε **True Positives (TP), True Negatives (TN)**, **False Positives (FP)** και **False Negatives (FN)** για κάθε κατηγορία. Στη συνέχεια, οι μετρήσεις αυτές χρησιμοποιήθηκαν για τον υπολογισμό των δεικτών **Precision**, **Recall** και **F1-score**, οι οποίοι επιτρέπουν την ποσοτική αξιολόγηση της απόδοσης του συστήματος στην ανίχνευση ευαίσθητων δεδομένων.

6.3 Ποσοτική Αποτίμηση

Η ποσοτική αποτίμηση επικεντρώνεται στη μέτρηση της αποτελεσματικότητας και της απόδοσης του συστήματος, με σκοπό την αντικειμενική αξιολόγηση της ακρίβειας ανίχνευσης ευαίσθητων δεδομένων και της ταχύτητας εκτέλεσης των βασικών λειτουργιών.

Η αξιολόγηση πραγματοποιήθηκε μέσω δύο πειραμάτων:

1. **Αξιολόγηση ακρίβειας αναγνώρισης ευαίσθητων δεδομένων.**
2. **Αξιολόγηση απόδοσης και χρόνου απόκρισης λειτουργιών.**

6.3.1 Ορισμοί και Μετρικές Αξιολόγησης

Για την ποσοτική αποτίμηση χρησιμοποιήθηκαν δύο ομάδες δεικτών:

- **Δείκτες ακρίβειας ανίχνευσης (Precision, Recall, F1-score)**
- **Δείκτες ταχύτητας (min, max, avg execution time)**

(α) Δείκτες ακρίβειας ανίχνευσης

Ορισμοί Δεικτών Αξιολόγησης

- **True Positives (TP):** περιπτώσεις όπου το σύστημα εντόπισε σωστά ευαίσθητα δεδομένα.
- **True Negative (TN):** περιπτώσεις όπου το σύστημα δεν εντόπισε ευαίσθητα δεδομένα που πράγματι δεν ήταν ευαίσθητα.
- **False Positives (FP):** περιπτώσεις όπου το σύστημα αναγνώρισε δεδομένα ως ευαίσθητα ενώ δεν ήταν.
- **False Negatives (FN):** περιπτώσεις όπου υπήρχαν ευαίσθητα δεδομένα αλλά δεν ανιχνεύθηκαν.

Οι δείκτες υπολογίζονται ως εξής:

Precision (Ακρίβεια): μετρά το ποσοστό των σωστών θετικών ευρημάτων μεταξύ όλων των θετικών που ανέφερε το σύστημα.

- Precision=TP/(TP+FP) [111]

Recall (Ανάκληση): μετρά το ποσοστό των πραγματικών ευαίσθητων δεδομένων που εντόπισε το σύστημα.

- Recall=TP/(TP+FN) [111]

F1-score: ο αρμονικός μέσος των Precision και Recall, ώστε να αποτυπώνεται η συνολική αποτελεσματικότητα.

- F1= 2 × (Precision × Recall)/(Precision+Recall) [112]

(β) Δείκτες ταχύτητας

- **Ελάχιστος Χρόνος Εκτέλεσης (min):** ο μικρότερος χρόνος ολοκλήρωσης μιας λειτουργίας.

- **Μέγιστος Χρόνος Εκτέλεσης (max):** ο μεγαλύτερος χρόνος ολοκλήρωσης μιας λειτουργίας (αιχμή).

- **Μέσος Χρόνος Εκτέλεσης (avg):** ο μέσος όρος όλων των χρόνων εκτέλεσης για μια λειτουργία (ms).

Με βάση τους παραπάνω δείκτες πραγματοποιήθηκαν οι μετρήσεις για την αξιολόγηση της ταχύτητας του συστήματος.

6.3.2 Αξιολόγηση ακρίβειας αναγνώρισης ευαίσθητων δεδομένων συνολικά.

Ο παρακάτω πίνακας συνοψίζει **συνολικά** (Πινακάς 24) τα αποτελέσματα σε όλα τα δείγματα και για όλες τις κατηγορίες μαζί. Ο επόμενος πίνακας παρέχει πάλι αποτελέσματα ακρίβειας αλλά **ανά κατηγορία** (Πίνακας 25).

Πίνακας 25. Confusion Matrix

Πραγματικό / Προβλεπόμενο	**Ευαίσθητο (Predicted Sensitive)**	**Μη Ευαίσθητο (Predicted Non-Sensitive)**
Ευαίσθητο (Actual Sensitive)	**TP = 37**	**FN = 2**
Μη Ευαίσθητο (Actual Non-Sensitive)	**FP = 3**	**TN = 10**

Η συνολική αξιολόγηση βασίστηκε στα αποτελέσματα του παραπάνω πίνακα σύγχυσης, από τον οποίο προκύπτουν οι βασικοί δείκτες απόδοσης του συστήματος:

- **Precision (Ακρίβεια):**
  Precision=0.93. Δείχνει το ποσοστό των σωστών θετικών ευρημάτων σε σχέση με όλα τα θετικά που εντόπισε το σύστημα. Το υψηλό 0.93 σημαίνει ότι το eMailSec παράγει ελάχιστα ψευδώς θετικά αποτελέσματα.

- **Recall (Ανάκληση):**
  Recall=0.95. Μετρά την ικανότητα του συστήματος να εντοπίζει όλα τα πραγματικά ευαίσθητα δεδομένα. Η τιμή 0.95 δείχνει ότι ελάχιστες περιπτώσεις ευαίσθητων

δεδομένων δεν εντοπίστηκαν.

- **F1-score:**
  F1=0.94. Αποτελεί τον αρμονικό μέσο των δύο προηγούμενων δεικτών, παρέχοντας μια συνολική εικόνα ισορροπίας ανάμεσα στην ακρίβεια και την πληρότητα.

Ερμηνεία Αποτελεσμάτων

Το σύστημα eMailSec παρουσιάζει πολύ υψηλή ικανότητα αναγνώρισης ευαίσθητων δεδομένων, με ελάχιστα σφάλματα FP (false positives) και FN (false negatives). Η συνολική επίδοση (F1 = 0.94) αποτυπώνει έναν αξιόπιστο και αποδοτικό αλγόριθμο, ικανό να εντοπίζει τα περισσότερα ευαίσθητα δεδομένα με υψηλή ακρίβεια και συνέπεια.

Ωστόσο, η τιμή αυτή πρέπει να ερμηνευθεί με προσοχή. Το αποτέλεσμα προέρχεται από ελεγχόμενο σύνολο δεδομένων (golden set), όπου τα δείγματα είναι σαφώς καθορισμένα και αντιπροσωπεύουν συγκεκριμένες μορφές ευαίσθητων πληροφοριών. Σε πραγματικές συνθήκες χρήσης, όπου τα δεδομένα είναι πιο ανομοιογενή και απρόβλεπτα, το F1 αναμένεται να είναι χαμηλότερο, καθώς αυξάνονται οι πιθανότητες για λανθασμένες ή αμφίσημες ανιχνεύσεις.

Ακόμη και σε εμπορικά προϊόντα DLP, οι αντίστοιχοι δείκτες F1 συνήθως κυμαίνονται μεταξύ 0.75 και 0.88, ανάλογα με την πολυπλοκότητα του περιβάλλοντος και τη φύση των δεδομένων. Συνεπώς, η επίδοση 0.94 αποτελεί μια πολύ ενθαρρυντική πρώτη ένδειξη που δείχνει ότι το σύστημα θα μπορούσε, υπό ρεαλιστικές συνθήκες, να παράγει αρκετά καλά αποτελέσματα και να σταθεί επαρκώς σε πραγματικά σενάρια χρήσης.

6.3.3 Αξιολόγηση ακρίβειας αναγνώρισης ευαίσθητων δεδομένων ανα κατηγορία .

Παρακάτω εμφανίζονται τα αποτελέσματα που λήφθηκαν από το run (golden set = 52):

Πίνακας 26. Αξιολόγηση αναγνώρισης ευαιίσθητων δεδομένων.

Κατηγορία	**TP**	**FP**	**FN**	**Precision**	**Recall**	**F1**	**Σχόλια**
Email addresses	10	0	0	1.00	1.00	1.00	Υψηλή ακρίβεια
ΑΦΜ/ΑΜΚΑ	11	3	0	0.79	1.00	0.88	Ορισμένα FP
Τηλέφωνα	11	0	1	1.00	0.92	0.96	Edge case μορφοποίησης → 1 FN
IBAN / Οικονομικά δεδομένα	5	0	1	1.00	0.83	0.91	Χάθηκε case λόγω ιδιαίτερης μορφοποίησης IBAN (`GR12 3456.7890.1234.5678.90 12.345`)

Επεξήγηση αποτελεσμάτων

- **Διευθύνσεις Email**: Το σύστημα πέτυχε **τέλεια ανίχνευση** (Precision = 1.00, Recall = 1.00). Αυτό σημαίνει ότι όλα τα έγκυρα email εντοπίστηκαν σωστά χωρίς καμία ψευδή ανίχνευση.

- **ΑΦΜ/ΑΜΚΑ**: Παρατηρείται **υψηλό Recall (1.00)**, δηλαδή εντοπίστηκαν όλα τα έγκυρα παραδείγματα, αλλά και κάποια ψευδώς θετικά (Precision = 0.79). Αυτό δείχνει ότι η προσθήκη validators (π.χ. έλεγχος checksum για ΑΦΜ, έγκυρη ημερομηνία για ΑΜΚΑ) βελτίωσε σημαντικά την ακρίβεια σε σχέση με την αποκλειστική χρήση regex, μειώνοντας τα FP σε χαμηλά επίπεδα. (βλ. Ενότητα 4.4.6)

- **Τηλέφωνα**: Το Precision είναι **τέλειο (1.00)** και το Recall **πολύ υψηλό (0.92)**, με μόλις ένα FN σε edge case μορφοποίησης.Το μοναδικό False Negative προήλθε από δείγμα με ασυνήθιστη μορφοποίηση αριθμού κινητού ("Τηλ: 698-123-4567"), όπου οι παύλες δεν καλύπτονταν από το τρέχον regex μοτίβο. Αυτό δείχνει ότι η αναγνώριση τηλεφώνων είναι αξιόπιστη, χωρίς να δημιουργούνται ψευδείς συναγερμοί.

- **IBAN/Οικονομικά δεδομένα**: Εμφανίζει **τέλειο Precision (1.00)** και Recall **0.83**, δηλαδή δεν εντοπίζονται λάθος IBAN, αλλά χάνεται μία περίπτωση λόγω μορφοποίησης ("GR12 3456.7890.1234.5678.9012.345"). Αυτό μπορεί να διορθωθεί με περαιτέρω βελτιώσεις στον parser (π.χ. αφαίρεση τελειών/παρενθέσεων).

Συνολικά, τα αποτελέσματα δείχνουν ότι το σύστημα είναι **ιδιαίτερα αξιόπιστο στην ανίχνευση email και τηλεφώνων**, ενώ για ΑΦΜ/ΑΜΚΑ και IBAN απαιτούνται μικρές βελτιώσεις στους validators ώστε να περιοριστούν τα false positives και να αυξηθεί το recall σε edge cases. Το γεγονός ότι όλα τα F1-scores (per grooup) είναι >0.85 αποδεικνύει την **αποτελεσματικότητα της υλοποίησης** και την πρακτική χρησιμότητά της για πρόληψη διαρροής δεδομένων.

Σημείωση: Στον πίνακα ανά κατηγορία δεν περιλαμβάνεται η τιμή True Negative (TN), καθώς η αξιολόγηση εστιάζει αποκλειστικά στην ανίχνευση ευαίσθητων δεδομένων. Τα TN αντιστοιχούν σε περιπτώσεις όπου δεν υπάρχουν ευαίσθητα δεδομένα και το σύστημα δεν εντόπισε κανένα κάτι που, αν και σημαντικό για τη συνολική ακρίβεια, δεν συνεισφέρει ουσιαστικά στην ποιοτική ανάλυση της ικανότητας αναγνώρισης ανά κατηγορία ευαίσθητης πληροφορίας.

6.3.4 Αξιολόγηση απόδοσης και χρόνου απόκρισης λειτουργιών.

Για την αξιολόγηση της αποδοτικότητας του προσθέτου πραγματοποιήθηκαν μετρήσεις χρόνου εκτέλεσης σε ένα σύνολο βασικών λειτουργιών. Στόχος ήταν να καταγραφεί ο χρόνος απόκρισης κατά την κανονική χρήση, ώστε να εκτιμηθεί η εμπειρία του τελικού χρήστη και η σταθερότητα της λύσης. Οι μετρήσεις προέρχονται από πραγματικές εκτελέσεις στο περιβάλλον του Gmail και, παρότι ενδέχεται να επηρεάζονται από εξωτερικούς παράγοντες (π.χ. φόρτο συστήματος ή μέγεθος δεδομένων), παρέχουν ένα αντιπροσωπευτικό δείγμα για τη συνολική συμπεριφορά του συστήματος.

Η αξιολόγηση απόδοσης και χρόνου περιέλαβε δύο επιμέρους ομάδες μετρήσεων:

(α) χρόνους εκτέλεσης των βασικών λειτουργιών του προσθέτου (π.χ. φόρτωση UI, σάρωση ευαίσθητου περιεχομένου, έλεγχος παραληπτών, διαχείριση επαφών), και

β) την ταχύτητα απόκρισης των λειτουργιών κρυπτογράφησης και αποκρυπτογράφησης, οι οποίες εξετάστηκαν ξεχωριστά λόγω της εξάρτησής τους από το μέγεθος του μηνύματος και το περιβάλλον εκτέλεσης στο backend.

(α)Ταχύτητα λειτουργιών

Πίνακας 27. Ταχύτητα εκτέλεσης βασικών λειτουργιών

Λειτουργία	**Δοκιμές**	**Ελάχιστος Χρόνος (ms)**	**Μέγιστος Χρόνος (ms)**	**Μέσος Χρόνος (ms)**	**Σχόλια**
onHomepage	20	1.770 s	2.913 s	~2.3 s	Εκτέλεση 1.7–2.9 s, μέση τιμή ~2.3 s, αποδεκτή απόδοση.

Sensitive Data Scan	20	1.001 s	5.357 s	~2.2 s	Σταθερή εκτέλεση 1–3 s, μεμονωμένες αιχμές έως 5 s, λόγω καθυστέρησης απόκρισης του GmailAPI (Ελέγχθηκαν 7 drafts μεγέθους ~1 KB έως 100 KB, εκ των οποίων τα 4 περιείχαν ευαίσθητα δεδομένα)
menuContact	20	0.892 s	1.587 s	~1.3 s	Σταθερή εκτέλεση <1.6 s, χωρίς ιδιαίτερες αιχμές
showKeyManagementCard	20	1.178 s	4.742 s	~2.5 s	Καλή απόδοση στις περισσότερες εκτελέσεις, με μία αιχμή στα 4.7 s
Compose menu	20	0.615 s	5.928 s	~1.5 s	Οι περισσότερες εκτελέσεις <1.2 s, μερικές αιχμές 3–6 s

verifySignatureHandler	20	1.082 s	5.757 s	~2.1 s	Οι περισσότερες εκτελέσεις ~1–1.5 s, μεμονωμένη αιχμή στα 5.7 s
onOpenMailpage	20	0.779 s	0.962 s	~0.9 s	Σταθερή εκτέλεση, όλες κάτω από 1 s
onCheckMessageLinks	20	0.914 s	4.609 s	~2.5 s	Οι περισσότερες εκτελέσεις κάτω από 2 s, με μία αιχμή στα 4.6 s (Μεμονωμένη αιχμή εκτέλεσης – όχι επαναλαμβανόμενη πιθανώς λόγω runtime καθυστέρησης)
onCheckDangerousAttachments	20	0.695 s	26.367 s	~6.1 s	Σταθερές εκτελέσεις ~1 s, μεμονωμένη αιχμή στα 26 s που επηρεάζει τον μέσο όρο

Οι καταγεγραμμένοι χρόνοι εκτέλεσης αποτελούν ενδεικτικό δείγμα της λειτουργίας του προσθέτου σε πραγματικές συνθήκες χρήσης. Η πλειονότητα των μετρήσεων κυμαίνεται σε αποδεκτά επίπεδα (κάτω των 3 δευτερολέπτων), γεγονός που επιβεβαιώνει τη λειτουργική καταλληλότητα και τη χρηστική ανταπόκριση του συστήματος. Παρά την ύπαρξη μεμονωμένων ακραίων τιμών, όπως στην περίπτωση του **onCheckDangerousAttachments**, οι αποκλίσεις αυτές μπορούν να αποδοθούν σε εξωτερικούς παράγοντες (π.χ. στιγμιαίο φόρτο συστήματος, περιορισμοί πλατφόρμας) και δεν αλλοιώνουν τη συνολική εικόνα αξιοπιστίας. Συνεπώς, τα αποτελέσματα υποδεικνύουν ότι το σύστημα επιτυγχάνει ικανοποιητική σταθερότητα και ταχύτητα απόκρισης, με περιθώρια περαιτέρω βελτιστοποίησης σε σενάρια όπου παρατηρούνται αιχμές.

(β)Ταχύτητα απόκρισης λειτουργιών κρυπτογράφησης και αποκρυπτογράφησης

Η αξιολόγηση της ταχύτητας απόκρισης των λειτουργιών **κρυπτογράφησης και αποκρυπτογράφησης** πραγματοποιείται ξεχωριστά από τις βασικές λειτουργίες του προσθέτου, καθώς η απόδοσή τους εξαρτάται σε μεγάλο βαθμό από το **μέγεθος του μηνύματος**[12]. Για τον σκοπό αυτό σχεδιάστηκε δοκιμή με τρία διαφορετικά σενάρια, όπου χρησιμοποιούνται μηνύματα μικρού, μεσαίου και μεγάλου μεγέθους. Σε κάθε περίπτωση μετρήθηκε ο χρόνος που απαιτείται για την διαδικασία κρυπτογράφησης (encrypt) και για την αντίστοιχη διαδικασία αποκρυπτογράφησης (decrypt), ώστε να εξαχθεί μια πιο ολοκληρωμένη εικόνα της συμπεριφοράς του συστήματος σε συνθήκες διαφορετικού φόρτου δεδομένων. Τα αποτελέσματα συνοψίζονται στον ακόλουθο πίνακα.

Πίνακας 28. Μέτρηση ταχύτητας κρυπτογράφησης και αποκρυπτογράφηση.

Μέγεθος Μηνύματος	Μέσος Χρόνος Encrypt (ms)	Μέσος Χρόνος Decrypt (ms)	Σχόλια
1 KB (Μικρό)	1.255 s	0.597 s	Πολύ γρήγορη εκτέλεση, πρακτικά αμελητέος χρόνος για τον χρήστη
100 KB (Μεσαίο)	1.496 s	0.656 s	Σταθερή απόδοση, μικρή αύξηση χρόνου σε σχέση με το μικρό μήνυμα

[12]*Για τον υπολογισμό του μεγέθους των email που χρησιμοποιήθηκαν στην αξιολόγηση, αξιοποιήθηκε το εργαλείο* ***Mailmeteor Email Size Tool****.*

500 KB (Μεγάλο)	1.825 s	0.746 s	Ομαλή κλιμάκωση, χρόνοι παραμένουν <2 s, αποδεκτή εμπειρία και σε μεγαλύτερα μεγέθη
~1 MB (Πολύ Μεγάλο)	7.993s	4.678s	Σε αρκετές δοκιμές εντοπίστηκε ότι η λειτουργία κρυπτογράφησης απέτυχε σιωπηλά (no explicit error), ενώ στο decrypt φάνηκε σαν «επιτυχή» αλλα επιστράφηκε χωρίς κάποιο περιεχόμενο.

Οι μετρήσεις δείχνουν ότι οι χρόνοι κρυπτογράφησης και αποκρυπτογράφησης παραμένουν σε χαμηλά επίπεδα για μικρά και μεσαία μηνύματα, με σταθερή συμπεριφορά και ομαλή κλιμάκωση (<2 δευτερόλεπτα κατά μέσο όρο). Ωστόσο, σε περιπτώσεις μεγάλων payloads (κοντά στο 1 MB) παρατηρήθηκαν αυξημένοι χρόνοι απόκρισης, συχνά άνω των 8 δευτερολέπτων, ενώ σε αιτήματα που υπερέβαιναν το όριο του 1 MB η λειτουργία δεν ολοκληρωνόταν επιτυχώς, με αποτυχία σε σχεδόν όλες τις εκτελέσεις. Το φαινόμενο αυτό δεν οφείλεται στον ίδιο τον αλγόριθμο κρυπτογράφησης, αλλά σε περιορισμούς του περιβάλλοντος εκτέλεσης του Node.js server στο Render, όπως τα όρια payload, request size και διαθέσιμης μνήμης. Αξίζει να σημειωθεί ότι η εφαρμογή φιλοξενείται στο δωρεάν επίπεδο (free tier) της πλατφόρμας Render, το οποίο επιβάλλει αυστηρούς περιορισμούς σε υπολογιστικούς πόρους και μέγεθος αιτημάτων επομένως, επομένως τα φαινόμενα αυτά δεν σχετίζονται με την ίδια τη λειτουργικότητα του συστήματος αλλά με το περιβάλλον εκτέλεσης. Σε αντίστοιχες επαγγελματικές λύσεις, η διαχείριση τέτοιων δεδομένων μεταφέρεται σε εξειδικευμένες server-side υποδομές με δυνατότητες streaming και βελτιστοποιημένης διαχείρισης μεγάλων όγκων πληροφορίας.

Στο πλαίσιο της παρούσας εργασίας, πραγματοποιήθηκαν βελτιστοποιήσεις στον κώδικα και στις ρυθμίσεις του backend, που οδήγησαν σε σημαντική μείωση του όγκου των δεδομένων που αποστέλλονται προς κρυπτογράφηση — για παράδειγμα, αποστέλλεται μόνο το καθαρό κείμενο (plain text) του email, χωρίς μορφοποίηση ή HTML markup. Η προσέγγιση αυτή βελτίωσε αισθητά την απόδοση και περιόρισε τα σφάλματα σε μεγάλα payloads, χωρίς ωστόσο να εξαλείφει πλήρως το πρόβλημα σε ακραίες περιπτώσεις (άνω του 1 MB).

6.4 Ποιοτική Αποτίμηση

Η ποιοτική αξιολόγηση εστιάζει στη συνολική εμπειρία χρήσης του προσθέτου, όπως αυτή προκύπτει κατά την αλληλεπίδραση με το περιβάλλον του Gmail. Στο πλαίσιο της παρούσας εργασίας δεν πραγματοποιήθηκε οργανωμένη μελέτη χρηστών (user study). Συνεπώς, η αξιολόγηση βασίστηκε σε **χειροκίνητες δοκιμές (manual testing)** που εκτελέστηκαν από τον ίδιο τον δημιουργό, ακολουθώντας τα σενάρια χρήσης της Ενότητας 5.2 .

Με βάση μια **πρώτη και βασική ανάλυση των αποτελεσμάτων που πραγματοποιήθηκε από τον δημιουργό του συστήματος**, προκύπτουν αρχικά συμπεράσματα σχετικά με τη λειτουργικότητα, την ευχρηστία και τη συνοχή του προσθέτου, τα οποία μπορούν να αποτελέσουν σημείο εκκίνησης για μελλοντική αξιολόγηση με ανεξάρτητους χρήστες.

Κατά τη διαδικασία αυτή προέκυψαν τα εξής συμπεράσματα:

- **Κατανοητότητα προειδοποιήσεων**: Οι ειδοποιήσεις εμφανίζονται με σαφήνεια και δομημένο τρόπο, διευκολύνοντας τον χρήστη να αντιληφθεί την αιτία του προβλήματος.
- **Ευκολία χρήσης**: η εκτέλεση ενεργειών (π.χ. σάρωση, κρυπτογράφηση, διαχείριση παραληπτών) εμφανίζεται άμεση και διαισθητική, χωρίς να απαιτείται πρόσθετη εκπαίδευση. Ωστόσο, η παρατήρηση αυτή προκύπτει από την αρχική φάση αξιολόγησης και θα πρέπει να επιβεβαιωθεί με δοκιμές σε διαφορετικούς χρήστες που διαθέτουν βασική εμπειρία στη χρήση του Gmail.
- **Συνοχή με Gmail UI**: Το πρόσθετο έχει σχεδιαστεί με τρόπο που ευθυγραμμίζεται πλήρως με τη δομή, τα χρώματα και τη ροή εργασίας του Gmail. Οι κάρτες, τα κουμπιά και οι ειδοποιήσεις ακολουθούν το ίδιο οπτικό και λειτουργικό πρότυπο με τις εγγενείς διεπαφές του Gmail, επιτρέποντας στον χρήστη να αλληλεπιδρά με το πρόσθετο χωρίς να χρειάζεται να μάθει νέα πρότυπα ή διαδικασίες. Με αυτόν τον τρόπο, ο χρόνος εξοικείωσης μειώνεται σημαντικά και η μετάβαση μεταξύ των λειτουργιών γίνεται ομαλά και φυσικά.
- **Αποτελεσματικότητα στην πράξη**: Κατά την εκτέλεση των σεναρίων χρήσης επιβεβαιώθηκε ότι το πρόσθετο συμβάλλει ουσιαστικά στην πρόληψη σφαλμάτων (π.χ. αποστολή σε λάθος παραλήπτες ή διαρροή δεδομένων), χωρίς να επιβαρύνει τη ροή εργασίας.

Τα παραπάνω δείχνουν ότι το πρόσθετο δεν περιορίζεται μόνο σε τεχνική ακρίβεια αλλά προσφέρει και θετική εμπειρία χρήσης, γεγονός που αποτελεί κρίσιμο παράγοντα για την αποδοχή και την πρακτική αξιοποίησή του.

6.5 Συνολική Αποτίμηση

Συνδυάζοντας τα ποσοτικά και ποιοτικά αποτελέσματα, καθίσταται σαφές ότι το πρόσθετο για το Gmail ανταποκρίνεται στον κεντρικό του στόχο: την ενίσχυση της ασφάλειας της ηλεκτρονικής αλληλογραφίας και τη μείωση του κινδύνου διαρροής ευαίσθητων δεδομένων. Σε τεχνικό επίπεδο, η απόδοση στην αναγνώριση διευθύνσεων email και τηλεφωνικών αριθμών είναι σχεδόν άριστη, με μηδενικά ή ελάχιστα σφάλματα. Στις κατηγορίες ΑΦΜ/ΑΜΚΑ και IBAN, αν και τα αποτελέσματα είναι θετικά, παρατηρούνται περιθώρια βελτίωσης που μπορούν να επιτευχθούν με την ενσωμάτωση πιο εξελιγμένων μηχανισμών ελέγχου εγκυρότητας (validators) και με την ανάπτυξη πιο ευέλικτων parsers ικανών να χειρίζονται edge cases.

Από την πλευρά της χρηστικότητας, οι δοκιμές έδειξαν ότι το πρόσθετο ενσωματώνεται ομαλά στη ροή εργασίας του Gmail, χωρίς να επιβαρύνει τη διαδικασία σύνταξης και αποστολής email. Οι προειδοποιήσεις εμφανίζονται με τρόπο κατανοητό και η παρεχόμενη λειτουργικότητα (π.χ. σάρωση περιεχομένου, έλεγχος παραληπτών, κρυπτογράφηση) προσφέρει άμεση υποστήριξη στον χρήστη, ενισχύοντας την εμπιστοσύνη του προς το σύστημα.

Παράλληλα, οι μετρήσεις χρόνου απόκρισης σε βασικές λειτουργίες έδειξαν ότι η πλειονότητα των ενεργειών ολοκληρώνεται σε λιγότερο από 3 δευτερόλεπτα, με ομαλή και προβλέψιμη κλιμάκωση ακόμη και σε πιο απαιτητικά σενάρια (π.χ. κρυπτογράφηση/αποκρυπτογράφηση μεσαίου μεγέθους μηνυμάτων). Οι όποιες αιχμές σε ειδικές περιπτώσεις μπορούν να αποδοθούν σε περιορισμούς της πλατφόρμας ή σε πολύ μεγάλα payloads (σε αιτήματα που υπερέβαιναν το 1 MB), χωρίς να αλλοιώνεται η συνολική εικόνα σταθερότητας και αποδοτικότητας. Εξαιτίας των παραπάνω περιορισμών και του σκοπού της παρούσας μελέτης, δεν κρίθηκε αναγκαία η εκτέλεση δοκιμών με ιδιαίτερα μεγάλα payloads. Επιπλέον, η εκτέλεση των δοκιμών πραγματοποιήθηκε στο δωρεάν περιβάλλον (free tier) της πλατφόρμας Render, το οποίο διαθέτει περιορισμούς σε μνήμη και μέγεθος αιτημάτων· συνεπώς, η ένταξη δοκιμών με payloads πολλαπλάσιου μεγέθους δεν θα παρείχε ουσιαστικά ή συγκρίσιμα αποτελέσματα. Για τους παραπάνω λόγους, η αξιολόγηση επικεντρώθηκε σε σενάρια χρήσης που αντιστοιχούν σε συγκεκριμένα (βλ. Πίνακα 27) μεγέθη μηνυμάτων ηλεκτρονικής αλληλογραφίας.

Η συνολική εικόνα αποτυπώνεται σε δείκτες απόδοσης με F1-scores άνω του 0.85, ενώ ο συνολικός πίνακας σύγχυσης έδειξε F1 = 0.94. Επιπλέον, η ανάλυση ανά κατηγορία ευαίσθητων δεδομένων έδειξε ότι όλοι οι επιμέρους δείκτες F1 υπερέβησαν το 0.85. Το σύνολο αυτών των αποτελεσμάτων αποτελεί ένα πρώτο θετικό δείγμα καλής λειτουργίας του συστήματος, αποδεικνύοντας ότι η προσέγγιση είναι τεχνικά ορθή και αποτελεσματική. Παράλληλα, αναγνωρίζεται ότι τα ποσοστά αυτά ενδέχεται να διαφοροποιηθούν σε πιο ρεαλιστικές συνθήκες ή με μεγαλύτερη ποικιλία δεδομένων, καθώς το πραγματικό περιβάλλον χρήσης παρουσιάζει αυξημένη πολυπλοκότητα.

Συμπερασματικά, η αποτίμηση δείχνει ότι το σύστημα μπορεί να χρησιμοποιηθεί με επιτυχία σε πραγματικά περιβάλλοντα, συμβάλλοντας ουσιαστικά στη μείωση του κινδύνου διαρροής δεδομένων.

7

Συμπεράσματα και Μελλοντική Εργασία

7.1 Σύνοψη Ευρημάτων και Αντίκτυπος

Η ανάπτυξη του προσθέτου για το Gmail ανέδειξε τη δυνατότητα ενίσχυσης της ασφάλειας της ηλεκτρονικής αλληλογραφίας μέσα από ένα εύχρηστο και επεκτάσιμο εργαλείο. Το σύστημα που υλοποιήθηκε παρείχε λειτουργίες εντοπισμού ευαίσθητων δεδομένων, ειδοποίησης του χρήστη για πιθανούς κινδύνους και παροχής ενεργειών για την αντιμετώπισή τους, όπως κρυπτογράφηση, διαχείριση παραληπτών και αποκλεισμό μη αξιόπιστων αποστολέων.

Τα ευρήματα από την υλοποίηση δείχνουν ότι το πρόσθετο συμβάλλει ουσιαστικά στη μείωση του κινδύνου διαρροής προσωπικών και εμπιστευτικών πληροφοριών, καθώς προσφέρει προληπτική προστασία τη στιγμή της σύνταξης ενός μηνύματος. Παράλληλα, η ενσωμάτωση μηχανισμών κρυπτογράφησης και διαχείρισης κλειδιών επιτρέπει στους χρήστες να διασφαλίσουν την εμπιστευτικότητα των επικοινωνιών τους με έναν τρόπο πιο άμεσο και απλό σε σχέση με κλασικές λύσεις κρυπτογράφησης.

Συνολικά, το πρόσθετο αποδεικνύει ότι μια στοχευμένη προσέγγιση σε επίπεδο πελάτη ηλεκτρονικής αλληλογραφίας μπορεί να ενισχύσει την ασφάλεια, να βελτιώσει την εμπιστοσύνη των χρηστών στη χρήση του email ως εργαλείο επικοινωνίας και να μειώσει σημαντικά την πιθανότητα ακούσιας ή σκόπιμης διαρροής δεδομένων.

Πέρα από τον γενικό αντίκτυπο, το εργαλείο που αναπτύχθηκε στο πλαίσιο της παρούσας εργασίας απέδειξε την πρακτική του αξία, καθώς προσέφερε στον χρήστη δυνατότητες που μέχρι σήμερα δεν ήταν άμεσα διαθέσιμες στο Gmail: έγκαιρη ανίχνευση ευαίσθητων δεδομένων, αξιολόγηση κινδύνου (risk score), ενσωματωμένες επιλογές κρυπτογράφησης, καθώς και διαχείριση επαφών με αποθήκευση και επαλήθευση δημόσιων κλειδιών. Η συνεισφορά αυτή

δείχνει ότι είναι εφικτό να παραχθεί ένα αποδοτικό, φιλικό προς τον χρήστη και τεχνολογικά καινοτόμο εργαλείο που ενισχύει ουσιαστικά την προστασία της ηλεκτρονικής αλληλογραφίας.

7.2 Προτάσεις για Μελλοντικές Βελτιώσεις

Παρά την ολοκληρωμένη λειτουργικότητα που επιτεύχθηκε, υπάρχουν στοχευμένες κατευθύνσεις που μπορούν να ενισχύσουν περαιτέρω την ακρίβεια, τη διαλειτουργικότητα και την ευχρηστία του προσθέτου:

- **Ενσωμάτωση Μηχανικής Μάθησης με αξιοποίηση αναφορών χρηστών**: Πέρα από κανόνες/regex, μπορούν να αξιοποιηθούν μοντέλα Μηχανικής Μάθησης (Μ.Μ.) που εκπαιδεύονται προοδευτικά από «σήματα» προέλευσης χρήστη (π.χ. αναφορές/καταγγελίες για ύποπτο περιεχόμενο ή λανθασμένες ανιχνεύσεις). Με αυτόν τον τρόπο, το σύστημα «μαθαίνει» από πραγματικές περιπτώσεις και βελτιώνει διαρκώς την ταξινόμηση ευαίσθητων δεδομένων και την ανίχνευση κοινωνικής μηχανικής, μειώνοντας ψευδώς θετικά/αρνητικά. Η συλλογή σημάτων θα πρέπει να γίνεται με ρητή συγκατάθεση και σεβασμό στην ιδιωτικότητα.

- **Λειτουργία σε οποιονδήποτε email client:** Η αρχιτεκτονική μπορεί να επεκταθεί ώστε το εργαλείο να λειτουργεί ως ανεξάρτητο middleware (π.χ. μέσω add-in/extension ή gateway), υποστηρίζοντας Outlook, Thunderbird κ.ά., με κοινό πυρήνα κανόνων/μοντέλων και λεπτά προσαρμοσμένους προσαρμογείς (adapters) για κάθε πλατφόρμα. Η προσέγγιση αυτή διευκολύνεται από τη δομή του συστήματος, η οποία εν μέρει ακολουθεί αρχές εξαγωνικής αρχιτεκτονικής, επιτρέποντας την ευκολότερη απομόνωση και επαναχρησιμοποίηση του βασικού πυρήνα λογικής ανεξάρτητα από το περιβάλλον εκτέλεσης.

- **Οριζόντια ενσωμάτωση σε όλη τη σουίτα της Google**: Πέρα από το Gmail, οι δυνατότητες ανίχνευσης/προστασίας μπορούν να φανούν χρήσιμες σε **Google Docs/Sheets/Slides** (π.χ. προειδοποίηση πριν τον διαμοιρασμό εγγράφου με ευαίσθητα πεδία), **Drive** (σάρωση πριν το share ή τη δημοσιοποίηση συνδέσμου), καθώς και **Chat/Meet** (π.χ. επισήμανση διαμοιραζόμενων δεδομένων σε πραγματικό χρόνο). Έτσι δημιουργείται ενιαίο «στρώμα» πρόληψης διαρροής σε όλα τα σημεία ροής πληροφορίας.

- **Βελτίωση ευχρηστίας και διεπαφής**: Η βελτίωση της ευχρηστίας και της διεπαφής μπορεί να επιτευχθεί με πιο άμεση οπτικοποίηση των κινδύνων, την παροχή έξυπνων προτάσεων ενεργειών και την απλούστευση της διαχείρισης κλειδιών. Συγκεκριμένα, η προσθήκη **εικονιδίων κινδύνου (risk badges)** και **επιπέδων ευαισθησίας** δίπλα σε στοιχεία, όπως οι παραλήπτες ή το θέμα του μηνύματος, θα επιτρέπει στον χρήστη να αντιλαμβάνεται αμέσως τον βαθμό επικινδυνότητας κάθε email. Παράλληλα, η εισαγωγή **έξυπνων προτάσεων ενεργειών** (π.χ. «Κρυπτογράφησε το μήνυμα και αφαίρεσε μη αξιόπιστους παραλήπτες») θα καθοδηγεί τον χρήστη στην άμεση λήψη σωστών αποφάσεων χωρίς τεχνική εμπλοκή. Τέλος, η **απλούστερη διαχείριση κλειδιών** μέσω

καθοδηγούμενων βημάτων (*guided flows*) και αυτόματης επαλήθευσης υπογραφών θα βελτιώσει σημαντικά την εμπειρία χρήσης, καθιστώντας τη διαδικασία δημιουργίας, ανταλλαγής και επιβεβαίωσης PGP κλειδιών πιο εύκολη και αξιόπιστη.

- **Αυτοματοποιημένη ανταλλαγή/επαλήθευση κλειδιών**: Διασύνδεση με keyservers, αυτόματη ανάκτηση/ανανεώσεις, και καθοδηγούμενη επαλήθευση (detached signatures) ώστε να μειωθεί η χειροκίνητη τριβή και να αυξηθεί η υιοθέτηση της κρυπτογράφησης.

- **Προηγμένη ανάλυση κινδύνου**: Εμπλουτισμός του risk score με ιστορικά μοτίβα επικοινωνίας, συχνότητα/συμφραζόμενα ευαίσθητων όρων και δυναμικές πολιτικές με βάση περιεχόμενο και παραλήπτες.

- **Υιοθέτηση Υβριδικής Κρυπτογράφησης:** Μια ακόμη κατεύθυνση βελτίωσης αφορά τη μετάβαση από αμιγώς ασύμμετρη σε υβριδική κρυπτογράφηση, η οποία αποτελεί πλέον τη βέλτιστη πρακτική στα σύγχρονα συστήματα ασφαλούς επικοινωνίας. Στην υβριδική προσέγγιση, η διαδικασία συνδυάζει ασύμμετρη κρυπτογράφηση για την ασφαλή ανταλλαγή ενός συμμετρικού κλειδιού και συμμετρική κρυπτογράφηση για το περιεχόμενο του μηνύματος όπου το συμμετρικό κλειδί παράγεται τυχαία και αλλάζει σε κάθε διαφορετικό μήνυμα προς αποστολή. Ουσιαστικά, παράγεται ένας ψηφιακός φάκελος αποτελούμενος από το κρυπτογραφημένο μήνυμα (βάσει συμμετρικού κλειδιού) και το κρυπτογραφημένο (με ασύμμετρο τρόπο) συμμετρικό κλειδί. Η χρήση αυτής της μεθόδου θα μπορούσε να βελτιώσει ουσιαστικά την ταχύτητα εκτέλεσης και τη συνολική αποδοτικότητα, ιδιαίτερα κατά την επεξεργασία μεγάλων μηνυμάτων, διατηρώντας το ίδιο επίπεδο ασφάλειας.

Η πρακτική αυτή θα ήταν ιδανική σε περιβάλλον cloud εκτέλεσης, όπου οι διαθέσιμοι πόροι είναι αυξημένοι και η απόδοση των λειτουργιών κρυπτογράφησης βελτιστοποιείται σημαντικά σε σχέση με περιορισμένα περιβάλλοντα, όπως το free-tier της πλατφόρμας Render. Επομένως, η ενσωμάτωση ενός υβριδικού μοντέλου κρυπτογράφησης θα ενίσχυε περαιτέρω τη σταθερότητα, επεκτασιμότητα και ταχύτητα του συστήματος, χωρίς συμβιβασμούς στην ασφάλεια.

Επιπλέον, από την ανάλυση της **Ικανοποίησης των Απαιτήσεων** (Ενότητα 4.5) προκύπτει ότι ορισμένες λειτουργίες δεν υλοποιήθηκαν πλήρως, αλλά θα μπορούσαν να αποτελέσουν αντικείμενο μελλοντικής επέκτασης και περαιτέρω ανάπτυξης, όπως οι εξής:

- **Επέκταση του μηχανισμού αναγνώρισης τύπων βάσει προτιμήσεων χρήστη (FR2):** Προτείνεται η προσθήκη δυνατοτήτων παραμετροποίησης των κανόνων ανίχνευσης, ώστε κάθε χρήστης ή οργανισμός να μπορεί να καθορίζει ποιοι τύποι δεδομένων θεωρούνται ευαίσθητοι. Μέσω ενός απλού περιβάλλοντος ρυθμίσεων, ο χρήστης θα μπορεί να ενεργοποιεί ή να απενεργοποιεί συγκεκριμένα μοτίβα (regex ή λέξεις-κλειδιά), προσφέροντας ευελιξία και προσαρμογή του μηχανισμού στις εκάστοτε ανάγκες.

- **Ανάπτυξη συστήματος ταξινόμησης συνημμένων κατά ιδιωτικότητα (FR3):** Μια μελλοντική επέκταση μπορεί να περιλαμβάνει αυτόματη αξιολόγηση των συνημμένων αρχείων και κατάταξή τους σε επίπεδα ευαισθησίας (π.χ. Δημόσιο, Εμπιστευτικό, Εσωτερικό). Η λειτουργία αυτή θα μπορούσε να βασίζεται σε περιεχόμενο, τύπο αρχείου ή παρουσία ευαίσθητων στοιχείων, παρέχοντας οπτική σήμανση και προειδοποίηση πριν την αποστολή.

Συνολικά, αυτές οι κατευθύνσεις μετατρέπουν το πρόσθετο από ένα ισχυρό εργαλείο προστασίας email σε μια **ενοποιημένη πλατφόρμα πρόληψης διαρροής** που μαθαίνει από τη χρήση, λειτουργεί σε πολλαπλούς clients και επεκτείνεται οριζόντια στη σουίτα της Google, ενισχύοντας ουσιαστικά την ασφάλεια χωρίς να θυσιάζει την εμπειρία χρήστη.

7.3 Προσωπική Εμπειρία και Αποκόμιση Γνώσεων

Η εκπόνηση της παρούσας διπλωματικής αποτέλεσε μια εμπειρία με ιδιαίτερη αξία, καθώς συνδύασε θεωρητική έρευνα και πρακτική ανάπτυξη σε ένα πραγματικό και σύνθετο πεδίο, όπως είναι η ασφάλεια της ηλεκτρονικής αλληλογραφίας. Μέσα από τη διαδικασία, αποκτήθηκαν γνώσεις που αφορούν τόσο τις αρχές της προστασίας δεδομένων και τα συστήματα πρόληψης διαρροής (DLPS), όσο και τις τεχνικές δεξιότητες που σχετίζονται με τον προγραμματισμό, τη σχεδίαση αρχιτεκτονικής και την ενσωμάτωση πολλαπλών τεχνολογιών.

Η ανάπτυξη του προσθέτου επέτρεψε την εμβάθυνση στη χρήση του **Google Apps Script** και τη δημιουργία διεπαφών με το **CardService**, την υλοποίηση μηχανισμών επικοινωνίας με **Node.js backend** για την κρυπτογράφηση/αποκρυπτογράφηση δεδομένων, καθώς και την εφαρμογή τεχνικών διαχείρισης κλειδιών. Η ανάγκη αντιμετώπισης πρακτικών προκλήσεων, όπως η διαχείριση drafts στο Gmail, η ανίχνευση ευαίσθητου περιεχομένου και η αλληλεπίδραση με εξωτερικές υπηρεσίες (π.χ. keyservers), συνέβαλε ουσιαστικά στην ανάπτυξη δεξιοτήτων επίλυσης προβλημάτων και προσαρμοστικότητας.

Πέρα από τις τεχνικές γνώσεις, η διαδικασία ανέδειξε και τη σημασία της **συστηματικής μεθοδολογίας ανάπτυξης**, καθώς και της σαφούς τεκμηρίωσης των λειτουργιών, ώστε το τελικό αποτέλεσμα να είναι κατανοητό, επεκτάσιμο και χρήσιμο. Επιπλέον, η σύνδεση της θεωρητικής ανάλυσης με την πρακτική εφαρμογή έδωσε την ευκαιρία να διαπιστωθεί πώς οι αρχές της ασφάλειας και της προστασίας προσωπικών δεδομένων μπορούν να μετατραπούν σε λειτουργικό λογισμικό.

Συνολικά, η εμπειρία από την εκπόνηση της διπλωματικής και ειδικότερα από την ανάπτυξη του προσθέτου συνέβαλε ουσιαστικά στην προσωπική και επαγγελματική εξέλιξη, ενισχύοντας δεξιότητες που αφορούν τόσο στην τεχνολογική εξειδίκευση όσο και στην ερευνητική προσέγγιση και κριτική σκέψη.

Βιβλιογραφία

[1] S. Alneyadi, E. Sithirasenan, and V. Muthukkumarasamy, "A survey on data leakage prevention systems," *J. Netw. Comput. Appl.*, vol. 62, pp. 137–152, Feb. 2016, doi: 10.1016/j.jnca.2016.01.008.

[2] V. R. Carvalho, R. Balasubramanyan, and W. W. Cohen, "Information Leaks and Suggestions: A Case Study using Mozilla Thunderbird".

[3] V. R. Carvalho and W. W. Cohen, "Preventing Information Leaks in Email," in *Proceedings of the 2007 SIAM International Conference on Data Mining*, Society for Industrial and Applied Mathematics, Apr. 2007, pp. 68–77. doi: 10.1137/1.9781611972771.7.

[4] K. A. Scarfone and P. M. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-94, 2007. doi: 10.6028/NIST.SP.800-94.

[5] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," *Comput. Hum. Behav. Rep.*, vol. 4, p. 100126, Aug. 2021, doi: 10.1016/j.chbr.2021.100126.

[6] N. Kumar, "Gmail Statistics (2025) – Market Share & Users Data," DemandSage. Accessed: Nov. 03, 2025. [Online]. Available: https://www.demandsage.com/gmail-statistics/

[7] "2024 Data Breach Investigations Report | Verizon." Accessed: Nov. 03, 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[8] "Build Google Workspace add-ons | Google for Developers." Accessed: Nov. 03, 2025. [Online]. Available: https://developers.google.com/workspace/add-ons/how-tos/building-workspace-addons

[9] H. N. Chua, J. S. Ooi, and A. Herbland, "The effects of different personal data categories on information privacy concern and disclosure," *Comput. Secur.*, vol. 110, p. 102453, Nov. 2021, doi: 10.1016/j.cose.2021.102453.

[10] "Art. 4 GDPR – Definitions," General Data Protection Regulation (GDPR). Accessed: Nov. 03, 2025. [Online]. Available: https://gdpr-info.eu/art-4-gdpr/

[11] M. Poddębniak, "Personally identifiable information: PII, non-PII & personal data," Piwik PRO. Accessed: Nov. 03, 2025. [Online]. Available: https://piwik.pro/blog/what-is-pii-personal-data/

[12] "What is special category data?" Accessed: Nov. 03, 2025. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/

[13] "ThymianidouM_2024.pdf." Accessed: Nov. 03, 2025. [Online]. Available: https://repo.lib.duth.gr/jspui/bitstream/123456789/19606/1/ThymianidouM_2024.pdf

[14] "MELETES_PANAGOPOULOU.indd." Accessed: Nov. 03, 2025. [Online]. Available: https://www.dpa.gr/sites/default/files/2019-12/meletes_panagopoulou.pdf

[15] "What To Know About Identity Theft," Consumer Advice. Accessed: Nov. 03, 2025. [Online]. Available: https://consumer.ftc.gov/articles/what-know-about-identity-theft

[16] "What Is a Data Breach?," Palo Alto Networks. Accessed: Nov. 03, 2025. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/data-breach

[17] "General Data Protection Regulation (GDPR) – Legal Text," General Data Protection Regulation (GDPR). Accessed: Nov. 03, 2025. [Online]. Available: https://gdpr-info.eu/

[18] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, vol. 119. 2016. Accessed: Nov. 03, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj

[19] U. S. G. A. Office, "Consumer Data: Increasing Use Poses Risks to Privacy | U.S. GAO." Accessed: Nov. 03, 2025. [Online]. Available: https://www.gao.gov/products/gao-22-106096
[20] "What is automated individual decision-making and profiling?" Accessed: Nov. 03, 2025. [Online]. Available: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/
[21] "De-Anonymization: What It is, How It Works, How it's Used," Investopedia. Accessed: Nov. 03, 2025. [Online]. Available: https://www.investopedia.com/terms/d/deanonymization.asp
[22] Sivan-Sevilla (Ido), Parham (Patrick), and McGuigan (Lee), "'Cookie-less' identification for/against privacy?" Accessed: Nov. 03, 2025. [Online]. Available: https://policyreview.info/articles/analysis/cookie-less-identification-foragainst-privacy
[23] "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices," Federal Trade Commission. Accessed: Nov. 03, 2025. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer
[24] R. LLP, "Data Minimization and Avoiding the Over-Retention of Personal Information," Redgrave LLP. Accessed: Nov. 03, 2025. [Online]. Available: https://www.redgravellp.com/publication/data-minimization-and-avoiding-over-retention-personal-information
[25] "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," Federal Trade Commission. Accessed: Nov. 03, 2025. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers
[26] "EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf." Accessed: Nov. 03, 2025. [Online]. Available: https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf
[27] H. Jiang, J. Jia, and C. H. Shen, "Legal protection of trade secrets and corporate investment efficiency," *Int. Rev. Econ. Finance*, vol. 104, p. 104681, Dec. 2025, doi: 10.1016/j.iref.2025.104681.
[28] "ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΤΟΥ ΑΝΗΛΙΚΟΥ."
[29] "Ε.Ε: Πώς διαμορφώνεται η ηλικία ψηφιακής συναίνεσης σε κάθε χώρα.," SaferInternet4kids. Accessed: Nov. 03, 2025. [Online]. Available: https://saferinternet4kids.gr/nea/gdpr-ee/
[30] "California Consumer Privacy Act (CCPA)," State of California - Department of Justice - Office of the Attorney General. Accessed: Nov. 03, 2025. [Online]. Available: https://oag.ca.gov/privacy/ccpa
[31] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD. Accessed: Nov. 03, 2025. [Online]. Available: https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html
[32] D. L. Mitrou, "DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES -".
[33] "Cybersecurity: social engineering," Consilium. Accessed: Nov. 03, 2025. [Online]. Available: https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/
[34] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *2014 Information Security for South Africa*, Johannesburg, South Africa: IEEE, Aug. 2014, pp. 1–9. doi: 10.1109/ISSA.2014.6950510.
[35] M. Zaoui, B. Yousra, S. Yassine, M. Yassine, and O. Karim, "A Comprehensive Taxonomy of Social Engineering Attacks and Defense Mechanisms: Toward Effective Mitigation Strategies," *IEEE Access*, vol. 12, pp. 72224–72241, 2024, doi: 10.1109/ACCESS.2024.3403197.
[36] H. Aldawood and G. Skinner, "A Taxonomy for Social Engineering Attacks via Personal Devices," *Int. J. Comput. Appl.*, vol. 178, no. 50, pp. 19–26, Sept. 2019, doi: 10.5120/ijca2019919411.
[37] "Advancements and Best Practices in Data Loss Prevention: A Comprehensive Review," *Glob. J. Univers. Stud.*, vol. 1, no. 1, pp. 190–225, June 2024, doi: 10.70445/gjus.1.1.2024.190-225.
[38] chrfox, "Learn about data loss prevention." Accessed: Nov. 04, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
[39] "Cloud-Native Next-Gen Endpoint Data Loss Protection," Fortinet. Accessed: Nov. 04, 2025. [Online]. Available: https://www.fortinet.com/products/fortidlp
[40] "Data Loss Prevention - What Is DLP?," Cisco. Accessed: Nov. 04, 2025. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-data-loss-prevention-dlp.html
[41] CDC, "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," Public Health Law. Accessed: Nov. 04, 2025. [Online]. Available: https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

[42] Y. Shapira, B. Shapira, and A. Shabtai, "Content-based data leakage detection using extended fingerprinting".
[43] "Data Loss Prevention (DLP) Data Classification - SearchInform." Accessed: Nov. 04, 2025. [Online]. Available: https://searchinform.com/articles/cybersecurity/measures/dlp/essentials/dlp-data-classification/?utm_source=chatgpt.com
[44] European Union Agency for Cybersecurity., *ENISA threat landscape 2023: July 2022 to June 2023.* LU: Publications Office, 2023. Accessed: Nov. 04, 2025. [Online]. Available: https://data.europa.eu/doi/10.2824/782573
[45] K. L. Dempsey *et al.*, "Information Security Continuous Monitoring (ISCM) for federal information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-137, 2011. doi: 10.6028/NIST.SP.800-137.
[46] C. Sabau, "DLP Encryption: Techniques for Optimal Data Loss Prevention," Endpoint Protector Blog. Accessed: Nov. 04, 2025. [Online]. Available: https://www.endpointprotector.com/blog/dlp-encryption-techniques-for-optimal-data-loss-prevention
[47] "The Difference between Format-Preserving Encryption and Tokenization".
[48] "Best Practices." Accessed: Nov. 04, 2025. [Online]. Available: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-1/maintaining-the-dlp-system/about-high-availability-and-disaster-recovery-for/dlp-ha-dr-best-practices.html
[49] "What Is Data Loss Prevention (DLP) Compliance?," Palo Alto Networks. Accessed: Nov. 04, 2025. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/data-loss-prevention-dlp-compliance
[50] chrfox, "Get started with the DLP Alerts dashboard." Accessed: Nov. 04, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-alerts-dashboard-get-started
[51] "About DLP - Google Workspace Admin Help." Accessed: Nov. 04, 2025. [Online]. Available: https://support.google.com/a/answer/9646351
[52] "Enforce Server Platform." Accessed: Nov. 04, 2025. [Online]. Available: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/25-1/introducing/about-the-enforce-server-platform.html
[53] "Introducing Indexed Document Matching (IDM)." Accessed: Nov. 04, 2025. [Online]. Available: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/data-loss-prevention/16-0/about-data-loss-prevention-policies-v27576413-d327e9/introducing-indexed-document-matching-idm-v27388119-d327e27601.html
[54] "CloudSOC DLP Index Matching." Accessed: Nov. 04, 2025. [Online]. Available: https://techdocs.broadcom.com/us/en/symantec-security-software/information-security/symantec-cloudsoc/cloud/protect-home/about-dlp-indexes.html
[55] "McAfee Total Protection for Data Loss Prevention".
[56] "brochure-dlp-data-loss-prevention-en.pdf." Accessed: Nov. 04, 2025. [Online]. Available: https://www.forcepoint.com/sites/default/files/2025-01/brochure-dlp-data-loss-prevention-en.pdf
[57] "Introduction | Trend Micro." Accessed: Nov. 04, 2025. [Online]. Available: https://docs.trendmicro.com/en-us/documentation/article/apex-central-as-a-service-widget-and-policy-management-guide-introduction
[58] V. Roussev, "Data Fingerprinting with Similarity Digests," in *Advances in Digital Forensics VI*, vol. 337, K.-P. Chow and S. Shenoi, Eds., in IFIP Advances in Information and Communication Technology, vol. 337. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 207–226. doi: 10.1007/978-3-642-15506-2_15.
[59] "Set up rules for advanced email content filtering - Google Workspace Admin Help." Accessed: Nov. 04, 2025. [Online]. Available: https://support.google.com/a/answer/1346934
[60] chrfox, "Send email notifications and show policy tips for DLP policies." Accessed: Nov. 05, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-use-notifications-and-policy-tips
[61] chrfox, "Data Loss Prevention policy reference." Accessed: Nov. 04, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/dlp-policy-reference
[62] "Turn on hosted S/MIME for message encryption - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/answer/6374496?hl=en
[63] cabailey, "Apply encryption using sensitivity labels." Accessed: Nov. 05, 2025. [Online]. Available: https://learn.microsoft.com/en-us/purview/encryption-sensitivity-labels
[64] AbbyMSFT, "Overview - Microsoft Defender for Cloud Apps." Accessed: Nov. 05, 2025. [Online]. Available: https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

[65] D. Crocker, "Internet Mail Architecture," RFC Editor, RFC5598, July 2009. doi: 10.17487/rfc5598.
[66] "Message Submission for Mail RFC 6409."
[67] "Simple Mail Transfer Protocol RFC5321 J. Klensin October 2008."
[68] "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1 RFC3501 M. Crispin March 2003."
[69] "Post Office Protocol - Version 3 RFC1939 J. Myers,Carnegie Mellon,M. Rose May 1996."
[70] P. Hoffman, "SMTP Service Extension for Secure SMTP over Transport Layer Security," RFC Editor, RFC3207, Feb. 2002. doi: 10.17487/rfc3207.
[71] "The Transport Layer Security (TLS) Protocol Version 1.3 RFC8446 E. Rescorla , Mozilla August 2018."
[72] C. Newman, "Using TLS with IMAP, POP3 and ACAP," RFC Editor, RFC2595, June 1999. doi: 10.17487/rfc2595.
[73] "Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 RFC 7208 April 2014."
[74] "DomainKeys Identified Mail (DKIM) Signatures RFC6376 D. Crocker, Ed. Brandenburg T. Hansen, Ed. Category: Standards Track AT&T Laboratories M. Kucherawy, Ed. Cloudmark September 2011 ISSN: 2070-1721."
[75] M. Kucherawy and E. Zwicky, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)," RFC Editor, RFC7489, Mar. 2015. doi: 10.17487/rfc7489.
[76] "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification RFC5751 B. Ramsdell, S. Turner ISSN: 2070-1721 January 2010."
[77] "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification RFC8551 J. Schaad B. Ramsdell S. Turner sn3rd April 2019 ISSN: 2070-1721."
[78] "OpenPGP Message Format RFC4880 J. Callas L. Donnerhacke H. Finney PGP Corporation D. Shaw R. Thayer November 2007."
[79] "OpenPGP RFC9580 P. Wouters, Ed. Aiven D. Huigens J. Winter Y. Niibe July 2024."
[80] "Send email over a secure TLS connection - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/answer/2520500?hl=en
[81] "Set up DKIM - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/answer/174124?hl=en&ref_topic=9061731
[82] "Set up DMARC - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/answer/2466580?hl=en
[83] "Set up SPF - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/answer/33786?hl=en
[84] "Encrypt emails with S/MIME - Google Workspace Admin Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.google.com/a/topic/9061730?hl=en&ref_topic=2683828
[85] chrisda, "Email authentication - Microsoft Defender for Office 365." Accessed: Nov. 05, 2025. [Online]. Available: https://learn.microsoft.com/en-us/defender-office-365/email-authentication-about
[86] "Send S/MIME or Microsoft Purview encrypted emails in Outlook - Microsoft Support." Accessed: Nov. 05, 2025. [Online]. Available: https://support.microsoft.com/en-us/office/send-s-mime-or-microsoft-purview-encrypted-emails-in-outlook-373339cb-bf1a-4509-b296-802a39d801dc
[87] R. Sipes, "OpenPGP in Thunderbird 78," The Thunderbird Blog. Accessed: Nov. 05, 2025. [Online]. Available: https://blog.thunderbird.net/2020/09/openpgp-in-thunderbird-78/
[88] "Signed mail with S/MIME | Thunderbird Support Forum | Mozilla Support." Accessed: Nov. 05, 2025. [Online]. Available: https://support.mozilla.org/en-US/questions/1335307
[89] "Setup your email account for using End-To-End Encryption | Thunderbird Help." Accessed: Nov. 05, 2025. [Online]. Available: https://support.mozilla.org/en-US/kb/thunderbird-help-setup-account-e2ee
[90] K. Kaur, I. Gupta, and A. K. Singh, "A Comparative Evaluation of Data Leakage/Loss Prevention Systems (DLPS)," in *Computer Science & Information Technology (CS & IT)*, Academy & Industry Research Collaboration Center (AIRCC), Aug. 2017, pp. 87–95. doi: 10.5121/csit.2017.71008.
[91] European Union Agency for Cybersecurity., *ENISA threat landscape 2024: July 2023 to June 2024.* LU: Publications Office, 2024. Accessed: Nov. 05, 2025. [Online]. Available: https://data.europa.eu/doi/10.2824/0710888
[92] P. Zilberman, S. Dolev, G. Katz, Y. Elovici, and A. Shabtai, "Analyzing group communication for preventing data leakage via email," in *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*, Beijing, China: IEEE, July 2011, pp. 37–41. doi: 10.1109/ISI.2011.5984047.

[93] L. Wan, K. Wang, H. Wang, and G. Bai, "Is It Safe to Share Your Files? An Empirical Security Analysis of Google Workspace," in *Proceedings of the ACM Web Conference 2024*, Singapore Singapore: ACM, May 2024, pp. 1892–1901. doi: 10.1145/3589334.3645697.
[94] "What Is a Cloud Access Security Broker (CASB)? | Microsoft." Accessed: Nov. 05, 2025. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb
[95] J. Pioth, "The Problems of Cloud Access Security Broker (CASB)." Accessed: Nov. 05, 2025. [Online]. Available: https://www.coeosolutions.com/news/problems-of-casb
[96] "Proofpoint Email DLP and Email Encryption".
[97] "Forcepoint DLP for Email Available: https://www.forcepoint.com/sites/default/files/resources/brochures/brochure-dlp-for-email-en.pdf."
[98] "Data Loss Prevention (DLP) | Trend Micro." Accessed: Nov. 05, 2025. [Online]. Available: https://docs.trendmicro.com/en-us/documentation/article/hosted-email-security-administrator-guide-data-loss-prevention
[99] mimecast, "Data Loss Prevention (DLP) Solutions," Mimecast. Accessed: Nov. 05, 2025. [Online]. Available: https://www.mimecast.com/content/dlp-solutions/
[100] "Cisco Secure Email Threat Defense," Cisco. Accessed: Nov. 05, 2025. [Online]. Available: https://www.cisco.com/site/us/en/products/security/secure-email/index.html
[101] "About Rspamd | Rspamd Documentation." Accessed: Nov. 05, 2025. [Online]. Available: https://rspamd.com/
[102] "Software Engineering Life Cycles & Processes Διαφάνειες Μαθήματος Τεχνολογία Λογισμικού ΜΠΕΣ." Accessed: Nov. 05, 2025. [Online]. Available: https://eclass.aegean.gr/modules/document/file.php/ICSD121/%CE%94%CE%B9%CE%B4%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CF%8C%20%CE%A0%CE%B1%CE%BA%CE%AD%CF%84%CE%BF/%CE%94%CE%B9%CE%B1%CF%86%CE%AC%CE%BD%CE%B5%CE%B9%CE%B5%CF%82%20%CE%9C%CE%B1%CE%B8%CE%AE%CE%BC%CE%B1%CF%84%CE%BF%CF%82/SoftwareEngineering_03_LifeCycles%26Processes.pdf
[103] C. Larman, *Applying UML and patterns: an introduction to object oriented analysis and design and iterative development*, 3. ed., 13. print. Upper Saddle River, NJ: Prentice Hall PTR, 2010.
[104] "Unified Modeling Language, v2.5.1".
[105] "Unified Modeling Language (UML) description, UML diagram examples, tutorials and reference for all types of UML diagrams - use case diagrams, class, package, component, composite structure diagrams, deployments, activities, interactions, profiles, etc." Accessed: Nov. 06, 2025. [Online]. Available: https://www.uml-diagrams.org/
[106] M. Fowler, "bliki: Include And Extend," martinfowler.com. Accessed: Nov. 06, 2025. [Online]. Available: https://martinfowler.com/bliki/IncludeAndExtend.html
[107] "Cockburn Ch 1 Scan.pdf." Accessed: Nov. 06, 2025. [Online]. Available: https://www.cs.cmu.edu/~jhm/Readings/Cockburn%20Ch%201%20Scan.pdf
[108] "Microsoft Word _ Book_AfterFinal_doc." Accessed: Nov. 06, 2025. [Online]. Available: https://fabiofumarola.github.io/nosql/readingMaterial/Evans03.pdf
[109] "hexagonal-architecture." Accessed: Nov. 06, 2025. [Online]. Available: https://alistair.cockburn.us/hexagonal-architecture
[110] M. Fowler, *Patterns of enterprise application architecture*, Nineteenth printing. in The Addison-Wesley Signature Series. Boston San Francisco New York Toronto Montreal London Munich Paris Madrid Capetown: Addison-Wesley, 2013.
[111] C. Manning, P. Raghavan, and H. Schuetze, "Introduction to Information Retrieval," 2009.
[112] D. Powers, "Evaluation: From Precision, Recall and F-Factor to ROC, Informedness, Markedness & Correlation".
[113] J. Nielsen, *Usability Engineering*. Morgan Kaufmann, 1994.