Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Εφαρμογές της Κρυπτογραφίας Βάσει Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση και στη Ναυσιπλοΐα

Διδακτορική διατριβή
του
Αθανάσιου Γουδόση

Επιβλέπων: Σωκράτης Κάτσικας
Καθηγητής

23 Ιουνίου 2021

Περίληψη

Η παρούσα διατριβή εστιάζει στη διερεύνηση και πειραματική εφαρμογή προτάσεων βασισμένων σε σχήματα Κρυπτογραφίας Βάσει Ταυτότητας (ΚΒΤ) με απώτερο στόχο την επίλυση προβλημάτων Ηλεκτρονικής Διακυβέρνησης και την ασφάλεια της Ναυσιπλοΐας. Η ΚΒΤ είναι μία ιδιαίτερη μορφή κρυπτογράφησης δημόσιου κλειδιού, η οποία δεν χρησιμοποιεί πιστοποιητικά διότι το δημόσιο αναγνωριστικό κάθε οντότητας είναι το δημόσιο κλειδί της. Αυτή η μοναδική ιδιαιτερότητα της ΚΒΤ, έχει προσελκύσει την προσοχή των ερευνητών, την τελευταία δεκαετία, στη διερεύνηση πιθανών εφαρμογών τις οποίες οι παραδοσιακές μεθοδολογίες κρυπτογράφησης δεν καλύπτουν επαρκώς. Χωρίς να την αντιμετωπίζουμε ως πανάκεια, και με κριτικό πνεύμα, εξετάζουμε αρχικά και προτείνουμε στη συνέχεια την εφαρμογή συγκεκριμένων υλοποιήσεων της ΚΒΤ στις έμπιστες διαδικτυακές επώνυμες και ανώνυμες αναφορές στον τομέα της Ηλεκτρονικής Διακυβέρνησης, καθώς και στην ενίσχυση της ασφάλειας της ναυσιπλοΐας στον τομέα της Ναυτιλίας.

Στις σύγχρονες δικτυοκεντρικές κοινωνίες η ηλεκτρονική επικοινωνία τείνει να υποκαταστήσει τις ανθρώπινες επαφές τόσο σε προσωπικό όσο και σε επίπεδο οργανισμών ελέγχου και πρόληψης της παραβατικότητας. Αυτή η απρόσωπη ηλεκτρονική επικοινωνία του πολίτη που επιθυμεί να αναφέρει την παρατήρηση ή την ανησυχία του σε έναν οργανισμό, έχει το θετικό της αποστασιοποίησης και της ανώνυμης καταγγελίας. Όμως, μία ανώνυμη σχέση συνεχούς επικοινωνίας μεταξύ αναφέροντος και παραλήπτη της αναφοράς (αρχή, οργανισμός), σε βάθος χρόνου, δεν φαίνεται να έχει επιτευχθεί με τις έως τώρα χρησιμοποιούμενες τεχνολογίες ηλεκτρονικής επικοινωνίας.

Σ' αυτήν τη διατριβή εξετάζουμε τη χρήση της ΚΒΤ, ιδιαίτερα των σχημάτων BLMQ-SKIBE και ECCSI-SAKKE, στην επίτευξη ανώνυμης επικοινωνίας σε βάθος χρόνου μεταξύ αναφερόντων και παραληπτών της αναφοράς με το επιπλέον πλεονέκτημα της δυνατότητας της ανά πάσα στιγμή απόδειξης από τον ανώνυμο αναφέροντα της πραγματικής του ταυτότητας. Στη συνέχεια, αναπτύσσουμε και αξιολογούμε μία πειραματική υλοποίηση της πρότασής μας, βασισμένη στο σχήμα ECCSI-SAKKE, αποτεινόμενη σε οργανισμούς με περιορισμένους πόρους (ανθρώπινους, οικονομικούς, υπολογιστικούς).

Η σύγχρονη ναυσιπλοΐα διαφέρει άρδην από την εικόνα των απομονωμένων σκαφών στη μέση της θάλασσας, όταν η μόνη επικοινωνία γινόταν μέσω ασυρμάτου, και η περιοχική ναυσιπλοΐα βασιζόταν σε οπτικά μέσα και στα ραντάρ. Σήμερα, το βασικό μέσο ασφαλούς ναυσιπλοΐας είναι το Automatic Identification System (AIS), το οποίο εγκαθίσταται υποχρεωτικά σχεδόν σε όλα τα σκάφη και στέλνει περιοδικά, σε πραγματικό χρόνο, πληροφορίες για την ταυτότητα και τον πλου του σκάφους. Στοιχεία που το σύστημα AIS, μη διαθέτοντας κατάλληλους μηχανισμούς, αδυνατεί να προστατέψει από επιθέσεις εύκολα αναγνωρίσιμες στο σύγχρονο περιβάλλον των δικτύων και των πληροφοριακών συστημάτων. Η έλλειψη ταυτοποίησης του σκάφους εκπομπής και διαφύλαξης της ακεραιότητας των δεδομένων που μεταδίδονται μέσω του AIS αφήνει ανοιχτό το πεδίο σε επιθέσεις πλαστογράφησης σκάφους προέλευσης ή/και δεδομένων εκπομπής. Η έλλειψη εμπιστευτικότητας επιτρέπει τη χρησιμοποίηση των δεδομένων εκπομπής από επίδοξους πειρατές και τρομοκράτες προκειμένου να επιτεθούν στο σκάφος και από παπαράτσι προκειμένου να

παραβιάσουν την ιδιωτικότητα σημαινόντων επιβατών. Σ' αυτήν τη διατριβή εξετάζουμε τη χρήση της ΚΒΤ, ιδιαίτερα των σχημάτων BLMQ-SKIBE και ECCSI-SAKKE, στον εμπλουτισμό του συστήματος AIS με μηχανισμούς εμπιστευτικότητας, ταυτοποίησης και ακεραιότητας δεδομένων. Στη συνέχεια αναπτύσσουμε και αξιολογούμε μία πειραματική υλοποίηση της πρότασής μας, με το σχήμα ECCSI-SAKKE, επιδεικνύοντας ότι είναι δυνατή η κατ' αρχήν λειτουργία χωρίς αλλαγές του υφιστάμενου πρωτοκόλλου του συστήματος AIS και με μικρές αλλαγές, σε επίπεδο λογισμικού, στις υφιστάμενες συσκευές AIS.

Θεωρούμε ότι αυτή η εργασία μπορεί να αποτελέσει τη βάση, ή απλά την αφορμή, για περαιτέρω έρευνα στον τομέα των εφαρμογών της ΚΒΤ, ιδιαίτερα στους τομείς της ηλεκτρονικής διακυβέρνησης και της ναυτιλίας.

Abstract

Applications of Identity Based Cryptography (IBC) in Maritime and E-Governance sectors

This research focuses on investigating the feasibility of using Identity-Baced Cryptography (IBC) schemes to develop, implement, and test solutions to problems in e-governance and maritime security. IBC is a special form of public key cryptography which does not need to use certificates, as the public identifier of each entity is its own public key. In the last decade, the unique qualities of IBC have attracted research attention in areas where traditional public key cryptography methods do not lend themselves. We first examine the applicability of IBC and we then develop concrete proposals for leveraging IBC towards developing anonymous reporting in the e- government domain on one hand, and towards enhancing the security of marine navigation on the other.

In modern, networked, societies electronic communication tends to substitute human contacts. This applies both to communications among individuals, but also to communications between individuals and authorities with responsibility for controlling and preventing delinquency or even crime. The electronic communication of a citizen who intends to report events or warnings to an authority potentially offers the advantage of distancing and anonymity. However, secure repeated anonymous communication between a reporter and an authority, in the long term, has not been made possible to date.

In this thesis we study the use of IBC, in particular of the BLMQ-SKIBE and ECCSI-SAKKE schemes, to achieve secure, repeated anonymous communication between a reporter and the authorities, with the added advantage of offering the ability to the reporter, should and when they so wish, to reveal and prove their identity at any time. Then, we develop and evaluate an experimental implementation of our proposed solution based on the ECCSI-SAKKE scheme. The proposed solution addresses the needs of agencies with limited resources (human, financial, computing) at their disposal.

Marine navigation has changed considerably in the last decades. Nowadays, one of the main technological aids of safe navigation is the Automatic Identification System (AIS), which is compulsorily on almost every ship and sends intermittently data in real time about a vessel's identity and voyage. AIS does not have mechanisms to protect such data from attacks, whose feasibility is not hard to recognize in a contemporary network and information systems environment. The lack of authentication of a vessel's transmitted identity, and the preservation of the integrity of the data transmitted via its AIS enable attacks that will falsify either the vessel's identity or the data it transmits. The absence of mechanisms to protect the confidentiality of the transmitted data allows potential pirates or terrorists to leverage such data to attack the ship or paparazzi to invade the privacy of celebrities on board it.

In this research we study the use of IBC, particularly of the BLMQ-SKIBE and ECCSI-SAKKE schemes, to enhance the AIS with mechanisms of confidentiality, authentication, and data integrity. Furthermore, we develop and evaluate an

experimental implementation of our proposal with the ECCSI-SAKKE scheme, thereby demonstrating that the proposed solution can be put to operational use without changing the existing AIS communication protocol, and by making minor only changes to the software of the existing AIS devices.

We aspire that this thesis may form a basis, or simply provide food for thought, for further research in possible applications of IBC, particularly in the e-governance and maritime domains.

Ευχαριστίες

Στον άνθρωπο, και εποπτεύοντα καθηγητή μου, Σωκράτη Κάτσικα, θα ήταν αταίριαστο οτιδήποτε άλλο από ένα βαθύ, μεστό, τεράστιο αλλά ταυτόχρονα λιτό «ευχαριστώ» . Τον ευχαριστώ για τον καταλυτικό ρόλο που έχει διαδραματίσει στη ζωή μου από τις πρώτες συζητήσεις μας στα φοιτητικά μου χρόνια *(… και πάνε πάρα πολλά χρόνια από τότε)*, έως και σήμερα στην πραγμάτωση αυτής της εργασίας. Ευχαριστώ πολύ για όλα!

Στην πραγματικότητα αυτή είναι μία συλλογική εργασία, με πολλούς συμμετέχοντες! Πέραν του καθηγητή μου, ευχαριστώ … τις γυναίκες της ζωής μου, Κωνσταντίνα, Μαρίνα και Ελένη για την αγάπη, την υποστήριξη και την ανοχή τους όλα αυτά τα χρόνια. Τη μητέρα μου Μαρίνα, που έβαλε γερά θεμέλια και είναι πάντα «εδώ», του πατέρα μου Κωνσταντίνο, του παππού μου Ιωάννη και τη γιαγιά μου Ελένη που δυστυχώς δεν πρόλαβαν να με ζήσουν πολύ, αλλά η παρακαταθήκη τους είναι πάντα «εδώ». Του Διονύση, «αδερφό» από επιλογή και όχι εκ συγγενείας. Του Παύλο, τη Βάσω, την Ευγενία, και τον Γιώργο γιατί είναι μέρος των παιδικών μου χρόνων και, τελικά, μέρος του «τι είμαι». Τη θεία μου τη Μαίρη, που ο ήρεμος λόγος της έχει πολύ μεγαλύτερη δύναμη από όσο φαντάζεται κανείς. Τους Σπύρο, Έφη, Κώστα, Γιώτα, Ειρήνη και Στέφη, τη ¨νέα¨ μου οικογένεια, που κουράστηκαν να ακούν φράσεις όπως, «… αφήστε του, κάνει το διδακτορικό του..»! Την Ταρώ για τις ώρες που πέρασε μπροστά στον Η/Υ και τις υποδείξεις της. Τέλος, όλους τους φίλους μου και όλα τα άτομα που συμμετείχαν με έμμεσο η άμεσο τρόπο στον δρόμο μου!

Αυτή η εργασία είναι αφιερωμένη στις κόρες μου Μαρίνα και Ελένη, που τους εύχομαι αυτή η εμπειρία που ζήσαμε μαζί να τις βοηθήσει, με όποιο τρόπο, να χαράξουν τους δικούς τους δρόμους …

Εφαρμογές της Κρυπτογραφίας Βάσει Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση και στη Ναυσιπλοΐα

Αθανάσιος Γουδόσης
a.goudosis@gmail.com

23 Ιουνίου 2021

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Από την περασμένη δεκαετία, η Κρυπτογραφία Βάσει Ταυτότητας - ΚΒΤ (IBC) χωρίς πιστοποιητικά έχει προσελκύσει την προσοχή των επιστημόνων που εργάζονται στην εφαρμοσμένη κρυπτογραφία. Σ΄ αυτήν τη διατριβή διερευνούμε την πιθανή χρήση μηχανισμών ΚΒΤ (IBC) αφενός στη ναυσιπλοΐα και ειδικότερα στην ασφάλεια του συστήματος Automatic Identification System (AIS)[1], και αφετέρου στην ηλεκτρονική διακυβέρνηση και ειδικότερα στα συστήματα αναφοράς παραβατικών πράξεων.

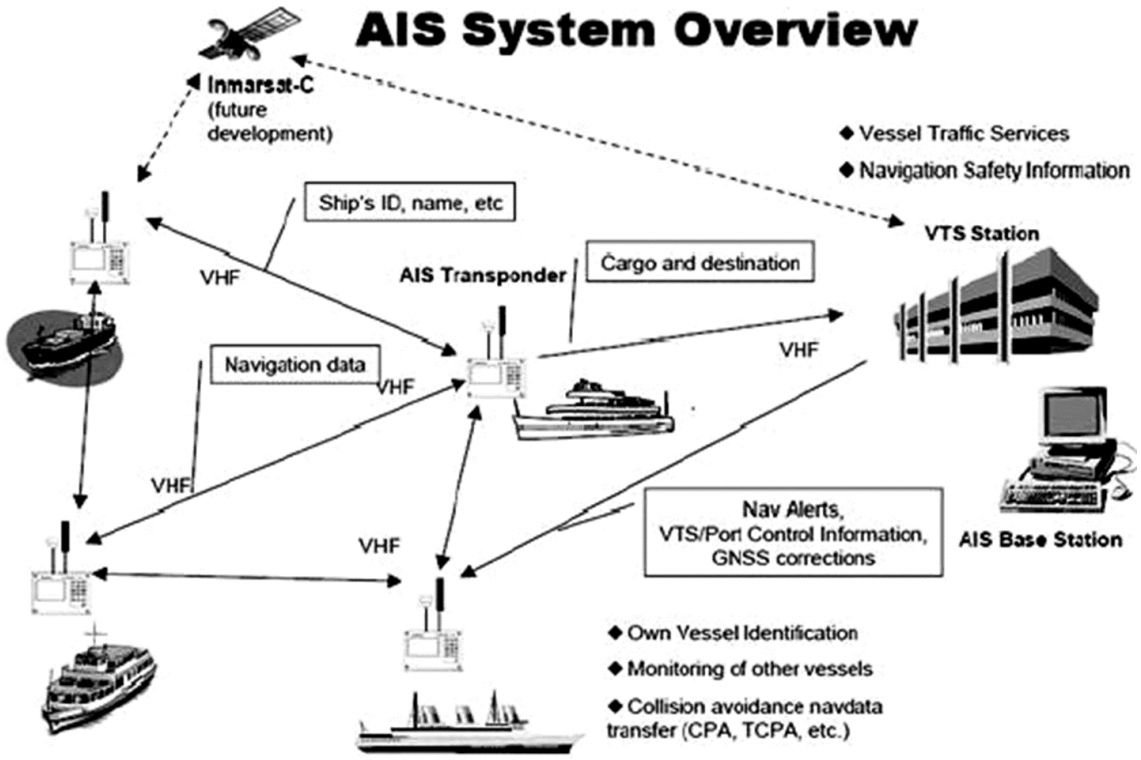
1.1 Συνοπτική περιγραφή του αντικειμένου της διατριβής

1.1.1 Ναυσιπλοΐα και Automatic Identification System (AIS)

Η ασφάλεια της σύγχρονης ναυσιπλοΐας με πληθώρα σκαφών όλων των τύπων που κινούνται ακατάπαυστα προϋποθέτει συνεχή και ακριβή ροή πληροφοριών για την κίνησή τους, σε πραγματικό χρόνο. Το σύστημα Automatic Identification System (AIS) αποτελείται από μια συσκευή που δέχεται σε πραγματικό χρόνο δεδομένα από τα συστήματα ναυσιπλοΐας του σκάφους (π.χ. θέση, κατεύθυνση, ταχύτητα), τα συνδυάζει με στατικά στοιχεία του σκάφους (π.χ. όνομα, τύπος) και τα μεταδίδει περιοδικά μέσω μιας κεραίας (βλ. Σχήμα 1.1). Αυτά τα δεδομένα τα λαμβάνουν όλα τα σκάφη εντός της εμβέλειας της κεραίας που διαθέτουν αντίστοιχη συσκευή του συστήματος AIS, και τα προωθούν στα αντίστοιχα συστήματα ναυσιπλοΐας τους. Είναι ουσιαστικά μια αυτοματοποιημένη μέθοδος γνωστοποίησης των βασικών στοιχείων του σκάφους, της κατάστασής του σε πραγματικό χρόνο και των προθέσεών του. Μαζί δε με το ραντάρ είναι τα de-facto συστήματα αυτοματοποιημένου έλεγχου της ναυσιπλοΐας στον τομέα των θαλάσσιων μεταφορών. Στη σύγχρονη ναυτιλία το AIS είναι διασυνδεδεμένο με την ¨ηλεκτρονική πλοήγηση e-navigation¨ και την ¨ηλεκτρονική γέφυρα (e-bridge)¨ έτσι ώστε όλες οι πληροφορίες που συγκεντρώνει από τα υπόλοιπα σκάφη στην περιοχή να συνδυάζονται μαζί με τις πληροφορίες από το ραντάρ και τους ηλεκτρονικούς χάρτες σε ολοκληρωμένες εφαρμογές απεικόνισης του περίγυρου του σκάφους.

Εκ του σχεδιασμού του το AIS δεν διαθέτει μηχανισμούς ασφαλείας, έλλειψη που το καθιστά ευάλωτο σε κακόβουλες ενέργειες με κίνητρα όπως η πειρατεία, η

[1] Αυτόματο Σύστημα Αναγνώρισης



Σχήμα 1.1: Το σύστημα AIS [1].

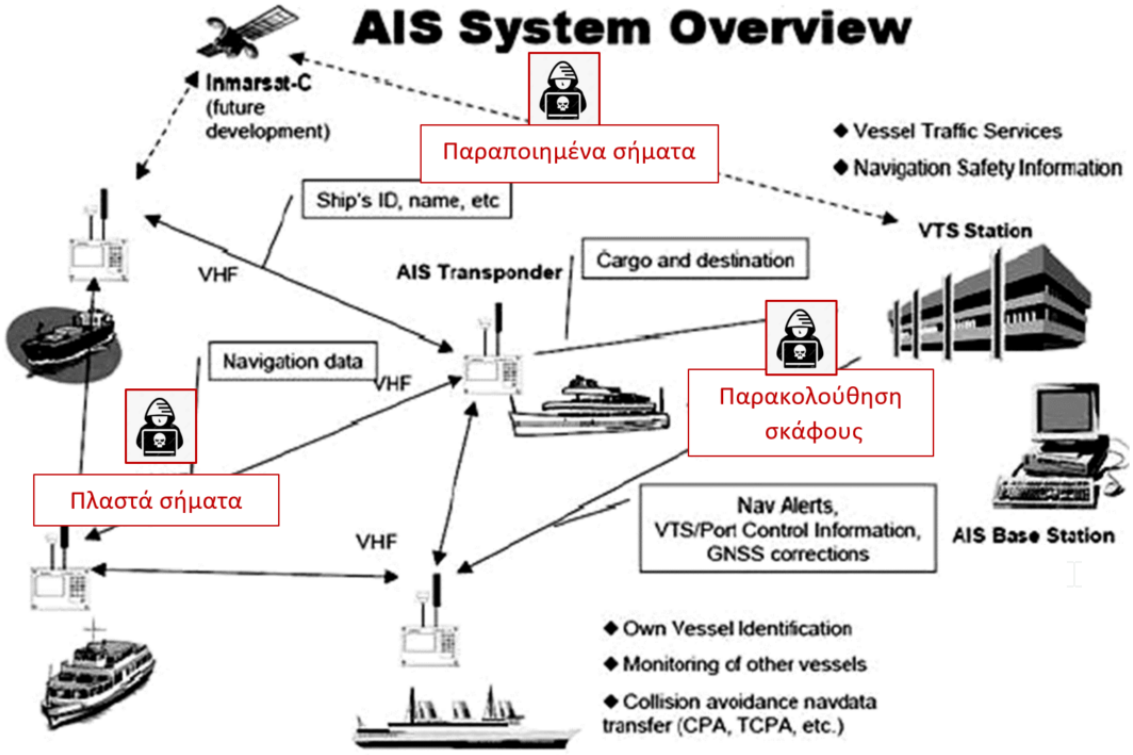
τρομοκρατία, το λαθρεμπόριο, η παραβίαση της ιδιωτικότητας και η οικονομική και εμπορική κατασκοπεία [4], [5] (βλ. Σχήμα 1.2).

Η διατριβή αυτή επικεντρώνεται στην ασφάλεια του πρωτοκόλλου μετάδοσης δεδομένων του συστήματος AIS. Επισημαίνουμε ότι δεν εξετάζεται η ασφάλεια της ηλεκτρονικής υποδομής του συστήματος AIS, η ακεραιότητα των δεδομένων που συλλέγει η συσκευή του AIS από τον εξοπλισμό του πλοίου, αλλά ούτε και επιθέσεις στο ηλεκτρομαγνητικό φάσμα μετάδοσης που χρησιμοποιεί το AIS.

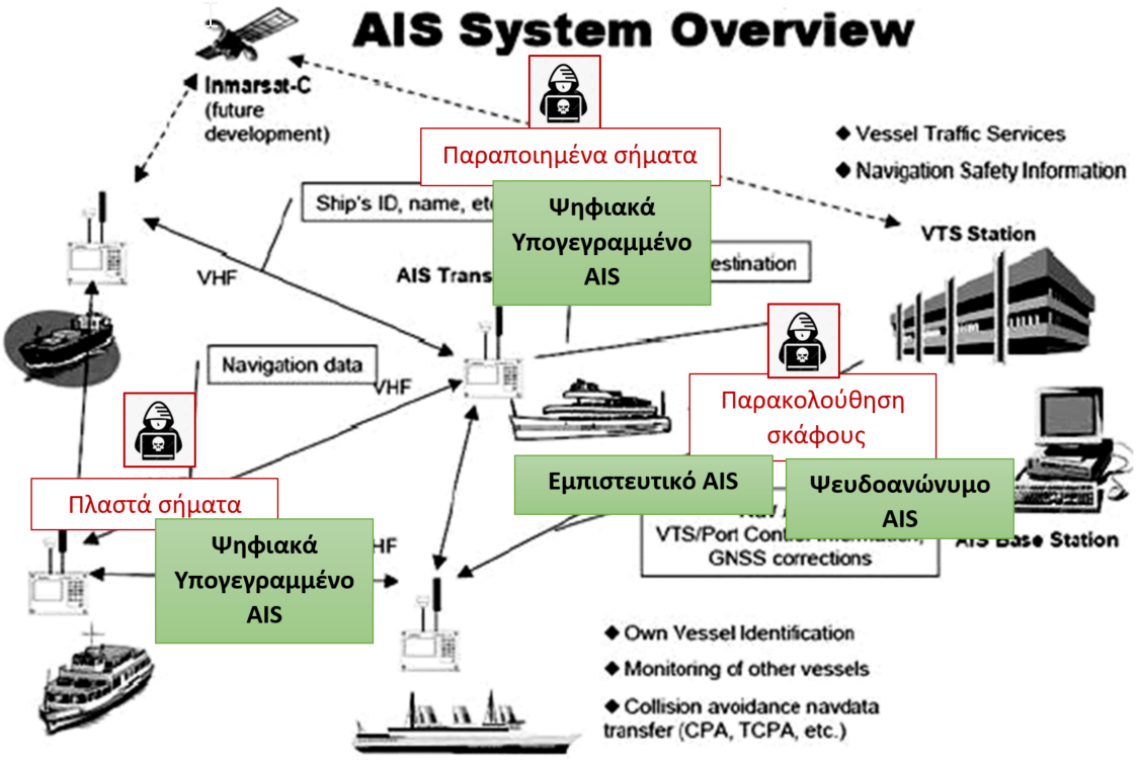
Για την αντιμετώπιση των ζητημάτων ασφαλείας του AIS, προτείνουμε την ανάπτυξη μιας υποδομής κρυπτογράφησης δημόσιου κλειδιού βάσει ταυτότητας χωρίς πιστοποιητικά, σχεδιασμένης για τον ναυτιλιακό τομέα. Η πρότασή μας, με την ονομασία "maritime-IBC-AIS (mIBC-AIS)", προσδίδει στο AIS δυνατότητες ταυτοποίησης και ελέγχου της ακεραιότητας των δεδομένων που εκπέμπονται, ψευδωνυμοποίηση του εκπομπέα (ανωνυμια κατ' απαίτηση), και δυνατότητες κρυπτογράφησης. Το Σχήμα 1.3 απεικονίζει τις αναβαθμισμένες λειτουργίες που η πρότασή μας προσδίδει στο AIS.

1.1.2 Ηλεκτρονική Διακυβέρνηση: ασφαλείς αναφορές παραβατικών πράξεων

Η αναφορά παραβατικών πράξεων στις αρχές αποτελεί θεμελιώδες δικαίωμα για τους πολίτες υπό δημοκρατική διακυβέρνηση. Ωστόσο, υπαρκτοί ή ιδεοληπτικοί ανασταλτικοί παράγοντες, όπως π.χ. φόβος αντιποίνων από τους δράστες, φόβος ότι δεν θα γίνουν πιστευτοί, αίσθημα ανασφάλειας για εμπλοκή σε περίπλοκες διαδικασίες, οδηγούν πολλούς εν δυνάμει αναφέροντες σε ατολμια αναφοράς αυτών



Σχήμα 1.2: Οι κύριες απειλές ασφάλειας κατά του συστήματος AIS. Προσαρμογή από το [1].



Σχήμα 1.3: Αναβαθμισμένες λειτουργίες του AIS. Προσαρμογή από το [1].

των παραβατικών πράξεων. Οι τυπικές λύσεις ανώνυμης επικοινωνίας του αναφέροντα με τις αρχές έχουν ως σημαντικότερο μειονεκτήμα ότι η ανώνυμη επικοινωνία είναι μονόδρομη και χωρίς διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των μεταφερόμενων δεδομένων.

Σ' αυτήν τη διατριβή προτείνουμε ένα (Ανώνυμο) Σύστημα Αναφοράς βασισμένο στην κρυπτογραφία βάσει ταυτότητας ΚΒΤ (IBC), το οποίο ονομάζουμε Anonymous Reporting IBC (ARIBC), με δυνατότητες αμφίδρομης εμπιστευτικής επικοινωνίας μεταξύ του αναφέροντα και των αρχών μέσω κρυπτογράφησης, και αμφίδρομο έλεγχο ταυτότητας και ακεραιότητας δεδομένων μέσω ψηφιακών υπογραφών. Ταυτόχρονα, υπάρχει η επιλογή ο αναφέρων να παραμείνει ανώνυμος μέσω ψευδωνυμοποίησης και μόνο όταν θελήσει εκείνος να αποκαλύψει, αλλά και να πιστοποιήσει, την πραγματική του ταυτότητα.

1.2 Στόχοι της έρευνας

Κύριος στόχος της έρευνας που περιγράφεται στην παρούσα διατριβή ήταν να διερευνηθεί η δυνατότητα χρήσης εφαρμοσμένων κρυπτογραφικών τεχνικών βάσει ταυτότητας ΚΒΤ (IBC) στη ναυσιπλοΐα και στην ηλεκτρονική διακυβέρνηση. Αυτός ο κύριος στόχος αναλύεται περαιτέρω στους εξής επιμέρους στόχους:

- Να σχεδιαστεί και υλοποιηθεί ένα σύστημα ανώνυμης αναφοράς παραβατικών πράξεων που να παρέχει αμφίδρομη ασφαλή επικοινωνία μεταξύ του αναφέροντος και των αρχών μέσω κρυπτογράφησης, αμφίδρομη πιστοποίηση και ακεραιότητα των μηνυμάτων μέσω ψηφιακών υπογραφών, επιλογή του αναφέροντα να παραμείνει ανώνυμος, ανεξαρτησία από άλλες υποδομές ελέγχου ταυτότητας και εξουσιοδότησης, ευκολία εφαρμογής και χρήσης. Το εύρος του πεδίου εφαρμογής του προτεινόμενου συστήματος θα πρέπει να είναι εκτεταμένο και να μπορεί να υλοποιηθεί και να λειτουργήσει σε ευρύ φάσμα αρχών, που κυμαίνεται από ένα μικρό και αυτόνομο τμήμα ενός οργανισμού έως και σε μεγάλες διαλειτουργικές αυτόνομες δομές μέσα από διακρατικές συμφωνίες.
- Να σχεδιαστεί και υλοποιηθεί μια λύση ενίσχυσης της ασφάλειας του πρωτοκόλλου μετάδοσης δεδομένων του συστήματος AIS, που θα προσδίδει στο σύστημα δυνατότητες ταυτοποίησης, εμπιστευτικότητας, ακεραιότητας δεδομένων και ψευδωνυμιας, χωρίς την ανάγκη τροποποίησης της υποκείμενης επικοινωνιακής υποδομής του συστήματος AIS. Το εύρος της προτεινόμενης λύσης για ένα ασφαλές AIS θα πρέπει να κυμαίνεται από μια παγκόσμια υλοποίηση από διεθνείς (π.χ. International Maritime Organization) ή αυτόνομες εθνικές ναυτιλιακές αρχές, έως αυτόνομες ιδιωτικές υλοποιήσεις από μεμονωμένες ναυτιλιακές εταιρείες ή διαλειτουργικός συνδυασμός των παραπάνω.

1.3 Σχετικά έργα και βιβλιογραφία

Αυτή η ενότητα χωρίζεται σε τρία διακριτά μέρη, αφιερωμένα στην παράθεση βιβλιογραφίας σχετικής με:

1. την Κρυπτογραφία Βάσει Ταυτότητας ΚΒΤ (IBC) χωρίς πιστοποιητικά

2. την ασφάλεια του Automatic Identification System (AIS)

3. την ηλεκτρονική αναφορά παραβατικών πράξεων

1.3.1 Κρυπτογραφία Βάσει Ταυτότητας χωρίς πιστοποιητικά ΚΒΤ (IBC)

Την τελευταία δεκαετία, η ΚΒΤ (IBC) προσελκύει όλο και περισσότερο το επιστημονικό ενδιαφέρον σε εφαρμογές όπου υπάρχει μια κεντρική αρχή συντονισμού και στο Διαδίκτυο των Πραγμάτων (Internet of Things (IoT)). Επειδή η ΚΒΤ (IBC) δεν απαιτεί τη χρήση πιστοποιητικών, θεωρείται ελαφριά και ευπροσάρμοστη λύση που προτείνεται ιδιαίτερα: για την ασφάλεια σε ad-hoc κινητά δίκτυα (mobile ad-hoc networks (MANET)) [6], για ασφαλείς εφαρμογές ηλεκτρονικού ταχυδρομείου [7], για την ασφαλή ανώνυμη επικοινωνία ηλεκτρονικού ταχυδρομείου [8], για ασφάλεια σε υπηρεσίες νέφους [9], για τη διασφάλιση της εμπιστευτικότητας των δεδομένων υγείας των ασθενών [10], για τη δημιουργία ελαφρών ασφαλών κινητών αρχείων υγείας (Mobile-Personal health records) [11], για τον έλεγχο ταυτότητας σε κινητό σύστημα παρακολούθησης ηλεκτρονικής υγείας [12], για την προστασία του συστήματος (Automatic Dependent Surveillance-Broadcast, ADS-B) στην αεροπλοΐα [13] [14], και στην ηλεκτρονική διακυβέρνηση ως μια λύση που συνδυάζει βιομετρικά στοιχεία και κρυπτογραφία βάσει ταυτότητας [15].

Συνοπτικά, οι προτάσεις μας για την αξιοποίηση της ΚΒΤ βασίζονται στις παρακάτω εργασίες:

1. Στις οδηγίες του προτύπου IEEE 1363.3-2013, "Standard for Identity-Based Cryptographic Techniques using Pairings" [16]) για τις διγραμμικές αντιστοιχίσεις πάνω από ελλειπτικές καμπύλες (bilinear mappings over elliptic curves) γνωστές ως ¨ζεύγη¨ (pairings). Το πρότυπο IEEE 1363.3-2013 [16] περιγράφει οκτώ κρυπτογραφικά σχήματα βάσει ταυτότητας που χρησιμοποιούν ζεύγη και εφαρμόζουν κρυπτογράφηση δεδομένων, ψηφιακές υπογραφές και ανταλλαγές συμμετρικών κλειδιών κρυπτογράφησης συνόδου. Επίσης, το πρότυπο παρουσιάζει τυποποιημένους αλγόριθμους για τον υπολογισμό των ζευγών με τις κατάλληλες παραμέτρους για την εκπλήρωση των απαιτήσεων ασφάλειας βιομηχανικού επιπέδου, όπως αυτές παρουσιάζονται στο National Institute of Standards and Technology (NIST) [17].

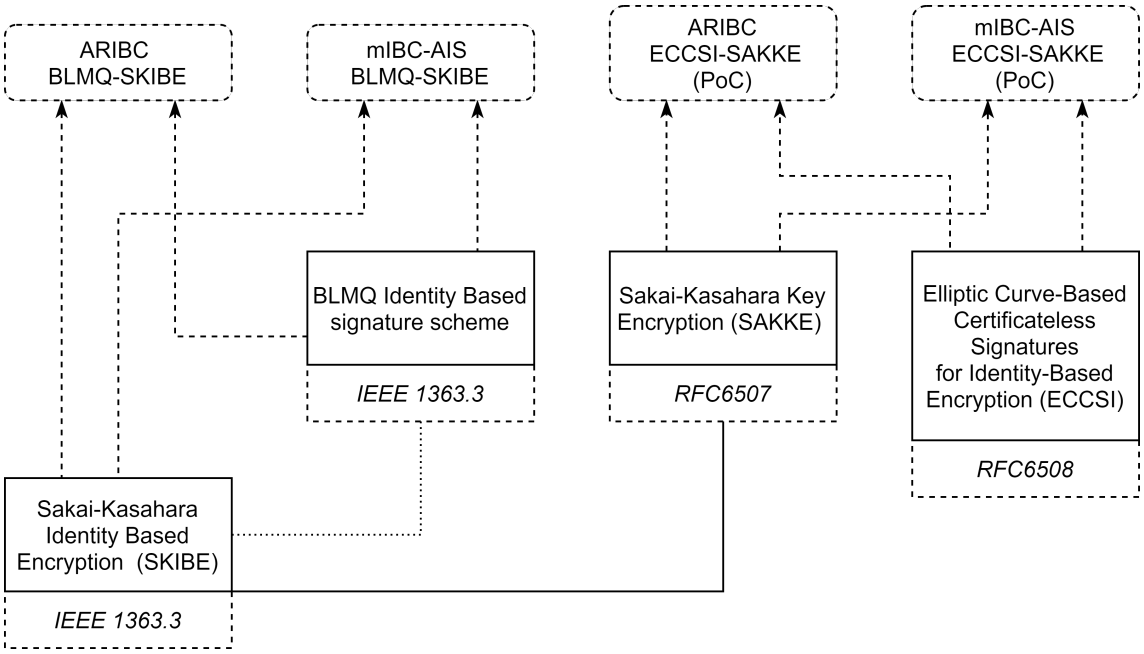
2. Το q-Bilinear Diffie-Hellman Inversion problem (q-BDHIP), όπως προτείνεται στο σχήμα κρυπτογράφησης βάσει ταυτότητας Sakai-Kasahara Identity-Based Encryption (SKIBE) [18] [19] και αναλύθηκε στο [20].

3. Τη μεθοδολογία ψηφιακών υπογραφών BLMQ [2] όπως προτείνεται στο [22] και σύμφωνα με τις οδηγίες του προτύπου IEEE 1363.3-2013 “Standard for Identity-Based Cryptographic Techniques using Pairings” [16].

4. Το σχήμα ECCSI-SAKKE, που παρουσιάστηκε σε δύο RFCs από τον M. Groves [3], το οποίο προτείνει συγκεκριμένους αλγόριθμους υλοποίησης: Το RFC6507

[2]"... είναι ουσιαστικά το σχήμα υπογραφής του σχήματος Sakai-Kasahara", σελ.15 στο [21]

[3]Εργαζόμενος τότε στην UK Government’s National Technical Authority for Information and Assurance (CESG) που τώρα ονομάζεται The National Cyber Security Centre (NCSC).



Σχήμα 1.4: Σχέσεις μεταξύ των εργασιών ΚΒΤ στις οποίες στηρίχθηκε η διατριβή.

"Elliptic Curve-based Certificateless Signatures for Identity-based encryption (ECCSI)" [2] και το RFC6508 "Sakai-Kasahara Key Encryption (SAKKE)" [3] [4].

Στο Σχήμα 1.6 παραθέτουμε μια απεικόνιση των σχέσεων μεταξύ των εργασιών ΚΒΤ στις οποίες στηρίχθηκε η διατριβή.

1.3.2 Ασφάλεια του Automatic Identification System (AIS)

Στα [23] [24] [25] εξετάζονται οι σημαντικότερες από τις απειλές που αντιμετωπίζει σήμερα το Automatic Identification System (AIS). Οι παραπάνω εργασίες, ιδιαίτερα αυτές του IMO, δείχνουν ότι η έλλειψη ασφάλειας του AIS είναι ένα σημαντικό ζήτημα που απασχολεί τη ναυτική κοινότητα. Ένα νέο σύστημα ανταλλαγής δεδομένων, που ονομάζεται VHF Data Exchange System (VDES), θεωρείται ότι αντιμετωπίζει τις αυξανόμενες απαιτήσεις της σύγχρονης ναυσιπλοΐας, συμπεριλαμβανομένων ορισμένων πτυχών ασφάλειας, αλλά δεν αναμένεται να γενικευθεί σύντομα η πλήρης χρήση του [26].

Στο [27] προτάθηκε ένα νέο πρωτόκολλο για το AIS, βασιζόμενο σε μια προσέγγιση τριών επιπέδων για την ασφάλεια, και με την ταυτότητα του σκάφους να επαληθεύεται από πιστοποιητικά που έχουν εκδοθεί από μια εγκρίνουσα αρχή. Αυτή η λύση, όμως, προϋποθέτει την ύπαρξη ολοκληρωμένης κρυπτογραφικής υποδομής που να παρέχει στη ναυτιλιακή κοινότητα κάποιες κρυπτογραφικές δυνατότητες.

Οι συγγραφείς του [28] χρησιμοποιούν τα Maritime Mobile Service Identities (MMSIs)[5] των πλοίων και Έμπιστες Τρίτες Οντότητες (Trusted Third Parties) για να προτείνουν

[4] Σύμφωνα με το ίδιο το RFC6508 (σελ. 2), υπάρχει ως Sakai-Kasahara Key Encapsulation Mechanism (SK-KEM στο πρότυπο IEEE P.1363-3 [16]

[5] Το MMSI αποτελείται από 9 ψηφία και ταυτοποιεί μοναδικά κάθε σκάφος. Εκχωρείται σε όλες τις ραδιοεπικοινωνίες αυτού του σκάφους και αλλάζει όταν ένα σκάφος αλλάζει σημαία και αρχή νηολόγησης.

ένα σύστημα αμοιβαίου ελέγχου ταυτότητας τριών βημάτων, που χρησιμοποιεί το AIS ως μέσο επικοινωνίας για να παρέχει δυνατότητες ελέγχου ταυτότητας στα πλοία, χωρίς όμως να προσδίδει στο ίδιο το AIS πρόσθετες δυνατότητες ασφάλειας.

Οι συγγραφείς του [29] πρότειναν μια λύση που βασίζεται στη δημιουργία μιας παγκόσμιας, ναυτιλιακής υποδομής δημόσιου κλειδιού (PKI) τύπου x.509, όπου οι Αρχές εγγραφής και πιστοποίησης θα είναι ο IMO και οι Εθνικές Ναυτιλιακές Αρχές. Η συγκεκριμένη πρόταση έχει δυσκολίες στην υλοποίηση της υποδομής PKI στο περιβάλλον της ναυτιλίας. Επιπλέον, τα πιστοποιητικά είναι πολύ απαιτητικά σε επικοινωνιακούς πόρους και ως εκ τούτου αποτελούν δαπανηρή λύση στο δύσκολο περιβάλλον της ασύρματης θαλάσσιας επικοινωνίας.

Για τους ίδιους λόγους, εργασίες που στοχεύουν στη βελτίωση της ασφάλειας παρόμοιων συστημάτων, όπως είναι το Automatic Dependent Surveillance-Broadcast (ADS-B) στην αεροπλοΐα, προτείνουν τη χρήση κρυπτογραφίας βάσει ταυτότητας και συμμετρικής κρυπτογραφίας [30] [14]. Ωστόσο, οι προτάσεις αυτές είναι δύσκολο να μεταφερθούν στο θαλάσσιο περιβάλλον.

Ο συγγραφέας του [31] έχει αναπτύξει το "protected-AIS (pAIS)" το οποίο είναι παρόμοιο με τον έλεγχο ταυτότητας του προτεινόμενου από εμάς mIBC-AIS στη λειτουργία (mode 2). Ωστόσο, λόγω της χρήσης του RSA, παρουσιάζει όλα τα εγγενή προβλήματα των Υποδομών Δημόσιου Κλειδιού που βασίζονται σε πιστοποιητικά σε δύσκολα περιβάλλοντα, όπως αυτό του AIS, και τη χρήση αδύναμου κλειδιού όπως το 256bit-RSA.

Διάφοροι κατασκευαστές προσφέρουν προϊόντα AIS που χρησιμοποιούν συμμετρική κρυπτογραφία (Alltek[6], FURUNO[7], KONGSBERG[8], SAAB[9], iMarine[10]). Ωστόσο, αυτά τα προϊόντα προσφέρουν μόνο υπηρεσία εμπιστευτικών μηνυμάτων AIS μέσω συμμετρικής κρυπτογράφησης και μόνο μεταξύ προϊόντων του ίδιου κατασκευαστή. Επιπλέον, τα συμμετρικά κλειδιά πρέπει να είναι προεγκατεστημένα ή να επανεγκαθίστανται χειροκίνητα στις συσκευές. Αυτές οι λύσεις στοχεύουν κυρίως σε περιπτώσεις όπου υπάρχει προκαθορισμένος στόλος συγκεκριμένων και ελεγχόμενων σκαφών. Η υιοθέτηση ενός συμμετρικού συστήματος κρυπτογραφίας που θα χρειαζόταν να διαχειριστεί συμμετρικά κλειδιά σε ένα μεγάλο αριθμό σκαφών παγκοσμίως είναι πολύ περίπλοκη, αν όχι αδύνατη. Επομένως, θεωρούμε ότι μία τέτοια λύση δεν είναι κατάλληλη για συστήματα με χαρακτηριστικά παρόμοια με αυτά του AIS [32].

Τέλος, εργασίες που δεν είναι ακόμη σαφές εάν ή πώς μπορεί να επηρεάσουν το μέλλον της ασφάλειας του AIS είναι επίσης σε εξέλιξη [33].

1.3.3 Ηλεκτρονική αναφορά παραβατικών πράξεων

Πολλές αρχές ελέγχου και πρόληψης παραβατικότητας σε όλο τον κόσμο είναι συνδεδεμένες με συστήματα αναφοράς παραβατικών πράξεων. Η πλειονότητα αυτών

[6] https://www.alltekmarine.com/solution.php?nid=3

[7] http://www.furuno.fr/Multimedia/Brochure_FA-170_EAIS_E.pdf

[8] https://www.kongsberg.com/globalassets/maritime/km-products/product-documents/datasheet_ais300bf.pdf

[9] https://www.saab.com/products/r5-supreme-w-ais

[10] https://www.imarine.com.tr/project/secure-ais-transponder/

υποστηρίζει αναφορές είτε μέσω ηλεκτρονικού ταχυδρομείου είτε μέσω ενός ιστότοπου. Ως εκ τούτου, συχνά δεν διαθέτουν δυνατότητα ανώνυμης αναφοράς, δεν υποστηρίζουν αμφίδρομη επικοινωνία (μεταξύ της αρχής και του αναφέροντα) και ο συσχετισμός πολλαπλών αναφορών της ίδιας πράξης μεταξύ τους είναι δυσχερής. Αυτή η λειτουργικότητα μπορεί να είναι επαρκής για την ικανοποίηση των βασικών αναγκών μιας υπηρεσίας, αλλά απαιτούνται πιο εξελιγμένες προτάσεις για την πλήρη υποστήριξη της διαδικασίας αναφοράς. Ως αποτέλεσμα, πολλές διαδικτυακές μεθοδολογίες έχουν προταθεί σε αυτήν την κατεύθυνση, ορισμένες από τις οποίες υποστηρίζουν ανώνυμες αναφορές, ενώ άλλες απαιτούν επώνυμες αναφορές με έμμεση ή άμεση ταυτοποίηση του χρήστη στην αναφέρουσα αρχή.

Μια μέθοδος επεξεργασίας φυσικής γλώσσας, σε συνδυασμό με ένα ηλεκτρονικό σύστημα αναφοράς, το οποίο βελτιώνει την ανάκτηση πληροφοριών από μάρτυρες και θύματα, παρουσιάζεται στα [34] [35] [36]. Το "Cry Help App", είναι ένα διακριτικό σύστημα αναφοράς εγκλημάτων για πανεπιστημιακά περιβάλλοντα [37]. Στο [38] παρουσιάζεται ένα σύστημα αναφοράς εγκλημάτων, βασιζόμενο σε τεχνολογίες νέφους, που μπορεί να επεξεργαστεί αναφορές παράνομης δραστηριότητας από την αναφορά ενός συμβάντος έως και την έκδοση κάποιου είδους ανταμοιβής. Στο [39] περιγράφεται η αποδοχή ενός Διαδικτυακού Συστήματος Αναφοράς Τρίτων (O-TPRS) που αναπτύχθηκε από την VESTA Social Innovation Technologies, κυρίως από θύματα σεξουαλικής επίθεσης. Στο [40] προτείνεται το "ReportCoin", ένα ανώνυμο σύστημα αναφοράς βασισμένο σε τεχνολογία “Blockchain", που ενσωματώνει και μηχανισμό κινήτρων. Το "Say Something Anonymous Reporting System"[11] είναι ένα ανώνυμο σύστημα αναφοράς που βοηθά στην πρόληψη βίαιων πράξεων από νέους που μπορεί να σχεδιάζουν να βλάψουν τον εαυτό τους ή τους άλλους. Ένα σύστημα αναφοράς εγκληματικών ενεργειών με τέσσερις φόρμες αναφοράς (δηλ. έντυπο αναφοράς ή αναφοράς αποστολής, έντυπο αναφοράς συμβάντος εγκλήματος, έντυπο αναφοράς παρακολούθησης και έντυπο αναφοράς σύλληψης) και τρεις λειτουργικές ενότητες (π.χ. ενότητα συλλογής δεδομένων, ενότητα διαχείρισης-ελέγχου και μονάδα αξιοποίησης δεδομένων) περιγράφεται στο [41]. Στο [42] προτείνεται (για το Ριάντ) μια διαδικασία αναφορών που βοηθά τις αρχές να διαχειρίζονται αποτελεσματικότερα τις αναφορές. Μία υποδομή διακομιστή-πελάτη για έξυπνα τηλέφωνα, που έχει τη δυνατότητα να ανταλλάσσει διάφορες κατηγορίες πληροφοριών σχετικά με εγκληματικές πράξεις και με επιπλέον υπηρεσίες επιβολής του νόμου σε πραγματικό χρόνο, προτείνεται στο [43].

1.4 Ερευνητικά ερωτήματα

Με βάση τους στόχους της έρευνας και την ανασκόπηση της βιβλιογραφίας, τα ερευνητικά ερωτήματα που καλείται να απαντήσει η διατριβή είναι τα εξής:

1. Πώς μπορεί να αξιοποιηθεί η KBT για την παροχή αξιόπιστων επώνυμων και ανώνυμων ηλεκτρονικών υπηρεσιών σε αναφέροντες παραβατικών πράξεων; Ποιο

[11] https://www.saysomething.net/: "SHP is a national, nonprofit organization led by several family members whose loved ones were killed in the tragic mass shooting at Sandy Hook School on December 14, 2012. SHP is focused on preventing gun violence (and other forms of violence and victimization) BEFORE it happens by attracting, educating and mobilizing youth and adults to identify, intervene and get help for individuals who may be at-risk of hurting themselves or others – we achieve this through delivery of our four Know the Signs prevention programs."

είναι το πλαίσιο και ποια τα κύρια χαρακτηριστικά μιας πιθανής εφαρμογής;

2. Πώς μπορεί να αξιοποιηθεί η ΚΒΤ για τη δημιουργία ενός ασφαλέστερου AIS; Ποιο είναι το πλαίσιο και ποια τα κύρια χαρακτηριστικά μιας πιθανής εφαρμογής;

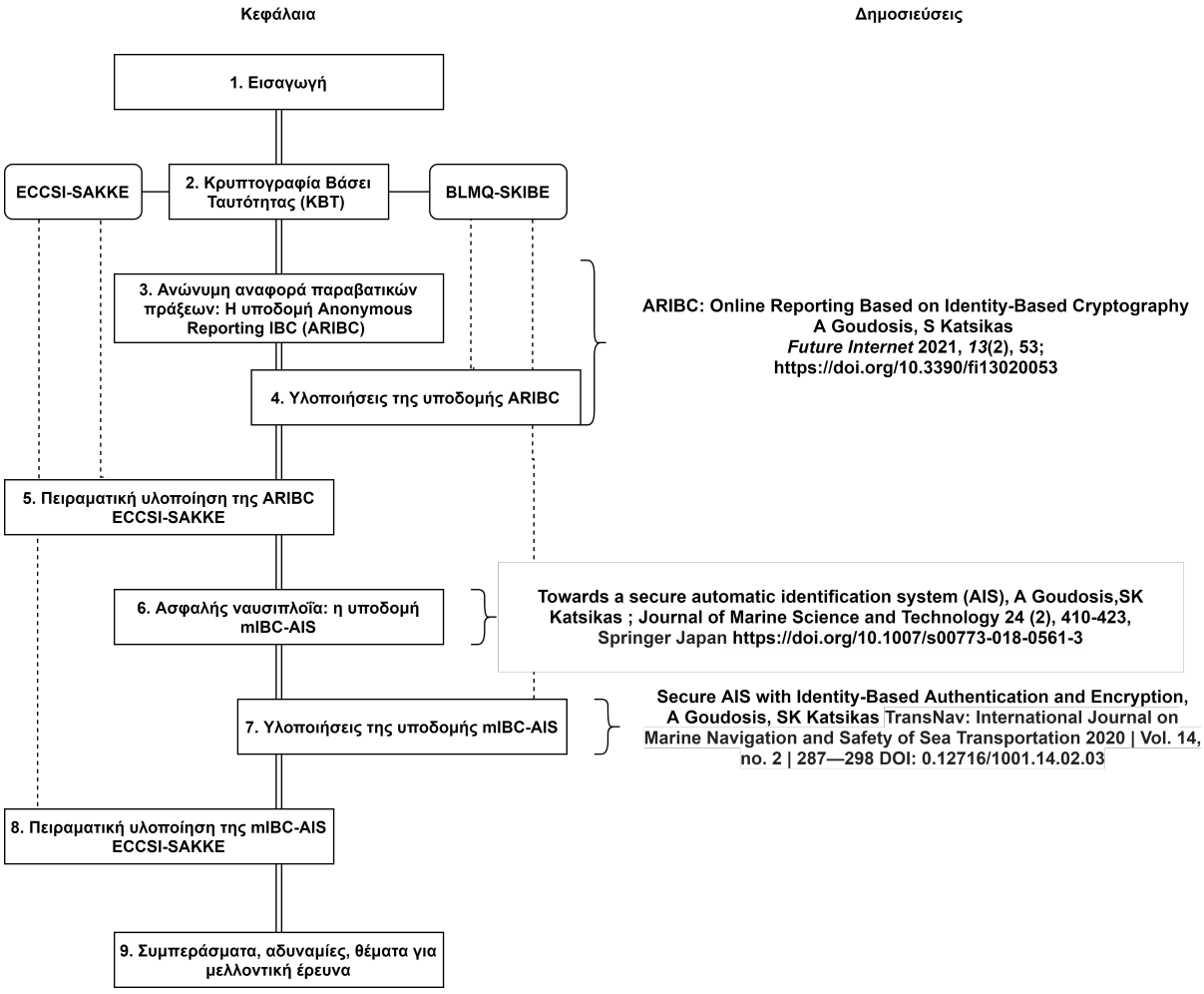
1.5 Επισκόπηση της διατριβής

Η διατριβή χωρίζεται σε τέσσερις ενότητες: Τα θεμέλια (κεφάλαια 1 και 2), το προτεινόμενο Anonymous Reporting IBC (κεφάλαια 3 έως 5), τα προτεινόμενα maritime-IBC (mIBC) και mIBC-AIS (κεφάλαια 6 έως 8) και, τέλος, τα συμπεράσματά μας, οι αδυναμίες της έρευνας και θέματα για μελλοντική έρευνα, που καταγράφονται στο κεφάλαιο 9.

Η πρώτη ενότητα περιλαμβάνει το παρόν εισαγωγικό κεφάλαιο, όπου σκιαγραφούμε το πλαίσιο αυτής της εργασίας και το 2ο κεφάλαιο, όπου παρουσιάζεται η κρυπτογραφική βάση στην οποία θεμελιώνουμε τις προτάσεις μας. Συγκεκριμένα, στο 2ο κεφάλαιο παρουσιάζονται λεπτομερώς τα σχήματα ΚΒΤ(IBC) που χρησιμοποιούνται στην εργασία μας: (α) ο μηχανισμός ψηφιακών υπογραφών BLMQ, (β) ο μηχανισμός κρυπτογράφησης Sakai-Kasahara Identity Based Encryption (SKIBE), όπως παρουσιάζεται στο IEEE1363.3 [16], (γ) ο μηχανισμός ψηφιακών υπογραφών Elliptic Curve-Based Certificateless Signatures IBC (ECCSI), όπως παρουσιάζεται στο RFC6507 [2] και, τέλος, (δ) ο μηχανισμός ενθυλάκωσης Sakai-Kasahara Key Encryption (SAKKE) , όπως παρουσιάζεται στο RFC6508 [3].

Η δεύτερη ενότητα (κεφάλαια 3, 4 και 5) είναι αφιερωμένη στην ηλεκτρονική διακυβέρνηση και ειδικότερα στην ανώνυμη αναφορά παραβατικών πράξεων. Στο κεφάλαιο 3 διερευνούμε τα χαρακτηριστικά των ανώνυμων αναφορών, προσδιορίζουμε τις απαιτήσεις ασφαλείας και σκιαγραφούμε την πρότασή μας (που ονομάζουμε ARIBC). Στο κεφάλαιο 4 διερευνούμε τα χαρακτηριστικά που προσδίδει στην πρότασή μας η χρήση του συνδυασμού του σχήματος ARIBC-BLMQ για έλεγχο της ακεραιότητας και ταυτοποίηση των δεδομένων και του σχήματος ARIBC-SKIBE για εμπιστευτική επικοινωνία. Στο κεφάλαιο 5 διερευνούμε τις ιδιότητες της πρότασής μας με χρήση του συνδυασμού των ARIBC-ECCSI για έλεγχο της ακεραιότητας και ταυτοποίηση των δεδομένων και του σχήματος ARIBC-SAKKE. Το τελευταίο χρησιμοποιείται ως το ενδιάμεσο βήμα για την εμπιστευτική επικοινωνία μέσω συμμετρικής κρυπτογράφησης και συγκεκριμένα για την έμπιστη, μέσω ενθυλάκωσης, αποστολή υλικού για τη δημιουργία του συμμετρικού κλειδιού συνόδου (session key). Τέλος, επιδεικνύουμε τη λειτουργία του προτεινόμενου ARIBC-ECCSI, μέσω ειδικά αναπτυγμένης εφαρμογής και πειραματικής υλοποίησης.

Η τρίτη ενότητα (κεφάλαια 6,7 και 8) είναι αφιερωμένη στην ασφάλεια του AIS. Στο κεφάλαιο 6 διερευνούμε το AIS και τα απαιτούμενα χαρακτηριστικά ενός ασφαλούς AIS και προτείνουμε το maritime-IBC (mIBC) ως βάση για ένα ασφαλές mIBC-AIS. Στο κεφάλαιο 7 διερευνούμε τα χαρακτηριστικά που προσδίδει στην πρότασή μας η χρήση του συνδυασμού αφενός του σχήματος mIBC-AIS-BLMQ για έλεγχο της ακεραιότητας και ταυτοποίηση των δεδομένων και αφετέρου του σχήματος mIBC-AIS-SKIBE για εμπιστευτική επικοινωνία. Στο κεφάλαιο 8 διερευνούμε τις ιδιότητες της πρότασής μας για το mIBC-AIS με τη χρήση του συνδυασμού αφενός του mIBC-AIS-ECCSI για έλεγχο της ακεραιότητας και ταυτοποίηση των δεδομένων και



Σχήμα 1.5: Δομή της διατριβής.

αφετέρου του σχήματος mIBC-AIS-SAKKE ως μέσου εμπιστευτικής μεταφοράς υλικού για τη δημιουργία συμμετρικών κλειδιών συνόδου, τα οποία θα χρησιμοποιηθούν σε εμπιστευτική επικοινωνία μέσω συμμετρικών αλγόριθμων κρυπτογράφησης. Τέλος, επιδεικνύουμε τη λειτουργία του mIBC-AIS ECCSI-SAKKE μέσω ειδικά αναπτυγμένης εφαρμογής και αντίστοιχης πειραματικής υλοποίησης.

Τέλος, το κεφάλαιο 9 αφιερώνεται στην ανακεφαλαίωση των συμπερασμάτων μας, στον σχολιασμό των αδυναμιών αυτής της έρευνας και στην παράθεση θεμάτων για μελλοντική έρευνα.

Στο Σχήμα 1.5, παρουσιάζουμε μια απεικόνιση της δομής αυτής της διατριβής, η οποία βοηθά τον αναγνώστη να παρακολουθήσει τη ροή των κεφαλαίων της.

Στον Πίνακα 1.1 απεικονίζεται η συσχέτιση μεταξύ των ερευνητικών ερωτημάτων και των κεφαλαίων της διατριβής.

1.6 Σύνοψη της συνεισφοράς της διατριβής

Η έρευνά μας προσθέτει στον τομέα της εφαρμοσμένης κρυπτογραφίας νέα πεδία εφαρμογής της κρυπτογράφησης βάσει ταυτότητας KBT (IBC) στους κλάδους της

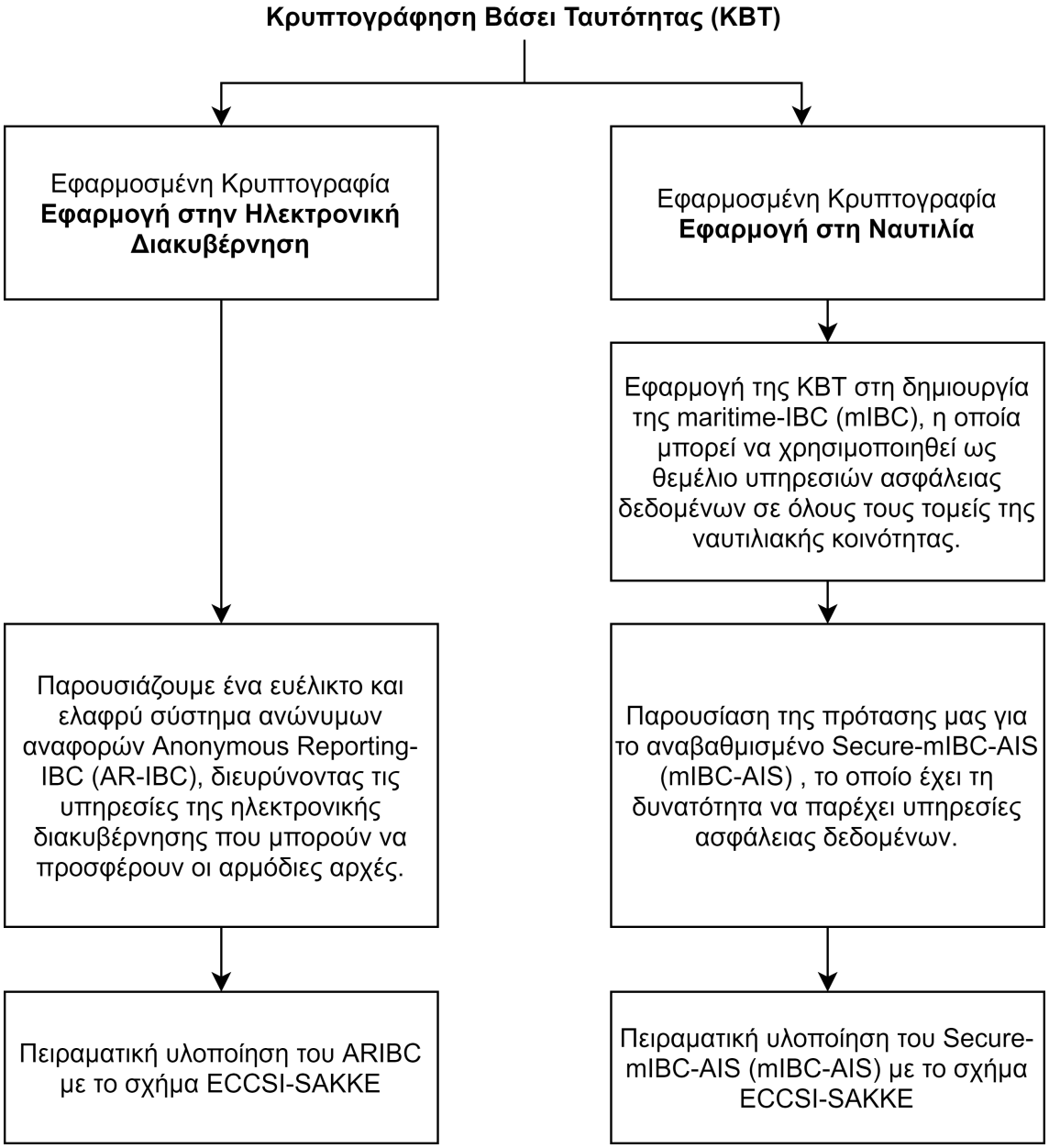
Ερευνητικά ερωτήματα	**Κεφάλαια**	**Δημοσιεύσεις**
Πώς θα αξιοποιηθεί η ΚΒΤ για την παροχή αξιόπιστων επώνυμων και ανώνυμων ηλεκτρονικών υπηρεσιών σε αναφέροντες παραβατικών πράξεων; Ποιο είναι το πλαίσιο και ποια τα κύρια χαρακτηριστικά μιας πιθανής εφαρμογής;	3, 4, 5	1."ARIBC: Online Reporting Based on Identity-Based Cryptography" Goudosis, A.; Katsikas, S. ; Future Internet 2021, 13, 53. ; https://doi.org/10.3390/fi13020053.
Πώς θα αξιοποιηθεί η ΚΒΤ για τη δημιουργία ενός ασφαλέστερου AIS; Ποιο είναι το πλαίσιο και ποια τα κύρια χαρακτηριστικά μιας πιθανής εφαρμογής;	6, 7, 8	2."Towards a secure automatic identification system (AIS)", A Goudosis, SK Katsikas, Journal of Marine Science and Technology 24 , 410-423, Springer Japan 3."Secure AIS with Identity-Based Authentication and Encryption", A Goudosis, SK Katsikas, TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 2020 Vol. 14, no. 2 287—298 DOI: 0.12716 1001.14.02.03;

Πίνακας 1.1: Συσχέτιση μεταξύ των ερευνητικών ερωτημάτων και των κεφαλαίων της διατριβής.

ηλεκτρονικής διακυβέρνησης και της ασφαλούς ναυσιπλοΐας. Συγκεκριμένα:

- Χρησιμοποιούμε την κρυπτογραφία βάσει ταυτότητας ΚΒΤ (IBC) ώστε να δημιουργήσουμε, και εν μέρει να υλοποιήσουμε πειραματικά, ένα ευέλικτο και ελαφρύ σύστημα ανώνυμων αναφορών Anonymous Reporting-IBC (AR-IBC), διευρύνοντας τις υπηρεσίες της ηλεκτρονικής διακυβέρνησης που μπορούν να προσφέρουν οι αρμόδιες αρχές.
- Η συνεισφορά μας στη ναυτιλία έχει δύο σκέλη:
    1. Στο 1ο σκέλος παρουσιάζουμε μια εφαρμογή της ΚΒΤ, την Maritime-IBC (mIBC), η οποία μπορεί να χρησιμοποιηθεί ως θεμέλιο υπηρεσιών ασφάλειας δεδομένων σε όλους τους τομείς της ναυτιλιακής κοινότητας.
    2. Στο 2ο σκέλος η προσφορά μας εξειδικεύεται, με την πρότασή μας για το αναβαθμισμένο Secure-mIBC-AIS (mIBC-AIS) , το οποίο έχει τη δυνατότητα να παρέχει υπηρεσίες ασφάλειας δεδομένων.

Σχηματική απεικόνιση της συνεισφοράς της διατριβής φαίνεται στο Σχήμα 1.6.



Σχήμα 1.6: Συνεισφορά της διατριβής.

Κεφάλαιο 2

Κρυπτογραφία Βάσει Ταυτότητας ΚΒΤ (IBC)

Αυτό το κεφάλαιο παρουσιάζει τα στοιχεία εκείνα της Κρυπτογραφίας Βάσει Ταυτότητας ΚΒΤ (IBC) στα οποία θεμελιώνεται η διατριβή. Το κεφάλαιο ξεκινά με μια γενική περιγραφή των χαρακτηριστικών της συγκεκριμένης μεθόδου και συνεχίζει με την παρουσίαση των κρυπτογραφικών σχημάτων που χρησιμοποιούνται στις προτάσεις μας.

Η ιδέα ενός συστήματος κρυπτογράφησης δημόσιου κλειδιού το οποίο θα χρησιμοποιούσε ως δημόσιο κλειδί ένα ευρέως γνωστό, διακριτό, αναγνωριστικό της ταυτότητας του κάθε χρήστη παρουσιάστηκε για πρώτη φορά από τον Shamir το 1984 [44]. Σ΄ αυτόν τον τύπο κρυπτογράφησης το δημόσιο κλειδί μπορεί να επιλέξουμε να είναι οποιοδήποτε διακριτό αναγνωριστικό, (π.χ. το όνομα μιας υπηρεσίας ή μιας διεύθυνσής της, η διεύθυνση ηλεκτρονικού ταχυδρομείου, ο αριθμός τηλεφώνου, ένας μοναδικός αναγνωριστικός αριθμός). Το αντίστοιχο ιδιωτικό κλειδί θα δημιουργηθεί από ένα αξιόπιστο κέντρο δημιουργίας ιδιωτικών κλειδιών.

Το κύριο κίνητρο αυτής της προσέγγισης είναι η εξάλειψη της ανάγκης χρήσης ψηφιακών πιστοποιητικών και, συνεπώς, των δυσκολιών στη διαχείρισή τους. Αυτός είναι ο λόγος για τον οποίο τέτοια σχήματα ονομάζονται *συστήματα κρυπτογράφησης δημόσιου κλειδιού χωρίς πιστοποιητικά*.

Η ιδέα, ωστόσο, παρέμεινε ανεκμετάλλευτη για αρκετό καιρό, λόγω του ότι δεν είχε συμπληρωθεί με πρόταση υλοποίησης. Μόνο στην αρχή της χιλιετίας οι εργασίες των Boneh και Franklin [45], [19] πρότειναν κάποια σχήματα της ΚΒΤ με καλές προοπτικές πρακτικής υλοποίησης. Και οι δύο εργασίες βασίζονται στα Διγραμμικά Ζεύγη πάνω σε Ελλειπτικές Καμπύλες (Bilinear Pairings on elliptic curves) σε πεπερασμένα πεδία και η ασφάλειά τους έγκειται σε παραλλαγές του υπολογιστικά δύσκολου προβλήματος Bilinear Diffie-Hellman (BDH). Περισσότερες τεχνικές πληροφορίες που σχετίζονται με την ΚΒΤ υπάρχουν στα [16], [46], [20], [22] [47, 48].

Έκτοτε, σχήματα ΚΒΤ έχουν χρησιμοποιηθεί σε πολλές διαφορετικές εφαρμογές, όπως: ασφάλεια δικτύου κινητών επικοινωνιών [6], ασφαλείς εφαρμογές ηλεκτρονικού ταχυδρομείου [8, 49], ασφάλεια σε εφαρμογές νέφους [9], ασφάλεια συστημάτων υγείας [10–12], ασφάλεια ηλεκτρονικής διακυβέρνησης [15], ασφάλεια έξυπνου

δικτύου ηλεκτρικής ενέργειας (smart grid) [50], ασφάλεια στην αεροπλοΐα και στη ναυσιπλοΐα [14, 51]. Τα διακριτά χαρακτηριστικά, τα οφέλη και τα μειονεκτήματα της ΚΒΤ έναντι των πιο παραδοσιακών Υποδομών Δημόσιου Κλειδιού - ΥΔΚ (PKI) έχουν συζητηθεί στα [52], [53].

2.1 Περιγραφή της ΚΒΤ

2.1.1 Εισαγωγή

Όπως αναφέραμε, η ΚΒΤ είναι μια παραλλαγή της κρυπτογράφησης δημόσιου κλειδιού που προτάθηκε ως λύση στο πρόβλημα της ασφαλούς διανομής των δημόσιων κλειδιών των χρηστών στις συνήθεις ΥΔΚ. Στις συνήθεις ΥΔΚ τα ιδιωτικά και τα δημόσια κλειδιά δημιουργούνται μαζί, ως ζεύγος κλειδιών, και η απομνημόνευσή τους είναι αδύνατη λόγω της μορφής και του μεγέθους τους. Αντίθετα, σε σχήματα ΚΒΤ το Ιδιωτικό Κλειδί του Χρήστη (ΙΚ) εξάγεται μέσω αλγορίθμου από ένα προεπιλεγμένο Δημόσιο Αναγνωριστικό του χρήστη (ΔΑ). Επειδή τα σχήματα ΚΒΤ έχουν τη δυνατότητα να χρησιμοποιούν μια αυθαίρετη συμβολοσειρά ως το ΔΑ, οποιοδήποτε διακριτό, δημόσια γνωστό, αναγνωριστικό του χρήστη μπορεί να χρησιμοποιηθεί ως το ΔΑ του. Στη συνέχεια, το αντίστοιχο ΙΚ εξάγεται από έναν Αξιόπιστο Κεντρικό Συντονιστή (ΑΚΣ), γνωστό επίσης ως Public Key Generator (PKG) ή Key Management Server (KMS), μέσω ειδικού αλγορίθμου εξαγωγής ΙΚ από το Δημόσιο Αναγνωριστικό (ΔΑ) του αντίστοιχου χρήστη. Αυτή η προσέγγιση εξαλείφει την ανάγκη χρήσης των πιστοποιητικών που χρησιμοποιούνται από τις σύγχρονες ΥΔΚ (π.χ. X509 based PKIs), επειδή το ΔΑ είναι γνωστό και κατανοητό στο κοινό. Ωστόσο, πρέπει να επισημάνουμε ότι αυτή η ευκολία συνοδεύεται και από ένα μεγάλο κόστος: τα ΙΚ είναι γνωστά, εκτός από τους κατόχους τους, και στον ΑΚΣ που τα δημιούργησε.

Μια υποκατηγορία των σχημάτων ΚΒΤ είναι αυτά που προσφέρουν Ενθυλάκωση Βάσει Ταυτότητας (ΕΒΤ) *(Identity-Based Key Encapsulation Mechanism (KEM)*). Αυτά τα σχήματα χρησιμοποιούνται για την εμπιστευτική μεταφορά παραμέτρων που θα χρησιμοποιηθούν από τον παραλήπτη για τη δημιουργία ενός συμμετρικού κλειδιού κρυπτογράφησης που θα αξιοποιηθεί αργότερα στην κρυπτογραφημένη, με ένα συμμετρικό αλγόριθμο, επικοινωνία[1] .

2.1.2 Συντμήσεις-Συμβολισμοί-Ορολογία

Δεν υπάρχουν ακόμα καθιερωμένες, μοναδικές συντμήσεις, συμβολισμοί και ορολογία για την ΚΒΤ και τις υποκατηγορίες της στη διεθνή βιβλιογραφία. Αυτή η πολυ-σημειογραφία πολλές φορές δυσκολεύει τον αναγνώστη να συγκρίνει μεθόδους και σχήματα της ΚΒΤ. Γι' αυτόν τον λόγο αποφασίσαμε να ακολουθήσουμε τις παρακάτω συμβάσεις:

- Όπου δεν δημιουργείται πρόβλημα, όπως στα εισαγωγικά κείμενα, χρησιμοποιούμε μεταφρασμένους όρους (π.χ. ΚΒΤ αντί ΙΒC).
- Στις προτάσεις μας, όπου βασιζόμαστε σε συγκεκριμένες μεθόδους, η ορολογία

[1] Στην ΚΒΤ ο αποστολέας κρυπτογραφεί το μυστικό μήνυμα και ο παραλήπτης το αποκρυπτογραφεί. Στην ΕΒΤ ο αποστολέας ενθυλακώνει (encapsulates) το μυστικό μήνυμα και ο παραλήπτης το αποθυλακώνει (decapsulates).

Περιγραφή	**IEEE 1363.3**	**ECCSI (RFC6507)**	**SAKKE (RFC6508)**
Δημόσιες παράμετροι (ΔΠ) της εφαρμογής μας.	(Public Parameters PP)	ECCSI Public Parameters (ECCSI-PP)	SAKKE Public Parameters (SAKKE-PP)
Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ)	Private Key Generator (PKG)	Key Management Server (KMS)	Key Management Server (KMS)
Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ) του Αξιόπιστου Κεντρικού Συντονιστή	PKG Master Secret (MS)	KMS ECCSI Secret Authentication Key (KSAK)	KMS SAKKE Secret Authentication Key (z_T)
Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ) του Αξιόπιστου Κεντρικού Συντονιστή	PKG Public key (MS_{pub})	KMS ECCSI Public Authentication key (KPAK)	KMS SAKKE Public Authentication key (Z_T)
Ιδιωτικό Κλειδί (ΙΚ) κάθε χρήστη	Private (Secret) key ($ID_{Private}$)	ECCSI private Secret Signing key (SSK)	SAKKE private Receiver's Secret key (RSK)
Δημόσιο Κλειδί / Δημόσιο Αναγνωριστικό (ΔΑ) χρήστη	ID	ID	ID

Πίνακας 2.1: Συσχέτιση της ορολογίας του IEEE 1363.3 και αυτής των ECCSI (RFC6507) SAKKE (RFC6508)

είναι στα Αγγλικά, όπως χρησιμοποιείται στις αντίστοιχες δημοσιεύσεις. Έτσι διευκολύνεται ο αναγνώστης στη συσχέτιση των γραφομένων μας με τις αντίστοιχες πηγές μας.

Στον πίνακα 2.1 παρουσιάζεται η συσχέτιση της ορολογίας του IEEE 1363.3 και αυτής των ECCSI (RFC6507) SAKKE (RFC6508).

Θεμελιώδεις διαδικασίες ενός συστήματος ΚΒΤ

Οι ακριβείς διαδικασίες και αλγόριθμοι εξαρτώνται από το επιλεγμένο σχήμα υλοποίησης της ΚΒΤ, σε κάθε περίπτωση όμως απαρτίζονται από τις εξής θεμελιώδεις κατηγορίες διαδικασιών:

1. Σχεδιασμός και Δημιουργία μιας εφαρμογής ΚΒΤ

   (α') Ορίζονται οι Δημόσιες Παράμετροι ΔΠ(*PP*) της σχεδιαζόμενης ΚΒΤ.

   (β') Επιλέγεται το Θεμελιώδες Μυστικό Κλειδί ΘΜΚ του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ)

   (γ') Υπολογίζεται, εκ του ΘΜΚ, το Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ-ΑΚΣ/MS_{Pub}) του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ).

   (δ') Εξάγονται τα Ιδιωτικά Κλειδιά (ΙΚ) των συμμετεχόντων χρηστών, μέσω συγκεκριμένων αλγορίθμων, από το ΘΜΚ του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ) και το Δημόσιο Αναγνωριστικό ΔΑ(*ID*) του κάθε χρήστη.

2. Υπηρεσία εμπιστευτικότητας

(α') Αλγόριθμοι είτε για κρυπτογράφηση είτε για ενθυλάκωση δεδομένων.

(β') Αλγόριθμοι για αποκρυπτογράφηση ή αποθυλάκωση δεδομένων αντίστοιχα.

3. Υπηρεσία ψηφιακών υπογραφών για ταυτοποίηση/ακεραιότητα

(α') Αλγόριθμοι για δημιουργία ψηφιακής υπογραφής δεδομένων.

(β') Αλγόριθμοι για επαλήθευση ψηφιακής υπογραφής.

2.1.3 Κύρια πλεονεκτήματα και μειονεκτήματα της ΚΒΤ

Σε αυτήν την ενότητα συζητούνται μειονεκτήματα και πλεονεκτήματα της ΚΒΤ σε σχέση με άλλες δημοφιλείς μεθοδολογίες:

ΚΒΤ έναντι Συμμετρικής Κρυπτογράφησης

Καμιά σύγχρονη κρυπτογράφηση δημόσιου κλειδιού δεν μπορεί να συγκριθεί με την απλότητα και την ταχύτητα που προσφέρει η συμμετρική κρυπτογράφηση. Αυτός είναι και ο λόγος για τον οποίο συνήθως σε επικοινωνίες με μεγάλο όγκο δεδομένων, όπως προτείνουμε και εμείς, προσπαθούμε να χρησιμοποιούμε μηχανισμούς συμμετρικής κρυπτογράφησης. Όμως η συμμετρική κρυπτογράφηση έχει δύο προβλήματα που η ΚΒΤ προσπαθεί να αντιμετωπίσει.

- Ο αριθμός των κλειδιών που απαιτούνται για την παροχή υπηρεσίας εμπιστευτικής επικοινωνίας σε ομάδες χρηστών ανά ζεύγη με ένα συμμετρικό αλγόριθμο δίνεται από τον τύπο $(n * (n-1)/2)$, όπου n ο αριθμός των χρηστών. Παρατηρούμε ότι ο αριθμός των συμμετρικών κλειδιών και αντίστοιχα η δυσκολία διαχείρισής τους αυξάνεται ταχύτατα με τον αριθμό των χρηστών. Η παρατήρηση αυτή έχει ακόμα μεγαλύτερη σημασία όταν συνδυαστεί με την επόμενη.

- Το δεύτερο πρόβλημα απορρέει από την ανάγκη για συχνή, σχετικά, αλλαγή του συμμετρικού κλειδιού. Διότι, σε περίπτωση που παραβιαστεί η εμπιστευτικότητα του κλειδιού, καταρρέει η εμπιστευτικότητα όλων των προηγούμενων συνομιλιών στις οποίες είχε χρησιμοποιηθεί το κλειδί αυτό. Συνεπώς, προτιμάται η χρήση συμμετρικών κλειδιών συνόδου τα οποία έχουν διάρκεια ζωής όσο και μια σύνοδος. Αυτό το πρόβλημα συνεπάγεται την ανάγκη ύπαρξης μιας μεθόδου ανταλλαγής αυτών των κλειδιών με ασφάλεια από τα αντίστοιχα μέρη. Οι επικρατούσες γενικές μέθοδοι, με πολλές παραλλαγές είναι:

  - Η αποστολή του συμμετρικού κλειδιού συνόδου μέσω ενός αλγορίθμου δημόσιου κλειδιού ο οποίος διασφαλίζει εκτός από την εμπιστευτικότητα, μέσω κρυπτογράφησης, και την πιστοποίηση και ακεραιότητα του κλειδιού, μέσω ψηφιακών υπογραφών. Η μέθοδος που προτείνουμε έχει ως βάση το σχήμα BLMQ-SKIBE.

  - Η ανταλλαγή, μεταξύ των μελών, πληροφοριών για τη δημιουργία ενός συμμετρικού κλειδιού χωρίς την ανάγκη αποστολής του ίδιου του μυστικού κλειδιού. Οι πιο διαδεδομένοι μηχανισμοί είναι παραλλαγές του μηχανισμού ανταλλαγής μυστικού κλειδιού Diffie-Hellman. Σημειώστε όμως ότι οι παραπάνω μηχανισμοί δεν προσφέρουν ούτε πιστοποίηση της ταυτότητας των μερών ούτε και της ακεραιότητας των δεδομένων, συνεπώς

χρειάζεται και κάποιος επιπλέον μηχανισμός ασφαλείας (π.χ. Κρυπτογράφηση Δημόσιου Κλειδιού). Η μέθοδος που προτείνουμε χρησιμοποιεί την παραπάνω γενική ιδέα, δηλαδή χρήση του μηχανισμού ECCSI για την πιστοποίηση των δεδομένων και του μηχανισμού SAKKE, αντί για Diffie-Hellman, για την έμπιστη ενθυλακωμένη αποστολή των πληροφοριών για τη δημιουργία του συμμετρικού κλειδιού συνόδου. Το πλεονέκτημα του μηχανισμού SAKKE είναι η αποστολή ενός μοναδικού μηνύματος, έναντι των μηχανισμών Diffie-Hellman, στους οποίους η απαίτηση ανταλλαγής μηνυμάτων θέλει τα μέρη σε κάποιου είδους σύγχρονη σύνοδο. Συνεπώς, ο μηχανισμός SAKKE είναι πολύ ευκολότερο να χρησιμοποιηθεί και σε σχήματα όπου υπάρχει ασύγχρονη επικοινωνία (π.χ. κρυπτογραφημένη αποστολή δεδομένων μέσω ηλεκτρονικού ταχυδρομείου).

ΚΒΤ έναντι ΚΔΚ (PKI) με πιστοποιητικό

Τρεις είναι οι μεγάλες διαφορές μεταξύ των τυπικών σχημάτων κρυπτογράφησης δημόσιου κλειδιού που χρησιμοποιούν πιστοποιητικά ΚΔΚ(PKI) και των ΚΒΤ που χρησιμοποιούμε εδώ. Όπως έχουμε ήδη συζητήσει, η πρώτη σχετίζεται με τη φύση των δημόσιων κλειδιών και η δεύτερη με τη δημιουργία των ιδιωτικών κλειδιών. Εν γένει θεωρείται ότι:

- Λόγω της απουσίας πιστοποιητικών, οι μηχανισμοί ΚΒΤ μπορεί να θεωρηθούν πιο εύχρηστοι και πιο εύκολοι στην υλοποίησή τους.
- Από την άλλη, η δημιουργία των ιδιωτικών κλειδιών από τους ΑΚΣ στις ΚΒΤ θεωρείται το μεγαλύτερο μειονέκτημα, μιας και προϋποθέτει αμέριστη εμπιστοσύνη στους ΑΚΣ. Σε ορισμένες όμως εφαρμογές μπορεί να είναι πλεονέκτημα, ιδιαίτερα όταν ο συντονιστής θέλει να έχει δυνατότητα πλήρους ελέγχου ή δυνατότητες ανάκτησης των μυστικών κλειδιών των χρηστών.
- Τέλος, αξίζει να επισημανθεί ακόμα μια ιδιαιτερότητα των ΚΒΤ η οποία δεν απαντάται σε άλλο είδος κρυπτογράφησης. Οποιοσδήποτε μπορεί να στείλει ένα κρυπτογραφημένο ή ενθυλακωμένο μήνυμα σε οποιονδήποτε άλλον, χωρίς να ανήκει κάποιος από αυτούς εξαρχής σε καμια υλοποίηση ΚΒΤ. Κάλλιστα ο Α μπορεί να κρυπτογραφήσει (ή ενθυλακώσει) ένα μήνυμα χρησιμοποιώντας ένα δημόσιο αναγνωριστικό του Β (ID_B) και τις δημόσιες παραμέτρους (ΔΠ) μιας υλοποίησης ΚΒΤ. Ο παραλήπτης Β εν συνεχεία επικοινωνεί με τη συγκεκριμένη ΚΒΤ, ταυτοποιείται (με άλλα μέσα), και παραλαμβάνει το ιδιωτικό κλειδί (ΙΚ) που αντιστοιχεί στο δημόσιο αναγνωριστικό (ID_B) που χρησιμοποιήθηκε για την κρυπτογράφηση (ή ενθυλάκωση) του μηνύματος.

Μια εναλλακτική πρόταση για το πρόβλημα της γνώσης των ιδιωτικών κλειδιών των χρηστών από τον ΑΚΣ παρουσιάστηκε στο [54] ως Κρυπτογράφηση Δημόσιου Κλειδιού Χωρίς Πιστοποιητικό (Certificateless Public Key Cryptography). Σ' αυτήν την προσέγγιση ο ΑΚΣ υπολογίζει μόνο ένα μέρος του ιδιωτικού κλειδιού του χρήστη *A* με βάση το δημόσιο αναγνωριστικό του ID_A. Έπειτα ο χρήστης *A* συνδυάζει το μερικό ιδιωτικό κλειδί με κάποιες μυστικές πληροφορίες (γνωστές μόνο σε εκείνον) προκειμένου να δημιουργήσει το τελικό ιδιωτικό κλειδί του ($ID_{Private}$) το οποίο δεν είναι γνωστό στον ΑΚΣ. Στη συνέχεια, ο χρήστης συνδυάζει τις δημόσιες παραμέτρους

ΔΠ(PP) του ΑΚΣ και συνδυάζει το τελικό ιδιωτικό κλειδί του ($ID_{Private}$) προκειμένου να δημιουργήσει το δημόσιο κλειδί του. Το πλεονέκτημα εδώ είναι ότι αυτό το δημόσιο κλειδί δεν χρειάζεται πλέον να πιστοποιηθεί, καθώς περιέχει την ταυτότητα του χρήστη. Εάν το κέντρο δημιουργίας κλειδιών (ΑΚΣ) είναι αξιόπιστο, και οι δημόσιες παράμετροι του κέντρου δημιουργίας κλειδιών είναι αυθεντικές, μπορεί να υποθέσει κανείς ότι ο χρήστης που σχετίζεται με το αναγνωριστικό ID_A αντιστοιχεί πραγματικά στον A. Ωστόσο, το σχήμα αυτό δεν μπορεί να χαρακτηριστεί ως πραγματική Κρυπτογράφηση Βάσει Ταυτότητας ΚΒΤ (IBC).

Η λεπτομερής ανάλυση των πλεονεκτημάτων και μειονεκτημάτων της ΚΒΤ, εκτός του ότι είναι πέραν των στόχων αυτής της διατριβής, θα απαιτούσε και ανάλυση υποκατηγοριών και εξειδίκευση των εκάστοτε παραμέτρων. Κάτω από αυτό το πρίσμα, θεωρούμε την παρακάτω παράθεση επαρκή επιστημονικά και αξιοποιήσιμη από τον αναγνώστη.

Πλεονεκτήματα:

- Το Δημόσιο κλειδί κάθε οντότητας είναι το δημόσιο αναγνωριστικό (ΔΑ) του. Επομένως, δεν υπάρχει ανάγκη για μεθόδους ελέγχου της αυθεντικότητας του δημόσιου κλειδιού, όπως γίνεται με τον έλεγχο των ψηφιακών πιστοποιητικών στα παραδοσιακά σχήματα κρυπτογραφίας δημόσιου κλειδιού.
- Άμεσο αποτέλεσμα της παραπάνω ιδιότητας της ΚΒΤ είναι οτι η εφαρμογή ενός σχήματος ΚΒΤ είναι απλούστερη και χρειάζεται λιγότερους πόρους συγκριτικά με τα παραδοσιακά σχήματα κρυπτογραφίας δημόσιου κλειδιού [6], [55], [56], [57].

Μειονεκτήματα:

- Το βασικότερο μειονέκτημα των ΚΒΤ είναι ότι πέρα από τον κάτοχο του κλειδιού, και ο Αξιόπιστος Κεντρικος Συντονιστής (ΑΚΣ) γνωρίζει τα ιδιωτικά κλειδιά (ΙΚ) των χρηστών.

2.2 Συνδυαστικό σχήμα BLMQ και SKIBE

Στη συνέχεια παρουσιάζουμε ένα συνδυαστικό σχήμα ΚΒΤ βασισμένο στην έρευνα των Sakai-Kasahara [18] και συγκεκριμένα στους μηχανισμούς που προτείνονται στο IEEE 1363.3-2013 “Standard for Identity-Based Cryptographic Techniques using Pairings”:

- Χρήση του μηχανισμού BLMQ [22] [16] για την ταυτοποίηση και την προστασία της ακεραιότητας των δεδομένων μέσω ψηφιακών υπογραφών [2].
- Χρήση του μηχανισμού SKIBE: Sakai-Kasahara Identity Based Encryption [18], [20], [16] για την προστασία της εμπιστευτικότητας των δεδομένων μέσω κρυπτογράφησης.

Σημειώνουμε ότι η ασφάλεια των μηχανισμών Sakai-Kasahara έχει αποδειχθεί στο [20].

Ακολουθώντας τα βήματα εφαρμογής των ΚΒΤ της ενότητας 2.1.2 ορίζουμε τις διαδικασίες και τους αντίστοιχους αλγορίθμους για το συνδυαστικό σχήμα BLMQ και

[2] Όπως αναφέρεται στο [21] στη σελ.15, το BLMQ ¨... είναι ουσιαστικά το σχήμα υπογραφής των Sakai-Kasahara¨

SKIBE.

Τα σύμβολα που εμφανίζονται στον Πίνακα 2.2[3] θα χρησιμοποιηθούν στη συνέχεια, όπου χρησιμοποιούμε το σχήμα BLMQ-SKIBE.

2.2.1 Ορισμός δημόσιων παραμέτρων (ΔΠ/PP)

Εν γένει συνιστάται [16] η χρήση παραμέτρων που είναι ευρύτερα αναγνωρισμένες. Ακολούθως παραθέτουμε τις κύριες δημόσιες παραμέτρους που πρέπει να συμφωνηθούν πριν από κάθε εφαρμογή του σχήματος.

1. Επιλέγουμε μια παράμετρο ασφαλείας (t) η οποία είναι το μέγεθος (σε bits) ενός πρώτου (prime) αριθμού p. Σημειώνεται ότι το επίπεδο ασφάλειας κάθε εφαρμογής ΚΒΤ είναι ανάλογο με το μέγεθος του t, αλλά η απόδοσή της είναι αντιστρόφως ανάλογη μ' αυτό.

2. Επιλέγουμε έναν πρώτο (prime) αριθμό p μεγέθους t bits, που καθορίζει την τάξη της διγραμμικής απεικόνισης (bilinear mapping) των κυκλικών ομάδων G_1, G_2, $G_{T(target)}$ που θα δημιουργηθούν σε επόμενα βήματα.

3. Επιλέγουμε κατάλληλη ελλειπτική Καμπύλη (Elliptic Curve)

4. Παράγουμε τρείς διγραμμικές απεικονίσεις των πεπερασμένων κυκλικών υποομάδων G_1, G_2, $G_{T(arget)}$ τάξης $p > 2^t$ σημείων της ελλειπτικής καμπύλης, ακολουθώντας τις οδηγίες στα [20], [22], και [46].

5. Ακολουθώντας τις υποδείξεις των RFC5091, FIPS186-2 διαλέγουμε μια γεννήτρια τυχαίων αριθμών R.

6. Επιλέγουμε $P_{G_2} \in G_2$ τυχαίο γεννήτορα της πεπερασμένης κυκλικής υποομάδας G_2 σημείων της ελλειπτικής καμπύλης και κατάλληλο τυχαίο γεννήτορα $P_{G_1} \in G_1$ της πεπερασμένης κυκλικής υποομάδας G_1 σημείων της ελλειπτικής καμπύλης, τέτοιους ώστε να υπάρχει ένας αποτελεσματικός ισομορφισμός $\phi : G_2 \rightarrow G_1$ τέτοιος ώστε $P_{G_1} = \phi(P_{G_2})$.

7. Δηλώνουμε ως e την αντιστοίχιση (bilinear pairing mapping) $e : G_1 \times G_2 \rightarrow G_{T(target)}$. Για να βελτιώσουμε την αποτελεσματικότητα του σχήματος, έχουμε τη δυνατότητα να υπολογίσουμε και να αποθηκεύσουμε τη σταθερή τιμή αντιστοίχισης $e(P_{G_1}, P_{G_2}) \in G_{T(target)}$.

8. Ορίζουμε τις συναρτήσεις κατακερματισμού που θα χρησιμοποιηθούν:

   (α') H_1**:** $\{0,1\}^* \rightarrow \mathbb{Z}_p^*$, όπου p = τάξη των G_1, G_2, G_T, είναι μια κρυπτογραφική συνάρτηση κατακερματισμού που χρησιμοποιείται για τον κατακερματισμό των αναγνωριστικών των χρηστών (ID) [46]. Στο [16] προτείνεται η χρήση των Secure Hash Algorithms (SHA) [58][4]. Περισσότερες λεπτομέρειες υπάρχουν στις ενότητες 5.2.6 και 6.1.1 του [16]. Σημειώνουμε ότι η H_1 χρησιμοποιείται τόσο στην υπηρεσία αυθεντικότητας και ακεραιότητας δεδομένων όσο και στην υπηρεσία εμπιστευτικότητας.

[3] Προσαρμογή σε αυτήν την εργασία της ενότητας "5. Mathematical conventions", στη σελίδα 12 του προτύπου IEEE 1363.3.

[4] Σύμφωνα με την τιμή της παραμέτρου ασφαλείας t: t=80/SHA-1, t=112/SHA-224, t=128/SHA-256, t=192/SHA-384, t=256/SHA-512. [16]

Σύμβολο	**Ερμηνεία**
GF_p	Πεπερασμένο Σώμα αποτελούμενο από p στοιχεία, αναπαριστάται ως ακέραιοι *modulo* p, όπου p πρώτος (¨prime¨) αριθμός
GF_q	Πεπερασμένο Σώμα αποτελούμενο από q στοιχεία, όπου q το αποτέλεσμα πρώτου ("prime") αριθμού υψωμένου σε δύναμη.
E/GF_q	Η *ελλειπτική καμπύλη* που ορίζεται πάνω στο Πεπερασμένο Σώμα GF_q,
$E(GF_q)$	Η προσθετική ομάδα σημείων πάνω στην παραπάνω ελλειπτική καμπύλη E/GF_q
G_x	Πεπερασμένη, τάξης πρώτου αριθμού, κυκλική ομάδα x, υπομάδα σημείων της ελλειπτικής καμπύλης
P_{G_x}	Ένας *γεννήτορας* του G_x
$e : G_1 \times G_2 \rightarrow G_T$	Ζεύξη (pairing-bilinear mapping): μια αποδοτικά υπολογίσιμη συνάρτηση.
$\mathbb{Z}_x$	Το σύνολο των ακεραίων modulo x
t	Παράμετρος ασφαλείας, μέγεθος (σε bits) του p ($p > 2^t$), όπου p τάξη της Διγραμμικής Απεικόνισης της κυκλικής ομάδας G_x
ϕ	Ισομορφισμός $\phi : G_Y \rightarrow G_X$ τέτοιος ώστε $\exists P_{G_X} = \phi(P_{G_Y})$, όπου P_{G_Y} τυχαίος γεννήτορας του G_Y
MS_{Secret}	Το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ), πολύ μεγάλος τυχαίος ακέραιος
MS_{Pub}	Το Θεμελιώδες Δημόσιο κλειδί (ΘΔΚ), σημείο στην ελλειπτική καμπύλη
ID_x ή σκέτο ¨X¨	Το Δημόσιο Αναγνωριστικό του x
$ID_{Private}$	Το Ιδιωτικό κλειδί που εξάγεται από το ID_x
PP	Οι Δημόσιες Παράμετροι της συγκεκριμένης υλοποίησης
$X \oplus Y$	Το δυαδικό XOR των στοιχείων των X και Y (που έχουν το ίδιο μέγεθος)
R	Επιλεγμένος γεννήτορας τυχαίων αριθμών
r	Τυχαίος ακέραιος
Plaintext	Το αρχικό (μη κρυπτογραφημένο) μήνυμα
Ciphertext(c)	Το κρυπτογραφημένο) μήνυμα.

Πίνακας 2.2: Σύμβολα του σχήματος BLMQ-SKIBE

(β') H_2: $\{0,1\}^* \times G_T \rightarrow \mathbb{Z}_p^*$ είναι μια κρυπτογραφική συνάρτηση κατακερματισμού. Σημειώνουμε ότι η H_2 χρησιμοποιείται μόνο στην υπηρεσία αυθεντικότητας και ακεραιότητας δεδομένων.

(γ') H_3: $G_T \rightarrow \{0,1\}^{length}$ είναι μια κρυπτογραφική συνάρτηση κατακερματισμού που χρησιμοποιείται για το *XOR* των μεταδιδόμενων δεδομένων. Περισσότερες λεπτομέρειες υπάρχουν στις ενότητες 5.2.6 και 6.1.1 του [16]. Η H_3 χρησιμοποιείται μόνο στην υπηρεσία εμπιστευτικότητας.

(δ') H_4: $\{0,1\}^{length} \times \{0,1\}^{length} \rightarrow \mathbb{Z}_p^*$. Η H_4 χρησιμοποιείται μόνο στην υπηρεσία εμπιστευτικότητας.

(ε') H_5: $\{0,1\}^{length} \rightarrow \{0,1\}^{length}$ προκειμένου να γίνει XOR με το πρωτότυπο μήνυμα. Η H_5 χρησιμοποιείται μόνο στην υπηρεσία εμπιστευτικότητας.

2.2.2 Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ) και Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ)

1. Επιλέγουμε τυχαίο ακέραιο αριθμό ως το *Θεμελιώδες Μυστικό κλειδί (ΘΜΚ)*/(MS_{Sec}) $\in \mathbb{Z}_p^*$ της παρούσας υλοποίησης ΚΒΤ, όπου p η τάξη της Διγραμμικής Απεικόνισης στην κυκλική ομάδα G_x. Επισημαίνουμε ότι το Θεμελιώδες Μυστικό κλειδί (ΘΜΚ)/MS_{Sec} είναι το ίδιο ευαίσθητο με το ιδιωτικό κλειδί μιας Αρχής Πιστοποίησης σε μια από τις συνήθεις υλοποιήσεις ΥΔΚ με πιστοποιητικά (X509 PKI).

2. Υπολογίζουμε το *Δημόσιο Κλειδί (ΘΔΚ)/(MS_{Pub})* χρησιμοποιώντας πολλαπλασιασμό ελλειπτικών καμπυλών και συγκεκριμένα πολλαπλασιάζοντας MS_{Sec} φορές το σημείο P_{G_2} το οποίο είναι γεννήτορας της κυκλικής ομάδας G_2, $MS_{Pub} = [MS_{Sec}]P_{G_2}$. Υπενθυμίζουμε ότι το MS_{Sec} είναι ακέραιος αριθμός και το P_{G_2} είναι σημείο πάνω στην ελλειπτική καμπύλη, [59]. Σημειώνουμε ότι είναι εξίσου ασφαλές να ορίσουμε το $MS_{Pub} \in G_2$.

3. Ο Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ) δημοσιεύει το ΘΔΚ/(MS_{Pub}) και τις Δημόσιες Παραμέτρους ΔΠ/(*PP*), δηλαδή τις (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, $e(P_{G_1}, P_{G_2})$, ϕ , H_1, H_2, H_3, H_4, H_5). Αυτές οι παράμετροι είναι στατικές και οι χρήστες της συγκεκριμένης υλοποίησης ΚΒΤ μπορούν να τις αποθηκεύσουν για μελλοντική χρήση.

2.2.3 Εξαγωγή του Ιδιωτικού Κλειδιού του χρήστη ($ID_{Private}$)

Το Ιδιωτικό Κλειδί ($ID_{Private}$) εξάγεται από τον Αξιόπιστο Κεντρικό Συντονιστή (ΑΚΣ) με τη χρήση του μοναδικού αναγνωριστικού *ID* του χρήστη, του *Θεμελιώδους Μυστικού Κλειδιού ΘΜΚ/(MS_{Sec})* του ΑΚΣ και των Δημόσιων Παραμέτρων ΔΠ(*PP*).

Τα βήματα είναι, σύμφωνα με το [59]:

1. Εκφράζουμε το *ID* του χρήστη σε bits $\in \{0,1\}$
2. Υπολογίζουμε τη συνάρτηση κατακερματισμού $H_1(ID)$
3. Υπολογίζουμε το ιδιωτικό κλειδί $ID_{Private} = \frac{P_{G_2}}{H_1(ID)+MS_{Sec}}$

2.2.4 Ακεραιότητα και Πιστοποίηση με το μηχανισμό ψηφιακής υπογραφής BLMQ

Ο μηχανισμός BLMQ παρέχει τους αλγορίθμους ψηφιακής υπογραφής δεδομένων καθώς και τους αντίστοιχους αλγορίθμους επαλήθευσής της. Στη συνήθη διαδικασία ψηφιακής υπογραφής και επαλήθευσης συμμετέχουν δύο οντότητες, ο Υπογράφων (Signer) και ο Επαληθευτής (Verifier). Ο Υπογράφων υπογράφει τα δεδομένα με την ψηφιακή του υπογραφή και ο Επαληθευτής επαληθεύει την εγκυρότητα της υπογραφής προκειμένου να πιστοποιήσει την αυθεντικότητα και την ακεραιότητα των υπογεγραμμένων δεδομένων. Ο Υπογράφων πρέπει να είναι οποιοσδήποτε εγγεγραμμένος χρήστης μιας υλοποίησης KBT. Ο Επαληθευτής μπορεί να είναι οποιοσδήποτε, αρκεί να γνωρίζει το αναγνωριστικό του Υπογράφοντα ID_{Signer}. Ο μηχανισμός BLMQ, όπως παρουσιάζεται στα [22], [16], υλοποιείται μέσω δύο διαδικασιών: τη διαδικασία Δημιουργίας Ψηφιακής Υπογραφής των δεδομένων (Signature Generation) και τη διαδικασία Επαλήθευσης της Ψηφιακής Υπογραφής (Signature Verification). Σημειώνουμε ότι στα παραδείγματά μας ακολουθούμε το [22] και δηλώνουμε το $MS_{Pub} \in G_1, ID_{Private} \in G_2$ προς αποφυγή των πράξεων στο G_2 κατά την επαλήθευση της ψηφιακής υπογραφής. Όμως, όπως σημειώνεται στη βιβλιογραφία[5], θα ήταν εξίσου ασφαλής η δήλωση του $MS_{Pub} \in G_2$, του $MS_{Sec} \in G_1$ και του υπογεγραμμένου μηνύματος στο $\{0,1\}^* \times \mathbb{Z}_{\kappa}^* \times G_1$, προκειμένου να μειωθεί το μέγεθος της υπογραφής.

Διαδικασία Δημιουργίας Ψηφιακής Υπογραφής υπό το μηχανισμό BLMQ

Δεδομένα Εισόδου

1. Τα δεδομένα προς υπογραφή DATA: $DATA \in \{0,1\}^{length}$, (όπου *length* = το μέγεθος των δεδομένων σε bits)
2. Οι Δημόσιες Παράμετροι (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, MS_{Pub}, $e(P_{G_1}, P_{G_2})$, φ , H_2)
3. Το Ιδιωτικό κλειδί του Υπογράφοντα $ID_{Private}$
4. Ένας τυχαίος ακέραιος r, τέτοιος ώστε $(0 < r < p - 1]$, εξαγόμενος από τον γεννήτορα R που περιγράψαμε στην ενότητα 2.2.1.

Αλγόριθμος

1. $u = e(P_{G_1}, P_{G_2})^r$, όπου e είναι η αντιστοίχιση $e(P_{G_1}, P_{G_2}) \in G_T$
2. $h = H_2(DATA, u), H_2$, όπου H_2 η συνάρτηση κατακερματισμού που έχει ορισθεί στις Δημόσιες Παραμέτρους.
3. $S = (r + h)ID_{Private}$.

Αποτέλεσμα

Η Ψηφιακή Υπογραφή είναι η τριάδα:

$$Signature = [DATA, h, S] \in [\{0,1\}^{length} \times \mathbb{Z}_p \times G_2]$$

.

[5]Στο [22], και ιδιαίτερα στην ενότητα 9.1, σελ. 60 του [16]

Διαδικασία Επαλήθευσης Ψηφιακής Υπογραφής υπό το μηχανισμό BLMQ

Δεδομένα Εισόδου

1. Η ψηφιακή υπογραφή προς επαλήθευση: $Signature = [DATA, h, S] \in [0, 1]^{length} \times \in \mathbb{Z}_p \times G_2]$
2. Οι Δημόσιες Παράμετροι: $(PP = (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, MS_{Pub}, e(P_{G_1}, P_{G_2}), \phi, H_1, H_2)$
3. Το Δημόσιο αναγνωριστικό του Υπογράφοντα: ID_{Signer}.

Αλγόριθμος

1. $u = \frac{e(S, H_1(ID_{signer})P_{G_1} + MS_{Pub})}{e(P_{G_1}, P_{G_2})^h}$
2. $H_2(DATA, u)$

Αποτέλεσμα

3. Εάν και μόνο εάν $h = H_2(DATA, u)$, η ψηφιακή υπογραφή επαληθεύεται, ειδάλλως η ψηφιακή υπογραφή δεν επαληθεύεται.

2.2.5 Εμπιστευτικότητα υπό το μηχανισμό SKIBE

Ο μηχανισμός SKIBE παρέχει αλγορίθμους κρυπτογράφησης δεδομένων καθώς και τους αντίστοιχους αλγορίθμους αποκρυπτογράφησής τους. Στη συνήθη διαδικασία εμπιστευτικής επικοινωνίας συμμετέχουν δύο οντότητες, ο Αποστολέας (Sender) ο οποίος κρυπτογραφεί τα δεδομένα χρησιμοποιώντας το δημόσιο αναγνωριστικό του Παραλήπτη (Recipient), ο οποίος στη συνέχεια αποκρυπτογραφεί τα δεδομένα.

Στη συνέχεια παρουσιάζουμε την προσαρμογή της πρότασής μας στους αλγορίθμους του μηχανισμού SKIBE, όπως παρουσιάζονται στην Ενότητα 3 του [20].

Διαδικασία Κρυπτογράφησης υπό τον μηχανισμό SKIBE

Δεδομένα Εισόδου

1. Τα αρχικά δεδομένα τα οποία θα κρυπτογραφηθούν $Plaintext \in \{0, 1\}^{length}$, (όπου $length$ = το μέγεθος σε bits)
2. Οι Δημόσιες Παράμετροι, $PP = (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, MS_{Pub}, e(P_{G_1}, P_{G_2}), \phi, H_1, H_3, H_4, H_5)$
3. Ένας τυχαίος ακέραιος $\sigma \in \{0, 1\}^{length}$, εξαγόμενος από τον γεννήτορα R που περιγράψαμε στην ενότητα 2.2.1
4. Το δημόσιο αναγνωριστικό του Παραλήπτη $ID_{Recipient} \in \{0, 1\}^*$

Αλγόριθμος

1. $r = H_4(\sigma, Plaintext)$ όπου H_4: $\{0, 1\}^{length} \times \{0, 1\}^{length} \rightarrow \mathbb{Z}_p^*$
2. $g^r = e(P_{G_1}, P_{G_2})^r$
3. $Q = (H_1(ID_{Recipient})P_{G_1} + MS_{Pub})$, όπου H_1: $\{0, 1\}^* \rightarrow \mathbb{Z}_p^*$
4. $U = r(Q)$

5. $V = \sigma \oplus H_3(g^r)$ όπου H_3: $G_T \rightarrow \{0, 1\}^{length}$
6. $W = Plaintext \oplus H_5(\sigma)$ όπου H_5: $\{0, 1\}^{length} \rightarrow \{0, 1\}^{length}$
7. $c = (rQ, \sigma \oplus H_3(g^r), Plaintext \oplus H_5(\sigma)) = (U, V, W) \in (G_1 \times \{0, 1\}^{length} \times \{0, 1\}^{length})$

Αποτέλεσμα

Το αποτέλεσμα είναι η τριάδα:

$$Ciphertext(c) = (U, V, W) \in (G_1 \times \{0, 1\}^{length} \times \{0, 1\}^{length})$$

Διαδικασία Αποκρυπτογράφησης υπό τον μηχανισμό SKIBE

Δεδομένα Εισόδου

1. Οι Δημόσιες Παράμετροι $PP = (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, MS_{Pub}, e(P_{G_1}, P_{G_2}), \varphi, H_1, H_3, H_4, H_5)$
2. Το Ιδιωτικό κλειδί του Παραλήπτη $Recipient_{Private} \in G_2$

Αλγόριθμος

1. $g' = e(U, Recipient_{Private})$
2. $\sigma' = V \oplus H_3(g')$
3. $m' = W \oplus H_5(\sigma')$
4. $r' = H_4(\sigma', m')$

Αποτέλεσμα

5. Εάν και μόνο εάν $U = r'(H_1(ID_{recipient})P_{G_1} + MS_{Pub})$, το αποκρυπτογραφημένο μήνυμα m' επαληθεύεται, δηλαδή $m' = Plaintext$, ειδάλλως το αποκρυπτογραφημένο μήνυμα θεωρείται πλαστό ή εσφαλμένο.

2.3 Συνδυαστικό σχήμα ECCSI (RFC6507) και SAKKE (RFC6508)

Το σχήμα ECCSI-SAKKE παρουσιάστηκε σε δύο RFCs από τον M. Groves. Το σχήμα προτείνει συγκεκριμένους αλγορίθμους υλοποίησης ΚΒΤ (IBC) τόσο για υπηρεσίες πιστοποίησης δεδομένων μέσω ψηφιακών υπογραφών, όσο και για υπηρεσίες εμπιστευτικότητας μέσω της εμπιστευτικής ενθυλάκωσης και αποστολής υλικού για τη δημιουργία διαμοιραζόμενου συμμετρικού κλειδιού συνόδου (symmetric session key). Συγκεκριμένα, το σχήμα αποτελείται απο:

1. Το RFC6507 Elliptic Curve-based Certificateless Signatures for Identity-based encryption (ECCSI) [2]. Τον μηχανισμό ECCSI (RFC6507) τον χρησιμοποιούμε για πιστοποίηση της προέλευσης των δεδομένων (data origin authentication) και για ακεραιότητα δεδομένων (data integrity). Σημειώνουμε ότι ο μηχανισμός ECCSI είναι ο πάροχος της λειτουργίας ελέγχου ταυτότητας και ακεραιότητας και για τον μηχανισμό ενθυλάκωσης του συμμετρικού κλειδιού συνόδου SAKKE.

2. Το RFC6508 Sakai-Kasahara Key Encryption (SAKKE) [3], το οποίο, σύμφωνα με το ίδιο το RFC6508 το βρίσκουμε και στο πρότυπο IEEE P.1363-3 ως SK-KEM [16]. Ο μηχανισμός SAKKE (RFC6508) χρησιμοποιείται για την ασφαλή ενθυλάκωση και αποστολή υλικού για τη δημιουργία ενός συμμετρικού κλειδιού συνόδου (π.χ. (AES session key).

3. Τα παραπάνω RFCs μαζί με το RFC6509 [60] αποτελούν το σχήμα MIKEY-SAKKE το οποίο χαρακτηρίζεται από το National Cyber Security Centre (NCSC) του Ηνωμένου Βασιλείου ως ένα ανοικτό κρυπτογραφικό πρότυπο. Περισσότερες λεπτομέρειες υπάρχουν στα [61], [62]. Το συγκεκριμένο πρότυπο δεν χρησιμοποιείται σ' αυτήν τη διατριβή και παρατίθεται για λόγους πληρότητας.

Στο σχήμα 2.1 παρουσιάζεται η χρήση του συνδυαστικού σχήματος ECCSI-SAKKE, όπως αυτό χρησιμοποιείται σ' αυτήν τη διατριβή.

2.3.1 Γιατί το σχήμα ECCSI-SAKKE αντί του BLMQ-SKIBE;

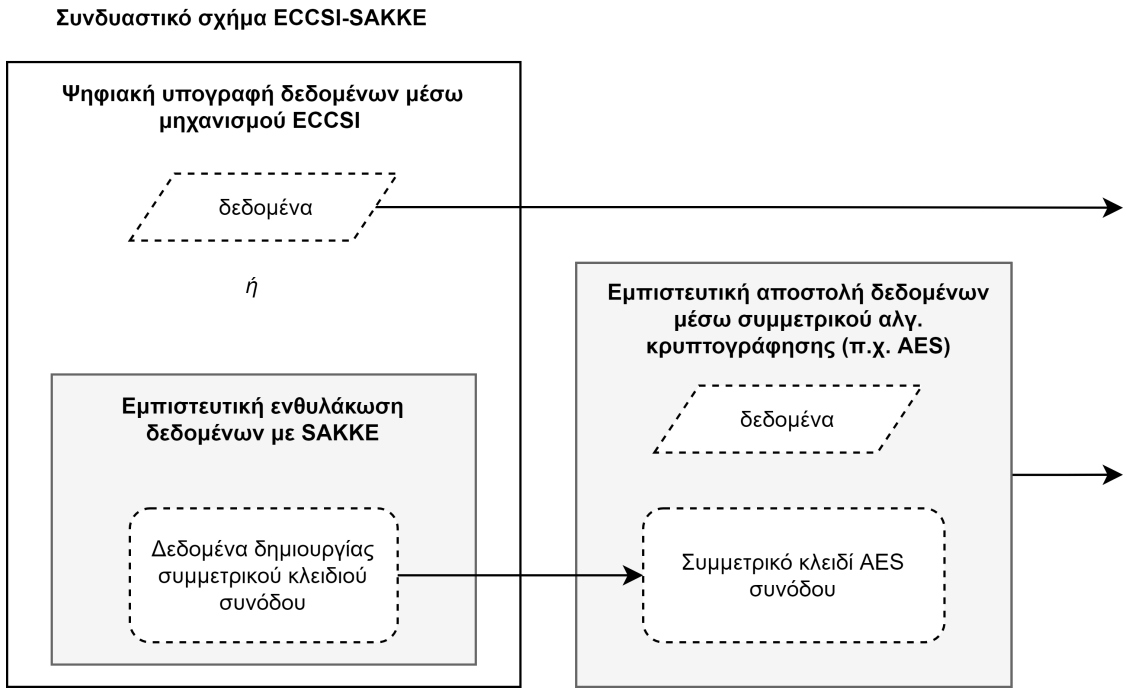
Η διατριβή χρησιμοποιεί το σχήμα BLMQ-SKIBE για τη θεωρητική θεμελίωση των γενικών ιδεών που προτείνουμε, και το σχήμα ECCSI-SAKKE για την επίδειξη λειτουργίας των προτάσεών μας. Αυτή η διαφοροποίηση έγινε προκειμένου:

1. Να αποδειχθεί η ευπλαστότητα και η ευελιξία των προτάσεών μας μέσα από τη λειτουργία τους σε παρεμφερή σχήματα ΚΒΤ.

2. Να δοκιμαστούν και επιδειχθούν οι προτάσεις μας σε σχήματα όπως το ECCSI-SAKKE, τα οποία είναι ήδη λειτουργικά σε διάφορες εφαρμογές, π.χ. εφαρμογές εμπιστευτικής επικοινωνίας όπως το Cryptify[6] αλλά και στο Διαδίκτυο των Πραγμάτων [63].

3. Να δοκιμαστούν και επιδειχθούν οι προτάσεις μας σε σχήματα όπως το ECCSI-SAKKE, τα οποία παρέχουν υλικό επιβεβαίωσης των αποτελεσμάτων μας.

[6] https://www.ncsc.gov.uk/products/cryptify-call



Σχήμα 2.1: Η χρήση του σχήματος ECCSI-SAKKE

Για παράδειγμα, στα RFCs όπου περιγράφεται το σχήμα, περιλαμβάνονται παραρτήματα με συγκεκριμένες τιμές και παραδείγματα, ώστε να μπορεί να ελεγχθεί η ορθότητα των υλοποιήσεών μας.

4. Το σχήμα ECCSI-SAKKE είναι ένα βήμα πιο κοντά σε παραγωγικό περιβάλλον συγκριτικά με το σχήμα BLMQ-SKIBE, λόγω της ευελιξίας που παρέχει ο αρχικός του σχεδιασμός. Το σχήμα ECCSI-SAKKE παρέχει την εύκολη επιλογή διαφορετικού σχήματος πιστοποίησης των δεδομένων ή εμπιστευτικότητας. Για παράδειγμα:

   (α') Πλήρες ECCSI-SAKKE: Χρήση του πρωτοκόλλου SAKKE ως μηχανισμού έμπιστης ανταλλαγής υλικού για τη δημιουργία συμμετρικού κλειδιού ενθυλάκωσης και του ECCSI ως μηχανισμού ελέγχου της ταυτότητας του αποστολέα του μηνύματος του SAKKE.

   (β') Μόνο ο μηχανισμός SAKKE: Χρήση του πρωτοκόλλου SAKKE ως μηχανισμού έμπιστης ανταλλαγής υλικού για τη δημιουργία συμμετρικού κλειδιού ενθυλάκωσης και διαφορετικού μηχανισμού πιστοποίησης δεδομένων (π.χ. πιστοποιητικά που βασίζονται σε X509, εάν υπάρχουν ήδη.

   (γ') Μόνο ο μηχανισμός ECCSI: Χρήση ενός εναλλακτικού μηχανισμού ανταλλαγής κλειδιών (π.χ. Diffie-Hellman) και του ECCSI ως μηχανισμού πιστοποίησης των μηνυμάτων Diffie-Hellman.

Πέρα από την ευελιξία του ως σχήμα, αξίζει να αναφερθούν δύο επιπλέον πλεονεκτήματα του σχήματος ECCSI-SAKKE [64][7].

[7] Είναι αξιοσημείωτο ότι το αναφερόμενο άρθρο αναγνωρίζει αυτά τα πλεονεκτήματα παρά το ότι επικρίνει έντονα το σχήμα ECCSI-SAKKE

1. Αντίθετα με άλλα σχήματα δημιουργίας κλειδιού συνόδου (π.χ. Diffie-Hellman) το σχήμα ECCSI-SAKKE χρειάζεται την αποστολή μόνο ενός μηνύματος.
2. Το σχήμα ECCSI-SAKKE μεταφέρει το πρόβλημα της συνεχούς επικυρωμένης διανομής των δημόσιων κλειδιών (π.χ. μέσω πιστοποιητικών) των χρηστών σε όλους, σε μια και μοναδική ασφαλή απόδοση των ιδιωτικών κλειδιών των χρηστών στους κατόχους τους.

Τα κύρια μειονεκτήματα του σχήματος ECCSI-SAKKE συγκριτικά με το σχήμα BLMQ-SKIBE είναι τα εξής:

1. Το SKIBE είναι ο μηχανισμός κρυπτογράφησης. Συνεπώς, έχει τη δυνατότητα αυτοτελούς μεταφοράς εμπιστευτικών δεδομένων χωρίς να είναι απαραίτητη η συνύπαρξη με άλλο μηχανισμό. Αντίθετα, ο μηχανισμός SAKKE έχει τη δυνατότητα μόνο ενθυλάκωσης και εμπιστευτικής μεταφοράς υλικού για τη δημιουργία συμμετρικού κλειδιού κρυπτογράφησης συνόδου (π.χ. κλειδί συνόδου για τη χρήση του με το συμμετρικό αλγόριθμο Advanced Encryption Standard (AES)).
2. Το σχήμα ECCSI-SAKKE, σε σχέση με το σχήμα BLMQ-SKIBE, είναι πολύ πιο πολύπλοκο στην εφαρμογή του, διότι χρειάζεται στην πραγματικότητα δύο παράλληλες διακριτές υποδομές, με ξεχωριστές δημόσιες παραμέτρους και ξεχωριστά κλειδιά.

   Ενδεικτικά: Ο Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ) ή Key Management Server (KMS) όπως αναφέρεται στα RFC6507-RFC6508:

   (α') Ορίζει:

      i. τις Δημόσιες Παραμέτρους για τον μηχανισμό: ECCSI-PP

      ii. τις Δημόσιες Παραμέτρους για τον μηχανισμό: SAKKE-PP

   (β') Επιλέγει και Υπολογίζει αντίστοιχα:

      i. Επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ECCSI-ΘΜΚ/KSAK) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ECCSI-ΘΔΚ/KPAK) που θα χρησιμοποιείται με τον μηχανισμό ECCSI.

      ii. Επιλέγει το Θεμελιώδες Μυστικό Κλειδί (SAKKE-ΘΜΚ/z_T) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (SAKKE-ΘΔΚ/Z_T) που θα χρησιμοποιείται με τον μηχανισμό SAKKE.

   (γ') Εκδίδει τα Ιδιωτικά κλειδιά των χρηστών:

      i. το Ιδιωτικό Κλειδί ψηφιακής Υπογραφής (ΙΚΥ) (Secret Signing key (*SSK*)) και το Δημόσιο Τεκμήριο Επικύρωσης (ΔΤΕ) (Public Validation Token (*PVT*)) για την ψηφιακή υπογραφή των δεδομένων με τον μηχανισμό ECCSI.

      ii. το Μυστικό Κλειδί Αποδέκτη (ΜΚΑ) (Receiver Secret key (RSK)) που θα χρησιμοποιείται στην αποθυλάκωση με τον μηχανισμό SAKKE

2.3.2 Τεχνική περιγραφή του μηχανισμού ECCSI (RFC6507)

Ο μηχανισμός ECCSI βασίζεται στον αλγόριθμο ψηφιακών υπογραφών Elliptic Curve Digital Signature Algorithm (ECDSA)[8] με κύρια διαφορά το Δημόσιο Κλειδί του χρήστη. Στις τυπικές εφαρμογές ECDSA το δημόσιο κλειδί του χρήστη λαμβάνεται από τον Επαληθευτή της ψηφιακής υπογραφής μέσω κάποιου πιστοποιητικού (π.χ. X509), ενώ στο μηχανισμό ECCSI εξάγεται από το δημόσιο αναγνωριστικό (*ID*) του υπογράφοντος. Τέλος, όπως συμβαίνει και στις τυπικές εφαρμογές ECDSA η εγκυρότητα της ψηφιακής υπογραφής εξαρτάται από τη μυστικότητα του Ιδιωτικού κλειδιού (SSK) του υπογράφοντα.

Τα αντικείμενα που εμπλέκονται στο πρωτόκολλο είναι:

- **KMS Secret Authentication key (KSAK)**: είναι το Θεμελιώδες Μυστικό κλειδί (ΘΜΚ) του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ). Στην πραγματικότητα είναι ένας τυχαίος ακέραιος αριθμός, του οποίου η μυστικότητα είναι η βάση της ασφάλειας όλης της υποδομής μας.
- **KMS Public Authentication key (KPAK)**: είναι το Θεμελιώδες Δημόσιο κλειδί (ΘΜΚ), το οποίο είναι σημείο πάνω στην ελλειπτική καμπύλη. Υπολογίζεται χρησιμοποιώντας την πράξη του πολλαπλασιασμού ακεραίου με σημείο πάνω σε ελλειπτική καμπύλη. Συγκεκριμένα, πολλαπλασιάζουμε KSAK φορές το σημείο γεννήτορα (G) της υποομάδας τάξης q της ελλειπτικής καμπύλης: $KPAK = [KSAK]G$.
- **(ID)** το δημόσιο αναγνωριστικό του χρήστη, το οποίο μέσω συνάρτησης κατακερματισμού αναπαρίσταται από έναν ακέραιο $\in (2, q-1]$.
- **Secret Signing key (SSK)**: Το Ιδιωτικό κλειδί του χρήστη, ένας ακέραιος αριθμός.
- **Public Validation Token (PVT)**: Ένα τυχαίο σημείο στην ελλειπτική καμπύλη, μοναδικό για κάθε χρήστη, το οποίο είναι δημόσιο και χρησιμοποιείται για τον υπολογισμό του SSK.
- **Ψηφιακή Υπογραφή** (r, s, PVT): Η τριάδα με τις τρεις μεταβλητές είναι η ψηφιακή υπογραφή κάθε μηνύματος. Σημειώνουμε ότι η μεταβλητή *PVT* είναι συνδεδεμένη με το αναγνωριστικό του υπογράφοντος και συνεπώς παραμένει σταθερή για όλα τα μηνύματα που έχει υπογράψει ψηφιακά ο ίδιος χρήστης.
- Οι δημόσιες παράμετροι του πρωτοκόλλου ECCSI (RFC6507) είναι οι: p, n, q, EC, G, $Hash_x$, $KPAK$.

Διαδικασία δημιουργίας των κλειδιών *KSAK/KPAK* του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ/KMS)

Η διαδικασία αποτελείται από την επιλογή του *KSAK* και τον υπολογισμό του αντίστοιχου *KPAK*.

1. Επιλογή του *KSAK*: επιλέγεται τυχαίος ακέραιος αριθμός $\in (2,\chi\text{-}1]$.

[8] X9.62-2005, "Public key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 2005.

Σύμβολο	Ερμηνεία
PP	οι Δημόσιες Παράμετροι (Public Parameters) της υλοποίησής μας
$\mathbb{F}_p$	το πεπερασμένο Σώμα (Field) αποτελούμενο από p στοιχεία, όπου p είναι πρώτος
p	η τάξη του πεπερασμένου σώματος $\mathbb{F}_p$
n	παράμετρος ασφαλείας, μέγεθος (σε bits) του p, ($p > 2^n$).
$\mathbb{F}^*$	πολλαπλασιαστική ομάδα των μη-μηδενικών στοιχείων του σώματος F
$\mathbb{F}_p^*$	πολλαπλασιαστική ομάδα του πεπερασμένου σώματος $\mathbb{F}_p$
EC ή E	ελλειπτική καμπύλη που ορίζεται πάνω στο $\mathbb{F}_p$ με υποομάδα τάξης q.
0	το ουδέτερο σημείο (¨σημείο στο άπειρο¨) κάθε προσθετικής ομάδας με σημεία πάνω σε ελλειπτική καμπύλη.
$P(P_x, P_y)$	σημείο πάνω στην ελλειπτική καμπύλη με συντεταγμένες $P_x, P_y \in \Phi_p$ που ικανοποιούν την εξίσωση της EC. Π.χ. το σημείο $P(P_x, P_y)$ βρίσκεται πάνω στην ελλειπτική καμπύλη $y^2 \equiv x^3 - 3x + B$ εάν $y^2 - x^3 + 3x - B$ modulo $p \equiv 0$.
$G(G_x, G_y)$	όπου $G(G_x, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης q
q	η τάξη του G στην ελλειπτική καμπύλη EC πάνω στο $\mathbb{F}_p$
$P + Q$	πρόσθεση σημείων της ελλειπτικής καμπύλης EC
$[k]P$	πρόσθεση k φορές του σημείου $P \in EC$ στον εαυτό του, όπου k ακέραιος
Hash (H)	κρυπτογραφική συνάρτηση κατακερματισμού, π.χ. η SHA256 της οικογένειας Secure Hash Algorithm

Πίνακας 2.3: Σύμβολα του πρωτοκόλλου ECCSI (RFC6507)

2. Υπολογισμός του *KPAK*: Υπολογίζεται το $KPAK = [KSAK]G$, όπου $G(G_x, G_y) \in EC$ είναι γεννήτορας της υποομάδας τάξης q και η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στην EC με ακέραιο αριθμό.

Αλγόριθμοι δημιουργίας Ιδιωτικού κλειδιού (*SSK*) και Δημόσιου Τεκμηρίου Επικύρωσης (ΔΤΕ)/Public Validation Token (*PVT*)

Στην πραγματικότητα είναι μια ομάδα αλγορίθμων που περιλαμβάνουν:

- την επιλογή του *PVT* του χρήστη
- τον υπολογισμό του ιδιωτικού κλειδιού (*SSK*) του χρήστη με τη χρήση του Δημόσιου Τεκμήριου Επικύρωσης (ΔΤΕ)/Public Validation Token (*PVT*) και του *ID* του, και
- την επαλήθευσή τους.

Δεδομένα Εισόδου

Οι αλγόριθμοι χρησιμοποιούν τα: *KSAK*, το δημόσιο αναγνωριστικό *ID* του χρήστη, και τον γεννήτορα (G).

Αλγόριθμος

(α) Υπολογισμός του *PVT*

(1) Επιλέγουμε v, τυχαίο (εφήμερο), μη-μηδενικό στοιχείο του F_q

(2) Υπολογίζουμε το $PVT = [\upsilon]G$

(β) Υπολογισμός του SSK

(3) Υπολογίζουμε τη συνάρτηση κατακερματισμού: $HS = hash(G||KPAK||ID||PVT)$

(4) Υπολογίζουμε το: $SSK = (KSAK + HS * \upsilon) \mod q$

(5) Έλεγχος: Εάν το SSK ή το HS είναι μηδέν $\mod q$, τότε το SSK είναι ΜΗ-ΕΓΚΥΡΟ και η διαδικασία υπολογισμού του πρέπει να επαναληφθεί.

Αποτέλεσμα

(6) Εξαγωγή του ζεύγους (SSK, PVT). Σημειώνουμε ότι το υ πρέπει να διαγραφεί[9].

(γ) Επικύρωση του SSK/PVT από τον χρήστη

Ο χρήστης πρέπει να επικυρώσει το ζεύγος SSK/PVT πριν τα χρησιμοποιήσει, ακολουθώντας τα παρακάτω βήματα:

(1) Ελέγχει αν $PVT \in EC$

(2) Υπολογίζει το $HS = hash(G||KPAK||ID||PVT)$. Σημειώνεται ότι το HS είναι στατικό, οπότε ο χρήστης μπορεί να το αποθηκεύσει ώστε να μη χρειάζεται να υπολογίζεται κάθε φορά.

(3) Αν $KPAK = [SSK]G - [HS]PVT$[10] τότε το ζεύγος SSK/PVT είναι έγκυρο.

Ψηφιακή Υπογραφή υπό ECCSI

Δεδομένα Εισόδου

1. Το μήνυμα (m) που θα υπογραφεί ψηφιακά
2. Το αναγνωριστικό (ID) του Υπογράφοντα
3. Το ιδιωτικό κλειδί (SSK) του Υπογράφοντα
4. Το PVT του Υπογράφοντα
5. Το Δημόσιο Κλειδί ($KPAK$) του Αξιόπιστου Κεντρικου Συντονιστή ΑΚΣ(KMS) του Υπογράφοντα

Αλγόριθμος

(1) Επιλογή τυχαίου (εφήμερου), μη-μηδενικου στοιχείου $j \in F_q$

(2) Υπολογισμός του $J = (Jx, Jy)$ τέτοιου ώστε $J = [j]G$, εν συνεχεία θέτουμε $r = Jx$, δηλαδή το r ισούται με την τετμημένη Jx του J.

(3) Υπολογισμός $HS = hash(G||KPAK||ID||PVT)$. Εάν έχουμε αποθηκεύσει το HS δεν χρειάζεται να το υπολογίσουμε ξανά.

(4) Υπολογισμός της συνάρτησης κατακερματισμού $HE = hash(HS||r||M)$·

[9]Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην υποενότητα 5.1.1 του RFC6507

[10]Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην υποενότητα 5.1.2 του RFC6507

(5) Έλεγχος: Εάν ισχύει η σχέση $(HE + r * SSK)\ modulo\ q \neq 0$, η ψηφιακή υπογραφή είναι έγκυρη, αλλιώς η διαδικασία πρέπει να επαναληφθεί με νέο $j \in F_q$.

(6) Υπολογισμός $s' = ((\frac{1}{HE+r*SSK}) * j)\ modulo\ q$. Μετά τον υπολογισμό η τιμή j πρέπει να διαγράφεται.

(7) Θέτουμε $s = s'$ ή, εάν s' είναι πολύ μεγάλο για να χωρέσει σε ένα N-octet ακέραιο, θέτουμε $s = q - s'$.

Αποτέλεσμα

Η ψηφιακή υπογραφή είναι η τριάδα (s, r, PVT)[11].

Επαλήθευση Ψηφιακής Υπογραφής υπό ECCSI

Δεδομένα Εισόδου

1. Η ψηφιακή υπογραφή (s, r, PVT)
2. Το υπογεγραμμένο μήνυμα (m)
3. Το δημόσιο αναγνωριστικό (ID) του Υπογράφοντα
4. Το Δημόσιο Κλειδί $(KPAK)$ του Αξιόπιστου Κεντρικού Συντονιστή ΑΚΣ (KMS) του Υπογράφοντα

Αλγόριθμος

(1) Ελεγχος αν $PVT \in EC$

(2) Υπολογισμός του $HS = hash(G||KPAK||ID||PVT)$

(3) Υπολογισμός $HE = hash(HS||r||M)$

(4) Υπολογισμός $Y = [HS]PVT + KPAK$

(5) Υπολογισμός $J = [s]([HE]G + [r]Y)$

Αποτέλεσμα

(6) Η Ψηφιακή Υπογραφή είναι ΕΓΚΥΡΗ μόνο εάν $Jx = r\ modulo\ p$ και $Jx\ modulo\ q \neq 0$. Σε αντίθετη περίπτωση η υπογραφή θεωρείται άκυρη[12].

2.3.3 Τεχνική περιγραφή του μηχανισμού SAKKE (RFC6508)

Το SAKKE (RFC6508)[13] έχει σχεδιαστεί προκειμένου ο αποστολέας να στέλνει εμπιστευτικά στον παραλήπτη μυστικές πληροφορίες (SSV) που θα αξιοποιηθούν για τη δημιουργία ενός συμμετρικού κλειδιού κρυπτογράφησης που θα χρησιμοποιηθεί μετέπειτα ως κλειδί συνόδου. Σημειώνουμε ότι ο αποστολέας δεν μεταδίδει άμεσα στον Παραλήπτη το SSV αλλά μεταδίδει ειδικές τιμές, που ονομάζονται Ενθυλακωμένα

[11] Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην υποενότητα 5.2.1 του RFC6507

[12] Για περισσότερες λεπτομέρειες ο αναγνώστης μπορεί να ανατρέξει στην υποενότητα 5.2.2 του RFC6508

[13] Ο μηχανισμός Sakai-Kasahara Key Encryption (SAKKE) (RFC6508) βασίζεται στον μηχανισμό Sakai-Kasahara Key Encapsulation Mechanism (SKKEM), όπως περιγράφεται στην ενότητα 8.1 "SKKEM scheme" του [16].

Δεδομένα ("Encapsulated Data") και από τις οποίες ο παραλήπτης εξάγει το SSV. Συνοπτικά, ο αποστολέας υπολογίζει τα ενθυλακωμένα δεδομένα από το SSV, το αναγνωριστικό του παραλήπτη ($ID_{Receiver}$) και το Θεμελιώδες Δημόσιο Κλειδί Z_T του ΑΚΣ του παραλήπτη, ο οποίος υπολογίζει το SSV χρησιμοποιώντας τα ενθυλακωμένα δεδομένα, το ιδιωτικό κλειδί του ($RSK_{Receiver}$) και το Θεμελιώδες Δημόσιο Κλειδί Z_T του ΑΚΣ του.

Επιπλέον, στις αποδείξεις των γενικών αρχών του ARIBC και του mIBC-AIS, επιλέξαμε να ακολουθήσουμε την περιγραφή του RFC6508 και να παρουσιάσουμε το περίπλοκο σενάριο SAKKE, όπου τα δύο επικοινωνούντα μέρη ανήκουν σε διαφορετικές υλοποιήσεις SAKKE-KBT, με διαφορετικούς Αξιόπιστους Κεντρικούς Συντονιστές (ΑΚΣ). Αυτή η επιλογή έγινε για δύο λόγους: Ο πρώτος είναι η θέλησή μας για όσο το δυνατόν εγκυρότερη υλοποίηση των προτάσεών μας μέσω της πιστότητας των ακολουθούμενων διαδικασιών και φυσικά των αντίστοιχων τιμών ελέγχου που παρέχονται στο RFC6508. Ο δεύτερος λόγος είναι ότι χάρη στο περίπλοκο σενάριο SAKKE θα μπορέσουμε να κατανοήσουμε πώς τα μέλη διαφορετικών αρχών ARIBC ή διαφορετικών εφαρμογών mIBC-AIS μπορούν να επικοινωνούν με ασφάλεια. Συνεπώς, ακολουθώντας εφεξής το RFC6508, υποθέτουμε ότι έχουμε δύο διαφορετικές υλοποιήσεις SAKKE-KBT, που ονομάζονται «T» και «S» αντίστοιχα και δύο επικοινωνούντα μέρη, τον Αποστολέα ("a") που ανήκει στην υλοποίηση T και τον «Παραλήπτη» ("b") ο οποίος ανήκει στην υλοποίηση S.

Τέλος, επισημαίνουμε ότι σε αυτήν τη διατριβή η χρήση του μηχανισμού SAKKE ακολουθεί τις υποδείξεις του RFC6508 και συνεπώς έχει τις παρακάτω κρυπτογραφικές ιδιαιτερότητες:

- Ο μηχανισμός που περιγράφεται περιορίζεται στην supersingular ελλειπτική καμπύλη $y^2 = x^3 - 3x \mod p$, όπου $p = 3 \mod 4$[14]
- Διγραμμική Απεικόνιση Tate-Lichtenbaum από το $E(F_p)[q] \times E(F_p)[q]$ στην υποομάδα $\in PF_p$.
- Κοινή Μυστική Τιμή (Shagreen Secret Value (SSV)). Ο σκοπός του σχήματος SAKKE είναι ο αποστολέας να μεταδώσει εμπιστευτικά, μέσω των ενθυλακωμένων δεδομένων, μια κοινή μυστική τιμή στον παραλήπτη. Το SSV είναι ακέραιος αριθμός $\in (0, 2^n - 1]$
- Ενθυλακωμένα Δεδομένα (Encapsulated Data) Τα ενθυλακωμένα δεδομένα χρησιμοποιούνται για τη μετάδοση εμπιστευτικών πληροφοριών (SSV) με ασφάλεια στον παραλήπτη. Μπορούν να υπολογιστούν απευθείας από το Δημόσιο Αναγνωριστικό του Παραλήπτη ($ID_Receiver$) και τις δημόσιες παραμέτρους (PP) της υλοποίησης KBT στην οποία ανήκει ο Παραλήπτης. Στο SAKKE, τα ενθυλακωμένα δεδομένα είναι ένα σημείο τάξης $q \in E(F_p)$ και ένας ακέραιος αριθμός $\in (0, (2^n) - 1]$.
- (ID) το δημόσιο αναγνωριστικό του χρήστη, το οποίο μέσω συνάρτησης κατακερματισμού αναπαρίσταται από έναν ακέραιο $\in (2, q - 1]$.

[14]Στην ενότητα 2.1 του RFC6508 αναφέρεται: "This document is restricted to a particular family of curves (see Section 2.1) that have the benefit of a simple and efficient method of calculating the pairing on which the Sakai-Kasahara IBE cryptosystem is based."

- Μυστικό Κλειδί Αποδέκτη (ΜΚΑ) (Receiver Secret key (RSK)) είναι το Ιδιωτικό κλειδί του χρήστη που του παρέχεται από τον εκάστοτε Αξιόπιστο Κεντρικό Συντονιστή.

Στον πίνακα 2.4 επεξηγούνται τα σύμβολα που χρησιμοποιούνται στον μηχανισμό SAKKE (RFC6508).

Οι δημόσιες παράμετροι του μηχανισμού SAKKE (RFC6508)

Οι δημόσιες παράμετροι του μηχανισμού SAKKE (RFC6508) είναι οι: $p, n, q, EC, G, g =< G, G >, Hash$.

Υπενθυμίζουμε ότι στις πειραματικές υλοποιήσεις σ' αυτήν τη διατριβή χρησιμοποιούμε δύο υλοποιήσεις SAKKE-ΚΒΤ με αντίστοιχους Αξιόπιστους Κεντρικούς Συντονιστές (ΑΚΣ):

1. KMS_T: Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ-Τ) της υλοποίησης ΚΒΤ-Τ, με Θεμελιώδες Δημόσιο κλειδί Z_T και Θεμελιώδες Μυστικό Κλειδί z_T, όπου ανήκει ο Αποστολέας ("a").
2. KMS_S: Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ-Σ) της υλοποίησης ΚΒΤ-Σ, με Θεμελιώδες Δημόσιο κλειδί Z_S και Θεμελιώδες Μυστικό Κλειδί z_S, όπου ανήκει ο Παραλήπτης ("b").

Δημιουργία των κλειδιών $(z_T)/Z_T$ των Αξιόπιστων Κεντρικών Συντονιστών (ΑΚΣ)

1. Επιλέγεται τυχαίος ακέραιος αριθμός $(z_T) \in (2, q-1]$.
2. Υπολογίζεται το $Z_T = [z_T]G$, όπου $G(G_x, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης q. Η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στην EC με ακέραιο αριθμό.

Η ίδια διαδικασία ακολουθείται από το KMS_S για να δημιουργήσει το Θεμελιώδες Μυστικό Κλειδί (z_S) και το Θεμελιώδες Δημόσιο κλειδί (Z_S) αντίστοιχα.

Εξαγωγή Ιδιωτικού κλειδιού Receiver Secret Key Extraction (RSK) από τον Αξιόπιστο Κεντρικό Συντονιστή (ΑΚΣ)

Στο πλαίσιο αυτού του παραδείγματος, $RSK_{(a,T)}$ είναι το ιδιωτικό κλειδί του χρήστη με ID = "a" που ανήκει στην υποδομή KMS_T. Θυμίζουμε ότι το a έχει μετατραπεί σε ακέραιο αριθμό μέσω συνάρτησης κατακερματισμού.

(1) Υπολογισμός του: $RSK_{(a,T)} = [(a + z_T)^{-1}]G$

(2) Επαλήθευση: το Ιδιωτικό Κλειδί γίνεται αποδεκτό μόνο εάν ισχύει η ισότητα: $< [a]G + Z_T, K_{(a,T)} >= g$, ειδάλλως απορρίπτεται.

Η ίδια διαδικασία ακολουθείται από το χρήστη b της KMS_S προκειμένου αυτός να αποκτήσει το δικό του $RSK_{(b,S)}$

Σύμβολο	**Ερμηνεία**
PP	οι Δημόσιες Παράμετροι (Public Parameters) της υλοποίησής μας
n	παράμετρος ασφαλείας, μέγεθος (σε bits) του p, $(p > 2^n)$
p	η τάξη του πεπερασμένου σώματος $\mathbb{F}_p$, $p \equiv 3(mod 4)$
$\mathbb{F}_p$	το πεπερασμένο Σώμα (Field) αποτελούμενο από p στοιχεία, όπου p είναι πρώτος
$\mathbb{F}^*$	πολλαπλασιαστική ομάδα των μη-μηδενικών στοιχείων του σώματος F
$\mathbb{F}_p^*$	πολλαπλασιαστική ομάδα του πεπερασμένου σώματος $\mathbb{F}_p$
q	περιττός πρώτος αριθμός που διαιρεί το $p-1$ από το πεπερασμένο Σώμα $\mathbb{F}_p$.
$(SS) - EC$	ο μηχανισμός που περιγράφεται περιορίζεται στην supersingular ελλειπτική καμπύλη $y^2 = x^3 - 3x \quad modp$ όπου $p = 3mod4$
$E(F)$	η προσθετική ομάδα από σημεία με συντεταγμένες (x, y) όπου $x, y \in F$, και ικανοποιούν την εξίσωση της ελλειπτικής καμπύλης EC.
0	το ουδέτερο σημείο (¨σημείο στο άπειρο¨) κάθε προσθετικής ομάδας με σημεία πάνω σε ελλειπτική καμπύλη.
F_p^2	η επέκταση βαθμού 2 του σώματος F_p. Στο RFC6508, μια συγκεκριμένη επέκταση $F_p^2 = F_p[i]$, όπου $i^2 + 1 = 0$.
PF_p	η προβολή του F_p, ορίζουμε να είναι $(F_p^2)^* / (F_p)^*$. Η PF_p είναι κυκλική τάξης $p + 1$, η οποία διαιρείται από το q, εκ του ορισμού του.
$G[q]$	υποομάδα αποτελούμενη από σημεία τάξης $q \in G$.
$< , >$	Διγραμμική Απεικόνιση Tate-Lichtenbaum από το $E(F_p)[q] \times E(F_p)[q]$ στην τάξης q υποομάδα $\in PF_p$.
$P(P_x, P_y)$	σημείο πάνω στην ελλειπτική καμπύλη με συντεταγμένες $P_x, P_y \in \Phi_p$ που ικανοποιούν την εξίσωση της EC.
$G = (G_x, G_y)$	όπου $G(G_x, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης q σημείων της ελλειπτικής καμπύλης EC. Σημειώνεται ότι στο RFC6508 ο γεννήτορας συμβολίζεται ως $P = (P_x, P_y)$.
$P + Q$	η πράξη της πρόσθεσης σημείων ελλειπτικής καμπύλης EC
$[k]P$	η πράξη του ¨πολλαπλασιασμού¨ σημείων ελλειπτικής καμπύλης, δηλαδή η πρόσθεση k φορές του σημείου $P \in EC$ στον εαυτό του με την πράξη πρόσθεσης σημείων ελλειπτικής καμπύλης, όπου k ακέραιος
Hash (H)	κρυπτογραφική συνάρτηση κατακερματισμού, π.χ. η SHA256

Πίνακας 2.4: Σύμβολα του μηχανισμού SAKKE (RFC6508)

Αποστολή Ενθυλακωμένου Μηνύματος

Σ′ αυτό το παράδειγμα, ο Αποστολέας ενθυλακώνει τα δεδομένα, δηλαδή την Κοινή Μυστική Τιμή (*SSV*), και τα στέλνει στον Παραλήπτη ($ID_{Receiver} =' b'$).

Σημειώνουμε ότι η ακόλουθη λειτουργία χρησιμοποιεί τη συνάρτηση κατακερματισμού σε ακέραιο (HashToIntegerRange)[15]. Πρόκειται για έναν αλγόριθμο, που περιγράφεται στην υποενότητα 5.1. του RFC6508 και χρησιμοποιεί μια συνάρτηση κρυπτογραφικού κατακερματισμού (π.χ. SHA256) και λαμβάνει ως είσοδο συμβολοσειρές σε οκτάδα και έναν ακέραιο (n) και εξάγει έναν νέο ακέραιο $v \in (0, n-1]$.

Δεδομένα Εισόδου

(1) Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = b$
(2) Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ-S-SAKKE: Z_S

Αλγόριθμος

Ο Αποστολέας:

(1) Επιλέγει ως *SSV* τυχαίο (εφήμερο) ακέραιο, μη-μηδενικό στοιχείο $SSV \in (0, (2^n) - 1]$

(2) Υπολογίζει: $r = HashToIntegerRange(SSV||b, q, Hash)$

(3) Υπολογίζει: $R_{(b,S)} = [r]([b]G + Z_S) \in E(F_p)$ Hint, (H)

(4α) Υπολογίζει: g^r[16]

(4β) Υπολογίζει: $H := SSV \oplus HashToIntegerRange(g^r, 2^n, Hash)$

Αποτέλεσμα

(5) Αποστέλλει: στον b τα ενθυλακωμένα δεδομένα $(R_{(b,S)}, H)$
(6) Εξάγει: *SSV*

Παραλαβή και αποθυλάκωση Μηνύματος

Σ′ αυτό το παράδειγμα, ο Παραλήπτης ($ID_{Receiver} = b$) παραλαμβάνει τα ενθυλακωμένα δεδομένα $(R_{(b,S)}, H)$.

Δεδομένα Εισόδου

(1) Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = b$
(2) Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ-S-SAKKE: Z_S

Αλγόριθμος

Ο Παραλήπτης:

(1) Εξάγει: $R_{(b,S)}$ και H από τα ενθυλακωμένα δεδομένα $(R_{(b,S)}, H)$
(2) Υπολογίζει: $w =< R_{(b,S)}, RSK_{(b,S)} >$
(3) Υπολογίζει: $SSV = H \oplus HashToIntegerRange(w, 2^n, Hash)$
(4) Υπολογισμός του $r = HashToIntegerRange(SSV||b, q, Hash)$
(5) Υπολογίζει: $TEST = [r]([b]G + Z_S) \in E(F_p)$

[15] Αναφέρεται επίσης ως ¨η μάσκα¨ στο RFC6508 Appendix A.
[16] Περισότερες πληροφορίες στην ενότητα 2.1 του RFC6508

Αποτέλεσμα

(6) Τα ενθυλακωμένα δεδομένα γίνονται αποδεκτά μόνο εάν ισχύει η ισότητα $TEST = R_{(b,S)}$, ειδάλλως τα ενθυλακωμένα δεδομένα απορρίπτονται
(7) Εξάγει: *SSV*

Κεφάλαιο 3

Ανώνυμη αναφορά παραβατικών πράξεων: Η υποδομή Anonymous Reporting IBC (ARIBC)

3.1 Εισαγωγή

Απρόσκλητη βία, σεξουαλική παρενόχληση και επίθεση, ενδοοικογενειακή βία, ρατσιστικές συμπεριφορές, καταπάτηση δικαιωμάτων, εμπόριο όπλων και ναρκωτικών και οικονομικές ατασθαλίες είναι πλέον μέρος της καθημερινότητάς μας. Ακόμα και σε χώρους που μέχρι πρότινος θεωρούσαμε απόλυτα ασφαλείς, η κατάσταση φαίνεται ότι έχει αλλάξει. Όπως γνωρίζουμε, όλο και περισσότερα περιστατικά παραβατικών πράξεων συμβαίνουν σε χώρους εργασίας, σε εκπαιδευτικά ιδρύματα, σε κάθε είδους κοινωνικές εκδηλώσεις, ακόμα και στο σπίτι.

Η αναφορά τέτοιων περιστατικών έχει μεγάλη αξία, τόσο για τη διερεύνηση του ίδιου του συμβάντος, όσο και για την πρόληψη άλλων. Ωστόσο, οι μάρτυρες αλλά και τα ίδια τα θύματα είναι πολλές φορές απρόθυμοι να γνωστοποιήσουν τα περιστατικά, ή τα πιθανά περιστατικά, στην αρμόδια αρχή, για διάφορους λόγους όπως: φόβος αντιποίνων από τους δράστες, φόβος ότι δεν θα γίνουν πιστευτοί, αίσθημα ανασφάλειας. Ως αποτέλεσμα, ένα σημαντικό ποσοστό περιστατικών δεν αναφέρεται. Αυτό ισχύει ιδιαίτερα για περιστατικά σεξουαλικής επίθεσης και για κλοπές [65]. Δυσκολίες επίσης παρουσιάζονται και στον χειρισμό των αναφορών από τις αρμόδιες αρχές, ιδίως όταν λαμβάνονται πολλαπλές αναφορές για το ίδιο περιστατικό. Συχνά ένας μάρτυρας ή θύμα κάνει αναφορά σε περισσότερες από μια υπηρεσίες για το ίδιο περιστατικό, ιδιαίτερα κατά τη διαδικασία διερεύνησης του συμβάντος. Έτσι, υποβάλλονται πολλές αναφορές από το ίδιο άτομο για το ίδιο ή περισσότερα από ένα σχετικά περιστατικά (όπως π.χ. στην περίπτωση οικονομικών ατασθαλιών ή εγκλημάτων). Αυτές οι αναφορές πρέπει να αποδοθούν στον ίδιο αναφέροντα από τις ανακριτικές αρχές, να τυγχάνουν σωστού χειρισμού και να αξιοποιούνται σωστά.

Τα διαδικτυακά συστήματα αναφοράς παρέχουν ένα μέσο για την υπέρβαση του τελευταίου εμποδίου. Ωστόσο, η προσέγγιση που ακολουθείται συχνότερα σε τέτοια συστήματα είναι να συσχετιστεί κάθε αναφορά με την επαληθευμένη ταυτότητα του αναφέροντα ή με ένα αναγνωριστικό συμβάντος, που αντιστοιχεί στην πρώτη

υποβληθείσα αναφορά. Ενώ αυτό διευκολύνει σημαντικά τη διαχείριση της διαδικασίας αναφοράς, δεν αντιμετωπίζει τις ανησυχίες των αναφερόντων σχετικά με την αποκάλυψη της πραγματικής τους ταυτότητας. Το πρόβλημα αυτό μπορεί να επιλυθεί επιτρέποντας ανώνυμες αναφορές. Στο παρελθόν, οι ανώνυμες αναφορές γίνονταν επί το πλείστον μέσω μονόδρομης επικοινωνίας (π.χ. αποστολή ανώνυμου μηνύματος ηλεκτρονικού ταχυδρομείου) και θεωρούνταν λιγότερο αξιόπιστες από ότι οι επώνυμες. Πρόσφατα διαπιστώθηκε ότι, όταν χρησιμοποιείται αμφίδρομη επικοινωνία, η αξιοπιστία του ανώνυμου αναφέροντος είναι στατιστικά όμοια με αυτήν ενός επώνυμου. Επιπλέον, πρόσφατη έρευνα [66] έδειξε ότι οι αρχές είναι διατεθειμένες να αξιολογήσουν τόσο επώνυμες όσο και ανώνυμες αναφορές. Αυτά τα αποτελέσματα υποστηρίζουν τη χρήση ανώνυμης, αμφίδρομης επικοινωνίας σε διαδικτυακά συστήματα αναφοράς. Οι ανώνυμοι αναφέροντες θα επωφεληθούν από τη δυνατότητα διατήρησης ενός ενεργού διαλόγου με αυτούς που διερευνούν το περιστατικό, χωρίς να διακυβεύεται η ασφάλειά τους ή η αποτελεσματικότητα της έρευνας.

3.1.1 Προδιαγραφές της υποδομής ARIBC

Υποθέτουμε ότι η υποδομή θα υλοποιηθεί, εγκατασταθεί, και λειτουργήσει υπό την ευθύνη μιας αρχής, αρμόδιας για την αναφορά και διερεύνηση παραβατικών πράξεων. Παραδείγματα τέτοιων αρχών είναι πρωτίστως οι διωκτικές αρχές, αλλά και δομές υποστήριξης θυμάτων παραβατικών πράξεων, καθώς και δομές πρόληψης τέτοιων πράξεων. Επιπλέον, δεν είναι απαραίτητο η υπηρεσία ανώνυμης αναφοράς που μια τέτοια υποδομή μπορεί να προσφέρει να αφορά αυστηρά ποινικά κολάσιμες παραβατικές πράξεις· θα μπορούσε κάλλιστα να χρησιμοποιηθεί για οποιουδήποτε τύπου καταγγελίες, όπως π.χ. παραβιάσεις της ακαδημαϊκής δεοντολογίας. Στο πλαίσιο αυτό, η υποδομή θα πρέπει να πληροί τις εξής προδιαγραφές:

1. **Χρηστικότητα:** Η υποδομή πρέπει να είναι απλή στη χρήση και φιλική προς τους χρήστες.
2. **Απλότητα:** Η υποδομή πρέπει να είναι απλή στην υλοποίηση, εγκατάσταση, και λειτουργία, έτσι ώστε ακόμη και ένας μικρός ή μεσαίος οργανισμός, ή τμήμα ενός οργανισμού να μπορεί να την υλοποιήσει, να την εγκαταστήσει και να διαχειριστεί τη λειτουργία της, με περιορισμένους ανθρώπινους, υλικούς, και οικονομικούς πόρους.
3. **Ανώνυμοι και Επώνυμοι αναφέροντες:** Οι αναφέροντες θα πρέπει να έχουν την ίδια αντιμετώπιση ως προς τη χρήση των ασφαλών ηλεκτρονικών υπηρεσιών που προσφέρει η υποδομή, είτε επιλέξουν να είναι επώνυμοι είτε επιλέξουν να είναι ανώνυμοι.
4. **Αυτονομια και ανεξαρτησία:** Η υποδομή πρέπει να είναι, κατά το δυνατόν, αυτόνομη και ανεξάρτητη από άλλες υποδομές που λειτουργούν σε άλλες αρχές.
5. **Διαλειτουργικότητα:** Η υποδομή πρέπει να είναι διαλειτουργική. Διαφορετικές εγκαταστάσεις υποδομών ARIBC θα πρέπει να μπορούν να συνυπάρχουν και να συνεργάζονται απρόσκοπτα.
6. **Ευελιξία:** Η υποδομή πρέπει να είναι ευέλικτη και αξιοποιήσιμη από διάφορες εφαρμογές επικοινωνίας (π.χ. ηλεκτρονικό ταχυδρομείο, σύγχρονη ή ασύγχρονη

ηχητική επικοινωνία, κτλ.)

7. **Προσφερόμενες υπηρεσίες:** Η υποδομή θα πρέπει να παρέχει τις ακόλουθες υπηρεσίες:

   (α′) **Αμφίδρομη εμπιστευτικότητα δεδομένων:** Η υποδομή θα πρέπει να προσφέρει ευέλικτη αμφίδρομη εμπιστευτικότητα σε όλες τις επικοινωνίες του πολίτη προς τις αρχές.

   (β′) **Αμφίδρομη πιστοποίηση της ταυτότητας του αποστολέα και της ακεραιότητας των δεδομένων:** Η υποδομή πρέπει να προσφέρει υπηρεσίες ψηφιακής υπογραφής των δεδομένων για όλες τις πλευρές, ακόμα και για τον ανώνυμο πολίτη.

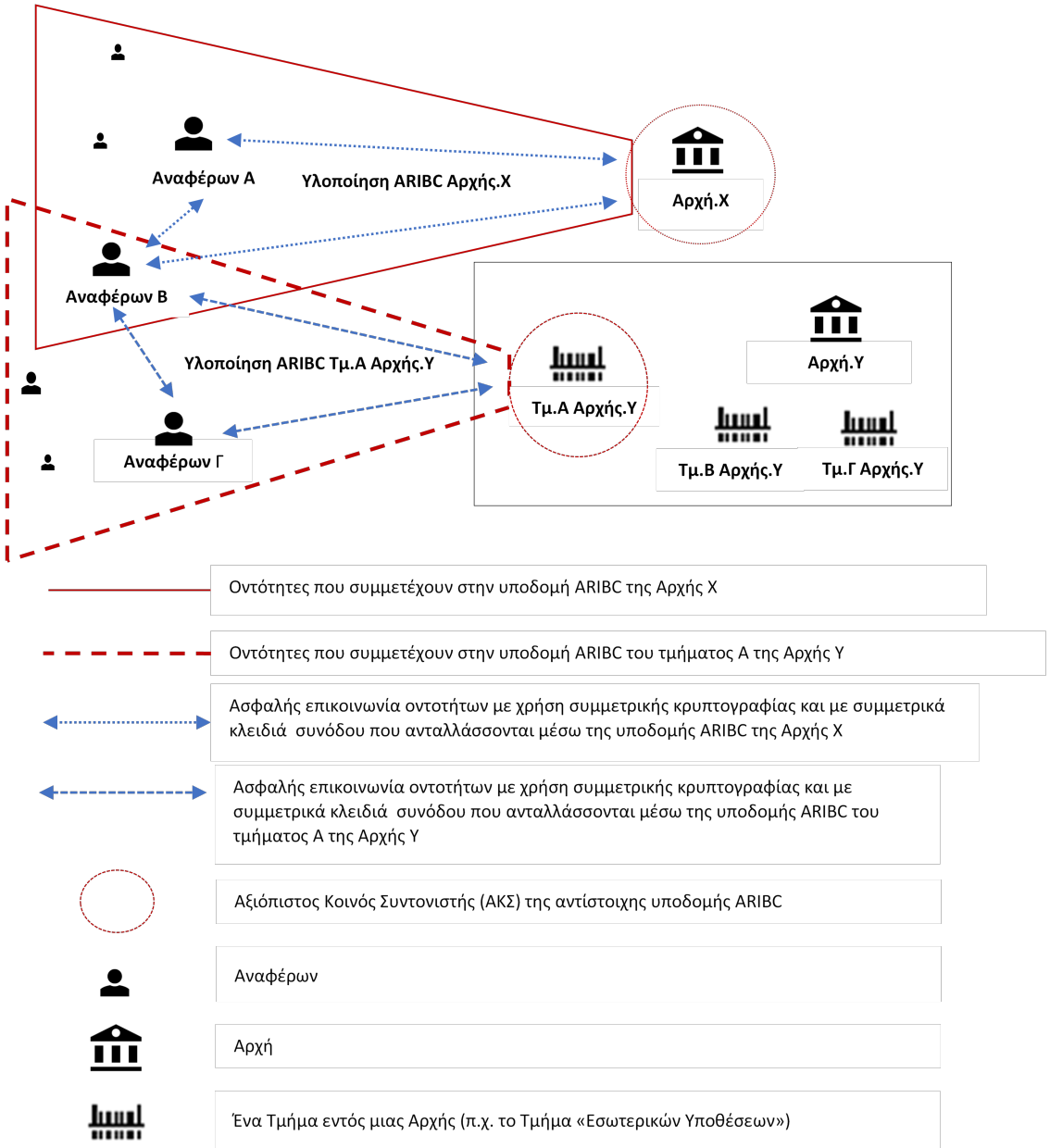
   (γ′) **Μη υποχρέωση εγγραφής στην υποδομή:** Η πρώτη εμπιστευτική επικοινωνία δεν πρέπει να προϋποθέτει να ανήκει κάποιο από τα δύο επικοινωνούντα μέρη σε μια υποδομή ARIBC. Εάν ο Παραλήπτης δεν είναι εγγεγραμμένος στη συγκεκριμένη υποδομή ARIBC, θα λάβει το ενθυλακωμένο υλικό. Στη συνέχεια θα απευθυνθεί στην αρμόδια υποδομή ARIBC και μόνο εφόσον ταυτοποιηθεί θα παραλάβει το αντίστοιχο ιδιωτικό κλειδί που θα αποθυλακώνει το μήνυμα.

3.2 Η υποδομή ARIBC

3.2.1 Οντότητες-συμμετέχοντες

Όπως φαίνεται στο Σχήμα 3.1, οι κύριες οντότητες και οι κύριοι συμμετέχοντες σε μια υποδομή ARIBC είναι: οι αναφέροντες, η αρχή στην οποία λειτουργεί η υποδομή, και ίσως μεμονωμένοι χρήστες από άλλες υπηρεσίες.

Στο Σχήμα 3.1 η Αρχή Χ χρησιμοποιεί μια υποδομή ARIBC. Ορισμένοι αναφέροντες, συμπεριλαμβανομένων των αναφερόντων Α και Β, έχουν εγγραφεί στην Αρχή Χ και μπορούν να επικοινωνούν με ασφάλεια μ′ αυτήν. Το Τμήμα Α της Αρχής Υ φιλοξενεί επίσης μια δική του υποδομή ARIBC, στην οποία έχουν εγγραφεί αναφέροντες, συμπεριλαμβανομένων των Αναφερόντων Β και Γ. Σημειώνεται ότι ο ίδιος χρήστης ενδέχεται να έχει εγγραφεί σε περισσότερες από μια υποδομές ARIBC. Και οι δύο υποδομές ARIBC προσφέρουν στους εγγεγραμμένους αναφέροντες υπηρεσίες εμπιστευτικής επικοινωνίας, ελέγχου ταυτότητας και ακεραιότητας. Σημειώστε επίσης ότι οι αναφέροντες που έχουν εγγραφεί σε οποιαδήποτε υποδομή ARIBC μπορούν επίσης να επικοινωνούν με ασφάλεια μεταξύ τους. Αυτή η επικοινωνία είναι δυνατή χωρίς τη διαμεσολάβηση των αντίστοιχων αρχών, αρκεί όμως οι αρχές να έχουν ενημερώσει τις αντίστοιχες οντότητες. Για παράδειγμα, η Αρχή Χ θα μπορούσε να είναι μια εθνική εσωτερική υπηρεσία που να ασχολείται με την παράνομη διακίνηση και εκμετάλλευση ανθρώπων και η Αρχή Υ μια αντίστοιχη υπηρεσία της ΕΕ. Σημειώνουμε ότι σε κάθε περίπτωση καμια οντότητα, εκτός από την αρχή στην οποία έγινε η αρχική αναφορά, δεν έχει τη δυνατότητα να συσχετίσει ένα περιστατικό με τους αναφέροντες.



Σχήμα 3.1: Οι κύριες οντότητες και οι κύριοι συμμετέχοντες σε μια υποδομή ARIBC

3.2.2 Δημόσια αναγνωριστικά χρηστών

Η μορφή των δημόσιων αναγνωριστικών (UserIDs) των χρηστών μιας υποδομής ARIBC είναι πολύ σημαντική. Συνεπώς, κάθε υποδομή ARIBC καθορίζει τη μορφή και τους ακριβείς κανόνες σύνταξης που πρέπει να πληρούν τα δημόσια αναγνωριστικά των χρηστών της (π.χ. έγκυροι και μη έγκυροι χαρακτήρες, το μέγιστο και το ελάχιστο μέγεθος ενός έγκυρου αναγνωριστικού, κλπ). Οι ακριβείς διαδικασίες επαλήθευσης και εγγραφής ενδέχεται να διαφέρουν ανάλογα με το επίπεδο ταυτοποίησης του χρήστη που απαιτείται για την παροχή των υπηρεσιών που παρέχονται από την Αρχή. Για παράδειγμα, μια απλή επαλήθευση μέσω ηλεκτρονικού ταχυδρομείου μπορεί να είναι επαρκής για ορισμένες αρχές, ενώ άλλες ενδέχεται να εφαρμόζουν ισχυρότερες μεθόδους ταυτοποίησής τους. Όταν τα μέλη είναι εσωτερικά τμήματα, υπάλληλοι της αρχής ή εξωτερικά συνεργατικά μέρη, οι διαδικασίες επαλήθευσης και εγγραφής μπορούν εύκολα να προσαρμοστούν στις εσωτερικές διαδικασίες του οργανισμού. Συγκεκριμένες διαδικασίες για την εγγραφή των χρηστών μιας υποδομής ARIBC περιγράφονται στην ενότητα 4.2.2. Τέλος, όλα τα καταχωρημένα δημόσια αναγνωριστικά αποθηκεύονται μαζί με τα δεδομένα αναγνώρισης χρήστη σε έναν κατάλογο τύπου LDAP.

3.2.3 Διανομή παραγόμενων ιδιωτικών κλειδιών

Όπως έχουμε ήδη αναφέρει, ο Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ) μιας υποδομής ARIBC δημιουργεί το ιδιωτικό κλειδί που αντιστοιχεί σε κάθε χρήστη. Ωστόσο, επειδή κανένας μηχανισμός ΚΒΤ (IBC) δεν παρέχει κάποιο μέσο για την ασφαλή διανομή των ιδιωτικών κλειδιών στους νόμιμους κατόχους τους, στην ενότητα 4.2.2 προτείνουμε κάποιες ενδεικτικές μεθόδους. Προς το παρόν, υποθέτουμε ότι οι χρήστες παραλαμβάνουν τα ιδιωτικά τους κλειδιά με τρόπο τέτοιο ώστε να διασφαλίζεται η εμπιστευτικότητά τους.

3.2.4 Δημοσίευση - Διαχείριση - Ανάκληση Δημόσιων Αναγνωριστικών και Ιδιωτικών Κλειδιών

Δεδομένου ότι τα δημόσια αναγνωριστικά είναι (έμμεσα) τα δημόσια κλειδιά των χρηστών μιας υποδομής ARIBC, δεν υπάρχει ανάγκη για ειδικές διαδικασίες για τη δημοσίευσή τους. Για παράδειγμα, τα έγκυρα δημόσια αναγνωριστικά των υπαλλήλων ή των τμημάτων ενός οργανισμού μπορεί εύκολα να βρεθούν στον επίσημο ιστότοπο του οργανισμού (π.χ. ένα συνθετικό των ονομάτων των υπηρεσιών ή της διεύθυνσης του ηλεκτρονικού ταχυδρομείου τους). Επομένως, είναι εύκολο να ανακληθεί ένα δημόσιο κλειδί, απλώς αντικαθιστώντας το με το νέο στον επίσημο ιστότοπο του οργανισμού[1]. Είναι αυτονόητο ότι η ανάκληση του ιδιωτικού κλειδιού ενός χρήστη συνεπάγεται και την ανάγκη ανανέωσης του δημόσιου αναγνωριστικού του χρήστη. Μία απλή λύση σε αυτό το πρόβλημα είναι το δημόσιο αναγνωριστικό να περιέχει και κάποια επιπρόσθετη προσδιοριστική τιμή, για παράδειγμα, «a.goudosis.ARIBC-IBC.gr.2020v1». Η δημιουργία των ιδιωτικών κλειδιών από τον ΑΚΣ δίνει τη δυνατότητα επιλογής της πολιτικής που θα ακολουθηθεί στη διαχείριση των ιδιωτικών κλειδιών. Δηλαδή, ανάλογα με τις ανάγκες και την πολιτική του

[1]Επειδή ένας παραβιασμένος ιστότοπος μπορεί να προωθεί πλαστογραφημένα δημόσια αναγνωριστικά, είναι σημαντικό να διασφαλιστεί η ακεραιότητά του.

οργανισμού, ο ΑΚΣ μπορεί να επιλέξει μεταξύ της αποθήκευσης των ιδιωτικών κλειδιών σε ένα ασφαλές αποθετήριο για μελλοντική χρήση ή να τα καταστρέψει μετά την απόδοσή τους στον νόμιμο ιδιοκτήτη.

3.2.5 Διάδραση με τους χρήστες

Προκειμένου να καταστεί δυνατή η διάδραση μιας υποδομής ARIBC με τους χρήστες, πρέπει να ικανοποιούνται ορισμένες προϋποθέσεις, οι οποίες αναφέρονται παρακάτω. Οι προϋποθέσεις αυτές αφορούν ένα πιθανό σενάριο υλοποίησης, που θεωρούμε ότι καλύπτει ένα ευρύ φάσμα οργανισμών.

1. Υπάρχει μια διαδικτυακή πύλη (π.χ. ARIBC-portal) που έχει ως ρόλο την υποδοχή νέων μελών. Μεταξύ άλλων, η πύλη επιτελεί τις λειτουργίες της υποδοχής ενός δημόσιου αναγνωριστικού, της εξαγωγής του αντίστοιχου ιδιωτικού κλειδιού και της αποστολής του, μαζί με τις δημόσιες παραμέτρους, στον χρήστη. Σημειώνεται ότι το ARIBC-portal χρησιμοποιείται μόνο μια φορά, κατά την αρχική φάση εγγραφής του χρήστη στη συγκεκριμένη υποδομή ARIBC.

2. Η διαδικτυακή πύλη (ARIBC-portal), όπως η πλειονότητα των ιστοσελίδων σήμερα, διαθέτει ένα κατάλληλο ζεύγος κλειδιών και τα αντίστοιχα πιστοποιητικά τους (π.χ. X509v3) μιας τυπικής υποδομής Public Key Infrastructure (PKI). Η ύπαρξη αυτής της υποδομής διευκολύνει τη φάση διανομής του ιδιωτικού κλειδιού, μέσω της δημιουργίας εικονικών δικτύων.

3. Υπάρχει δυνατότητα δημιουργίας εικονικών δικτύων VPNs, με χρήση ή συνδυασμό χρήσης ευρέως διαδεδομένων και σε καθημερινή χρήση πρωτόκολλων όπως τα: HTTPS/ Transport Layer Security (TLS), IPSec.

4. Για λόγους ασφαλείας, ο ΑΚΣ και όλος ο μηχανισμός δημιουργίας ιδιωτικών κλειδιών της ΚΒΤ (IBC) λειτουργεί σε εξυπηρετητή διαφορετικό απο εκείνον που φιλοξενεί τη διαδικτυακή πύλη (ARIBC-portal) και, αν είναι δυνατό, εκτός σύνδεσης με το δίκτυο.

5. Η διαδικτυακή πύλη (ARIBC-portal) περιέχει ενημερωτικές πληροφορίες για τις διαδικασίες που θα πρέπει να ακολουθήσουν οι χρήστες για να εγγραφούν και για το μορφότυπο που θα πρέπει να έχει το δημόσιο αναγνωριστικό τους.

6. Η αλληλεπίδραση των χρηστών με τον ΑΚΣ, μέσω της διαδικτυακής πύλης (ARIBC-portal), γίνεται μέσω ειδικής εφαρμογής (ARIBC-app), η οποία θα μπορεί να λειτουργήσει τόσο σε Η/Υ όσο και σε ευφυές κινητό τηλέφωνο. Η εφαρμογή (ARIBC-app) θα προσφέρει και δυνατότητα ψευδωνυμοποίησης του δημόσιου αναγνωριστικού του χρήστη.

7. Η υποδομή ARIBC δεν προσφέρει ανωνυμια σε επίπεδο δικτύου· τέτοια προστασία είναι εκτός του πλαισίου της διατριβής. Όμως, για λόγους πληρότητας, επισημαίνουμε ότι ένας ανώνυμος αναφέρων θα πρέπει να αποκρύψει πιθανά αναγνωριστικά του δικτύου (π.χ. διευθύνσεις IP, κάρτες ταυτότητας, αναγνωριστικά βάσει μηχανής) και του εξοπλισμού του (π.χ. διευθύνσεις IP, κάρτες ταυτότητας, αναγνωριστικά βάσει μηχανής κτλ.). Οι πολίτες που επιθυμούν να διασφαλίσουν πλήρως την ανωνυμια τους θα πρέπει επιπρόσθετα να χρησιμοποιούν και κατάλληλες τεχνικές διαδικτυακής

ανωνυμοποίησης, για παράδειγμα Εικονικά Ιδιωτικά Δίκτυα ανωνυμοποίησης (anonymizing VPNs) ή/και φορητά λειτουργικά συστήματα ανωνυμοποίησης (π.χ. Amnesic OSs).

Κεφάλαιο 4

Υλοποιήσεις της υποδομής ARIBC

4.1 Εισαγωγή

Σ΄ αυτό το κεφάλαιο παρουσιάζουμε δύο υλοποιήσεις της υποδομής ARIBC που περιγράφηκε στο Κεφάλαιο 3. Η πρώτη υλοποίηση βασίζεται στον μηχανισμό κρυπτογράφησης Sakai-Kasahara Identity Based Encryption (SKIBE) και στον μηχανισμό ψηφιακής υπογραφής BLMQ που έχει ως βάση τον μηχανισμό Sakai-Kasahara[1], όπως αυτός προτείνεται στο [22] σύμφωνα με τις οδηγίες του IEEE 1363.3-2013 [16]. Οι τεχνικές λεπτομέρειες του σχήματος αυτού περιγράφηκαν αναλυτικά στην ενότητα 2.2.

Η δεύτερη υλοποίηση βασίζεται στο συνδυαστικό σχήμα ECCSI (RFC6507) - SAKKE (RFC6508), που αναλύσαμε στην ενότητα 2.3.

4.2 Υλοποίηση με το σχήμα BLMQ-SKIBE

4.2.1 Σύσταση της υποδομής ARIBC BLMQ-SKIBE

Η υλοποίηση ARIBC BLMQ-SKIBE αρχίζει από τη δημιουργία ενός ΑΚΣ, τον οποίο στην ενότητα 2.2 ο ονομάσαμε (PKG), συνεπώς εδώ (ARIBC-PKG), προκειμένου να υπάρχει συμφωνία και εύκολη αντιστοίχιση με το πρότυπο IEEE 1363.3.

Η ρύθμιση του ARIBC-PKG περιλαμβάνει τα εξής στάδια:

1. **Ορισμός παραμέτρων ασφαλείας (ΠΑ) και δημόσιων παραμέτρων (ΔΠ/*PP*) του ARIBC-PKG**. Οι παράμετροι ασφάλειας κάθε υποδομής ARIBC BLMQ-SKIBE πρέπει να επιλεγούν έτσι ώστε να επιτυγχάνεται η σωστή ισορροπία μεταξύ αποτελεσματικότητας και ζητούμενου επιπέδου ασφάλειας. Ο προσδιορισμός των βέλτιστων παραμέτρων απαιτεί μεθοδική διερεύνηση των ειδικών αναγκών και των χαρακτηριστικών της Αρχής στην οποία πρόκειται να εγκατασταθεί η υποδομή ARIBC BLMQ-SKIBE. Σ΄ αυτήν τη διατριβή περιγράφουμε μια γενική υποδομή ARIBC, ακολουθώντας τις γενικές οδηγίες και προτάσεις του προτύπου IEEE 1363.3-2013 [16]. Οι τεχνικές λεπτομέρειες περιγράφηκαν αναλυτικά στην ενότητα 2.2.1.

[1] Όπως αναφέρεται στο [21]: ¨είναι ουσιαστικά το σχήμα υπογραφής Sakai-Kasahara¨

2. **Επιλογή του Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ/MS_{Secret}) και υπολογισμός του Θεμελιώδους Δημόσιου Κλειδιού (ΘΔΚ) (MS_{Pub}) του ARIBC-PKG.** Επιλέγεται ένας τυχαίος ακέραιος ως το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/MS_{Secret}) του ARIBC-PKG και υπολογίζεται το Θεμελιώδες Δημόσιο Κλειδί, το οποίο στη συνέχεια σ' αυτό το κεφάλαιο θα συμβολίζεται ως (MS_{Pub}). Οι σχετικές τεχνικές λεπτομέρειες περιγράφηκαν αναλυτικά στην ενότητα 2.2.2 Υπενθυμίζουμε ότι ο ΑΚΣ (ARIBC-PKG) της συγκεκριμένης υλοποίησης είναι υπεύθυνος για τη λήψη όλων των απαραίτητων μέτρων για τη διασφάλιση της εμπιστευτικότητας και της διαθεσιμότητας του Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ) (MS_{Secret}).

3. **Δημοσίευση Δημόσιων Παραμέτρων (ΔΠ/*PP*) του ARIBC-PKG.** Αυτές οι παράμετροι είναι στατικές και οι χρήστες της συγκεκριμένης υποδομής ARIBC μπορούν να τις αποθηκεύσουν για μελλοντική χρήση.

4. **Εξαγωγή του Ιδιωτικού Κλειδιού ($ID_{Private}$).** Το ιδιωτικό κλειδί εξάγεται από τον ΑΚΣ με τη χρήση του μοναδικού αναγνωριστικού *ID* του χρήστη, του *Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ/(MS_{Sec})* του ΑΚΣ και των Δημόσιων Παραμέτρων (*PP*). Οι σχετικές τεχνικές λεπτομέρειες περιγράφηκαν αναλυτικά στην ενότητα 2.2.3.

4.2.2 Εγγραφή του Αναφέροντος

Η υποδομή ARIBC BLMQ-SKIBE υποστηρίζει τόσο ανώνυμους όσο και επώνυμους αναφέροντες. Είναι αυτονόητο ότι οι διαδικασίες εγγραφής θα είναι διαφορετικές για επώνυμους και ανώνυμους χρήστες, και μπορούν να καθοριστούν ανάλογα με τις ανάγκες της υπηρεσίας. Η εγγραφή των επώνυμων αναφερόντων μπορεί να γίνει είτε με τη συνδρομή είτε ανεξάρτητα από τον ΑΚΣ (ARIBC-PKG) της συγκεκριμένης υποδομής. Κατά συνέπεια, μπορούν να συνδυαστούν διαφορετικής ισχύος διαδικασίες για να εξακριβωθεί η πραγματική ταυτότητα του αναφέροντος. Για παράδειγμα, μπορεί να χρησιμοποιηθεί μια απλή ταυτοποίηση μέσω ενός λογαριασμού ηλεκτρονικού ταχυδρομείου ή πολύ ισχυρή ταυτοποίηση, μέσω της παρουσίασης ενός επίσημου εγγράφου αναγνώρισης (π.χ. δελτίο ταυτότητας, διαβατήριο) ή ενός ηλεκτρονικού λογαριασμού σε άλλη υπηρεσία (π.χ. Τράπεζα, ΓΓΠΣ κτλ.). Αντίθετα, η εγγραφή ανώνυμων αναφερόντων πραγματοποιείται αποκλειστικά ηλεκτρονικά, μέσω του ΑΚΣ (ARIBC-PKG).

Οι βασικές διαδικασίες και λειτουργίες της Εγγραφής διακρίνονται σε:

- Διαδικασίες και λειτουργίες που δεν σχετίζονται άμεσα με την υποδομή ARIBC BLMQ-SKIBE (π.χ. τεχνικές ανωνυμοποίησης δικτύου, λήψη ειδικών εφαρμογών από το Διαδίκτυο).
- Εσωτερικές διαδικασίες στην πλευρά των χρηστών (π.χ. η εφαρμογή ARIBC-App).
- Εσωτερικές διαδικασίες στην πλευρά του ΑΚΣ (π.χ. ο ιστότοπος της υποδομής ARIBC BLMQ-SKIBE (ARIBC-PKG-Portal) και ο ΑΚΣ (Private Key Generator (PKG)).
- Επικοινωνία-Ανταλλαγή δεδομένων μέσω διαδικτύου μεταξύ της εφαρμογής ARIBC-client-app και του ΑΚΣ (ARIBC-PKG) (π.χ. η μετάδοση των αναγνωριστικών των οντοτήτων στον ΑΚΣ).

Η διαδικασία εγγραφής, τόσο για τον ανώνυμο όσο και για τον επώνυμο αναφέροντα, παρουσιάζεται στο Σχήμα 4.1, όπου τα μπλε βέλη υποδηλώνουν επικοινωνία που προστατεύεται από το TLS-VPN (δηλαδή, μια τυπική σύνδεση HTTPS/TLS που χρησιμοποιεί ένα τυπικό πιστοποιητικό ιστότοπου π.χ. X509), ενώ τα κόκκινα βέλη και κελιά υποδηλώνουν επικοινωνία που προστατεύεται από την υποδομή ARIBC. Σημειώστε ότι ο ανώνυμος αναφέρων πρέπει να επιλέξει (ή να δημιουργήσει) το *ID* που θα χρησιμοποιεί στην υποδομή ARIBC προκειμένου να συνδεθεί στον ΑΚΣ, ο οποίος στη συνέχεια θα εξάγει και θα αποστείλει το ιδιωτικό κλειδί στον αναφέροντα.

Το επιλεγμένο *ID* μπορεί να είναι οποιαδήποτε συμβολοσειρά, συμπεριλαμβανομένης της εξόδου μιας κρυπτογραφικής συνάρτησης κατακερματισμού της επιλογής του αναφέροντος. Έτσι, παρέχεται η δυνατότητα στον αναφέροντα, εφόσον το επιθυμεί, να χρησιμοποιήσει την πραγματική του ταυτότητα σε συνδυασμό με ένα μυστικό κλειδί ως εισαγωγή στη συνάρτηση κατακερματισμού. Έτσι, εάν κάποια στιγμή ο αναφέρων θελήσει να αποδείξει την πραγματική του ταυτότητα, δεν έχει παρά να παρουσιάσει το κλειδί για την αποκρυπτογράφηση του (κατακερματισμένου) *ID* του.

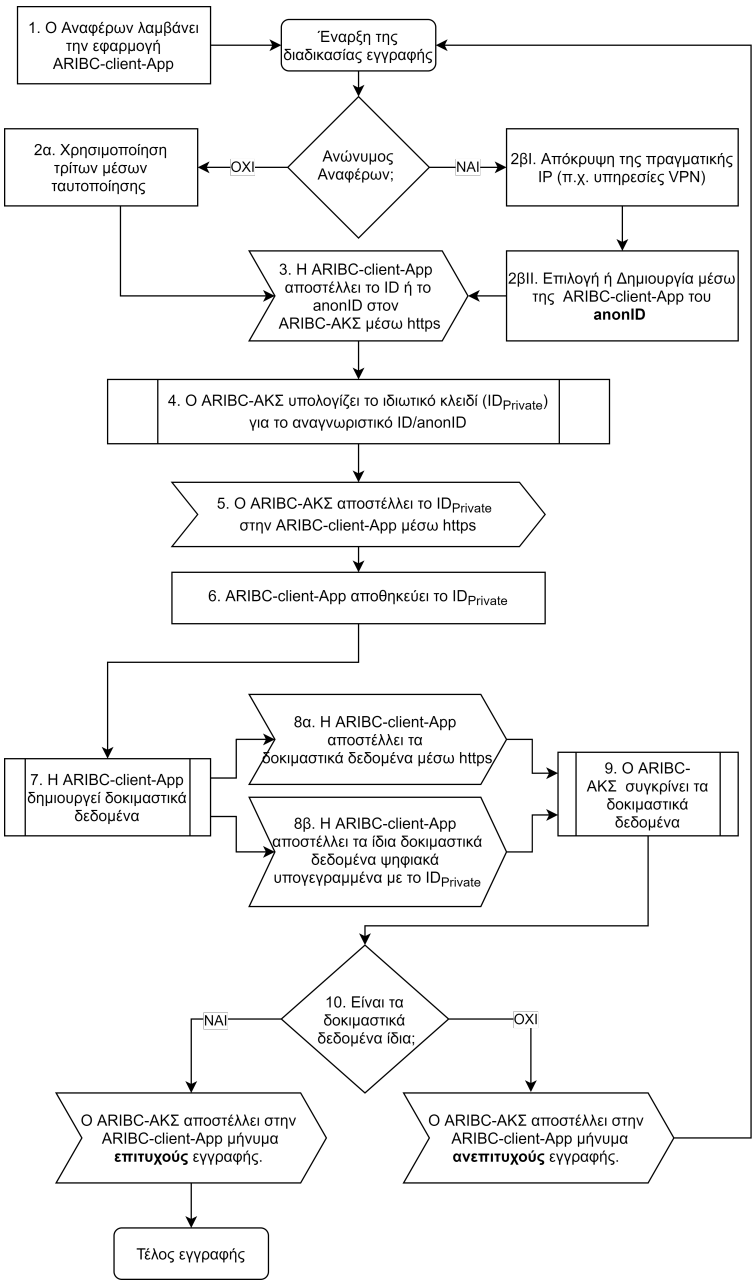
4.2.3 Υπηρεσίες Ακεραιότητας και Γνησιότητας μέσω Ψηφιακής Υπογραφής

Η υποδομή ARIBC BLMQ-SKIBE προσφέρει υπηρεσίες ακεραιότητας και γνησιότητας μέσω ψηφιακής υπογραφής όλων των δεδομένων που αποστέλλονται από τους εγγεγραμμένους χρήστες της. Σημειώνουμε ότι οποιοσδήποτε, όχι μόνο οι εγγεγραμμένοι χρήστες της ARIBC BLMQ-SKIBE, μπορεί να επαληθεύσει την ψηφιακή υπογραφή και, συνεπώς, την αυθεντικότητα και την ακεραιότητα των ψηφιακά υπογεγραμμένων δεδομένων.

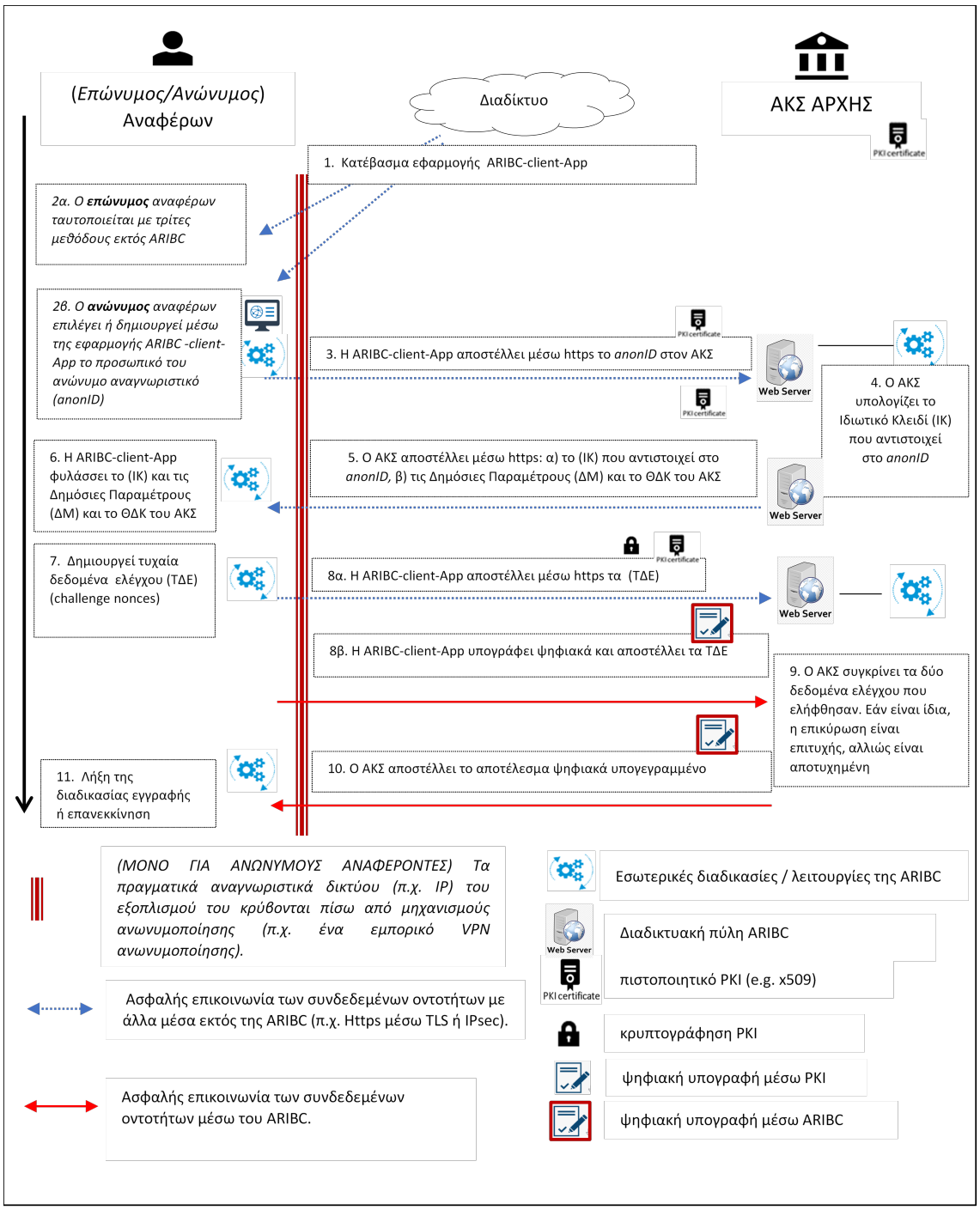
Στη διαδικασία ελέγχου της αυθεντικότητας και της ακεραιότητας των ψηφιακά υπογεγραμμένων δεδομένων συμμετέχουν δύο οντότητες, ο Υπογράφων (Signer) και ο Επαληθευτής (Verifier). Ο Υπογράφων υπογράφει ψηφιακά τα δεδομένα με την ψηφιακή του υπογραφή και ακολούθως ο Επαληθευτής επαληθεύει την εγκυρότητα της υπογραφής και συνεπώς την αυθεντικότητα και την ακεραιότητα των υπογεγραμμένων δεδομένων. Ο Υπογράφων μπορεί να είναι οποιοσδήποτε εγγεγραμμένος χρήστης της υποδομής ARIBC BLMQ-SKIBE, π.χ. ένας αναφέρων, ο οποίος διαθέτει έγκυρο ιδιωτικό κλειδί $Signer_{Private}$. Ο Επαληθευτής, ο οποίος δεν είναι κατ' ανάγκη εγγεγραμμένος χρήστης της υποδομής ARIBC BLMQ-SKIBE, χρειάζεται μόνο το (δημόσια διαθέσιμο) ID_{signer} του υπογράφοντος και τις δημόσιες παραμέτρους του ΑΚΣ/ ARIBC-PKG στον οποίο ανήκει ο Υπογράφων, προκειμένου να επικυρώσει την υπογραφή.

Η υπηρεσία ακεραιότητας και γνησιότητας μέσω ψηφιακής υπογραφής υλοποιείται μέσω των διαδικασιών που προσφέρει η υπογραφή βάσει ταυτότητας του μηχανισμού BLMQ [22], [16], δηλαδή της διαδικασίας δημιουργίας και επαλήθευσης ψηφιακών υπογραφών. Οι σχετικές τεχνικές λεπτομέρειες περιγράφηκαν αναλυτικά στην ενότητα 2.2.4.

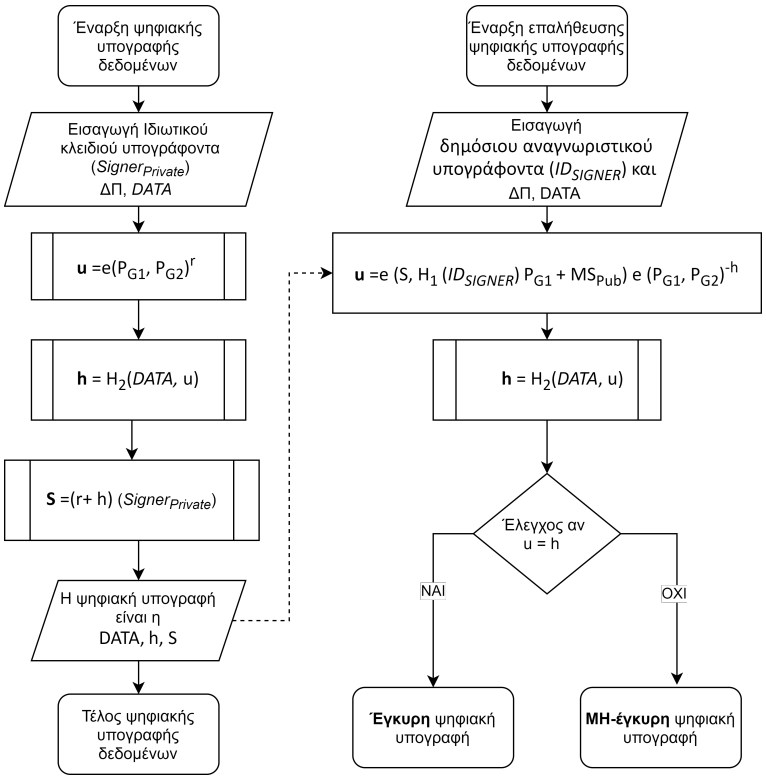
Η ροή της διαδικασίας Ψηφιακής Υπογραφής όσο και της διαδικασίας Επαλήθευσής της στην υποδομή ARIBC BLMQ-SKIBE παρουσιάζεται στο Σχήμα 4.3.



Σχήμα 4.1: Ροή διαδικασίας εγγραφής επώνυμων και ανώνυμων αναφερόντων στην υποδομή ARIBC BLMQ-SKIBE.



Σχήμα 4.2: Διαδικασία εγγραφής επώνυμων και ανώνυμων αναφερόντων στην υποδομή ARIBC BLMQ-SKIBE.



Σχήμα 4.3: Ροή των διαδικασιών Δημιουργίας και Επαλήθευσης ψηφιακής υπογραφής στην υποδομή ARIBC BLMQ-SKIBE

4.2.4 Υπηρεσία εμπιστευτικότητας

Η υποδομή ARIBC BLMQ-SKIBE προσφέρει υπηρεσίες εμπιστευτικότητας δεδομένων μέσω κρυπτογράφησης των δεδομένων που αποστέλλονται προς τους εγγεγραμμένους χρήστες της, με τη χρήση του δημόσιου αναγνωριστικού ($ID_{Receiver}$) του παραλήπτη. Σημειώνουμε ότι οποιοσδήποτε, όχι μόνο οι εγγεγραμμένοι χρήστες της υποδομής ARIBC, μπορεί να κρυπτογραφήσει δεδομένα και να τα στείλει προς τους εγγεγραμμένους χρήστες της. Ο παραλήπτης, και μόνο αυτός, μπορεί να αποκρυπτογραφήσει το μήνυμα, χρησιμοποιώντας το αντίστοιχο ιδιωτικό κλειδί του ($Receiver_{Private}$).

Στην υπηρεσία εμπιστευτικότητας δεδομένων συμμετέχουν δύο οντότητες: ο Αποστολέας των δεδομένων (Sender) και ο Παραλήπτης (Receiver). Ο Αποστολέας κρυπτογραφεί τα δεδομένα και ο Παραλήπτης τα αποκρυπτογραφεί. Ο Αποστολέας χρειάζεται μόνο το δημόσια διαθέσιμο $ID_{Receiver}$ του Παραλήπτη και τις δημόσιες παραμέτρους του ΑΚΣ/ARIBC-PKG που ανήκει ο Παραλήπτης προκειμένου να κρυπτογραφήσει τα δεδομένα. Ο Παραλήπτης μπορεί να είναι οποιοσδήποτε εγγεγραμμένος χρήστης της υποδομής ARIBC BLMQ-SKIBE, π.χ. ένας αναφέρων, ο οποίος διαθέτει έγκυρο ιδιωτικό κλειδί $Receiver_{Private}$.

Η υπηρεσία εμπιστευτικότητας δεδομένων μέσω κρυπτογράφησης των δεδομένων υλοποιείται μέσω των διαδικασιών Κρυπτογράφησης και Αποκρυπτογράφησης που προσφέρει ο μηχανισμός SKIBE [20], [16], δηλαδή της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης δεδομένων. Οι σχετικές τεχνικές λεπτομέρειες περιγράφηκαν αναλυτικά στην ενότητα 2.2.5.

Η ροή τόσο της διαδικασίας Κρυπτογράφησης όσο και της διαδικασίας Αποκρυπτογράφησης δεδομένων της υποδομής ARIBC BLMQ-SKIBE παρουσιάζεται στο Σχήμα 4.4.

Επειδή η χρήση ασύμμετρης κρυπτογράφησης θεωρείται μη αποδοτική για την κρυπτογράφηση μεγάλου όγκου δεδομένων, η δυνατότητα εμπιστευτικής αποστολής δεδομένων που παρέχει η υποδομή ARIBC BLMQ-SKIBE μπορεί να χρησιμοποιηθεί και για την εμπιστευτική ανταλλαγή ενός συμμετρικού κλειδιού συνόδου.

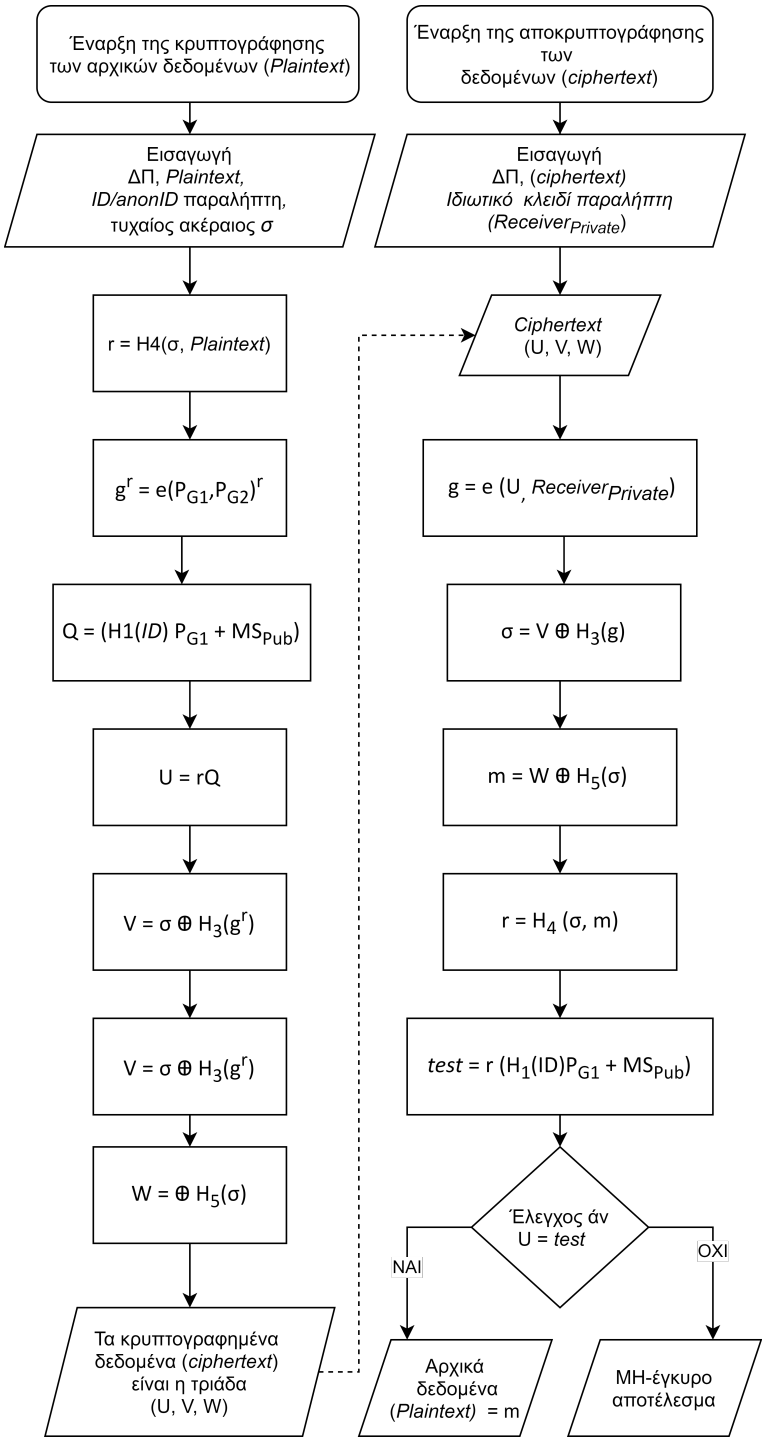
4.3 Υλοποίηση με το σχήμα ECCSI-SAKKE

Το σχήμα ECCSI-SAKKE προσθέτει μεν πολυπλοκότητα στην υλοποίηση, αλλά προσφέρει δοκιμασμένους αλγορίθμους υλοποίησης, τιμές ελέγχου και επιβεβαίωσης, στα σχετικά Παραρτήματα των RFC6507 και RFC6508, διευκολύνοντας έτσι την επίδειξη της λειτουργίας της υποδομής ARIBC ECCSI-SAKKE που παρουσιάζεται στο Κεφάλαιο 5.

4.3.1 Διαφορές της ARIBC ECCSI-SAKKE από την ARIBC BLMQ-SKIBE

Ενώ η ιδέα, η αρχή λειτουργίας της υποδομής ARIBC, ο τρόπος με τον οποίο οι χρήστες αντιλαμβάνονται την υποδομή και τις υπηρεσίες της, καθώς και οι οντότητες που την απαρτίζουν είναι οι ίδιες, ανεξάρτητα από το σχήμα που θα χρησιμοποιηθεί για την υλοποίησή της, η υλοποίηση με βάση το σχήμα ECCSI-SAKKE διαφέρει απ' εκείνη με βάση το σχήμα BLMQ-SKIBE. Παρακάτω συνοψίζουμε τις σημαντικότερες διαφορές της υποδομής ARIBC ECCSI-SAKKE από την υποδομή ARIBC BLMQ-SKIBE. Οι τεχνικές λεπτομέρειες του σχήματος ECCSI-SAKKE περιγράφηκαν αναλυτικά στην ενότητα 2.3.

1. Η χρήση του μηχανισμού ECCSI αντί του σχήματος BLMQ για έλεγχο ταυτότητας (βλ. Σχήμα 4.6).
2. Η χρήση του μηχανισμού SAKKE αντί του γενικού μηχανισμού SKIBE των Sakai-Kasahara. Στην πραγματικότητα, ο μηχανισμός SAKKE είναι η βασική παραλλαγή του SKIBE ως μηχανισμού ενθυλάκωσης (SKKEM), όπως το βρίσκουμε στο IEEE1363-3 [16] (βλ. RFC6508).
3. Επειδή το σχήμα ECCSI-SAKKE επιτρέπει στην υποδομή ARIBC ECCSI-SAKKE τη χρήση διαφορετικού σχήματος πιστοποίησης των δεδομένων ή εμπιστευτικότητας, ανάλογα με τις επιθυμίες της Αρχής που φιλοξενεί την υποδομή (βλ. Σχήμα 2.1), μια Αρχή που υιοθετεί το ARIBC ECCSI-SAKKE έχει τη δυνατότητα να χρησιμοποιήσει τον μηχανισμό ECCSI για (ανώνυμους) αναφέροντες σε συνδυασμό με πιστοποιητικά που βασίζονται σε X509 (εάν υπάρχουν ήδη) των υπαλλήλων της για τον έλεγχο ταυτότητας των μηνυμάτων του μηχανισμού SAKKE που θα χρησιμοποιείται για τη διανομή συμμετρικών κλειδιών συνόδου.
4. Για τον ίδιο όπως παραπάνω λόγο, μια Αρχή στην οποία λειτουργεί υποδομή ARIBC ECCSI-SAKKE έχει τη δυνατότητα να χρησιμοποιήσει τον μηχανισμό SAKKE για τη δημιουργία συμμετρικών κλειδιών συνόδου σε ασύγχρονες



Σχήμα 4.4: Ροή διαδικασιών Κρυπτογράφησης δεδομένων και Αποκρυπτογράφησης δεδομένων στην υποδομή ARIBC BLMQ-SKIBE

εφαρμογές (π.χ. ηλεκτρονικό ταχυδρομείο), σε συνδυασμό με μηχανισμούς τύπου Diffie-Hellman για τη δημιουργία συμμετρικών κλειδιών συνόδου σε σύγχρονες (online) εφαρμογές. Σε κάθε περίπτωση, η ταυτοποίηση των συναλλασσόμενων μερών θα μπορεί να γίνεται μέσω του μηχανισμού ECCSI.

5. Στην πραγματικότητα, το ECCSI και το SAKKE είναι δύο παράλληλες υλοποιήσεις που μπορεί να λειτουργούν αυτόνομα ή σε συνδυασμό. Ως εκ τούτου, χρησιμοποιούμε ένα διπλό ΑΚΣ, τα δυο μέρη του οποίου ονομάζουμε KMS-ECCSI και KMS-SAKKE αντίστοιχα, ακολουθώντας την ορολογία των RFC65108, RFC6509, όπου ο ΑΚΣ ονομάζεται Key Management Server (KMS). Ο διπλός ΑΚΣ ορίζει τις Δημόσιες Παράμετρους KMS-ECCSI-PP του KMS-ECCSI και τις Δημόσιες Παράμετρους KMS-SAKKE-PP του KMS-SAKKE. Στο σχήμα 4.5 απεικονίζεται η ροή διεργασιών για την υλοποίηση ενός διπλού ΑΚΣ σε υποδομή ARIBC ECCSI-SAKKE.

6. Ο κάθε ΚΜΣ χρησιμοποιεί διαφορετικές κρυπτογραφικές δημόσιες παραμέτρους, διαφορετικά Θεμελιώδη Κλειδιά και διαφορετικά Ιδιωτικά Κλειδιά για κάθε χρήστη. Έτσι, ο KMS-ECCSI επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/KSAK) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ/KPAK) που θα χρησιμοποιείται με το πρωτόκολλο ECCSI, ενώ ο KMS-SAKKE επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/z) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ/Z) που θα χρησιμοποιείται με το πρωτόκολλο SAKKE.Ανάλογα, ο KMS-ECCSI εκδίδει το Secret Signing key (SSK) και το Public Validation Token (PVT) για την ψηφιακή υπογραφή των δεδομένων που θα χρησιμοποιούνται με το πρωτόκολλο ECCSI , ενώ ο KMS-SAKKE εκδίδει το Receiver Secret key (RSK) που θα χρησιμοποιείται στην αποθυλάκωση με το πρωτόκολλο SAKKE.

4.3.2 Διαλειτουργικότητα υποδομών ARIBC ECCSI-SAKKE

Διαφορετικές Αρχές ενδέχεται να υποστηρίζουν και να λειτουργούν τις δικές τους υποδομές ARIBC ECCSI-SAKKE, που θα πρέπει να μπορούν να διαλειτουργήσουν. Υποθέτουμε ότι δύο διαφορετικές Αρχές, η X και η Y υλοποιούν δύο ανεξάρτητες ARIBC ECCSI-SAKKE, με αντίστοιχους ΑΚΣ τους KMS-X-ECCSI/KMS-X-SAKKE και KMS-Y-ECCSI/KMS-Y-SAKKE.

Στη συνέχεια υποθέτουμε ότι μια οντότητα (π.χ. ένας αναφέρων) A έχει εγγραφεί στην υποδομή ARIBC-X ECCSI-SAKKE και αντίστοιχα μια οντότητα (π.χ. ένας υπάλληλος μιας υπηρεσίας) B έχει εγγραφεί στην υποδομή ARIBC-Y ECCSI-SAKKE.

Στο σενάριο αυτό:

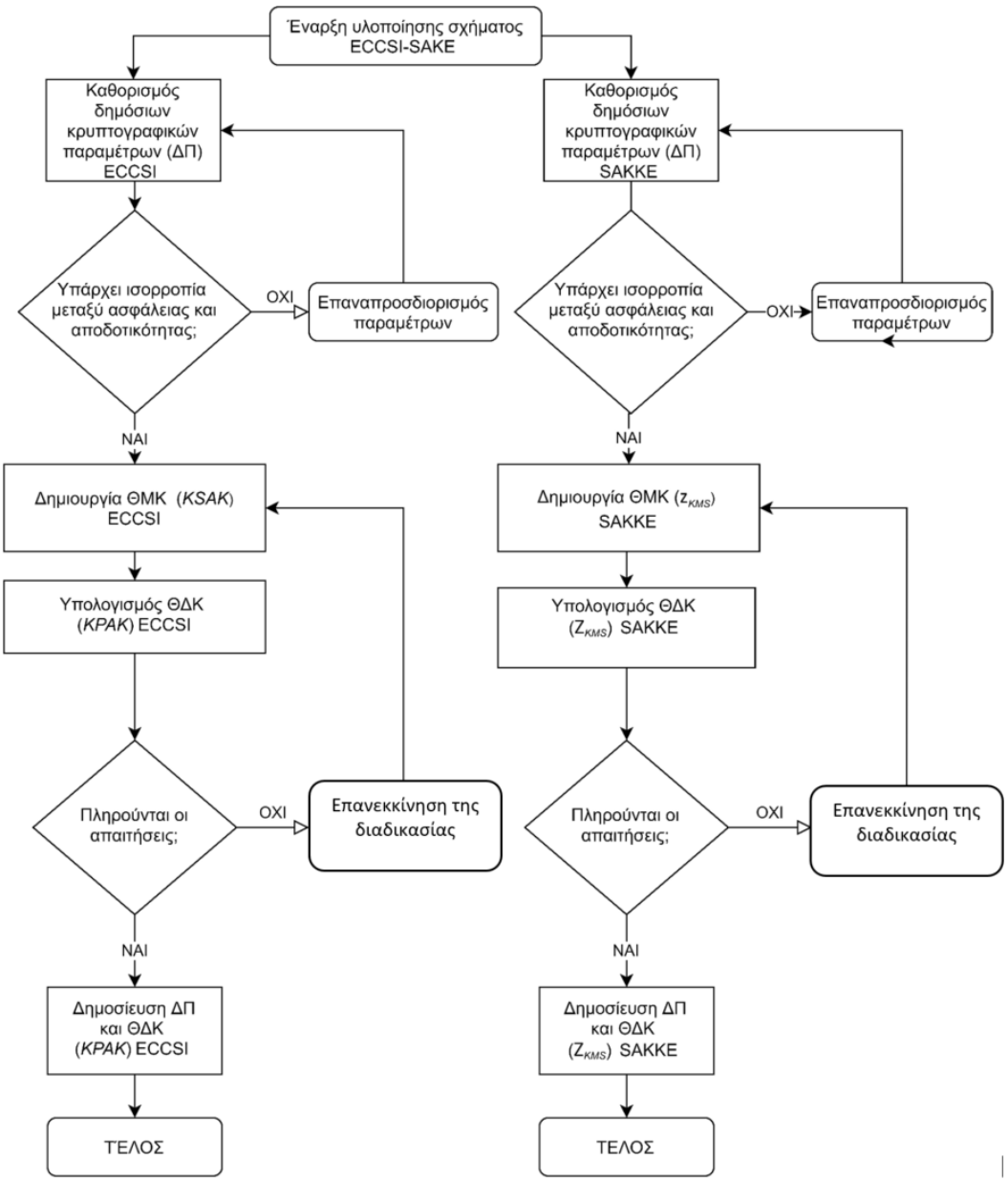
1. Στην υποδομή ARIBC-X ECCSI-SAKKE λειτουργούν οι KMS-X-ECCSI και /KMS-X-SAKKE.

2. Ο KMS-X-ECCSI έχει:

   (α΄) Τις Δημόσιες Παραμέτρους: ECCSI-PP$_X$

   (β΄) Το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ): $KSAK_X$

   (γ΄) Το Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ): $KPAK_X$



Σχήμα 4.5: Ροή διεργασιών υλοποίησης ενός διπλού ΑΚΣ σε υποδομή ARIBC ECCSI-SAKKE.

3. Ο KMS-X-SAKKE έχει:

   (α΄) Τις Δημόσιες Παραμετρούς: SAKKE-PP$_X$

   (β΄) Το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ): z_X

   (γ΄) Το Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ): Z_X

4. Τα Ιδιωτικά κλειδιά του A είναι:

   (α΄) το Ιδιωτικό Κλειδί ψηφιακής Υπογραφής (ΙΚΥ)/(Secret Signing key (SSK_A)) και το Δημόσιο Τεκμήριο Επικύρωσης (ΔΤΕ)/(Public Validation Token (PVT_A)) για την ψηφιακή υπογραφή των δεδομένων με το πρωτόκολλο ECCSI.

   (β΄) το Μυστικό Κλειδί Αποδέκτη (ΜΚΑ)/(Receiver Secret key RSK_A) που θα χρησιμοποιείται στην αποθυλάκωση με το πρωτόκολλο SAKKE.

Αντίστοιχα ισχύουν για την υποδομή ARIBC-Y ECCSI-SAKKE, στην οποία λειτουργούν οι KMS-Y-ECCSI και /KMS-Y-SAKKE και στην οποία έχει εγγραφεί η οντότητα B.

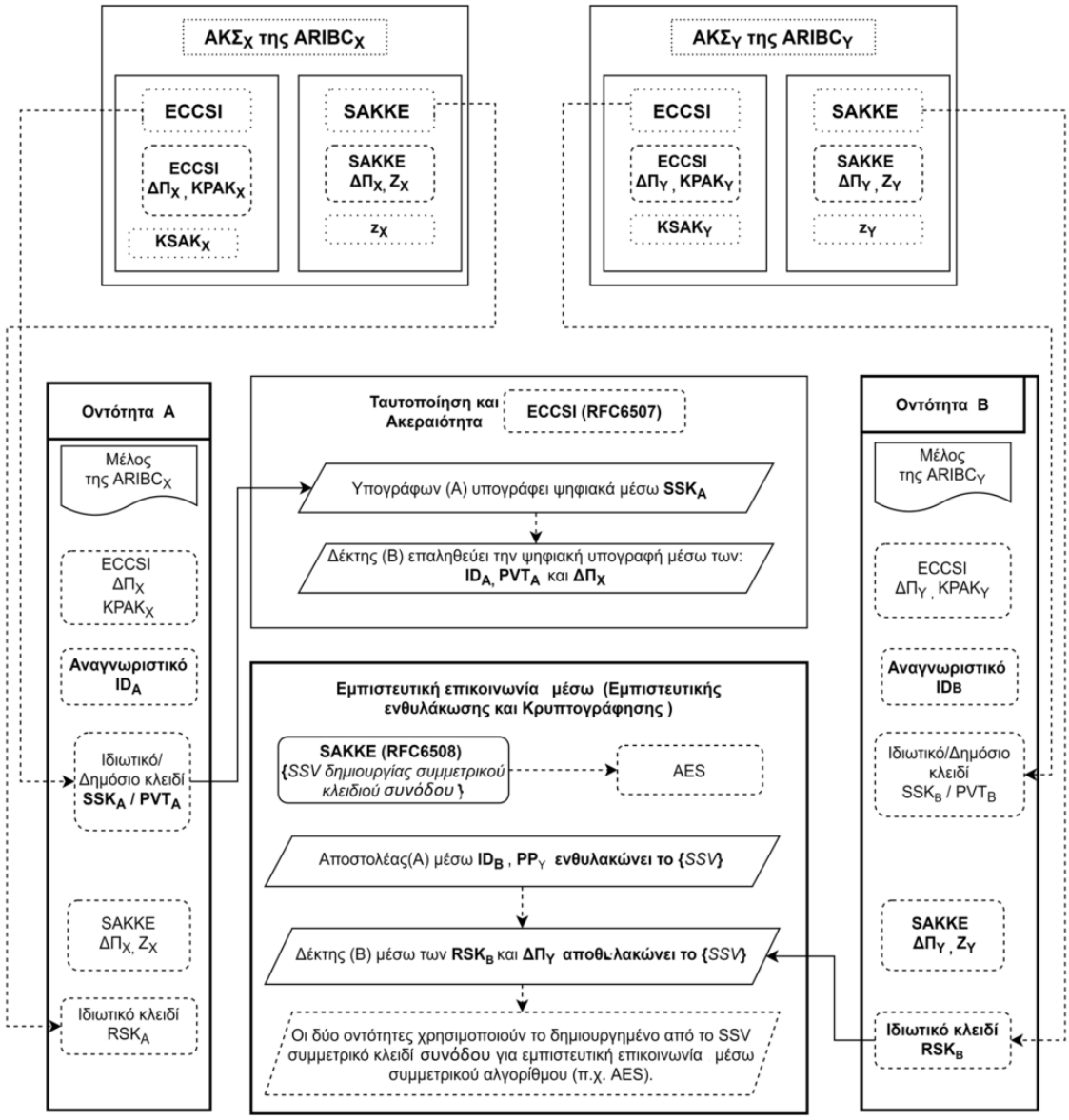
Στο Σχήμα 4.6 απεικονίζεται διαγραμματικά η διαδικασία αποστολής από την οντότητα $A \in$ ARIBC-X ECCSI-SAKKE στην οντότητα $B \in$ ARIBC-Y ECCSI-SAKKE υλικού (SSV) για τη δημιουργία συμμετρικού κλειδιού συνόδου, ενθυλακωμένου μέσω του μηχανισμού (SAKKE) και ψηφιακά υπογεγραμμένου με τον μηχανισμό (ECCSI).

4.3.3 Πρωτόκολλο Εγγραφής (ανώνυμου) αναφέροντος στην υποδομή ARIBC ECCSI-SAKKE

Η γενική αρχή, οι διαδικασίες, η εφαρμογή και οι λειτουργίες της υποδομής ECCSI-SAKKE ARIBC είναι παρόμοιες μ΄ εκείνες της υποδομής ARIBC-BLMQ-SKIBE , που περιγράφηκαν στην ενότητα 4.2.2. Μία εύχρηστη εφαρμογή (ARIBC-App) στην πλευρά του αναφέροντος είναι υπεύθυνη για τις διάφορες διαδικασίες εγγραφής στην υποδομή ARIBC ECCSI-SAKKE. Συνοπτικά, η εφαρμογή πελάτη έχει βοηθητικά προγράμματα για να δημιουργήσει το αναγνωριστικό του αναφέροντος σύμφωνα με τους κανόνες τυποποίησης της συγκεκριμένης υποδομής ARIBC ECCSI-SAKKE, να ολοκληρώσει τη φάση εγγραφής, να υπογράψει ψηφιακά ένα μήνυμα μέσω του μηχανισμού ECCSI, και να ενθυλακώσει το υλικό δημιουργίας συμμετρικού κλειδιού συνόδου (SAKKE). Η ίδια εφαρμογή (ARIBC-App) στην πλευρά του Παραλήπτη θα πιστοποιήσει την αυθεντικότητα του ληφθέντος ενθυλακωμένου υλικού και εν συνεχεία θα το αποθυλακώσει, προκειμένου να ανακτήσει το συμμετρικό κλειδί συνόδου.

Η φάση εγγραφής παρουσιάζεται σχηματικά στο Σχήμα 4.7, τόσο για τον ανώνυμο όσο και για τον επώνυμο αναφέροντα. Με μπλε βέλη υποδεικνύεται η επικοινωνία που προστατεύεται από το TLS VPN (δηλαδή, μια τυπική σύνδεση HTTPS / TLS που χρησιμοποιεί ένα τυπικό πιστοποιητικό ιστότοπου). Οι επώνυμοι αναφέροντες χρησιμοποιούν την πραγματική τους ταυτότητα, ενώ ο ανώνυμος αναφέρων πρέπει να επιλέξει (ή να δημιουργήσει) το ανώνυμο δημόσιο αναγνωριστικό του (*anonID*).

Όπως και στην υλοποίηση με το σχήμα BLMQ-SKIBE, οι βασικές διαδικασίες και λειτουργίες της Εγγραφής διακρίνονται σε:



Σχήμα 4.6: Διαλειτουργικότητα υποδομών ARIBC ECCSI-SAKKE.

- Διαδικασίες και λειτουργίες που δεν σχετίζονται άμεσα με την υποδομή ARIBC ECCSI-SAKKE (π.χ. τεχνικές ανωνυμοποίησης δικτύου, λήψη ειδικών εφαρμογών από το Διαδίκτυο).
- Εσωτερικές διαδικασίες στην πλευρά των χρηστών (π.χ. η εφαρμογή ARIBC-App).
- Εσωτερικές διαδικασίες στην πλευρά του ΑΚΣ (π.χ. ο ιστότοπος της υποδομής ARIBC ECCSI-SAKKE και ο ΑΚΣ (ARIBC-KMS-Portal).
- Επικοινωνία-Ανταλλαγή δεδομένων μέσω διαδικτύου μεταξύ της εφαρμογής ARIBC-client-app και του ΑΚΣ (ARIBC-KMS) (π.χ. η μετάδοση των αναγνωριστικών των οντοτήτων στον ΑΚΣ).

Στο Σχήμα 4.7 παρουσιάζεται η διαδικασία εγγραφής των επώνυμων και ανώνυμων αναφερόντων σε υποδομή ARIBC ECCSI-SAKKE. Σημειώνεται ότι σε σύγκριση με τη διαδικασία εγγραφής σε υποδομή ARIBC BLMQ-SKIBE, παραλείπουμε τα επιπλέον βήματα επικύρωσης 7-11 στο Σχήμα 4.2, επειδή οι μηχανισμοί του σχήματος ECCSI-SAKKE περιλαμβάνουν διαδικασίες επικύρωσης των ληφθέντων ιδιωτικών κλειδιών. Ωστόσο, αυτά τα επιπλέον βήματα θεωρούμε σκόπιμο να χρησιμοποιηθούν και στην υποδομή ARIBC ECCSI-SAKKE, επειδή η εγγενής διαδικασία επικύρωσης (βήματα 6α και 6β εδώ) δεν προστατεύει τους αναφέροντες από επιθέσεις τύπου κακόβουλου ενδιάμεσου (Man-In-The-Middle attack) κατά την αρχική διαδικασία εγγραφής.

4.3.4 Τεχνική παρουσίαση ΑΚΣ υποδομής ARIBC-X ECCSI

Για λόγους αυτάρκειας αυτής της διατριβής, σ' αυτήν την ενότητα παρουσιάζουμε περιληπτικά μια τεχνική περιγραφή των διαδικασιών υλοποίησης και λειτουργίας ΑΚΣ (KMS-X-ECCSI) μιας υποδομής ARIBC-X ECCSI στην οποία ανήκει μια οντότητα A.

Δημόσιες παράμετροι

Οι δημόσιες παράμετροι του μηχανισμού ECCSI (RFC6507) είναι οι: p, n, q, EC, G, $Hash_x, KPAK$. Λεπτομέρειες για τα δημόσια δεδομένα, και την ορολογία που χρησιμοποιούμε εδώ υπάρχουν στην ενότητα 2.3.2 και στον πίνακα 2.3.

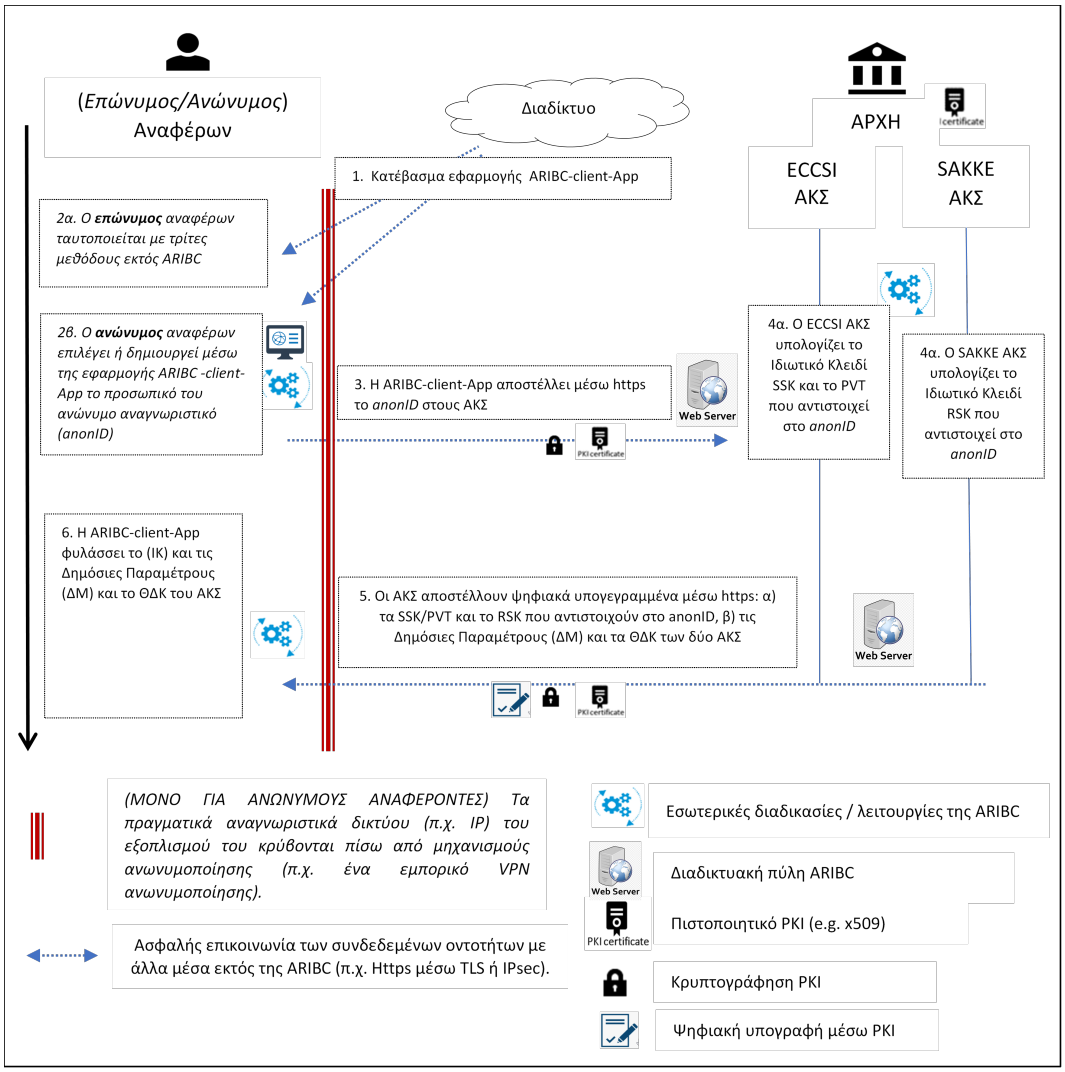
Δημιουργία των κλειδιών $KSAK/KPAK$ του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ/KMS-X-ECCSI)

Ο ΑΚΣ/KMS-X-ECCSI επιλέγει $KSAK$ και υπολογίζει το αντίστοιχο $KPAK$.

(1) Επιλογή του $KSAK_X$: επιλέγεται τυχαίος ακέραιος αριθμός $\in (2, q-1]$.

(2) Υπολογισμός του $KPAK_X$: Υπολογίζεται το $KPAK_X = [KSAK_X]G_X$, όπου $G_X(G_x, G_y) \in EC$ και είναι σημείο γεννήτορας της υποομάδας τάξης q σημείων της ελλειπτικής καμπύλης. Η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στον EC με ακέραιο αριθμό.

Οι διαδικασίες που παραθέτουμε βασίζονται στις οδηγίες και τους αλγορίθμους της ενότητας 4.2. "Community Parameters" του RFC6507.



Σχήμα 4.7: Διαδικασία εγγραφής των επώνυμων και ανώνυμων αναφερόντων σε υποδομή ARIBC ECCSI-SAKKE.

Η ροή διαδικασιών της δημιουργίας των κλειδιών $KSAK_X/KPAK_X$ του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ/KMS-X-ECCSI) φαίνεται στο αριστερό τμήμα του Σχήματος 4.5.

Δημιουργία των (ΙΚΥ)/ (SSK) και ΔΤΕ/PVT στην υποδομή ARIBC ECCSI

Θεωρούμε οντότητα (π.χ. αναφέρων) A, με δημόσιο αναγνωριστικό $ID_{Sender} = ID_A$, η οποία εγγράφηκε στην υποδομή ARIBC-X ECCSI-SAKKE και αναμένει την δημιουργία των κλειδιών ψηφιακής υπογραφής SSK_A/PVT_A.

Η διαδικασία κατασκευής των SSK_A/PVT_A περιλαμβάνει:

Τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) του (ΑΚΣ/KMS-X-ECCSI)

- την επιλογή του PVT_A του χρήστη
- την εξαγωγή του ιδιωτικού κλειδιού (SSK_A) του χρήστη, με τη χρήση του Δημόσιου Τεκμηρίου Επικύρωσης (ΔΤΕ)/Public Validation Token(PVT_A) και του ID_A του χρήστη
- την επαλήθευσή τους.

Δεδομένα Εισόδου

Είσοδοι στους αλγορίθμους είναι το *KSAK*, το δημόσιο αναγνωριστικό *ID* του χρήστη, και ο γεννήτορας (G).

Αλγόριθμος

(1) Επιλογή v, τυχαίου (εφήμερου), μη-μηδενικού στοιχείου του F_q

(2) Υπολογίζουμε το $PVT_A = [v]G_X$

(3) Υπολογίζουμε τη συνάρτηση κατακερματισμού: $HS_A = hash(G_X||KPAK_X||ID_A||PVT_A)$

(4) Τέλος, υπολογίζουμε το: $SSK_A = (KSAK_X + HS_A * v) \mod q$

(5) Εάν το SSK_A ή το HS_A είναι μηδέν modulo q, τότε το SSK_A είναι ΜΗ-ΕΓΚΥΡΟ και η διαδικασία εξαγωγής του πρέπει να επαναληφθεί.

Αποτέλεσμα

(6) Εξαγωγή του ζεύγους (SSK_A, PVT_A). Σημειώνουμε ότι το στοιχείο v πρέπει να διαγραφεί με το πέρας του αλγορίθμου.

(γ) Επικύρωση από τον χρήστη του SSK_A/PVT_A

Ο χρήστης πρέπει να επικυρώσει το ζεύγος SSK_A/PVT_A πριν τα χρησιμοποιήσει, ακολουθώντας τα παρακάτω βήματα.

(1) Ελέγχει ότι $PVT_A \in EC$

(2) Υπολογίζει το $HS = hash(G_X||KPAK_X||ID_A||PVT_A)$, το οποίο είναι στατικό, οπότε ο χρήστης μπορεί να το αποθηκεύσει ώστε να μη χρειάζεται να το υπολογίζει κάθε φορά.

(3) Εάν $KPAK_X = [SSK_A]G_X - [HS_A]PVT_A$, τότε ζεύγος SSK_A/PVT_A είναι έγκυρο.

Λεπτομέρειες παρέχονται στην ενότητα 2.3.2 της διατριβής και στις ενότητες 5.1.1 και 5.1.2 του RFC6507.

Ψηφιακή Υπογραφή στην υποδομή ARIBC ECCSI

Θεωρούμε οντότητα (π.χ. αναφέρων) A με δημόσιο αναγνωριστικό ID_A, η οποία εγγράφηκε στην υποδομή ARIBC-X ECCSI και διαθέτει κλειδιά ψηφιακής υπογραφής SSK_A/PVT_A.

Η διαδικασία Ψηφιακής Υπογραφής του μηνύματος (m) από την οντότητα A περιλαμβάνει:

Δεδομένα Εισόδου

1. Το μήνυμα (m) που θα υπογραφεί ψηφιακά
2. Το αναγνωριστικό (ID_A) του Υπογράφοντος
3. Το ιδιωτικό κλειδί (SSK_A) του Υπογράφοντος
4. Το (PVT_A) του Υπογράφοντος
5. Το Δημόσιο Κλειδί ($KPAK_X$) του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ/KMS του Υπογράφοντος

Αλγόριθμος

(1) Επιλογή τυχαίου (εφήμερου), μη-μηδενικού στοιχείου $j \in F_q$

(2) Υπολογισμός το $J = (Jx, Jy)$ τ.ω. $J = [j]G$. Στη συνέχεια θέτουμε $r = Jx$, δηλαδή το r ισούται με την τετμημένη Jx του J.

(3) Υπολογισμός $HS = hash(G_X||KPAK_X||ID_A||PVT_A)$. Εάν έχουμε αποθηκεύσει το HS, δεν χρειάζεται να το υπολογίσουμε ξανά.

(4) Υπολογισμός της συνάρτησης κατακερματισμού $HE = hash(HS_A||r||m)$.

(5) Έλεγχος: Εάν ισχύει η σχέση $(HE + r * SSK_A)\ modulo\ q \neq 0$, η ψηφιακή υπογραφή είναι έγκυρη, αλλιώς η διαδικασία πρέπει να επαναληφθεί με νέο $j \in F_q$.

(6) Υπολογισμός $s' = ((\frac{1}{HE+r*SSK_A}) * j)\ modulo\ q$. Μετά τον υπολογισμό η τιμή j πρέπει να διαγράφεται.

(7) Θέτουμε $s = s'$ ή, εάν s' είναι πολύ μεγάλο, τότε θέτουμε $s = q - s'$.

Αποτέλεσμα

Η ψηφιακή υπογραφή είναι η τριάδα (s, r, PVT_A)

Επαλήθευση Ψηφιακής Υπογραφής στην υποδομή ARIBC ECCSI

Δεδομένα Εισόδου

1. Η ψηφιακή υπογραφή (s, r, PVT_A)
2. Το υπογεγραμμένο μήνυμα (m)
3. Το δημόσιο αναγνωριστικό (ID_A) του Υπογράφοντος

4. Το Δημόσιο Κλειδί ($KPAK_X$) του Αξιόπιστου Κεντρικού Συντονιστή ΑΚΣ(KMS) του Υπογράφοντος

Αλγόριθμος

(1) Ελεγχος αν $PVT_A \in EC$

(2) Υπολογισμός του $HS = hash(G_X||KPAK_X||ID_A||PVT_A)$

(3) Υπολογισμός $HE = hash(HS_A||r||m)$

(4) Υπολογισμός $Y = [HS]PVT_A + KPAK_X$

(5) Υπολογισμός $J = [s]([HE]G_X + [r]Y)$

Αποτέλεσμα

(6) Η Ψηφιακή Υπογραφή είναι ΕΓΚΥΡΗ μόνο αν $Jx = r \ modulo \ q$ και $Jx \ modulo \ q \neq 0$. Σε αντίθετη περίπτωση η υπογραφή θεωρείται ΑΚΥΡΗ.

Λεπτομέρειες παρέχονται στην ενότητα 2.3.2 της διατριβής και στις ενότητες 5.2.1 και 5.2.2 του RFC6507.

4.3.5 Τεχνική παρουσίαση του ΑΚΣ υποδομής ARIBC-Y SAKKE

Δημόσιες παράμετροι του μηχανισμού ARIBC-SAKKE

Οι δημόσιες παράμετροι του μηχανισμού ARIBC-SAKKE είναι οι: $p, n, q, EC, G_Y, g =< G, G >, Hash$.

Δημιουργία των κλειδιών z_Y/Z_Y του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ/KMS-Y-SAKKE)

1. Επιλογή του z_Y: επιλέγεται τυχαίος ακέραιος αριθμός $z_Y \in (2, q-1]$.
2. Υπολογισμός του Z_Y: Υπολογίζεται το $Z_Y = [z_Y]G$, όπου $G_Y(G_x, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης q. Η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στον EC με ακέραιο αριθμό.

Η ίδια διαδικασία ακολουθείται από το KMS_Y για να δημιουργήσει το Θεμελιώδες Μυστικό Κλειδί (z_Y) και το Θεμελιώδες Δημόσιο κλειδί (Z_Y) αντίστοιχα. Περισσότερες λεπτομέρειες παρέχονται στην ενότητα 2.3.3 της διατριβής και στην ενότητα 6.1 του RFC6508.

Εξαγωγή Ιδιωτικού Κλειδιού Receiver Secret Key Extraction (RSK)

Στο πλαίσιο αυτού του παραδείγματος, στο οποίο ο Παραλήπτης είναι η οντότητα B που ανήκει στην υποδομή KMS_Y με $ID_{Receiver} = B$, υπολογίζουμε το ιδιωτικό κλειδί του $RSK_{(B,Y)}$.

Δεδομένα Εισόδου

(1) Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = B$
(2) Θεμελιώδες Μυστικό Κλειδί ΑΚΣ--SAKKE: z_S

Αλγόριθμος

(1) Υπολογισμός του: $RSK_{(B,Y)} = \frac{G_Y}{B+z_Y}$

Αποτέλεσμα

(2) Το Ιδιωτικό Κλειδί γίνεται αποδεκτό μόνο εάν ισχύει η ισότητα: $< [B]G_Y + Z_Y, RSK_{(B,Y)} >= g$, ειδάλλως απορρίπτεται.

Περισσότερες λεπτομέρειες παρέχονται στην ενότητα 2.3.3 της διατριβής και στην ενότητα 6.1.2 του RFC6508.

Αποστολή Ενθυλακωμένου Μηνύματος

Σ' αυτό το παράδειγμα, ο Αποστολέας ($ID_{Sender} = A$) σχηματίζει την Κοινή Μυστική Τιμή (SSV) και την αποστέλλει ενθυλακωμένη στον Παραλήπτη ($ID_{Receiver} = B$).

Η διαδικασία της ενθυλάκωσης δεν προϋποθέτει να έχει ήδη κάποιου είδους κλειδί ο Παραλήπτης B, συνεπώς μπορεί να προηγείται της διαδικασίας απόδοσης ιδιωτικού κλειδιού που περιγράφηκε προηγουμένως. Ισχύει όμως η προϋπόθεση ότι ο Παραλήπτης θα ζητήσει ιδιωτικό κλειδί που θα αντιστοιχεί στο δημόσιο αναγνωριστικό $ID_{Receiver} = B$ που έχει χρησιμοποιήσει ο αποστολέας.

Δεδομένα Εισόδου

(1) Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = B$
(2) Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ-Υ-SAKKE: Z_Y

Αλγόριθμος

(1) Επιλογή ως SSV τυχαίου (εφήμερου) ακέραιου, μη-μηδενικού στοιχείου, $SSV \in (0, 2^n - 1]$

(2) Υπολογισμός του: $r = HashToIntegerRange(SSV||B, q, Hash)$

(3) Υπολογισμός του: $R_{(B,Y)} = [r]([B]G_Y + Z_Y) \in E(F_p)$ Hint, (H)

(4α) Υπολογισμός του g^r[2].

(4β) Υπολογισμός του $H := SSV \oplus HashToIntegerRange(g^r, 2^n, Hash)$

Αποτέλεσμα

(5) Τα ενθυλακωμένα δεδομένα προς αποστολή στον Β' είναι τα: $(R_{(B,Y)}, H)$
(6) Εξαγωγή του SSV.

Περισσότερες λεπτομέρειες παρέχονται στην ενότητα 2.3.3 της διατριβής και στην ενότητα 6.2.1 του RFC6508.

Παραλαβή και Αποθυλάκωση Μηνύματος

Σ' αυτό το παράδειγμα, ο Παραλήπτης ($ID_{Receiver} = B$) παραλαμβάνει τα ενθυλακωμένα δεδομένα $(R_{(B,S)}, H)$, τα αποθυλακώνει και εξάγει το μυστικό υλικό για τη δημιουργία του συμμετρικού κλειδιού συνόδου SSV.

Δεδομένα Εισόδου

[2]Περισσότερες πληροφορίες υπάρχουν στην ενότητα 2.1 του RFC6508

(1) Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = B$
(2) Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ-S-SAKKE: Z_Y

Αλγόριθμος

(1) Εξάγει τα $R_{(B,Y)}$ και H από τα ενθυλακωμένα δεδομένα $(R_{(B,Y)}, H)$
(2) Υπολογίζει το $w :=< R_{(B,Y)}, RSK_{(B,Y)} >$
(3) Υπολογίζει το $SSV = H \oplus HashToIntegerRange(w, 2^n, Hash)$
(4) Υπολογίζει το $r = HashToIntegerRange(SSV||B, q, Hash)$
(5) Υπολογίζει το $TEST = [r]([B]G_Y + Z_Y) \in E(F_p)$

Αποτέλεσμα
(6) Τα ενθυλακωμένα δεδομένα γίνονται αποδεκτά μόνο εάν ισχύει η ισότητα $TEST = R_{(B,Y)}$, ειδάλλως τα ενθυλακωμένα δεδομένα απορρίπτονται.
(6) Εξαγωγή του SSV.

Περισσότερες λεπτομέρειες παρέχονται στην ενότητα 2.3.3 της διατριβής και στην ενότητα 6.2.2 του RFC6508.

Κεφάλαιο 5

Πειραματική υλοποίηση της ARIBC ECCSI-SAKKE

5.1 Εισαγωγή

Σ' αυτό το κεφάλαιο παρουσιάζουμε μια πειραματική υλοποίηση μέρους της υποδομής ARIBC BLMQ-SKIBE και συγκεκριμένα του τμήματος των υπηρεσιών πιστοποίησης και ακεραιότητας δεδομένων. Ο κύριος στόχος της πειραματικής υλοποίησης είναι η επίδειξη της καταλληλότητας του προτεινόμενου σχήματος ARIBC-ECCSI, που αφορά την πιστοποίηση της αυθεντικότητας και της ακεραιότητας των δεδομένων τόσο για επώνυμους όσο και για ανώνυμους αναφέροντες. Για την πειραματική υλοποίηση χρησιμοποιούμε δικό μας κώδικα και δημόσιες κρυπτογραφικές βιβλιοθήκες. Οι περισσότερες κρυπτογραφικές βιβλιοθήκες αυτού του κώδικα παρέχονται από τον οργανισμό "Legion of the Bouncy Castle"[1]

Η πειραματική υλοποίηση περιλαμβάνει την ψευδωνυμοποίηση του δημόσιου αναγνωριστικού ενός αναφέροντος και των σχετικά νέων τεχνολογιών όπως αυτή των ψηφιακών υπογραφών μέσω του μηχανισμού ECCSI. Συγκεκριμένα, περιλαμβάνει:

- Υλοποίηση Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ) με την ονομασία "agou-ska-KMS", που θα μπορούσε να αποτελεί μέρος μιας υποδομής ARIBC-ECCSI. Περιλαμβάνεται κώδικας σε Java για τη δημιουργία των αντίστοιχων Θεμελιωδών Μυστικών και Δημόσιων κλειδιών (*KSAK*/*KPAK*).
- Τυποποίηση κανόνων αποδεκτών αναγνωριστικών (*userID*) χρηστών της υποδομής ARIBC-ECCSI και μια μέθοδο για τη δημιουργία τους από τα δημόσια αναγνωριστικά (π.χ. ονόματα) των χρηστών.
- Μέθοδο χρονικά ελεγχόμενης ψευδωνυμοποίησης, από ανώνυμους αναφέροντες.
- Κώδικα σε Java που δημιουργεί το Ιδιωτικό Κλειδί ψηφιακής Υπογραφής (ΙΚΥ) (*SSK*) και το Δημόσιο Τεκμήριο Επικύρωσης (ΔΤΕ) (*PVT*) χρήστη.
- Κώδικα σε Java για την ψηφιακή υπογραφή μηνυμάτων.
- Κώδικα σε Java για την πιστοποίηση ενός ψηφιακά υπογεγραμμένου μηνύματος.

[1] `https://www.bouncycastle.org/java.html` με άδεια τύπου MIT.

Περιγραφή βάση RFC6507	Σύμβολο	**Τιμή**
Παράμετρος ασφαλείας, μέγεθος (σε bits) του p ($p > 2^N$), πάνω στην οποία πρόκειται να πραγματοποιηθεί κρυπτογραφία ελλειπτικής καμπύλης.	N	256 [2]
Η τάξη του πεπερασμένου σώματος $\mathbb{F}_p$	p	FFFFFFFF00000001000000000000000000000000 FFFFFFFFFFFFFFFFFFFFFFFF
Ελλειπτική καμπύλη που ορίζεται πάνω στο $\mathbb{F}_p$ με υποομάδα τάξης q	E	Ελλειπτική καμπύλη NIST P-256 και συγκεκριμένα η p256r1
Στοιχείο του F_p, όπου το E ορίζεται από τον τύπο $y^2 = x^3 - 3x + B$ modulo p.	B	5AC635D8AA3A93E7B3EBBD55769886BC651D06B 0CC53B0F63BCE3C3E27D2604B
Σημείο $G(G_x, G_y) \in E$ και γεννήτορας της υποομάδας τάξης q	G	Με συντεταγμένες: Gx=6B17D1F2E12C4247F8BCE 6E563 A440F277037D812DEB33A0F4A13945D898C296 Gy=4FE342E2FE1A7F9B8EE7EB4A7C0F9E162 BCE33576B315ECECBB6406837BF51F5
Η τάξη του G στην ελλειπτική καμπύλη E πάνω στο $\mathbb{F}_p$	q	FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7 17984F3B9CAC2FC632551
Κρυπτογραφική συνάρτηση κατακερματισμού	Hash	SHA-256, της οικογένειας Secure Hash Algorithm

Πίνακας 5.1: Οι δημόσιες παράμετροι (*PP*) της πειραματικής υλοποίησης σε σχέση μ' εκείνες του RFC6507.

Η πειραματική υλοποίηση δεν περιλαμβάνει τα μέρη της ARIBC-ECCSI που αποτελούνται από εδραιωμένες τεχνολογίες, όπως ο ιστότοπος (portal) του ΑΚΣ, η δημιουργία του εικονικού ασφαλούς δικτύου VPN για την αποστολή του ιδιωτικού κλειδιού στον αναφέροντα, ή τα συστήματα διαδικτυακής ανωνυμοποίησης του αναφέροντα.

5.2 Το πλαίσιο της πειραματικής υλοποίησης

Η άμεση συσχέτιση της υλοποίησης με το RFC6507 επιτρέπει την εύκολη επικύρωση της ορθότητας του κώδικα, διά της απλής αντικατάστασης των τιμών των διάφορων μεταβλητών μ' αυτές του Παραρτήματος Α ("Δεδομένα δοκιμής") του RFC6507 και της σύγκρισης των αποτελεσμάτων.

Στους πίνακες 5.2 και 5.2 παρουσιάζουμε περιληπτικά τη σχέση μεταξύ των κρυπτογραφικών τιμών που χρησιμοποιούνται στην πειραματική μας υλοποίηση και εκείνων στο Παράρτημα Α του RFC6507. Σημειώνουμε ότι το RFC6507 συνιστά τα p, E και G να επιλέγονται από τις τυποποιημένες τιμές που δίνονται στο [FIPS 186-3].

5.3 Η εγκατάσταση του ΑΚΣ ARIBC-ECCSI/(KMS)

Η πειραματική υλοποίηση δημιουργεί τον Αξιόπιστο Κεντρικό Συντονιστή (ΑΚΣ)/KMS), τον οποίο ονομάσαμε "agou-ska-KMS" [3] και το αντίστοιχο ζεύγος θεμελιωδών κλειδιών.

[3]Το όνομα επιλέχθηκε σκόπιμα ώστε να περιέχει τα αρχικά a.goudosis και s.katsikas ως αποδεικτικό στοιχείο χρήσης πρωτότυπης υλοποίησης και όχι τυχαίων στιγμιότυπων οθόνης.

Περιγραφή	Σύμβολο	**Τιμή**
Θεμελιώδες Μυστικό κλειδί (ΘΜΚ) και Θεμελιώδες Δημόσιο κλειδί (ΘΜΚ)	*KSAK*/*KPAK*	Η πειραματική υλοποίηση έχει τη δυνατότητα δημιουργίας των κλειδιών *KSAK*/*KPAK*
Τυποποίηση κανόνων αποδεκτών αναγνωριστικών χρηστών	*userID*	Η πειραματική υλοποίηση προσφέρει ψευδωνυμοποίηση
Ιδιωτικό Κλειδί ψηφιακής Υπογραφής (ΙΚΥ)/Δημόσιο Τεκμήριο Επικύρωσης (ΔΤΕ)	SSK_{UserID} / PVT_{UserID}	Η πειραματική υλοποίηση έχει τη δυνατότητα δημιουργίας των κλειδιών SSK_{UserID} / PVT_{UserID}

Πίνακας 5.2: Παράμετροι της πειραματικής υλοποίησης που διαφέρουν από εκείνες του RFC6507

```
 4 KMSname
 5 agou-ska-KMS
 6 KSAK
 7 34A9928EF1A182DC061ECD85F096EFB950329234FB84E8DDC7268B3519F31CC9
 8 KPAKx
 9 60D04A81DA257A1942A60A93BAA8529CBABB26FFEF4F267846419AEF1DD24E90
10 KPAKy
11 1800230CD248BF4CAE9B32C45C144EB17344FD9A6DA728B3DC81E303E81A1A5D
```

Σχήμα 5.1: Στιγμιότυπο οθόνης από τη διαδικασία εγκατάστασης του ΑΚΣ της πειραματικής υλοποίησης.

Υλοποιείται η διαδικασία δύο σταδίων που περιγράφεται στην ενότητα 4.3.4 της διατριβής. Συγκεκριμένα:

1. Ο κώδικας δημιουργεί έναν ψευδοτυχαίο μη-μηδενικό ακέραιο αριθμό, μεγέθους 256bits, ο οποίος θεωρείται πλέον το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/*KSAK*) του "agou-ska-KMS". Στην υλοποίησή μας το *KSAK* δημιουργήθηκε από γεννήτρια ψευδοτυχαίων αριθμών μέσω αντίστοιχης κρυπτογραφικής κλάσης της Java.
2. Στη συνέχεια, χρησιμοποιώντας πολλαπλασιασμό ελλειπτικής καμπύλης, υπολογίζεται το Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ/*KPAK*), το οποίο είναι το γινόμενο του *KSAK* επί το σημείο γεννήτορας (*G*), (δηλαδή *KPAK* = [*KSAK*]*xG*). Τα υπολογισμένα $KPAK_X$ και $KPAK_Y$ είναι οι συντεταγμένες του *KPAK* πάνω στην ελλειπτική καμπύλη *E*.

Στο Σχήμα 5.1 φαίνεται ένα στιγμιότυπο της οθόνης εξόδου του κώδικα της πειραματικής υλοποίησης από την αρχική εγκατάσταση της υπηρεσίας του Αξιόπιστου Κεντρικού Συντονιστή (ΑΚΣ)/KMS) που ονομάσαμε "agou-ska-KMS", και το αντίστοιχο ζεύγος θεμελιωδών κλειδιών που δημιουργήθηκε. Το *KSAK*, ένας ακέραιος αριθμός, το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/*KSAK*) και το σημείο πάνω στη ελλειπτική καμπύλη $KPAK = (KPAK_X, KPAK_Y)$ είναι το Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ). Το *KSAK* αποκαλύπτεται εδώ μόνο επειδή το "agou-ska-KMS" είναι μια υλοποίηση επίδειξης δυνατοτήτων. Σε μια παραγωγική υλοποίηση η μυστικότητα του Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ/*KSAK*) πρέπει να είναι απόλυτη.

5.4 Τυποποίηση των κανόνων αποδεκτών δημόσιων αναγνωριστικών

Η υποδομή ARIBC δεν θέτει τεχνικούς περιορισμούς στη μορφή των δημόσιων αναγνωριστικών. Ωστόσο, η τυποποίησή τους σύμφωνα με το περιβάλλον υλοποίησης θεωρείται καλή πρακτική. Στην πειραματική υλοποίηση επιλέξαμε να χρησιμοποιήσουμε ως βάση τη μορφή των διευθύνσεων του ηλεκτρονικού ταχυδρομείου, και συγκεκριμένα μια τυποποίηση της μορφής αναγνωριστικό.έτος@υποτομέας.τομέας (π.χ. "a.goudosis2020@orgX.gr"). Προσεγγίσεις παρόμοιου τύπου θεωρούμε ότι σε ορισμένους οργανισμούς μπορεί να έχουν κάποια από τα παρακάτω πλεονεκτήματα:

- Σαφής διαχωρισμός αναγνωριστικού χρήστη και υλοποίησης.
- Δυνατότητα κατηγοριοποίησης των χρηστών σε τομείς και υποτομείς. (π.χ. εσωτερικοί-εξωτερικοί χρήστες, προσωπικά αναγνωριστικά, διατμηματικά αναγνωριστικά).
- Η ίδια μεθοδολογία δημιουργίας δημόσιου αναγνωριστικού μπορεί να χρησιμοποιηθεί για ανώνυμους αλλά και για τυπικούς χρήστες.
- Η εξοικείωση των χρηστών με μια μορφή τύπου διεύθυνσης ηλεκτρονικού ταχυδρομείου ενδέχεται να αυξήσει το επίπεδο αποδοχής της υποδομής ARIBC από τους χρήστες.
- Η επιλογή αυτή προσαρμόζεται σχετικά εύκολα στις ανάγκες μας. Για παράδειγμα, έχουμε τη δυνατότητα να προσθέσουμε ημερομηνία λήξης (π.χ. sokratis.katsikas2020@orgX.gr) ή να αλλάξουμε ελαφρώς το αναγνωριστικό, εάν χαθεί ή παραβιαστεί το ιδιωτικό κλειδί (π.χ. sokratis.katsikas2020-new@orgX.gr).

Ωστόσο, η ακριβής διαδικασία δημιουργίας του αναγνωριστικού για έναν επώνυμο χρήστη διαφέρει από εκείνη ενός ανώνυμου χρήστη.

Επώνυμος χρήστης: Στο επόμενο παράδειγμα, ακολουθώντας τις διαδικασίες που έχουμε περιγράψει, χρησιμοποιούμε το όνομα του καθηγητή Σωκράτη Κάτσικα ως αντιπροσωπευτικό επώνυμο χρήστη ο οποίος προτίθεται να γίνει μέλος της υποδομής AIRBC-orgX του οργανισμού orgX. Στο Σχήμα 5.2 βλέπουμε στιγμιότυπο οθόνης από την πειραματική υλοποίηση του ΑΚΣ/KMS και συγκεκριμένα τη δημιουργία των ιδιωτικών κλειδιών. Στο πλαίσιο Α παρατηρούμε ότι έχει δημιουργηθεί το δημόσιο αναγνωριστικό βάσει του οποίου θα υπολογιστούν τα αντίστοιχα ιδιωτικά κλειδιά. Σημειώνουμε ότι σε μια πραγματική υλοποίηση το πλαίσιο Α θα αποτελεί μέρος της προτεινόμενης εφαρμογής στην πλευρά του χρήστη (ARIBC-client-app) αλλά στην πειραματική υλοποίηση οι δύο εφαρμογές συνυπάρχουν, για λόγους απλότητας.

Ανώνυμος χρήστης Ένας ανώνυμος αναφέρων έχει τη δυνατότητα να επιλέξει ή να δημιουργήσει το ανώνυμο αναγνωριστικό του. Επίσης, όπως έχει αναφερθεί, δίνεται η δυνατότητα στους ανώνυμους αναφέροντες, μόνο εφόσον το επιθυμούν, να διατηρήσουν τη δυνατότητα να αποδείξουν την πραγματική τους ταυτότητα στο μέλλον, όποτε και εάν οι ίδιοι το θελήσουν. Στην πειραματική υλοποίηση επιλέξαμε να υλοποιήσουμε την

τελευταία περίπτωση, ως την περισσότερο σύνθετη από τις προτεινόμενες σ' αυτήν τη διατριβή.

Η διαδικασία που ακολουθούμε είναι η ακόλουθη: Ο ανώνυμος χρήστης σχηματίζει ένα αλφαριθμητικό συνδυάζοντας το πραγματικό του όνομα με ένα μυστικό κλειδί της επιλογής του. Στη συνέχεια, το παραγόμενο αλφαριθμητικό χρησιμοποιείται ως είσοδος σ' έναν αλγόριθμο κατακερματισμού SHA-1.

Το αποτέλεσμα του κατακερματισμού με τον SHA-1 θα είναι το ψευδώνυμο αναγνωριστικό του χρήστη. Οποιαδήποτε εφαρμογή αλγόριθμων κατακερματισμού μπορεί να χρησιμοποιηθεί από τον χρήστη για την παραπάνω διαδικασία. Όμως, μόνο προς διευκόλυνση του χρήστη, ο σχεδιασμός μας τη συμπεριλαμβάνει στην εφαρμογή στην πλευρά του χρήστη ARIBC-client-app. Στην παρούσα υλοποίηση ωστόσο, για απλότητα, ενσωματώνουμε την εφαρμογή κατακερματισμού στο κύριο πρόγραμμά μας.

Στο επόμενο παράδειγμα, ακολουθώντας τις διαδικασίες που έχουμε περιγράψει, υποθέτουμε ότι ο χρήστης "a.goudosis" που επιθυμεί να παραμείνει ανώνυμος συνενώνει την πραγματική ταυτότητά του ("a.goudosis") με ένα μυστικό κλειδί που επέλεξε ("MyKey123456") για να σχηματίσει το αλφαριθμητικό ("a.goudosis myKey123456") ως είσοδο στον αλγόριθμο κατακερματισμού SHA-1 (πλαίσιο Α στο στιγμιότυπο οθόνης του Σχήματος 5.4). Το αποτέλεσμα του κατακερματισμού ("F96D1...") με τον SHA-1 είναι το ψευδώνυμο αναγνωριστικό του χρήστη "a.goudosis" (πλαίσιο Β στο στιγμιότυπο οθόνης του Σχήματος 5.4). Τέλος, όπως στην περίπτωση του ΑΚΣ/KMS, και συγκεκριμένα της δημιουργίας των ιδιωτικών κλειδιών των ανώνυμων χρηστών, το ψευδώνυμο αναγνωριστικό συνενώνεται με το επίθεμα του οργανισμού ("@orgX.gr"), προκειμένου να παραχθεί το ψευδώνυμο αναγνωριστικό του χρήστη ("F96D1...@orgX.gr") (πλαίσιο Β στο στιγμιότυπο οθόνης του Σχήματος 5.4).

5.4.1 Δημιουργία των (ΙΚΥ)/ (SSK) και ΔΤΕ/PVT Επώνυμου χρήστη

Συνεχίζοντας την προσομοίωση του επώνυμου χρήστη με το δημόσιο αναγνωριστικό "sokratis.katsikas_2020@orgX.gr" (πλαίσιο Α στο στιγμιότυπο οθόνης του σχήματος 5.2), παραθέτουμε τα επόμενα βήματα του "agou-ska-KMS" για τη δημιουργία των (ΙΚΥ)/(SSK) και ΔΤΕ/PVT του χρήστη με $ID_{sokratis.katsikas2020@orgX.gr}$.

Προς τούτο τεχνικά υλοποιείται η μεθοδολογία που παρουσιάστηκε στην ενότητα 4.3.4 της διατριβής:

1.
   - Επιλογή του ΔΤΕ/$PVT_{sokratis.katsikas2020@orgX.gr}$ (πλαίσιο Ε στο στιγμιότυπο οθόνης 5.2, όπου φαίνονται οι συντεταγμένες (PVT_X, PVT_Y) που προσδιορίζουν το σημείο *PVT*)
   - Υπολογισμός του ιδιωτικού κλειδιού (ΙΚΥ/$SSK_{sokratis.katsikas2020@orgX.gr}$) (πλαίσιο F στο στιγμιότυπο οθόνης 5.2)
   - Επαλήθευσή τους.
2. Ο "agou-ska-KMS" στέλνει με ασφάλεια, με άλλα μέσα εκτός της υποδομής ARIBC (π.χ. HTTPS/IPSec)), στον επώνυμο χρήστη τα ακόλουθα δεδομένα:

(Στιγμιότυπο οθόνης του Σχήματος 5.3) :

(α΄) Τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) του ΑΚΣ ("agou-ska-KMS"). Στην πειραματική υλοποίηση θεωρούμε σταθερά όλα τα ΔΠ πλήν του Θεμελιώδους Δημόσιου Κλειδιού *KPAK* του ΑΚΣ της υλοποίησης.

(β΄) Το επίσημο δημόσιο αναγνωριστικό του χρήστη, προς αποφυγή παρερμηνειών.

(γ΄) Το Ιδιωτικό κλειδί υπογραφής (ΙΚΥ/*SSK*) του χρήστη.

(δ΄) Τις συντεταγμένες (PVT_X , PVT_Y), που προσδιορίζουν το ΔΤΕ/*PVT* του χρήστη.

(ε΄) Το *HS*, το οποίο είναι μια στατική τιμή δεμένη με κάθε αναγνωριστικό που χρησιμοποιείται τόσο στις διαδικασίες δημιουργίας ψηφιακής υπογραφής όσο και σ΄ εκείνες της επικύρωσης της υπογραφής. Ο καθένας μπορεί να το υπολογίσει εκ νέου, αλλά προτείνεται η αποστολή και αποθήκευσή του για μελλοντική χρήση, προκειμένου να αποφεύγεται ο επανυπολογισμός του.

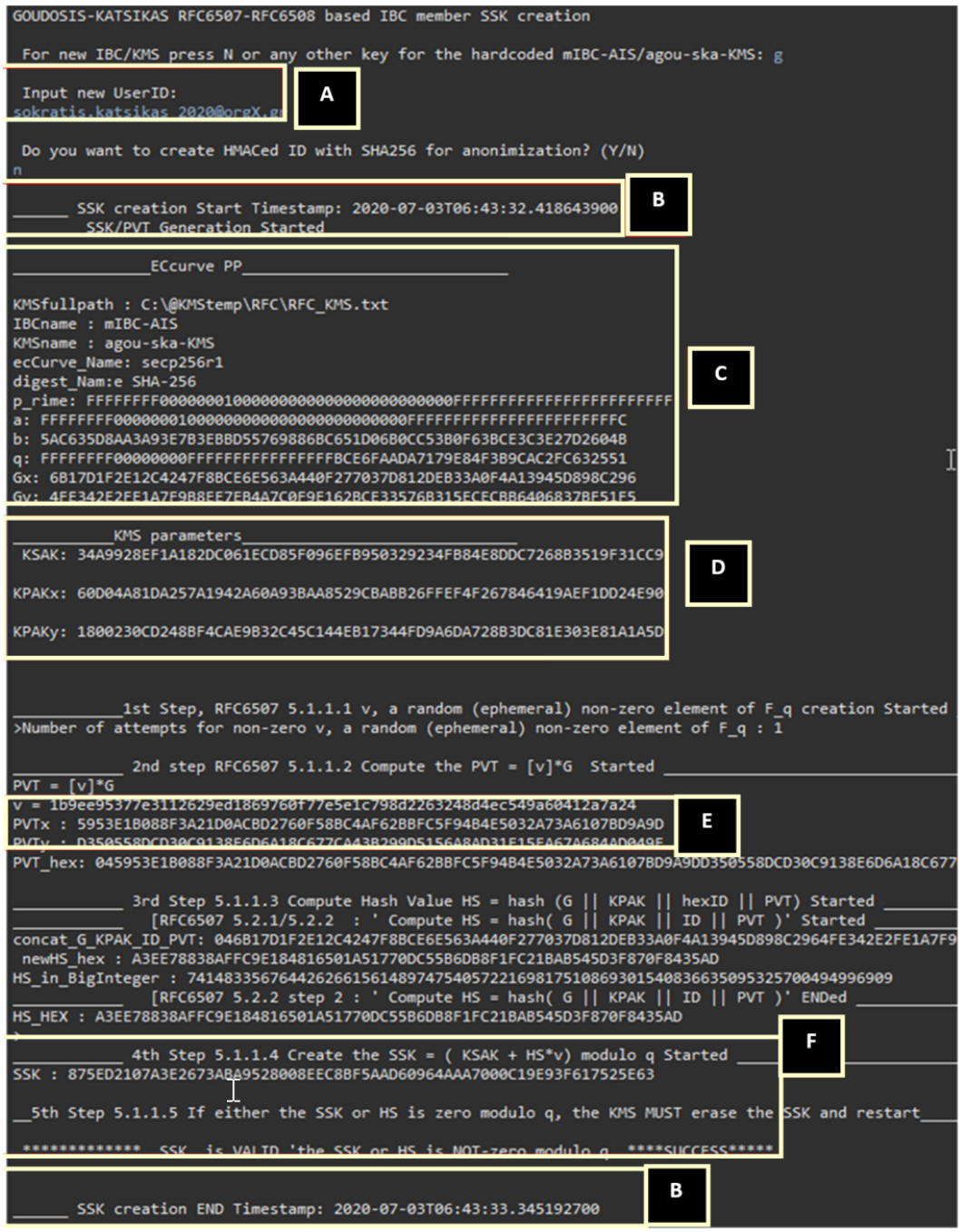
Στο στιγμιότυπο οθόνης του Σχήματος 5.2 φαίνεται, στο πλαίσιο A, το δημόσιο αναγνωριστικό του χρήστη, στα πλαίσια με ένδειξη B φαίνεται η ώρα έναρξης και λήξης της διαδικασίας, στο πλαίσιο C οι βασικές δημόσιες παράμετροι, στο πλαίσιο D το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/*KSAK*) και οι συντεταγμένες του Θεμελιώδους Δημόσιου Κλειδιού (ΘΔΚ/*KPAK*) του "agou-ska-KMS". Σημειώνουμε ότι σε ένα παραγωγικό περιβάλλον, τα ΙΚΥ/*SSK* του χρήστη και το ΘΜΚ/*KSAK* του "agou-ska-KMS" δεν θα εμφανίζονταν ποτέ.

5.5 Δημιουργία των (ΙΚΥ)/ (SSK) και ΔΤΕ/PVT Ανώνυμου χρήστη

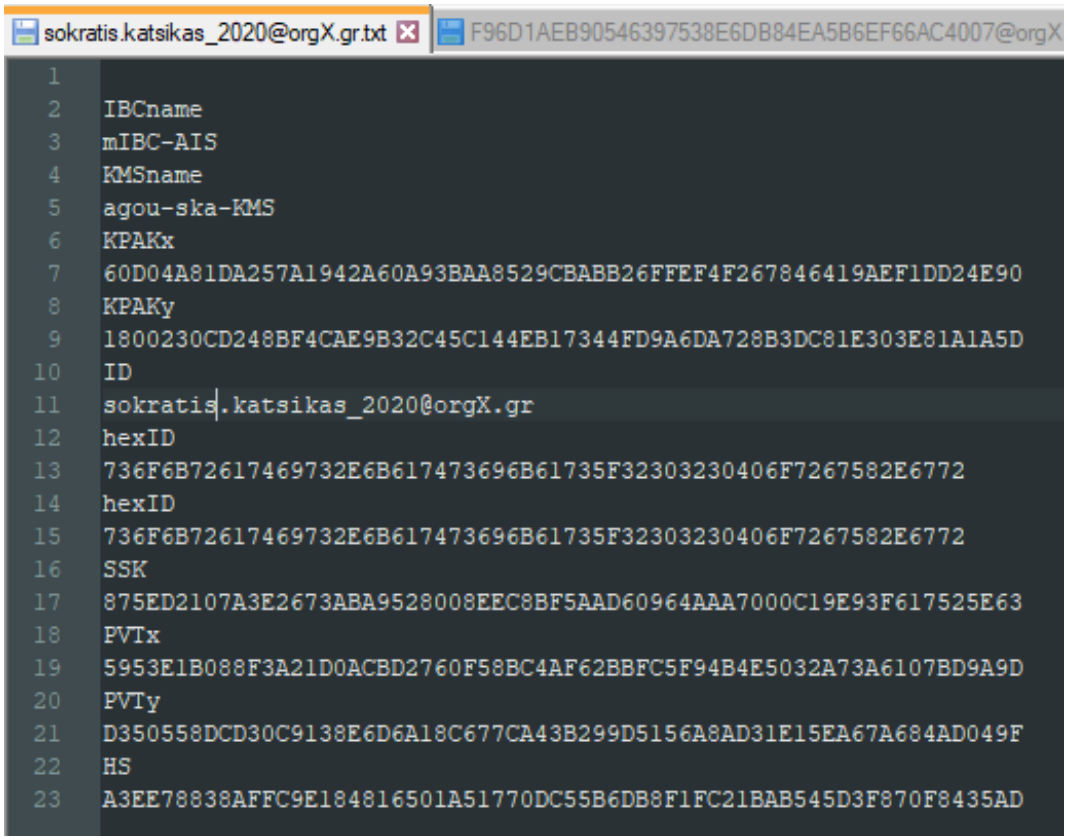
Συνεχίζοντας την προσομοίωση του ανώνυμου χρήστη a.goudosis, της ενότητας 5.4, με το δημόσιο αναγνωριστικό (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.), παραθέτουμε τα επόμενα βήματα του "agou-ska-KMS" για τη δημιουργία των (ΙΚΥ)/(SSK) και ΔΤΕ/PVT του χρήστη a.goudosis με το ψευδώνυμο ως δημόσιο αναγνωριστικό του.

Προς τούτο τεχνικά υλοποιείται η μεθοδολογία που παρουσιάστηκε στην ενότητα 4.3.4 της διατριβής.

1. Ο χρήστης συνενώνει την πραγματική ταυτότητά του ("a.goudosis") με το μυστικό κλειδί ("MyKey123456") και σχηματίζει το αλφαριθμητικό ("a.goudosis myKey123456") που θα χρησιμοποιηθεί ως είσοδος στον αλγόριθμο κατακερματισμού SHA-1, (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.Α). Το αποτέλεσμα του κατακερματισμού ("F96D1. . . ") με τον SHA-1 είναι το ψευδώνυμο αναγνωριστικό του χρήστη "a.goudosis", (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.Β). Η εργασία αυτή, σε παραγωγική υλοποίηση, γίνεται στην πλευρά του χρήστη.
2. Το ψευδώνυμο αναγνωριστικό συνενώνεται με το επίθεμα του οργανισμού ("@orgX.gr") προκειμένου να παραχθεί το ψευδώνυμο αναγνωριστικό του χρήστη ("F96D1. . . @orgX.gr") (πλαίσιο Β στο στιγμιότυπο οθόνης του Σχήματος 5.4).



Σχήμα 5.2: Στιγμιότυπο οθόνης από τη δημιουργία του Ιδιωτικού Κλειδιού Υπογραφής (SSK) και του Δημόσιου Τεκμηρίου Επικύρωσης (PVT) του επώνυμου χρήστη.



Σχήμα 5.3: Στιγμιότυπο οθόνης του αρχείου που στέλνει ο ΑΚΣ στον επώνυμο χρήστη.

3.
   - Υπολογισμός του ΔΤΕ/$PVT_{a.goudosis}$ με συντεταγμένες (PVT_X, PVT_Y), (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.F) .
   - Υπολογισμός του ιδιωτικού κλειδιού (ΙΚΥ/$SSK_{a.goudosis}$), (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.F)
   - Επαλήθευσή τους (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.4.F).
4. Ο "agou-ska-KMS" στέλνει με ασφάλεια με άλλα μέσα, εκτός της υποδομής ARIBC (π.χ.HTTPS/IPSec), στον ανώνυμο χρήστη τα ακόλουθα δεδομένα (Στιγμιότυπο οθόνης του Σχήματος 5.5):

   (α΄) Τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) του ΑΚΣ ("agou-ska-KMS"). Στην πειραματική υλοποίηση θεωρούμε σταθερά όλα τα ΔΠ πλην του Θεμελιώδους Δημόσιου Κλειδιού του ΑΚΣ "agou-ska-KMS".

   (β΄) Το επίσημο δημόσιο αναγνωριστικό του χρήστη, προς αποφυγή παρερμηνειών.

   (γ΄) Το Ιδιωτικό Κλειδί υπογραφής (ΙΚΥ/*SSK*) του χρήστη.

   (δ΄) Τις συντεταγμένες (PVT_X, PVT_Y) που προσδιορίζουν το ΔΤΕ/*PVT* του χρήστη.

   (ε΄) Το *HS*, το οποίο είναι μια στατική τιμή, δεμένη με κάθε αναγνωριστικό και που χρησιμοποιείται τόσο στις διαδικασίες δημιουργίας ψηφιακής υπογραφής όσο και σ' εκείνες της επικύρωσης της υπογραφής. Ο καθένας μπορεί να το υπολογίσει εκ νέου, αλλά προτείνεται η αποστολή και

αποθήκευσή του για μελλοντική χρήση, προκειμένου να αποφεύγεται ο επανυπολογισμός του.

Στο στιγμιότυπο οθόνης του Σχήματος 5.4 φαίνεται, στο πλαίσιο B, το δημόσιο αναγνωριστικό του χρήστη, στα πλαίσια με ένδειξη C η ώρα έναρξης και λήξης της διαδικασίας, στο πλαίσιο D οι βασικές δημόσιες παράμετροι, στο πλαίσιο E το Θεμελιώδες Ιδιωτικό Κλειδί (ΘΙΚ/*KSAK*) και οι συντεταγμένες του Θεμελιώδους Δημόσιου Κλειδιού (ΘΔΚ/*KPAK*) του "agou-ska-KMS". Τέλος, στα πλαίσια Fa, Fb φαίνονται το Ιδωτικό κλειδί υπογραφής (ΙΚΥ/*SSK*) και οι συντεταγμένες (PVT_X, PVT_Y) που προσδιορίζουν το ΔΤΕ/*PVT* του χρήστη. Σημειώνουμε ότι σε ένα παραγωγικό περιβάλλον τα ΙΚΥ/*SSK* του χρήστη και το ΘΜΚ/*KSAK* του "agou-ska-KMS" δεν θα εμφανίζονταν ποτέ.

5.6 Το λειτουργικό κόστος δημιουργίας των (ΙΚΥ)/ (SSK) και ΔΤΕ/PVT

Σε Η/Υ με Intel Core ™ i7-5600U CPU @ 2.60Hz, RAM: 16GB, OS: 64-bit Windows 10 Pro, οι πόροι και ο χρόνος που απαιτούνται για την εκτέλεση των διαδικασιών των (ΙΚΥ)/ (SSK) και ΔΤΕ/PVT των χρηστών είναι αμελητέοι. Για παράδειγμα, η δημιουργία ενός χρήστη διαρκεί περίπου ένα δευτερόλεπτο, όπως μπορούμε να δούμε στις χρονικές σημάνσεις έναρξης και λήξης στα στιγμιότυπα οθόνης των Σχημάτων 5.2.B και 5.4.C.

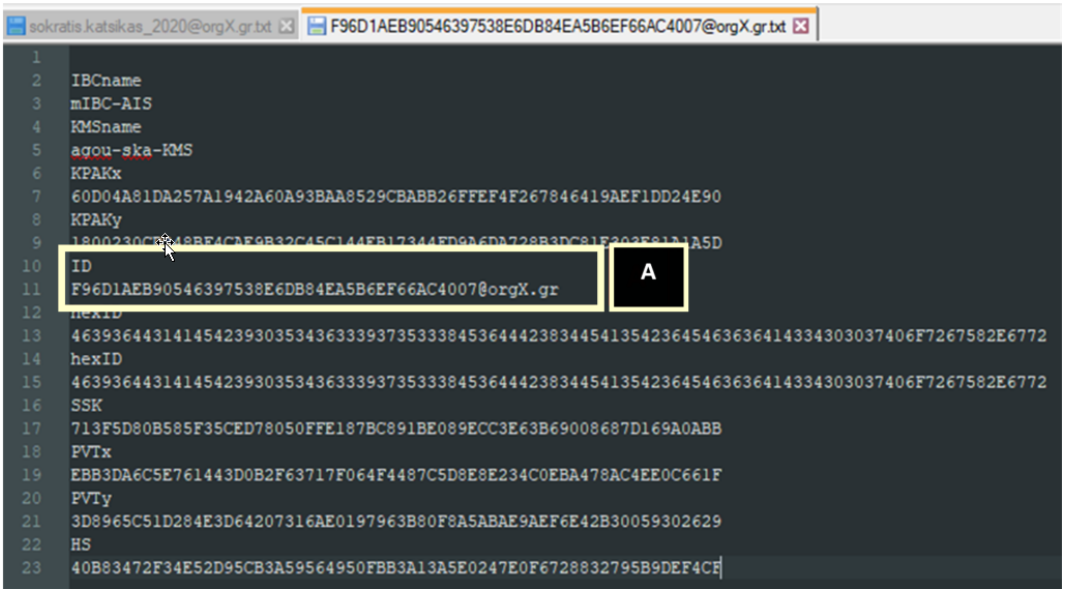
5.7 Δημιουργία Ψηφιακής Υπογραφής υπό ARIBC-ECCSI

Η εφαρμογή για την υπογραφή ενός μηνύματος και την επικύρωση της υπογραφής είναι η ίδια τόσο για τον τυπικό χρήστη όσο και για τον ανώνυμο χρήστη. Ωστόσο, εδώ παρέχουμε παραδείγματα και για τους δύο. Θυμίζουμε ότι η υπογραφή ενός μηνύματος αποτελείται από το τρίπτυχο: Signature = (*PVT, r, s*). Δηλαδή το, στατικό για όλα τα μηνύματα του υπογράφοντος, *PVT* και τις μεταβλητές τιμές *r, s* που υπολογίζονται για κάθε μήνυμα.

Τεχνικά υλοποιείται η μεθοδολογία που παρουσιάστηκε στην ενότητα 4.3.4 της διατριβής. Η εφαρμογή ψηφιακής υπογραφής δέχεται ως είσοδο:

1. Το μήνυμα (*m*) που θα υπογραφεί ψηφιακά είναι το "iaIBC TEST MSG" στην περίπτωση του επώνυμου χρήστη, (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.6.A) και "TEST mesg to be signed" στην περίπτωση του επώνυμου χρήστη, (βλ. Στιγμιότυπο οθόνης του Σχήματος 5.7.A)
2. Το αναγνωριστικό (*ID*) του Υπογράφοντος, (βλ. αντίστοιχα στιγμιότυπα οθόνης 5.6.A και 5.7.A)
3. Το Ιδιωτικό Κλειδί υπογραφής (ΙΚΥ/*SSK*) του Υπογράφοντος, (βλ. αντίστοιχα στιγμιότυπα οθόνης των Σχημάτων 5.6.A και 5.7.A)
4. Τις συντεταγμένες (PVT_X, PVT_Y) που προσδιορίζουν το ΔΤΕ/*PVT* του Υπογράφοντος, (βλ. αντίστοιχα στιγμιότυπα οθόνης των Σχημάτων 5.6.A και

Σχήμα 5.4: Στιγμιότυπο οθόνης από τη δημιουργία του Ιδιωτικού Κλειδιού Υπογραφής (SSK) και του Δημόσιου Τεκμηρίου Επικύρωσης (PVT) του ανώνυμου χρήστη.



Σχήμα 5.5: Στιγμιότυπο οθόνης του αρχείου που στέλνει ο ΑΚΣ στον ανώνυμο χρήστη.

5.7.Α)

5. Τις συντεταγμένες ($KPAK_X$,$KPAK_Y$) του Δημόσιου Κλειδιού ($KPAK_{agou-ska-KMS}$) του Αξιόπιστου Κεντρικου Συντονιστή ΑΚΣ(KMS) agou-ska-KMS στον οποίο είναι εγγεγραμμένος ο Υπογράφων.

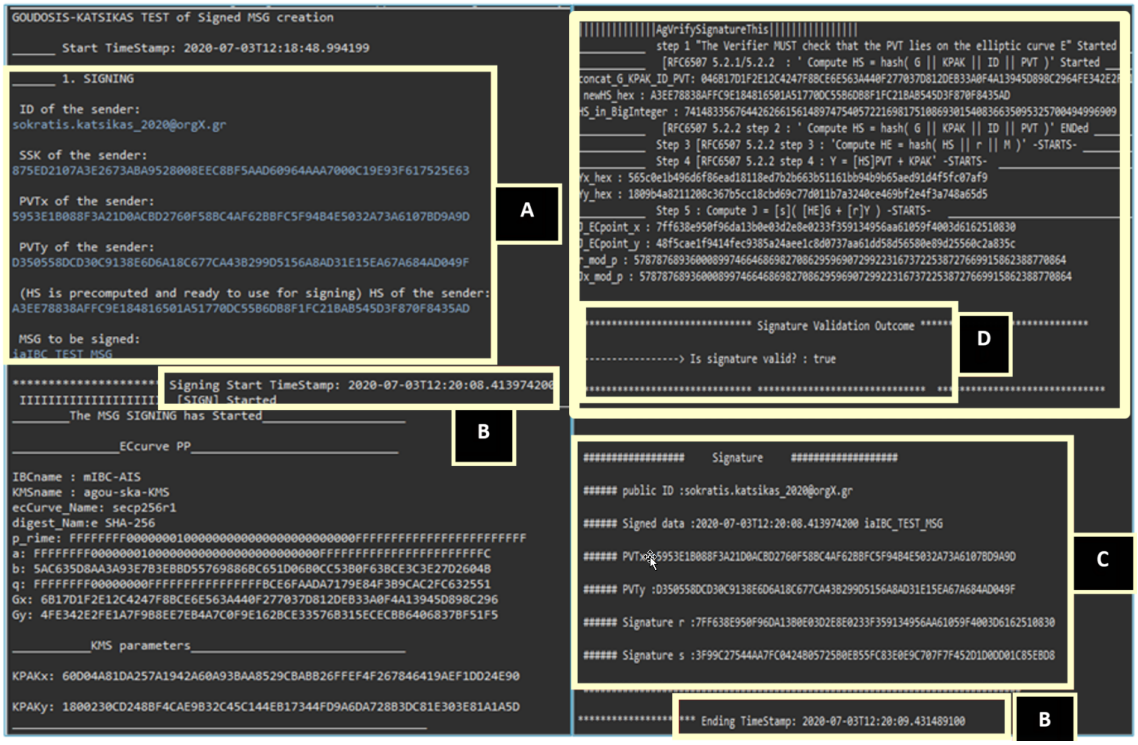
Η εφαρμογή δημιουργεί την ψηφιακή υπογραφή και ελέγχει την εγκυρότητά της (βλ. αντίστοιχα στιγμιότυπα οθόνης των Σχημάτων 5.6.D και 5.7.D).

Εάν η υπογραφή είναι έγκυρη, η εφαρμογή την εμφανίζει (βλ. αντίστοιχα στιγμιότυπα οθόνης των Σχημάτων 5.6.C και 5.7.C).

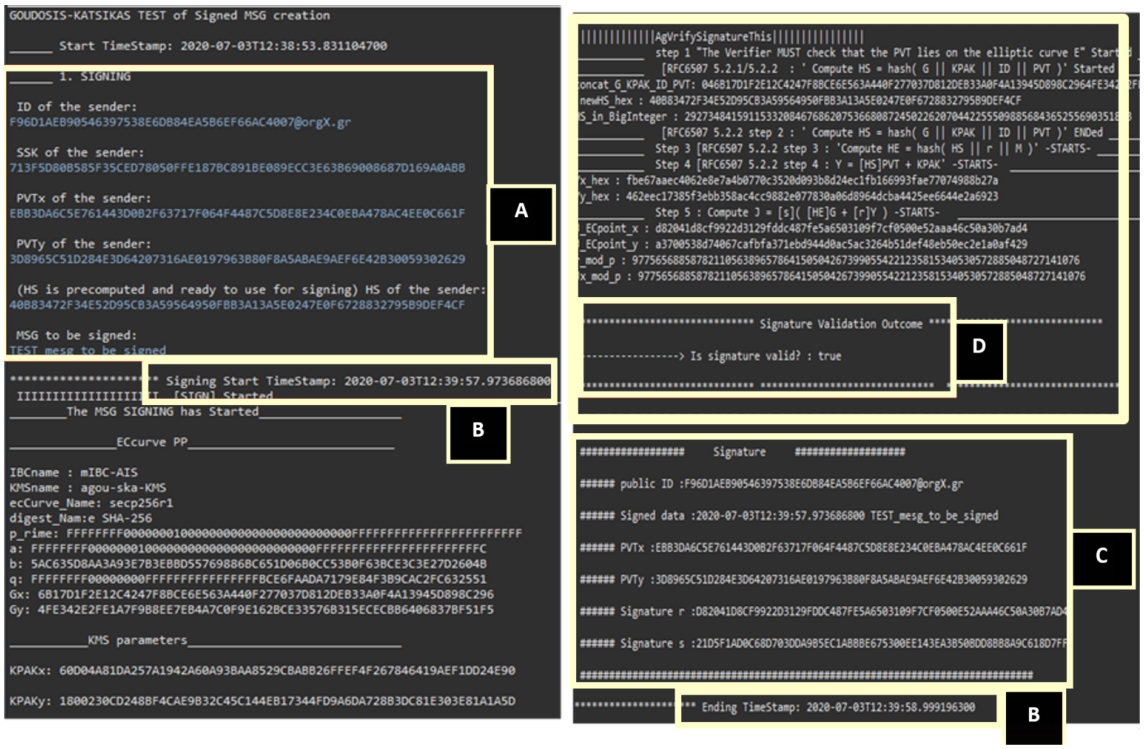
Για λόγους απλότητας, ο κώδικας ελέγχου της εγκυρότητας της ψηφιακής υπογραφής είναι ενσωματωμένος στην εφαρμογή της δημιουργίας της ψηφιακής υπογραφής. Στα αντίστοιχα στιγμιότυπα οθόνης των Σχημάτων 5.6 και 5.7, ο κώδικας ελέγχου της εγκυρότητας της ψηφιακής υπογραφής αντιστοιχεί στα μέρη που περικλείονται από το πράσινο διακεκομμένο πλαίσιο.

5.8 Το λειτουργικό κόστος δημιουργίας ψηφιακής υπογραφής

Σε Η/Υ με Intel Core ™ i7-5600U CPU @ 2.60Hz, RAM: 16GB, OS: 64-bit Windows 10 Pro, οι πόροι και ο χρόνος που απαιτούνται για την εκτέλεση των διαδικασιών ψηφιακής υπογραφής μηνύματος από ανώνυμο χρήστη και η επακόλουθη επαλήθευση της ψηφιακής υπογραφής είναι αμελητέοι. Για παράδειγμα, η δημιουργία ενός χρήστη διαρκεί περίπου ένα δευτερόλεπτο, όπως μπορούμε να δούμε στις χρονικές σημάνσεις έναρξης (πλαίσια Β) και λήξης (πλαίσια (C) στα στιγμιότυπα οθόνης των Σχημάτων 5.6 και 5.7.



Σχήμα 5.6: Στιγμιότυπο οθόνης δημιουργίας ψηφιακής υπογραφής μηνυμάτων από επώνυμο χρήστη και η επακόλουθη επαλήθευση της ψηφιακής υπογραφής.



Σχήμα 5.7: Στιγμιότυπο οθόνης δημιουργίας ψηφιακής υπογραφής μηνυμάτων από ανώνυμο χρήστη και η επακόλουθη επαλήθευση της ψηφιακής υπογραφής.

Κεφάλαιο 6

Ασφαλής ναυσιπλοΐα: Η υποδομή mIBC-AIS

6.1 Εισαγωγή

Το σύγχρονο παγκόσμιο ναυτιλιακό περιβάλλον είναι περίπλοκο και τα διασυνδεδεμένα μέρη του περιλαμβάνουν διεθνείς οργανισμούς, εθνικές αρχές, ναυτιλιακούς πράκτορες, ασφαλιστικές και ναυτιλιακές εταιρείες, σκάφη, πληρώματα, προμηθευτές και μια πανσπερμια συστημάτων ναυσιπλοΐας [67]. Το κανονιστικό του πλαίσιο είναι εξίσου πολύπλοκο, αφού διέπεται από εθνικούς κανονισμούς και νόμους αλλά και από διεθνείς συμβάσεις και συνθήκες. Οι επικοινωνίες είναι συνήθως αναξιόπιστες, με περιορισμένο εύρος ζώνης και ιδιαίτερα ακριβές όταν χρησιμοποιούνται δορυφορικά συστήματα.

6.2 Το σύστημα αυτόματης αναγνώρισης AIS (Automatic Identification System)

Η ασφάλεια της σύγχρονης ναυσιπλοΐας, με πληθώρα σκαφών όλων των τύπων που κινούνται ακατάπαυστα, προϋποθέτει συνεχή και ακριβή ροή πληροφοριών σε πραγματικό χρόνο. Το ραντάρ ήταν και παραμένει υψίστης σημασίας για την αντίληψη της κατάστασης του περίγυρου ενός σκάφους αλλά έχει σημαντικούς περιορισμούς, με κυριότερο τη μεταβλητότητα της ακρίβειας των δεδομένων που παρέχει. Η ακρίβεια των δεδομένων του ραντάρ είναι συνάρτηση της μέγιστης εμβέλειάς του, των καιρικών συνθηκών, της παρουσίας εμποδίων (π.χ. μικρά ή μεγάλα τμήματα ξηράς) το μέγεθος ή τη φύση του στόχου, η οποία επηρεάζει την Τιμή Διατομής-Ραντάρ (Radar cross-section (RCS)) κ.α.

Το AIS είναι ηλεκτρονικό βοήθημα ασφάλειας της ναυσιπλοΐας το οποίο βασίζεται στις αυτόματες μεταδόσεις πληροφοριών του σκάφους όπου είναι εγκατεστημένο. Συνεπώς, αντίθετα με το ραντάρ που ¨ανακαλύπτει¨ τα σκάφη γύρω του, το AIS εκπέμπει οικειοθελώς τις πληροφορίες του σκάφους. Σε κάθε σκάφος οι πληροφορίες που λαμβάνονται σε πραγματικό χρόνο από τις συσκευές AIS των άλλων σκαφών εντός εμβέλειας ή δορυφορικά, εάν υπάρχει αντίστοιχη ζεύξη, συγκεντρώνονται και εμφανίζονται στον ηλεκτρονικό χάρτη πλοήγησης του σκάφους, προσφέροντας στον

αξιωματικό υπηρεσίας μια αναβαθμισμένη εικόνα της θαλάσσιας κυκλοφορίας στην περιοχή όπου πλέει το σκάφος.

Το AIS αποτελείται από τις ηλεκτρονικές συσκευές (συσκευή συγκέντρωσης των δεδομένων και κεραία μετάδοσης) και ένα πρωτόκολλο επικοινωνίας που επιτρέπει την κωδικοποίηση των εκπεμπόμενων δεδομένων. Το πρωτόκολλο επικοινωνίας του AIS περιγράφει συγκεκριμένες μορφοποιήσεις και ομαδοποιήσεις των δεδομένων ανάλογα με τη χρήση τους. Για παράδειγμα, μια ομάδα δεδομένων συγκροτεί τα συνήθη μηνύματα προσδιορισμού θέσης του σκάφους (π.χ. μηνύματα AIS τύπου 1,2 και 3) και διαφορετική ομάδα τα μηνύματα βοήθειας (π.χ. μηνύματα AIS τύπου 21). Μία γενική κατηγοριοποίηση των δεδομένων που μεταδίδει το AIS είναι η παρακάτω:

- Στατικά δεδομένα που αφορούν κυρίως την ταυτότητα του σκάφους όπως ο μοναδικός αριθμός ταυτότητας Maritime Mobile Service Identity (MMSI)[1], ο μοναδικός αριθμός ταυτότητας του IMO[2], ο τύπος του σκάφους, οι διαστάσεις του κ.α.
- Δυναμικά δεδομένα ναυσιπλοΐας πραγματικού χρόνου, όπως η θέση του σκάφους σύμφωνα με το Global Navigation Satellite System (GNSS), η κατεύθυνση, η ταχύτητα κλπ.
- Δυναμικά δεδομένα που αφορούν το συγκεκριμένο ταξίδι, όπως ο τύπος του φορτίου, το λιμάνι αναχώρησης, το λιμάνι προορισμού.
- Διάφορα άλλα δεδομένα κατά περίπτωση.

Το AIS είναι πλέον υποχρεωτικό να υπάρχει στην πλειονότητα των σκαφών βάσει της σύμβασης "Solas Chapter V- Annex 17 - Automatic Identification Systems (AIS)" [68] και η χρήση του ρυθμίζεται από τον «Κανονισμό 19» της σύμβασης SOLAS Κεφάλαιο 5, [68] υπό την επίβλεψη του Διεθνούς Ναυτιλιακού Οργανισμού (IMO) και της Διεθνούς Ένωσης Τηλεπικοινωνιών (ITU) [69] [70].

Στα Σχήματα 6.1 και 6.2 φαίνονται οι πληροφορίες που λαμβάνονται μέσω ραντάρ και αυτές που λαμβάνονται μέσω του συστήματος AIS.

Τα τελευταία χρόνια, πολλοί σταθμοί ξηράς εξοπλισμένοι με δέκτες AIS προωθούν τα λαμβανόμενα δεδομένα σε βάσεις δεδομένων και τελικά σε εξειδικευμένους ιστότοπους στο διαδίκτυο, όπου ελεύθερα ή με συνδρομή έχει πρόσβαση ο καθένας[3] (βλ. Σχήμα 6.3).

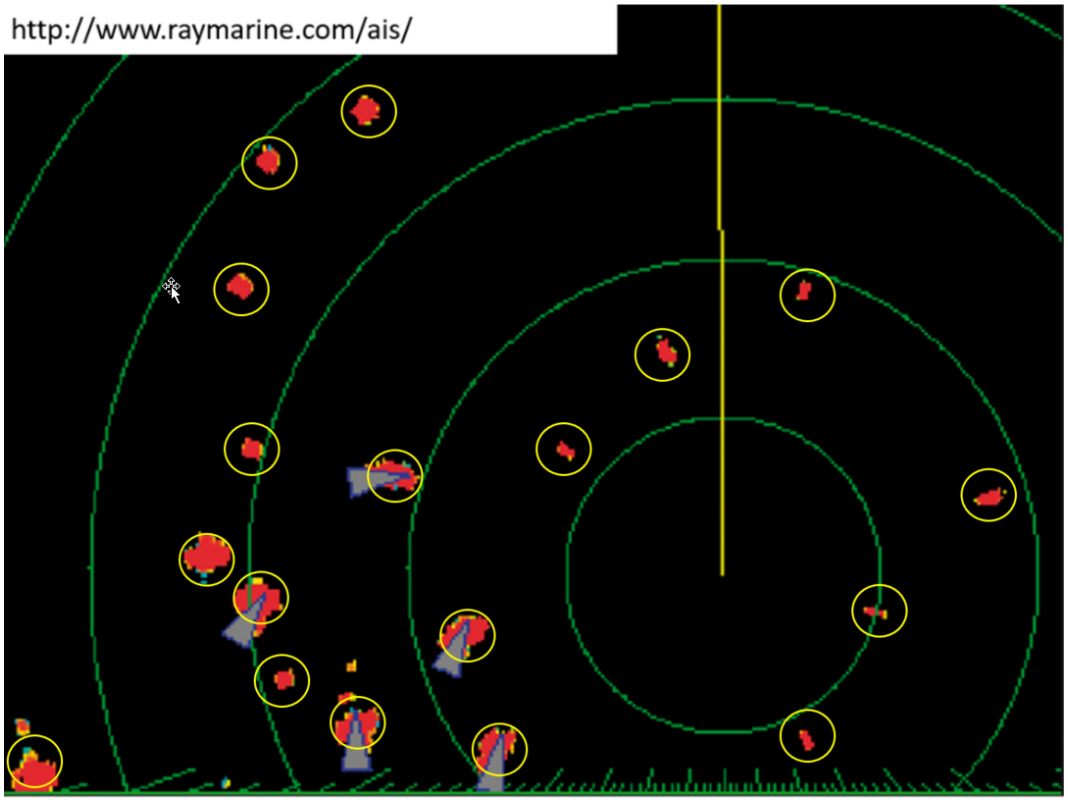
6.2.1 Το πλαίσιο λειτουργίας του AIS: Τα "AIS Ad-hoc Networks (AISANETs)"

Τα σκάφη που είναι εξοπλισμένα με AIS δημιουργούν μη-σταθερά, αλληλεπικαλυπτόμενα, εφήμερα και δυναμικά, επί τούτω δίκτυα, που τα ονομάσαμε

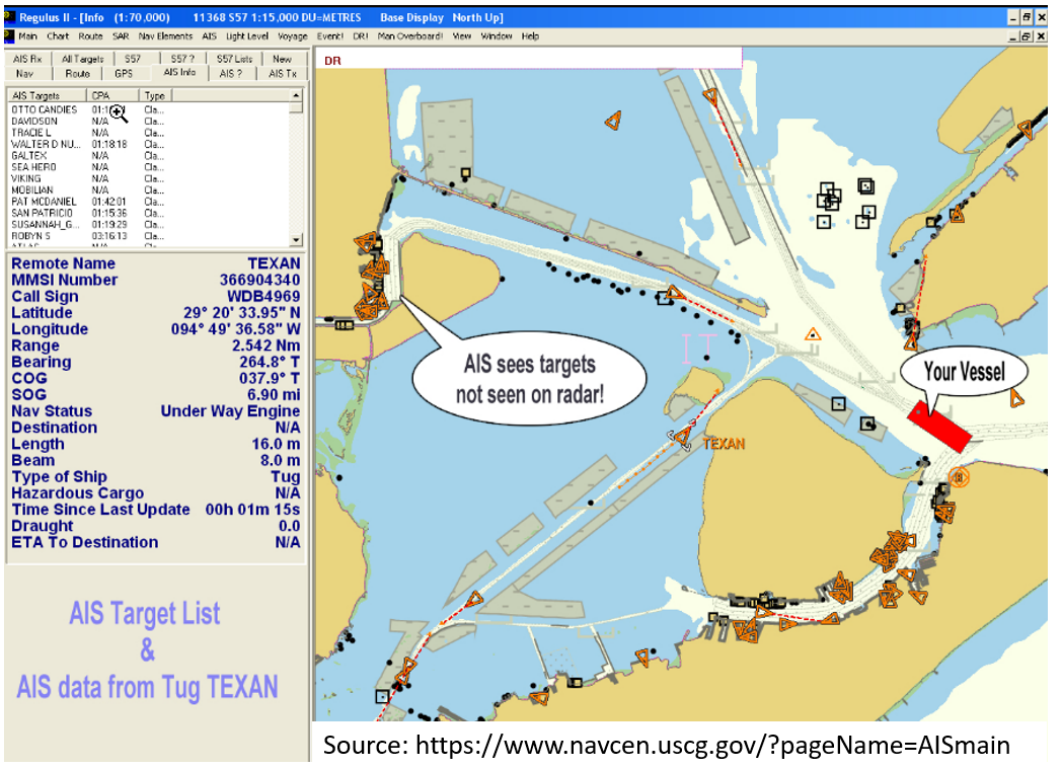
[1]Το MMSI αποτελείται από 9-ψηφία και ταυτοποιεί μοναδικά κάθε σκάφος. Εκχωρείται σε όλες τις ραδιοεπικοινωνίες αυτού του σκάφους και αλλάζει μόνο όταν ένα σκάφος αλλάζει σημαία και αρχή νηολόγησης.

[2]Ο αριθμός του Διεθνούς Ναυτιλιακού Οργανισμού (International Maritime Organization (IMO)) είναι ακόμα ένα αναγνωριστικό του σκάφους. Σχηματίζεται από το πρόθεμα IMO ακολουθούμενο από 7 ψηφία. Η κύρια διαφορά με το MMSI είναι ότι ο αριθμός IMO παραμένει σταθερός σε ένα σκάφος, από την αρχή της ζωής του έως το τέλος του.

[3]π.χ. `https://www.marinetraffic.com`



Σχήμα 6.1: Συνδυαστική απεικόνιση πληροφοριών που προέρχονται από το ραντάρ (κόκκινα στίγματα) και πληροφοριών που λαμβάνονται μέσω του συστήματος AIS. Στη δεύτερη περίπτωση προσδιορίζεται και η κατεύθυνση του σκάφους.(πηγή: www.raymarine.com/ais.)



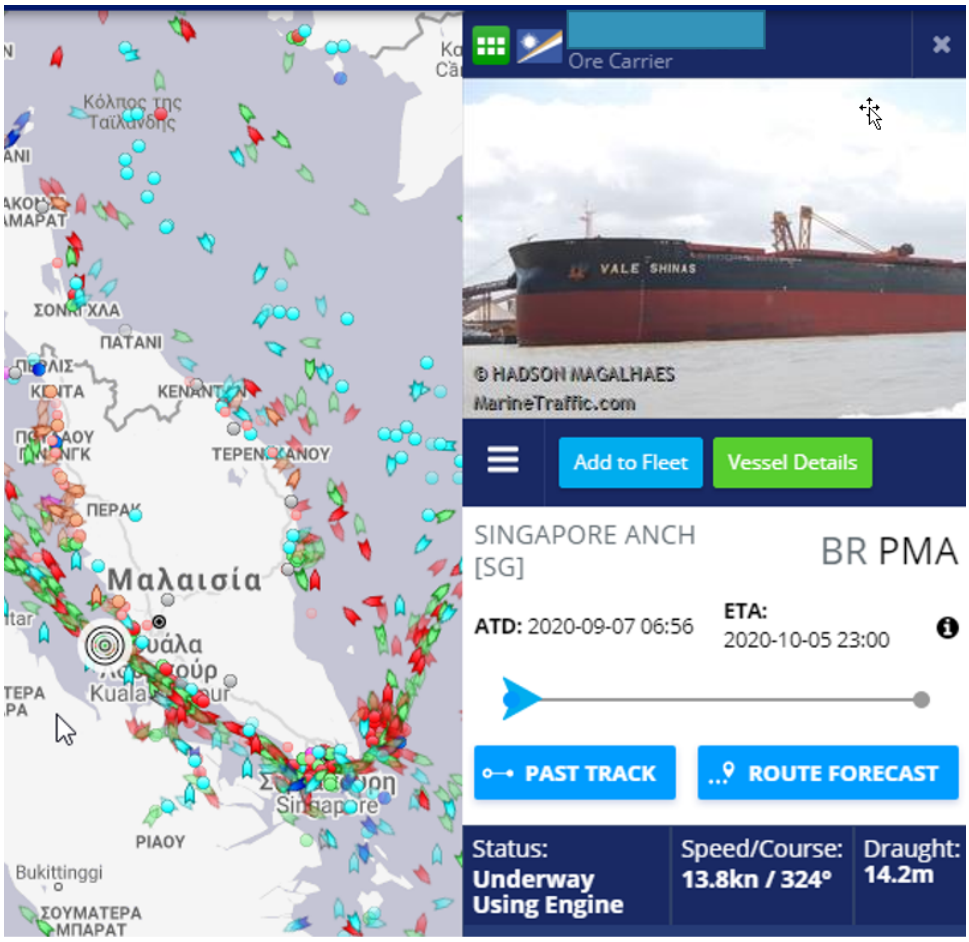
Σχήμα 6.2: Στιγμιότυπο δεδομένων του συστήματος AIS που εμφανίζονται σε ηλεκτρονικά διαγράμματα πλοήγησης σε πραγματικό χρόνο.

AIS Ad-hoc Networks (AISANETs) όπως απεικονίζονται στο Σχήμα 6.4. Όταν βρίσκεται στη θάλασσα, κάθε σκάφος μεταδίδει και λαμβάνει δεδομένα AIS εντός ενός τυπικού εύρους 20+ ναυτικών μιλίων[4].

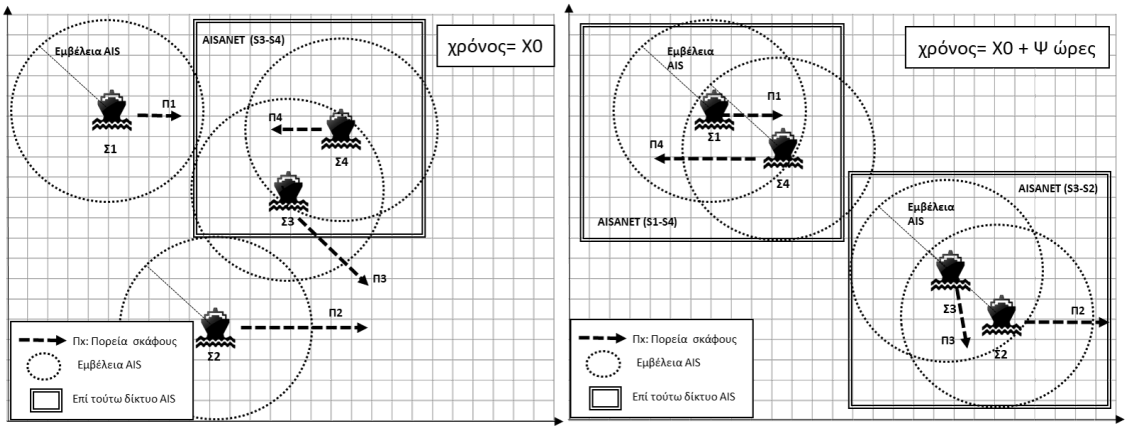
Σ' αυτήν τη διατριβή αντιμετωπίζουμε τα AIS Ad-hoc NET ως ειδική περίπτωση Mobile Ad-hoc NETworks (MANETs) [71], όπου οι κινητές οντότητες είναι τα πλοία και το πρωτόκολλο επικοινωνίας είναι το AIS. Λόγω της συνεχούς κίνησης και εναλλαγής των συμμετεχόντων σκαφών στα AISANETs, η διάρκεια ζωής τους και η τοπολογία τους είναι δυναμική. Ομοιότητες μπορούν επίσης να εντοπιστούν μεταξύ των AISANET, των VANET και του συστήματος αυτόματης ανίχνευσης (ADS-B) στην αεροπλοΐα.

Η απουσία πιστοποιητικών στις υλοποιήσεις KBT μας επιτρέπει να σχεδιάζουμε εφαρμογές δημόσιου κλειδιού σημαντικά απλούστερες και λιγότερο απαιτητικές σε πόρους, ιδιότητα ιδιαίτερα ελκυστική για εφαρμογή σε επί τούτω κινητά δίκτυα (MANET). [6] [72] [56] [57] [73]. Επιπλέον, στο [6], η KBT θεωρείται ως ιδιαίτερα κατάλληλη όταν ¨απαιτείται αποτελεσματική διαχείριση κλειδιών και μέτριο επίπεδο ασφάλειας¨. Λόγω όλων των παραπάνω, θεωρούμε ότι η KBT είναι μια πολλά υποσχόμενη τεχνολογία για τη θωράκιση της ασφάλειας των AISANETs.

[4]Η εμβέλεια του AIS ποικίλλει ανάλογα με το ύψος της κεραίας, την ισχύ της, τη θέση του σκάφους στην υδρόγειο (λόγω της διαφορετικής γήινης καμπυλότητας), καθώς και τις καιρικές συνθήκες στην περιοχή.



Σχήμα 6.3: Στιγμιότυπο της ναυσιπλοΐας στα Στενά της Μαλάκκα στις 09/09/2020, 15:30 (πηγή: `www.marinetraffic.com`)



Σχήμα 6.4: AIS Ad-hoc Networks (AISANETs)

6.3 Τα προβλήματα ασφάλειας του AIS

Σ' αυτήν την ενότητα συζητάμε ορισμένα από τα προβλήματα ασφάλειας του AIS. Επισημαίνουμε ότι δεν εξετάζεται η ασφάλεια της ηλεκτρονικής υποδομής του συστήματος AIS, η ακεραιότητα των δεδομένων που διοχετεύονται στο AIS από τον εξοπλισμό του πλοίου, αλλά ούτε και πιθανές επιθέσεις στο ηλεκτρομαγνητικό φάσμα μετάδοσης των μηνυμάτων AIS. Όπως διευκρινίσαμε και στην εισαγωγή αυτής της διατριβής, η έρευνά μας επικεντρώνεται στην ασφάλεια του πρωτοκόλλου του συστήματος AIS και μόνο, εξεταζόμενη ως μια περίπτωση ασύρματου πρωτοκόλλου μετάδοσης δεδομένων και ιδιαίτερα των Mobile Ad-hoc NETworks (MANETs). Συνεπώς, σ' αυτήν τη διατριβή εξετάζουμε εάν το πρωτόκολλο του συστήματος AIS προσφέρει, και, εάν ναι, υπό ποιες προϋποθέσεις, τις παρακάτω υπηρεσίες: διαθεσιμότητα, εμπιστευτικότητα δεδομένων, πιστοποίηση ταυτότητας του αποστολέα, ακεραιότητα δεδομένων και μη-αποποίηση αποστολής (non-repudiation).

Ανεπίσημα, κατά καιρούς υπήρξαν πολλές φωνές που αντιμετώπιζαν με σκεπτικισμό την έλλειψη ασφάλειας στον σχεδιασμό του AIS, αλλά ήταν οι εργασίες των Balduzzi κ.ά στα [74], [25], που έδειξαν ότι κατασκευάζοντας ένα πομπό AIS, με υλικά που μπορεί να βρει ο καθένας και δημιουργώντας αντίστοιχο ειδικό λογισμικό, μπορεί κάποιος να στείλει πλασματικά μηνύματα, που όσοι τα λαμβάνουν δεν θα έχουν τη δυνατότητα να διακρίνουν την πλαστότητά τους.

Επίσης με σκεπτικισμό αντιμετωπίζεται από πολλούς και η ανεξέλεγκτη δημοσίευση των δεδομένων ναυσιπλοΐας σε πραγματικό χρόνο στο διαδίκτυο. Χαρακτηριστικό παράδειγμα ήταν ένα άρθρο σε ναυτιλιακό ηλεκτρονικό περιοδικό ανταλλαγής απόψεων όπου ένας πλοίαρχος εξέφραζε την απορία του για το γεγονός ότι σε περιοχές με αυξημένα περιστατικά πειρατείας, την ίδια στιγμή που τα πολεμικά σκάφη επιφορτισμένα με τη διαφύλαξη της ασφαλούς ναυσιπλοΐας στην περιοχή έπλεαν «σε καθεστώς ηλεκτρονικής σιγής», τα εμπορικά σκάφη στην περιοχή ήταν υποχρεωμένα να έχουν τα συστήματα AIS εν λειτουργία και μάλιστα προσφέροντας όλα τα στοιχεία της ταυτότητας, του τύπου, του φορτίου, και του πλου του σκάφους τους στη διάθεση των πειρατών [5]. Παρόμοιες απορίες εκφράζονται και από πλοιάρχους πολυτελών σκαφών που προσπαθούν να προστατέψουν την ιδιωτική ζωή των επιφανών πελατών τους από άτομα που, μέσω του διαδικτύου, έχουν τη δυνατότητα να γνωρίζουν πού βρίσκεται το σκάφος που τους μεταφέρει κάθε στιγμή. Οι παραπάνω εκφρασμένες ανησυχίες υποθάλπτουν την εσκεμμένη απενεργοποίηση του συστήματος από το πλήρωμα του σκάφους, είτε ακολουθώντας τις επίσημες οδηγίες του IMO σε περιοχές με αυξημένα περιστατικά πειρατείας[5], είτε προφασιζόμενοι τεχνικές δυσλειτουργίες, υποσκάπτοντας έτσι τη διαθεσιμότητα του συστήματος.

Αν και εκτός του πεδίου της έρευνάς μας, αναφέρουμε την εργασία [75] στην οποία τεκμηριώνονται αρκετές επιθέσεις εναντίον της διαθεσιμότητας (Denial of Service attacks) του AIS, είτε μέσω παρεμβολών στις συχνότητές του, είτε μέσω μετάδοσης υπερβολικά μεγάλου, μη-διαχειρίσιμου, όγκου δεδομένων.

Τέλος, στα [26] [31] οι συγγραφείς (Gary C Kessler, Craiger, and Haass), πέραν των

[5]Στις 2/12/2015, ο IMO ενέκρινε το ψήφισμα A.1106 (29) «Αναθεωρημένες οδηγίες για την επιχειρησιακή χρήση των συστημάτων αυτόματης αναγνώρισης πλοίου (AIS)» όπου στο άρθρο 22 υπάρχει η ακόλουθη οδηγία: *"If the master believes that the continual operation of AIS might compromise the safety or security of his/her ship or where security incidents are imminent, the AIS may be switched off"*.

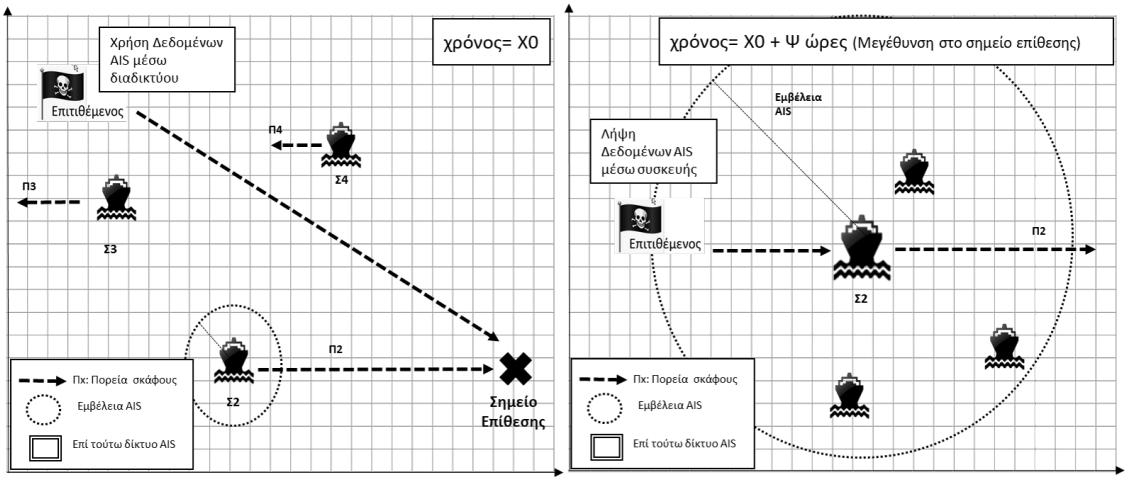
Ψηφιακές απειλές στο πρωτόκολλο του AIS	Κατηγορία	Απειλή	Πιθανότητα	Δριμύτητα	Ευκολία
Απενεργοποίηση AIS	Διαθεσιμότητα	Άνθρωπος	Μικρή	Καταστροφική	Τετριμμένο
Πλαστογράφηση πλοίου	Ακεραιότητα, Αυθεντικότητα	Έγχυση δεδομένων	Μικρή	Κρίσιμη	Απλό
Υποκλοπή δεδομένων	Εμπιστευτικότητα Αυθεντικότητα,	Υποκλοπή	Συχνά	Αμελητέα	Τετριμμένο
Άρνηση παροχής υπηρεσιών	Διαθεσιμότητα,	Έγχυση δεδομένων	Μικρή	Οριακή	Δύσκολο
Δημιουργία σκάφους-φαντάσμα	Ακεραιότητα, Αυθεντικότητα, Άχρηστα δεδομένα	Έγχυση δεδομένων	Μικρή	Οριακή	Δύσκολο
Πλαστογράφηση Closest Point-of-Approach/AIS SAR Transponder (CPA/AIS-SART)	Ακεραιότητα, Αυθεντικότητα, Άχρηστα δεδομένα	Έγχυση δεδομένων	Απίθανη	Κρίσιμη	Δύσκολο
Εξαφάνιση σκαφών	Ακεραιότητα, Διαθεσιμότητα	Έγχυση δεδομένων	Μικρή	Κρίσιμη	Δύσκολο
Πλαστογράφηση Aids-to-Navigation (AtoN)	Ακεραιότητα, Αυθεντικότητα, Άχρηστα δεδομένα	Έγχυση δεδομένων	Μικρή	Κρίσιμη	Δύσκολο
Τροποποίηση μηνύματος	Ακεραιότητα, Διαθεσιμότητα, Αυθεντικότητα, Άχρηστα δεδομένα	Τροποποίηση μηνύματος	Μέτρια	Κρίσιμη	Δύσκολο
Πλαστογράφηση πρόγνωσης καιρού	Ακεραιότητα, Αυθεντικότητα, Άχρηστα δεδομένα	Έγχυση δεδομένων	Μικρή	Οριακή	Δύσκολο

Πίνακας 6.1: Κύριες ψηφιακές απειλές στο πρωτόκολλο του AIS

λεπτομερών αναλύσεών τους για τα θέματα ασφαλείας του AIS, παραθέτουν πολύ ενδιαφέροντες πίνακες τους οποίους χρησιμοποιήσαμε ως βάση για τη διαμόρφωση του πίνακα 6.1.

6.3.1 Επιπτώσεις έλλειψης μηχανισμού εμπιστευτικότητας στο AIS

Η έλλειψη μηχανισμού εμπιστευτικότητας των μηνυμάτων του AIS επιτρέπει το ακόλουθο σενάριο επίθεσης: Πειρατές ή τρομοκράτες χρησιμοποιούν τους ιστότοπους αναπαραγωγής δεδομένων του AIS, που προαναφέραμε, προκειμένου στη συνέχεια να παρακολουθούν τον στόχο τους. Ταυτόχρονα, γνωρίζοντας την ακριβή πορεία του στόχου, επιλέγουν την περιοχή της επίθεσης στην οποία ένας παθητικός δέκτης AIS στο επιτιθέμενο σκάφος αρκεί για να τους οδηγήσει σε οπτική επαφή με το στόχο. Το σενάριο αυτό σκιαγραφείται στο Σχήμα 6.5, όπου ο επιτιθέμενος χρησιμοποιεί τις εκπομπές AIS του στόχου μέχρι την τελική επίθεση. Η αναγνώριση της πιθανότητας του σεναρίου αυτού οδήγησε τον IMO να αναγνωρίσει στους πλοιάρχους το δικαίωμα να απενεργοποιήσουν το AIS, παρόλο που αυτό μειώνει την ασφάλεια της ναυσιπλοΐας



Σχήμα 6.5: Σενάριο επίθεσης στο AIS: Πειρατές επιλέγουν στόχο, τον παρακολουθούν και προγραμματίζουν την επίθεσή τους μέσω του AIS.

σ' αυτήν την περιοχή. Ας σημειωθεί ότι στην περίπτωση της τρομοκρατίας το επιτιθέμενο σκάφος μπορεί να είναι μη επανδρωμένο, οπότε αυτόματα θα ακολουθεί παθητικά το σήμα του στόχου μέχρι τη στιγμή που θα χρησιμοποιηθεί κάποια άλλη τεχνολογία για την τελική προσέγγιση.

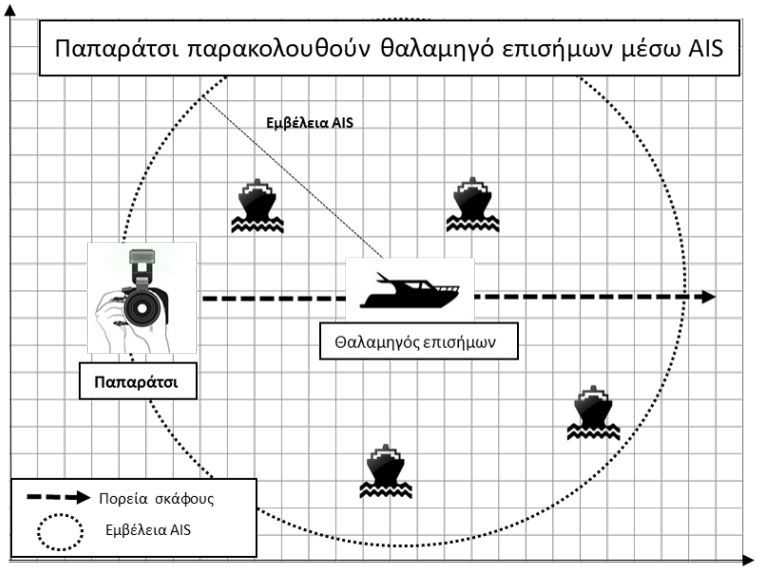
Παρόμοια μεθοδολογία αναγνώρισης και παρακολούθησης σκάφους στο οποίο επιβαίνουν επιφανή άτομα μπορεί να ακολουθήσουν δημοσιογράφοι προκειμένου να παραβιάσουν την ιδιωτικότητα των στόχων τους. Το σενάριο αυτό συνιστά άλλη μια περίπτωση όπου οι πλοίαρχοι καλούνται να επιλέξουν μεταξύ της νομιμότητας και της ασφάλειας της ναυσιπλοΐας και του συμφέροντος των πελατών τους (βλ. Σχήμα 6.6).

Τέλος, χωρίς αυτή τη στιγμή να είναι δυνατό να τεκμηριωθεί το σενάριο, θεωρούμε μη μηδενική την πιθανότητα τρομοκρατικής επίθεσης από μη-επανδρωμένο σκάφος-βόμβα με τη χρήση, μεταξύ άλλων, και του συστήματος AIS.

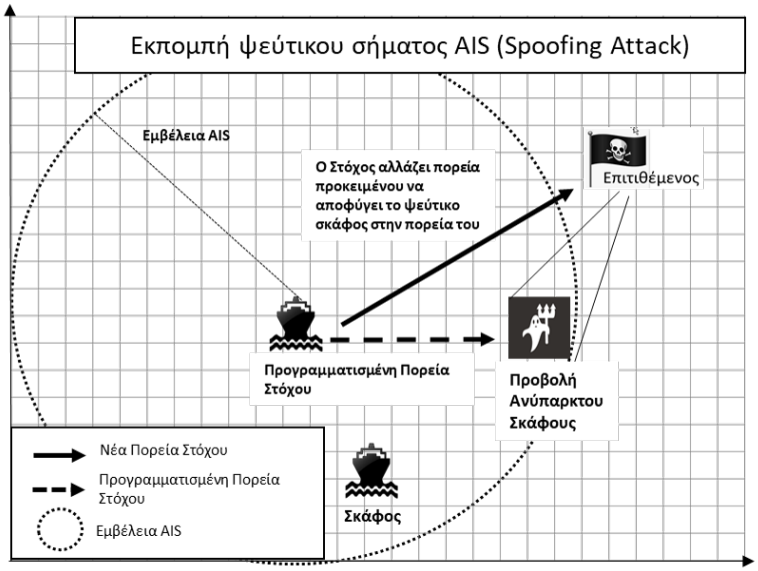
6.3.2 Επιπτώσεις έλλειψης μηχανισμού πιστοποίησης στα μηνύματα του AIS

Η απουσία μεθόδων πιστοποίησης της ταυτότητας της πηγής αλλά και της ακεραιότητας του κάθε μηνύματος AIS καθιστά το σύστημα ευάλωτο. Κατασκευασμένα ή αλλοιωμένα μηνύματα AIS ενδέχεται να φαίνονται ότι προέρχονται από υπαρκτά ή ανύπαρκτα σκάφη και να μεταδίδουν ψευδείς πληροφορίες ελιγμών, συναγερμών, βοηθημάτων ναυσιπλοΐας κλπ.

Ιδιαίτερα σε περιπτώσεις όπου η διασταύρωση των αλλοιωμένων/ψευδών στοιχείων με άλλα μέσα είναι δύσκολη ή αδύνατη, οι αξιωματικοί υπηρεσίας είναι υποχρεωμένοι να λάβουν αποφάσεις με βάση τα αλλοιωμένα/ψευδή στοιχεία που έχουν στη διάθεσή τους μέσω του AIS. Ένα τέτοιο σενάριο σκιαγραφείται στο Σχήμα 6.7, όπου παρουσιάζεται ο επιτιθέμενος να μεταδίδει ένα ψευδές μήνυμα AIS προκειμένου να εμφανίσει ανύπαρκτο σκάφος στην πορεία του στόχου και να τον ωθήσει να αλλάξει κατεύθυνση.



Σχήμα 6.6: Σενάριο επίθεσης στο AIS: Paparazzi παρακολουθούν μέσω του AIS πολυτελές σκάφος με επιφανείς επιβάτες.



Σχήμα 6.7: Ψευδές σήμα AIS που εμφανίζει ανύπαρκτο σκάφος.

Τέλος, επειδή το AIS χρησιμοποιείται ευρέως για τη συμμόρφωση των σκαφών σε κανονισμούς περί σεβασμού θαλάσσιων ζωνών (π.χ. θαλάσσια πάρκα) ή εντοπισμού μόλυνσης του θαλάσσιου περιβάλλοντος, η πιστοποίηση της ταυτότητας της πηγής εκπομπής του σήματος θα αύξανε την αξιοπιστία του στη διερεύνηση θαλάσσιων ατυχημάτων ή παραβιάσεων της ναυτικής νομοθεσίας.

6.4 Προδιαγραφές ενός ασφαλούς AIS

Με βάση την παραπάνω συζήτηση, οι προδιαγραφές που οφείλει να ικανοποιεί το ασφαλές AIS είναι τουλάχιστον οι εξής:

1. Κατ' επιλογήν πιστοποίηση αυθεντικότητας μηνύματος: Κατ' επιλογήν αποστολή AIS μηνυμάτων με δυνατότητα πιστοποίησης της ταυτότητας του αποστολέα και της ακεραιότητας των δεδομένων.

2. Κατ' επιλογήν εμπιστευτικότητα των AIS μηνυμάτων: Ο αποστολέας πρέπει να έχει τη δυνατότητα να στέλνει εμπιστευτικά AIS μηνύματα που να είναι αναγνώσιμα μόνο από ταυτοποιημένους δέκτες (π.χ. τις αρχές, ταυτοποιημένα σκάφη στην περιοχή, τα γραφεία της ναυτιλιακής εταιρείας κλπ.)

3. Κατ' επιλογή δυνατότητα ψευδωνυμιας κατόπιν αιτήματος. Θα πρέπει να προσφέρεται η επιλογή της, πιστοποιημένης από τις αρχές, ψευδωνυμοποίησης των μηνυμάτων του AIS κατόπιν αιτήματος, προκειμένου να διατηρείται η ηλεκτρονική ανωνυμια ενός σκάφους. Όμως, προκειμένου να αποφευχθεί η χρήση της ψευδωνυμοποίησης για άνομες πράξεις, θα πρέπει να διατηρείται η δυνατότητα ταυτοποίησης του σκάφους από τις αρχές εάν αυτό θεωρηθεί επιβεβλημένο.

4. Αναβάθμιση του υπάρχοντος AIS και όχι νέο AIS. Η λύση θα πρέπει να είναι συμβατή με το υπάρχον σύστημα και εφικτή με όσο το δυνατόν ελάχιστες μετατροπές στο υφιστάμενο περιβάλλον του συστήματος του AIS.

Πριν προχωρήσουμε, στην επόμενη ενότητα, στην περιγραφή της υποδομής mIBC-AIS, αναφέρουμε δύο επιχειρησιακού τύπου προτάσεις που θα επιτρέψουν την ευρεία υιοθέτησή της από την παγκόσμια ναυτιλιακή κοινότητα, στην οποία και επαφίεται η σε βάθος ανάλυση και βελτίωσή τους:

1. **Ορισμός της ¨επισφαλούς¨ θαλάσσιας περιοχής**: Όπως έχει ήδη αναφερθεί, ο IMO επιτρέπει τη νόμιμη απενεργοποίηση του AIS ¨... *εάν ο πλοίαρχος πιστεύει ότι η συνεχής λειτουργία του AIS ενδέχεται να θέσει σε κίνδυνο την ασφάλεια του πλοίου του...* ¨ [23]. Σ' αυτό το πλαίσιο, ορίζουμε ότι «επισφαλής θαλάσσια περιοχή» είναι μια θαλάσσια περιοχή όπου οι επίσημοι ναυτικοί οργανισμοί θα ορίζουν ότι η συνεχής λειτουργία του AIS ενδέχεται να θέσει σε κίνδυνο την ασφάλεια του πλοίου. Μια ¨επισφαλής θαλάσσια περιοχή¨ πρέπει να έχει συγκεκριμένα γεωγραφικά όρια (π.χ. η θαλάσσια περιοχή της Σομαλίας, ορισμένες παράκτιες περιοχές στη Δυτική Αφρική, τα Στενά της Μαλάκκα) και μπορεί να ορίζεται επί τούτω, βάσει διαθέσιμων στοιχείων π.χ. πληροφοριών για τρομοκρατική επίθεση, μεταφορά επικίνδυνων φορτίων. Η ναυτιλιακή κοινότητα θα πρέπει να καθορίσει διαδικασίες για την επίσημη δήλωση, τον ορισμό και την επισήμανση των «επισφαλών θαλάσσιων περιοχών» παγκοσμίως.

2. **Ορισμός επί τούτω Έμπιστου Τρίτου Μέρους (Trusted Third Party) σε μια επισφαλή θαλάσσια περιοχή**: Η ικανότητα διάκρισης ανά πάσα στιγμή μεταξύ των ύποπτων σκαφών μέσα σε κάθε επισφαλή θαλάσσια περιοχή είναι πολύ σημαντική για την υιοθέτηση της πρότασής μας. Ο ρόλος του Έμπιστου Τρίτου Μέρους που θα κάνει τη διάκριση μπορεί να ανατεθεί σ' έναν εκπρόσωπο μιας αρχής επιβολής του νόμου στην περιοχή. Στην πράξη, το Έμπιστο Τρίτο Μέρος μπορεί να είναι ένα σκάφος επιφανείας ή ένα αεροσκάφος κάποιας αρχής που περιπολεί στην επισφαλή θαλάσσια περιοχή και είναι επιφορτισμένο με την επισήμανση ύποπτων σκαφών.

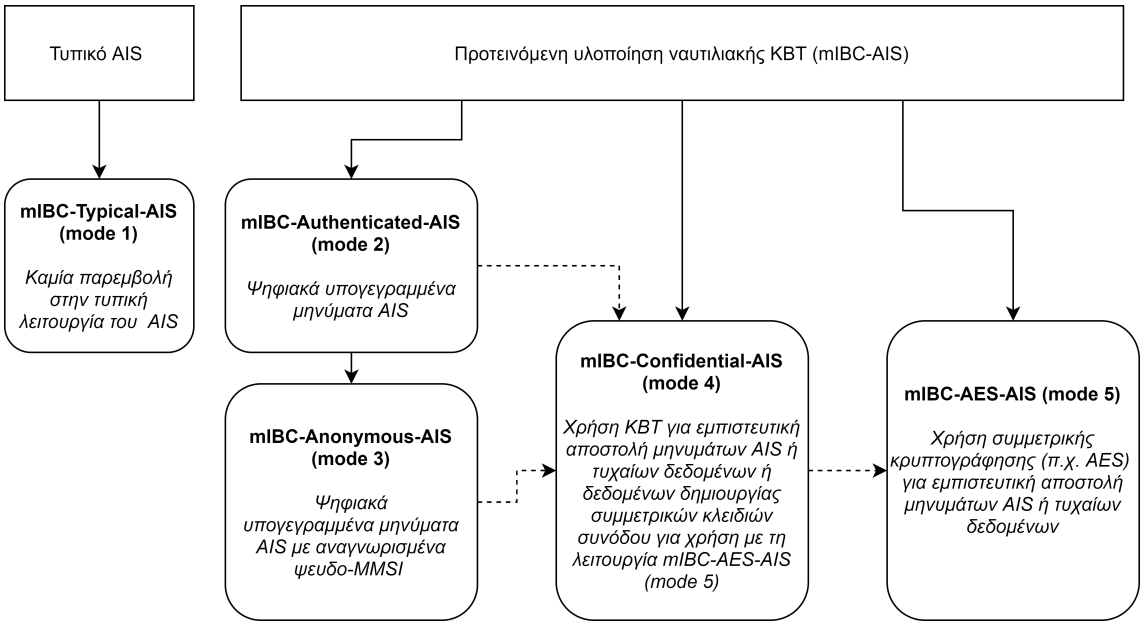
6.5 Η υποδομή mIBC-AIS: Επισκόπηση

Η υποδομή mIBC-AIS είναι υποδομή ΚΒΤ. Χρησιμοποιεί δύο, υφιστάμενα, ειδικού τύπου μηνύματα του πρωτοκόλλου AIS ως μεταφορείς των δεδομένων. Περιλαμβάνει την εφαρμογή mIBC-AIS-app, που περιγράφεται στην ενότητα 6.8, η οποία λειτουργεί ως πάροχος των αναβαθμισμένων λειτουργιών ασφάλειας του AIS και μπορεί να εγκατασταθεί είτε αυτόνομα ως ενδιάμεσος μεταξύ των κεραιών και των συσκευών δημιουργίας των σημάτων στις υπάρχουσες συσκευές AIS ή στις ίδιες τις συσκευές, μέσω ενημερώσεων υλικολογισμικού (firmware updates).

6.5.1 Τρόποι λειτουργίας

Η υποδομή mIBC-AIS ικανοποιεί τις προδιαγραφές που τέθηκαν στην ενότητα 6.4, επιτρέποντας τους εξής τρόπους λειτουργίας του AIS:

1. **Συμβατικό AIS, (mIBC-Typical-AIS (mode 1))**: Όπου δεν υπάρχουν ειδικές συνθήκες το AIS θα συνεχίσει να λειτουργεί όπως λειτουργεί σήμερα.
2. **Κατ' επιλογήν πιστοποίηση αυθεντικότητας μηνύματος, mIBC-Authenticated-AIS (mode 2)**: Δυνατότητα ψηφιακής υπογραφής των μηνυμάτων του AIS. Προσφέρει πιστοποίηση της ακεραιότητας και της ταυτότητας της μεταδιδόμενης πληροφορίας μέσω ψηφιακά υπογεγραμμένων μηνυμάτων AIS. Στο mIBC-AIS, μια συσκευή AIS υπογράφει ψηφιακά τα δεδομένα του AIS και οι αποδέκτες πιστοποιούν την ταυτότητα των υπογεγραμμένων δεδομένων AIS χρησιμοποιώντας το MMSI του πομπού.
3. **Κατ' επιλογή δυνατότητα ψευδωνυμιας κατόπιν αιτήματος, mIBC-Anonymous-AIS (mode 3)**: Ψηφιακά υπογεγραμμένα, πιστοποιημένα από τις αρχές, ψευδώνυμα ψευδο-MMSIs. Μια συσκευή AIS μεταδίδει, αντί του πραγματικού MMSI του σκάφους, ένα ψευδο-MMSI που δημιουργείται και υπογράφεται κρυπτογραφικά από τον ΑΚΣ κάποιας ναυτιλιακής αρχής. Από κρυπτογραφική άποψη, το mIBC-Anonymous-AIS (mode 3) είναι ίδιο με το mIBC-Authenticated-AIS (mode 2) αλλά χρησιμοποιεί ψευδο-MMSI αντί για το πραγματικό MMSI των πλοίων.
4. **Κατ' επιλογήν εμπιστευτικότητα των AIS μηνυμάτων, mIBC-Confidential-AIS (mode 4)**: Δυνατότητα κρυπτογράφησης των μηνυμάτων του AIS μέσω κάποιου μηχανισμού ΚΒΤ. Προσφέρονται δύο επιμέρους δυνατότητες:



Σχήμα 6.8: Προτεινόμενες λειτουργίες του mIBC-AIS

(α΄) Δυνατότητα επιλογής κρυπτογράφησης όλου ή μέρους του μηνύματος του AIS. Για παράδειγμα, τα στοιχεία ναυσιπλοΐας μπορεί να είναι αναγνώσιμα απ΄ όλους (μη κρυπτογραφημένα), αλλά ο τύπος φορτίου (π.χ. τοξικά, όπλα) είναι κρυπτογραφημένος και αναγνώσιμος μόνο από τις αρχές.

(β΄) Δυνατότητα ανταλλαγής κρυπτογραφικών συμμετρικών κλειδιών συνόδου για ένα-προς-ένα επικοινωνία με τις αρχές ή τη ναυτιλιακή εταιρεία ή για τη δημιουργία έμπιστων AIS Ad-hoc NET (AISANET) στα οποία θα συμμετέχουν μόνο ταυτοποιημένα, αξιόπιστα μέρη.

5. **Εμπιστευτικότητα με συμμετρική κρυπτογράφηση, mIBC-AES-AIS (mode 5)**: Επιτρέπει τη μετάδοση κρυπτογραφημένων μηνυμάτων AIS σε αξιόπιστα σκάφη μέσω συμμετρικής κρυπτογραφίας[6].

Στο Σχήμα 6.8 φαίνονται οι παραπάνω τρόποι λειτουργίας.

6.5.2 Οντότητες που συμμετέχουν στην υποδομή mIBC

Σε αυτήν την ενότητα περιγράφουμε τις οντότητες που συμμετέχουν στην υποδομή mIBC και την κανονιστική δομή της. Οι συμμετέχουσες οντότητες χωρίζονται στις παρακάτω κατηγορίες:

1. Κεντρικές οντότητες, που έχουν κανονιστικό, συντονιστικό, και λειτουργικό ρόλο στη δημιουργία των ιδιωτικών κλειδιών των οντοτήτων χρηστών, δηλαδή έχουν και το ρόλο του ΑΚΣ. Τέτοιες οντότητες είναι:

   - Διεθνείς οργανισμοί, για παράδειγμα International Maritime Organization (IMO), International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA),

[6]Για παράδειγμα, με χρήση του Advanced Encryption Standard («Federal Federal Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)» 2001 [76]

- Εθνικές Ναυτιλιακές Αρχές, για παράδειγμα οι εθνικοί νηογνώμονες κάθε κράτους.

2. Οντότητες - χρήστες της mIBC:
   - Οντότητες που χρησιμοποιούν έμμεσα η άμεσα την υποδομή mIBC-AIS, όπως: σκάφη, beacons, σημαντήρες, κ.α.
   - Οντότητες που χρησιμοποιούν τις δυνατότητες που προσφέρει η υποδομή mIBC και η KBT, ανεξάρτητα από τη χρήση της στο AIS, όπως: Ναυτιλιακές Αρχές, Ναυτιλιακές εταιρείες, ασφαλιστικές εταιρείες, μεσάζοντες κλπ. Σ' αυτήν τη διατριβή δεν θα αναφερθούμε περαιτέρω σε αυτές τις οντότητες.

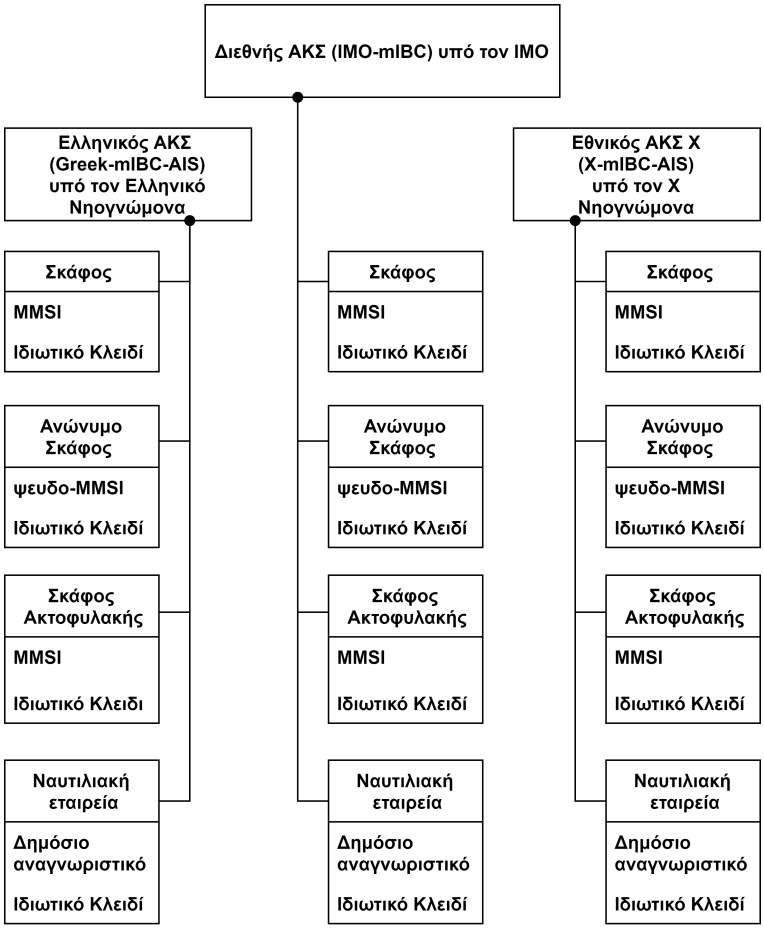
Το ακριβές μοντέλο της κανονιστικής δομής υποδομής mIBC-AIS μπορεί να είναι ιεραρχικό, όπως αυτό που φαίνεται στο Σχήμα 6.9, ή να αποτελείται από ανεξάρτητες, διαλειτουργικές, επιμέρους εθνικές δομές. Σε κάθε περίπτωση, τα Δημόσια Κλειδιά των σκαφών ή αντίστοιχα των συσκευών ή εγκαταστάσεων που διαθέτουν συσκευή AIS θα προέρχονται από τους αντίστοιχους αριθμούς MMSI και τα ιδιωτικά τους κλειδιά θα δημιουργούνται από τον ΑΚΣ της υποδομής στην οποία είναι εγγεγραμμένα τα σκάφη ή οι συσκευές. Η διαδικασία εγγραφής των σκαφών στις κανονιστικές αρχές και στους αντίστοιχους ΑΚΣ που διαθέτουν αυτές είναι εκτός του πεδίου της διατριβής. Τέλος, η διανομή των ιδιωτικών κλειδιών στις συσκευές mIBC-AIS μπορεί να γίνεται είτε δια ζώσης, μέσω μιας συσκευής μεταφοράς κρυπτογραφικών κλειδιών, είτε με κάποιου είδους παραλλαγή της διαδικασίας που έχουμε περιγράψει για την υποδομή ARIBC, στην ενότητα 4.2.2. Στη συνέχεια, λόγω της ιδιαιτερότητας του ναυτιλιακού κανονιστικού περιβάλλοντος, θεωρούμε ότι η μεταφορά γίνεται δια ζώσης, μέσω ειδικής συσκευής.

6.6 Η υποδομή mIBC-AIS: Προσφερόμενες υπηρεσίες

6.6.1 Διατήρηση ανωνυμίας: Anonymous-AIS και ψευδο-MMSIs

Ο όρος ¨ψηφιακό ψευδώνυμο¨ ή απλώς ¨ψευδώνυμο¨ εισήχθη από τον D. Chaum το 1985, σε ένα άρθρο στο οποίο προσπάθησε να εισαγάγει την έννοια της ¨ασφάλειας χωρίς ταυτοποίηση¨ [77]. Στο πλαίσιο που μελετάμε, τα ψευδώνυμα έγιναν δημοφιλή λόγω των εργασιών για την ανωνυμια στα VANETs, που οδήγησαν στην ομάδα προτύπων IEEE 1609 «Wireless Access in Vehicular Environment (WAVE)») [78]. Στο πλαίσιο της mIBC, τα πιστοποιημένα ψευδώνυμα που προτείνουμε δίνουν σ' ένα σκάφος τη δυνατότητα να διατηρεί την ανωνυμια του στις μεταδόσεις AIS όποτε το επιθυμεί. Όμως, στο παγκόσμιο περιβάλλον της ναυτιλίας πολλοί θα ήταν αυτοί που θα επιθυμούσαν να κρύψουν παράτυπες ή παράνομες ενέργειες κάτω από την ανωνυμια ενός πιστοποιημένου νομότυπου ψευδώνυμου. Αυτός είναι ο λόγος που στην πρότασή μας, χρησιμοποιώντας τις ιδιότητες της KBT, τα ψευδώνυμα δημιουργούνται και πιστοποιούνται από τις αρχές· κατά συνέπεια, οι αρχές ανά πάσα στιγμή θα είναι τεχνικά έτοιμες να προσδιορίσουν την πραγματική ταυτότητα τους σκάφους.

Τα χαρακτηριστικά των ψευδωνύμων ψευδο-MMSI είναι:



Σχήμα 6.9: Πιθανή κανονιστική δομή της υποδομής Maritime IBC (mIBC)

- Τα ψευδώνυμα (ψευδο-MMSI) ακολουθούν τη γενική μορφή των MMSI, ώστε να είναι συμβατά με το πρωτόκολλο του AIS, αλλά έχουν κάποιο χαρακτηριστικό συνδυασμό αριθμών που δηλώνει ότι είναι ψευδώνυμα.
- Τα ψευδο-MMSI δημιουργούνται από τις αρχές και υπογράφονται ψηφιακά από τους αντίστοιχους ΑΚΣ. Έτσι οι αρχές γνωρίζουν την αντιστοιχία των ψευδο-MMSI με την πραγματική ταυτότητα των σκαφών.
- Τα σκάφη στην περιοχή που λαμβάνουν τα σήματα AIS με το ψευδώνυμο ψευδο-MMSI μπορούν να πιστοποιήσουν την εγκυρότητά του. Συνεπώς, αν και δεν γνωρίζουν το όνομα του σκάφους, γνωρίζουν ότι είναι νόμιμο και ότι οι αρχές μπορούν να το ταυτοποιήσουν.
- Τα σκάφη που χρησιμοποιούν τα ψευδώνυμα σε συνδυασμό με τον τρόπο λειτουργίας mIBC-Authenticated-AIS (mode 2) δεν μπορούν να αμφισβητήσουν την αποστολή τους. Συνεπώς, τα ψευδο-MMSI δεν μπορούν να χρησιμοποιηθούν για απόκρυψη παράνομων πράξεων.

Η διαδικασία απόκτησης ψευδο-MMSI έχει ως εξής:

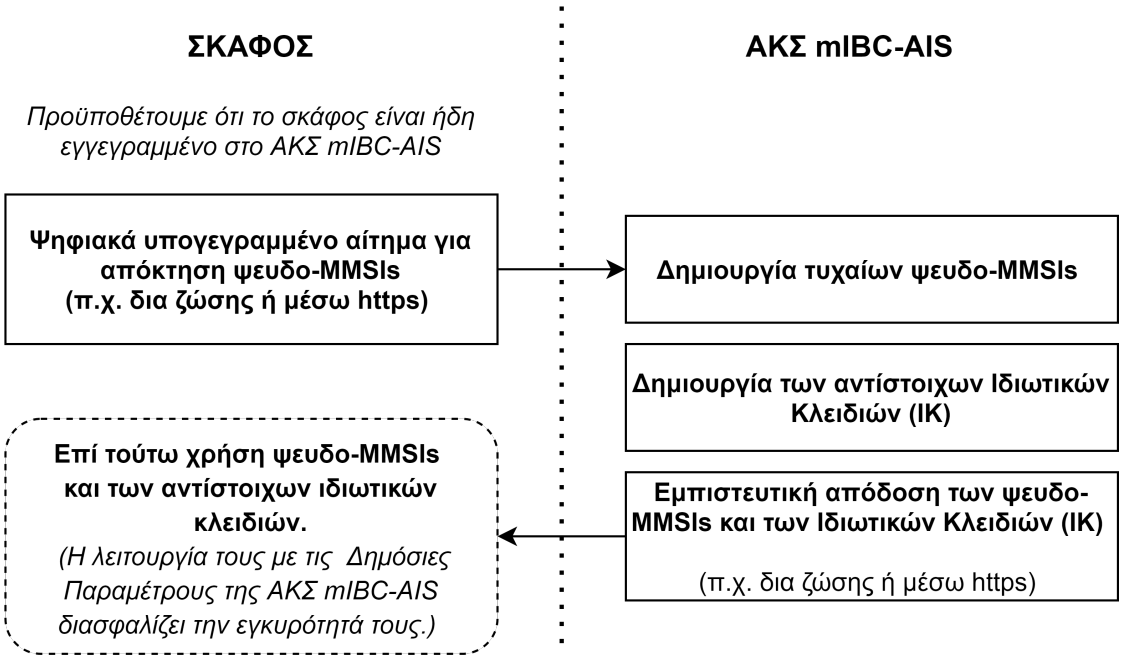
- Ο ΑΚΣ μιας αρχής δημιουργίας ιδιωτικού κλειδιού mIBC δημιουργεί ψευδο-MMSI τα οποία διαθέτουν ένα τυπικό πρόθεμα (π.χ. ¨000-¨) ώστε να διακρίνονται από τα πραγματικά, και έχουν εννέα ψηφία προκειμένου να διασφαλιστεί η συμβατότητα με το υπάρχον πρωτόκολλο AIS. Εναλλακτικά, μπορεί να χρησιμοποιηθεί ως σημαία ένα εφεδρικό bit, το οποίο υπάρχει στα μηνύματα του AIS τύπου 6 και 8 που θα αποτελέσουν τους φορείς των δεδομένων του mIBC-AIS. Σε κάθε περίπτωση οι λεπτομέρειες είναι θέμα διευθέτησης από τους διεθνείς ναυτιλιακούς οργανισμούς.
- Σκάφος που θέλει να χρησιμοποιήσει τις υπηρεσίες ψευδωνυμιας ταυτοποιείται στον ΑΚΣ και παραλαμβάνει τυχαία ψευδο-MMSI μαζί με τα αντίστοιχα ιδιωτικά κλειδιά τους. Μία πιθανή ροή διαδικασιών παρουσιάζεται στο Σχήμα 6.10, όπου ένα τυχαίο σκάφος επικοινωνεί με τον ΑΚΣ που λειτουργεί στην υποδομή του εθνικού mIBC-AIS του νηογνώμονα, προκειμένου να αποκτήσει ψευδο-MMSI.

Σενάριο χρήσης της υπηρεσίας διατήρησης ανωνυμιας

Ναυτιλιακή εταιρεία παρακολουθεί ολόκληρο τον στόλο της σε όλο τον κόσμο μέσω του AIS, αλλά αυτά τα δεδομένα είναι διαθέσιμα και στο κοινό μέσω του διαδικτύου. Λόγω ορισμένων ευαίσθητων φορτίων, η ναυτιλιακή εταιρεία θέλει συγκεκριμένα πλοία του στόλου της να ελέγχουν τα δεδομένα AIS που γνωστοποιούνται δημόσια. Ο έλεγχος των πληροφοριών AIS είναι αδύνατος σήμερα, οπότε είτε το AIS είναι απενεργοποιημένο είτε τα δεδομένα AIS είναι δημόσια διαθέσιμα.

Ωστόσο, με χρήση της υπηρεσίας διατήρησης ανωνυμιας της υποδομής mIBC-IS, η ναυτιλιακή εταιρεία εφαρμόζει την ακόλουθη πολιτική:

1. Τα πλοία της θα αποκτήσουν και θα χρησιμοποιούν ψευδο-MMSI στις μεταδόσεις AIS τους.
2. Θα κρυπτογραφεί τα δεδομένα που σχετίζονται με την ασφάλεια πλοήγησης AIS με το δημόσιο κλειδί της εταιρείας, χρησιμοποιώντας τη μερικώς



Σχήμα 6.10: Διαδικασία απόκτησης ψευδο-MMSI

κρυπτογραφημένη λειτουργία AIS, υποθέτοντας ότι η εταιρεία έχει προμηθευτεί και αυτή ψευδο-MMSI με το αντίστοιχο ιδιωτικό κλειδί.

3. Τα δεδομένα AIS που σχετίζονται με την ασφάλεια της ναυσιπλοΐας και μόνο θα μένουν μη κρυπτογραφημένα.

Έτσι, τα διαθέσιμα στο κοινό δεδομένα AIS είναι εκείνα που σχετίζονται με την ασφάλεια πλοήγησης, αλλά λόγω των ψευδο-MMSI, είναι δύσκολο για κάποιον να τα συνδέσει με την πραγματική ταυτότητα του πλοίου. Μόνο η ναυτιλιακή εταιρεία μπορεί να χρησιμοποιήσει το ιδιωτικό κλειδί της για να αποκρυπτογραφήσει τα κρυπτογραφημένα δεδομένα AIS που μεταδίδονται από τα πλοία του στόλου της που μεταφέρουν ευαίσθητο φορτίο. Ως εκ τούτου, η ναυτιλιακή εταιρεία μπορεί να ελέγξει τη διάδοση πληροφοριών σχετικά με τον στόλο της, προστατεύοντας παράλληλα την ασφάλεια της ναυσιπλοΐας.

Ωστόσο, η ακτοφυλακή εντοπίζει μια διαρροή πετρελαίου στη διαδρομή ενός σκάφους. Αν και δεν μπορεί να ξέρει από το ψευδο-MMSI την ταυτότητα του σκάφους, γνωρίζει λόγω των ψηφιακά υπογεγραμμένων μηνυμάτων σε ποια αρχή θα πρέπει να απευθυνθεί προκειμένου να αποκαλυφθεί η πραγματική ταυτότητα του σκάφους. Θυμίζουμε ότι:

- Τα εκδιδόμενα ψευδο-MMSI καταγράφονται και αρχειοθετούνται με ασφάλεια από τον εκδότη τους.
- Ο τρόπος λειτουργίας mIBC-Anonymous-AIS (mode 3) είναι ίδιος με τον mIBC-Authenticated-AIS (mode 2), με τη διαφορά ότι χρησιμοποιεί ψευδο-MMSI αντί για το πραγματικό MMSI των πλοίων, δηλαδή τα μηνύματα του AIS είναι ψηφιακά υπογεγραμμένα με το ιδιωτικό κλειδί που αντιστοιχεί στο ψευδο-MMSI.

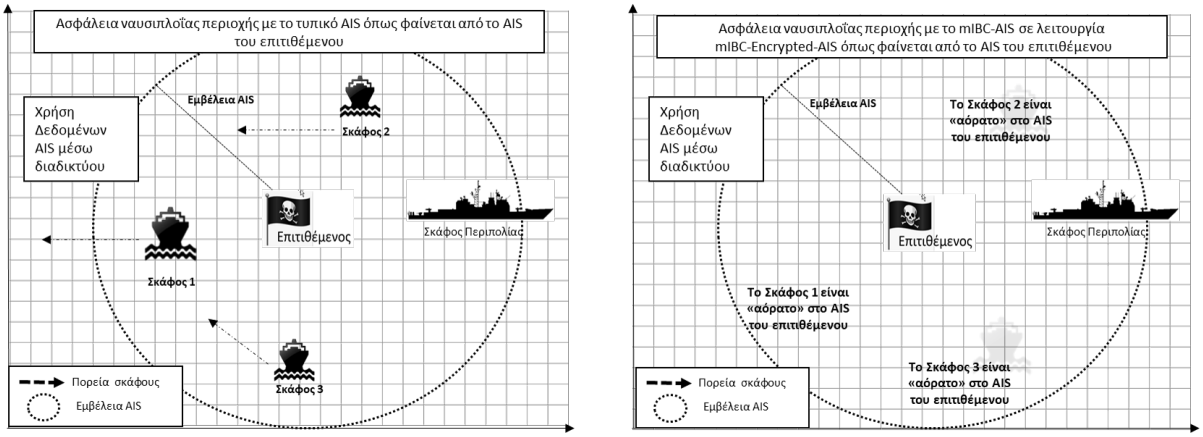
6.6.2 Κρυπτογραφημένη λειτουργία AIS σε επισφαλείς θαλάσσιες περιοχές

Στόχος μας είναι να δώσουμε μια εναλλακτική λύση ασφαλούς ναυσιπλοΐας αντί για την απενεργοποίηση του AIS, όπως υπαγορεύουν οι οδηγίες του IMO όταν υπάρχουν ανησυχίες σχετικά με την ασφάλεια του πλοίου. Όπως έχουμε προαναφέρει, ο τελικός στόχος μας είναι να αποτρέψουμε την απενεργοποίηση του AIS σε επισφαλείς θαλάσσιες περιοχές, δίνοντας τη δυνατότητα μετάδοσης κρυπτογραφημένων μηνυμάτων AIS τα οποία, ενώ όλοι θα τα λαμβάνουν, μόνο έμπιστοι λήπτες θα έχουν τη δυνατότητα αποκρυπτογράφησής τους. Όμως, η κυκλοφορία στις επισφαλείς θαλάσσιες περιοχές δεν είναι προκαθορισμένη· αρκετά σκάφη μπορεί να εισέρχονται σε μια επισφαλή θαλάσσια περιοχή, ενώ άλλα να την εγκαταλείπουν. Σ' αυτές τις θαλάσσιες περιοχές δημιουργούνται προσωρινά, μεταβλητά, επί τούτω, AISANETs.

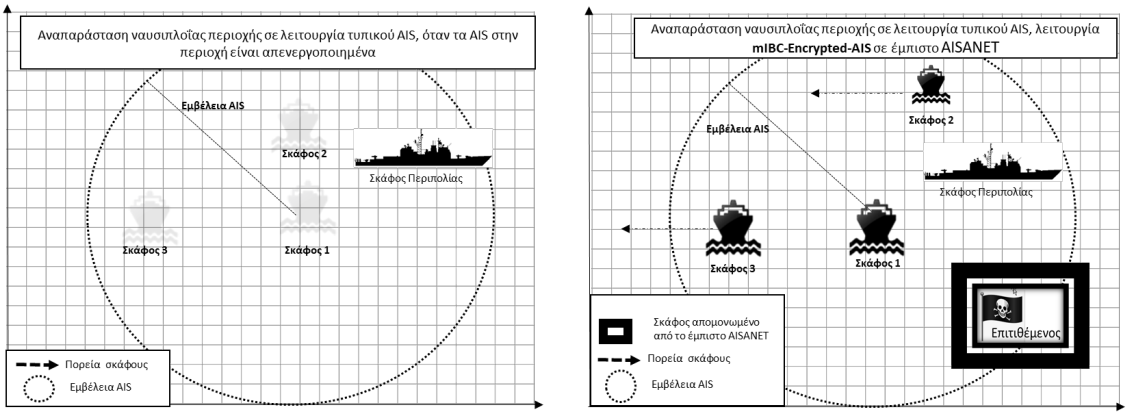
Ωστόσο, είναι αδύνατο να προκαθορίσουμε όλα τα νόμιμα σκάφη, επειδή η υπόθεση ότι ένα επίσημα νηολογημένο πλοίο είναι και έμπιστο δεν είναι ρεαλιστική. Έτσι, επικεντρωνόμαστε στη χρήση του κρυπτογραφημένου AIS μόνο σε επίσημα δηλωμένες επισφαλείς θαλάσσιες περιοχές. Υπενθυμίζουμε ότι, όπως συζητήσαμε στην ενότητα 6.4, μέσα σ' αυτές τις περιοχές, μια αρχή επιβολής του νόμου (π.χ. ένα περιπολικό σκάφος ή αεροσκάφος) θα έχει το ρόλο του Έμπιστου Τρίτου Μέρους (ETM) που θα είναι επιφορτισμένο να διακρίνει τα έμπιστα πλοία (π.χ. φορτηγά πλοία) από τα ύποπτα (π.χ. θαλάσσιοι πειρατές). Αυτό θα επιτρέψει τη διανομή, από το Έμπιστο Τρίτο Μέρος (ETM), ενός συμμετρικού κλειδιού συνόδου στα θεωρούμενα ως έμπιστα πλοία, προκειμένου αυτά να μπορούν να στέλνουν κρυπτογραφημένα μηνύματα AIS σε τρόπο λειτουργίας mIBC-AES-AIS (mode 5), δημιουργώντας έτσι έμπιστα AISANETs.

Είναι αυτονόητο ότι τα ύποπτα σκάφη που δεν θα έχουν λάβει το συμμετρικό κλειδί συνόδου δεν θα έχουν τη δυνατότητα αποκρυπτογράφησης αυτών των μηνυμάτων. Συνεπώς, τα πληρώματα δεν απενεργοποιούν το AIS και η ασφάλεια της ναυσιπλοΐας προστατεύεται χωρίς να δίνονται πληροφορίες σε εν δυνάμει επιτιθέμενους. Η συμμετρική κρυπτογραφία χρησιμοποιείται ήδη σε εμπορικά προϊόντα AIS [79] και από ορισμένες ακτοφυλακές σε όλο τον κόσμο. Ωστόσο, αυτές οι υλοποιήσεις χρησιμοποιούνται για την ασφαλή επικοινωνία AIS μεταξύ προκαθορισμένων σκαφών (blue force), π.χ. τα σκάφη της ακτοφυλακής. Σε αντίστιξη, επιθυμούμε να χρησιμοποιήσουμε το κρυπτογραφημένο AIS σε μεταβλητά, βραχύβια, επί τούτω, έμπιστα AISANETs στην περιοχή. Προς το σκοπό αυτό, προτείνουμε τη χρήση υβριδικής κρυπτογραφίας, δηλαδή τη χρήση του mIBC-Confidential-AIS (mode 4) για τη διανομή του συμμετρικού κλειδιού συνόδου στα σκάφη των έμπιστων AISANETs της περιοχής.

Στην αριστερή πλευρά του Σχήματος 6.11 παρατίθεται μια εικονική άποψη των πληροφοριών που διαθέτει ένας επιτιθέμενος χάρη στο AIS όπως λειτουργεί σήμερα, ενώ στη δεξιά πλευρά η ίδια εικόνα όπως θα είναι όταν χρησιμοποιείται το mIBC-AES-AIS (mode 5) σε έμπιστα AISANETs. Στην δεύτερη περίπτωση κρυπτογραφείται όλη η επικοινωνία AIS μεταξύ των σκαφών του έμπιστου AISANET. Δεδομένου ότι ο ύποπτος δεν διαθέτει το συμμετρικό κλειδί συνόδου, δεν δύναται να αποκρυπτογραφήσει τα μηνύματα AIS που ανήκουν στα σκάφη του έμπιστου AISANET και συνεπώς αυτά είναι αόρατα όσον αφορά το AIS.



Σχήμα 6.11: Εικονική άποψη των πληροφοριών που διαθέτει ένας επιτιθέμενος με: τυπικό AIS(1α), και με λειτουργία mIBC-Encrypted-AIS (1β) στα έμπιστα AISANET



Σχήμα 6.12: Εικονική άποψη των πληροφοριών που διαθέτει ένα σκάφος σε επισφαλή θαλάσσια περιοχή όταν τα σκάφη έχουν απενεργοποιημένο το AIS (αριστερά) και όταν ανήκουν σε έμπιστα AISANET σε λειτουργία mIBC-AES-AIS (mode 5) (δεξιά)

Σε αντιπαραβολή, η επίδραση στην ασφάλεια της ναυσιπλοΐας αποτυπώνεται στο Σχήμα 6.12, όπου παρατίθεται μια εικονική άποψη της ναυσιπλοΐας, εάν τα σκάφη στην περιοχή απενεργοποιούσαν τα AIS, φοβούμενα μήπως δώσουν πληροφορίες σε κάποιον επιτιθέμενο (αριστερή πλευρά), και η εικόνα που θα έχουν τα σκάφη του έμπιστου AISANET, και μόνο, εάν χρησιμοποιείται το mIBC-AES-AIS (mode 5) (δεξιά πλευρά).

6.7 Τα μηνύματα mIBC-AIS

Με στόχο την ικανοποίηση της προδιαγραφής ότι οι νέες δυνατότητες που προσφέρει η υποδομή mIBC-AIS πρέπει να λειτουργούν χωρίς τροποποίηση του τρέχοντος πρωτοκόλλου AIS, η εφαρμογή ¨mIBC-AIS-App¨ χρησιμοποιείται ως διεπαφή μεταξύ της υποδομής mIBC-AIS και της υπάρχουσας υποδομής AIS. Όπως θα δούμε στην ενότητα 6.7.4, χρησιμοποιούμε το πρωτόκολλο AIS ως υποκείμενο πρωτόκολλο μεταφοράς για τη μετάδοση των υπογεγραμμένων / κρυπτογραφημένων δεδομένων mIBC-AIS. Συγκεκριμένα, τα δεδομένα mIBC-AIS ενθυλακώνονται από την εφαρμογή mIBC-AIS-App ως δεδομένα σ' έναν ειδικό τύπο υπαρχόντων μηνυμάτων AIS τύπου 6

και 8. Όπως θα δούμε, τα τελευταία είναι ειδικά μηνύματα AIS που επιτρέπουν την ενθυλάκωση δεδομένων για χρήση από τρίτες εφαρμογές, που δεν σχετίζονται με το AIS.

Η mIBC-AIS-App του αποστολέα δημιουργεί τα κατάλληλα δεδομένα mIBC-AIS και στη συνέχεια τα ενσωματώνει στα ειδικά μηνύματα AIS (τύπου 6, 8) που μεταδίδονται μέσω της τυπικής υποδομής AIS. Στο άλλο άκρο, ο δέκτης mIBC-AIS-App αποθυλακώνει και επεξεργάζεται τα ληφθέντα δεδομένα του mIBC-AIS. Ανάλογη μεθοδολογία στα δίκτυα είναι η ενθυλάκωση των δεδομένων του Transmission Control Protocol (TCP) μέσα στα πακέτα του Internet Protocol (IP).

6.7.1 Δομή των μηνυμάτων του AIS

Το AIS ορίζει 27 διαφορετικούς τύπους μηνυμάτων AIS. Σε κάθε τύπο αντιστοιχεί ένας κωδικός τύπου μηνύματος (Message-ID) [80]. Για παράδειγμα, τα μηνύματα με κωδικό τύπου 1, 2 και 3 είναι μηνύματα αναφοράς της θέσης του σκάφους, εκείνα με κωδικό τύπου 4 είναι μηνύματα αναφοράς σταθμού βάσης, με κωδικό τύπου 21 είναι αναφοράς σταθμού βοήθειας προς πλοήγηση (AtoN) κλπ.

Το AIS εκπέμπει σε αλυσίδες χρονοθυρίδων με συγκεκριμένο όριο μεταφοράς δεδομένων κάθε φορά. Εννοιολογικά όμως, ανάλογα με το μέγεθος των δεδομένων, ένα μήνυμα AIS μπορεί να αποτελείται από τα δεδομένα μιας χρονοθυρίδας ή από τη σύνθεση δεδομένων έως και πέντε χρονοθυρίδων το πολύ. Εν γένει, αφαιρώντας τα δεδομένα του ίδιου του AIS, το τελικό ωφέλιμο φορτίο δεδομένων προς μεταφορά σε κάθε χρονοθυρίδα είναι 168 bits. Όμως υπάρχουν ειδικοί τύποι μηνυμάτων AIS (π.χ. τα "AIS ADDRESSED BINARY MESSAGE", με κωδικό τύπου 6 και "AIS BINARY BROADCAST MESSAGE", με κωδικό τύπου 8), που έχουν τη δυνατότητα να χρησιμοποιήσουν το μέγιστο των 5 χρονοθυρίδων και να προσφέρουν συνολικά περίπου 900 bits δεδομένων ωφέλιμου φορτίου. Τα συγκεκριμένα μηνύματα είναι αυτά που χρησιμοποιούμε, μέσω της mIBC-AIS-App, προκειμένου να υλοποιήσουμε την υποδομή mIBC-AIS.

Το πρωτόκολλο του AIS υπαγορεύει την ακριβή δομή κάθε μηνύματος. Η δομή περιλαμβάνει γενικές παραμέτρους (πεδία) που βρίσκονται σε όλα τα μηνύματα AIS (π.χ. Αναγνωριστικό μηνύματος (έως 6 bits), αριθμός MMSI (έως 30 bits), κ.λπ.) και ειδικές παραμέτρους για συγκεκριμένα μηνύματα (π.χ. Χρονική σήμανση (έως 6 bits), Κατάσταση πλοήγησης (5 bits), Ρυθμός στροφής (έως 8 bits) κλπ.). Τα μηνύματα AIS περιλαμβάνουν μια χρονική σήμανση (έως 6 bits) σε ακρίβεια δευτερολέπτου της συντονισμένης παγκόσμιας ώρας (UTC), που δημιουργείται από το ηλεκτρονικό σύστημα καθορισμού θέσης (EPFS).

Ένα παράδειγμα της δομής ενός τυπικού μηνύματος αναφοράς θέσης AIS κλάσης Α (τύπος 21) φαίνεται στον Πίνακα 6.2.

6.7.2 Το μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6)

Το μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) προσφέρει ωφέλιμο χώρο 920 bits για δεδομένα τρίτων εφαρμογών που απευθύνονται σ' έναν συγκεκριμένο αποδέκτη, δηλαδή, όλες οι συσκευές AIS που δεν θα έχουν το συγκεκριμένο MMSI

Παράμετροι	**Bits**	**Περιγραφή**
Τύπος	1	Το αναγνωριστικό του μηνύματος
MMSI	30	MMSI
Κατάσταση ναυσιπλοΐας	4	0 = πορεία με χρήση μηχανής· 1 = αγκυροβολημένο· 2 = ακυβέρνητο· 3 = περιορισμένη δυνατότητα ελιγμών· 4 = παρεμποδίζεται από το βύθισμά του· 5 = προσδεδεμένο· 6 = προσαραγμένο κλπ.
Ρυθμός στροφής (ROT)	8	0 - +126 = δεξιά στροφή έως και 708 μοίρες ανά λεπτό ή υψηλότερο, κλπ.
Ταχύτητα σε σχέση με τον βυθό (SOG)	10	Ταχύτητα σε σχέση με τον βυθό (0-102.2 κόμβοι)
Ακρίβεια θέσης	1	1 = υψηλή, (<= 10 μ), 0 = χαμηλή (> 10 μ)
Γεωγραφικό μήκος	28	Γεωγραφικό μήκος σε 1/10000 λεπτά
Γεωγραφικό πλάτος	27	Γεωγραφικό πλάτος σε 1/10000 λεπτά
Πορεία σε σχέση με τον βυθό (COG)	12	Πορεία σε σχέση με τον βυθό 1/10 = (0-3599).
Αληθής κατεύθυνση	9	Μοίρες (0-359)
Χρονοσήμανση	6	Δευτερόλεπτο Συντονισμένης Παγκόσμιας Ώρας (UTC)
Ειδικός δείκτης ελιγμών	2	0 = μη διαθέσιμο = προεπιλογή, 1 = δεν εκτελεί ειδικό ελιγμό, 2 = εκτελεί ειδικό ελιγμό
Εφεδρικό	3	Δεν χρησιμοποιείται. Πρέπει να οριστεί ίσο με το μηδέν. Διατηρείται για μελλοντική χρήση.
Receiver autonomous integrity monitoring (RAIM)	1	Κωδικός ακεραιότητας του προσδιορισμού θέσης μέσω GPS.
Κατάσταση επικοινωνίας	19	καθορίζεται από το Rec. ITU-R M.1371-5 Table 49
Συνολικά bits	**168**	

Πίνακας 6.2: Παράδειγμα τυπικού σήματος AIS Κλάσης Α τύπου 1 αναφοράς προόδου θέσης πλοίου.

Παράμετροι	**Bits**	**Περιγραφή**		
Τύπος	6	Το αναγνωριστικό του μηνύματος 6		
Δείκτης επανάληψης	2	Υποδεικνύει πόσες φορές έχει επαναληφθεί ένα μήνυμα 0-3, προεπιλογή = 0, 3 = να μην επαναλαμβάνεται πλέον		
Σταθμός Προέλευσης	30	Αριθμός MMSI του σταθμού προέλευσης		
Αριθμός ακολουθίας	2	0-3		
Σταθμός προορισμού	30	Αριθμός MMSI του σταθμού προορισμού		
Σημαία επανάληψης διαβίβασης	1	0 = μη επανάληψη διαβίβασης = εξ ορισμού· 1 = επανάληψη διαβίβασης		
Εφεδρικό	1	Δεν χρησιμοποιείται. Πρέπει να οριστεί ίσο με το μηδέν. Διατηρείται για μελλοντική χρήση.		
Δυαδικά δεδομένα	Μεγ. 936	Αναγνωριστικό εφαρμογής	16 bits	**mIBC-AIS-App ID**
		Ενθυλακωμένα δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 920 bits	Δεδομένα mIBC-Confidential-AIS (mode 4)
Μέγ. bits	Μεγ. 1008	Καταλαμβάνει 3-5 χρονοθυρίδες		

Πίνακας 6.3: Μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) με ενθυλακωμένα δεδομένα mIBC-Confidential-AIS (mode 4)

αποδέκτη θα απορρίψουν το λαμβανόμενο μήνυμα. Λεπτομέρειες της δομής ενός τέτοιου μηνύματος βλέπουμε στον Πίνακα 6.3, ο οποίος απεικονίζει ένα τυπικό μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) με δεδομένα της εφαρμογής mIBC-AIS-App ενθυλακωμένα στην ενότητα ¨Δυαδικά δεδομένα¨. Αυτός ο τύπος μηνύματος θα χρησιμοποιείται για την αποστολή των AIS μηνυμάτων του τύπου λειτουργίας mIBC-Confidential-AIS (mode 4).

Σύμφωνα με τις προδιαγραφές των μηνυμάτων τύπου 6, η εφαρμογή που δηλώνεται στο πεδίο ¨Αναγνωριστικό εφαρμογής¨ είναι υπεύθυνη για τη διαχείριση των ενθυλακωμένων δεδομένων στο πεδίο ¨Δεδομένα εφαρμογής¨. Στην περίπτωση του mIBC-AIS, χρησιμοποιούμε το ¨Αναγνωριστικό εφαρμογής¨ για να δηλώσουμε την εφαρμογή mIBC-AIS-App ως τη διαχειρίστρια εφαρμογή των ενθυλακωμένων δεδομένων στο πεδίο «Δυαδικά δεδομένα». Επισημαίνουμε ότι η υποδομή του AIS δεν αλληλεπιδρά με τα δεδομένα στο πεδίο αυτό.

6.7.3 Το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπος 8)

Το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπος 8) προσφέρει ωφέλιμο χώρο περίπου 960 bits για δεδομένα τρίτων εφαρμογών που εκπέμπονται προς όλους, δηλαδή, όλες οι συσκευές AIS αποδέχονται το λαμβανόμενο μήνυμα. Λεπτομέρειες

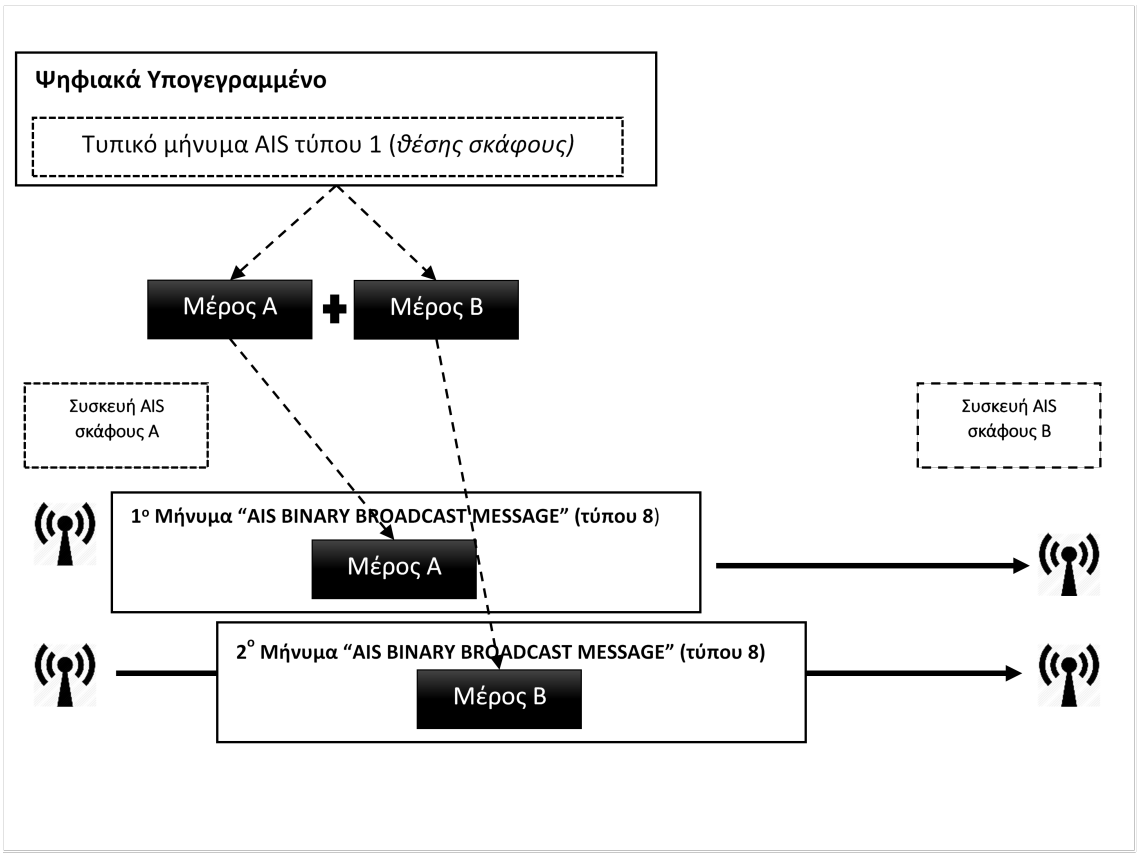
Παράμετροι	**Bits**	**Περιγραφή**		
Τύπος	8	Το αναγνωριστικό του μηνύματος 8		
Δείκτης επανάληψης	2	Υποδεικνύει πόσες φορές έχει επαναληφθεί ένα μήνυμα 0-3, προεπιλογή = 0, 3 = να μην επαναλαμβάνεται πλέον		
Σταθμός Προέλευσης	30	Αριθμός MMSI του σταθμού προέλευσης		
Αριθμός ακολουθίας	2	0-3		
Σημαία επανάληψης διαβίβασης	1	0 = μη επανάληψη διαβίβασης = εξ ορισμού· 1 = επανάληψη διαβίβασης		
Εφεδρικό	1	Δεν χρησιμοποιείται. Πρέπει να οριστεί ίσο με το μηδέν. Διατηρείται για μελλοντική χρήση.		
Δυαδικά δεδομένα	Μεγ. 968	Αναγνωριστικό εφαρμογής	16 bits	**mIBC-AIS-App ID**
		Ενθυλακωμένα δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 952 bits	Δεδομένα των: mIBC-Authenticated-AIS (mode 2), mIBC-AES-AIS (mode 5)
Μέγ. bits	Μεγ. 1008	Καταλαμβάνει 3-5 χρονοθυρίδες		

Πίνακας 6.4: Μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 8) με ενθυλακωμένα δεδομένα των τρόπων λειτουργίας mIBC-Authenticated-AIS (mode 2) και mIBC-AES-AIS (mode 5)

της δομής ενός τέτοιου μηνύματος βλέπουμε στον Πίνακα 6.4, ο οποίος απεικονίζει ένα τυπικό μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπος 8) με δεδομένα της εφαρμογής mIBC-AIS-App ενθυλακωμένα στην ενότητα ¨Δυαδικά δεδομένα¨. Αυτός ο τύπος μηνύματος θα χρησιμοποιείται στους τρόπους λειτουργίας mIBC-Authenticated-AIS (mode 2) και mIBC-AES-AIS (mode 5). Σημειώνουμε ότι είναι ακριβώς το ίδιο μήνυμα με το AIS ADDRESSED BINARY MESSAGE (Τύπος 6), χωρίς διεύθυνση παραλήπτη· γι' αυτό διαθέτει περισσότερα bits για τα ενθυλακωμένα δεδομένα.

6.7.4 Μεταφορά των δεδομένων mIBC-AIS μέσω των μηνυμάτων AIS τύπου 6, 8

Όπως προαναφέραμε, τα δεδομένα mIBC-AIS δεν χωρούν σε μια χρονοθυρίδα AIS, συνεπώς θα πρέπει να χρησιμοποιούνται περισσότερες. Όπως θα δούμε στην πειραματική υλοποίηση της υποδομής mIBC-AIS, στο Κεφάλαιο 8, χρειαζόμαστε από 3 έως 5 χρονοθυρίδες. Το πρωτόκολλο του AIS -και επομένως οι συσκευές AIS- δίνουν τη δυνατότητα σύνθεσης των δεδομένων που μεταφέρονται μέχρι και σε 5 χρονοθυρίδες, όπως φαίνεται στο Σχήμα 6.13. Ακόμα όμως και εάν σε ειδικές περιπτώσεις χρειαστεί να χρησιμοποιήσουμε παραπάνω από 5 χρονοθυρίδες, επομένως 2 μηνύματα AIS τύπου 6, 8, η εφαρμογή mIBC-AIS-app έχει τη δυνατότητα να συνθέσει τα δεδομένα του mIBC-AIS.



Σχήμα 6.13: Μεταφορά των δεδομένων mIBC-Authenticated-AIS (mode 2): Ψηφιακά υπογεγραμμένο μήνυμα AIS (τύπου 1) ενθυλακωμένο σε δύο μηνύματα AIS τύπου 8, ενότητα 6.5

Παράμετροι	**Bits**	**Περιγραφή**		
Τύπος	6	Το αναγνωριστικό του μηνύματος 8		
Σταθμός Προέλευσης	30	Αριθμός MMSI του σταθμού προέλευσης. Θα διασταυρώνεται με τον ψηφιακά υπογεγραμμένο MMSI από την mIBC-AIS-App		
Ενθυλακωμένα Δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 968	Κωδικός Εφαρμογής	16 bits	Κωδικός mIBC-AIS-App
		Δεδομένα mIBC-AIS-App	μεγ. 952 bits	**Δεδομένα mIBC-AIS-App σε λειτουργία mIBC-Authenticated-AIS (mode 2) Μέρος 1/2** • Δεδομένα προς την εφαρμογή mIBC-AIS-App με τον αριθμό των μηνυμάτων "AIS BINARY BROADCAST MESSAGE" (τύπου 8) που θα αποτελούν την ψηφιακή υπογραφή. Σ' αυτό το παράδειγμα θα είναι 2. • Το αρχικό μήνυμα AIS τύπου 1 που υπογράφεται ψηφιακά. • Τα δεδομένα της ψηφιακής υπογραφής. (Μέρος 1ο)

Πίνακας 6.5: Παράδειγμα δομής μηνύματος "AIS BINARY BROADCAST MESSAGE" (τύπου 8) που ενθυλακώνει ψηφιακά υπογεγραμμένο μήνυμα σε λειτουργία mIBC-Authenticated-AIS (mode 2)

Στους πίνακες 6.5 και 6.6 φαίνονται παραδείγματα της δομής των δύο μηνυμάτων "AIS BINARY BROADCAST MESSAGE" (τύπου 8), τα οποία θα μεταφέρουν δεδομένα του mIBC-Authenticated-AIS (mode 2). Στους πίνακες 6.7 και 6.8 φαίνονται παραδείγματα της δομής των δύο μηνυμάτων "AIS BINARY ADDRESSED MESSAGE" (τύπου 6), τα οποία θα μεταφέρουν δεδομένα του mIBC-Confidential-AIS (mode 4). Για λόγους εξοικονόμησης χώρου, παραλείπονται παράμετροι που δεν σχετίζονται με το mIBC-AIS.

6.8 Η εφαρμογή mIBC-AIS-App

Ο κώδικας της εφαρμογής mIBC-AIS-App μπορεί να ενσωματωθεί στις υπάρχουσες συσκευές AIS είτε μέσω ενημέρωσης του υλικολογισμικού είτε σε ξεχωριστό υλικό που θα συνδεθεί μεταξύ της συσκευής AIS και της κεραίας. Λειτουργεί ως ενδιάμεσος που είτε απλά προωθεί (transparent) τυπικά μηνύματα AIS, είτε αναλαμβάνει τη διαχείρισή τους εάν είναι μηνύματα mIBC-AIS. Η mIBC-AIS-App έχει την αποκλειστική ευθύνη για την ενθυλάκωση, αποθυλάκωση, και όλες τις κρυπτογραφικές λειτουργίες τις σχετικές με τα μηνύματα mIBC-AIS.

Παράμετροι	**Bits**	**Περιγραφή**		
Τύπος	6	Το αναγνωριστικό του μηνύματος 8		
Σταθμός Προέλευσης	30	Αριθμός MMSI του σταθμού προέλευσης. Θα διασταυρώνεται με τον ψηφιακά υπογεγραμμένο MMSI από την mIBC-AIS-App		
Ενθυλακωμένα Δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 968	Κωδικός Εφαρμογής	16 bits	Κωδικός mIBC-AIS-App
		Δεδομένα mIBC-AIS-App	μεγ. 952 bits	**Δεδομένα mIBC-AIS-App σε λειτουργία mIBC-Authenticated-AIS (mode 2) Μέρος 2/2** • Δεδομένα προς την εφαρμογή mIBC-AIS-App με τον αριθμό των μηνυμάτων "AIS BINARY BROADCAST MESSAGE" (τύπου 8) που θα αποτελούν την ψηφιακή υπογραφή. Σε αυτό το παράδειγμα θα είναι 2. • Τα δεδομένα της ψηφιακής υπογραφής. (Μέρος 2ο)

Πίνακας 6.6: Παράδειγμα δομής μηνύματος "AIS BINARY BROADCAST MESSAGE" (τύπου 8) με ψηφιακά υπογεγραμμένο μήνυμα σε λειτουργία mIBC-Authenticated-AIS (mode 2)

Παράμ.	**Bits**	**Περιγραφή**			Κατάσταση
Τύπος	6	Το αναγνωριστικό του μηνύματος 6			Ανοιχτά
Σταθμός Προέλευσης	30	Αριθμός MMSI του σταθμού προέλευσης. Θα διασταυρώνεται με το MMSI στο κρυπτογραφημένο αρχικό μηνυμα από την mIBC-AIS-App			Ανοιχτά
Ενθυλακ. Δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 936	Κωδικός Εφαρμογής	16 bits	Κωδικός mIBC-AIS-App	Ανοιχτά
		Δεδομένα mIBC-AIS-App	μεγ. 920 bits	**Δεδομένα mIBC-AIS-App σε λειτουργία mIBC-Confidential-AIS (mode 4) Μέρος 1/2** Δεδομένα προς την εφαρμογή mIBC-AIS-App με τον αριθμό των μηνυμάτων "AIS BINARY ADDRESSED MESSAGE" (τύπου 6) που θα αποτελούν το κρυπτογραφημένο μήνυμα. Σ' αυτό το παράδειγμα θα είναι 1/2. Τα κρυπτογραφημένα δεδομένα. (Μέρος 1ο)	Ανοιχτά Κρυπτογρ.

Πίνακας 6.7: Παράδειγμα δομής του 1ου μηνύματος "AIS BINARY ADDRESSED MESSAGE" (τύπου 6) που ενθυλακώνει ένα κρυπτογραφημένο μήνυμα σε λειτουργία mIBC-Confidential-AIS (mode 4)

Παράμ.	**Bits**	**Περιγραφή**			Κατάσταση
Τύπος	6	Το αναγνωριστικό του μηνύματος 6			Ανοιχτά
Σταθμός Προέλευση	30	Αριθμός MMSI του σταθμού προέλευσης. Θα διασταυρώνεται με το MMSI στο κρυπτογραφημένο αρχικό μηνυμα από την mIBC-AIS-App			Ανοιχτά
Ενθυλακ. Δεδομένα (Χρονοθυρίδες 1-5)	Μεγ. 936	Κωδικός Εφαρμογής	16 bits	Κωδικός mIBC-AIS-App	Ανοιχτά
		Δεδομένα mIBC-AIS-App	μεγ. 920 bits	**Δεδομένα mIBC-AIS-App σε λειτουργία mIBC-Confidential-AIS (mode 4) Μέρος 2/2** Δεδομένα προς την εφαρμογή mIBC-AIS-App με τον αριθμό των μηνυμάτων "AIS BINARY ADDRESSED MESSAGE" (τύπου 6) που θα αποτελούν το κρυπτογραφημένο μήνυμα. Σ' αυτό το παράδειγμα θα είναι 2. Τα κρυπτογραφημένα δεδομένα. (Μέρος 2ο)	Ανοιχτά Κρυπτογρ.

Πίνακας 6.8: Παράδειγμα δομής του 2ου μηνύματος "AIS BINARY ADDRESSED MESSAGE" (τύπου 6) που ενθυλακώνει ένα κρυπτογραφημένο μήνυμα σε λειτουργία mIBC-Confidential-AIS (mode 4)

6.8.1 Χειρισμός εξερχόμενου σήματος AIS

Η εφαρμογή mIBC-AIS-App χειρίζεται τα εξερχόμενα σήματα AIS ως εξής:

1. mIBC-AIS σε λειτουργία τυπικού AIS (mode 1): Η εφαρμογή mIBC-AIS-App απλά προωθεί τα σήματα προς την κεραία του AIS χωρίς να παρεμβαίνει.
2. mIBC-AIS σε λειτουργία mIBC-Authenticated-AIS (mode 2): Η εφαρμογή mIBC-AIS-App ανακόπτει το αρχικό σήμα και στη συνέχεια:
   (α΄) το υπογράφει ψηφιακά με το ιδιωτικό κλειδί του σκάφους
   (β΄) ενθυλακώνει το αρχικό μήνυμα μαζί με την ψηφιακή υπογραφή του σε ένα μήνυμα AIS τύπου AIS BROADCAST BINARY MESSAGE (Τύπος 8)
   (γ΄) προωθεί το δημιουργημένο μήνυμα AIS τύπου AIS BROADCAST BINARY MESSAGE (Τύπος 8) προς την κεραία για μετάδοση
3. mIBC-AIS σε λειτουργία mIBC-Anonymous-AIS (mode 3): Η εφαρμογή mIBC-AIS-App, υποθέτοντας ότι έχει πρόσβαση στο ψευδο-MMSI και τα αντίστοιχα κλειδιά του στην υποδομή ΚΒΤ στην οποία είναι εγγεγραμμένο το σκάφος, ανακόπτει το αρχικό σήμα και στη συνέχεια:
   (α΄) αντικαθιστά το αυθεντικό MMSI του σκάφους με το ψευδο-MMSI.
   (β΄) προωθεί το αλλαγμένο μήνυμα προς υπογραφή και μετάδοση στη λειτουργία mIBC-Authenticated-AIS (mode 2). Υπενθυμίζουμε ότι για λόγους ασφάλειας τα ψευδο-MMSIs πρέπει να είναι ψηφιακά υπογεγραμμένα, προκειμένου να πιστοποιείται η αυθεντικότητά τους.
4. mIBC-AIS σε λειτουργία mIBC-Confidential-AIS (mode 4): Υποθέτουμε ότι η εφαρμογή mIBC-AIS-App έχει πρόσβαση στα δημόσια δεδομένα της υποδομής ΚΒΤ στην οποία είναι εγγεγραμμένο το σκάφος στο οποίο αποστέλλεται το έμπιστο μήνυμα. Στη συνέχεια:
   (α΄) Το πλήρωμα έχει τη δυνατότητα να επιλέξει:
      i. είτε η εφαρμογή mIBC-AIS-App ανακόπτει κάποιο τυπικό σήμα AIS και διαβάζει τα δεδομένα του προκειμένου στη συνέχεια να τα εκπέμψει εμπιστευτικά .
      ii. είτε εισάγεται από το πλήρωμα απευθείας ένα εμπιστευτικό μήνυμα, άσχετο με το AIS, στην εφαρμογή mIBC-AIS-App προκειμένου να το εκπέμψει εμπιστευτικά στη συνέχεια.
      iii. είτε επιλέγεται η δημιουργία υλικού για τη δημιουργία συμμετρικού κλειδιού συνεδρίας οπότε η εφαρμογή mIBC-AIS-App δημιουργεί αυτόματα τα κατάλληλα κρυπτογραφικά δεδομένα προκειμένου να το εκπέμψει εμπιστευτικά στη συνέχεια.
   (β΄) Η εφαρμογή mIBC-AIS-App κρυπτογραφεί τα εμπιστευτικά δεδομένα χρησιμοποιώντας το δημόσιο κλειδί (MMSI) του παραλήπτη και τα δημόσια δεδομένα της υποδομής ΚΒΤ στην οποία είναι εγγεγραμμένο το σκάφος στο οποίο αποστέλλεται το μήνυμα.

(γ΄) Η εφαρμογή mIBC-AIS-App κατασκευάζει εξ αρχής ένα μήνυμα AIS τύπου AIS ADDRESSED BINARY MESSAGE (Τύπος 6) στο οποίο ενθυλακώνει τα κρυπτογραφημένα δεδομένα.

(δ΄) Η εφαρμογή mIBC-AIS-App περνά το δημιουργημένο μήνυμα AIS τύπου AIS ADDRESSED BINARY MESSAGE (Τύπος 6) από συνάρτηση κατακερματισμού, υπογράφει ψηφιακά το αποτέλεσμα και ενθυλακώνει το αρχικό μήνυμα μαζί με την ψηφιακή υπογραφή του σε ένα δεύτερο μήνυμα AIS τύπου AIS ADDRESSED BINARY MESSAGE (Τύπος 6)

(ε΄) Η εφαρμογή mIBC-AIS-App προωθεί προς την κεραία για μετάδοση τα δύο δημιουργημένα μηνύματα AIS τύπου AIS ADDRESSED BINARY MESSAGE (Τύπος 6)

5. mIBC-AIS σε λειτουργία mIBC-AES-AIS (mode 5): Υποθέτουμε ότι η εφαρμογή mIBC-AIS-App έχει πρόσβαση στο συμμετρικό κλειδί συνόδου και στη συνέχεια η εφαρμογή:

   (α΄) είτε:

      i. ανακόπτει το αρχικό σήμα και διαβάζει τα δεδομένα του

      ii. δέχεται ως είσοδο απευθείας ένα εμπιστευτικό μήνυμα mIBC-AIS-App

   (β΄) κρυπτογραφεί τα εμπιστευτικά δεδομένα χρησιμοποιώντας το συμμετρικό κλειδί συνόδου.

   (γ΄) κατασκευάζει εξ αρχής ένα μήνυμα AIS AIS ADDRESSED BINARY MESSAGE (Τύπος 6), εάν το μήνυμα απευθύνεται σε έναν παραλήπτη, ή ένα μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπος 8) εάν απευθύνεται σε AISANET, στο οποίο ενθυλακώνει τα κρυπτογραφημένα δεδομένα.

6.8.2 Χειρισμός εισερχόμενου σήματος AIS

Η εφαρμογή mIBC-AIS-App χειρίζεται τα εισερχόμενα σήματα AIS ως εξής:

1. mIBC-AIS σε λειτουργία τυπικού AIS (mode 1): Η εφαρμογή mIBC-AIS-App απλά προωθεί τα σήματα προς τη συσκευή AIS.

2. mIBC-AIS σε λειτουργία mIBC-Authenticated-AIS (mode 2): Η εφαρμογή mIBC-AIS-App ανακόπτει το εισερχόμενο μήνυμα AIS τύπου AIS BROADCAST BINARY MESSAGE (Τύπος 8) και στη συνέχεια:

   (α΄) αποθυλακώνει το αρχικό μήνυμα AIS και τη συνοδευτική ψηφιακή υπογραφή

   (β΄) ελέγχει την ψηφιακή υπογραφή με βάση το MMSI του αποστολέα.

      i. Εάν η ψηφιακή υπογραφή είναι έγκυρη, προωθεί το αποθυλακωμένο αρχικό σήμα προς τη συσκευή AIS.

      ii. Εάν η ψηφιακή υπογραφή είναι άκυρη, ανάλογα με την ισχύουσα πολιτική, είτε το αποθυλακωμένο αρχικό σήμα δεν προωθείται προς

τη συσκευή AIS, είτε προωθείται με κάποιο ειδικό τρόπο που καθιστά σαφή τη μη εγκυρότητα της ψηφιακής υπογραφής.

3. mIBC-AIS σε λειτουργία mIBC-Anonymous-AIS (mode 3): Οι ενέργειες είναι ακριβώς οι ίδιες με εκείνες στη λειτουργία mIBC-Authenticated-AIS (mode 2). Η μόνη διαφορά είναι ότι η ψηφιακή υπογραφή ελέγχεται για το ψευδο-MMSI.

4. mIBC-AIS σε λειτουργία mIBC-Confidential-AIS (mode 4): Υποθέτουμε ότι η εφαρμογή mIBC-AIS-App έχει πρόσβαση στο ιδιωτικό κλειδί του σκάφους. Στη συνέχεια η εφαρμογή mIBC-AIS-App:

   (α΄) Ανακόπτει το εισερχόμενο σήμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) και την ψηφιακή υπογραφή του σε 2ο σήμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) και διαβάζει τα ενθυλακωμένα δεδομένα των μηνυμάτων.

   (β΄) Ελέγχει με τον μηχανισμό της mIBC-Authenticated-AIS (mode 2) την εγκυρότητα της ψηφιακής υπογραφής και αποθυλακώνει το αποτέλεσμα της συνάρτησης κατακερματισμού των κρυπτογραφημένων δεδομένων που έχει στείλει ο αποστολέας.

   (γ΄) Αποκρυπτογραφεί τα κρυπτογραφημένα δεδομένα και τα περνά από τη συμφωνημένη συνάρτηση κατακερματισμού. Συγκρίνει το αποτέλεσμα με το ψηφιακά υπογεγραμμένο απεσταλμένο αποτέλεσμα και, εάν αυτά συμφωνούν, δέχεται ως έγκυρα τα αποκρυπτογραφημένα δεδομένα. Στη συνέχεια,

      i. εάν τα δεδομένα είναι κάποιο σήμα AIS, τότε προωθούνται στη συσκευή AIS

      ii. εάν τα δεδομένα είναι εμπιστευτικό μήνυμα εκτός πρωτοκόλλου AIS, ο χειρισμός εξαρτάται από την υλοποίηση της εφαρμογής mIBC-AIS-App

      iii. εάν τα δεδομένα είναι ανταλλαγής συμμετρικού κλειδιού συνόδου για χρήση, τότε αποθηκεύονται με ασφάλεια για χρήση στη λειτουργία mIBC-AES-AIS (mode 5).

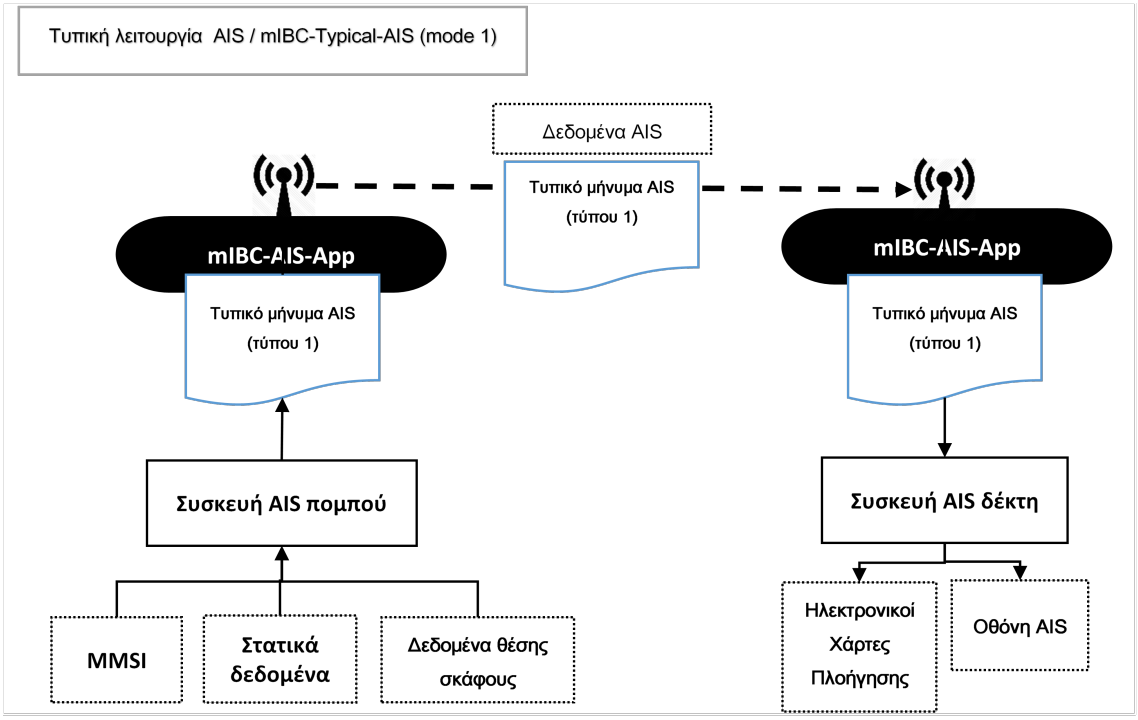
5. mIBC-AIS σε λειτουργία mIBC-AES-AIS (mode 5): Υποθέτουμε ότι η εφαρμογή mIBC-AIS-App έχει πρόσβαση στο συμμετρικό κλειδί συνόδου. Στη συνέχεια, η εφαρμογή mIBC-AIS-App

   (α΄) Ανακόπτει το εισερχόμενο αρχικό σήμα, είτε αυτό είναι AIS ADDRESSED BINARY MESSAGE (Τύπος 6), είτε AIS BROADCAST BINARY MESSAGE (Τύπος 8), και διαβάζει τα δεδομένα του.

   (β΄) Αποκρυπτογραφεί τα κρυπτογραφημένα δεδομένα χρησιμοποιώντας το συμμετρικό κλειδί συνόδου. Στη συνέχεια:

      i. εάν τα δεδομένα είναι κάποιο σήμα AIS, τότε προωθούνται στη συσκευή AIS

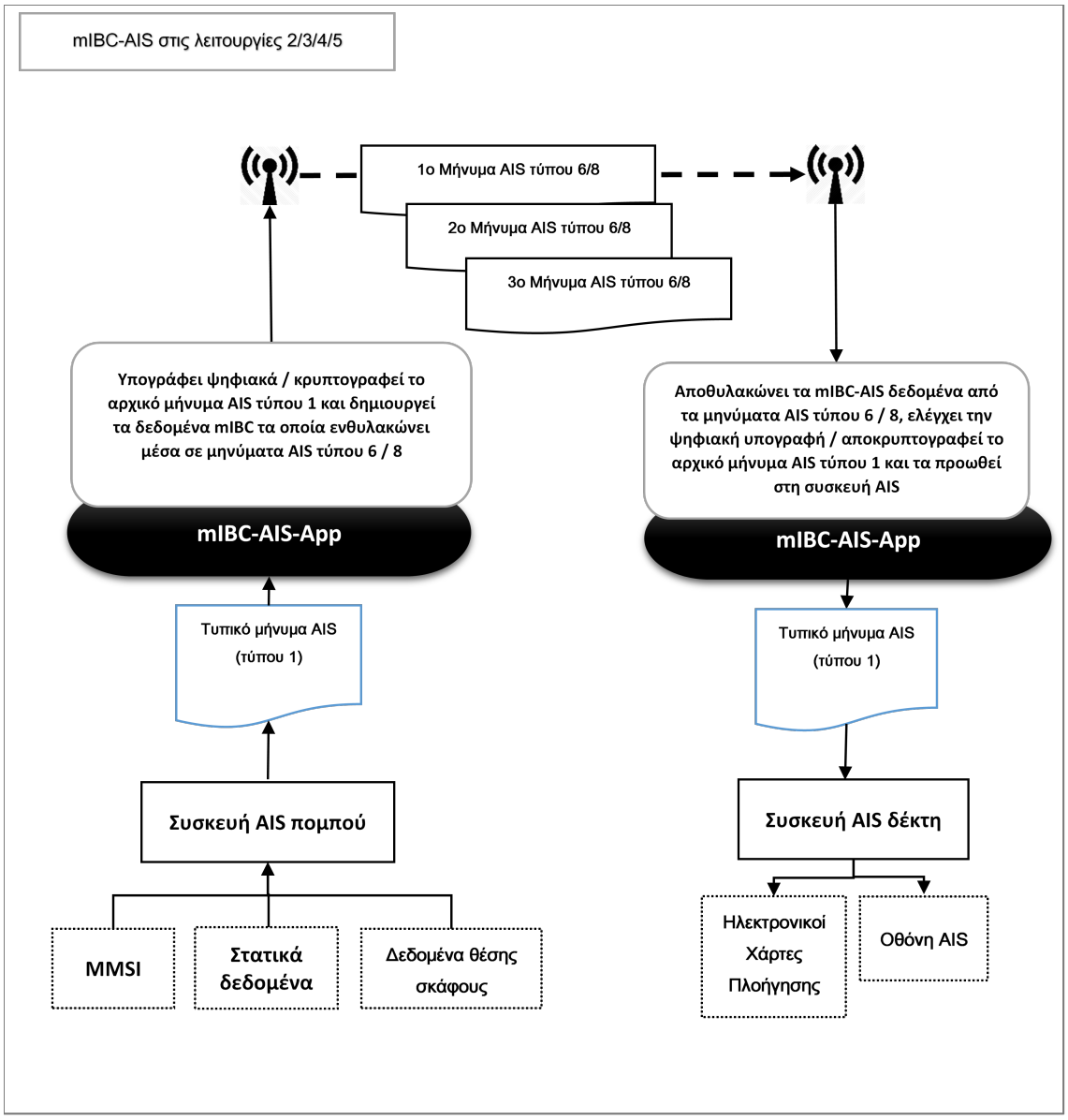
      ii. εάν τα δεδομένα είναι εμπιστευτικό μήνυμα εκτός πρωτοκόλλου AIS, ο περαιτέρω χειρισμός εξαρτάται από την υλοποίηση της εφαρμογής mIBC-AIS-App



Σχήμα 6.14: Η εφαρμογή mIBC-AIS-App στη λειτουργία mIBC-Typical-AIS (mode 1) απλά προωθεί τα μηνύματα του AIS από και προς τις συσκευές AIS

.

iii. εάν τα δεδομένα είναι ανταλλαγής συμμετρικού κλειδιού συνόδου για χρήση, τότε αποθηκεύονται με ασφάλεια για χρήση στη λειτουργία mIBC-AES-AIS (mode 5).



Σχήμα 6.15: Θέση και λειτουργίες της εφαρμογής mIBC-AIS-App.

Κεφάλαιο 7

Υλοποίηση της υποδομής mIBC-AIS BLMQ-SKIBE

7.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο προτείναμε τη βελτίωση της ασφάλειας του AIS με τη χρήση μια υποδομής ΚΒΤ προσαρμοσμένης στις ανάγκες της ναυτιλίας (mIBC). Η mIBC μπορεί να υλοποιηθεί είτε υπό μια διεθνή ναυτιλιακή αρχή (π.χ. IMO) είτε υπό τον συνδυασμό διαλειτουργικών εθνικών ή ιδιωτικών αρχών. Σ΄ αυτό το κεφάλαιο παρουσιάζουμε την υλοποίηση μιας παγκόσμιας υποδομής mIBC που χρησιμοποιεί τους μηχανισμούς BLMQ για ψηφιακή υπογραφή δεδομένων και SKIBE για κρυπτογράφηση δεδομένων, που ονομάζουμε mIBC-AIS-BLMQ-SKIBE.

7.2 Σύσταση της mIBC-AIS-BLMQ-SKIBE

Η υλοποίηση της mIBC-AIS-BLMQ-SKIBE ξεκινά με τη δημιουργία ενός ΑΚΣ, τον οποίο στην ενότητα 2.2, όπου παρουσιάσαμε την υλοποίηση μιας υποδομής ΚΒΤ κατά BLMQ-SKIBE, τον ονομάσαμε (PKG), συνεπώς εδώ τον ονομάζουμε (mIBC-PKG).

Την παραμετροποίηση του mIBC-PKG αναλαμβάνει η υλοποιούσα ναυτιλιακή αρχή, π.χ. στο παράδειγμά μας ο IMO, και περιλαμβάνει τα παρακάτω, όπως αναλυτικά έχουν παρουσιαστεί στην ενότητα 2.2.

- **Ορισμός παραμέτρων ασφαλείας (ΠΑ) και δημόσιων παραμέτρων (ΔΠ/*PP*)** του mIBC-PKG. Οι παράμετροι ασφαλείας κάθε υλοποίησης mIBC BLMQ-SKIBE πρέπει να επιλεγούν έτσι ώστε να επιτυγχάνεται η σωστή ισορροπία μεταξύ αποτελεσματικότητας και ζητούμενου επιπέδου ασφάλειας. Ο προσδιορισμός των βέλτιστων παραμέτρων απαιτεί μεθοδική διερεύνηση των ειδικών αναγκών και των χαρακτηριστικών της ναυτιλίας και των ηλεκτρονικών συστημάτων που θα καλύπτει, όπως το AIS. Σ΄ αυτήν τη διατριβή περιγράφουμε μια γενική παρουσία mIBC, ακολουθώντας τις γενικές οδηγίες και προτάσεις του προτύπου IEEE 1363.3-2013 [16]. Οι τεχνικές λεπτομέρειες περιγράφονται αναλυτικά στην ενότητα 2.2.1 της διατριβής.
- **Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ) (MS_{Pub}) και Θεμελιώδες Μυστικό**

Κλειδί (ΘΜΚ/MS_{Secret})του mIBC-PKG. (α) Επιλογή ενός τυχαίου ακέραιου ως το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/MS_{Secret}) του mIBC-PKG. (β) Υπολογισμός του **Θεμελιώδους Δημόσιου Κλειδιού**, το οποίο σε αυτό το κεφάλαιο στο εξής θα συμβολίζεται ως (MS_{Pub}). Οι τεχνικές λεπτομέρειες περιγράφονται αναλυτικά στην ενότητα 2.2.2 της διατριβής. Υπενθυμίζουμε ότι ο ΑΚΣ (mIBC-PKG) της συγκεκριμένης υλοποίησης είναι υπεύθυνος για τη λήψη όλων των απαραίτητων μέτρων για τη διασφάλιση της εμπιστευτικότητας και της διαθεσιμότητας του Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ) (MS_{Secret}).

- **Δημοσίευση Δημόσιων Παραμέτρων (ΔΠ/*PP*) του mIBC-PKG.** Αυτές οι παράμετροι είναι στατικές και οι χρήστες της υποδομής μπορούν να τις αποθηκεύσουν για μελλοντική χρήση. Οι τεχνικές λεπτομέρειες περιγράφονται αναλυτικά στην ενότητα 2.2.1 της διατριβής. Η απόκτηση των (ΔΠ/*PP*) από τα σκάφη μπορεί να γίνεται είτε δια αντιπροσώπου, δια ζώσης, μέσω ενός usb token που το σκάφος θα προμηθεύεται από κάποια επίσημη ναυτιλιακή αρχή, είτε μέσω του ιστότοπου της αρχής υλοποίησης, π.χ. του IMO.
- **Το Ιδιωτικό Κλειδί (**$MMSI_{Private}$**)** εξάγεται από τον Αξιόπιστο Κεντρικό Συντονιστή (ΑΚΣ) με τη χρήση του μοναδικού αναγνωριστικού *MMSI* του σκάφους, του Θεμελιώδους Μυστικού Κλειδιού (ΘΜΚ/(MS_{Sec}) του ΑΚΣ και των Δημόσιων Παραμέτρων (ΔΠ/*PP*). Οι τεχνικές λεπτομέρειες περιγράφονται αναλυτικά στην ενότητα 2.2.3 της διατριβής.

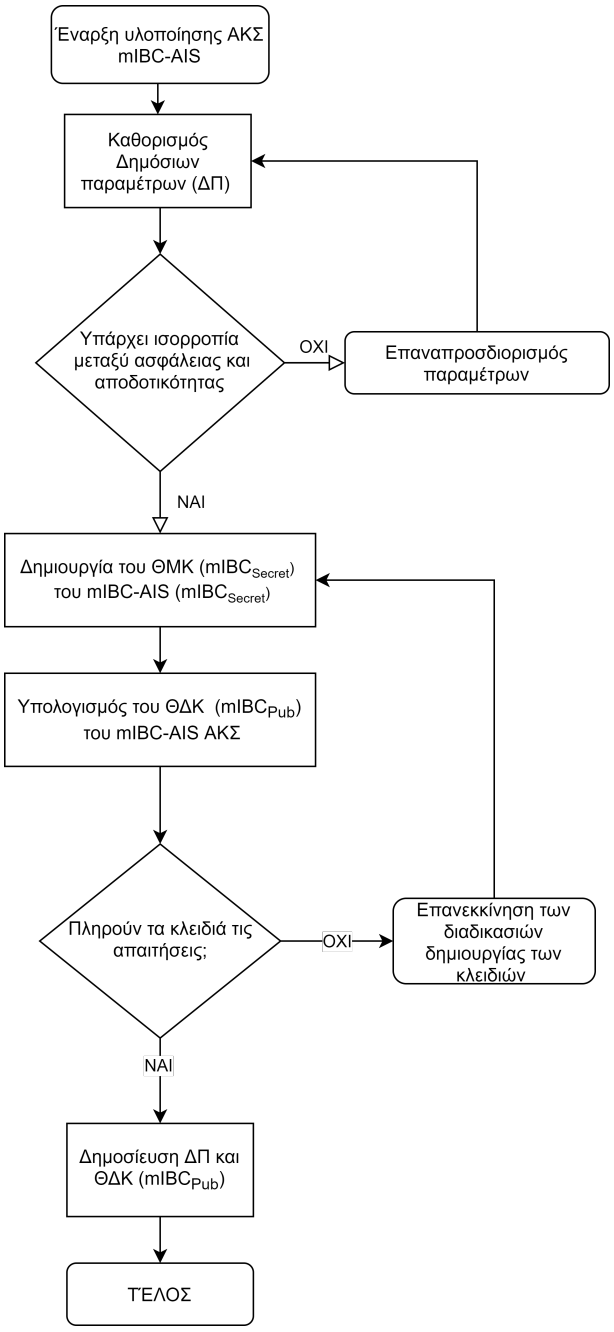
7.3 Εξαγωγή των ιδιωτικών κλειδιών των σκαφών από τον mIBC-PKG

Ο mIBC-PKG χρησιμοποιεί το MMSI (ή το ψευδο-MMSI) του σκάφους, τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) και το Θεμελιώδες Μυστικό κλειδί ($mIBC_{Secret}$) προκειμένου να εξάγει το ιδιωτικό κλειδί του σκάφους ($MMSI_{Private}$). Η υποχρεωτική χρήση του Θεμελιώδους Μυστικού κλειδιού ($mIBC_{Secret}$) στη διαδικασία υπολογισμού του συνδέει το ιδιωτικό κλειδί του σκάφους ($MMSI_{Private}$) με το συγκεκριμένο MMSI (ή το ψευδο-MMSI) και τη συγκεκριμένη υλοποίηση mIBC-AIS.

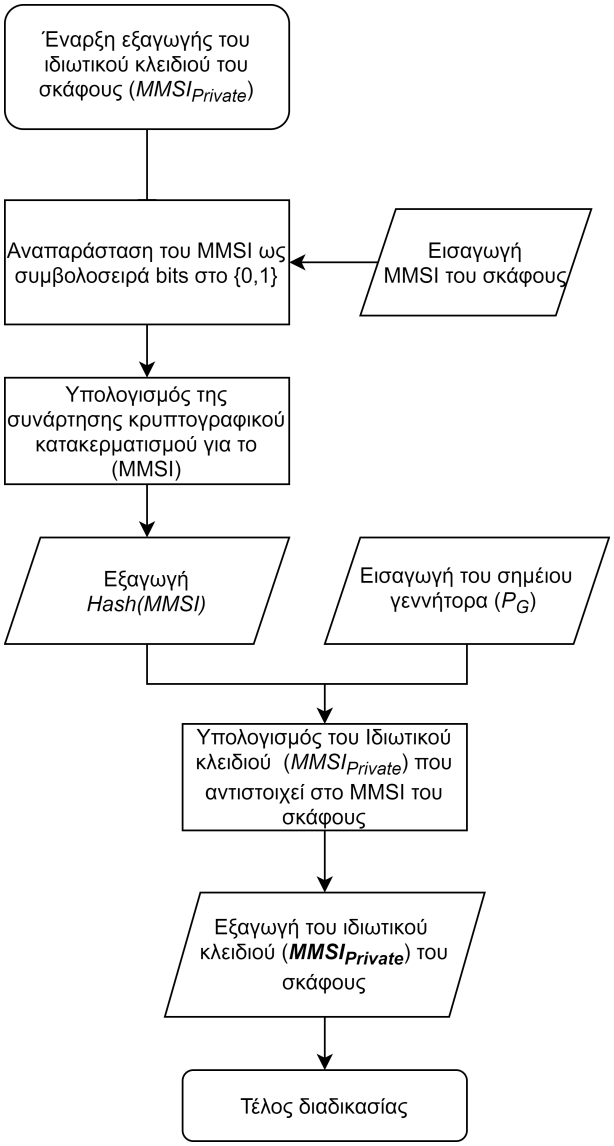
Τα βήματα είναι τα παρακάτω:

1. Αναπαριστούμε το MMSI (ή το ψευδο-MMSI) του σκάφους ως ακολουθία bits $\in \{0, 1\}$.
2. Ο ΑΚΣ (mIBC-PKG) υπολογίζει το αποτέλεσμα της συνάρτησης κατακερματισμού $H_1(MMSI)$ επί της ακολουθίας αυτής.
3. Στη συνέχεια υπολογίζει το ιδιωτικό κλειδί του σκάφους για τη συγκεκριμένη υλοποίηση $MMSI_{Private} = \frac{P_{G_2}}{H_1(MMSI)+mIBC_{Secret}}$.

Περισσότερες λεπτομέρειες για τα παραπάνω βήματα παρέχονται στην ενότητα 2.2.2 της διατριβής.



Σχήμα 7.1: Ροή διαδικασιών δημιουργίας του ΑΚΣ (mIBC-PKG) της υποδομής mIBC-AIS-BLMQ-SKIBE



Σχήμα 7.2: Ροή διαδικασιών δημιουργίας του ιδιωτικού κλειδιού ($MMSI_{Private}$) του σκάφους

7.4 Λειτουργία mIBC-BLMQ-Authenticated-AIS (mode 2)

Σ' αυτήν την ενότητα συζητάμε τη λειτουργία πιστοποίησης μηνύματος AIS στο πλαίσιο του mIBC-BLMQ-Authenticated-AIS (mode 2). Υποθέτουμε ότι σκάφος με MMSI = $MMSI_{Signer}$ υπογράφει ψηφιακά αρχικό μήνυμα AIS (AIS_{DATA}) προκειμένου να ενθυλακώσει το αρχικό μήνυμα AIS και την ψηφιακή υπογραφή του σε μήνυμα AIS BROADCAST BINARY MESSAGE τύπου 8, το οποίο και τελικά θα εκπέμψει. Οι δέκτες θα χρησιμοποιήσουν το δημόσια εκπεμπόμενο MMSI = $MMSI_{Signer}$ προκειμένου να ελέγξουν την εγκυρότητα της ψηφιακής υπογραφής.

Σημειώνουμε ότι όλες οι παρακάτω διαδικασίες υλοποιούνται με τη χρήση της εφαρμογής mIBC-AIS-App, χωρίς να τροποποιούν το υφιστάμενο πρωτόκολλο AIS.

Συνοπτικά, τα βήματα των διαδικασιών είναι τα παρακάτω (περισσότερες λεπτομέρειες υπάρχουν στην ενότητα 2.2.4):

7.4.1 Ψηφιακή υπογραφή μηνύματος AIS

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του πομπού ανακόπτει το αρχικό μήνυμα AIS_{DATA} πριν την εκπομπή του και στη συνέχεια:

Δεδομένα Εισόδου

- Μετατρέπει το αρχικό μήνυμα AIS_{DATA} προς υπογραφή σε μια ακολουθία bits $\in \{0, 1\}^{length}$, όπου *length* = το μήκος του AIS_{DATA} σε bits.
- Ανακαλεί από τη μνήμη τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) του (mIBC-PKG): (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, $mIBC_{Public}$, $e(P_{G_1}, P_{G_2})$, φ , H_2).
- Ανακαλεί από τη μνήμη το ιδιωτικό κλειδί του σκάφους ($MMSI_{Signer-Private}$).
- Δημιουργεί ένα τυχαίο ακέραιο αριθμό r, τ.ω. $(0 < r < p - 1]$.

Αλγόριθμος

Έπειτα εκτελεί τους παρακάτω υπολογισμούς:

1. $u = e(P_{G_1}, P_{G_2})^r$, όπου e είναι η δυαδική ζεύξη bilinear pairing mapping $e(P_{G_1}, P_{G_2}) \in G_T$.
2. $h = H_2(AIS_{DATA}, u), H_2$, όπου H_2 η συνάρτηση κατακερματισμού που έχει ορισθεί στις Δημόσιες Παραμέτρους.
3. $S = (r + h)MMSI_{Signer-Private}$.

Αποτέλεσμα

Η Ψηφιακή Υπογραφή που θα ενθυλακωθεί αποτελείται από την τριάδα

$$[AIS_{DATA}, h, S] \in [\{0, 1\}^{length} \times \mathbb{Z}_p \times G_2]$$

.

7.4.2 Έλεγχος ψηφιακά υπογεγραμμένου μηνύματος AIS από τον δέκτη

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του δέκτη ανακόπτει το μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 8 που έρχεται από τη κεραία πριν φτάσει στη συσκευή AIS. Το μήνυμα περιέχει ενθυλακωμένη την ψηφιακή υπογραφή $[AIS_{DATA}, h, S]$. Στη συνέχεια:

Δεδομένα Εισόδου

- Αποθηκεύει το αναγνωριστικό Signer-MMSI ή ψευδο-Signer-MMSI που υπάρχει στο μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 8. Αυτό το αναγνωριστικό θα χρησιμοποιηθεί ως το δημόσιο κλειδί του αποστολέα και έναντι αυτού θα ελεγχθεί η εγκυρότητα της ψηφιακής υπογραφής.
- Αποθυλακώνει τα δεδομένα που υπάρχουν στο μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 8, ιδίως την ψηφιακή υπογραφή $([AIS_{DATA}, h, S] \in [\{0,1\}^{length} \times \in \mathbb{Z}_p \times G_2])$.
- Ανακαλεί από τη μνήμη τις Δημόσιες Παραμέτρους της mIBC-AIS του πομπού $(PP): G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, mIBC_{Public}, e(P_{G_1}, P_{G_2}), \phi, H_1, H_2$. Στο παράδειγμά μας αυτές είναι κοινές για όλους, διότι θεωρούμε ότι έχουμε μια υποδομή mIBC-AIS-BLMQ-SKIBE, υπό τον IMO.

Αλγόριθμος

Εκτελεί τους παρακάτω υπολογισμούς:

(1) $u = \frac{e(S, H_1(MMSI_{Signer})P_{G_1} + mIBC_{Public})}{e(P_{G_1}, P_{G_2})^h}$.

(2) $H_2(AIS_{DATA}, u)$.

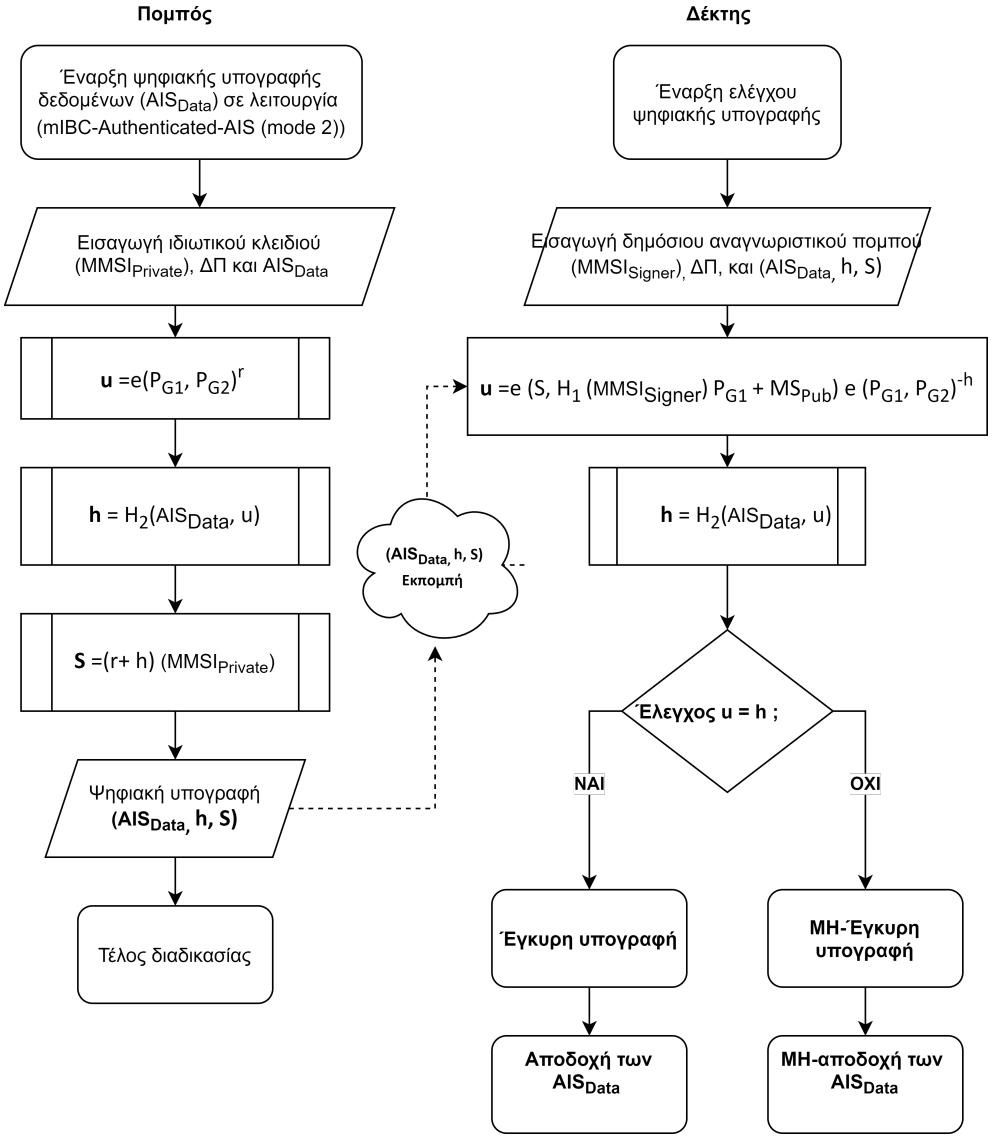
Αποτέλεσμα

(3) Εάν και μόνο εάν $h = H_2(AIS_{DATA}, u)$ η ψηφιακή υπογραφή επικυρώνεται, ειδάλλως η ψηφιακή υπογραφή δεν επικυρώνεται.

Περισσότερες λεπτομέρειες για τον μηχανισμό BLMQ υπάρχουν στην ενότητα 2.2.4 της διατριβής.

7.5 Λειτουργία mIBC-SKIBE-AIS (mode 4)

Όπως έχουμε προαναφέρει, το σχήμα mIBC-SKIBE-AIS (mode 4) παρέχει τη δυνατότητα κρυπτογράφησης ολόκληρων τυχαίων μηνυμάτων, ή μεμονωμένων δεδομένων μηνυμάτων AIS, που μπορεί να είναι κλειδιά συνόδου συμμετρικής κρυπτογράφησης ή υλικό που μπορεί να χρησιμοποιηθεί για την κατασκευή τέτοιων κλειδιών. Ο πομπός, με αναγνωριστικό ($MMSI_{Recipient}$) κρυπτογραφεί το μήνυμα μέσω του μηχανισμού SKIBE και στη συνέχεια το ενθυλακώνει σε μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 6, το οποίο και τελικά θα εκπέμψει. Ο δέκτης που θα λάβει το μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 6, αρχικά θα αποθυλακώσει τα δεδομένα και στη συνέχεια θα τα αποκρυπτογραφήσει.



Σχήμα 7.3: Ροή διαδικασιών ψηφιακής υπογραφής μηνύματος AIS_{DATA} (αριστερό σκέλος) και ελέγχου ψηφιακής υπογραφής (δεξί σκέλος) σε λειτουργία mIBC-BLMQ-Authenticated-AIS (mode 2)

Σημειώνουμε ότι όλες οι παρακάτω διαδικασίες υλοποιούνται με τη χρήση της εφαρμογής mIBC-AIS-App και δεν τροποποιούν το υφιστάμενο πρωτόκολλο AIS.

Συνοπτικά τα βήματα των κρυπτογραφικών διαδικασιών είναι τα παρακάτω (περισσότερες λεπτομέρειες υπάρχουν στην ενότητα 2.2.5):

7.5.1 Κρυπτογράφηση δεδομένων υπό mIBC-SKIBE-AIS (mode 4)

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του πομπού ανακόπτει το αρχικό μήνυμα AIS_{DATA} πριν την εκπομπή του και στη συνέχεια:

Δεδομένα Εισόδου

- Μετατρέπει το αρχικό μήνυμα AIS_{DATA} προς υπογραφή σε ακολουθία bits $\in \{0,1\}^{length}$, όπου $length$ = το μήκος του AIS_{DATA} σε bits.
- Ανακαλεί από τη μνήμη τις Δημόσιες Παραμέτρους (ΔΠ/*PP*) του (mIBC-PKG) του δέκτη: $(G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, mIBC_{Public}, e(P_{G_1}, P_{G_2}), \varphi, H_2)$. Στο παράδειγμά μας αυτές είναι κοινές για όλους, διότι θεωρούμε ότι έχουμε μια υποδομή mIBC-AIS-BLMQ-SKIBE, υπό τον IMO.
- Εξάγει έναν τυχαίο ακέραιο $\sigma \in \{0,1\}^{length}$, μέσω του γεννήτορα R που περιγράψαμε στην ενότητα 2.2.1
- Εντοπίζει το δημόσιο αναγνωριστικό του Παραλήπτη $MMSI_{Recipient} \in \{0,1\}^*$

Αλγόριθμος

Εκτελεί τους παρακάτω υπολογισμούς:

1. $r = H_4(\sigma, AIS_{DATA})$ όπου H_4: $\{0,1\}^{length} \times \{0,1\}^{length} \rightarrow \mathbb{Z}_p^*$.
2. $g^r = e(P_{G_1}, P_{G_2})^r$.
3. $Q = (H_1(MMSI_{Recipient})P_{G_1} + mIBC_{Public})\cdot$ όπου H_1: $\{0,1\}^* \rightarrow \mathbb{Z}_p^*$.
4. $U = r(Q)$.
5. $V = \sigma \oplus H_3(g^r)$ όπου H_3: $G_T \rightarrow \{0,1\}^{length}$.
6. $W = AIS_{DATA} \oplus H_5(\sigma)$ όπου H_5: $\{0,1\}^{length} \rightarrow \{0,1\}^{length}$.
7. $c = (rQ, \sigma \oplus H_3(g^r), AIS_{DATA} \oplus H_5(\sigma)) = (U, V, W) \in (G_1 \times \{0,1\}^{length} \times \{0,1\}^{length})$.

Αποτέλεσμα

Το αποτέλεμα της κρυπτογράφησης είναι η τριάδα

$$Ciphertext(c) = (U, V, W) \in (G_1 \times \{0,1\}^{length} \times \{0,1\}^{length})$$

την οποία η εφαρμογή mIBC-AIS-App ενθυλακώνει σε μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 6, που θα προωθηθεί στην κεραία για εκπομπή.

7.5.2 Αποκρυπτογράφηση δεδομένων υπό mIBC-SKIBE-AIS (mode 4)

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του δέκτη ανακόπτει το μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 6 που έρχεται από τη κεραία, πριν φτάσει στη συσκευή AIS. Το μήνυμα περιέχει ενθυλακωμένα τα κρυπτογραφημένα δεδομένα ψηφιακής υπογραφής $[AIS_{DATA}, h, S]$.

Δεδομένα Εισόδου

- Οι Δημόσιες Παράμετροι (ΔΠ/*PP*) του (mIBC-PKG) του δέκτη: $PP = (G_1, G_2, G_T, e, P_{G_1}, P_{G_2}, MS_{Pub}, e(P_{G_1}, P_{G_2}), \phi, H_1, H_3, H_4, H_5)$

- Το Ιδιωτικό κλειδί του δέκτη $MMSI_{Recipient-PRIVATE} \in G_2$

Αλγόριθμος

1. $g' = e(U, MMSI_{Recipient-PRIVATE})$.
2. $\sigma' = V \oplus H_3(g')$.
3. $m' = W \oplus H_5(\sigma')$.
4. $r' = H_4(\sigma', m')$.

Αποτέλεσμα

5. Εάν και μόνο εάν $U = r'(H_1(MMSI_{Recipient})P_{G_1} + mIBC_{Public})$, το αποκρυπτογραφημένο μηνύμα m' επικυρώνεται ώστε $m' = AIS_{DATA}$, ειδάλλως το αποκρυπτογραφημένο μηνύμα θεωρείται πλαστό ή λάθος.

Στο σχήμα 7.4 φαίνεται η ροή διαδικασιών κρυπτογράφησης εμπιστευτικών δεδομένων (στο αριστερό σκέλος) και αποκρυπτογράφησης (στο δεξί σκέλος), σε λειτουργία mIBC-SKIBE-AIS (mode 4).

7.6 Λειτουργία mIBC-AES-AIS (mode 5)

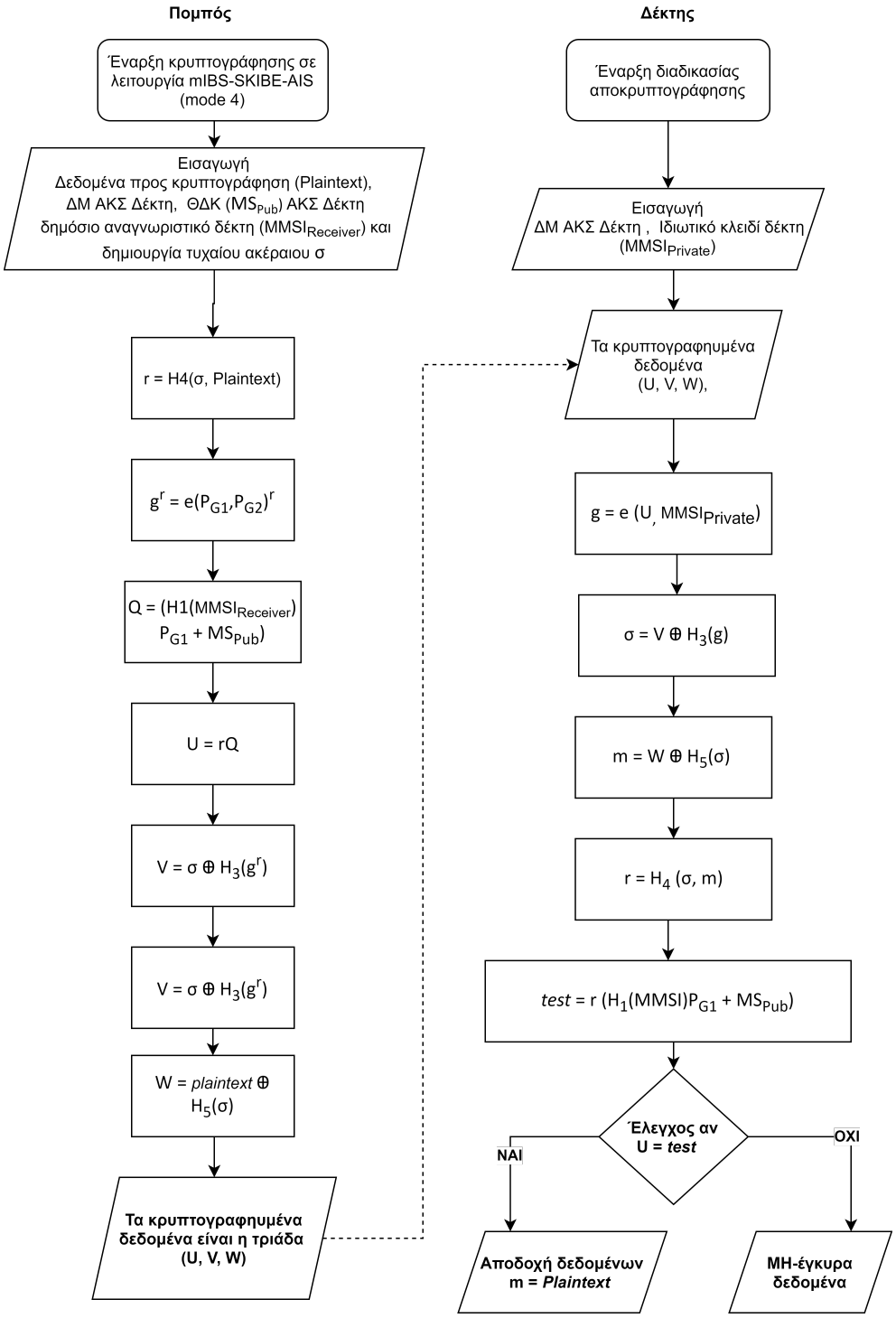
Έχουμε ήδη αναφέρει ότι η μεταφορά δεδομένων μέσω συμμετρικής κρυπτογράφησης με τη χρήση προ-εγκατεστημένων συμμετρικών κλειδιών στις συσκευές AIS δεν είναι κάτι νέο. Η επιπλέον δυνατότητα που προσφέρει η πρότασή μας είναι η δυνατότητα επί τούτω διαμοιρασμού συμμετρικών κλειδιών συνόδου σ' ένα ή παραπάνω σκάφη, προκειμένου να χρησιμοποιηθούν στη συμμετρική κρυπτογράφηση.

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του πομπού δημιουργεί το συμμετρικό κλειδί συνόδου (ή το υλικό για τη δημιουργία του) και, μέσω της λειτουργίας mIBC-SKIBE-AIS (mode 4), το στέλνει σε κάθε σκάφος που νομιμοποιείται να συμμετάσχει στην εμπιστευτική σύνοδο.

Συνοπτικά:

Η εφαρμογή mIBC-AIS-App που βρίσκεται στο σκάφος του πομπού:

- Δημιουργεί το συμμετρικό κλειδί συνόδου (ή το υλικό για τη δημιουργία του).
- Δημιουργεί τη λίστα με τα MMSI των σκαφών που θα συμμετέχουν στη σύνοδο.



Σχήμα 7.4: Λειτουργία mIBC-SKIBE-AIS (mode 4). Ροή διαδικασιών κρυπτογράφησης (αριστερό σκέλος) και αποκρυπτογράφησης (δεξί σκέλος).

- Περνά σε λειτουργία mIBC-SKIBE-AIS (mode 4), κρυπτογραφεί το συμμετρικό κλειδί συνόδου (ή το υλικό για τη δημιουργία του), δημιουργεί το αντίστοιχο μήνυμα AIS ADDRESSED BINARY MESSAGE τύπου 6 και το προωθεί στην κεραία AIS.

Αντίστοιχα, η εφαρμογή mIBC-AIS-App που βρίσκεται σε κάθε σκάφος δέκτη λαμβάνει το συμμετρικό κλειδί συνόδου, το οποίο και χρησιμοποιεί στη λειτουργία mIBC-AES-AIS (mode 5).

Τέλος, η λειτουργία mIBC-AES-AIS (mode 5) χρησιμοποιεί τον γνωστό αλγόριθμο κρυπτογράφησης AES προκειμένου να κρυπτογραφήσει τα εμπιστευτικά δεδομένα, να τα ενθυλακώσει σε μηνύματα AIS ADDRESSED BINARY MESSAGE τύπου 6 και να τα εκπέμψει.

Κεφάλαιο 8

Πειραματική υλοποίηση mIBC-AIS-ECCSI-SAKKE

8.1 Εισαγωγή

Σ' αυτό το κεφάλαιο παρουσιάζουμε το mIBC-AIS ECCSI-SAKKE, δηλαδή τη λειτουργικότητα της υποδομής mIBC-AIS όπως την έχουμε περιγράψει, βασιζόμενη στο συνδυαστικό σχήμα ECCSI (RFC6507) και SAKKE (RFC6508) που αναλύσαμε στην ενότητα 2.3. Επίσης, προς επαλήθευση της ορθότητας της πειραματικής υλοποίησης, παρουσιάζουμε τη μερική εφαρμογή του mIBC-AIS ECCSI-SAKKE και συγκεκριμένα το μέρος των υπηρεσιών ψηφιακής υπογραφής δεδομένων mIBC-ECCSI-Authenticated-AIS (mode 2) και εμπιστευτικής αποστολής δεδομένων δημιουργίας συμμετρικού κλειδιού συνόδου mIBC-SAKKE-AIS (mode 4).

Συγκεκριμένα, το κεφάλαιο αυτό περιλαμβάνει:

- μια εισαγωγική παράθεση των λόγων για τους οποίους επιλέξαμε να χρησιμοποιήσουμε τους μηχανισμούς ECCSI και SAKKE για την πειραματική υλοποίηση της υποδομής mIBC-AIS,
- την περιγραφή των διαδικασιών του σχήματος mIBC-AIS ECCSI-SAKKE,
- την περιγραφή του περιβάλλοντος της υλοποίησης,
- την περιγραφή της λειτουργίας mIBC-ECCSI-Authenticated-AIS (mode 2) μέσω της εφαρμογής mIBC-AIS-App και
- την περιγραφή της λειτουργίας mIBC-SAKKE-AIS (mode 4) μέσω της εφαρμογής mIBC-AIS-App

Επισημαίνουμε ότι, σε αντίθεση με την πειραματική υλοποίηση του κεφαλαίου 5, όπου στόχος ήταν να δείξουμε στοιχεία της λειτουργίας των μηχανισμών ECCSI και SAKKE στο πλαίσιο του ARIBC, σ' αυτό το κεφάλαιο στόχος μας είναι να δείξουμε ότι το υφιστάμενο πρωτόκολλο AIS μπορεί να υποστηρίξει τη μεταφορά των κρυπτογραφικών δεδομένων των μηχανισμών ECCSI και SAKKE. Συνεπώς, η πειραματική υλοποίηση αυτού του κεφαλαίου είναι η συνέχεια μιας πειραματικής υλοποίησης για το mIBC-AIS, αντίστοιχης αυτής του κεφαλαίου 5, η οποία παραλείπεται για δύο λόγους. Ο πρώτος διότι θα ήταν μια επανάληψη του κεφαλαίου

5 και ο δεύτερος διότι θέλαμε να χρησιμοποιήσουμε τις ακριβείς τιμές ελέγχου που παρατίθενται στα ECCSI (RFC6507) και SAKKE (RFC6508), προκειμένου να είμαστε σίγουροι για την ορθή μεταφορά τους μέσω του υφιστάμενου πρωτοκόλλου AIS. Τέλος, αντίθετα με την παρουσίαση του mIBC-AIS BLMQ-SKIBE, όπου θεωρούσαμε ότι υπήρχε μια μοναδική δομή mIBC-AIS υπό τον IMO, σ' αυτό το κεφάλαιο παρουσιάζουμε και υλοποιούμε πειραματικά την εκδοχή δύο διαλειτουργικών δομών mIBC-AIS.

Υπενθυμίζεται ότι η χρήση των μηχανισμών ECCSI και SAKKE προσθέτει πολυπλοκότητα, αλλά προσφέρει τη δυνατότητα χρήσης δοκιμασμένων αλγορίθμων υλοποίησης, τιμές ελέγχου και επιβεβαίωσης, στα σχετικά Παραρτήματα των RFC6507 και RFC6508· αυτά αποτελούν πολύτιμες συμβολές στην πειραματική υλοποίηση της υποδομής mIBC-AIS. Σημειώνουμε, επίσης, ότι οι συμβολισμοί των RFCs που εν γένει θα χρησιμοποιηθούν σ' αυτό το κεφάλαιο περιγράφονται στο κεφάλαιο 2 της διατριβής.

8.2 Επισκόπηση της υλοποίησης

Οι σημαντικότερες διαφοροποιήσεις του mIBC-AIS ECCSI-SAKKE σε σχέση με το mIBC-AIS BLMQ-SKIBE φαίνονται στα Σχήματα 2.1 και 4.6 που αναφέρονται στην υποδομή ARIBC. Αυτές είναι:

- Η χρήση του μηχανισμού ECCSI αντί του μηχανισμού BLMQ για έλεγχο ταυτότητας.
- Η χρήση του μηχανισμού SAKKE αντί του γενικού μηχανισμού κρυπτογράφησης SKIBE των Sakai-Kasahara. Στην πραγματικότητα, ο μηχανισμός SAKKE είναι η βασική παραλλαγή του SAKKE ως μηχανισμού ενθυλάκωσης (SKKEM), σύμφωνα με το πρότυπο IEEE1363-3 [16] [1].
- Εάν θέλουμε να εκμεταλλευτούμε μια υποδομή mIBC και πέραν του AIS, το σχήμα ECCSI-SAKKE, λόγω της ανεξαρτησίας των μηχανισμών του, προσφέρει την ευελιξία της χρήσης του κάθε μηχανισμού σε συνδυασμό με άλλα σχήματα (βλ. Σχήμα 2.1. Για παράδειγμα:
  - μια ναυτιλιακή αρχή που υιοθετεί το mIBC-AIS ECCSI-SAKKE έχει τη δυνατότητα να βασίζεται στο μηχανισμό ECCSI για ψηφιακή υπογραφή σημάτων ηλεκτρονικών μέσων (όπως το παρουσιαζόμενο mIBC-AIS ECCSI) ή σε πιστοποιητικά X509 (εάν υπάρχουν ήδη για άλλες υπηρεσίες στο σκάφος) για ψηφιακή υπογραφή των μηνυμάτων του μηχανισμού SAKKE που θα χρησιμοποιείται για τη διανομή συμμετρικών κλειδιών συνόδου.
  - Αντίστοιχα, μια αρχή που υιοθετεί το mIBC ECCSI-SAKKE έχει τη δυνατότητα να χρησιμοποιήσει το μηχανισμό SAKKE για τη δημιουργία συμμετρικών κλειδιών συνόδου με την αποστολή ενός και μόνο μηνύματος σε εφαρμογές με λιγοστούς πόρους (όπως το AIS) και μηχανισμούς τύπου Diffie-Hellman για τη δημιουργία συμμετρικών κλειδιών συνόδου σε εφαρμογές χωρίς περιορισμένους πόρους. Σε κάθε περίπτωση, η

[1] Βλέπε RFC6508.

ταυτοποίηση των μηνυμάτων θα γίνεται μέσω του μηχανισμού mIBC ECCSI.

- Υπενθυμίζουμε ότι ενώ η ιδέα, η αρχή λειτουργίας της υποδομής mIBC-AIS, η αντίληψη των χρηστών, και οι οντότητες (ναυτιλιακές αρχές, σκάφη) που την απαρτίζουν είναι οι ίδιες, η υλοποίησή της με βάση το Σχήμα ECCSI-SAKKE διαφέρει. Στην πραγματικότητα, το ECCSI και το SAKKE είναι δύο παράλληλες υλοποιήσεις που μπορεί να λειτουργούν αυτόνομα ή σε συνδυασμό. Ως εκ τούτου, χρησιμοποιούμε ένα διπλό ΑΚΣ, τα δύο μέρη του οποίου ονομάζουμε KMS-ECCSI και KMS-SAKKE αντίστοιχα, ακολουθώντας την ορολογία των RFC65108, RFC6509 όπου ο ΑΚΣ ονομάζεται Key Management Server (KMS). Η κάθε υλοποίηση χρησιμοποιεί διαφορετικές κρυπτογραφικές δημόσιες παραμέτρους, διαφορετικά Θεμελιώδη κλειδιά και διαφορετικά Ιδιωτικά κλειδιά για κάθε χρήστη. Στο Σχήμα 8.1 απεικονίζεται η ροή διεργασιών της σταδιακής υλοποίησης ενός διπλού ΑΚΣ σε ένα σχήμα mIBC-AIS ECCSI-SAKKE.

Οι βασικές λειτουργίες του mIBC-AIS ECCSI-SAKKE είναι οι εξής:

1. Ο διπλός ΑΚΣ/KMS ορίζει:
   (α΄) Τις Δημόσιες Παραμέτρους KMS-ECCSI-PP του KMS-ECCSI.
   (β΄) Τις Δημόσιες Παραμέτρους KMS-SAKKE-PP του KMS-SAKKE.
2. Κάθε KMS επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ):
   (α΄) Ο KMS-ECCSI επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/KSAK) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ/KPAK) που θα χρησιμοποιείται με το πρωτόκολλο ECCSI.
   (β΄) Ο KMS-SAKKE επιλέγει το Θεμελιώδες Μυστικό Κλειδί (ΘΜΚ/z) και υπολογίζει το αντίστοιχο Θεμελιώδες Δημόσιο Κλειδί (ΘΔΚ/Z) που θα χρησιμοποιείται με το πρωτόκολλο SAKKE.
3. Κάθε KMS εκδίδει τα αντίστοιχα ιδιωτικά κλειδιά των χρηστών της mIBC-AIS ECCSI-SAKKE:
   (α΄) Ο KMS-ECCSI εκδίδει το Secret Signing key (SSK) και το Public Validation Token (PVT) για την ψηφιακή υπογραφή των δεδομένων που θα χρησιμοποιούνται με το πρωτόκολλο ECCSI.
   (β΄) Ο KMS-SAKKE εκδίδει το Receiver Secret key (RSK) που θα χρησιμοποιείται στην αποθυλάκωση με το πρωτόκολλο SAKKE.

Οι τεχνικές λεπτομέρειες του σχήματος ECCSI-SAKKE περιγράφονται αναλυτικά στην ενότητα 2.3 της διατριβής.

8.3 Η πειραματική υλοποίηση της υποδομής mIBC-AIS ECCSI-SAKKE)

Σ΄ αυτήν την ενότητα περιγράφουμε την εκδοχή διαλειτουργικών δομών mIBC-AIS. Συγκεκριμένα, θεωρούμε δύο πλοία που ανήκουν σε δύο διαφορετικές και ανεξάρτητες υποδομές mIBC-AIS, τις (mIBC-AIS-Gr και mIBC-AIS-No). Το σκάφος με MMSIa είναι μέλος της δομής mIBC-AIS-Gr και το σκάφος με MMSIb είναι μέλος της δομής mIBC-AIS-No.

Στις ακόλουθες ενότητες περιγράφουμε τα εξής:

1. Την υλοποίηση του ΑΚΣ (mIBC-AIS-ECCSI-KMS που υποστηρίζει τη λειτουργία mIBC- ECCSI -AIS (mode 2). Ως παράδειγμα χρησιμοποιούμε την υποδομή mIBC-AIS-Gr με ΑΚΣ ECCSI-KMS$_{Gr}$ και σκάφος με MMSI = MMSIa το οποίο υπογράφει ψηφιακά τα σήματα (AIS_{DATA}) μέσω της εφαρμογής mIBC-AIS-App. Συγκεκριμένα:

   (α΄) Στην ενότητα 8.3.1 παρουσιάζεται η κατασκευή των θεμελιωδών κλειδιών (($KSAK_{Gr}$ / $KPAK_{Gr}$) του ECCSI-KMS$_{Gr}$.

   (β΄) Στην ενότητα 8.3.1 παρουσιάζεται ο υπολογισμός του ιδιωτικού κλειδιού του σκάφους $MMSIa_{SSK}$ μαζί με το $MMSIa_{PVT}$.

   (γ΄) Στην ενότητα 8.3.1 παρουσιάζεται ο αλγόριθμος ψηφιακής υπογραφής των δεδομένων του AIS (AIS_{DATA}) από το σκάφος με MMSIa μέσω της εφαρμογής mIBC-AIS-App.

   (δ΄) Στην ενότητα 8.3.1 παρουσιάζεται ο αλγόριθμος ελέγχου της εγκυρότητας των ψηφιακά υπογεγραμμένων δεδομένων του AIS (AIS_{DATA}) από τυχαίο δέκτη μέσω της εφαρμογής mIBC-AIS-App.

2. Την υλοποίηση του ΑΚΣ (mIBC-AIS-SAKKE-KMS) που υποστηρίζει τη λειτουργία mIBC-SAKKE-AIS (mode 4). Ως παράδειγμα χρησιμοποιούμε την υποδομή mIBC-AIS-No με ΑΚΣ SAKKE-KMS$_{No}$, και σκάφος με MMSI = MMSIb. Προς αυτό το σκάφος κάποιος θα αποστείλει εμπιστευτικά, μέσω του mIBC-SAKKE-AIS (mode 4), υλικό για τη δημιουργία συμμετρικού κλειδιού συνόδου. Συγκεκριμένα:

   (α΄) Στην ενότητα 8.3.2 παρουσιάζεται η κατασκευή των θεμελιωδών κλειδιών (Z_T / z_T) του SAKKE-KMS$_{No}$.

   (β΄) Στην ενότητα 8.3.2 παρουσιάζεται ο υπολογισμός του ιδιωτικού κλειδιού του σκάφους $MMSIb_{RSK}$.

   (γ΄) Στην ενότητα 8.3.2 παρουσιάζεται ο αλγόριθμος εμπιστευτικής ενθυλάκωσης, μέσω της εφαρμογής mIBC-AIS-App, του υλικού δημιουργίας συμμετρικού κλειδιού, κατά τον μηχανισμό SAKKE, προς τον νόμιμο παραλήπτη με MMSI = MMSIb ο οποίος ανήκει στη δομή του SAKKE-KMS$_{No}$.

   (δ΄) Στην ενότητα 8.3.2 παρουσιάζεται ο αλγόριθμος εμπιστευτικής αποθυλάκωσης, μέσω της εφαρμογής mIBC-AIS-App, κατά τον μηχανισμό

SAKKE, του υλικού δημιουργίας συμμετρικού κλειδιού από τον νόμιμο παραλήπτη με MMSI = MMSIb.

8.3.1 Διαδικασίες υλοποίησης ΑΚΣ (mIBC-AIS-ECCSI-KMS) που υποστηρίζει τη λειτουργία mIBC-ECCSI-AIS (mode 2)

Περισσότερες λεπτομέρειες για τα δημόσια δεδομένα και την ορολογία που χρησιμοποιούμε υπάρχουν στην ενότητα 2.3.2 και στον πίνακα 2.3. Σημειώνουμε ότι οι διαδικασίες που παραθέτουμε βασίζονται στις οδηγίες και τους αλγόριθμους της ενότητας 4.2. "Community Parameters" του RFC6507.

Οι δημόσιες παράμετροι του μηχανισμού ECCSI (RFC6507) είναι οι: $p, n, q,\ EC, G,$ $Hash(es)_x, KPAK$

Η διαδικασία δημιουργίας των Θεμελιωδών κλειδιών ($KSAK_{Gr}$ / $KPAK_{Gr}$) του ECCSI-KMS$_{Gr}$ είναι:

1. Επιλογή του $KSAK_{Gr}$: Επιλέγεται τυχαίος ακέραιος αριθμός $\in (2, q-1]$.

2. Υπολογισμός του $KPAK_{Gr}$: Υπολογίζεται το $KPAK_{Gr} = [KSAK_{Gr}]G_{Gr}$, όπου $G_{Gr}(G_{Gr}, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης q. Η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στην EC με ακέραιο αριθμό.

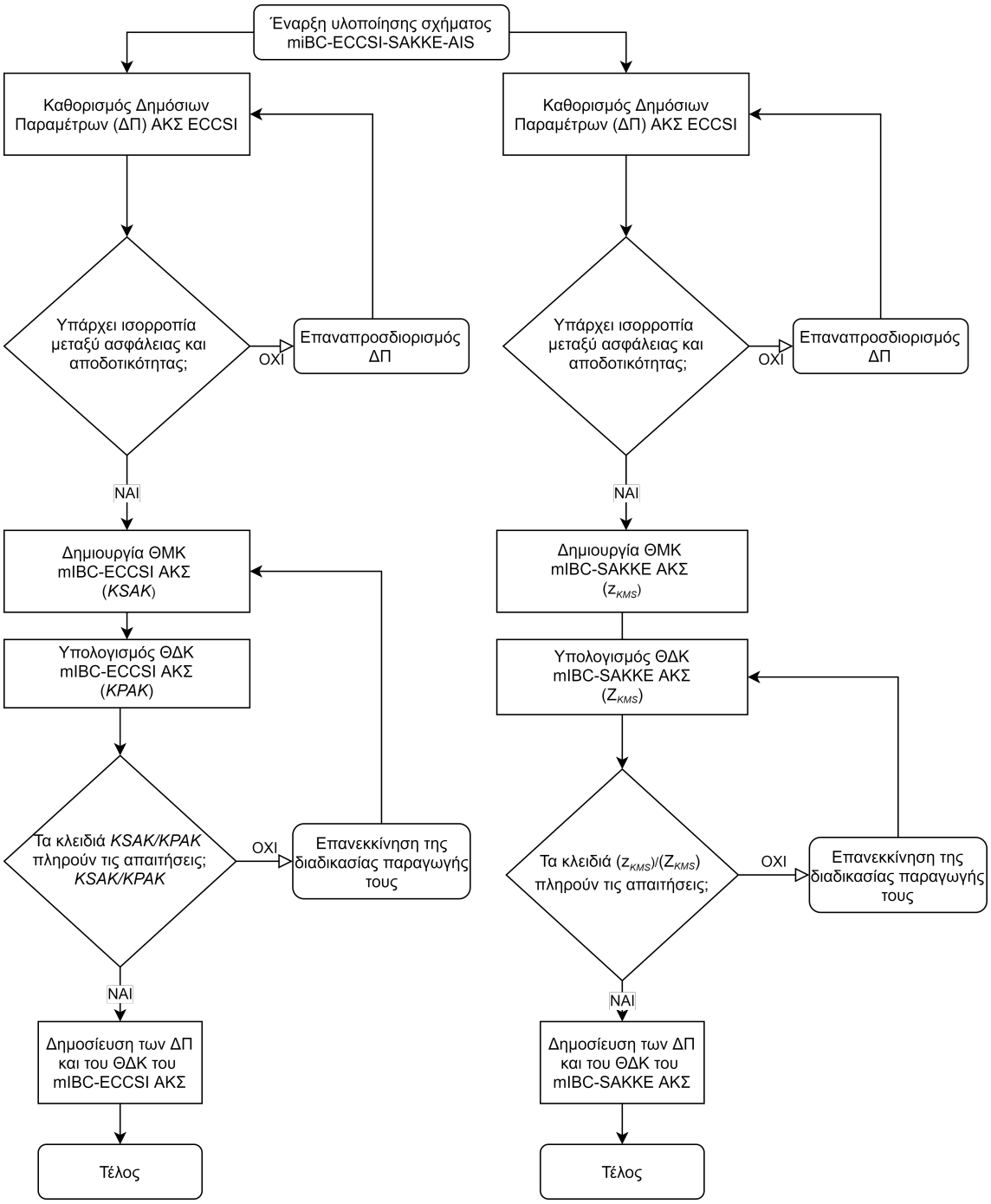
Στον αριστερό κλάδο του Σχήματος 8.1 απεικονίζεται η ροή διεργασιών για την ενεργοποίηση ενός ΑΚΣ (mIBC-AIS-ECCSI-KMS.

Η διαδικασία κατασκευής των κλειδιών $MMSIa_{SSK}$/$MMSIa_{PVT}$ ψηφιακής υπογραφής ενός σκάφους A με δημόσιο αναγνωριστικό $MMSIa$, το οποίο εγγράφηκε στην υποδομή mIBC-AIS-ECCSI-KMS, περιλαμβάνει:

- Την επιλογή του $MMSIa_{PVT}$ του σκάφους.
- Την εξαγωγή του ιδιωτικού κλειδιού ($MMSIa_{SSK}$) του, με τη χρήση του Δημόσιου Τεκμηρίου Επικύρωσης (ΔΤΕ)/Public Validation Token($MMSIa_{PVT}$) και του $MMSIa$ του.
- Την επαλήθευσή τους.

Προς τούτο:

1. Επιλογή του $MMSIa_{PVT}$:
   (α΄) Επιλέγουμε v, τυχαίο (εφήμερο), μη-μηδενικό στοιχείο του F_q.
   (β΄) Υπολογίζουμε το $MMSIa_{PVT} = [v]G_{Gr}$.
2. Υπολογισμός του $MMSIa_{SSK}$:
   (α΄) Υπολογίζουμε τη σύνοψη $HS_a = hash(G_{Gr}||KPAK_{Gr}||MMSIa||MMSIa_{PVT})$.
   (β΄) Υπολογίζουμε το $MMSIa_{SSK} = (KSAK_{Gr} + HS_a * v)$ modulo q.
   (γ΄) Ελέγχουμε αν το $MMSIa_{SSK}$ ή το HS_a είναι μηδέν modulo q. Εάν ναι, τότε το $MMSIa_{SSK}$ είναι ΜΗ-ΕΓΚΥΡΟ και η διαδικασία εξαγωγής του πρέπει να επαναληφθεί.



Σχήμα 8.1: Διάγραμμα ροής διεργασιών υλοποίησης ενός διπλού ΑΚΣ/(KMS), του KMS-ECCSI (αριστερός κλάδος) και KMS-SAKKE (δεξιός κλάδος), σ' ένα σχήμα mIBC-AIS ECCSI-SAKKE.

(δ΄) Εξάγουμε το ζεύγος $(MMSIa_{SSK}, MMSIa_{PVT})$. Σημειώνουμε ότι το v πρέπει να διαγραφεί.

3. Ο χρήστης πρέπει να επικυρώσει το ζεύγος $MMSIa_{SSK}/MMSIa_{PVT}$ πριν τα χρησιμοποιήσει, ακολουθώντας τα παρακάτω βήματα:

   (α΄) Ελέγχει ότι $MMSIa_{PVT} \in EC$.

   (β΄) Υπολογίζει το $HS = hash(G_{Gr}||KPAK_{Gr}||MMSIa||MMSIa_{PVT})$, το οποίο είναι στατικό, οπότε ο χρήστης μπορεί να το αποθηκεύσει ώστε να μη χρειάζεται να το υπολογίζει κάθε φορά.

   (γ΄) Ελέγχει αν $KPAK_{Gr} = [MMSIa_{SSK}]G_{Gr} - [HS_a]MMSIa_{PVT}$.

Περισσότερες λεπτομέρειες υπάρχουν στην υποενότητα 2.3.2 της διατριβής και στις υποενότητες 5.1.1 και 5.1.2 του RFC6507.

Διαδικασία ψηφιακής υπογραφής των δεδομένων του AIS (AIS_{DATA}) από το σκάφος με MMSIa

Δεδομένα Εισόδου

1. Τα δεδομένα AIS (AIS_{DATA}) που θα υπογραφούν ψηφιακά.
2. Το αναγνωριστικό ($MMSIa$) του υπογράφοντος σκάφους.
3. Το ιδιωτικό κλειδί ($MMSIa_{SSK}$) του υπογράφοντος σκάφους.
4. Το $MMSIa_{PVT}$ του υπογράφοντος σκάφους.
5. Το Δημόσιο Κλειδί ($KPAK_{Gr}$) του ΑΚΣ/KMS του υπογράφοντος σκάφους.

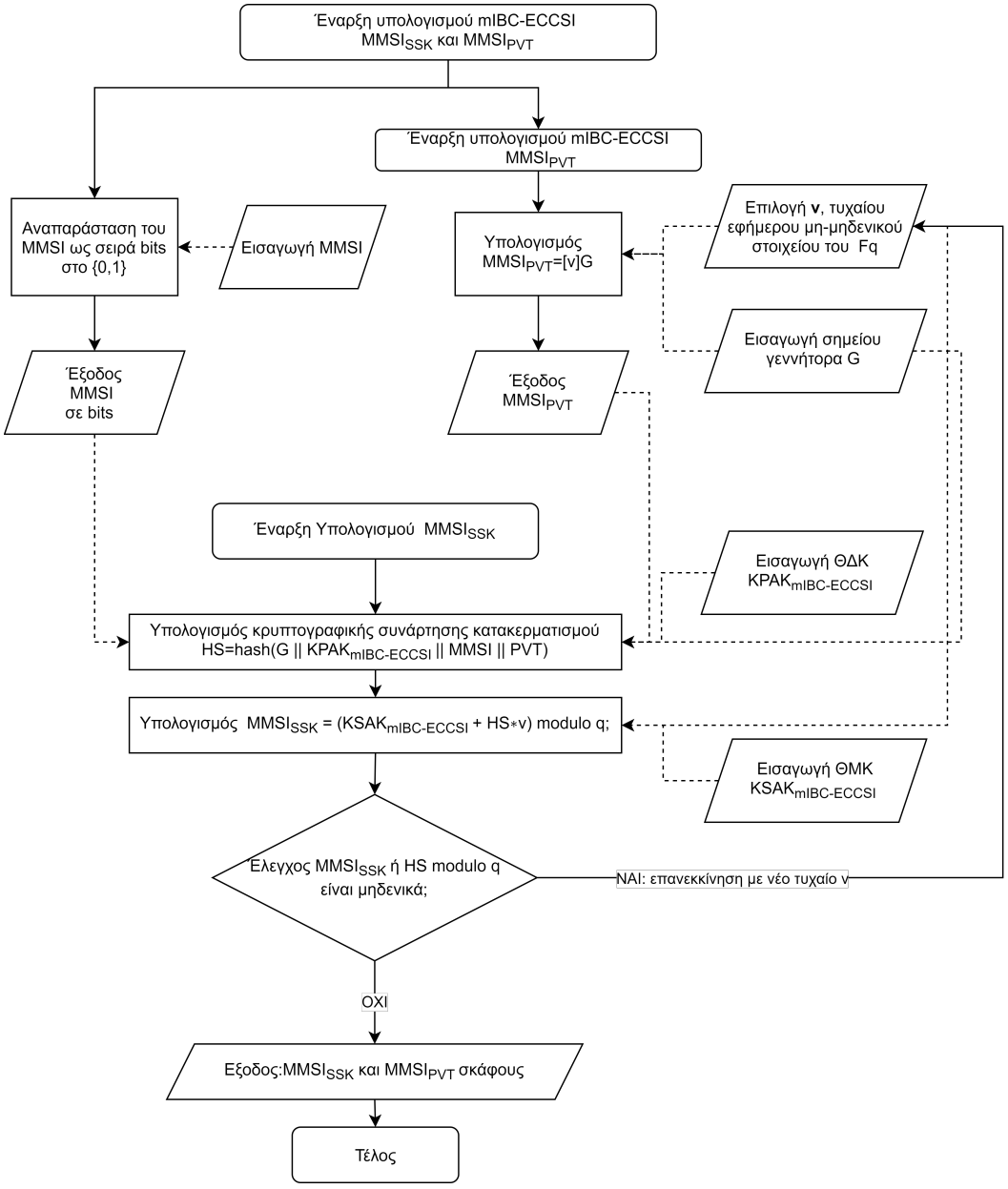
Αλγόριθμος

Η διαδικασία ψηφιακής υπογραφής του μηνύματος (AIS_{DATA}) από την εφαρμογή mIBC-AIS-App A περιλαμβάνει:

1. Επιλογή τυχαίου (εφήμερου), μη-μηδενικού στοιχείου $j \in F_q$.
2. Υπολογισμός του $J = (Jx, Jy)$ τ.ω. $J = [j]G_{Gr}$. Στη συνέχεια θέτουμε $r = Jx$, δηλαδή το r ισούται με την τετμημένη Jx του J.
3. Υπολογισμός του $HS = hash(G_{Gr}||KPAK_{Gr}||MMSIa||MMSIa_{PVT})$. Εάν έχουμε αποθηκεύσει το HS δεν χρειάζεται να το υπολογίσουμε ξανά.
4. Υπολογισμός της σύνοψης $HE = hash(HS_A||r||m)$.
5. Έλεγχος εάν ισχύει η σχέση $(HE + r * MMSIa_{SSK})\ modulo\ q \neq 0$. Εάν ναι, η ψηφιακή υπογραφή είναι έγκυρη, αλλιώς η διαδικασία πρέπει να επαναληφθεί με νέο $j \in F_q$.
6. Υπολογισμός του $s' = ((\frac{1}{HE+r*MMSIa_{SSK}}) * j)\ modulo\ q$. Μετά τον υπολογισμό η τιμή j πρέπει να καταστρέφεται.
7. Θέτουμε $s = s'$ ή, εάν s' είναι πολύ μεγάλο, τότε θέτουμε $s = q - s'$.

Αποτέλεσμα

Η ψηφιακή υπογραφή είναι η τριάδα $(s, r, MMSIa_{PVT})$.



Σχήμα 8.2: Διάγραμμα ροής των διεργασιών που εμπλέκονται στον υπολογισμό του ιδιωτικού κλειδιού του σκάφους στη λειτουργία mIBC-ECCSI-AIS (mode 2)

Διαδικασία ελέγχου της εγκυρότητας ψηφιακά υπογεγραμμένων δεδομένων του AIS

Δεδομένα Εισόδου

1. Η ψηφιακή υπογραφή $(s, r, MMSIa_{PVT})$.
2. Το υπογεγραμμένο μήνυμα (AIS_{DATA}).
3. Το δημόσιο αναγνωριστικό $(MMSIa)$ του υπογράφοντος σκάφους.
4. το Δημόσιο Κλειδί $(KPAK_{Gr})$ του ΑΚΣ/KMS του υπογράφοντος σκάφους.

Αλγόριθμος

1. Έλεγχος αν $MMSIa_{PVT} \in EC$.
2. Υπολογισμός του $HS = hash(G_{Gr}||KPAK_{Gr}||MMSIa||MMSIa_{PVT})$.
3. Υπολογισμός $HE = hash(HS_{Gr}||r||AIS_{DATA})$.
4. Υπολογισμός $Y = [HS]MMSIa_{PVT} + KPAK_{Gr}$.
5. Υπολογισμός $J = [s]([HE]G_{Gr} + [r]Y)$.

Αποτέλεσμα

6. Εάν $Jx = r \, modulo \, q$ και $Jx \, modulo \, q \neq 0$, η Ψηφιακή Υπογραφή είναι έγκυρη, αλλιώς η υπογραφή θεωρείται άκυρη.

Περισσότερες λεπτομέρειες υπάρχουν στην υποενότητα 2.3.2 της διατριβής και στις υποενότητες 5.2.1 και 5.2.2 του RFC6507.

8.3.2 Διαδικασίες υλοποίησης του ΑΚΣ (mIBC-AIS-SAKKE-KMS) που υποστηρίζει τη λειτουργία mIBC-SAKKE-AIS (mode 4)

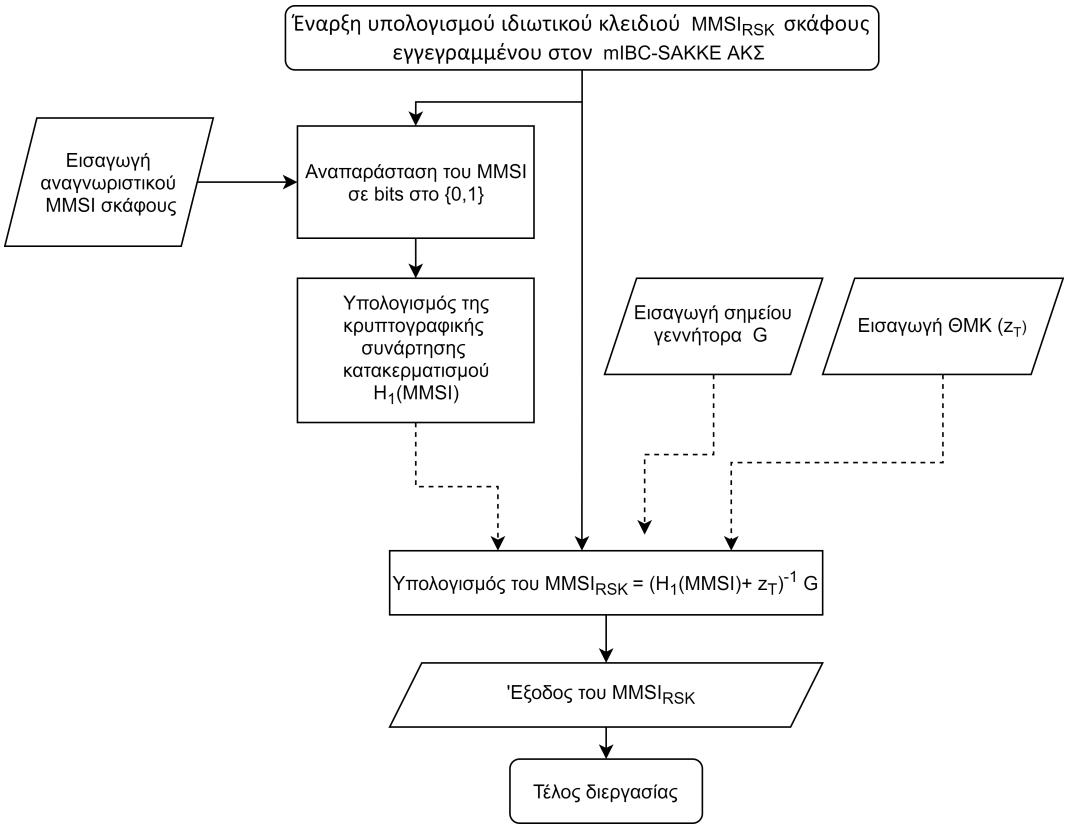
Στην ενότητα αυτή περιγράφουμε τις διαδικασίες υλοποίησης ενός ΑΚΣ (mIBC-AIS-SAKKE-KMS) και τις διαδικασίες ενθυλάκωσης και αποθυλάκωσης υλικού για τη δημιουργία συμμετρικού κλειδιού συνόδου. Ως παράδειγμα θεωρούμε τον $ΚΜΣ_{No}$, που υποστηρίζει τη λειτουργία mIBC-SAKKE-AIS (mode 4), δημιουργία ιδιωτικού κλειδιού $MMSIb_{RSK}$ για το σκάφος 'b' με MMSI = MMSIb.

Στον δεξιό κλάδο του Σχήματος 8.1 απεικονίζεται η ροή διεργασιών για την ενεργοποίηση ενός ΑΚΣ (mIBC-AIS-SAKKE-KMS).

Οι δημόσιες παράμετροι του μηχανισμού mIBC-SAKKE είναι οι: $p, n, q, EC, G_{No}, g =< G, G >, Hash$. Περισσότερες λεπτομέρειες υπάρχουν στην ενότητα 2.3.3 της διατριβής και στο RFC6508.

Κατασκευή των Θεμελιωδών κλειδιών (Z_{No} / z_{No}) του SAKKE-KMS$_{No}$

1. Επιλογή του z_{No} ως Θεμελιώδους Μυστικού κλειδιού του ΑΚΣ : επιλέγεται τυχαίος ακέραιος αριθμός $(z_{No}) \in (2, q-1]$.
2. Υπολογισμός του Z_{No} ως Θεμελιώδους Δημόσιου κλειδιού του ΑΚΣ : Υπολογίζεται το $Z_{No} = [z_{No}]G_{No}$, όπου $G_{No}(G_x, G_y) \in EC$ και γεννήτορας της υποομάδας τάξης



Σχήμα 8.3: Ροή διαδικασιών για τη δημιουργία του ιδιωτικού κλειδιού του σκάφους $MMSI_{RSK}$ από τον SAKKE-KMS.

q. Η πράξη είναι πολλαπλασιασμός σημείου που ανήκει στην EC με ακέραιο αριθμό.

Εξαγωγή του Ιδιωτικού κλειδιού του σκάφους $MMSIb_{RSK}$

Στο πλαίσιο αυτού του παραδείγματος θα υπολογίσουμε το ιδωτικό κλειδί $MMSIb_{RSK}$ του δέκτη, που είναι το σκάφος με $MMSI_{Receiver} = MMSIb$ το οποίο ανήκει στον ΑΚΣ $KMS - No$. Προς τούτο:

1. Υπολογισμός του: $MMSIb_{RSK} = \frac{G_{No}}{MMSIb+z_{No}}$.
2. Έλεγχος, μέσω της εφαρμογής mIBC-AIS-App του σκάφους με $MMSIb$, για το εάν ισχύει η ισότητα $< [b]G_{No} + Z_{No}, MMSIb_{RSK} >= g$. Εάν ναι, το Ιδιωτικό Κλειδί γίνεται αποδεκτό, ειδάλλως απορρίπτεται.

Περισσότερες λεπτομέρειες υπάρχουν στην ενότητα 2.3.3 της διατριβής και στην υποενότητα 6.1.2 του RFC6508.

Εμπιστευτική ενθυλάκωση μέσω του μηχανισμού SAKKE

Σ΄ αυτό το παράδειγμα, το σκάφος εκπομπής μέσω της εφαρμογής mIBC-AIS-App σχηματίζει την Κοινή Μυστική Τιμή (SSV) και την αποστέλλει ενθυλακωμένη στο σκάφος δέκτη ($MMSIb$). Υπενθυμίζουμε ότι η διαδικασία της ενθυλάκωσης δεν προϋποθέτει να έχει ήδη κάποιου είδους κλειδί ο δέκτης ($MMSIb$), συνεπώς μπορεί να προηγείται της διαδικασίας απόδοσης ιδιωτικού κλειδιού που παρουσιάστηκε

παραπάνω. Φυσικά ισχύει η προϋπόθεση ότι ο δέκτης θα ζητήσει ιδιωτικό κλειδί που θα αντιστοιχεί στο δημόσιο αναγνωριστικό *MMSIb* που έχει χρησιμοποιήσει ο αποστολέας.

Δεδομένα Εισόδου

1. Αναγνωριστικό Παραλήπτη: $ID_{Receiver} = MMSIb$
2. Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ παραλήπτη: Z_{No}

Αλγόριθμος

Τα βήματα του Αποστολέα A είναι:

1. Επιλογή ως SSV τυχαίου (εφήμερου) ακέραιου, μη-μηδενικού στοιχείου, $SSV \in (0, 2^n - 1]$.
2. Υπολογισμός του: $r = HashToIntegerRange(SSV||MMSIb, q, Hash)$.
3. Υπολογισμός του: $R_{MMSIb} = [r]([MMSIb]G_{No} + Z_{No}) \in E(F_p)$ Hint, (H).
4. Υπολογισμός του g^r[2].
5. Υπολογισμός του $H := SSV \oplus HashToIntegerRange(g^r, 2^n, Hash)$.

Αποτέλεσμα

6. Τα ενθυλακωμένα δεδομένα προς αποστολή στον MMSIb είναι τα: (R_{MMSIb}, H).

Περισσότερες λεπτομέρειες υπάρχουν στην ενότητα 2.3.3 της διατριβής και στην υποενότητα 6.2.1 του RFC6508.

Εμπιστευτική αποθυλάκωση μέσω του μηχανισμού SAKKE

Σ΄ αυτό το παράδειγμα ο Παραλήπτης ($ID_{Receiver} = B$) παραλαμβάνει τα ενθυλακωμένα δεδομένα $(R_{(B,S)}, H)$ και, μέσω της εφαρμογής mIBC-AIS-App, τα αποθυλακώνει και εξάγει το μυστικό υλικό SSV για τη δημιουργία του συμμετρικού κλειδιού συνόδου.

Δεδομένα Εισόδου

1. Ιδιωτικό κλειδί (ΙΚ) παραλήπτη: $MMSI_{RSK}$
2. Θεμελιώδες Δημόσιο Κλειδί ΑΚΣ παραλήπτη: Z_{No}

Αλγόριθμος

1. Εξαγωγή των R_{MMSIb} και H από τα ενθυλακωμένα δεδομένα $(R_{B,Y}, H)$.
2. Υπολογισμός του $w :=< R_{MMSIb}, MMSI_{RSK} >$.
3. Υπολογισμός του $SSV = H \oplus HashToIntegerRange(w, 2^n, Hash)$.
4. Υπολογισμός του $r = HashToIntegerRange(SSV||MMSIb, q, Hash)$.
5. Υπολογισμός του $TEST = [r]([MMSIb]G_{No} + Z_{No}) \in E(F_p)$.

[2]Περισσότερες πληροφορίες στην ενότητα 2.1, σελ.5 ατο RFC6508

Αποτέλεσμα

6. Τα ενθυλακωμένα δεδομένα γίνονται αποδεκτά μόνο εάν ισχύει η ισότητα $TEST = R_{MMSIb}$, ειδάλλως απορρίπτονται.
7. Εξαγωγή του SSV.

8.4 Το περιβάλλον της πειραματικής υλοποίησης

Προκειμένου να ελέγξουμε την εγκυρότητα των αποτελεσμάτων μας αναπτύξαμε ένα περιβάλλον πειραματικής υλοποίησης της υποδομής mIBC-AIS με τα παρακάτω κύρια χαρακτηριστικά:

1. Χρησιμοποιούμε τις κρυπτογραφικές τιμές του «Παραρτήματος Α: Δεδομένα δοκιμής» που παρουσιάζονται στα RFC6507 (ECCSI) και RFC6508 (SAKKE).
2. Χρησιμοποιούμε συμβατικά μηνύματα AIS τύπου 6, 8 ως φορείς των κρυπτογραφικών παραμέτρων mIBC-AIS (βλ. ενότητα 6.7).
3. Η εφαρμογή mIBC-AIS (βλ. ενότητα 6.8) αναπτύχθηκε σε Java.
4. Εξομοιώνουμε τις συμβατικές συσκευές AIS χρησιμοποιώντας έναν αποκωδικοποιητή AIS VDM/VDO τρίτου μέρους ως δέκτη των μηνυμάτων AIS τύπου 6, 8 που κατασκευάζονται από την εφαρμογή mIBC-AIS.

Τα πλεονεκτήματα της παραπάνω προσέγγισης είναι:

- Μπορούμε να ελέγξουμε την εγκυρότητα του κώδικα της πειραματικής υλοποίησης, του κώδικα της mIBC-AIS-app, των δημιουργούμενων κρυπτογραφικών παραμέτρων, καθώς και τη μεταφορά τους μέσω των συμβατικών μηνυμάτων AIS τύπου 6, 8, συγκρίνοντας απλώς τα αποτελέσματά μας με αυτά στο ¨Παράρτημα Α: Δεδομένα δοκιμής¨ των αντίστοιχων RFCs.
- Δοκιμάζουμε τη λειτουργία της υποδομής mIBC-AIS σ' ένα κρυπτογραφικό περιβάλλον, με υψηλότερο επίπεδο ασφάλειας από αυτό που ίσως να είναι πραγματικά απαραίτητο. Αυτή η προσέγγιση όχι μόνο δεν διευκολύνει την πειραματική υλοποίηση, αλλά προσθέτει στο συνολικό μέγεθος των μεταδιδόμενων δεδομένων και κατά συνέπεια στην πολυπλοκότητα της υλοποίησης. Για παράδειγμα, στην πραγματική λειτουργία mIBC-ECCSI-AIS της mIBC το αναγνωριστικό κάθε σκάφους θα είναι το 9ψήφιο MMSI του, αλλά στην πειραματική υλοποίηση χρησιμοποιούμε ως αναγνωριστικό το προτεινόμενο στο Παράρτημα ¨Α: Δεδομένα δοκιμής¨ του RFC 6507 δηλαδή το "2011-02\0tel:+447700900123\0".

Ο Πίνακας 8.1 παρουσιάζει τη συσχέτιση μεταξύ των κρυπτογραφικών παραμέτρων της mIBC όπως περιγράφονται σ' αυτήν τη διατριβή και των κρυπτογραφικών παραμέτρων του Παραρτήματος ¨Α: Δεδομένα δοκιμής¨ των RFCs, [2], [3] που χρησιμοποιούμε στην πειραματική υλοποίηση.

8.4.1 Μεταφορά κρυπτογραφικών δεδομένων

Τα κρυπτογραφικά δεδομένα της υποδομής mIBC-AIS μεταφέρονται μέσω της συμβατικής υποδομής AIS και τα ειδικού τύπου μηνύματα (τύποι 6 και 8)

Ονομασία ΑΚΣ	Πειραματική υλοποίηση IMO-mIBC-KMS (Key Management Serve)
Δημόσια Δεδομένα	Δημόσια Δεδομένα των RFCs
mIBC-Authenticated-AIS (mode 2)	Δημιουργία ψηφιακής υπογραφής τυχαίου μηνύματος AIS τύπου 1 (θέσης/κατάστασης σκάφους) και ενθυλάκωσή της σε μήνυμα AIS τύπου 8
Το Αναγνωριστικό του σκάφους εκπομπής	Ως MMSI του σκάφους εκπομπής χρησιμοποιούμε το 2011-02\0tel:+447700900123\0 (RFC6507 Appendix A')
Το Ιδιωτικό κλειδί του σκάφους εκπομπής	Ως $MMSI_{Private}$ χρησιμοποιούμε το Signer Secret Key (SSK) (RFC6507 Appendix A'). Λόγω μεγάλου μεγέθους παραλείπεται η παρουσίασή του.
Το $MMSI_{PVT}$ του σκάφους εκπομπής	Ως $MMSI_{PVT}$ χρησιμοποιούμε το Public Validation Token (PVT) (RFC6507 Appendix A'). Λόγω μεγάλου μεγέθους παραλείπεται η παρουσίασή του.
mIBC-SAKKE-AIS (mode 4)	Ενθυλάκωση βάσει μηχανισμού SAKKE και εκ νέου ενθυλάκωση σε μήνυμα AIS τύπου 6
Το Αναγνωριστικό του σκάφους δέκτη	Ως $MMSI_{Recipient}$ χρησιμοποιούμε το 3230 31312D30 32007465 6C3A25B34 34373730 30 39030 31323300 (RFC6508 Appendix A')
Το Ιδιωτικό κλειδί του σκάφους δέκτη	Ως $MMSI_{Recipient-Private}$ χρησιμοποιούμε το Receiver Secret Key (RSK) (RFC6508 Appendix A')

Πίνακας 8.1: Συσχέτιση μεταξύ των κρυπτογραφικών παραμέτρων της mIBC όπως περιγράφονται σ' αυτήν τη διατριβή και των κρυπτογραφικών παραμέτρων των RFCs, [2], [3] που χρησιμοποιούμε στην πειραματική υλοποίηση.

χρησιμοποιούνται για τη μεταφορά δεδομένων τρίτων εφαρμογών. Στο κεφάλαιο 6 παρουσιάσαμε αναλυτικά τη δομή των συγκεκριμένων μηνυμάτων, καθώς και το θεωρητικό υπόβαθρο της παραπάνω προσέγγισης. Επίσης, αναδείξαμε την ομοιότητα της δομής των δύο τύπων μηνυμάτων καθώς και το γεγονός ότι η μοναδική πρακτικά διαφορά τους είναι ότι στο μήνυμα AIS ADDRESSED BINARY MESSAGE (Τύπος 6) υπάρχει ένα επιπλέον πεδίο όπου προστίθεται το MMSI του αποδέκτη της εκπομπής.

Στην πειραματική υλοποίηση χρησιμοποιούμε ως μεταφορέα των κρυπτογραφικών δεδομένων το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπος 8) για την επίδειξη των λειτουργιών mIBC-ECCSI-AIS (mode 2) και mIBC-SAKKE-AIS (mode 4). Συγκεκριμένα, τα κρυπτογραφικά δεδομένα των παραρτημάτων ¨A: Δεδομένα δοκιμής¨ των RFCs, [2], [3] που χρησιμοποιούμε στην πειραματική υλοποίηση:

- στη μεν λειτουργία mIBC-ECCSI-AIS (mode 2) μεταφέρονται από δύο μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8). Το πρώτο μεταφέρει το δημόσιο κλειδί (PVT) του αποστολέα, το οποίο μπορεί να αποθηκευτεί για μελλοντική χρήση. Το δεύτερο μεταφέρει ψηφιακά υπογεγραμμένο πρωτότυπο μήνυμα AIS.
- στη δε λειτουργία mIBC-SAKKE-AIS (mode 4) μεταφέρονται από τρία μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8).

8.4.2 Η εξομοίωση των συμβατικών συσκευών AIS

Για να επιδειχθεί ότι το προτεινόμενο mIBC-AIS λειτουργεί πάνω από τη συμβατική υποδομή του AIS χωρίς να επηρεάζεται η λειτουργία του, θα πρέπει να δείξουμε ότι

είναι συμβατό με τους αποκωδικοποιητές των σημάτων AIS. Ελλείψει συσκευής εκπομπής και λήψης σημάτων AIS, εξομοιώσαμε τις συσκευές μέσω λογισμικού. Η συσκευή εκπομπής που χρησιμοποιεί την ειδική εφαρμογή mIBC-AIS-app για να δημιουργήσει τα κρυπτογραφικά δεδομένα και να τα ενθυλακώσει σε ένα μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) εξομοιώνεται μέσω δικού μας κώδικα γραμμένου σε Java. Όμως, προκειμένου να διασφαλίσουμε ότι τα κρυπτογραφικά δεδομένα φτάνουν αναλλοίωτα στο δέκτη χρησιμοποιήσαμε ως συσκευή αποκωδικοποίησης τον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO και συγκεκριμένα τη διεύθυνση `https://www.maritec.co.za/tools/aisvdmvdodecoding/` όπως ήταν στις 23/9/2019, στον οποίο αντιγράφουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) και εξάγουμε τα κρυπτογραφικά δεδομένα.

8.4.3 Η εφαρμογή mIBC-AIS-App

Η εφαρμογή mIBC-AIS-App είναι υπεύθυνη για όλες τις επιπρόσθετες δυνατότητες που προσφέρει η υποδομή mIBC-AIS στις συμβατικές συσκευές AIS. Στην πειραματική υλοποίηση ο κώδικας της εφαρμογής mIBC-AIS-App υποστηρίζει τις λειτουργίες mIBC-ECCSI-AIS (mode 2), mIBC-Anonymous-AIS (mode 3) και mIBC-SAKKE-AIS (mode 4). Η εφαρμογή είναι γραμμένη σε Java και επιτρέπει την ενσωμάτωση οποιουδήποτε ανοικτού πηγαίου κώδικα και κρυπτογραφικών βιβλιοθηκών. Στην ενότητα 8.4.4 αναφέρουμε κώδικα τρίτων που χρησιμοποιήσαμε.

Επισημαίνουμε ότι σε κάθε υλοποίηση της mIBC-AIS το δημόσιο αναγνωριστικό του σκάφους είναι το MMSI του και συνεπώς όλες οι κρυπτογραφικές λειτουργίες θα πρέπει να γίνονται βάσει αυτού. Όμως, στην πειραματική υλοποίηση χρησιμοποιούμε ως δημόσια αναγνωριστικά τα αναγνωριστικά που χρησιμοποιούνται στα Παραρτήματα Α των RFCs, τα οποία είναι διαφορετικά από το MMSI του αρχικού μηνύματος AIS τύπου 1 που έχουμε ως παράδειγμα μηνύματος AIS προς ψηφιακή υπογραφή και ενθυλάκωση. Συνεπώς, τονίζουμε ότι η διαφορά μεταξύ των MMSI του αρχικού μηνύματος AIS και του MMSI του μηνύματος φορέα (τύπου 6, 8) των κρυπτογραφικών δεδομένων δεν επηρεάζει καθόλου την αξιοπιστία της πειραματικής υλοποίησης μεν, αλλά σε μια πραγματική εφαρμογή θα καθιστούσε άκυρη την ψηφιακή υπογραφή και την αποθυλάκωση.

8.4.4 Κώδικας τρίτων που χρησιμοποιούμε στην πειραματική υλοποίηση

Παρακάτω παραθέτουμε κώδικα τρίτων μερών που χρησιμοποιήθηκε στην πειραματική υλοποίηση.

1. Στον κώδικά μας χρησιμοποιούμε τις κρυπτογραφικές βιβλιοθήκες Java ανοικτού κώδικα που παρέχονται από το Legion of the Bouncy Castle Inc. (ABN 84 166 338 567), `https://www.bouncycastle.org/java.html` . Η εν λόγω επιλογή έγινε διότι θεωρείται ότι πρόκειται για αξιόπιστες κρυπτογραφικές βιβλιοθήκες Java με άδεια τύπου MIT.
2. Ορισμένα μέρη του κώδικά μας, είτε ανήκουν είτε βασίζονται στην υλοποίηση ανοικτού κώδικα ECCSI-SAKKE (RFC6507-RFC6508), MIKEY-SAKKE

(RFC6509) όπως αυτή υπήρχε το 2019 στο GitHub, `https://github.com/jim-b/ECCSI-SAKKE` με το όνομα jim-b / ECCSI-SAKKE.

8.4.5 Παράδειγμα της μεθοδολογίας επίδειξης

Ως παράδειγμα παραθέτουμε (εν συντομια) τα βήματα της επίδειξης στο Σχήμα 8.4 και τα αντίστοιχα βήματα της επίδειξης ενός παραδείγματος λειτουργίας mIBC-ECCSI-AIS (mode 2), που απεικονίζονται στο Σχήμα 8.5.

1. Η είσοδος στην εφαρμογή mIBC-AIS-app περιέχει το αρχικό μήνυμα AIS, (AIS_{DATA}), στο οποίο προστίθεται μια χρονική σήμανση και ένα πρόσθετο αλφαριθμητικό (λειτουργικό της εφαρμογής μας) προκειμένου να σχηματιστεί το τελικό κείμενο που θα υπογραφεί ψηφιακά.

2. Η εφαρμογή mIBC-AIS-app υπογράφει ψηφιακά το τελικό κείμενο και εξάγει την ψηφιακή υπογραφή που αποτελείται από τις μεταβλητές r και s και το στατικό $MMSI_{Sender-PVT}, (PVTx, PVTy)$.

3. Το στατικό $MMSI_{Sender-PVT}, (PVTx, PVTy)$ ενσωματώνεται σε ένα μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8).

4. Τα AIS_{DATA} και οι μεταβλητές r και s της ψηφιακής υπογραφής είναι ενθυλακωμένες σε ένα άλλο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8).

Στη συνέχεια, για την επίδειξη της εκπομπής στον αέρα, τα δύο μηνύματα AIS τύπου 8 αντιγράφονται στον διαδικτυακό αποκωδικοποιητή που αναφέρθηκε στην ενότητα 8.4.2. Τέλος, ελέγχεται εάν τα αποθυλακωμένα δεδομένα μεταφέρθηκαν σωστά.

8.5 Επίδειξη της λειτουργίας mIBC-ECCSI-AIS (mode 2)

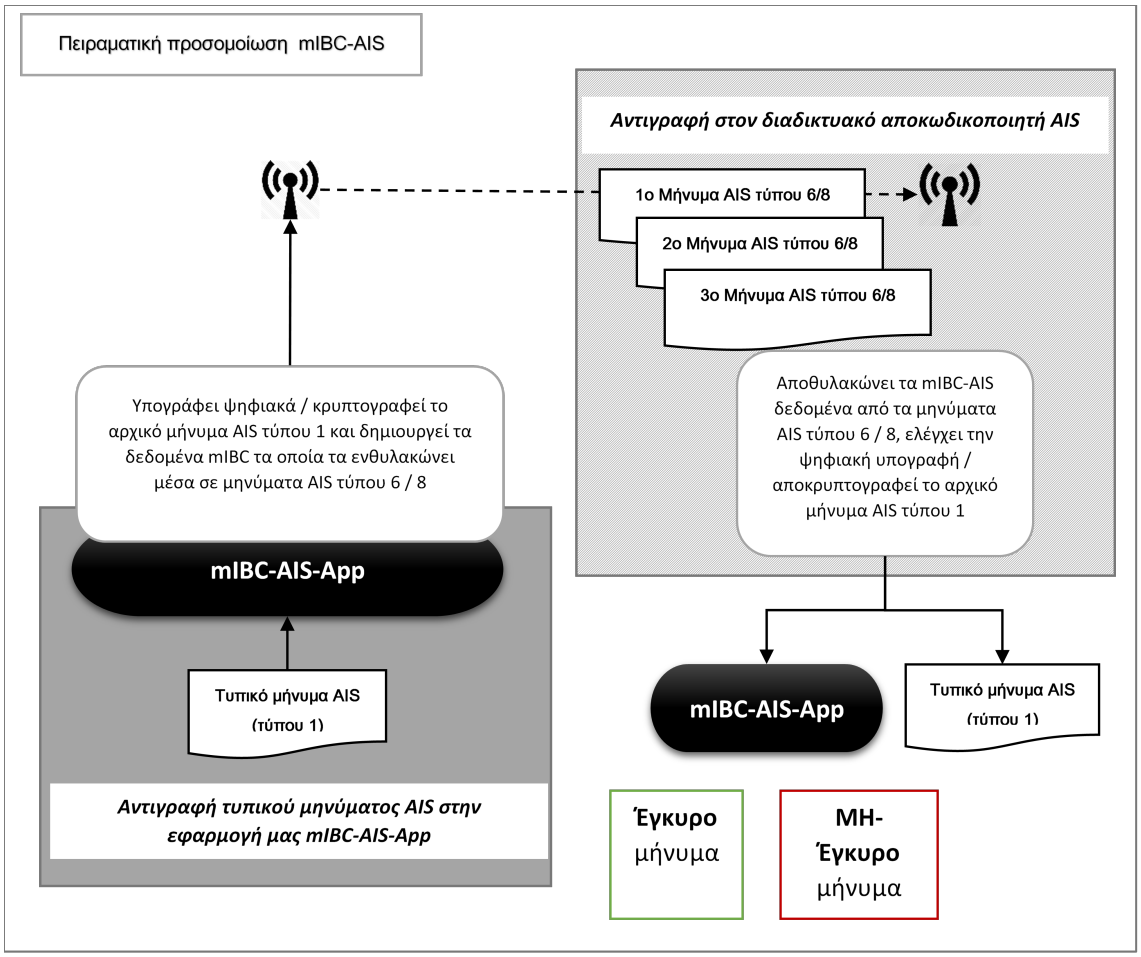
Στη λειτουργία mIBC-ECCSI-AIS (mode 2), κάθε συσκευή εφοδιασμένη με mIBC-AIS έχει τη δυνατότητα να υπογράφει ψηφιακά τα εκπεμπόμενα μηνύματα AIS_{DATA} με το ιδιωτικό κλειδί $MMSI_{SSK}$), ενώ οι δέκτες μπορούν να επικυρώσουν την αυθεντικότητα των δεδομένων AIS_{DATA} που ελήφθησαν ελέγχοντας την ψηφιακή υπογραφή τους. Εν συντομια, το παραπάνω σενάριο επιδεικνύεται ως εξής:

1. Ψηφιακή υπογραφή μηνύματος AIS τύπου 1 (positional) από την εφαρμογή mIBC-AIS-App.

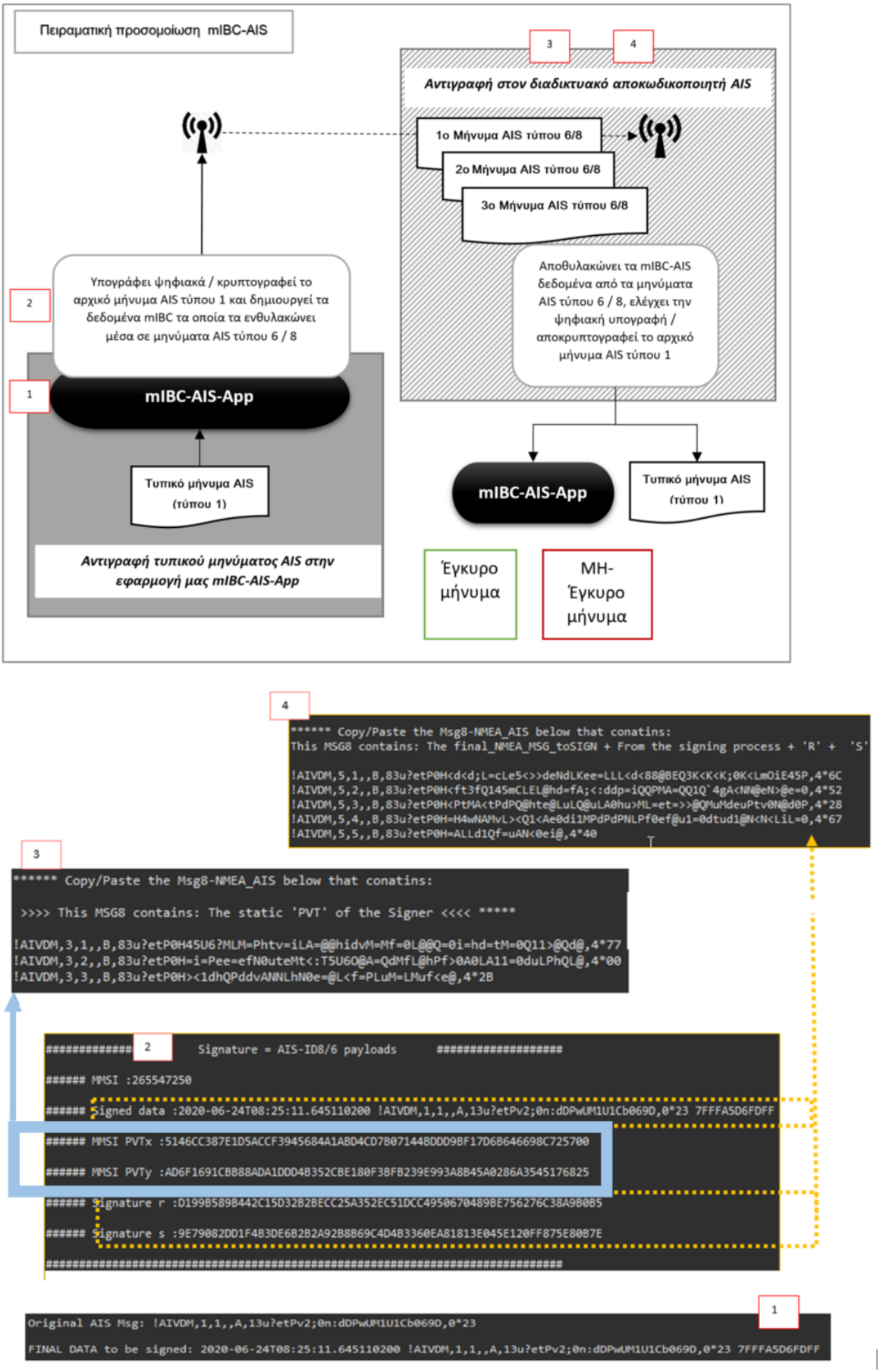
2. Έλεγχος της ψηφιακής υπογραφής του μηνύματος AIS τύπου 1 (positional) από την εφαρμογή mIBC-AIS-App.

3. Ενθυλάκωση της ψηφιακής υπογραφής σε μήνυμα AIS τύπου 8 από την εφαρμογή mIBC-AIS-App

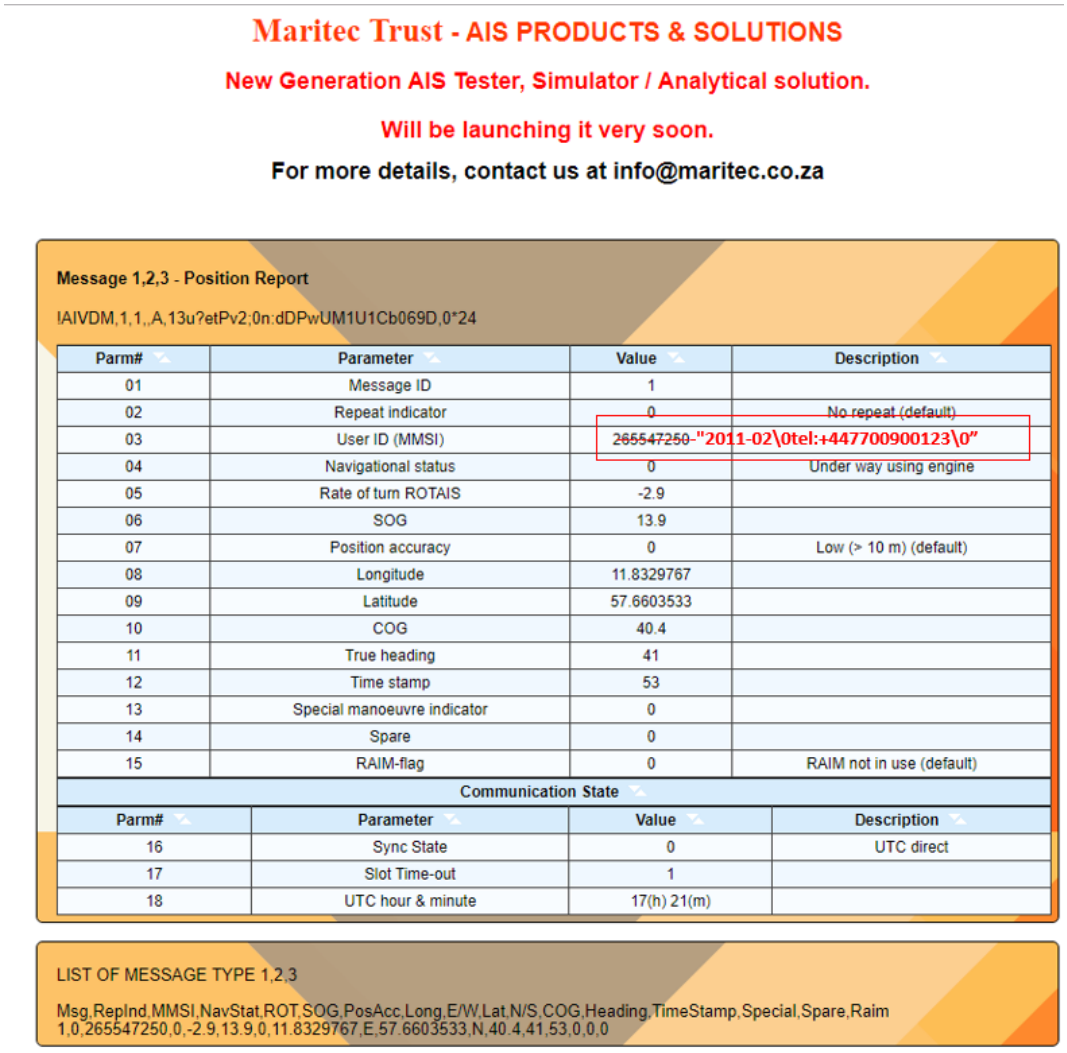
4. Επίδειξη της επικοινωνίας των mIBC-AIS δεδομένων μέσω των συμβατικών συσκευών AIS μέσω του διαδικτυακού αποκωδικοποιητή AIS VDM/VDO στον οποίο αντιγράφουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8).



Σχήμα 8.4: Τα κύρια βήματα της μεθοδολογίας επίδειξης.



Σχήμα 8.5: Παράδειγμα της μεθοδολογίας επίδειξης.



Σχήμα 8.6: Στιγμιότυπο οθόνης του αρχικού συμβατικού μηνύματος AIS τύπου 1 (positional) που υπογράφεται ψηφιακά.

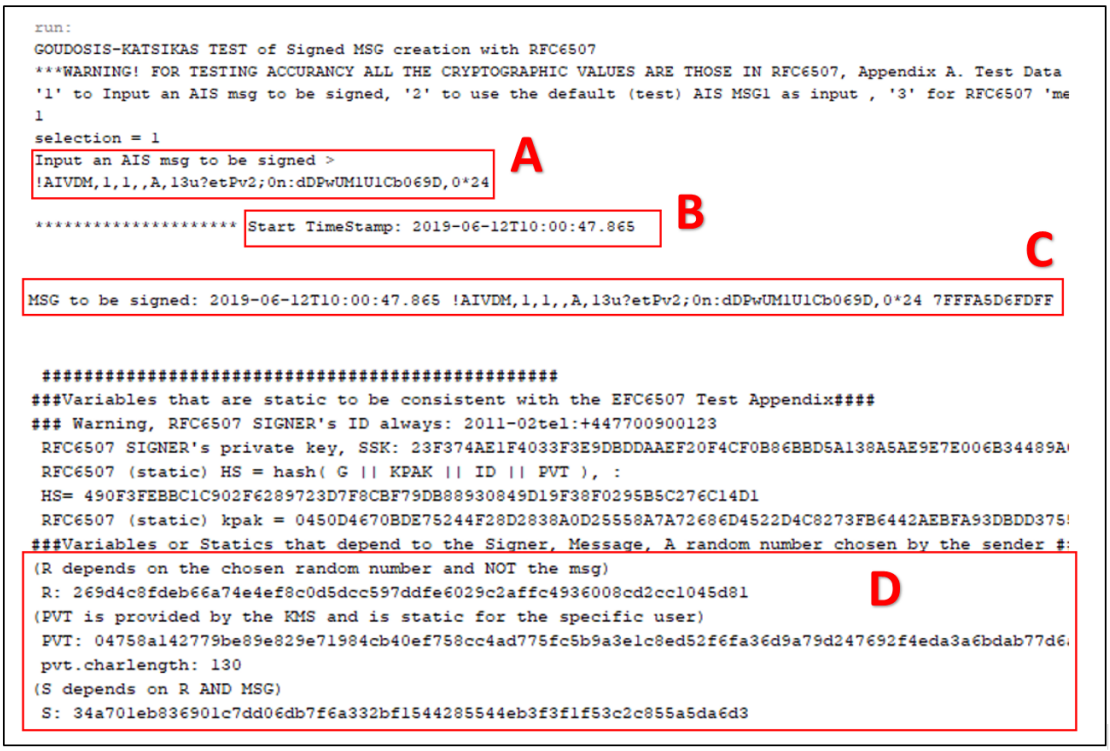
5. Επίδειξη του ελέγχου εγκυρότητας της ψηφιακής υπογραφής από τον δέκτη.

8.5.1 Επίδειξη ψηφιακής υπογραφής μηνύματος AIS από την εφαρμογή mIBC-AIS-App

Στο Σχήμα 8.6 παραθέτουμε το αρχικό μήνυμα AIS τύπου 1 το οποίο θα υπογραφεί ψηφιακά. Παρατηρήστε τη διαφορά που θα υπάρχει μεταξύ του MMSI του αυθεντικού μηνύματος και του MMSI στην ψηφιακή υπογραφή και το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) (με κόκκινο) όπως έχουμε εξηγήσει στην ενότητα 8.4.3.

8.5.2 Δημιουργία ψηφιακής υπογραφής του μηνύματος AIS τύπου 1

Η συσκευή AIS του πομπού στέλνει το αρχικό μήνυμα AIS για μετάδοση. Πριν το μήνυμα φτάσει στην κεραία AIS, η εφαρμογή mIBC-AIS το ανακόπτει και δημιουργεί



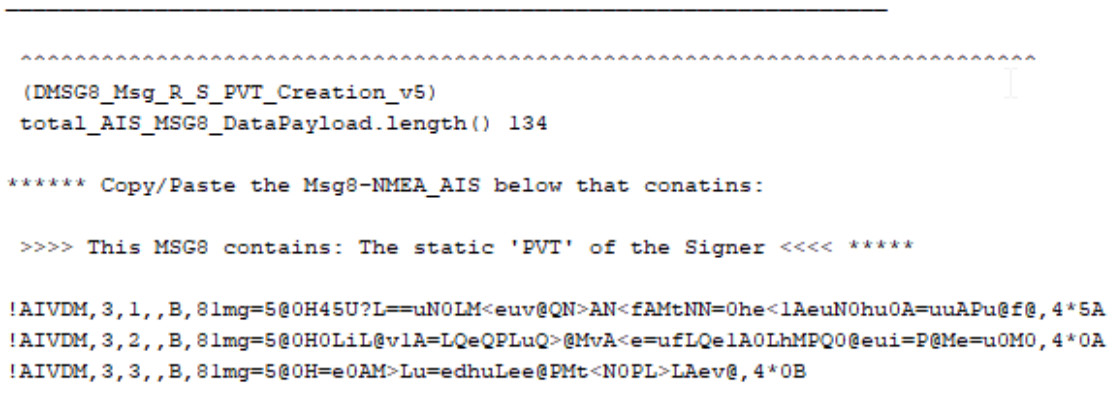
Σχήμα 8.7: Στιγμιότυπο οθόνης από την επίδειξη της δημιουργίας ψηφιακής υπογραφής.

την ψηφιακή υπογραφή ελέγχου εγκυρότητας του μηνύματος AIS.

Στην επίδειξη αντιγράφουμε το αρχικό μήνυμα AIS τύπου 1 (δηλαδή το "!AIVDM,1,1,A,13u?etPv2;0n:dDPwUM1U1Cb069D,0*24") στην εφαρμογή μας mIBC-AIS-App (βλ. Σχήμα 8.7, πεδίο A). Η εφαρμογή mIBC-AIS-App προσθέτει αυτόματα μια χρονοσήμανση (βλ. Σχήμα 8.7 πεδίο B), και έναν δεκαεξαδικό αριθμό για λειτουργικούς λόγους. Η προσθήκη της υπογεγραμμένης χρονοσήμανσης είναι απαραίτητη προς αποφυγή επιθέσεων επανάληψης μηνύματος (replay attacks), κατά τις οποίες κάποιος κακόβουλα μπορεί να χρησιμοποιήσει ετεροχρονισμένα καταγεγραμμένα ψηφιακά υπογεγραμμένα μηνύματα mIBC-AIS. Επομένως, ένα έγκυρο μήνυμα mIBC-AIS θα πρέπει να έχει έγκυρη υπογραφή και σωστή χρονική σήμανση.

Ο δεκαεξαδικός λειτουργικός αριθμός μεταφράζεται σε δυαδικό αριθμό προκειμένου να διατηρήσουμε την πληροφορία για το ποια γράμματα του αρχικού μηνύματος είναι κεφαλαία και ποια μικρά, διότι στη διαδικασία της ψηφιακής υπογραφής και της ενθυλάκωσης η συγκεκριμένη πληροφορία χάνεται. Επομένως, το τελικό μήνυμα που πρόκειται να οδηγηθεί προς ψηφιακή υπογραφή έχει την ακόλουθη μορφή: συνένωση των συμβολοσειρών [χρονοσήμανση] + [αρχικό μήνυμα AIS τύπου 1] + [βοηθητικός δεκαεξαδικός αριθμός], όπως φαίνεται στο Σχήμα 8.7, πεδίο C.

Τέλος, στο πεδίο D του Σχήματος 8.7 παρουσιάζονται τα αποτελέσματα της ψηφιακής υπογραφής S, R και η στατική τιμή PVT.



Σχήμα 8.8: Στιγμιότυπο οθόνης του μηνύματος AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει τη στατική παράμετρο PVT της ψηφιακής υπογραφής.

8.5.3 Ενθυλάκωση της ψηφιακής υπογραφής σε μήνυμα AIS τύπου 8

Πραγματοποιείται έλεγχος της ψηφιακής υπογραφής του μηνύματος AIS τύπου 1 (positional) και ενθυλάκωσή της σε αντίστοιχα μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8).

Η εφαρμογή μας mIBC-AIS-App διαχωρίζει την ψηφιακή υπογραφή σε στατικό και μεταβλητό μέρος και δημιουργεί τα αντίστοιχα μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8) με ενθυλακωμένες τις αντίστοιχες μεταβλητές της ψηφιακής υπογραφής. Τέλος, γίνεται έλεγχος της εγκυρότητας της ψηφιακής υπογραφής με τον ίδιο κώδικα που διαθέτει και ο δέκτης.

Στην πράξη, η ψηφιακή υπογραφή έχει δύο μέρη, ένα στατικό και ένα μεταβλητό.

- Το στατικό μέρος της υπογραφής είναι το (PVT), που είναι μοναδικό και είναι μαθηματικά συνδεδεμένο με το αναγνωριστικό $MMSI_{Sender-PVT}$ του σκάφους. Στο στιγμιότυπο οθόνης του Σχήματος 8.8 βλέπουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει τη στατική παράμετρο PVT της ψηφιακής υπογραφής. Σημειώνουμε ότι το συγκεκριμένο μήνυμα θα μπορούσε να μην αποστέλλεται μαζί με κάθε ψηφιακή υπογραφή, αλλά περιοδικά και τα σκάφη που το δέχονται για πρώτη φορά να το αποθηκεύουν για κάποιο χρονικό διάστημα.
- Το μεταβλητό μέρος της υπογραφής περιέχει τις μεταβλητές R και S, καθώς και το αρχικό μήνυμα AIS_{DATA}. Στο στιγμιότυπο οθόνης του Σχήματος 8.9 βλέπουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8), που ενθυλακώνει τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής.

Ο παραπάνω διαχωρισμός μάς επιτρέπει να χωρίσουμε την υπογραφή σε δύο ανεξάρτητα μέρη και να τα ενθυλακώσουμε σε δύο διαφορετικά μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8).

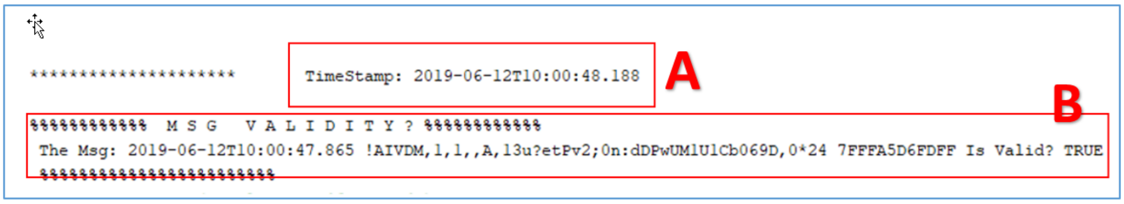
Τέλος, στο στιγμιότυπο οθόνης του Σχήματος 8.10 φαίνεται ο έλεγχος επικύρωσης της ορθότητας της ψηφιακής υπογραφής. Στο πεδίο A υπάρχει η χρονοσήμανση και στο πεδίο B το αποτέλεσμα του ελέγχου.

```
^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 (DMSG8_Msg_R_S_PVT_Creation_v5)
 total_AIS_MSG8_DataPayload.length() 218

****** Copy/Paste the Msg8-NMEA_AIS below that conatins:
This MSG8 contains: The original AIS Msg1 + From the signing process the the 'R' and  'S'

!AIVDM,5,1,,B,81mg=5@0H<d<NKL=cLLU<L>d<>e=sf=eH8@BEQ3K<K<K;0K<LmOiE45dft3fQ0,4*6E
!AIVDM,5,2,,B,81mg=5@0H145mCLEL@hd=fA;<:de8=iQQPMA=QQ1Q`4gLefA=0v1Q1@eePMu1@,4*07
!AIVDM,5,3,,B,81mg=5@0H=1Af0t1=A0huNMi11QMd<f@tPAQPu>Lud<>0i<PhtL==A><H4wLu0,4*47
!AIVDM,5,4,,B,81mg=5@0H0Mt<A@f<ufL<@uil<=Q0eiePLttPQdMM=<f=MM=1@dididAeLhtPh,4*3D
!AIVDM,5,5,,B,81mg=5@0H>=M@MA0MQ<h,4*68
```

Σχήμα 8.9: Στιγμιότυπο οθόνης του μηνύματος AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής.



Σχήμα 8.10: Στιγμιότυπο οθόνης του μέρους της εφαρμογής mIBC-AIS-App που ελέγχει την εγκυρότητα της ψηφιακής υπογραφής.

8.5.4 Το λειτουργικό κόστος δημιουργίας της ψηφιακής υπογραφής

Οι υπολογιστικοί πόροι που απαιτούνται για τις διαδικασίες υπογραφής, κωδικοποίησης και ενθυλάκωσης είναι αμελητέοι. Συγκεκριμένα, η διάρκεια εκτέλεσης όλων των παραπάνω διαδικασιών είναι μικρότερη από ένα δευτερόλεπτο σ' έναν υπολογιστή με τα ακόλουθα χαρακτηριστικά: Επεξεργαστής: Intel Xeon ® CPU E5-1620 Vv2 @ 3.70GHz, RAM 16GB, OS 64-bit Windows 10 Pro. Συγκεκριμένα, ώρα έναρξης: 2019-06-12T10: 00: 47.867, (βλ. Σχήμα 8.7: Πεδίο B) και ώρα λήξης: 2019-06-12T10: 00: 48.188 (βλ. Σχήμα 8.10 (Πεδίο A).

8.5.5 Επίδειξη της μεταφοράς των δεδομένων mIBC-AIS μέσω των συμβατικών συσκευών AIS

Στη συνέχεια, η εφαρμογή mIBC-AIS-app προωθεί τα μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8) στη συμβατική κεραία AIS για μετάδοση και οι συμβατικές συσκευές AIS τα λαμβάνουν και αποθυλακώνουν τα δεδομένα του mIBC-AIS , δηλαδή τις μεταβλητές της ψηφιακής υπογραφής και του αρχικού μηνύματος AIS τύπου 1.

Στον πίνακα 8.2, παρουσιάζουμε λεπτομερώς τις παραπάνω ενέργειες μαζί με την επίδειξή τους. Υπενθυμίζουμε ότι η συμβατική συσκευή AIS του δέκτη εξομοιώνεται από τον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO, στον οποίο αντιγράφουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) και εξάγουμε τα κρυπτογραφικά δεδομένα.

	Ενέργειες της συμβατικής συσκευής AIS του δέκτη	**Εξομοίωση**
1	Ο δέκτης λαμβάνει το κωδικοποιημένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει το PVT του πομπού.	Αντιγράφουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει το PVT, (στιγμιότυπο οθόνης στο Σχήμα 8.9]) στον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO.
2	αποθυλακώνει το PVT του αποστολέα.	Ο διαδικτυακός αποκωδικοποιητής AIS VDM/VDO αποθυλακώνει από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) (στιγμιότυπο οθόνης στο Σχήμα 8.11, πεδίο A) και αποκαλύπτει στην ενότητα «Δεδομένα εφαρμογής» ("Application Data) το PVT, (στιγμιότυπο οθόνης στο Σχήμα 8.11, πεδίο C)
3	Ο δέκτης λαμβάνει το κωδικοποιημένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής.	Αντιγράφουμε το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) που ενθυλακώνει τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής, (στιγμιότυπο οθόνης στο Σχήμα 8.12]) στον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO.
4	αποθυλακώνει τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής.	Ο διαδικτυακός αποκωδικοποιητής AIS VDM/VDO αποθυλακώνει από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) (στιγμιότυπο οθόνης στο Σχήμα 8.12, πεδίο A) και αποκαλύπτει στην ενότητα «Δεδομένα εφαρμογής» ("Application Data") τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής, (στιγμιότυπο οθόνης στο Σχήμα 8.12] πεδίο C) στον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO.

Πίνακας 8.2: Πίνακας συσχέτισης των διαδικασιών εξομοίωσης με τις ενέργειες της συμβατικής συσκευής AIS του δέκτη.

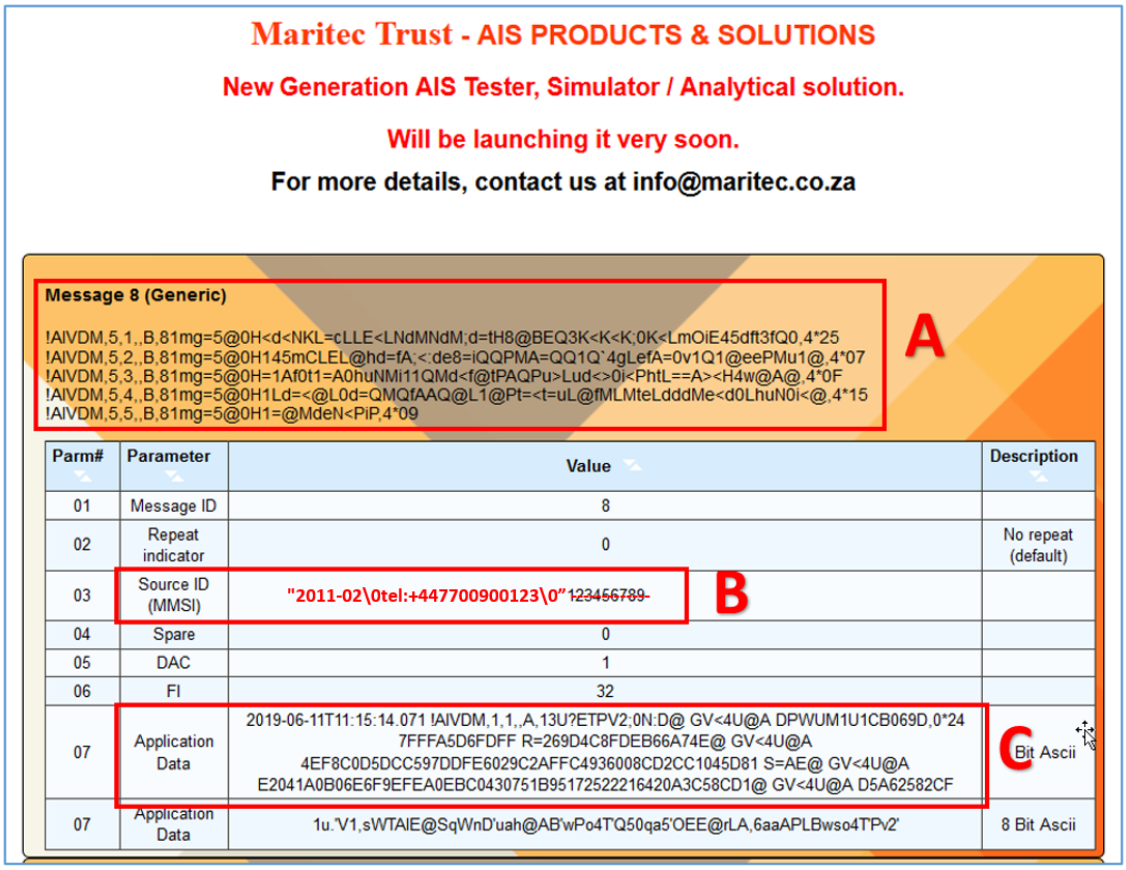
Σχήμα 8.11: Ο διαδικτυακός αποκωδικοποιητής AIS VDM/VDO αποθυλακώνει τα δεδομένα από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) και αποκαλύπτει στην ενότητα «Δεδομένα εφαρμογής» το PVT του αποστολέα.

Στο στιγμιότυο οθόνης του Σχήματος 8.11 ο διαδικτυακός αποκωδικοποιητής AIS VDM/VDO αποθυλακώνει από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) [πεδίο A] και αποκαλύπτει στην ενότητα «Δεδομένα εφαρμογής» (Application Data) το PVT, [πεδίο C]. Στο πεδίο B, σημειώνουμε ότι χρησιμοποιούμε ένα έγκυρο MMSI προκειμένου να γίνει δεκτό από τον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO το μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) αλλά στην ψηφιακή μας υπογραφή χρησιμοποιούμε ως MMSI το αναγνωριστικό του παραρτήματος A του RFC6507. Στην πραγματικότητα μια τέτοια διαφορά θα ήταν ένδειξη επίθεσης παραπλάνησης/πλαστογράφησης και, φυσικά, ο έλεγχος της ψηφιακής υπογραφής θα αποτύγχανε. Παράδειγμα ένδειξης επίθεσης παραπλάνηση/πλαστογράφηση και συνεπώς μη-εγκυρης ψηφιακής υπογραφής παραθετουμε στην υποενότητα 8.5.8.

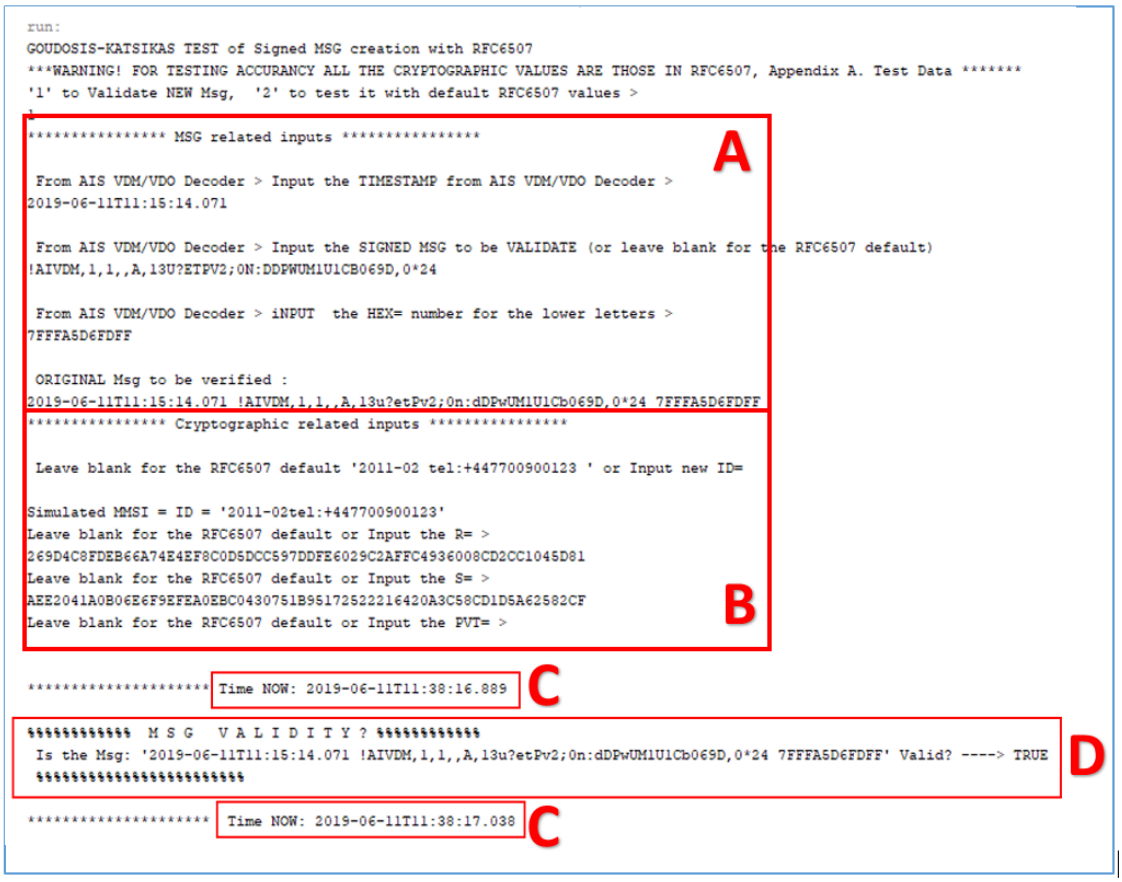
8.5.6 Επίδειξη του ελέγχου εγκυρότητας της ψηφιακής υπογραφής από τον δέκτη.

Η εφαρμογή mIBC-AIS-App του δέκτη χρησιμοποιεί το αναγνωριστικό *MMSI* του αποστολέα, τις αποθυλακωμένες μεταβλητές S, R, PVT, καθώς και το αρχικό μήνυμα AIS_{DATA}, προκειμένου να ελέγξει την εγκυρότητα της ψηφιακής υπογραφής.

Προς τούτο αντιγράφουμε τα αποθυλακωμένα δεδομένα από τον διαδικτυακό αποκωδικοποιητή AIS VDM/VDO, το PVT (στιγμιότυπο οθόνης στο Σχήμα 8.11, πεδίο



Σχήμα 8.12: Ο διαδικτυακός αποκωδικοποιητής AIS VDM/VDO αποθυλακώνει τα δεδομένα από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8) και αποκαλύπτει στην ενότητα «Δεδομένα εφαρμογής» τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής.



Σχήμα 8.13: Στιγμιότυπο οθόνης από την εκτέλεση της εφαρμογής mIBC-AIS-App που επιδεικνύει τον έλεγχο ψηφιακά υπογεγγραμένου μηνύματος AIS από τον δέκτη.

C) και τις μεταβλητές παραμέτρους S, R, AIS_{DATA} της ψηφιακής υπογραφής, (στιγμιότυπο οθόνης στο Σχήμα 8.12) και τα εισάγουμε στην εφαρμογή μας mIBC-AIS-App (στιγμιότυπο οθόνης στο Σχήμα 8.13).

Συγκεκριμένα, στο στιγμιότυπο οθόνης του Σχήματος 8.12, από την εκτέλεση της εφαρμογής μας mIBC-AIS-App παρατηρούμε:

- Στο πεδίο A, αντιγράφουμε από τα αποθυλακωμένα δεδομένα τη χρονοσήμανση, το αρχικό μήνυμα AIS τύπου 1, και τον βοηθητικό δεκαεξαδικό αριθμό.
- Στο πεδίο B, αντιγράφουμε από τα αποθυλακωμένα δεδομένα τη μεταβλητή R και τη μεταβλητή S. Εάν θέλουμε, μπορούμε να αντιγράψουμε το PVT ή, όπως στο παράδειγμά μας, να θεωρήσουμε ότι είναι αποθηκευμένο από προηγούμενο μηνυμα.
- Στο πεδίο C φαίνεται η ώρα έναρξης και λήξης του ελέγχου της ψηφιακής υπογραφής.
- Τέλος, στο πεδίο D παρουσιάζεται το αποτέλεσμα του ελέγχου της ψηφιακής υπογραφής. Στο παράδειγμά μας η υπογραφή είναι έγκυρη (“true”).

8.5.7 Το λειτουργικό κόστος του ελέγχου εγκυρότητας της ψηφιακής υπογραφής

Οι πόροι που απαιτούνται για τις διαδικασίες υπογραφής, κωδικοποίησης και ενθυλάκωσης είναι αμελητέοι. Συγκεκριμένα, η διάρκεια εκτέλεσης όλων των παραπάνω διαδικασιών είναι μικρότερη από ένα δευτερόλεπτο σ' έναν υπολογιστή με τα ακόλουθα χαρακτηριστικά: Επεξεργαστής: Intel Xeon ® CPU E5-1620 Vv2 @ 3.70GHz, RAM 16GB, OS 64-bit Windows 10 Pro. Σγκεκριμένα, έλεγχος έγκυρης υπογραφής ωρα έναρξης:11:38:16.889 και ώρα λήξης:11:38:17.03 (στιγμιότυπο οθόνης στο Σχήμα 8.13, πεδία C) και έλεγχος μη-έγκυρης υπογραφής ώρα έναρξης:11:40:10.422 και ώρα λήξης: 11:40:10.576 (στιγμιότυπο οθόνης στο Σχήμα 8.14, πεδία C και πεδίο D)

8.5.8 Επίδειξη μη-έγκυρου ψηφιακά υπογεγραμμένου μηνύματος AIS

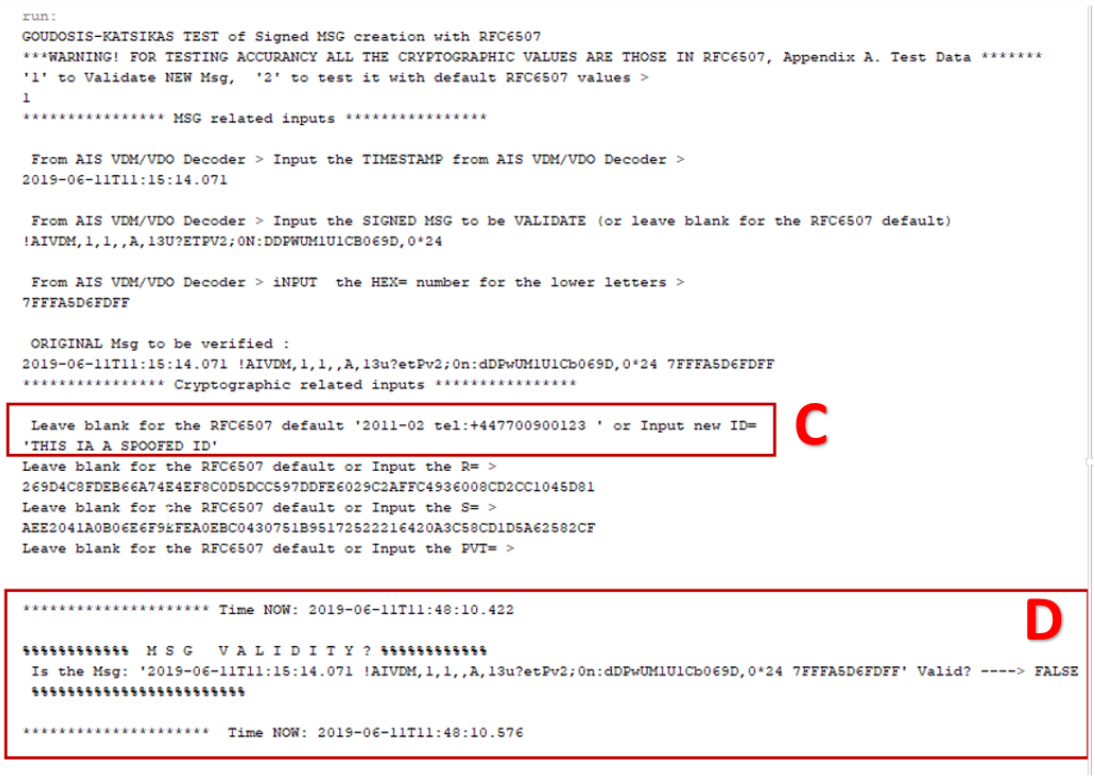
Παρακάτω επιδεικνύουμε μια αποτυχημένη δοκιμή ελέγχου ταυτότητας μηνύματος AIS. Στο παράδειγμά μας κακόβουλος πομπός AIS χρησιμοποιεί πλαστό αναγνωριστικό MMSI (συγκεκριμένα το "THIS IS A SPOOFED ID") προκειμένου να διασπείρει υποκλαπέν ψηφιακά υπογεγραμμένο μήνυμα AIS τύπου 1, που ανήκει στο σκάφος με MMSI = ¨2011-02 \ 0 τηλ: +447700900123 \ 0¨.

Χρησιμοποιούμε την ίδια διαδικασία επικύρωσης υπογραφής και τις ίδιες παραμέτρους όπως στην ενότητα 8.5.6, αλλά ως το αναγνωριστικό MMSI του σκάφους εισαγάγαμε το "THIS IS A SPOOFED ID", όπως φαίνεται στο στιγμιότυπο οθόνης του Σχήματος 8.14, πεδίο C. Όπως παρατηρούμε, το αποτέλεσμα της διαδικασίας ελέγχου ταυτότητας είναι FALSE (στιγμιότυπο οθόνης στο Σχήμα 8.14, πεδίο D). Επομένως, το ενσωματωμένο αρχικό μήνυμα AIS τύπου 1 απορρίπτεται ως λάθος ή παραπλανητικό.

8.6 Επίδειξη της λειτουργίας mIBC-SAKKE-AIS (mode 4)

Στη λειτουργία mIBC-SAKKE-AIS (mode 4), κάθε συσκευή εφοδιασμένη με mIBC-AIS έχει τη δυνατότητα εμπιστευτικής αποστολής υλικού για τη δημιουργία συμμετρικού κλειδιού συνόδου με ένα μόνο μήνυμα, γνωρίζοντας το αναγνωριστικό MMSI του δέκτη. Στην πειραματική μας υλοποίηση επικεντρωθήκαμε στην επίδειξη της αποστολής των κρυπτογραφικών παραμέτρων μέσω μηνυμάτων AIS BROADCAST BINARY MESSAGE (Τύπου 8). Όπως έχουμε επισημάνει, σε πραγματική εφαρμογή θα πρέπει να χρησιμοποιηθεί AIS ADDRESSED BINARY MESSAGE (Τύπου 6) διότι ο δέκτης είναι ένα συγκεκριμένο σκάφος, αλλά λόγω των κοινών χαρακτηριστικών τους δεν επηρεάζεται η πειραματική υλοποίηση.

Σημειώνουμε ότι, αντίθετα με την επίδειξη της λειτουργίας mIBC-ECCSI-AIS (mode 2), όπου έχουμε δημιουργήσει κώδικα για την πλήρη λειτουργία mIBC-ECCSI-AIS (mode 2), εδώ περιοριζόμαστε μόνο στο να επιδείξουμε τη δυνατότητα μεταφοράς των κρυπτογραφικών παραμέτρων που παρουσιάζονται στο παράρτημα A του SAKKE-RFC6508 μέσω του συστήματος AIS. Διαδικαστικές λεπτομέρειες οι οποίες ήδη έχουν αναλυθεί σε προηγούμενες ενότητες παραλείπονται.



Σχήμα 8.14: Επίδειξη μη-έγκυρου ψηφιακά υπογεγραμμένου μηνύματος AIS

Τα βασικά μέρη της επίδειξης της λειτουργίας mIBC-SAKKE-AIS (mode 4) είναι συνοπτικά τα παρακάτω:

1. Χρησιμοποιούμε ακέραιες τις κρυπτογραφικές παραμέτρους H, R του παραρτήματος Α του SAKKE-RFC6508.
2. Χωρίζουμε την κρυπτογραφική παράμετρο R στις δύο συντεταγμένες της R_x και R_y.
3. Δημιουργούμε τρία μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8) προκειμένου να ενθυλακώσουν αντίστοιχα τις κρυπτογραφικές παραμέτρους H, R_x και R_y, όπως φαίνεται στο στιγμιότυπο οθόνης του Σχήματος 8.15.
4. Η επικοινωνία των δεδομένων mIBC-AIS μέσω των συμβατικών συσκευών AIS γίνεται μέσω του διαδικτυακού αποκωδικοποιητή AIS VDM/VDO που αναφέραμε παραπάνω, στον οποίο αντιγράφουμε ένα-ένα τα μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8).
5. Τέλος, ελέγχουμε οπτικά ότι τα αποθυλακωμένα δεδομένα από τα αντιγραμμένα μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8) στην ενότητα «Δεδομένα εφαρμογής» έχουν μεταφερθεί σωστά, όπως φαίνεται στο στιγμιότυπο οθόνης του Σχήματος 8.16.

```
******************** Start TimeStamp: 2019-06-28T09:24:53.610

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 (DMSG8_Msg_R_S_PVT_Creation_v5)
 total_AIS_MSG8_DataPayload.length() 32

****** Copy/Paste the Msg8-NMEA_AIS below that conatins:

 >>>> This MSG8 contains: The H *****

!AIVDM,1,1,,B,81mg=5@0H>>AL0Pued@@LANLMdv1MP@hv=1M>MeL=h,4*67

 (MSG8_Msg_R_S_PVT_Creation_v5) NMEA_AIS_Msg8_final_result.length(): 61 characters

_________________________________________________________________

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 (DMSG8_Msg_R_S_PVT_Creation_v5)
 total_AIS_MSG8_DataPayload.length() 256

****** Copy/Paste the Msg8-NMEA_AIS below that conatins:

 >>>> This MSG8 contains: The Rbx *****

!AIVDM,5,1,,B,81mg=5@0H==1N0A==0@f=NLPMPM@Li10hM@if>MPutN<=<ud=PL<A=eL11Aduh,4*0F
!AIVDM,5,2,,B,81mg=5@0H0L<Aduhtdf0tttQPttMtuM1LPteu1=10Af0A<<<L=M0uuPiMMvMt@,4*4B
!AIVDM,5,3,,B,81mg=5@0H0uQe=>=Q=Mtdt=<ted@uL=Q@Qe@QM<vleLi1L=1d=ehuuuQL11<hP,4*25
!AIVDM,5,4,,B,81mg=5@0H=t@MdfL<Lttf<ute@MLtQdd@AdM=LLeQ0tA=uui@htehQML><u@Q0,4*14
!AIVDM,5,5,,B,81mg=5@0H<f<>N0f0Mti>Af<<A>>LuvLhM<AQe@u>@f=iMvAdPQM1=MPi@,4*16

 (MSG8_Msg_R_S_PVT_Creation_v5) NMEA_AIS_Msg8_final_result.length(): 401 characters

_________________________________________________________________

^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
 (DMSG8_Msg_R_S_PVT_Creation_v5)
 total_AIS_MSG8_DataPayload.length() 256

****** Copy/Paste the Msg8-NMEA_AIS below that conatins:

 >>>> This MSG8 contains: The Rby *****

!AIVDM,5,1,,B,81mg=5@0H=MMiLLu0A>=@PdA=0f@iM1f0QM0d>0LLPP@QeM@dA=QdA=hMdv<<@,4*01
!AIVDM,5,2,,B,81mg=5@0H>A@Lf1LM@@d@vAeuduuAQ1<LdL1=1e<uL@f@L<>M>=PeidiA==Pv@,4*63
!AIVDM,5,3,,B,81mg=5@0H=eA1A<Q><10A1M1dv0uetdA=LPthA<L<hLL1@Q<fMNLe>0e1Ad<=P,4*5A
!AIVDM,5,4,,B,81mg=5@0H><uPQd>Mu=>1MdL=hvAA1ANAPet=><di1dNNAf<tPvL=@AM=Af0LP,4*68
!AIVDM,5,5,,B,81mg=5@0H==hL=tQ>1AetfA@@PuALeuMu0d=utv@du0QMu0MLtQeu=hf=P,4*1A

 (MSG8_Msg_R_S_PVT_Creation_v5) NMEA_AIS_Msg8_final_result.length(): 401 characters

_________________________________________________________________

******************** End TimeStamp: 2019-06-28T09:24:53.636
```


Σχήμα 8.15: Τα τρία μηνύματα AIS BROADCAST BINARY MESSAGE (Τύπου 8) τα οποία ενθυλακώνουν τις κρυπτογραφικές παραμέτρους H, R_x, R_y.

Σχήμα 8.16: αποθυλάκωση των δεδομένων από το αντιγραμμένο μήνυμα AIS BROADCAST BINARY MESSAGE (Τύπου 8), (πεδίο A), και αποκάλυψη (στην ενότητα «Δεδομένα εφαρμογής») της κρυπτογραφικής παραμέτρου *H* (πεδίο H).

8.6.1 Το λειτουργικό κόστος της δημιοψργίας των τριών μηνυμάτων AIS BROADCAST BINARY MESSAGE (Τύπου 8)

Οι πόροι που απαιτούνται για τη δημιουργία των τριών μηνυμάτων AIS BROADCAST BINARY MESSAGE (Τύπου 8) ενθυλάκωσης των κρυπτογραφικών μεταβλητών είναι αμελητέοι. Συγκεκριμένα, η διάρκεια όλων των παραπάνω διαδικασιών είναι μικρότερη από ένα δευτερόλεπτο σε έναν υπολογιστή με τα ακόλουθα χαρακτηριστικά: Επεξεργαστής: Intel Xeon ® CPU E5-1620 Vv2 @ 3.70GHz, RAM 16GB, OS 64-bit Windows 10 Pro. Συγκεκριμένα, ώρα έναρξης: 09:24:53:636 και ώρα λήξης: 09:24:53:636 (στιγμιότυπο οθόνης στο Σχήμα 8.15, πεδία C και D).

Κεφάλαιο 9

Συμπεράσματα

9.1 Εισαγωγή

Σ΄ αυτό το κεφάλαιο παρουσιάζουμε τα συμπεράσματα, τη συνεισφορά και μελλοντικές ερευνητικές κατευθύνσεις που προέκυψαν απ΄ αυτήν την έρευνα, καθώς και τις -αναπόφευκτες- αδυναμίες της. Συνοπτικά, στην πρώτη ενότητα παρουσιάζεται η συνεισφορά της διατριβής, σύμφωνα με τα ερωτήματα που τέθηκαν στην αρχή αυτής της έρευνας και στη συνέχεια συνοψίζουμε τα συμπεράσματά μας. Στη δεύτερη ενότητα με αυτοκριτική διάθεση αναγνωρίζουμε και καταγράφουμε τις αδυναμίες της. Τέλος, στην τρίτη ενότητα παραθέτουμε τις σκέψεις μας για τις μελλοντικές κατευθύνσεις στις οποίες θα μπορούσε να συνεχιστεί η έρευνα αυτή.

9.2 Περίληψη των συμπερασμάτων και συνεισφορά

9.2.1 Όσον αφορά την πρόταση της υποδομής ARIBC

Προτείναμε μια νέα υποδομή που υποστηρίζει διαδικτυακές επώνυμες και ανώνυμες αναφορές και βασίζεται στην Κρυπτογραφία Βάσει Ταυτότητας (ΚΒΤ) μέσω του σχήματος BLMQ-SKIBE ή του σχήματος ECCSI-SAKKE. Η προτεινόμενη υποδομή επιτρέπει την ασφαλή, συνεχή και αμφίδρομη επικοινωνία μεταξύ ανώνυμων αναφερόντων και των αρμόδιων αρχών, αντιμετωπίζοντας τις ανησυχίες των αναφερόντων και διασφαλίζοντας ταυτόχρονα την ακεραιότητα και την αποτελεσματικότητα της έρευνας. Το σχήμα υποστηρίζει τη δυνατότητα, εάν ο αναφέρων το επιθυμεί, να διατηρήσει την επιλογή να αποδείξει την ταυτότητά του σε μεταγενέστερο στάδιο. Τα πλεονεκτήματα του προτεινόμενου σχήματος έναντι των υπαρχουσών εναλλακτικών λύσεων είναι η ευκολία εφαρμογής του, ακόμη και με περιορισμένους πόρους.

Επίσης, αναπτύξαμε μια πειραματική υλοποίηση της πρότασής μας χρησιμοποιώντας το σχήμα ECCSI-SAKKE και επιδείξαμε τη δυνατότητα εφαρμογής του σε περιβάλλον με περιορισμένους πόρους (ανθρώπινους, οργανωτικούς και υπολογιστικούς).

9.2.2 Όσον αφορά την πρόταση του mIBC-AIS

Σ' αυτή την εργασία παρουσιάσαμε μια πρόταση που πιθανόν θα βοηθήσει τη ναυσιπλοΐα να γίνει ασφαλέστερη, προσδίδοντας στο σύστημα AIS δυνατότητες ασφαλείας μέσω Κρυπτογράφησης Βάσει Ταυτότητας (KBT). Συγκεκριμένα, παρουσιάσαμε αρχικά το πλαίσιο λειτουργίας ναυτικών υλοποιήσεων KBT mIBC και ιδιαίτερα των σχημάτων BLMQ-SKIBE και ECCSI-SAKKE. Στη συνέχεια, στις προαναφερθείσες υλοποιήσεις θεμελιώσαμε τη λειτουργία του προτεινόμενου αναβαθμισμένου mIBC-AIS.

Προτείναμε μια εφαρμογή, που την ονομάσαμε mIBC-AIS-app, η οποία θα λειτουργεί παράλληλα με το τυπικό πρωτόκολλο του AIS προσφέροντας στις υφιστάμενες συσκευές του πέντε τύπους λειτουργίας. Ο πρώτος τύπος (mIBC-Typical-AIS (mode 1)) δεν επεμβαίνει καθόλου στα μηνύματα του τυπικού AIS, ο δεύτερος τύπος (mIBC-Authenticated-AIS (mode 2)) υπογράφει ψηφιακά τα τυπικά μηνύματα του AIS, ο τρίτος τύπος (mIBC-Anonymous-AIS (mode 3)) χρησιμοποιεί ψευδο-MMS προκειμένου να προστατέψει την ιδιωτικότητα της ταυτότητας του σκάφους, ο τέταρτος τύπος (mIBC-Confidential-AIS (mode 4)) δίνει τη δυνατότητα εμπιστευτικής αποστολής μικρών μηνυμάτων ή την αποστολή συμμετρικών κλειδιών συνόδου μέσω τυπικών μηνυμάτων AIS, ενώ ο πέμπτος τύπος (mIBC-AES-AIS (mode 5)) δίνει τη δυνατότητα εμπιστευτικής εκπομπής των τυπικών μηνυμάτων AIS σε έμπιστο AISANET μέσω συμμετρικής κρυπτογράφησης με κλειδιά συνόδου ανταλλασσόμενα μέσω της λειτουργίας mIBC-Encrypted-AIS (mode 4).

Επίσης, αναπτύξαμε μια πειραματική υλοποίηση της πρότασής μας, χρησιμοποιώντας το σχήμα ECCSI-SAKKE και επιδείξαμε τη δυνατότητα εφαρμογής της. Σημειώνουμε ότι η περιγραφείσα υποδομή mIBC μπορεί να χρησιμοποιηθεί ως μια γενική βάση παροχής υπηρεσιών ασφαλείας στον ναυτιλιακό τομέα, επιπλέον της χρήσης της στο mIBC-AIS. Συγκεκριμένα, περιγράψαμε το πλαίσιο υλοποίησης της υποδομής mIBC μέσω των σχημάτων KBT, BLMQ-SKIBE και ECCSI-SAKKE.

9.3 Αδυναμίες αυτής της έρευνας

Σ' αυτήν την ενότητα, με αυτοκριτική διάθεση, θα προσπαθήσουμε να αναγνωρίσουμε τις αδυναμίες αυτής της έρευνας, έχοντας υπόψη την εγγενή δυσκολία του εγχειρήματος να κρίνουμε ένα αποτέλεσμα όχι ως τρίτοι εξωτερικοί παρατηρητές, αλλά ως δημιουργοί του.

Οι αδυναμίες της έρευνάς μας διακρίνονται σε τρεις γενικές κατηγορίες. Στην πρώτη κατηγορία κατατάσσεται η αδυναμια μας να έχουμε μια συστηματική και ολοκληρωμένη μελέτη των αναγκών των τομέων στους οποίους απευθυνόμαστε, στη δεύτερη εγγενείς αδυναμίες των προτάσεων μας, και τέλος στην τρίτη η αδυναμια μας να επιδείξουμε τα αποτελέσματα της έρευνάς μας σε πραγματικές συνθήκες.

9.3.1 Αδυναμίες της προκαταρκτικής μας έρευνας

Τόσο η προκαταρκτική έρευνά μας για τις ανάγκες ασφαλείας των ανώνυμων αναφορών όσο και για την ασφάλεια του συστήματος AIS βασίστηκε σε βιβλιογραφικές πηγές, με εξαίρεση το σύστημα AIS, για το οποίο διενεργήθηκαν άτυπες συζητήσεις με ανθρώπους της ναυτιλίας. Δεν μπορεί όμως να θεωρηθεί ότι έγινε μια συστηματική

και εμπεριστατωμένη αποτύπωση των αναγκών ασφαλείας στις περιπτώσεις που ερευνήσαμε.

Θεωρούμε ότι στη μεν περίπτωση των ανώνυμων αναφορών θα ήταν πολύ ενδιαφέρουσα μια έρευνα που θα μπορούσε να συνδυάσει κοινωνιολογικά και τεχνικά στοιχεία προκειμένου να γίνει πολύ πιο κατανοητή η ψυχολογία του αναφέροντα απέναντι στις ηλεκτρονικές ανώνυμες αναφορές. Επίσης, θεωρούμε ότι θα ήταν πολύ ενδιαφέρουσα η δημοσιοποίηση στοιχείων και η μεθοδική έρευνα του ρόλου που παίζει το σύστημα AIS σε έκνομες ενέργειες, όπως πειρατείες, λαθρεμπόριο και τρομοκρατία. Ακόμα, θα ήταν χρήσιμο να ερευνηθεί ανάμεσα στα στελέχη της ναυτιλίας το πόσες φορές και για ποιους λόγους κλείνει το σύστημα AIS και τι επιπτώσεις θεωρούν ότι αυτό έχει στην ασφάλεια της ναυσιπλοΐας.

9.3.2 Τεχνικές Αδυναμίες

Όσον αφορά την πρόταση του ARIBC

Η μείζων τεχνική αδυναμια της πρότασής μας έγκειται στο εγγενές χαρακτηριστικό της ΚΒΤ ότι ο Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ) δημιουργεί τα ιδιωτικά κλειδιά των ανώνυμων αναφερόντων. Αυτό διασφαλίζει μεν τις αρχές, αλλά μπορεί σε ορισμένες περιπτώσεις να είναι αποτρεπτικός παράγοντας για κάποιους ανώνυμους αναφορείς όταν υπάρχει δυσπιστία απέναντι στις αρχές. Επί του παρόντος δεν έχουμε κάποια συγκεκριμένη πρόταση για την επίλυση αυτής της αδυναμιας και αφήνουμε για το μέλλον την έρευνα για τη δημιουργία κάποιου μηχανισμού επίλυσής της.

Όσον αφορά την πρόταση του mIBC-AIS

Η μείζων τεχνική αδυναμια που θεωρούμε ότι παρουσιάζει η πρότασή μας είναι το μέγεθος των μεταφερόμενων κρυπτογραφικών δεδομένων συγκριτικά με τα δεδομένα του τυπικού AIS. Δεδομένου ότι το μέγεθος των κρυπτογραφικών δεδομένων του mIBC-AIS είναι ανάλογο με το μέγεθος των χρησιμοποιούμενων κρυπτογραφικών παραμέτρων, μια προφανής λύση είναι να μειωθεί το επίπεδο της κρυπτογραφικής ασφάλειας που προσφέρει το mIBC-AIS. Ωστόσο, η έρευνα για τη βέλτιστη ισορροπία, μεταξύ της προσφερόμενης ασφάλειας και του κόστους λειτουργίας της απαιτεί συστηματική ανάλυση κινδύνων από τη χρήση του AIS, με τη συμμετοχή της ναυτιλιακής κοινότητας.

Στην περίπτωση του mIBC-Confidential-AIS (mode 4) δεν θεωρούμε ότι υπάρχει πρόβλημα, λόγω της σπανιότητας της ανάγκης ανταλλαγής κλειδιών συμμετρικών αλγορίθμων. Αντίθετα, για τη λειτουργία mIBC-Authenticated-AIS (mode 2), πιστεύουμε ότι αξίζουν να εξεταστούν οι παρακάτω προτάσεις: Το mIBC-Authenticated-AIS (mode 2), χρησιμοποιεί δύο μηνύματα AIS BROADCAST BINARY MESSAGE (τύπου 8) για τη μετάδοση ψηφιακά υπογεγραμμένου μηνύματος AIS. Ωστόσο, το αρχικό μήνυμα AIS BROADCAST BINARY MESSAGE (τύπου 8) μεταφέρει τη στατική μεταβλητή PVT, η οποία είναι συνδεδεμένη με το MMSI του σκάφους εκπομπής και σταθερή για όλα τα μηνύματα τα οποία εκπέμπονται από έναν συγκεκριμένο πομπό. Επομένως, για να αποφευχθεί η περιττή αναμετάδοση της ίδιας πληροφορίας με κάθε ψηφιακά υπογεγραμμένο μήνυμα AIS, οι δέκτες μπορούν να αποθηκεύσουν το ζευγάρι PVT/MMSI για μελλοντική χρήση. Τα PVTs θα μπορούν να γνωστοποιούνται σε νέα σκάφη που εισέρχονται στο συγκεκριμένο AISANET με μια

από τις παρακάτω μεθόδους:

- Δημιουργία ενός νέου μηνύματος mIBC-AIS, το οποίο θα ονομάζεται PVT-Request και θα ενθυλακώνεται, με τις μεθόδους πού έχουμε περιγράψει σε ένα τυπικό μήνυμα AIS ADDRESSED BINARY MESSAGE (τύπου 6), και θα αποστέλλεται όταν ένα σκάφος χρειάζεται να μάθει το PVT ενός άλλου.
- Εναλλακτικά, σε θαλάσσιες περιοχές όπου τα AISANETs αλλάζουν δυναμικά πάρα πολύ γρήγορα, δηλαδή θα υπάρχει δυσανάλογα μεγάλος αριθμός PVT-Requests, αυτόματα το mIBC-AIS του σκάφους θα εκπέμπει το PVT περιοδικά.

Τέλος, μια επιπρόσθετη πρόταση μείωσης του αριθμού των σημάτων mIBC-Authenticated-AIS (mode 2), με αντίστοιχη μείωση βέβαια της ασφάλειας της ναυσιπλοΐας, είναι ο ετεροχρονισμένος έλεγχος αυθεντικότητας των συμβατικών μηνυμάτων AIS. Ανάλογα με την κατάσταση της ναυσιπλοΐας στην περιοχή, προαποφασισμένος αριθμός συμβατικών μηνυμάτων AIS (π.χ. 5-10) περνά από συνάρτηση κατακερματισμού, το αποτέλεσμα της οποίας υπογράφεται ψηφιακά και αποστέλλεται μέσω σήματος mIBC-Authenticated-AIS (mode 2). Έτσι οι δέκτες ελέγχουν, έστω και ετεροχρονισμένα, την αυθεντικότητα των 5-10 τελευταίων συμβατικών μηνυμάτων AIS που έλαβαν από το συγκεκριμένο σκάφος.

Όσον αφορά τις πειραματικές υλοποιήσεις

Για διάφορους λόγους, οι προτάσεις μας δεν ήταν δυνατόν να δοκιμαστούν σε πραγματικές συνθήκες και ο παρουσιαζόμενος έλεγχός τους σε πειραματικό περιβάλλον είναι μια αυτονόητη αδυναμια αυτής της εργασίας. Συγκεκριμένα, στη μεν περίπτωση των ανώνυμων αναφορών και του προτεινόμενου ARIBC, η ολοκληρωμένη πειραματική υλοποίησή του ήταν τεχνικά εφικτή, αλλά χωρίς ερευνητικό ενδιαφέρον διότι δεν θα μπορούσε να λειτουργήσει σε συνθήκες όπου θα κρινόταν η αποδοχή του από ανώνυμους αναφορείς σε πραγματικές συνθήκες. Στην περίπτωση δε του συστήματος AIS και του προτεινόμενου mIBC-AIS, μια ολοκληρωμένη πειραματική υλοποίησή του ήταν τεχνικά ανέφικτη διότι απαιτούσε τεχνικό εξοπλισμό και πρόσβαση σε στοιχεία τα οποία δεν ήταν δυνατόν να έχουμε.

9.4 Θέματα για μελλοντική έρευνα

Θεωρούμε ότι είναι σύνηθες το τέλος μιας ερευνητικής προσπάθειας να αφήνει ανάμικτα συναισθήματα μη εκπληρωμένων στόχων. Οι μελλοντικοί μας στόχοι χαράσσονται βάσει της επιθυμιας μας να βελτιώσουμε όσο γίνεται αυτό που θεωρούμε ότι δεν είναι ολοκληρωμένο.

9.4.1 Στο επίπεδο της εφαρμοσμένης κρυπτογραφίας

Στο επίπεδο της εφαρμοσμένης κρυπτογραφίας επικεντρωθήκαμε στη δοκιμή διαφορετικών μηχανισμών και τεχνικών KBT προκειμένου να βελτιώσουμε περαιτέρω τις προτάσεις μας. Συγκεκριμένα, στην περίπτωση των ανώνυμων αναφορών και του προτεινόμενου ARIBC η ερευνητική μας προσπάθεια θα είναι στην περαιτέρω διασφάλιση του ανώνυμου αναφέροντα. Όσον αφορά την ασφάλεια του συστήματος

AIS και την ασφάλεια της ναυτιλίας, στόχος μας είναι οι δοκιμές με αντίστοιχες προσπάθειες χρήσης ΚΒΤ στον χώρο του Διαδικτύου των Αντικειμένων (Internet of Things), προκειμένου να αυξήσουμε την αποδοτικότητα του mIBC-AIS.

9.4.2 Στο επίπεδο των ανώνυμων αναφορών

Περαιτέρω έρευνα, σε συνδυαστικό τεχνολογικό και κοινωνιολογικό επίπεδο, μέσω πιλοτικών εφαρμογών σε συγκεκριμένους χώρους (π.χ. πανεπιστημιακούς) θεωρούμε ότι θα βοηθούσε στην εξαγωγή ασφαλέστερων συμπερασμάτων τόσο για την αξία ή όχι του ARIBC αλλά και ως βάση για άλλες προτάσεις.

9.4.3 Στο επίπεδο της ασφάλειας της ναυσιπλοΐας

Όσον αφορά το τεχνικό σκέλος αυτής της έρευνας, μελλοντικός στόχος μας είναι η βελτίωση του κώδικα της εφαρμογής mIBC-AIS-app, η ενσωμάτωσή της σε πραγματικές συσκευές AIS και η δοκιμή λειτουργίας της σε πραγματικές συνθήκες.

Τέλος, θα θέλαμε να πιστεύουμε ότι αυτη η εργασία θα μπορούσε να είναι η αφορμή για περαιτέρω ερευνητικές προσπάθειες στους παραπάνω τομείς.

Παράρτημα Α΄

Απόδοση αγγλικών όρων στα ελληνικά

Αγγλικά	**Ελληνικά**
authentication	Αυθεντικοποίηση, Πιστοποίηση
authorities	Αρχές
authorization	Εξουσιοδότηση, Αδειοδότηση
availability	Διαθεσιμότητα
Bilinear map	Διγραμμική Απεικόνιση
Cyclic groups	Κυκλικές ομάδες
confidentiality	Εμπιστευτικότητα
Decapsulation	Αποθυλάκωση
e-government	Ηλεκτρονική διακυβέρνηση
Encapsulation	Ενθυλάκωση
Field	Σώμα
hash function	Συνάρτηση κατακερματισμού
identification	Ταυτοποίηση
Identity-Based Cryptography (IBC)	Κρυπτογραφία Βάσει Ταυτότητας (ΚΒΤ)
Internet of Things	Διαδίκτυο των Αντικειμένων
integrity	Ακεραιότητα
MANET: Mobile Ad hoc NETwork	Επί τούτω κινητό δίκτυο
Non-repudiation	Μη άρνηση αναγνώρισης, μη αποκήρυξη
non-degenerate	Μη εκφυλισμένος/η
Public Key Infrastructure (PKI)	Κρυπτογράφηση Δημόσιου Κλειδιού (ΚΔΚ)
Public Key	Δημόσιο Κλειδί (ΔΚ)
Private Key	Ιδιωτικό Κλειδί (ΙΚ)
Public Identifier	Δημόσιο Αναγνωριστικό (ΔΑ)
Public Parameters of IBC	Δημόσιες Παράμετροι (ΔΠ) της ΚΒΤ
Public Validation Token	Δημόσιο Τεκμήριο Επικύρωσης (ΔΤΕ)
Pairing-bilinear map	Ζεύξη
Proof of Concept	Πειραματική υλοποίηση
Reporter	Αναφέρων ή καταγγέλλων
Receiver Secret Key (RSK)	Μυστικό Κλειδί Αποδέκτη (ΜΚΑ)
Session key	Κλειδί Συνόδου
Secret Signing Key (SSK)	Ιδιωτικό Κλειδί ψηφιακής Υπογραφής (ΙΚΥ)
Trusted Central Coordinator	Αξιόπιστος Κεντρικός Συντονιστής (ΑΚΣ)
Time slot	Χρονοθυρίδα
Verifier	Επαληθευτής
Vehicular Ad-hoc NETwork	Επί τούτω δίκτυο για οχήματα

Πίνακας Α΄.1: Απόδοση αγγλικών όρων στα ελληνικά

Βιβλιογραφία

[1] K. Oo, C. Shi, H. Qinyou, and A. Weintrit, "Clustering analysis and identification of marine traffic congested zones at wusongkou, shanghai," *Zeszyty Naukowe Akademii Morskiej w Gdyni*, pp. 101–113, 01 2010.

[2] M. Groves, "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)," Internet Requests for Comments, RFC Editor, RFC 6507, 2012.

[3] ——, "Sakai-Kasahara Key Encryption (SAKKE)," Internet Requests for Comments, RFC Editor, RFC 6508, 2012.

[4] "Should ship data be open to the public? - ship technology." [Online]. Available: https://www.ship-technology.com/features/featureship-data-be-open-public-security/

[5] B. Ellison, "Mandated ais, an aid to pirates?" https://www.panbo.com/mandated-ais-an-aid-to-pirates/, April 2009.

[6] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 380–399, 2012.

[7] S. T. Faraj Al-Janabi and H. K. Abd-Alrazzaq, "Combining mediated and identity-based cryptography for securing e-mail," in *Communications in Computer and Information Science*, vol. 194 CCIS. Springer, Berlin, Heidelberg, 2011, pp. 1–15.

[8] A. G. A. G. Karatop, E. Sava\cs, and E. Savaş, "An identity-based key infrastructure suitable for messaging and its application to e-mail," *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm'08*, 2008. [Online]. Available: https://doi.org/10.1145/1460877.1460890

[9] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 767–778, 2017.

[10] M. K. Aditia, S. Paida, F. Altaf, S. Maity, and P. I. Jabalpur, "Certificate-less Public Key Encryption For Secure e-Healthcare Systems," in *2019 IEEE Conference on Information and Communication Technology*. IEEE, 2019, pp. 1–5.

[11] R. Ssembatya and A. V. D. M. Kayem, "Secure and Efficient Mobile Personal Health Data Sharing in Resource Constrained Environments," *Proceedings - IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2015*, pp. 411–416, 2015.

[12] N. H. Kamarudin and Y. M. Yussoff, "Authentication scheme interface for mobile e-health monitoring using unique and lightweight identity-based authentication," *AIP Conference Proceedings*, vol. 1774, no. October, 2016.

[13] J. Baek, E. Hableel, Y.-j. Byon, D. S. Wong, K. Jang, and H. Yeo, "How to Protect ADS-B : Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption," pp. 1–11, 2016.

[14] J. Baek, E. Hableel, Y.-J. Byon, D. Wong, K. Jang, and H. Yeo, "How to protect ads-b: Confidentiality framework and efficient realization based on staged identity-based encryption," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 690–700, 2017.

[15] D. Aljeaid, X. Ma, and C. Langensiepen, "Biometric identity-based cryptography for e-Government environment," in *2014 Science and Information Conference*. The Science and Information (SAI) Organization, 2014, pp. 581–588.

[16] "Identity-Based Cryptographic Techniques using Pairings," IEEE Standards Association, Piscataway, NJ, USA, IEEE Standard 1363.3-2013, 2013.

[17] NIST, "NIST SP 800-57 Pt. 1 Rev. 4," Tech. Rep., 2016. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

[18] R. Sakai and M. Kasahara, "Id based cryptosystems with pairing on elliptic curve," *IACR Cryptology ePrint Archive*, vol. 2003, pp. 13–23, 04 2003.

[19] ——, "Id-based cryptosystems with pairing on elliptic curve," *IEEE Networks*, vol. 13, no. 6.

[20] L. Chen and Z. Cheng, "Security proof of sakai-kasahara's identity-based encryption scheme," *Cryptography and Coding*, vol. 3796, pp. 442–459, Especially the p.449, 2005.

[21] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, and L. Chen, "Report on Pairing-based Cryptography," vol. 120, 2015. [Online]. Available: http://dx.doi.org/10.6028/jres.120.002

[22] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. J.-J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," in *Advances in Cryptology - ASIACRYPT 2005*, B. Roy, Ed., vol. 3788 LNCS. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 515–532.

[23] I. Maritime Organization, "No Title," 2015. [Online]. Available: https://edocs.imo.org/Final

[24] International Maritime Organization (IMO), "Maritime Security and Piracy," \url{http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx}, 2020.

[25] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14, vol. 2014-Decem, no. December. New York, NY, USA: ACM, 2014, pp. 436–445. [Online]. Available: http://doi.acm.org/10.1145/2664243.2664257https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

[26] G. C. Kessler, J. P. Craiger, and J. C. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 12, no. 3, p. 429, 2018.

[27] J. Hall, J. Lee, J. Benin, C. Armstrong, and H. Owen, "Ieee 1609 influenced automatic identification system (ais)," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, 2015, pp. 1–5.

[28] S. H. Oh, D. Seo, and B. Lee, "S3 (secure ship-to-ship) information sharing scheme using ship authentication in the e-navigation," *International Journal of Security and its Applications*, vol. 9, no. 2, pp. 97–110, 2015.

[29] A. Goudosis, T. Kostis, and N. Nikitakos, "Automatic Identification System Stated Requirements for Naval Transponder Security Assurance," in *Hellenic Military Academy, 2nd International Conference on Applications of Mathematics & Informatics In Military Sciences (AMIMS)*, VARI, GREECE, 2013.

[30] D. He, N. Kumar, K.-K. R. Choo, and W. Wu, "Efficient Hierarchical Identity-Based Signature with Batch Verification for Automatic Dependent Surveillance-Broadcast System," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 454–464, 2017.

[31] G. C. Kessler, "Protected ais: A demonstration of capability scheme to provide authentication and message integrity," *TransNav*, vol. 14, no. 2, pp. 279–286, 2020.

[32] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[33] IALA, "e-Navigation Portal - IALA AISM." [Online]. Available: https://www.iala-aism.org/technical/e-navigation/

[34] C. H. Ku, A. Iriberri, and G. Leroy, "Crime Information Extraction from Police and Witness Narrative Reports," in *2008 IEEE Conference on Technologies for Homeland Security*, 2008, pp. 193–198.

[35] A. Iriberri, G. Leroy, and N. Garrett, "Reporting On-Campus Crime Online: User Intention to Use," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 4, 2006, pp. 82a–82a.

[36] A. Iriberri and G. Leroy, "Natural Language Processing and e-Government: Extracting Reusable Crime Report Information," in *2007 IEEE International Conference on Information Reuse and Integration*, 2007, pp. 221–226.

[37] A. B. Sakpere, A. V. D. M. Kayem, and T. Ndlovu, "A Usable and Secure Crime Reporting System for Technology Resource Constrained Context," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, 2015, pp. 424–429.

[38] T.-F. Shih, C.-L. Chen, B.-Y. Syu, and Y.-Y. Deng, "A Cloud-Based Crime Reporting System with Identity Protection," *Symmetry*, vol. 11, no. 2, p. 255, 2019. [Online]. Available: http://dx.doi.org/10.3390/sym11020255

[39] B. Obada-Obieh, L. Spagnolo, and K. Beznosov, "Towards Understanding Privacy and Trust in Online Reporting of Sexual Assault," in *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020)*. {USENIX} Association, 2020, pp. 145–164. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/obada-obieh

[40] S. Zou, J. Xi, S. Wang, Y. Lu, and G. Xu, "Reportcoin: A Novel Blockchain-Based Incentive Anonymous Reporting System," *IEEE Access*, vol. 7, pp. 65 544–65 559, 2019.

[41] R. G. Jimoh, K. T. Ojulari, and O. A. Enikuomehin, "A Scalable Online Crime Reporting System," *African Journal of Computing & ICT*, vol. 7, no. 1.

[42] D. K. Tabassum, D. H. Shaiba, S. Shamrani, and S. Otaibi, "E-Cops: An Online Crime Reporting and Management System for Riyadh City," in *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 2018, pp. 1–8.

[43] A. William and A. Milliscent, "Mobile Solution for Metropolitan Crime Detection and Reporting," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 4.

[44] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, G. R. Blakley and D. Chaum, Eds., vol. 196 LNCS. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-39568-7{_}5https://link.springer.com/content/pdf/10.1007/3-540-39568-7{_}5.pdf

[45] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *Appears in SIAM J. of Computing Lecture Notes in Computer Science*, vol. 32, no. 2139, pp. 586–615, 2003. [Online]. Available: http://courses.cs.vt.edu/{~}cs6204/Privacy-Security/Papers/Crypto/IBE-Weil-Pairing.pdf

[46] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," *International Journal of Applied Cryptography*, vol. 1, no. 1, pp. 3–21, 2008. [Online]. Available: http://ai.stanford.edu/{~}xb/ijact08/practicalIBE.pdf

[47] A. Joux, "A One Round Protocol for Tripartite Diffie–Hellman," *J. Cryptol.*, vol. 17, no. 4, pp. 263–276, 2004. [Online]. Available: https://doi.org/10.1007/s00145-004-0312-y

[48] J. Baek, J. Newmarch, R. Safavi-naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. of Australian Unix Users Group Annual Conference*, 2004, pp. 95–102.

[49] S. T. Faraj Al-Janabi and H. K. Abd-alrazzaq, "Combining mediated and identity-based cryptography for securing e-mail," in *Digital Enterprise and Information Systems*, E. Ariwa and E. El-Qawasmeh, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1–15.

[50] H. W. Lim, "On the Application of Identity-Based Cryptography in Grid Security," Ph.D. dissertation, Royal Holloway, University of London, 2006.

[51] A. Goudossis, S. K. Katsikas, A. Goudosis, and S. K. Katsikas, "Towards a secure automatic identification system (AIS)," *Journal of Marine Science and Technology*, vol. 24, no. 2, pp. 410–423, may 2019. [Online]. Available: http://link.springer.com/10.1007/s00773-018-0561-3

[52] K. G. Paterson and G. Price, "A comparison between traditional public key infrastructures and identity-based cryptography," *Information Security Technical Report*, vol. 8, no. 3, pp. 57 – 72, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S136341270300308X

[53] Girish and H. Phaneendra, "Identity-based cryptography and comparison with traditional public key encryption: A survey," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 4, pp. 5521–5525, 2014.

[54] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology - ASIACRYPT 2003*, C.-S. Laih, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 452–473.

[55] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Communications*, vol. 16, no. 2, pp. 24–30, 2009.

[56] Y. Zhou, Y. Fang, Y. Zhang, Y. F. Y. Zhou, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[57] M. . M. A. Bohio, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Networks*, vol. 2, no. 3, pp. 309–317, 2004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870504000198

[58] "Secure hash standard (shs)," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, Standard, 08 2015.

[59] P. S. Barreto, A. Deusajute, E. De, S. Cruz, G. Pereira, R. Silva, and Machado Deusajute, "Toward efficient certificateless signcryption from (and without) bilinear pairings," in *Conference: VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 2008. [Online]. Available: https://www.researchgate.net/publication/228662897{_}Toward{_}efficient{_}certificateless{_}signcryption{_}from{_}and{_}without{_}bilinea

[60] M. Groves, "MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY)," Internet Requests for Comments, RFC Editor, RFC 6509, 2012.

[61] Secure Chorus, "White paper: EMERGENCY SERVICES Secure Chorus Compliant Products interoperability with," Tech. Rep. November, 2018.

[62] CESG, "Using MIKEY-SAKKE Building secure multimedia services," no. 1.0, pp. 1–14, 2014. [Online]. Available: www.cesg.gov.uk

[63] ITU-T, "Itu-t recommendation x.1365: Security methodology for the use of identity-based cryptography in support of internet of things (iot) services over telecommunication networks," *ITU-T Recommendation*, 3 2020. [Online]. Available: http://handle.itu.int/11.1002/1000/14089

[64] S. J. Murdoch, "Insecure by design: Protocols for encrypted phone calls," *Computer*, vol. 49, pp. 25–33, 2016. [Online]. Available: https://bitbucket.org/

[65] "Auto thefts most likely to be reported, murders most likely to be solved," \url{https://www.pewresearch.org/fact-tank/2020/11/20/facts-about-crime-in-the-u-s/ft_20-11-12_crimeintheus_5/}.

[66] J. A. Young, J. F. Courtney, R. J. Bennett, T. S. Ellis, and C. Posey, "The impact of anonymous, two-way, computer-mediated communication on perceived whistleblower credibility," *Information Technology & People*, vol. ahead-of-p.

[67] B. H. A. Smith, "Finding Information in the Maritime Ecosystem," pp. 1–12.

[68] International Maritime Organization, "SOLAS CHAPTER V: SAFETY OF NAVIGATION," \url{http://www.imo.org/en/OurWork/facilitation/documents/solas\%20v\% London, UK, 2014.

[69] ITU-R, "Technical characteristics for a VHF data exchange system in the VHF maritime mobile band," *Recommendation ITU-R*, vol. M.[VDES], no. January, pp. 1–54, 2014.

[70] International Telecommunications Union (ITU), "Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band M Series Mobile, radiodetermination, amateur, and related satellite services," International Telecommunication Union, Geneva, CH, Recommendation, 2014. [Online]. Available: http://www.itu.int/ITU-R/go/patents/en

[71] M. Mclntyre, L. Genik, P. Mason, and T. Hammond, "Towards an Understanding of Security , Privacy and Safety in Maritime Self- Reporting Systems," vol. 238, pp. 185–206.

[72] X. Z. Y. Fang and Y. Zhang, ""Securing resource-constrained wireless ad hoc networks,"," *IEEE Wireless Communications,*, vol. 16, no. 2, pp. 24–30, 2009.

[73] M. Bohio and A. Miri, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Networks*, vol. 2, no. 3, pp. 309–317, 2004.

[74] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of ais automated identification system," in *Proceedings of the 30th Annual Computer Security Applications Conference*, 12 2014, pp. 436–445.

[75] F. Mazzarella, A. Alessandrini, H. Greidanus, M. Alvarez, P. Argentieri, and D. Nappo, "Data Fusion for Wide-Area Maritime Surveillance Data Fusion for Wide-Area Maritime Surveillance," *Proceedings of the Workshop on Moving Objects at Sea*, no. June, pp. 1–5, 2013.

[76] "Federal Information Processing Standards Publication 197 Announcing the ADVANCED ENCRYPTION STANDARD (AES)," Tech. Rep., 2001. [Online]. Available: http://csrc.nist.gov/csor/

[77] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[78] "IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, Jan 2012," *IEEE 1609.2/D12, January 2012*, 2012.

[79] SAAB, "R5 Supreme W-AIS," 2020. [Online]. Available: https://saab.com/security/maritime-traffic-management/traffic-management/r5-supreme-w-ais//

[80] U.S. Coast Guard Navigation Center, "HOW AIS WORKS," \url{https://www.navcen.uscg.gov/?pageName=AISMessage6}, 2016. [Online]. Available: http://www.navcen.uscg.gov/?pageName=AISworks