modulus

SIP Interconnection **Technical Specifications.**

Ανανεωμένο το 2026

Περιεχόμενα

1. Overview **02.**

2. Inbound Calls **03.**

3. Outbound Calls **04.**

4. SIP Servers **05.**

5. Media & Audio Codecs **07.**

6. Encryption **08.**

7. Number Formatting **09.**

8. SIP Headers & CLI Presentation **10.**

9. NAT & Firewall Requirements **11.**

10. Network Requirements **12.**

11. Integration & Testing **12.**

1. Overview

Η modulus παρέχει υπηρεσίες **VoIP over Public Internet**, υποστηρίζοντας SIP connectivity για εισερχόμενη και εξερχόμενη επικοινωνία. Σε όλο το παρόν έγγραφο οι όροι *εισερχόμενη* και *εξερχόμενη* χρησιμοποιούνται με τις έννοιες που τους αποδίδονται από τη σκοπιά του συνδρομητή:

- **εισερχόμενη/inbound/incoming:** modulus to subscriber
- **εξερχόμενη/outbound/outgoing:** subscriber to modulus

Για inbound και outbound traffic υποστηρίζονται διαφορετικά authentication και routing models ανάλογα με τις απαιτήσεις της διασύνδεσης.

2. Inbound Calls

Υποστηρίζονται οι ακόλουθοι μέθοδοι παράδοσης των κλήσεων στο άκρο του συνδρομητή.

Σημειώνεται ότι στην περίπτωση όπου ο εξοπλισμός ή η πλατφόρμα στο άκρο του συνδρομητή είναι πιθανό να χρησιμοποιείται και από άλλα πρόσωπα, θα πρέπει να διερευνηθεί εάν η μέθοδος που επιλέγεται διασφαλίζει την ασφαλή παράδοση της επικοινωνίας υπό το λογικό έλεγχο του συνδρομητή και μόνο.

Επειδή οι μέθοδοι διασφάλισης αυτής της απαίτησης διαφέρουν ανά πλατφόρμα, το παρόν έντυπο δεν μπορεί να τις αποτυπώσει παραθέτοντάς τες. Αν η πλατφόρμα που έχει επιλέξει ο συνδρομητής δεν έχει προηγούμενο διασύνδεσης με το δίκτυο της modulus, οι όποιοι διαθέσιμοι μηχανισμοί θα πρέπει να αξιολογηθούν ως προς την επάρκειά τους πριν την υλοποίηση της λογικής διασύνδεσης.

SIP Registration

Ο εξοπλισμός ή η πλατφόρμα που χρησιμοποιεί ο συνδρομητής πραγματοποιεί **SIP REGISTER** προς τους **registrar servers** της modulus. Η παράδοση των κλήσεων θα γίνεται στο άκρο του συνδρομητή όπως αυτό κοινοποιείται στη modulus μέσω των SIP μηνυμάτων αυτών.

Η δυνατότητα αξιοποίησης μηχανισμών υψηλής διαθεσιμότητας με αυτή τη μέθοδο παρέχεται μόνο εφόσον ο εξοπλισμός ή η πλατφόρμα του συνδρομητή υποστηρίζει το πρότυπο **RFC5626** (SIP outbound).

Static Locations

Δηλώνονται οι **δημόσιες IP διευθύνσεις/θύρες** ή το **SIP URI** του εξοπλισμού ή της πλατφόρμας που χρησιμοποιεί ο συνδρομητής.

Οι εισερχόμενες κλήσεις παραδίδονται απευθείας στις συγκεκριμένες IPs χωρίς να απαιτείται SIP Registration, και ο μηχανισμός υψηλής διαθεσιμότητας επιτυγχάνεται εφόσον δηλωθούν περισσότερα από ένα locations στη modulus για την παράδοση των κλήσεων στο άκρο του συνδρομητή.

3. Outbound Calls

Υποστηρίζονται οι ακόλουθες μέθοδοι διαπίστευσης:

SIP Digest Authentication

Οι εξερχόμενες κλήσεις πραγματοποιούνται με **SIP Authentication** μέσω username/password.

IP Authentication

Οι εξερχόμενες κλήσεις μπορούν να πιστοποιούνται βάσει της public source IP και προαιρετικά σε συνδυασμό με το source port.

Οποιαδήποτε κλήση παραδίδεται στα συστήματα της modulus από **IP(/port)** που έχει αντιστοιχιστεί σε συγκεκριμένο συνδρομητή θεωρείται ότι προέρχεται από τον συγκεκριμένο συνδρομητή.

Για τον λόγο αυτό, η μέθοδος αυτή είναι διαθέσιμη μόνο στις περιπτώσεις όπου ο συνδρομητής είναι σε θέση να εγγυηθεί ότι είναι ο μοναδικός χρήστης των **source IP/port** συνδυασμών που θα δηλωθούν για αυτή τη χρήση.

Platform-specific authentication

Για τις περιπτώσεις όπου το άκρο του συνδρομητή είναι σε κοινή χρήση με άλλα πρόσωπα, θα πρέπει να διερευνηθεί ανά περίπτωση ποιος μηχανισμός είναι διαθέσιμος από την πλατφόρμα για τον ασφαλή προσδιορισμό της ταυτότητας του συνδρομητή για κάθε SIP μήνυμα που παραδίδεται στο δίκτυο της modulus.

Επειδή οι μηχανισμοί αυτοί διαφέρουν ανά πλατφόρμα, το παρόν έντυπο δεν μπορεί να τους αποτυπώσει παραθέτοντάς τους. Αν η πλατφόρμα που έχει επιλέξει ο συνδρομητής δεν έχει προηγούμενο διασύνδεσης με το δίκτυο της modulus, οι όποιοι διαθέσιμοι μηχανισμοί θα πρέπει να αξιολογηθούν ως προς την επάρκειά τους πριν την υλοποίηση της λογικής διασύνδεσης.

4. SIP Servers

Η modulus διατηρεί **High Availability Geo-Redundant Cluster** από SIP Servers πίσω από το hostname:

voips.modulus.gr

High availability στην εξερχόμενη κατεύθυνση

Ο μηχανισμός εξαρτάται από την πλαφόρμα του συνδρομητή

Το **failover/load balancing** στην εξερχόμενη κατεύθυνση βρίσκεται στον έλεγχο της πλατφόρμας ή του εξοπλισμού στο άκρο του συνδρομητή.

Η υποδομή της modulus συνεισφέρει στο μηχανισμό μόνο την ύπαρξη δύο άκρων προς τα οποία μπορούν να παραδίδονται τα εξερχόμενα μηνύματα, αλλά δεν μπορεί να ελέγξει το πότε αυτά επιλέγονται ως προορισμοί, ή αν μία αποτυχία στην παράδοση θα οδηγήσει σε νέα προσπάθεια στο εναλλακτικό άκρο.

DNS SRV lookup

Προτείνεται η χρήση **DNS SRV Lookup** για την αξιοποίηση της redundant υποδομής, μόνο εφόσον η πλατφόρμα ή ο εξοπλισμός του συνδρομητή αξιοποιεί την απάντηση του συστήματος DNS για το σκοπό αυτό. Συγκεκριμένα θα πρέπει:

- Εφόσον η διαπίστευση γίνεται με τη μέθοδο **SIP Digest Authentication**, η πλατφόρμα θα πρέπει να κατευθύνει ένα SIP μήνυμα που περιλαμβάνει την απάντηση σε ένα challenge στο ίδιο άκρο στο οποίο παραδόθηκε το μήνυμα που έγινε challenged.
- Μηνύματα που ανήκουν σε υφιστάμενο transaction ή dialog πρέπει να χρησιμοποιούν το ίδιο άκρο σε όλο τον κύκλο ζωής του transaction ή του dialog.

- Οι εναλλακτικές εγγραφές που περιλαμβάνονται στα **DNS SRV records** πρέπει να αξιοποιούνται από την πλατφόρμα για την υλοποίηση λογικής failover σε σενάρια όπου το failover έχει νόημα και με τρόπο που να είναι διαφανής για τους χρήστες. Η υποστήριξη SRV lookup από μόνη της δεν είναι επαρκές κριτήριο για την ύπαρξη failover μηχανισμών που το αξιοποιούν αποδοτικά ή και καθόλου. Ενδεικτικά, μία αποδοτική υλοποίηση θα περιελάμβανε:
    - Επαναδρομολόγηση μηνύματος εκτός dialog στο εναλλακτικό SRV record εφόσον η απάντηση της πρώτης προσπάθειας υποδηλώνει σφάλμα εξοπλισμού και όχι κάποιο έγγυρο κωδικό σφάλματος (π.χ. failover σε μηνύματα της κατηγορίας 5XX μόνο).
    - Καθορισμός του Timer B (**RFC 3261**) σε τιμή τέτοια ώστε ο χρήστης να μην αναμένει υπερβολικό χρόνο χωρίς ένδειξη για την εξέλιξη της κλήσης (π.χ. 2 δευτερόλεπτα).

Supported Signaling Protocols

- UDP: `5060` ή `6050`
- TLS: `5061`

Η χρήση **TLS** προτείνεται για την **κρυπτογράφηση** του SIP signalling.

5. Media & Audio Codecs

Υποστηρίζονται τα ακόλουθοι codecs:

- G.722
- G.711 A-law
- G.711 μ-law
- G.729
- T.38 για Fax

Codec Priority

Προτείνεται η ακόλουθη σειρά προτεραιότητας:

1. G.722
2. G.711 A-law
3. G.711 μ-law
4. G.729

Media Transport

Υποστηρίζονται:

- RTP
- SDES-SRTP
- DTLS-SRTP

Η χρήση **SRTP** σε συνδυασμό με **TLS** παρέχει κρυπτογράφηση τόσο της σηματοδοσίας (SIP signalling) όσο και του περιεχομένου της επικοινωνίας (media stream).

Η κρυπτογράφηση του media stream μόνο δεν μπορεί να γίνει με ασφάλεια, συνεπώς η χρήση SRTP για το περιεχόμενο της επικοινωνίας συνεπάγεται υποχρεωτικά και τη χρήση TLS για τη σηματοδοσία.

6. Encryption

Υποστηρίζονται **TLS v1.2** και **TLS v1.3**.

TLS v1.2

Supported cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

TLS v1.3

Supported cipher suites:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

Όπου είναι διαθέσιμο, προτείνεται η χρήση **TLS v1.3**.

7. Number Formatting

Για κλήσεις από και προς Ελλάδα χρησιμοποιείται εξ ορισμού national format.

National Format

Ενδεικτικά:

- 210xxxxxxx
- 69xxxxxxxx

Για διεθνείς κλήσεις, όπου CC το πρόθεμα της χώρας:

00CCxxxxxxx ή +CCxxxxxxx

Κατόπιν αιτήματος μπορεί να χρησιμοποιηθεί **+E.164 format** για το σύνολο των κλήσεων.

Ενδεικτικά:

- +30210xxxxxxx
- +3069xxxxxxxx
- +44xxxxxxxxx

8. SIP Headers & CLI Presentation

Για την παρουσίαση και πιστοποίηση του calling number υποστηρίζονται, κατά σειρά προτεραιότητας:

1. P-Asserted-Identity (PAI)
2. P-Preferred-Identity (PPI)
3. Remote-Party-ID (RPID)
4. From

9. NAT & Firewall Requirements

Για την απρόσκοπτη λειτουργία της υπηρεσίας πρέπει να επιτρέπεται η απαραίτητη κίνηση προς το δίκτυο:

`185.73.40.0/22`

SIP Servers

- `185.73.42.250/32` — UDP `5060` , UDP `6050` , TCP `5061`
- `185.73.43.250/32` — UDP `5060` , UDP `6050` , TCP `5061`

Media / RTP Servers

- `185.73.43.248/29` — UDP `20000-60000`
- `185.73.42.248/29` — UDP `20000-60000`

Για λειτουργία πίσω από NAT προτείνονται:

- SIP ALG: Disabled
- Endpoint-Independent NAT mapping
- Address-Dependent NAT filtering
- Keep Alive / OPTIONS Support
- QoS Prioritization για Voice Traffic

Θα πρέπει επίσης να λαμβάνονται υπόψη τα εκάστοτε **Security Guidelines** της υπηρεσίας.

10. Network Requirements

Για βέλτιστη ποιότητα φωνής προτείνονται:

- Latency < 150 ms
- Jitter < 30 ms
- Packet Loss < 1%

11. Integration & Testing

Πριν από την παραγωγική ενεργοποίηση προτείνεται η πραγματοποίηση δοκιμαστικής διασύνδεσης ώστε να επιβεβαιωθούν:

- SIP signaling
- Inbound routing & failover
- Outbound routing & failover
- Authentication
- CLI presentation
- Number formatting
- Codec negotiation
- RTP / SRTP media
- NAT / Firewall compatibility

Μετά την επιτυχή ολοκλήρωση των δοκιμών μπορεί να ακολουθήσει το production onboarding.