**Request for Proposal (RFP): Deep Packet Inspection (DPI) Solution and Policy Control and Charging Rules Function (PCRF-PCF) Solution**

Contents

[1. Introduction 2](#_Toc182563216)

[2. Scope of Work 2](#_Toc182563217)

[3. General Requirements 4](#_Toc182563218)

[4. Technical Requirements 5](#_Toc182563219)

[5. Vendor Qualifications 9](#_Toc182563220)

[6. Reporting 9](#_Toc182563221)

[7. Signature Database and Updates 14](#_Toc182563222)

[8. Administration 14](#_Toc182563223)

[9. Service Level Agreement 16](#_Toc182563224)

[10. Professional Services 18](#_Toc182563225)

[11. Project Delivery and Implementation Plan 18](#_Toc182563226)

[12. Documentation 19](#_Toc182563227)

[13. References 19](#_Toc182563228)

[14. Training 20](#_Toc182563229)

[15. Dimensioning and Capacity 20](#_Toc182563230)

[16. Installation and Hardware 20](#_Toc182563231)

[17. Killing Factors 21](#_Toc182563232)

[18. Bill of Quantity 21](#_Toc182563233)

[19. Pricing 22](#_Toc182563234)

# Introduction

This Request for Proposal (RFP) is issued by MIC2 seeking proposals from qualified vendors for the supply, deployment, integration and maintenance of a Deep Packet Inspection (DPI) and Policy Control and Charging Rules Function (PCRF-PCF) solution. The Solution is intended to create new revenue streams, enhance network security, traffic management, and content filtering capabilities. Solution need to be implemented IN-LINE and to be able to perform the below tasks such as: Accurate Signature Database, Traffic Blocking, Traffic mirroring on different criteria, PCAP capture, End-to-End trace, ..

# Scope of Work

The selected vendor must provide a DPI and PCRF-PCF solution that offers comprehensive real-time packet analysis, content filtering, intrusion detection, policy enforcement, policy control, targeted advertising, Quota management, and traffic shaping functionalities. The solution must seamlessly integrate with MIC2 existing network infrastructure and to be scalable to accommodate future network expansion.

The Main purpose is to accurately identify and categorize internet traffic by application type. Once traffic is identified and categorized, solution should allow MIC2 to enforce specific policies for each type of data bundle by integrating with MIC2 different systems. Such solution is needed to process and inspect data, in real time, being sent over MIC2 Network to take actions such as alerting, blocking, re-routing, or logging. Solution must accurately track when and how much of the data is used, the precise tracking ensures that only the data used for the specified services is counted against the bundle’s data allowance.

Solution need to provide granular, real-time data analysis required to implement dynamic policies based on the actual content of the traffic, such as prioritizing or throttling certain types of traffic. Solution will take decision based on the type of traffic identified to provide the necessary network resources.

Ensure network resources are allocated according to the established policies, real-time adjustments to policies based on changing, network conditions, user behavior, or MIC2 requirement, appropriate charging mechanisms are applied for each subscriber session, managing and enforcing QoS policies for data sessions, ensuring a consistent and reliable user experience (5G new core should be supported)

Main functionality should include in addition to the above the capability to easily perform the below examples:

* Block VPN applications (example FortiClient, WireGuard, NordVPN,..) for certain users at certain location
* Create bundles related to the categories:
  + Gaming
  + Streaming
  + Online meeting,..
* Integration with Online Charging System (OCS)

Interact with the Charging Gateway Function (CGF) to manage the charging aspects of subscriber sessions, exchange information related to charging control and ensuring that charging policies are applied consistently across the network.

OCS provide credit control information to PCRF-PCEF, to make decisions about whether a subscriber has sufficient credit to continue a service session, enable enforcement of charging policies as data sessions progress, to manage subscriber usage and preventing over consumption – integration will be done through the Gy interface and Nchf interface for UPF 5G (should be supported)

* Integration with CRM

Get the necessary data from CRM related to service plans and customer account details.

* Integration with Provisioning System
* Integration with SMSC/ Notification Server (SMPP, SOAP,..)

Get the necessary data from

* Integration with IMS
* Solution should support integration through Diameter interfaces with all the needed platforms (Rx, Sy, Sd, Gxx, Gi,..),
* Solution should support standard SOAP interface
* Solution should be 5G ready and provide following interworking functions with SMF/AF/AMF/CHF:
  + N7, N5, N15, N28,..
* Solution should support optional and mandatory AVPs.
* Integration with Packet Core:
  + Interoperate with the packet core elements such as Serving Gateway (SGW), PDN Gateway (PGW) for 4G, and Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) for 5G.
  + Connection is needed with all elements in order to provide enrichment related to the IMSI/IMI and cell-id of the user, in case you can provide this with no integration, please provide technical details. In case vendor can provide this information through other integration to specify

Solution should be dimensioned for 3 million data customers including 800,000 active VoLTE/eSRVCC capability.

Traffic per site is around 40 Gb/second (distributed over 4 sites)

Solution should be deployed in 4 Core Sites with a centralized reporting and management location with high availability and redundancy, for the PRCF-PCF it can be deployed in two of these 4 sites.

*Bidders must specify if DPI or PCRF-PCF will fulfill the technical requirements in the compliancy sheet.*

# General Requirements

* Solution should be high available and guarantee 99.999% availability
* Power supply should be implemented in redundant design.
* Solution must support restart of single process software without affecting other processes and with no impact on the customer or services
* Solution should support traffic failover capabilities in N+1 configuration
* Solution should be vendor agnostic
* Solution should be topology agnostic
* Solution should cover all traffic for all customers regardless of the device used.
* No impact on customer experience should be observed
* No interruption to service should be observed
* No impact on service or customer experience during patches or system upgrade
* By-pass mechanism should be available to avoid any interruption of traffic
* Solution should cover all the traffic regardless of the content provider.
* Nothing should be needed from the end-user in terms of software or application in order to classify and identify the traffic.
* For Intrusion Detection, solution must have the needed signatures to be able to identify suspicious, and malicious threat patterns on a network.
* Solution should support different generation from 2G till 5G-NR radio networks as well as 4G EPC and 5G SA core packet cores.
* Solution must support dual mode for PCRF-PCF
* Solution must support convergence and use of WiFi and fixed broadband access technologies.
* Solution should process the user plane and enforcement in the Gi for 4G deployment. And on N4, N6 & N9 for 5G SA (should be supported).
* Solution should be scalable with the increase of traffic in the network.
* Solution should have RADIUS for accounting traffic in order to maintain accounting information on a subscriber basis for the time the subscriber session lasts.
* Solution should provide capabilities to capture IPv4 and IPv6
* Solution must support traffic classification and management per subscriber basis in dynamic IP address environment.
* Solution should support IPv6 transitioning techniques:
  + NAT44
  + Tunneling
  + Dual Stack approach
* Solution should support correlation/enrichment for individual and unique subscribers by maintaining a mapping between the MSISDN- IMSI – and IP address for the duration of the subscriber session. (please detail how this will be done)
* Solution should support 10GE and 100GE interfaces
* Solution must have centralized management solution to apply policies across all sites.
* Real time synchronization of all configuration and customer information shall be available between the different geographical redundant sites.
* Solution should support automatic Backup Setup
* Solution should support automatic flow control
* Solution should support automatic load balancing
* Solution should support automatic rollback upon upgrade failure

# Technical Requirements

The solution should meet the following technical criteria:   
- High-performance metrics, including but not limited to, throughput and latency.  
- Scalability to support growing data and network traffic.  
- Compliance with relevant industry standards and regulatory requirements (3GPP standards)

* Solution should be NFV- ready.
* Proposed deployment architecture should be shared.
* Solution should be offered as hardware based.
* Solution should have a user friendly interface for System administration to do the below:
  + Configuration Management
  + Equipment management
* Solution should support TCP Acceleration requirements.
* Solution should support TCP Acceleration requirements.
* Solution should support Video Management and Optimization Requirements – including encrypted Video Management.
* Solution shall provide a user friendly web interfaces to manage service/policy/rule/condition/action/notification/etc. configuration
* Solution should support Dynamic and Static Policy Control based on:
  + Volume usage
  + Time- duration
  + Date-time period
  + APN
  + Service Zone
  + User Terminal Type
  + User bundle/ subscription
  + User Category (VIP, Data only, Corporate,..)
  + QoS
  + Roaming Region (bill shock solutions- define single or multiple operators in a region based on traffic on the required QoS or notifications,..)
  + Shared usage (feasibility to set usage threshold limits for every shared user)
  + Group shared usage (users within a group to share all group services with feasibility to set usage threshold limits for every shared user)
  + Rating (for bill shock solutions, to apply rating for every roaming operator with flexible rounding mechanism per operator).
* Solution should be transparent both to the end-user and content provider
* Solution should provide a SOAP interface for Provisioning system and applications to:
  + Add/delete/update/ and retrieve user profile
  + Add/delete/ update/ retrieve service/ bundle/ package/ accumulation
  + Add/delete/ update/recharge/ retrieve/ reset/ clear user quota/ account
  + Add/delete/ update/ retrieve user threshold
* Solution should provide batch mode support for provisioning/ service configuration/ subscriber profile update
* Ability to manage quota per service and setting the action taken when quota is depleted for example: stop service, pay as you go, decrease the QoS, ….
* Solution should provide an advanced bill shock prevention for roaming customers
* Solution should provide an advanced bill shock prevention for data consumption locally based on each subscriber profile.
* Fair usage policy with usage monitoring over Gx
* Device based policies
* Solution should have a flexible data sharing functionality which allows several customers to share the same data bundle with configurable thresholds for each customer.
* Solution should be able to send user notification via multiple channels: SMS, Email, SOAP request to third party application...
* Solution should support Event Data Recording to generate records of the event changes for subscribers
* The platform shall support Multi -Quota to provide users with different quotas based on his usage.
* Solution must have the signatures to be able to identify suspicious, and malicious threat patterns on a network.
* Predefined priorities shall apply for the quotas, ex: when quota1 depleted, user can used quota 2
* The platform shall support Top-Up Quota to allow user to recharge his quota before or after quota depletion
* The platform shall support Tethering Control to be able to restrict or charge tethering traffic
* The platform shall support Multimedia Priority Service to provide priority for VoLTE calls when network gets congested for a subscriber category
* The platform shall support ADC (Application and Detection Control) over Gx
* The platform shall support setting threshold limits for users based on their profile categories
* The platform shall support converting quota volumes to KB, MB, GB, TB in notifications
* The platform shall support Bandwidth on Demand to enable subscribers to request higher bandwidth for a certain time period
* Solution should rely on heuristics engine to classify encrypted flows
* Solution should rely on heuristics and not through simple detection
* Solution should detect the IMEI and the device type in order to dynamically adjust the throttle rate to match a defined video resolution.
* Solution should have the capability to differentiate between video streaming and video downloads.
* Solution should support HD video optimization in real time
* The platform shall support Cell Congestion Control by automatically updating the QoS of subscribers
* Solution should provide heuristics-based signatures to categorize and optimize video to a configurable bitrate
* Solution must support ability to load heuristics logic into the DPI classification engine (Application Recognition Module) and update the heuristics with regular signature updates without requiring a software update.
* Solution signature should be based on different technologies including SNI extraction, heuristics analysis, and behavioral metrics. (detail how this will be done)
* Vendor must provide details of methods used to keep up with the ongoing changes of encryption technologies being utilized by content providers.
* Solution must provide capability to send targeted advertising for the customers based on different criteria.
* Solution must identify whether a customer is on a prepaid or postpaid plan.
* Solution must be able to identify traffic consumption if customer has different data plans at the same time.
* Solution must provide advertisement injection capability
* Solution should provide multi PCEF support (Establish Gx sessions with multiple PCEFs, bind these sessions together, and deliver different policies to different PCEFs based on policy configuration. It should be able to deliver updated policies to other PCEFs if the subscriber status on one PCEF changes.)
* Quota reset date can be daily/monthly/yearly, per calendar day/month/year, per subscriber billing cycle, or customizable per subscriber
* The platform shall support multi-Service APN to allow subscriber to access multiple Packet data networks over one APN
* The platform shall support Multi -Quota to provide users with different quotas based on his usage.
* Support URL filtering and blocking unauthorized or inappropriate URLs
  + Parental control
  + Periodic URL categories update
  + The system must allow creating whitelists/Blacklists
* Solution must have the capability to prevent over-consumption- and allow to notify customers about the consumption % per bundle (in case several bundles are available)
* Solution must provide policy enforcement by, not limited to :
  + Content, application, plan, time, traffic pattern, Zero rating…
  + Tethering devices such as Type of devices, Number of devices tethered, Consumption per device flow
* Solution should support Traffic Control: Allow, block, mark, http or Https redirect, TCP reset, shape, divert,… (vendor should detail how this will be done)
* Solution should support Event Based triggers: Ability to create policies triggered by specific events, such as network events, user behavior, or application specific occurrences.
* Solution should support IMS traffic Identification, precise identification and handling of IMS traffic.
* Solution should support Roaming Subscriber Recognition: Ability to recognize and handle traffic from roaming subscribers per operator/ country, including accurate detection of visited networks same
* Solution should be able to identify if user is connected to 5G sites in case of 5G NSA core (detailed explanation of how this will be done is needed)
* PCRF must support embedded SPR
* Supports 3GPP interfaces: Gx/Sd, Rx, Sy, Sh, Ud, Gy,…
* Support for SOAP
* Provides REST API for provisioning profiles and usage plans
* Support real-time services (like VoLTE) and non-real time services (like video streaming), enabling dynamic QoS adjustments and charging.

# Vendor Qualifications

Vendors must demonstrate:

- Proven experience in successfully implementing DPI / PCRF-PCF solutions, with similar scope – at least 3 references in mobile network operator with at least 3 million customers per operator.   
- Comprehensive support and training Center capabilities.  
- A clear product roadmap showcasing innovation and future updates – 3 years roadmap.

# Reporting

-Friendly and easy to use Graphical User Interface (GUI)

-Data, stats should be available on Map level to check which apps are being used in each area and if a new app is being used in specific area only.

-Ability to define KPIs from the fields generated not limited to (traffic, location, group, device type, latency, application,..)

-Generate reports for all existing services, policies, rules, quota, QoS, … and ability to add/ remove any field

-Ability to create different criteria related to customers data bundle – location – age group,..

-Generate reports related to consumption related to each specific bundle – in case user has more than one bundle at the same time

- Executive dashboard for top apps usage in the network, top handsets, top users,…

-Video and VoIP reports:

* + 1. Call Destination
    2. Average call duration
    3. Average calls per user
    4. Number of initiated calls
    5. Number of received calls
    6. Calls by provider (e.g., Skype, WhatsApp, etc.)
    7. Minutes by protocol
    8. Minutes by provider
    9. QoE, including MOS, latency, and jitter

-Solution must provide Customer Behavioral Analysis: identify different segments based on patterns, trends, usage, Devices, Packages/bundles, ..

- Solution must provide Consumption Analysis per each bundle separately (if customer is subscribed to more than 1 bundle) in addition to traffic type

-Solution should provide but not limited to Statistical report generation(Number of requests per interface(Gx, Rx, Sy, SMPP, SMTP etc.) and per entity (GGSN, EPC, OCS, IMS, SMSC, Mail Server, etc.), successful/failed requests, CPU Load Measurement, Subscribers Statistics, Service Statistics, Quota Consumption Statistics, flow control statistics etc. and for selective time periods (minutes, hours, days, weeks, months, years)

-Network Performance and Quality Indicators:

* QoE metrics per service and application
* Traffic classification per service type and application
* Accurately measure and report latency, packet loss and throughput per user (service- application)
* Solution must aggregate metrics per cell, site, region, core, network,..
* Solution must provide ability to compare the metrics across different criteria
* Solution to provide detailed QoE analysis per handset type
* Solution must provide real-time reporting capabilities
* Solution should provide KPIs and QoE on interactive map in real time

-Video QoE Analysis:

* Comprehensive analysis of Video Experience per Application, Location, User and device level
* Analytics related to video resolution, consumption, and streaming health (buffer time)

- Gaming QoE Analysis:

* Comprehensive analysis of Gaming Experience per app, location, user and device level.

- Solution must integrate with necessary elements to provide all related information in the metadata such as:

* IMSI, IMEI, Cell-id,..

-Solution must log every single subscriber connection –flow, including:

* Time of usage
* Application used
* Available metadata form the flow
* Source IP
* Destination IP
* Source Port
* Destination Port
* Device Used

-Solution must have AI/ML for:

* Application Signature
* Anomaly Detection
* Clustering of customers per traffic, usage, behavior, revenue stream and volume
* Intelligent Reporting/ Analytics including but not limited to prediction for customers willingness, high financial capabilities, and interests
* Live dashboard and advanced AI engines with dynamic score for each Customer

-Solution must provide score card for different services provided and overall network figure with ability to drill down/up

-Solution must provide Geo-IP capability integrated with map on the GUI.

- Vendor’s DPI solution must be able to log every single HTTP request:

* Time of request
* URL
* Content type information

- Solution must generate PCAP of desired traffic and export PCAP files

* Per specific user
* Per specific application
* Per specific port
* Per specific IP
* Per specific destination IP

- Several PCAPs can be collected simultaneously.

- Solution should support classification operating between Layer 3 and L7

- Solution should support the generation of statistics such as:

* Processing time
* Response time
* CPU Load
* Gx Errors
* Gx Response time
* Rx Errors
* Sy statistics

- Solution should automatically categorize applications into logical groupings (Streaming, VoiP, File sharing, Entertainment,…)

- Vendor must commit to a level/ proportion of unclassified traffic based on volume and number of sessions.

- Not less than 97% of the volume and the session number of traffic should be accurately identified.

- Solution must identify all unknown applications and services and provide the ability to correctly and accurately identify them.

- Solution must identify and report multicast traffic.

- EMS should provide but not limited to Statistical report generation(Number of requests per interface(Gx, Rx, Sy, SMPP, SMTP etc.) and per entity (GGSN, EPC, OCS, IMS, SMSC, Mail Server, etc.), successful/failed requests, CPU Load Measurement, Subscribers Statistics, Service Statistics, Quota Consumption Statistics, flow control statistics etc. and for selective time periods (minutes, hours, days, weeks, months, years)

- Solution must support real-time system and traffic logging and reporting.

- Solution must support traffic logging and reporting (at least 1 months of raw data – 3 years aggregated data) – please provide details and how hardware dimensioning is done based on this point

- Solution must allow for custom reports based on different criteria

- Solution should have different level of access role permissions and ability to mask confidential/ subscriber identity.

- Solution must allow the search per specific subscriber for a specific period of time to collect all the related detailed metadata.

- Solution must have the capability to identify customers facing QoE degradation and report the list of IMSIs and count in real time

-Solution must have the capability to give number of users in specific time using specific application.

- Solution should provide scoring dashboard for key traffic categories

- Solution should provide centralized reporting platform (collected from different sites)

- Reports generated must be exportable in PDF, CSV,..

- All metadata should be streamed to third-party solution in real-time

- Solution must allow filtering of data related to specific customers or fields before export.

- All data should be exportable through North Bound Interface

- Ability to filter out certain subscribers/IMSIs from the export

- Export and data from database in customizable output formal (example CSV, PDF,..)

- Solution must be able to report on all calls occurring over applications that include number of users, total data traffic / duration, and list of users.

- Solution must have the capability to prevent over-consumption

- Solution should generate report related to the number of customers per bundle, and the traffic consumed vs the actual bundle limit on daily-weekly-monthly levels.

- Solution should generate reports about the IN & Out of bundle consumption separately and traffic type.

# Signature Database and Updates

- Solution must ensure bi-weekly update

- Vendor must provide evidence of a dedicated team related to signature if done in-house, and details about the signature database if obtained from third party.

- Solution must support updates with no impact on live traffic

- Protocol recognition should be custom and locally configurable by MIC2 using simple and syntax based signatures.

- Vendor must explain the mechanism used for signature and how each application is categorized.

- Solution should allow easy to capture PCAP traffic for new applications to identify and apply new signature.

-Solution signature should be based on different technologies (to be explained in detail) such as SNI extraction, Heuristics analysis, and Behavioral metrics.

# Administration

- Role based access level.

-Solution should be able to provide detailed logs about who accessed confidential data

-Data should be anonymized based on roles/ privilege

- No limitation on number of users for the GUI.

- Automatic schedule for common administration tasks (backup, health check, logs, performance reports dumps, inventory, logical and physical configuration, etc...). Log data should be kept for 6 months, PM data should be kept for 1 month

- Single interface for management

- Solution should support ability to trigger an alarm based on particular pre-defined action.

- Solution should support policy configurations and updates through a graphical user interface (GUI)

- Solution must support simultaneous shaping in both upstream and downstream directions at different rates.

- Solution must have the capability to block certain traffic on certain users (example gambling websites)

- Solution shall support end-to-end user trace

- The solution should support backup for all the needed data, the vendor should provide all the backup layers and provide information about it

- Solution must have the capability to block certain applications if requested (example block VPN apps)

- Solution must support ability to copy subscriber traffic and send out an interface to third-party system.

- Solution must enable traffic monitoring with zero impact on the traffic flow.

- Solution must allow video and VOIP traffic management not limited to blocking VoIP calls when needed (by Time, Location, Bundle, User, User Group, Application,..)

- Solution must allow block certain application (by Time, Location, Bundle, User, User Group)

- Solution must allow throttle/limit throughput (by time, location, bundle, user, user group, application,..)

- Solution must allow promotion of freebies (by time, location, bundle, user, user group, application,..)

- Solution must allow to force throughput based on Device to optimize MB usage/minimize congestion.

- Build a dynamic customer profile database, based on customer location, activities, interests, traffic, etc,..

- Tracking and reporting for all actions done on the system by user- ip,….

- Automatic dump of operation, security and system logs (storage period for logs for 1 year)

-Solution should be configured to send all logs to SIEM solution

-Solution must ensure protection of sensitive subscriber data, and access control policies are enforced to prevent unauthorized data access

- Full control over users, all users should have user ID – Password that define their access level and what functions – information they can do or retrieve.

- Fault management solution should be available to provide the below:

* Acknowledge alarms and by choice delete alarms
* Alarm history and event history
* NMS should allow to export alarms to external system
* Threshold feature (in case certain events exceed a certain limit- alarm need to be generated)
* Alarm correlation
* Define actionable commands through rules
* Graphical and tabular representation of multiple measurements (real time and offline).

# Service Level Agreement

* No impact on customer experience should exist (bypass mechanism should be available)
* Daily health check for all the processes
* Vendor should support in creation of new bundles, ensuring successful testing, troubleshooting and implementation of the solution.
* Bidder must provide support services, including response times and escalation procedures.
* Bidder must provide availability of software updates and patches.
* Support should include automate health check for all the processes ensuring no impact on network or customer experience
* No traffic loss on the network – customer level is allowed or tolerated
* Bidder must provide hardware warranty and replacement policies.
* Bidder must provide 3 years warranty and support for the overall solution – hardware and software.
* Vendor should specify repair and return time (with no impact on the customers or experience).
* Vendor must provide support for 3 years that start with the acceptance of the solution
* Bidder must provide support services, including response times and escalation procedures.
* Repair and Return for the damaged hardware is needed.
* Solution should run on the latest version during acceptance, and throughout the 3 years of support the latest version should be provided and installed as part of the support agreement
* Support should start after Final acceptance and for a three years period
* Bidder must attach escalation chart email address and helpdesk number to contact in case of a breach or support.
* Bidder support must be backed up with vendor support
* Health Check Assessment: to audit all configuration changes that occurred on the platform. Health Check to be conducted each quarter or earlier if needed
* Solution should not impact the performance from end customer perspective (less than 1 milliseconds for responsive services)
* Solution should not lead to packet loss
* Solution should by Synchronized with all sites and with the network to reflect the correct timing in reporting across the sites that reflect the actual time
* Bidder must provide on-site support and/or remote support: 24 hours a day, 7 days a week and a maximum response time based on the below SLA :

|  |  |  |
| --- | --- | --- |
| * Crucial Priority (Severity A) (Impact on MIC2’s Performance) | * Immediate response by phone or email | * Maximum 2 hours resolution time as of the response / 24 hours - 7 days a week |
| * Average Priority (System Urgent or Severity B) | * Response by phone or email within maximum 3 hours | * Maximum 6 hours resolution time as of the response / 24 hours - 7 days a week |
| * Not Critical (System is running with no threat) | * Response by phone or email within maximum 5 hours | * Maximum 5 working days for resolution as of the response including site visit upon MIC2’s request |
| * Query | * Response by phone or email within maximum 1 day | * Maximum 2 weeks for resolution as of the response including site visit upon MIC2’s request |
| * Hardware Repair and Return | * Response by phone or email within maximum 1 day | * Maximum 6 weeks for resolution time as of the response |
| * Signature Update | * Response by phone or email within maximum 1 day | * Classify minimum 97% of the traffic (Based on the traffic and number of sessions). * Bi-weekly update of the signature. * Classification of new applications or websites whenever identified new by MIC2, in addition to their update within 2 weeks as of the response |

# Professional Services

* Bidder must install and migrate existing rules and policies
* Certified on-site engineer need to have full knowledge about the solution for a period of 3 years after Final Acceptance
* Onsite Engineer must handle all the needed tasks
* Onsite Engineer must perform Knowledge-Transfer to the team

# Project Delivery and Implementation Plan

* MIC2 expects the bidder to clearly outline and detail the expected delivery, installation, and integration and validation times.
* Detailed project implementation plan (PIP), mentioning each milestone
* Delivery of the project should adopt Agile methodology – phase approach delivery of the project
* Vendor must provide and share previous implementations of such projects – references to be provided
* Vendor must provide reference of large-scale implementations for similar solutions
* Vendor is responsible for end-to-end integration including hardware, racking, cabling, and power connectivity
* Bidder must submit a minimum 3 years roadmap for the proposed solution.
* Solution should be finalized within 8 months of PO issuance
* Vendor is responsible for end to end installation of the solution with integration with all the needed network elements to include the needed resources (cables, …)
* Vendor is responsible for policy migration from existing PCRF, packet core or DNS in relation to website blocking or bundle created
* Vendor is responsible for all the integration
* Vendor is responsible for the commissioning

# Documentation

* Bidder must provide product description.
* Full system documentation including full feature list
* User Manual
* System features that are included in the offer only.
* Selected Vendor (after project is awarded) should provide all acceptance documents

# References

* Vendor must provide references for similar deployments in mobile network operators
* Vendor must provide the features implemented that are similar to our requirements in each deployment
* At least 3 similar deployments for the solution should be available

# Training

* Training shall cover all areas of the solution (end user part and administration part)
* End user part should cover the usage of the solution, how to create dashboards and how to retrieve data from the GUI.
* An advanced certified training should be delivered in an appropriate laboratory setting and include the costs of accommodation and travel. A minimum of Five (5) trainees for DPI training is required to cover all aspects for the solution
* An advanced certified training should be delivered in an appropriate laboratory setting and include the costs of accommodation and travel. A minimum of Four (4) trainees for PCRF/PCF training is required to cover all aspects for the solution
* Advanced training should cover courses for DPI (at least 5 days) and courses for PCRF (at least 5 days)
* Vendor to specify exactly the training for DPI attendees
* Vendor to specify exactly the training for PCRF attendees
* Travel Expenses must be included for the advanced training
* Accommodation Expenses must be included for the advanced training

# Dimensioning and Capacity

* 4 Core sites distributed over Lebanon
* 3 million data customers (each customer might have more than one data bundle at same time)
* 40 Gbps in each core site
* Solution must be scalable to ensure that growth in data traffic can be handled with minor upgrades if needed to at least double this traffic
* Solution must ensure that 5G NSA and SA are available and once rolled out in MIC2 network it should be supported with no additional license
* Vendor must ensure that the solution is running on the latest version at acceptance and the latest version should be downloaded as part of the support throughout the 3 years of support as part of the agreement.

# Installation and Hardware

* Vendor must provide all the needed hardware for installation
* Solution should be NFV ready
* All parts related to installation and integration with existing network elements (cables, sfp,..)
* 40 Gbps in each core site
* Power redundancy should be included
* Solution should encompass redundancy and reliability: redundant and hot swappable power supplies, fans, hard drives, fail to wire capability, N+1 redundancy, and support for active/ active deployment
* Vendor to provide the required ventilation requirements in each site and expected peak and average power consumption of the Solution
* Solution must be high available in each site and in the central site
* Vendor must provide all needed parts related to installation including cables, SFP, switches, ..
* Labeling must be done during installation and before acceptance
* Bidder to provide detailed hardware specifications and all third party licenses should be included in the offer.

# Killing Factors

* The bidder must provide on-site and remote support based on the requested service level agreement.
* Vendor must ensure seamless integration with OCS – provide references
* Vendor must ensure seamless integration with Packet Core – provide references
* Vendor must ensure seamless migration of the current policies implemented on PCRF PCF, packet core and DNS in relation to bundles or website/ URL blocking
* At least 3 similar deployment for the solution in similar environment in terms of throughput and number of customers in Mobile Network Operator for the complete solution including integration – provide references
* Solution signature should be based on different technologies (to be explained in detail) such as SNI extraction, Heuristics analysis, and Behavioral metrics.
* Vendor should support in creation of new bundles, ensuring successful testing, troubleshooting and implementation of the solution.
* Vendor to provide 3 years roadmap
* Vendor must have a clear AI/ML integrated within the solution (to provide details)
* No impact on customer experience should exist (bypass mechanism should be available)

# Bill of Quantity

* Bidder must provide pricing summary for the 3years after acceptance
* Bidder must provide detailed unbilled BoQ for the technical evaluation
* All features and licenses provided must be included
* Vendor must provide all the needed hardware for installation
* All parts related to installation and integration with existing network elements (switches, cables, sfp,..)
* 40 Gbps in each core site
* Solution must be scalable to ensure that growth in data traffic can be handled with minor upgrades if needed
* Solution must ensure that 5G NSA and SA are available and once rolled out in MIC2 network it should be supported with no additional license
* Test bed should be available to test the backups and the restore procedure without affecting the live system
* Vendor need to provide all the spare parts needed to be available on site (at MIC2 possession) in case of any hardware failure to make immediate replacement.
* Repair and return is a must.
* Any missing needed hardware spare part will result in penalty.

# Pricing

* Break Down of all the prices must be provided with all hardware, features and licenses including third party licenses
* Detailed Unbilled price list to be provided in the technical offer
* Vendors are required to provide a detailed cost breakdown, including hardware, software, license, installation, maintenance, and support services. Latest Software version for all modules should be available during acceptance.
* MIC2 can chose any or all of the features provided.
* **Any license or feature mentioned in the compliancy sheet and/or in the technical response will be considered as part of the solution/ additional features that are not included in the solution should be clearly mentioned**