Body of European Regulators for Electronic Communications

BEREC

BoR (17) 179

Net neutrality measurement tool specification

5 October 2017

Table of Contents

Executive summary

The Net neutrality QoS[1] Feasibility study [1] which was adopted by BEREC Board of Regulators (BoR) in December 2015 recommended that BEREC[2] could specify QoS measurement software for NRAs[3] on an opt-in basis for adoption, and then implement such opt-in software, subject to approval by BoR to move forward from the specification phase to implementation phase. This report covers the specification of the software implementation phase only.

The opt-in software specification builds on the high-level software architecture recommended in the Feasibility study (defined in [1]), which in this report is being further detailed into a software specification. The architecture is based on previous work by the IETF as described in [2] and also taking into account variations across Europe in terms NRA jurisdictions, NRA remit and the presence of exiting NRA measurement systems.

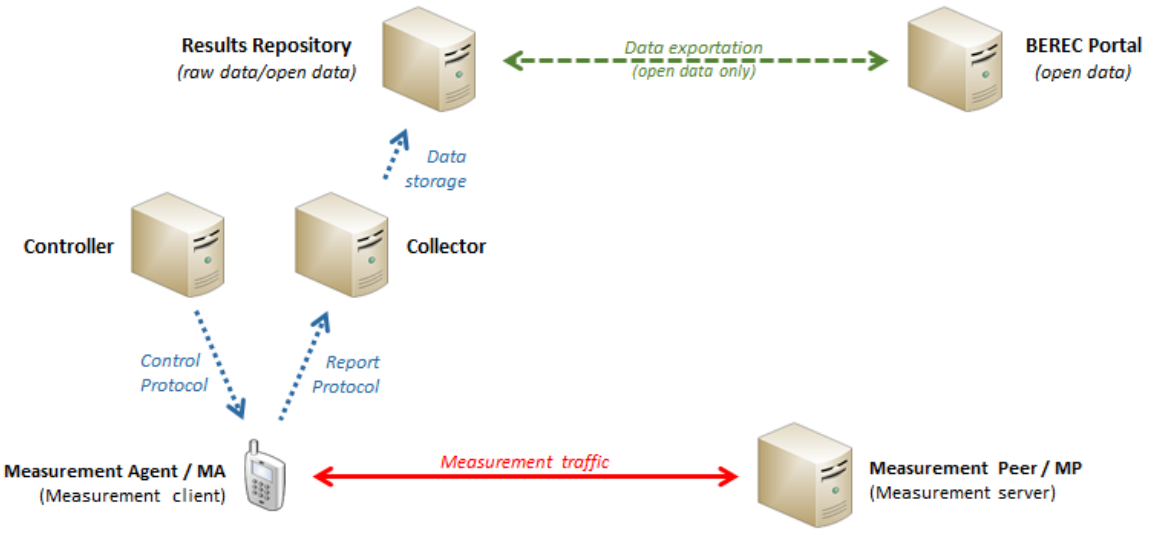

Figure 1: System architecture overview

The net neutrality measurement tool is specified to support harmonised measurement metrics and methodologies in a federated platform for measurements of IAS quality. It also provides a basis for further researching the area of net neutrality supervision, in a cost-efficient manner over the long term.

The report covers both technical and non-technical aspects; and all relevant aspects regarding usage of the net neutrality measurement tool, such as security, data protection and system governance.

[1] QoS, Quality of Service
[2] BEREC, Body of European Regulators for Electronic Communications, established by [7]
[3] NRA, National Regulatory Authority

NRAs that **don't have** a measurement system in place could use the software as a basis for a national measurement system. NRAs that **already have** a national measurement system could choose to apply selected metrics from the software, e.g. application-specific measurements which are not yet covered by its national system. This concept allows NRAs to re-use the design and software in its entirety or parts of it, and in order to minimize CAPEX[4] and OPEX[5] and provide interconnection between national instances of the tool.

This concept furthermore allows NRAs to retain full control over their national systems, especially regarding privacy and integrity. At the same time this approach allows for cooperation and harmonization without significant effects on existing systems. The deployment at national level is voluntary, so that NRAs already operating their own system can use the Tool in addition to their existing one.

In the long term, the BEREC tool could be a platform enabling NRAs to share knowledge, experience and expertise, including providing a basis for further piloting and researching the area of measuring quality of internet access services.

[4] CAPEX, capital expenditure (investment costs)
[5] OPEX, operating expenditure (cost of operation)

1. Introduction

This report provides the specifications of a reference measurement tool for the monitoring of Internet Access Services (IAS). Such a tool was recommended in the Net Neutrality Quality of Service (QoS) Feasibility Study that was adopted by the Board of Regulators in December 2015 [1]. The software implementation of the measurement tool will be available from BEREC as an opt-in solution, whereby individual NRAs can participate on a voluntary basis.

BEREC's Net Neutrality Regulatory Assessment Methodology provides methods for IAS related measurements and also serves as a recommendation for NRAs [2]. The methods described in [2] will underpin the software implementation of the measurement tool.

1.1 Objective

The objective of the measurement tool is to provide a reference system for monitoring the QoS aspects of IAS, such as speed and delay, as well as aspects of traffic management such as the blocking and throttling of Internet-based applications. It will be implementing the methods described in BEREC's Net Neutrality Regulatory Assessment Methodology [2].

A specific objective that is fulfilled by the implementation of the software tool and its reference system is increased levels of harmonization of NN-related IAS measurement metrics and methodology.

1.2 Benefits and challenges

The benefits of developing such a net neutrality measurement tool include the following[6]:

- It would enhance credibility in QoS measurements due to broad deployment and adoption amongst several regulators, as well as a large user base.
- It would enable convergence of measurement methodology, using the same measurement tools and allowing the statistical analysis of a larger data set.
- It is likely to provide an increased set of measurements and particularly cross-border measurements thus reflecting more real Internet connectivity across Europe. This would be at small initial cost, if any, and whose return-on-investment increases as more NRAs decide to adopt the measurement tool.
- It would reduce individual NRAs' costs relating to future development of national measurement tools, especially regarding application-specific and Net Neutrality related measurements.
- It would further facilitate collaborative regulatory partnership; sharing of knowledge, experience and expertise, including providing a forum for further piloting and researching the area.

Challenges include the following:

[6] Some of these benefits have already been identified previously in [1].

- A long-term commitment by the NRAs is likely to be needed in support of the multi-NRA functionality. This could be perceived by NRAs as additional "cost of cooperation" which may deter NRAs from adoption.
- Implementation of the reference measurement system could take longer than expected thus delaying adoption by NRAs.
- Low NRAs adoption of the system in the short term may lead to weakened levels of harmonisation.

1.3 Considerations regarding existing measurement systems

In developing the specifications for the practical implementation of the measurement tool, BEREC NN EWG took into consideration the following set of scenarios:

- **NRAs that don't have** a measurement system in place and they are currently aspiring to establish such national system.
- **NRAs that already have** a national measurement system.
- **The long-term aspirations** for enabling NRAs to share knowledge, experience and expertise, as well as establishing a platform for further researching the area of IAS measurements.

To best serve the above, BEREC NN EWG adopted two key notions: software modularity and adoption on an opt-in basis. Together, these two furnish the necessary flexibility needed by NRAs to cover the above scenarios and in the following ways:

Software modularity: Here, NRAs that already have a national measurement system can choose *which* modules/functions to adopt from the overall software implementation (e.g. a module that implements the measurement of a given metric or a particular system function), that are not covered by their current national system. Also, those NRAs can choose *when* to make that adoption. The timing for adoption would be chosen to best fit the NRA needs and system maintenance cycle. This helps such NRAs in different ways subject to the decision made by the NRAs. That is, the implementation of the software tool

1) Could play a supplementary role to an existing system by the adoption of the modules that an NRA needs integrated into their existing system, such as detection of traffic management practices.
2) Could set a roadmap for adoption over time and in an incremental fashion. This could be part of a long-term system engineering cycle[7] upon which measurement systems are normally maintained.

Clearly, software modularity allows the protection of the return on investment from current operational systems whilst maximising the opportunity to realise the benefits listed in section 1.2.

Adoption of system on an opt-in basis: This allows the NRAs that don't have a national measurement system to make full use of the software implementation as the basis for their

[7] Such cycle includes requirements, development, deployment, operation, maintenance and decommissioning.

aspirations for a national measurement system. Alternatively, the adoption here may be in an incremental fashion, where initially key system functions and basic metrics are adopted with other modules being added as time evolves.

Knowledge sharing and research platform: The software implementation of the tool together with the practical reference system will strengthen the level of harmonisation in Internet measurements amongst the NRAs. In addition to the commonality of measurement metrics and methods, it will also establish a common nomenclature for practical measurements systems, which will help increasing the efficiency of future collaboration amongst the NRAs in the area of IAS related measurement.

1.4 Scope

The scope of the software implementation revolves around the development of the required open-source software combined with a recommended hardware-based installation, together with the support needed for the installation and operations of a reference version of the tool within the BEREC domain.

What is *not* in scope is the tailoring of the measurement tool for dedicated deployment at NRAs (e.g. language translation), as well as detailed hardware specifications that are required for deployment.

The open-source software development consists of:

- Software applications for the measurement clients: mobile apps (Android, Apple-iOS) and (fixed) web browser client.
- Software for the different network servers of the system:
    - Measurement server,
    - Controller,
    - Collector, and
    - Results Repository.
- Software for post-processing of measurement data in the BEREC portal.
- Supporting documentations (user and developer manuals).

The hardware and operations of the reference system consists of:

- Hardware for the different network servers of the system:
    - Measurement server,
    - Controller,
    - Collector, and
    - Results Repository.
- Other supporting documentation including
    - Configuration of the reference system.
    - Hosting of the reference system.
    - Terms and conditions.

1.5 Outline of the report

The outline of this report is as follows.

- Chapter 2 provides a high-level overview of the measurement tool.
- Chapter 3 specifies the different measurement tasks covered by the tool.
- Chapter 4 deals with the measurement system architecture.
- More detailed information about the various aspects is contained in several annexes.

2. Tool overview and system concept

As described above, this document specifies a Tool which regulators can use either as a supplement to existing national measurements systems, or standalone in case no national measurement system exists.

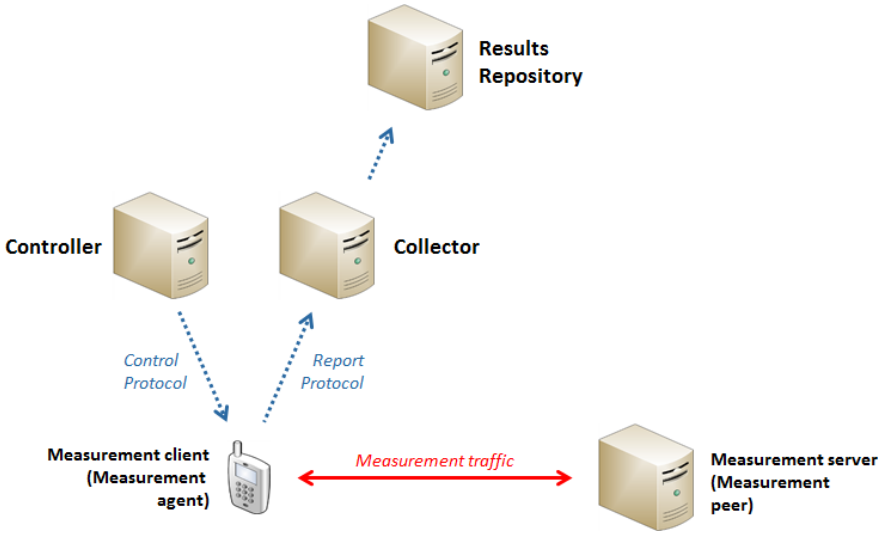

Figure 2. Tool configuration of a single NRA

Regulators can participate on varying levels, from full participation to small-scale contributions with a shared measurement server and/or sharing of measurement results. Each national instance would be controlled by its NRA, while also contributing to a collaborative functionality among NRAs and possible future initiatives at the BEREC level. (Ref. Management summary of [3]) The tool supports a federated architecture which can interconnect autonomously running national instances of the Tool.

The Tool itself shall to be Open Source[8], thus any interested party can reuse parts of the software or the entire software with reduced costs[9]. The measurement results shared

[8] *Open Source software* makes the source code of the software publicly available and it can be - under certain conditions depending on the selected open source license (e.g. Apache License) - modified and enhanced by everyone (Open Source software based are for example Android smartphone operating system, Firefox, Thunderbird, Moodle, Apache web server). For more information see: http://opensource.org, http://www.fsf.org, http://www.gnu.org/philosophy/free-sw.en.html, http://opensource.org/osd, http://opensource.org/faq#free-software.

[9] Financial advantages of Open Source software: License costs do not arise, thus the NRA does not have to pay for the basic-software, but only for services and support (e.g. adapting the software, maintenance). In addition, there is a bigger scope for negotiation towards companies. Open Source software also ensures that the source code is permanently available. This is - especially for long-term projects - rather important.

between NRAs shall be Open Data[10]. Also the measurement results made available by the portal shall be Open Data. (The portal and other network elements used by the Tool are further elaborated later in the document.)

One main characteristic of the Tool is that it is decentralised and scalable where multiple NRAs collaborate on an optional basis. The overall architecture will be composed of NRAs running their own software configurations which interconnect to an overall collaborative architecture. This implies that the software can extend its coverage over time with deployment on more measurement clients and servers, where NRAs can start deploying the software at different points in time when suitable for each NRA.

With such architecture, quality measurements can be performed between measurement agents in different countries, coordinated measurement campaigns can be conducted across Europe, and measurement results can be accumulated to perform comprehensive data analysis. Each NRA's software configuration is autonomously functioning as a stand-alone tool for national measurements, while also contributing to cross-border measurements emulating end users' ordinary way of using their Internet access service.

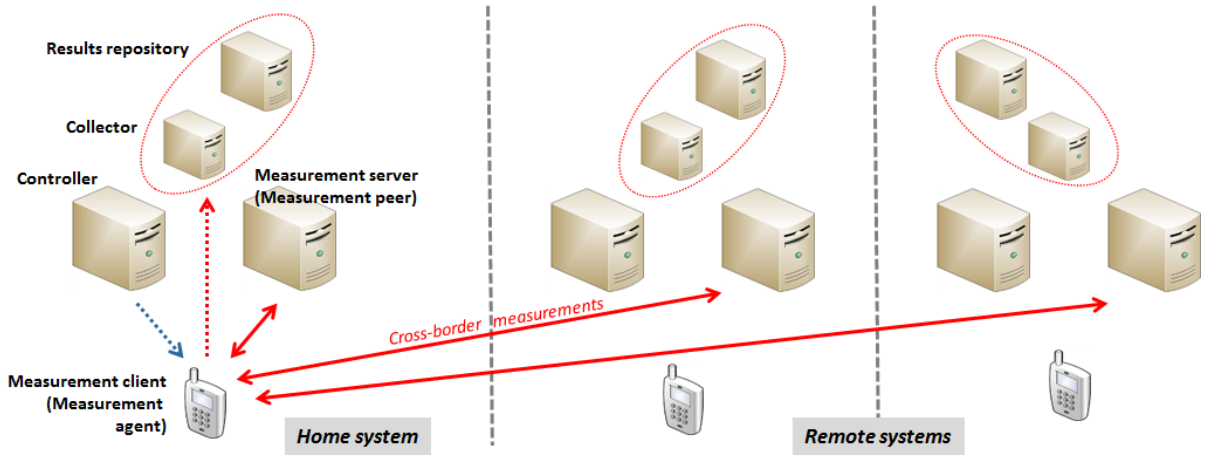

Figure 3. Collaborative architecture in a multi-NRA configuration

The remainder of the report provides technical information about components, architecture, interfaces, functionalities security aspects and other legal and organizational aspect in order to implement the Tool.

[10] Data that is collected when measuring IAS quality is referred to as Raw Data. Such raw data *"…has not been subjected to processing or any other manipulation…"* (http://en.wikipedia.org/wiki/Raw_data). Raw data can only be processed, as defined in Art 4(2) of the General Data Protection Regulation, by whomever, even the provider of the system if this is in compliance with the privacy policy of the respective Tool.
Open Data is data that is made publicly available. *Personal data* (including special categories of personal data, such as racial, ethnic, political, religious etc data), as defined in the General Data Protection Regulation, is never Open Data.
Thus it needs to be clearly distinguished between all the data that a measurement system needs and acquires from the individual user of the system (= raw data) and data that is made public (Open Data).

3. Functional description

The Tool shall support different measurement tasks (tests). It shall allow for measurements of “IAS as a whole” as well as detection of traffic management practices that impact individual applications running over IAS. The system might be reviewed and possibly updated after a period of time.

3.1 Measurement functions to be included

The measurement tasks described in the Net Neutrality Regulatory Assessment Methodology will be conducted by one or more of the components that together make up the architecture. Regarding measurement tasks and their output, these are defined below as *functions*, being provided by software modules as explained in *Chapter 1 Introduction*.

3.1.1 IAS quality measurement functions

A prerequisite for the Tool, in order to provide an NRA with means to supervise and monitor IAS quality, is for it to support the following mandatory functions which shall be made available through dedicated software modules:

- Speed measurements (downlink and uplink)
- Delay measurements

Additional functions:

- Delay variation measurements
- Packet loss measurements (for downlink and uplink)
- Availability of connectivity

In line with chapter 2, the following nodes are needed in order to monitor IAS quality:

- Measurement client/agent (mobile app as well as web browser client)
- Measurement server/peer
- Controller
- Collector
- Results Repository

3.1.2 Application-specific measurement functions

In addition to the IAS quality measurement functions, it is required to provide functions that enable dedicated review on how specific applications, i.e. the data flows they generate, are treated by the serving network(s). These mandatory functions are required for the Tool:

- Port blocking:
    - Is traffic to or from specific TCP ports blocked? Such tests can be used to uncover if a specific application relying on TCP as transport protocol, will work or not.
    - Is traffic to or from specific UDP ports blocked? Such tests can be used to uncover if a specific application relying on UDP as transport protocol, will work or not.

In addition, BEREC foresees that a set of *additional* application-specific measurement functions will be made available by implementing corresponding software modules:

- DNS: manipulation of specific DNS-requests, performed by the underlying network
- Proxy: detect whether there are any intermediaries along the network path that in one way or another modifies a request
- Web: browsing performance
- Audio/Video: detect whether treatment of audio/video streaming might affect the performance as perceived by the end-user
- VoIP: detect how traffic to or from such applications are treated
- Peer to peer: are such type of communications blocked or are they being exposed to any traffic management

To support these application-specific measurement functions, the same system nodes as mentioned above regarding IAS quality measurements are needed.

3.2 Options for NRAs to employ selected functions

Different options exist for NRAs that already have a national measurement system in place, to expand the current measurement capabilities. In general terms these options are:

1. Keep their existing system and run the new functions through separate user interfaces like an alternative app or web page
2. Integrate the selected functionality from the Tool into the current national measurement system and thus keep existing user interface
3. Let the developed Tool replace any current national measurement system, when time comes to make new investments due to maintenance etc.

It will be up to the NRA to evaluate and decide on which option to select. Important factors to consider are life time cycle of existing measurement system, uptake of national system among the users as well as any national regulations.

Common for all three options, but especially for option 1 and 2, are an evaluation of the following:

- User interface: resources needed to translate measurement functions and associated text into national language(s), as well as design schemes and branding necessary to comply with NRA design profile
- Hardware and/or software environment: whether there is a need to increase number of servers, interconnection capacity towards the local internet exchange, increased capacity towards any transit providers, volume of software licenses
- Operations: to what extent adding new functionalities could influence on recourses needed to operate and maintain the service
- User terms and conditions: how added functionality might affect existing terms and condition that users already have agreed to. Examples are increased data usage for mobile apps and sharing of open data across borders

Integration of functions from the Tool into existing national measurement services (Option 2) will most likely trigger some software development, depending on existing implementation.

3.3 Options for NRAs that don’t have a measurement system

For NRA’s that don't have a measurement system in place, they can use the complete solution for their sole measurement system. The tool will contain the basic and advanced measurement functions that are specified above. Each NRA can use the modular architecture of the system to decide how to use and implement the tool. The options for implementing a tool without an existing measurement system are as follows:

1. Complete solution: deploy a comprehensive tool with basic and advanced functions for IAS quality measurements and detection of traffic management practices
2. Basic solution: deploy basic measurement functions only
3. Custom solution: deploy a complete solution enhanced with custom functions

A comprehensive manual to implementing the measurement tool on the level of an NRA will provide the steps for deploying the system including basic system core configuration, modules implementation, system functionality settings, and hardware requirements.

The Reference System will provide guidance regarding how to use, manage, maintain, and troubleshoot the measurement tool. NRA choosing to host their own measurement server in their country would typically do this in a national peering centre. The cost of hosting, operation and connectivity is the respective NRA’s responsibility.

3.4 Options for exchanging data between systems

For a smooth exchange of data using the “open data” interface, it's necessary that these data be clearly defined. Any system could implement and process these data based on a description of the format and structure of open data. Format specification of open data etc. can be found in Annex D “Data collection and storage”

Figure 4 illustrates data fetched from Collector and data transfer to the BEREC portal.

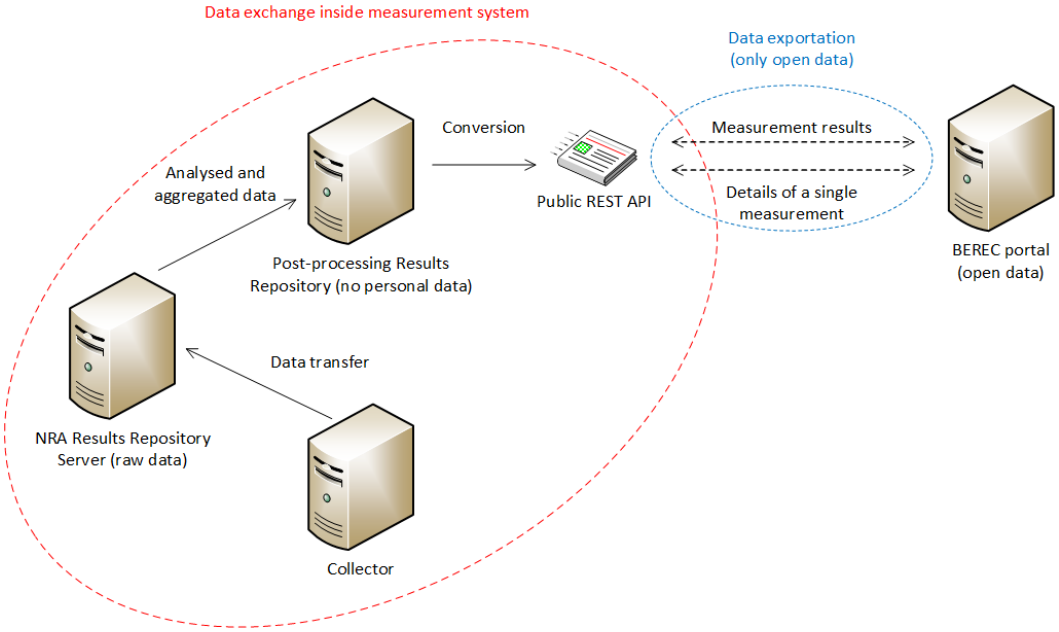

Figure 4. Actual data exchange

3.5 Post-processing functions to be included

Functionality for post-processing of measured data shall be developed. The following steps must be included in the software modules that perform post-processing:

Validation:
The Tool shall verify whether data is relevant or irrelevant. Removing irrelevant data from statistics should be done based on the specified list of grounds for exclusion (e.g. 2G too high download speed, 3G too high download speed, false location data, unreasonable latency values and so on).

Anonymization:
Presentation of data must comply with any privacy policy accepted by the users of the Tool, ref. Annex E “Privacy Issues”.

Conversion:
All presented parameters and their associated values must adhere to a common set of formatting rules, ref, also to annex D.3.

Presentation:
The measurement data in the Repository will then be statistically analyzed and presented in reports and on maps, as described in the next section. Data can be presented by a Presenter of the NRA, and/or exported to the BEREC Portal.

3.6 Presentation functions to be included

Functionality for presentation of measured data shall be developed. The following functions must be included in the software modules that perform displaying of results:

The user interface of the Measurement Agent should easily be extendable to multiple languages. During measurements the progress should be displayed, and the results should be presented clear and comprehensible way when the measurement is finished. End users should also be able to access their own previous measurement results.

Presenters, including the BEREC Portal, must contain an application for NRAs creating reports on a regular basis (e.g. annual reports) and presenting statistics including a map overlay with measurement results collected and stored in the repository. Parts of this functionality could also be made available to end users.

Statistical measurement data (not containing personal data) should be published as interactive maps with various filtering functions, such as selected metrics, access technology and time window. Maps provide an overview on the collected results and can be used by end users as an indication of what kind of quality can be expected within their vicinity.

Further details are available in Annex C “Presentation of results”.

4. System architecture

4.1 Introduction

The Feasibility study of quality monitoring in the context of net neutrality assumes that a strictly centralised architecture would not be suitable, since it would be less flexible regarding the national operation of measurements, and could also be less resilient and possibly introduce single-points-of-failure. On the other hand, it is also clear that running decentralised software that can be used by several NRAs is challenging, particularly regarding system governance.

It is clearly preferential that a *standardised architecture* is used. The study recommends building on the work of IETF's LMAP[11] working group[12] and expanding this work with additional functionality as needed. This report therefore reuses terminology and concepts, to the degree practical and suitable, from RFC 7594.

The following text elaborates the system architecture. This description is not necessary exhaustive, and components/nodes may be grouped differently depending on what is seen as the most effective implementation strategy.

In addition to the description provided in this chapter, details about each of the architectural elements are available in annex A "System Nodes". Furthermore, how the system architecture should be deployed on physical network nodes is elaborated in annex B "Description of the hardware".

4.2 Basic single NRA configuration

In Figure 5, the components of the architecture are named according to the standardised LMAP architecture. The Measurement agent (MA) performs measurement tasks. MAs can be of different types; software-based or hardware-based, fixed or mobile nodes. The Controller manages the MAs through use of a dedicated *control protocol*. The Collector receives measurement results provided by MAs through the use of a dedicated *report protocol*. The Collector then stores the results in a Results Repository where data later can be fetched for statistical analysis. Both the control protocol and the report protocol shall be based on existing protocol standards (ref. RFC 7594), and possibly further extending such protocols. Both protocols should provide high levels of security and integrity.

[11] LMAP, Large-Scale Measurement of Broadband Performance [6]
[12] See http://datatracker.ietf.org/wg/lmap/

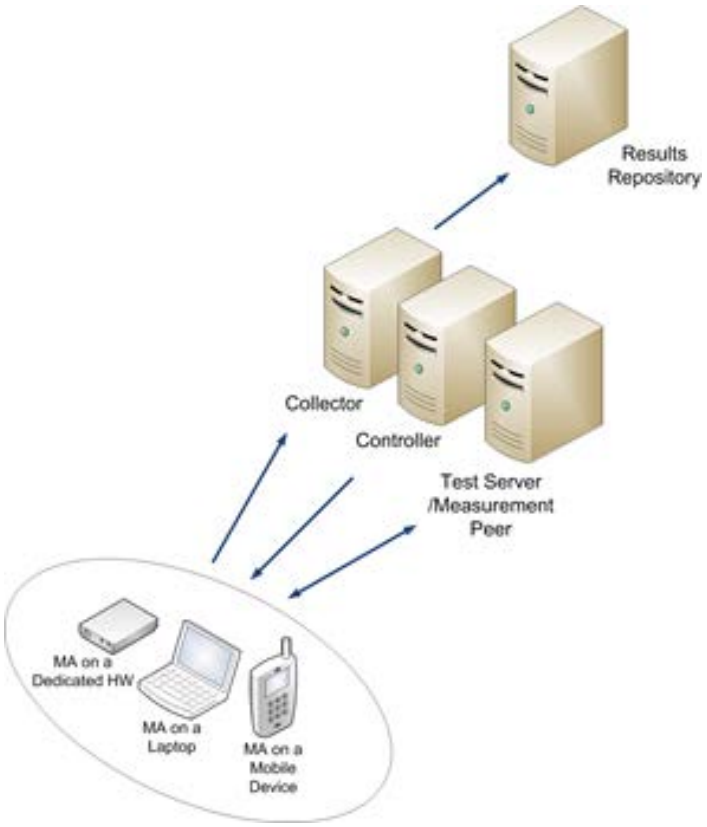

Figure 5. Components in a basic configuration

When measurement tasks are running, an MA typically communicates with other entities (e.g. sending measurement traffic). Where an MA communicates with another entity (e.g. a measurement server) which is also instructed by the Controller, the other entity also constitutes an MA. Where an entity is involved which is not interfaced with the Controller, it is called a Measurement Peer (MP). An example of the latter could be an ordinary web server.

4.3 Main functionalities

First of all, the measurement system must be able to support the collaborative/multilateral quality measurement functionality as described in the different measurement tasks taking into account the Net Neutrality Regulatory Assessment Methodology [2][13].

Secondly, the system should produce Net neutrality QoS measurement reports with accuracy, comparability, trustworthiness, openness and future-proofness. Software design should ensure flexibility, extensibility, scalability and adaptability applying cost-effectiveness as a general rule-of-thumb to all phases of the measurement software lifecycle, including development, deployment and operation.

Finally within the general system requirements, the measurement system should present high-performance, robustness, high availability and high resilience.

[13] The following paragraphs are taken from the Annex of the Feasibility Report [5].

The decentralised federated system architecture would need to balance between the autonomous functioning of individual NRAs' software configurations and the central coordination needed to achieve the overall functionality, where cross-border measurements is a typical example.

4.4 Federated multi-NRA configuration

A federated multi-NRA configuration would allow for coordination between the NRAs, e.g. sharing configuring information on shared measurement servers. This could be performed either through manual administrative tasks or using some configuration server handling this more or less automatically. Manual administration seems most likely for an early installation, while automatic configuration may be needed as the software grows in functionality and coverage. In the scenario below, the blue dotted arrows illustrate the flow of configuration information.

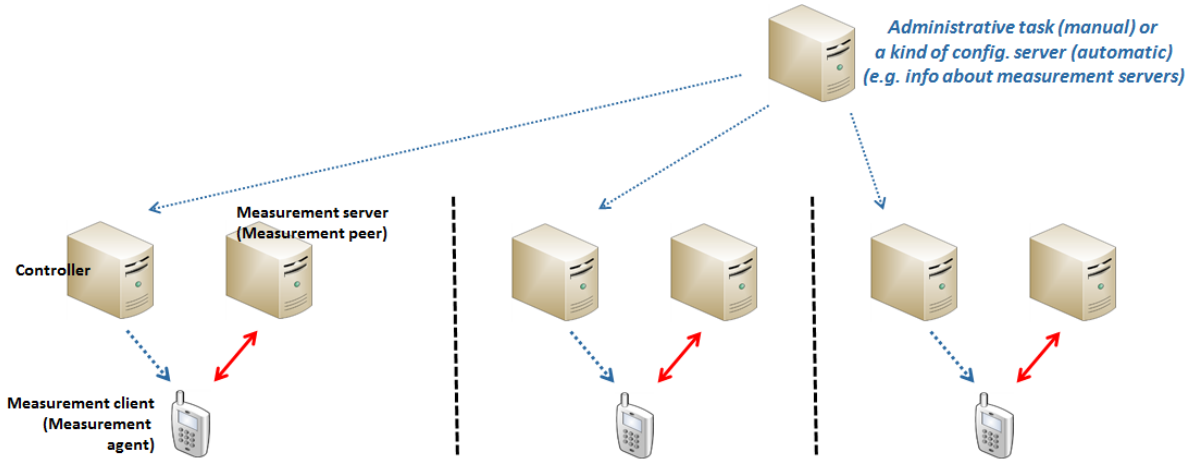

Figure 6. Components in a federated multi-NRA configuration

The coordination function is closely linked with the governance of the overall system.

IAS quality measurements need to reflect the transnational topology and usage of the Internet, which makes it relevant to measure performance across borders, and check the ability to access content from different parts of Europe when the end user is at home, in his domestic network, and when connecting from a visited network when roaming.

Regarding future-proofness - i.e. flexibility, extensibility, scalability and adaptability - NRAs should be able to opt-in to the software through a gradual transition period and adapt the quality measurement process based on their needs.

Software can extend its coverage over time with deployment on more measurement clients and servers.

4.5 Collaborative measurement functionality

Different NRA software configurations can be interconnected to measure cross-border communications, thereby emulating end users' ordinary ways of using their Internet access service. When performing cross-border measurements, test traffic is sent between a

measurement agent in an NRA's software configuration (home system) and a measurement peer in another NRA's software configuration (remote system).

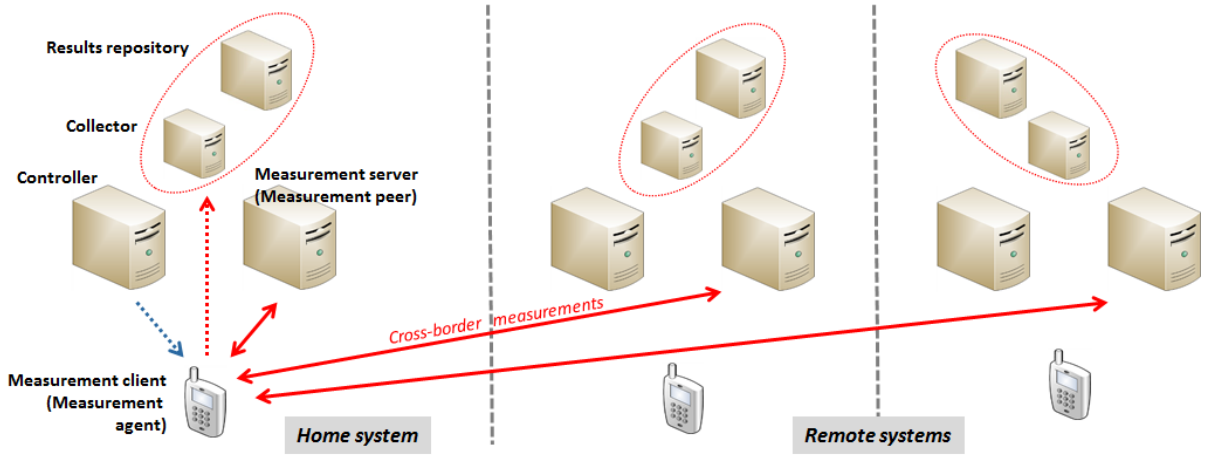

Figure 7. Proposed collaborative architecture

The ownership of the measurement results resides in the home system, which can thereby manage confidentiality and similar aspects. Measurement results from each NRA are stored in the Results repository. From the different NRAs' Results repositories only open data may be exchanged. Open Data can thereby be collected for centralised analysis of shared open data, or individual external NRAs can import Open Data from other NRAs for dedicated comparison of results.[14]

In order to make the participating NRAs' software configurations collaborate to constitute an overall functionality, some coordination of common software parameters is needed. The decentralised federated architecture would need to balance between the autonomous functioning of individual NRAs' software configurations and the central coordination needed to achieve the overall functionality.

Additional servers increased capacity should allow for higher resilience. In case a specific server is overloaded (e.g. peak local demand) or not available (e.g. maintenance or outage) alternative servers can be selected.

The load on the server can always be controlled by the home NRA, thus it is up to each NRA to decide what capacity is shared for cross-border measurements and what capacity is reserved for national use of the proposed Tool.

[14] Privacy aspects and the relationship between raw data and open data are specified in the annex.

References

[1] BoR (15) 208, "Feasibility study of quality monitoring in the context of net neutrality," 11 30 2015. [Online]. Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5576-feasibility-study-of-quality-monitoring-in-the-context-of-net-neutrality.

[2] BoR (17) XXX, "Net Neutrality Regulatory Assessment Methodology," 2017. [Online]. .

[3] BoR (14) 117, "Monitoring quality of Internet access services in the context of net neutrality BEREC report," 25 9 2014. [Online]. Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/4602-monitoring-quality-of-internet-access-services-in-the-context-of-net-neutrality-berec-report.

[4] Eardley, P., Morton, A., Bagnulo, M., Burbridge, T., Aitken, P., and A. Akhter, "A Framework for Large-Scale Measurement of Broadband Performance (LMAP)". *RFC 7594.*

[5] "Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (Text with EEA relevance)," [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0001:0010:EN:PDF.

[6] "Regulation (EU) 2015/2120 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (TSM Regulation)," [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120.

[7] "Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)," [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0022:20091219:EN:PDF.

[8] "Directive 95/46/EC (Data Protection Directive)," [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:PDF.

[9] "Creative Commons licenses," [Online]. Available: https://creativecommons.org.

Annex
A. System Nodes

The description of the system nodes is based on IETF's LMAP architecture, ref. RFC 7594.

A.1 Measurement Agent

The Measurement agent performs measurement tasks. It is foreseen that the Measurement Agent should generate (and receive) traffic specially created for the purpose and measure some metric associated with its transfer. Measurement agent should be able to connect to wired and/or wireless networks and have the possibility to run a variety of measurement tasks depending on the instructions given.

The Measurement Agent is responsible for orchestrating the measurement. This will have to be done in tandem with functionality in the Measurement Peer. It is the Measurement Agent that will collect measurement results and associated metadata before sending it to the Collector for final processing and storage. The measurement will have to support both IPv4 and IPv6, and use TCP as transport protocol. The Measurement Agent should also have measurement viewing capabilities but this would depend on the (physical) measurement platform the MA runs on. It shall display detailed information on own measurements and allow browsing in public available measurement results.

A single Measurement Agent should be instructed by a single Controller.

A.2 Measurement Peer

Since an important characteristic of an IAS service is its connectivity to the entire Internet, NRAs need to scrutinize the quality of this connectivity. Ideally, Measurement Peers are fully distributed over the Internet, but for practical reasons there will be a limited number of such end points. This implies that end users need to carefully evaluate the representativeness of the cross-border measurement results obtained.

The Measurement Peer's main responsibility should be to assist multiple MAs in conducting their measurements. In order to perform two-way measurements the Measurement Peer must replicate and match the measurement functionality of the MA and must be able to send, receive and analyse measurement traffic. The Measurement Peer should also have the necessary functionality to evaluate its own system load and report this to its upstream Controller if a configurable limit has been reached. Through this, the Measurement Peer will assist the Controller in performing its load balancing.

System load should consist of a defined set of key performance indicators (KPIs). Each KPI should be configurable i.e. the system administrator should be able to define a threshold that will indicate whether the KPI in question is in green or red state. A Measurement Peer that has one or more KPIs in the red area should be treated with caution by its Controller.

A.3 Controller

The Controller should manage Measurement Agents (MA) through a control protocol. The protocol is used for communicating set of instructions to the MAs. These instructions constitute measurement tasks including, but not necessarily limited to, what kind of metrics that should be measured and the time when the tasks are to be performed.

Important tasks for the Controller will be to maintain admission control, load balancing of the measurement Peers and measurement configuration functionality for the implementation of the system. The Controller will be the first point of contact for the MAs when conducting measurements.

There could be more than one Controller in the Tool. For example, different MAs could have different Controllers, or different locations could have different Controllers.

A.4 Collector

The Collector receives reports from MAs with the measurement results from its measurement tasks, using the report protocol. It then provides the results to a repository.

The Collector should receive the measurement results and metadata from the MAs. It is foreseen that the Collector must adopt logic in order to validate and verify integrity of measurement results received from the MAs. Furthermore, the Collector should be able to augment the results with information from third party data-sources including adding location data based on Geo-IP data and to verify ISP by IP address blocks.

A.5 Results Repository

A Results Repository records all measurement results in an equivalent form so that they can be subsequently accessed for data analysis.
Content will depend on measurement configuration and version. The Results Repository should be divided in two parts; one for raw data and one for open data intended shared with the public and/or other parties.
The Results Repository should be able to support different interfaces for exchanging information either with other servers or as channels dedicated to human/end user interactions. These APIs[15] might be either closed or open depending on the role they are intended to have. Any implementation of such APIs should also support different degree of security depending on the information provided through them, or who has access to use them.

It might be necessary with access control based on blacklists in order to control load and machine resources for the Results Repository.

[15] API, application programming interface

A.6 Presenter

The Presenter should have the possibility to present open data and/or aggregated data to the general public. The results should be presented to end users by collecting them from the results repository and make them available in one or several ways. One such way must be through the use of a web server that lets end users interact with the Presenter through web browsers. The BEREC Portal is an example of a Presenter.

The Presenter should have the possibility to run one or more APIs. One of those APIs should be open to the general public and let them collect Open Data (measurement results) in a structured and standardized way.

It is foreseen that the Presenter shall interact with the Results Repository. The communication between these two nodes should be sufficiently protected in order to ensure integrity of the transmitted data. The interaction should be based on the principles described in the text on Results Repository.

B. Description of the hardware

Hardware requirements can be subdivided into three major components:

- Measurement agent,
- Measurement peers (measurement server),
- General servers such as database, processing and presentation.

B.1 Measurement agent

This chapter describes which (physical) platforms the measurement agent (MA) must be able to run on. The overall system concept decides how an MA should be implemented. The architecture described in the previous chapters outlines that an MA will take the role as “client” in a typical client-server communication set-up. It is not foreseen that peer-to-peer like implementations shall be considered.

The agent’s location depends on the scope of the measurement. There are two basic approaches: measurement of the provider's IAS performance, and measurement of the end user’s perceived IAS performance. Measurement results received from the latter approach do not allow for identifying whether the end user environment (e.g. Wi-Fi home network) or provider network is the source of quality degradation.

B.2 Mobile apps

The Tool should enable end users to perform measurements through agents (hereafter: apps) running on end user owned smartphones and tablets. Measurements performed through the apps shall be visible to the public via the web pages as described elsewhere in this document. Measurement results shall also be visible to the end user in the apps themselves.

Apps for the most prolific operating systems are required in order to cover the majority of smartphones and tablets. These are iOS from Apple, and Android from Google.

Windows Mobile has a low percentage proliferation and will not be considered at this stage. The distribution is listed in Table 3 as confirmed by a Gartner study from May 2016; please see http://www.gartner.com/newsroom/id/3323017 for more information.

Operating System	**1Q16 Units**	**1Q16 Market Share (%)**	**1Q15 Units**	**1Q15 Market Share (%)**
Android	293,771.2	84.1	264,941.9	78.8
iOS	51,629.5	14.8	60,177.2	17.9
Windows	2,399.7	0.7	8,270.8	2.5
Blackberry	659.9	0.2	1,325.4	0.4
Others	791.1	0.2	1,582.5	0.5
Total	349,251.4	100.0	336,297.8	100.0

Table 1. Worldwide Smartphone Sales to End Users by Vendor in 1Q16 (Thousands of Units)

It is foreseen that apps will most likely be required since operating system specific metrics must be read from the handsets.

As the smartphone market shows sign of saturation both Google and Apple have expanded their platforms into wearables, connected home devices, in-car entertainment and TVs. Such devices could in principle provide interesting platforms for either tailored or standardized MAs, provided that they process adequate processing power, memory and connectivity. They are however out of scope for this report due to expected development costs and market distribution compared to what is achievable for traditional smartphones.

B.3 Browsers

Ideally a browser based Measurement Agent should be independent from the type of browser used. It is however a fact that stability, plugin support and compatibility with the underlying hardware environment as well as operating system plays a role when it comes to performance and suitability.

To list those may not be straightforward, since different sources give different listings. This is typically due to the fact that different sites attract different audiences: Some web sites attract developers using professional hardware, while other sites attract hobbyists using older computers.

As a general rule, the Measurement agent should at least be able to run and provide persistent results in any browser with a market share of more than a specific percentage[16].

B.4 Measurement agent's hardware environments

Hardware agents are out of scope for the Tool. But even when the Tool does not provide any hardware agents, NRAs might consider re-using the software for hardware based solutions other than those using mobile phones, tablets or web browsers.

B.4.1 Embedded home-network environments

Automated measurements which are carefully scheduled provide a good basis for reliable measurements, and this method is well suited for measurement campaigns conducted by NRAs. Such measurements will traditionally run in dedicated hardware environments either located in the end user home network (connected directly to the home gateway) or the software client might be embedded in the home gateway itself. Examples of the former could be end user devices like set-top boxes, Smart-TVs and gaming consoles while for the latter category one could imagine that the MA was installed by the vendor or added by the ISP through the use of management protocols like TR-069.

[16] Statistics market shares of web browser can be found here:
https://www.w3counter.com/globalstats.php?year=2017&month=3

While running MAs in such kind of hardware environments have several merits, such solution is out of scope for this report. That does not mean that interested parties should not consider exploring such options, provided they can muster the necessary resources.

B.4.2 Personal Computers

PCs and Macs are also viable hardware platforms for hosting MAs. Such environments represent strong computational resources and have in general no problems with running complex measurement operations. Several measurement systems already offer MAs in the shape of dedicated software that can be downloaded and installed. Examples are Bredbandskollen (TPTEST) and Neubot.

From a technical point of view there can be good arguments for developing this kind of agents. One can tailor functionality and performance to the specific hardware environment in question, meaning adapt to operating system and processor and at the same time avoid dependence from third party software like Flash and Java.

B.5 Measurement peers and general servers

It is imperative for the measurements that both the general public and the providers have trust in any published measurement results. This could mean adopting a level of transparency on how the Tool is implemented, also including when it comes to physical properties like memory and CPUs, use of operating system and virtualization. At the same time, such transparency should be in balance with security considerations and any need to keep critical details of network topology confidential.

It is expected that both the general public and stakeholders will be interested in how server components are implemented when it comes to network connectivity. This would be especially true regarding measurement servers due to their important connection with the measurement clients. Thus, NRAs must take the utmost care to make sure measurement servers have connectivity sufficient to avoid that measurement results are influenced by the available bandwidth.

B.5.1 Implementation of national measurement system

This section provides general advice for NRAs that considers implementing a national measurement system based on the proposed system architecture. The discussion is not meant to cover all details that might be relevant in such a process but rather raise points that should be considered in the planning and implementation stages.

B.5.1.1 Connection and visibility

Deploying a national measurement system available to end users is not only about physical connections and link capacity. It is also about making sure data to and from the system gets transmitted in the most efficient way possible and that this happens under conditions that are transparent to the NRA. The optimum way for ensuring this will be to host the measurement system in its own Autonomous System (AS) and thus be independent from other ISPs when regarding IP-addresses and routing policies. Should this not be possible and beyond available resources, the NRA should ensure high quality hosting providers and through contractual terms and revisions make sure their interests are taken care off.

B.5.1.2 Connectivity

A core requirement for a measurement system is that it offers good opportunities for ISPs to connect with it. This means offering public peering at established IXPs where there are good opportunities for domestic ISPs to be present. Peering agreements should be free of charge for the ISPs and should follow best practises regarding technical and administrative provisions. The NRA should also ensure that the measurement system has ample connection to at least one transit provider, so that traffic from smaller operators/ISPs and foreign measurement agents has the best possible connectivity.

The NRA should ensure that the hardware running the measurement server is connected as close to the IXP switch as possible. This means that the number of physical paths between the main IXP switch and the gateway serving the system should be kept at a minimum. This is applicable whether the implementation runs inside the network of a hosting provider or directly on hardware under control of the NRA itself, in a separate AS. The goal is to minimize latency added due to the communication paths.

B.5.1.3 Local resource management

Due to the nature of a public measurement tool, NRAs should be prepared for significant traffic loads towards the system from time to time. Such spikes are often beyond the control of the NRA and typically derive from the measurement tool being featured in popular online newspapers or television broadcasts. It is almost impossible to prepare for such sudden spikes and in most cases it would not be financially feasible to build and maintain an extra network and/or processing capacity, thus access to servers needs to be controlled

This leaves two options: The first is that the NRA scales the infrastructure (in cooperation with any hosting provider) to cope with average demand as seen over a defined time frame, and then let the system serve measurement requests until it simply overloads and fails. The second option is to establish and implement load balancing, application level scheduling and high availability routines. Such solutions can be a bit more costly but adds flexibility, a better chance for graceful failovers and should result in a better experience for the end users. The choice would be for each NRA to decide individually, based on the available resources.

B.5.1.4 Reference implementation

Based on the recommended system architecture and the preceding discussions, the reference implementation in the figure below is recommended. The implementation is building on connectivity to the Internet through an appropriate IXP where ISPs within the NRA’s jurisdiction physically connect (see [4]). A layer-3 router/switch acting as the gateway for the measurement system is needed to connect the system to the IXP. The router/switch will be responsible for the logical configurations which facilitate IP connectivity (BGP, DNS, etc.) between the NRA’s servers on one hand; and the Internet and ISPs on the other.

The NRA will also need to deploy hardware to run different servers described earlier in the document. These servers are: Measurement Peer, Collector, Controller, Repository and Presenter (portal).

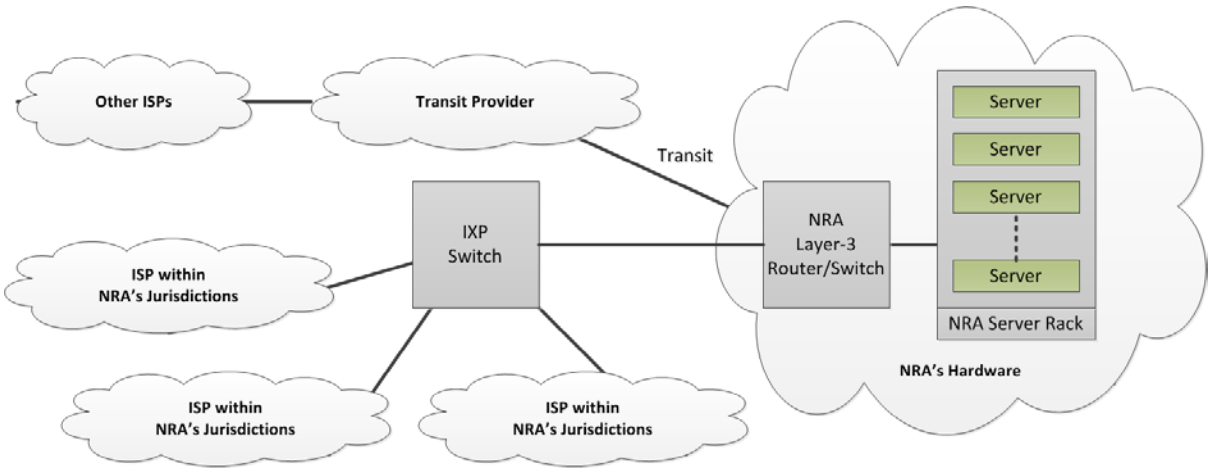

Figure 8. Reference implementation of a national measurement system

In principle, servers such as Controller and Collector might use virtual machines, in many cases low-cost "cloud-based" (i.e. hosted) solutions would be sufficient as long as computational performance is adequate. Due to security and privacy considerations the Tool shall only use dedicated physical hardware (see chapter "Infrastructure Security") but it is up to the individual NRA to decide whether to use virtualization or not.

C. Presentation of results

C.1 Design and usability of Measurement Agent

The use of the Tool should be user-friendly and intuitive. Thus, the format and the layout on the screen should be designed in a manner that the end user can easily understand.

The user interface (UI) of the Measurement Agent should be well presented on different screen sizes - smart telephones of varying sizes, tablets and desktops (up to 4k).

The application shall be configurable for multiple languages.

During the measurement task the measurement agent will show the progress both graphically and numerically.

After the measurement task has finished, the results will be presented in a clear and comprehensible way. The end user should not need to wait for the presentation of results.

C.2 Start/Display of current measurement results

This part will describe the initial interface the end user uses to start the measurement task.

The initial user interface should be as simple and user-friendly as possible, enabling end users to start the measurement tasks quickly (one click away from the result). Measurement tasks shall be initiated manually (e.g. “Start measurement” button).

Furthermore, it has to be ensured that the usage of the Tool (thus the start of the measurement task) is only technically possible after explicit consent to the privacy policy and terms of use by the end user and that the consent is logged for evidence reasons[17].

It is recommended to avoid forms/asking questions before running the measurement tasks.

The duration of the measurement tasks should be limited to avoid users quitting before the measurement task is completed.

During the measurement tasks, the display should inform the end user about the progress of the tasks, e.g. displaying intermediate results.

C.3 History of measurement results

This section describes the way end users can access their previous measurement results.

[17] Please see appendix E for more details on privacy issues.

Individually, end users should be able to access the previous measurement results (history of measurements). History of measurements can include information going beyond Open Data, because only the end user has access to the history.

C.4 Help/Documentation

This section describes the information/documentation provided to end users.

Apart from performing the measurement tasks and presenting the results, the Tool empowers end users.

- A user manual (e.g. FAQ [18]) should explain to end users the different metrics, their importance and how to interpret the results in the case of their individual access.
- This should also explain to end users what can influence their measurement results and performance of the applications (the equipment, the Wi-Fi, etc.), how they can try avoid error sources. Also legal information should be provided.
- Precise details on the how the Tool works should also be provided for particularly interested end uses/experts.
- Finally it is recommended that end users can contact the provider of the Tool (BEREC Office, individual NRA) via e-mail.

C.5 Data display/reporting to end users

Presenters, including the BEREC Portal, must contain an application for NRAs creating reports on a regular basis (e.g. annual reports) and presenting statistics including a map overlay with measurement results collected and stored in the repository. Parts of this functionality could also be made available to end users.

The Presenter should be able to generate reports with pre-defined structure about measurement results in PDF and the ability to export filtered and un-filtered tables to Excel. Data display elements (charts, graphs, tables) shall be dynamic with the options to resize the elements, sort by data, filter by data. Data display elements shall be interactive. On element selection detailed information about the element shall be displayed in a related field or table preferably in the same view. Graphs shall be able to display multiple data sets in the same graph. The end user shall be able to select which data sets to display on the graph.

The web page should include parameters for filtering as e.g. the app, the measurement results, the terminal type, the location etc. generating thus a filterable map. The code for the web page code should be Open Source as the other parts of the Tool.

The general public should be able to view limited functionality of the web frontend from a computer using any modern web browser. Modern means: current version of Mozilla Firefox, Google Chrome, MS Edge and Apple Safari.

[18] FAQ, frequently asked questions, a collection of common issues.

C.6 Mapping of measurement results

The Open Data measurement results can be published as an interactive map with various filtering functions. Measurement results are shown as coloured tiles representing the average quality for a specific area. Maps provide an overview on the collected results and can be used by end users as an indication of what kind of quality can be expected within their vicinity. There should be a topological layer and a satellite layer.

The map can be evaluated and filtered by several criteria, e.g.:

- Metric: e.g. Upload speed, download speed, signal strength, ping/latency, all other QoS parameters that will be measured (depending on measurement task)
- Only browser, mobile or Wi-Fi
- Statistics (percentiles)
- Internet Service Provider
- Time window (1 week, 1 month, 3 months, 6 month, one year, etc.)
- Access technology (mobile and fixed line are distinguished) (3G, LTE, etc. or DSL, cable, etc.)
- Map display with heat map, points or zip codes / areas.

Also for each measurement result it should be possible to view Open Data, like date, time, download speed, upload speed, ping, signal strength and access technology.

C.7 Reports/statistics

Any statistics shall be based on Open Data, e.g.

1. Recently performed measurement tasks (including wide range of filtering options)
2. Statistics by operators:
   (a) Metric: e.g. Upload speed, download speed, signal strength, ping/latency (depending on measurement task), all other QOS parameters that will be measured, number of measurement tasks
   (b) Filter
   (c) Measurement agent type (mobile, browser, …)
   (d) Access technology (mobile and fixed line are distinguished) (3G, LTE, etc. or DSL, cable, etc.)
   (e) Statistical optimization (80% percentile, median, 20% percentile)
   (f) Location accuracy (each, <2 km, <10km, …)
3. Statistics by mobile devices or browsers:
   (a) Device type (device e.g. “iPhone 5s”, “Galaxy S5”, etc. resp. Browser e.g. “Safari”, “Opera”, etc.)

D. Data collection and storage

D.1 Generic information model

Each measurement task has some “Meta-data” associated. The task is performed at a specific date/time, at a specific location, using a specific access network, measurement method etc. Some information is apparently relevant (like date/time), while other information (like air temperature) might seem less relevant.

Thus it needs to be decided what information is processed and shared as open data for each measurement task. The privacy policy and the terms of use need to be taken into account.

This chapter contains a description of Meta-data and indicates how it shall be processed.

1. Unique Identifier of the measurement task: For this purpose an UUID[19] version 4 according to RFC4122 can be used. Such an identifier is an (pseudo-)random 16 byte number which can be assumed to be unique.
2. Measurement task: The measurement task and the method applied for measuring shall be recorded. This information shall include the software version of relevant components.
3. Date/Time of measurement task: This information shall be stored in UTC[20] together with the time zone in which the measurement task was performed.
4. Location of the measurement task: The quality and availability of location information heavily depends on the specific client used. Smartphones/Tablets usually allow for GNSS[21] location when used outdoors or close to windows. When no GNSS signal is available Smartphones/Tablets use mobile radio signals and Wi-Fi signals to estimate the client’s location. If neither such a network location nor a GPS location is available the measurement might use the IP address to get a very rough estimate of location. Location information might include the following details:
   - Source of location information (e.g. GNSS, network, IP-address)
   - Latitude and Longitude of location
   - Date and time (in UTC) of location fix
   - Accuracy (on x-axis)
   - Accuracy (on z-axis)
   - Altitude
   - Speed
   - Heading
5. Information on the client used for the measurement task. This information shall include the software version of the client.
6. Information on the access network where the client was connected. When available mobile network codes shall be registered. If that information is not available, the IP address can be used to retrieve the AS (autonomous system number) of the client’s access network.

[19] UUID, universally unique identifier; A 128-bit number used to identify information
[20] UTC, Coordinated Universal Time, the primary standard time defined by ITU-R TF.460-6
[21] GNSS .. Global Navigation Satellite System

In addition, data collection will augment the measurement results with information from third party data-sources which could optionally include the addition of location data based on Geo-IP data, map physical location to country, city & municipality, town area/street, time/day/date, duration, etc.

D.2 Data storage and exportation

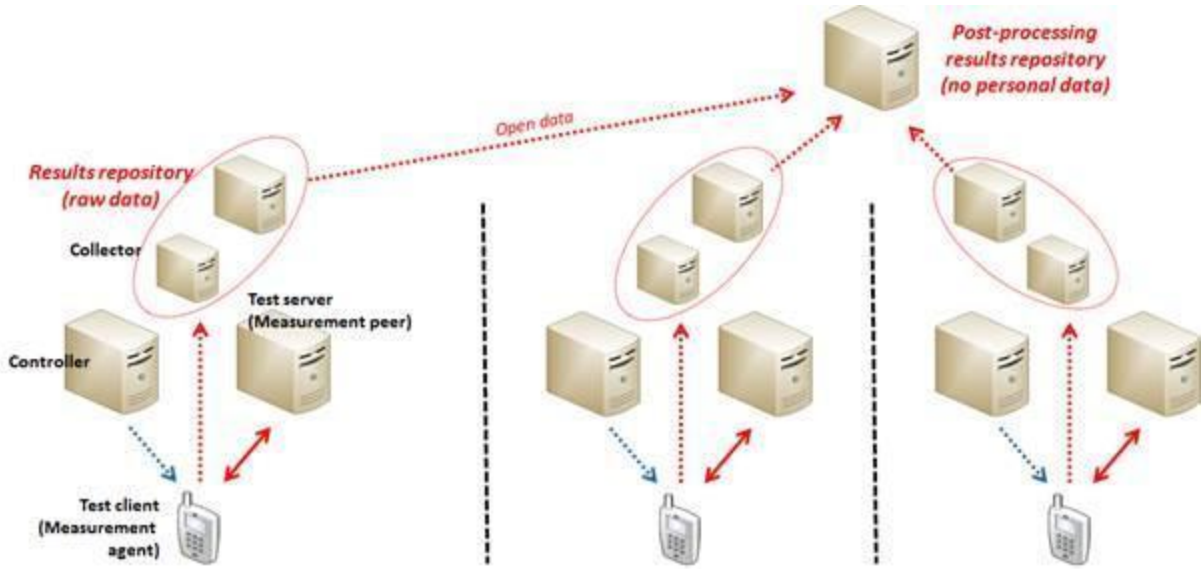

Figure 9. Data transfer from the Reference Systems (bottom) to the BEREC Portal (top)

The scenario given in Figure 9 illustrates NRA transferring measurement results from the Collector to the Results repository over an internal interface. Open Data is stored in the Results repository for statistical analysis. From the different NRAs' Results repositories only open data may be exchanged. The red dotted arrows illustrate the flow of measurement results.

Experience from existing tools shows that usage can vary widely, ranging from 10 to 1500 measurements per million inhabitants per day. The system shall be designed that the upper value can be handled by the architecture. It shall be evaluated what resources (e.g. amount of data) is needed during a measurement task and what amount of storage/capacity is needed to store the measurement results.

When results are made available via an Open Data interface, data can be collected for centralised post-processing of shared data, such as the BEREC Portal, or individual external NRAs can import data from other NRAs for analysis of results. A common subset of information and minimum requirements can be defined for the exchange of Open Data offered as JSON[22] (REST[23]) or XML[24]. CSV[25] would not be suitable for automatic data exchange.

[22] JSON, JavaScript Object Notation, a standard human readable data exchange format, see https://en.wikipedia.org/wiki/JSON
[23] REST, representational state transfer (a stateless web service), see https://en.wikipedia.org/wiki/Representational_state_transfer
[24] XML, extensible markup language, a data exchange format, see https://en.wikipedia.org/wiki/XML

The Tool shall make available Open Data using JSON. The BEREC portal shall support the automatic import of data in JSON format using the specific format defined for the Tool. The portal shall support import from different instances of the Tool.

NRAs decide what information to share as Open Data from their national system. In order to allow exchange of measurement results, mandatory and optional data fields need to be defined. Mandatory fields are those that are presented as Open Data. Typical examples of Open Data could be globally unique ID of the measurement task (so called UUID), ID of the measurement system, type and timestamp of measurement tasks etc.

Open Data shall be provided in line with the privacy policy. The data should be made available in a suitable format for Open Data using JSON.

The information model shall be aligned with the IETF/LMAP information model, ref. RFC 7594 describing the LMAP architecture and in particular RFC 8193 describing the LMAP information model.

Furthermore, the data format shall be compatible with the IETF/IPPM metric registry (currently draft-ietf-ippm-metric-registry-12 / draft-ietf-ippm-initial-registry-04).

D.3 REST interfaces

In order to provide measurement results to the BEREC portal, NRA Result Repository servers shall implement a public REST (Representational State Transfer) interface for exchanging open data. For this, two endpoints are defined.

D.3.1 Listing new measurement results

This endpoint shall be used to pull measurement results (as well as some basic information) from the individual NRAs. By default, the most recent results are returned. For providing pagination, a measurement task UUID is accepted as a parameter. If this is set, all returned results are older than this parameter.

Request: GET <nra_rest_interface>/task
Parameters:
task_uuid: Optional, uuid of a measurement task, then all returned measurement results shall be older than this measurement task.

Response:
tasks: Array, containing entries of type MeasurementTaskData, at most n entries, whereas n is defined by the individual NRAs.

Structure of type MeasurementTask Data

- *task_uuid*: String. Unique identifier of a single measurement task

[25] CSV, comma separated value, a common, very old data exchange format which uses commas (or characters such as tab) to separate different fields.

- *time*: String. Time of the single measurement task (UTC)
- *download_kbit*: Numeric. Measured download speed in kilobit per second
- *upload_kbit*: Numeric. Measured upload speed on TCP kilobit per second

[*some other basic measurement metrics*]

Example response:

```
tasks: {
 [
  {
        "task_uuid": "f31d6c09-662b-4df8-83c1-66d949f51315",
        "time": "2017-03-23 13:59:35",
        "download_kbit": 50847,
        "upload_kbit": 30415
   },  ...,
   {
        "task_uuid": "adbfc094-0d4b-488a-a866-b11b3e8a90f3",
        "time": "2017-03-23 13:59:23",
        "download_kbit": 132303,
        "upload_kbit": 43133
   }
 ]
}
```

D.3.2 Listing details of a single measurement

This endpoint shall be used to provide detailed information about a single measurement task described with the task_uuid parameter.

Request: GET <nra_rest_interface>/task/{task_uuid}
Url Parameter:
task_uuid: Required, uuid of the desired measurement task

Response:
JSON Object containing all open data details of a single measurement task, e.g. https://www.netztest.at/en/OpenDataSpecification.html#open-data-for-one-specific-test

Example response:

```
{
        "task_uuid": "f31d6c09-662b-4df8-83c1-66d949f51315",
        "time": "2017-03-23 13:59:35",
        "download_kbit": 50847,
        "upload_kbit": 30415,
        "lat": 48.1872816,
        "long": 18.1739476,
        "loc_accuracy": 20.649999618530273,
        ...
}
```

E. Privacy Issues

E.1 Issues that need to be considered when developing and operating the Tool

When the Tool will master its first practice tests, thus be available for the general public, the General Data Protection Regulation will be in force. [26] This Regulation replaces the Data Protection Directive 95/46/EC.

For the provider of the Tool, thus the BEREC Office (in case of the reference system) or an NRA (in the case of a national implementation), it is important to consider the requirements of the General Data Protection Regulation and also in some specific cases, where the Data Protection regulation explicitly leaves member states room for concretization, respective national law, already when the specification for the Tool is being developed.

In addition, in some cases, e.g. for the BEREC Office, the Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by EU institutions and bodies and on the free movement of such data, applies as well. Art. 2(3) of the General Data Protection Regulation states in this regard: "*For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.*" In case new European privacy rules are adopted, the Tool should be updated accordingly.

The motto of the owner[27] of the Tool, thus BEREC Office or an NRA, should be: "*The less personal data the better and no special categories[28] of personal data*".[29]

In the following some major issues that the owner of the Tool has to consider are listed[30]:

1. *Personal data* means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

[26] The Regulation shall apply from 25 May 2018. For in-depth information on the Regulation see for example: EC websites on data protection reform: http://www.eugdpr.org/ + http://ec.europa.eu/justice/data-protection/reform/index_en.htm + https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS; Knyrim (ed), Datenschutzgrundverordnung, Manz, 2016 (German only);

[27] The owner of the Tool is the provider of the Tool, who bears the overall responsibility for the Tool. Legally we speak of the so-called *controller* of the Tool.

[28] Special categories of personal data are data revealing racial or ethnic origin, political opinions or philosophical beliefs, genetic data, health data etc. For more information on special categories of personal data see Art 9 General Data Protection Regulation.

[29] Regarding the principles of processing of personal data see also Art 5 of the General Data Protection.

identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Art 1 of the General Data Protection Regulation)

2. *Processing of personal data* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Art 4(2) General Data Protection Regulation)
3. The owner of the Tool is the *controller*. He determines the purposes and means of the processing of personal data. (Art 4(7), Art 5, Art 12 of the General Data Protection Regulation). Note also, a controller can process data
4. The *processor* (which could be a third party developing the tool, but it could also be BEREC office or an NRA) processes personal data on behalf of the controller. (Art 4(8) + 28 of the General Data Protection Regulation)
5. Processing of personal data is, amongst others, only lawful if the data subject has given consent to the processing of her or his personal data for one or more specific reasons; the controller is subject for compliance with a legal obligation; performing a task carried out in the public interest or in the exercise of official authority vested in the controller. (Art 5-6 + Art 9 of the General Data Protection Regulation)
6. Where processing of personal data is based on consent of the data subject, the controller needs to be able to demonstrate this consent. At the same time the data subject must have the right to withdraw her or his consent any time. If the data subject is a child below the age of 16, processing of personal data is only lawful if consent is given or authorised by the holder of parental responsibility. (Art. 7 + Art. 8 of the General Data Protection Regulation)
7. The controller of the Tool has to ensure transparent information, communication and modalities for the exercise of the rights of the data subject. Especially where personal data relating to a data subject are collected, the controller has to provide the data subject with detailed information. It is recommended to include this information in the applicable privacy rules of the Tool[31], but also in the FAQ. (Art 12-22 + Art 34 of the General Data Protection Regulation)
8. The controller and the processor of the Tool have to implement appropriate technical and organisational measures to ensure and be able to demonstrate that processing of personal data is performed in accordance with the Data Protection Regulation. Thus it is necessary that security as well as legal aspects are considered throughout the development of the Tool**.** Depending on the final detailed specifications for the development of the Tool a data protection impact assessment and/or a security assessment may be considered. (Art 24-31, Art 32 + Art 35-36 of the General Data Protection Regulation)
9. Any person who has suffered material or non-material damage as a result of an infringement of the Data Protection regulation shall have the right to receive compensation from the controller or processor. The following sanctions can be imposed: a warning in writing in cases of first and non-intentional non-compliance regular periodic data protection audits, a fine up to 10.000.000 EUR or up to 2% of

[31] See for this also appendix E.2 Privacy policy for the Tool".

the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is higher (Art 83(4)) , a fine up to 20.000.000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is higher (Art 83(5)). (Art 82- 91 of the General Data Protection Regulation)

E.2 Privacy policy for the Tool[32]

E.2.1 General guidance regarding the privacy policy

As explained before, it is of utmost importance that the owner of the Tool, thus BEREC Office or the respective NRA, strictly abides by the respective European and national legal requirements[33], and also provides end users and the public with adequate information about this.

The Tool requires a privacy policy which will have to comply, amongst others, with the General Data Protection Regulation (Regulation (EU) 2016/679)[34]. In addition it is recommended to provide information on privacy issues in the respective FAQ of the Tool.

The provider of the Tool generally needs to distinguish between the following data terms:

- *Raw Data*: All data that is collected/required by the Tool is referred to as raw data. This includes non-personal data as well as personal data. Such raw data *"…has not been subjected to processing or any other manipulation…"*[35]
- Open Data: This is raw data, which is made - within the legal framework of the privacy policy - publicly available under an Open Data license[36]. Anyone using Open Data is also subject to the General Data Protection Regulation. Open Data cannot include any personal data as this would be in violation with the General Data Protection Regulation[37].

[32] Examples of privacy policies of QoS measurement tools can be found here:
https://www.netmetr.cz/en/terms.html;
https://www.akostest.net/en/tc;
https://www.rtr.at/en/tk/netztestterms;
http://hyperiontest.gr/?action=terms;
https://breitbandmessung.de/nutzungsbedingungen;
http://www.nettfart.no/

[33] Regarding the applicable legal requirements please see the above sub-chapter "Issues that need to be considered when developing and operating the Tool".

[34] See online: Regulation (EU) 2016/679 (General Data Protection Regulation). The Regulation entered into force on 24 May 2016, it shall apply from 25 May 2018 in all EU member states.

[35] See: http://en.wikipedia.org/wiki/Raw_data/ which specific raw data the Tool will require, will only be determined at the time of the concrete specification for the Tool (maybe even only during the developing phase).

[36] The most commonly applied Open Data licenses are the ones from "Creative Commons". These licenses give the public permission to share and use Open Data under certain conditions (such as attribution, share-alike, non-commercial and no-derivatives conditions).

[37] E.g.: When personal data is processed the end used must give her or his consent. As the end user must be informed what is exactly being done with his personal data, when it is being erased and as she or he also has the right to withdraw this consent at any time, personal data cannot be Open Data. The consent of an end user is not legally valid, if she or he does not know what is explicitly being done with her or his personal data. At the same time, anything can be done with Open Data. Also, Open Data cannot be erased anymore.

The content of the privacy policy should contain in a concise, transparent, intelligible and easy accessible form, using clear and plain language, among others, the following information[38]:

- identity and contact details of the owner of the Tool (= controller)
- the legal basis for the Tool
- the purposes for processing (and transmitting) of personal data as well as data (also explanation of the terms *personal data*, *processing* and *transmitting*)
- usage of the Tool is only technically possible after explicit consent to the privacy policy and terms of use by the end user and that the consent is logged for evidence reasons,
- the end user has the right to withdraw her or his consent at any time[39] and in case of changes made to the processing and transmitting of personal data (e.g. updates or new releases of the Tool) the end user will have to renew her or his consent
- any age-limitations and under which conditions under-16 years may use the Tool,
- which specific personal data and data is being processed and (transmitted) (simply list the respective data, highlighting clearly the personal data)
- reasons why personal data is processed[40] and that it is not transmitted (thus it is neither disclosed or published and also not retrievable as Open Data),
- information how long personal data is stored respectively when it is deleted,
- explanation which data is published as Open Data,
- explaining the meaning of Open Source and Open Data and naming/linking the applied Open Source and Open Data licences.
- the end-user should also have the right to delete his/her profile (if a profile exists), and all personal data associated with it

E.2.2 Guidance for the reference implementation of the Tool and BEREC Portal

BEREC Office needs to draft a privacy policy in line with the Regulation (EU) 2016/679 (General Data Protection Regulation), the Regulation (EC) No 45/2001 and with what is determined (e.g. (required) technical data that is transmitted and (maybe also) processed by the measurement system) in this report.

BEREC Office shall distinguish between raw data, Open data and personal data. BEREC Office shall determine which specific raw data from the Tool shall be available as Open Data. Personal data shall never be Open Data. It should be closely cooperated with those who have to ensure that legal compliance with the respective laws is given. A data protection impact assessment and/or a security assessment shall be considered.[41]

The BEREC Portal should be able to present - besides Open Data from the Tool - data from

[38] See: Art. 6-8, Art. 12-17 of the General Data Protection Regulation

[39] Note that there are time limits till when the controller must react, e.g. Art. 12(3) General Data Protection Regulation

[40] E.g. regarding the IP address: in order to be able to assign the measurements to individual operators (via routing information (AS) or host names), to identify improper use and compile a history of use for the users)

[41] European Data Protection Supervisor, Guidance on Security Measures for Personal Data Processing - Article 22 of Regulation 45/2001, online available: https://edps.europa.eu/data-protection/our-work/publications/guidelines/security-measures-personal-data-processing_en

other NRAs which is also Open Data or which is aggregated and consent is given by the respective NRA.

BEREC Office shall use the Creative Commons Attribution CC BY License[42] for providing Open Data. This license lets others distribute, remix, tweak, and build upon the work, even commercially, as long as they credit the provider of the Open Data for the original creation.

E.2.3 Guidance for national measurement system

This section describes guidance for the national measurement systems that will be based on the open source software or will use parts of the open source software or/and will contribute with data from their national measurement system to the BEREC Portal.

It is for the individual NRA to decide if it commits itself to the principle of Open Data or not, and to determine which specific raw data shall be available as Open Data. As explained before, personal data is never Open Data.

Which raw data is made available as Open Data mostly depends on the (national) privacy issues and the overall national (political) attitude towards Open Data in this respect. An NRA can also contribute to the BEREC Portal with data other than Open Data, such as aggregated data.

[42] https://creativecommons.org/share-your-work/licensing-types-examples/licensing-examples/#by

F. Security

Raw data should be secured and only exported in Open Data format without any personal data. To this end, infrastructure hardening and audit is needed to find out existing vulnerabilities or flaws.[43]

Different security requirements (confidentiality, integrity and availability) should be guaranteed by the Tool.

- The whole measuring and analysis process should be confidential and anonymous for external parties to ensure security and privacy of end users' data.
- The Tool should also provide integrity to avoid data alteration or system compromise.
- The Tool should also be available to end users to provide information when a request is sent (distributed architecture to avoid single point of failure).

Authentication procedures/ciphering algorithms/secured exchanges and storage have to be used to make sure security requirements are met. Security should thus be provided by design.

Depending on the kind of data used, as well as the extent and purpose of the use, and considering the state of technical possibilities and economic justifiability, it has to be ensured that data are protected against accidental or intentional destruction or loss, that they are properly used and, and that they are not accessible to unauthorized persons. [44] Amongst other things, it is necessary to:

- expressly lay down the distribution of functions between the organisational units as well as the operatives regarding the use of data;
- tie the use of data to valid orders of the authorized organisational units or operatives;
- instruct every operative about her/his duties according to the respective national law and the internal data protection regulations, including data security regulations;
- regulate the right of access to the premises of the data controller or processor;
- regulate the right of access to data and programs as well as the protection of storage media against access and use by unauthorised persons;
- lay down the right to operate the data processing equipment and to secure it against unauthorised operation by taking precautions for the machines and programs used;
- keep logs in order that the processing steps that were actually performed - in particular modifications, consultations and transmissions - can be traced to the extent necessary with regard to their permissibility;
- keep documentation on the measures taken pursuant to the afore-mentioned points to facilitate control and conservation of evidence.

Cloud computing and virtualization are nowadays widely used and their added value, especially in terms of capacity allocation and cost reduction is undeniable. However, due to

[43] See in this regard also Art 32 of the General Data Protection Regulation.
[44] See: Art 32 of the General Data Protection Regulation.

the risks related to sharing infrastructures and the attacks that can occur (side channel attacks, for example), restrictions on hardware should be applied. In fact, all infrastructure servers (virtualized or not) use dedicated physical hardware only, and in no way shared with any other users (i.e. no use of shared virtual machines).

More specifically, data collection servers expose an API over HTTPS to allow measurement agents to report measurement results. Measurement agents and data reporting servers expose a web based reporting interface over HTTPS, secured by TLS using SSL certificate chained from a public CA.

All servers shall use firewalls to restrict access to necessary services. They are monitored and have their core statistics (network traffic, load average) tracked and graphed continually to check any dysfunction.

Besides, the Tool may use Kerberos across its server estate, backed by LDAP to control access to servers. Access is set according to roles; administrative access to servers is conducted entirely over SSH or HTTPS for web interfaces.

Concerning data, no personally identifiable information is ever exported from the Results repository. Passwords are never stored or transmitted in plain text. They have to be hashed and salted. Moreover, all data transferred from the collector servers to the management/analysis server(s) is conducted over SSH authentication using public/private key pairs.

Eventually, after setting up the Tool, BEREC Office could consider take care of running a security assessment campaign according to data protection rules and EDPS guidance.

This also applies to respective NRAs who decide to reuse the Open Source specification for the Tool in order to set-up their own national measurement system.

G. Terms of Use[45]

Terms of use (also known as terms of service or terms and conditions) are rules by which the end user must agree to comply with in order to use a service. It is recommended to separate the Terms of use and the Privacy policy, although there might be some overlaps.

Typical content of Terms of use are, amongst others:

- end users use the Tool at their own risk,
- information on age limitations,
- legal authorisation/source of the Tool,
- open source license information,
- open data license information,
- renunciation for any responsibility regarding the linking to third party content (Internet links)
- no legal claim to permanent availability of the offer (thus the provider of the Tool reserves the right to change, add to or delete parts of the Tool or the whole Tool without prior announcement, or to cease publication of it temporarily or finally,
- information that to ensure the correctness of the results, implausible and/or obvious abusive measurements may be marked and/or removed by the provider of the Tool,
- the right of the provider of the Tool to initiate appropriate legal action in case of non-compliance (implausible or/and obvious abusive measurements).
- no liability for the up-to-dateness, correctness, completeness or quality of the information and offers provided,
- no claims can be brought against the provider of the Tool for material or immaterial disadvantages and/or losses resulting from the use or non-use of information provided or from the use of incorrect and incomplete information,
- where the provider of the Tool cannot assert a full waiver of liability due to the statutory provisions applicable in the individual case, liability shall be limited to gross negligence and malicious intent,
- date of publication and version number of Terms of use.

[45] Examples of terms of use of QoS measurement tools can be found here:
https://www.netmetr.cz/en/terms.html;
https://www.akostest.net/en/tc;
https://www.rtr.at/en/tk/netztestterms;
http://hyperiontest.gr/?action=terms;
https://breitbandmessung.de/nutzungsbedingungen

H. Maintenance

The Tool should be able, by design, to handle faults and exceptions, by redirecting processes of calling new ones. In this context, a fault handling workflow should be defined.

End users should be able to report bugs (problems in general) or missing functionalities that can be added in next versions of the Tool (feedback). The implementation of the Tool should thus be done with an "agile"[46] process, so that it can be improved and faults can be corrected on a regular basis. The tool and its results should be reviewed and enhanced after a certain period of time.

Besides, all servers have to be kept up to date with the latest security patches. Periodic update should be provided to improve user experience and system functionalities. Exceptional updates should be taken into account for patch/code correction purposes. Measures collected during the update process are not taken in consideration.

[46] Agile software development, see https://en.wikipedia.org/wiki/Agile_software_development/