(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 January 2018 (18.01.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/010958 A2

(51) International Patent Classification:
G06F 21/33 (2013.01)

(21) International Application Number:
PCT/EP2017/065932

(22) International Filing Date:
27 June 2017 (27.06.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16179011.8 12 July 2016 (12.07.2016) EP

(71) Applicant: **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, 53113 Bonn (DE).

(72) Inventors: **FRIELINGSDORF, Matthias**; Königswinterer Straße 258, 53227 Bonn (DE). **SCHENK, Volker**; In den Herbstbenden 17, 53881 Euskirchen (DE).

(74) Agent: **SCHWÖBEL, Thilo** et al.; Kutzenberger Wolff & Partner, Theodor-Heuss-Ring 23, 50668 Köln (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2018/010958 A2

(54) Title: METHOD FOR DETECTING AND/OR IDENTIFYING DATA STREAMS WITHIN A TELECOMMUNICATIONS NETWORK; SYSTEM, TELECOMMUNICATIONS NETWORK, AND CONTENT SERVER ENTITY FOR DETECTING AND/OR IDENTIFYING DATA STREAMS WITHIN A TELECOMMUNICATIONS NETWORK, PROGRAM AND COMPUTER PROGRAM PRODUCT

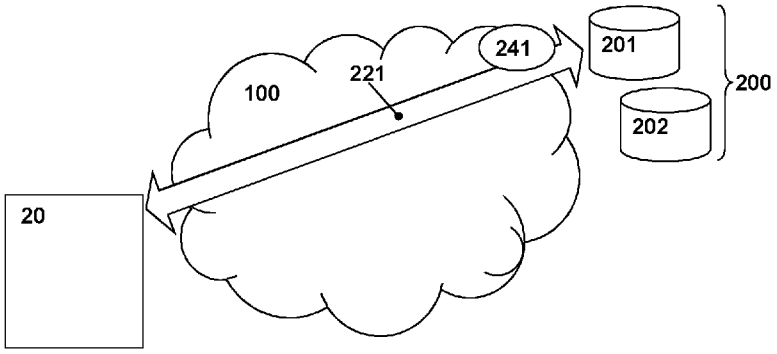

Fig. 1

(57) Abstract: The invention relates to a method for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment is connected - via an access network of the telecommunications network - with the telecommunications network, wherein, additionally, the telecommunications network is connected to at least one server entity, wherein the user equipment is able to receive payload data of at least one payload type - as a data stream and using a data connection between the user equipment and the at least one content server entity - from the at least one content server entity, wherein the payload data of the data stream are transmitted, between the at least one content server entity on the one hand, and the user equipment on the other hand, via the telecommunications network, and involving a server certificate information, wherein in order to transmit the payload data of the data stream, the method comprises the following steps: - in a first step, the server certificate information is assigned to the at least one content server entity and/or to the data stream, wherein the server certificate information comprises or is associated with a stream class information, - in a second step, subsequent to the first step - either while the data connection enabling the data stream is established or after the data connection enabling the data stream is established but while the data connection enabling the data stream is still available -, the stream class information of or associated with the server certificate information is both - transmitted, by the at least one content server entity, to the telecommunications network and/or provided by the at least one content server entity, and - detected and/or identified by a network node of the telecommunications network.

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

Method for detecting and/or identifying data streams within a telecommunications network; system, telecommunications network, and content server entity for detecting and/or identifying data streams within a telecommunications network, program and computer program product

BACKGROUND

[0001] The present invention relates to a method for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment and at least one server entity are connected with the telecommunications network, wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity.

[0002] The present invention further relates to a system for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment and at least one server entity are connected with the telecommunications network, wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity.

[0003] Additionally, the invention relates to a telecommunications network for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment and at least one server entity are connected with the telecommunications network, wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity.

[0004] Furthermore, the invention relates to a content server entity for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment and at least one server entity are connected with the telecommunications network, wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity.

[0005] Furthermore, the invention relates to a program comprising a computer readable program code and to a computer program product for providing an enhanced level of authentication related to a secure software client application provided by an application distribution entity.

[0006] With the growth of the Internet, a number of applications relating to multimedia content, such as music, software, or movie download, video share, Short message and multimedia message have come into existence. However, also a number of issues or problems are known related with such services, comprising but not being limited to copyright issues, spam, illegal information, as well as virus and malicious software code become. High market penetration, broader availability of flatrates and keen competition within the telecommunications market are leading to cost pressure among all telecommunication providers. Those companies are therefore demanded to offer new products and service plans to differentiate themselves from their competitors.

[0007] One approach consists in more or less deep inspecting network traffic, and to directly inspect the network traffic in order to retrieve the content thereof or to identify the content thereof. However, from the perspective of an operator of a telecommunications network, such as a mobile communication network and/or a fixed line telecommunications network, it might be preferable not to inspect network traffic on an important scale.

SUMMARY

[0008] An object of the present invention is to provide a cost-effective and comparatively fast, easy, as well as secure solution, for detecting and/or identifying data streams within a telecommunications network, wherein the detection and/or identification of the data streams serve to be able to differentiate and/or to treat different data streams differently without the need to inspect the data streams – and especially the content thereof (or the payload data of the data streams) – on an important scale and/or to a great extent (or depth) and/or to decrypt the (payload data) content of data streams that comprise (at least in part) encrypted content data or encrypted payload data, wherein the data streams are typically provided by content server entities towards clients or subscribers of the telecommunications network.

[0009] The object of the present invention is achieved by a method for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment is connected – via an access network of the telecommunications network –

with the telecommunications network,

wherein, additionally, the telecommunications network is connected to at least one server entity, wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity,

wherein the payload data of the data stream are transmitted, between the at least one content server entity on the one hand, and the user equipment on the other hand, via the telecommunications network, and involving a server certificate information,

wherein in order to transmit the payload data of the data stream, the method comprises the following steps:

-- in a first step, the server certificate information is assigned to the at least one content server entity and/or to the data stream, wherein the server certificate information comprises or is associated with a stream class information,

-- in a second step, subsequent to the first step – either while the data connection enabling the data stream is established or after the data connection enabling the data stream is established but while the data connection enabling the data stream is still available –, the stream class information of or associated with the server certificate information is both

-- transmitted, by the at least one content server entity, to the telecommunications network and/or provided by the at least one content server entity, and

-- detected and/or identified by a network node of the telecommunications network.

[0010] According to the present invention, it is thereby advantageously possible that data streams between at least one content server entity and a user equipment (via the telecommunications network) can be detected and/or identified. The telecommunications network corresponds to either a fixed-line telecommunications network (i.e. the client or user equipment is typically connected to the telecommunications network using a wireline connection, typically to a router entity or (home) gateway entity or CPE (customer premises equipment), wherein a wireless (local area network, WLAN) connection is often used between the router entity and the user equipment) or a mobile communication network (also referred to as a public land mobile network, and typically comprising an access network comprising a plurality of base station entities, wherein the user equipments (of the mobile communication network or connected to the mobile communication network) are connected to at least one base station entity of the plurality of base station entities using an air interface, especially according to a 3GPP (Third Generation Partnership Project) standard) or to a combined or integrated fixed-line and mobile communication network, i.e. a telecommunications network comprising (in at least

a first part or in a first area) components of a wireline telecommunications network, and comprising (in the first part and/or in at least a second part or in a second area) components of a mobile communication network. Typically, the telecommunications network is connected to a plurality of content server entities, e.g., different streaming servers, e.g. for video streaming, audio streaming or other content providers.

[0011] It is assumed according to the present invention, that the user equipment is able to receive payload data of at least one payload type from the at least one content server entity. Typically, the user equipment is able to receive payload data of a plurality of different payload types, typically from a plurality of different content server entities and/or from the at least one content server entity, wherein both the case of the at least one content server entity providing different payload types (i.e. at least two different payload types) to the user equipment as well as the case of each content server entity providing each one a different payload type to the user equipment, as well as mixed scenarios thereof could be realized. The payload data of one data stream are typically transmitted using a data connection between the user equipment and the at least one content server entity, via the telecommunications network.

[0012] According to the present invention, each data stream typically consists of a plurality, even a multitude, of different data packets (typically internet protocol packets), and the payload data (or payload data packets) of such a data stream are transmitted, between the at least one content server entity on the one hand, and the user equipment on the other hand, via the telecommunications network, and involving a server certificate information. By means of the server certificate information, it is advantageously possible to detect and/or to identify each data stream, or also a plurality of data streams (having something in common). Advantageously according to the present invention, this detection and/or identification (of one or a plurality data streams) can be provided in a secure and/or protected manner due to the detection and/or identification being performed or conducted upon the server certificate information (of the content server entity, wherein the server certificate information provides a certain level of authentication regarding the data stream, and especially regarding its origin, i.e. the respective content server entity). The detection and/or identification itself is done, according to the present invention, by means of a stream class information being part of the server certificate information and/or being associated with the server certificate information.

[0013] Only in order to provide an example of an embodiment of the present invention, and without limiting the scope of the present invention, the server certificate information might comprise,

-- regarding a first data stream, the string (or subdomain information) "video.contentprovider1.com",

-- regarding a second data stream, the string "video.contentprovider2.com", and

-- regarding a third data stream, the string "audio.contentprovider1.com".

According to a first use case according to the present invention, the stream class information could correspond to or be associated to detecting and/or identifying the string "video", which would, according to the exemplary embodiment, result in identifying the first and second data stream, whereas in case of a second use case and the stream class information corresponding to or be associated to (detecting and/or identifying) the string "contentprovider1", the exemplary embodiment would result in identifying the first and third data stream. Of course, the use of "video.contentprovider1" or "video.contentprovider1.com" would result in identifying the first data stream.

[0014] Hence, according to the present invention, in a first step according to the inventive method, the server certificate information is assigned to the at least one content server entity and/or to the data stream, wherein the server certificate information comprises or is associated with a stream class information, and in a second step of the inventive method, subsequent to the first step – either while the data connection enabling the data stream is established or after the data connection enabling the data stream is established but while the data connection enabling the data stream is still available –, the stream class information of or associated with the server certificate information is both

-- transmitted, by the at least one content server entity, to the telecommunications network and/or provided by the at least one content server entity, and

-- detected and/or identified by a network node of the telecommunications network.

[0015] According to the present invention, it is advantageously possible to be able to conduct different actions based on the detected and/or identified data streams that are transported by the telecommunications network, typically to the multitude of user equipments being connected to the telecommunications network.

[0016] According to an embodiment of the present invention, in a third step, subsequent to the second step, a handling alternative – out of a plurality of handling alternatives, to be potentially applied to data streams within the telecommunications network – is applied to the data stream in dependency of the detected and/or identified stream class information,

wherein the plurality of handling alternatives comprise

wherein the plurality of handling alternatives comprise

-- applying a different-rating to the data stream and/or

-- applying a different rating information to the data stream, especially corresponding to zero-rating for end customers, and/or

-- applying a different measurement information to the data stream, especially a dedicated volume counter, and/or

-- charging the transferred data within the data stream to a third party, especially to the provider of the content server entity and/or

-- applying a certain quality-of-service level and/or

-- applying a certain quality-of-experience level and/or

-- applying a maximum or minimum transmission bandwidth towards the user equipment and/or

-- manipulating the data stream information or a subset of it and/or

-- blocking and/or filtering the data stream.

[0017] By means of applying different handling alternatives in dependency of the detected and/or identified stream class information, it is advantageously possible to effectively handle the different data streams traversing the telecommunications network based on a piece of information associated with the server certificate information transmitted and/or provided by the corresponding content server entity the data stream in question is originating from.

[0018] According to a further embodiment of the present invention, the stream class information corresponds to or is associated with at least one out of the following:

-- a domain name information of the at least one content server entity, the domain name information especially being a part of the server certificate information, and especially being a subdomain name information,

-- a uniform resource identifier information of the at least one content server entity, the uniform resource identifier information especially being a part of the server certificate information,

-- a payload type information of the data stream, the payload type information especially being a part of the server certificate information,

-- a user equipment information of the user equipment.

[0019] According to the present invention, it is especially advantageous to use a domain name information (or a part thereof) of the at least one content server entity, especially being part of the server certificate information, and especially being a subdomain name information (such as “video.contentprovider1.com” or only “video.contentprovider1”) as the stream class information. Alternatively or cumulatively, it is advantageous to use a uniform identifier information (or a part thereof) of the at least

one content server entity, especially being part of the server certificate information as the stream class information. Alternatively or cumulatively, it is advantageous to use a payload type information (or a part thereof) of the data stream, especially being part of the server certificate information as the stream class information. Still alternatively or cumulatively, it is advantageous to use a user equipment information of the user equipment as the stream class information.

[0020] According to still a further embodiment of the present invention, the stream class information of or associated with the server certificate information is linked to the domain name information and/or to the uniform resource identifier information of the at least one content server entity, and wherein a different stream class information corresponds to a different domain name information and/or to a different uniform resource identifier information of the at least one content server entity.

[0021] Thereby, it is advantageously possible according to the present invention to detect and/or identify the different data streams based on different pieces of stream class information.

[0022] According to still a further embodiment of the present invention, after the stream class information of or associated with the server certificate information has been detected, the domain name information and/or the uniform resource identifier information of the server certificate information – corresponding to the domain name information and/or to the uniform resource identifier information of the at least one content server entity – is compared to the domain and/or to the uniform resource identifier initially requested by the user equipment.

[0023] Thereby, it is advantageously possible to provide a further verification step and to ensure a still higher level of integrity of the data streams.

[0024] According to a further embodiment of the present invention, while establishing the data connection enabling the data stream, a response message is generated, especially by the at least one content server entity, wherein the response message comprises – especially within the HTTP-header – a content type information of the data stream, wherein the content type information especially corresponds to a signed information, and the detection of the content type being based on the detection of the server certificate information.

[0025] Thereby, it is advantageously possible to associate the content type information with the server certificate information, thus, it is advantageously possible to

verify (or ensure) the integrity of the content server entity (especially by (a network node of) the telecommunications network and/or by the user equipment. Furthermore, it is advantageously possible, by means of detecting the content type, to flexibly adapt the appropriate handling of the data stream in accordance (or in dependency) of the content type as indicated by means of the server certificate information; e.g. it would be possible to re-classify the data strams involving a specific content such as, for example, MP4 content.

[0026] According to a further embodiment of the present invention, while establishing the data connection enabling the transmission of the data stream, a response message is generated, especially by the at least one content server entity, wherein the response message comprises a signed information being the result of a signature generating operation on an IP-address (Internet Protocol address) information, wherein a validation of the at least one content server entity and/or of the user equipment and/or of the content of the data stream is performed based on the detection of the server certificate information, wherein the IP-address information especially comprises the IP-address and/or the port number and/or a random number and/or a hashed value of a part of the content data of the data stream.

[0027] By means of using a signed information, as part of the response message, being the result of a signature generating operation on an IP-address (Internet Protocol address) information, wherein a validation of the at least one content server entity and/or of the user equipment and/or of the content of the data stream is performed based on the detection of the server certificate information, it is advantageously possible to relate a data stream to the at least one content server entity. Especially, it is advantageously possible according to the present invention that the signed information is the result of a signature generating operation on the following pieces of information:

-- the IP address and/or the (TCP/UDP) port number used by the content server entity for the considered data stream and/or

-- the IP address and/or the (TCP/UDP) port number used by the user equipment for the considered data stream.

[0028] According to a further embodiment of the present invention, while establishing the data connection enabling the transmission of the data stream, a response message is generated, especially by the at least one content server entity, and a challenge information is transmitted, from the telecommunications network to the at least one content server entity, wherein the response message comprises a response information being the result of a signature generating operation on the challenge information, wherein

a validation of the at least one content server entity and/or of the user equipment and/or of the content of the data stream is performed based on the detection of the server certificate information.

[0029] By using a challenge information transmitted to the content server entity and a response information being the result of a signature generating operation on the challenge information, it is advantageously possible to validate the at least one content server entity and/or the user equipment and/or the content of the data stream.

[0030] According to a further embodiment of the present invention, the payload data of the data stream are at least partly encrypted and/or signed, especially using a TLS (Transport Layer Security) encryption protocol, wherein the server certificate information especially corresponds to a server certificate according to the X509 specification.

[0031] According to all embodiments of the present invention, it is advantageously possible to use encryption to transmit the payload data of the data stream. Under the assumption of transmitting the payload data of the data stream in encrypted form, the payload data of data stream can either not be efficiently controlled at all, or these payload data need to be inspected on a large scale, which in turn may cause additional processing effort to be conducted by the operator of the telecommunications network, and/or may require the user's consent to do so in accordance to data protection regulation and/or law. By means of being able – using the server certificate information and the stream class information – to easily detect and/or identify different data streams travelling through the telecommunications network, it is advantageously possible to both apply the correct handling to the respective data streams, and to avoid additional processing effort and/or avoid obtaining at least one out of the user's consent to decrypt and/or breaches of data protection law.

[0032] Furthermore, the present invention relates to a system for detecting and/or identifying data streams within a telecommunications network, wherein a user equipment is connected – via an access network of the telecommunications network – with the telecommunications network,
wherein, additionally, the telecommunications network is connected to at least one content server entity,
wherein the system comprises the telecommunications network, the user equipment, and the at least one content server entity,
wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity,

wherein the payload data of the data stream are transmitted, between the at least one content server entity on the one hand, and the user equipment on the other hand, via the telecommunications network, and involving a server certificate information,
wherein in order to transmit the payload data of the data stream, the system is configured such that:

-- the server certificate information is assigned to the at least one content server entity and/or to the data stream, wherein the server certificate information comprises or is associated with a stream class information,

-- the stream class information of or associated with the server certificate information is – either while the data connection enabling the data stream is established or after the data connection enabling the data stream is established but while the data connection enabling the data stream is still available – both

-- transmitted, by the at least one content server entity, to the telecommunications network and/or provided by the at least one content server entity, and

-- detected and/or identified by a network node of the telecommunications network.

[0033] By means of such a system, it is advantageously possible according to the present invention that data streams between at least one content server entity and a user equipment (via the telecommunications network) can be detected and/or identified.

[0034] Additionally, the present invention relates to a telecommunications network for detecting and/or identifying data streams within the telecommunications network, wherein a user equipment is connected – via an access network of the telecommunications network – with the telecommunications network,
wherein, additionally, the telecommunications network is connected to at least one content server entity,
wherein the user equipment is able to receive payload data of at least one payload type – as a data stream and using a data connection between the user equipment and the at least one content server entity – from the at least one content server entity,
wherein the payload data of the data stream are transmitted, between the at least one content server entity on the one hand, and the user equipment on the other hand, via the telecommunications network, and involving a server certificate information,
wherein in order to transmit the payload data of the data stream, the telecommunications network is configured such that:

-- the server certificate information is assigned to the at least one content server entity and/or to the data stream, wherein the server certificate information comprises or is associated with a stream class information,

-- the stream class information of or associated with the server certificate information is

– either while the data connection enabling the data stream is established or after the data connection enabling the data stream is established but while the data connection enabling the data stream is still available – both

-- transmitted, by the at least one content server entity, to the telecommunications network and/or provided by the at least one content server entity, and

-- detected and/or identified by a network node of the telecommunications network.

[0035] By means of such a telecommunications network, it is advantageously possible according to the present invention that data streams between at least one content server entity and a user equipment (via the telecommunications network) can be detected and/or identified.

[0036] Furthermore, the present invention relates to a content server entity for detecting and/or identifying data streams within an inventive telecommunications network suitable to be used in an inventive system.

[0037] Furthermore, the present invention relates to a program comprising a computer readable program code which, when executed on a computer or on a network node of a telecommunications network or on a content server entity, or in part on a network node of a telecommunications network and/or in part on a content server entity and/or in part on a content server entity, causes the computer and/or the network node of the telecommunications network and/or the content server entity to perform an inventive method.

[0038] Still additionally, the present invention relates to computer program product for detecting and/or identifying data streams within a telecommunications network, the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a network node of a telecommunications network or on a content server entity, or in part on a network node of a telecommunications network and/or in part on a content server entity and/or in part on a content server entity, causes the computer and/or the network node of the telecommunications network and/or the content server entity to perform an inventive method.

[0039] These and other characteristics, features and advantages of the present invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, which illustrate, by way of example, the principles of the invention. The description is given for the sake of example only, without

limiting the scope of the invention. The reference figures quoted below refer to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0040] Figure 1 schematically illustrates an exemplary system and situation according to the present invention where a telecommunications network – with a user equipment connected to the telecommunications network – is connected to content server entity, and the content server entity is able to provide a data stream to the user equipment.

[0041] Figure 2 schematically illustrates a communication diagram related to the invention.

DETAILED DESCRIPTION

[0042] The present invention will be described with respect to particular embodiments and with reference to certain drawings but the invention is not limited thereto but only by the claims. The drawings described are only schematic and are non-limiting. In the drawings, the size of some of the elements may be exaggerated and not drawn on scale for illustrative purposes.

[0043] Where an indefinite or definite article is used when referring to a singular noun, e.g. “a”, “an”, “the”, this includes a plural of that noun unless something else is specifically stated.

[0044] Furthermore, the terms first, second, third and the like in the description and in the claims are used for distinguishing between similar elements and not necessarily for describing a sequential or chronological order. It is to be understood that the terms so used are interchangeable under appropriate circumstances and that the embodiments of the invention described herein are capable of operation in other sequences than described or illustrated herein.

[0045] In Figure 1, a system for realizing the present invention is schematically shown, the system comprising a telecommunications network 100, especially a mobile communication network (also called public land mobile network) or a fixed-line

telecommunications network. The telecommunications network 100 is connected to a user equipment 20. The system furthermore also comprises at least one content server entity 201. Typically, a plurality of content server entities 200 is connected to the telecommunications network 100, comprising a first content server entity 201 and a second content server entity 202.

[0046] According to the present invention, the at least one content server entity 201 (or first content server entity 201) provides data to be transmitted to the user equipment 20, especially streaming data. The data or payload data are transmitted to the user equipment 20 by means of at least one data stream 221 (illustrated in Figure 1 by means of a double arrow). Typically, a plurality of data streams are transmitted from the (first) content server entity 201 to the user equipment 20 or from the first and the second content server entity 201, 202 to the user equipment 20.

[0047] According to the present invention, a data stream 221, being transmitted between the at least one content server entity 201 and the user equipment 20, involves a server certificate information 241, the server certificate information 241 being assigned to the at least one content server entity 201 and/or to the data stream 221. Furthermore, the server certificate information 241 comprises or is associated with a stream class information.

[0048] In Figure 2 a communication diagram relating to the present invention is schematically represented. The communication diagram involves the user equipment 20, the (first or at least one) content server entity 201, and the telecommunications network 100. In a first processing step 301, the server certificate information 241 associated with the first content server entity 201 is transmitted to the telecommunications network 100. In a second processing step 302, the user equipment 20 requests content data to be transmitted, the content data being typically provided by the content server entity 201, and transmitted via the telecommunications network 100 to the user equipment 20. In a third processing step 303, the first content server entity 201 transmits a response message to at least the telecommunications network 100 (or, as it is shown in Figure 2, also to the user equipment 20). It is to be said that what is shown in Figure 2 essentially corresponds to the steps relevant for the present invention: In fact, typically the user equipment 20 is requesting content data, and hence a TLS channel is established, and thereby the server certificate information 241 is transmitted. Thereafter, the user equipment 20 (or client) is able to transmit the request to the content server entity 201.

[0049] Especially in case that the content, i.e. the payload data of the data stream 221 is encrypted, especially end-to-end encrypted from the first content server entity 201

to the user equipment 20 (and/or vice versa), additional measures would have to be implemented, within the telecommunications network, in order to decrypt the payload data.

[0050] According to the present invention, it is advantageously possible to use different pieces of subdomain information (such as “audio.contentprovider1.com”, “video.contentprovider1.com”, “html.contentprovider1.com”) and different server certificate information in order to detect and/or to identify different types of content within the payload data. It is especially advantageous according to the present invention that one server certificate information is generated (and exchanges with the telecommunications network 100) for each subdomain information.

[0051] It is then possible, within the telecommunications network 100, to detect and/or to identify different data streams – by means of using the server certificate information – based on a stream class information, e.g. all the data streams of a certain content server entity 201, 202 (by means of using, e.g., a string of “*.contentprovider1”) or all the data streams relating to a specific type of service (by means of using, e.g., a string of “video.*”) or a combination thereof.

[0052] Typically the server certificate information (or server certificates) are linked or pinned to the subdomain information and/or the certificates are transmitted per TCP/UDP connection. The certificates are able to be detected by means of different methods, e.g. by means of using the bit pattern in the data stream and/or by analyzing the data stream.

PATENT CLAIMS

1. Method for detecting and/or identifying data streams within a telecommunications network (100), wherein a user equipment (20) is connected – via an access network of the telecommunications network (100) – with the telecommunications network (100),
wherein, additionally, the telecommunications network (100) is connected to at least one server entity (201), wherein the user equipment (20) is able to receive payload data of at least one payload type – as a data stream (221) and using a data connection between the user equipment (20) and the at least one content server entity (201) – from the at least one content server entity (201),
wherein the payload data of the data stream (221) are transmitted, between the at least one content server entity (201) on the one hand, and the user equipment (20) on the other hand, via the telecommunications network (100), and involving a server certificate information (241),
wherein in order to transmit the payload data of the data stream (221), the method comprises the following steps:
-- in a first step, the server certificate information (241) is assigned to the at least one content server entity (201) and/or to the data stream (221), wherein the server certificate information (241) comprises or is associated with a stream class information,
-- in a second step, subsequent to the first step – either while the data connection enabling the data stream (221) is established or after the data connection enabling the data stream (221) is established but while the data connection enabling the data stream (221) is still available –, the stream class information of or associated with the server certificate information (241) is both
-- transmitted, by the at least one content server entity (201), to the telecommunications network (100) and/or provided by the at least one content server entity (201), and
-- detected and/or identified by a network node of the telecommunications network (100).

2. Method according to claim 1, wherein in a third step, subsequent to the second step, a handling alternative – out of a plurality of handling alternatives, to be potentially applied to data streams within the telecommunications network (100) – is applied to the data stream (221) in dependency of the detected and/or identified

stream class information,

wherein the plurality of handling alternatives comprise

-- applying a different-rating to the data stream (221) and/or

-- applying a different rating information to the data stream (221), especially corresponding to zero-rating for end customers, and/or

-- applying a different measurement information to the data stream (221), especially a dedicated volume counter, and/or

-- charging the transferred data within the data stream (221) to a third party, especially to the provider of the content server entity (201) and/or

-- applying a certain quality-of-service level and/or

-- applying a certain quality-of-experience level and/or

-- applying a maximum or minimum transmission bandwidth towards the user equipment (20) and/or

-- manipulating the data stream (221) information or a subset of it and/or

-- blocking and/or filtering the data stream (221).

3. Method according to one of the preceding claims, wherein the stream class information corresponds to or is associated with at least one out of the following:

-- a domain name information of the at least one content server entity (201), the domain name information especially being a part of the server certificate information (241), and especially being a subdomain name information,

-- a uniform resource identifier information of the at least one content server entity (201), the uniform resource identifier information especially being a part of the server certificate information (241),

-- a payload type information of the data stream (221), the payload type information especially being a part of the server certificate information (241),

-- a user equipment information of the user equipment (20).

4. Method according to one of the preceding claims, wherein the stream class information of or associated with the server certificate information (241) is linked to the domain name information and/or to the uniform resource identifier information of the at least one content server entity (201), and wherein a different stream class information corresponds to a different domain name information and/or to a different uniform resource identifier information of the at least one content server entity (201).

5. Method according to one of the preceding claims, wherein the stream class information of the server certificate information (241) is detected by means of

detecting a bit pattern of or associated with at least part of the server certificate information (241) within the data stream (221) and/or by means of analyzing and decoding the data stream (221).

6. Method according to one of the preceding claims, wherein, after the stream class information of or associated with the server certificate information (241) has been detected, the domain name information and/or the uniform resource identifier information of the server certificate information (241) – corresponding to the domain name information and/or to the uniform resource identifier information of the at least one content server entity (201) – is compared to the domain and/or to the uniform resource identifier initially requested by the user equipment (20).

7. Method according to one of the preceding claims, wherein, while establishing the data connection enabling the data stream (221), a response message (303) is generated, especially by the at least one content server entity (201), wherein the response message (303) comprises – especially within the HTTP-header – a content type information of the data stream (221), wherein the content type information especially corresponds to a signed information, and the detection of the content type being based on the detection of the server certificate information (241).

8. Method according to one of the preceding claims, wherein, while establishing the data connection enabling the transmission of the data stream (221), a response message (303) is generated, especially by the at least one content server entity (201), wherein the response message (303) comprises a signed information being the result of a signature generating operation on an IP-address (Internet Protocol address) information, wherein a validation of the at least one content server entity (201) and/or of the user equipment (20) and/or of the content of the data stream (221) is performed based on the detection of the server certificate information (241), wherein the IP-address information especially comprises the IP-address and/or the port number and/or a random number and/or a hashed value of a part of the content data of the data stream (221).

9. Method according to one of the preceding claims, wherein, while establishing the data connection enabling the transmission of the data stream (221), a response message (303) is generated, especially by the at least one content server entity (201), and a challenge information is transmitted, from the telecommunications

network (100) to the at least one content server entity (201), wherein the response message (303) comprises a response information being the result of a signature generating operation on the challenge information, wherein a validation of the at least one content server entity (201) and/or of the user equipment (20) and/or of the content of the data stream (221) is performed based on the detection of the server certificate information (241).

10. Method according to one of the preceding claims, wherein the payload data of the data stream (221) are at least partly encrypted and/or signed, especially using a TLS (Transport Layer Security) encryption protocol, wherein the server certificate information (241) especially corresponds to a server certificate according to the X509 standard.

11. System for detecting and/or identifying data streams within a telecommunications network (100), wherein a user equipment (20) is connected – via an access network of the telecommunications network (100) – with the telecommunications network (100),
wherein, additionally, the telecommunications network (100) is connected to at least one content server entity (201),
wherein the system comprises the telecommunications network (100), the user equipment (20), and the at least one content server entity (201),
wherein the user equipment (20) is able to receive payload data of at least one payload type – as a data stream (221) and using a data connection between the user equipment (20) and the at least one content server entity (201) – from the at least one content server entity (201),
wherein the payload data of the data stream (221) are transmitted, between the at least one content server entity (201) on the one hand, and the user equipment (20) on the other hand, via the telecommunications network (100), and involving a server certificate information (241),
wherein in order to transmit the payload data of the data stream (221), the system is configured such that:
-- the server certificate information (241) is assigned to the at least one content server entity (201) and/or to the data stream (221), wherein the server certificate information (241) comprises or is associated with a stream class information,
-- the stream class information of or associated with the server certificate information (241) is – either while the data connection enabling the data stream (221) is established or after the data connection enabling the data stream (221) is

established but while the data connection enabling the data stream (221) is still available – both

-- transmitted, by the at least one content server entity (201), to the telecommunications network (100) and/or provided by the at least one content server entity (201), and

-- detected and/or identified by a network node of the telecommunications network (100).

12. System for detecting and/or identifying data streams within the telecommunications network (100), wherein a user equipment (20) is connected – via an access network of the telecommunications network (100) – with the telecommunications network (100),
wherein, additionally, the telecommunications network (100) is connected to at least one content server entity (201),
wherein the user equipment (20) is able to receive payload data of at least one payload type – as a data stream (221) and using a data connection between the user equipment (20) and the at least one content server entity (201) – from the at least one content server entity (201),
wherein the payload data of the data stream (221) are transmitted, between the at least one content server entity (201) on the one hand, and the user equipment (20) on the other hand, via the telecommunications network (100), and involving a server certificate information (241),
wherein in order to transmit the payload data of the data stream (221), the telecommunications network (100) is configured such that:
-- the server certificate information (241) is assigned to the at least one content server entity (201) and/or to the data stream (221), wherein the server certificate information (241) comprises or is associated with a stream class information,
-- the stream class information of or associated with the server certificate information (241) is – either while the data connection enabling the data stream (221) is established or after the data connection enabling the data stream (221) is established but while the data connection enabling the data stream (221) is still available – both

-- transmitted, by the at least one content server entity (201), to the telecommunications network (100) and/or provided by the at least one content server entity (201), and

-- detected and/or identified by a network node of the telecommunications

network (100).

13. Content server entity (201) for detecting and/or identifying data streams within a telecommunications network (100) suitable to be used in a system according to claim 11 or in a telecommunications network (100) according to claim 12.

14. Program comprising a computer readable program code which, when executed on a computer or on a network node of a telecommunications network (100) or on a content server entity (201), or in part on a network node of a telecommunications network (100) and/or in part on a content server entity (201) and/or in part on a content server entity (201), causes the computer and/or the network node of the telecommunications network (100) and/or the content server entity (201) to perform a method according one of claims 1 to 10.

15. Computer program product for detecting and/or identifying data streams within a telecommunications network (100), the computer program product comprising a computer program stored on a storage medium, the computer program comprising program code which, when executed on a computer or on a network node of a telecommunications network (100) or on a content server entity (201), or in part on a network node of a telecommunications network (100) and/or in part on a content server entity (201), causes the computer and/or the network node of the telecommunications network (100) and/or the content server entity (201) to perform a method according one of claims 1 to 10.

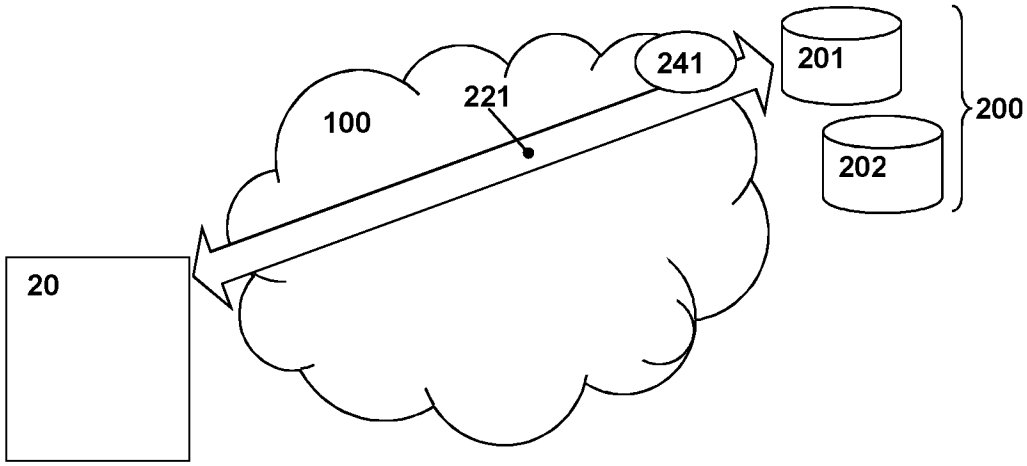

Fig. 1

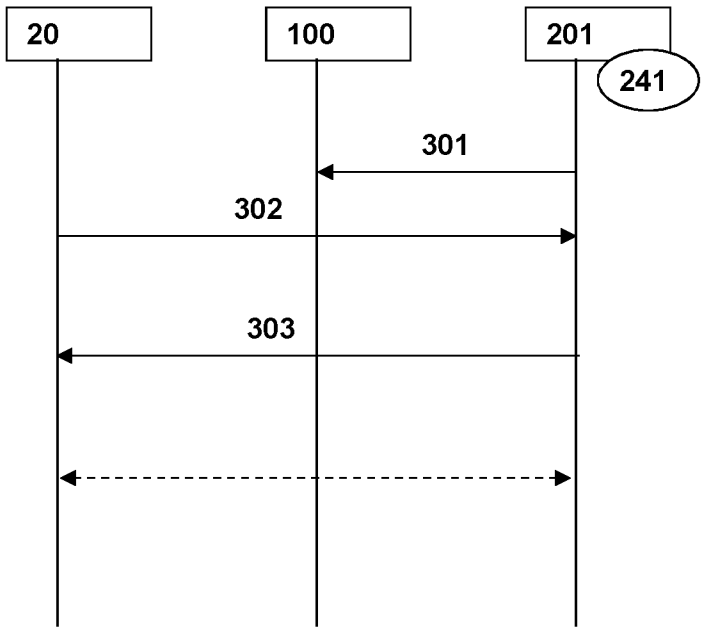

Fig. 2