



New connection on: : 01-10-2020 : 21:17:06 - Last disconnection on: : 01-10-2020 : 21:16:43

V 4.0.0.44803(LP,U,linux) (Rev:43856 2017-04-27 09:03:29 +0200#{D201820}) (RPM D201820)

Welcome to EPOQUE Rebuild under the Production Environment

[EPODOC: SS 38] OTP and Mobile_device and Internet and Server and Authentication and Network

Results in EPODOC 4

[SS 39] ..li



1/4 © EPODOC / EPO

PN - [TW201417597](#) A 20140501

PNFP - TWI473507B B 20150211

PR - TW20120139580 20121025

AP - [TW20120139580](#) 20121025

DT - I

PA - (A B)
UNIV CHIEN HSIN SCI & TECH [TW]

TI - (A)
QR code interactive **OTP** password **authentication** method

AB - (A)
The present invention discloses a QR code interactive **OTP** (one-time password) password **authentication** method, primarily comprising the following steps: when a user logs in the identity certification, a management **server** at least transferring a randomly generated QR code once to a client's user interface; the QR code being subjected to scanning by a user-designated **mobile device**, so as to obtain an interactive **OTP** password corresponding to the QR code; and the management **server** completing the **authentication** of the interactive **OTP** password corresponding to the QR code before the user can log in successfully. In this way, a relatively more positive means can be used to prevent **Internet** attacks of trojan horse, keylogger, phishing sites, man-in-the-middle attack, spyware and brute force attack, etc. The present invention relates to a **network** account identity **authentication** technique, and more particularly to a QR code **OTP** password **authentication** method that requires a user-designated **mobile device** to scan the QR code displayed on the user interface in order to obtain the interactive **OTP** password corresponding to the QR code, so that a basis for the management **server** to confirm the user login identity can be provided.

2/4 © EPODOC / EPO

PN - [WO2012045908](#) A1 20120412

PR - WO2010FI50773 20101006

AP - [WO2011FI50380](#) 20110427

DT - *: Rep

CT - */FI/ ISR (A1)*
 FI115745B B 20050630 [X]
 (DELTA GON GROUP OY [FI]);
[US2010022254](#) A1 20100128 [Y]
 (ASHFIELD JAMES [US], et al);
[US2007136573](#) A1 20070614 [Y]
 (STEINBERG JOSEPH [US]);
[US2009235346](#) A1 20090917 [Y]
 (STEINBERG JOSEPH [US]);
[US2002099942](#) A1 20020725 [A]
 (GOHL ERIKA MONIKA [US]);
[WO9966666](#) A2 19991223 [A]
 (CSAFE LTD [IL])

CTNP - */FI/ ISR (A1)*
 [X] - "D3 Envelope method -
 Receiver authentication.
 Datasheets", DELTAGON, (2008),
 URL: http://web.archive.org/web/20080411210134/www.deltagon.com/envelope_method.html, (20110201)

CCI - [H04L9/3228](#) ; [H04L51/24](#) ;
[H04L63/0838](#) ; [H04L63/0853](#) ;
[H04W12/0608](#)

CCA - [H04L63/107](#) ; [H04L63/18](#) ;
[H04L2463/082](#) ; [H04W4/14](#) ;
[H04W12/00503](#)

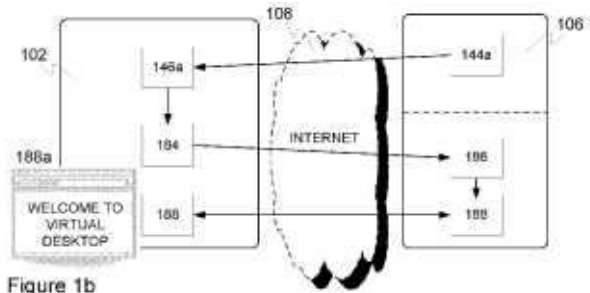
CI - H04L9/3228 (EP)
 - H04L51/24 (EP)
 - H04L63/0838 (EP, US)
 - H04L63/0853 (EP)
 - H04W4/029 (US)
 - H04W12/0608 (EP, US)

CA - H04L63/107 (EP)
 - H04L63/18 (EP)
 - H04L2463/082 (EP)
 - H04W4/14 (EP)
 - H04W12/00503 (EP, US)

PA - APLCOMP OY [FI]; PITKAENEN
 MARTTI [FI]

TI - ARRANGEMENT AND METHOD FOR
 ACCESSING A **NETWORK** SERVICE

AB - An arrangement (106), such as
 a **server** apparatus or a plurality



of at least functionally connected **server** and/or other apparatuses, for controlling access to a **network** service, such as a cloud service, utilizing multi-factor, at least two-factor, **authentication** comprising a processing entity (150) and a memory entity (152) for processing and storing data, respectively, and a data transfer entity (156) for receiving and sending data, the arrangement being configured to send an e-mail notice (128) to an e-mail address associated with a predetermined user, the e-mail notice including a preferably secure link for a browser, such as an **Internet** browser, receive an indication of the activation of the preferably secure link (134), such as a data request like a web resource request sent via a browser, in response to which the arrangement being further configured to send first browser data, such as web page data, requesting the user of the browser to input a secret (136), and a one-time password (**OTP**) to a **mobile device** associated with the predetermined user (138b), receive user input relative to the request for secret (140), determine whether the user input matches the sent **OTP** (142), and if that is the case, enable the user of the browser and related terminal device, thus authenticated as the predetermined user, to access the service (144, 144a, 186, 88) . Enabling preferably includes transfer of enabling data such as program and/or password data to the terminal device. A corresponding method is presented.

PNFP	- GB2481587 B 20160323
PR	- GB20100010797 20100628
AP	- GB20100010797 20100628
DT	- *, Rep
CT	- <i>// STSE (A B)</i> EP1804418 A1 20070704 [] (BEIJING WATCH DATA SYS CO LTD [CN]); WQ2010000455 A1 20100107 [] (VODAFONE HOLDING GMBH [DE], et al); WQ2007126227 A1 20071108 [] (MI RAE TECHNOLOGY CO LTD [KR], et al); WQ2007062787 A1 20070607 [] (VODAFONE HOLDING GMBH [DE], et al); US2008168544 A1 20080710 [] (VON KROGH CHRISTOPHER JURGEN [US]); US2007250923 A1 20071025 [] (M RAIHI DAVID [US]); US2007058812 A1 20070315 [] (ALI ASAD M [US], et al)
CCI	- G06F21/335 ; G06Q20/3229 ; G06Q20/385 ; H04L9/0872 ; H04L9/3228 ; H04L9/3234 ; H04L63/0838 ; H04W12/0602 ; H04W12/0608
CCA	- H04L2209/80
CI	- G06F21/335 (EP, US) - G06Q20/3229 (EP, US) - G06Q20/385 (EP, US) - H04L9/0872 (EP, US) - H04L9/3228 (EP, US) - H04L9/3234 (EP, US) - H04L29/06789 (GB) - H04L29/06795 (GB) - H04L29/06802 (GB) - H04L63/0838 (EP, US) - H04W12/06 (GB) - H04W12/0602 (EP, US) - H04W12/0608 (EP, US)
CA	- H04L2209/80 (EP, US)
PA	- (A B) VODAFONE IP LICENSING LTD [GB]
TI	- (A) Generating one-time passwords (OTP) using a mobile phone - (B) Authentication
AB	- (A) An arrangement for authenticating a transaction between a users mobile device 1 and an entity such as a corporate server 50 is disclosed. The Universal Integrated Circuit Card, UICC 20, (or Subscriber Identity Module (SIM)) of the users mobile device is adapted to generate a time-dependent authentication code (or one-time password (OTP)) which is dependent on a time value and which is usable to authenticate the transaction only during a predetermined period. The time value may be based on the coordinated universal time clock (UTC) obtained via the Internet 32 or a local clock (fig. 5A). A time verification processor 42 verifies the time value to ensure the authentication code was generated using the correct value. An authentication calculator 44 uses the verified time to generate the authentication code which is then used to authenticate the transaction. The mobile device may be operable to only generate the authentication code when the UICC is registered with a cellular telecommunications network .

4/4 © EPODOC / EPO

PN - [KR100824743B](#) B1 20080423

PR - KR20070129445 20071212

AP - [KR20070129445](#) 20071212

DT - I

CT - *// STSE (B1)*
[KR20040001207](#) A 00000000 [];
[KR20050071768](#) A 00000000 [];
[KR20060087804](#) A 00000000 [];
[KR20060102458](#) A 00000000 [];
[KR20070046337](#) A 00000000 [];
[US2007113269](#) A1 00000000 []

CI - H04W4/02 (KR)
- H04W12/06 (KR)
- H04W60/00 (KR)
- H04W88/021 (KR)
- H04W88/18 (KR)

PA - CHO IN SOOK [KR]

TI - METHOD FOR USER **AUTHENTICATION** USING MOBILE PHONE AND SYSTEM THEREFOR

AB - A method and a system for authenticating a user using a mobile phone are provided to improve convenience by performing an **authentication** if a received message is checked and a **mobile device** is connected to a call back URL(Uniform Resource Locator). A system for authenticating a user using a mobile phone includes a mobile communication **server**, a mobile **authenticationserver**, a financial **server**, and an **internet network**. The mobile communication **server** performs a wireless communication with a mobile phone, and has an **OTP**(One Time Password) function. The mobile **authentication server** has an **OTP** function, and includes a user database, a WAP(Wireless Application Protocol) **server** and an **authenticationserver**. The user database stores a mobile phone number, personal information, an identifier number and browser request head information of a data packet. The **authenticationserver** has a WAP gateway function and performs an **authentication** process. The financial **server** has an identifier of an automated teller machine and a database for a geographical position. The financial **server** controls an automated teller machine. The **internet network** performs an information exchange and a wireless communication between the mobile **authentication server** and the mobile communication **server**.