International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.31-40
http://dx.doi.org/10.14257/ijsia.2016.10.3.04

Secure Signature Authentication Algorithm in Mobile Internet

Hualin Sun[1]

[1]*Changzhou Institute of mechatronic technology, Changzhou 213164, China*
sunhualin021@126.com

Abstract

Mobile Internet can access to the Internet networkat anytime and anywhere, thus bringing convenient in the application. At the same time, it also brings the hidden trouble of safety certification, and reduces the cost of access, aiming at this problem, this paper proposes the authentication signature algorithm. This algorithm is based on domain alliance, which can effectively prevent attacks, so as to improve the safety and the stability of the system, and enhance its ability to deploy.

***Keywords**: Internet,Security, Authentication,Mobile Signature*

1. Introduction

With the rapid development of communication technology, mobile communication has become more and more mature. At the same time, the development of the information age leads to the continuous progress and perfection of the Internet. So the mobile communication and the Internet were combined, which the advantages are very obvious, but the combination of mobile communication and the Internet also has some disadvantages, and that is its security flaws[1-3]. Mobile communication and the IP of the traditional Internet continue to emerge from the risks and threats and make the mobile Internet is becoming increasingly unsafe. Therefore, the research of mobile internet security has become more and more urgent.

Internet security

With the continuous increase of service business, the diversification of network types, the intelligence of the network terminal, these have become an important component of the Internet.

Email, NFS, NDS, WINS, FTP and DHCP are service based on TCP / IP protocol, the IP protocol is an open performance, these services in terms of security defects has become more and more obvious, and TCP / IP protocol in attacks against the network itself has a certain fragility.

The continuous upgrading of applications and operating systems, managers often work, but when the kick down the patch, then it will produce new vulnerabilities and terminal network will also show on the safe side suddenly and uncontrollably. Also in order to enable more convenient access, when in the web site and web server access to, the visitor usually is not require certification, although this has brought convenience, but viruses and Trojans are more likely to take the initiative to attack network, network security is a great challenge. This is a security issue that is often the open architecture.

Through the malicious Trojan was implanted into the network, and then getting the user's information, remote attacks and cyber-crime. This has become a gray phenomenon in the political interests and economic interests driven. Through the research, we can get that the Internet is a security problem because it uses an open architecture based on IP protocol, which is mainly expressed in two aspects:

1) The concealment of visitor to the network. Relative to characteristicswhich the network has a very transparent to visitors, visitors to the network is very subtle, so it is difficult for visitors to monitor. When a large number of non-regulatoryauthentication of the visitor access network, the terminal's security capabilities and security situation is not controllable and cannot be seen. Visitors can have any false address, and it is difficult to trace the source.

2) Theopenness of network to visitors. Now the network is based on open IP framework, such that the opening can allow visitors free access to the IP address of the network nodes, and the network vulnerabilities to attack and scanning, the topology of the network is also very easy to de got by visitors. Visitors can get the data which needed in the arbitrary network nodes, and changes which need to be delivered, then the user's data cannot guarantee safety.

The security of mobilecommunication network

Before the Internet and mobile communications network integration, there are still some securities issues need to be addressed, such as the defects of one-way authentication. That is to say, only the authentication of the user, users on the network and no certified, so criminals can fake base station, to obtain the information of others, in addition, if data is only to be encrypted and protected, not tested, then the data once it has been tampered with, it is found. But 2G mobile communication network is relatively safe, because the access type of 2G network is compared with the single or support for CDMA, or support GSM, single network type makes authentication becomes more reliable. In addition, the 2G business is relatively small, the early mobile networks rarely have data services, the terminal can control the resource is very limited, mainly voice service. From the network architecture, which is also very closed, most network operators is to build their own proprietary network to transmit data, not through the public network transmission, so that by outside influence is very small. The control plane and the media surface are independent of each other, and the TDM is transmitted in a way that the control surface is not disturbed by the media. 2G mobile network terminal has no real operating system, so it is not easy to be infringed by virus. Because of the use of the authentication mechanism, they can also track the trajectory[4-6].

Compared to the 2G era, mobile communication network security issues become more prominent, which is mainly reflected in the following several aspects:

1) IP concept was introduced to the IMS network and security risks will become more and more large,the flat and high rate of LTE will increase the likelihood of an attack; the universal application of the intelligent mobile terminal, the risk of attack become more difficult to control; the diversity of applications and services are provided, which will inevitably lead to increased vulnerability, andincrease the 4G network security risks.

2) After applying tothe integration that interconnectionof mobile communication and themobilization of Internet communication network, the security of the network becomes more prominent. The type of access terminal continues to increase, the function of the processing is also strengthened, but the safety of muchapplication software is also changed. Access has become more diversified, such as mobile phones can be through the WiFi access network, and can also through a mobile communication network such as Internet access, mobile communication network can access the Internet via WAP, the increase in the number of network, rich bearing business, attacks the explosive growth, mobile payment and electronic commerce application sensitive business easier attacked.

3) Secure secret key length increased to 128 bit, certification by the one-way conversion for bidirectional, the data gives more stringent protection, application

playback sequence number to prevent attacks, which makes the future of 3G communication network security was strengthened.

In short, the convergence of the Internet and mobile networks, while maintaining the behavior can be traced, the inherent characteristics of the authentication, the security threat is becoming more and more serious.

2. Related Works

Information security research is mainly from the beginning of the security of military secrets, followed by the development of the demand ofnonmilitary areas and the development of technology. Western developed countries have already developed a strategy for national information security. Mobile internet security increases with the complexity of the environment and the factors of insecurity. Considering the intelligent terminal security situation, which including identity theft, mobile phone viruses and privacy *etc*. From the operating platform to consider, security issues, including information theft and denial of service, *etc*. From the service provider test rate, the main problem is not the security of business, malicious deductions and bad information dissemination. The characteristics of the mobile Internet makes it more secure than the traditional Internet security[7-9]. With the continuous development of telecom business, the number of mobile Internet users is increasing, and the level of user protection is also reduced. To accelerate the development of low-end smart phones, all terminal manufacturers launched a different system of smart phones, mobile internet terminal types have become more, the security flaw also increased. Due to the user has natural viscous, personal information has very high value, continuous expansion of payment and business office functions, carrying a huge commercial value, so threats than a computer user more serious[10-12]. IP processing of telecommunication network can make the closed network interconnection, but this also introduces the Internet's system vulnerabilities and security threats to the telecommunication network, which makes the security risk increased. The propagation properties n of the wireless signal transmission, which makes information eavesdropping, AP deception, illegal access and other security threats were increased. In the era of mobile Internet, cloud computing gradually into the server business, the characteristics of cloud computing multi-tenant, resource virtualization, dynamic scheduling makes the security problem of mobile Internet increase, fusion of sensor network and the mobile Internet in the Internet of things, the certification management brought challenges, increased demand for the new security.For existing mobile internet security issues, it has been proposed that the different security solutions, such as enterprise class security solving scheme, the terminal security solutions and network security solutions, but this scheme is not a very satisfied. In order to solve the problem of mobile internet security, many countries in the world have introduced some laws to restrict and regulate the related behavior. For example, Japan's "information network reliability benchmark" and the electronic signature ofthe America

Mobile Internet covers three aspects meaning, namely: terminal interconnection, network access, network services. But it cannot simply think that the mobile Internet is only a user access to the Internet through the mobile terminal, it is not dedicated to provide users with independent Internet network. It is the integration of the Internet and mobile networks and establishing the architecture and service system based on this. The mobile communication network, which is composed of the Internet and mobile communication, and should have some characteristics[13]:

1) The mobile Internet should inherit the characteristics of mobile communication, such as uniform authentication, complete network roaming, seamless coverage, *etc*.

2) The mobile Internet should inherit the advantages of the communication network in the security and performance, and provide the guarantee.

3) The Internet and mobile Internet should maintain a high degree of consistency in the application, content, and access.

As can be seen from Table 1,in terms of security requirements, the traditional Internet and mobile Internet are still very different. In the form of performance, the traditional Internet is open, free, and has access to the rich resources. Its open design principle determines that it is not necessary to authenticate on the traditional Internet, and it is difficult to operate. The protection of mobile Internet users and the user's privacy is muchstressed, therefore, the mobile Internet is very high security requirements. Until today, the mobile Internet in the mobile level and business applications still have a lot of security risks and vulnerabilities cannot be ignored. Along with more and more the terminal type, so it faces a more severe challenge.One of the advantages of mobile Internet is variety of the business applications, so the users of enjoyingthese services will inevitably receive all kinds of information, or in the experience and order some business applications to steal and reveal the user's information. But the traditional Internet terminal preventive mechanism is relatively mature, external threats through the firewall and antivirus software, internal risk through patches of business information and the terminal data protection, mobile Internet in this regard is the lack of mature technology.

Blending traditional Internet and mobile communication network, mobile Internet has great advantages, but also inevitably inherited the traditional Internet and mobile communication network security shortcomings. Traditional Internet continues to emerge from the risks and threats, mobile communication network IP to bring more security issues for mobile internet. If no longer be prevented and attention, mobile internet security issues will become increasingly serious.

Table 1. The Mobile Internet and Traditional Internet Security Comparison

	Mobile Internet security	Traditional Internet security
security hole	Similar to the traditional Internet	Traditional computer operating systems, network devices, applications have holes
DDOSattacking	Mobile Internet phone zombie software, such as BotSMS.sends junk software	Traditional Internet uses botnets to launch DDOS attacks which are difficult to prevent
malicious code	The viruses which according to various operating system have more than four thousand kinds	A large number of viruses, worms, trojans, botnets
information stealing	Mobile phones virus could become a bug, which can steal text messages, phone records, notepad content	A lot of Trojan can steal sensitive data, privacy and even state secrets
phishing	Through SMS cheat users to install malicious software and implement malicious order	Phishing site with network Trojan steal e-currency account, online games, illegal profit
malicious payment	Mobile service automatically with the function of billing, Internet, communication, malicious orders will be deduction, it has attracted many attentions of the grey economy	Difficult to direct deduction from the terminal, less dangerous

Due to the mobile Internet is the fusion of two kinds of network, its security problem is becoming more complex, related research of the security problems, "stratification research" method is generally adopted. Using common methods that security model usually could be divided into three layers of security model is analyzed, namely the business security, terminal security and network security. As shown in Figure 1.

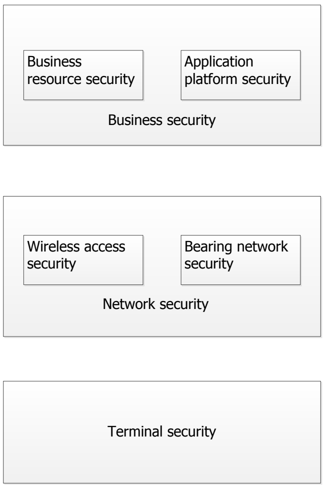

Figure 1. Mobile Internet Security Foundation Model

4) Network Security

The security problem of network layer: data confidentiality and data integrity is destroyed, illegal access. Denial of service attack, producing huge amounts of packet make network load, *etc*. In addition to using system vulnerabilities, bugs, sniffer tools to attack the network.

Either the early 2Gor 3G, the level of the mobile Internet access has a set of relatively complete security mechanism. The early 2G DAMPS based system and GSM system based on TDMA. This two kinds system have a big difference on the realization of security mechanism, but the same is that they have adopted based on the private key password system to share private data security protocols, the access of user authentication, data will be confidential.

5) Business Security

Business level is the major security threat: illegal access to data, denial of service attack, illegal access business, *etc*. And, of course, including the spread of unhealthy and garbage information, sensitive personal information leakage, unreasonable use of piracy abuse and content *etc*.

In view of the security issues, 3GPP has formulated the corresponding mechanism, such as the presence of business security mechanism, WAP security mechanism, mobile payment business security mechanism and the positioning business security mechanism, *etc*. And spam filtering mechanism, in view of copyright under the OMA DRM standard, *etc*.

6) Terminal Security

With the progress of technology and the development of mobile communication, the ability of memory and processor is more and more strong, and the degree of terminal intelligence is becoming higher and higher, and terminal operating system is becoming more and more open. The development and progress has also brought new problems of network security: illegal access, malicious code mischief, viruses, through the operating system free to modify terminal information and willfully distorting information. In order to make the terminal more secure, first of all, we should carry out the identity authentication of the mobile internet terminal, so that the terminal can have access control ability for various business applications and system resources. Identity authentication can guarantee the security of the system by means of password card, smart card, entity authentication and so on. Data on the terminal can be achieved through the establishment of access control to ensure the safety of the effect. In order to guarantee the security of the terminal internal data, it can be realized by using the method of hierarchical isolation, classification storage and data integrity detection.

3. Proposed Scheme

3.1 Three Elements of Mobile Internet Identity Management

Mobile Internet identity management system includes three elements: service provider SP, identity information provider IDP and mobile users USER.

The service provider SP is a provider that provides services for mobile users on the mobile Internet, which is an IDP user identity information consumer, it will provide a wide variety of services for users to use.

As the core of the mobile Internet identity management and information service provider, the identity information provider IDP can be used as a proxy for other users and trusted parties. On the one hand, IDP accepts authentication requests from the SP, the user's identity will be legitimate authentication, and SP will be related to the service provided to the user. On the other hand, IDP also provides the user with the corresponding identity services, such as user registration request is accepted, the user's identity information is verified. In particular, IDP provides trust level evaluation and provides information privacy for the user to assess the level of SP access to the user information management is realized.

Mobile telecom operators can be used as the user information storage which the reasonis:

1) Many SP cannot understand in the user side, as well as the user's own security concerns that user information can not be fully open.
2) The degree of dependenceto user information of mobile Internet business, and user demand for personalized, timely and high service experience, making user information open has become the key to the development of mobile Internet.
3) Mobile operators do not want to be bound by the pipeline.
4) Mobile operators have a large number of user resources, with a huge influence and reliable brand, then the user and SP will have a certain amount of trust.

3.2 A Mechanism for Realizing Virtual Identity Alliance

As global enterprises to participate in the field more and more widely, and other organizations of the increasingly close relationship. Therefore, it is necessary to develop a cross Internet domains or multiple security authentication system. This section will propose an effective solution for the virtual identity alliance, we will build the trust chain.

Scheme design:

There are two ways to achieve cross multiple domains landing system: one is the single point of the cross domain landing, the other is the single point of the union landing. Cross domain single sign on the use of security assertion markup language, through a policy agent to support single point landing. Alliance single point landing defines the identity Federation, in order to make a single point landing on the identity providers and service providers in multiple domains. The liberal alliance is a standard for many industry experts to support the implementation of a single point of landing and the implementation of the alliance to extend the security assertion markup language.

For the deployment of a non-alliance authentication platform in the network, cross domain single point landing requires more attention, this is because the developer does not know the token format. This section presents a trust chain of cross domain authentication system. It not only supports a non-alliance single point login domain and a coalition of single point login domain integration for a virtual identity alliance and non-alliance of the single point landing between security domains in the implementation of a virtual identity federation based on. This system does not require the relevant knowledge of the authentication platform and does not need to modify the old authentication platform.

1) Virtual Identity Alliance System

Virtual identity federation system between an alliance domain and non-alliance domain including: a trust proxy, a virtual server and based on anold token adapter in the non-union authentication system. This system will manage the new token and the old token. The new token is released by the virtual union server and accord to the form of alliance token. When the token adapter replaces the old token and manages the new token andthe mapping tableof old token, the user will receive a new token after the authentication center is recognized as a new token. When users access the application in the local domain, the old token will be replaced by the new token, and then the user will use the new token to access the union domain,

2) Token trust Chain is Established

Carrying out a single sign between a coalition and a non-alliance domain, a certain trust relationship must be established. In analliance single sign, the alliance server can use a KPI based signature or an interactive authentication protocol to authenticate a token that is issued by the authentication center in the other domain. In this scheme, the virtual alliance server and the local authentication center establish the trust relationship, and then establish the token trust chain. An efficient authentication protocol is used to validate the token and signature, signature token is not as the token and transfer, it can through other channels of communication to send, so that you can avoid to use the original agreement.

The new authentication protocol assumes that there is a secret key shared between the virtual server and the local certification center, the shared secret key has been through a distributed PKI secret key or shared symmetric secret key build manually. Assuming a symmetric secret key "Y" between the two trust agent pre shared, the agreement totally includes two stages: initial stage and token release stage.

a) Initial stage. In the beginning, the two trust agent through encrypted communication will exchange random secretseed "S"and symmetric key K. They are generated by random seed S to generate a Hash chain n $H^{(1)}(S),H^{(2)}(S),H^{(3)}(S),...,$

$H^{(n-1)}(S),H^{(n)}(S)$, where, $H^{(n)}(S)$is the $n-th$ Hass operation. For the first token, the token can be calculated by the following formula: $MAC = H\left(Token\|AgentID\|nH^{(n)}(S)\right)$.For the $n-th$ token, the token can be expressed as: $MAC = H\left(Token\|AgentID\|nH^{(n)}(S)\right)$. $AgentID$ isthe ID fortrust proxy, MAC as the signature, which will be sent from the local authentication center to the virtual identity federation server.

b) Token request phase. When a SSO token is requested, the token adapter will be from the local certification center request SSO token, local certification center will old sending the token to the token adapter, trust agent signature and identification of the token, the token signature are sent to a virtual server alliance trust agent. The old token will be sent to the virtual union server, and the trust proxy will be verified by the token. If the token is valid, the virtual union server will release a new alliance token to the token adapter. The new token is used in the identity federation. The new token will be sent to the user.

c) Seeds were randomly updated. When the Hass chain is carried out, the seeds must be updated to be updated for safety reasons. According to the security policy decision, two trust agents in order to update the random seed will repeat the beginning stage.

3) Token Management in Virtual Identity Federation

As shown in Figure 2, when the new token is received by the user, the token server will maintain a list of old and new tokens. When the local application is accessed by the new token, the new token will be sent to the authentication agent for confirmation. Token ring adapter will make old tokens instead of a new token, then the authentication proxy server forwarding confirmation message to the local certification center, the token is verified, the authentication agent will transmit the results to the application.

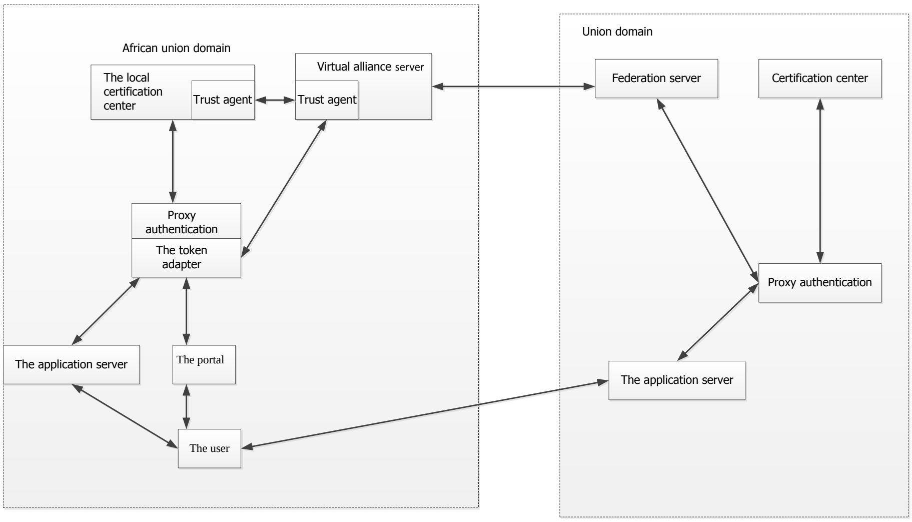

Figure 2. Token Management in the Virtual Identity Alliance

4. Experiment Results and Analysis

Virtual alliance servers are used to cross domain authentication and publish new tokens. The token adapter is installed with the authentication proxy for token management and token request. Trust agents between the virtual alliance server and the authentication center are used to build trust chain and verify old token. Two trust agents will share a symmetric key.

1) Initial stage. As shown in Figure 3， local authentication center (TA-LAC)generates a random number and uses the ID (AgentID1) and S to calculateMAC1, then the AgentID1, S and the MAC1 are connected in a string. With a shared secret key k to encrypt these valuesand they will be sealedin the message with amessageheader, such as: $MsgHeader\|E_k\left(AgentID1\|S\|MAC1\right)\|$ .This message is sent to the virtual server's trust

agent $(TA-VFS)$. $TA-LAC \rightarrow TA-VFS$: $MsgHeader\|E_k(AgentID1\|S\|MAC1)\|$ .After receiving the message, the virtual alliance server decrypts the message and checks MAC1. If it is legal, it will return a response which includes $MAC2=H(AgentID2\|S)$ .If the response is legal, so it will think the beginning was a success. $TA-LAC \rightarrow TA-VFS$ $MAC2=H(AgentID2\|S)$ $MsgHeader\|E_k(AgentID1\|S\|MAC2)\|$.

2) Requesting a single sign on the tokenprocess. As shown in Figure 4. The user is authenticated by sending the authentication material to the authentication agent. The local authentication center will post a new token for the user after the authentication is finished. When the trust agent in the local authentication center receives the token, the token is calculated: $MAC=H\left(Token\|AgentID\|n\|H^{(n)}(S)\right)$.The trust agents of the local certification center to send $MsgHear\|Token\|AgentID\|n\|MAC$ to trust agent. The signature MAC will be tested by the latter, if it is legal, then the signature and the token will be stored in a temporary table. When the trust agent in the virtual alliance server receives the old token from the token adapter in the authentication proxy, it will be verified by the temporary token table.

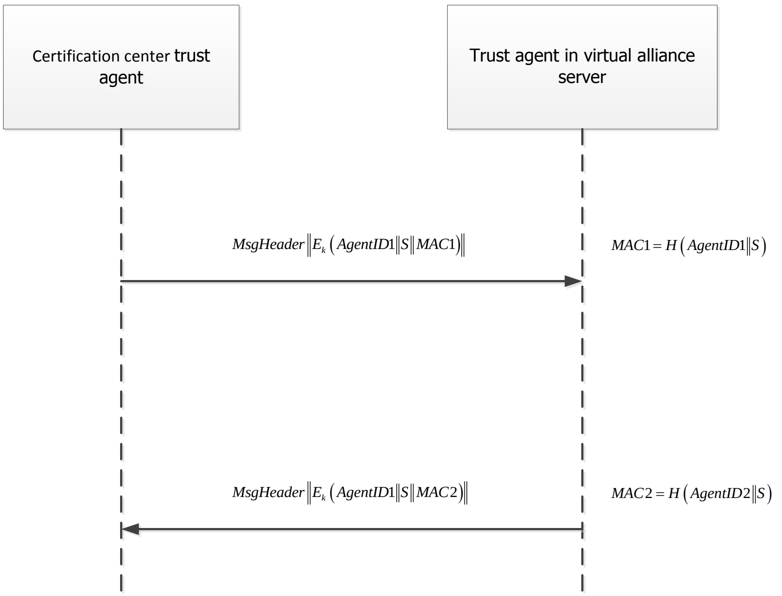
Certification center trust agent
Trust agent in virtual alliance server
$MsgHeader\|E_k(AgentID1\|S\|MAC1)\|$
$MAC1=H(AgentID1\|S)$
$MsgHeader\|E_k(AgentID1\|S\|MAC2)\|$
$MAC2=H(AgentID2\|S)$

Figure 3. Virtual Identity Alliance Initial Phase

5. Inclusions

In this paper, we design a trust agent, and established the trust relationship between the virtual server and the authentication center. Trust agent uses the sniff mode in the operation of the local center and got the token when sending, signature of the token is calculated with trust agent in the local certification center, and sends directly to the trust agent of virtual server alliance, so that the mobile Internet security based on of the virtual alliance identity authentication of token trust chain.

The token is authenticated by the trusted proxy of the virtual server, and a new token is issued after the authentication is completed.

Based on the key problems of mobile internet security authentication and related security application, this articleproposes a virtual alliance mechanism, through this mechanism, the security of the mobile Internet is improved, and the ability to deploy more robust.

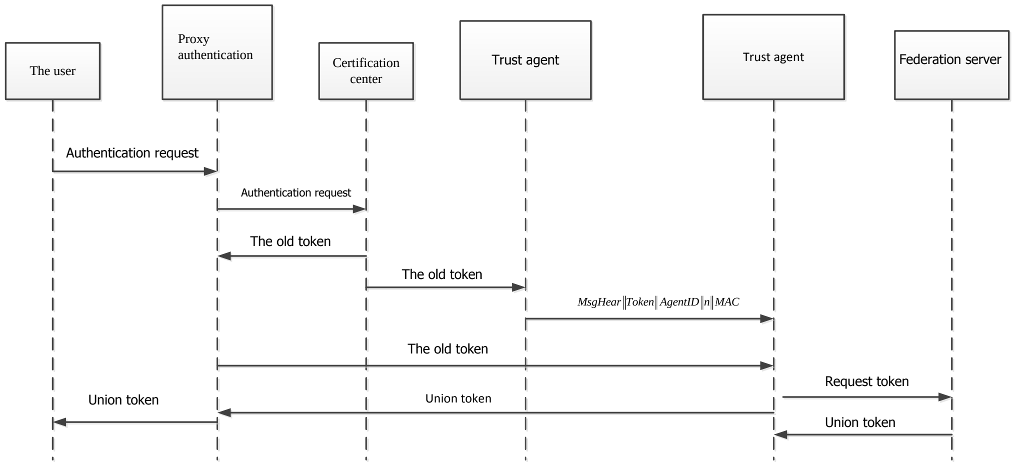

Figure 4. Single Sign Token Phase

References

[1] Z. C. Huang, P.P. K Chan, Ng W W Y, “Content-based image retrieval using color moment and Gabor texture feature”, Machine Learning and Cybernetics (ICMLC), 2010 International Conference on. IEEE, (**2010**), vol. 2, pp. 719-724.

[2] M. Arevalillo-Herráez, F J Ferri, S Moreno-Picot, “A hybrid multi-objective optimization algorithm for content based image retrieval”. Applied Soft Computing, vol. 13, no. 11, **(2013)**, pp. 4358-4369.

[3] G. G. Wan, Z Liu, “Content-based information retrieval and digital libraries”. Information Technology and Libraries, vol. 27, no. 1, **(2013)**, pp. 41-47.

[4] N. D. Thang, T Rasheed, Y K Lee, “Content-based facial image retrieval using constrained independent component analysis”. Information Sciences, vol. 181, no. 15, **(2011)**, pp. 3162-3174.

[5] P Järventausta, S Repo, A Rautiainen, “Smart grid power system control in distributed generation environment[J]”. Annual Reviews in Control, vol. 34, no. 2, **(2010)**, pp. 277-286.

[6] M E ElAlami. “A new matching strategy for content based image retrieval system”, Applied Soft Computing, **(2014)**, 14:, pp. 407-418.

[7] N Amoda, R K Kulkarni, “Efficient Image Retrieval using Region Based Image Retrieval”, International Journal of Applied Information Systems (IJAIS)–ISSN, **(2013)**, pp. 2249-0868.

[8] D. Liu, X. S. Hua, H. J. Zhang, “Content-based tag processing for internet social images”. Multimedia Tools and Applications, vol. 51, no. 2, **(2011)**, pp. 723-738.

[9] P. P. K. Chan, Z C Huang, W W Y Ng, “Dynamic hierarchical semantic network based image retrieval using relevance feedback”, Machine Learning and Cybernetics (ICMLC), 2011 International Conference on. IEEE, **(2011)**, vol. pp. 1746-1751.

[10] T. Furuya, R. Ohbuchi, “Visual Saliency Weighting and Cross-Domain Manifold Ranking for Sketch-Based Image Retrieval”, MultiMedia Modeling. Springer International Publishing, **(2014)**, pp. 37-49.

[11] A. Arampatzis, K. Zagoris, S A Chatzichristofis., “Dynamic two-stage image retrieval from large multimedia databases”, Information Processing & Management, vol. 49, no. 1, **(2013)**, pp. 274-285.

[12] R. Jin, G Yang, G. Agrawal, “Shared memory parallelization of data mining algorithms: Techniques”, programming interface, and performance”, Knowledge and Data Engineering, IEEE Transactions on, vol. 17, no. 1, **(2005)**, pp. 71-89.

[13] J. Ekanayake, G. Fox, “High performance parallel computing with clouds and cloud technologies”, Cloud Computing. Springer Berlin Heidelberg, **(2010)**, pp. 20-38.

Author

Hualin Sun, He received his Master’s degree in Technology of Computer Application from Southwest Petroleum University in Chengdu, China in 2008. He is Currently a lecturer in Changzhou Institute of mechatronic technology in Changzhou, China. His research interests include Software component technology, Image processing and algorithm,Cloud Computing, etc.