**Telecommunications and Information Exchange Between Systems**

# ISO/IEC JTC 1/SC 6

| | |
|---|---|
| **Document Number:** | 6N15797 |
| **Date:** | 2013-11-11 |
| **Replaces:** | |
| **Document Type:** | Text for DTR ballot |
| **Document Title:** | Text for DTR ballot of ISO/IEC 29181-5, Future Network: Problem Statement and Requirements - Part 5: Security |
| **Document Source:** | Project Editor |
| **Project Number:** | |
| **Document Status:** | As per the SC 6 Seoul resolution 6.7.4, this text is forwarded to JTC 1 Secretariat for DTR ballot. |
| **Action ID:** | FYI |
| **Due Date:** | |
| **No. of Pages:** | 15 |

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

# Title: Text for DTR Ballot of ISO/IEC 29181-5, Future Network: Problem Statement and Requirements - Part 5: Security

**Source:** Project editors (October 11, 2013)

**Project Editors:** Yadong Liu (ydliu915@vip.sina.com, China)
Wang Hao (wanghaonet@163.com, China)

**Status:**

This is the text for DTR Ballot of ISO/IEC 29181-5, Future Network: Problem Statement and Requirements - Part 5: Security, produced at the SC 6/WG 7 Chongqing Interim meeting in October 2013.
According to the resolutions 6.7.4, of June 2013 SC 6 meeting in Seoul, Korea, this text is scheduled for the DTR ballot processing after the SC 6/WG 7 Chongqing interim meeting.

ISO/TC /SC6 N 15797

Date: 2013-10-11

ISO-IEC TR 29181-5

# Future Network: Problem Statement and Requirements – Part 5: Security

Document type:

Document subtype:

Document stage:

Document language:

Contents Page

1. Scope ..... 7

2. Normative references ..... 7

3. Terms and definitions ..... 7

3.1 Future Network (FN) [ISO/IEC TR 29181-1] ..... 7

3.2 Net Space ..... 7

3.3 FN Space ..... 7

4. Abbreviations ..... 8

5. General ..... 8

5.1 Security environment in FN ..... 8

5.2 Related works on security in FN ..... 8

6. Problem statement of current network in security environment ..... 9

6.1 The existing problems and reasons of network security ..... 9

**6.1.1 Network users undertake the security risk and responsibilities** ..... 9

**6.1.2 Irregular Address and no truly proof for origin** ..... 9

**6.1.3 Central control may lead to security disaster** ..... 9

6.2 The current network security protection measures and effect ..... 10

**6.2.1 Current security protection means of common network user** ..... 10

**6.2.2 Current security protection means of professional users** ..... 10

6.3 Disadvantages of existing network security defense system ..... 11

7. The goal and requirements of FN security ..... 11

7.1 The goal of FN security ..... 11

7.2 The requirements of FN security ..... 11

**7.2.1 From passive defense to active management** ..... 12

**7.2.2 Replace computing confrontation with authentication technology** ..... 12

**7.2.3 Forming one to more system solution with authentication technology** ..... 12

7.3 FN security technical system....12

**7.3.1 Identity Authentication system**....12

**7.3.2 Platform security (Trusted Computing)**....12

**7.3.3 Secure connection and transmission**....12

**7.3.4 Application security**....12

**7.3.5 The functional requirements of FN security system**....12

8. Consideration of Key technology for FN security implementation....13

8.1 Support the real-name and anonymity authentication....13

8.2 Support large-scale application....13

8.3 Support end-to-end directly authentication and key exchange....13

8.4 Support management domain segmentation and cross-domain authentication....13

8.5 Simple structure, convenient use, low cost, and easy popularized....13

8.6 The application method to realize Identity Authentication....13

# Forward

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29181-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, Telecommunications and information exchange between systems.

ISO/IEC TR 29181 consists of the following parts, under the general title Future Network — Problem statement and requirements:

- TR 29181-1 - Part 1: General Aspects
- TR 29181-2 - Part 2: Naming and Addressing
- TR 29181-3 - Part 3: Switching and Routing
- TR 29181-4 - Part 4: Mobility
- TR 29181-5 - Part 5: Security
- TR 29181-6 - Part 6: Media Distribution, and
- TR 29181-7 - Part 7: Service Composition

# Introduction

This part of TR 29181 (Future Network: Problem Statement and Requirements) describes the problems of the current network and the requirements for Future Network in the security perspective. The general description on the problem statement and requirements for Future Network is given in the TR 29181-1. In addition, this TR 29181-5 establishes the problem statement and requirements for Future Network in the viewpoint of architecture and functionality for security support.

In general, network security includes information security and network's own security. Network security is concerned with hardware, software, basic communication protocol, network frame structure, communication mechanism factors of the network, and involving a wide range of many things. This report will focus on changing the security mechanism of network security from the perspective of the future.

This Technical Report may be applicable to the overall design of Future Network architecture.

# Future Network: Problem Statement and Requirements — Part 5: Security

## 1. Scope

This Technical Report describes the problem statements of current network and the requirements for Future Network in the security perspective. This Technical Report mainly specifies

- Problems of the current network in security environment; and
- Requirements for security support in Future Network.

## 2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC TR 29181 (all parts), Information technology — *Future Network: Problem Statement and Requirements ISO/IEC TR 29181*

## 3. Terms and definitions

For the purposes of this document, the following terms and definitions apply.

### 3.1 Future Network (FN) [ISO/IEC TR 29181-1]

The FN is the network of the future which is made on clean-slate design approach as well as incremental design approach. It should provide futuristic capabilities and services beyond the limitations of the current network including the Internet.

### 3.2 Net Space

Net Space is derived and expended from network. It indicates the new dimensional time-space system created by human with communication, computer and other information technology, which provides new space for human information activities (including information gathering, processing, storing, transmission etc.) and is becoming an ever important part of the survival and development environment for human society.

### 3.3 FN Space

FN Space will be the development and improvement of Net Space. It will be the main space for information

activities of human society and finally developed to the virtual world corresponding to and closely interacted with the physical world.

## 4. Abbreviations

| | |
|---|---|
| FN | Future Network |
| ID | Identifier |
| IP | Internet Protocol |
| TR | Technical Report |
| KMI | Key Management Infrastructure |
| PKI | Public Key Infrastructure |
| USB-key | Universal Serial BUS Key |
| IC card | Integrated Circuit Card |

## 5. General

### 5.1 Security environment in FN

For the FN, people have various assumptions. In all imagination there is one thing in common, that is the FN must be a reliable and secure network. It can provide reliable and effective support to a variety of political, economic, cultural, business and social activities for people, at the same time, provide security for the application and personal privacy as well.

In the FN, drawbacks of existing network security will be overcome, people don't have always to face the threat of net crime, because the new security system has made such a network environment in which all criminal behavior such as the wanton peeping and plunder of information, attacks etc, and network war simply cannot exist. Even if malicious activities happened, it will be detected and deterred immediately. The FN will realize "data security", "network security" and "application security". People can safely use the network to engage in all kinds of business and exchange information between each other at ease.

### 5.2 Related works on security in FN

In the framework of the current network, the communication protocol and the security protection means is impossible to meet the demand of FN security. Therefore to gain the FN security we must break through the limitations of the existing mechanism and system, to design a brand-new architecture, basic communication protocol and rules with new concept. So the construction of FN security system is not only a complicated and difficult system task but also a revolution of mechanism and system.

# 6. Problem statement of current network in security environment

## 6.1 The existing problems and reasons of network security

At the beginning of the development of network technology, since the network application range was small and in relatively closed environment, security problem was not so serious. As the ability of original computer and network equipment was very limited, it is very reasonable to use the limited resources to improve the basic function and convenience. The popularity of the Internet has brought a completely open application environment, which made the security a crucial problem. Because the original design has not systematically consider the security factor, now the only choice is to take remedial measures for security problems as mending holes in a clothes with patches. As time passed, although the system has become fully covered with patches, but the information security problem remained the same. At present, when a new virus appears on the Internet, the global 1.8 - 2 billions computers have to upgrade virus database and take new means for protection, that will consume a lot of resource and energy.

### 6.1.1 Network users undertake the security risk and responsibilities

The existing internet has no sufficient security mechanism. The network user has to undertake the security risk and protection responsibility. This congenitally deficient is the intrinsic reasons and restricts for the network security.

The current network operation is very similar to the postal system. As long as someone posted a letters or parcels, the post office will sent them to the recipient, regardless whether he is willing or not. The letter or parcels are expected to be opened and inspected by the recipient who assumed security responsibility. As long as a network user send e-mail or has the communicating requirements, regardless of the content of the message is good or bad, no matter whether it contains malicious acts, network system will deliver the mail , or establish communicating connection. As the network users generally have no ability for security judgment, they have to use security tools and services from the third party. But if the user cannot keep highly synchronization with the provider, he cannot respond effectively against net attacks with new means.

### 6.1.2 Irregular Address and no truly proof for origin

A big flaw in IP communication system is that IP address is irregular number. People only know he is communicating with an IP address but does not know with whom he is communicating, unless the communicator himself shows his identity, even if the network user knows the actual place of this IP address through query. Besides the existing IP protocol provides no proof for origin address, it cannot prevent illegal access.

### 6.1.3 Central control may lead to security disaster

Because the existing network control system applied the tree architecture with a single center, there is possibility to bring security disaster to the whole network once the control center fails or in trouble.

The above defects are the main causes for overflowing of viruses and Trojans and opening the convenient door for plundering information, low-cost attack and network crime. Network can even be manipulated to

wage net war, this is certainly not what the world people are willing to accept.

## 6.2 The current network security protection measures and effect

The existing network security protection system is a dynamic self information protection system, which is designed for private network and LAN, and for detection, response and recovery against network attack under the guidance of defense-in-depth strategy. Since there is no consideration about Internet as a whole, it is difficult to establish a stable, large-scale trusted system with interconnection, intercommunication, mutual trust and interoperability.

### 6.2.1 Current security protection means of common network user

Common network user:

Protection means：Firewall plus upgrading anti-virus software；

Protection methods: Very old comparison method；

This kind of protection means has congenital defects；

Firewall is the mostly used security device on the network. It can allow or restrict the data transmission according to certain rules. But it is also a computing device or an executive program in a computer, so it can't prevent threat by its vulnerability, cannot prevent the attack using defect in standard operating systems and network protocols. Firewall implements security strategy through open or closed some protocol and port but cannot prevent attacks using some permitted protocols and access port to the server (or computer); in addition it cannot prevent the file which is infected by the virus to be transmitted.

The existing anti-virus software applied typical one to one solution. When a Trojan or virus detected and analyzed, the virus feature code is taken and kept in virus-base followed by seeking out the virus killing method. Network user should constantly update anti-virus software to scan all executive programs and remove virus and Trojan whenever found with special tools.

The disadvantages of this approach are: First it can only detect knowing viruses which can be found only after being infected; secondly the new and upgraded virus increase continually and quickly, even breakthrough millions. The maintenance work of upgrading antivirus software and tools is arduous; thirdly finding and killing the virus will cost a lot of time and waste valuable system resources which greatly decrease the efficiency of the system.

### 6.2.2 Current security protection means of professional users

Professional network users:

Protection means：Encryption system plus third party certificate and

Defense system based on risk management;

Protection method：Date encryption, Digital signature and

Detection and response;

Professional network protection system is built on two bases: key management infrastructure / public key infrastructure (KMI/PKI) used in the production, distribution and management of keys and security certificates, as well as the infrastructure for the early warning, detection, identifying of possible network attacks, make effective response by investigation and analysis of aggressive behavior. The former focuses on issues of information authenticity and security, the latter mainly focuses on network security problem. Because these two factors are relatively independent, it is difficult to support each other or share resources.

### 6.3 Disadvantages of existing network security defense system

The current network security protection system is based on passive defense strategy and completely gave up the initiative. There are three major disadvantages in it：

- Losing of initiative and the effective reaction ability against attack
- Attacker always has the absolute advantage with same level of computer technology
- One to one solution to each threat caused the complexity of system and black hole of cost

The above three points have determined the existing security system is built on the premise of the failure, it can only improve the safety probability and cannot provide security guarantee.

The final and the only way are to design a new system with security mechanism.

## 7. The goal and requirements of FN security

### 7.1 The goal of FN security

FN is a common subject explored by global scientific community.

FN is not only a technical network but also a social network. It is a new dimensional time-space system (Net Space or FN Space) created by human with wisdom and technology. It will become the main bearing space for information activities of human society, and the virtual world corresponding to and interacted with the physical world. Therefore, the FN security system should be a comprehensive system oriented to social management, which includes security, trust and management functions in one. It is the extension of the national and social security system of the physical world to Net Space. In the premise of Net Space integrity and order, it should design a brand-new security mechanism, architecture, basic protocol and rules with new concept, and provide technical support to safeguard national sovereignty and the right of management, guarantee the legitimate rights and freedom to engage in information activities for individuals and groups, under the law frame and give them the ability to protect their information security.

### 7.2 The requirements of FN security

In the FN, all the entities in the physical world will be expressed as abstract Identity which is the same to both Net Space and FN Space. Set up the proving relationship between identity and entity and guarantee

the authenticity of identities with authentication technology is the foundation and precondition of future network security. On the basis of above the following necessary works should be done:

### 7.2.1 From passive defense to active management

With the help of identity authentication system, the whole security system will be established on strict identity authentication management basis and achieved the transformation from passive defense to active management.

### 7.2.2 Replace computing confrontation with authentication technology

Replaces computing confrontation with authentication (the core is crypto technology) completely changes the premise of security.

### 7.2.3 Forming one to more system solution with authentication technology

Unifying the security strategies and methods on the authentication technology, form a one to more system solution, greatly reduce the construction and maintenance cost, and gain initiative.

## 7.3 FN security technical system

FN security technical system is based on identity authentication system and consists of platform security (Trusted Computing), secure connection and application security.

### 7.3.1 Identity Authentication system

By constructing authentication infrastructure to Issue electronic ID cards for each subject (including people and things) which gave them the ability for digital signature and key exchange.

### 7.3.2 Platform security (Trusted Computing)

Through digital signature and authentication for each executable program, prevent the Trojan virus and other illegal program from loading and execution to ensure the security of computing platform;

### 7.3.3 Secure connection and transmission

Changing after-verifying to pre-authenticating communication rules, and through pre-authenticating and encrypting the transmission content, ensures the trusted connection and the security for transmission content.

### 7.3.4 Application security

Authentication system will be embedded into the application system to achieve application security.

### 7.3.5 The functional requirements of FN security system

- No limitation for the scale and architecture of security system. On prerequisite of standardization, it can meet the requirement to construct secure network information system crossing countries, sectors, and systems;

- Cell level security. People, equipment, device and even software process will be a security unit, which can be used to construct any scalable cell level independent security system;
- Private secret service. With the help of digital signature and key exchange ability, which is provided by identification authentication system, anyone can enjoy privacy and share information with each other securely;
- Simple and efficient. Through constructing of standardized public authentication infrastructure to minimize the cost for construction, maintenance, operation;

## 8. Consideration of Key technology for FN security implementation

Because the trust of identity is the base of FN security, the identity authentication system that can directly generate public-private key pair from identity, and support direct authentication is the key technology. In order to establish an integrated system that can support global trusting environment, the Authentication System should meet the following conditions:

### 8.1 Support the real-name and anonymity authentication

Support the real-name and anonymity authentication to match the current social management system and meet the cognitive habits of people and society;

### 8.2 Support large-scale application

Able to support global or large-scale application, to meet social requirement;

### 8.3 Support end-to-end directly authentication and key exchange

Support end-to-end direct authentication and key exchange, can provide technical support for the new generation of security system;

### 8.4 Support management domain segmentation and cross-domain authentication

Support management domain segmentation and end-to-end direct cross-domain authentication in order to meet the requirements for sovereignty and the management right of different countries, regions, units etc. and the need to build a large globalized security system;

### 8.5 Simple structure, convenient use, low cost, and easy popularized

### 8.6 The application method to realize Identity Authentication

Identity Authentication System is the core of FN security, its basic function will be achieved through distribution and embedding. The distribution is to distribute key device containing authentication system and identity key (can be encapsulated into a variety of forms such as USB-key, IC card, wireless devises etc.) to each person or piece of equipment. The embedding is to embed the authentication system into a variety of

devices and applications through standardized interfaces to achieve security function.