

A Study on the Policies and Regulations of Cyber Electronic Identity Management

Zou Xiang¹, Hu Chuanping¹, Fang Binxing², Chen Bing¹

1. The Third Research Institute of the Ministry of Public Security of the PRC, Shanghai 200031, China

2. Cyber Security Association of China, Beijing 100010, China

Abstract: This paper analyzes and describes the policies, laws, and regulations of cyber electronic identity management in major countries, regions in foreign countries, and China. It discusses the development of China's cyber identity management, and outlines the 13th Five-Year Plan's policies and regulations for cyber electronic identity management in China, including the development of ideas and constructive suggestions, the strengthening of cyberspace identity management, and the construction of a cyberspace identity management system. In this way, we hope to provide a reference for policy changes in the development of China's cyber identity management regulations during the 13th Five-Year Plan period.

Keywords: cyber electronic identity; identity management; policies and regulations

1 Introduction

Cyberspace has become the fifth strategic domain, after land, sea, air, and space. As General Secretary of the CPC Central Committee Xi Jinping pointed out: "if there is no cyber security, there will be no national security." Cyberspace security has risen to become a national security strategy. Cyberspace identity management is an important foundation for constructing a credible cyberspace, and directly affects the security of that cyberspace. The US and other western countries attach great importance to cyberspace identity management; just a few years ago, the US decided on cyberspace identity management as one of its national cyber security strategy, and made efforts to strengthen the overall planning and accelerate the deployment of this implementation. At present, the development of China's cyberspace identity management lags behind that of some western countries. If China does not speed up its top-level design and infrastructure construction from a strategic perspective, it will seriously threaten China's national security and cyberspace security.

Therefore, this paper analyzes and comprehensively combs through the policies, laws, and regulations related to cyber electronic identity (eID) management that is in place in major countries and regions around the world. We examine China's cyber eID management development situation and put forward development ideas and constructive suggestions for the 13th Five-Year Plan regarding relevant policies and regulations. In this way, we hope to provide a reference for policy changes in the development of China's cyber eID management regulations during the 13th Five-Year Plan period.

2 Cyber eID management policies and regulations in major foreign countries

In today's world, social interactions are inextricably linked with the Internet. In addition, the cyberspace security situation is becoming increasingly grim, which makes safeguarding national security, social stability, commercial credit, and electronic transaction security greatly challenging. Many countries around the

Received date: 10 September 2016; **Revised date:** 20 September 2016

Corresponding author: Zou Xiang, The Third Research Institute of the Ministry of Public Security of the PRC, Researcher. Major research fields include cyber security and big data application. E-mail: xzou@eid.net.cn

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 023-027

Cited item: Zou Xiang et al. A Study on the Policies and Regulations of Cyber Electronic Identity Management. *Strategic Study of CAE*, <http://10.15302/J-SSCAE-2016.06.005>

world have been carrying out large-scale strategic deployment and implementation of cyberspace identity management. The following discussion focuses on the European Union (EU) and its member states, the US, and Asia as represented by South Korea and Japan.

2.1 The EU and its member states

The EU uses the cyber eID as an implementation method of cyber identity management [1]. The EU's construction of policy and regulation systems ensures the effective implementation and promotion of the eID. This includes emphasizing top-level design at the strategic level, laying emphasis on privacy rights and the free cross-border flow of personal data, establishing the legal status of the electronic signature, maintaining the eID in cross-border operations and ensuring its credible service, and establishing eID law [2,3].

2.1.1 Determining top-level design from a strategic planning level

Since the year 2000, as described in the i2010 Strategy, the European e-Government Action Plan 2011–2015, and the Europe 2020 strategic plan, the European Commission has been planning to implement the eID across the EU, and has also proposed the construction of a unified management framework for the eID on a pan-European level. Thus far, more than 100 technical standards related to cyber identity management in the EU have been set. These include: basic technical standards for electronic signature algorithms, signature equipment, and signature generation; credible service standards for time stamps and credible authentication service; and cross-border interoperability standards.

2.1.2 Emphasizing personal data privacy and free cross-border data flow

The EU promulgated an instruction on the free flow of personal data in 1995, describing its action as the protection of personal data privacy. EU member states should emphasize the protection of the fundamental rights and freedoms of the individual, with a particular focus on the processing of personal data privacy. Member states should not restrict or prohibit the free movement of personal data for any reason. In 1997, Germany promulgated the Information and Communication Services Act; in 2002, it promulgated the Federal Data Protection Act and then revised this Act in 2006, thereby adding more user data protection.

2.1.3 Establishing the legal status of an electronic signature

In 1999, the EU issued a directive on the establishment of a community legal framework for electronic signatures, and thereby established a legal framework for electronic signatures and certification services. The main goal of this framework is to

promote the development of the domestic market for electronic signatures within EU countries, to ensure the legal status of an electronic signature, and to create a suitable environment for activities related to e-commerce. In 1997, Germany promulgated the Digital Signature Law, and in 2001, it published the Legal Framework of Electronic Signatures, which established national legislation for the strong protection of citizens' electronic signatures.

2.1.4 Specifying the cross-border operation of electronic identities and credible services

In 2006, the EU promulgated Directive 2006/123/EC on services in the internal market, and in 2014, it promulgated a regulation on electronic identities and credible services for electronic transactions in the internal market. This regulation ensured that business personnel within the EU member states can develop public service transactions with their eID in other member states. It also created a credible European electronic service market, including electronic signatures, electronic seals, time stamps, electronic file transfers, web authentication, and so on. Finally, it ensured that countries involved in cross-border eID transactions operate with the same legal status. The supporting policies include provisions for and resolutions on the implementation of the eID and credible electronic services.

2.1.5 Establishing eID law

In 2009, Germany promulgated the Act on Identity Cards and Electronic Identification, and thus developed an overall legal framework for the cyber eID in order to establish an identity management system (IdMS) for online authentication. The Act included all aspects of the implementation of eID constraints in Germany. In 2010, Germany promulgated eID regulations, thus clearly defining the new generation of German eID card infrastructure security and data protection requirements. In 2010, Germany promulgated regulations on the provisions of eID card fees and calculation formulas.

2.2 The United States

The construction of cyber eID management policies and regulatory systems in the US ensures the effective implementation of all aspects of cyber eID management and promotion, including management and promotion at the national strategic level, the legal status of electronic signatures, cyber security and information safety, and personal cyber identity authentication [4].

2.2.1 Attending to top-level design from the national strategic level

In April 2011, the US promulgated a national strategy to establish credible identities in cyberspace over a period of about 10 years. The goals of this strategy are to build a cyber identity ecosystem and to promote the use of safe, efficient, and easy-to-use identity solutions for individuals and organizations in

cyberspace. This strategy seeks to establish dominant power and control over cyberspace, and aims to lead the new trend in the world's economy through the prosperity of its cyber economy—the global economic ground of the future.

2.2.2 Establishing the legal status of an electronic signature

In 2000, the US enacted the Electronic Signatures in Global and National Commerce Act, thus giving equal legal status to an electronic signature and a handwritten signature, and dealing with the legal obstacles to using electronic signatures.

2.2.3 Emphasizing cybersecurity and information security

In 2002, the US announced the Federal Information Security Management Act, and in 2009, it promulgated the Cybersecurity Act of 2009. Thus, the US established an overall system framework for federal information system security, specified management responsibility, and stressed the importance of cyber security and information security.

2.2.4 Focusing on personal cyber identity authentication

In August 2004, the US issued its twelfth homeland security presidential directive (HSPD-12). This directive provided a new standard strategy of identity management for government departments to manage the secure identification of federal employees and contract employees. In response to HSPD-12, the National Institute of Standards and Technology (NIST) issued a federal information-processing standard designed for government employees and contractors, in order to establish personal identity verification (PIV) standards. This standard defined the technical requirements and framework and identified all standards used for federal identity recognition systems.

2.3 South Korea and Japan

In South Korea and Japan, cyber eID management policies and regulations regarding electronic (digital) signatures, authentication services, personal information protection, and so forth, have effectively promoted the application of cyber eID management [4].

2.3.1 Establishing the legal status of an electronic (digital) signature

In 1997, South Korea presented the Basic Act on Electronic Commerce (which came into force in 1999). This Act included the definition of digital signatures and other basic concepts, and defined the effectiveness of communication information. In 2000, Japan promulgated the Law Concerning Electronic Signatures and Certification Services, which covered the legislative principles, purposes, types, and status of electronic signatures; punishment for electronic-signature-related crime; and other related aspects.

2.3.2 Establishing the legal status of certification services

As noted earlier, Japan promulgated the Law Concerning Electronic Signatures and Certification Services in 2000, thus establishing the legal status of certification services, recognizing electronic instructions issued by foreign authorities, and establishing the punishment for crimes related to electronic certification services.

2.3.3 Protecting personal information

The Basic Act on Electronic Commerce in South Korea included detailed provisions regarding various aspects of personal information security, such as the collection, disposal, transmission, and storage of such information. In 2003, Japan promulgated the Act on the Protection of Personal Information, which established the proper handling of personal information, along with basic principles on the protection of personal information. This Act was aimed at clarifying the responsibilities of national and local government regarding personal information protection, and establishing strong protection for personal information.

3 China's cyber eID management policies and regulations

China's cyber eID management policies and regulations establish preliminary progress in electronic (digital) signatures and the cyber real-name system, and strengthen the protection of electronic information [5].

3.1 Establishing the legal status of an electronic signature

In April 2005, China promulgated the Electronic Signature Law of the People's Republic of China, establishing that a reliable electronic signature has the same status as a handwritten signature or seal, and validating the legal basis of an electronic signature. In 2000, the Hong Kong Special Administrative Region of China issued the Electronic Transactions Ordinance, establishing the validity of electronic contracts and digital signatures, and clearly focusing on digital signatures generated by asymmetric cryptography technology.

3.2 Developing cyber real-name regulations

From 2005 to 2013, the Ministry of Education of the People's Republic of China issued Suggestions for Further Strengthening the Management of Campus Networks at Colleges, and initiated the implementation of the cyber real-name system in college education networks. The Ministry of Information Industry of the People's Republic of China issued a Non-operating Internet Information Service Management Approach, which prescribes that non-operating sites need to register for non-operating Internet information services; the State Administration for Industry

& Commerce of the People's Republic of China issued the Interim Measures for the Administration of Cyber Behavior of Commodity Transaction and Related Services to implement a policy commonly referred to as "online stores' real names;" the Ministry of Culture of the People's Republic of China issued the Interim Measures for Online Games Management to practice a policy commonly referred to as "online games' real names;" the Ministry of Finance of the People's Republic of China issued the Interim Measures for Online Lottery Sales Management to carry out a policy commonly referred to as "lotteries' real names;" the Ministry of Industry and Information Technology of the People's Republic of China issued the Regulations on Registering the True Identity of Telephone Subscribers, which requires users to register when they handle business for fixed-line telephone and mobile telephone (including wireless network cards) [6–11].

3.3 Strengthening the protection of personal cyber information

In December 2012, the National People's Congress (NPC) Standing Committee deliberated the National People's Congress Standing Committee Decision Concerning Strengthening Cyber Information Protection (hereinafter referred to as Decision) that had been passed through the Council of the Chairman. The legislative purpose of the Decision is to protect personal cyber information such that it will not be leaked, tampered with, or abused. The vice director of the Legislative Affairs Commission of the NPC Standing Committee, Li Fei, noted that the Decision emphasized that the state should protect electronic information that identifies a citizen's personal identity and is related to the privacy of the individual. In addition, the state should give rules to network service providers and other enterprises and institutions for the collection and use of personal information, and regarding their obligations to protect personal electronic information. The relevant government departments and their staff members should have the same duty of confidentiality and protection in order to protect the personal information of citizens as the government performs its function [12].

4 Thoughts and suggestions for cyber eID management policies and regulations in China

Based on an analysis of the cyber eID management policies and regulations of the major countries discussed above, combined with China's national conditions, we put forward the following suggestions for the construction of China's cyber eID management policies and regulations.

First, we suggest that attention should be paid to top-level design from the national strategic level, including clear legal support for cyber eID. We should study and determine legislative demands, including increasing the emphasis on the fact that an eID signed by China is a trusted source of citizens' electric

identity in the Cyber Security Law of the People's Republic of China, and formulating an act on cyber electronic identity card.

Second, we suggest that the promotion of the formulation of cyber identity management laws and regulations should refer to current mechanisms of social identity management, according to different scenarios in which an eID card might be applied. In real life, people need to be able to verify their true identity while on a plane or train, in a hotel, using bank accounts or securities accounts, and in other situations related to personal safety and public security. In such situations, people should show a citizen identity card issued by the public security department. However, while shopping, eating at restaurants, visiting attractions, watching movies, and carrying out other activities like these, people do not need to verify their real names. In fact, cyberspace is very similar to real life in this aspect: All the different kinds of Internet applications can be divided into three categories. The first category requires real-name registration so that people use their real name. The applications in this category are used in situations that involve financial security, personal property security, and public security, which always require identity authentication; examples of such activities include large-scale electronic commerce, financial transactions, and personal online government public services to individuals. The second category requires anonymous registration of real names, and includes applications such as online games, e-mail, and other similar applications. In situations in this category, people may not want to appear using their real name; however, if an account number is stolen or lost, authentication is needed to retrieve the account or other virtual property. The third category requires anonymous registration only, and includes activities such as Internet browsing. For cyber operations containing a range of activities or a range of cyber identity management levels, the user's wishes and business needs should determine the level of anonymity, and such decisions should be recognized and accepted by the public.

Third, we suggest that the purpose of developing cyber identity management laws and regulations should stem from national and civil rights and interests. Within the environment of the Internet, people need to provide different account names and passwords in order to use different Internet applications. As they apply for each account, they must submit their relevant personal information, which will lead to privacy leakage. Therefore, it is necessary to establish and perfect a legal system and enforcement mechanism that will protect personal information. It is also necessary to strictly regulate the scope and methods of using identity information to prevent users from submitting a link to personal information when acquiring an account, thereby reducing the risk of loss of privacy, avoiding identity theft and the misuse of identity information, and effectively ensuring the protection of personal privacy. In the implementation of digital identity management strategies, each country has attached great importance to the establishment of a sound legal framework for the protection of personal information and of effective legal

enforcement mechanisms. The US and EU member states have adopted strict privacy policies that require a service provider to complete a privacy protection design and risk assessment on a technical level each time it collects, uses, and discloses users' information.

Fourth, we suggest that the process of establishing cyber identity management laws and regulations should give full play to the role of the parties. In the case of the US, which released a national strategy for its cyberspace in 2011, credible identity authentication is defined as a kind of market service activity; not only can it satisfy the demands of enterprises and users for cyber security and privacy protection, but it can also meet the needs of market supply. In the cyber identity ecosystem, individual users, service providers, and the government all play important roles, and will restrict and influence each other. The market mechanism dominates the normal operation of the system, and government plays a leading, coordinating, and integrating role. China's cyber identity management laws and regulations should reflect the rights, obligations, and responsibilities of the entities of state and society.

References

- [1] Identity management [EB/OL]. (2016-09-02) [2016-09-10]. http://en.wikipedia.org/wiki/Identity_management.
- [2] European Commission. i2010—A European information society for growth and employment [R/OL]. Brussels: Communication department of the European Commission. (2005-06-01) [2016-09-10]. http://europa.eu/rapid/press-release_MEMO-05-184_en.htm.
- [3] European Commission. A roadmap for a pan-European eIDM Framework by 2010 [R/OL]. Brussels: Communication department of the European Commission. (2010-02-01) [2016-09-10]. <http://www.statewatch.org/news/2008/jul/eu-com-eidm-roadmap-paper.pdf>.
- [4] Hu C P, Zou X, Yang M H, et al. Global network identity management: Current status and development [M]. Beijing: People's Posts and Telecommunications Press, 2014. Chinese.
- [5] Cyber Real-name system [EB/OL]. (2015-05-22) [2016-09-10]. <http://baike.baidu.com/view/731760.htm>. Chinese.
- [6] Ministry of education of the People's Republic of China, Central Committee of the Communist Youth League. Opinions on further strengthening the management of campus network in colleges and universities [EB/OL]. (2010-05-23) [2016-09-10]. http://www.ssbgzzs.com/txt/2010-05/23/content_3525176.htm. Chinese.
- [7] Shenzhen Public Security Bureau Network Security Supervision Branch. Notice on carrying out the work of cleaning up and rectification of public information service sites in the network [EB/OL]. (2005-07-20) [2016-09-10]. <http://news.qq.com/a/20050720/001544.htm>. Chinese.
- [8] Ministry of Culture and the Ministry of Information Industry of the People's Republic of China. Some suggestions on the development and management of online game [EB/OL]. (2005-08-04) [2016-09-10]. http://www.gov.cn/jrzg/2005-08/04/content_20403.htm. Chinese.
- [9] State Administration for Industry and Commerce of the People's Republic of China. Interim Measures for the administration of online commodity trading and related services [EB/OL]. (2010-06-01) [2016-09-10]. http://www.gov.cn/gzdt/2010-06/01/content_1618532.htm. Chinese.
- [10] Ministry of Culture of the People's Republic of China. Interim measures for the administration of online games [EB/OL]. (2010-06-22) [2016-09-10]. http://www.gov.cn/flfg/2010-06/22/content_1633935.htm. Chinese.
- [11] Ministry of Finance of the People's Republic of China. Interim measures for the administration of Internet sales of lottery tickets [EB/OL]. (2010-10-09) [2016-09-10]. http://www.gov.cn/fwxx/sh/2010-10/09/content_1718158.htm. Chinese.
- [12] Member of the Standing Committee of the National People's Congress. Decision on strengthening the protection of cyber information [EB/OL]. (2012-12-29) [2016-09-10]. http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm. Chinese.