

Development and Application of Cyber Electronic Identity Management in Global Regions

Hu Chuanping¹, Chen Bing¹, Fang Binxing², Zou Xiang¹

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 study analyzes and elaborates the latest developments in and typical applications of cyber electronic identity management in major global regions, including China. In addition, it also presents a 13th Five-Year Plan for cyber electronic identity management in China, detailing the development of ideas and constructive suggestions that aim to strengthen China's cyberspace identity management and support the construction of this system. Such a system can help regulate the behavior of Internet users, fight against cyber crime, build cyber power, safeguard national security and cyberspace sovereignty, and protect the privacy of Internet users. Furthermore, this study can serve as a reference for the development of China's cyberspace identity management while the 13th Five-Year Plan is implemented.

Keywords: cyber electronic identity; identity management; digital signature

1 Introduction

In recent years, the issue of Internet anonymity afforded to users has become increasingly serious, leading to the loss of Internet integrity and frequent occurrence of illegal criminal activities. Consequently it has become an important factor that affects national security and social stability. Therefore, the Internet real-name system [1] has become a crucial management technique with its increasing popularity in cyberspace. In 2014 and 2015, the Office of the Central Leading Group for Cyberspace Affairs made Internet real-name system one of its key agendas. However, due to lack of effective technical support in this mechanism, Internet users are required to submit personal identity information to service institutions. This process has contributed to a large number of online identity information leaks.

Consequently, this study analyzes and systematizes the latest developments in and typical applications of global cyber electronic identity management, particularly in China. Furthermore, we discuss the development of ideas and constructive suggestions in order to strengthen cyber electronic identity manage-

ment, and the construction of a system thereof, through the presentation of a 13th Five-Year Plan. In addition, these ideas and suggestions aim to help regulate the behavior of Internet users, fight against cyber crime, build cyber power, safeguard national security and cyberspace sovereignty, and protect the privacy of Internet users. This would then aid in accomplishing the 13th Five-Year Plan objectives, while also providing a reference for China's cyber electronic identity management development during this period.

2 Development and application of cyber electronic identity management in major countries and regions

Major countries and regions have been vigorously promoting cyberspace identity management [2]. Most of them already use the cyber electronic identification (eID) cards as their landing method. The technology implementation uses a public key infrastructure (PKI) system based on a digital (electronic) signature, which is the core component of the asymmetric cryptographic algorithm.

Received date: 10 October 2016; **revised date:** 18 October 2016

Corresponding author: Hu Chuanping, The Third Research Institute of the Ministry of Public Security of the PRC, Director and Researcher. Major research fields include network security and big data applications. E-mail: chenbing@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): 099–103

Cited item: Hu Chuanping et al. Development and Application of Cyber Electronic Identity Management in Global Regions. *Strategic Study of CAE*, <http://10.15302/J-SSCAE-2016.06.020>

2.1 Development of cyber electronic identity management in major countries and regions

2.1.1 The European Union (EU)

The European Commission led the implementation of various projects, plans, strategies, public laws, and regulations on the interoperability of European electronic identity management. The EU issued a community framework for electronic signatures in 1999 that established the technical route of cyber electronic identity management. Since 2000, as part of the i2010 strategy, the European e-Government Action Plan 2011–2015 and the Europe 2020 strategic plan established and improved the identity management system, covering the entire EU as a key task. Currently, 16 of the EU's 28 member states have implemented eIDs based on electronic signature technology, with 150 million eIDs issued within the EU. Through the construction of this system, EU countries not only realized cyber identity and authentication in their countries, but also EU cross-border identification and trusted services. For instance, Estonia is one of the world's most digitally advanced countries with 600 citizen electronic services and 2 400 enterprise electronic services. These services span the Internet, including e-government, e-banking, online shopping, online medical care, online contract signing, and electronic voting fields. Furthermore, they have already begun to issue visas embedded with eIDs to foreigners [3,4].

2.1.2 The United States

In 2011, the United States issued the National Strategy for Trusted Identities in Cyberspace (NSTIC), which aims to establish a nationwide cyber identity ecosystem with standards for individuals, institutions, and other types of entities under the unified mutual authentication process. In a span of about 10 years, it plans to build a cyber identity ecosystem, promote personal and organizational security, and provide efficient, easy-to-use identity solutions on the Internet. The United States government suggested the private sector's operation of this ecosystem. While the government efforts are still in the early stages, it has already completed a demonstration application for guidance and protection. The NSTIC has also adopted a technical route based on e-signatures [5]. In 2014, Pennsylvania, Michigan, California, and other states began to carry out online authentication, online testing of related bills, and other related work in the fields of e-commerce, residents, health, online education, and others.

2.1.3 Asian and Latin American Countries

In recent years, many countries in Asia and Latin America have also built cyber identity management systems with related infrastructure. For example, since 2003, the United Arab Emirates government has been constructing a national key infrastructure that issues eIDs based on citizens' electronic signatures, used mainly for online payment, file signatures, notarization, electronic voting, and other services. Peru has also implemented the Na-

tional Registry of Identification and Civil Status (RENIEC) project, which issues eIDs based on electronic signatures for online identity authentication in national elections, and in the banking and public sectors. In addition, it has also implemented electronic seals that can be used to authenticate enterprises on the Internet.

2.2 The United Nations “seminar on legal issues related to identity management and trusted services”

In April 2016, the United Nations Commission on International Trade Law (UNCITRAL) held a seminar in Austria on the legal issues of identity management and trusted services. More than 200 representatives from more than 50 countries attended the seminar. It discussed the work of North and South America, the United States, the EU, Russia, Asia, Saudi Arabia, and other countries and regions in promoting electronic identity management. The Office of the Central Leading Group for Cyberspace Affairs sent eight delegates to this seminar in Vienna, including cyber security academician Fang Binxing from the Cyber Security Association of China. At the seminar, Hu Chuanping, director of the Third Research Institute of Ministry of Public Security, presented a report on the use of China's electronic identity management technology in practice. The topics of the seminar mainly included the following:

(1) Electronic identity management has progressed very rapidly in the international community, and has been popularized in both developed and developing countries.

(2) The issues of identity, services, and legal interoperability in cross-border transactions pose significant concerns. The basis of electronic trade is identification and verification. The construction of an international identity authentication environment has become the key factor in supporting international electronic trade.

(3) Security and privacy protection are recognized as the principles of electronic identity management. Electronic identity management is a basic task that involves a large number of users' personal information.

2.3 Application development

Significant progress has been made in support and promotion of eID applications in the EU. Currently, most EU member states have put forward an eID development plan for identity authentication, electronic (digital) signatures, data protection, and other issues in Internet applications. European Smart Card Association statistics show that, as of the end of 2013, the EU issued more than 150 million eIDs. According to these statistics, Belgium, Austria, Estonia, Italy, Spain, and other countries have a very high eID penetration rate. In Belgium, which has a population of about 11 million, more than 9 million people use eIDs—They are widely used in e-government, e-commerce, financial payments, and other such fields. In e-government public

services, eIDs enable the mutual recognition of European travel documents across borders. Currently, in Europe, eIDs are used in Estonia, Austria, Norway, Turkey, Finland, Sweden, Holland, Iceland, Italy [6].

3 Development and application of cyber electronic identity management in China

Combined with the requirements for the protection of identity information, China's eID technology system is designed using the international mainstream PKI technology. One reason for this is to promote further innovation and to comply with the two principles of "confrontation" and "protection of identity information." The system has three basic functions: efficiently identify eIDs remotely without disclosing identity information; promote the use of eIDs as digital signatures and implement a law that makes the eID card holder's online behavior verifiable; and effectively ensure the security of eID card holders (by requiring holders to enter a password when using their eIDs).

The 12th Five-Year Plan period saw significant progress in eID management, laying a solid foundation for the construction of a cyber identity management system.

3.1 Building the Ministry of Public Security's Internet-based identity recognition system for citizens and forming a complete technical system

During the 12th Five-Year Plan period, and based on cyber identity management key technology research and demonstration applications, the Ministry of Science and Technology deployed a project preferentially as a major project to support the implementation of cyber eIDs. This project is called "domain space identity management along with its application technology and system." The project was launched in collaboration with the Third Research Institute of Ministry of Public Security, National University of Defense Technology, Beijing University of Posts and Telecommunications, and dozens of other top domestic scientific research institutions, colleges and universities, and enterprises. The project, which is the largest among the national 863 Program projects in the field of information security, has made a breakthrough with the development and technical validation of a prototype system—the Ministry of Public Security's Internet-based identity recognition system for citizens—which has been reviewed for safety by the State Cryptography Administration.

3.2 Forming an eID standards system and ensuring high eID security and reliability

At the end of 2013, the China Communications Standards Association set up a space domain identity management standard sub-working group. The Third Research Institute of Ministry of Public Security governs more than 30 national and industry

standards for eIDs, including for Electronic Identity Format Specification. The eID standards system, which includes four levels of basic, management, service, and application standards, can ensure the high security and reliability of eIDs, and develop an eID industry technology roadmap to achieve a comprehensive specification.

3.3 Executing large-scale pilot application to complete eID promotion of complete verification process

In September 2012, an eID pilot project was officially launched at the Beijing University of Posts and Telecommunications. Nearly 30 000 eIDs were issued to the university's teachers and students, including the key staff of the school in charge of the university's business processes. On this basis, the Third Research Institute of Ministry of Public Security and the Industrial and Commercial Bank of China (ICBC) reached a strategic cooperation agreement, wherein the latter issued 500 000 financial ID cards embedded with eIDs everyday. Presently, the ICBC has issued more than 55 million eIDs, and the Internet application exists in many regions and typical industries. The ICBC is currently cooperating with three operators—China Telecom, China Mobile, and China Unicom—to achieve eID-embedded SIM cards for cell phones.

Dozens of organizations have been established in the eID cyber identity recognition services. These eID real-name authentication service applications have been embedded in other applications used by people, such as 360 mobile phone assistant with near field communication (NFC) access to Financial IC card to pay, digital livelihood socialization service platforms, industry and commerce informatization in the Jiangsu Province, and Internet convenient service platforms of public security organization. In addition, online applications are being developed for e-commerce, such as Umetrip, Anbaohong logistics alliance, Fadada (electronic contract), UTS Finance (P2P), and Fu Jian Amoy. Among social media, Sina, a micro-blogging application, implemented an automatic real-name identity authentication service based on eIDs, so as to not require Internet service providers to submit users' personal identity information. This would consequently enhance user experience. The most important function of eIDs is to implement more credible certification in order to effectively prevent and identify malicious acts. Both functions ensure the validity of real-name authentication requirements to protect the privacy of individuals. Moreover, eIDs can be used in the mobile Internet environment, such as in cell phone applications, with NFC access to eIDs. Thus, eIDs ensure safe and efficient logins, while effectively avoiding the risk of passwords being stolen.

3.4 Forming an eID framework of implementation and promotion

eIDs were implemented to promote the concepts of openness, cooperation, innovation, win-win approach, and orderly

development in protecting the safety of citizens' personal identity information, private information, and online activities. The five-in-one implementation of the framework will create a closed industry loop of the eID-sustainable development vision, and ultimately receive approval and support from the state, enterprises, people, and the media.

4 Promoting eIDs and supporting effective implementation of cyberspace identity management recommendations

4.1 Strengthening top-level design and accelerating the construction of China's cyberspace identity management system

Cyberspace identity management, which involves national security, public security, and citizens' vital interests, is a complex type of system engineering that focuses on achieving current and long-term goals, coordinating resources, and meeting diversified needs to actively and steadily push forward the cyberspace identity management. It is recommended that the Office of the Central Leading Group for Cyberspace Affairs and the Ministry of Public Security should ally with the Ministry of Industry and Information Technology of the People's Republic of China, the National Development and Reform Commission, and the State Cryptography Administration to set up a special working group under the unified leadership of the Central Committee of the Communist Party of China. This multi-organization arrangement would then be responsible for coordinating the promotion and construction of China's cyberspace identity management system. Furthermore, it would also solicit and listen to opinions and suggestions, and learn from the experiences of other countries through research. It would help develop China's cyberspace identity management system with a view to implement diverse views, clear construction planning, system framework, and routes, and clarify the functions and responsibilities of enterprises and government departments.

4.2 Establishing China's cyberspace identity management infrastructure based on eIDs

The mainstream international space landing method of cyberspace identity management is based on the asymmetric cryptographic algorithm PKI digital signature technology for eIDs. The EU and its member states, Russia, and Australia have effectively adopted eIDs with positive outcomes. In 2014, the United States also implemented an eID pilot project. During the 12th Five-Year Plan period, the Ministry of Science and Technology and the National Development and Reform Commission, starting with key technologies from cyberspace identity management research and development and demonstration applications, prioritized the deployment of major national 863 Program projects

for eIDs and information security to support the implementation of eIDs. The eID infrastructure—the Ministry of Public Security's Internet-based identity recognition system for citizens—has been built, and it has been reviewed by the State Cryptography Administration system for security and identification authority. In addition, an effective standards system has been formed based on more than 30 eID national and industry standards. On the basis of this system, a large-scale pilot application have been carried out, completing the promotion of the eID validation process in order to build the infrastructure of China's cyberspace identity management.

4.3 Developing eIDs to promote the application, and to speed up the construction of China's cyberspace identity management system

The following are suggestions for the promotion and application of cyber eIDs.

First, the establishment of cyber eIDs needs an expert group that can provide advice and carry out program checks. Planning China's cyberspace identity management requires supporting policies, regulations, a standards system, international mutual recognition, and an ecosystem formation mechanism.

Second, it is necessary to clear legal support for eIDs. Studies should be conducted to determine the legislative needs. For example, in the current discussion of the Cybersecurity Law of the People's Republic of China, a article "eID cards issued by state can be regarded as a trusted source to identify citizens' cyber identities" should be added.

Third, it is also necessary to develop a cyberspace identity authentication technique route according to China's national conditions. China can gradually restrict and control the collection of basic citizen information that is exclusive of information required by statutory cyber services, so as to strengthen the protection of citizens' personal information.

Fourth, local and industrial laws and regulations related to Internet real name should be developed to promote eID cards as the main real-name authentication method. Furthermore, these laws should encourage all industries and regions to issue security smart cards or devices embedded with eIDs.

Fifth, the eID plan should be implemented in the next three years to gradually increase the eID coverage; further improve the China's cyber identity management system; promote the integrity of the Internet, which plays a major role in improving social governance; and highlight the credibility and cohesion of the government and parties in the eyes of the people.

References

- [1] Network real-name system [EB/OL]. (2015-05-22) [2016-09-10]. <http://baike.baidu.com/view/731760.htm>. Chinese.
- [2] Identity management [EB/OL]. (2016-09-02) [2016-09-10].

- http://en.wikipedia.org/wiki/Identity_management.
- [3] European Commission. i2010—a European information society for growth and employment [R/OL]. (2005-06-01) [2016-09-10]. Brussels: Communication department of the European Commission. http://europa.eu/rapid/press-release_MEMO-05-184_en.htm.
- [4] European Commission. A roadmap for a pan-European eIDM framework by 2010 [R/OL]. (2010-02-01) [2016-09-10]. Brussels: Communication department of the European Commission. <http://www.statewatch.org/news/2008/jul/eu-com-eidm-roadmap-paper.pdf>.
- [5] Hu C P, Zou X, Yang M H, et al. Status and development of global network identity management [M]. Beijing: People's Posts and Telecommunications Press, 2014. Chinese.
- [6] Eurosmart. Landscape of eID in Europe in 2013 [R/OL]. (2013-07-07) [2016-09-10]. Brussels: Eurosmart. <http://www.eurosmart.com/images/doc/WorkingGroups/e-ID/Papers/eurosmart%20eid%20landscape%20white%20paper.pdf>