Information material for open consultations "Building an enabling environment for access to the Internet" within the frameworks of CWG-Internet

(13-14 October 2016, Geneva, Switzerland)

1. Introduction

February meeting of CWG-Internet approved open consultations on "Building an enabling environment for access to the Internet" containing the following questions:

1. What are the elements of an enabling environment to promote Internet connectivity?

2. What are the elements of an enabling environment to promote an affordable Internet?

3. What are the elements of an enabling environment to promote the quality of access to the Internet?

4. What are the elements of an enabling environment to build confidence and security in the use of the Internet?

5. What is the role of Governments in building an enabling environment?

Building an enabling environment for access to the Internet implies the entire system of organizational and/or technical measures, the set of which is defined by the level and the range of services offered online. That's why the issues proposed for open consultations consider various aspects of access and work in the Internet including the issues of connectivity, quality of access, security and government policies.

If we are considering the service of core Internet access, then the building an enabling environment for access to the Internet first of all implies building physical infrastructure for access. If we speak about a full range of e2e services implying secure work through the Internet, then building an enabling environment for access will further include capabilities for protection from malicious activity, viruses, spam, capabilities for secure and confidential Internet operations (as appropriate), including regulatory frameworks and legislative initiatives, regulating application of these capabilities for protection of private life and network stability. A State will be the guarantor of rights and obligations in such Internet environment.

Internet services are evolving. At dawn of its existence, Internet primarily provided access to the information, i.e. "search and read" service, but today Internet is the complex services ecosystem including financial services, remote education, telemedicine, state services and many others. Undoubtedly, the "Enabling environment for Internet access" concept includes both physical access to network and capabilities for protection from malicious activity, viruses; authentication capabilities on the one hand, and confidentiality capabilities on the other hand.

Following the logics of Internet services development, we would like to focus at the issue of confidentiality and security in the use of Internet as a tool for creating elements of enabling environment providing confidentiality and security of Internet use (question № 4 of open consultations), and the role of governments in building an enabling environment for access to the Internet. We believe that enabling environment to build confidence and security in the use of the Internet shall include serious protection of private life, compliance with principles of proportionality and necessity, prohibition of mass surveillance of Internet user activity by commercial companies.

2. World practice of applying electronic authentication

As a rule, governments establish their own legislation, implemented through executive bodies, to provide reliable and confidential Internet services and eliminate barriers between people online. To achieve this, governments use different approaches. One approach is to adopt facultative laws aimed at legalization of electronic documents and making them equal to those which are signed traditionally. The second approach is to adopt the laws which regulate certain technologies in the sphere of authentication. The third one is to introduce the laws harmonizing the existing regulation of electronic transactions in different countries. However different methods to eliminate the obstacles create uncertainties both in domestic and external business relations in various jurisdictions.

Legislation of most countries in the sphere of Internet authentication is based on special technical directives. They are developed to provide necessary regulation and freedom for secure information exchange in the field of e-commerce, during Internet voting, using state Internet services. Participating States implementing such directives are required to take them into account in their national law.

International regulations on electronic authentication

Title	Country	Adoption date	Description	Document status
ISO/IEC CD 9798-3:1998/Cor 2:2012 Information technology. Security techniques. Entity authentication. Part 3:	USA	1993	One of the first authentication standards consisting of three parts (common approach, use of symmetric and asymmetric cryptography). Authentication of subjects is described using algorithm with public key. The standard defines five different protocols for unidirectional and bidirectional	Fundamental and important standard for state systems.

Mechanisms using digital signature techniques. Technical corrigendum 2			authentication. See www.iso.org for a short review.	
The Declaration on Authentication for Electronic Commerce	USA	1996	This document recognizes the need to develop electronic authentication within OECD countries for the purpose of interoperability and development of international e-commerce.	Set of existing standards of different purposes.
Authentication SASL Mechanism ISO/IEC 9798-3	USA	2001	The document defines authentication SASL mechanism (Simple Authentication and Security Layer) based on earlier standards for authentication of subjects. This mechanism provides authentication of subjects using certificates of ITU-T X.509 format, but does not ensure integrity and confidentiality of user data.	Recommending standard. It could be applied in those cases when integrity and confidentiality are ensured at application level.
NIST SP-800-33	USA	2001	Special guidance which gives reasons to the need to introduce authentication guarantees to ensure confidentiality, integrity and availability of information.	Document has important meaning for the USA and some other countries.
CEN Workshop Agreement	EU	From 2001 to 2004	European regulations. CWA means "CEN Workshop Agreement". Set of CWA documents have played a great role in application of identification/authentication for electronic signature in EU countries. In particular, some CWA documents are devoted to SSCD − Secure Signature-Creation Devices.	The Agreement is widely used in Europe with regard to identification/authentication regulation for application of electronic signatures.

M04-04 Memorandum and E-Authentication Guidance for Federal Agencies	USA	2003	The guidance takes into account existing practices in the field of authentication for access to electronic transactions, and facilitates identification of requirements on authentication of state services sites, i.e. it proposes to conduct "e-authentication risk assessments" in e-commerce to obtain positive response from the government on the selected approach.	Special verification/authentication methods are obligatory to American state systems for security and protection of citizens' personal data.
NIST SP 800-63	USA	2006	This standard is an addition to the recommendations on e-authentication for federal agencies, where four levels of authentication are established depending on consequences of authentication errors and improper use of e-certificates. It also provides definitions for technical terms, and information on password usage.	It is obligatory for e-government portals and sites of federal state powers.
FIPS PUB 201-2 Authetication standards "Federal Information Processing Standard"	USA	2013	FIPS 201-2 is the USA standard prepared by NIST. It introduces term "PIV" (Personal Identity Verification) instead of "authentication".	FIPS 202 is recommended for use in state bodies to protect *unclassified* information.

United Nations Commission on International Trade Law (UNCITRAL) developed Model Law on Electronic Commerce. This law offers to national legislative bodies a set of rules adopted at international level, recommending ways to overcome certain legal barriers and aspects in e-commerce. It is a model for countries assessing and modernizing certain aspects of their legislation and practice in the field of e-authentication. Model Law on Electronic Commerce establishes functional compliance between electronic (or traditional) signatures and authentication methods. It had an effect on many foreign jurisdictions. And though UNCITRAL Model Law on Electronic Commerce is widely applied (some governments use it as the basis for e-commerce regulation), it could not be said that it is universal.

In its turn, European Commission has adopted Directive 1999/93/EC on a Community framework for electronic signatures when accessing the services and then in 2014 Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market. The main reason for this decision was the need in unified European regulatory framework which could be obtained from regulatory practice of member-states. An example of implementation of the directive 1999/93/EC is the Great Britain with its Electronic Communications Act 2000 as a regulating document.

Using these technical directives, the legal regulation has been currently applied successfully by different States. Federal Government of Canada introduced *Personal Information Protection and Electronic Documents Act* in order to harmonize electronic communications and transactions with the federal law. In 1998, the Uniform Electronic Commerce Act 1999 was adopted describing different aspects of Internet-commerce, including remote interoperation with government bodies when receiving services.

Different USA states had a need to allow electronic authentication of documents and signatures through electronic devices. Then in 1999, Uniform Electronic Transactions Act 1999 (UETA) was adopted. E-voting in the USA is regulated differently in the states, but each state shall meet specific requirements of the following legal acts:

1) Voting Rights Act establishing voting provisions for specific categories of persons with disabilities.

2) Uniformed and Overseas Citizen Absentee Voting Act of 1986 requiring that states shall grant citizens the right to be registered and to vote absentee in elections.

To meet requirements of the above acts, the U.S. Congress adopted Help America Vote Act in 2002. This Act aims at three targets, i.e. establishment of a centralized Federal agency for a collection of voting information; allocation of funds to certain states for their election system management and updating voting technologies; and establishment of minimum standards for each state in the election system.

Arizona became the first state that made transitional steps towards online voting. Each registered citizen received a personal identification number by mail and had a choice to either cast ballot at a designated polling center or vote online from his/her own home. Online voter is required to enter his/her PIN and answer two personal questions. Once the verification process is completed, he/she receives voting options.

Australian legislative initiatives on authentication are provided in Electronic Transactions Act 1999.

In 2013, the Electoral Council of Australia and New Zealand released a paper on Internet voting in Australian election systems.

In Australia, according to the federal election right, the voting process at federal elections and referendums is mandatory for all persons aged 18 years or older. Non-voters shall either provide a valid and sufficient reason for failing to vote or pay a $20 penalty. Upon declining to pay the $20 penalty, the matter might be referred to a court. If the matter is judged and a citizen is found guilty, he/she may be fined up to $180 and a criminal case may be initiated. For proper implementation of the voting process, iVote is used for remote voting. In order to vote, a citizen needs to register himself (either through Internet or iVote call-centre). First, at the registration stage, he/she needs to enter a six-digit PIN, and then a unique eight-digit registration number would be sent back by SMS, mail, e-mail or phone call. To vote, a citizen shall provide both the numbers to the iVote via Internet, however, as an alternative, a call to the call-centre is proposed. For remote voting via telephone, a voter will be provided with instructions and names of candidates. After voting, a voter will be required to verify his/her identity – to do so he/she will be sent a specific receipt number. The receipt number along with the PIN and iVote number should be entered in the callback SMS for confirmation.

3. Russian experience in the establishment of Unified System for Identification and Authentication (USIA) to provide government services to the population and legal entities

The Russian Federation has been actively developing e-government services. Relevant Federal Law of 27 July 2010 No 210-FZ "On Provision of State and Municipal Services" regulates relationships emerging due to provisioning of state and municipal services to the population and legal entities. The objective of the Russian Government is the following: 70 % of all government services by 2018 must be provided online to improve living standards and conditions of doing business. In addition to Federal Law No 210-FZ, Decree of the Russian Government of 24 October 2011 No 861 was issued approving:

- Regulations on Federal State Information System "Federal Register of State and Municipal Services (Functions)"
- Rules of Maintaining the Federal State Information System "Federal Register of State and Municipal Services (Functions)"
- Regulations on Federal State Information System "Common Government Services Portal of the Russian Federation".

Based on these fundamental documents, the system of government services and the Unified System for Identification and Authentication (USIA) have been established as being needed for the e-government operation. Currently, a citizen of the Russian Federation can enjoy the following e-services: filling in an application for international and regular passports, making an appointment with a motor vehicle inspection, applying for driving license, checking unsettled

penalties, registering at the place of stay and residence, making an invitation to foreign visitors to Russia, submitting a tax statement, tracking pension savings, making an appointment with a doctor, and many others.

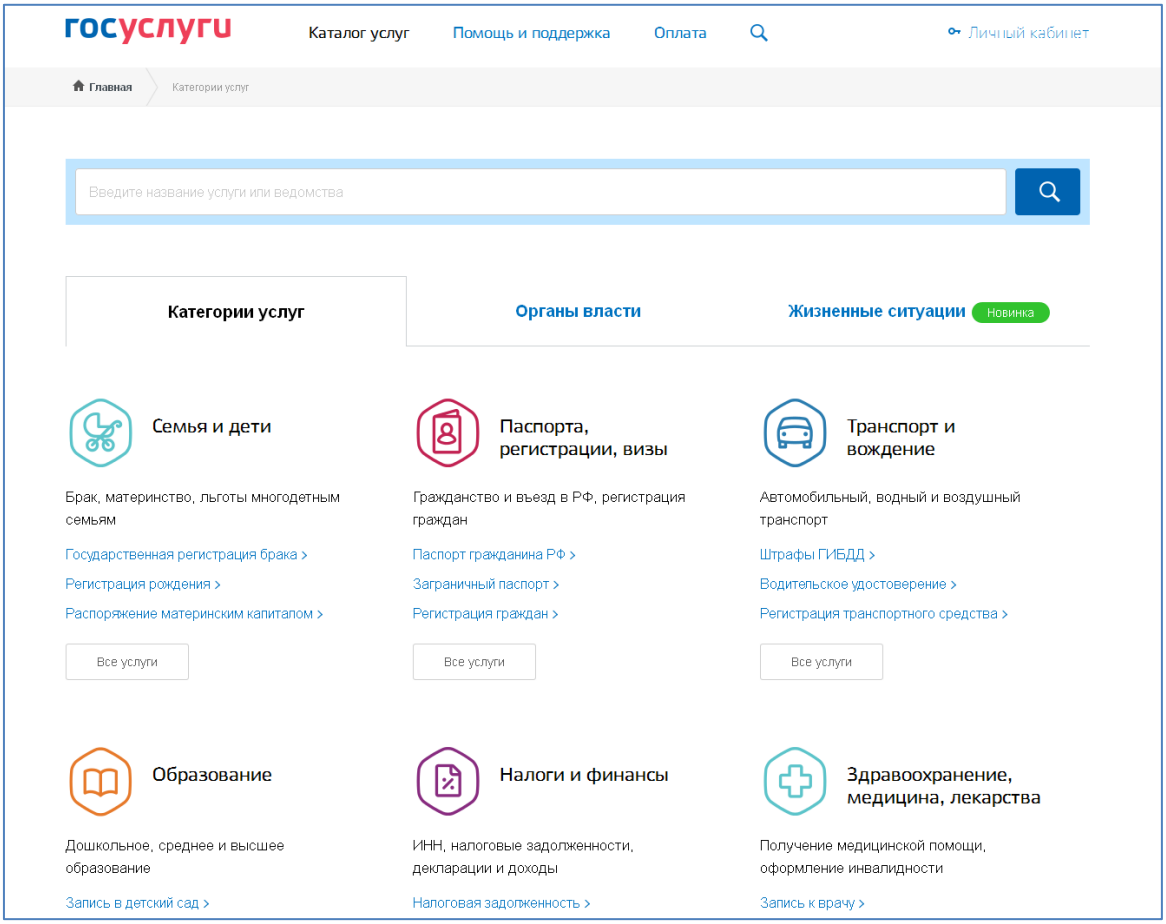

Figure 1. Example of Common Government Services Portal webpage with service categories

Migration to government and municipal services in electronic format requires that Government shall provide citizens and public authorities with a tool for secure online identification.

The Russian Ministry of Telecom and Mass Communications within the e-government structure has established and is developing a Unified System for Identification and Authentication (USIA) with the aim to harmonize and centralize the processes of user registration, identification, authentication and authorization.

The USIA has the following functions:

a. Provides technical solution to information systems of public authorities on trusted identification of users (natural and legal persons, public authorities). The trustworthiness is achieved through the following:

- Registration in USIA involves checking significant personal criteria

- USIA protects information within the system in accordance with the Russian Law.

b. USIA is a user-friendly system offering the following capabilities:

- Identification and authentication through a single account and using a wide choice of supported authentication methods, when accessing a variety of public information systems
- User management of personal data accommodated within the USIA and monitoring their distribution to public information systems.

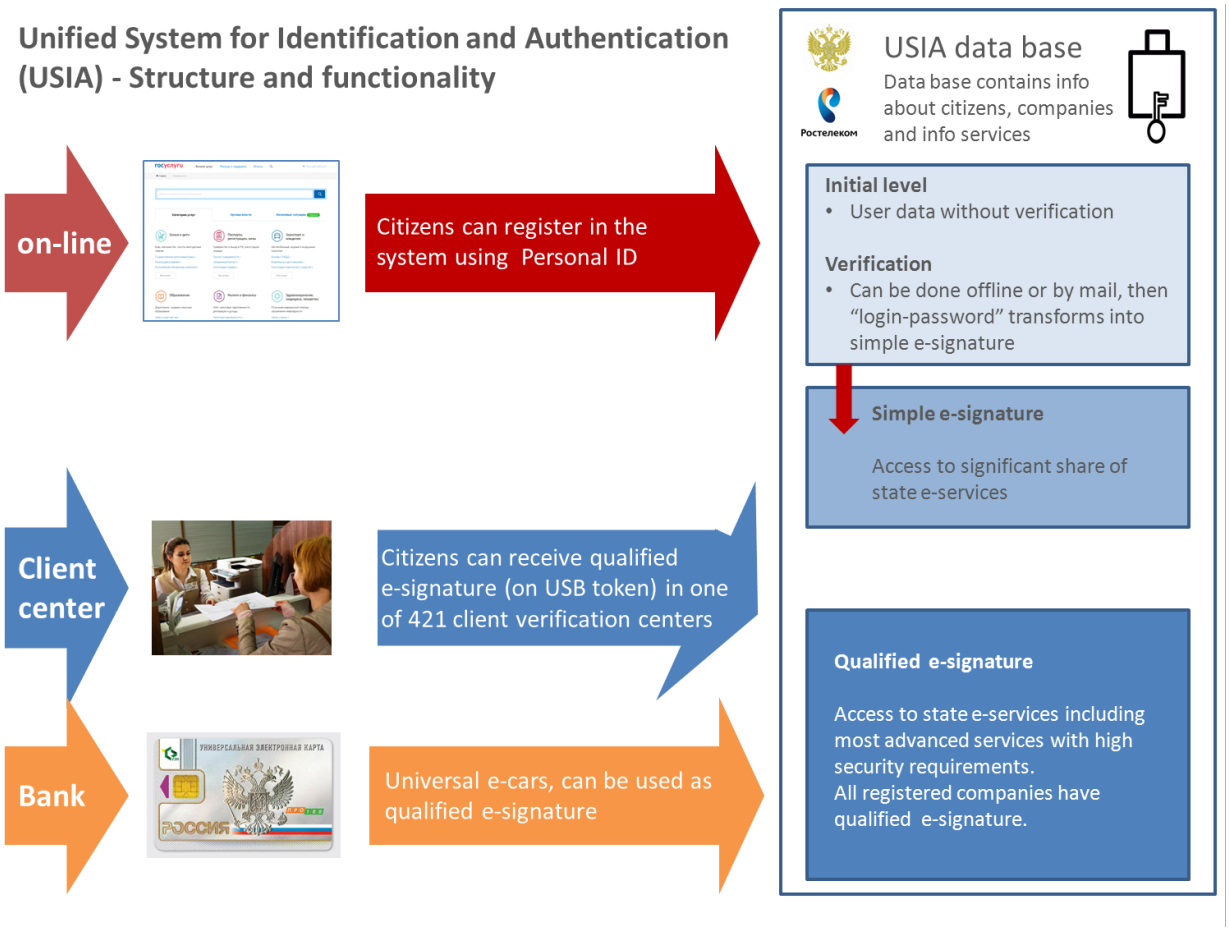

Figure 2. USIA structure and functionality

The USIA main functionality:

- Identification and authentication of users, including:
  - single-factor authentication which gives USIA users the following benefit: once going through identification and authentication procedure

in USIA, user within one session could have access to any information system utilizing USIA without re-identification and re-authentication

    - support of different authentication methods: by password, digital signature, as well as two-factor authentication (permanent password and single-use password sent by SMS)
    - support of trusted levels of user identification (simplified account, standard account, confirmed account)
- Identification data maintenance: maintenance of registries for individuals, legal entities, bodies, organizations, officials and information systems
- Authorization of government officials when accessing the following functionality of USIA:
    - maintenance of governmental officials registry in USIA
    - maintenance of handbook on powers related to information system, and granting USIA users (registered in USIA as officials) powers to have access to resources of systems registered in USIA
    - delegation of the above-mentioned powers to the officials of the subordinate governmental bodies
- Maintenance and provision of information on user powers related to information systems registered in USIA.

Currently there are 29 million users registered in the USIA. First half of 2016 have seen the increase of 6.4 million users, keeping the growth rate seen at the end of 2015 − more than one million users per month.

Currently, the share of citizens registered in the USIA in 43 Subjects of the Russian Federation is more than 20%. Primorsky Krai, Khanty-Mansi Autonomous Okrug, Tyumen Oblast, Kaliningrad Oblast, and Yamalo-Nenets Autonomous Okrug are among the leaders with the share higher than 40%.

Updated "Government Services" mobile application is also showing a considerable increase in requested federal services: 168 thousand requests in the first half of 2015, 43.6 million in 2016. Currently, the mobile application is being run monthly by more than 500 thousand users getting access to 9.1 million government services. The latest version of the application is rated 4.5 out of 5 in application stores.

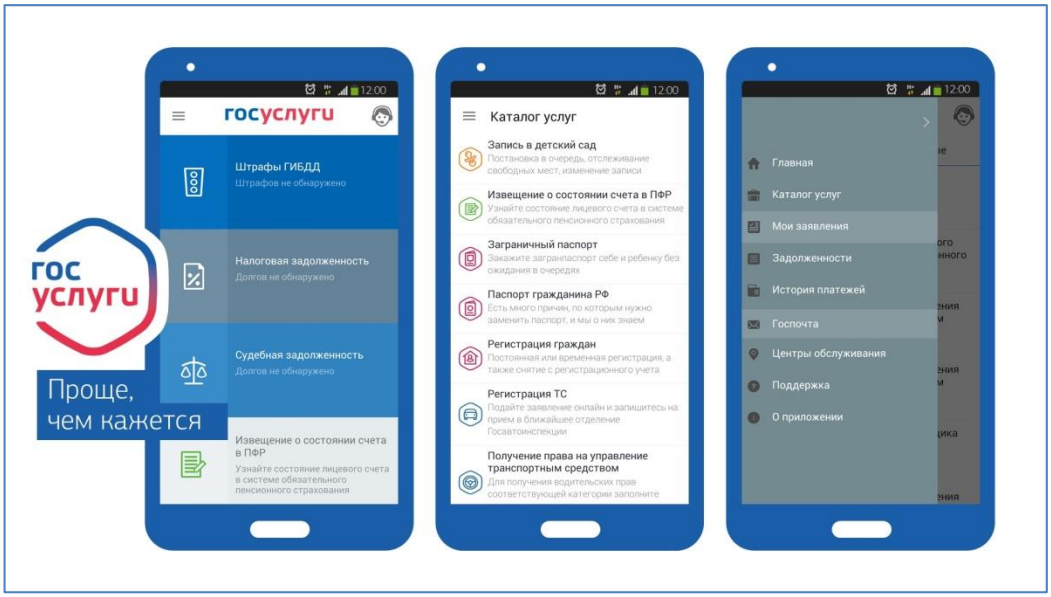

Figure 3. USIA mobile application

In the first half of 2016, users of Common Government Services Portal and users of its beta version have completed 2.4 million successful payments for a total of 2.3 billion rubles. This is 3.5 times more compared to the same period in 2015 when there were 714 thousand payments for a total of 656 million rubles.

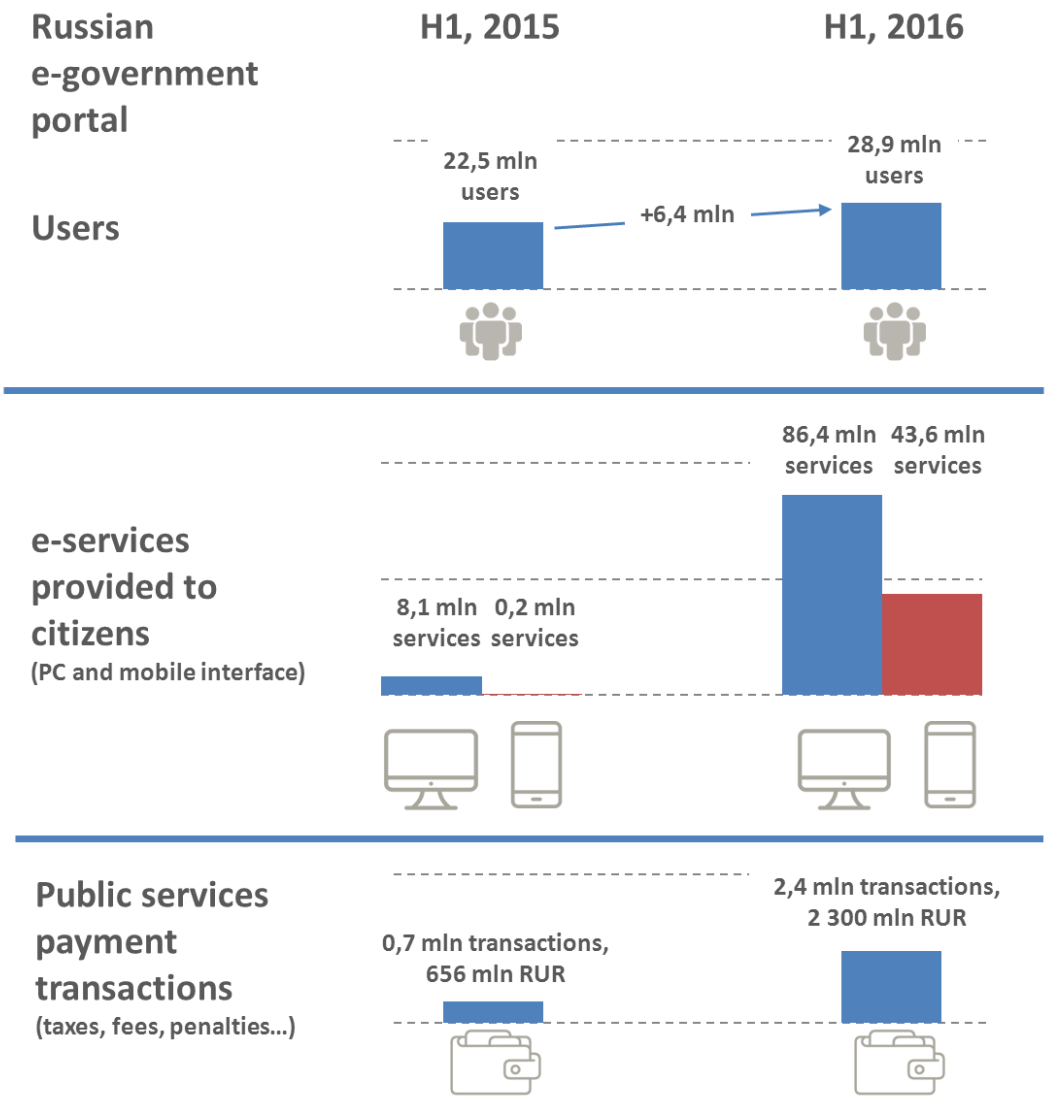

Figure 4. USIA evolution (June 2016)

4. Current state and challenges of implementing electronic authentication worldwide

The previous section of the document has shown that the practice of implementing electronic authentication is being applied worldwide. Only few examples of using electronic authentication to ensure confidential and reliable operation of services in Internet have been shown, however, actually far more countries have legislative regulation in the field of authentication. However, a number of challenges related to electronic authentication needs to be noted:

1. Despite a cross-border nature of Internet services, legal initiatives in the field of electronic authentication are local national matters (except European Union initiatives implying their implementation in all EU countries). Undoubtedly there is an urgent need for coordination of activities between governments on developing electronic authentication systems. CWG-

Internet could serve as a platform for discussing and coordinating the issues related to electronic authentication.

2. Lack of practical experience and sharing of best practices and lessons learned in the field of applying digital authentication. Despite the sufficiently active implementation of authentication mechanisms, it is deemed to be extremely useful to organize sharing of opinions and best practices on state policies with regard to authentication.

3. "Industry point of view" on authentication issues. Nowadays the matters of electronic authentication are considered for addressing certain specific tasks, for implementing e-commerce services, procedures of electronic voting via Internet. However it is deemed useful to discuss the unified and universal authentication system, taking into account increasing requirements for privacy and personal data protection in such fields as telemedicine, education, government e-services, related to registration and management of rights, accrued taxes, etc.

5. Summary

Thus, it could be noted that many countries have developed and implemented state policies aimed at implementation and operation of electronic identification and authentication systems, showing the importance of the issue. Nevertheless, state polices related to identification and authentication systems are at the different levels of development in different countries, with a large number of challenges remained and a number of issues requiring more studies. This leads to a need in organizing within CWG-Internet sharing of opinions on the matter of authentication system as a whole and on the matter of state policies in particular. In this regard, administration representatives could be invited to submit their best practices in the field of electronic authentication and its regulation, and also analyze practices of applying electronic authentication and legislative regulation of the related services, and then develop recommendations for the ITU Council on the role of governments in ensuring confidentiality and protection of personal data and information.