I. INTRODUCTION

Following the global trends, several large modern information systems have already been introduced in BiH, such as the BiH Agency for Identification Documents, Registers and Data Exchange (IDDEEA) information system, information system supporting treasury operations, information system of the tax administration, court registry of businesses, information system of the border police, customs information system, system of the Central Bank of BiH and clearing (Clearing House), ICT system to support the privatization process, etc. However, many of the implemented IT projects just solved “burning” issues and for that reason the implemented IT projects remained isolated since they were developed only to address a single problem instead of being an integral part of the coherent reform in applying IT in the public administration.

As a member to Electronic South Eastern Europe (eSEE) Initiative, Bosnia and Herzegovina signed the “eSEEurope Agenda for the Development of the Information society” in 2002 in Belgrade. As a part of the Agenda, it was agreed that the signatory countries develop and endorse policy and strategy for development of information society and through the priority area “Single SEE Information Space” define the manner of establishing public infrastructure for secure commerce based on qualified electronic signature. Moreover, in the upcoming period IDDEEA is planning to provide some of 12+8+3 e-services contained in the eSEE Agenda Plus. Yet, lateness in implementation of the BiH Law on Electronic Signature renders impossible these services to become transactional. By comparing the achievements with the requirements from the eSEE Agenda Plus and the 23 basic services of e-Government which should be established by the end of 2011, BiH is unfortunately lagging far behind even in comparison with countries in the region, and in particular Europe and globally. Key problems that affect this are: inexistence of institutional arrangements necessary for coordination of activities in the domain of e-Government at different government levels and in different ministries, uneconomic utilization of inadequately allocated IT human resources, and still inadequate ICT policies, legal frameworks, methodologies and standards for implementation of e-Government projects. Hence, the enthusiasm to move forward is now additionally slowed down due to the growing awareness that successful e-Government requires a combination of
organizational change, policy reform and investment in technology.

In 2004 the Council of Ministers of BiH adopted the Policy, Strategy, and Action Plan for Development of Information Society in BiH for the period 2004-2010; the Law on Electronic Signature of BiH and the Law on Electronic Legal and Business Transactions were adopted in 2006. Decisions which regulate the domain of using electronic signature and providing certification services and ensure the necessary legal aspects for digital signature implementation were also endorsed.

In terms of infrastructure, a highly sophisticated communications network in SDH technology, which allows for fast, reliable, and efficient exchange of data, visual image and sound, has been put in place for transfer of data of security institutions of BiH. SDH network represents a closed system, it is not linked to the Internet and functions within a particular range of frequencies secured for that purpose. The institution which provides technical maintenance for the SDH network is IDDEEAA which is responsible for the domain of identification documents, safekeeping, personalization and transport of documents, as well as centralized maintenance of records and data exchange between the competent bodies in BiH. IDDEEA monitors, coordinates and institutionally regulates the development of identification documents, and has, as such, developed the electronic signature in a closed system. IDDEEA experiences in terms of application of electronic signatures in closed systems are of great importance for implementation of the BiH Law on Electronic Signature in open systems as well.

II. DEFINING THE PROBLEM

2.1 Objectives of the State


Although the Policy for Development of Information Society is based on eight development pillars, Strategy for Development of Information Society refers to five development pillars, namely:

- eLegislation
- eEducation
- eAdministration
- ICT infrastructure
- ICT industry

The objectives defined in the Policy for Development of Information Society through broad application of information and communication technologies are:

- Increasing the knowledge and competencies of citizens for living and working in information society;
- Creating a new market environment, business processes and knowledge, and new forms of organization;
Increasing cost-effectiveness, competitiveness, quantity and quality of products and services, application of innovations in the economy, administration, education and other fields;

- Increasing investments and employment;
- Developing ICT industry;
- Developing small and medium enterprises as pillars of economic development;
- Achieving sustainable economic development along with environmental protection;
- Increasing the standard of citizens;
- Achieving even development of the society, including rural areas;
- Growth of GDP;
- Meeting requirements for EU integrations.

In line with these goals, introduction of the electronic signature as the infrastructure for improving business processes imposes itself as a priority. The goal is to create an electronic business environment for circulation of electronic documents in the state administration, judiciary, commercial sector and other domains, and thereby create conditions for development of competitive economy, as well as more efficient, effective and economic public administration. Also, through establishment of the eServices, to improve mutual communications between businesses, public administration and citizens as it reduces costs of doing business, contributes to savings, generates greater value added, reduces the grey economy, and minimize corruption. Likewise, the goal is to enable citizens, businesses and other entities to meet their obligations or address their requests to the administration in the most efficient possible way, with minimal costs and number of physical points of contact with administration bodies, and all this by means of several different electronically based channels for service delivery (web, mobile telephones, etc.).

Important segments of e-commerce are issuance and delivery of electronic invoices, as the majority of legal entities already has capacities to perform electronic invoicing (through their own information systems or through the electronic banking infrastructure), and e-procurement, which are important catalysts of change as they require a comprehensive integration of systems and business processes throughout the public and private sector. Development of state-level solutions for all eServices should be observed in the context of broader changes with the aim of modernizing government and achieving an absolute interoperability.

Specific objectives are:

1. Establish the state-level Public Key Infrastructure (PKI) as a system for development and use of electronic signature, as a precondition for the entire range of interactive services which must be accomplished in the G2C scenarios (government to citizens services);
2. Ensure interoperability and recognition of all accredited certification authorities (CAs) in the territory of BiH;
3. Make equal validity of electronic and standard (hard-copy) submissions and documents;
4. Enable use of all accredited and secure electronic signatures for doing business with the public administration.

In order for these goals to be successfully implemented in the future and to introduce the
electronic signature into the business processes of the information society, it is necessary to meet the following preconditions and implement the following steps:

1. Establish legal framework for eCommerce by developing laws and by-laws in accordance with the Acquis Communautaire of the European Union (EU);
2. Establish institutional framework necessary for secure and successful implementation of eSignature in business processes in BiH;
3. Harmonize all laws and by-laws in the domain of e-commerce at all levels of government in line with the relevant EU legislation, and ensure harmonization of other legal enactments relevant for the area of implementation of eSignature in BiH.

2.2 Legal Aspect

Information society is a global phenomenon and therefore the legal framework of the country needs to be based on global initiatives for harmonization as well as initiatives within the European Union. Below are the most important decrees, directives and other legal enactments of the EU which pertain to the domain of electronic signatures, electronic commerce and electronic government.

**Directive 1999/93/EC on a Community framework for electronic signatures**

This Directive establishes the legal framework at European level for electronic signatures and certification services. The aim is to make electronic signatures easier to use and help them become legally recognized within the Member States.


This Decision gives the references of three generally recognized standards for electronic signature products which presume compliance with the qualified electronic signature.


This Decision sets out the criteria that Member States must take into account when designating national bodies to evaluate the conformity of secure signature-creation devices.


The Electronic Commerce Directive, adopted in 2000, sets up an Internal Market framework for electronic commerce, which provides legal certainty for business and consumers alike. It establishes harmonized rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations.
of liability of intermediary service providers.

**Directive 2006/112/EC of 28 November 2006 on the common system of value added tax**

Since most of the invoices are VAT invoices, a VAT compliance is an important issue for businesses. First EU norm in the area of electronic VAT invoicing were the invoicing rules in the 1977 6th Directive (77/388/EC). In response to concerns from business about still very divergent rules in some member states and in response to the technological developments, the European Commission issued an amendment in the form of the EC Directive on Invoicing (2001/115/EC). This directive provided a single European standard for Invoice content for VAT, and allowed for electronic invoicing and storage within all member states. The VAT invoicing rules are now contained in the VAT Directive (2006/112/EC). In accordance with the directive we can identify three principal e-invoicing areas: the content of an invoice (articles 226 to 231 and article 238 of the VAT Directive), electronic invoicing (articles 232 to 236 of the VAT Directive) and the storage (archiving) of invoices (articles 244 to 249 of the VAT Directive).

**The EU public procurement directives**

The main principle of EU legal framework for e-procurement is that every business should be able to participate, with simple and commonly used equipment and basic technical know-how, in a public procurement process which takes place partially or entirely by electronic means. This legal framework can be found in the procurement regulations and directives:


In response to need to develop and harmonize its legal framework with the global and European legal developments over the last two decades the legislation in Bosnia and Herzegovina has been adopted on the state level, while particular legal enactments have also been passed on the entity level. The primary elements are presented below.
State level

The state has adopted modern legislation, first of all the Law on Electronic Signature, Law on Electronic Legal and Business Transactions and accompanying by-laws for the domains of electronic signatures, electronic government sessions, web pages, etc. Amendments to the Law on General Administrative Procedure, which regulate the widest possible array of government procedures, were also adopted in order to build the foundations for electronic services.

In that regard, the following legal enactments are currently in force:

- Law on Electronic Signature (“BiH Official Gazette”, number 91/06);
- Law on Electronic Legal and Business Transactions (“BiH Official Gazette”, number 88/07);
- Law on Administrative Procedure (“BiH Official Gazette”, numbers 29/02, 12/04, 88/07, 93/09);
- Decision on the Basis for Use of E-signature and Provision of Certification Services (“BiH Official Gazette”, number 21/09);
- Decision on Electronic Commerce and e-Government (“BiH Official Gazette”, number 07/10);
- Decision on Office Administration of Ministries, Services, Institutions and Other Bodies of the Council of Ministers of BiH – (“BiH Official Gazette”, numbers 21/01, 29/03);
- Instruction on Developing and Maintaining Official Web Pages of Institutions of BiH (“BiH Official Gazette”, number 21/09).

Moreover, the following legal enactments are currently also being prepared:

- Rulebook on Internal Organization of the Ministry of Communications and Transport of BiH (establishment of the Office for Supervision and Accreditation);
- Law on Agency for Development of Information Society.

Republika Srpska (RS)

In line with the eGovernment Strategy 2009 - 2012, the Government of Republika Srpska adopted the following laws and by-laws:

- Law on Electronic Signature of RS (“RS Official Gazette”, number 59/08)

This Law regulates the use of electronic signature in legal operations and other legal actions, as well as the rights, obligations and responsibilities in relation to electronic certificates (verifications). Together with the Law, an entire range of by-laws was also adopted which regulates areas such as repository of certification authorities (CA), single registry of CAs that issue qualified certificates, measures and procedures for use and protection of e-signature, means for developing e-signature, mandatory insurance of CAs, namely:

- Rulebook on Repository of Providers of Electronic Signature Certification to Certified Bodies (“RS Official Gazette”, number 88/09);
- Rulebook on the Contents and Manner of Keeping the Repository of Certification
Authors for Issuance of Qualified Electronic Certificates (“RS Official Gazette”, number 88/09);
- Rulebook on the Measures to Protect Electronic Signature and Qualified Electronic Signature, Lowest Price of Mandatory Insurance and Application of Organizational and Technical Measures of Certificate Protection – (“RS Official Gazette”, number 88/09);
- Rulebook on Technical Rules for Ensuring Connection between Repositories (“RS Official Gazette”, number 88/09)

Pursuant to provisions of the Law on Republika Srpska Government and the Law on System of Public Services, in 2007 the RS Government adopted the Decision on establishing public institution “Agency for Development of Information Society of Republika Srpska”. Through this enactment, RS established the institution in charge of monitoring development of information society and promoting use of information and communications technologies. Work of the Agency, on behalf of the RS Government, is supervised by the RS Ministry of Science and Technology.

- **Law on Electronic Document of RS** (“RS Official Gazette”, number 110/08)

This Law regulates right of private persons and legal entities to use electronic document in all business actions and activities, and in procedures handled by the authorities of the RS administration in which electronic equipment and programs may be applied in preparation, transfer, archiving and safekeeping of information in electronic form. The Law also regulates legal validity as well as use and transactions of electronic documents.

- **Law on Electronic Commerce of RS** (“RS Official Gazette”, number 59/09)

This Law defines provision of services and rules in connection with entering into a e-form contract.

**Federation of Bosnia and Herzegovina (FBiH)**

Federation of BiH does not have the legislation on electronic signature, as it relies on the Law on Electronic Signature of BiH.

**Brčko District of BiH (BD)**

- **Law on Electronic Signature of Brčko District of BiH** (“BD Official Gazette”, numbers 39/10, 61/10); planned to enter into force 1 January 2011 – postponed until 31 June 2011.
- **Law on Electronic Document of Brčko District of BiH** (“BD Official Gazette”, numbers 39/10, 61/10); planned to enter into force 01 J2011 – postponed until 31 June 2011.

The Law on Electronic Signature of Brčko District of BiH does not differ from the Law adopted by the Parliamentary Assembly of BiH in 2006 or the Law in Republika Srpska. Due to lack of pre-conditions for implementation of the BiH Law on Electronic Signature i.e. inexistence of Supervisory Authority for Supervision and Accreditation of CA, the legislators
in Brčko District of BiH assessed that it is more optimal to adopt a separate law in the District and in that way apply the legislation of electronic signature.

Pursuant to Article 9 of the Law on Electronic Signature of Brčko District of BiH, the Department for Public Registry shall prescribe measures for protection of electronic signature and advanced electronic signature, as well as the measures for checking the identity of the signatory.

Article 43 also prescribes that the Head of the Department for Public Registry will adopt all required by-laws stipulated in the Law within six months from the date when the Law on Electronic Signature of Brčko District of BiH enters into force.

Harmonization of laws with fundamental requirements of the EU

The BiH Law on Electronic Signature is to a large extent harmonized with the accomplishments and regime of electronic signatures in the EU documents, for example:

Market access – Member countries may not allow that certification services are subject to prior authorization of any kind, or limit the number of accredited certification services providers or restrict provision of certification services which come from another member country in the areas covered by the Directive. Programs of voluntary accreditation may be introduced with the aim to improve the provision of certification procedures – Article 7 and Article 24 of the BiH Law on Electronic Signature.

Legal impacts of electronic signatures – Fundamental provisions of the Directive state that the advanced electronic signature based on a qualified certificate satisfies legal requirements for signature related to data in electronic form in the same way that the personal signature satisfies requirements for data in hard-copy form, and that is should be used in legal procedures – Article 4 and Article 5 of the BiH Law on Electronic Signature.

Liability – Member countries must ensure that the certification provider who is issuing the qualified certificate is liable vis-à-vis each party that relies upon the certificate for: accuracy of all information in the qualified certificate, upholding of all requirements from the Directive in the course of issuance of qualified certificate, assurance that the owner identified in the qualified certificate at the time of issuance of the certificate was in possession of all data for forming of the signature which match data for checking the signature contained in the certificate provided or identified in the certificate, in instances when the certification services provider retrieves data for generating or verifying the signature ensuring that the data for generating the signature and the data reconciled with them for signature verification are appropriate in a complementary sense.

Certification services provider shall not be held liable for damages incurred in connection with use of qualified certificate for transactions with value beyond the stated limitation – Article 19 of the Law on Electronic Signature of BiH.

International aspects – Member countries must ensure implementation of mutual legal recognition of qualified certificates and electronic signatures from third countries if particular validity requirements are fulfilled – Article 24 of the BiH Law on Electronic Signature.
Data protection – Member countries must ensure that the certification service providers and national bodies responsible for accreditation or supervision are in line with the Directive 95/46/EC on protection of personal data in articles 14, 15 and 18 of the BiH Law on Electronic Signature.

The Law should not be implemented without appropriate implementing by-laws. As a part of Article 26 (2), the Council of Ministers of BiH should enforce by-laws on implementation of the Law, within six months from the date of publication of the enactment in the Official Gazette (i.e. in 2006). On the other hand, the Ministry of Communications and Transport of BiH did not manage to get an approval from the Council of Ministers of BiH and establish the Office for Supervision and Accreditation of CA, in accordance with Article 20 of the Law on Electronic Signature of BiH.


We can hence conclude that there is a modern and quite detailed legislative framework. This framework provides predictable and reliable responses to questions concerning integrity, authenticity, and non-repudiation of electronic form and electronic signatures. In spite of general harmonization with the EU directives and global models for legal documents, there are particular problems:

1. some of the provisions are complicated or impractical and in some areas too restrictive;
2. laws and the obligation to register the activity of CA exist at the state-level but also at the entity-level;
3. some legal matters remain unresolved; in instances in which it is not possible to rely on measures of the EU Acquis, local legislation is inconsistent and incomplete regarding particular, very practical aspects (e.g. legal effects of transferring hard-copy documentation to electronic form, long-term electronic archiving, electronic government procedures, electronic court procedures, etc.);
4. even when the laws are neutral in terms of technology or form (where the text does not refer solely to hard-copy documents) and would thus permit the use of contemporary ICT tools, the competent public bodies mostly interpret laws in the traditional way allowing only for use of hand-written signatures and hard-copy documents.

2.3 Institutional and Political Aspect

Although the Law on Electronic Signature of BiH has been in force since 2006, many unresolved institutional and political questions arose which prevent or slow down the processes of implementing the Law, and consequently application of eSignature in BiH, of which the following are the most significant:

- Lack of understanding of competencies in the domain of electronic signature and
electronic commerce;
- Institutions in BiH have not been sufficiently committed to implementation of the Law on Electronic Signature of BiH;
- Slow progress of public administration reform and poor business environment in the society decrease significance of implementing eSignature and all benefits that are accomplished;
- Non-existence of the Office for Supervision and Accreditation of CA within the Ministry of Communications and Transport of BiH;

At the state level, it is necessary to form the Office for Supervision and Accreditation of CA in the Ministry of Communications and Transport of BiH as foreseen by the current Law (Article 20, Paragraph 1). Because of the size of the country and experiences from other countries, it is believed that this Office requires very small number of staff. This Office is necessary for all options for application of the BiH Law on Electronic Signature that will be proposed further below in this document.

In terms of systematization of jobs in the Office for Supervision and Accreditation, the proposal is to have five employees, while noting that in the beginning it is necessary to hire three civil servants for the following posts, namely:

1. **Head of the Office**, tasked with managing the Office activities, proposing adoption of appropriate measures and procedures in connection with the use of electronic signatures in „e-Government“ projects, cooperating with other bodies in the domain of development and improvement in use of electronic signature, etc.;

2. **Expert Advisor for Inspections**, tasked with inspection control, and work in connection with registration, accreditation and maintenance of CA registries, as well as services of recall of inspection supervision.


In addition, it is necessary to establish the Central Registry of Trust and Services (center of trust) as common repository on all levels of government which would contain the register of contacts and records for all information related to the validity of qualified certificates and trusted certification services.

### 2.4 Technical Aspect

The fundamental technical component is made up of one or more Public Key Infrastructures (PKI). This can either be a central infrastructure with one body for issuance of certificates and subordinated bodies which issues certificates for electronic signatures or more independent structures at a particular degree of interoperability.

In Bosnia and Herzegovina, there is currently no PKI on the state level for legal entities and private persons. However, there is an entire range of independent PKIs, principally electronic banking and partially in the sector of electronic government which operate in closed systems, which currently encompass or will encompass over 10,000 companies and almost 10,000 civil
servants.

Hence, the technical problem is not to such a large extent grounded on the lack of PKI at the state level. This is more a problem of gathering and linking different existing PKIs and information systems.

### 2.5 Assessment of possible consequences

Possible adverse consequences are most easily seen in the business sector and B2B and G2B transactions, where insufficiently secure and efficient regulatory environment prevents operations aimed at increasing competitiveness by decreasing costs and time required for business transactions and commerce with the government. This will also prevent companies from taking part in foreign tenders and contracts which will require electronic contracts or electronic invoices.

Implementation of the electronic signature will increase the efficiency of governments at all levels.

## III. POSSIBLE OPTIONS

The following options are proposed for implementation of the Law on Electronic Signature of BiH:

Option 1: “Do nothing”

Option 2: “Changes in the existing institutional, legal and technical framework - Root CA for BiH”

Option 3: “Model using the Pareto approach”

Option 4: “‘Bridge of Trust Model’”.

### 3.1 Option 1 – “Do nothing”

This option means keeping the current institutional and legal framework in force. Currently, in BiH businesses with certificates from the EU and third countries operate within a closed system. If this option is selected, consequences described in Chapter 2.5 will arise.

**Option 1: Benefits**

This option does not offer any benefits.

**Option 1: Costs**

It is anticipated that in case of no measures taken, the following costs will occur: increased direct and indirect/administrative costs for the public sector and the private sector.
According to the data collected from the Tax Administration of FBiH, RS and BD on costs of delivering invoices and data obtained from legal entities on the average number of invoices sent on the monthly level; also based on statistical data on population, the total annual costs of invoicing of both commercial sector and governmental institutions of BiH, FBiH, RS and BD are presented below.

The analysis includes bills for utility services, invoices between legal entities, and invoices between governmental institutions and the private sector.

In that regard, and taking into account the average GDP\(^1\) growth, the following tables and graphs present the total costs of invoicing of government institutions and the private sector in BiH.

\[\text{Table 1: Projection of total}\(^2\) costs of invoice delivery of the government sector, for a 5-year period}\]

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gov't sector</td>
<td>2,904,930 KM</td>
<td>3,024,322 KM</td>
<td>3,148,622 KM</td>
<td>3,278,030 KM</td>
<td>3,412,757 KM</td>
</tr>
</tbody>
</table>

\[\text{Graph 1: Costs of invoicing by the government}\]

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gov't sector</td>
<td>2,904,930 KM</td>
<td>3,024,322 KM</td>
<td>3,148,622 KM</td>
<td>3,278,030 KM</td>
<td>3,412,757 KM</td>
</tr>
</tbody>
</table>

\[\text{Table 2: Projection of total costs of invoice delivery of the commercial sector, for a 5-year period}\]

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priv sector</td>
<td>274,983,336 KM</td>
<td>278,894,052 KM</td>
<td>282,965,498 KM</td>
<td>287,204,282 KM</td>
<td>291,617,279 KM</td>
</tr>
</tbody>
</table>

\(^1\) Average growth of GDP was projected for the period 2011-2015 using the World Bank data for the period 2005-2009.

\(^2\) Data on total costs of invoicing have been obtained from the private sector and Tax Administrations and they include costs of paper, printing, envelopes, postage, as well as average time required to send out one invoice.
1.2 Option 2 – Changes in the existing institutional, legal and technical framework - Root CA for BiH

1.2.1 General remarks

This option is based on a model of hierarchical structure of trust and is known as the “root” PKI model (Chart 1).

There is only one “Root” CA generating digital certificate which further certifies subordinated CAs in a hierarchical structure all the way to the end-user of digital certificate. Each subordinated CA is superior to the one below, and subordinated to the one above. "Root” CA is the superior CA to all CAs and in this architecture the domain of trust represents the originating point of trust and the absolute authority.

*Chart 1. Schematic representation of the hierarchical structure of trust model*
1.2.2 Architecture in BiH

This option envisages establishment of a hierarchical PKI, whereby an institution at the State level (e.g., Ministry of Communications and Transport of BiH), competent to implement the Law on Electronic Signature, would be responsible for issuance and generation of the digital certificate, as the originating point of trust and would represent the Main “Root” CA for BiH. The Ministry can outsource operational services for the Main CA BiH to private person or legal entity meeting requirements prescribed in the Law on Electronic Signature of BiH and by-laws which then becomes the Operation Authority (OA) of the Main “Root” CA of BiH. In BiH, OA could be another state level agency, such as the Central Bank of BiH, telecommunications operators in BiH, post operators in BiH or other publicly-owned or private company which has capacities to be an OA. The decision on appointment of the Operation Authority (OA) shall be made by the Council of Ministers of BiH upon the proposal of the line Ministry responsible for implementation of the Law on Electronic Signature of BiH.

The Operation Authority would issue digital certificates to subordinated CAs on behalf of the public institution i.e. “Root” CA. CAs would further distribute digital certificates to end users under the hierarchical PKI model. In such PKI infrastructure the OA would serve as the originating point of trust or, in technical term, as the “Root” CA of BiH.

“Root” CA for BiH could, in line with the intended purpose, generate various kinds of digital certificates, among which the most important are:

- personal (for citizens),
- business (for businesses), and
- for institutions of public administration at all levels of government

Chart 2 presents one of the possible solutions in BiH under the model of “Root” CA for BiH. The PKI is hierarchical, with a principal top certificate (State-level institution of BiH). This solution, within the proposed option, to a maximum extent respects the complex (“Dayton”) administrative structure in BiH, as the subordinated CAs of this hierarchical structure are envisaged in the entities of RS and FBiH, and in Brčko District of BiH. Other solutions under this model are possible which would be subject to agreement of competent parties.

The Main “Root” CA of BiH issues certificates to entity-level CAs (RS and FBiH) and CA of Brčko District of BiH, which will further issue qualified certificates to lower subordinate CAs (or directly to end users), and these CAs further to subordinate CAs, following the hierarchical structure, all the way to the end users as the final point of trust of the PKI of BiH. In addition the Main “Root” CA of BiH could also issue digital certificates to government institutions as end users for use of digital certificates in the institutions of BiH (G2G, G2B and G2C services of the eGovernment).
A very apt candidate for the function of the Operation Authority for the “Root“ CA of BiH is the state-level Agency IDDEEA, which should surely be taken into account when choosing the OA (Operation Authority). Namely, Agency IDDEEA has a successful legacy of the strategic information project “Citizen Identity Protection System” (CIPS). CIPS provided numerous services to BiH citizens, in particular in the domain of issuance of personal documents and protection of their personal data. Likewise, IDDEEA is the CA in a closed domain of trust and issues digital certificates for public administration officers. Also, IDDEEA is the Operation Authority of the Subordinated CA of BIH (Ministry of Communications and Transport of BiH) for issuing digital certificate in a closed “Root“ PKI of EU for use of the “TachoNet” service (service for issuance of cards for digital tachographs) in the transportation sector, where the Main “Root“CA of EU of this domain of trust is the ERCA (European Root Certificate Authority) located in the EU (Italy).

It is therefore evident that IDDEEA has all the technical, professional and human resources and that, with amendments to the existing legislation which pertains to the work of the Agency, is a strong pretender for Operation Authority of the Main “Root“ CA of BiH for all types of digital certificates, if this option is selected.

Possibly, another Operation Authority for issuance of certificates for business sector only could be established within another state-level authority or in cooperation among several authorities which is a matter of possible variants of this option.

Application of this model leaves the opportunity for issuance of digital certificate by CAs registered in the EU, and CAs registered in BiH.
This option, naturally, assumes the existence of the Office for Supervision and Accreditation at the state level which will carry out the accreditation and supervision over all accredited CAs in the country.

3.2.3. Legal framework

It is necessary to establish the Office for Supervision and Accreditation of CAs which is foreseen in the Law (Article 20, Paragraph 1).

Option 2 assumes that issues which pertain to lack of harmonization between legislation are resolved, and, in that regard, a review of legislation would be carried out and necessary amendments endorsed.

Regardless of the adopted solution, it is clear that all actors need to reach an agreement to apply single supervision; otherwise they will face the costs of duplicated supervisory functions and bureaucratic restrictions on doing business throughout Entities and State.

It is necessary to harmonize the Law on Electronic Signature in RS and Law on Electronic Signature of Brčko District of BiH with the Law on Electronic Signature of BiH, as well to adopt appropriate by-laws defined in Article 26 of the Law on Electronic Signature of BiH, and to draft new by-laws that will enable adequate implementation of the Law. Although the Law on Electronic Signature of BiH (“BiH Official Gazette”, number 91/06) is fully harmonized with the Directive 1999/93/EC on the Community's framework for electronic signatures, it is necessary to amend the Decision on the Basis for Use of E-signature and Provision of Certification Services (“BiH Official Gazette”, number 21/09), as the Decision contains provisions which contrary to the EU Directive.

Article 2 which regulates fees and Article 19 on supervision and accreditation cause a particular doubt that the State imposes verification before registration of CA. Such requirement directly opposes the EU Directive and it is therefore necessary to amend the Decision in order to more appropriately regulate registration, fees and accreditation.

In addition, the Decision does not regulate in detail all the matters for which the Law on Electronic Signature of BiH (“BiH Official Gazette of BiH”, number 91/06) prescribes adoption of implementing by-laws (Article 26). Also, there are both international and European technical standards and recommendations, which need to be introduced into the legal system of BiH. These shortcomings can be removed in a way to amend the existing Decision or to adopt new by-laws for groups or for each individually, as follows:

- IETF/RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- IETF/IEC 3161, 5816 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- CAdES - CMS Advanced electronic signatures
- PAdES - PDF Advanced electronic signatures
- XAdES - XML Advanced electronic signatures
• TS 101 733 CMS Advanced electronic signatures (CadES)
• TS 102 734 Profiles of CMS of Advanced electronic signatures based on TS 101 733 (CadES)
• TS 101 903 XML Advanced electronic signatures (XadES)
• TS 102 904 Profiles XML of Advanced electronic signatures based on TS 101 903 (XadES)
• TS 102 778 Profiles of PDF of Advanced electronic signatures (Sections 1 through 5)
• TR 102 047 International Harmonization of Electronic Signature Formats
• TR 102 438 Application of Electronic Signature Standards in Europe
• TR 102 605 Registered E-Mail
• TS 102 640 Registered Electronic Mail (REM) (Parts 1 to 3)
• TS 102 231 Provision of harmonized Trust-service status information
• TS 101 861 Time stamping profile
• TS 101 862 Qualified Certificate profile
• TR 102 272 ASN.1 format for signature policies
• TS 102 280 X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
• TS 101 456 Policy requirements for certification authorities issuing qualified certificates
• TR 102 437 Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)
• TS 102 023 Policy requirements for time-stamping authorities
• TR 102 040 International Harmonization of Policy Requirements for CAs issuing Certificates
• TS 102 042 Policy requirements for certification authorities issuing public key certificates
• TS 102 158 Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
• TR 102 572 Best Practices for handling electronic signatures and signed data for digital accounting
• TS 102 573 Policy requirements for trust service providers signing and/or storing data for digital accounting
• TS 102 176-1 Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
• TS 102 176-2 Algorithms and Parameters for Secure Electronic Signatures.

3.2.4. Benefits

- Clear and comprehensive legal framework, equal for both state and entity level. A common legal framework would also mean the removal of administrative obstacles and guarantee of equal treatment for all CAs which would issue certificates.
- The PKI already exists, only upgrading required.
- Developing own public PKI would mean strengthened administrative and technical infrastructure within government institutions; and savings from reduced number of documents in traditional hard-copy form, as well as in time required for delivery of these documents in
both government and private sector. This benefit may be used for all the proposed options.

- Issuance of originate certificate by the State CA Root in BiH assumes a BiH chain of certification and control that is trustworthy, or, more precisely, the state stands as a guarantor behind each issued certificate.
- This option represents the most streamlined technical solution and offers the shortest path from the originating point of trust to end user.

Table 5: Projected savings from use of e-signatures and e-documents for the government sector, for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
</tr>
<tr>
<td>Government</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>341,276</td>
</tr>
</tbody>
</table>

Table 6: Projected savings from use of e-signatures and e-documents for the private sector, for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
<td>KM</td>
</tr>
<tr>
<td>Private</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32,305,477</td>
</tr>
</tbody>
</table>
3.2.5. Risks

Due to substantial political and institutional problems the implementation of this option might result in failure which would in fact be equal to Option 1 “Do nothing”. Option 2 could also be put at jeopardy unless additional funding for its implementation is ensured at all government levels, as demonstrated in the table with costs.

The risk for implementation of this option lies also in the fact that various digital certificates are used in existing closed systems within the state and entity-level institutions (RS Agency of Information Society, High Judicial and Prosecutorial Council of BiH, etc). If this option is implemented all these institutions would need to harmonize their PKIs with the PKI of BiH, and adopt the same digital certificate from the “Root” CA of BiH, which may be an issue.

3.2.6. Costs

Costs may arise from establishment of the Office for Supervision and Accreditation which requires procurement of necessary IT equipment, and human resources as envisaged in the document Systematization of Work Posts in the Office for Supervision and Accreditation. Also, minimal costs may arise for amending the current legislation.

The funds for establishment of PKI\(^3\) for the government sector have been calculated for infrastructures in the Entities and in Brčko District (taking into account that IDDEA already has the established PKI) and these funds would amount to approximately 1,606,197 KM, while its maintenance costs would amount to around 47,337 KM annually. Costs of the Office for Accreditation and Supervision\(^4\) amounting approximately 104,592 KM annually have been added.

---

\(^3\) Costs of establishing PKI and costs for smart cards, USB and certificates have been obtained from Halcom and Entrust

\(^4\) Costs of the Office for Accreditation and Supervision refer to gross salaries of staff in the Office
Table 3: Projected costs of use of e-signatures and e-documents for the government sector, for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government sector</td>
<td>1,710,789 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
</tr>
</tbody>
</table>

Note: In addition to the stated costs, costs of establishment of the PKI in the government sector also include costs for contracts with third parties on maintenance and implementation (outsourcing).

Planned costs for the private sector in the amount of approximately 900,000 KM which refer to purchase of smart cards, card readers or USBs, and appropriate certificates.

Table 4: Projected costs of use of e-signatures and e-documents for the private sector, for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private sector</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>894,249 KM</td>
</tr>
</tbody>
</table>

Graph 5: Costs of use of eSignature and eDocuments for the government

Graph 6: Costs of use of eSignature and eDocuments for the private sector
1.3 Option 3 – ”Model using the Pareto approach”

3.3.1. General Remarks

Pareto principle (also known as the ”80-20 rule”, the law of the vital few, and the principle of factor sparsity) states that, in many cases, roughly 80% of the consequences come from 20% of causes. This common rule of doing business (e.g., "80% of your sales come from 20% of your clients") has mathematical foundations. Where something is divided among a large enough number of participants, there must be a number x between 50 and 100 so that "x% takes (100 − x)% of participants". This number x ranges from 50 through 100, however, in reality this number moves around 80%. Pareto principle does not depend on the nature of the activity. It represents a simple, yet a powerful approach to observing organization, and, more importantly, focus on matters which are truly important.

For the areas that are analyzed in this document, the Pareto principles can be formulated in the form of the following statements and goals:

1. 80% of all G2B transactions come from 20% of subjects;
2. 20% of government services contribute to 80% of business activity;
3. 80% of citizens/companies complaints originate from 20% of administrative burdens;
4. 20% of government's effort and time achieves 80% of the desired results;
5. 80% of the value for the society / business is generated by 20% of the processes.

Hence, Option 3 anticipates resolving only important issues and pragmatically neglecting those which present a large legal or institutional obstacle or would yield too few benefit.

3.3.2 Architecture for BiH

Instead of building individual PKIs of the public sector, the existing infrastructure would be used for those purposes. Where the public sector PKI has already been established or will be established (IDDEEA PKI for citizens, closed systems in public authorities, post service, etc.) and where the legal matters are resolved, that infrastructure would be used. At the same time, the private sector infrastructure (banks and other businesses) would be used under equal conditions and as an addendum to the public sector infrastructure.
One example of such infrastructure in BiH is the infrastructure for electronic banking (Chart 3), with over 10,000 legal entities and private persons (clients) who are already using the PKI for their electronic transactions (eBanking) in the closed systems. In such banking systems, certificates are generated by CAs accredited in the EU; the CAs are contracted by the banks which use the certificates for their clients. With an additional effort, through agreement between BiH institutions and banks, the infrastructure for electronic banking can be effectively used for services of eAdministration so that with minor software and hardware upgrades the bank certificates could be used as qualified in the open system for citizens and legal entities, and for C2G and B2G services.

This solution will enable bank clients who are already eBanking users to use the same digital certificates for an access to public administration services through the banking communication channels (PKIs).

In this case, the banks would also provide particular services of electronic archiving, document safekeeping and management, all with the aim of exchanging eSubmissions and eDecisions of their clients in communication with the public administration.

As a part of Option 3, it is necessary to establish semantic and software interoperability reflected in the standardization of documents and linkage of different PKI domains to meet...
the principles of operability, openness, neutrality, economy and generalization, independently of any political impacts, which would allow to achieve complementarity and connectivity of different PKI architectures.

This approach opens possibility to use PKI via mobile telephony for which some countries in the region have already established the appropriate infrastructure. If the same infrastructure were to be established in Bosnia and Herzegovina, it would represent an ideal communications channel for small and medium companies and citizens.

### 3.3.3. Legal framework

It is necessary to form the Office for Supervision and Accreditation of CAs which is foreseen in the current Law (Article 20, Paragraph 1).

In line with the above, the Pareto principle assumes minor regulatory changes with the aim of improving efficiency of the legislation and removing unnecessary administrative burdens. Moreover, domestic service providers will be enabled to choose between registrations at the state or entity level; in addition, the existing legislation ensures the use of certificates issued in the EU. All the changes can be effected through amending by-laws which would reduce need for long and complicated legislative procedures for amending the legislation (refers to amendments to the Decision on the Basis for Use of E-signature and Provision of Certification Services, as stated under Option 2).

### 3.3.4. Benefits

- Minimal amendments to the existing legislation;
- Minimal upgrading of the existing infrastructure for enabling use of the electronic signature in open systems;
- Citizens who are bank clients and eBanking users can access the public administration’s eServices from the same place (web portal);
- Legal entities which do business with banks electronically may establish B2G services in communication with public administration authorities from the same place;
- Savings in both sectors would be evident already one year after the implementation.

Table 8: Projected savings from use of e-signatures and e-documents for the government sector, for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Government sector</strong></td>
<td>0 KM</td>
<td>302,432 KM</td>
<td>566,752 KM</td>
<td>708,055 KM</td>
<td>688,012 KM</td>
</tr>
</tbody>
</table>
### Table 9: Projected savings from use of e-signatures and e-documents for the private sector for the period of 5 years

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private sector</td>
<td>0 KM</td>
<td>28,628,515 KM</td>
<td>53,649,265 KM</td>
<td>67,025,099 KM</td>
<td>65,127,842 KM</td>
</tr>
</tbody>
</table>

### Graph 7: Savings from use of eSignature and eDocuments for the government

### Graph 8: Savings form use of eSignature and eDocuments for the private sector

#### 3.3.5. Risks

The only real risk is that the private sector does not acknowledge digital certificates issued by BIH accredited CAs.

#### 3.3.6. Costs

As in all options, costs may arise due to establishment of the Office for Supervision and Accreditation which requires procurement of the necessary IT equipment as well as human resources envisaged in the systematization of jobs at the Office.

Minimal costs are entailed because the base infrastructure exists.
This option incurs costs only for the institutions in BiH (governments) as the key assumption of this option is to use of the existing PKIs for electronic commerce. The costs pertain to the web portal and its maintenance and the Office for Supervision and Accreditation.

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government sector</td>
<td>137,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
</tr>
</tbody>
</table>

3.4. **Option 4 –“Bridge of Trust” Model**

3.4.1 **General remarks**

“Bridge of Trust” or the domain with connecting architecture is a model in which two or more independent domains of trust with different architectures, via their principal CAs, mutually “cross certificate“ through the ”Bridge of Trust” CA (BCA), making up a joint domain of trust in which all differently generated certificates are mutually acknowledged. The “Bridge of Trust“ CA is not the originating point of trust, i.e. it does not issue a digital certificate, but acts exclusively as the implementer of trust by linking different PKIs and their main CAs as the originating points of their PKIs (as presented in Chart 4).
3.4.2 Architecture in BiH

The “Bridge of Trust“ model (Chart 4), as an option for implementing the Law on eSignature of BiH, takes into account the complex administrative structure of Bosnia and Herzegovina and enables establishment of independent PKIs within the established domain of trust for eCommerce, so that one domain of trust in BiH could also be the Entity. The primary characteristic of the model is that it enables one and more CAs (certificate authority) to operate within a single domain, while each domain has one principal CA. The organization within a single domain of trust is subject to preference; either hierarchical (Root) or connecting (Bridge) and in that case the principal CAs would be either the Root CA or the Bridge CA. All these individual domains may mutually acknowledge each other by establishing a “trust” center at the state level, which represents the ”Bridge of Trust” for all trusted domains and their CAs regardless of their internal organization. This establishes a single joint domain of trust of BiH within which transactions in the electronic environment can take place without obstacles by mutual acknowledgement of all digital certificates of linked domains.

By establishing the ”Trust Center” at the level of BiH, the ”cross” certification or other level of trust among all established PKI domains and their principal CAs of any organization allows for establishment of an uninterrupted eCommerce in the entire country, and the “Trust Center“ as a ”hub” serves as a connection and trust among PKI domains within BiH and abroad.

Mutual trust is achieved by harmonizing policies of different domains of trust (Certificate Policy-CP), which are linked into a common domain of trust of BiH, which ensures:
- Linking domains of trust within BiH as the joint PKI for BiH
- Linking joint domain in BiH (PKI of BiH) with trusted domains outside BiH.

Graph 5 represents one possible example of PKI architecture in BiH and connection with other PKI domains in BiH and abroad, which to the maximum extent respects the political structure of BiH, so that the domains of trust and their accompanying PKIs are the Entities of Republika Srpska with its principal CA, Federation of BiH with its principal CA, Brčko District of BiH with its principal CA, as well as other domains of trust which do not belong to any of those, with, also, their principal CAs. Other solutions under this model are also possible which would ultimately be a matter of agreement between the competent parties.

Principal CAs are the originating points of trust for their domains.

![Chart 5. Schematic representation of one possible solution for "Bridge of Trust (BoT)" in BiH](image)

In this case, the Entities, Brčko District of BiH and others may separately and individually establish their own PKI or several of them, and through the “Trust Center” (BoT) on the level of BiH accomplish mutual link and trust.

In addition to the solution presented in Chart 5, many other solutions are also possible which can be implemented in case Option 3 from Chart 4 is applied.

Policy of trust in the PKI domain of BiH would be adopted by the Policy Management Authority (PMA), which would be appointed by the Council of Ministers of BiH, and whose members would include an equal number of representatives of the State-level of government, Entities and Brčko District of BiH, as well as representatives of principal CAs of their
domains. Thereby, the PMA would manage the work of the “Trust Center” “(BofT) and its repository. All competencies and responsibilities of this body would be specified in detail if this option were to be accepted.

Implementation of this model also requires establishment of the Office for Supervision and Accreditation at the State level, but also opens the possibility to establish the “Entity-level” office as well, provided that it is essential to establish adequate coordination between the “Entity-level” office and the ”State-level” Office that will ensuring all necessary standards and legal framework for safe and unhindered eCommerce in the PKI domain of BiH.

By implementing this option, all interested parties in BiH would be able to select where to submit requests to act as certification service providers, while their digital certificates would be valid across the BiH, regardless of where they were issued.

3.4.3 Legal framework

The legal framework includes amendments to the Decision on the Basis for Use of E-signature and Provision of Certification Services, as explained under Option 2. It is also necessary to form the Office for Supervision and Accreditation which is envisaged in the relevant legislation (Article 20, Paragraph1).

3.4.4 Benefits

This option takes into account the complex administrative structure of Bosnia and Herzegovina and allows for implementation of the Law on eSignature of BiH in a highly decentralized way.

It also provides for the possibility to include both Option 3 and, partially, Option 2 (hierarchic structure within particular domains of trust), it recognizes the current legal framework for eCommerce with minimal amendments as in Option 3.

It also allows:
- Validity and mutual acknowledgment of all digital certificates across the entire BiH,
- Commerce with different certificates without jeopardizing a safe environment for eCommerce in line with the international standards,
- Establishment of a free market of certification service providers in the whole BiH,
- Citizens, legal and commercial entities as users of digital certificates have free choice of a digital certificate and its provider.

3.4.5 Risks

Possible risks may arise through setting level of trust among domains of trust in the architecture of the connecting domain (bridge).

Longer paths from the originating point of trust to the end user and procedures of mutual acknowledgment require a more complex technical security aspect.

Technical risks primarily refer to the interoperability framework. Bosnia and Herzegovina still does not have a developed interoperability framework which should be harmonized with the European Interoperability Framework. For that reason, difficulties may arise in the course of communication with the CAs that are accredited in the EU member countries.
3.4.6 Costs
-Costs related to establishment of the Office;
-Costs related to establishment of the “Trust Center” at the State level;
-Costs of establishment of PKIs in the Entities and Brčko District of BiH;
-Overall costs should be substantially reduced because of the use of the existing infrastructures.

IV. POTENTIAL IMPACTS

Accelerating the introduction of eSignature is of a great importance for BiH as the country is currently lagging behind in its implementation which also means that implementation of all services that use eSignature are also slowed down (eTrade, eBanking, eAdministration, eCommerce).

If a decision were made not to change anything (Option 1), BiH would fall even further behind other EU member countries and countries in the region in terms of eCommerce. In that case, there would be an increase in direct and indirect/administrative costs for the public sector and private sector.

Option 2 is technically the simplest, but requires harmonization of legislation in BiH in this area (Laws on eSignature of RS and Brčko District of BiH are to be harmonized with the Law on eSignature of BiH), which would ensure a clear competency at the State and Entity level, and strengthen the administrative and technical infrastructures with skills and knowledge.

The main problem for implementation of Option 2 is of political nature where particular political circles believe that implementation of this option would jeopardize the competencies of the Entities, which is absolutely not correct. As a result of such and similar opposing political positions, implementation of Option 2 might result in failure, which would ultimately be equal to Option 1 “Do nothing”.

If Option 3 were applied, meaning pragmatic introduction of all those changes which under the Pareto principle (20% changes for 80% effect) would bring about greatest benefits, minimum changes to the existing legislation and minimal costs would be implied as the base infrastructure already exists and this represents an upgrade of the existing status and good foundation for implementing Option 4.

Option 4 is ultimately decentralized, takes into account the complex structure of Bosnia and Herzegovina, enables transactions with different certificates, and also establishes a market of certification service providers in the entire BiH. By implementing Option 4, requests to act as certification service providers would be submitted at the place of own choice and, thereby, all types of certificates would be acknowledged in the entire BiH. Option 4 currently represents the state-of-the-art solution in application of electronic signatures and as such should be the ultimate goal towards which BIH strives in the upcoming period.
Costs and savings for particular options for the government and private sector are provided in tables 10 to 13.

Table 10: Costs of individual options for the government sector

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION 1</td>
<td>2,904,930 KM</td>
<td>3,024,322 KM</td>
<td>3,148,622 KM</td>
<td>3,278,030 KM</td>
<td>3,412,757 KM</td>
</tr>
<tr>
<td>OPTION 2</td>
<td>1,710,789 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
<td>151,929 KM</td>
</tr>
<tr>
<td>OPTION 3</td>
<td>137,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
<td>107,592 KM</td>
</tr>
</tbody>
</table>

Table 11: Costs of individual options for the private sector

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION 1</td>
<td>274,983,336 KM</td>
<td>278,894,052 KM</td>
<td>282,965,498 KM</td>
<td>287,204,282 KM</td>
<td>291,617,279 KM</td>
</tr>
<tr>
<td>OPTION 2</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>894,249 KM</td>
</tr>
<tr>
<td>OPTION 3</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
</tr>
</tbody>
</table>

Table 12: Savings from individual options for the government sector

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION 1</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
</tr>
<tr>
<td>OPTION 2</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>341,276 KM</td>
</tr>
<tr>
<td>OPTION 3</td>
<td>0 KM</td>
<td>302,432 KM</td>
<td>566,752 KM</td>
<td>708,055 KM</td>
<td>688,012 KM</td>
</tr>
</tbody>
</table>

Table 13: Savings from individual options for the private sector

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTION 1</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
</tr>
<tr>
<td>OPTION 2</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>0 KM</td>
<td>32,305,477 KM</td>
</tr>
<tr>
<td>OPTION 3</td>
<td>0 KM</td>
<td>28,628,515 KM</td>
<td>53,649,265 KM</td>
<td>67,025,099 KM</td>
<td>65,127,842 KM</td>
</tr>
</tbody>
</table>

Note: Savings of Option 3 are evident immediately in 2013, since Option 2 requires the most time for implementation.

V. PERFORMANCE INDICATORS – MONITORING AND AUDIT

The following are proposed as the main indicators for monitoring of implementation:

First indicator is the **successful harmonization of by-laws in line with the legal framework and technical regulations of the EU**. The existing Decision on the Basis for Use of E-signature and Provision of Certification Services (“BiH Official Gazette”, number 21/09) is not harmonized with the EU Directive and does not regulate all matters for which the Law prescribes adoption of by-laws; or matters regulated by international and European technical
standards and recommendations which need to be introduced in the legal system of BiH. Consequently, adoption of all required by-laws is a clear indicator.

Second indicator is the establishment and efficiency of supervision by the competent authorities. At this time, the competent ministry does not have capacities for carrying out supervision over implementation of the law in the area of e-signature. In that regard, successful implementation is primary reflected in establishing the Office for Supervision and Accreditation within the competent ministry and, afterwards, in the number of inspection and administrative proceedings carried out by the Office.

As each person requires a certificate for eSignature, the number of issued regular and the number of issued qualified certificates by domestic or EU CAs clearly demonstrates the status. Nowadays the estimate for BiH is that around 12,000 regular certificates (10,000 for enterprises and 2,000 for civil servants) and around 100 qualified certificates have been issued. Comparative data for EU countries demonstrate 30 times greater number of issued certificates (if the data is put in relation to the population), and for the countries in the region 2 to 3 time more issued certificates then in BiH.

Last two indicators are the percentage of use of eBanking services and eAdministration for the population and for companies. Indicators for EU demonstrate that eBanking for population is used by about 60% of the population and the services of eAdministration by around 40% of the population. In terms of companies, eBanking is used by 80 to 95% of companies and the services of eAdministration by about 75% enterprises. In addition to these indicators, it is possible to use all 60 EU indicators (http://ec.europa.eu/information_society/eeurope/i2010/benchmarking/index_en.htm).

VI. CONSULTATIONS

In the course of preparation of this document passive and active consultations with all relevant partners in the government sector and the private sector were conducted.

Active consultations

a) As a part of active consultations, three workshops were held which served as the platform for exchange of opinions with stakeholders from the public and private sectors and relevant experts from this domain:

1. The first workshop on the topic of "Use of eSignature in closed systems in BiH with the focus on electronic banking", held on 1 December 2010 in Sarajevo, provided substantial support of all participants (32 participants from 15 institutions and companies) for the idea of conducting a comprehensive impact analysis that would remove all existing dilemmas and obstacles and would enable full implementation of eSignature in BiH.

2. As the first step in development of impact assessment methodology, training on Methodology of Regulatory Impact Analysis (RIA) with a focus on eSignature was held in Sarajevo on 21 December 2010, with the aim of making all relevant participants in the process familiar with the methodology. Active contribution during this workshop was
3. The first working paper with options on implementation of the Law on e-Signature of BiH was presented in a two-day workshop in Teslić, on 19 and 20 of April 2011, attended by 40 participants from 26 institutions, organizations and companies.

b) As a part of active consultations, 10 individual meetings were held with a focus on matters of special interest, requiring specific knowledge, experience and skills.

c) The first working draft document of the Regulatory Impact Analysis on the legal and institutional framework for electronic signature with the proposal of options for implementing the Law on eSignature of BiH has been submitted by e-mail to 31 institutions, organizations and companies; out of which feedback was received from 27 institutions, organizations and companies, as follows:

1. General Secretariat of the Council of Ministers of Bosnia and Herzegovina  
2. Ministry of Finance and Treasury of Bosnia and Herzegovina  
3. Parliamentary Assembly of Bosnia and Herzegovina  
4. Central Bank of Bosnia and Herzegovina  
5. High Judicial and Prosecutorial Council of Bosnia and Herzegovina  
6. Indirect Taxation Authority of Bosnia and Herzegovina  
7. BiH Agency for Identification Documents, Registers and Data Exchange (IDDEEA)  
8. Accreditation Institute of Bosnia and Herzegovina  
9. Public Administration Reform Coordinator’s Office (PARCO)  
10. General Secretariat of the Government of Federation of BiH  
11. Federal Ministry of Communications and Transport of Federation of BiH  
12. General Secretariat of the Government of Republika Srpska  
13. Ministry of Science and Technology of Republika Srpska  
14. Tax Administration of Federation of BiH  
15. Tax Administration of Republika Srpska  
16. Agency for Information Society of Republika Srpska  
17. Government of Brčko District of BiH  
18. Agency for Informatics and Statistics of Canton Sarajevo  
19. Employers' Association of Bosnia and Herzegovina  
20. Association of Banks of Bosnia and Herzegovina  
21. Association of Informatics of Bosnia and Herzegovina  
22. Association for information technologies in Bosnia and Herzegovina B@IT  
23. BH Telecom  
24. m:tel  
25. Asseco, South Eastern Europe Pexim Solutions  
26. Electronic Banking Bureau (EBB)/Halcom  
27. Lanaco Banja Luka

Below is a summary of results of the consultations:

- It is necessary to develop and endorse an Action Plan which clearly defines steps and obligations of all stakeholders for a full implementation of electronic signature in BiH. Also,
it is necessary to define outstanding issues by adoption of appropriate by-laws pursuant to the Law on Electronic Signature of BiH and also form an appropriate supervisory authority which will monitor the implementation and control the regulations. It is important to note that additional amendments to other relevant by-laws will be necessary for a full implementation of electronic signature. It is equally important to establish an appropriate practice on particular issues, for example that the email as the mean of communication may and should be considered equally valid and acceptable as the fax or any other statement and, in that regard, to make additional corrections to by-laws to prescribe very strict rules (use of qualified signature, time stamp, etc.).

- It is necessary to coordinate future activities on implementation of the electronic signature within BiH to achieve the best possible quality results, and, thereby, the effects of implementation of the electronic signature as efficient as possible.

- The need for developing high-quality electronic services that would help not only the government and private sector, but also citizens was pointed out. The example for this statement is the anticipated possibility of issuing the e-identification card in 2013, in line with the adopted strategy of the Council of Ministers of BiH for the period 2010 - 2015. Without adequate electronic services, efforts on introducing the e-identification card will not provide desired results.

- The private sector, and IT companies in particular, represents a huge development potential in BiH and further delay in use of electronic signature constitutes a direct loss for economic development in BiH and brings this sector into even more unfavorable position comparing to IT companies in the region.

- Implementation of electronic signature is of extreme importance for further development of the banking sector, in particular for further development of modern electronic banking; slow implementation of e-signature slows down establishment of links between business community and tax administration, and daily e-transactions. The establishment of a secure and modern electronic banking is necessary for monitoring and control of possible “money laundering” activities and for combating funding of illegal activities. The existing banking PKI can serve as a realistic basis for introduction of e-Government, in particular with a view to costs of developing and maintaining PKI as well as the size and actual needs of the country.

- It is necessary to take into account the IT literacy of citizens, business community and the public sector in BiH. In this regard, the experiences and professional knowledge of the existing associations of IT professionals in BiH should be used. Also, introducing electronic signature would entail the work on developing the consumer protection.

- Adequate and efficient implementation of electronic signature should be followed by well-prepared public campaign which would point out all the benefits of full application of electronic signature.

- It is important to underline that social consequences of increased use of electronic signature should be considered as the comprehensive implementation of electronic signature and further informatization might lead to lay-offs.
VII. SUMMARY AND RECOMMENDATIONS

In preparing the final document of the Regulatory Impact Analysis, Ministry of Communications and Transport of BiH as the initiator and responsible authority undertook comprehensive activities with all stakeholders, and the consultations included representative of the government, business and non-government sector, as stated above.

Upon adoption of this document, the following activities of the Ministry of Communications and Transport of BiH are required:

a) To develop by-laws for implementation of the Law on Electronic Signature of BiH and initiate the procedure for their adoption;
b) To initiate procedure for amending the Rulebook on Internal Organization and Systematization of Work Posts in order to meet requirements for establishing the Office for Supervision and Accreditation and complete the hiring procedure to fill the vacancies in the Office;
c) To launch the process of hiring for vacancies in the Office for Supervision and Accreditation by internal or external reallocation of civil servants in the Office; and
d) To ensure adequate training of staff at the Office.

The working team analyzed data and opinions gathered through the consultations, also the experience and available information from other countries in the region and the European Union.

As the most realistic and most rational solutions for implementation of the BiH Law on Electronic Signature the working team proposes implementation of Option 3 – Method using Pareto principle, and Option 4 - Bridge of Trust as the further upgrade and the path towards establishment of a single joint domain of trust for electronic commerce in BiH that takes into account the complex administrative structure of BiH.

The implementation of these options would enable the local CAs to choose to register either on the State or on the Entity level. Also, the existing regulations provide for use of certificates issued in the EU and all certificates would be mutually acknowledged through a third “Trust Center”. Instead of high costs for establishment of public PKIs, the existing channels and infrastructure would be used. In those instances where the public sector PKI is already established or will be established (IDDEEA PKI for citizens, closed systems in public authorities, post services, etc.) and where legal matters are resolved, this existing infrastructure would be used. At the same time and under equal terms the private sector infrastructure, mostly the bank infrastructure, would be used as the supplement to the public sector infrastructure. As the business entities already have digital certificates and the required software, such certificates would be upgraded from the existing closed system to open systems with qualified digital certificates.
### ANNEX 1

#### Required data and assumptions for CBA analysis

<table>
<thead>
<tr>
<th>Data</th>
<th>Source</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>BIH Statistics Agency, data for 2010</td>
<td>3,842,566</td>
</tr>
<tr>
<td>Number of invoices for population</td>
<td>According to data from earlier analysis, assumption is that the citizens pay (1.5) invoices per capita monthly</td>
<td></td>
</tr>
<tr>
<td>Number of invoices for 1 company</td>
<td>Private sector</td>
<td>40 invoices a month</td>
</tr>
<tr>
<td>Cost of sending out (1) invoice</td>
<td>Post offices, bookstores – assumption is that the parties mostly use regular mail</td>
<td>2.6 KM</td>
</tr>
<tr>
<td>Total number of enterprises and entrepreneurs in BiH</td>
<td>Tax Administrations, data for 2010</td>
<td>105,862</td>
</tr>
<tr>
<td>Costs of Tax Administration of RS, FBIH and DB for invoicing</td>
<td>Tax Administrations of FBIH, RS and BD</td>
<td>832,634.50 KM</td>
</tr>
<tr>
<td>Cost of the government of RS, FBIH, BD and BiH for invoicing</td>
<td>Assumption is that the total number of sent invoices by the government sector is (2.5) times greater that the invoices of Tax Administration</td>
<td></td>
</tr>
<tr>
<td>Average growth of GNP</td>
<td>The World Bank Group database - data obtained on the grounds of average GNP growth in the last (5) years</td>
<td>4.11%</td>
</tr>
<tr>
<td>Time needed to send out (1) invoice</td>
<td>Private sector, government sector</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Average hourly wage</td>
<td>BIH Statistics Agency, data for 2010</td>
<td>6.88 KM</td>
</tr>
<tr>
<td>Establishing PKI (CA): Authority Security Manager (CA)</td>
<td>Entrust – analysis done for (3) CAs ((3) entity-level CAs with assumption that IDEEA will assume the role of the key CA)</td>
<td>25,000 EUR</td>
</tr>
<tr>
<td>150,000 certificates</td>
<td></td>
<td>150,000 EUR increased by (20)% of clients who will use services of (2) CAs</td>
</tr>
<tr>
<td>Implementation services</td>
<td></td>
<td>50,000 EUR</td>
</tr>
<tr>
<td>Server and HSM HW</td>
<td></td>
<td>100,000 EUR</td>
</tr>
<tr>
<td>Web portal costs</td>
<td>Entrust and Halcom</td>
<td>60,000 KM</td>
</tr>
<tr>
<td>CA maintenance</td>
<td>Entrust and Halcom</td>
<td>5,000 EUR</td>
</tr>
<tr>
<td>Web portal maintenance</td>
<td>Entrust and Halcom</td>
<td>10% value of the web portal</td>
</tr>
<tr>
<td>Smart card Card reader USB Certificate (3 years)</td>
<td>EBB – client is using either a smart card or a USB- average costs for analysis taken Halcom and Entrust</td>
<td>104.50 KM 58.50 KM 156 KM 68.50 KM</td>
</tr>
<tr>
<td>Number of companies using the Internet</td>
<td>Regulatory Agency for Communications – assumption is that in the first year (10)% of these enterprises will use e-signature and e-documents</td>
<td>50%</td>
</tr>
<tr>
<td>Office for Supervision and Accreditation</td>
<td>Government sector</td>
<td>1. Head of the Office = 39,024 KM 2. Expert Advisor for Inspections = 32,784 KM</td>
</tr>
<tr>
<td>3. Expert Advisor for Development of e-Signature and e-Commerce</td>
<td>32,784 KM</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Total gross salaries and benefits on the annual level– 104,592 KM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>