Project Fiche – IPA Annual Action Programme 2007 for Bosnia and Herzegovina

Public Key Infrastructure (PKI) implementation on Citizen Identification Protection System - CIPS locations responsible for issuing CIPS documents

1. Basic information

1.1 CRIS Number:

1.2 Title: Public Key Infrastructure (PKI) implementation on Citizen Identification Protection System- CIPS locations responsible for issuing CIPS documents

1.3 ELARG Statistical code: 03.10 – Information society and media

1.4 Location: Bosnia and Herzegovina, Ministry of civil affairs BIH, Directorate of CIPS, Sarajevo

Implementing arrangements:

1.5 Contracting Authority (EC): EC Delegation in Bosnia and Herzegovina

1.6 Implementing Agency:

EC Delegation in Bosnia and Herzegovina
Task Manager: Jeroen Willems
Contact: jeroen.willems@ec.europa.eu

1.7 Beneficiary:

- Institution: Directorate for CIPS project implementation
  Ministry of civil affairs BIH
  Senior Programming Officer (SPO):
  Name: Mr. Srđan Nogo
  Address: Trg BIH 1, Sarajevo
  Phone: +387 33 713 270
  Fax: +387 33 219 412
  E-mail: srdjan@cips.gov.ba, sinisa.macan@cips.gov.ba, dimitrije@cips.gov.ba, it_sector@cips.gov.ba

Secondary beneficiaries:

- Ministries of internal affairs in BIH(Republic Srpska , Federation BIH and Brcko District).

1.8 Overall cost: 400,000 EUR

1.9 EU contribution: 400,000 EUR

1.10 Final date for contracting: N+2

1.11 Final date for execution of contracts: N+4

1.12 Final date for disbursements: N+5

2. Overall Objective and Project Purpose

2.1 Overall Objective

Modernisation of public administration

2.2 Project purpose

Improve security level of CIPS information systems through introduction of PKI technology.

2.3 Link with AP/NPAA / EP/ SAA

The draft Stabilisation and Association Agreement (SAA) makes a reference to the White book of European Union component dealing with the protection of personal data. Article 79 of the draft SAA states:

"Bosnia and Herzegovina will harmonise its legislation concerning personal data protection with Community law and other European and international legislation on privacy upon the entry into force of this Agreement. Bosnia and Herzegovina will establish independent supervisory bodies with sufficient financial and human resources in order to efficiently monitor and guarantee the enforcement of national personal data protection legislation. The Parties will cooperate to achieve this goal."

2.4 Link with MIPD

The MIPD 2007-09 section on European standards, more in particular section 2.2.3.2, refers to the need for the BIH Strategy and Action Plan for the development of the BIH information society to be implemented. The national legislation to the EU regulatory framework for electronic communication and services will need to be aligned with existing EU standards in order to improve the security level of CIPS information systems. This could be done through the introduction of PKI technology.

The political requirements section of the MiPD, and more in particular section 2.2.1.3 states that Implementation of the Public Administration Reform Strategy and action plans, would need to be supported. The introduction of PKI in the BiH public administration is explicitly mentioned in the PAR Action Plan.

2.5 Link with National Development Plan

N/A

2.6 Link with national/ sector investment plans:

As mentioned above, this project is fully aligned with the PAR Strategy. Action Plan 1 states the following ambition: Activity IT.3.5 Implement Public Key Infrastructure (PKI).

PKI is the most common technology used to implement electronic signatures. With the passing of appropriate legislation, such as the Law on Electronic Commerce and Electronic Signatures, the introduction of PKI has become necessary for their implementation.

This project is aligned with the European Integration Strategy, and particularly its section on information society (section 2.3.3.1). It states the need for data files and computer programmes to be better regulated and to start introducing ICT standards to administrative bodies.

3. Description of project

3.1 Background and justification:

The Directorate for CIPS project implementation was established by the Decision of the Council of Ministers published in the Official Gazette 12/02, and defined as an independent Department within the Ministry of Civil Affairs by the Law on Ministers and other Administrative Bodies (Official Gazette BIH No. 5/03).

Pursuant to Article 2 of the Decision on the establishment of the CIPS Directorate, its mandate is defined as: "i) to implement CIPS projects, ii) to cooperate with competent authorities in Bosnia and Herzegovina and international organisations involved in CIPS projects implementation, iii) to coordinate and manage the activities of providing financial resources for CIPS projects implementation, and iv) to perform other tasks and duties pertaining to CIPS project implementation".

The laws from which the above described tasks for the CIPS Directorate originate, have been published in the Official Gazette BIH No. 32/01 *(Details in Annex3)*. The aforementioned laws initiated the establishment of CIPS Directorate. The activities of the CIPS Directorate are also regulated through the laws pertaining to registers as defined in the Law on Central Records and Data Exchange *(Details in Annex3).*

The main aim defined in the Decision on the establishment of the CIPS Directorate is the implementation of the CIPS project. Since its establishment many additional projects and ICT infrastructure essential for a number of institutions has been established, which are all maintained by the CIPS Directorate.

In 2006, by changes and amendments to the Election Law, the role of CIPS Directorate was defined within the election process. Also by conclusions and decisions of the Council of Ministers as well as by signatures of memorandum with the Delegation of European Commission to BIH, it has been defined that the Directorate manages and owns the network for data transfer for the needs of public security in BIH.

Though the Directorate for CIPS project implementation is a direct beneficiary of the proposed assistance, it has important impact to the overall public administration structures in BIH. In accordance with laws describing CIPS directorate responsibilities, it has been implementing or supporting a number of information systems that are important for the entire state of Bosnia and Herzegovina.

Among others, these include the following:

- JMB number
- Residence
- ID card
- Driver's licenses
- Registration of vehicles
- Passports
- Visas and residence permits
- Standard police reports
- Criminal records and records of criminal acts perpetrators
- Records of companies' registers
- Citizenships records
- Database of Nationality-Citizenship
- Database of personal weapons of citizens and official persons

The running information system centrally maintained by the CIPS Directorate connects several central databases with around 350 remote locations in order to allow the issuing of personal documents (ID, driver licence, passport etc..) by administrative institutions on all governmental levels (cantons, municipalities).

CIPS provides technical facilities (networking, maintains databases and servers etc.) to the relevant responsible institutions; mainly the Ministries of internal affairs in BIH (Republic Srpska, Federation BIH and Brcko District).

The BiH Ministry of civil affairs is the authorised body for personal data entry of BIH citizens through web CIPS application. CIPS locations are functioning under the tutelage of the Ministry of civil affairs and within its premises.

To ensure security of the information systems, the CIPS Directorate uses standard security tools for protection of its databases and applications against unauthorized access to the information systems. The CIPS Directorate has made an assessment of security risks, and concluded that the standard tools currently used are insufficient to ensure an adequate security

level of its information systems.

This conclusion derives from the fact that the data flows between central CIPS databases and remote locations are not encrypted, which potentially allows unauthorised access to the data and pilferage of personal identities. Moreover, any user of the information system, who has access to only limited parts of the database can also potentially access other personal data of BIH citizens to which he/she is not authorised.

With the accumulation of more and more databases (and more users) to the existing CIPS information system, this risk will only further increase. Moreover, due to the incremental growth of the CIPS information system, ad hoc security measures can only partially mitigate these risks. Therefore a more systemic solution, such as through the introduction of PKI, is urgently called for. Through the systemic introduction of PKI in the CIPS information system, access to personal data will be better channelled and organized.

Through implementing PKI technology for all its information systems, CIPS will be able to improve the security level of all above mentioned databases and ensure an appropriate security level of future databases.

Through the introduction of PKI, the following can be achieved:

1. In order to accomplish protection level for all database access it is necessary to create a system for issuing certificate and crypto keys.
2. Crypto keys are going to be installed on a "smart card" issued to all beneficiaries on CIPS locations for issuance of personal documents.
3. Mentioned security will provide two factors: auto-unification necessary to keep confidence in system and data entries in CIPS database.
4. In the frame of security measures needed for CIPS information system, the following are specifically requested: keeping confidence, integrity and information availability in property, and certain organization units.
5. Security measures in order for all employees be responsible for entering data, all contractor and business partners to accept the roles and responsibilities in the mentioned process, access, exchange and movement of all electronic information that is kept or is passing through the CIPS information system.

These measures are fully in line with the provisions set out in the White book of European Union component dealing with the protection of personal data. This document states amongst others that technical progress in the field of information processing of personal data for various government purposes (administrative checks, business purposes, scientific research especially epidemiology, public statistics, etc.) have highlighted the need to protect the private life of individuals and their fundamental freedoms and rights. There is evidence of significant increase in flows of personal data within the EU, in particular because of the completion of the single market. These flows include the flows between companies, between divisions of the same company, between national administrations, between centres of epidemiological research etc. *As mentioned above, the proposed project is also in line with art 79 of the SAA.*

3.2 Assessment of project impact, catalytic effect, sustainability and cross border impact

The systematic introduction of PKI technology is a high priority for the CIPS Directorate. As stated above, it would ensure better and more secured access to the various CIPS databases, in line with ICAO standards. Hence, through the introduction of PKI infrastructure, security will become in line with ICAO standards and the protection of personal data can be better guaranteed. Moreover, it is envisaged that PKI introduction will lead to an enhanced technical performance of the entire CIPS information system and should trigger other administrative institutions to follow the same example, in line with the ambitions set by the PAR strategy.

Impact:
The results of the project; i.e. enhanced security level of CIPS information systems, will provide a fundament for a strong country-wide push towards the development of e-Government in line with Information Society Development Strategy adopted by the Council of Ministers in 2004. The Strategy emphasizes re-engineering of the public administration, communication and IT infrastructure, inter-operability, security, computerization of fundamental registers, digitalization of joint and specialized functions of the administration, e-democracy, electronic services as well as Internet portals and access points. Introduction of PKI is in line with this ambition.

Catalytic effect:

The introduction of PKI infrastructure in the CIPS information systems, will allow for the introduction of other ICT services, such as E–passport, Integration of Civil registry and passport information systems.

Sustainability:

The PKI system will require regular updating and maintenance after its installation. The CIPS Directorate estimates that approximately 40,000 EUR/year (additional equipment and staff – 2-3 persons) might be required for this purpose. CIPS Directorate will ensure that these resources necessary are budgeted for as of 2009.

CIPS will ensure that as of 2009 annual maintenance costs for the PKI system – approximately 40,000 Euro per year – are budgeted for.

3.3 Results and measurable indicators:

Result 1: PKI infrastructure and applications provided to all CIPS systems

Result 2: Internal capacity building to ensure security PKI system is in place

Measurable indicators

- PKI applications installed and accepted by the beneficiary
- PKI applications become operative
- Training need assessments report
- Certification for trainers
- Number of staffed trained

3.4 Activities:

To deliver the results specified, inputs from one supply and one service contracts will be required. The CIPS Directorate will prepare detailed technical specifications of the required hardware and software for PKI system that is compatible with existing and planned information systems of CIPS. CIPS will deliver these specifications in the last quarter of 2007, in order for the EC to start the procurement procedure right after signature of the Financing Agreement.

The activities for these two contracts are further detailed below:

The supply contract:

1.1 Installation of hardware and software

The service contract:

2.1 PKI system developed in accordance with functional technical requirements.

2.1.1 Development of application solutions of Identity and Card Management Subsystem, Personalization Center Subsystem.

2.1.1.1 Development of module of application solution Identity Check and Validation.

2.1.1.2 Development of module of application solution Prohibition Management.

2.1.1.3 Development of module of application solution Management.

2.1.1.4 Development of module of application solution Database Management.

2.1.1.5 Development of module application solution Production Management System.

2.2 Development of PKI and Security Subsystem

2.2.1 Development of module of application solution Certification Authority Client.

2.2.2.1 Development of module of application solution PKI Client,

2.2.2.2 Development of module of application solution Crypto Firewall,

2.2.2.3 Development of module of application solution ID CA

2.2.2.4 Development of module of application solution Certification Authority Server.

2.2.2.5 Development of module of application solution HTTP Crypto Proxy,

2.2.2.6 Development of module of application solution Secure log-on,

2.2.2.7 Development of module of application solution Cryptographic API.

3.1 Training of the trainers

3.1.1 Delivering of the training for 10 systems administrators and 30 local administrators (local administrators will pass "Train the trainers")

3.1.2 Preparing training manuals for system administrators, local administrators and users on the CIPS remote locations for issuing personal documents

3.2 Installation, configuration, tuning and testing of PKI system

3.3 Documentation management

3.3.1 System usage documentation.(Minimum)

3.3.2 Development of system operative procedure (backup and recovery)

3.3.3 Installation procedures for entire PKI system

3.4 PKI system enters exploitation

3.5 Conditionality and sequencing:

There is no conditionality to start project activities. The contracts can be tendered simultaneously.

3.6 Linked activities:

Previous CARDS projects where CIPS was direct partner in implementation are listed below:

Information migration system (MIS)

The goal of the project is to construct and implement a Migration Information System for the government of Bosnia and Herzegovina (BIH). At the Network operational center (NOC) in Sarajevo, the central database will be stored and a mirror of this database will be located in NOC Banja Luka. In all the other locations it is possible to connect to the central database and relevant information will be entered into the database and it will be possible to see the status of the procedures a foreigner is processing in BIH. The MIS will provide information that will assist the parties involved to manage migration information, data collection, processing and dissemination by keeping record of the stay and movement of aliens who have been admitted to BIH, including :

- All residence permits that have been issued by the Ministry of Security
- Foreign nationals that have been admitted to BIH with visas
- Foreign nationals who have been ordered to leave BIH and/or been put under supervision until they are removed
- Foreign nationals who have entered BIH as a result of a readmission agreement
- A file tracking system for the administrative decisions related to aliens

The MIS will be integrated with other national information systems. The key beneficiary of the project has been Ministry of Security, while CIPS Directorate has been provided technical support in development of MIS.

Synchronous Digital Hierarchy SDH communication network

CARDS 2005 project with overall objective of providing assistance to CIPS Directorate for Building SDH. This telecommunication network system should provide coordination between institutional units who are responsible for providing security masers by using digital exchange of information, access central databases and access through integrated communications. This project removed organizational and operative problems when it comes to using confidential information and rendered using and exchange information more secure.

Other relevant projects are:

Support to the Office of the Coordinator for Public Administration Reform (1.5 MEUR)

This project is assisting the PAR Coordination Office with the design and implementation of a comprehensive nation-wide PAR strategy. The strategy describes a longer term vision for the Public Administration in BiH, which will be further operationalised in action plans. PAR Action Plan drafting will be done in two phases and will subsequently contain two chapters. Action Plan 1 focuses on strengthening of the horizontal systems: public finance, human resources management, legislative drafting, administrative procedures, ICT/e-Government, and inter-institutional communication and was adopted together with the Strategy. Action Plan 2, in the making, will focus more on the sectoral functional reviews and will take a look at the reorganisation of sectoral responsibilities, as well as the entire "administrative architecture". In addition, the project also builds capacity of the PARCO; particularly in the area of PAR policy making and coordination and procurement of PAR projects through the newly established PAR fund, which pools funds from DfID, Sida and the Dutch Government.

e-Government (1.5 M EURO)

This project aims to enhance the efficiency of the Council of Ministers BIH through the introduction and utilization of comprehensive and crosscutting set of ICT tools and solutions, as well as through necessary re-engineering of CoM business processes. It further supports the building of capacity of the Government to manage grant resource.

3.7 Lessons learned

Specific problems which are persisting and impact upon the overall effectiveness of the implementation of the past CARDS projects are:

Network. Project implemented in the past and directly financed trough CARDS program was very important for CIPS directorate in the early beginning of Directorate establishing.

During implementation of these projects we had constant problems with network connection

and project partner correspondence through CIPS system. (We did not have a good solution for connecting partners work station on the CIPS system through existing networks.)

Other users from other state institutions that are not connected to CIPS network systems solved their connection problem by installing Asymmetric Digital Subscriber Line (ADSL) (which is a form of DSL, a data communications technology that enables faster data transmission over copper telephone lines than a conventional modem can provide) in their Diplomatic Posts Overseas.

We realised from the past experience how we need to implement PKI infrastructure solution just and only on the working station which are CIPS' property and which are fully controlled by the CIPS Directorate system.

Procedures. In the sense of learning from the past experiences and after deep analysis of the existing CIPS system we realise how existing procedures need to be updated with PKI Infrastructure. General idea is that we will follow applicable standards already used in countries candidates for joining EU.

Legislation. Prior to any operational use of any future developed systems it is necessary to complete the relevant Books of Rules.

4. Indicative Budget (amounts in €)

Activities	TOTAL COST	SOURCES OF FUNDING										
		EU CONTRIBUTION				NATIONAL PUBLIC CONTRIBUTION					PRIVATE	
		Total	% *	IB	INV	Total	% *	Central	Regional	IFIs	Total	% *
Supply of hardware and software	164,000.00	164,000.00	100		*164,000.00*	0	**0**					
Service contract	236,000.00	236,000.00	100	*236,000.00*		0	**0**					
TOTAL	**400,000.00**	**400,000.00**		**236,000.00**	**164,000.00**	**0**	**0**					

5. Indicative Implementation Schedule (periods broken down per quarter)

Contracts	Start of Tendering	Signature of contract	Project Completion
Supply of hardware and software	Q1 2008	Q2 2008	Q3 2008
Service contract	Q1 2008	Q2 2008	Q1 2009

6. Cross cutting issues

6.1 Equal Opportunity

Equal opportunity for participation of men and women will be assured in all aspects of project implementation.

6.2 Environment

The project will not have any negative environmental effects.

6.3 Minorities

Participation in the project activities will be guaranteed on the basis of equal access regardless of racial or ethnic origin, religion or belief, disability, sex or sexual orientation.

LOGFRAME PLANNING MATRIX FOR Project Fiche	Programme name and number: Public Key Infrastructure (PKI) implementation on (Citizen Identification Protection System- CIPS locations responsible for issuing CIPS documents	
	Contracting period expires	Disbursement period expires
	Total budget : 400,000 EURO	IPA budget: 400,000 EURO

Overall objective	**Objectively verifiable indicators**	**Sources of Verification**	
Modernisation of public administration	Assessment of EC: - CIPS information system is web organized system and implementation PKI infrastructure for personal documents of the BIH citizens is upgrade in purpose of implementing of e-government components in state information system. - All users of CIPS systems are using this infrastructure.	Project reports Project internal correspondence Internal procedures Internal log's of the system Strategy of CIPS development plan Annual activity reports	
Project purpose Improve security level of CIPSS information systems through introduction of PKI technology.	**Objectively verifiable indicators** Assessment on: Technical performance of entire CIPS network and CIPS Web services will rise. 137 CIPS secure connection point will rise there communication capacities. no intrusion to system Administrators of system will have	**Sources of Verification** Technical documentation and reports of PKI infrastructure from contractor Project reports from contractor Server logs on the system Internal survey Internal work reports of CIPS system by managing board and maintains body Decisions on internal procedures approved by CIPS management.	**Assumptions** R: Technical problems regarding corporations network infrastructure use in the system where CIPS directorate is not owner.

	better control of the system implementation process. Agreement reached and approved on procedures regarding system access on PKI infrastructure(will be main authority on state level for personal document of citizens)	Number of active secure connection points	
Results	**Objectively verifiable indicators**	**Sources of Verification**	**Assumptions**
• R1 PKI infrastructure and applications provided to all CIPS systems. • R2 Internal capacity building to ensure security PKI application is in place	- PKI applications installed - PKI applications become operative - Training need assessments report - Trainers certified Number of organized training for CIPS staff	Activity reports prepare by contractor Annual report prepare by contractor Test reports prepare by contractor Project reports prepare by contractor Certificate of Acceptance Reports on database security and working procedures Training evaluation reports	R: Delays due complex tendering procedures R: Need for additional human resources
Activities	**Means**	**Costs**	**Assumptions**
1.1 Installation of hardware and software 2.1 PKI system developed in accordance with in a functional technical requirement. 2.1.1 Development of application solutions of Identity and Card Management Subsystem, Personalization Center Subsystem. 2.1.1.1 Development of module of application solution Identity Check and Validation. 2.1.1.2 Development of module of application solution Prohibition Management.	Supply Technical Assistance	400,000 EURO	

2.1.1.3 Development of module of application solution Management. 2.1.1.4 Development of module of application solution Database Management. 2.1.1.5 Development of module application solution Production Management System. 2.2 Development of PKI and Security Subsystem 2.2.1 Development of module of application solution Certification Authority Client. 2.2.2.1 Development of module of application solution PKI Client, 2.2.2.2 Development of module of application solution Crypto Firewall, 2.2.2.3 Development of module of application solution ID CA 2.2.2.4 Development of module of application solution Certification Authority Server. 2.2.2.5 Development of module of application solution HTTP Crypto Proxy, 2.2.2.6 Development of module of application solution Secure log-on, 2.2.2.7 Development of module of application solution Cryptographic			

API. 3.4 Training of the trainers 3.4.1 Delivering of the training for 10 systems administrators and 30 local administrators(Local administrators will pass ‘’Train the trainers’’) 3.4.2 Preparing training manuals for system administrators, local administrators and users on the CIPS remote locations for issuing personal documents 3.5 Installation, configuration, tuning and testing of PKI system 3.6 Documentation management 3.3.1 System usage documentation.(Minimum) 3.3.2 Development of system operative procedure (backup and recovery) 3.3.3 Installation procedures for entire PKI system 3.4 PKI system enters exploitation			

Pre-conditions

ANNEX II: amounts (in €) Contracted and disbursed by quarter for the project

Contracted	Q1/2008	Q2/2008	Q3/2008	Q4/2008	Q1/2009	Q2/2009	Q3/2009	Q4/2009	Q1/2010	Q2/2010	Q3/2010	Q4/2010	Q1/2011	Q2/2011	Q3/2011
Contract 1		162,000													
Contract 2			238,000												
Cumulated		**162,000**	**400,000**												
Disbursed															
Contract 1		97,200		64,800											
Contract 2			142,800		95,200										
Cumulated		**97,200**	**240,000**	**304,800**	**400,000**										

ANNEX III Reference list of relevant laws and regulations about CIPS

Laws from which definition of tasks for CIPS Directorate originate have been published in the Official Gazette BiH No. 32/01 and these are the following:

1. Law on Central Records and Data Exchange
2. Law on ID number
3. Law on residence and domicile
4. Law on ID card
5. Law on Personal Data Protection

The aforementioned laws initiated the establishment of CIPS Directorate. CIPS Directorate activities are associated also with other laws relating to registers defined in the Law on Central Records and Data Exchange. These are primarily:

1. Law on Passports
2. Law on Movement and Residence of Foreigners
3. Other laws and secondary legislation relating to register records and competent authorities relating to registers from the Law on Central Records and Data Exchange

In 2006, by changes and amendments of the Election Law, role of CIPS Directorate was defined within the election process. Also by conclusions and decisions of the Council of Ministers as well as by signatures of memorandum with the Delegation of European Commission to BIH, it has been defined that the Directorate manages and owns the network for data transfer for the needs of public security in BIH.

- Decision of the Council of Ministers published in the Official Gazette 12/02, and defined as an independent Department within the Ministry of Civil Affairs by the Law on Ministers and other Administrative Bodies (Official Gazette BIH No. 5/03).