Application Development and Implementation Plan

General Design Principles

Bigg-Sistems-Hice Plc. have many years of experience in large scale systems integration projects. The proposed EPPS system design builds on this and is based around tried and tested components, methodologies and software from similar successful systems. In particular we have drawn from the "Suspect Index" system, a major immigration clearance project commissioned by the British Government and currently in use at all major British ports of entry and overseas embassies. We have also included proven elements of passenger handling technology from BSH Travel's extensive portfolio of rail projects, including the London Underground mass transit system and the Channel Tunnel rail link. Finally, BSH Retail's extensive experience with many clients has lead them to establish long term relationship with kiosk suppliers and to have determined a "best of breed" set of kiosk components and design strategies.

This experience has been combined and distilled to provide the following guiding design principles that we have applied to the EPPS proposals:

- Wherever possible, industry standard components have been used, and each component is available from more than one supplier.

- Industry standard operating systems, database management software and development tools have been used throughout.

- Resilience has been ensured by two means – through component duplication to avoid any single point of failure; and through the ability of individual parts of the system to continue in operation if other parts are not available.

- The system has been designed with future applications in mind. This means ensuring adequate processing, storage and network capacity for both the phase I implementation and anticipated future developments so that these can implemented with minimum cost and disruption.

- We have taken account of the structure of the central EPPS authority and recognised the requirement for individual airports to have individually tailored applications for local use.

- We recognise that the design of the passenger reception and immigration process is at least, if not more important then the hardware and software solution. Advice and guidance has been sought from experienced customs and immigration officials who have reviewed all stages of the proposal.

Technical Specifications of Proposed Solution

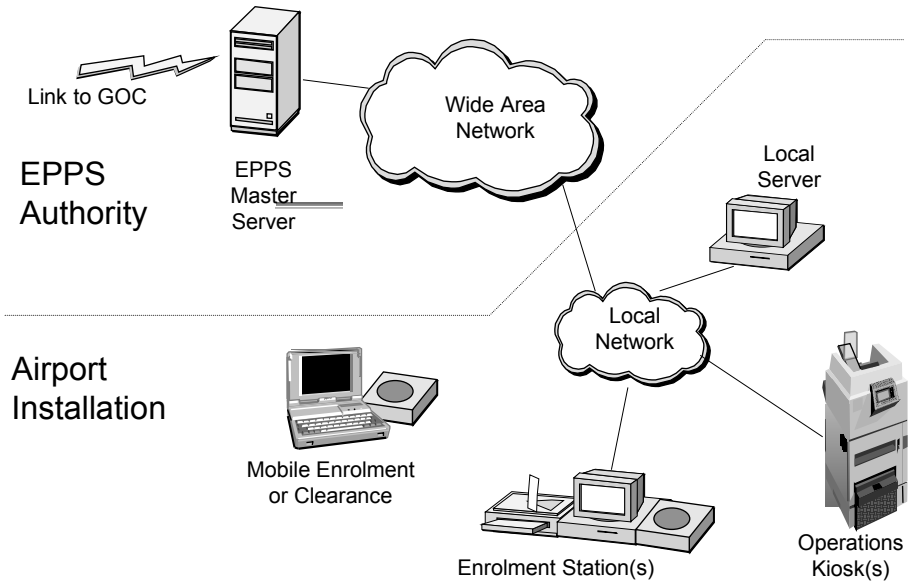
Overview of Proposed Solution

The proposed solution is a client server system with a central database server owned and managed by the EPPS Authority. This has wide area network connections to each airport installation and to the Government of Canada.

Each airport installation is based on a local area network, with one local server and any number of client enrolment stations and operations kiosks. . The airport installation design also supports fully mobile enrolment and immigration clearance should this be required.

A high level the system is shown below:

EPPS Overview Design



The EPPS master server maintains a database of scheme members and their tombstone information, biometrics and so on. External communications link this database to the Government of Canada to allow them to grant or deny entry permission to members as required. Each operations kiosk acts as a client to this database, maintaining its own "in-memory" copy of the data. Updated information, either in the form of new enrolments, updates of personnel information or GOC changes to entry permissions are propagated in real time to all clients. The client / server software combines to ensure that the kiosks are automatically re-synchronised with the master data if there is a communications, kiosk or server failure.

This architecture exhibits a number of advantages making it ideal for the EPPS application:

- The Database Management System, and the computer installation to run it are required only at the central location. The resources to house such a system, and the operator skills need to run it are obtained by the EPPS authority and the cost of these can be amortised over the airports licensing the EPPS system. We recommend that the hosting of the master server and the management of the wide area network be outsourced. Our partner company, BSH-Canada Inc. has extensive experience in this area.

- Conversely, neither the kiosks or the enrolment stations need a database management system as the data is held in memory mapped files. This greatly reduces the required PC specification, and the support skills required at the airport, minimising costs.

- The clients will operate autonomously from the master server, and in fact in case of serious disruption will operate without the local network. Only the kiosk cabinet will need to be provided with back-up power supplies, minimising cost to the airports.

- The fact that a client can operate without a connection to the master database, and be re-synchronised later; and the small memory and processor "footprint" of the client application mean that a portable PC can be used if required. The biometrics readers operate from 12V DC supplies and hence a totally mobile installation can be provided if required. This, and possible applications are discussed in more detail on page 9.

- The local server provides local network logon validation and also maintains a copy of the data files in order to restore failed kiosks. In future phases it will be used to host local applications,

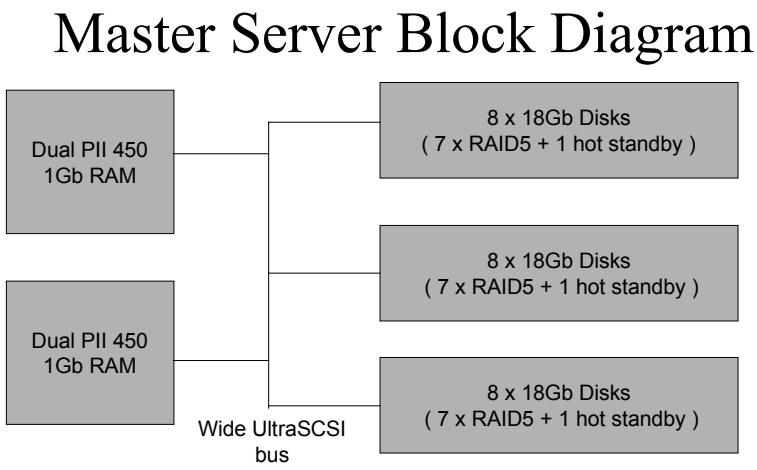
allowing each airport to have their own set of EPPS applications, independent of the EPPS authority.

The architecture proposed is presently in use for the British Government Suspect Index system. The master server provides updates to 80 clients, each of which can search the 500,000 records with sub-second response times. The system is currently being upgraded to handle up to 12 million records.

EPPS Master Server Description

The master server runs the Oracle 8 Database Management System; the EPPS server application; central management, reporting and auditing; and links to Government of Canada systems.

In view of its central role in the EPPS system a high availability system has been specified. We recommend an NT Cluster server with two, dual Pentium CPUs and three RAID5 disk arrays. Network connectivity is also duplicated, and full backup facilities and uninterruptable power supplies are included. The basic arrangement of components is shown below. The cluster components, including UPS and a keyboard / screen / mouse switch can all be housed in a single full height 19" rack cabinet.



The target hours of operation of the master database system will need to be 24 hours per day, 365 days per year. This is due to wide opening times of the airports involved and the number of timezones between Vancouver and Halifax. There is a short window available for planned maintenance and off-line backups if required, however we must assume a requirement for daily on-line backups. See the chart below for timings relative to GMT. This chart is based on the assumption that airports can expect arrivals between 06:00 and 23:59 local time, except for YVR, which has scheduled arrivals from 02:35 local. It will be seen that either earlier arrivals at YHZ, or later arrivals at YVR will close the available maintenance window.

GMT	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Δ
YHZ																									-4
YYZ																									-5
YWG																									-6
YEG																									-7
YVR																									-8

In view of the specialist skills required to operate such a system, and the physical and IT infrastructure required we strongly recommend that the master server be hosted by an experienced third party; BSH-CANADA are acknowledged leaders in this field. Our preliminary discussions with them suggest that the BSH-CANADA datacentre in [where?] would be the most appropriate.

A parts list of the major master server components is given below:

- 19” Full height Rack x 1, + associated shelving, blanking panels etc.
- Screen / keyboard / mouse switch x 1 + associated cabling
- Monitor, keyboard, mouse x1
- 3kVA UPS x 1, + associated power cabling
- PC Server, dual 450MHz PII Xeon, 1 Gb RAM, dual 4Gb SCSi disk, dual power supplies x 2
- 12Gb Internal DAT drives (server backups) x2
- 20Gb External DLT4000 tape drives (disk node backups) x2
- Fast, wide SCSI controller (AHA-2940UW) x 2
- Disk Node cabinets, dual power supplies x 3
- 18Gb SCSI disk x 24 + SCSI cabling & SCSI helpers
- NT Server software (High Availability Option)
- Oracle 8 DBMS software

EPPS Local Server Description

The local server is an industry standard PC Server running Microsoft Windows NT Server. In phase I it will provide local logon validation for enrolment station users and will also act as a “dummy” kiosk client, writing the information to disk. These disk images can be used to rapidly restore failed kiosks. A suite of local management reports will also be available for the use of the airport operator.

The local server will also provide network DHCP, DNS and WINS resolution services. See the EPPS Network Description on page 7 for more details.

In future phases the local server will be used to host local applications, specific to each airport. These applications may require a local database and the server has been specified to cope with this, although such database software has not been included in this quotation. Similarly, a backup tape drive has been included even though for phase I the only “local” information will be the user list, which typically needs to be backed up only weekly. When local applications are installed in future phases the equipment can be used to carry out more frequent backups.

Although initially the server could be sited in an office environment, in view of its more critical role in future phases it would be better sited in a suitable machine room. Note that for phase I, the local server will not require a UPS for continuous operation as it is not a critical part of the kiosk immigration process. A power conditioner and battery backup sufficient for clean shutdown only have been

specified. Future phases may require more resilience in the face of power problems but it is difficult to determine these requirements at present; and the machine room environment may be equipped with stand-by power. UPS requirements for the local server should be reconsidered in phase II.

A parts list of the major local server components is given below:

- PII 450 or above Server, 256Mb RAM, dual 10Gb or above hard disks x 1
- 15" CRT monitor, keyboard, mouse x 1
- Floppy drive, CD-ROM drive x 1
- 10/100Mb PCI ethernet cards (e.g. 3COM 3C905 TX) x 2
- 24Gb backup tape (e.g. HP SureStore DAT24i) x 1
- UPS with auto-shutdown capability

- Windows NT Server

EPPS Kiosk Description

The kiosk design is based on some initial ideas on the flow of passengers through the immigration process. These ideas lead to the following requirements for the passenger flow:

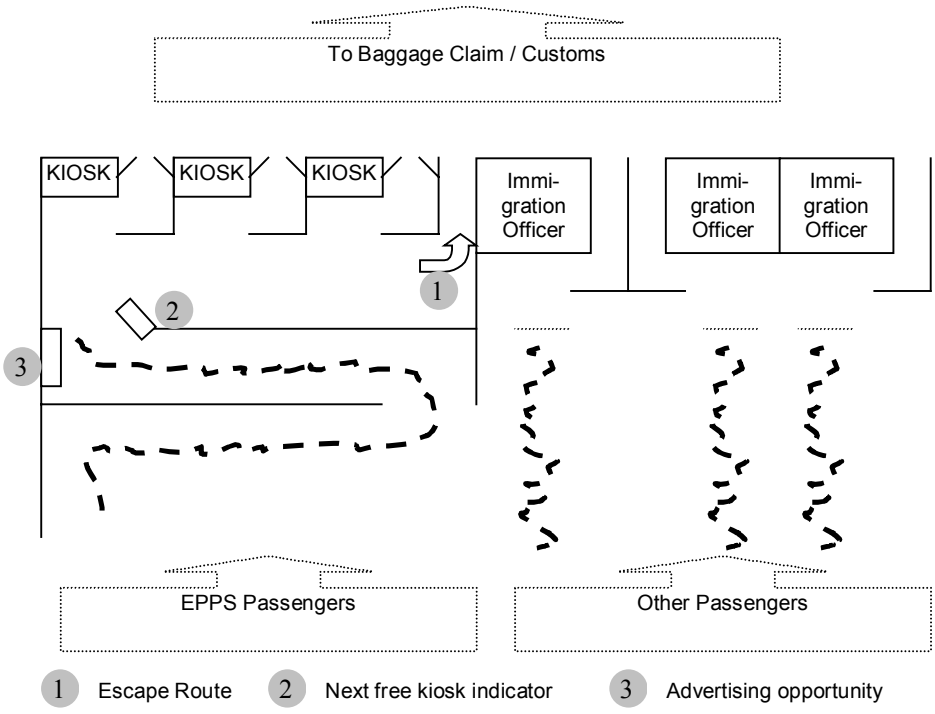
1. There must be an "escape" route for those rejected by the system, unidentified by the biometrics or simply non-EPPS members in the wrong queue.

2. The flow must be "hand baggage friendly"; i.e. no need to remove shoulder bags, operable using one hand, no turnstiles or awkward turns.

3. For ease of use, and future biometrics through face recognition, the kiosk should be facing the passenger, in full view as they approach it.

4. The kiosk / barrier combination must be secure but not intimidating or claustrophobic.

For the purposes of costing and kiosk design we have thus assumed the following layout of the airport immigration area:



The kiosk design has been based on the United States INSPASS program design, modified to suit CAC requirements and the passenger flows above. An early part of the development project will be to build a "proof of concept" kiosk for usability testing. This testing will include not only consideration of passenger access and ease of use; but also ease of access for daily maintenance (paper / ink refills) and repairs (printer replacements etc.). These tests may require kiosk design changes which may in turn affect kiosk pricing. Similarly, the quotation is for a basic steel kiosk casing. If other materials or finishes are required to adapt to local airport décor then these will have to be priced separately.

An artist's impression of the basic kiosk is shown below:

Note that the process followed by the kiosk users naturally draws them from the left of the unit to the right, hence the placement of the exit barriers at the right hand side of the unit.

We do not recommend the use of a secondary biometrics reader as this is likely to confuse the EPPS user. Should the biometrics fail to positively identify the user we recommend the use of the video camera. This would give a head and shoulders view of the user which could be displayed to an immigration official, alongside the picture originally taken at the point of enrolment. We also recommend that this is a two-way video link in that the user can see their own image on the screen as well as the facial image of the immigration official. The kiosk would also include a directional microphone and speakers (not shown in the artist's impression) to allow spoken conversations. This mechanism could also be used if the user has any other sort of problem with the system and requires help. The local area network infrastructure has been specified to be capable of carrying bi-directional full motion video to support this functionality.

The receipt printer specified is capable of detecting whether the receipt has been removed by the EPPS user and hence we can provide an interlock between the taking of the receipt and the release of the exit barrier. If for any reason the receipt is not taken by the user it is withdrawn and stored internally.

The exit barrier to be used will require further consultation with the airport authorities to confirm with airport décor and local safety regulations. We recommend the use of ¾ height, outward opening, motorised, glass doors as these are not intimidating and can accommodate a person with shoulder bags, briefcases and so on. Some further work will be required at the design stage to identify the fallback of the exit barriers in case of power failure. The barrier power requirements (current) may be quite high,

requiring a costly UPS system, or it may be that the barriers fail into a manual mode such that they can be opened by the passenger.

The major kiosk components are as follows:

- PII 400 or above PC, 128Mb RAM, 10Gb or above hard disk, onboard sound card x 1
- Floppy drive, CD-ROM drive x 1
- 10/100Mb PCI ethernet cards (e.g. 3COM 3C905 TX) x 1
- Additional serial ports (4) card x 1
- Interface card for barrier control and "available kiosk" lighting x 1
- 15" touchscreen monitor x 1
- Motorised smart card reader x 1
- Thermal printer with loop control, paper out warning and removal detection (e.g. Star Micronics XX???) x 1
- Impact printer x 1
- Video camera, directional microphone, mono speaker x1 (recommended option)
- UPS with auto-shutdown capability

- Windows NT Workstation

The software running in each kiosk is:-

1. Windows NT operating system, including SNMP management client

2. Bespoke user interface application, controlling all kiosk components

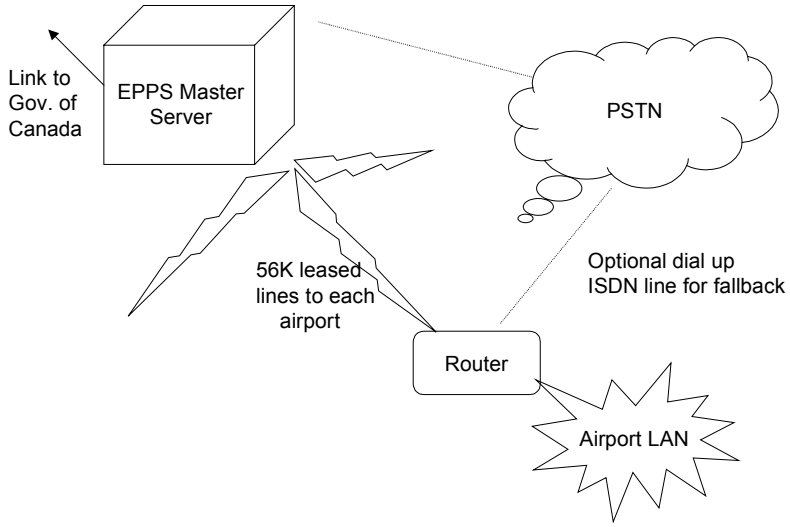
3. The Suspect Index search client application for passenger clearance

An initial high level functional description of the kiosk processing is shown below:

EPPS Network Description

There are two major parts to the EPPS network, a wide area network connecting the master server to each of the airport sites; and a local area network at each airport. We will consider the wide area network first, an overview is shown below:

EPPS Wide Area Network Overview



The basic network topology is a set of point to point links from the master server to each airport. TCP/IP is used as the network communications protocol throughout. In normal operation these links carry new enrolment information up to the master server, which is then distributed to all clients; and changes to entry conditions entered by the Government of Canada and distributed to all clients.

In the event of catastrophic failure at an airport the link would also be used to reload the memory map files used by the clients. Assuming a 25% communications overhead, and that the data files are 20Mb in size then the files could be downloaded in 65 minutes. Note that this would only be required if *all* of the local copies of the files were lost. The client and server will automatically re-synchronise changes to an out of date local file.

The local router can also act as a fallback DHCP and DNS server. In the case of failure of the 56K leased line it is possible to use a dial-up ISDN line as a fallback. Whether this is required will depend on the service levels offered by the leased line provider and the criticality of the link information. Note that the client kiosks and enrolment stations will continue to function without the link to the central server as they hold local copies of the data. When the link is restored the data will automatically be re-synchronised. The cost of fallback ISDN lines has not been included in the current quotation.

The master server also acts as a master WINS Name Resolution server, updated from the local WINS servers at each airport. The server uses WINS names to locate and update its clients.

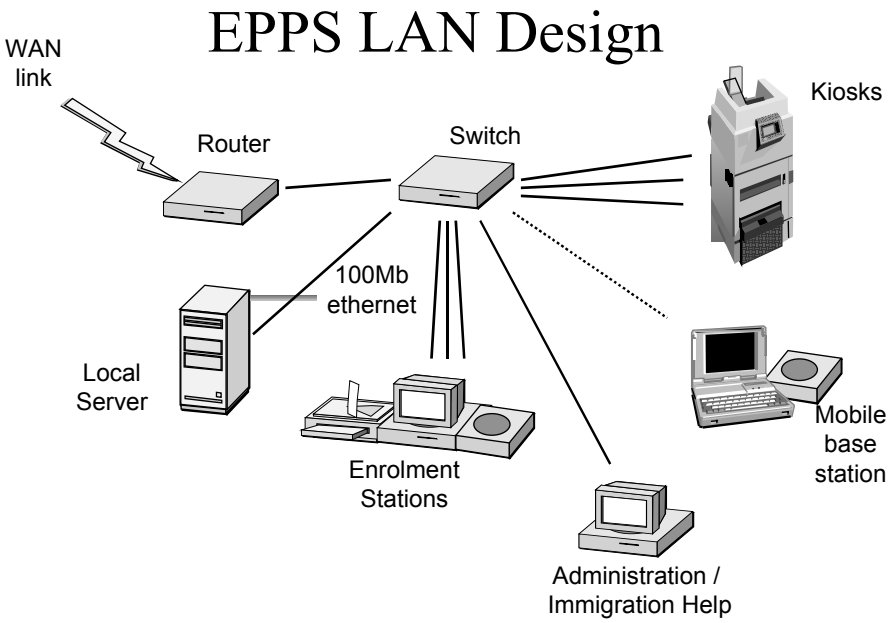
The communications interface to the Government of Canada is not known at the moment. For the purposes of the quotation we have assumed that this is also a 56K leased line.

Although the leased lines are “point to point” connections it is not known to the customer where and how that data is transmitted, and how secure it is. For additional security it is possible to add hardware encryption devices to each end of the leased line. Guidance should be sought from the Government of Canada and appropriate Canadian data protection legislation as to whether this additional level of security is required. Hardware encryption devices have not been included in this quotation.

In view of the requirements for continuous network monitoring we strongly recommend that the management of the EPPS wide area network be out-sourced. It would be most appropriate for this management to be done by the same organisation that is hosting the central server and we would recommend BSH-CANADA for this role. They already have an extensive global communications network maintained and managed 24 hours per day.

The local network also uses TCP/IP communication protocols. To adequately support future high-bandwidth applications we recommend the use of 100Mbit switched ethernet as the communications medium. Although this is not strictly required for the data flows expected in phase I, it will negate the requirement to re-cable or refit communications equipment for future phases. In an airport environment, especially airside we recognise that cabling work can be disruptive and expensive and this approach ensures that such work only needs to be done once.

A high level overview of a typical airport installation is shown below:



Mobile EPPS Description

As noted above, the architecture allows for a truly mobile EPPS client, which can be used both for enrolment and immigration clearance. For example, an enrolment station could be set up in public areas such as shopping malls or in suitably equipped vehBSHes or trailers at public events. In this scenario members of the public would enrol, providing the required personal information and have their biometrics measurements taken. At the end of the day the portable PC would be returned to the airport, placed in a docking station and the data would be uploaded. The cards could then be printed and mailed to the enrolees. It would be possible to take the card printer to shopping malls and other places where mains power is available, however these are physically quite large devices and an additional level of security is obtained through the use of a mailing address.

The same set of equipment could also be used for immigration clearance, for example on the tarmac, in the VIP lounge or in an emergency situation. Prior to use the portable PC would be placed in the docking station and receive the most up to date set of data by copying it from the local server. This data would then be used to validate passengers by manually swiping cards and assisting passengers with taking biometrics readings. Again, at the end of the session the portable would be returned to its docking station and the data uploaded to the central server. This system could be extended through the use of GSM modems to handle on-line credit card validation, or even real-time links to the central server for continuous updates. Some airports may also be considering the installation of wireless LANs, which would be a very good fit for this mobile application.

If a mobile system is installed we would recommend that it is normally stored attached to base station and switched on, receiving database updates. This will ensure that whenever it is required, the battery will be fully charged and it will contain the most up to date clearance information.

Components Outside the Current Scope

The sections above discussed several components which are not considered to be required for phase I but which may be needed for future phases. None of these components are included in the current quotation. For ease of reference the complete list is repeated here:

- Oracle Software for local servers
- Portable equipment for mobile enrolment and clearance
- Fallback ISDN lines for each airport and the central server
- Airport network cabling (to be tendered for at each airport)
- [etc…]

In addition to these components there are some that may or may not be useful to the EPPS authority, and which have not been included in the current quotation. For example, the EPPS authority may wish to have a development server and small “airport” installation for acceptance testing and research. This might consist of a small central server (a single CPU and disk node, with no UPS etc.), a local server, an enrolment station and an operations kiosk. All to be installed in a suitable location within the EPPS authority premises.