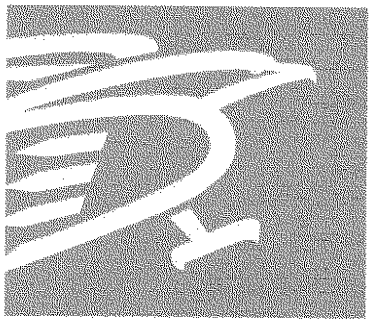


Submission

Exposure Draft of the Human Services (Enhanced Service Delivery) Bill 2007

Document Issue Date
28 February 2007

Submitted To
Committee Secretary
Senate Finance and Public Administration Committee
Department of the Senate
P.O Box 6100, Parliament House
Canberra ACT 2600 Australia
fpa.sen@aph.gov.au

TABLE OF CONTENTS

Eaglehawk Limited Submission Authority:

Submission of this document is hereupon authorized by Eaglehawk Limited.

John L. Merity

Digitally signed by John L. Merity
DN: cn=John L. Merity, c=AU, o=Eaglehawk Limited, ou=Managing Director, email=john.merity@eaglehawk.com
Date: 2007.02.25 20:54:29 -05'00'

John L. Merity, Managing Director

Eaglehawk Limited Contact Details:

Name: Mr. John L. Merity
Title: Managing Director
Address: 22 Albert Street, Unit 3, Edgecliff, N.S.W. 2027
Phone: (02) 9328-1220
Mobile: (04) 2526-1255
Email: john.merity@eaglehawk.com

Terms of Reference relevant to this Submission

1. Enhanced scope and purpose of the Access Card
2. The information to be included in the card's register and card's chip and on the card surface
3. Prohibiting improper use of the card

Introduction

The purpose of the Submission is to show how Eaglehawk's StrongBox™ (SBX) data security technology can easily, and with little disruption to in-place architectures, massively enhance the security sought for Access Card applications, ensuring that the primary objective/benefits sought by the Government with the introduction of an Access Card can be achieved in a simple cost effective manner and yet satisfy the primary objections to the programme relating to:

- Privacy; and
- Ensuring that the Access Card cannot be used as a National Identity Card.

Eaglehawk's solution to these issues is set out in the attached PowerPoint presentation entitled "Australian Government Access Card Programme" and, should the Senate deem appropriate, a representative from Eaglehawk will avail to attend upon the Committee to give this presentation in person. In addition, a step-by-step example of the operation of Eaglehawk's solution with respect to a specific Agency is set out in Appendix 1 below for ease of understanding.

Comments on the Exposure Draft

Eaglehawk's comments on the Exposure Draft focus on two areas of concern regarding the privacy & security of data:

- Data stored in the Central Registry
- Data stored in the Access Card/Chip itself

As a fundamental first principal regarding the security & privacy of data to be stored in the Central Registry, Eaglehawk maintains that ALL private/sensitive information should be de-identified. Stated differently, through the use of SBX technology, no direct linkage will exist between an individual's Access Card ID (name, account number) and any individually identifiable private/sensitive information about that individual. Simply stated, therefore, in the event the Central Registry is penetrated by unauthorized entities there will be no way to link Private data to specific individuals.

As a fundamental second principal, Eaglehawk maintains that, for a variety of security, privacy, and efficiency-related factors, the data stored on the Access

Card itself should be kept to a minimum. In this regard, data stored on the Access Card will predictably become out-of-date – one only has to recall the difficulty of getting people to keep their address details up-to-date on their driver's licenses to understand this problem. This problem will thus force the Agency and emergency personnel that it is intended to help to seek alternate sources of data, thereby increasing delays and cost of delivery of services and the eventual dismissal of the card as a valuable asset in the service delivery process.

It should also be noted that the potential for fraud increases as perception of the card's value diminishes: over time, and given enough experiences with out-dated cards, Agency personnel may begin to discount the value of the Access Card as a reliable source of information about the recipient of services and, predictably, will become more willing to accept various explanations for inconsistencies represented by the card/cardholder.

Notwithstanding the currency of the information on the Access Card/Chip, storage of the proposed range of sensitive information on millions of individual cards constitutes a huge – and unnecessary – security vulnerability. Cards will be lost, stolen, hacked, and cloned.

At a time when pervasive network access is becoming the norm, the approach of trying to create and maintain a distributed dataset of millions of entity records is being attempted with the Access Card data. The alternate methods offered by SBX provide a viable secure solution at less cost and disruption to the clients being served. Additionally, SBX provides the types of access safeguards that can be built into the service architecture to ensure that the proposed Access Card is not a National Identity Card.

Addressing Data Security & Privacy With StrongBox™

StrongBox™ provides a simple, low-friction solution to the data security & privacy issues of the proposed system by logically separating each individual's Access Card from that individual's data deemed private or sensitive.

From a design perspective, a Secure Customer Registration Service (SCRS) database with a limited dataset would meet the 'telephone book' standard for Public Domain data required to confirm the identity of an individual presenting the Access Card. For all private or sensitive data being maintained, SBX provides the means by which that information is made anonymous thereby rendering it valueless to inappropriate access (hacking).

The SCRS database should separate Address from Personal details that could contribute to identity theft or misuse (photograph, signature). StrongBox can also independently secure items such as Date of Birth if necessary.

The use of StrongBox™ provides benefits in three distinct areas:

- Access Card anonymity (de-identification) as it relates to private and sensitive data elements.
- Access control with regard to individual data elements in the SCRS and identifiers for agency databases.
- Fine-grained audit of Access Card activity including application level audit for agency specific interaction.

SBX also provides a path to additional uses for the Access Card without compromising the original privacy concerns that are already addressed by StrongBox™ technology.

Regarding the potential for the Access Card to become a National Identity Card, inter-agency access to a card holder's data will not be possible using a StrongBox™ solution. In this regard, Agency-specific installations of SBX would be separated physically and logically from other Agencies, resulting in an environment that is impervious to individual unauthorized data access across Agencies. Within such an SBX environment, multiple access authorities must be negotiated for a single Agency to access its own data, and that authority simply does not exist in a separate Agency's SBX environment. The Access Control List (ACL) authorities of SBX extend to individual data elements within its in-memory repository, resulting in both exceptional security and high-speed processing.

The audit of activity within a StrongBox environment is flexible, comprehensive, durable and incorruptible. Where fine-grained audit is necessary, SBX can be configured to audit individual Agency application processes. To this end an additional benefit of SBX audit functionality is as an independent audit process for many Agency activities, even where they would not normally interact with Access Card events. Where high-value data elements are concerned and/or specific data interactions require additional audit protection, StrongBox™ provides for independent ACL protected mechanisms to prove audit entries have not been tampered with.

StrongBox provides an elegant solution to the concerns raised by Senator Stott Despoja in question HS36 to the Minister for Human Services; particularly questions 2 and 3. In addition StrongBox™ satisfies the requirements of the Minister outlined in paragraph 3 of the Minister's Response, which is to ensure that the security of the system to be used to protect the central registry meets the highest standard of security available. In particular, Senators should know that StrongBox™ has recently been evaluated on behalf of the United States Department of Homeland Security, and that the assertions made by Eaglehawk with respect to SBX capabilities have been found to be valid.

Conclusion

In a simple, elegant, and cost effective manner that enhances the security, privacy, and efficiency of both the Central Registry and the Access Card/Chip itself, StrongBox™ enables the primary objectives & benefits sought by the Government through introduction of an Access Card system to be reconciled with the primary objections against such a system.

In this regard, however, if it is considered that the decisions on the scope of the information to be included on the Access Card have progressed too far to adopt the minimalist datasets proposed by Eaglehawk, then Eaglehawk urges the committee to recommend to the Government that StrongBox™ be utilised to protect the information in the Central Registry as well as the proposed multiple sub-set registries, (individual Agencies) which will ensure denial of access to unauthorised agency personnel and denial of access to authorised Agency personnel with respect to any information not necessary for them to perform their specific Agency duties. In addition all access will be subject to audit and any unauthorised attempts to gain access will be recorded.

APPENDIX 1
PROCESS OVERVIEW

The following provides a detailed example of Access Card processes where StrongBox™ is implemented to strengthen authentication, security and audit.

A client seeks service at a Government office.

- Presence of Access Card is acknowledged.
- Government staff member (staff) requests that the client insert their card into the card reader. Immediately, the client's Access Card Number, Name, Picture and Signature are displayed on the government computer monitor. All these data elements are resident on the Access Card.
- The staff member acknowledges client by name with visual verification to picture from the card. The client is then invited to enter his/her personal PIN into the reader.
- Following entry of the PIN, the client's Access Card Number is transmitted to a StrongBox™ server where it is verified as valid. Following validation of the Access Card Number, the PIN (encrypted) is transmitted to the StrongBox™ server and validated against the previously verified Access Card Number.
- Now that the Client is authorized, the Agency's software application retrieves the client's Name and Address from the SCRS using the Access Card Number and displays it on the staff monitor. Staff solicits street address from the client completing the client verification process.
    - At this point in the process, additional verification could be achieved by accessing a separate StrongBox™ server to retrieve the key to the Private Data stored for the client in a separate SCRS database.
    - In this database, the client's picture and digitized signature are kept along with various other confidential data elements and, for example, the client's picture and/or signature could be presented on the staff monitor for comparison with the picture/signature from the Access Card.
- Upon completion of the verification process, the staff member now begins the process of accessing the Agency's database to process the client's requests.
    - The Agency staff member, using their own staff ID, accesses a separate SBX server to retrieve the Private Access Card Key for

the client's Access Card. This key exists only in the StrongBox™ servers and is not used in any external documentation or Agency databases.

- Using the Private Access Card Key, a separate Agency-specific SBX server is accessed to retrieve the key (account number) for the data maintained for the client at that Agency.

- Serving the client with full agency confidence that the correct client is present may begin.

Using the method provided by a Private Access Card Key, a significant barrier to unauthorized penetration (hacking) of any of the Agency database servers as they relate to individual Access Card holders is easily maintained.

- All activity with StrongBox™ servers is managed with session authentication that changes with every individual message.

- All interaction with an SBX server requires that the Agency staff member's ID be authenticated, and that the staff member's User Group (Agency) have access authority to any data element that the staff member is attempting to access.

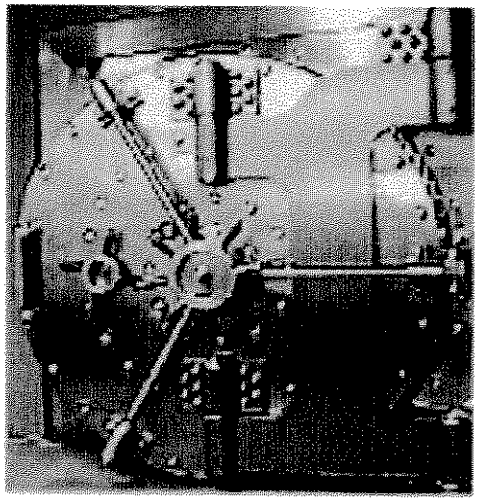
- Additionally, an overriding Agency authority is also required on the Access Control List of any data element in a StrongBox™ server so that only data belonging to a particular Agency can be exposed to the appropriate Agency personnel.

- This overriding authority assists in preventing any cross-agency access to data elements, fulfilling the Government's mandate that the Access Card not become a National Identification Card.

Comprehensive audit for authentication activity and data element access is provided, ensuring that the Access Card ID, staff member, StrongBox™ activity and date/time are recorded for review. StrongBox™ can also provide audit for non-SBX events in existing and future Agency applications, simplifying and centralizing audit of many Agency activities.

It should be noted that all StrongBox servers are components of a Service Oriented Architecture (SOA) and as such can be made available on a 24/7 basis to support static or mobile wireless applications.

Australian Government Access Card Programme



Enhancing Data Security with StrongBox™

eaglehawk

February 2007

Key Points in the Government's Initiative

Scope Of The Proposal

- Registration & access card required by 15-20 million Australians to receive government-provided health & social service benefits post-2010

Primary Objectives/Benefits Sought by the Government

- Improved management & efficiency of social benefit programs ($100b distributed annually through Medicare, Centrelink, & Dept. Veteran Affairs)
- Reduced fraud through improved beneficiary identification
- Simplified process for individuals (1 card vs up to 17 currently)

Primary Objections to the Programme

- Privacy & data security issues
  - related to the data in the central registry
  - related to the data on the card itself
- Access Card = National Identity Card

Issues Addressed Specifically by StrongBox™ (SBX)

Privacy & Data Security Issues

Registration Database

- **Centralizes all registrant/beneficiary information**
- **Accessible by all participating benefits agencies**
- **Privacy & security issues**
  - Potential for unauthorized access to comprehensive personal information
  - Potential for abuse, e.g., identify theft, misuse of benefits, etc.
  - Potential foundation for National Identity Card

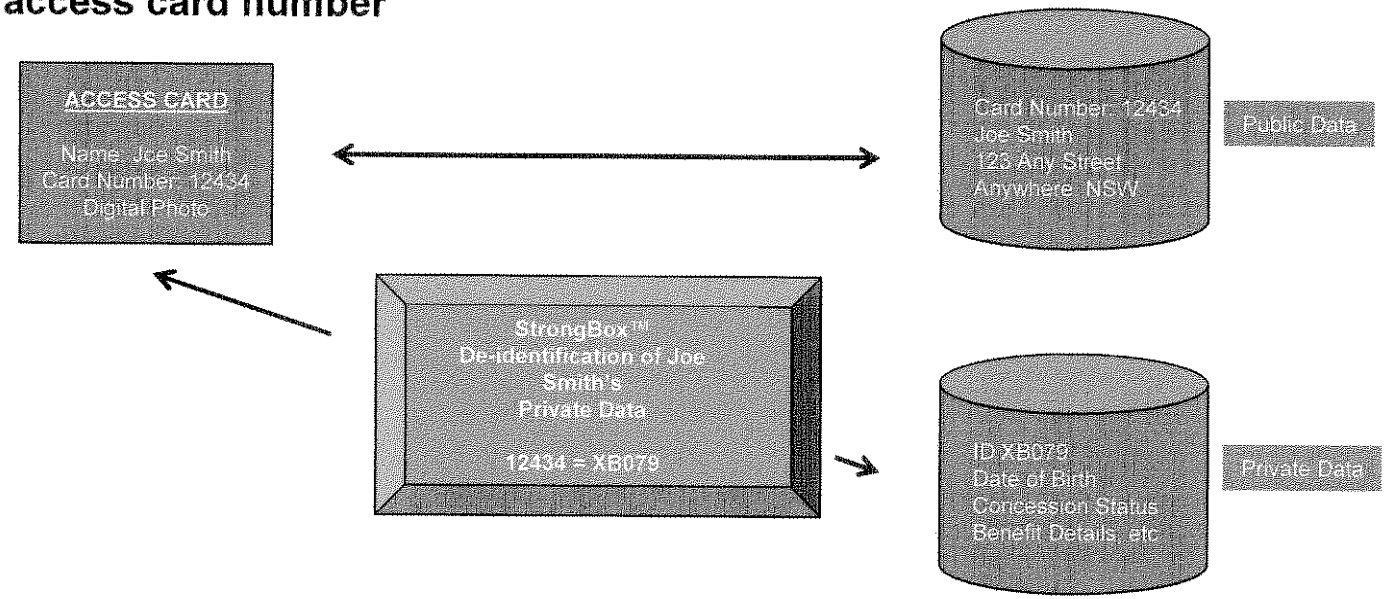
Access Card/Chip

- **Contains basic identification information**
- **Contains sensitive personal/confidential information**
- **Contains encrypted PIN, plus optional "owner" data fields**
- **Privacy & security issues**
  - Potential for cards to be lost, stolen, or otherwise compromised
  - Unnecessary/dangerous duplication of sensitive data on the card/chip itself
    - Sensitive data already centralized in Registration Database
    - Duplication on card/chip increases privacy risks by factor of 15-20 million

Registration Database - Applying StrongBox™

SBX provides a solution that simply & effectively addresses the privacy & security issues identified above

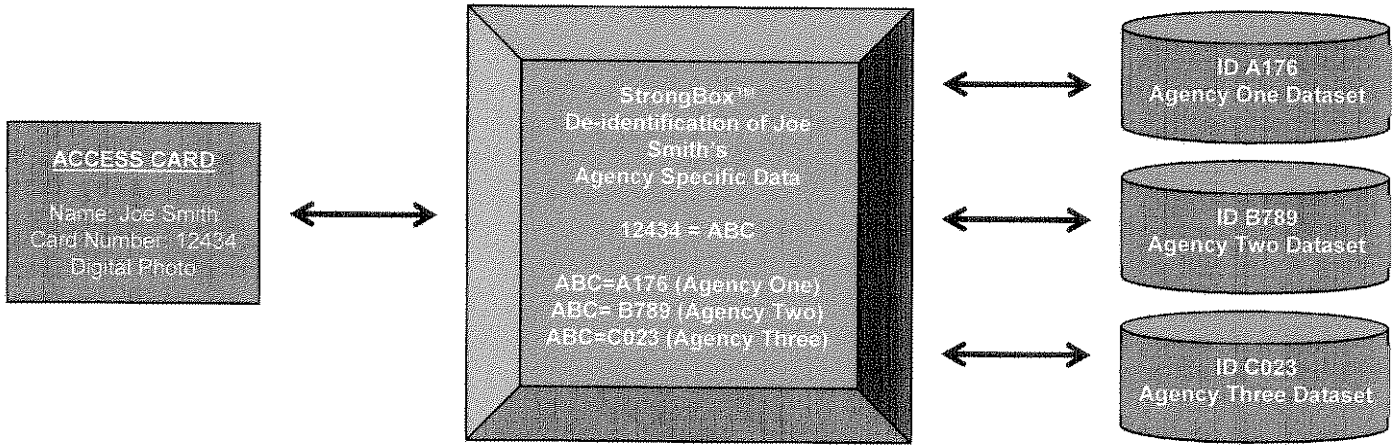
- Separate Public Data (name, address) from all other Private Data (date-of-birth, concession status, benefit details etc.) stored in Registration Database
- De-identify all Private Data by eliminating direct linkages to a beneficiary's name & access card number



Registration Database - Applying StrongBox™

This simple & effective SBX solution can be extended to address concerns that the Access Card is equivalent to a National Identity Card

- For each individual Agency dataset, de-identify the beneficiary's agency-specific data by eliminating direct linkages to the Access Card (name, card number)



- Access to any Agency-specific data restricted via Access Control Lists to individual Agency staff with appropriately assigned authority – no "cross-Agency access"
- All access subject to comprehensive audit (who, what, when)