Bloomberg Philanthropies

DATA FOR HEALTH INITIATIVE

Ghana CRVS Digitisation Project

CRVS Target System Architecture

Vital Strategies

PLAN INTERNATIONAL

Overview

This document outlines a target system architecture that is designed to meet the CRVS target business process maps. It builds on the target system enhancements to describe the technical details of how the system components can be arranged to meet the needs of the target business processes.

Architectural vision and principles

This section breaks down each of the fundamental architectural principles that guide this architecture. These principles follow international best practices and consider the context in which this architecture will be implemented.

1. A centralized CRVS system

The first and most fundamental principle is that there will be a centralized system that is responsible for all CRVS data. Traditionally, this has not been the case in Ghana and each ministry or government agency has had their own (electronic or paper-based) system for capturing civil registration data. In this architecture it is proposed that a single logical system be created to be the central store for all of this information.

This enables the system to track all vital event for a person within a single system and enables vital statistics to be drawn up that encompass the full spectrum of vital events for the population. If this were not the case, a complex mechanism for linking data from several separate systems would be needed. This is a complex and error prone task as each system would have to synchronize any changes that affects the other systems linked records. A single, central system mitigates much of this complexity as the data is managed in a single place.

In addition, a central system fits well in a context where there is strong connectivity and infrastructure in built-up areas yet weak connectivity and poor infrastructure in rural areas. A central system allows the core services that the CRVS system provides to be highly available and allows sites to connect to it when they have connectivity. Offline capabilities and synchronisations functions can be built into software used in the rural sites and this can synchronise to the stable central service on demand.

2. OpenHIE patterns

In this architecture we attempt to follow the architectural principles suggested by the OpenHIE community (https://ohie.org/). These architectural patterns have been proven to work in low resource setting and combine the learning from multiple eHealth experts from around the globe.

The particular OpenHIE patterns that are followed are listed below:

- The logical arrangement of system components
- The reliance on open standards for data exchange
- Central registries to be responsible for management and consistency of data
- The use of an interoperability layer to secure the exchange and to help manage the exchange

3. Messaging standards

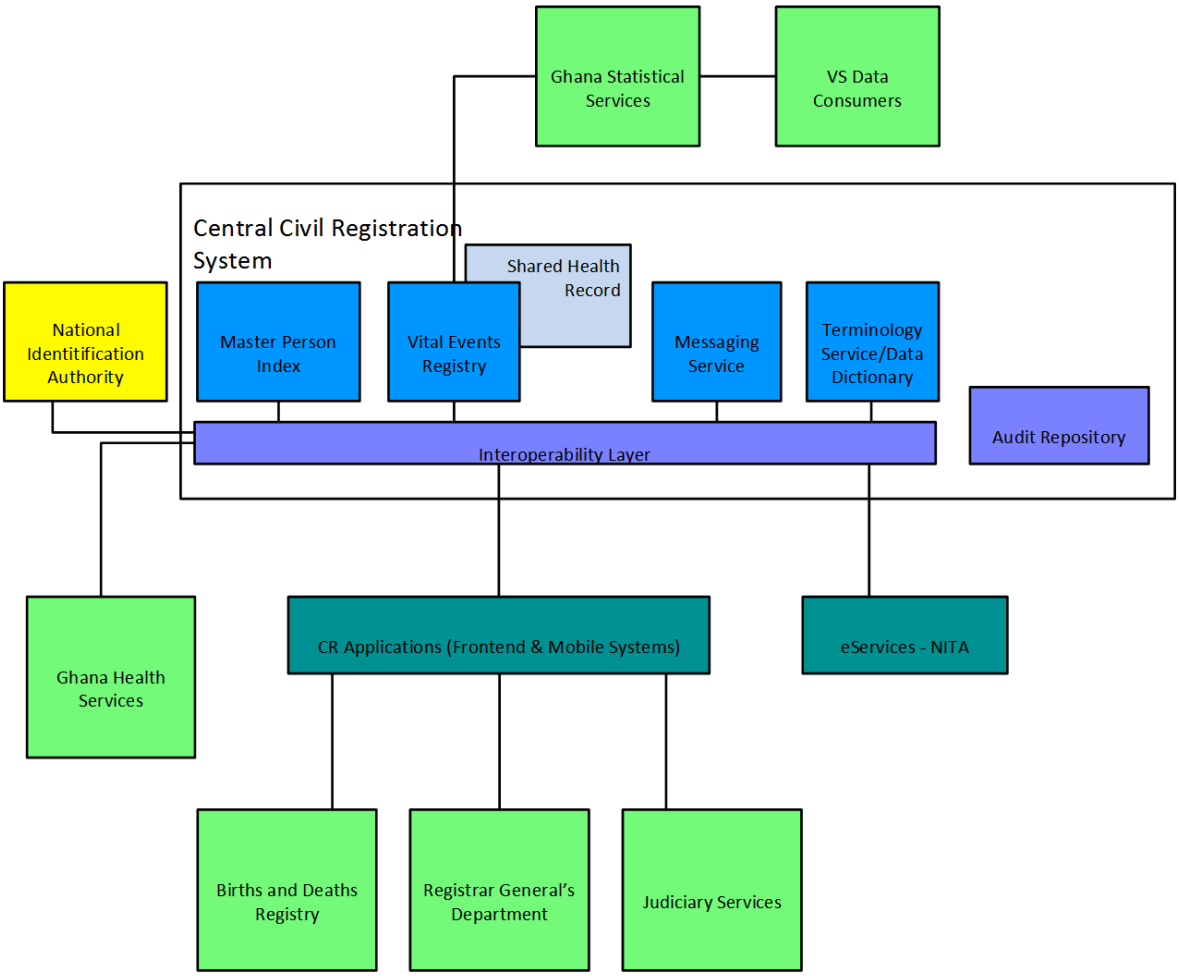
Standards-based messaging is an important architectural principle as it avoids lock-in to proprietary software and also provides a common interface that each of the multiple systems use to communicate. A common interface is useful as each system that links into the exchange can leverage knowledge and tools that are produced either by existing open source tools or implementation of

the common interface in other systems within this architecture. Standard messaging formats also allow the implementer to leverage data models, principles and experience-based considerations from the consortium that produced the standard.

Logical architecture

In this section the logical architecture will be presented. Firstly, an overview diagram is presented and following this the importance and scope of each component is discussed.

In the diagram below the green boxes represent organisations that interact with the exchange in a particular capacity. The blue boxes make up the core components of the central CRVS system and the purple components make up the interoperability components. In teal we have the client applications which certain organisation use to access and manage data within the central CRVS system. The yellow block represents NIA which will be an external central system that needs to interface with the central CRVS system components.



Central civil registration system

The central CRVS system is made up of several components that work together. These components are each responsible for a single concern within the system. The split of these components also closely matches up with the defined components of the OpenHIE architecture. These components and their concerns are described below.

Vital events registry

This component is responsible for storing and retrieving vital events data. It acts as the authority on vital events data within the system. Each vital event record will be linked to a person in the master person index.

The vital event registry also overlaps with a **Shared Health Record (SHR).** A Shared Health Record system is a central repository of longitudinal clinical information stored for patients for the continuity of care in the health information system. There will be certain overlap between a SHR and the vital events registry such as cause of death and a birth record. These systems should work together to ensure information about a person is not unnecessarily replicated in central registries. It is possible to build these two systems using the same technological platform so that it is easier to integrate this data. Both the SHR and the vital event registry should link to the same person record in the master person index.

Master person index

This component is responsible for storing a person's demographic and identifying information. All events in the vital event registry link to a person in the master person index. This enables a person's vital events to be grouped together. The master person index also allows multiple person identifiers to be stored and provides a single enterprise identifier to universally identify a person within the exchange. An advanced master person index also provides matching algorithms to detect and resolve duplicate person records.

Interoperability layer and audit repository

These two components are separate, yet related. The interoperability layer provides a single point of entry into the information exchange. By doing this it provides a single place to secure the communication channels between systems and to ensure that systems are authenticated and authorised. It also provides tools to monitor the operations of the exchange and a single place for client system to connect to in order to connect to the services of the exchange.

The audit repository is another security component; it ensures that interactions with the CRVS system are audited so that there is accountability from the system interact with the exchange. It also provides a history of what happened to a record if an investigation is necessary.

Messaging service

This component is responsible for communication with the general population regarding their vital event records. It should support multiple mechanisms that are deemed most appropriate for the implementation. E.g. email and sms.

Terminology service

The terminology service is responsible to make sure that all system exchange information is well understood by other systems. It stores code lists and tree structures representing terminology. This project only requires a very simple terminology service to be utilized as vital event records have a small set of well-defined fields. In this case the terminology service would merely provide access to code lists that provide codes for things like vital event type, status, facility lists etc.

CR Applications

The CR applications are the civil registry applications that the registrars from each of the different agencies use to capture registrations and to retrieve pending notifications. Ideally this would be a

single system which is used across agencies. It would be most efficient to have all agencies contribute to a single system, however, it would be possible to have multiple applications if an agency has particular needs or workflows.

All CR application/s will use the same set of standards to communicate with the CRVS system so it would be easy to add/replace applications as time goes on.

NIA

NIA is an external system that the exchange will need to interface with to validate and request a person's unique personal identification number (PIN). It is unknown how this system will look and what integration interfaces it will have at this point. The exchange will need to link into this system once it is deployed so it is vital that it is considered within this architecture.

eServices

The eServices are an external set of systems that provide services to the general population regarding civil events. These systems will interface with the system through the same standards-based interface that the CR applications do to provide the services that are required. The eServices software must make sure that only authorised information is returned to the general population.

Interoperability architecture

This architecture centres on the use of an interoperability layer to ease the challenges of managing an interoperable set of system as well as defining a standardised set of interfaces within the exchange for systems to utilize. These two core aspects are discussed in more detail below.

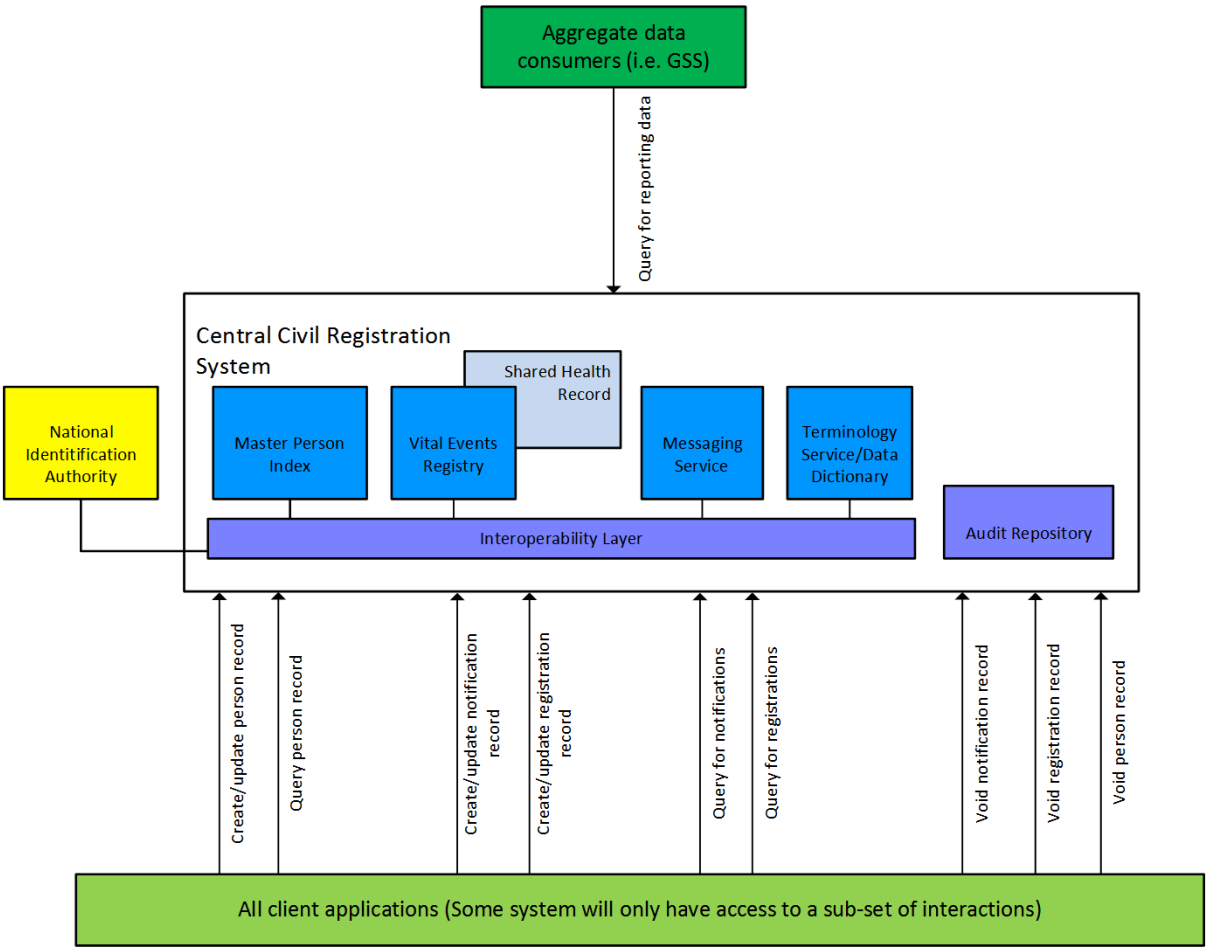
Importance of an interoperability layer

An interoperability layer provides a single point of entry into the exchange. It is responsible for ensuring that only authorised systems can communicate with the exchange and it also routes messages from systems to the correct component within the exchange. This allows each component to only handle a single concern. It also allows for a space where message transformation and/or orchestration can take place.

The interoperability layer also, importantly, provides a mechanism to monitor how the exchange of information is running and to flag any error in the running of the system. This is essential for the sustained operation of an interoperability architecture at scale.

In the diagram below and the security diagram further on in this document the interoperability layer can be seen playing an important role in easing system integration.

Interactions, messaging formats and exchange mechanisms



The diagram above maps out the interactions that are required for the client systems to function. There are no differences in the way different vital events communicated other than a difference in their data that is collected as a part of the record. Thus, the interactions can be generalised to cover each of the 4 vital events.

The diagram also shows an interaction where reporting data can be queried from the system for further use. The vital events registry will be responsible for making this data available as a periodic report of population data for a particular window of time.

Each of these interactions should be standardized using a message exchange format and mechanism. Below some potential solutions are discussed.

Standards-based interfaces

The use of messaging standards for interoperability is an important principle within this architecture. It allows each system to communicate with the central CRVS server using the same standardised format. This allows additional applications that interface with the CRVS system to be easily created and integrated into the exchange without the need for additional work to occur on the central service other than configuring the system to allow access. In addition, it allows the use of tools and technologies that already exist that integrate with that standards-based interface.

The type of data stored is highly structured and should be modified only with extreme care. It should also be possible to verify that the record remains valid and unchanged by un-authorised parties. This

situation lends itself to the use of document sharing mechanisms where each vital event is represented as a document that is then attached a person record.

Potential messaging standards

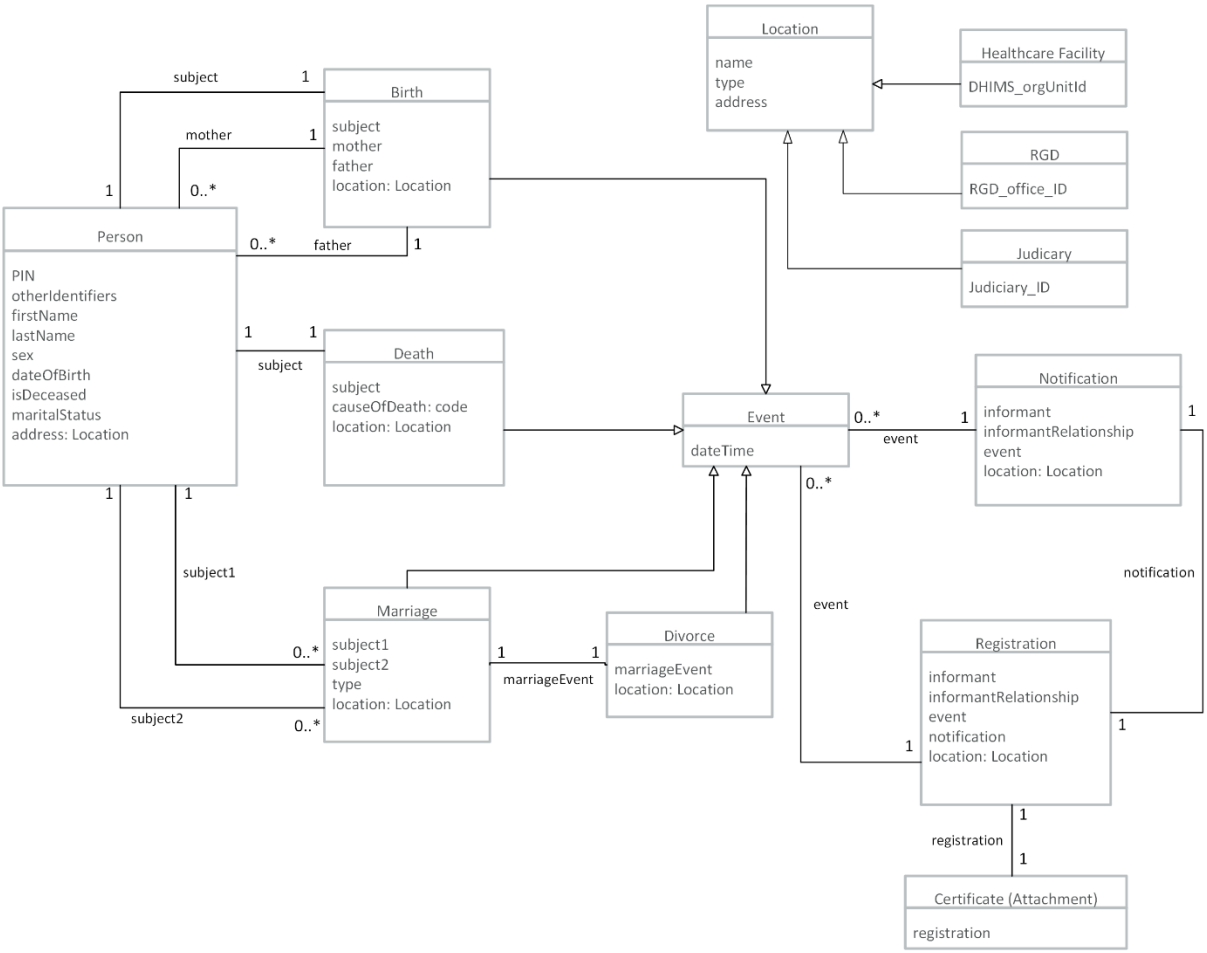
There are various standards in the eHealth space that provide a mechanism to create documents for information exchanges. The most modern and simplest to implement option in this space is the Mobile Health Documents (MHD) specification from Integrating the Healthcare Enterprise (IHE). This specification enables documents to be shared and queried between various systems. It also allows documents to be signed so that they cannot be changed in an un-authorised manner.

This standard describes the piping of how to send documents from one system to another and the metadata attached to documents, however, it doesn't describe the structure or contents of the document.

To describe the document structure and contents the use of FHIR documents is recommended. In FHIR a document can be created out of a bundle of FHIR resources. The data model proposed could be implemented using FHIR resources and bundled together to form a Vital Event electronic document. It is also possible to attach images or binary content to a document so that a scan of the original certificate could be stored alongside the electronic record. FHIR resources may have to be extended or custom resources created in places where the existing resources do not meet requirements for civil events, however, several useful resources already exist. Such as the Patient resource and the Location resource which would be suitable for this project's needs.

Data architecture

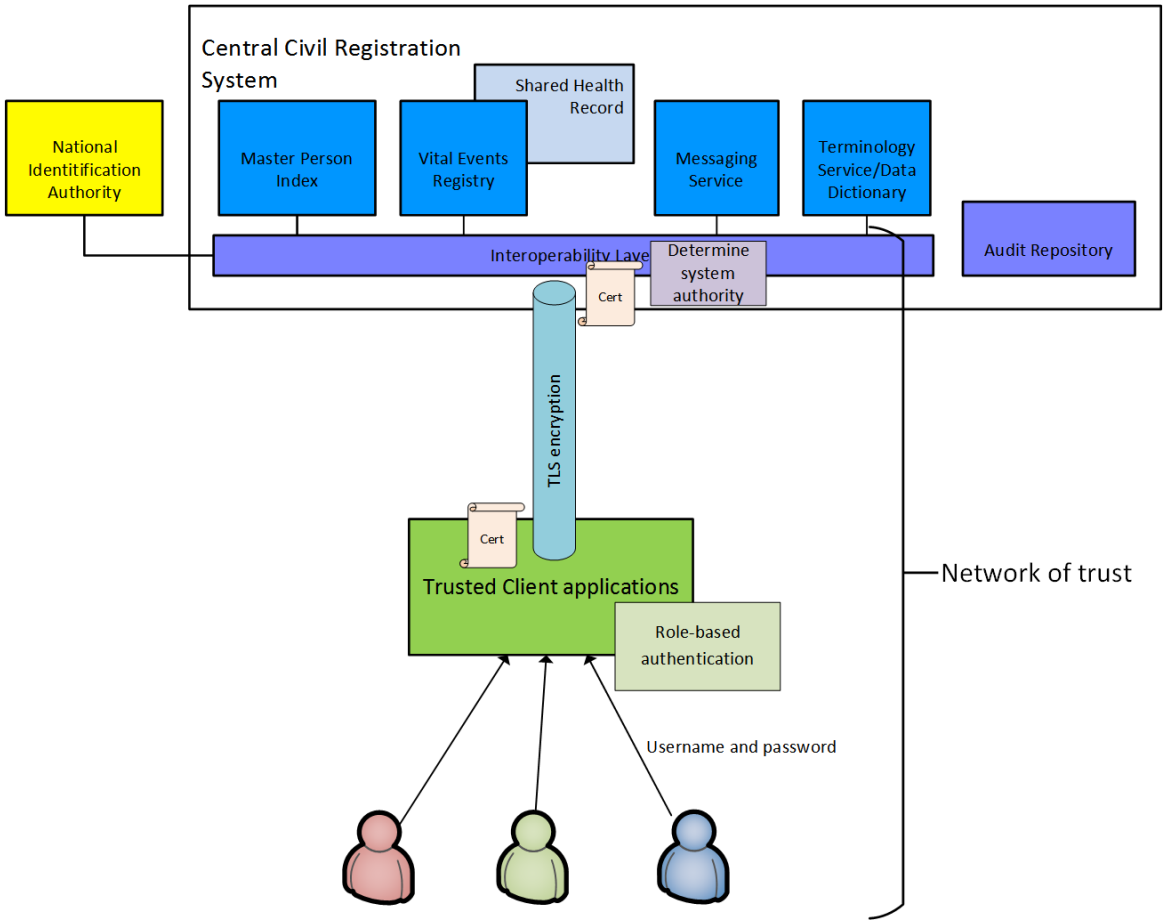
In the figure below the core elements of a conceptual data model to support the CRVS workflows has been drawn out. This diagram indicates the core relationships between each entity however, it does not impose any sort of restrict on the component that is responsible for storing each entity.



This architecture suggests that multiple components be created within the central CRVS system each with separate concerns. This often implies that they will handle a particular type of entity. In the following table, each entity is mapped to the component that is responsible for it.

Component	Entity/entities
Master person index	Person
Vital event registry	Event (Birth, Death, Marriage, Divorce)
Vital event registry	Notification
Vital event registry	Registration + Certificate
Terminology service/Data dictionary	Location

Security architecture



The security model in this architecture is based on the principle that only particular authorised systems are allowed to send messages to the exchange and that their actions are to be trusted. Certain systems will have access to interfaces that allow vital events to be created and edited and some systems will only have read access.

The Interoperability Layer is responsible for authenticating systems. This should be done using peer-certificate authentication using TLS. This is the same mechanism that allows websites to be secured over the internet however, in addition to the server presenting a certificate, both the client and the server presents a certificate. This ensures that both the client and the server are who they say they are. This also implies that every interaction with the central CRVS system must be encrypted to prevent un-authorised access to the data during transmission.

The interoperability layer should also handle system authority depending on identity of the authenticated system. A distinction should be made for systems that can view civil events data and those that can create and/or update event information or perform registration.

User authentication and authorisation is not handled by the Interoperability Layer but rather each trusted client system in the exchange is responsible for providing role-based authentication for each user. These roles will differ depending on the particular system. With only trusted system being allowed access to the exchange and each system performing their own role-based access control, a network of trust is created. This allows the exchange to stay secure without the complexity of managing individual users at the central level. However, it does require that systems should only be allowed access if they are engineered using good security principles. There should be process of

system verification and validation before a new system is authorised to use the exchange for the first time.

In addition to these security controls the system must also provide auditing services so that each record keeps track of who changes a record and where and when this took place. The audit repository in the central CRVS system is responsible for storing and archiving this data.

It is also recommended that the data stored by the central CRVS system be encrypted at rest by the database technology that is used.