DRAFT - ICT Project Guidance

<TODO>

Version:

0.1

Author:

<name>, <role>, <group>

## Description

<TODO>

## Synopsis

<TODO>

## Contents

[Description 1](#_Toc145232973)

[Synopsis 1](#_Toc145232974)

[Contents 2](#_Toc145232975)

[Synopsis 3](#_Toc145232976)

[Introduction 3](#_Toc145232977)

[Heading Level 3 3](#_Toc145232978)

[Heading Level 4 3](#_Toc145232979)

[Appendices 4](#_Toc145232980)

[Appendix A - Document Information 4](#_Toc145232981)

[Images 4](#_Toc145232982)

[Tables 4](#_Toc145232983)

[References 4](#_Toc145232984)

[Review Distribution 4](#_Toc145232985)

[Audience 4](#_Toc145232986)

[Structure 4](#_Toc145232987)

[Diagrams 4](#_Toc145232988)

[Terms 5](#_Toc145232989)

## Introduction

BOSSCARD/ RAID: Background [], Objective, Options, Scope[In/Out], Stakeholders [Users], Constraints, Assumptions, Risks, Dependencies, Decisions, Deliverables.

# Integrations

## Client

Although self-explanatory, the first interaction requiring calling out is the connection between a Service Client and a Service.

Considerations:

* Communication between the devices must be secured against eavesdropping.
* On the HTTP based section of the WAN, this is done via using HTTPS instead of HTTP.
* Achieved by permanently redirecting all unsecured HTTP traffic towards an HTTPS equivalent.
* This redirection can be requested of Maintenance specialists to update the within the Infrastructure as Code instructions pushed to develop and maintain the underlying web server, or on a WAF in front of it, or wider solution (e.g. CloudFlare).
* Because insecure Cookies containing confidential information – e.g. a session cookie containing a session identifier -- may be sent over the unprotected HTTP channel before they are redirected back to a secure HTTPS equivalent, they have to be marked ‘secure’. Marking them ‘http-only’ at the same time is also recommended.

## Identity

Identity Provider (IdP) services are an essential

## Data Storage

### Confidential key store

The use of confidential key datastores are current best practice for persisting confidential system integration credentials.

Confidential key stores have features such that once entered, control panel GUIs don’t show the key value and block copy/pasting it back to desktops. Accesses are audited and logged for later review.

Note:  
In legacy designs, a system config file (e.g.: config.xml) might have been the recommended place to persist integration information.

The approach of using a config file had several security impacting limitations: as the information was in a code file, it often got checked into a code repository, with the inability of clearing it out once discovered, essentially compromising system security. If encrypted using a device MAC or similar, it required all servers to be configured with the same MAC, which is impossible to implement on shared servers, PaaS, etc.

Credentials that are stored in a keystore include the services described in this paper - namely:

* Data storage:
  + Relational database connection string identities
  + Document database credentials
  + Graph databases
* Caching:
  + Caching service credentials
* Search:
  + Search API credentials
  + Ip-location geolocation api credentials
* Etc.

Caching Services are in-memory key/value datastores shared between servers. They provide a necessary work around to the bottleneck of other forms of datastores (relational databases, etc., described next) that interact with underlying physical hard drives and are orders of magnitude slower than in-memory operations.

Note:  
In this list caching is purposely put before other forms of data storage simply because if not implemented early, developers don’t get into an habit of requesting resources from cache first, only falling back to datastore queries second, when the cache item has timed out, or it’s simply not appropriate to cache. Caching is one of those cross cutting services that takes a tremendous unnecessary amount of effort and cost to retrofit in correctly later.

### Relational Database

For decades the relational database has reigned supreme as the most practical and efficient means of persisting data[[1]](#footnote-2).

While ‘old’ compared to more modern forms of data storage (NoSql, etc.), it still rightly holds its primary position[[2]](#footnote-3) in critical systems.

Partly due to its age, it doesn’t use HTTP/S to accept request, it uses other ports  
(Sql Server default port is 1433).[[3]](#footnote-4)

The credentials required for developing a connection string to query this service are either retrieved at startup from the credential store mentioned earlier, or better yet, one uses password-less service accounts (e.g. Microsoft Secure Identities).

### Document Database

While current relational databases are now capable of also persisting document records, there are often reasons to persist data in databases services that are specialised in document storage.

Use cases for document storage include the storage of documents, tagged with non-relational database.

Note:  
document databases have several advantageous and disadvantages compared to relational databases. Advantages include ease of use, as well as the ability to get going when a relational schema has not been defined, and/or standards are still evolving, requiring a flexible storage format. Disadvantages include the requirement to perform schema validation in the logic layer (as it is not performed at the data layer), as well as the high cost of multi-record updates when relational patterns become apparent later.

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

### Graph Databases

While fringe 15 years ago, graph databases are front and center data stores in current designs. They are the basis of establishing links between resources to develop context (parent, children) and sequences (prev, next, and next choices), as well as relationships (equivalencies, opposites, recommendations, etc.).

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

### Search

Similar in some regards to cache, Search services are another type of high-speed mostly-in-mem database (they are also backed by storage).

Most forms of relational or non-relational database services suck at providing a means to search through them in the way that users use them in the real world. For one users mistype terms all the time, spelling phonetically, for another they also forget the exact term and write synonyms for a term they are looking for, and finally, they expect it to be blindingly fast, usable for auto completes, or returning values while they are still typing.

This essentially is everything that traditional databases, which focus on being good at other things, are not especially good at.

Hence the need for a specialised in-memory service that are being updated when records are being stored in a the traditional databases, making search tokens phonetically, etc.

Elastic search is a market leader in this space offered by all the major cloud service providers.

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

## Notification Services

SMTP Email Service

Every system needs to send out notifications.

In may be that some dependency services – eg. IdPs – will handle their own email notification needs, but every mature system evolves to needing to send out its own notifications.

This may be to inform users that a system may be unavailable for a duration of time starting on a specific date and time, due to an upgrade.

This may be to inform users that a new major release is available, with a list of new features.

This may be to inform users that a disclosure statements (e.g. tracking, privacy, data use, terms & conditions, etc.) of the service have been updated and the latest version can review and accept by them by clicking a specific link, etc.

The service used may be either an internal enterprise service (e.g., Microsoft Exchange, Google Apps, etc.) or a dedicated one-way service (Mailchimp, etc.).

Note:  
It is highly recommended that the domain used by the mail service as the sender domain comply with DMARC protocol and similar requirements – anything to improve the credibility and recognisability of the sender.

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

### Pop / IMAP Email Service

There are very few cases where a service needs to use IMAP or POP to query an email service to get a listing of email messages waiting for a person. But it can happen.

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

### Public Twitter / X / Mastadon / etc.

There may be some cases where a system needs to integrate with a social media service to publish notifications to the world and not just its users (as email based notifications are limited to).

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

## Service Monitoring Services

…

## Functionality Control Services

…

## User Services

### Feature or Resource User Rating Services

…

### User Self Help Services

…

### User Assistance Services

…

## Information Services

### IP-Geo Conversion Service

In enterprises there is a fascination with letting WAFs Geoblock requests from certain countries[[4]](#footnote-5). For this reason, geo-blocking is not seen as an application capability, and hence adding a IP-geo conversion service is often not added or added much later.   
We recommend that knowing where your service consumers come from, when, is an essential analysis concern, and instead recommend adding it early.

There are several services one can consider. Not many are free or offered by cloud providers, so a 3rd party subscription is required – which implies the expiration of accounts and/or payment methods needs to be put on both the risk and recurring events registry of the delivery program.  
  
The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

### Mapping Services

Another service that mature systems seem to over time evolve to relying on is a mapping/postal address services, useful for improving data quality by autocompleting billing and shipping address entries, finding the postal code for an address, find the geolocation of an address, distances between points, placing GPS values on a map, etc.

Note:  
For other metadata about addresses, e.g., voting blocks/wards, school districts, etc. other services are required, but at least a mapping service can ensure the address is correct and accurate before launching a request for more information based on them.

The credentials required for informing and/or querying this service are of course retrieved at startup from the credential store mentioned earlier.

## Decision and Workflow Management Services

### Rule Engine Services

### Workflow Management Services

Appendices

Appendix A - Document Information

### Images

[Figure 1: TODO Image 2](#_Toc144995112)

### Tables

[Table 1: TODO Table 3](#_Toc145048484)

[Table 2: TODO Table 2 3](#_Toc145048485)

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
|  |  |
|  |  |
|  |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to the project’s Glossary.

##### IT

: acronym for Information, using Technology to automate and facilitate its management.

##### ICT

: acronym for Information & Communication Technology, the domain of defining Information elements and using technology to automate their communication between entities. IT is a subset of ICT.

1. So much so that it swanned a whole era of incorrect system design that referred to a “data layer”, at the expense of mentioning other necessary integrations. [↑](#footnote-ref-2)
2. *when configured and used correctly.* [↑](#footnote-ref-3)
3. This becomes important when later developing Subnets around both web servers and storage services. [↑](#footnote-ref-4)
4. Nato embargoed, etc. [↑](#footnote-ref-5)