ENGAGEMENT SOLUTIONS

PRODUCT: ENGAGE

VERSION 11.1.0

FULL TECHNICAL OVERVIEW

TABLE OF CONTENTS

SECTION 1

1.1.Network

Civica: Engagement Solutions' Engage application along with the application databases reside on high powered servers within defined security level segments. All hardware devices within Civica:Engagement Solutions live hosting environment are duplicated to facilitate a highly redundant and resilient network.

Market leading security appliances at the perimeter provide rich stateful inspection of traffic flows protecting the application servers from malicious activity. The Intrusion Detection and Prevention Systems detect suspected efforts of network intrusion by using specially designed intrusion detection parameters and automatically block these attempts at security breaches.

All servers and follow the CIS (Center for Internet Security) guidelines which help reduce the attack surface through implementing best practise security configurations.

The Application servers are load balanced to enhance performance and improve availability. Should one of the servers fail the other will automatically service the load until the failed server is returned back to its functioning state.

The database server is hosted within an isolated network forcing database requests to be inspected a second time by the firewall. The database servers utilise clustering which provdes high avalabilty and disaster recovery *(explained in section 2)*. The data is secured at rest using Transparent Data Encryption. The databases are further protected with database level passwords and access-granting security features.

Weekly scans ensure our web sites, servers, and security devices are free of known vulnerabilities. It also determines whether our site passes the SANS Top 20 Internet Security Vulnerabilities list as defined by SANS, the FBI and FedCIRC.

Quarterly scans are carried out by an Approved Scanning Vendor (ASV) ensuring that the systems and Internet facing IPs adjacent to these systems are in line with PCI Compliance.

Secure Hosting

Our hosting environment is contained within the secure Tier 4 datacentre managed by one of the world's leading communications providers. These facilities are in line with UK Government's exacting security standards:

- *Card key entry systems* – the facility provides a secure environment that allows only authorized users to access the resources they need.

- *Diesel-powered emergency generators* – the site is able to provide uninterrupted power in the event of an electrical power outage.

- *Climate-controlled environment* – sensors help maintain climate conditions at the facility to prevent any problems that may be precipitated by changes in temperature, moisture, etc.

- *Secure cabinets* – within the facility, secure, tamper-resistant storage cabinets further protect the data.

- *Redundant Internet connections* – redundant connections provide assurance that breakdowns in Internet connections do not disrupt online processes.

- *24-hour security* - the hosting facility provides 24x7 monitoring, maintenance, and security, including video camera surveillance and dry fire suppression.

1.2.Data Access

The security, integrity, and confidentiality of data is protected with a limited number of Civica: Engagement Solutions employees allowed access to the databases. Accessing the production databases requires passwords from each member of the Civica technical team.

1.3.Application Development

Application development proceeds through four discrete levels: *Programming, Testing, Client Review,* and *Production.*

Change Control manages the transition of the application through the four levels of the development process. This ensures division of work and minimizes the potential for collusion.

- *Programming* develops the application and has access only to test data.

- *Testing* is performed by the QA department. The QA department has read-only access to the QA machines. Strict exit criteria must be passed for an application to be considered acceptable and to be moved to the next level.

- *Client Review* is the final phase of testing, where the final application build becomes the production version of the application for the client to review.

- *Production* oversees the hosting facility and is responsible for the security of the application. *Production* is the only group to use real data.

SECTION 2

2.1. Application Architecture

The product is designed from the ground up as a secure, high-availability, n-tier internet-facing application.

The software is structured to take advantage of current mainstream Microsoft .NET technologies deployed in a secure Windows server-farm environment with redundancy and fail-over designed in.

The product does not require the installation of any software on the user's systems. A standard internet browser with the Adobe Flash player and an internet connection is all that is needed.

2.2. User Interface Layer

The user interface layer utilises the Adobe Flex system. This is an application presentation system from the same family as the ubiquitous Adobe Flash player (the end-user must have the standard Adobe Flash player installed). Communication with the server is secure, using SOAP over TLS 1.2 (HTTPS) with the wrapper web service.

The Flash Player security rules disallow access to data resources unless the domains match exactly, including sub domains and even if the domain names resolve to the same physical address. That means that a *.swf* deployed at www.example.com cannot access data from test.example.com or even example.com unless the server explicitly allows access.

For security reasons – we are not exposing the main web service to the client (exposing = publish in the same domain as the .swf file) so we created a wrapper web service published on the same domain as the .swf file.

The clients will have access only to this server.

2.3. Presentation Layer

The presentation layer runs on Web Servers which consist of two parts

- The Flex application
- The Wrapper Web Service (written in .Net 4.0)

The Flex application is executed on the client side by the Flash Player. All the client requests are sent to the Member DB web service through the wrapper.

2.4. Business Layer

The business layer is implemented as a .NET web service which connects to a SQL Server 2014 database. We will refer to this web service as the Member DB web service.

The Member DB web service is the “brain” of this system. This web service implements

- the algorithms used by the system to generate the reports
- the process for postcode / address validation
- the security layer
- defines the business objects
- the business rules

The Member DB web service has direct access to the database server and it is not accessible from outside the network (not public facing).

All the methods calls are validated in respect of the following

- Security ID – composed from a user ID and a Pin
- Token – received by the client application at login
- Time – the time when the command was sent

No database connection will be made unless the method call is validated.

2.5. Data Layer

The data layer consists of a SQL Server 2014 database. Engage has been designed to be fast and reliable.

The well-defined database structure facilitates membership reports, addition of new members as well as searching and amending the existing members.

2.6. Communication Security

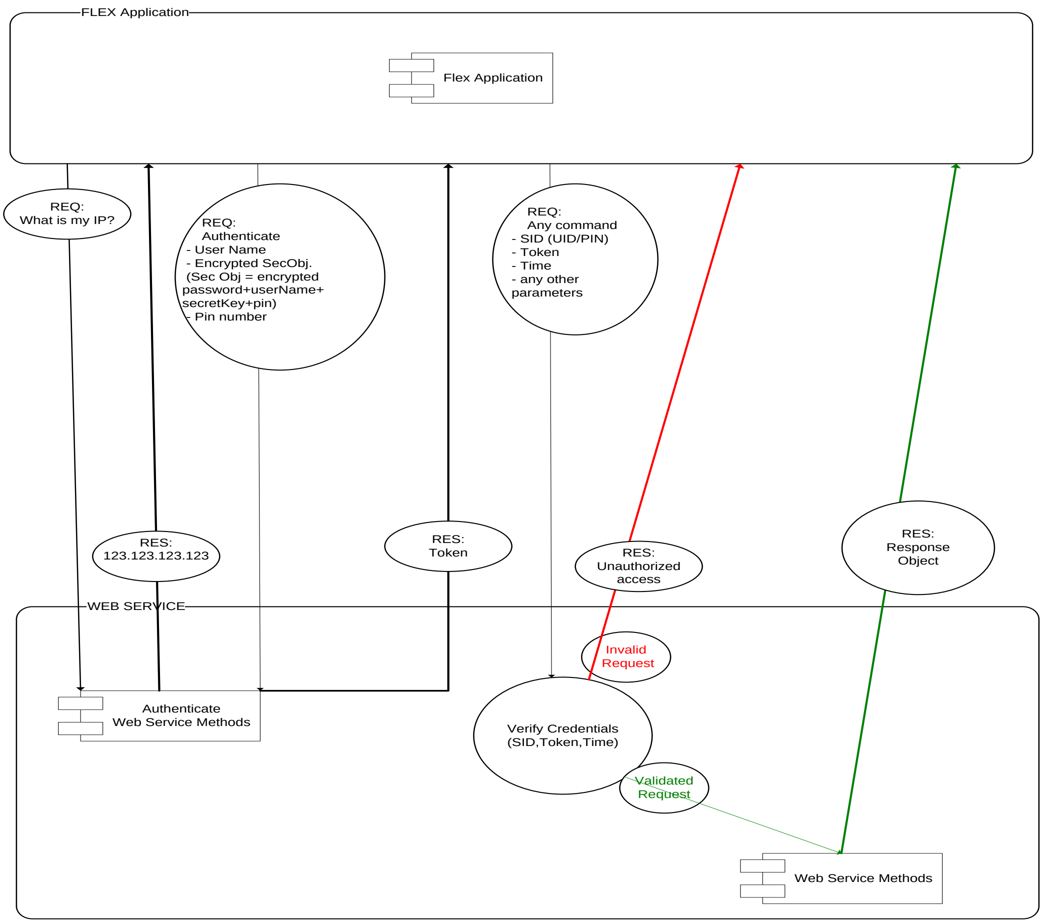
The security layer is designed to mitigate a number of security threats arisen from the implementation of an N-tier model through web services.

More specifically, the following issues have been taken into account:

a. For each web service call:
    a. User authentication (i.e. who is the current user?)
    b. Client identity (i.e. making sure the session is maintained from a single client)
    c. Session identity (i.e. making sure one user has only one session open at a time)
    d. Call validity (i.e. has the call been tampered with?)

b. Initial user authentication (logging in to the application)
    a. Authentication through sensitive information (e.g. password)

This system relies on the MD5 checksum algorithm and Base64 encoding.



2.7. Path taken by Secure Session

Figure 1 displays and explains the logical path a secure web session takes when entering the hosting network.

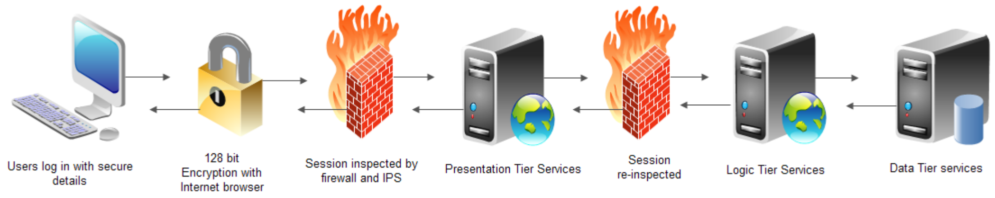


Figure 1

SECTION 3

3.1. Disaster Recovery

ERS’ has implemented a disaster recovery plan to facilitate Web Service continuity should a major catastrophe take place at the Datacenter. The procedure would involve all Web Services being redirected to ERS’ HO where a ‘skeleton network’ would then service all incoming requests. This environment has redundant internet connections via two separate Points of Presence.

This would allow ERS to make the necessary arrangements to recover the Datacenter, or in worst case scenario, implement a new hosting environment at one of our service provider’s alternate locations.

3.2. Web Hosting and Disaster Recovery Base Design

Figure 2 displays ERS’ live hosting infrastructure along with the DR failover site.

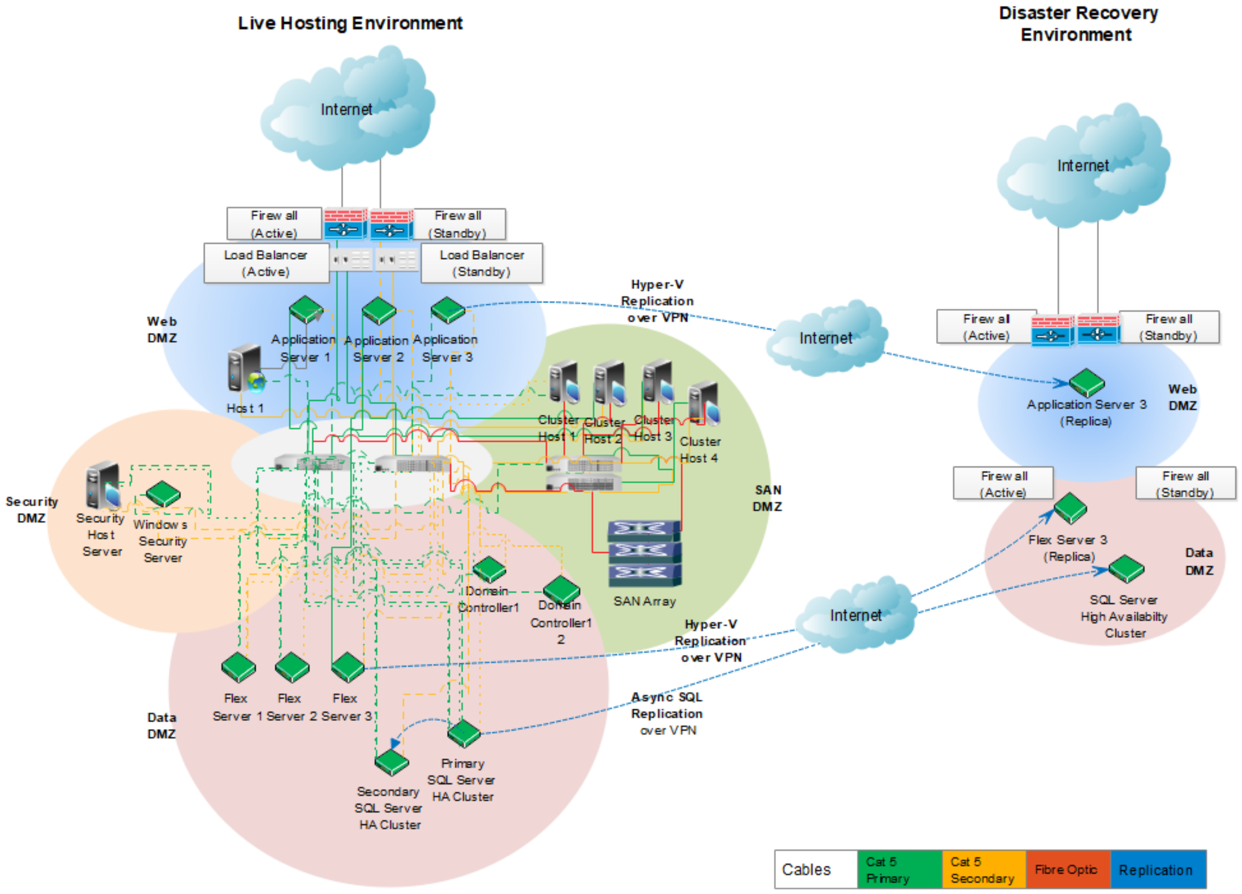


Figure 2

SECTION 4

4.1. Web Services and Network Monitoring

ERS has implemented several 24/7 monitoring services in order to proactively counteract and eliminate downtime.

Third party Web Site Performance Monitoring provides ERS with graphical overviews including Total Response Times and Overall Uptime Status. This monitoring platform takes place from three separate locations namely, London, New York and Los Angeles where thresholds within the monitoring have been set. Should they be exceeded, engineers are automatically notified via text message and email.

Further to that, ERS has implemented its own internal monitoring, not only on Web Service responses, but all critical devices within the network. Again, should thresholds be exceeded engineers are notified via text message and email.

SECTION 5

5.1. Summary

ERS utilizes industry best practice, third party software and multiple levels of security to safeguard its client’s information. ERS strives to meet the highest levels of Web Service availability possible through its resilient and fully redundant network.

Authors: Hannah Staunton
Damian Coverly

Revised: 19/09/2019