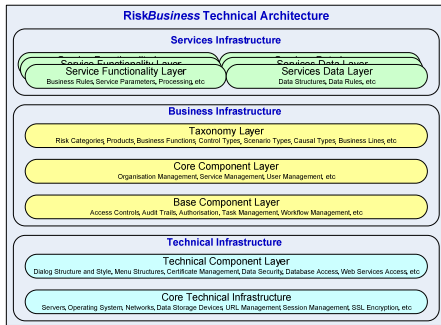


# Technical Architecture



**Introduction:** The overall technical architecture upon which all of the RiskBusiness Services have been designed is to provide a platform where many different services can be configured and reside on a single hosted platform supporting many organisations.

This technical architecture provides great flexibility in supporting the demands of this environment and we have utilised a parameter driven component design to deliver fast cost effective solutions to our subscribers.

The technical and business infrastructure layers support many services layers. The list of components in each layer are not exhaustive but illustrative of the type of function performed at each layer.

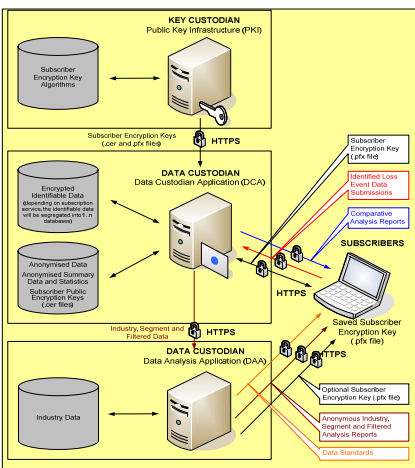
The technical architecture has been built using standard Microsoft technologies and deployed onto standard Microsoft server and database technologies. Client access to the system is either via a browser or a web service. Microsoft Excel is the primary tool used for data analytics and reporting. No proprietary tools are used anywhere within the overall architecture.

Essentially, the technical architecture delivers an application server provider (ASP) model whereby a set of web services are exposed across the internet, along with a standard user interface to execute the services, all within a security environment.

**Security:** The technology architecture underlying RiskBusiness Services has been primarily designed to ensure that appropriate and adequate levels of confidentiality and security are in place. The technology environment incorporates the following main architectural elements:

- User authentication;
- Data submission technology;
- Data storage and security;
- Data verification and checking applications;
- Data analysis applications; and
- Reporting applications for generating statistical reports and analytics.

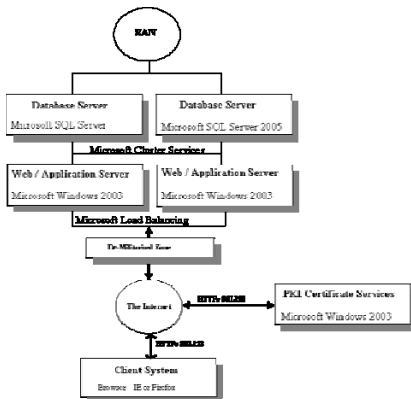
Subscriber data is exchanged with the application servers using a 128-bit encrypted SSL session (HTTPs) between the application/database servers and the Subscriber's access point to ensure that the data is not intercepted and deciphered as it is transmitted over the Internet. The SSL digital certificate is issued by Verisign and stored on the data application/database web servers, which is separate to the PKI security used for data storage purposes.



Establishing absolute security for Subscribers data is a key objective that is met through the use of Public-Key Infrastructure (PKI) technology. PKI technology is a well-known and accepted approach to providing ***distributed security*** for internet-based applications or security where the users are not part of the same network and have no common security credentials.

PKI solutions provide a robust approach for enabling user identification and data encryption and decryption. PKI provides three capabilities that are especially valuable to businesses:

- First, it provides privacy for data. The keys are the primary mechanism for data encryption (using the public key) and decryption (using the private key).
- Second, PKI allows for robust identification, or *authentication*, of users.
- Finally, PKI provides for non-repudiation – the ability to irrefutably prove that someone took a particular action. This capability can be further enhanced by issuing a token that stores the private key of the PKI certificate on a personal device, thereby eliminating the need for the one-time password solution.



In short, PKI provides an efficient way to manage data encryption and can be extended to enhance user authentication.

A public-key system (or asymmetric encryption) uses *two* keys: a ***public*** key which is shared and a ***private*** key that must be closely held. These keys are complementary: if you encrypt something with the public key, it can only be decrypted with the corresponding private key, and vice versa. Public-key systems depend on the mathematical relationship between the public and private keys. One key cannot be derived from the other.

The goal of encryption is to obscure data in such a way that it can only be read by the intended party. In the use of public-key cryptography within the various RiskBusiness Subscription Services, the data servers hold the public-key (contained in a digital certificate) used for data encryption. To decrypt the data, the data server needs access to the private key, which must be provided by an authorised user within the organisation that owns the data. Only the Subscriber's 'Key Administrator' User controls private key distribution. Access to the private key allows for data to be decrypted. Note that there is ***no*** "master" private key that will allow the RiskBusiness Services Team or any other application or user to decrypt any encrypted data.

For more information on the Technical Architecture, please contact RiskBusiness International through one of the contacts provided on our website or email us at [info@RiskBusiness.com](mailto:info@RiskBusiness.com).

