# Fact Sheet

Cogito Group

# TLS / SSL Encrypted Defence

## What are TLS and SSL?

Transport Layer Security (TLS) and Secure Socket Layer (SSL) security are cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network. TLS is an updated, more secure, version of SSL. Most data transmitted over the internet is unencrypted, meaning sensitive information can be easily monitored and tracked by unknown third parties, including:

- Login details.
- Credit card details.
- Personal details.
- Browsing habits.
- E-mail correspondence.
- Online chats.
- Conferencing calls.

By ensuring your client and server applications support TLS, you ensure data transmitted between them is encrypted by secure algorithms and not viewable by third parties. The TLS/SSL security protocol can be used to help protect against masquerade attacks, 'man-in-the-middle' or 'bucket brigade' attacks, rollback attacks, and replay attacks. To ensure a high level of security, TLS uses a combination of Symmetric and Asymmetric Key Cryptography.

### Symmetric Key Cryptography

Within the Symmetric Key Cryptography process, data is encrypted and decrypted with a secret key known to both sender and recipient. This process is efficient in terms of computation, but a common secret key requires the sharing of the key between parties to be conducted in a highly secure manner.

### Asymmetric Key Cryptography

Asymmetric Cryptography uses key pairs for a public key and a private key. The public key is mathematically related to the private key, but of sufficient length that it is computationally impractical to derive the private key from the public key. This allows the recipient's public key to be used by the sender to encrypt the data, but also that this data can only be decrypted with the recipient's private key.

# TLS / SSL Encrypted Defence

Fact Sheet

The advantage of Asymmetric Key Cryptography is the process of sharing encryption keys does not necessarily have to be secure, but the mathematical relationship between public and private keys means that much larger key sizes are required. Once the session is over, the session key is discarded. When utilising TLS, it is desirable that a client connecting to a server is able to validate ownership of the server's public key. This is normally undertaken using an X.509 digital certificate issued by a trusted third party known as a Certificate Authority (CA) which asserts the authenticity of the public key.

## Benefits

The high-level benefits of TLS/SSL security protocols include:

- The enablement of secure internet connections.
- Safeguarding sensitive data that is being sent between two systems.
- Preventing unwanted third parties from reading and modifying any information transferred, including potential personal details.
- Ensuring that any data transferred is impossible to read.
- Utilising encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.
- Can be used to protect any sensitive or personal data including credit card numbers, other financial information, names, and addresses.

For complete security, it is necessary to use TLS/SSL protocols in conjunction with a publicly trusted X.509 Public Key Infrastructure (PKI) in order to authenticate that a system to which a connection is being made is indeed what it claims to be.

## About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.