

Nursery-Net - Security Technologies

This document is intended to inform you on the security practices used throughout the Nursery-Net software and the number of different encryptions and security methods used to keep all data secure.

SSL

In Nursery-Net all web service communication is over HTTPS connections, via a secure Nursery-Net certificate validation. SSL allows the Nursery-Net client to communicate with our servers across the internet in a way designed to prevent eavesdropping and tampering.

VPN

Client data communication to our remote servers is over encrypted VPN connections instigated by the client. Currently there are two VPN types supported, these are PPTP (Point-to-Point Tunnelling protocol) and the more secure L2TP (Layer 2 Tunnelling Protocol). Communicating over VPN gains a high level of security, using advanced encryption and authentication protocols to safeguard data from snoops, data thieves and other unauthorised parties.

MD5 / SHA1 Hashing

Passwords entered into Nursery-Net are at no point stored as plain text, when a password is stored in Nursery-Net it is cryptographically stored as a Digital Fingerprint (sometimes called a hash value) making all passwords able to withstand all known types of cryptanalytic attack.

RSA Public-Key Cryptography

This is the first encryption method used by Nursery-Net over SSL to retrieve login and connection settings for the client's specific service. Rather than using a single password or Key to both encrypt and decrypt data, Public-Key (or "asymmetric") cryptography uses a pair of complementary keys meaning, data encrypted with one of the keys can *only* be decrypted by the other

AES/Rijndael Symmetric Cryptography

AES is used primarily for Nursery-Net web service communication; it provides traditional private-key encryption/decryption using the "Rijndael" algorithm which has been adopted as the US Government's Advanced Encryption Standard. The same key is used to decrypt data as was originally used to encrypt it, this ensures a single session that can only be translated to and from the server and client who made the request. This means a high level of security as if the data was intercepted midway it could not be decrypted as only the client machine has the decryption key.

Nursery-Net Remote Servers

The Nursery-Net remote servers are Non-Shared servers, meaning they are solely used by Nursery-Net for Nursery-Net data only. They are protected via a number of Firewalls and are limited to only establishing VPN connections; in addition to this the servers are not physically accessible to anyone apart from our CRB checked maintenance personnel. In the unlikely event that a server was compromised all data is stored encrypted and so would be unreadable and useless to anyone.