

easipay plus has been designed as an n-tier application.

Customers using the **easipay plus** web application communicate with the ASP.NET **easipay plus** web applications. These are hosted on a web server running Microsoft Internet Information Services (IIS). Customers are authenticated against the **easipay plus** internal authentication mechanism and log into **easipay plus** using a user name provided by Trace Payroll Services. Customers will be provided with an initial one-time password by Trace Payroll Services which the user is forced to change the first time they login.

Role Based Security

easipay plus uses its own internal role based security model to control user access to the application. A role has the following properties and privileges assigned to it:

- Application Security – Data and screens within the system are divided into user defined applications. Application security defines which of these applications a role can access
- Module Security – Controls access to the Document Explorer application
- Table Security – Defines table, row and field level security for data
- Object Security – Documents, reports and communities are security on an object by object basis. Each object has read, write and delete access defined to it

Password Rules

Internal Authentication supports the following password rules:

- Letters-only passwords not allowed
Determines if a user's password must contain numbers as well as letters.
- Minimum password length - Determines the minimum number of characters a password can contain.
- Maximum failed logon attempts - Defines the maximum number of invalid logon attempts allowed before a user's account is frozen.
- Password Never Expires - Determines how many days a password is valid for and if the password expires. When a password has expired, the user account is suspended and the user can no longer log on to the application. The user is warned ten days before password expiration and prompted to change their password.

Authentication

Authentication is the process of checking a user's credentials in order to confirm they are who they say they are. This is performed when the user logs into **easipay plus**.

The user name and password is matched against a list of user names and passwords stored in the **easipay plus** database. The passwords are stored in an encrypted format. The user name and password entered in the logon screen is passed from Internet Explorer to the **easipay plus** web application in plain text and Secure Sockets Layer (SSL) is used to encrypt this data.

Internal Authentication is performed using ASP.NET Forms Authentication. If a user attempts to access the **easipay plus** web application without first authenticating then they are automatically redirected to the logon page.

ASP.NET Forms Authentication transmits the user name and password from Internet

Explorer to the **easipay plus** web application in clear text, SSL is used to encrypt this traffic.

Once a user has successfully authenticated they are issued with a security key which is stored in a cookie on the user's machine. This key is passed with all subsequent requests and is used by ASP.NET to determine if the user has been authenticated. The cookie used to store the security key on the user's PC is non-persistent and is present only as long as their browser is open. Also, once the user logs out, or has been inactive for a period of time, this security key becomes invalidated on the web server.

Authorisation

Authorisation is the process of checking if a user has security access to a particular resource or function within **easipay plus**.

easipay plus uses its own custom authorisation based upon roles assigned to a user. Each role has a set of privileges assigned to it.

Before a user's request is processed a test is performed to see if any of the roles assigned to the user have the required privileges to perform the requested action.

If the user does not have the required privileges then an application exception is thrown. This exception is handled in the **easipay plus** web application and administrator console application and an error message is display to the user informing them that they do not have the required privileges.

Data Security

Microsoft SQL Server is used to store the **easipay plus** data. Microsoft SQL Server is a well established and secure database management system.

Table and Column Security

Users can be prevented from reading, writing or deleting records from specified tables. Security can be controlled down to column level within a table. This has been implemented using SQL Server Views.

Row Level Data Security

Row-level security has been implemented in **easipay plus** as Microsoft SQL Server does not support row security at a granular level as required in **easipay plus**. This allows control, at a fine level, of the records that a user can view, modify and delete. Row level security is defined for **easipay plus** roles and roles are then assigned to users. For example, a view that enables a line manager to only see their own personal details and the details of the employees that directly report to them may be defined. This level of control enables Trace Payroll Services system administrators to precisely define the data that may be viewed, modified and deleted by users.

Secure Sockets Layer Encryption of Network Data

easipay plus uses Secure Sockets Layer to provide 128 bit encryption of the data transferred between the client, Microsoft Internet Explorer and the **easipay plus** server applications.

Auditing of Data Changes

easipay plus enables the optional auditing of changes made to the data contained in **easipay plus** database tables. Auditing is controlled at table level and can be switched on or off for individual tables. When a change is made to a row within the table the original and new row is stored in the audit table.

Prevention of Common Security Issues

SQL Injection

easipay plus uses parameterised SQL statements and stored procedures to eliminate the possibility of SQL Injection attacks.

In addition to this **easipay plus** executes SQL statements and stored procedures that receive parameter value input from the user under dedicated SQL Server user accounts that do not have access to view system tables or perform Data Definition Language (DDL) statements.

Cross Site Scripting (XSS) / HTML & Script Injection

On some sites, it is possible for a user to type HTML tags and/or script into an input field. For example, the site may ask the user to enter a review of a book on sale on the site. The user can enter HTML / script in the input field, and this will be saved in the database on the web site. When the web site then displays this data back to other users, their browsers interprets this HTML / script as part of the page, thereby altering the page layout, running script in the user's browsers, etc.

ASP.NET (used by **easipay plus**) prevents HTML and script character combinations being entered in input fields, in the query string, etc; thereby preventing the above form of attack.

ViewState Modification

ViewState is a hidden field stored in a number of pages on the site. This field stores temporary information about the controls displayed on the current page. When the user submits this page back to the server, our application makes use of some of the values stored in the ViewState, in order to correctly display controls on the next response page.

To prevent the user from altering any value in the ViewState, we enable ViewStateMac in ASP.NET. If the user manually modifies with any value in the ViewState, or tries to manually create their own ViewState, the server will detect a change has occurred, and it will reject the request.

Disclosure of Sensitive Information

Applications can inadvertently disclose information that can potentially help a hacker compromise the security of a web site. **easipay plus** protects against this using several methods.

Hashing of Passwords

Passwords stored in the database are not stored as plain text but are encrypted using Salted Password Hashes. Hashing is a one way process where the passwords are encrypted. It is mathematically unfeasible to decrypt them. Therefore, if a user inadvertently gains access to the table in which passwords are stored then they will not be able to read the passwords.

Encryption of Sensitive Application Settings

Application settings such as database connection strings are stored in configuration files in a secure encrypted format using Microsoft Data Protection Application Programming Interface (DPAPI).

All Application Errors are Handled

Configuration settings in ASP.NET applications make it possible for unhandled application errors to be displayed to the user along with the source code where the error occurred.

easipay plus disables this option and additionally handles all un-trapped errors messages and displays a user friendly error dialog. In addition to this, all un-trapped errors are logged to the **easipay plus** database and optionally the Windows Event Log.

Theft of Authentication Cookies

Once a user has been authenticated a Cookie is issued to the user. If another user steals this Cookie then they can access the system as if they were the original authenticated user. **easipay plus** authentication Cookies are restricted to use SSL only. This provides a very strong defence against Cookie theft.

easipay plus System Segregation

Although databases exist on the same physical server, they are completely separate from each other; each customer system uses its own virtual folders for access via HTTPS which point directly to their own databases.

Physical Infrastructure

Physical

All hardware is secured behind triple locked doors in a dedicated communications room. Access to the communications room is restricted to authorised key holder personnel and is locked at all times.

Web Servers

All web facing servers are in a separate perimeter network and are double firewall protected. Access to the **easipay plus** hosted service is accessible from any PC with an internet connection, however access to the servers and their operating systems are kept restricted to Trace Payroll Services support staff, this reflects the service on offer; unrestricted access to your data via the web with secured access to the underlying servers to Trace Payroll Services support staff only.

SSL Connectivity

- Access to the customer system is not restricted to IP address in order to allow the widest possible access (i.e. from home, customer site, abroad etc) to Payroll and HR data.
- To enhance security, connections to the web servers are protected by 128bit SSL encryption.
- All HTTP requests are redirected.
- Security certificates are supplied by Verisign/Thawte.

Network

- Internal network protected by multiple firewalls.
- Windows servers are monitored and kept up-to-date with Microsoft security updates. Internet access within the LAN filtered and restricted using Websense.
- Passwords changed every 30-days.
- Up to date and centrally managed antivirus software is deployed on all computers. All email scanned by trusted external bureau for spam and viruses before it even reaches Trace's own email servers.
- All emailed scanned again for viruses on email servers and again on employee PC's (i.e. triple scanned with different AV products).
- Network access is security audited.
- Elevated network privileges only held by a small number of trusted staff.
- Technical team who maintain the in-house systems are all Microsoft qualified and trained to cover Data Protection Act issues.