TRAMS PCI FAQs

The purpose of this document is to explain the encryption process and other security related features in Trams and ClientBase with the goal of assisting agencies with their PCI questions and compliance.

DISCUSSION POINTS:

- What is PCI?
- What role does Trams and ClientBase play with agency PCI compliance?
- How do Trams and ClientBase products address encryption?
- How does encryption work?
- What role does password security play?
- Future PCI enhancements.

What is PCI?

The payment card industry (PCI) compliance and validation regulations spell out what security measures must be taken to protect the private information during any transaction occurring with the use of a credit card. The PCI Data Security Standard is used by all card brands to assure the security of the data gathered when transacting on behalf of a customer.

There are two different types of PCI standards, PCI-DSS and PA-DSS:

- PCI-DSS covers the overall security of Credit Card data storage and transmission.
- PA-DSS covers turnkey software that is installed on the client premises that needs to be PCI-compliant.

For more information regarding PCI, please visit: https://www.pcisecuritystandards.org/index.shtml

Fundamental PCI Guidelines

- Don't store credit card data if it's not absolutely needed.
- Mask credit card data as much as possible.
- Encrypt credit card data wherever it is stored.
- Implement controls so only people who need access to the unmasked credit card data can see it.

What role does Trams and ClientBase play with agency PCI Compliance?

Trams Back Office and ClientBase Windows (distributed applications):

Since Trams Back Office and ClientBase Windows are distributed applications, and the database is not hosted by Trams/Sabre, our software is just one component to your agency's overall responsibilities as they relate to PCI. We have taken steps to implement required PCI and security functionality within our products to support our customers' PCI compliance, but we do not hold any responsibility to assist agencies with their self-assessment (SAQD) efforts nor supply letters of attestation. Self-assessment questions apply to an agency's environment and internal employee practices as it pertains to handling and protecting credit card data as a Credit Card Merchant.

If you are a credit card merchant, you are required to validate and report compliance to your merchant processor to ensure that you remain compliant and avoid potential non-compliance fees. There are a number of companies that you can engage to help navigate through the self-assessment questionnaire or conduct on-site audits. For example, iATS has coordinated with a company called Security Metrics who charges a reasonable fee to guide an agency through completing the necessary questionnaire and scanning. Here's a link to this information:
http://www.iatspayments.com/english/securitymetrics.html

ClientBase Online (hosted application):

As a Sabre hosted solution, ClientBase Online goes through annual PCI certification audits and is regularly updated in order to comply with the PCI certification guidelines.

How do Trams and ClientBase products address encryption?

Trams Back Office | ClientBase Windows | ClientBase Browser | ClientBase Online

As of Trams Back Office 3.3 and ClientBase Windows 3.6, all regular credit card and customer bank account data stored in the database is encrypted, and access to unencrypted data is controlled and logged.

As of version 4.0, the ClientBase Live Connect User Name, Account Number, and Password fields, as well as the TBO CC Processor User Name, and Password fields, are encrypted (these changes were done for security purposes and not as part of PCI compliance). In addition, we use a stronger hash function (SCrypt) for storing user passwords in the database. All credit card numbers in the database, whether valid or invalid, are now masked.

Database Central/ClientBase Marketing Services

All sync copies in DBC are either encrypted (ClientBase Windows 3.4 and up) or are not storing Credit Card data.

Live Connect and Sync

These systems pass encrypted data from ClientBase via web services or web apps. The data transmissions use SSL and HTTPS to encrypt data being sent from ClientBase to the booking engine or Sync Web Service.

How does encryption work?

How are encrypted credit card numbers stored?

Credit card numbers are stored in the database encrypted and masked throughout all of the Trams applications. A field exists in the database to accommodate the encrypted credit card number, and another field contains a masked version of the number. During encryption, a cleaning and masking routine takes place to standardize all of the credit card numbers so they can be properly masked for all applications utilizing the masked credit card field.

Does encryption delete or hide credit card numbers in the database?

No, the encryption process does not hide, remove, or delete credit card numbers from the database. However, in all Trams programs the full credit card number is not displayed unless absolutely necessary. Most screens will display a masked version (example: VI 41-XXXX-1111). In ClientBase and Trams Back Office, viewing the full credit card number is controlled with user permission so the agency can determine which users have access to full credit card numbers. When a user views the full credit card number, a log event is created including:

- Date/Time
- Username
- Credit Card number
- Screen or report they were in when the full cc number was viewed

An Audit Report can be located in Trams Back Office under **Reports|Payments|Audit**.

What other changes will I see in the database after encryption?

When entering credit card data, a validation on the card number is performed. If ClientBase detects the number is invalid, the system prompts the user with a message. Trams Back Office validates credit card numbers for the CC Merchant form of payment if the option is enabled.in ClientBase, a prompt was added when connecting to a Live Connect provider that uses HTTP and not the secure connection (HTTPS).

How do I know if the database is encrypted?

In ClientBase Windows, go to **Help | About ClientBase.** If CC Encryption Done = Yes, then the database is encrypted. In Trams Back Office, go to **Help | About**. If Database Encrypted = Yes, then the database is encrypted. In ClientBase Browser, go to **Tools | About**. If CC Encryption Done = Yes, then the database is encrypted. ClientBase Online has always been encrypted.

What type of encryption does Trams use?
Trams products use AES-128 encryption. Passwords are stored encrypted in the admin.ib file on the server. Interbase XE and higher supports AES as the encryption method, although DES is still available.

Can encryption key access be restricted?
The encryption key is generated from a password. Only provide the password to those with permission to generate key. A unique encryption key will be generated for each agency that can be used in product development for applications that will need to read the full credit card number. The key can be obtained by a SYSDBA log-in only by going to Utilities | Credit Card Encryption Key and entering a password provided by the Trams Support desk (Trams.TBOsupport@sabre.com). A CCEncrypt.dll file is installed that allows access to the Trams database to view un-encrypted Credit card numbers.
For the purpose of rotating an encryption key, version 117 or higher of the DBUP.exe can be used (with the additional command line parameter –REENCRYPT, will allow for credit card numbers to be re-encrypted so that a new encryption key may be generated. This feature is only available for *non-syncing* databases.

Can old credit card information be removed?
In ClientBase and Trams Back Office, old credit card data can be permanently masked so that the ability to view a full credit card number no longer exists (See Utilities/Purge/Credit Card).

What role does password security play?

Password Security Best Practices:
- ***SYSDBA*** *Password should never be left as the default*
- *Individual User Logins should be created and used when logging into the database*
- *User Login Passwords should be updated periodically*
- *User Login Passwords should never be shared*
- *User Login Passwords should not be easily guessed*

Extended Password Security (EUA enabling must be configured))
To enable EUA within your database, please email Trams.TechDesk@Sabre.com. Once enabled:
- Password Strength: At least 8 chars, alpha + numeric.
- Forced Renewal: Password must be changed every 60 days.
- No repeating passwords: System remembers the last 4 passwords entered.

Future PCI Enhancements

Encryption Key Rotation
- PCI requirement is that the encryption key be rotated (changed) at least yearly.
- We have a manual solution in place today and are working on a more automated process.

Disable SYSDBA Login
- PCI requirement is that each user log in with a unique username. Currently, certain operations need to be done as SYSDBA. Change will be to prompt the administrative user for SYSDBA password when performing these operations and to restrict being able to log in as SYSDBA.