



Secure Storage to Token Management Service Migration



Integration Guidance



Contents

1. Introduction	3
Summary	3
Audience and Purpose	3
Pre-requisites	3
2. Token Management Service	3
Introducing Token Management Service	3
What's New?	4
Functional changes compared to Secure Storage	4
Considerations when migrating to Token Management Service	5
Token Management Service Permissions	5
3. Token Management Service Migration Process	5
Requesting a Secure Storage to Token Management Service migration	5
Criteria for a MID to be eligible for a Token Management Service migration	6
Token Management Service Migration timeframes	7
Cancelling a Token Management Service Migration	7
4. Token Management Service New Token Formats	8
Token Management Service formats compared with Secure Storage	8
Unsupported Token formats on Token Management Service	8
5. Token Management Service New Token Types	9
Token Management Service Token Types comparison	9
Customer Token	10
Payment Instrument	10
Instrument Identifier	10
6. Token sharing on Token Management Service	10
Introducing the Token Management Service Vault	10
Unsupported token sharing formats on Token Management Service	11
7. Using Token Management Service with Connection Methods	11
Simple Order API - NVP	11
SOAP Toolkit API – XML	12
REST API	14
Secure Acceptance	14
8. Token Management Service New Response fields	15

WSDL Versions for New Response fields.....	15
New Response fields per Connection Method.....	15

1. Introduction

Summary

This is a help and guidance document for merchants wishing to migrate their Tokenization Product from Secure Storage to the Token Management Service which is CyberSource's new Tokenization offering.

This guide is designed to support merchants in understanding the key differences between Secure Storage and Token Management Service, and to assist the integration changes that might be required, depending on the merchant's integration specifics.

Audience and Purpose

The intended audience for this document is Merchants who are currently using Secure Storage / Recurring Billing and intend to migrate onto Token Management Service to take advantage of the new features and functionalities that this offers.

Pre-requisites

In order for merchants to migrate onto Token Management Service, they must have Secure Storage and / or Recurring Billing enabled for their MIDs in either CAS or Production. There are a number of eligibility requirements for merchants to successfully migrate which will be called out in this document.

2. Token Management Service

Introducing Token Management Service

Token Management Service (TMS) enables you to safely store customer information, including payment data, in secure Visa data centers. It replaces this data with tokens that can be used when requesting other Cybersource services.

Token Management Service is an evolution of the Secure Storage Tokenization product, designed to replace Secure Storage and offer enhanced functionalities.

Once migrated onto Token Management Service, merchants can take advantage of the new functionalities and services that Token Management Service offers.

What's New?

Token Management Service comes with new capabilities and the following benefits:

- **Storage cost per unique PAN:**

Token Management Service charging is per unique Instrument Identifier (PAN) rather than per token so, some merchants with duplicate tokenised PANs may see a cost reduction.

- **PAN multichannel tracking:**

Token Management Service provides Intelligent Single-Instance Storage (SIS) of PANs, providing a merchant with multichannel tracking abilities.

- **Customer wallet:**

Token Management Service supports a full customer wallet capability with multiple payment & shipping options per customer.

Token Management Service is interoperable with the latest Cybersource products & services such as Microform & Unified Checkout.

- **Network token ready:**

Token Management Service is network token ready providing improved authorisation rates & PAN lifecycle updates.

- **REST API integration:**

Token Management Service is accessible via REST APIs in addition to SCMP, Simple Order API, SOAPI & Secure Acceptance, as well as Cybersource other connection methods providing a modern development experience.

Functional changes compared to Secure Storage

Token Management Service has a number of functional changes that are different to Secure Storage once integrated, each of which are called out in this document. Outside of the new services Token Management Service offers above, there will also be a potential change in the token formats, token types, token sharing structure and response fields that merchants are used to when using Secure Storage.

For a more detailed breakdown on each of the changes mentioned, please proceed to section 3 onwards of this guide where these are called out with examples provided.

Considerations when migrating to Token Management Service

Once migrated to Token Management Service, there will be new services and functionalities offered which are outlined in section 5 of this guide onwards. Merchants must understand these changes to ensure their integration can support the potential differences and are able to take advantage of the enhanced offerings of Token Management Service. Cybersource **strongly** recommend that all MIDs are first migrated in our CAS testing environment, so merchant integrations can be tested and validated before doing this in the Production. If merchants explicitly request a migration in the Production environment without testing CAS, Cybersource would require a business case as to why CAS testing is being excluded, with a written request to proceed with the migration in Production. Once the request is approved, Cybersource will schedule the migration in Production as normal.

Token Management Service Permissions

When creating and managing Tokens via the EBC UI, there are different EBC User Permissions for Token Management Service vs Secure Storage. For EBC users who have custom user roles with specific permissions for Secure Storage, these same custom user roles will need to have Token Management permissions added to ensure users can continue to view, create, retrieve, edit and delete tokens using the EBC UI.

3. Token Management Service Migration Process

Requesting a Secure Storage to Token Management Service migration

For merchants proactively looking to migrate to Token Management Service, this can be done by contacting Cybersource support through your normal support channels and formally requesting a Token Management Service migration in writing.

Once approved, the migration can start after a minimum **48** hours, but this is subject to Cybersource existing migrations that are already in progress. On occasion, Cybersource will schedule this after other migrations which are already in progress meaning the start time will be more than **48** hours in the future.

As per Cybersource plan to End of Life Secure Storage and migrate all MIDs onto Token Management Service, we are actively working through a list of MIDs that are currently eligible for a migration and are

contacting merchants through their Account Managers with dates as to when we will initiate a migration from Cybersource side. Merchants who are deemed eligible and contacted will be given **60** days' notice before the migration will start as per our standard notice for all Production changes. This notice period will give merchants a chance to prepare their integration and raise any queries they may have in the meantime with regards to the changes when using Token Management Service.

Criteria for a MID to be eligible for a Token Management Service migration

The following criteria must be met per MID for all merchants migrating to Token Management Service:

- **Secure Storage / Recurring Billing**

MIDs must have Secure Storage or Recurring Billing enabled to migrate.

- **16 Digit Last 4 Preserving token format**

The 16 digit Last 4 Preserving token format is not supported on Token Management Service. MIDs using this token format on Secure Storage will need to switch to one of the other supported formats before the migration can start. Existing tokens in this format on Secure Storage can still be migrated over to Token Management Service, but Token Management Service does not support the creation of **NEW** tokens in this format. Token Management Service will continue to return the last 4 digits of the customer's PAN once migrated, however these will be returned in the new "*Instrument Identifier*" field in the API response. Please see section **8** of this guide for the API location where the last 4 digits of the PAN will be returned on TMS.

- **Account Updater**

Account Updater must be disabled for the duration of the migration. Token Management Service and Account Updater are compatible, but the Account Updater service must be disabled whilst the migration is in progress and can be re-enabled once the migration has completed in full.

- **Token sharing structure**

MIDs that plan to token share on Token Management Service must sit inside the same Single Sign On (SSO) Account for them to continue token sharing once migrated. MIDs token sharing outside of a singular SSO will need to be updated to sit inside the same account before the migration can start. For more information on the token sharing structure on Token Management Service, please refer to section **6** of this guide.

Merchants who have MIDs that are deemed not eligible due to any of the above points will be contacted by Cybersource with options provided on how to make their MIDs eligible for migration.

Token Management Service Migration timeframes

As per section **3** of this guide, the soonest a Token Management Service migration can start once a MID is deemed eligible is **48** hours in the future, subject to existing migrations that are already in progress. Once the migration has been initiated, there will then be a 14-day period for the migration to run and complete. This brings the total migration period including the 48-hour scheduling to 16 days in total.

Merchants proactively requesting a Token Management Service migration with their Account Managers will be provided a specific start and end date, with timestamps as to when the migration is expected to complete. For merchants who are contacted by Cybersource to be migrated on our eligible MIDs schedule, Cybersource will provide a 2-week period in which the migration will begin.

There will be no interruption to service in the 16 days whilst the migration is in progress, merchants can continue to run Secure Storage tokenization requests and process transactions using tokens without issue. Token Management Service tokens will continue to be synced back into Secure Storage during this period, in the event a Token Management Service migration is cancelled for any reason.

Cancelling a Token Management Service Migration

Merchants are able to request that a Token Management Service migration is cancelled any time in the 16-day migration period mentioned above by contacting Cybersource through their Account Managers or through their normal support channels. Merchants should provide a business case for the migration cancellation as well as ensure this request is made within 48 hours of the migrations expected completion date to ensure this request can be processed and completed. Once cancelled, the MIDs being migrated will be reverted to back to Secure Storage and the tokens created in the migration period will be reverted in kind and continue to be available.

4. Token Management Service New Token Formats

Token Management Service formats compared with Secure Storage

Token Management Service will respond with a Token Identifier in the same manner as Secure Storage, but certain formats will start with different values when compared as per the below table. Merchants should ensure they are not using logic that incorporates the leading digits of the token before upgrading to Token Management Service. This leading digit change will only impact the format of **NEW** tokens created once migrated; the existing tokens identifiers will remain the same as they were on Secure Storage to ensure merchants can continue to retrieve these as normal.

Token Format	Secure Storage starting with	TMS Post Migration starting with
22 Digit	0-9	0-9 (No Change)
16 Digit Mod 10	99	95
16 Digit Last 4 Preserving	99	Not supported on TMS

Unsupported Token formats on Token Management Service

As per section **3** of this guide, the 16 Digit Last 4 preserving token format is not supported on Token Management Service. Existing tokens in this format on Secure Storage can still be migrated to Token Management Service, but Token Management Service does not support the creation of **NEW** tokens in this format.

Merchants using this format will need to switch to another supported format before the migration is initiated; Cybersource recommendation would be the existing 16 Digit Mod 10 format.

5. Token Management Service New Token Types

Token Management Service Token Types comparison

Token Management Service offers enhanced Token Types over Secure Storage, meaning tokens are now broken down into a 3-level hierarchy with a token identifier for each element. Each level of the Token Management Service token will now have its own unique identifier which stores specific elements of customer information from the next. Merchants wanting to continue using Token Management Service in the same method as Secure Storage should present the "Customer Token" value or the "Subscription ID" in place of the Secure Storage token value, to ensure the same level of customer information is automatically presented in each request.

The below table confirms which Token Management Service token types contain and present which customer information elements based on each:

Token Type	Credit Card	eCheck
Customer	<i>Payment Instrument plus:</i> Shipping Information	<i>Payment Instrument plus:</i> Shipping Information
Payment Instrument	<i>Instrument Identifier plus:</i> Card Type Expiry Date Billing Information	<i>Instrument Identifier plus:</i> Account Type Drivers Licences Information Billing Information Company Tax ID SEC Code Merchant Descriptors Merchant Defined Data
Instrument Identifier	PAN	Account & Routing Number

Customer Token

Providing the Customer Token value in an authorization request will present all of the available customer information inside a token, including the Shipping and Billing details. Providing this token value will be consistent with the behavior of passing the Subscription ID value used on Secure Storage.

Payment Instrument

Providing the Payment Instrument value in an authorization request will present all of the information from the Instrument Identifier token, plus the Billing information, expiry date and merchant defined data.

Instrument Identifier

Providing the Instrument Identifier value in an authorization request will present just the Payment Account Number value for the token. For Cybersource services that require a Billing Address, Card Type or expiry date; merchants will need to provide these in addition to the Instrument Identifier value.

6. Token sharing on Token Management Service

Introducing the Token Management Service Vault

Token sharing on Token Management Service has now been revised compared to Secure Storage. All Token Management Service tokens are now stored in a Token Management Service Vault, which is owned by a Single Sign on Account (SSO) instead of a singular transacting MID. This means tokens are no longer stored at MID level, but at the SSO account level that sits above one or more transacting MIDs. All MIDs that require token sharing on Token Management Service must now sit inside the same SSO, which is a functional difference from secure storage.

Unsupported token sharing formats on Token Management Service

As part of the migration eligibility checks that are conducted when a Token Management Service migration is requested, Cybersource will report on any MIDs that are currently token sharing between different SSO Accounts. Merchants with MIDs in this sharing format will need to make a decision to either bring the different MIDs under one SSO Account with Cybersource or forfeit token sharing on the MIDs highlighted.

7. Using Token Management Service with Connection Methods

Simple Order API - NVP

The Simple Order API Connection Method is backwards compatible with Token Management Service and Secure Storage, meaning merchants should not need to change their standard integration to continue using tokenization requests once migrated.

See the below request examples for each tokenization service using Simple Order API:

- **Creating a Token Management Service Token**

Continue to call the [PaySubscriptionCreateService](#) in the same method as Secure Storage. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

- **Retrieving a Token Management Service Token**

Continue to call the [PaySubscriptionRetrieveService](#) in the same method as Secure Storage, passing the Token Management Service Customer Token value in place of the Secure Storage Subscription ID. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

`recurringSubscriptionInfo->subscriptionID = 'EE49871E7A9566ABE053AF598E0A4EF9';`

- **Updating a Token Management Service Token**

Continue to call the [PaySubscriptionUpdateService](#) in the same method as Secure Storage, passing the Token Management Service Customer Token value in place of the Secure Storage Subscription ID. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

```
recurringSubscriptionInfo->subscriptionID = 'EE49871E7A9566ABE053AF598E0A4EF9';
```

- **Deleting a Token Management Service Token**

Continue to call the [PaySubscriptionDeleteService](#) in the same method as Secure Storage, passing the Token Management Service Customer Token value in place of the Secure Storage Subscription ID.

```
recurringSubscriptionInfo->subscriptionID = 'EE49871E7A9566ABE053AF598E0A4EF9';
```

SOAP Toolkit API – XML

The SOAP Toolkit API Connection Method is backwards compatible with Token Management Service and Secure Storage, meaning merchants should not need to change their standard integration to continue using tokenization requests once migrated.

- **Creating a Token Management Service Token**

Continue to call the [PaySubscriptionCreateService](#) in the same method as Secure Storage. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

```
<paySubscriptionCreateService run="true">  
</paySubscriptionCreateService>
```

- **Retrieving a Token Management Service Token**

Continue to call the [PaySubscriptionRetrieveService](#) in the same method as Secure Storage, passing the Token Management Service Customer Token value in place of the Secure Storage Subscription ID. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

```
<recurringSubscriptionInfo>  
<subscriptionID>EFE0F26C9F6A9B42E053AF598E0A304E</subscriptionID>  
</recurringSubscriptionInfo>  
<paySubscriptionRetrieveService run="true">  
</paySubscriptionRetrieveService>
```

- **Updating a Token Management Service Token**

Continue to call the [PaySubscriptionUpdateService](#) in the same method as Secure Storage. Token Management Service will respond with new response fields, see section **8** of this guide for examples.

```
<recurringSubscriptionInfo>  
<subscriptionID>EFE0F26C9F6A9B42E053AF598E0A304E</subscriptionID>  
</recurringSubscriptionInfo>  
<paySubscriptionUpdateService run="true">  
</paySubscriptionUpdateService>
```

- **Deleting a Token Management Service Token**

Continue to call the [PaySubscriptionDeleteService](#) in the same method as Secure Storage, passing the Token Management Service Customer Token value in place of the Secure Storage Subscription ID.

```
<recurringSubscriptionInfo>  
<subscriptionID>EFE0F26C9F6A9B42E053AF598E0A304E</subscriptionID>  
</recurringSubscriptionInfo>  
<paySubscriptionDeleteService run="true">  
</paySubscriptionDeleteService>
```

REST API

Token Management Service is compatible with Cybersource's REST API Connection method, offering enhanced support with the new REST API endpoints below. These new endpoints can be used to take advantage of the new Token Management Service token types and offers flexibility for merchants utilizing these token types at any level.

- **Customer**

<https://apitest.cybersource.com/tms/v2/customers>

- **Payment Instrument**

<https://apitest.cybersource.com/tms/v1/paymentinstruments>

- **Instrument Identifier**

<https://apitest.cybersource.com/tms/v1/instrumentidentifiers>

For more details on how to utilize each of these Token Management Service REST API endpoints, please see the [Cybersource Developer Center](#). Token Management Service API request and response examples can also be viewed and tested on the [Cybersource Developer API reference](#).

NOTE: REST API integrations are not available during the migration to Token Management Service, including the 16-day rollback period. Once the rollback period is complete and clients are fully activated for Token Management Service, new REST API integrations following the above guidance can begin.

Secure Acceptance

Merchants integrating with Secure Acceptance Hosted Checkout, or Checkout API can continue to pass the Token Management Service Customer Token value in place of the Secure Storage Subscription ID, which is in the **PAYMENT_TOKEN** field for all tokenization services.

8. Token Management Service New Response fields

WSDL Versions for New Response fields

For Cybersource Simple Order API and SOAP Toolkit API, the new response fields for Token Management Service services will not be returned until merchants have also updated their WSDL version in their integration to version **1.135** or later.

For a full list of WSDL versions including the latest, please see the below link:

<https://ics2wsa.ic3.com/commerce/1.x/transactionProcessor/>

New Response fields per Connection Method

Once a MID has been migrated to Token Management Service and the WSDL version has been updated as above, there will be new response fields returned for certain services per Connection Method which are listed as below with examples. Per section **3** of this guide, Merchants who were using the last 4 digits of the customer's PAN suffix on TMS can now find this in the highlighted "*InstrumentIdentifierId*" field below:

- **Simple Order API - NVP**

The Simple Order API Connection method will return **new** response fields for the following services:

PaySubscriptionCreateService

PaySubscriptionRetrieveService

PaySubscriptionUpdateService

Name Value Pair example:

```
[paySubscription*Reply] => stdClass Object
(
  [reasonCode] => 100
  [subscriptionID] => EFA1F65B40744D8AE053AF598E0A0735
  [instrumentIdentifierID] => 7030000000010691111
  [instrumentIdentifierStatus] => ACTIVE
  [instrumentIdentifierNew] => N
)
```

- **SOAP Toolkit API – XML**

The SOAP Toolkit API Connection method will return the **new** response fields for the following services:

PaySubscriptionCreateService
 PaySubscriptionRetrieveService
 PaySubscriptionUpdateService

XML Example:

```
<paySubscription*Reply>
  <reasonCode>100</reasonCode>
  <subscriptionID>F02D0DD6556A4956E053AF598E0A6769</subscriptionID>
  <instrumentIdentifierID>7010000000054930005</instrumentIdentifierID>
  <instrumentIdentifierStatus>ACTIVE</instrumentIdentifierStatus>
  <instrumentIdentifierNew>N</instrumentIdentifierNew>
</paySubscriptionCreateReply>
```

- **Secure Acceptance – Hosted Checkout**

The Secure Acceptance – Hosted Checkout integration will automatically handle the new response fields inside the Cybersource hosted payment response page.

- Secure Acceptance – Checkout API

The Secure Acceptance – Checkout API Connection method will return the **new** response fields for the following services:

Create_payment_token

Update_payment_token

reason_code:	100
payment_token:	F0E1842777F8AD76E053AF598E0AE0A9
payment_token_instrument_identifier_id:	703000000000208 4242
payment_token_instrument_identifier_status:	ACTIVE
payment_token_instrument_identifier_new	N