







## GS525 – Document Archival and Compliance Audits in Globalization Studio

Submitting invoices or tax documents is only half the story. Many jurisdictions require businesses to retain signed documents for years, and be able to produce them instantly during an audit.

If your documents are scattered across desktops, emails, or local folders, you're at serious risk.

In this article, you'll learn how to:

-  Archive documents securely using **Azure Key Vault** and **Blob Storage**
-  Optionally use **SharePoint** for user-friendly access
-  Enable audit reporting with Power BI and Submission History
-  Apply retention policies to comply with country-specific requirements

 This article connects with [GS514 – Output Routing](#), and [GS517 – Error Logs](#)




---

### Why Archiving Matters

Compliance regulations require:

- Storing **signed** versions of invoices or tax files
- Keeping records for **5–10 years**
- Providing evidence of **submission and result**
- Ensuring **auditability** on request

Without proper archiving:

-  You may be non-compliant
  -  Waste hours digging through logs
  -  Risk reputational damage and financial penalties
-



## Electronic Invoicing Prerequisites: Why Azure Key Vault and Storage Are Required

Component	Purpose
Azure Key Vault	Stores digital certificates used for invoice signing securely
Azure Blob Storage	Stores output files like XMLs, PDFs, metadata, and logs
Storage SAS URL / Managed Identity	Grants secure access to the configured blob container

When used with **Electronic Invoicing**, these tools help ensure:

- Regulatory compliance (e.g., Spain SII, Italy SDI)
- Secure and auditable storage
- Scalable, cloud-native document management

---

## Step-by-Step: Configure Key Vault and Storage for Archiving

### ☒ Step 1: Create an Azure Key Vault

1. Sign in to Azure Portal
2. Go to **Key Vaults > + Create**
3. Fill in:
  - Name: d365-keyvault-prod
  - Region: Same as your Dynamics 365 instance
4. Under **Access configuration**, select Vault access policy
5. Click **Review + Create**, then **Create**



Key vault

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Resource visualizer

Events

Objects

Keys

Secrets

Certificates

Settings

Access configuration

Networking

Microsoft Defender for Cloud

Properties

Locks

Monitoring

Automation

Help

Delete → Move ↕ Refresh Open in mobile

JSON View

Resource group (move) : KeyVault

Location : United Kingdom West

Subscription (move) : 54

Subscription ID : 54

Tags (edit) : Add tags

Vault URI : https://[redacted].azure.net/

Sku (Pricing tier) : Standard

Directory ID : [redacted]901

Directory Name : Comline

Soft-delete : Enabled

Purge protection : Disabled

Get started Properties Monitoring Tools + SDKs Tutorials

Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.

Control access to key vault

Assign access policy and determine whether a given service principal, namely an application or user group, can perform different operations on key vault keys, secrets or certificates.

Access configuration

Access policies

Access control (IAM)

Enable logging and set up alerts

Enable logging to monitor how, when and by whom your key vaults are accessed. Monitor performance and configure alerts for key vault metrics e.g., service API latency, error code, throttling.

View

Turn on recovery options

For protection against accidental or malicious deletion, soft-delete is enabled. Turn on purge protection to guard against manual purging of deleted key vaults and items. [Learn more](#)

Explore

Add or remove favorites by pressing Ctrl+Shift+F

## ☑ Step 2: Create a Blob Storage Account

1. Go to **Storage accounts > + Create**
2. Set:
  - Name: d365archivestorage
  - Performance: Standard
  - Redundancy: Locally-redundant (LRS)

ypeistorageaccount

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for

Upload Open in Explorer Delete → Move ↕ Refresh Open in mobile CU / PS Feedback

JSON View

Resource group (move) : [redacted]

Location : United Kingdom West

Primary/Secondary Location... : Primary: West Europe, Secondary: North Europe

Subscription (move) : [redacted] CA

Subscription ID : [redacted] 54

Disk state : Primary: Available, Secondary: Available

Tags (edit) : Add tags

Properties Monitoring Capabilities (7) Recommendations (1) Tutorials Tools + SDKs

Blob service

Hierarchical namespace : Disabled

Default access tier : Hot

Blob anonymous access : Disabled

Blob soft delete : Enabled (7 days)

Container soft delete : Enabled (7 days)

Versioning : Disabled

Change feed : Disabled

NFS v3 : Disabled

Allow cross-tenant replication : Disabled

Storage tasks assignments : None

File service

Large file share : Enabled

Identity-based access : Not configured

Default share-level permissions : Disabled

Performance : Standard

Replication : Read-access geo-redundant storage (RA-GRS)

Account kind : StorageV2 (general purpose v2)

Provisioning state : Succeeded

Created : [redacted]

Security

Require secure transfer for REST API operations : Enabled

Storage account key access : Enabled

Minimum TLS version : Version 1.2

Infrastructure encryption : Disabled

Networking

Public network access : Enabled

Public network access scope : Enabled from all networks

Private endpoint connections : 0

Network routing : Microsoft network routing

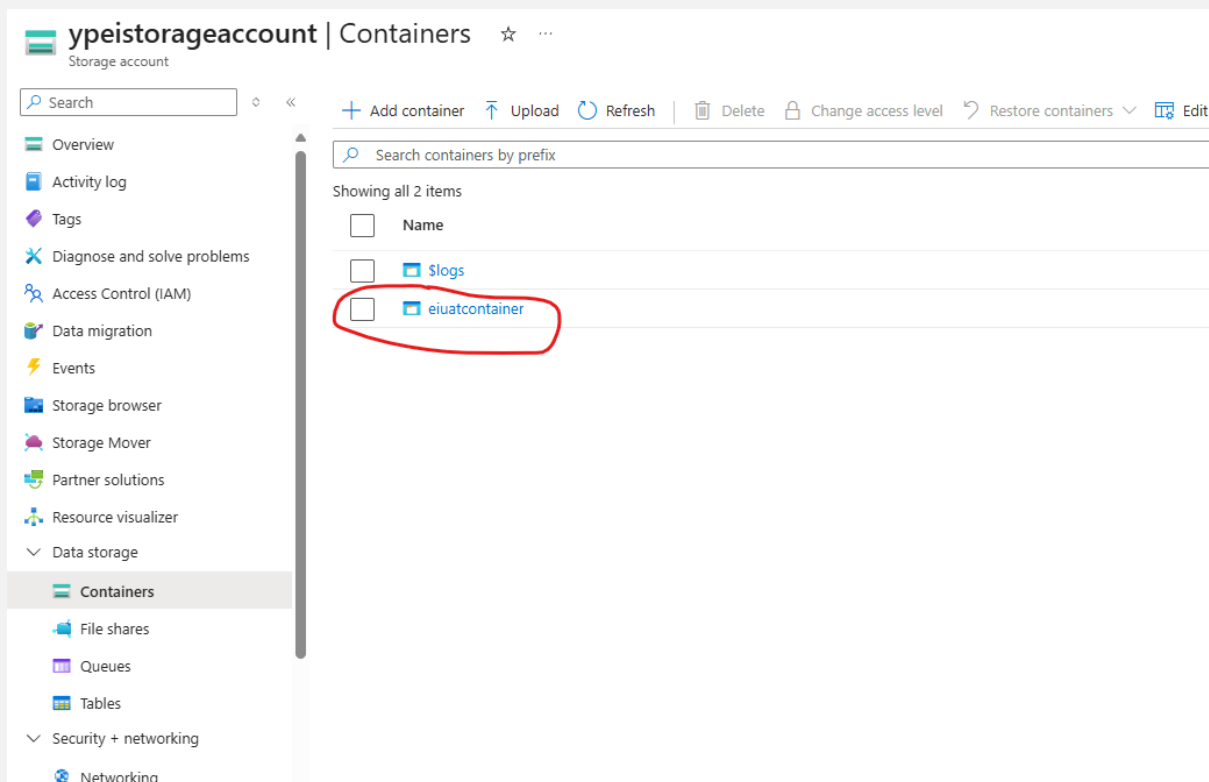
Endpoint type : Standard

Add or remove favorites by pressing Ctrl+Shift+F



3. After creation, go to **Containers** and add a new container:

- Name: e-invoicing
- Access level: Private (no anonymous access)



### ☒ Step 3: Store Storage account secret in Key Vault

1. Collect Storage account connection string



ypeistorageaccount | Access keys ☆ ...

Storage account

Search

Set rotation reminder Refresh Give feedback

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account.  
[Learn more about managing storage account access keys](#)

Storage account name  
ypeistorageaccount

**key1** Rotate key  
Last rotated: 26/06/2025 (34 days ago)  
Key  
..... Show  
Connection string  
..... Show

**key2** Rotate key  
Last rotated: 26/06/2025 (34 days ago)  
Key  
..... Show  
Connection string  
..... Show

## 2. Go to Key Vault > Object > Secret > Generate/Import

Key vault | Secrets ☆ ...

Search

+ Generate/Import Refresh Restore Backup Manage deleted secrets View sample code

Name	Type	Status
------	------	--------



Home > Key vaults > CIBProd | Secrets >

## Create a secret

Upload options: Manual

Name \*  Provide a name

Secret value \*  Enter the secret. Add Blob primary connection string here

Content type (optional)

Set activation date ☐

Set expiration date ☐

Enabled: Yes No

Tags: 0 tags

## Step 4: Setup Entra ID app and key vault access

### 1. Register Entra App

KeyVaultApp

Search

Overview

- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
  - Branding & properties
  - Authentication (Preview)
  - Certificates & secrets
  - Token configuration
  - API permissions
  - Expose an API
  - App roles
  - Owners
  - Roles and administrators
  - Manifest
- Support + Troubleshooting

Essentials

Display name	: KeyVaultApp	Client credentials	: 0 certificate, 2 secret
Application (client) ID	: 9[redacted]61	Redirect URIs	: Add a Redirect URI
Object ID	: [redacted]0c	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: [redacted]01	Managed application in L	: KeyVaultApp
Supported account types	: My organization only	State	: Activated

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

### Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

#### Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

#### Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

[View all quickstart guides](#)

#### Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

[Go to Enterprise applications](#)

### 2. Generate Certificate & secret



KeyVaultApp | Certificates & secrets

Search

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication (Preview)

**Certificates & secrets**

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (2)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
SecretN	027	v...	be...

### 3. Give Graph permission

Branding & properties

Authentication (Preview)

Certificates & secrets

Token configuration

**API permissions**

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Configured permissions

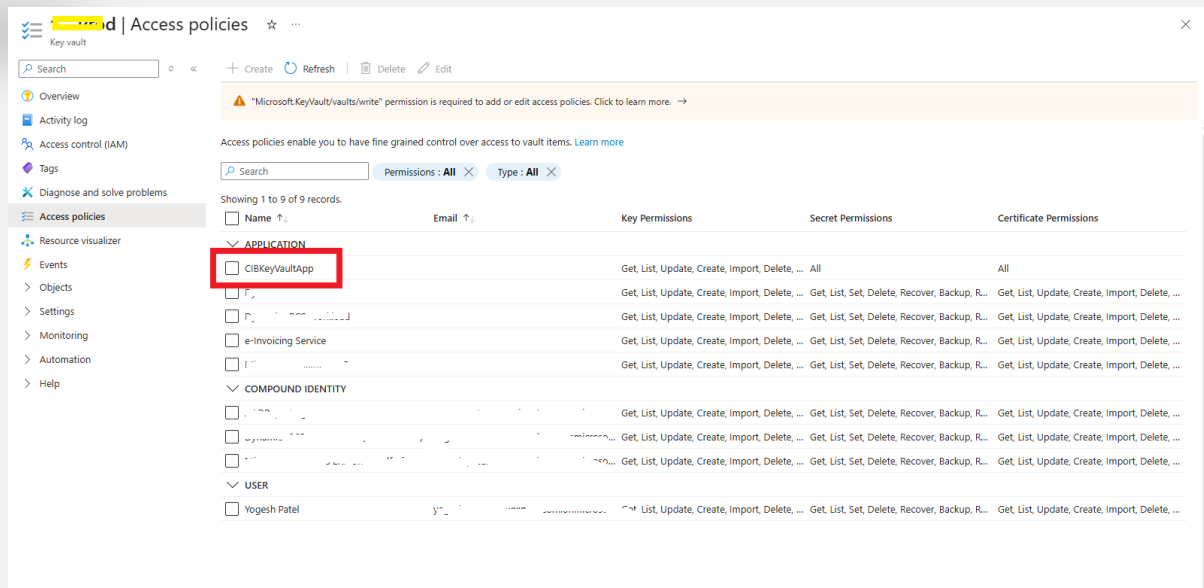
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions shows all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for

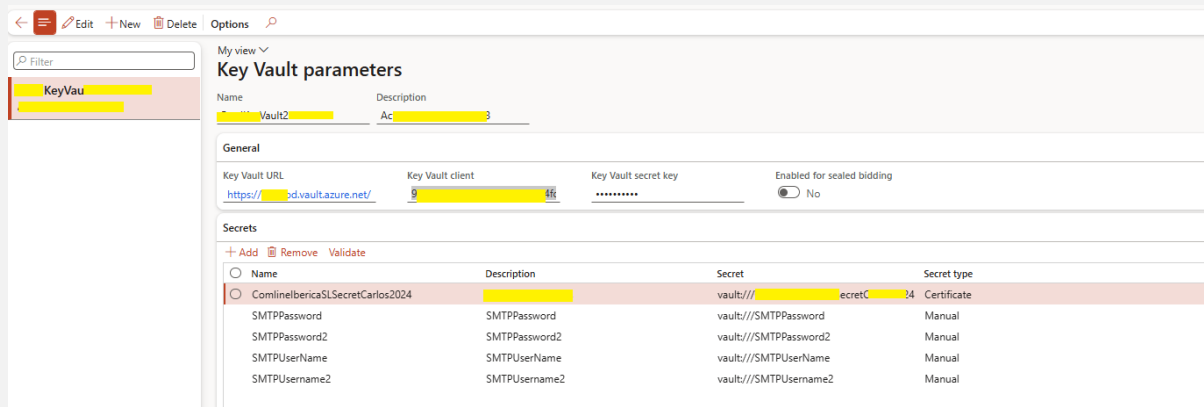
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

### 4. Give Key vault permission to the entra app



## ✓ Step 5: Complete Kay Vault Parameters in Dynamics



## ✓ Step 6: Storage of Invoice submission in Storage account

1. Each submitted documents are now automatically get stored under blob storage > container that is created above





Home > Storage accounts > ypestorageaccount | Containers >

**eiuatcontainer**  
Container

Search

+ Add Directory Upload Refresh Delete Copy Paste Rename Acquire lease Break lease Edit columns

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

Shared access tokens

Access policy

Properties

Metadata

eiuatcontainer > a01 > uat-01

Authentication method: Access key (Switch to Microsoft Entra user account)

Search blobs by prefix (case-sensitive)

Showing all 61 items

<input type="checkbox"/>	Name	Last modified	Access tier
<input type="checkbox"/>	[...]		
<input type="checkbox"/>	02a311c4-9abd-4423-b6ac-1af4f06c5c66.zip	29/06/2025, 02:35:44	Hot (Inferred)
<input type="checkbox"/>	1006bfd1-096f-462d-a296-e2716583697f.zip	30/07/2025, 18:53:13	Hot (Inferred)
<input type="checkbox"/>	2c79aa83-b5d1-407f-b494-ff50d002fc2e.zip	29/06/2025, 11:02:22	Hot (Inferred)
<input type="checkbox"/>	356647cb-ba43-4aa1-bee7-afae7831fc48.zip	29/06/2025, 01:56:26	Hot (Inferred)
<input type="checkbox"/>	3ef7212e-73d6-479b-af8-24852389f8a9.zip	14/07/2025, 18:06:37	Hot (Inferred)
<input type="checkbox"/>	5637144585.Generate invoice.OutputFile.60724a26-a825-4160-9d12-5bab23d7fd54.zip	28/06/2025, 23:27:37	Hot (Inferred)
<input type="checkbox"/>	5637144586.Generate invoice.OutputFile.bd5d375c-25c2-4d78-8d97-31dc50b64933.zip	28/06/2025, 23:38:28	Hot (Inferred)
<input type="checkbox"/>	5637144587.Generate invoice.OutputFile.d324fcd9-8bae-4580-8907-862e0b621158.zip	28/06/2025, 23:59:15	Hot (Inferred)
<input type="checkbox"/>	5637144588.Generate invoice.OutputFile.eef663d3-4c08-4b38-8b61-3927ec9b7ffa.zip	29/06/2025, 00:18:48	Hot (Inferred)
<input type="checkbox"/>	5637144589.Generate invoice.OutputFile.c76dc320-0224-4da0-9dd1-af2f9bf2610e.zip	29/06/2025, 01:19:00	Hot (Inferred)
<input type="checkbox"/>	5637144590.Generate invoice.OutputFile.cc4c5b65-cc0a-4fd6-8425-7ab64f42e469.zip	29/06/2025, 01:44:32	Hot (Inferred)
<input type="checkbox"/>	5637144591.Generate invoice.OutputFile.a0220b1a-f626-4859-b8a0-3713a2e4e0c0.zip	29/06/2025, 01:47:32	Hot (Inferred)
<input type="checkbox"/>	5637144593.Generate invoice.OutputFile.0d5cac2e-557f-4033-bc0a-99396a4c5576.zip	29/06/2025, 01:56:37	Hot (Inferred)
<input type="checkbox"/>	5637144594.Generate invoice.OutputFile.305038e7-62dc-41c4-8909-9803be7f329d.zip	29/06/2025, 02:05:03	Hot (Inferred)
<input type="checkbox"/>	5637144595.Generate invoice.OutputFile.e37add7e-9892-4ac6-9194-d17517100f75.zip	29/06/2025, 02:13:11	Hot (Inferred)
<input type="checkbox"/>	5637144596.Generate invoice.OutputFile.a6b2af2f-e64e-4893-bc1c-8181da869be7.zip	29/06/2025, 02:15:33	Hot (Inferred)

Add or remove favorites by pressing Ctrl+Shift+F

## High-Level: Alternative Storage in SharePoint

### Use Case:

- SharePoint offers a user-friendly way to **access and review submitted files**.

### High-Level Setup:

- Use **Power Automate** to monitor a folder in Azure Blob or OneDrive
- Trigger flow to:
  - Upload the document to SharePoint Document Library
  - Apply retention label (e.g., "Finance – 6 Year")
  - Tag with metadata (e.g., invoice number, date, entity)

✚ Use the same file naming structure to ensure consistency.

### Storage Option Best For

### Notes

#### Blob

Scalable, secure archival

Built into D365

#### SharePoint

End-user access, finance team review External setup via Power Automate

#### Dataverse

Structured logs with integration

Suitable for Power Platform workflows



## Include Metadata for Audits

Ensure every stored document includes:

- Invoice number
- Submission timestamp
- Legal entity & VAT registration
- Submission result (Success, Failed)
- Original vs. signed copy



You can store this as:

- File/folder name
- Separate metadata JSON file
- Entry in **Dataverse Submission History** entity



## Apply Retention Policies

Platform	Method	Example
Azure Blob	Lifecycle Management Policy	Delete after 7 years
SharePoint	Retention Labels + Policies	Retain 6 years post-create
Power Automate	Flag or move archived documents	Monthly or yearly review



## Country-Specific Archival Rules

### Country Retention Requirement

Spain	6 years	Facturae signed XML + FACe Response
UK	6 years	HMRC VAT, customs, declarations
Italy	10 years	Signed FatturaPA + timestamps
Germany	10 years	Must be electronically accessible



## Related Articles

- [GS506 – Processing Pipelines](#)
- [GS514 – Output Storage](#)
- [GS517 – Logs and Errors](#)


---


## You've Reached the End of the GS500 Series

This concludes the **Globalization Studio GS500 Series**, a comprehensive journey covering every major component of compliance automation within Dynamics 365 Finance & Supply Chain.

By now, you've learned how to:

- Design, deploy, and manage localization features
- Automate document formatting, submission, and validation
- Integrate with Power Platform and Azure
- Handle versioning, exceptions, and audits—all without custom code

 Whether you're an architect, functional consultant, or compliance manager, this series equips you with the skills to implement Globalization Studio confidently and effectively.

 Feel free to revisit specific articles:

- Need a refresher on pipeline execution? See [GS506](#)
- Want to automate document flows? Jump to [GS514](#)
- Looking for version control guidance? Review [GS522](#)