







GS515 – Digital Signatures and Key Vault Integration in Globalization Studio

Digital signatures are a key part of global compliance. Whether you're submitting invoice XMLs to a government platform or protecting PDF layouts from tampering, a digital signature proves:

-  The document was sent by your company
-  The content hasn't been changed after generation
-  The file meets government or customer legal requirements

In this article, we'll explore:

- What a digital signature is and how it works
- How signing is handled in **Electronic Invoicing** features
- How it differs from digital handling in **Spain's SII (MTD)**
- How to configure **Azure Key Vault** for digital signing in Dynamics 365
- Tips for managing certificates across regions

 Builds on previous articles:

[GS506 – Pipelines](#), [GS510 – Feature Reuse](#), and [GS514 – Document Routing](#)

What Is a Digital Signature?

A **digital signature** is a cryptographic seal applied to an electronic document to prove its authenticity and integrity. It's generated using a certificate file (usually .pfx) issued by a trusted certification authority like FNMT, Camerfirma, or GlobalSign.


Once a document is signed:


- It is cryptographically locked
 - Any tampering or changes invalidate the signature
 - Government or business receivers can verify the sender identity
-



Where Digital Signatures Are Used in Globalization Studio

Scenario	Framework	Signing Location	Signature Required?
Spain – Facturae (e-invoice XML)	Globalization Studio	Inside XML payload	✓ Required
Italy – FatturaPA	Globalization Studio	Embedded XML signature	✓ Required
Saudi Arabia – Phase 2 e-invoice	Globalization Studio	XML/QR Code	✓ Required
France – Invoice compliance (optional)	Globalization Studio	Embedded XML or PDF signature	Optional
Spain – SII / MTD	Electronic Messaging	Applied at HTTP transport level	✓ Required

 In Globalization Studio, digital signatures are configured in **pipeline steps** using certificates stored in **Azure Key Vault**.

 For Spain's **SII (MTD)**, signing is handled at the **transport level** using the Electronic Messaging framework, not in the XML content, and not via Globalization Studio pipelines.

Real-World Use Case: Signing a Facturae XML

Your Spanish entity uses the **Spanish electronic invoice (ES)** feature to submit Facturae XMLs to the FACe portal.

△ Microsoft does not provide out-of-box web service submission for Spain. This pipeline exports and signs XML for external submission.

After **signing**, the file can be:

- Sent to **Azure Blob or SharePoint** for archiving or external pickup
- Posted to **Azure Logic App** to connect with a government-approved intermediary (ISV or FACe)
- Processed offline and manually submitted via Spain's **FACe portal**

Here's what the Globalization Studio pipeline looks like:



1. Configure Feature Pipeline → ER format creates the Facturae XML

V3_Spanish electronic invoice (ES) 13 : Sales invoice gen... | Standard view

Feature version setup

Processing pipeline

Set up actions and parameters

This step transforms invoice data into the Facturae 3.2.1 XML format using the ER configuration (Sales invoice (ES) format). It outputs the raw, unsigned XML file.

Sends the digitally signed XML as an attachment to an external recipient Outlook (for webservice e.g. tax consultant, third-party platform, or internal archive). The input file must be mapped to the output from the signature step.

This step applies an X.509 digital signature to the XML generated in the previous step using a certificate stored in Azure Key Vault. It is mandatory for Spain's e-invoice submission.

Action	Action name	Description	Enable retry	Retry action	Export result	Update action
Transform document	Generate invoice	Action to generate Sales invoice electronic format				
Sign xml document	Sign xml document (3)	Digital Signature Action			✓	
Send an Email	Send an Email (2)	Send an xml file via email				

Parameters	Description	Value
Configuration	Configuration describes format which will be executed	Sales invoice (ES) derived (3): Sales invoice (ES) derived (3)
Custom file name	Custom file name from the client	
Direction	Direction describes which format will be used: import or export	export
Input file	Source file provides to the action the data to be executed.	Variable: BusinessDocumentDataModel
Configuration integration point	Source file provides a data to the reporting runtime	InvoiceCustomer

Configuration user input parameters	Name	Data type	Value
User input parameter	Country	string	

2. Sign document Step → XML is signed using a Key Vault certificate

Feature version setup

Processing pipeline

Set up actions and parameters

Action	Action name	Description	Enable retry	Retry action	Export result	Update action
Transform document	Generate invoice	Action to generate Sales invoice electronic format				
Sign xml document	Sign xml document (3)	Digital Signature Action			✓	
Send an Email	Send an Email (2)	Send an xml file via email				

Parameters	Description	Value
Input file	Input xml file with document that need to be signed with electronic signature	Generate invoice Output file
Certificate name	Name of certificate in storage	CertificateName
Signature type	Type of signature to use	RSA
Signature method name	Name of signature method which used to generate electronic signature	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Digest method name	Digest method which used to generate digest string in digital signature	http://www.w3.org/2001/04/xmldsig-more#sha256
Canonicalization method name	Canonicalization method used to calculate signature hash	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Reference attribute name	Attribute name to where insert reference id in signature element	
Name of element to sign	Specifies name of xml element inside document which need to be signed with electronic si...	Facturae
Name of element to insert signature	Name of xml element to where we need to insert generated digital signature. If not specific...	Signature
Xslt file with digest transform	Xslt file with rules of digest transformation rules to generate digest string for electronic sig...	
Path to insert digest string	Specifies path in <elementName>.<AttributePath> format to locate where generated dige...	

3. Process Invoice → Submit Electronic Document and check processing log



SC0342 : 6/28/2025 12:00:00 AM | Standard view ▾

Submission details

Created date and time Execution state
14/07/2025 17:49:48 Completed

Processing actions

Created date and time	Action result state	Action name	
14/07/2025 17:49:59	Completed	Generate invoice	
14/07/2025 17:50:01	Completed	Sign xml document (3)	
14/07/2025 17:50:02	Completed	Send an Email (2)	

Action files

View

Action parameter Id	
OutputFile	
ERFileName	

Processing action log

UTC timestamp	Message code	Message	Log level
We didn't find anything to show here.			

4. Exported result

YP Test - please ignore



Summary by Copilot



Comline Documents

To: ● Yogesh Patel



output.xml
5 KB



Reply



Forward

5. Verify XML file digitally signed



```
<TotalPaymentsOnAccount>0.00</TotalPaymentsOnAccount>
<TotalExecutableAmount>[REDACTED]</TotalExecutableAmount>
</InvoiceTotals>
<Items>
  <InvoiceLine>
    <ItemDescription>Brake Pad [REDACTED] 716</ItemDescription>
    <Quantity>1.0</Quantity>
    <UnitOfMeasure>EA</UnitOfMeasure>
    <UnitPriceWithoutTax>[REDACTED] 200</UnitPriceWithoutTax>
    <TotalCost>[REDACTED] 0</TotalCost>
    <GrossAmount>[REDACTED] 3</GrossAmount>
    <TaxesOutputs>
      <Tax>
        <TaxTypeCode/>
        <TaxRate>[REDACTED] 0</TaxRate>
        <TaxableBase>
          <TotalAmount>[REDACTED] 3</TotalAmount>
        </TaxableBase>
        <TaxAmount>
          <TotalAmount>[REDACTED] 2</TotalAmount>
        </TaxAmount>
      </Tax>
    </TaxesOutputs>
  </InvoiceLine>
</Items>
</Invoice>
</Invoices>
<Signature>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"/>
      <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <Transform Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2001/04/xm1enc#sha256"/>
        <DigestValue>[REDACTED] zw1uqa/s=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>[REDACTED] /4H3BLVt1cxn8bwaJRUCpw
  </SignatureValue>
  <KeyInfo>
    <X509Certificate>[REDACTED] yZXN1bnRhY2ZnO2s24wfhct1tji
    </X509Certificate>
    </X509Certificate>
    </KeyInfo>
  </Signature>
</Facturae>
```


Digital Signature Included in XML
File

Step-by-Step: How to Set Up Digital Signing

☒ Step 1: Obtain a Valid Certificate

You'll need a .pfx certificate file issued by a trusted provider. It should:

- Be issued to your legal entity
- Support electronic signing
- Include a private key

Name	Type	Size
 Electronic Signature	Personal Information Exchange	

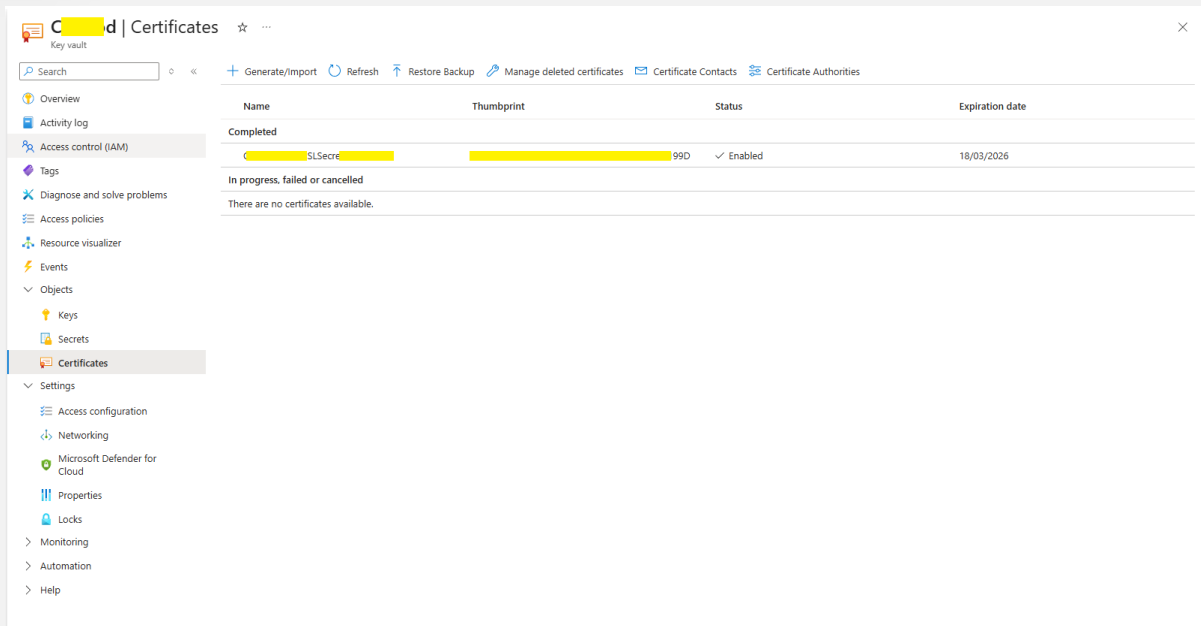
☒ Step 2: Import the Certificate to Azure Key Vault

In Azure:

1. Open your **Key Vault**
2. Go to **Certificates > Import**
3. Upload the .pfx file
4. Name it clearly (e.g., FacturaeCert2025)



5. Add an **access policy** to allow Dynamics 365 access using your Azure AD app registration



☒ Step 3: Register Key Vault in Dynamics 365

In D365:

- 1.
2. Go to **Globalization Studio > Electronic document parameters > Electronic Invoicing**
3. Open the **Key Vault Parameter** under Key Vault Settings, Add your details



https://businessdocumentsubmission.operations365.dynamics... | Standard view ▾

Key Vault parameters

Name	Description	Key Vault URI
EInv	EInv	https://[redacted].vault.azure.net/

Certificates

+ Add - Delete

<input type="radio"/>	<input type="radio"/>	Name	Description	Type
<input checked="" type="radio"/>	<input type="radio"/>	EInv	EInv	Secret ▾
<input type="radio"/>	<input type="radio"/>	SMTPPassword	SMTPPassword	Secret
<input type="radio"/>	<input type="radio"/>	SMTPUserName	SMTPUserName	Secret

Standard view ▾

Electronic document parameters

Electronic document	Electronic Invoicing
Features	
Electronic Invoicing	
Integration channels	

Service parameters

Endpoint URL: https://[redacted]109.g... Environment: [redacted]-01

Key Vault settings

Key Vault parameters

Key Vault: EInv SAS token secret: EInv

Number sequences

+ New - Delete

Name	Description	InUse	Current Value
------	-------------	-------	---------------

This is the integration gateway URL for the Microsoft-hosted Electronic Invoicing (EI) service. It routes the pipeline steps to the correct EI environment. The URL is automatically generated and cannot be changed manually.

This identifies your connected EI environment. It represents the environment where your electronic invoicing features are deployed and executed. This is also used by Dataverse for feature version deployment. Make sure you copy/paste environment name from PP admin center

Specifies the Azure Key Vault resource (previously set up in Azure and authorized) where the digital certificates for XML signing are stored. This must match the name of the Key Vault linked to your EI feature.

Refers to the secret name in Azure Key Vault that stores the SAS token to securely access documents stored in Azure Blob storage.

4. Test the connection to confirm access



Synchronisation with the e-invoicing service was successful

Save Options

Standard view

Electronic document parameters

Electronic document

Features

Electronic Invoicing

Integration channels

Electronic Invoicing

Service parameters

Endpoint URL: Environment:

Key Vault settings

Key Vault parameters

Key Vault: SAS token secret:

Number sequences

+ New Delete

Name	Description	InUse	Current Value
------	-------------	-------	---------------

We didn't find anything to show here.

Remember you provide e-invoice service access to key vault

Home > CIBProd

Access policies

Search

Create Refresh Delete Edit

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Access policies

Resource visualizer

Events

Objects

Keys

Secrets

Certificates

Settings

Monitoring

Automation

Help

Access policies enable you to have fine-grained control over access to vault items. [Learn more](#)

Showing 1 to 9 of 9 records.

Name	Email	Key Permissions
APPLICATION		
[redacted]		Get, List, Update, C
[redacted]		Get, List, Update, C
[redacted]		Get, List, Update, C
[redacted]		Get, List, Update, C
e-Invoicing Service		Get, List, Update, C
COMPOUND IDENTITY		
USER		

Review changes to e-Invoicing Service

Permissions Review + save

Key Permissions

Key Management Operations	All selected
Cryptographic Operations	None selected
Privileged Key Operations	None selected
Rotation Policy Operations	All selected

Secret Permissions

Secret Management Operations	All selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	All selected
Privileged Certificate Operations	None selected

Principal

Principal name: e-Invoicing Service

Object ID: [redacted]

Application

Authorized application: None selected

Object ID: None selected

Previous Save

Step 4: Add a "Sign Document" Step in the Pipeline

Inside the **electronic invoice feature** (e.g., Spanish electronic invoice):

1. Open the **Feature Setup > Processing Pipeline**
2. Add a new action of type **Sign document**
3. Configure:
 - **Input file:** Output from previous ER format step



- **Certificate name:** From Key Vault (e.g., FacturaeCert2025)
- **Signature type:** XmlDsig
- **Digest method:** sha256
- **Canonicalization:** c14n

Every time the pipeline runs, the invoice XML is signed before it is exported

Feature version setup

Processing pipeline

Set up actions and parameters

Processing pipeline

Action	Action name	Description	Enable retry	Retry action	Export result	Update action
Transform document	Generate invoice	Action to generate Sales invoice electronic format				
Sign xml document (3)	Sign xml document (3)	Digital Signature Action				✓
Send an Email	Send an Email (2)	Send an xml file via email				

Parameters

Name	Description	Value
Input file	Input xml file with document that need to be signed with electronic signature	Generate invoice: Output file
Certificate name	Name of certificate in storage	FacturaeCert2025
Signature type	Type of signature to use	XML
Signature method name	Name of signature method which used to generate electronic signature	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Digest method name	Digest method which used to generate digest string in digital signature	http://www.w3.org/2001/04/xmldsig-more#sha256
Canonicalization method name	Canonicalization method used to calculate signature hash	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Reference attribute name	Attribute name to where insert reference id in signature element	
Name of element to sign	Specifies name of xml element inside document which need to be signed with electronic si...	Facturae
Name of element to insert signature	Name of xml element to where we need to insert generated digital signature. If not specific...	Signature
Xslt file with digest transform	Xslt file with rules of digest transformation rules to generate digest string for electronic sig...	
Path to insert digest string	Specifies path in <elementName> <AttributePath> format to locate where generated dige...	

📍 Where to View Signed Output

Location

What You'll See

**Electronic messages >
Attachments**

The signed XML (with <ds:Signature> block)

Submission logs

Confirmation of signing success/failure

**Outlook or Azure Blob or
SharePoint (if configured)**

Archived signed files by adding step in pipeline (**Azure File
share, Save file to sharepoint**)



SC0342 : 6/28/2025 12:00:00 AM | Standard view

Submission details

Created date and time: 14/07/2025 17:49:48 | Execution state: Completed

Processing actions

Created date and time	Action result state	Action name
14/07/2025 17:49:59	Completed	Generate invoice
14/07/2025 17:50:01	Completed	Sign xml document (3)
14/07/2025 17:50:02	Completed	Send an Email (2)

Action files

View

Action parameter Id
OutputFile
ERFileName

Processing action log

UTC timestamp	Message code	Message	Log level
We didn't find anything to show here.			

🔗 How This Differs from Spain's SII (MTD) Signing

Spain's SII does not sign the XML itself. Instead:

- The **electronic message transport layer** uses a certificate to sign the HTTP request
- The signing logic is configured in the **Send message action** within **Electronic message processing setup**
- No signature appears in the payload XML
- You do not use Electronic Document Parameters or Globalization Studio pipelines for SII

■ For full SII setup, see [GS518 – Electronic Messaging for SII](#)

💡 Tips for Managing Digital Certificates

Tip

Name certificates clearly

Use separate certs per country

Why It Helps

Easier to reference in multiple environments

Simplifies compliance and audit readiness



Tip

Rotate certificates early

Always test with a dummy cert in UAT

Why It Helps

Avoid failed submissions due to expiry

Avoids blocking production workflows



Summary

Digital signatures in Globalization Studio help ensure your invoice or document is:

- Authenticated
- Legally valid
- Protected from tampering

For **Electronic Invoicing features**, signing is managed through the pipeline and Azure Key Vault.

For **SII (MTD)** and similar integrations, signing is handled at the **message transport level** through Electronic Messaging.



Related Articles in This Series

- [GS507 – Electronic Invoicing Overview](#)
- [GS510 – Reusing and Adapting Microsoft Features](#)
- [GS514 – Document Routing and Storage](#)
- [GS516 – Connecting to Government APIs](#)



Coming Up Next

In [GS516 – Connecting to Government Portals](#), you'll learn:

- How to configure submission steps to web service endpoints like FAcE or SDI
- How retry logic, responses, and error handling work
- How to use Microsoft's prebuilt integration templates



[Continue to [GS516 → Government Web Service Submission](#) →]