PKI Complete Migration testing (for G3)

Testing Environment Description

Status: FINAL - Version: 1.2
Last updated: 19.11.2025

OpenPeppol AISBL
Rond-point Schuman 6, box 5
1040 Brussels Belgium

info@peppol.eu
www.peppol.org
Last updated: 19.11.2025

Table of Contents

1 Introduction

This document provides information related to the Peppol's Testbed PKI migration testing. It provides a high-level overview of the test suite, including its prerequisites and description of the test cases included. This document's intended audience is Service Providers (SPs) who wish to validate their AP implementations during the migration from G2 AP certificates to G3 AP certificates, ensuring compatibility with both the current (G2 legacy) and upcoming (G3 new) Peppol PKI infrastructure.

1.1 Glossary

Note: In this document, "G2" refers to the legacy generation of the Peppol PKI, and "G3" refers to the next generation of the Peppol PKI.

Abbreviations used in this document:

Abbreviation	Meaning
AP	Access Point
C2	Corner 2, sending AP
C3	Corner 3, receiving AP
CA	Certificate Authority
G2	Refers to the legacy generation of the Peppol PKI
G3	Refers to the next generation of the Peppol PKI
PKI	Public Key Infrastructure
SBD	Standard Business Document
SMK	Test instance of the SML
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SP	Service Provider
SUT	System Under Test
UI	User Interface

Table 1 glossary

2 Prerequisites

SPs must meet the following requirements before doing any testing.

2.1 Peppol PKI AP Certificate

SPs are authenticated to the Peppol Testbed using PKI client authentication. As a result, the SPs must obtain a Peppol PKI AP test certificate (G2 or G3) and import it into their browser's keystore.

2.2 Access Point deployment

SPs must have a Peppol AP deployed, as a result they need the following:

- An AS4 URL available – must refer to HTTPS.
- The AP must be accessible over the Internet.
- The AP must implement HTTPS with certificate chains to Certificate Authorities (CAs) which are trusted by Peppol.
- The AP must have installed the same Peppol PKI AP test certificate used for the authentication to the Testbed. This means that
    - if you authenticated to the Testbed with a G2 certificate your AP must also be operated with a G2 certificate
    - if you authenticated to the Testbed with a G3 certificate your AP must also be operated with a G3 certificate
- Participant identifiers intended for message reception during testing must be correctly registered in a Peppol SMP.

3 PKI Migration Testing

The Testbed offers three PKI Migration testing options:

- **PKI Reception Migration** test suite, which verifies that an SP can receive messages from both the legacy (G2) and new (G3) PKIs while still operating with a G2 certificate.
- **PKI Submission Migration** test suite**,** which verifies that an SP can send messages using a G3 certificate.
- **PKI Complete Migration** test suite, which includes reception and submission test cases designed to support the full migration to operating with a G3 certificate.

All three test suites are available in the Testbed. To execute a given test suite, the tester must log in with the corresponding certificate: **G2** for the PKI Reception Migration suite and **G3** for the PKI Complete Migration and PKI Submission Migration test suites.

The following sections describe in detail the test cases included in the **PKI Complete Migration test suite.**

- For information about the **PKI Reception Migration (for G2)** test suite, refer to the document "*PKI Reception Migration Environment Description for G2"*.
- For information about the **PKI Submission Migration (for G3)** test suite, refer to the document "*PKI Submission Migration Environment Description for G3"*.

In all test cases, there is a test participant created by the testing person and used during testing by the SP system (SUT) for which the PKI Migration test suite is enrolled. In addition, the testing person is responsible for:

- Preparing the test participant to be used by the test suite
- Enrolling the test participant to the test suite
- Selecting the test cases to be executed and
- Reading and interpreting the validation results

This applies to all following test cases and will not be restated in each one to avoid repetition and increase readability.

3.1 PKI Complete Migration Test Suite (for G3)

The **PKI Complete Migration** test suite is intended for SPs whose AP implementations are fully configured with a G3 certificate. Its purpose is to verify that the SP's AP can successfully send and receive BIS Billing 3.0 compliant documents while communicating with other APs that may still use G2 certificates or have already moved to G3, depending on the stage of the PKI migration plan.

The following test cases are included:

- G2 - Valid certificate message reception
- G2 - Invalid certificate message reception
- G3 - Valid certificate message reception
- G3 - Invalid certificate message reception
- G3 message submission with G2 SignalMessage reception
- G3 message submission with G3 SignalMessage reception

3.1.1 G2 - Valid certificate message reception

This test case verifies the SP's ability to operate as a receiving (C3) AP in compliance with the Peppol Network specifications when the sender uses a valid G2 certificate to sign the UserMessage. **This test case requires participant addressing information to be correctly registered in a Peppol SMP, as a precondition.**

The test evaluates the following capabilities:

- **Receiving** a BIS Billing 3.0 Invoice from a sender (C2 simulated by the Testbed) that uses a valid G2 certificate for signing the UserMessage via the Peppol Network.
- **Replying** to the Testbed AP (C2) with a corresponding SignalMessage (AS4 receipt), signed with a G3 certificate.

Test Flow Steps (C2 → C3 (SUT))

The steps for executing the test case are as follows, as indicated in Figure 1. Consider that an end user of the SUT AP (C3) has already selected the test case and started its execution. These interactions are omitted for brevity reasons.

1. **Document generation and submission**

   The Testbed AP (C2):

   - Generates a valid BIS Billing 3.0 Invoice.
   - Performs SMK/SMP lookup to discover the SUT AP's BIS Billing 3.0 Invoice receiving capability. Verify that a valid G3 certificate is used.
   - Submits the SBD Peppol AS4 to the SUT AP (C3), while signing the UserMessage with a valid G2 certificate. The payload is encrypted using the SUT AP participant's G3 certificate.

2. **BIS Billing 3.0 Invoice Processing**

   The SUT AP (C3) receives the Invoice and prepares an appropriate SignalMessage response signed with a G3 certificate

3. **Result handling**

   The Testbed AP receives and processes the SignalMessage from the SUT AP (C3)

   The Testbed UI displays:

   - Transaction trace and overall test result (pass, fail)

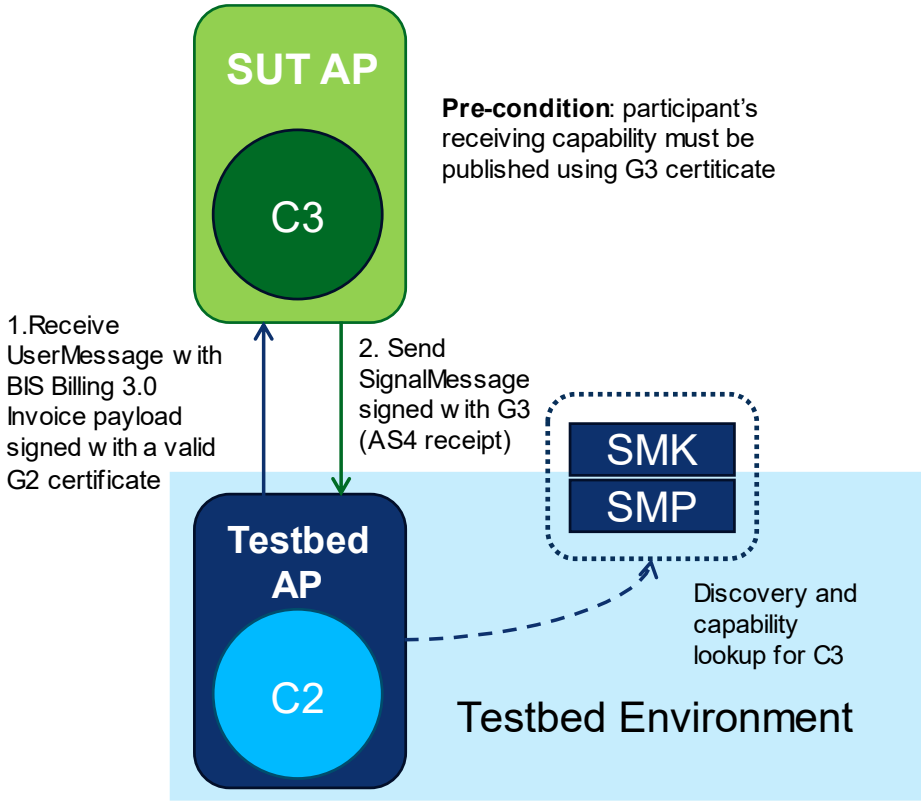

Figure 1 G2 - Valid certificate Message reception test case (Step 3 is omitted for brevity reasons)

A summary of the test case execution flow is provided in Table 2.

Step	Actor	Message Type	Action	Purpose
1	Testbed AP (C2)	BIS Billing 3.0 Invoice (G2 signed)	Generate and submit BIS Billing 3.0 Invoice to SUT AP (C3) signed with valid C2 certificate and encrypted with G3 certificate	Simulate sending of Invoice to the receiving AP
2	SUT AP (C3)	SignalMessage (AS4 Receipt – G3 signed)	Send back SignalMessage, signed with G3 certificate	Confirm successful receipt
3	Testbed	-	Process SignalMessage and display results to end user	Show test case outcome (fail/pass)

Table 2 Summary of reception testing flow

Success Criteria

To pass the test, the SP must:

- Receive and process a UserMessage with a BIS Billing 3.0 Invoice payload that has been signed with a **valid G2 certificate**. The proper SMP registration with a G3 certificate must be in place.
- Submit the corresponding SignalMessage (AS4 Receipt), signed with a valid G3 certificate, back to the Testbed AP (C2), accepting the transaction.

3.1.2 G2 - Invalid certificate Message reception

This test case verifies the SP's ability to operate as a receiving (C3) AP in compliance with the Peppol Network specifications when the sender uses an invalid (revoked) G2 certificate to sign the UserMessage. **This test case requires participant addressing information to be correctly registered in a Peppol SMP, as a precondition.**

The test evaluates the following capabilities:

- **Receiving** a BIS Billing 3.0 Invoice from a sender (C2 simulated by the Testbed) that uses an invalid G2 certificate for signing the UserMessage via the Peppol Network.
- **Replying** to the Testbed AP (C2) with a corresponding AS4 error message, signed with a G3 certificate.

Test Flow Steps (C2 → C3 (SUT))

The execution test flow steps are the same as in the first reception test case (see section 3.1.1), except that this time the Testbed AP (C2) signs the UserMessage with an invalid G2 certificate. The SUT AP (C3) must reject the transaction and return the corresponding AS4 error message.

Figure 2 illustrates the reception flow for the current test case.

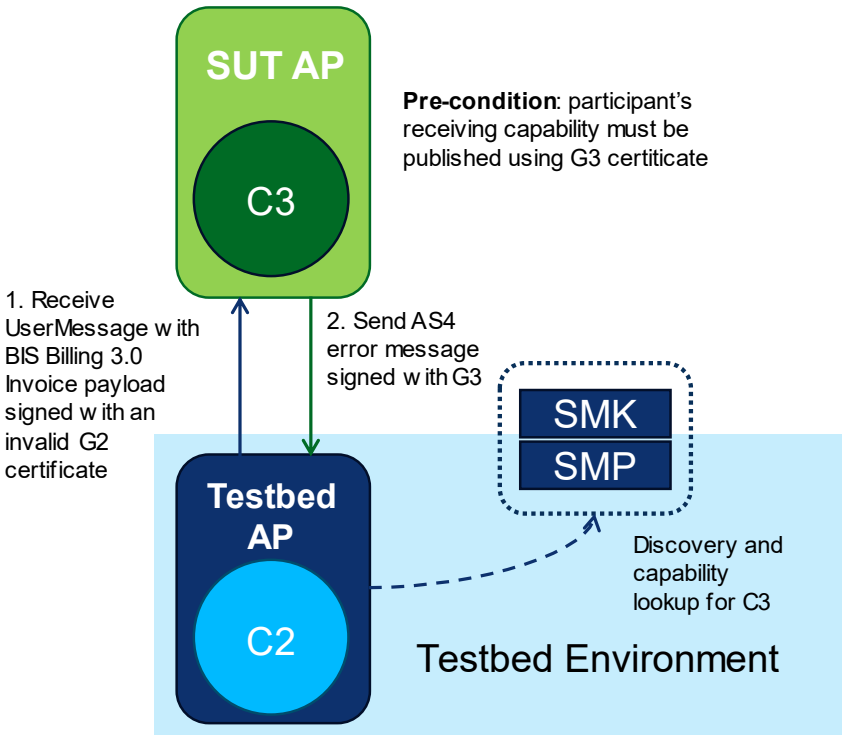

Figure 2 G2 - Invalid certificate Message reception test case (step 3 is omitted for brevity reasons)

Success Criteria

To pass the test, the SP must:

- Receive and process a UserMessage with a BIS Billing 3.0 Invoice payload that has been signed with an **invalid (revoked) G2 certificate**. The proper SMP registration with a G3 certificate must be in place.
- Reject the transaction and submit the corresponding SignalMessage (AS4 Error), signed with a valid G3 certificate, back to the Testbed AP (C2).

3.1.3 G3 - Valid certificate Message reception

This test case verifies the SP's ability to operate as a receiving (C3) AP in compliance with the Peppol Network specifications when the sender uses a valid G3 certificate to sign the UserMessage. **This test case requires participant addressing information to be correctly registered in a Peppol SMP, as a precondition.**

The test evaluates the following capabilities:

- **Receiving** a BIS Billing 3.0 Invoice from a sender (C2 simulated by the Testbed) that uses a valid G3 certificate for signing the UserMessage, via the Peppol Network.
- **Replying** to the Testbed AP with a corresponding SignalMessage (AS4 receipt), signed with a G3 certificate.

Test Flow Steps (C2 → C3 (SUT))

The execution test flow steps are the same as the first reception test case (see section 3.1.1), but this time the Testbed AP uses a valid G3 certificate to sign the UserMessage that is sent to the SUT AP (C3).

Figure 3 illustrates the reception flow for the current test case.

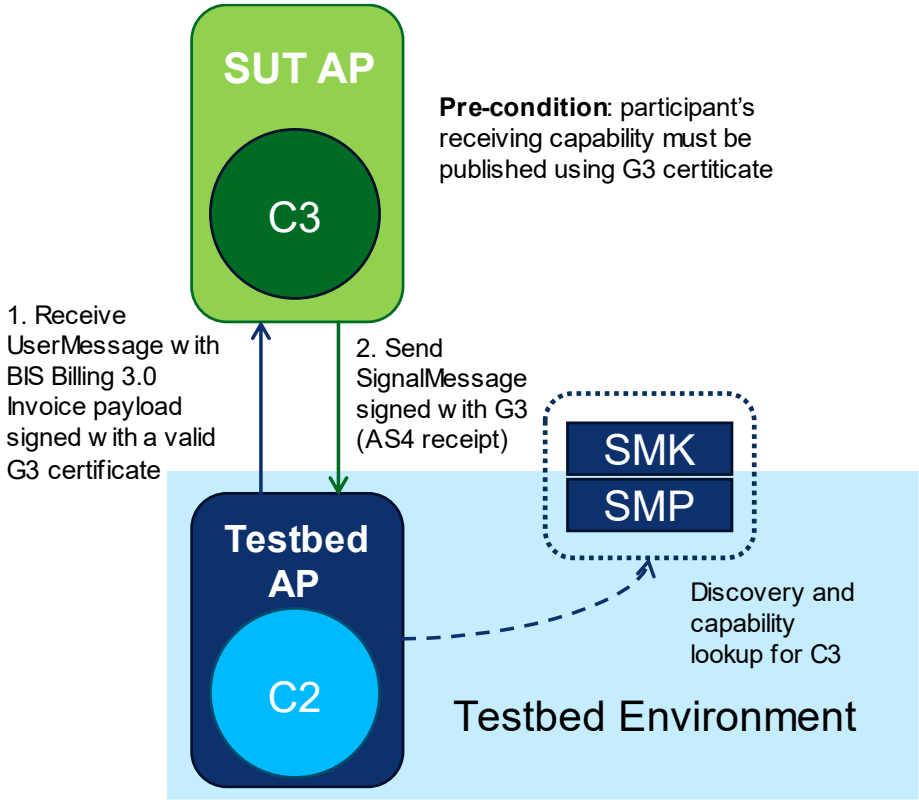

Figure 3 G3 - Valid certificate Message reception test case (step 3 ommited for brevity reasons)

Success Criteria

To pass the test, the SP must:

- Receive and process a UserMessage with a BIS Billing 3.0 Invoice payload that has been signed with a **valid G3 certificate**. The proper SMP registration with a G3 certificate must be in place.
- Submit the corresponding SignalMessage (AS4 Receipt), signed with a valid G3 certificate, back to the Testbed AP (C2), accepting the transaction.

3.1.4 G3 - Invalid certificate Message reception

This test case verifies the SP's ability to operate as a receiving (C3) AP in compliance with the Peppol Network specifications when the sender uses an invalid (revoked) G3 certificate to sign the UserMessage. **This test case requires participant addressing information to be correctly registered in a Peppol SMP, as a precondition.**

The test evaluates the following capabilities:

- **Receiving** a BIS Billing 3.0 Invoice from a sender (C2 simulated by the Testbed) that uses an invalid G3 certificate for signing the UserMessage, via the Peppol Network.
- **Replying** to the Testbed AP (C2) with a corresponding AS4 error message, signed with a G3 certificate.

Test Flow Steps (C2 → C3 (SUT))

The execution test flow steps are the same as the first reception test case (see section 3.1.1), except that this time the Testbed AP signs the UserMessage with an invalid G3 certificate. The SUT AP (C3) must reject the transaction and return the corresponding AS4 error message.

Figure 4 illustrates the reception flow for the current test case.

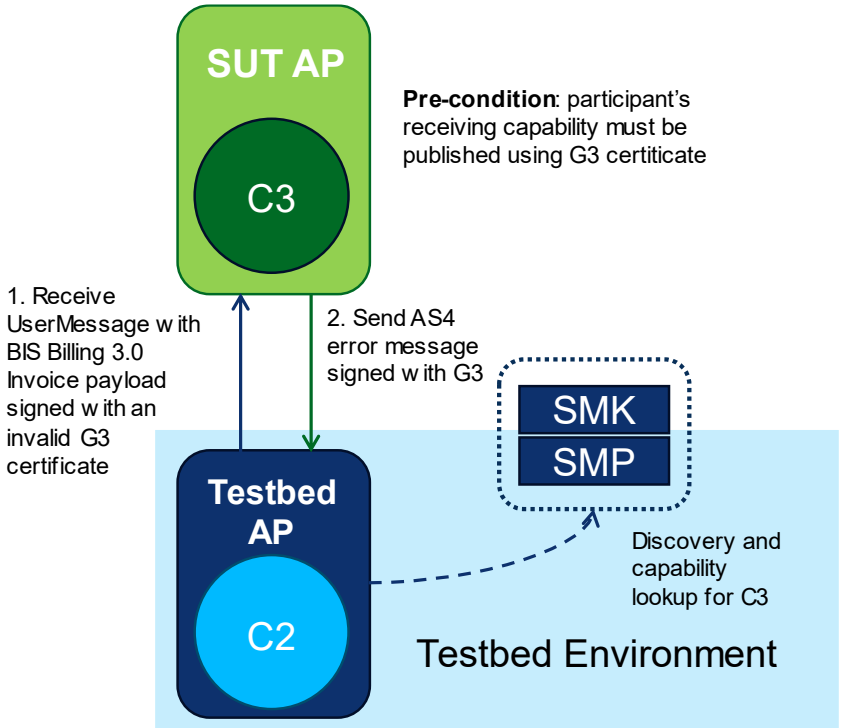

Figure 4 G3 - Invalid certificate message reception test case (step 3 omitted for brevity reasons)

Success Criteria

To pass the test, the SP must:

- Receive and process a UserMessage with a BIS Billing 3.0 Invoice payload that has been signed with an **invalid (revoked) G3 certificate**. The proper SMP registration with a G3 certificate must be in place.
- Reject the transaction and submit the corresponding SignalMessage (AS4 Error), signed with a valid G3 certificate, back to the Testbed AP (C2).

3.1.5 G3 message submission with G2 SignalMessage reception

This test case verifies the SP's ability to operate as a sending (C2) AP in compliance with the Peppol Network specifications when the receiver AP is configured with a valid G2 certificate.

The test evaluates the following capabilities:

- **Submitting** a BIS Billing Invoice 3.0 to a receiver (C3 simulated by the Testbed) that is configured with a valid G2 certificate via the Peppol Network.
- **Receiving** from the Testbed AP (C3) a SignalMessage (AS4 Receipt), signed with a G2 certificate.

To facilitate testing, the Testbed provides pre-built SBD file containing a BIS Billing 3.0 Invoice. The file is ready for immediate submission by the SUT AP (C2).

Test Flow Steps (C2 (SUT) → C3)

The steps for executing the test case are as follows, as indicated in Figure 5.

1. **Test Data Preparation**

   The Testbed environment:

   - Prepares a valid ready to be sent BIS Billing 3.0 Invoice for the tester to download and use during testing

2. **BIS Billing 3.0 Invoice submission**

   The SUT AP (C2) performs SMK/SMP lookups to discover:

   - Testbed AP's BIS Billing 3.0 Invoice recipient metadata

   And retrieves AS4 endpoint metadata for:

   - Testbed AP (C3)

   The SUT AP (C2), using Peppol AS4, submits:

   - The prepared invoice to the Testbed AP (C3)

3. **Receive AS4 receipt signed with G2 certificate**

   The Testbed AP (C3) validates that the received document is the expected and sends back to the SUT AP (C2) a SignalMessage signed with G2 certificate. The SUT AP (C2) receives the SignalMessage.

4. **Result handling**

   The Testbed UI displays:

   - Transaction trace and overall test result (pass, fail)

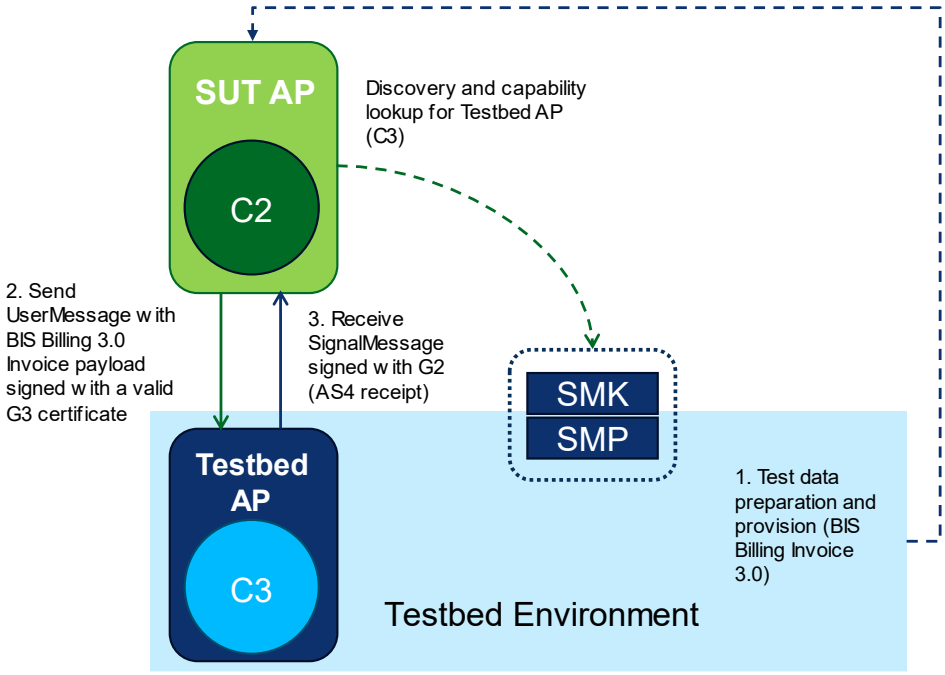

Figure 5 G3 message submission with G2 SignalMessage reception test case (step 4 is omitted for brevity reasons)

A summary of the test case execution flow is provided in Table 3.

Step	Actor	Message Type	Action	Purpose
1	Testbed	BIS Billing 3.0 Invoice	Prepare SBD with BIS Billing 3.0 Invoice payload	Prepare ready-to-be sent document by the SUT AP
2	SUT AP (C2)	BIS Billing 3.0 Invoice (G3 signed)	Submit BIS Billing 3.0 Invoice to Testbed AP (C3)	Send the UserMessage signed with G3 certificate
3	Testbed AP (C3)	SignalMessage (G2 signed)	Return SignalMessage signed with a valid G2 certificate back to SUT AP (C2)	Return message receipt and test interoperability with G2 certificate parties
4	Testbed	-	Display results to end users	show test case execution outcome (pass/fail)

Table 3 Summary of submission testing flow

Success Criteria

To pass the test, the SP must:

- Correctly identify recipient participant (C3) via SMK/SMP dynamic discovery and retrieve their endpoint metadata.
- Send the prepared BIS Billing 3.0 Invoice, signed with a valid G3 certificate.
- Receive the corresponding SignalMessage (AS4 Receipt) from the Testbed AP (C3), signed with a valid G2 certificate, to test interoperability with parties using G2 certificates.

3.1.6 G3 Message submission with G3 SignalMessage reception

This test case verifies the SP's ability to operate as a sending (C2) AP in compliance with the Peppol Network specifications when the receiver AP is configured with a valid G3 certificate.

The test evaluates the following capabilities:

- **Submitting** a BIS Billing Invoice 3.0 to a receiver (C3 simulated by the Testbed) that is configured with a valid G3 certificate via the Peppol Network.
- **Receiving** from the Testbed AP (C3) a SignalMessage (AS4 Receipt), signed with a G3 certificate.

Test Flow Steps (C2 (SUT) → C3)

The execution test flow steps are the same as the first submission test case (see section 3.1.5), but this time the Testbed AP uses a valid G3 certificate to sign the SignalMessage that is returned back to the SUT AP (C2).

Figure 6 illustrates the test case execution steps.

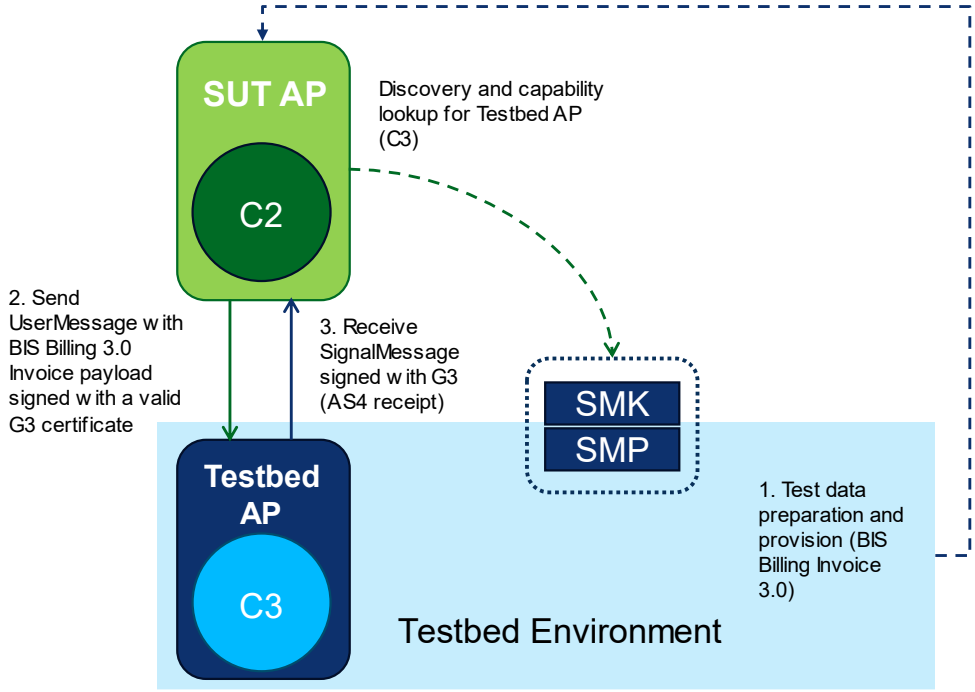

Figure 6 G3 message submission with G3 SignalMessage reception test case (step 4 omitted for brevity reasons)

Success Criteria

To pass the test, the SP must:

- Correctly identify recipient participant (C3) via SMK/SMP dynamic discovery and retrieve their endpoint metadata.
- Send the prepared BIS Billing 3.0 Invoice, signed with a valid G3 certificate.
- Receive the corresponding SignalMessage (AS4 Receipt) from the Testbed AP (C3), signed with a valid G3 certificate, to test interoperability with parties using G3 certificates.