The future is open

Peppol CTC Reference Document Addendum

CTC Community Working Group

September 2023

Version 1.0

Table of contents

Foreword

Peppol CTC is a set of specifications based on the concept of Decentralised Continuous Transaction Controls and Exchange, for use in both domestic and cross-border transactions.

However, the Peppol CTC specifications, together with the Peppol International Invoice model and the Peppol Network, can also support new and existing centralised clearance and reporting CTC schemes.

This addendum provides information that is additional to that provided in the first edition of the Peppol CTC Reference Document and reflects additional learning since publication of the first edition.

The purpose of the addendum is to:

- increase awareness among Tax Administrations about:
  - eInvoicing and CTC models
  - implementation details
  - the interconnection between differing requirements
  - the impact of differing obligations
- provide guidance based on experience and analysis of eInvoicing and CTC implementations in multiple jurisdictions
- encourage harmonisation relating to the adoption of eInvoicing and CTC principles, models and standards

The addendum is an interim document pending incorporation into a second edition of the Peppol CTC Reference Document.

Terminology

The following table introduces new, or clarifies existing terminology, beyond that used in 2021 Peppol CTC Reference Document.

Term/abbreviation	Explanation
Full DC	DC that is created for Full tax invoice for sales
Full DR	DR that is created for Full tax invoice for purchase
Simplified invoice or Receipt	Refers to a fiscal document that can be issued by the supplier to a buyer, but where such document includes less information compared to a complete invoice. A simplified invoice/receipt would typically be issued in the context of B2C transactions but, depending on jurisdiction-specific regulations, could also refer to a lower value B2B transaction. This is regulated in the EU by the VAT Directive, and further defined in jurisdiction-specific regulations
Simplified DC	DC that is created for Simplified sales invoice
Government	When used in this document, 'Government' may also include any government agency entitled to access and process data collected by C5
B2C	The selling of products and services from businesses to consumers (private persons)
B2C flag	Additional marking on BD to indicate that the buyer is not a taxable person
Intra-Community flag	Additional marking on BD to indicate that one of the parties is based in another jurisdiction, but both parties are based within the EU

1. Business Document and Tax Data Document content

Data minimisation

To implement a scalable CTC model, it is important to identify and agree those data elements to be provided to the Government. When defining these data elements, is important to note the following:

- Data minimisation – only data necessary, as determined by the TA to perform its task, should be collected

- Data protection and confidentiality – collection of data that can be considered personal or confidential should be justified

- Technical scalability – the collection of data elements should not impose an unnecessary technical and operational burden on taxpayers.

Technical scalability will be greater through use of the AS4 communication protocol between C2, C3 and C5 rather than use of API technologies. AS4 is a payload-agnostic technology, allowing implementation of changes to document content without the need to modify the communication protocol.

DC and DR content requirements

Peppol CTC can technically support two approaches to the amount of data to be shared with the Tax Administration:

- BD full - in this approach, the TDD fully matches the BD, based on Peppol BIS/PINT specifications, providing the simplest approach for implementation, deployment, and maintenance
    - in such a scenario, for scalability reasons, DC/DR will only correspond to the full BD content.

- BD subset[1] - this approach allows flexibility taking account of requirements such as data privacy and confidentiality. The TA will determine the BD subset for their respective jurisdiction
    - DC (required) - TA defines the content of DC to be produced by C2
    - DR (optional) - TA defines the content of DR to be produced by C3, should they want to implement reporting of purchase invoices.

[1] For clarification, BD subset is not aggregated, summarised, transformed, or otherwise manipulated information of BD, but is an extract of information that already exists in each individual BD. It is the responsibility of the SP to ensure that data in the BD subset does not differ or has not been manipulated compared to the underlying BD.

When using a BD subset to be reported to C5, the content of the Tax Data Document (TDD) can be extracted from the exchanged Business Document (BD). It should be an exact extract of data that already exists in each individual BD.

It is the responsibility of the Service Provider (SP) to ensure that this requirement is met.

Document Cleared (DC) and Document Response (DR) can utilise data that is aggregated, summarised, transformed or otherwise manipulated from the BD.

Example invoice data fields

Recognising that the TA will determine the DC BD subset, the following table illustrates some of the invoice data fields that could be implemented for a Full tax invoice in domestic transactions[2] (where both C1 and C4 are located in the same jurisdiction)[3].

OpenPeppol will have a coordinating role, primarily to align jurisdiction-specific requirements where possible, so that a global and unified BD subset TDD can be created.

General
Document type (including sub-types) – eg, invoice, part-invoice, credit note
Sequential numbering

Supplier data
Full legal name of the supplier
Full address of the supplier in country of establishment
Indirect tax identification number (if applicable)
Information of the fiscal representative of the supplier (if appointed)
Legal form of the supplier
Trade register number of the supplier
Other supplier data (e.g. court registration, legal seat, paid up capital)

[2] In principle, largely the same content specifications could apply for transactions at least within the EU (so called intra-Community transactions).

[3] This can be compared with the Full tax invoice requirements according to Council Directive 2006/112/EC ("**VAT Directive**")

Customer data
Full legal name of the customer
Full address of the customer in country of establishment
Bill-to address (if different from the registered address)
Indirect tax identification number (if applicable)
Information of the fiscal representative (if appointed)
Trade register number of the customer

Transaction data
Date of issue
Date of supply (chargeable event)
Date of prepayment
Description of goods/services
Quantity of goods supplied, or the extent of the services supplied
Purchase order number (optional)
Shipped from location (for the supply of goods)
Shipped to location (for the supply of goods)
Status of the goods (e.g. in bond, in free circulation)

Financial data
Taxable base per item (unit price excl. tax)
Total taxable base per tax rate or exemption
Tax rate applied, including exemptions
Total tax amount calculated per rate
Total tax amount payable
Discounts/rebates (if not included in the unit price)
Total gross amount (incl. tax)
Currency code
Exchange rate (if not issued in the local currency)
Terms of payment

Specific references
Invoice reference, where tax exempt, margin scheme, reverse charge, etc
Other reference, such as in the case of barter transactions, prepayments, etc
Reference to "cash accounting scheme" in B2B sales, where tax invoiced by the supplier is deductible by the customer upon payment
Self-billing statement

2. Implementation of MLR and IRM

It should be considered best practice to implement both Message Level Response (MLR - technical response) and Invoice Response Message (IRM - business response) for the exchange of BD between C1 and C4, rather than implement only MLR or IRM in isolation.

MLR implementation

If MLR is implemented, then it should be implemented for negative MLR, thereby notifying that there have been technical errors with the received BD, resulting in rejection of the BD.

Implementing a positive MLR has limited additional value to either party and is likely to create an unnecessary burden on the service providers, without bringing additional certainty or reliability to the document exchange process.

Note that, if the sending SP has done everything correctly, there will not be a negative MLR. The appearance of a negative MLR will be exceptional, indicating that the sending SP has not met the required responsibilities.

IRM implementation

Implementation of the obligation for the recipient of an eInvoice to issue an electronic business response to the sender and to the Government is an increasing trend. This requirement has been either implemented or is under consideration for implementation in, for example, Chile, Turkey, Italy (B2G), Serbia, and France.

For implementation of IRM, the following aspects should be considered:

- IRM obligation. Based on international experience and findings from TA interviews, we expect that it is highly likely that IRM will be introduced in more jurisdictions. While this is a positive development that will bring greater predictability for Governments, and greater efficiencies for businesses, some TAs may choose not to introduce an IRM obligation immediately with the introduction of eInvoicing. A delay on introduction need not be unnecessarily long, and could give tax subjects time to become accustomed to eInvoicing before IRM becomes a requirement.
- IRM issuance timeframe. Jurisdictions often introduce a timeframe for issuance of IRM. Although the precise timeframe will be a matter for each jurisdiction, we suggest that, from a business perspective, the timeframe should not be too short. For example, in Chile and Turkey, the IRM must be issued in 8 days which, while helpful from the perspective of tracking tax obligations, can be challenging for

businesses that execute controls on their operations. In contrast, Serbia requires 15 days for B2G transactions and 20 days for B2B transactions.

- Consequences for breach of the IRM timeframe. Jurisdictions should consider the consequences for breach of the required timeframe. We note two approaches based on existing practice. Either the issued document becomes final and non-disputable (for example, Chile, Turkey, Serbia B2G), or the issued document become null and void (for example, Serbia B2B, Italy B2G). Irrespective of the chosen approach, business efficiency will be improved by implementing a single approach for all transactions, rather than differ between B2B and B2G.

MLR TDD content guidance

In addition to data identifying the sending and the receiving parties, MLR TDD should include the following elements, as a minimum:

- DC reference, structured in the following sequence: SEI/CEI/DI/FY, where:
  - SEI - Supplier Endpoint Identifier
  - CEI - Customer Endpoint Identifier
  - DI - Document Identifier (e.g. invoice number)
  - FY - Issuance date[4]
- Status code
  - AB - Message Acknowledgement
  - IP - In Process
  - UQ - Under Query (may be repeated before moving forward)
  - CA - Conditionally Accepted
  - RE - Rejected
  - AP - Accepted
  - PD - Paid (may be in steps, partially paid and then paid)
- Use case number and/or name
  - 1 / Invoice in process
  - 2a / Invoice in process with additional reference data
  - 2b / Invoice in process but postponed
  - 3 / Invoice is accepted

[4] Playground should be updated to this from "Fiscal year"

- 4a / Invoice is rejected
- 4b / Invoice is rejected, and re-issue is requested
- 4c / Invoice is rejected, and replacement is requested
- 5 / Invoice is conditionally accepted
- 6a / Invoice is under query due to wrong or missing information
- 6b / Invoice is under query due to missing PO reference
- 6c / Invoice is under query due to incorrect details and a partial credit note is requested
- 7 / Invoice payment has been initiated
- 8 / Invoice is accepted by a third party acting for the buyer

IRM TDD content guidance

In addition to data identifying the sending and receiving parties, IRM TDD should include, as a minimum, the following elements:

- DC reference, structured in the following sequence: SEI/CEI/DI/FY, where:
  - SEI - Supplier Endpoint Identifier
  - CEI - Customer Endpoint Identifier
  - DI - Document Identifier (e.g. invoice number)
  - FY - Issuance date[5]

- Status code[6]
  - AB - Message acknowledgement
  - IP - In process
  - UQ - Under query (may be repeated before moving forward)
  - CA - Conditionally accepted
  - RE - Rejected
  - AP - Accepted
  - PD - Paid (can be in stages, partially paid and then paid)

[5] Playground should be updated to this from "Fiscal year"

[6] It is for the relevant national regulator to determine whether to implement some or all of these Status codes. This list represents the options available under Peppol CTC.

- Use case number and/or name[7]
    - 1 Invoice in process
    - 2a Invoice in process with additional reference data
    - 2b Invoice in process but postponed
    - 3 Invoice accepted
    - 4a Invoice rejected
    - 4b Invoice rejected requesting re-issue
    - 4c Invoice ejected requesting replacement
    - 5 Invoice conditionally accepted
    - 6a Invoice under query (wrong or missing information)
    - 6b Invoice under query (missing PO reference)
    - 6c Invoice under query (wrong details, credit note requested)
    - 7 Invoice payment has been initiated
    - 8 Invoice accepted by a third party acting for the Buyer

Use of 'unstructured' free text between trading parties to complement the predefined IRM elements should be excluded from the IRM.

More details about IRM can be found at:
https://docs.peppol.eu/poacc/upgrade-3/profiles/63-invoiceresponse/

Document flow orchestration

The flow for the BD is from C1 to C2 to C3 to C4, where:

- C1 is the supplier
- C2 is the sending SP acting for the supplier
- C3 is the receiving SP acting for the buyer
- C4 is the buyer

The flow for IRM and respective TDD will follow reversed roles where C1 is the buyer and C4 is the supplier.

The flow for the MLR and respective TDD is from C2 to C3, where

- C2 is the sending SP acting for the buyer
- C3 is the receiving SP acting for the supplier

Note that MLR does not need to reach C1 and C4.

[7] It is for the relevant national regulator to determine whether to implement some or all of these Use case numbers/names. This list represents the options available under Peppol CTC.

3. Cross-border transactions

Context

In most jurisdictions, import and export B2B transactions, which includes intra-Community transactions in the EU[8], (collectively 'cross-border') are typically initially exempted from CTC schemes.

When cross-border transactions are included, they often have a character of an additional reporting obligation, that is, the supplier reports the cross-border invoice to a predefined government infrastructure and thereafter issues the invoice to the buyer abroad.

In Peppol CTC, cross-border invoices can be addressed by eInvoicing and do not require a separate or additional process.

Defining the jurisdictions

In the EU ViDA proposal, reporting of DC of the issued (sales) invoice, and the reporting of DC for the received (purchase) invoice, will be done based on the Indirect Tax ID (VAT ID) registration of the tax subject that has been used when selling and buying, respectively.

In the context of Peppol CTC, this means:

- Sales invoices (export and/or intra-Community). C2 will report DC to C5.1 (the tax administration of C1, based on the supplier VAT ID used for the issued BD)
- Purchase invoices (import and/or intra-community). C3 will report DR to C5.4 (the tax administration of C4, based on the buyer VAT ID used for the received BD)
    - if the buyer is a non-taxable person and has no VAT ID, reporting to C5.4 shall be based on the corporate registration of the buyer

Note that the content requirements for cross-border DC and DR may be less extensive than for domestic transactions.

4. Business-to-Consumer transactions

Scope

While the approach to controls for Business-to-Consumer (B2C) transactions can vary significantly from country to country, it is important

[8] Note that B2C transactions are excluded from this section – the focus is B2B transactions.

to note that, within a jurisdiction, CTC models for B2B/B2G and B2C do not necessarily need to be identical. This section illustrates how the Peppol Network and Specifications can be leveraged for B2C.

This section focuses on potential implementation of CTC for domestic B2C transactions based on Peppol specifications, and thus may not be applicable to jurisdictions that have already implemented another approach which, as example, may be one of the following models:

- a supplier is opted in for one of the EU One-Stop Shop (OSS)[9] schemas. In this case, the supplier has the obligation to report relevant B2C transactions to the single EU jurisdiction

- a fiscalisation framework is implemented. In this case, the government may have implemented an Electronic Fiscal Device (EFD)[10] framework, under which only specific, certified hardware devices must be acquired and installed by the tax subjects to fulfil their reporting obligation, typically for 'bricks and mortar sales' sales.

Document types

For B2C transactions, it is necessary to differentiate between two BD types and a number of scenarios:

- full tax invoice. A document issued by the supplier to the buyer, either to receive a payment or as a confirmation of received payment for goods sold or services rendered
- simplified invoice[11]. A document issued by the supplier to the buyer, which can be issued under similar circumstances to the above. However, a simplified invoice is typically issued as a confirmation of payment received for goods sold or services rendered
    - the concept of 'simplified invoice' does not exist in all jurisdictions. Where it exists the supplier is allowed (but not obliged) to issue an invoice with less content compared to the full tax invoice, provided that the transaction fulfils certain criteria, for example, the transaction is below a value threshold, or the supplier operates in a certain industry

[9] https://vat-one-stop-shop.ec.europa.eu/one-stop-shop_en

[10] https://en.wikipedia.org/wiki/Fiscal_memory_device

[11] Note that such document type does not currently exist in Peppol and would have to be added. Use of a Simplified invoice would, typically, not be relevant in B2B or B2G circumstances, as such document would, normally, not suffice for the buyer from the content perspective.

- the most common use case is a physical sale via a point-of-sales, cash machine or otherwise in a 'bricks-and-mortar' environment, although online sales are becoming increasingly addressed
- a simplified invoice (or receipt) may be issued to businesses and government organisations, as well as private persons.

Principal considerations

Across different jurisdictions, there is little or no harmonisation of real-time controls for B2C transaction elements, such as:

- frequency/timing of reporting
- content of the reported information
- validation requirements
- distribution to the end-recipient

To achieve a complete picture (from the TA perspective) and unified processes (from both taxpayer and TA perspectives), we advise that the processing of B2C transactions in Peppol CTC stays as similar to the processing of B2B and B2G transactions as possible, although some deviation will be required. The most important aspects to consider are:

- simplified invoice. A new Peppol document type can be introduced to provide for the issuance of invoices with reduced content, irrespective of whether the buyer is a private individual or a business
- a B2C flag can be introduced to indicate that the buyer is a private person, irrespective of whether a full tax invoice or simplified invoice has been issued
- simplified DC. To indicate that a simplified invoice has been issued rather than a full tax invoice, where Full DC requirements would apply. This can be achieved with a 'Document Type Identifier', based on the Customisation ID
- simplified DC for B2C transactions. This can be slimmer than for B2B transactions, due to the nature of existing indirect tax requirements, and due to potential processing of personal or sensitive information relating to individuals. Our advice is to exclude the following data:
    - customer data - all data identifying the individual
    - transaction data - description of items, quantity, ship-to address
    - financial data - any amounts at line-item level

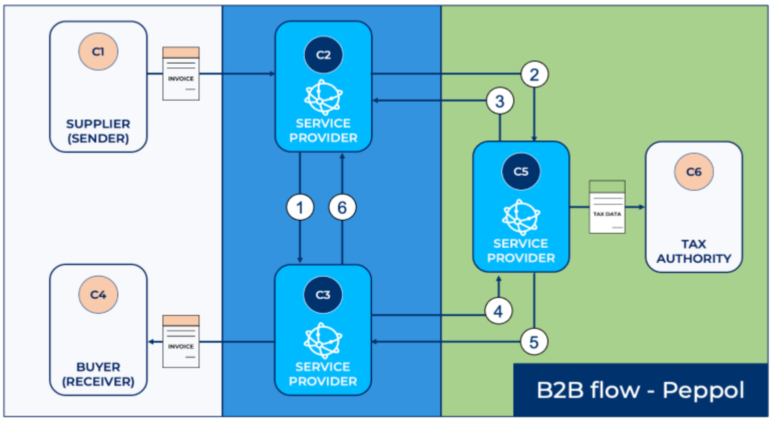
- DR subset. Reporting by C3/4 for B2C transactions does not bring the same value to the TA as reporting in other sectors. Consequently, DR subset reporting to C5 is not required for B2C
- Frequency of reporting. The data should be provided to C5 in (near) real-time and transaction-by-transaction by C2, as soon as it has been generated validation of the underlying BD
  - some jurisdictions consider implementation of aggregated handling of B2C transactions. To future-proof the approach, we advise that transactional reporting is implemented at the outset. Note that Chile abandoned aggregated reporting in favour of transactional reporting
- Timing of reporting. Validation of B2C transactions by C2 and initiation of reporting to C5 should be executed no later than 24 hours after the invoice is issued and distributed to the buyer
  - a convenient end-user experience, especially for customers physically at the point-of-sale, is an important consideration. Delays with validation of BD or reporting/receipt of B2C DC should be avoided, particularly since B2C transactions do not generally increase indirect tax deduction rights
  - experience from jurisdictions (e.g. Chile, Colombia, Hungary, South Korea, Spain, Taiwan, Uruguay) demonstrates, that prior validation of B2C transactions is unnecessary and near real-time reporting is sufficient
  - this can be seen as a minimum requirement, meaning that if the taxpayer would want to validate BD and initiate reporting of B2C DC to C5 prior to BD distribution, this should be allowed
- BD distribution. Since BD validation and DC reporting to C5 can be done within 24 hours from BD issuance, BD distribution can be done either by C1 or C2
- SMP. Peppol specifications require that all BD recipients are registered with the SML and SMP for real-time identification and routing. Registering individuals as recipients (unless some anonymisation mechanism implemented) in the SMP may pose concerns from the data privacy perspective
  - until this potential issue is resolved or an appropriate governance and regulatory framework implemented in a jurisdiction, our advice is that such individuals are not registered with an SMP
  - Peppol CTC for B2C transactions can instead be implemented as a '3-corner' approach, where:

    - C1 will issue BD and distribute it to C4 as printed document, PDF over e-mail, or other agreed means, outside the Peppol Network (otherwise C1 may authorise C2 to issue and distribute BD to C4)
    - C1 will provide BD for C2 for validation and reporting to C5 outside the Peppol Network
    - C2 will validate BD and, if successful, create and report DC to C5, or, if unsuccessful, reject the BD to C1 for correction
  - once data privacy considerations are resolved and individuals are registered in an SMP, standard Peppol CTC can be implemented. In this scenario, C3 could for instance be the bank account of C4, or a secure digital eMail address (such as for instance Kivra in Sweden).

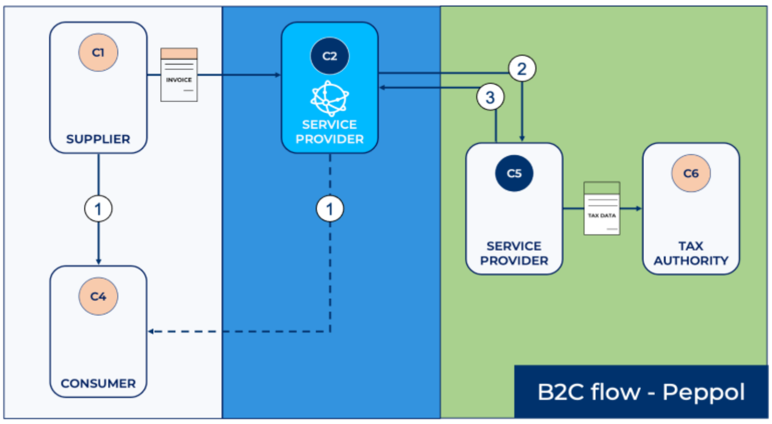
A non-deductible B2C transaction can be converted into a tax-deductible B2B transaction by provision of the necessary tax identification details of either the company, or the person if a sole proprietor.

Comparison of B2B and B2C flows

The following diagrams demonstrate the high-level differences between Peppol CTC flows for B2B and B2C transactions.



B2C flag:	No
Validation + reporting:	Real-time
DC content:	Full tax invoice/subset
BD distribution:	by C2 to C4



B2C flag:	Yes
Validation + reporting:	<24 hours
DC content:	Simplified Invoice
BD distribution:	by C1 or C2

Note that the B2C flow depicted covers the scenario where the consumer has no receiving access point – there is also a scenario where the consumer may use a banking app to receive invoices.

This app would be Corner 3 with a Peppol receiving capability in the model, thereby enabling the supplier to utilise a sending Peppol access point, in which case the B2B flow would apply.

5. Certification of Service Providers

General certification

Service Providers (SPs) must pass the general OpenPeppol controls to operate as Peppol-certified Service Providers. In addition, Peppol Authorities (PAs) can introduce additional requirements, albeit within parameters set out in the Peppol Authority agreement.

Additional certification requirements for CTC

Jurisdictions implementing Peppol CTC may want to implement additional requirements for SPs intending to offer CTC services.

In addition to the OpenPeppol certification requirements and Peppol Authority-Specific Requirements, we have created a list of further requirements that could be considered for implementation.

Requirement
Be a legal person
Have proven sound and stable financial standing o not be included in a regime of restructuring or bankruptcy o not be subject to a tax debt collection procedure o not have suspended any payments under current financial obligations o have a capital or asset value equal to or greater than [x amount] o have professional insurance according to defined requirements o provide regular ongoing confirmation of financial standing
Provide information related to legal representatives, board members, partners, shareholders, and direct and indirect controllers (beneficial owners) o not have a legal representative with an unspent criminal conviction o not have a legal representative subject to a tax collection procedure o demonstrate competency of staff in place
Maintain internationally recognised information security standards and certification
Have a business continuity and contingency plan
Meet defined requirements towards C5 o assurance of format and content compliance requirements for all required BDs and TDDs

o uphold specified uptime SLA o uphold specified response SLA towards C1/C4 o uphold specified TDD reporting SLA towards C5 o uphold specified BD exchange SLA between C2 and C3 o uphold specified audit requirements towards TA o offer opt-in security communication level towards C1 (by C2) and towards C4 (by C3)
Offer technical support towards C1/C4 o support receipt of mandatory format(s) and mandatory communications protocol
Successfully complete a defined testing process o Peppol BIS document formats o AS4 communication protocol o document legibility for BDs and TDDs
Uphold security standards towards the end user o while different interaction/connection options can be offered to end users, at least one should be considered as secure from a system-to-system perspective o alternatively, end users can be free to decide how to connect with their chosen SP

Certification requirements to avoid

Although the SP certification requirements below are found in several countries, they may impose unfair or discriminatory restrictions and have a negative impact on trade or business operations in general, as well as deployment of Peppol CTC across multiple jurisdictions, in particular:

- be a locally registered and/or established business
  - with global and regional cross-border trade, eInvoicing services are often provided by cloud-based vendors. This requirement restricts Tax Subjects from selecting the vendor of their preference (which they may already be using in other Peppol or CTC jurisdictions)
  - other more effective mechanisms for governments to oversee and control operations of such vendors may be available
  - this does not preclude governments from restricting service providers from specifically named selected jurisdictions, which are considered to be of higher risk, or otherwise not have mutual recognition or assistance agreements in place
- data residency in a specified jurisdiction or cloud (data sovereignty)
  - data often does not reside within country borders, as many tax subjects use multiple software solutions to support their daily operations (eg, eMail, ERP, workflow), which can either be in the the open cloud or hosted in another country

- where data sovereignty is considered, it should reasonably be allowed for SPs to process and store data in other jurisdictions considered safe by the specific country, based on specified criteria, such as mutual recognition or assistance agreements or personal data protection adequacy assessment

- to meet local information security requirements that cannot be substituted by, or interchangeable with, equivalent relevant international standards

For an efficient rollout of SP certification requirements across multiple jurisdictions, it is necessary to have dialogue and consensus between TAs regarding the final certification requirements criteria.

Scenarios for stricter requirements

The above certification requirements relate to SPs seeking certification to support suppliers and buyers (C1 and C4). Governments may wish to impose stricter additional requirements on:

- C5, which will be exchanging TDD with SPs
  - only C5 will be processing all data (TDD) issued and received by all tax subjects in a jurisdiction, since C2 and C3 will only process data for their Tax Subject customers. It is likely that a TA will have more strict data sovereignty requirements for C5
- SMP, which will maintain data on tax subjects
  - different levels of data sovereignty requirements may be applied, depending on the SMP model (centralised or decentralised):
    - the centralised SMP model offers greater flexibility to impose stricter data sovereignty approach or other requirements. With the centralised approach, the TA could be the entity in charge of the SMP, including hosting the registry within country borders
    - for the decentralised SMP model, we advise that the same approach is taken as for C2 and C3
- Government C5, which the government might want to deploy for certain groups of tax subjects.
  - a government may want to deploy their own C5 for certain categories of tax subject such as small and micro businesses, or specific industry sectors. Given that such an SP would be offered exclusively to domestic businesses, there can be a greater flexibility to impose stricter requirements, such as being a local entity, or hosting data within country borders.

6. Monitoring and audit of service providers

Monitoring

Monitoring[12]. For any CTC model to function properly, it is necessary for the TA, or TA-appointed agency, to monitor the quality of the services provided by the SPs. This includes monitoring of compliance both with standard Peppol requirements, as well as country-specific CTC requirements. The Peppol Interoperability Framework provides for this.

Non-compliance. The Peppol Service Provider Agreement includes a list of actions that can be taken against a SP not meeting the defined requirements. Depending on the severity of the non-compliance, these actions vary from warnings to revocation of the SP Certificate, preventing access to the Peppol Network.

Identifiers

The TA must be able to uniquely connect a specific BD to a TDD reported by an SP. To prevent any impact on the normal BD delivery in the Peppol Network, no new identifier needs to be introduced to the Peppol BIS or Peppol Envelope syntax. Instead, the Unique Identifier (SEI/CEI/DI/FY) can be derived from a combination of data elements pre-existing in the BD.

The Unique Identifier can be used in the following scenarios:

- during audit of C1 or C4 when matching the BD with the TDD
- enforcing increased control mechanisms by connecting a DC or DR received from a TA within a different jurisdiction

Auditing

SPs only need to be directly audited regarding CTC processes. Auditing of cleared BDs can be undertaken by C1 or C4, based on their SP agreement[13]. Example checks that could be undertaken include:

- identification of CTC jurisdiction
- creation of TDD (extraction of data based on business document)
- verification/validation of TDD
- application of TDD signature

---

[12] A set of reporting requirements is part of the standard OpenPeppol Service Provider Agreement

[13] Except where local regulations foresee legal mechanisms that allow the government to request data on tax subjects for third parties, such as injunction procedures