B Annex B: Examples of signatures and metadata

Enhanced PEPPOL defines two optional elements in the inner ASiC, additional signatures and meta data attributes.

They are placed in the inner ASiC, together with the Enhanced PEPPOL signature. The signatures and meta data are exchanged between Enhanced PEPPOL corners 1 and 4. As those data resides inside the encrypted inner ASiC, they are not available for Access Points (corners 2 and 3).

This annex gives examples of how to apply signatures and meta data but is not a complete list covering all possible situations. The examples are recommendations supplementing, but not a part of the Enhanced PEPPOL standard.

A.1 Parties involved

The examples are inspired by, but not limited to, payment handling. They cover two communication scenarios (in ISO 20022 terminology):

- An **initiating party** communicating directly with a **financial institution**.
- An **initiating party** communicating with a **financial institution** through an **intermediary agent** (3rd party).

In the examples the initiating party can be either the account owner or a debtor/creditor agent (power of attorney).

The communication between the initiating party and the financial institution is referred to as business level. The actual communication path through intermediaries, communication protocols, etc. may be referred to as transport level.

The initiating party and the financial institution will be referred to as sender and receiver, depending on the direction of the communication.

The role of the 3rd party is technical, meaning that the 3rd party offer IT services, for instance SAAS and data communication.

Most 3rd parties are connected to many initiating parties, acting as a hub.

A typical scenario is a service centre with an Enhanced PEPPOL connection to one or more banks. The bank customers (initiating parties) communicate through other protocols with the service centre.

In some cases, the initiating parties have applications in parallel, handling the same types of messages. For instance, different applications handling payments, salaries and pensions.

Typical challenges are to:

- Provide signatures and identifiers from the customers to the banks.
- Provide data needed by the 3rd party for routing to the customers.
- Provide data needed for routing to the right application at the 3rd party or customer.

A.2 Signatures

By signing the message payload before sending, the sender makes the receiver able to ensure the origin (authenticate) and integrity (no changes has occurred) of the payload.

Enhanced PEPPOL requires a signature in the inner ASiC. This is an enterprise level signature based on an Enhanced PEPPOL enterprise certificate. The certificate is issued by a Certificate Authority (CA) approved by Enhanced PEPPOL. This signature is applied automatically by the application being the Enhanced PEPPOL entry point. In the illustrations the Enhanced PEPPOL certificate and signatures based on this certificate are shown in blue.

Sometimes additional signatures are required. The following sections describes how to support such needs in Enhanced PEPPOL transfers. The additional certificates may be issued by other CAs than those approved by Enhanced PEPPOL. Additional certificates and signatures are illustrated in red.

Additional certificates and signatures are typically on business level or used in a wider context than the Enhanced PEPPOL signature.

A.2.1 Multiple signatures

Signatures in addition to the Enhanced PEPPOL signature may be a solution if:

- The sender and receiver have agreed that the message needs to be signed by more than one person (four eyes principle).
- The sender or receiver requires signatures based on another certificate than the Enhanced PEPPOL certificate.
- A personal signature is required.

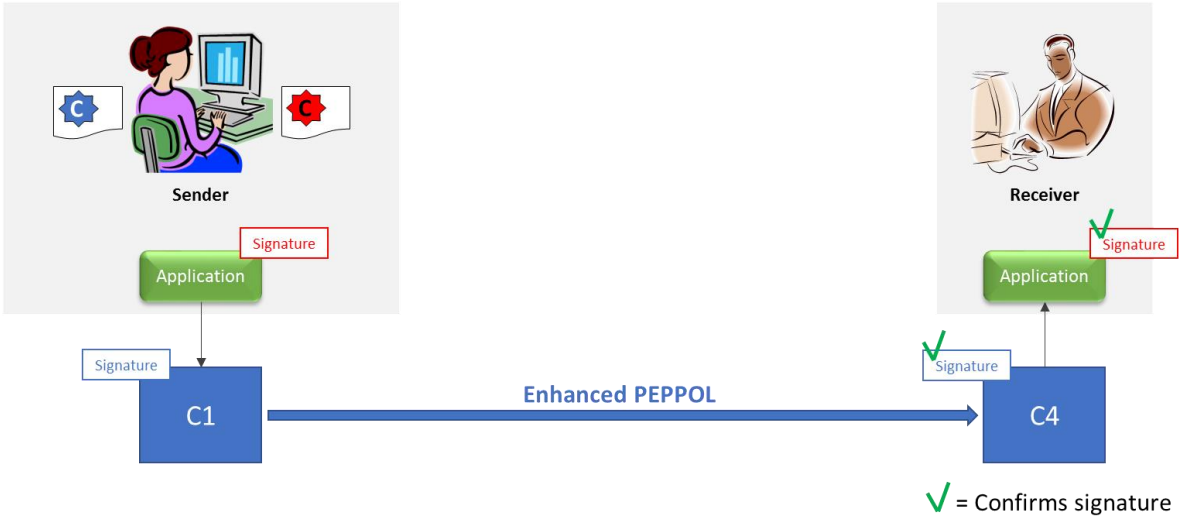

Figure 1: Dual signatures

Figure 1 shows two signatures based on two certificates. The Enhanced PEPPOL signature provides transport integrity between C1 and C4. The additional signature provides integrity on a business level.

The sender signing with the Enhanced PEPPOL certificate may be a legal entity or a person. This will depend on the signing procedure. If the application applying the Enhanced PEPPOL signature ensures only a specific person can sign with the Enhanced PEPPOL certificate, this may be considered a personal signature. If the signing with the Enhanced PEPPOL certificate is automated by the sending application, without any authorization check of who runs the application, this should be considered an enterprise signature. Based on the signature, it will not be possible to trace which person generated it.

A special case, illustrated in figure 2, occurs if the applications produce/consume the message (the content) and perform the Enhanced PEPPOL endpoint (C1 or C4) functionality. For instance, an ERP system produces a report, signs it with the Enhanced PEPPOL certificate and wraps it in the ASiC.

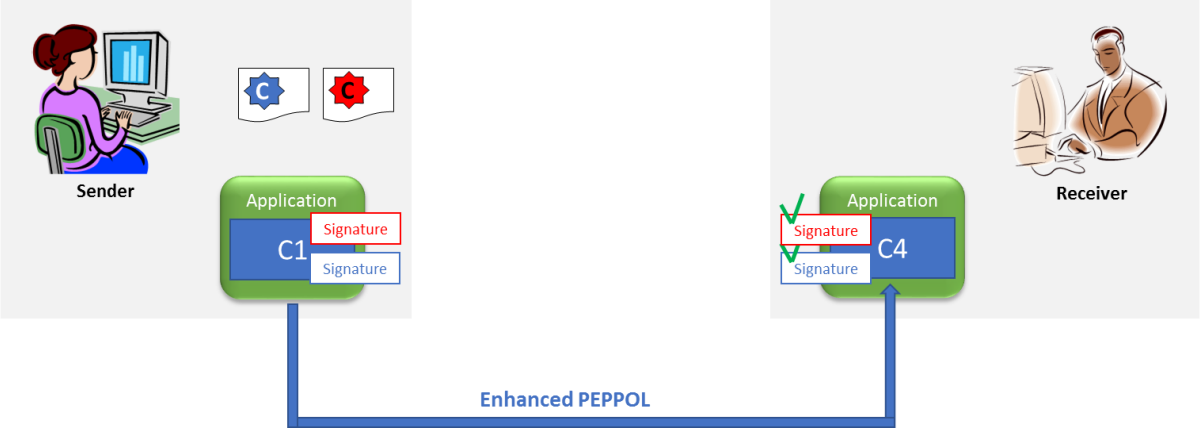

Figure 2: Applications including Enhanced PEPPOL endpoints

In such situations, it is not possible to separate the business and transport levels. Then the Enhanced PEPPOL signature may be considered as equal to a business level signature. The business partners may then agree to only use the Enhanced PEPPOL signature. The Enhanced PEPPOL signature will then serve both Enhanced PEPPOL transport integrity and business level integrity.

When one application produce/consume the message and another handle the ASiC, some may accept the Enhanced PEPPOL signature as a business level signature if the applications run on the same server or even in the same environment. This must be agreed between the business partners. Then other security mechanisms should also be considered, for instance manual confirmation of payments through an Internet bank.

Applications with such dual functionality may occur in all the examples, but for simplicity, the applications and Enhanced PEPPOL endpoints are illustrated as separated in the rest of this document.

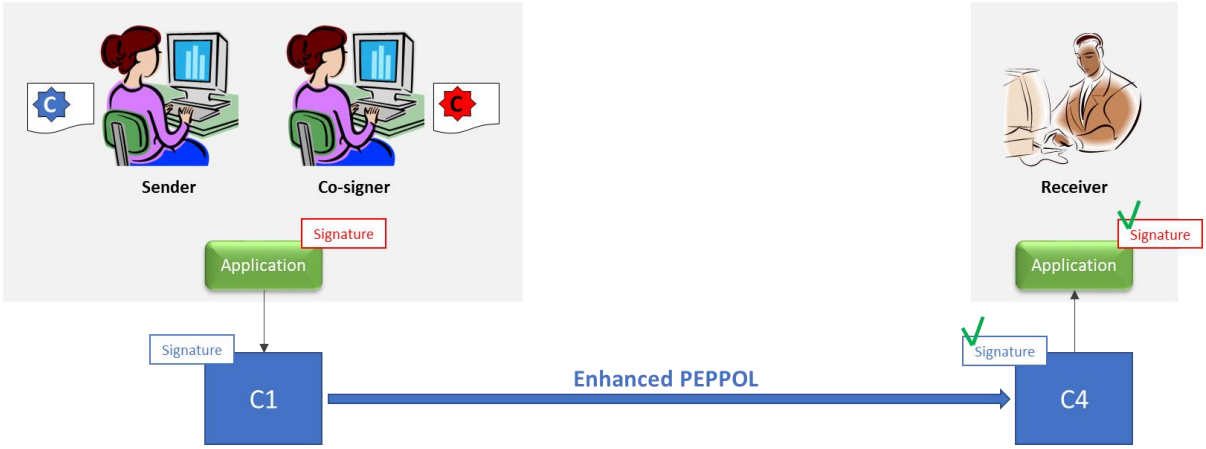

Figure 3: Co-signing

Figure 3 shows signing with two certificates. One being the Enhanced PEPPOL certificate. The other being a certificate issued to a specific person, the co-signer. The receiver validates and confirms both the Enhanced PEPPOL and additional signature.

To fulfil the four-eyes-principle, the signing with the Enhanced PEPPOL certificate shall meet the requirements for being a personal signature. If those requirements are not met, the signer should have a personal certificate, meaning that three certificates will be used. This is not illustrated.

More co-signers may be added. Each will need a personal certificate. Their signatures will be transferred as additional signatures.

A.2.2 A 3rd party controlling an Enhanced PEPPOL endpoint

In the 3rd party scenario, a 3rd party controls one of the end-points for the Enhanced PEPPOL communication. The communication between the business partners then consists of more than one segment. The 3rd party sits between two of those segments. A business partner uses a different protocol for communication with the 3rd party, which will forward messages by Enhanced PEPPOL to the other business partner. One can imagine more segments, but here we only show two.

The 3rd party handles IT services on behalf of a business partner. The business partner signs the messages itself. Meaning that the 3rd party has not a mandate to approve messages, for instance payment instructions, on behalf of the business partner. Use cases where a 3rd party has a power of attorney mandate from the account owner are not covered by this example.

A scenario could be, a service bureau offering advanced communication services to actors with small IT resources. By establishing a point-to-point communication with the service bureau, an actor can get access to the whole PEPPOL network.

The Enhanced PEPPOL signature only covers the Enhanced PEPPOL communication – between C1 and C4. Another signature is needed to ensure end-to-end message integrity and authenticate the sender.

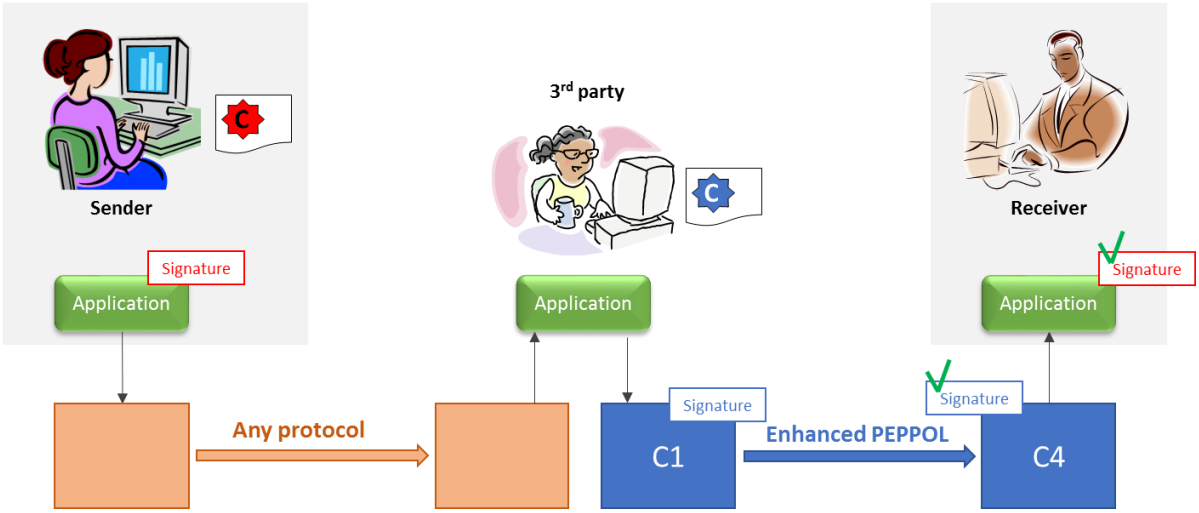

Figure 4: Communication via a 3rd party

The illustration shows the sender signing the message content before sending the message and signature to the 3rd party. The 3rd party has an application which places the message and signature in the ASiC structure and adds the Enhanced PEPPOL signature. (The third party only sign the message content, not the signature from the sender.)

The receiver will validate the Enhanced PEPPOL communication with the Enhanced PEPPOL signature and the message content with the signature from the sender.

When the receiver takes the sender role and returns messages (acts as C1), he will add two signatures. The 3rd party will validate the Enhanced PEPPOL signature. The receiver will only get and validate the business level signature (red). Ref. figure 5.

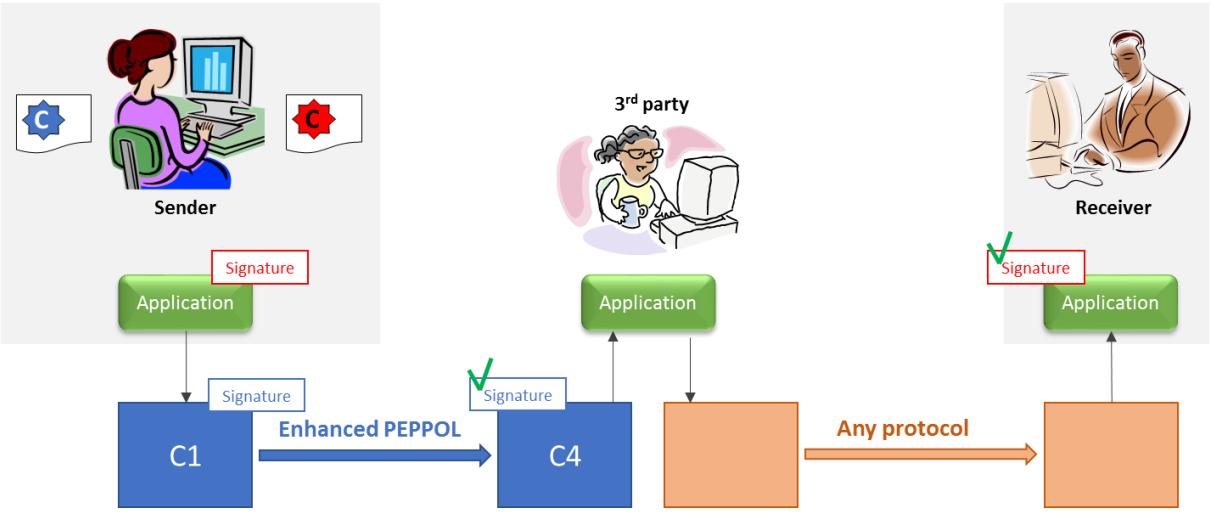

Figure 5: Communication via a 3rd party – return message

A.3 Meta data

The meta data in the inner ASiC is intended to transfer data needed by the receiver for internal routing, mapping of identifiers and authentication. The meta data shall only be used when the mechanisms in Enhanced PEPPOL is insufficient to solve a need.

The meta data consists of the attributes called Customer ID, Division, User ID, Destination ID, Destination Application and Supplementary Data.

The Division banking concept is deprecated and currently only used by a single bank. It will not be covered here. If needed the customers should agree how to use this attribute with the bank.

Supplementary Data is intended for future metadata attributes and is not covered here.

Some implementations separate message transfer from the processing of the message content. Typically, an application handling file/message exchange and security functions as their C1 and C4 implementation. This application may not be able to read the message content. Instead it will receive and route messages to the business applications producing or processing the message content. Some of the examples supports such a configuration.

A.3.1 Identifier mismatch

Enhanced PEPPOL identifies the participants with the PEPPOL Participant Identifier (PPID). If the receiver side applications use a different identifier, there is an "identifier mismatch" situation which needs to be bridged. A scenario might be if the receiver identifies customers with a proprietary customer number. When the customers send messages to the receiver, the receiver needs their customer number.

Such situations could be solved by:

- Adding the PPID as an alias to the identifier on the receiver side applications.
- Include the receiver side identifier in the Enhanced PEPPOL transfer.

This example shows how the identifier used by the receiver can be transferred as meta data, the second bullet above.

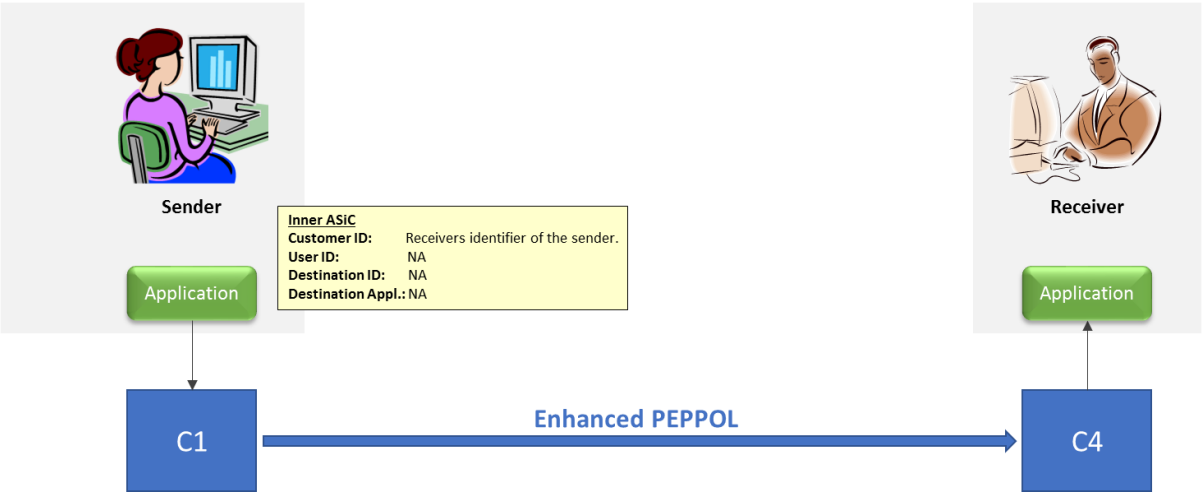

Figure 6: Handling identifier mismatch

The sender places the identifier (customer number) provided by the receiver in the **Customer ID** attribute.

A.3.2 Many applications on receiver side

The receiver has an application routing the messages coming in to several applications processing the messages. The SBDH doesn't contain enough information to identify the application to process each message.

For instance, if the receiver has different ERP systems handling general payments, pension and salaries. All the applications may receive the same ISO 20022 messages.

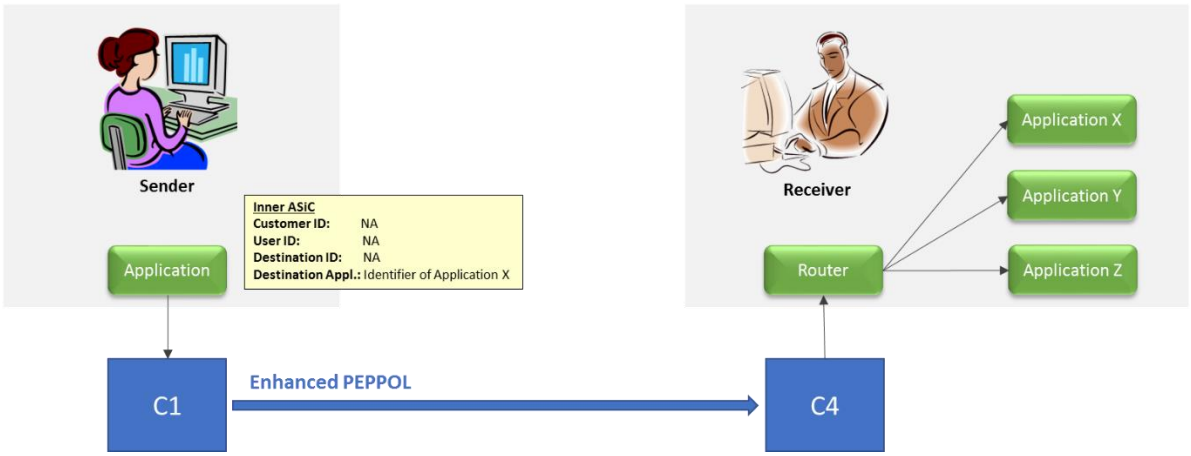

Figure 7: Routing to many receiving applications

The sender and receiver need to agree on how to identify the applications. The sender places the application identifier in the **Destination Application** attribute.

A.3.3 Many senders going through 3rd party

The sender provides the message payload, while the 3rd party is C1 in the Enhanced PEPPOL communication.

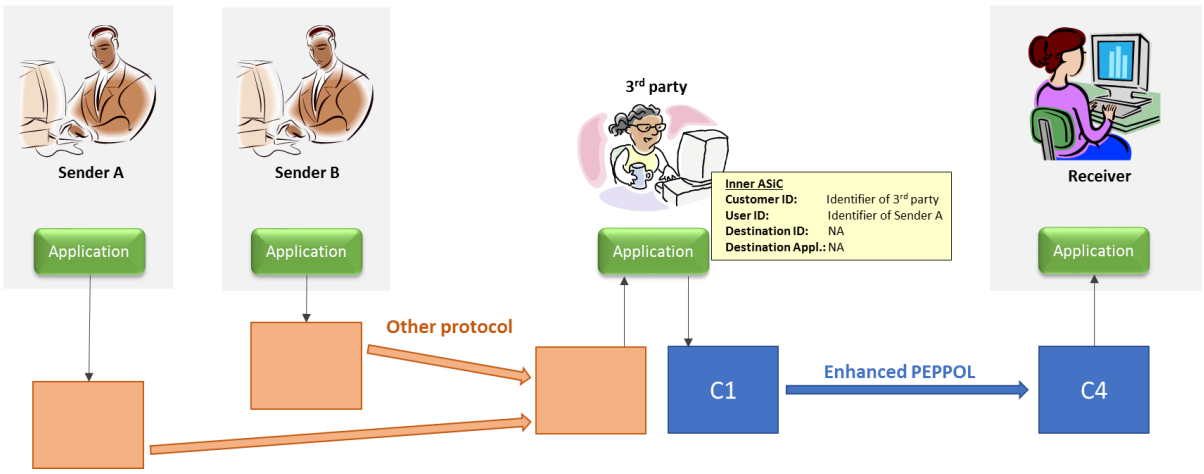

Figure 8: Senders using a 3rd party

Both the sender and 3rd party will be found in the receiver side customer (or agreement) register.

The receiver authorizes the 3rd party using the PPID or a customer identifier found in the **Customer ID** (permission to send files).

The receiver authorizes the sender using a customer identifier found in the **User ID** (permission to do business).

A.3.4 A 3rd party and many receivers

When returning messages in the previous example, the receiver takes the sender role. Let's first look at a case where the 3rd party needs to route on receiver level.

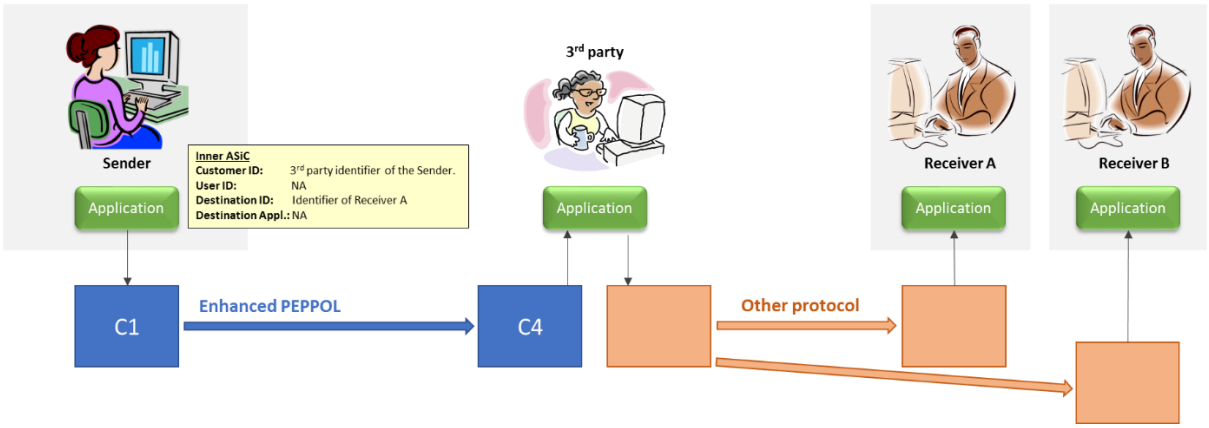

Figure 9: Many receivers connected to a 3rd party

The 3rd party may authorize the sender. If the 3rd party requires another identifier than the PPID, the sender needs to place their customer number in the **Customer ID**.

An identifier for the receiver will be needed by the 3rd party for routing to the right receiver. The sender places this identifier in the **Destination ID**.

A.3.5 A 3rd party, many receivers and many applications

If the receiver has several applications, routing will be needed first to the right receiver and then the receiver needs to route to the right application.

Illustration 10 also includes the signatures, to give a complete and complex example.

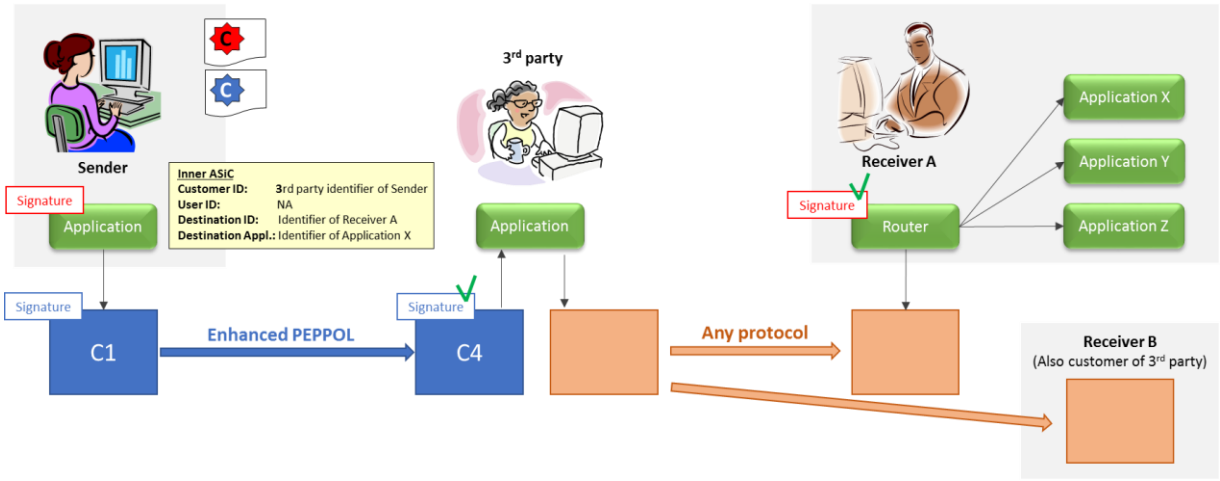

Figure 10: Many receivers, many applications and signatures

Signatures are handled as described in figure 4.

If the 3rd party needs an identifier for the Sender, this shall be placed in the **Customer ID**.

Identifier for the receiver should be placed in **Destination ID.** Place the identifier for the receiving application in the **Destination Application**.

The actual identifiers to be used must be agreed between the sender and receiver. A challenge on the sender side is keeping the data to be sent to different applications separated in the sender side applications.