Single Field Encryption for Securing Electronic Invoices

OFS Portal®

July 14, 2009

CONTENTS

1. Executive Summary 1

2. Why Single Field Encryption....................1

3. Electronic Invoice Security....................2

4. XML Data 2

5. Conversion of Electronic Invoices....................3

6. Current Methods of Sending Electronic Invoices Limit Adoption of Electronic Commerce 4

7. Single Field Encryption Eliminates Barriers to Adopting Electronic Invoicing 5

8. What is Single Field Encryption 6

9. How Does the Seller Use Single Field Encryption....................6

10. How the Buyer Validates an Invoice Using Single Field Encryption 8

11. Mexico’s Implementation of a Single Field Encryption Solution 10

12. Parties May Employ a Multiple Field Encryption Solution....................10

13. Conclusion 10

14. About OFS Portal....................11

LIST OF FIGURES

Figure 1 Converting an electronic invoice between formats 4

Figure 2 Building an electronic invoice with single field encryption....................7

Figure 3 Converting an electronic invoice with single field encryption....................8

Figure 4 Validating an electronic invoice with single field encryption....................9

1. Executive Summary

This paper presents a solution that allows electronic invoices to be converted from one XML format to another while providing a method of determining authenticity and integrity of the electronic invoice. A similar system has been implemented by Mexico's tax administration (Servicio de Administración Tributaria) (SAT) for secure electronic federal tax documents and has been operational since 2006. One key benefit of this solution is that it enables any third party service provider converting the electronic invoice to preserve the original authentication of the invoice by transmitting the sender's advanced electronic signature to the ultimate recipient. This solution eliminates the need for the service provider to sign the invoice "on behalf of" the original sender and therefore provides more reliable and trustworthy authentication of the electronic invoice.

2. Why Single Field Encryption

In today's environment it is very common for an electronic invoice to be converted from one format or transmission protocol to another when it is sent from the supplier to the buyer. The conversion is necessary because there is no universal format for invoices. Formats are often industry specific and some industries continue to support two or more common formats. While a universal format is desirable, it is unlikely that there will be a universal format that can be adopted across all industries in the foreseeable future. In order to achieve the benefits of electronic invoicing, both the buyer and the supplier want the invoice to be machine readable by their respective operating systems. This desire to have machine readable invoices for both trading partners drives the need to convert the invoice from the sender's preferred format to the recipient's preferred format.

Unfortunately, the conversion of the electronic invoice's format is not compatible with existing technologies to confirm the authenticity or integrity of the invoice. The conversion of the electronic invoice breaks an advance electronic signature associated with the invoice and renders the invoice non compliant with any requirement of a European Member State that the invoice be signed with an advanced electronic signature. This is true even if the conversion only alters the formatting of the invoice and does not alter any data values within the invoice.

An advanced electronic signature is the most common technological solution for ensuring the authenticity and integrity of a document. However, an advanced electronic signature prohibits any conversion of the invoice. A change in an XML invoice's electronic "tags" or "field names" will break the advanced electronic signature even though no data values have been altered. Trading partners wishing to ensure authenticity and integrity of the exchanged invoices are left with the unpalatable choice of sending untransformed invoices (which cannot be machine read by only one trading partner's computer system) or sending PDF documents or images of the invoice (which can only be read by humans and are not machine readable by either trading partners' computer systems). Neither choice allows the trading partners to gain the fullest potential from machine readable electronic invoices.

This dilemma is delaying the adoption of electronic invoicing and diminishes the benefits of electronic invoices.

In this paper, OFS Portal presents Single Field Encryption as a solution to this dilemma. Sending electronic invoices with certain data encrypted within a single field will allow conversion of the remainder of invoice so as to be machine readable by both the buyer's and seller's computer systems while providing a sufficient method of determining authenticity and integrity of the invoice for tax and other purposes.

3. Electronic Invoice Security

Title XI, Chapter 3, Section 5 of EU Directive 2006/112/EC imposes certain requirements on electronic invoices in the European Union. Article 232 of the Directive requires that the integrity of content and authenticity of origin of an electronic invoice be guaranteed by means of an advanced electronic signature, EDI or "other electronic means allowed by the Member States".

There are several common methods for securing electronic invoices to meet these objectives. Portable Document Format (PDF) files, digitally signed XML documents, and binary image files are three common ways in which the security and legal objectives can be met.

These methods have a common benefit of satisfying most tax or other legal requirements for guaranteeing the integrity and authenticity of the document. However, these methods share a common flaw. PDF or binary image files created from signed and scanned paper documents do not contain XML data that can be "read" by existing computer systems. Digitally signed XML documents (and some versions of PDF documents) do contain such XML data, but the data can only be "read" by the recipient if the recipient and the sender each configure their computer and operating systems to read documents in the same formats and use the same protocol. This can be particularly problematic when trading partners operating in different vertical industries exchange invoices. For example, a computer or office furniture supplier may sell to customers in the medical, energy, publishing or financial sectors. If each sector has developed its own unique format requirements for data to conform with its unique business processes, the computer or office furniture supplier must incur the expense of transmitting electronic invoices in each of these formats or the invoices will not be readable by its customers' computer systems.

If an electronic invoice needs to be converted from one format to another format then no current solution allows the electronic invoice to be signed with an advanced electronic signature.

4. XML Data

Extensible markup data (XML) provides a basic syntax that can be used to share information between different kinds of computers, different applications, and different organizations. XML, in combination with other standards, makes it possible to define the content of a document separately from its formatting, making it easy to reuse that content in other applications or for other presentation environments. It is classified as an extensible language, because it allows the user to define the mark-up elements through the use of "tags", "headers", "field names" and "attributes" that allow computers to recognize and sort different sorts of content data. Because of XML's flexibility, many industries, service providers and organizations have developed their own XML formats and standards suited to their particular business processes.

Under one XML data format (PIDX), the pricing elements of an invoice may appear as follows in the XML language:

```
- <pidx:Pricing>
        - <pidx:UnitPrice>
                <pidx:MonetaryAmount>9.35</pidx:MonetaryAmount>
                <pidx:CurrencyCode>Euro</pidx:CurrencyCode>
        </pidx:UnitPrice>
</pidx:Pricing>
```

A human reader of this electronic XML document would see “9.35 Euro”.

That same pricing element in another format (xCBL) would appear as follows:

```
<ListOfPrice>
        <Price>
                <UnitPrice>
                        <UnitPriceValue>9.35</UnitPriceValue>
                </UnitPrice>
                <Currency>
                        <CurrencyCoded>Euro</CurrencyCoded>
                </Currency>
        </Price>
</ListOfPrice>
```

A human reader of this electronic xCBL document would see the exact same information as a reader of the PIDX XML document above, “9.35 Euro”.

However, because the tags used by the PIDX format are different than the tags used in the xCBL document, the document cannot be both digitally signed and converted from one format to the other. The PIDX “tag” of “Monetary Amount” is not the same as the xCBL tag of “Unit Price Value” and this difference alone would be sufficient to break the advanced electronic signature associated with the document. If the PIDX invoice had been digitally signed and then converted to xCBL, the advanced electronic signature would be “broken” by the conversion of the tags even though the substantive data remained unaltered.

5. Conversion of Electronic Invoices

Because the sender and recipient of the electronic invoice often use different XML formats, one or both of the parties may wish to hire a third party service provider to convert the electronic invoice from one format to another. A common conversion process using a single service provider may look like this:

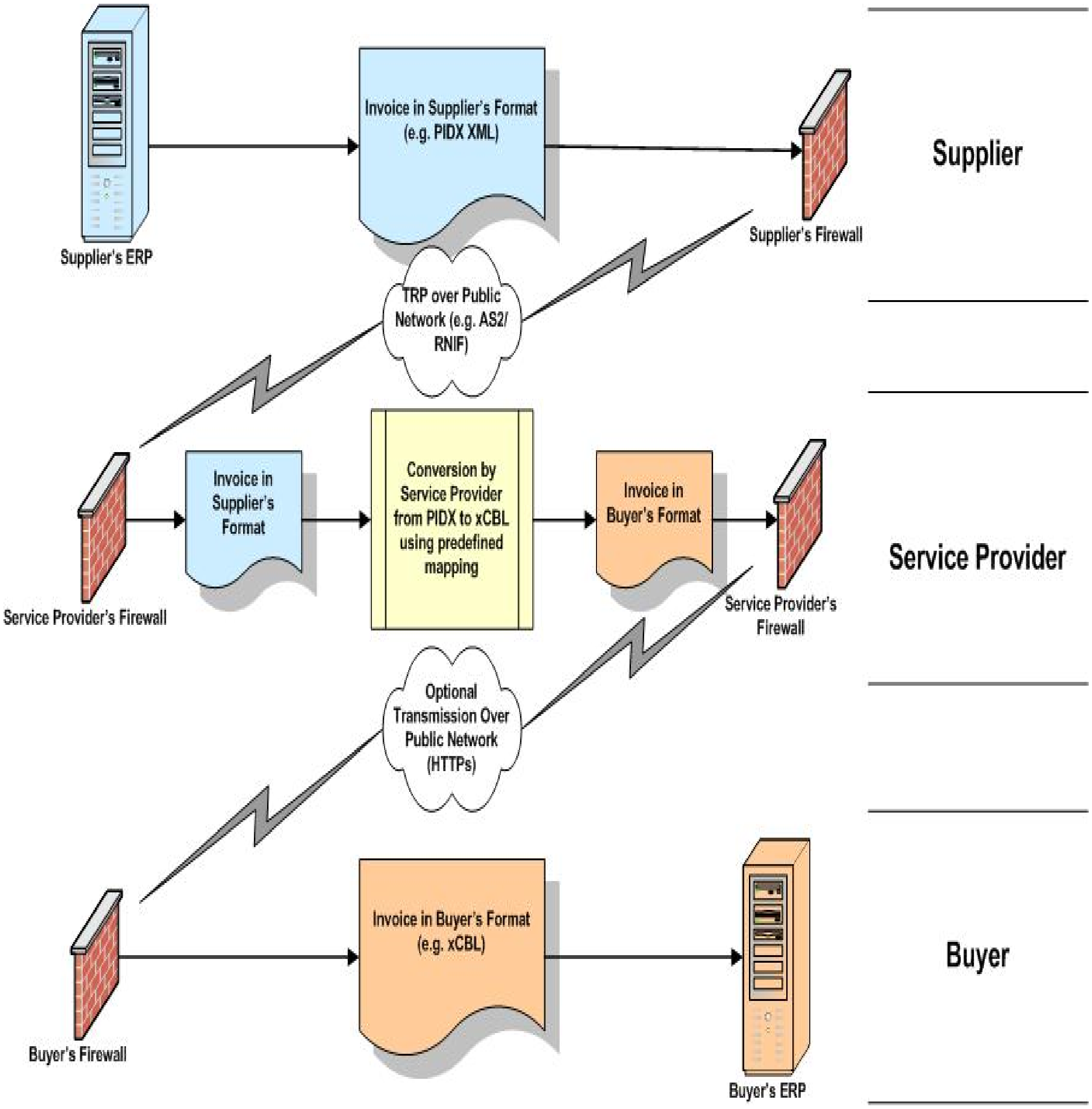

Invoice in Supplier's Format
(e.g. PIDX XML)
Supplier's ERP
Supplier's Firewall
Supplier
TRP over Public Network (e.g. AS2/ RNIF)
Invoice in Supplier's Format
Conversion by Service Provider from PIDX to xCBL using predefined mapping
Invoice in Buyer's Format
Service Provider's Firewall
Service Provider's Firewall
Service Provider
Optional Transmission Over Public Network (HTTPs)
Invoice in Buyer's Format
(e.g. xCBL)
Buyer's Firewall
Buyer's ERP
Buyer

Figure 1 Converting an electronic invoice between formats

6. Current Methods of Sending Electronic Invoices Limit Adoption of Electronic Commerce

The use of a scanned paper invoice in a PDF or binary image file does not allow dynamic use of data, so it adds cost without adding significant benefit over paper. Such a PDF or binary image file can be read by humans but not by computers. Therefore, while the pdf file can reliably be used to ensure the integrity of the actual invoice, it does not allow the sender's or the recipient's computer system to "read" the invoice and enter (or extract) the data into (or from) their respective financial software. In the case of pdf files that contain machine readable data, that data is formatted in a unique manner which may not comport with either the sender's or recipient's computer systems, requiring conversion of the file in a manner that would break any digital signature associated with the file.

With both a PDF file and a digitally signed XML invoice, the digital signature is applied to the format as well as the data. Any conversion of the format breaks the signature and renders the file non compliant with any requirement that the invoice be digitally signed.

The use of XML data requires the modification or reordering field names, tags, or attributes when converting the XML invoice from one format to another. This invalidates the digital signature even if the data has not been altered.

Moreover, differing XML formats may impose different requirements on unique fields within an invoice causing the appearance of the data within the field to be modified even if the meaning is preserved. For example, the recipient's XML format may require that all numeric fields have two decimal places, so the entry "4" in the sender's invoice would be converted to "4.00" in order to be validated in the recipient's XML format. Alternatively, units of measure are often varied, with one format recognizing, for example, "Kilograms" and another recognizing only "Kg." Any such conversion of data would break an advanced electronic signature and thereby fail to satisfy any requirement for an advanced electronic signature imposed by a EU Member state.

In order to send electronic invoices with advanced electronic signatures the senders and recipients of invoices must use the exact same format and transmission protocol. This may limit the number of potential electronic enabled trading partners in the foreseeable future. Alternatively, parties must support multiple formats, which is very expensive and ultimately not scalable beyond two or three formats.

For large organizations, supporting multiple formats increases the costs associated with e-commerce transactions. Where possible, the larger companies mitigate these costs by requiring their smaller trading partners to adopt a specific format. This imposes significant costs on small and medium enterprises (SME's) who have several larger trading partners or who have customers in different industry sectors. Trading partners who cannot adopt the prescribed electronic format must continue to transact on paper, reducing the e-commerce benefits the large organizations and the SMEs will realize.

Small organizations typically do not have the technical capability or staff to support multiple formats. If they choose a format that bests suits their own needs, they cannot use a service provider to convert the electronic invoices into other formats without breaking the advanced electronic signature. The SME's are unable to migrate from paper transactions to electronic transactions because the SME's simply do not have the resources or expertise to deal with the complexity of multiple formats.

7. Single Field Encryption Eliminates Barriers to Adopting Electronic Invoicing

The widespread adoption of electronic invoicing can greatly reduce transaction costs for large enterprises as well SME's.

To realize the maximum benefit of e-commerce, an organization needs to transact electronically with most of its trading partners, including SME's. Ideally, the organization will use a single electronic invoice format for all trading partners to reduce complexity and cost.

Because there is no single standard for electronic invoice formatting, SME's must support multiple invoice formats if they wish to participate in electronic commerce. SME's need the services of outside providers to convert electronic invoices to and from these different formats (e.g. between xCBL and PIDX or XBITS).

The difficulty is in converting the electronic invoices while retaining the ability to validate and authenticate the documents. The use of a single field encryption method accomplishes this goal.

8. What is Single Field Encryption

Single field encryption is a method for encrypting and digitally signing certain designated elements of an electronic invoice, then storing the signed encrypted data in a single XML field within an unencrypted and unsigned document.

There are a number of benefits to this method:

- The format of the remainder of the electronic invoice can be changed without altering the encrypted data or breaking the digital signature.
- The buyer can better verify document authenticity by validating the advanced electronic signature of the *original sender* and need not rely upon authentication performed by an intermediary service provider.
- The service provider converting the invoice need not sign the invoice on behalf of the sender and instead can pass along the sender's advanced electronic signature untouched with the converted invoice.
- The trading partners save money and eliminate administrative obstacles by not hiring and paying a service provider to sign an invoice "on behalf of" one trading partner.
- The recipient can easily validate unencrypted transaction data by comparing it to the encrypted field.
- The buyer can consume data from the unencrypted tags automatically.

9. How Does the Seller Use Single Field Encryption

The applicable tax authority must first designate the type of data and the sequence of that data in the single field. Each trading partner must comply with those requirements and the requirements must be implemented in a uniform way.

When building the electronic invoice, the seller also builds the string of designated data to be encrypted in the single field, in the prescribed sequence. For example, if the taxing authority required the name of the seller, the name of the buyer, the VAT amount of the invoice and the total amount of the invoice, then the encrypted field may appear as follows: 12345|20090605|SupplierA|BuyerB|1000.00|150.00[1].

The seller encrypts this data string using the hash and encryption algorithms and then signs the data string using the sender's digital certificate.

The seller converts the resulting signed and encrypted data string from binary to text using the encoding scheme, such as Base64.

The converted text string is stored in a single XML field within the electronic invoice.

[1] "12345" is the invoice number, "20090605" is the invoice date, "SupplierA" is the vendor, "BuyerB" is the customer, "1000.00" is the taxable amount, and "150.00" is the amount of the tax.

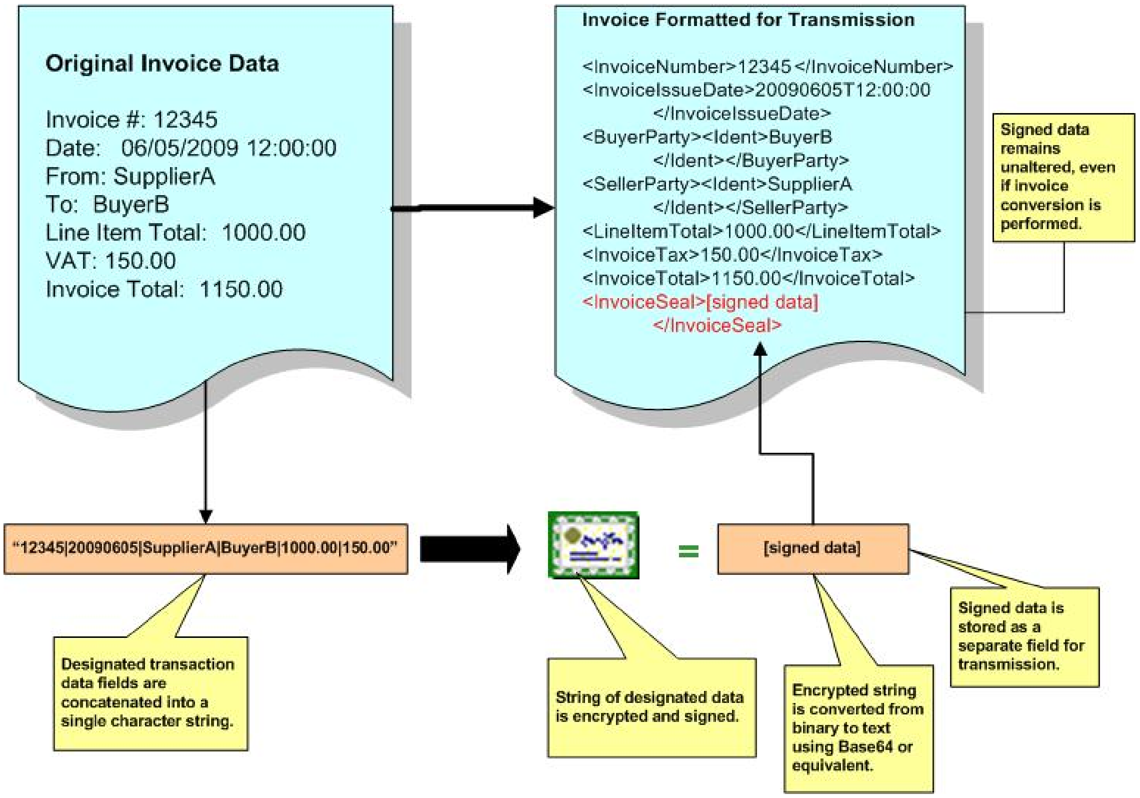
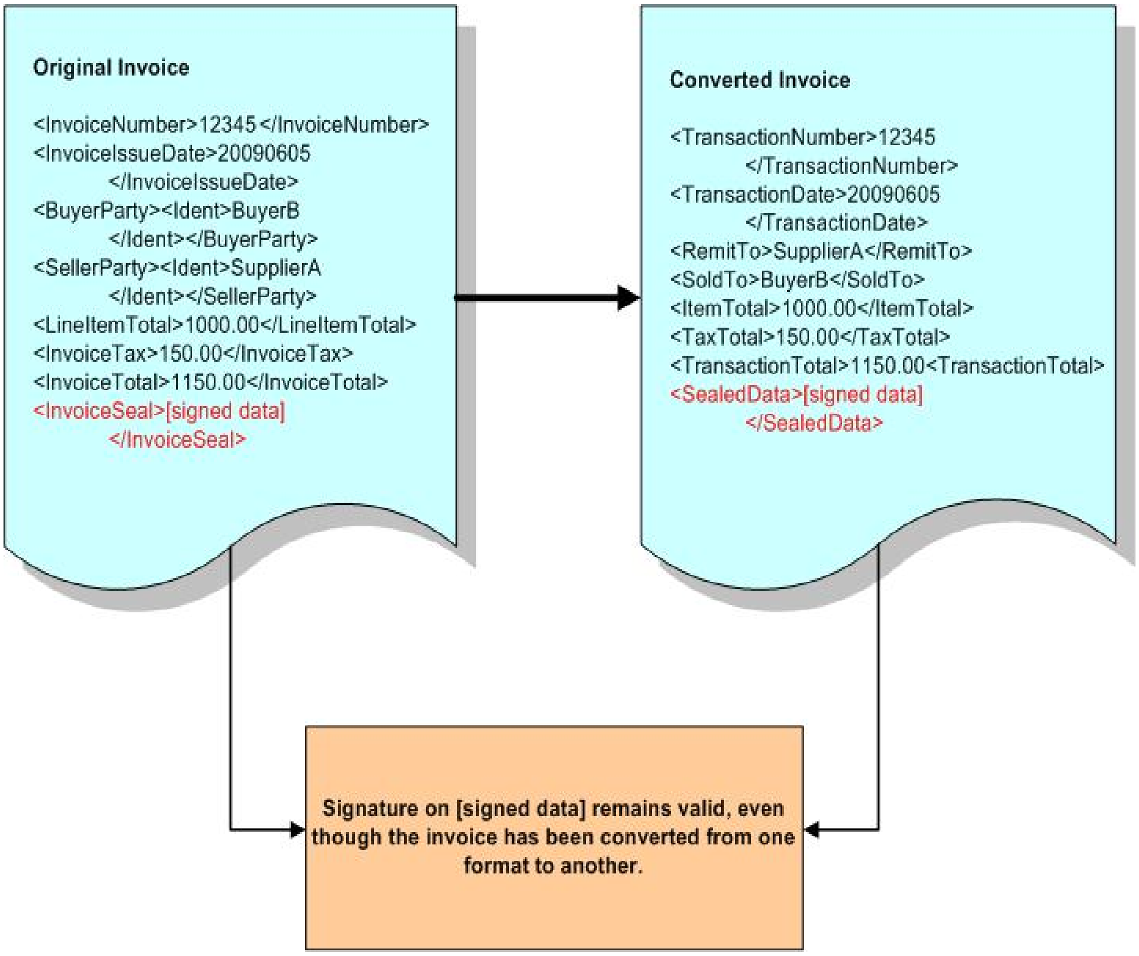

Original Invoice Data
Invoice #: 12345
Date: 06/05/2009 12:00:00
From: SupplierA
To: BuyerB
Line Item Total: 1000.00
VAT: 150.00
Invoice Total: 1150.00
Invoice Formatted for Transmission
<InvoiceNumber>12345</InvoiceNumber>
<InvoiceIssueDate>20090605T12:00:00 </InvoiceIssueDate>
<BuyerParty><Ident>BuyerB </Ident></BuyerParty>
<SellerParty><Ident>SupplierA </Ident></SellerParty>
<LineItemTotal>1000.00</LineItemTotal>
<InvoiceTax>150.00</InvoiceTax>
<InvoiceTotal>1150.00</InvoiceTotal>
<InvoiceSeal>[signed data] </InvoiceSeal>
Signed data remains unaltered, even if invoice conversion is performed.
"12345|20090605|SupplierA|BuyerB|1000.00|150.00"
=
[signed data]
Designated transaction data fields are concatenated into a single character string.
String of designated data is encrypted and signed.
Encrypted string is converted from binary to text using Base64 or equivalent.
Signed data is stored as a separate field for transmission.

Figure 2 Building an electronic invoice with single field encryption

The seller transmits the electronic invoice directly to the buyer or to an intermediary designated by either the seller or the buyer.

If the invoice is transmitted to an intermediary, the document is transformed from the seller's format to the buyer's format. The encrypted data within the single field and its associated digital signature are left unaltered. The intermediary transmits the transformed invoice to the buyer.


Original Invoice
Converted Invoice
Signature on [signed data] remains valid, even though the invoice has been converted from one format to another.

```
<InvoiceNumber>12345</InvoiceNumber>
<InvoiceIssueDate>20090605
          </InvoiceIssueDate>
<BuyerParty><Ident>BuyerB
          </Ident></BuyerParty>
<SellerParty><Ident>SupplierA
          </Ident></SellerParty>
<LineItemTotal>1000.00</LineItemTotal>
<InvoiceTax>150.00</InvoiceTax>
<InvoiceTotal>1150.00</InvoiceTotal>
<InvoiceSeal>[signed data]
          </InvoiceSeal>
```

```
<TransactionNumber>12345
          </TransactionNumber>
<TransactionDate>20090605
          </TransactionDate>
<RemitTo>SupplierA</RemitTo>
<SoldTo>BuyerB</SoldTo>
<ItemTotal>1000.00</ItemTotal>
<TaxTotal>150.00</TaxTotal>
<TransactionTotal>1150.00<TransactionTotal>
<SealedData>[signed data]
          </SealedData>
```

Figure 3 Converting an electronic invoice with single field encryption

10. How the Buyer Validates an Invoice Using Single Field Encryption

Upon receipt of the electronic invoice, either from the seller or from the intermediary, the buyer uses the seller's public key to validate the digital signature on the encrypted data field.

The buyer then *reconstructs* the string of designated data in the agreed format from Step 1, using data from the unencrypted fields in the invoice.

Using the same method from Step 2, the buyer calculates the hash digest for the reconstructed data string, converts it from binary to text, and compares the calculated hash digest to the hash digest transmitted in the encrypted/signed data field. If the two digests are identical, then the designated data in the unencrypted fields in the invoice are valid.

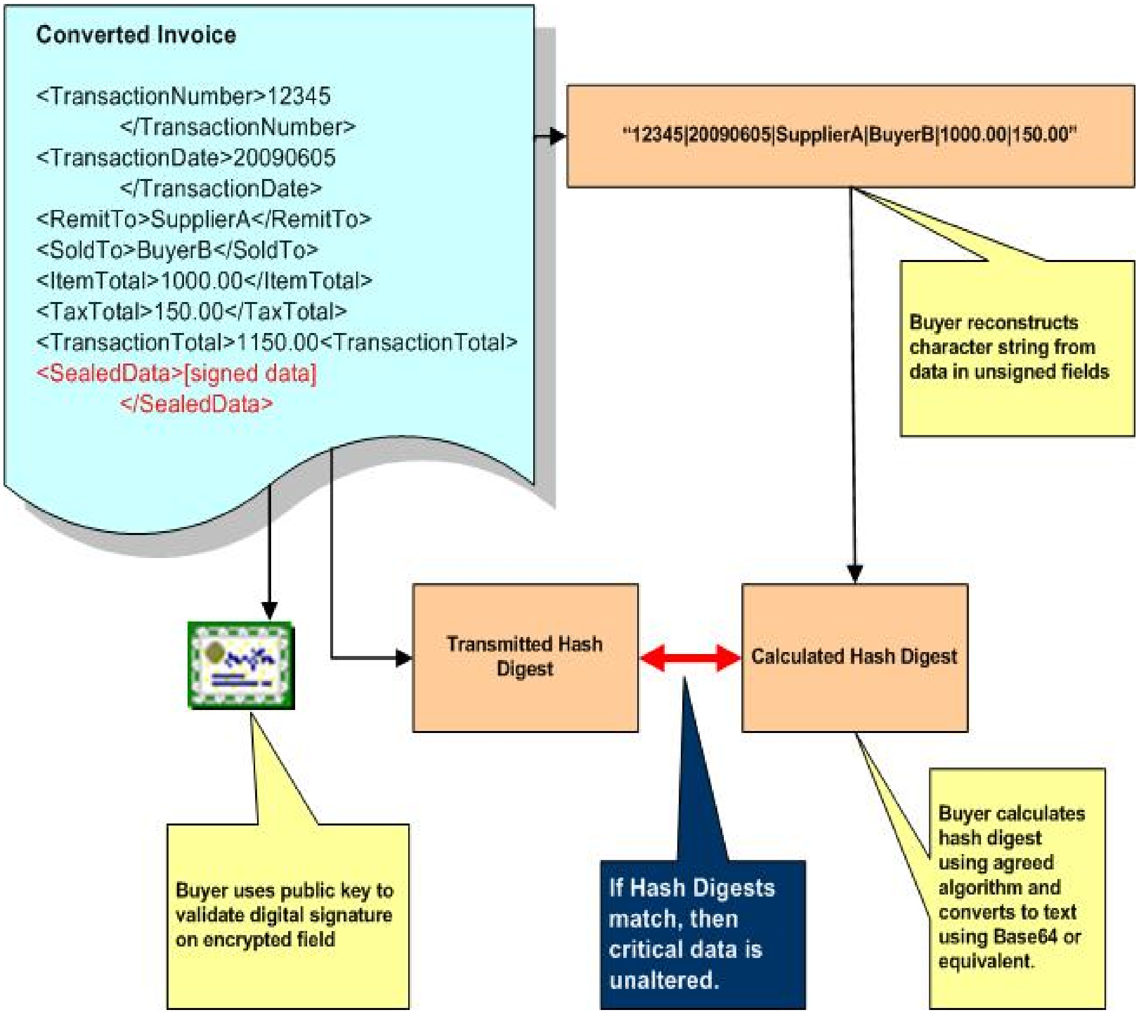

Converted Invoice
<TransactionNumber>12345 </TransactionNumber>
<TransactionDate>20090605 </TransactionDate>
<RemitTo>SupplierA</RemitTo>
<SoldTo>BuyerB</SoldTo>
<ItemTotal>1000.00</ItemTotal>
<TaxTotal>150.00</TaxTotal>
<TransactionTotal>1150.00<TransactionTotal>
<SealedData>[signed data] </SealedData>
"12345|20090605|SupplierA|BuyerB|1000.00|150.00"
Buyer reconstructs character string from data in unsigned fields
Transmitted Hash Digest
Calculated Hash Digest
Buyer uses public key to validate digital signature on encrypted field
If Hash Digests match, then critical data is unaltered.
Buyer calculates hash digest using agreed algorithm and converts to text using Base64 or equivalent.

Figure 4 Validating an electronic invoice with single field encryption

At this point, the sender of the invoice has been verified, and the designated data within the invoice has been validated. The buyer can safely consume the invoice and the buyer's computers can automatically read the data from the individual, unencrypted XML fields.

Today, when a service provider converts an electronic invoice from one format to another, that service provider must "break" the advanced electronic signature of the sender in order to convert the invoice. The service provider must then attach its own advanced electronic signature to the invoice as a substitute for the sender's advanced electronic signature. This step represents the weakest link in today's electronic invoice chain: the recipient must rely on a third party's signature (not his trading partner's) and the legal negotiations surrounding the risk assumed by the service provider when affixing its signature can be costly and time consuming. This is especially true in the three corner model when the recipient's service provider is expected to convert the electronic invoice and has no prior contractual relationship to the sender. Single field encryption eliminates this "weak link" in the chain, by allowing the service provider to pass through the original sender's advanced electronic signature untouched while converting the remainder of the invoice. The buyer can better determine who is the true sender of the invoice and the sender need not pay a third party to apply its own signature to the electronic invoice. Single field encryption allows for more trustworthy and reliable authentication of electronic invoices as the buyer can open and save the advanced electronic signature of the actual sender, rather than just the signature of an intermediary service provider.

11. Mexico's Implementation of a Single Field Encryption Solution

On July 5, 2006 Mexico promulgated new regulations governing electronic invoices, which is commonly referred to as "Anexo 20"[2]. Anexo 20 implements a version of single field encryption for electronic invoices subject to Mexican federal tax.

Since 2006, the Mexican government, under Servicio de Administración Tributaria (SAT), has implemented single field encryption in their electronic tax documents. Currently, electronic invoices using single field encryption are being transmitted in Mexico at a rate in excess of 1 billion documents per year[3].

12. Parties May Employ a Multiple Field Encryption Solution

If, for example, there are multiple taxing authorities exercising jurisdiction over the transaction, each taxing authority may want a different string of data to be signed and encrypted. In that case, two fields in the invoice would be set aside and each would be populated with the specific string of data specified by the applicable taxing authorities. Those two fields would be separately signed and encrypted for the benefit of each taxing authority. Any service provider performing the conversion would simple pass the two encrypted fields without converting them and the recipient would be able to open both "signed" fields upon receipt.

13. Conclusion

The proliferation of multiple format standards and transmission protocols for electronic invoices makes adoption difficult for small and medium enterprises. They often need the assistance of an outside service provider to convert electronic documents between the different formats or protocols. The single field encryption method ensures the authenticity and validity of electronic invoices even when the electronic invoices have been converted.

Single field encryption has been implemented by the tax authorities of certain countries. For example, Mexico has used a version of single field encryption to secure federal tax documents since 2006.

Single field encryption works because it encrypts and signs *only* certain designated data values contained in the invoice, not the attributes, tags, or field names.

[2] See http://www.sat.gob.mx/sitio_internet/e_sat/comprobantes_fiscales/15_6534.html

[3] Interview of Antonio Obregon, Departmento de Comunicaciones y Tecnologias de Informacion, on 5 June, 2009, Mexico City. Mr. Obregon and Baltazar Rodríguez, Administrador Central de Transformación Tecnológica, are principal architects of Mexico's single field encryption approach.

14. About OFS Portal

OFS Portal is a group of diverse, worldwide suppliers working together with a non-profit objective to provide standardized electronic information to B2B trading partners to facilitate e-Commerce (www.ofs-portal.com). OFS Portal works with global standards organizations and trading partners to develop and improve open and non-proprietary e-Commerce standards in order to reduce costs to all participants in a technologically neutral manner. For more information about single field encryption or OFS Portal, please contact:

William Le Sage
OFS Portal, LLC
CEO
+1 (832) 681-7332
wlesage@ofs-portal.com

Dave Wallis
OFS Portal, LLC
EAM&FE Rep.
+44 (0) 7780700782
dwallis@ofs-portal.com