



Melbourne House
46 Aldwych
London
WC2B 4LL
Tel: +44 (0) 870 165 7410
Fax: +44 (0) 207 240 2696
www.ob10.com

OB10 - Digital Signing and Verification

Version 2.3

January 2011



Summary

In order to comply with the requirements of different tax jurisdictions, the OB10 e-Invoicing Service includes the functionality to digitally sign invoices. Features included are;

- Ability to sign a PDF invoice image or invoice data file with the latter being based on data recipient (buyer) criteria
- Ability to use different certificates for signing
- Ability to verify digital signatures

This document summarises the legal requirements for digitally signed documents and sets out how the digital signing process works and the methods that can be employed by recipients of digitally signed invoices to verify their integrity.



Table of Contents

1	Introduction	4
2	EC Directive 2006/112/EC.....	4
3	Advanced Electronic Signatures	4
3.1	OB10's Advanced Electronic Signatures	5
3.2	OB10's Digital Certificates	6
3.3	OB10's Secure Signing Device	6
4	OB10 Client Set-up	6
5	Signing Process	7
5.1	Signing and Verification Technology	7
5.2	PDF Image Signing	7
5.3	PDF Image Timestamping (Italian e-Archive)	8
5.4	File Signing – Switzerland	8
5.5	File Signing – Clients	8
6	Client Signature Verification	9
7	OB10 signature verification service.....	10
8	Installation of Certificates and verifying signatures	11
8.1	Verifying Signed PDF Documents	11
8.1.1	Download Certificate	11
8.1.2	Install Certificate into Adobe	11
8.1.3	Configure Adobe	13
8.1.4	Verifying Signed Data Files	14
8.2	Extended Invoice Verification	16
8.2.1	Signature Check	16
8.2.2	Go to www.signature-check.com	16
8.2.3	File Verification	17
8.2.4	Verification Report	18



1 Introduction

OB10 Limited utilises a process within the OB10 Service to digitally sign invoices where the legal jurisdiction requires it, or, if this is not the case, the client additionally requests it as an enhanced security feature. The signing process is secure and is entirely in the control of OB10.

The process has been implemented in a manner in order to meet the varying demands of international legislation and client requirements and enables the signing process to be invoked;

- based on the specific sender of the data or the intended recipient
- with different certificates based on the specific sender of the data or the intended recipient

2 EC Directive 2006/115/EC

On 20 December 2001 the European Commission issued Directive 2001/115/EC which laid down conditions for harmonising rules in respect of Value Added Tax. The Directive was to be implemented by member States by 1 January 2004 and later incorporated in to Council Directive 2006/112/EC ('the VAT Directive'). The Directive included provisions for electronic invoices delivered by EDI or secured by the use of an advanced electronic signature. The relevant text is as follows (The full text of the Directive is included in Appendix 1):

'Invoices issued pursuant to point (a) may be sent either on paper or, subject to an acceptance by the customer, by electronic means. Invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the contents are guaranteed:

- by means of an advanced electronic signature within the meaning of Article 2(2) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (****); Member States may however ask for the advanced electronic signature to be based on a qualified certificate and created by a secure signature-creation device, within the meaning of Article 2(6) and (10) of the aforementioned Directive;
- or by means of electronic data interchange (EDI) as defined in Article 2 of Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange (*****) when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data; however Member States may, subject to conditions which they lay down, require that an additional summary document on paper is necessary.'

The OB10 Service secures invoices by the use of advanced electronic signatures.

3 Advanced Electronic Signatures

On 13 December 1999 a community Framework was agreed for Electronic Signatures. The EU Directive states, that qualified, signatures and qualified time stamp, which are generated within an EU-country and have been accepted within this EU Country as a qualified signature (qualified time stamp) have to be accepted as a qualified signature (qualified time stamp) in any other EU-Country (see Article 7 of the EU Directive 1999/93/EC).

The definition of advanced electronic signatures laid out in the EU Directive 1999/93/EC. Relevant provisions cover the definition, requirements for qualified certificates and requirements for secure signature creation devices. The relevant text is as follows:



Article 2

Definitions

For the purpose of this Directive:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
2. "advanced electronic signature" means an electronic signature which meets the following requirements:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using means that the signatory can maintain under his sole control; and
 - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

- (a) an indication that the certificate is issued as a qualified certificate;
- (b) the identification of the certification-service-provider and the State in which it is established;
- (c) the name of the signatory or a pseudonym, which shall be identified as such;
- (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
- (e) signature-verification data which correspond to signature-creation data under the control of the signatory;
- (f) an indication of the beginning and end of the period of validity of the certificate;
- (g) the identity code of the certificate;
- (h) the advanced electronic signature of the certification-service-provider issuing it;
- (i) limitations on the scope of use of the certificate, if applicable; and
- (j) limits on the value of transactions for which the certificate can be used, if applicable.

ANNEX III

Requirements for secure signature-creation devices

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:

- (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
- (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.

2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.'

3.1 OB10's Advanced Electronic Signatures

OB10's advanced electronic signatures are applied to invoices using a digital certificate provided by TeleSec (Germany) or Swisscom (Switzerland) - see Section 3.2. Each signature is

- uniquely linked to OB10 and the OB10 service
- capable of identifying OB10 and the OB10 service
- created using a means that OB10 maintains under its sole control; and
- linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

OB10 clients receiving signed invoices are issued with the public signing keys. These are installed on the clients' computer to enable the signature on individual invoices to be verified.



3.2 OB10's Digital Certificates

For the signing of invoices under the OB10 service, OB10 uses a qualified, class 3 digital certificate provided by Telesec or Swisscom

- The TeleSec certificate complies with the requirements of the German BSI, www.bsi.de
- The Swisscom certificate complies with the requirements of the Swiss ELDI-V, www.estv.admin.ch

3.3 OB10's Secure Signing Device

OB10's advanced electronic signatures are applied to invoices using a secure signing device.

OB10's signing device ensures that:

- the signature-creation-data used for signature generation can practically occur only once, and that secrecy is reasonably assured;
- the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
- the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others

The secure signing device does not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

More details about signing are included in Section 5 below.

4 OB10 Client Set-up

During the set-up of each client the need to digitally sign the invoice is determined in one of two ways;

1. If the client is located in a country where there is a requirement to digitally sign invoices, the selection of this option is automatic
2. If the client is located in a country where there is no requirement to digitally sign invoices, the PDF image will be signed using the TeleSec signature

Once digital signing has been selected, the source certificate to perform the signing is required.

In order to prevent unauthorised access, the source certificates themselves are only accessible by a systems administrator. The system administrator is responsible for assigning particular certificates and is also responsible for requesting new / additional certificates as necessary.



5 Signing Process

5.1 Signing and Verification Technology

The technology used for signing and verification comprises of hardware and software.

The hardware used to read the digital certificates is CyberJack e-com Version 4 Smart Card Reader, manufactured by Reiner SCT

The software used to read the digital certificates and apply the digital signature is e-Billing signature server v2.8.0 manufactured by Authentidate Deutschland GmbH.

The software used to verify the digital signatures and apply the verification stamp is signature check server v2.8.0 manufactured by Authentidate Deutschland GmbH.

The hardware and software is registered with the Bundesnetzagentur in Germany.

5.2 Overview of Authentidate products deployed at OB10

The Authentidate signing software is designed in such a way that the issuance of an electronic signature does not depend on the content or semantics of the document data to be signed. For the document data, a special mathematic algorithm in the signature process creates a unique “fingerprint” (hash value) that is embedded in the signature, constituting a link between the document data and the signature. If the signed data is modified or manipulated, the determined hash value for the modified document changes, breaking the logical link to the issued signature. Whether the document data was changed or content is added is irrelevant.

Proof of the integrity and authenticity of the original invoice requires a so-called signature verification. Here it is checked, among other things, whether the certificate used for the signature was valid at the time of signature creation. To do so, it is checked whether the certificate owner was authorized to create the signature. At the same time, the signature verification documents the integrity of the data with a positive verification report.

Verifying electronic signatures requires the appropriate legally compliant software or a legally compliant signature verification service. OB10 employs the Authentidate Signature check server which is used to check signed documents on a large scale and generates reports in PDF, HTML or XML format.

5.3 PDF Image Signing

As part of its standard processing, the OB10 System produces a human readable invoice in a PDF format.

This PDF invoice is digitally signed according to regulatory requirements.

In invoice processing PDF invoices are moved to a directory monitored by Authentidate software. Each PDF file is picked up by the software which then accesses a Reiner SmartCard reader containing a smart card with the digital certificate. The software verifies the card with the entered PIN and, providing this is correct, creates a digital signature which the Authentidate software embeds within the PDF file.

In technical terms, the signature creation forms the hash value of a file. The hash value is a unique fingerprint of a file. The integrity of the file can be checked at any time by means of the hash value. Manipulations can then be detected. The harsh algorithms from the SHA-2 family are methods used



by the e-Billing signature server recommended by the Federal Network Agency and the Federal Office for Information Security (BSI) and published in the Federal Gazette.

For creating the signature the hash value is encrypted with the private code (PIN protected) of the signature creator. The signature file itself then contains:

- The encrypted hash value
- The certificate of the signature creator
- The certificate of the signature creator contains the public code for decrypting the encrypted hash value.

Successfully signed PDF files are moved to a 'signed' directory. These are then picked up by OB10's software process for collation, archive storage and onward delivery to clients.

5.4 PDF Image Timestamping (Italian e-Archive)

It is a requirement for e-Archiving in Italy that all e-invoices must be timestamped by an Authorised Timestamping Authority within 15 days of the invoice being archived.

All OB10 Italian PDF Invoice images are timestamped within 15 days of archiving by Authentidate International AG
Rethelstraße 47
40237 Düsseldorf
Germany
www.authentidate.de

Authentidate is formally approved for signing and timestamping by the German Authorities (Bundesnotar).

5.5 File Signing – Switzerland

All invoice data files generated for a Swiss recipient are moved to a directory monitored by the Authentidate software. Each file is picked up by the software which then accesses a Reiner SmartCard reader containing a Swisscom SmartCard. This verifies the card with the entered PIN and, providing this is correct, creates a signature.

Successfully signed data files and their corresponding signature files are moved to a 'signed' directory. These are then picked up by OB10's delivery software process for collation and onward delivery to clients.

5.6 File Signing – Clients

This is an 'on-request only' service and is implemented in a bespoke configuration at a client's request. Prior to the signing process being instigated, the OB10 delivery system generates the required input files (e.g. a client may want their data files and corresponding image files zipped together to create a single file). The files are moved to a directory monitored by the Authentidate software. Each file is picked up by the software which then accesses a Reiner SmartCard reader containing a smart card with the digital certificate. This verifies the card with the entered PIN and, providing this is correct, creates a signature.

Successfully signed data files and their corresponding signature files are moved to a 'signed' directory. These are then picked up by OB10's delivery software process for collation and onward delivery to clients.



6 Client Signature Verification

When an invoice is received, the recipient can view the invoice image and also the certificate that was used in the signing process. If a warning message or error is displayed when opening the image it indicates a verification failure. This check of the signed data consists of an integrity check and online verification.

Automatic signature verification using the signature check server

The automatic signature verification implemented in the Signature Check Server consists of three steps: an integrity check, a local verification and the online validation of the signature.

Integrity check

In the Integrity check the encrypted hash value of the file is decrypted with the public code contained in the certificate. The mere possibility of decryption with the public code ensures the authenticity of the signature and the invoice.

The hash value of the invoice file is then determined and compares against the decrypted hash value in the signature file. A match between the two hash values confirms that the file has not been changed.

Local verification

After the integrity check, the certificates included in the signature will be mathematically verified to ensure the integrity of the signature.

Online validation

Besides the integrity check and local verification, online checks are made to determine whether the certificates used in the signature were available and not revoked at the time of the signature creation. For this purpose a connection is made to each of the OCSP responders in the certificate path and the status of the certificates queried.

Based on the result the Signature Check Server generates the verification report in the different possible formats and languages. This method has the advantage that communication between the Signature Check Server and the Signature Check Webservice is uniformly encrypted via HTTPS. Communication to the OCSP responders of the issuers and root occurs through the signature Check Webservice and need not be noted by the customer.

Manual signature verification using of signature –check.de/signature –check.com

In the described scenario the invoice recipient receives the result of the signature verification report in the different possible formats and languages. This method has the advantage that the communication between the Signature Check Server and the Signature Check Webservice is uniformly encrypted via HTTPS. Communication to the OCSP responders of the and root occurs through the Signature Check Webservice and need not be noted by the customer.

No additional software is required to be installed.

The signature check server:

- Checks the integrity of the document through the formation of the hash value and check of the "matchup" of the signature.
- Validation of the certificate path through the emulation of the certificate chain and comparison of the root certificate against a defined trustworthy anchor for certificates compliant with signature law.
- Check validity of the certificate at the time of signature creation through an online status query of the certification service provider.



There are three main causes of verification failure. These are;

1. the certificate used to sign the image is not trusted. This is overcome by installing the public signing keys
2. the certificate is not yet or no longer valid. The certificate used by the OB10 Service will be within its validity period when it is sent, however, if the image is viewed at a later date and after the expiry of the validity period, an error will be seen. This is not a severe validation failure as it can be easily established that the certificate was valid when the invoice was signed. Where the certificate issuer is OB10 it is ensured that the expiry date of the certificate is always after the maximum legal retention period of the invoice.
3. the content has been altered after the digital signing took place. This is a severe verification failure and indicates that the data cannot be trusted.

7 OB10 signature verification service

If the client requires it, OB10 can perform the signature verification process on behalf of the client.

During invoice processing, digitally signed invoices that require signature verification are moved to a directory monitored by Authentidate software.

For each PDF invoice, the Authentidate software;

- i. checks the date validity of the signing certificate
- ii. checks the integrity of the document to ensure it has not been modified since the signature was applied
- iii. places an Online Certificate Status Protocol (OCSP) call to the Telesec or Swisscom servers to determine if the digital certificate was revoked at the time of signing the document.

If the Telesec servers confirm that the digital certificate used for the signing has not been revoked then a verification report is added to the digitally signed PDF invoice.



8 Installation of Certificates and verifying signatures

In order to validate a digital signature, the public element of the signature is used. To ensure the integrity of the process, this must be obtained from a verifiable and reputable source.

OB10 provides the public certificate elements as downloadable items from www.ob10.com

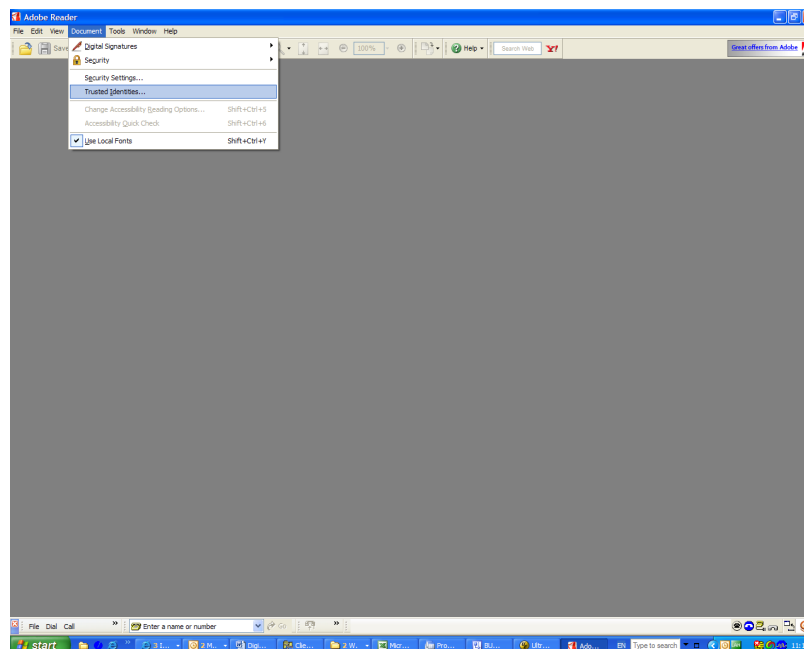
8.1 Verifying Signed PDF Documents

8.1.1 Download Certificate

Go to ob10.com and click "Contact Us" and then Customer Downloads. Download file OB10Signing.p7c

8.1.2 Install Certificate into Adobe

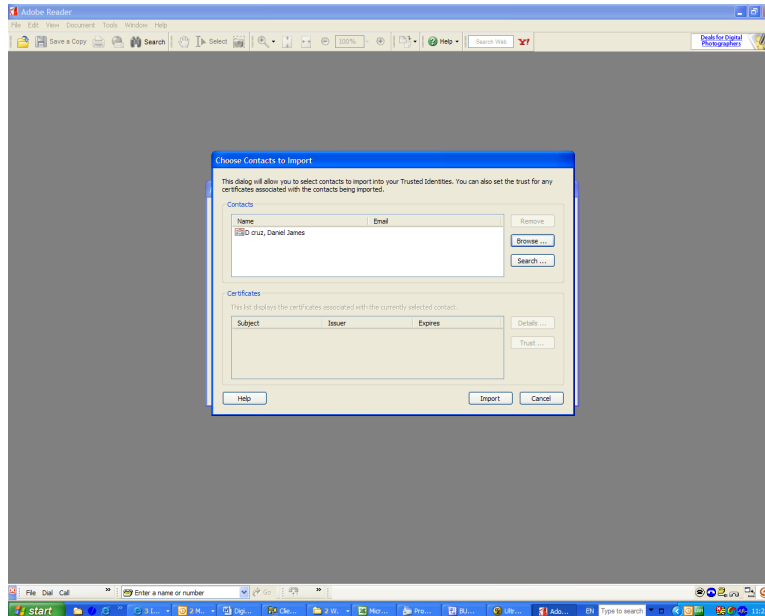
Open Adobe Reader (this must be version 7.0 or above) and go to Documents, Trusted Identities. For Adobe 10 users and above, go to Edit, Managed trusted identities.





Select 'Add Contacts' and then 'Browse', locating the file downloaded at step 8.1.1

Once located, highlight the file and then click on Open. You should see a screen similar to that shown below;



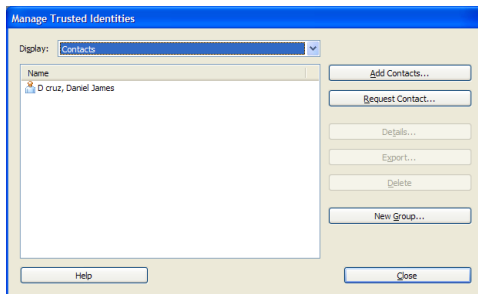
Click on 'Import' and this will install the contact and its corresponding certificate into Adobe Reader. The contact and their associated certificate certificates are employees of OB10, authorised to digitally sign invoices on behalf of the company.

You may need to download and install more than one contact as OB10 uses a number of approved certificates at any one time. For each contact/certificate, repeat the steps described in this section and section 8.1.3

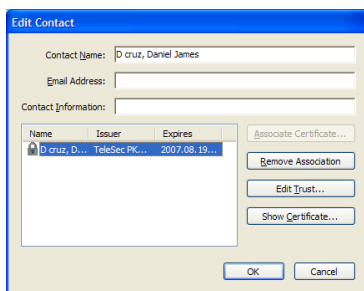


8.1.3 Configure Adobe

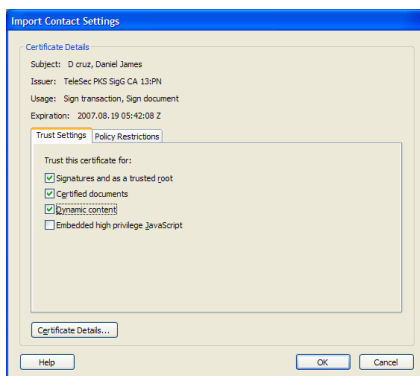
From the 'Trusted Identities' menu, highlight the installed contact (D Cruz, Daniel James) and click on 'Details';



Highlight the certificate and click on 'Edit Trust';



Check the three boxes as shown below and click on OK




Adobe Reader is now configured to verify PDF documents signed by OB10

8.1.4 Verifying Signed Data Files

PDF invoice images created by OB10 show a signature status on the bottom left-hand edge of the first page, as highlighted by the red circle below;

1 1		Discount %	0	Discount Amount	0.000
Discount		On if paid 30 days from invoice date		Tax Type	
Original Invoice No.				VAT at 17.5%	
Invoice Payment Information		Payment to be made as normal		VAT Amount	
Supplier Tax Registration Num.		ASC120		1.75	
Buyer Tax Registration Num.		94-1061430		Taxable Amount	
Supplier Company Registration Number		1200/Reg. City		10.00	
Country Level Ref.		12045 EUR		Net Value	
Supplier Data 1		If you have any queries on this invoice please telephone: 07950		10.00	
Supplier Data 2		002340		VAT Value	
Bank Name		Not Entered		1.75	
Bank Address				Gross Value	
Bank Sort Code				11.75	
Bank Account Number		01120560			
Account Name					
SWIFT Number					
OB10 e-Invoice			www.ob10.com		



Check the signature for free
AuthentiDate
 www.signature-check.com

Please Note: Verification of contained qualified signature requires specific information. Verification by using only Adobe Reader's internal standard verification engine may fail. Therefore please use free verification service at www.signature-check.com.

Clicking on the signature icon launches the Adobe Reader signature verification process;

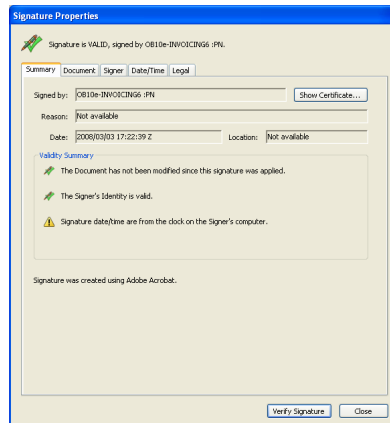
Signature Validation Status

 Signature is VALID, signed by OB10e-INVOICING6 :PN.
 - The Document has not been modified since this signature was applied.
 - The Signer's Identity is valid.

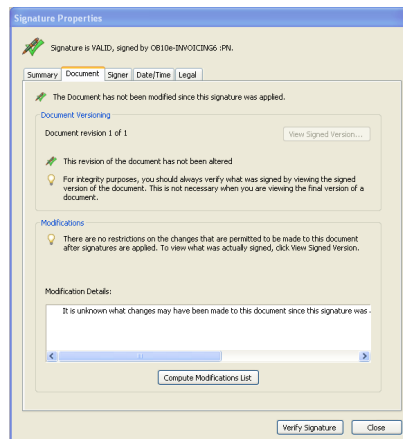
This first step indicates that the signature is valid (i.e. you trust the signer OB10) and the document has not been modified since the signature was applied. No further checking is required so you can click 'Close'. More details relating to the signature can be found if you click on 'Signature Properties'.



This opens up a dialogue box similar to the one shown below and allows you to find out more information about the document and the signature;



Note: when checking the document section, although the top half correctly reports that no modifications have been made to the document since the signature was applied, the lower section implies that changes may have been made and, if you click on 'Compute Modifications List', 4 miscellaneous changes are reported. These relate to the signature icon, allowing you to visibly see that the signature is OK by showing a green tick icon (as shown on the following page) and do not compromise the documents integrity.




8.2 Extended Invoice Verification

8.2.1 Signature Check

Should a customer wish to check that the certificate was in date when used to sign the document, they can use signature check. Signature check is a web based service that allows for the verification of digitally signed signatures and qualified time stamps.

8.2.2 Go to www.signature-check.com


Click "Start" on the homepage.



The screenshot shows the homepage of the Signature-Check website. At the top right is the logo "Signature-Check" with a green and red circular icon. Below the logo are navigation links: "Home", "Instruction", "FAQ", "Contact", "Support", and "Test data". On the left side, there is a grid of logos for various participating companies, including alpha, BOSCH, DELICom, HETRO Group, En3lu, GHX, GRACE, HAYS, HUBVCO, JPMorgan, and MBG. A large image of four business professionals looking at a laptop is positioned in the center. Below this image is a green banner with the text "Do you have digital signed documents? Here you may easily verify your documents & invoices!". To the left of this banner is a large orange "START" button. Below the button is a link: "Click here to start signature-verification 'Start'-button opens a new window". To the right of the button is a section titled "Do you receive electronic invoices?" with text explaining VAT regulations and how Signature-Check verifies signatures. Below this is another link: "This way to the test data ...". At the bottom of the page, there is a footer with the text "© 2010 AuthentiDate" and "Start | Contact | Privacy Statement | Legal notice".

8.2.3 File Verification

Select the PDF required for verification and click start verification.

Signature-Check 

Simple signature verification in a few steps only

1	<input type="text" value="H:\Workgroups\WAT and Tax\Sampl"/> <input type="button" value="Browse..."/>	Please choose the file for which the corresponding signature is to be verified. Should the file exceed 350kb, please use the Java-Applet.
2	<input type="text"/> <input type="button" value="Browse..."/>	Please choose the corresponding signature-file (.ads or .cms). In case the signature is integrated in the document, please just leave a blank.
3	<input checked="" type="radio"/> PDF <input type="radio"/> HTML	Please select the format for the verification report.
4	<input type="button" value="Start verification"/>	Please start the signature verification. The result can be saved or printed.



8.2.4 Verification Report

Signature check then produces a report providing details on whether the verification has been successful. It checks whether the hash value of the signed document created in the certified trust centre matches with the signature file. This proves the integrity of the data. The validity of the certificate, which was used to create the signature, is also checked via an online request to the issuer of the certificate. The centralised system is located at a certified trust centre which is managed by Authentidate. Authentidate is an accredited certification service pursuant to the German Signature Act and European Signature Regulations.

VerificationReport

Signature-Check
Your Signature Verification Service at <http://www.signature-check.de>
Verification Report for digital Signatures

Verification Date/Time:	2/25/10	3:57:02 PM UTC
Filename, signed file:	AAA000009961263.pdf	
Filename, signature file:		
HASH-Value, signed file:	569c9d379c35f49e5d2ef56abc42f986d272ae80	

Summary Signature Verification

File OK	Online verification successful
---------	--------------------------------

One of the algorithms used has become too weak.

Verificationlevel achieved 7

!The signature could be decoded successfully. Furthermore all certificates in the signature container could be mathematically checked for correctness. Additionally it is guaranteed the signer signed the signature with the key of his signature. The certificate path was checked. Also the check whether the signer certificate was valid during the signing time was performed successful. Furthermore it was successful verified that, the signers certificate and all superordinated certificates were shown as valid by the issuing certificate authority during signing time.!

The assessment of the algorithms used is based on the catalogue "SigG Algorithmenkatalog".

The algorithm SHA1withRSA / 2048 (SignerInfo[0].SignatureAlgorithm) on which the signature is based lost its eligibility for creating qualified electronic signatures on Thu Jan 01 00:59:59 UTC 2009 and thus after its use.

The algorithm SHA1 (SignerInfo[0].DigestAlgorithm) on which the signature is based lost its eligibility for creating qualified electronic signatures on Tue Jul 01 00:59:59 UTC 2008 and thus after its use.

The present signature is therefore a qualified electronic signature within the meaning of § 2 no. 3 of the Digital Signature Act (SigG.) with diminished probative value with regard to the authenticity and integrity of the related document. This could be counteracted by oversigning before the date on which the algorithm lost its eligibility in accordance with § 17 of the Digital Signature Ordinance (SigV).

Details of Signature

Format profile:	ISIS-MTT SigG
-----------------	---------------