

Banana.ch

Securing Accounting Data

January 2002

Note regarding the document publication in 2018

Domenico Zucchetti has prepared this document during 2001 / 2002, with the purpose of explaining the new certification technology to the people involved in the process of preparing the [patent application](#) and [verifying the compliance with the new Swiss rules](#) (linked document in German).

The method presented in the document and used in Banana Accounting software since 2002, is the first one to use the blockchain technology in the accounting and business world. Following a request of people interested in understanding how the technology was born, we decided to make the document public in 2018. No changes have been made, except for this note and the correction of a few typo errors.

The content is still pertinent and useful, especially regarding the accounting section. Meanwhile the MD5 algorithm is no longer considered secure. Current versions of Banana Accounting software use the SHA-256 algorithm. For long-term archival purposes, the PDF format is available next to the html.

Summary

Electronic Document Certification and Digital Signature	4
Content Certification	4
Digital Signature Certificate	4
Certificate Authorities	5
Passive Security of Accounting Data	6
Electronic Signature Legislation	6
Legal Framework for Electronic Documents	6
Preserving Certification Codes	7
Accounting Rules	7
True Evidence	8
Timely Manner	8
Filing Accounting Data	8
Accounting Organization and Auditing	9
Threat to Accounting Security	9
Reconsidering Accounting Security	10
Considering Different Aspects	10
Modifying Transactions	11
Using Certification Technique	11
Filing Data	11
Accounting Organization	11
Legal Requirements	12
The Active Security Technique Introduced by Banana.ch	13
Integrated Data Certification	13
Long-Term Electronic Storage	15
Legal Evaluation of the Active Security Functions	17
Using New Security for Banana Accounting	18
General Organisation Protocol (Switzerland)	19
Advantage of Active Security	20
Summary of the active Security functions	21
Technical Details	22

Securing Accounting Data

Legislation regarding the legal validity of electronic documents is changing all over the world. In order to have an electronic document legally recognized, new security techniques (certification) will have to be adopted, the accounting world included.

Banana.ch has developed a new, very simple technique that permits certification of live accounting data. Prior to this invention certification techniques could only be used with data sets that were final. Since new transactions are being added to an accounting continuously, certification of the accounting file could not be made until the accounting year was closed and made final.

This Banana.ch innovation permits the use of certification in the accounting world. Data integrity can be ensured in any environment even when accounting data is modified and transferred on unsecured computers. Accounting data can be certified, signed and legally recognized just like any other electronic document. This level of security and data integrity should surpass most current legal specifications. The accounting results should therefore be accepted in most countries of the world.

This document is intended to offer an in-depth explanation of the following themes:

- Electronic document certification and signature
- Legal framework for electronic documents
- Standard accounting principles affecting data security and conservation
- Certification techniques applied to the accounting system
- Long-term electronic storage of accounting data
- Technical specifications of the active security systems of Banana.ch

About the Author

Domenico Zucchetti completed business school and received a university degree in law from the University of St. Gallen, Switzerland in 1987. The thesis he presented at the end of his studies was on the theme "The contract between data bank provider and user". Mr. Zucchetti, founder and president of Banana.ch, is an expert programmer who has mastered C++ and other new technology. Prior to founding Banana.ch he was responsible for central credit administration at a primary Swiss bank.

Banana Accounting, an easy-to-use, low-cost, general accounting software, is aimed at small companies and clubs all over the world. In the year 2000, Banana Accounting was selected as one of five finalists by the Codie Awards jury (equivalent to the software Oscar) who judge the world's finest software packages.

Electronic Document Certification and Digital Signature

Electronic documents are increasingly becoming part of business practice. People need to be able to trust electronic documents. Today, many countries already consider an electronic signature to be legally binding. The process of signing an electronic document is, however, totally different from the one used for paper-based documents as there have to be different aspects in the process of certifying and signing a document:

- It must be possible to be absolutely certain the content of a document has not been altered after it was approved (evidence of integrity).
- It ought to be possible to validate the electronic signature. It should be possible to verify the identity of the signer (evidence of identity) and the validity of the signature (evidence of the intent to authenticate).

Content Certification

Computers can easily process the entire content of an electronic document. Two documents can be compared to see if there are any differences. It is also possible to compute a certification code that uniquely identifies a document. If any part of the document has been modified (if data has been displaced, changed, deleted, inserted), a new code will be generated. To check that the document has not been changed, a code is computed again and compared to the original one. If the codes are the same, the document has the original content. By using this system it will always be possible to check the integrity of a document.

This certification technique can be applied to any kind of document (text, images, music, video), large or small. A single code can also be computed to include different documents. The use of a code is practical because only a small piece of data need be stored or sent to ensure the validity of the document. This kind of code-based certification is extremely secure. With a typical code using 128bit there is one chance in thousands of billions that a different document will have the same code.

Code-based certification is the basis of digital signature technology and all modern certification and security systems.

Digital Signature Certificate

A signature is a mark used to authenticate. A signature is simply a name on a paper, a fax or an email. In the paper-based world, special recognition is given to a handwritten signature that is always the same. In the electronic world, such a constant and graphic signature could easily be copied and misused. To prevent duplication an electronic signature needs to be made specific to a document.

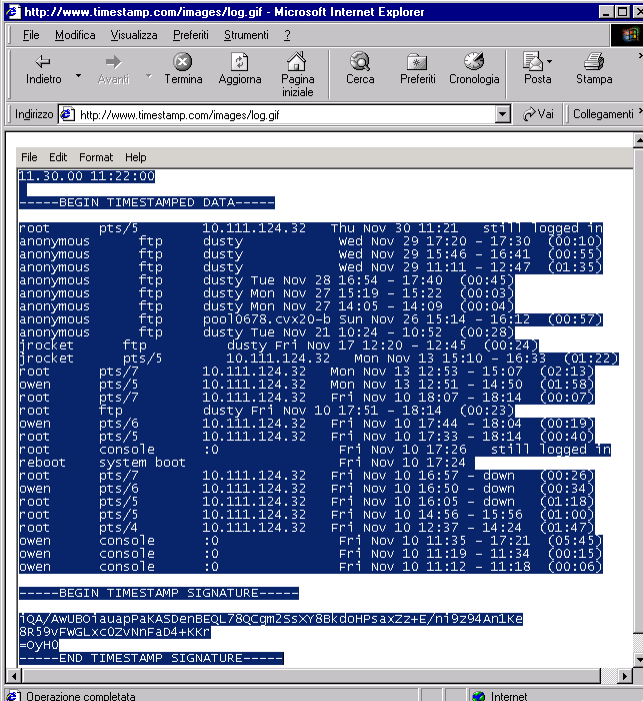
A digital signature certificate is a computed "code" based on personal identity (digital ID) and the content of the document. The signature will therefore be unique both to the individual and to the document. For each document and for each person, there will be different codes.

In order to sign a document, personal identification is required. A personal certificate (digital ID) is usually a two part data sequence that is unique to a person. The personal certificate has both a private and a public part. The private part is used to compute a signature and should therefore be kept secret (often on a chip card). The public part of the digital ID is used to check and validate the signature. The public part is thus made freely available.

There are other means of identification based on other techniques e.g., PIN, access codes, or on biometric data (fingerprints, retinal scans).

Certificate Authorities

Certificate authorities are entities that issue certificates and are similar to notaries. Certificate authorities issue identity certificates and certify that a personal certificate belongs to a specific individual. Certificate authorities can also issue other types of certificates. The timestamp certificate, for example, states that a certain message or transaction occurred at a specific time.



```

http://www.timestamp.com/images/log.gif - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Avanti Termina Aggiorna Pagina iniziale Cerca Preferiti Cronologia Posta Stampa
Inglizso http://www.timestamp.com/images/log.gif Vai Collegamenti

File Edit Format Help
11.30.00 11:22:00
-----BEGIN TIMESTAMPED DATA-----
root pts/5 10.111.124.32 Thu Nov 30 11:21 still logged in
anonymous ftp dusty wed Nov 29 17:20 - 17:30 (00:10)
anonymous ftp dusty wed Nov 29 15:46 - 16:41 (00:55)
anonymous ftp dusty wed Nov 29 11:11 - 12:47 (01:35)
anonymous ftp dusty Tue Nov 28 16:54 - 17:40 (00:45)
anonymous ftp dusty Mon Nov 27 15:19 - 15:22 (00:03)
anonymous ftp dusty Mon Nov 27 14:05 - 14:09 (00:04)
anonymous ftp pool0678.cvx20-b Sun Nov 26 13:14 - 16:12 (00:57)
anonymous ftp dusty Tue Nov 21 10:24 - 10:52 (00:28)
jrocket ftp dusty Fri Nov 17 12:20 - 12:45 (00:24)
jrocket pts/5 10.111.124.32 Mon Nov 13 15:10 - 16:33 (01:22)
root pts/7 10.111.124.32 Mon Nov 13 12:53 - 15:07 (02:13)
owen pts/5 10.111.124.32 Mon Nov 13 12:51 - 14:50 (01:58)
root pts/7 10.111.124.32 Fri Nov 10 18:07 - 18:14 (00:07)
root ftp dusty Fri Nov 10 17:51 - 18:14 (00:23)
owen pts/6 10.111.124.32 Fri Nov 10 17:44 - 18:04 (00:19)
root pts/5 10.111.124.32 Fri Nov 10 17:33 - 18:14 (00:40)
root console :0 Fri Nov 10 17:26 still logged in
reboot system boot Fri Nov 10 17:24
root pts/7 10.111.124.32 Fri Nov 10 16:57 - down (00:26)
owen pts/6 10.111.124.32 Fri Nov 10 16:50 - down (00:34)
root pts/5 10.111.124.32 Fri Nov 10 16:05 - down (01:18)
root pts/5 10.111.124.32 Fri Nov 10 14:56 - 15:56 (01:00)
root pts/4 10.111.124.32 Fri Nov 10 12:37 - 14:24 (01:47)
owen console :0 Fri Nov 10 11:35 - 17:21 (05:45)
owen console :0 Fri Nov 10 11:19 - 11:34 (00:15)
owen console :0 Fri Nov 10 11:12 - 11:18 (00:06)
-----BEGIN TIMESTAMP SIGNATURE-----
1QA/AwUB01auapPaKASDenBEQL78QCqm2SSxY8Bkd0HPsaXz2+E/n19z94AnLK6
8R59vFWGLxc0ZvNnFad4+KKr
=OyH0
-----END TIMESTAMP SIGNATURE-----
Operazione completata Internet

```

Certificate authorities are central to the process of certification. Legislators define their role, procedure, responsibility and liability in cases of fraud or error on the part of the certification authority.

Passive Security of Accounting Data

Defense systems only allow authorized personnel to have access to the accounting data, to be able to enter data and make changes. Security can be bypassed intentionally or unintentionally. An incorrect program could wrongly modify the data. Passive security:

- requires that data remains in a protected environment.
- requires a clear distinction between the person who oversees security and the people who use the data
- must be in place to ensure that the accounting data is only entered by authorized individuals
- is an important organization measure that ensures the quality of an accounting and safeguards the accounting data,

But passive security cannot offer full evidence of the integrity of the information.

Electronic Signature Legislation

There are basically three approaches that legislators have followed in order to define a valid digital signature:

- All electronic signatures are valid legal signatures.
- Electronic signatures are valid when they possess certain security attributes. The most restrictive legislation requires that a signature should be: unique to the person using it; capable of verification; under the sole control of the person using it; linked to the data in such a way that if the data is changed, the signature is invalidated. Others only prescribe that the method should be appropriate to the purpose for which the message was generated (UNICTRAL Model law).
- Only digital signature certificates are considered valid legal signatures.

Different countries and different states have regulated electronic signatures in different ways. A signature that may be valid in one country may not be valid in another. This varied approach will probably persist.

Legal Framework for Electronic Documents

From a legal point of view there are basically three types of electronic data:

- Any type of electronic data,
- Authenticated original data. Data for which a reliable assurance exists as to the integrity of the information from the time it was first generated to its final form.
- Signed electronic data. Where a reliable method exists to identify the person who approved the information contained in the document. If an electronic signature is considered to be a valid method of signature, then a signed electronic document is normally considered to be the legal equivalent of a paper document.

Basically, with new legislation, all electronic content should be considered valid written content. This principle may not apply in a specific case. A particular law may still require paper-based documents or qualified electronic documents. The legal validity of stored data may differ greatly and should be verified for each specific use.

Electronic documents and passive security cannot offer evidence of integrity on their own. Only by using certification and signature techniques is it possible to give full evidence of the integrity of the data.

There is no doubt that certified data can be considered far more secure from a legal point of view. The outcome of a trial or litigation may depend on the possibility to certify the integrity of the data. Legislation mostly accepts that accounting data is preserved on electronic media but also states that this data should not be modified. Certified documents may also be considered the only valid way to preserve data when evidence of integrity is required by the law. That may be the case for accounting data as well.

Preserving Certification Codes

To prove that a document has not been altered, it is necessary to keep the certification code in a form that can bring evidence to bear that the code is the original one.

The date of the code calculation should be preserved. As time passes it will always be possible to prove that a code already existed when the data was made final.

The certification code and the date of first calculation should therefore be authenticated in an appropriate way.

The code can be printed and the paper document authenticated by a notary in the traditional way. The code could also be mailed to an electronic certification center that will issue an electronic certificate that can always be checked online.

An easier way to "authenticate" the code and the date would consist in printing the code on paper and then having it signed by an auditor or by a company representative.

In some countries official forms are still in use. In such cases the code should be printed on these forms or annotated in a company book.

Accounting Rules

Accounting is fundamental to all proper administration. Keeping the accounts is mandatory for a large number of entities. Accounting is also the basis for tax collection, income calculation and determines the binding credit/debit positions of a company or individuals. The accounting as a

whole is a legally binding instrument. All countries have legislation that prescribes exactly how accounts should be kept. Tax regulations influence how transactions should be calculated and recorded as well.

All over the world accounting practice is standardized. The fundamental rules of accounting are:

- Accounting should give correct and true evidence of all transactions and of the financial situation. Principle of understandability, relevance, reliability, comparability, consistency indicated by the International Accounting Standard (IAS) and US Generally Accepted Accounting Principles (GAAP).
- Accounting should be kept in a timely manner.
- Accounting should be organized according to the size and needs of the company.
- Accounting is a legal document, should not be modified and should be preserved over time.
- Management is directly responsible for the accounting.

True Evidence

- Every transaction that influences the financial position of a company must be recorded.
- For every transaction there must be a document that supports the operation (invoice, receipt)
- Transactions must be recorded according to generally accepted accounting standards and fiscal accounting rules.
- If a transaction is not correct it should be rectified.

Timely Manner

Accounting should be kept on a regular basis. Accounting data and results should be made available in a timely manner.

Countries have similar regulations but with different time frames:

- Transactions should be registered within a certain amount of time from the time the transaction occurred.
- Balance Sheets and Income Statements should be completed within a specific amount of time after the close of the year.
- Tax legislation has deadlines. All transactions for a given period should be registered before filing a tax form.

Filing Accounting Data

- Accounting documents and data have to be kept for years.
- Accounting is a legal document and cannot be changed.
- Companies have to preserve and protect these documents.

Accounting Organization and Auditing

Accounting organization is very important in assessing the correctness of the accounting.

Accounting consists of a precise recording of each transaction. The quality of the accounting work can be checked by controlling that the transactions have been entered and conform to the documents.

In small organizations, few people are responsible for accounting. It is easy to verify that the work has been properly organized and whether all documents have been taken into consideration. It is simple to compare documents with the recorded transactions.

In large organizations with a large number of transactions, it is not possible to control all the records and all the documents. In large entities there are many individuals who supply information. This work must be properly coordinated, secured and checked.

Small companies will have a simple organization whereas large companies will have a structured and complex organization.

In certain cases, depending on legislation within the country and the legal form of the entity, the accounting needs to be audited and certified. The primary scope of the auditing process is to assess whether the accounting has been properly organized and whether it gives true evidence of the actual situation of the company.

Threat to Accounting Security

Paper-based accounting systems have evolved towards the use of accounting books. Pages and transactions are numbered sequentially. At the end of the page there is a sum of all transactions and this amount is carried forward to the next page. Accounting books provide a quite secure system. Accounting books can be easily read and filing poses no technical problems.

Computers have made it much easier to record transactions. Computerized systems instantly calculate the Balance Sheet and Income Statements. With an electronically based solution we never see the effective electronic document. We only see a copy represented on paper or on a screen.

Different problems arise:

- Electronic content is not bound to a support.
- Electronic data can be changed.
- Electronic data can be copied and replicated. Copies are totally similar to the original.
- Data filed on electronic media cannot be directly read by human beings. A technical process is necessary in order to access and view the information.

Reconsidering Accounting Security

The change from paper-based accounting to a computer-based accounting system requires that the security and legal validity of accounting data should be reconsidered.

The integrity of an electronic document is a fundamental requirement for the validity of a digital signature. If a document is changed the authenticity of the document is lost and the digital signature is no longer valid. A certification technique is the central criteria through which the law considers an electronic document to be valid.

A passive security system (password protection), as used in accounting systems, does not bring to bear total evidence of the integrity and authenticity of the content. A software failure may change the information. A passive security system will not detect such changes. Therefore passive security systems are not considered to be a valid technique to authenticate and sign electronic content by law.

The integrity of accounting data is fundamental to the validity of an accounting system. The law requires that the integrity of electronic content needs to be ensured through a certification technique. Access and password protection used on accounting systems should no longer be considered sufficient to ensure the integrity and legal validity of accounting data. From a legal point of view a new approach to accounting data security is needed.

Considering Different Aspects

In defining what should be a new approach to data security all aspects of the accounting work should be examined.

- Data security should enhance and not diminish generally accepted accounting principles.
- Data security and integrity should be measurable and independent from individual behaviour, computer systems or dimension of the organization.
- Security should be considered to facilitate the accounting task.
- A security system should be part of the whole accounting system and facilitate and allow for better organization of the accounting task.
- Security systems should support differing legal requirements .
- The system should provide the data with a form that can be certified and digitally signed.
- Accounting data should be continuously secure and readable for years without any particular technical intervention.

Modifying Transactions

The recording of accounting transactions should exactly reflect the nature of these transactions.

Most accounting software permits entering a transaction in a provisional journal. Before making them final, transactions can be checked and corrected with no need to create a reverse transaction. The accounting therefore becomes more readable.

To ensure the necessary quality, an accounting system should allow users to enter, check and edit the transactions before they are made final. At what time it becomes necessary to make the transactions final will depend on the accounting organization. Once the transactions have been finalized, then no changes should be allowed and the system should be able to give evidence of the integrity of the data.

Using Certification Technique

Documents certified and signed with a code-based certification technique are considered valid legal documents. Accounting data secured by such systems can be considered valid legal documents.

Certification technique is the way to go when developing security for accounting data.

Filing Data

Accounting data should be stored and constantly available for at least 10 years usually. The accounting organization should properly file and preserve the accounting data. Accounting data should always be accessible even if the computer system is changed. If the data is stored on external media, it should always be possible to have access and to be able to read the accounting data in a proper fashion.

Accounting Organization

It is up to management to organize the accounting system. If legislation is changed the organization should also be adapted. The security and integrity of the accounting data depends on how the computer system is conceived and maintained. Access to the data depends on individual behaviour and on the computer system. Accounting data should be kept secure and should be protected from unauthorized use. Backup copies should be available in case of data loss or security abuse.

The organization and system security should conform to the size of the company and its legal requirements.

Code-based data certification does not replace other security measures.

Data certification permits the detection of any changes, even ones caused by software or technical failure. Data certification ensures data integrity even

when data is restored or sent to another computer. Certification systems thus help to better organize accounting and keep the whole system totally secure.

Legal Requirements

Regulations regarding accounting or electronic documents differ from one nation to another. Different regulations also apply for different uses of the data. The law usually considers it adequate to store accounting data in electronic form. Different legislation may insist that for use in court, the data should bring full evidence of integrity. Accounting data should be conserved and not changed over time. This may sound equivalent to a data integrity requirement. The accounting information may be used for legal purposes where integrity is absolutely necessary. From different legal points of view, it appears that accounting data should also be certified and certifiable. Data certification can detect technical failure or intrusion into a system. Data certification may be an organisational requisite that ensures that the security system does not fail. By using a data certification technique, the same as the one used for electronic document certification, validity of accounting data becomes far more secure and incontestable. The law requires that data be stored and kept available for years. From a legal point of view accounting information should be stored in a final format that can be certified electronically and read at any time without technical intervention.

The Active Security Technique Introduced by Banana.ch

New legal requirements require that accounting software use active data security and certification techniques. Data certification should be an integral part of the accounting software. The integrity of the accounting data should be easily preserved and demonstrated.

Long-term data storage should also be part of the accounting solution. Banana.ch has invented a new data security technique that allows certification of live databases.

Thanks to this technical achievement, Banana.ch has introduced to Banana Accounting 4.0 what can be considered the first full series of measures that will make accounting software secure and prepared for any new and future legal requirements.

Integrated Data Certification

Data certification could only be used in an environment where the data set was immutable. If a document needs to be changed due to the addition of new transactions, the certification code for the data set changes continuously. Data certification techniques cannot be used in the accounting environment. Every time a transaction is added, the accounting file changes and the code also changes.

Banana.ch has invented a new process that allows certification by codes on an evolving database. The technique consists of two main steps:

- The data set receives a final, unique and identifiable data order. All transactions are numbered progressively.
- Each transaction is certified progressively. A certification code is computed for each transaction taking into consideration all data preceding the transaction (in the preserved order).

Using this technique all transactions receive a certification code that considers all data up to this transaction. It is like having a file certification code as each new file evolves.

If a transaction changes, then all codes from and following that transaction will change. If there are 100 transactions, only the certification code of the 101st. transaction needs to be annotated. If any prior transaction is changed, displaced or deleted then the code of the 102nd transaction will be different. To see if any transaction has changed it is only necessary to compare and check the certification code of the last transaction.

When new transactions are added new certification codes for all the new transactions will be created. The preceding transaction's code will not change.

Banana - [Double-Entry with VAT - 1]									
File Edit Data Format Options Account1 Account2 Window ?									
4100									
Accounts			Transactions		Totals		VAT Codes		
Date	Doc	Description	Debit A/C	Credit	Amount	LockNum	LockAmt	LockCrcProg	
3/1/2001		Withdrawal from post office account	1000	1010	350.00	1	350.00	da4148fa.7dd349a1.18aa	
5/1/2001		Office supplies	3260	1000	80.00	2	430.00	01624efc.2ea2b88e.d2ed	
6/1/2001		Sales in cash	1000	4100	8'000.00	3	8'430.00	2bbaf1f8.096784dd.96dc6	
10/1/2001		Purchase goods by Company	3000	SU-001	1'500.00	4	9'930.00	5eacbab7.60a1b3db.35e	
28/1/2001		Payment Company 1 invoice	SU-001	1020	1'500.00	5	11'430.00	aae24dab.60fdb2a7.78c9	
1/2/2001		Electricity	3250		200.00				
1/2/2001		Telephone	3270		100.00				
1/2/2001		Payment Electricity and Phon		1020	300.00				
9									

VAT	Total VAT	Cost Centers	Expiry Date	Lock
1000	Cash		8'000.00	9'278.88
4100	Income from sales		-7'272.73	-7'272.73
2070	VAT due		-727.27	-727.27
510	Sales at 10%			

It is not possible to foresee how many transactions will be added each month. At the end of the month there will be a finalised state. To certify all accounting data up to this month it will only be necessary to set aside the code for the last transaction of the month.

In order to verify the integrity of the transactions, you only need go to the specific transaction number and check the code is still the same.

The process works as follows:

- The transaction is numbered**
 Each transaction line receives a progressive number starting from one. This progressive number is unique. This numbering is independent from the document number and there cannot be a duplicate number. The number is saved within the transaction record and becomes part of the accounting data.
- The transaction receives a data certification code**
 A certification code is created based on the transaction data. If the transaction is changed then the code will be different. The code is saved within the transaction record and becomes part of the accounting data.
- The transaction receives a cumulative certification code**
 This code is computed including a progressive number and all the preceding transaction data. Each transaction line will therefore have a code that identifies all transaction data up to this point. The code is saved within the transaction record and becomes part of the accounting data.
- Checking all certification codes**
 The certification codes are stored with the other accounting data. The program can recalculate all codes and check at any time that the stored codes are the ones calculated. Any attempt to bypass the lock and change the transaction data will therefore be useless.

Long-Term Electronic Storage

The accounting software calculates the Balance Sheet, accounting cards and everything else that is necessary. Without the accounting software the data cannot be accessed. It is very difficult to ensure that old software will always work properly after a number of years. An alternative to electronic data storage was therefore printing out all the accounting information.

Banana.ch has introduced a new technique that allows for long-term electronic data storage that is always accessible without the need to have the original accounting software.

Once the accounting year has been closed, no more transactions are added. The Balance Sheet, Income Statements and the other accounting reports (account cards, VAT report) will always be the same. At the end of the year it makes sense to calculate and store the reports in their finalised form that can be viewed and printed without further calculation or the need to use the accounting software. The most widely used and accessible document format is the html (internet) format. Data stored in html can be viewed and printed on any computer. Documents saved in this format will be accessible for decades.

The html file can then be electronically certified and signed and becomes a valid legal document. The file can be given or sent to the auditor, lawyer, judge, tax inspector. Each one has individual access to all the relevant accounting information directly on their own computer without the original accounting software having been installed.

The image shows two screenshots of a web browser displaying accounting data for 'MyCompany Name Double-Entry Accounting'.

Top Screenshot: Accounts

MyCompany Name
Double-Entry Accounting
Accounts

Group	Account	Description	BClass	Gr	Opening EUR	Balance EUR
		ASSETS				
	1000	Cash	1	1	1'000.00	9'270.00
	1010	Post office current account	1	1	2'500.00	2'150.00
	1020	Bank 1	1	1	35'000.00	33'200.00
	1100	Clients	1	1		
10		Total Clients		1	1'000.00	1'000.00
	1150	Prepaid taxes	1	1		
	1170	Recoverable VAT (previous)	1	1		140.17

Bottom Screenshot: Transactions

MyCompany Name
Double-Entry Accounting
Transactions

Date	Doc	Description	Debit A/C	Credit A/C	Amount EUR	VATCode	% VAT	% Exempt	VAT Acc EUR
03.01.01		Withdrawal from post office account	1000	1010	350.00				
05.01.01		Office supplies	3260	1000	80.00	P5	5.00		3.81
06.01.01		Sales in cash	1000	4100	8'000.00	S10	10.00		-727.27
10.01.01		Purchase goods by Company 1	3000	SU-001	1'500.00	P10	10.00		136.36
28.01.01		Payment Company 1 invoice	SU-001	1020	1'500.00				
01.02.01		Electricity	3250		200.00				
01.02.01		Telephone	3270		100.00				
01.02.01		Payment Electricity and Phone		1020	300.00				

Legal Evaluation of the Active Security Functions

Certification of Current Year Data

The integrity of the content is the central question when considering the legal validity of an electronic signature. A digital signature is considered valid (according to most legislation) only if the signature can be bound to a specific content. If a document changes, the signature is no longer valid. Access and password protection are not considered valid methods to ensure the data integrity and authenticity of an electronic document by most current digital signature laws. Only certification techniques can ensure data integrity and therefore only certification techniques are considered valid methods to ensure the integrity and validity of a signed electronic document. A method that the law considers adequate to ensure the integrity of an electronic document should be considered more secure than methods that are not recognised by the law as valid methods for securing data integrity. Assuming that we proceed according to the "higher standard" of the digital signature laws, we can say that only a certified accounting file can be considered a fully valid electronic document. The same law will not consider a password-secured accounting file a valid electronic document. If the certification technique is a better technique to secure the data integrity of an electronic document, it is also a better technique to ensure the integrity of accounting data. From a legal standpoint (criterion used by the law) the certification technique is in principle a better solution to ensure the integrity of accounting data.

Assuming that the certification technique is effective it should be possible to say that accounting software that uses a certification technique should be considered at least as secure as an accounting system that uses a password-protected security system.

In principle, if today an accounting software using password protection is considered a valid legal solution, then an accounting system that uses a certification system should also be considered a valid accounting solution for today's legal requirements.

Long Term Accounting Data Storage

The law prescribes that accounting information needs to be kept for a specific amount of time (10 years). Accounting data is saved in a database. In order to access the accounting data (display and print reports) it is necessary to have the original accounting software. At year-end the data is saved on external disks or cassettes. This method of storage is considered to conform to the law and to current accounting principles.

With Banana Accounting, at year-end, all accounting reports (transactions, balance sheet, income statements, and accounting cards) are "printed" in a file in html format. All accounting information is then included in a file that can be accessed using any browser on any computer. The file is definitive

and the figures are immutable. The original accounting software is no more needed to display the original information.

If the law considers a proprietary format to be valid storage, then the law will surely also consider valid an easily readable file format that includes all accounting information in its final form to be equally valid. The html file generated by Banana Accounting is in standard Internet file format. It is generally known that Internet files can be electronically certified and signed. It can thus be stated that an html accounting file is predisposed to be electronically signed when required.

Accounting Organisation Protocol

Data certification is a technique that ensures data integrity. Digital signature is a broader methodology. Digital signature requires a working public key infrastructure that authenticates the information. Digital certificates contain other kinds of information (issuer, date of issuance, expiration) that needs to be considered differently from a legal point of view. The authentication process is not part of Banana Accounting.

Banana.ch proposes organisation "protocol" that should be used in order to ensure that the accounting conforms to specific legal requirements. The protocol should be adapted and revised based on the rules of the country.

Using New Security for Banana Accounting

Security functions should prevent alterations to the accounting data. From a user point of view active security works the same as passive security. The function that locks the transactions is also the one that certifies the transactions. The user only needs to specify a date. All transactions up to this date will be locked and certified. A locked transaction can't be modified. By using a lock, only transactions with a more recent date can be inserted. Accounting reports for previous periods will not be changed.

Using a lock, each transaction will be marked with a certification code. The certification code of the last transaction will be preserved so that it can serve as evidence that the accounting data has not been changed. The certification code, the progressive number and the current date should therefore be maintained. For most legislation it should be sufficient to print and file this information with the other accounting documents. Other countries may require that the information is authenticated by a public notary, printed on official paper or written in a company book.

The transaction lock prevents the user from making changes to the transactions. This transaction lock is not essential to the certification process. If the data is altered the certification numbers will be different. From a certification point of view the fact that the transactions can be modified is not significant. The transaction lock is provided so that users will not make changes to the data unintentionally. A function to undo the

lock and remove the certification codes is available. The transactions can be locked again. If the data is unchanged the codes will be the same.

General Organisation Protocol (Switzerland)

In order to ensure that the accounting is properly organised using the security function, the following procedure can be indicated.

- **Lock the transactions at period end**
At period end lock the transactions. The period can be the end of a month, quarter, year end or at any time when transactions are required to be made final by law, the situation or dimension of the company.
- **Print the last 10 transactions**
Select and print the last 10 transactions with their lock numbers visible (progressive number and certification code).
- **Date and sign the paper**
The accountant, or a company representative, should sign the paper with the certification information.
- **File the paper with the other accounting documents**
The signed paper should be numbered and filed with the other accounting documents. By having this document it will be possible to bring evidence to bear that the certification codes have not been changed.
- **Notarisation**
Depending on local requirements it may be necessary, especially at year end, to authenticate the accounting data. In such cases, print the last 10 transactions with their lock numbers and have the printout stamped by a notary.
- **Year end html filing**
At year end follow the procedure to create an html file that includes all accounting information. Copy the file to at least 2 diskettes (better still, to a write-once CD), and keep it together with all the other accounting documentation. If such a service is available, have the file content electronically certified.

The accountant can always bring evidence that the accounting data has been recorded within a specific time and that no changes have been made since then.

Such an organisation of the accounting will most likely conform to and be considered valid by most countries in the world.

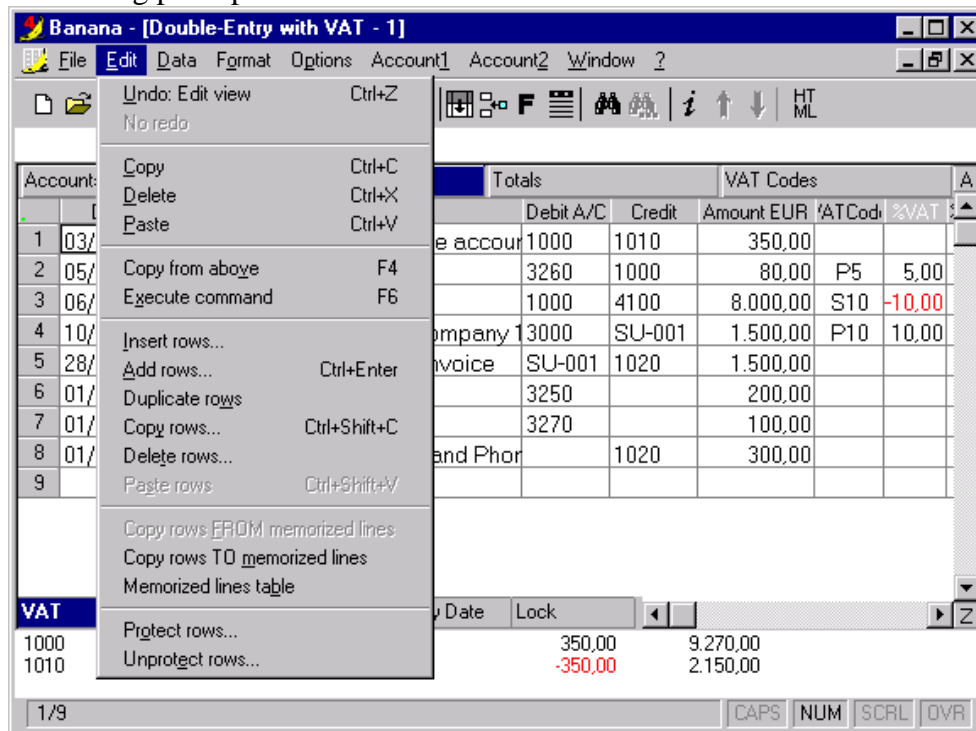
Some countries may require that the accounting data be printed on special official paper. If this is the case then such official papers should always be used.

The legal requirements regarding the keeping of accounts may vary from nation to nation, regarding timing and be different depending on the legal form and size (total revenue) of the company. It is up to company management to ensure that their accounting is properly organised.

Advantage of Active Security

The security system developed by Banana.ch is very easy to use.

Transactions can be entered and corrected so that they exactly match the document content. Once they can be considered final, they can be locked and certified. It is possible to verify that the accounting data has not been changed at any time. The Banana.ch environment allows and helps users to operate in a professional way that totally conforms to generally accepted accounting principles.



- Easy to use**
 Keeping the accounts becomes much easier. Banana.ch is the only accounting software to offer functions and an environment similar to a word processing program (undo, redo, copy, paste, search, replace).
- Increased security**
 The accountant can be sure that intruders or unauthorized individuals cannot make changes to the accounting. If the accounting files are changed he will notice this immediately.
- Less costs**
 Transactions can also be delegated to an untrained person. The accountant or manager can then check them later and correct any incorrectly entered transactions. Once all transactions have been checked and certified, the file can be given back to the person with no fear that past data can be changed. The next time only unsecured transactions will need to be checked.
- Greater interaction**
 People can interact with their consultants and auditors. The accounting

file can be sent via email with no fear that unauthorised changes will be made.

- **Simplified auditing of accounting**

Auditors and tax authorities will have no further reason to check for changes to the accounting data. Auditors and tax authorities can concentrate on substantial controls. The accounting data can be transferred to their computer where they can work freely, knowing that they are working on the same data the company is using. Auditors can check the accounting for a specific period and be sure that no changes will be made later on without their knowledge.

- **Better filing solution**

Copies of the accounting data can be stored in different places without supplementary cost. It is possible to know that the content has not been modified at any time. The unique html filing system guarantees that the data is stored and available for years in a readable form.

Summary of the active Security functions

- **Transactions lock** - Transactions can be locked at the user's request. As long as the transactions are locked no change, intentional or unintentional, can be made to the files.
- **Transactions certification** - At the same time that transactions are locked, they are also certified. Each transaction receives a progressive number, a single transaction certification code and a progressive certification code. Any change to the transactions can therefore be intercepted.
- **Certification of opening balance** - The opening balance is inserted in a different location. The program calculates a certification number for the opening balance. The accountant can easily check that the opening balance has not been changed.
- **Verification of the certification** - The program checks that the certification numbers and codes are correct. Any attempt to manipulate the accounting data by altering a file would be discovered.
- **HTML filing** - All accounting data (entries, accounts, VAT, account cards) can be exported in HTML format. This is the standard international method for the exchange of documents. On whatever kind of computer, even after several years, balance sheets, account cards, VAT reports, etc. can all be printed out.
- **Electronic signature** - The HTML file can be signed and endorsed electronically (a procedure external to Banana Accounting). In this way the file becomes a valid document under all legal aspects, conforms to the new regulations for the filing of documents and authentication of signatures and for digital documents.

- **Tools for the auditor** - Thanks to the certification of the transactions and HTML filing, the auditor or professional accountant can access all the data on their own computer and be certain that there have been no modifications made without them knowing about it.

Technical Details

Banana Accounting uses the following technology:

- **Certification number based on MD5**

In essence, MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods. MD5 was developed by Professor Ronald L. Rivest of MIT. The MD5 algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem.
- **Certification number with 32 Hex digits**

There is a chance over a number with 38 digits (trillion of trillion of trillion) that there can be a similar that return the same "fingerprint".
- **Incremental transaction's amounts**

The program calculate the sum of all preceding transactions. The transaction number and the total amount is a legal requirement when printing the accounting information.
- **Transactions lock**

To avoid the risk that transactions are altered by users unintentionally, the transactions are locked after the certification process. Users can unlock the transactions and proceed to make changes. They must then restart the functions that certify and lock the transactions.
- **Certification process initiated by the users**

After evaluating different solutions we have opted for one where the certification process is initiated by the user. Accountants work by periods. They enter transactions and wait until the end of the month to check that the data conforms to the bank statements. At the end of the month, quarter or year they prepare the VAT or tax report. Certification works in this way. The user indicates the date and the software certifies and locks all transactions with a date prior or equal to the one specified. Some countries specify a certain date for transactions to be reported in the books. With a free system users can adapt to these requirements.

- **Certification of opening balance**
The opening balance is inserted in a different place. The program calculates a certification code for the opening balance (8 hex number, 1 chance in 4.8 Mia) . The accountant can easily check that the opening balance has not been altered.
- **Verification of the certification**
The program checks that the certification numbers are correct. Any attempt to manipulate the accounting data by changing the file will be discovered.