THE BUILDING SITE WITHOUT PAPER - LEGAL ASPECTS IN AN IT-ENVIRONMENT

Dr jur. Eduard Ott
Legal Expert, Civil Engineer, Industrial Engineer
Munich, Germany

ABSTRACT

At present there is a anachronism using modern IT-Equipment for building projects:

- *files and data are transmitted between persons, far away from each other, within seconds. But legally binding orders or requests, what to do with this data, are transferred in a written form on a sheet of paper by registered mail, the delivery takes days and weeks. Or:*
- *CAD-files are distributed to the building participants for being able to work with them. But legally binding are only the drawings on paper.*

In a IT-environment the consideration of legal aspects is far behind the level of the achieved technical progress. Up to now only technical aspects have been considered when doing IT-based work.

Worldwide ToCEE[1], part of the ESPRIT-programme, funded partially by the European Commission, is the first research project dealing with IT (Information Technology) in the construction industry which also adresses the legal aspects, especially when developing the CAD - environment further to a Concurrent Engineering Environment (CEE) using electronic transmission of documents and files.

Many legal aspects arise because of using files and electronically stored data instead of paper. This leads for instance to the following problems:

- *How can legal actions be documented and transferred using electronic media instead of paper? "Electronic signature" and "Encryption" is one of the key points in this field.*
- *How is it possible to extract and present evidence from the electronically stored data?*
- *How can AEC-software-objects (AEC=Architecture-Engineering-Construction) be expanded with legal elements in order to be able to avoid the use of paper in a building project?*

Keywords: building site, without paper, digital signature, law, Trusted Third Party, declarations of legal intent, contractual model, contractual relation, power of attorney, AEC-object, approval, simultaneous working, Concurrent Engineering

[1] http://wwwcib.bau.tu-dresden.de/tocee/

INTRODUCTION

The demand for a paper-free building site gets presently stronger and stronger: no one is willing any more to send written letters on sheets of paper by registered mail if it needs only a click on the screen to send an e-mail via the internet. Thus already many of electronic paper-free messages are being transferred between building participants, especially within large building projects. But what happens when a slab has crashed down and only bits and bytes exist for the orders which led to the failure and not sheets of paper which have been personally signed? In such a case the problems of a paper-free building site get obvious. It will be shown in this paper how these problems can be solved. And more than that: using new 'legal' techniques in an object-oriented software environment, especially with AEC-elements, improves working together on a building site, thus being able to avoid many legal disputes and legal proceedings.

On a paper-free building site the following problems can occur:

- The receiver may deny that he has received a message to erect an additional column under the slab. This shows that on a paper-free building site a confirmation of receipt is necessary.
- The receiver may reply that the order for the column was legally not binding because the message was not personally (hand-)signed by the sender
- The receiver ignored the message because he was not sure that the message came in fact from the sender. That is the problem of the authenticity of the sender.
- The receiver did not have confidence in the wording of the message because on its way from the sender to him the text could have been altered.
- Messages not dedicated to the public (like calculations for prices and compensation) should be kept secret also when sending them via a network or the internet being transferred over several unknown servers.

All these requirements of how to establish legal acts by electronic media instead of paper can be fulfilled by using several software tools like 'Digital Signature' combined with some devices to check the flow of information. This is shown in the next chapter.

ESTABLISHING LEGAL ACTS BY ELECTRONIC MEDIA INSTEAD OF PAPER

To get a paper-free software system to work (concerning legal aspects), one of the essentials is to give declarations containing legal intent from one person to another one. There are one-way declarations like orders from the client to the contractor. And there are also two-way declarations, for example, when the contractor and his sub - contractor set up their contract. Such a contract consists of the one declaration of the sub - contractor that he is willing to work, and the other declaration of the contractor that he accepts. All these are declarations of legal intent.

Some time ago (until the year 1996/1997) the electronic form of declarations of legal intent seemed to pose a problem. This was because up to that time only paper - based declarations seemed to be legally accepted.

But already at that time there was a strong demand for the acceptance of declarations in electronic form. The banking sector especially realised the advantages of electronic declarations to and from their customers, for example for transferring money from one

account to another. Banking companies have made electronically transmitted declarations of legal intent a reality already. And there have been strong efforts by some governments to make electronic declarations of legal intent legally admissible. Several laws have been passed.[2] The first one in the world was in Utah (USA) in 1995. Some EU-countries have passed already some laws, others will follow. The European Commission is preparing a directive on digital signatures which will be valid in every EU-country[3]. With these laws - combined with suitable contract clauses - the electronically transmitted declarations will get the same legal authority as paper - based declarations.

The basic requirement in transferring reliable electronic declarations is the "digital signature".

Digital signature

The purpose of the digital signature is to have an electronic document (e.g. a file) transmitted rapidly, with protection against alteration or manipulation, and to know for sure who was the sender of the electronic document. The content of the document (like a text or the bitmap in the file) gets, with the use of a key (a sequence of numbers or digits) and an algorithm, encoded. This new file is impossible to read without the encryption algorithm and the key .
When decoding the file in order to read the original content, the knowledge of the key and the algorithm is necessary. The algorithm is public, but the key is secret. The key may be a password or a longer chain of digits. If the receiver knows the key (the sequence of digits), and knows that the key belongs to the individual sender, then we have - together with the public algorithm - a digital signature. Thus encryption (encoding) and decryption (decoding) is the method for a digital signature. This kind of digital signature is already practised in many cases.

To work with one secret key is only possible between clearly separated parties like banks and their customers. On a building site for each message between the different parties one key would be necessary. The following drawing shows the project participants on a sample building site with 5 parties.

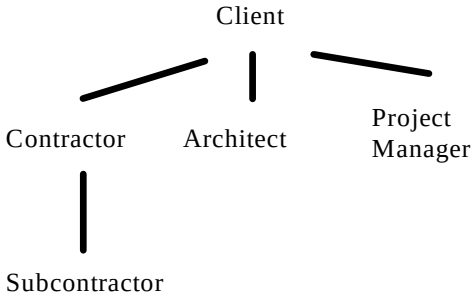

Table 1: Building Participants Relations

For a reliable communication between the 5 parties many secret keys would be necessary:

- 4 for the ways of communication shown in the drawing (e.g. from client to project manager, to architect, to contractor, from contractor to subcontractor)

[2] http://cwis.kub.nl/frw/people/koops/digsig.htm#g, Digital signature legislation
[3] Towards A European Framework for Digital Signatures And Encryption, http://www.ispo.cec.be/eif/policy, status: 12th January 1998

- and several more for the other paths (like from project manager to architect, from client to subcontractor, etc.)

This method is called a “secret-key signature method“. [4]

In this case the sender needs an additional key for every recipient. When using the digital signatures of more than a few people the administrative efforts for handling the keys get higher and higher, and then other encryption methods are necessary.
One of these other methods is the "public - keys". The encryption - programme creates two keys: one is private and is stored only on the hard-disk of the sender. The other one is public, and can be looked up by anyone, e.g. by looking up in public databases. After the sender encodes his message with his private key and sends it, for example by e-mail to the receiver the latter is able to decode it with the public key of the sender which he selected from - for example - the PGP-database in the internet[5]. Thus the receiver knows that the message has been sent off by the person who owns the secret key, that is the sender. Having been encoded by the sender, the message has been digitally signed. Thus a digital signature is not a handmade signature, done by a human for example with his PC-mouse. It is a calculation of a computer using a cluster of digits (the keys), created by the computer.

Using only the digital signature, other people than the receiver would be able to read the message because they can easily access the public key of the sender. If the message should be kept secret, to provide that only the receiver is able to read it and nobody else, the sender has to execute an additional step. After having encoded his message with his private key he encodes the message once more, but this time with the public key of the intended receiver. Also this public key is easily accessible by looking up in the public database. Then the sender transfers the double-encrypted message to the receiver. The receiver decodes the message twice: firstly with his private key and secondly with the public key of the sender. This procedure has some advantages:

- only the receiver is able to read the message,
- the message has been surely sent off by the sender and not another person and
- the receiver knows that the contents of the electronic message have not been altered on the way to him. He knows that the file/message he received is valid from the beginning of the file to its end.

All this is an advantage of the electronically transmitted form of document compared to paper-based "written" signatures and declarations.

Therefore, receivers and senders who do not know each other and have not exchanged any keys are able to send encrypted messages to each other.

The sender is not able to calculate the receiver’s private key by using the public key or the delivered message. He/she is only able to use the public key for decoding the message, but for nothing else.

This method is called the “public-key signature method“. The best known method in this field is RSA, created by Rivest-Shamir-Adleman, published in 1978.[6]

---

[4] http://www.digicash.com/publish/digsig,/digbig.htm, DigiCash, Digital Signatures and Smart Cards
[5] for example http://www.pca.dfn.de/dfnpca/pgpkserv
[6] http://www.rsa.com/about/

This system of pairs, like the “public- key signature method” is called an asymmetric method. One key is used for encoding, the other one for decoding. This is different to symmetric methods, like secret key methods, with single keys, as they have been described above at the beginning of this chapter. Symmetric methods use the same key for encoding and decoding.

One of the best known types of software in the area of “public-key signature method” is the programme "PGP - pretty good privacy", created by Phil Zimmermann[7]. It is freeware and can be downloaded in the internet.

One problem for the sender and receiver is that both have to be sure that the public keys are really the ones that the original person has used in the original database. The solution to this problem is the trusted third party, what will be demonstrated next.

Trusted Third Party

The main task of a trusted third party (or: trust center) is - concerning the digital signature- to check and keep track of whether the public key is in fact the one from the sender, and not from another person. That is the problem of the „authenticity“ of the sender. To ensure that the key is authentic a party in whom both sender and receiver trust gives a certificate for the public key. And this third party administrates the public key on its server - computer.

Instead of "private" trusted third parties in whom individuals trust, "public" trusted third parties can be established by national laws, like done in Germany[8]. The trusted third party needs the permission, or a licence from the government. When the trusted third party declares that a certain public key belongs to the person A one is legally „allowed“ to trust in that.
The use of digital signatures and established trusted third parties forms what is known as a "security infrastructure". This is essential for reliable electronic transfer of declarations of legal intent.

Common format for writing and reading

When talking about the transmission of electronic declarations of legal intent one important point is missing most times in the discussions: that is, the necessary common programme which sender and receiver both have to use. If for example the sender transmits a WordPerfect.7-file and the receiver tries to read this file with Microsoft Word 7 the receiver will not succeed. Each of the files has its own different format and a conversion is not possible because Microsoft Word 7 is not able to read WordPerfect 7. This has nothing to do with the digital signature. It is essential in a building project to be able to communicate between the parties.
So when transferring data it is necessary to define a common format or a common programme in which sender and receiver write and read their messages (their files).

All of the participating parties have to work, for example with the same software and the same version of it. This has to be set down in the contract(s) between the parties.

Conclusion

World wide, activities are on the way to establishing a secure way of electronic communication. With the digital signature, the creation of a “Trusted Third Party” and some

[7] http://www.ifi.uio.no/pgp/
[8] http://www.iid.de/rahmen/iukdgk.html

special clauses in the contracts between the building participants it is possible to create a paper-free electronic communication on building sites.

LEGAL EVIDENCE OUT OF ELECTRONIC MEDIA

Another problem when using electronic declarations and not sheets of paper for legally binding instructions is the matter of legally valid evidence. When a building failure or damage to a building occurs, it is often necessary to prove who caused the damage. With a paper-written instruction this is no problem. But when only bits and bytes exist on the hard-disk of the receiver the evidence is unsure.

Thus a system has to be developed which allows strong evidence to be found in the case of disputes. The problem for the accusing party is how he can prove that a declaration has found his way to the receiver. This is a matter of receipt of the declaration.

At least two ways are possible:

- Either the sender gets an automatic confirmation that the message has been opened and read by the receiver or
- All electronic messages are passed via a central server where they are stored and the delivery is monitored. This special server has to be under control of one person who is trusted by all parties, who takes care that no manipulations occur. This is another type of the before mentioned „Trusted Third Party".

For the second alternative some guidelines are already in existence like the British BSI-„Code of practice for legal accessibility of information stored on electronic document management systems" [9]. It gives some criteria for the problem of how electronic information can result in a safe evidence. Although this code covers only storage written once (like WORM), several of the points in the code can be used also for systems with storage that can be re-written (for example magnetic storage or tapes).

CONTRACTUAL MODEL

In the last chapter a solution for legally admissible electronic declarations instead of paper-based written messages has been described. But object oriented software can help much more to improve the legal handling in building projects.

Authority to create and alter data

In a IT-environment it is necessary to control the access of the project participants to the data which are stored or to be transferred. A contractor is not authorised to access the database and alter the architect's design. This can only be done by the architect himself or by the authority which is above the architect, this is the client. The same problem occurs when giving orders: the contractor is not allowed to give orders to the architect. Only the architect or the authority above the architect is allowed to give those orders. This system can vary: other people may have the authority to give orders, e.g. the project manager.

[9] British Standards Institution, Customer Services, Sales Department, 389 Chiswick High Road, GB-London W4 4AL

This shows that a system is necessary, which handles these accesses on data and orders. This is the ‘contractual model’.

From Contractual Relations to Authority: the Contractual Model

The structure in a building project is generally the same. The client makes contracts with different parties like designers, contractors and vendors. The contractor himself makes other contracts with sub-contractors, installers etc.. This contractual structure can be easily graphically represented:

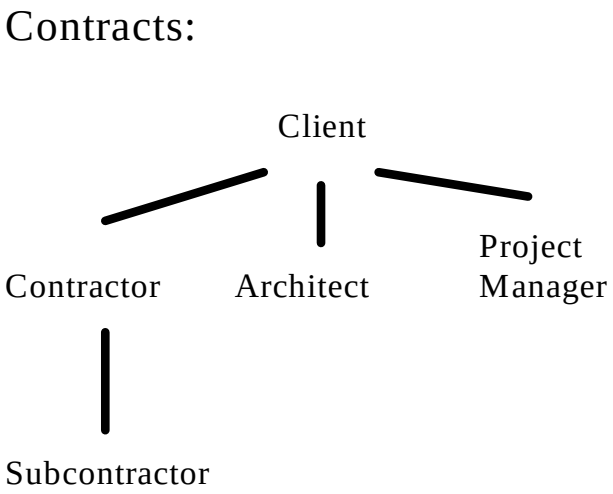

Table 2: Contractual relations

Looking at the subject from a legal point of view, additional matters can easily be derived from this structure, such as the authority to give legally binding orders on a building site to other parties.
The authority to give orders to other participating parties follows the contractual relations. This means that for example, the client is allowed to give his orders to the project manager (they have a contract with each other) and to the Architect, but the client is not permitted to give orders to the sub-contractor of the contractor because these two have no contract with each other.

The only way that this hierarchy of authority can change is by giving power of attorney to another party. This is done in most cases by the client, who gives his authority partially to the project manager or/and the architect. With this power of attorney the project manager (or the architect) is able to act in the name of the client, that means as the client is able to act. This can be described as directed relations and represented like this:

Authority

- to give orders

- to change data in the data pool

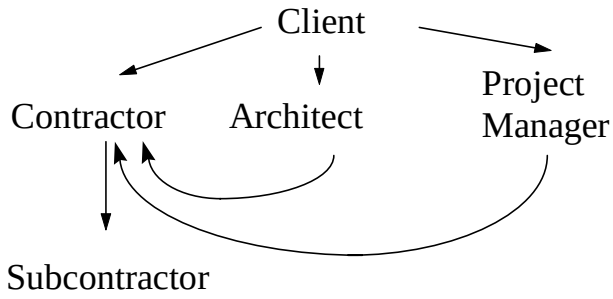

Table 3: Authority Relations

With the authority transferred by the client, the project manager is then able to give his orders for construction details or for the time schedule for example, to the contractor. Without the transferred power only the client has the power to give these orders.

This scheme has to be set up for every construction project . It can be called a “Contractual Model”. Several legal tools (like checking the power of attorney when sending declarations from one building-participant to another) can use it.

The most important consequence of the contract model is that access rights to computers can easily be defined. The project manager in the above example is allowed to access the database and to input and read data there. He is allowed to create new AEC-objects, to change existing AEC-objects and to permanently remove older objects. But this can only be done in respect of the contractor, not the sub-contractor. This authority to input and read data, and those who are permitted access has to be defined on every building project.

This system seems to be able to work, even if there have to be taken into account some limitations as the project manager for example, does normally receive only partial and not complete authority from the client.

LEGAL EXPANSIONS OF AEC-OBJECTS

Today the work on building sites is done on the basis of drawings on paper. These drawings are the results of manual work or CAD-computer programs. In future AEC-objects (these could be STEP- or IFC-objects) instead of drawings will be the basis for the work. This

change in the way of working has several consequences. The most important is the „track of approval“.

The Track of Approval

In order to control the building’s design every item during the construction needs the permission, sometimes of the HVAC-Engineer, sometimes of the Local Authorities, sometimes of the architect, or of the structural engineer etc. and sometimes of a combination of these people. Thus it is necessary to keep track of every part, or item of the building whether it was permitted, by whom, how and when. The person who has final responsibility that all dimensions and all materials of a building are correct and approved is normally the person on the building site, e.g. the architect or the project manager. This is the system like it is now and this will be the system in the future, too. But this system can be easier handled by using AEC-elements.

It is necessary to set up a system in the AEC-objects that shows which parts of the elements have been approved by the different people who are allowed to control the building. Thus the task is to figure out what the impact is on the AEC-objects when a drawing, or a dimension, or a part of a construction has been approved. A kind of tracking device needs to be set up, in order to monitor what is happening on the building site. Setting up this track leads to an AEC-object, for example, looking like this:

Approval by	Record No.	Type	length [m]	thickness [m]	height [m]	material	position lower left corner [m]	thickness of thermal insulation [m]
	34	wall	4	25	3	concrete	x=10 y=2 z=9	0.1
Loc. Authority		Y	Y	Y	Y	NPN	Y	NPN
Architect		Y	Y	Y	Y	Y	Y	Y
Structural Engineer		Y	Y	Y	Y	Y	Y	Y
HVAC-Engineer		Y	No	Y	No	Y	Y	Y
	78	hole	1	empty	2	empty	x=11.5 y=2 z=9.5	empty
Loc. Authority		Y	Y		Y		Y	
Architect		Y	Y		Y		Y	
	115	window	1	0.1	2	PVC	x=11.5 y=2.1 z=9.5	empty
Loc. Authority		Y	Y	Y	Y		Y	
Architect		Y	Y	Y	Y	Y	Y	
HVAC-Engineer		Y	Y	Y	Y	Y	Y	

Y = Yes, approved No = Not approved NPN = No Permission is necessary

Table 4: AEC-Object for Extended Track of Approval

In this example four different parties have approved the drawings which contained these elements. The architect has created the drawings initially which means that in every item on the line "architect" in the AEC-object where there is a Y for yes, the architect has approved. When the local authority had to approve something, their fields on the AEC-object contain a Y. Those items which do not need an approval by the particular party are marked with a NPN (No Permission Needed).

The structural engineer and the HVAC -engineer also had a look at the drawings. Those AEC -objects which had been affected by those persons when looking at the drawings are marked in the above matrix either with a Y or N, showing whether they approved or disapproved. The only rejection came from the HVAC-engineer and concerned the wall's length and height. This was because he cannot accept the wall's full dimensions because he wants a cut-out for

his pipelines.
These Y's, N's and NPN's are the newly created legal "track of approval". This system is legally essential for working in an IT-environment.
Every "N", or every field which has not been filled out by the appropriate person, has to show up on the software for the person responsible, usually the project manager or the architect, to see it, in order for the system to work properly.

Consequences of AEC-object-approvals: Concurrent working

The system of approvals in AEC-objects was invented - as shown above - as the solution to the problem of how to control every item's permission of the building during the construction. But the use of approvals in AEC-objects does more than this: it is essential for enabling a simultaneous (in this sense a concurrent) working system on a building - site.

In future the architect will send his "drawing" not only to the next party in the ordinary sequence (like e.g. the structural engineer) but also to all other appropriate parties (such as client, designers, contractors etc.). When the "drawings" with the approvals in the AEC-objects, come back to the architect, every part of the STEP- and IFC-objects is visible, showing whether it was approved and by whom. Thus it can be automatically checked which parts of the building have not been approved yet. With this advanced technology the tasks on a building site can be overlapped much more.

SUMMARY AND OUTLOOK

The elements shown in this paper demonstrate legal supplements which are necessary or valuable for a paper-free building site. Using the 'Digital Signature' the working with paper can be avoided. Special devices like an automatic confirmation for receipts of electronic messages guarantee a high level of legal evidence. The contractual structure of the building site can be used for the permission of access to data and of giving orders on the building site. And AEC-objects expanded with approvals enable reliable and even more simultaneous working. With these instruments it will not only be possible to work without paper but there will also be a significant decrease of legal disputes.

All these solutions are valid not only for building sites but also for other IT-using-projects with more than one participant (like in the automobile or airplane industry). It is surprising that ToCEE is the first project with a systematic legal approach to enable a paper-free working.

Dr jur. Eduard Ott
Legal Expert, Civil Engineer, Industrial Engineer
Vorhoelzerstr. 21, D-81477 Munich/Germany,
Tel +49/+89/749161-21
Fax+49/+89/749161-31 E-Mail: Eduard.Ott@T-Online.de