EURASIP Journal on Applied Signal Processing 2002:2, 174–184

Digital Watermarks Enabling E-Commerce Strategies: Conditional and User Specific Access to Services and Resources

Jana Dittmann

FHG IPSI—Fraunhofer Institute for Integrated Publication and Information Systems, Darmstadt, Germany
Email: jana.dittmann@ipsi.fraunhofer.de

Platanista GmbH, Darmstadt, Germany
Email: jana.dittmann@platanista.de

Martin Steinebach

Fraunhofer Institute IPSI - C4M: Competence for Media Security, Dolivostr. 15, D - 64293, Darmstadt, Germany
Email: martin.steinebach@ipsi.fraunhofer.de

Petra Wohlmacher

Regulatory Authority for Telecommunications and Posts, Germany
Email: petra.wohlmacher@regtp.de

Ralf Ackermann

Darmstadt University of Technology, Industrial Process and System Communications (KOM),
Merckstr. 25-64283 Darmstadt, Germany
Email: rac@kom.tu-darmstadt.de

Received 10 May 2001 and in revised form 31 October 2001

Digital watermarking is well known as enabling technology to prove ownership on copyrighted material, detect originators of illegally made copies, monitor the usage of the copyrighted multimedia data and analyze the spread spectrum of the data over networks and servers. Research has shown that data hiding techniques can be applied successfully to other application areas like manipulations recognition. In this paper, we show our innovative approach for integrating watermark and cryptography based methods within a framework of new application scenarios spanning a wide range from dedicated and user specific services, "Try&Buy" mechanisms to general means for long-term customer relationships. The tremendous recent efforts to develop and deploy ubiquitous mobile communication possibilities are changing the demands but also possibilities for establishing new business and commerce relationships. Especially we motivate annotation watermarks and aspects of M-Commerce to show important scenarios for access control. Based on a description of the challenges of the application domain and our latest work we discuss, which methods can be used for establishing services in a fast convenient and secure way for conditional access services based on digital watermarking combined with cryptographic techniques. We introduce an example scenario for digital audio and an overview of steps in order to establish these concepts practically.

Keywords and phrases: new applications of multimedia data hiding, digital watermarking, conditional access, e-commerce.

1. MOTIVATION

Multimedia systems are increasingly used and security has become one of the most significant and challenging problems for spreading new information technology. Capturing, storing, editing, retouching, printing, copying, and transmitting high quality colored images has become lucrative business, as well as one focus of national and international research institutions and organizations. With all this new and powerful imaging technology, unfortunately digital data can easily be manipulated and multiplied without information loss. To prevent the production of unauthorized copies, misuse, and theft of material, legal regulations and mainly security solutions are required to provide control mechanisms.

Digital watermarking itself and combined with other (cryptographic) mechanisms allows to offer several security

services today, based on steganographic systems by embedding information directly into the media data. In general, we find the following application areas for digital watermarking:[1]

- copyright watermark: watermarking the data with an owner or producer identification, see, for example, [1, 2, 3, 4, 5, 6, 7] or [8] for digital images, [9] or [10] for video, [11, 12] or [13] for audio signals and [14] for 3D models,
- fingerprint watermark: watermarking the data with customer identifications to track and trace legal or illegal copies, see [15, 16] or [17],
- copy control or broadcast watermark: ensuring copyrights with customer rights protocols, for example, for copy or receipt control, see [18],
- annotation watermark: annotations or captioning of the media data, this kind of watermark is also used to embed descriptions of the value or content of the data, see [19] or [20],
- integrity watermark: besides the authentication of the author or producer we want to ensure integrity of the data and recognize manipulations, see [21, 22, 23] or [24].

In this classification scheme we do not consider watermarking as information hiding technique to ensure a secure cover communication.

The most important properties of digital watermarking techniques are robustness, security, imperceptibility/transparency, complexity, capacity, invertibility, and possibility of verification. Robust digital watermarking can be used to claim copyright protection by inserting authors, producers, or customer information (known as copyright watermarks and fingerprint watermarks). Fragile watermarking techniques address the recognition of manipulations, known as integrity watermarks. Besides securing authenticity and integrity of digital data, watermarks are used to annotate the data and provide additional information to the users. Therefore, these watermarks are called annotation watermarks [25].

These watermarking approaches can facilitate additional value in electronic commerce. Printed documents annotated with watermarking information, allow to connect them with the digital world. For example, images of advertisements printed in newspapers may include annotation watermarks. Showing the image to a camera, the annotated image enables a direct and easy connection to the internet page of a dedicated company or vendor. This procedure is much easier and faster than typing in a URL which is, moreover, error-prone and difficult to handle. Technical solutions for this scenario are already available, for example, MediaBridge [19]. Furthermore, the embedded information can represent action descriptions to occur during retrieval of the watermark. This kind of annotation watermarks are also called active watermarks. For instance, with Digimarc MediaBridge, the watermark signal can be detected and read with a PC camera and the Digimarc MediaBridge reader, see [19].

Using these features, added watermarks convey much more information to the consumer than text or audio alone. And with the advent of such active digital watermarking, yet another level of information can be invisibly added to an image. This additional information remains dormant until the reader software detects it. The information can then be displayed, used to control the software or hardware that is processing the image, and used to obtain more information from the internet. This dormant information gives the image intelligence; hence Digimarc have coined the term "smart image" [20]. Annotation watermarks can bridge gaps between various media representations.

Besides these new applications for watermarks, there is another ongoing process that supports the increasing mobility of people. Particularly, the setup of UMTS-technology based networks form a basis for the crowing of mobile business (M-Business) and especially mobile commerce (M-Commerce). Prognoses claim that in 2003 more than one billion people are going to use mobile phones. Additionally, further developments of personal digital assistants (PDAs) together with appropriated security mechanisms are going to make them more suitable for mobile access to different networks. Both trends will lead to a high success for the M-Commerce sector.

Annotation watermarks are especially appropriated for M-Commerce, because they can easily support additional information which can be used for mobile access. Furthermore, since annotation watermarks are available in a separate medium, for example, in a hard-copy version, they allow an easy way to get people paid for these additional information. But it is quite clear that even unauthorized people owning a watermarked image, could try to get access to this information. Therefore, there is need for conditional access mechanisms. Those could combine annotation watermarks, strong cryptographic, and online-communication mechanisms as provided by innovative equipment like WAP cell phones or networked PDAs.

In our paper, we extend our discussion introduced in [26] to combine annotation watermark with additional security features to provide approaches for access control in M-Commerce applications. Our intention is to design a new conditional access mechanism combining annotation watermarks with cryptographical mechanisms. Section 2 describes important aspects and basics of M-Commerce. In Section 3, we give example scenarios to use annotation watermarks for access control strategies. In Section 4, we present technical watermarking solutions together with cryptographic issues and possible attacks. Section 5 discusses an approach for digital audio in detail. Finally, we give conclusions and point out important future work.

2. M-COMMERCE BASICS

Traditional economy is under a rapid development and change at the moment in order to adapt to the needs of global markets. The following issues can be identified as influential

[1] Today a wide variety of publications exists and we give only limited example references for the different applications.

to this change:

- the development of new communication devices and their general availability at relatively low prices,
- the ongoing deployment of new communication networks (such as GPRS or UMTS) that start to ensure a general network connectivity,
- the evolving uses of the internet for both identifying products and offers as well as for purchasing those.

That leads to a new innovative kind of business and communication relationships that we describe as M(obile)-Commerce.

The current mechanisms usually try to map existing procedures such as (search, order, and buy a product) to the new (networked advertising and purchasing) channels and thus do not exploit all the potential benefits. We give a definition of the area and the characteristics that we have identified. In the conventional case (e.g., a customer buying a book) the product that he purchases is static. For both, the customer (because he probably wants to receive updates, enhancements, or just additional information to the item he has purchased) as well as for the producer or vendor of the item (who, e.g., may want to sell more products or receive personalized information about the buyer), it is very reasonable to have further interaction.

There are a number of possible ways for establishing ongoing relationships, for example, think of a WWW page where new information is available for download or a kind of mailing or information list or a "push channel" that the customer is described to. But these concepts lack of fine granularity of identifying a particular partner and usually involve typing in a certain WWW address or filling out and sending a form. If the information how to do that is printed at the item itself without having an additional layer of indirection it may outdate and be incorrect very fast as well.

From those facts we can identify the following features that should be supported by a protocol framework appropriated for M-Commerce:

- placing individual information on an item should be possible at low cost, at a "late" (maybe just the selling) time within the production and selling process and regarding a fine granularity of distinguishing between customers, conditions, and point of sale as well as price,
- the placement of the information should be as less obtrusive as possible though this requirement may be lowered under certain circumstances,
- retrieving and using the information should be easy and convenient for a user; within the retrieval and usage process a flexibility (e.g., by means of an indirection step) should be possible,
- since the mechanisms described above may influence a customers privacy (e.g., by having the means for tracking transactions and even user behavior), possible approaches have to regard this fact at an early design phase. Legal regulations demand that a user should be aware of possible uses and must have a chance to actively influence or avoid them.

The application areas that we describe have a number of requirements that cannot fully meet using just conventional protocols. Especially they benefit from closing the existing gap between different media presentations and transport channels.

3. ACCESS CONTROL SCENARIOS

Access control mechanisms provide solutions for M-Commerce provider to limit access to additional value services for paying or preferred customers. In this section, we discuss example applications for access control using annotation watermarks: E-Book, Errata, Try&Buy, Long Term Customer Relationships, and Advertisement Bonus Program.

3.1. Buying books

Barcode and possible combination with other characteristics determine service. Buying books online or getting updates for them later on is a service that is very common meanwhile. A book holds a number of characteristics such as its ISBN that allow to identify it—but does that on a level that is not fine grain enough. By adding additional information via an annotation watermark to, for example, the printed barcode label there is a more flexible way to provide hidden information about the seller or the type of contract or price that was used or how to grant access to further information.

3.2. Errata

Update service with annotation watermarks. For a large number of products (either electronic but conventional ones as well) it is necessary to update information such as configuration data, firmware or just to provide corrections to the content. On the other hand, numerous distribution channels can exist, and different update service policies can come with them. In these cases, it is quite desirable to provide individual services. In this case, an (individual) annotation watermark can be used to uniquely identify the item as well as the selling channels. Thus, it is easier to ensure that the correct information is delivered and only persons that are also meant to receive it may use the service. The annotation watermark acts as a ticket for the update service with the embedded information ensuring a correct service regarding product and version number.

3.3. Try&Buy

Partial access to annotations. Try&Buy mechanisms support authors, producers, resellers, or content providers to allow evaluation of the data by potential customers. Interested parties receive data in inferior quality first to evaluate and to verify their intentions to buy the product. The data is not delivered in the original quality until the payment was done or until special conditions are fulfilled. Try&Buy transactions can be realized by a transparent encryption method.

Another method is to restrict the access to the annotation watermark. For instance instead of reducing the quality of the images, the access to the annotation watermark is limited. If the customer has paid, he receives access codes to the full

annotated data and the functionality. Furthermore, the prepaid services can be realized to activate services.

3.4. Long term customer relationships

Counting usage and getting additional service. Annotation watermarks can be used to support long term customer relationships by using the watermarks like discount stamps. A customer buying a product receives annotation watermarks embedded in it. These watermarks are detected by some mechanism and collected in a database. They provide additional service depending on the amount of annotation watermarks the user can present.

3.5. Advertisement bonus program

A watermark is embedded in a musicians online promotion song including the ID of the downloading party D and the artists' URL. Now D distributes the song, spreading it through the web. Whenever another listener accesses the artists' web site with the embedded URL, D's ID is also transmitted and the number of accesses is counted. Thereby, a bonus program like reduced CD prizes, other free promotion songs or merchandise can be established using watermarks as an indicator of the individual participants activity and at the same time as a information carrier for the URL.

In Section 4, we describe strategies to realize the above mentioned or similar conditional access mechanisms in general. In Section 5, we provide a more detailed scenario for the advertisement bonus program based on the first introduced approach in Section 4.1.

4. SOLUTIONS USING DIGITAL WATERMARKING

All aforementioned scenarios have to rely on cryptographic support for a number of reasons. Annotation watermarks are particularly appropriated because they cannot be forged since a specific (cryptographic) key is kept secret. Therefore, only the dedicated company owning the key is able to produce the watermark of an image. Additionally concerning images, the embedding of annotation watermarks cannot be detected by human eyes and therefore, these watermarks do not affect the optical vision. Particularly, a customer has an interest that the watermark is not damaged, lost or stolen, and thus, he will handle them with care.

As images including watermarks can be copied without information loss and hard copies can be given away to any other person than the legitimated owner, for example, the buyer of a book, further mechanisms are needed. These mechanisms should prevent the misuse of information by not legitimated persons or at least make it more difficult to misuse it. However, the level of security depends mainly on the amount of money that is investigated for security mechanisms—but the cost of the mechanisms should not be higher than the cost of a damage that might be caused without security mechanisms.

We suggest the use of annotation watermarks to provide conditional access for additional services or services for longer term customer relationships. To address all the scenarios of Section 3, we introduce four general strategies where annotation watermarking technology is applied. They differ regarding the information embedded as a watermark, the required characteristics of the watermark and additionally necessary mechanisms. Depending on the business model and the requirements these four strategies (or enhanced or modified versions) can solve several conditional access problems:

(1) *Discount approach*: annotation watermark is used as discount stamp. This strategy is mainly appropriate as solution for frequently customers, for example, for the long term customer relationship scenario or to provide additional value for the Buying book scenario.

(2) *Secret sharing approach*: annotation watermark is only accessible by combining several (shared) keys to get the information or additional service, for example, for the Try&Buy scenario.

(3) *Partial access approach*: annotation watermark is partly accessible and contains further protected information which is only accessible by combining several (shared) keys to get the information or additional service as enhanced feature, for example, for Try&Buy scenarios or prepaid services.

(4) *Key watermark approach*: annotation watermark is used as a key to get access to another annotation watermark useful, for example, as Errata concept, add on for the Buying Books scenario or as support for Long Time Customer Relationships.

These four approaches can be used to build several conditional access solutions and are discussed in detail in the following subsections.

4.1. Discount approach

This approach can be solved by an application, which counts the annotation watermarks registered by a user and provides the appropriate service depending on the accumulated discount stamps. Problems here are user identification and replay attacks. The annotation watermark needs to be designed like a fingerprint watermark to get unique identification of customers. To avoid replay attacks or limit the multiple usages, the application has to register the usage. Figure 1 illustrates an example of the discount protocol. A user has collected several watermarked data, he can register his data with the discount stamps via a discounting server, which can also be a part of the shop system itself. In the figure, the discounting server is shown as a separate part to collect discount stamps from different shops which are valued in all shops. The server creates a login for the user (here we can also use pseudonyms) and registers the watermarks. The shop systems have access to the discounting server, can request the accumulated watermarks and determine the discount stamps to grant discounts.

An advantage of the scenario is the independence to the shop systems itself. The customer can collect discount rates from every shop and use it in every shop. These approaches are very appropriate as a long term customer support or the additional value in Buying book scenarios.

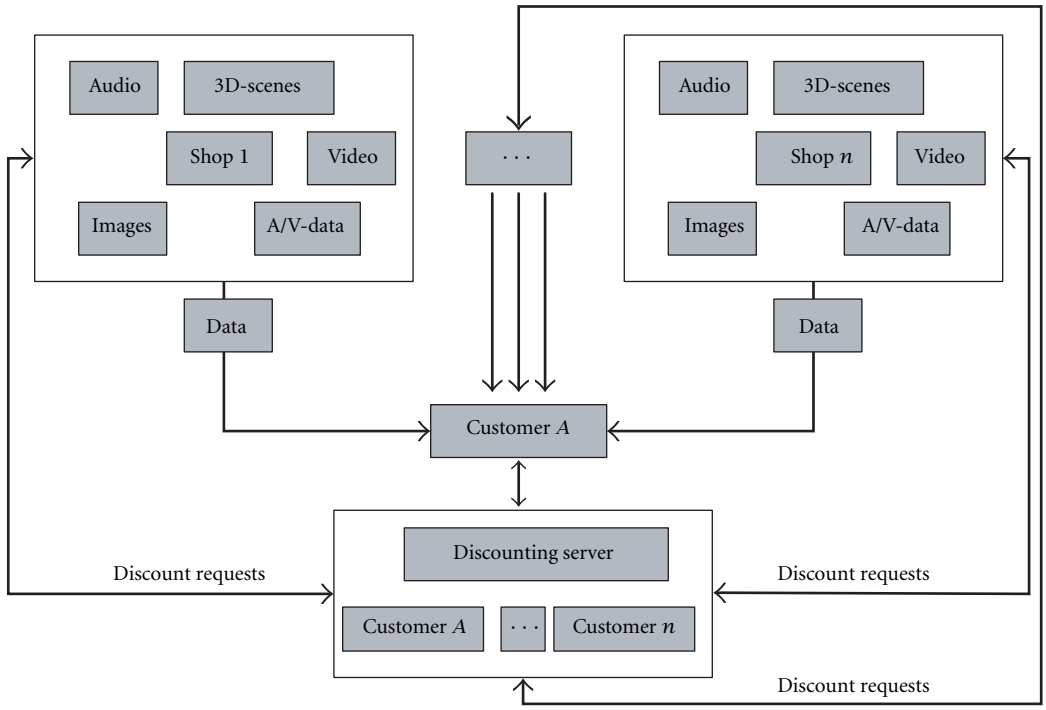

Figure 1: Discount approach.

4.2. Secret sharing approach

Approach (2) can be solved by cryptographic mechanisms, described in Section 3.1. The annotation watermark is only accessible when the user has collected all necessary shared keys or even a specific number of them. Figure 2 illustrates the secret sharing approach. The user retrieves several keys from other or the same party, which allows to access the annotation watermark. In the figure, he stores the partial keys in a key database locally. Only the annotation watermarking algorithm knows how to use the shared keys within a dedicated secret sharing scheme.

The secret sharing approach is shop independent without a discount server. The shops need a unique key basis to produce suitable shared keys.

To realize the secret sharing approach watermarking techniques can be combined with cryptographical mechanisms and organizational aspects. The main idea is to use a well-known cryptographic mechanism called secret sharing scheme where data are shared into several (secret) parts. Here, a secret split into n parts can be shared between n parties. The characteristic of these schemes is that the original data can only be reconstructed if and only if all n parts are known. There exist further secret sharing schemes like threshold schemes [27], where only at least t out of n parts (where $t \leq n$) need to be known to reconstruct the whole data. In the following, we will focus on the n-out-of-n approach where we need all parts. In our context, these parts are called partial keys.

Due to that, we split our data, for example, representing information about the customer-service into n partial keys. These keys should be stored on different places: firstly, we store one partial key as an annotation watermark in an image. All other $n-1$ partial keys are stored on other places—of course they can also be embedded in annotation watermark, and perhaps also different storage media in such a way that this data is only available separately. This means, the mechanisms might also differ in the way how partial keys are made available. Depending on the application, it needs to be analyzed how many partial keys and how many different storage media are practicable. For the description of the basic idea, in the following we will only look at data split into two partial keys.

Because in M-Commerce a large number of customers need to be addressed via a broadcast media (e.g., a newspaper), the annotation watermark represents one secret which is transported via the broadcast media. Therefore, a main requirement for annotation watermarks is that the embedded information is always identical. Otherwise, the application needs to provide different data for different users which cannot be realized from the perspective of a broadcast application. The other part of the necessary information (e.g., second part of the secret) is distributed via another way and might be stored on distinctive media. For instance, this secret data can be sold as an additional card concerning codes for access called access-code card. Those access codes can be presented, for example, by numbers or even barcodes, where a barcode-scanner can be connected with a personal computer or a personal digital assistant (PDA), or even by other images also including watermarks which can be recognized by the camera. If the card together with the annotation watermark is processed by the dedicated application, the original data

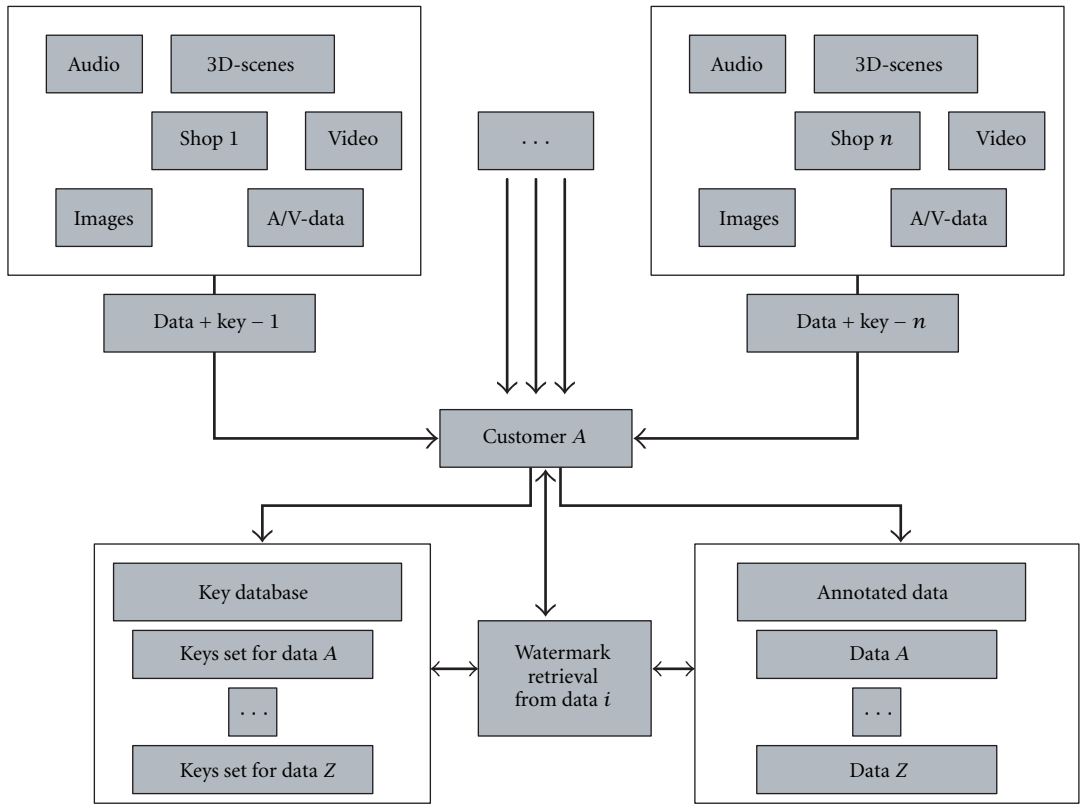

Figure 2: Secret sharing approach.

can be reconstructed by using both partial keys. Then, the user grants access to specific information or services. The secret sharing approach is very useful to realize Try&Buy transactions.

4.3. Partial access approach

In approach (3), the annotation watermark contains two parts: part 1 is fully accessible and part 2 is protected by one or more keys. Thus, approach (3) is a combination of a general accessible annotation watermark and approach (2). Figure 3 illustrates how the user can get access to the watermark.

We will point out the main proceeding and mechanisms by using two partial keys: a customer buys a newspaper where the images of advertisements include annotation watermarks but also one partial key k_1. Using his personal computer, he starts the dedicated application and shows the watermarked image to the camera used by the application. The camera scans the image and hands it over to the application that detects the annotation watermark as well as the partial key k_1. By using the information provided by the annotation watermarks, the customer gets connected to the dedicated internet page. The key k_1 causes the application to show the customer a message. This message concerns that he can get value-added services by buying specific access-code cards.

Now, the customer visits a (even internet-) shop where he can buy access-code cards. Here, he has to choose from different cards for different value-added services. He chooses one and pays for it.

Next time, the customer additionally shows his purchased access-code card providing another partial key k_2 for the specific service. This has to be done in an appropriate time window. Thus, the application reads the partial key k_2 and computes $I = f(k_1, k_2)$ by using the secret sharing scheme f. According to the value I, the application grants access to the web-pages and the value-added services.

Approach (3) is shop independent too, but needs a key distribution protocol. The partial access approach can be used to enhance Try&Buy mechanism by offering a combination of a free and a conditional access to the annotations. Furthermore, the approach can also be used as prepaid service.

4.4. Key watermark approach

In approach (4), the annotation watermark itself is used as a key for another annotation watermark, that contains, for example, the service for the customer. The key can represent, for example, information for the annotation watermarking algorithm how to retrieve the watermarking from specific data. This kind of annotation watermark can be used in approach (2) or (3) to provide the necessary keys. Here, the customer buys data with an annotation watermarking containing the key to access other annotation watermarks. The shop independent approach (4) is shown in Figure 4. The approach is appropriate for update services like Errata concepts where the update privileges are distributed as key watermarks.

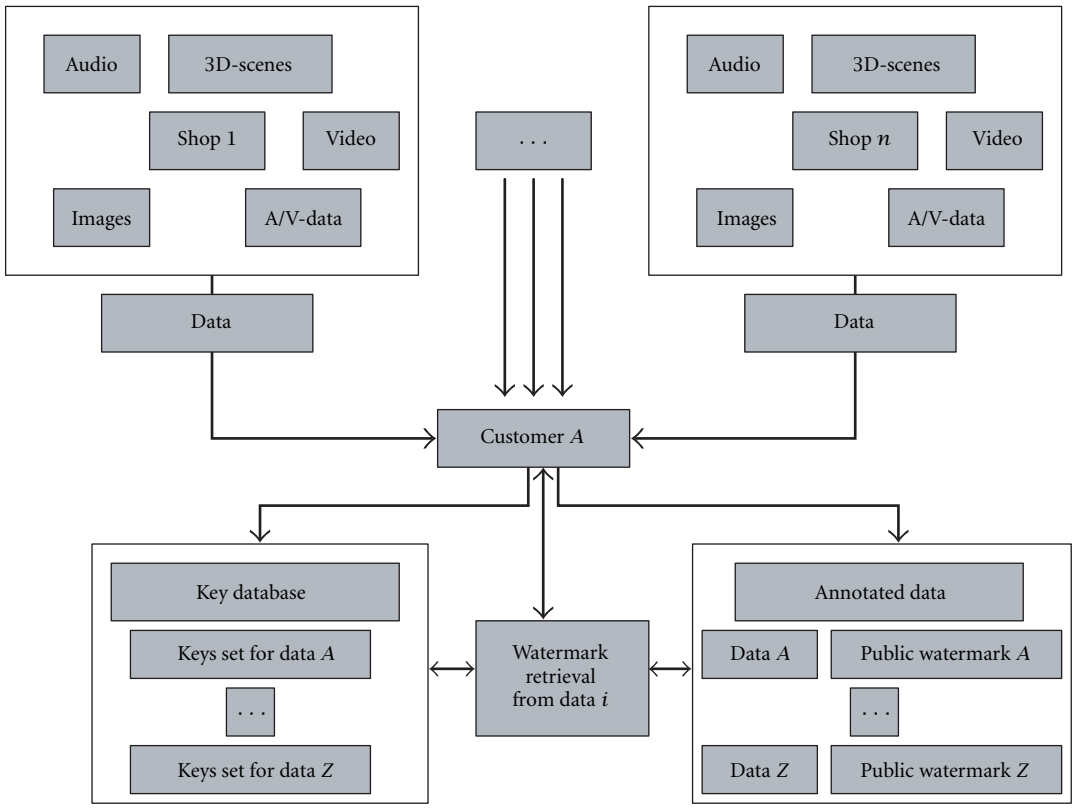

Figure 3: Partial access approach.

4.5. Watermarking parameter

As introduced, the most important properties of digital watermarking techniques are robustness, security, imperceptibility/transparency, complexity, capacity, invertibility, and possibility of verification. The annotation watermarks for conditional access solutions have the following requirements:

• *Robustness*: a watermark is called robust if it survives at least common media processing during transmission, storage and format conversions. Intended removal attacks are not to be expected in annotation watermarking, as the watermarks provide an additional service to the media owner.

• *Security*: the watermarking algorithm is considered secure if the embedded information cannot be destroyed, detected or forged, given that the attacker has full knowledge of the watermarking technique, has access to at least one piece of marked data material, but does not know the secret key. In opposition to robustness, the predicate security signifies resilience to intentional (nonblind) attacks on the watermark itself. Protocol attacks can also be seen as security attacks. They neither aim at destroying the embedded information nor at disabling the detection of the embedded information (deactivation of the watermark). Rather than that, they take advantage of semantic deficits of the watermark's implementation. An attack must not be able to copy the watermark. A copy attack, for example, would aim at copying a watermark from one image into another without knowledge of the secret key. Our annotation watermark should provide security against forged annotations and copying annotations from one media to another.

• *Imperceptibility*: the additional service must not reduce the quality of the transmitted media or else user or artist acceptance will not be sufficient. Therefore, the most important requirement of an annotation watermark is to keep the visual or audible quality of the media data. This leads to high perceptibility constrains.

• *Complexity*: in many cases the annotation watermarks are generated and embedded online into the media during the user request process (upload or transmission). Therefore, the embedding process has high performance requirements depending on the application scenario.

• *Capacity*: for the design of an annotation watermark we can use presence watermarks or binary information watermarks. The first class embeds a service specific pattern that can either be detected or not. The second class can embed a sequence of bits. These can be interpreted as service identifiers or other types of access control information.

• *Invertibility*: in most cases the watermark should be noninvertible. For some applications where high quality is required, invertibility could be an additionally provided service. Here the watermark could be detected and the connected service could be accessed. With the help of the embedded information the original cover data (as before the embedding process) could then be re-created. After this process the watermark cannot be detected any more.

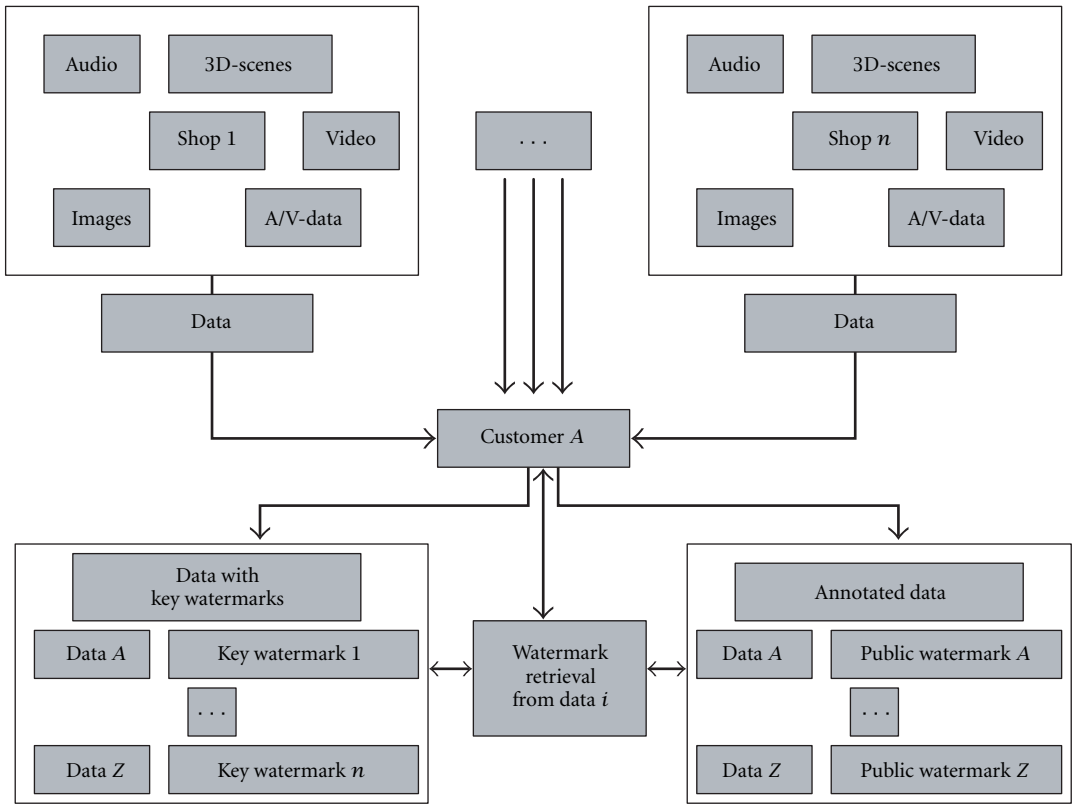

Figure 4: Key watermark approach.

• *Possibility of verification*: the watermark in most cases uses a symmetric key for embedding and retrieval. If an asymmetric method is required, the embedded information can be encrypted and decrypted with an appropriate scheme. The encrypted watermark could be detected by everyone, but only the owner of the correct key could interpret it correctly. In this case, an error correction code between encryption and watermarking will be necessary to ensure sufficient robustness.

4.6. Possible attacks

Initially, a value representing the access-right must be unique to a person who owns both, for example, the newspaper/image and the access code for additional data. This problem is easy to solve since the amount of possible values for secrets is large enough to prevent brute-force attacks.

Since access-code cards together with the watermarked image can easily be copied or handed out to other persons, there is need for additional mechanisms to prevent such a misuse. First of all, we can think of a (in some circumstances anonymous) registration where each user gets a unique registration number or registration data. This data can represent a third secret of a secret splitting scheme and therefore, the data can be used as an additional secret value within a secret sharing scheme.

Another solution to prevent misuse is that an access code can only be used once. After getting access to dedicated data, the access code gets invalid and thus, useless. This method might not be accepted by the customer because he has paid for the additional value. To avoid this, an additional (external) database provided by the dedicated company or even a trustworthy party might be established for keeping track of transactions attacks (e.g., store already invalid access codes and check for misuse) and vulnerabilities resulting by open issues. Of course, this raises the question of how to ensure privacy protection of customers—but this issue might be addressed with other methods.

A further solution to the problem mentioned above, is to change the access code by the company right after the customer used the code. This means that an access code is only used once (like a session code) and the customer gets another code for his next access. This is quite similar to the application of transaction numbers (TAN) well known from E-Banking. The code can also be generated after each session and then be transmitted to the customer. This assumes that the customer must allow to receive specific data that must be stored on his computer.

Finally, it needs to be determined how the application is set up, especially how many secrets are needed to support the access mechanisms for value-added services.

5. EXAMPLE SCENARIO: AUDIO ADVERTISEMENT BONUS PROGRAM

In this section, we describe in more details an example scenario using annotation watermarks as a tool for encouraging

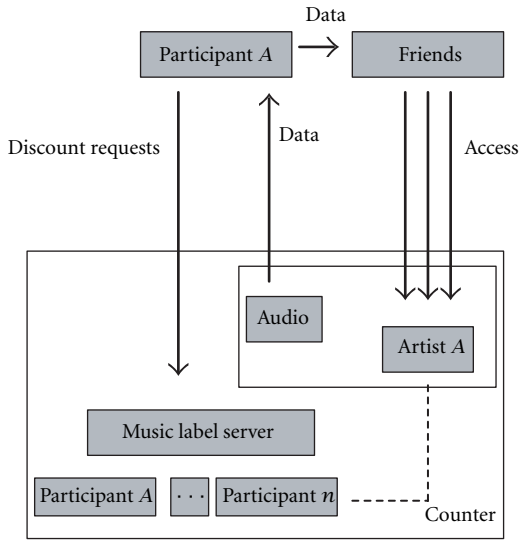

Figure 5: Example scenario based on the discount approach.

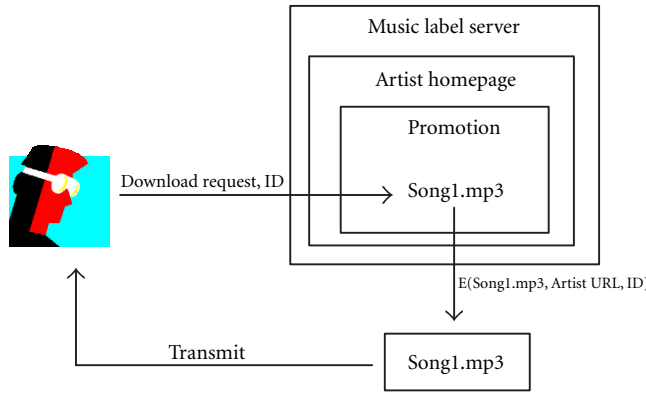

Figure 6: A song is marked with a URL and ID while downloaded.

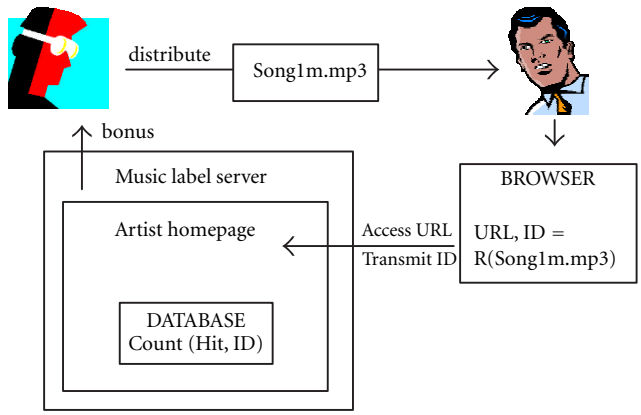

Figure 7: The song is distributed and the URL is used to access the corresponding website.

music fans to distribute promotional material of their favorite artists. It is the combination of Section 3.5 and an enhanced version of discount approach of Section 4. Using watermarking, technology distribution of the promotion material is analyzed by counting web hits and linked with the corresponding music fans ID.

Figure 5 shows how the discount approach has to be changed to fit into the bonus program scenario. In the original approach, the time the annotation watermark was accepted, was limited as it was used as a discount stamp. In the new scenario there is no limit. The number of times the watermark is used, is counted to calculate the success of the distributor. For the bonus program two annotated information types are necessary. The ID of the participant and the URL of the artist. The first is needed to identify the participant and provide a bonus. The later is the information that the party providing the bonus wants to be distributed.

An important issue is the voluntary nature of this approach. Annotation watermarking is used as an additional service and a technology to power a new kind of network for music fans. The downloading fans have to be aware that their identity is embedded in the songs. The ID should be anonymous in a way that the identity of the fan and the embedded ID can only be connected at the music server database.

In this scenario, there is a music fan F, an artist A, and a friend of F, G. First, F has to register at the music label server to get his ID. With this ID he is able to access promotional songs of the labels artists A. Whenever F downloads a song, a marked version is transmitted to him. In this version, his ID and the URL of A is included. Figure 6 shows this process.

The next step for F is to distribute the song among his friends, thereby doing advertisement work for A. Now G, one of the persons who get a copy of the marked song wants to learn more about the artist. G can use a special browser software reading the watermark of the song. The URL of A and the ID of F are retrieved. Now a web access can be established using the URL and at the same time transmitting the ID. The number of such accesses is counted in a database. Depending on this number, F can receive various bonus services like additional songs, price reduction at CD sales or merchandizing articles. Figure 7 illustrates the process.

In this way, a bonus program for advertising work of music fans can be set up without the need of new file formats and transparent to the customers that are not included in the program. The only problem is the special browser software. Only with a watermarking enabled browser the recipients of the marked songs can access the embedded information and thereby the artists' website. Such a browser should be free downloadable at the music label server. Then the distributor can provide a link together with the song for his friends to access the information. An important point is that the song, in this case coded as mp3, can still be played by every other software. The access to the information is a voluntary act.

The key distribution in this scenario is simple: everybody should be able to access the embedded information, the keys could be included in the browser software. Additional security against manipulations of the watermarks can be included using asymmetric encryption: the embedded information is encrypted using the music labels secret key, the browser

includes the public key to read the information. A third party cannot manipulate the embedded URL or ID and re-embed this information as the secret key is not available.

A possible attack here would be to use bots to simulate a large number of accesses and thereby collect many bonus points without having to distribute the song. The requirement for registration of everybody using the browser software could be one solution, but acceptance will be lower than with anonymous access to the artists' pages.

6. CONCLUSION AND FUTURE WORK

In our paper, we have introduced and discussed conditional access mechanisms for annotation watermarks. We have presented our approaches for conditional access solutions that will form the theoretical basis of our ongoing work. Currently, we are evaluating further approaches and develop and test a prototype system. Additionally, we analyze the importance and solutions of anonymity and pseudonymity to get an overall strategy without personalized registrations. Furthermore, the main goal is to have a shop independent or producer oriented approach.

Another key issue of our research is to ensure a high user acceptance. The process of hiding watermarks in the distributed and transmitted information with it has to be controllable by the user. He should be able to verify if information exists in the data, and in some approaches even could have the possibility of reading the embedded data before reacting to it.

We have discussed an example scenario using annotation watermarks for an advertisement bonus program using a modified discount approach. The watermarks are used as a transparent way to carry information. With this information, the success of individual participants of such a bonus program can be measured without much additional technical effort.

REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "A secure robust watermark for multimedia," in *Proc. Information Hiding: First Int. Workshop*, R. Anderson, Ed., vol. 1174 of *Lecture Notes in Computer Science*, pp. 183–206, Springer-Verlag, Cambridge, UK, 1996.

[2] M. Barni, F. Bartolini, V. Cappellini, A. Piva, and F. Rigacci, "A MAP identification criterion for DCT-based watermarking," in *Proc. European Signal Processing Conf. (EUSIPCO-98)*, vol. 1, pp. 17–20, proceedings published by the European Association for Signal Processing, Island of Rhodes, Greece, September 1998, ISBN 960-7620-05-4.

[3] D. Kundur and D. Hatzinakos, "A robust digital image watermarking scheme using the wavelet-based fusion," in *IEEE Signal Processing Society 1997: International Conference on Image Processing*, Santa Barbara, Calif, USA, October 1997, pp. 544–547.

[4] M. Kutter, F. Jordan, and F. Bossen, "Digital signature of color images using amplitude modulation," in *Proc. SPIE Storage and Retrieval for Image and Video Databases*, vol. 3022, pp. 518–526, San Jose, Calif, USA, February 1997.

[5] J. Fridrich, A. C. Baldoza, and R. J. Simard, "Robust digital watermarking based on key-dependent basis functions," in *Proc. Second International Workshop on Information Hiding*, pp. 143–157, Portland, Ore, USA, April 1998.

[6] J. Fridrich, "Combining low-frequency and spread spectrum watermarking," in *Proc. SPIE Int. Symposium on Optical Science, Engineering, and Instrumentation*, San Diego, Calif, USA, July 1998.

[7] S. Pereira, J. J. K. Ó Ruanaidh, and T. Pun, "Secure robust digital watermarking using the lapped orthogonal transform," in *Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 21–30, San Jose, Calif, USA, January 1999.

[8] J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection," in *Proc. International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies*, pp. 242–251, Vienna, Austria, August 1995.

[9] F. Hartung, JK. Su, and B. Girod, "Digital watermarking for compressed video, multimedia," in *Workshop at the Sixth ACM International Multimedia Conference*, pp. 77–79, Bristol, England, September 1998, Workshop notes published by GMD-Forschungszentrum Informationstechnik GmbH, GMD Report 41.

[10] J. Dittmann, M. Stabenau, and R. Steinmetz, "Robust MPEG video watermarking technologies," in *Proc. ACM Multimedia '98, The 6th ACM International Multimedia Conference*, pp. 71–80, Bristol, England, 1998.

[11] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals," in *Proc. IEEE International Conference on Multimedia Computing and Systems*, vol. 1174, Hiroshima, Japan, June 1996.

[12] P. Bassia and I. Pitas, "Robust audio watermarking in the time domain," in *Proc. European Signal Processing Conf. (EUSIPCO-98)*, vol. 1, pp. 25–28, proceedings published by the European Association for Signal Processing, Island of Rhodes, Greece, September 1998, ISBN 960-7620-05-4.

[13] L. Qiao and K. Nahrstedt, "Watermarking methods for MPEG encoded video: towards resolving rightful ownership," in *Proc. IEEE International Conference of Multimedia Computing and Systems*, pp. 276–285, Austin, Tex, USA, June 1998.

[14] O. Benedens, "Watermarking of 3D polygon based models with robustness against mesh simplification," in *Proc. SPIE Conference on Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 329–340, San Jose, Calif, USA, January 1999.

[15] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," in *Proc. Eurocrypt 96*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 84–95, Springer, Saragossa, Spain, May 1996.

[16] B. Pfitzmann, "Trials of traced traitors," in *Proc. First International Workshop on Information Hiding*, vol. 1174 of *Lecture Notes in Computer Science*, pp. 49–64, Springer, Isaac Newton Institute, Cambridge, UK, 30 May–1 June 1996.

[17] J. Dittmann, A. Behr, M. Stabenau, P. Schmitt, J. Schwenk, and J. Ueberberg, "Combining digital watermarks and collision secure fingerprints for digital images," in *Proc. SPIE Conference on Electronic Imaging '99, Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 171–182, San Jose, Calif, USA, January 1999.

[18] T. Kalker, "System issues in digital image and video watermarking for copy protection," in *IEEE International Conference on Multimedia Computing and Systems*, vol. 1, pp. 562–567, Florence, Italy, June 1999.

[19] "Digimarc, Mediabridge," www.digimarc.com.

[20] A. M. Alattar, "Bridging printed media and the internet via digimarc's watermarking technology," in *Electronic Proceedings ACM Multimedia 2000 Workshops*, Los Angeles, Calif, USA, November 2000, ISBN 1-58113-311-1.

[21] J. Fridrich, "Image watermarking for tamper detection," in *Proc. IEEE International Conference on Image Processing*, vol. 2, pp. 404–408, Chicago, Ill, USA, October 1998.
[22] J. Fridrich, "Methods for detecting changes in digital images," in *Proc. 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems (ISPACS '98)*, Melbourne, Australia, November 1998.
[23] R. Wolfgang and E. Delp, "Fragile watermarking using the VW2D watermark," in *Security and Watermarking of Multimedia Contents*, vol. 3657 of *Proceedings of SPIE*, pp. 204–213, San Jose, Calif, USA, January 1999.
[24] J. Dittmann, A. Steinmetz, and R. Steinmetz, "Content-based digital signature for motion pictures authentication and content-fragile watermarking," in *Proc. IEEE International Conference on Multimedia Computing and Systems*, vol. 2, pp. 209–213, Florence, Italy, June 1999.
[25] J. Dittmann, M. Steinebach, T. Kunkelmann, and L. Stoffels, "H2O4M-watermarking for media: classification, quality evaluation, design improvements," in *Proc. ACM Multimedia 2000 Workshops*, pp. 107–110, Los Angeles, Calif, USA, November 2000, ISBN 1-58113-311-1.
[26] J. Dittmann, P. Wohlmacher, and R. Ackermann, "Conditional and user specific access to services and resources using annotation watermarks," in *Communications and Multimedia Security Issues of the New Century, IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS-01), Darmstadt, Germany*, pp. 137–148, Kluwer, May 2001, ISBN 0-7923-7365-0.
[27] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

Jana Dittmann studied computer science and economy at the Technical University in Darmstadt and is a research assistant at the Fraunhofer Integrated Publication and Information System Institute (FHG-IPSI) since December 1996. She is specialized in the field of multimedia security. In 1999, she received her Ph.D. from the Technical University of Darmstadt. Her research is mainly focused on digital watermarking for copyright protection and content-based digital signatures for data authentication. In May 2001, she has opened at FHG-IPSI a competence center C4M (Competence for Media Security). Beside the design and realization of new security algorithms and applications, she publishes her work and has organized several special sessions about digital watermarking and the workshops "Multimedia and Security" at the ACM Multimedia '98, Bristol, UK, ACM Multimedia '99, Orlando, Fla, USA, ACM Multimedia '00, Los Angeles, Calif, USA, and ACM Multimedia '01, Ottawa, Canada. This year she organized the CMS2001 conference which took place in Darmstadt, Germany.

Martin Steinebach is a research assistant at Fraunhofer IPSI (Integrated Publication and Information Systems Institute). His main research topic is digital audio watermarking. Current activities are watermarking algorithms for mp2, MIDI and PCM data, feature extraction for content fragile watermarking, attacks on audio watermarks and concepts for applying audio watermarks in E-Commerce environments. He studied computer science at the Technical University of Darmstadt and finished his diploma thesis on copyright protection for digital audio in 1999. Martin Steinebach had been the organizing committee chair of CMS 2001 and is co-organizing the Watermarking Quality Evaluation Special Session at ITCC International Conference on Information Technology: Coding and Computing 2002. He is the representative of Ms. Dittmann at the C4M Competence Centre for Media Security.

Petra Wohlmacher is an assistant to the head of the section of electronic signatures at the Regulatory Authority for Telecommunications and Posts (Reg TP), Germany. During the last four years, she was a university assistant at the University of Klagenfurt, Austria. Before that, she was working as a researcher at the German National Research Center for Information Technology (GMD, now: Fraunhofer Institute) in Darmstadt within the smart card technology area. She derived a Dipl.-Math. in mathematics and informatics from the University of Darmstadt and a Doctors degree in mathematics from the University of Klagenfurt, Austria. She is a German Informatics Society member and sits on the leading committee of the Working Group 2.5.3, which is dealing with reliable IT-Systems.

Ralf Ackermann studied computer science at the Chemnitz University of Technology. After working for debis—the software company of Daimler Benz—he joined Darmstadt University of Technology in 1997 where he works on a Ph.D. dealing with IP Telephony in the team of Prof. Ralf Steinmetz (KOM - Industrial Process and System Communications). He leads and coordinates the efforts of a large scale IP Telephony Field Trial for the Darmstadt Scientific Region and is the author of a number of papers dealing with Distributed Interactive Multimedia Systems, IP-Telephony and Security.