Small or medium-scale focused research project (STREP) proposal

ICT Call 1

FP7-ICT-2007-1

Concealed Anonymous Private Actors

CAPA

Date of preparation: May 8th 2007

Participant no.	Participant organisation name	Part. short name	Country
1 (Coordinator)	Trialog	Trialog	France
2	Groupement des Cartes Bancaires	CB	France
3	Oracle	Oracle	Belgium
4	Telefónica Investigación y Desarrollo Sociedad Anónima Unipersonal	TID	Spain
5	Visual Tools	Vtools	Spain
6	Humboldt University	UBER	Germany
7	KU Leuven	KUL	Belgium
8	TU Dresden	TUD	Germany
9	U. Milano	UMIL	Italy

Work programme topics addressed

Objective ICT-2007.1.4: Secure, dependable and trusted Infrastructure

- Trusted computing infrastructures
- Identity management and privacy enhancing tools
- Longer term visions and research roadmap: metrics and benchmarks

Name of the coordinating person: Antonio Kung

e-mail: antonio.kung@trialog.com

fax: +33142928064

Proposal abstract

CAPA addresses the protection of private data. It will provide technology building blocks for the creation of "an invisibility cloak" (or "una CAPA invisible"). This involves

- an architecture for trusted storage platform suitable for embedded systems, based on an underlying secure operating system, secure file system and secure database system. The goal of this architecture is to limit the risk that private data be accidentally or maliciously disclosed. This risk is growing exponentially with the number of stakeholders who collect and analyze data.
- an architecture for privacy of actors, which combines algorithms that ensure protection of stored data with existing identity management building blocks. This architecture involves the use of a personal device that is based on the trusted storage platform, has communication capabilities, and has the ability to generate identifiers. The goal of this architecture is to show that intrusion of privacy can be avoided,
- addressing research challenges related to privacy, relating to
  - data linkage attacks, through means such as low-traffic analysis, surveillance, collusion etc…
  - privacy of access, through means such as steganographic file systems
  - policy management (e.g. to regulate release of private information, policies/metrics to assess the risks of information leakage when releasing private information)

A number of "CAPA invisible" use cases will be studied, related to privacy of payment, privacy of multimedia interaction, vehicle tracking avoidance, privacy-preserving surveillance. Demonstrations based on a reference implementation of the trusted storage platform integrated in a personal device are planned. CAPA will also investigate the impact of its results in terms of legal and ethical aspects and in terms of standardisation.

Table of contents

Glossary

DBA	Database Administrator
CAPA	Concealed Anonymous Private Actors
CVIS	Cooperative Vehicle Infrastructure Systems (IST IP project: http://www.cvisproject.org/)
EC	European Commission
EMC	Exploitation and Marketing Board
EPAS	Electronic Protocol Application Software (ITEA project)
FIDIS	Future of Identity in the Information Society (IST NOE project: www.fidis.net)
HGI	Home Gateway Initiative (www.homegatewayinitiative.org)
IT	Information Technology
OpenTC	Open Trusted Computing (http://www.opentc.net/)
OSGi	Open Service Gateway Initiative (www.osgi.org)
PET	Privacy Enhancing Technology
PMC	Project Management Committee
PASR	Preparatory Action for Security Research (http://ec.europa.eu/enterprise/security/index_en.htm)
PRIME	Privacy and Identity Management in Europe (IST IP project: https://www.prime-project.eu/)
RAS	Revealing Action Set
TCB	Trusted Computing Base
TCG	Trusted Computing Group (https://www.trustedcomputinggroup.org/)
TPM	Trusted Platform Module
TRL	Technology Readiness Level
TSP	Trusted Storage Platform
TTCN	Tree Tabular Combined Notation (ISO 9646)
SEPA	Single Euro Payments Area (http://en.wikipedia.org/wiki/Single_Euro_Payments_Area)
SEVECOM	Secure Vehicle Communication (IST STREP project: http://www.sevecom.org)
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
VM	Virtual Machine

Section 1: Scientific and/or technical quality, relevant to the topics addressed by the call

Concept and objectives

We are Electronically Naked

Electronically speaking, Europeans are naked. Cameras track our vehicles, credit cards timestamp our purchases, hospitals group our data, and vendors track our preferences. Some may argue that this is necessary for law enforcement purposes, but we disagree. After all, this wasn't the case before large databases and massive computational power made it possible. As database experts know too well, it is tempting for companies to mine medical, commercial, or even private marital data to "personalize" sales pitches or even to find likely targets for fraud. As this proposal tries to show, technology can be used to protect privacy just as it has been used to infringe it. Our goal is to show how far *it is possible* to protect privacy, recognizing that a lesser degree of privacy *may be preferable*. The devices and architectures we propose may be industrialized by telecommunications companies, banks, and vendors who believe that consumers may be interested in "buying privacy," not because those consumers have done anything wrong, but simply because human dignity demands it.

Concepts

The basic concept of our framework is that a user doesn't reveal his or her identity in his or her interactions with casual counterparties. Instead, one-time identifiers are used for purchases, hospital visits, location-based services, and even car-to-car communications. This potentially large set of identifiers is managed by a **user-private device** that can recall the identifier used in a particular interaction to, for example, return a defective device or obtain a discount. Occasionally, the user may wish to allow a counterparty to know that two or more of his or her identifiers refer to the same person or a video surveillance system may be able to make this inference. In either case, there is the danger that intersecting identifier sets may allow the possibility that privacy may be infringed. Estimating the risk of such infringement or inferring the cause is a second function of this **device**. As part of its communication function, the **device** will have to communicate with banks and credit card companies to pay for purchases and with governmental agencies to establish credentials such as eligibility for medical care. Managing such credential-enabled identifiers is the third major feature of this architecture. Finally, we will build on existing distributed database technologies to manage data transfer and querying of third party information, e.g. to aid the decision of which local restaurant to visit, in a privacy-preserving way.

Objectives

CAPA addresses three types of objectives

- an **architecture for trusted storage platforms** which will support a wide range of privacy aware applications. CAPA complements existing initiatives and projects focusing on identity management and related protocols by taking the database viewpoint. The goal of the CAPA trusted storage platform is to prevent collected private data from being accidentally or maliciously disclosed at the storage level. This risk is growing exponentially (1) with the growth of a pervasive computing infrastructure, (2) with the number of stakeholders in charge of collecting and exploiting data. CAPA will focus on embedded storage platforms (e.g. owned by a person, installed in a home, embedded in a vehicle, or in a specific embedded device – camera, roadside equipment). Such trusted storage platforms include a number of specific building blocks such as a secure operating system, a secure file system, a secure database system, policy management support, trust and empowerment support.
- an **architecture for privacy of actors**, which combines the building blocks ensuring protection of stored data (i.e. based on the CAPA embedded trusted storage platform) with existing identity management building blocks (e.g. from existing projects such as Prime or Sevecom). This architecture involves
  - the specification of a user-private device that can manage identifiers, obtain credentials, determine the danger of privacy infringement, and interact with the user if there is a privacy/convenience trade-off;
  - the development of a privacy-preserving surveillance use case. This involves the construction of privacy-preserving surveillance devices that will offer either two streams of video, one of high resolution in case an incident arises (but which is erased if there has been no incident) and the other of the least resolution necessary to detect suspicious or criminal behaviour. The result will be perturbed data after which the techniques of privacy-preserving data mining [1] can be applied.
  - the development of location tracking avoidance use case. This involves the construction of V2V and V2I communication devices which properly store collected data in an anonymous manner (using Sevecom building block) and in a protected manner (using CAPA building blocks)
  - the development of a privacy enabling payment use case. This involves the construction of a personal device which can be used by individual persons to carry out anonymous payment to multiple vendors with credentials.
  - The development of a privacy enabling multimedia interaction use case. This involves the replacement of a service gateway by a privacy aware service gateway in an e-inclusion application for elderly and handicapped persons.

  Our demonstrations might show: (i) the use of different identifiers to pay for different goods, (ii) the joining of different identifiers for purposes of convenience, (iii) video stream systems in which people have their identity masked but are nevertheless sufficient for criminal surveillance (iv) a congestion based pricing scheme where if an

anonymous payment takes place then the video surveillance shuts off – privacy need not be infringed if no criminal act has taken place (v) obtaining a credential from one authority and then using it when entering a hospital.

- Investigation of **challenges for privacy, with a focus on database**
  - Linkage attacks: linkage refers to the inference that several different identifiers all refer to the same person; a linkage attack is the attempt to associate a set of actions with an individual such that the actions would be sufficient to identify an individual with high likelihood. Such a set is called a "Revealing Action Set" or RAS below. The device will determine when the possibility of a linkage attack would result in a Revealing Action Set.
  - Privacy of access: much personal information can be derived from the observation of which information is retrieved by a particular user, as the access criteria reveals aspects of the profile of the user. We will investigate methods to guarantee privacy protection to users accessing information in a database or file system. These privacy-enhancing mechanisms should protect users even if the storage devices are controlled by the adversary.
  - Database policy management: this deals with the regulation of private data access and use, taking into account privacy threats over data collection/releases. We will need to get an understanding (1) on these privacy threats, (2) on how privacy can be measured in order to assess the risks of information leakage when releasing data. This will allow us to get an define policies to regulate access and use of private data and to identify techniques for associated privacy protection.

The table below summarises CAPA objectives, the associated milestone and the way these objectives can be verified.

Type of objective	Objective	Description	Milestone	Verification in project
Trusted Storage Platform	O1	*Architecture for trusted storage platform*	M2	Use in four privacy use cases (D22) Evaluation activity (D29,D31) Exploitation potential in PUD (D7,D20,D34)
	O2	*Secure operating system and file system*	M4	Integration in platform TRL indicator (D29)
	O3	*Secure database*	M4	Integration in platform TRL indicator (D29)
	O4	*Policy management support*	M4	Integration in platform TRL indicator (D29)
	O5	*Trust and empowerment support*	M4	Integration in platform TRL indicator (D29)
Architecture for Privacy of Actors	O6	*Architecture for privacy of actors involving a privacy aware personalised device*	M2	Four privacy use cases (D12) Evaluation activity (D29)
	O7	*Privacy enabling payment use case*	M4	Demonstration Evaluation activity (D29)
	O8	*Privacy enabling multimedia interaction use case*	M4	Demonstration Evaluation activity (D29)
	O9	*Vehicle tracking avoidance use case*	M4	Demonstration Evaluation activity (D29)
	O10	*Privacy preserving surveillance use case*	M4	Demonstration Evaluation activity (D29)
Challenges for Privacy	O11	*Linkage attacks roadmap* *Advance in collusion attacks*	M5	Research publications Proof of concept (D23) Roadmap (D30)
	O12	*Privacy of access roadmap* *Advance in privacy protection to users accessing information in a database*	M5	Research publications Proof of concept (D23) Roadmap (D30)
	O13	*Policy issues roadmap* *Advances in policy management to regulate access and use of data.*	M5	Research publications Proof of concept (D23) Roadmap (D30)

Note that CAPA objectives precisely address the issues related to data protection explained in the press release from the European commission published on May 2nd 2007 (see section 5).

1.2 Progress beyond the state-of-the-art

Data Protection versus Identity Management

CAPA takes the point of view that for most applications the privacy of actors can be achieved only through the combination of both identity management building blocks and of data protection building blocks. While many projects (FIDIS, PRIME, SEVECOM) are focusing on identity management, little work has been carried out concerning data protection building blocks for privacy. This is the objective of CAPA to fill this gap. We will therefore focus on building a suitable trusted storage platform.

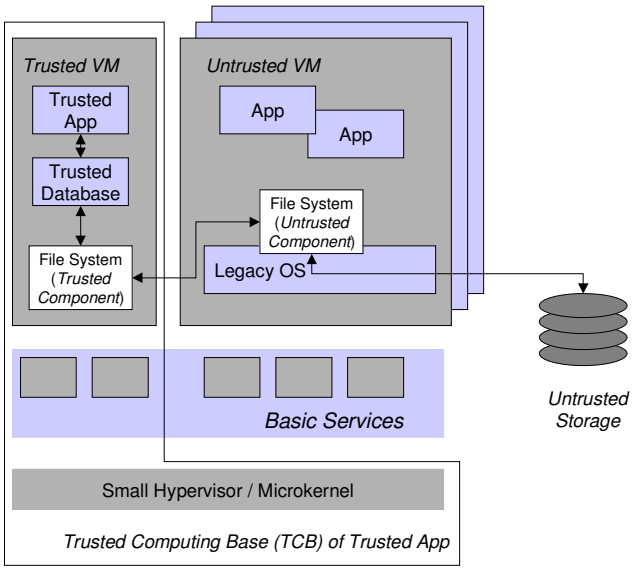
Privacy in Database

Because databases often store data about individuals, their very reason for being seems antagonistic to privacy. When databases were used primarily to process transactions, , their ability to infringe on privacy was nevertheless limited. For the last fifteen years, however, a confluence of algorithms and increasingly capable hardware has enabled data to be pooled and "mined". Linking and mining credit card, telephone, internet purchase, and banking transactions could practically enable near total surveillance of a population. The database research community has proposed mitigating technologies, notably data perturbation in which noise is added to data to permit aggregate conclusions (e.g., sell religious novels at airports) without infringing on privacy [1] as well as policy desiderata regarding the management and disposal of data (e.g. hippocratic databases [2]). Unfortunately, most of these technologies depend on trusting the organizations that collect data. A principle goal of CAPA is to reduce this necessary level of trust to a minimum. Specifically, CAPA provides each individual with a database on a personal device that tracks his or her activities. The data on that device is replicated nowhere else (at least not in the clear).

Trusted Operating Systems

Most operating systems (Oses) and storage systems today are difficult to trust. Mainstream operating systems such as Microsoft Windows or Linux suffer from a number of weaknesses that are rooted in their extremely complex architecture. They consist of millions of lines of code, with significant parts of their functionality being implemented within the kernel, for example, device drivers and complex protocol stacks such as networking stacks.

To cope with this, previous work in the area of operating-system construction therefore examined ways to decompose operating systems into separated components of lower complexity. During the last decade [38], an important example of this work has been conducted by the operating systems group at TU Dresden and resulted in the Nizza Security Architecture [28] with a reference implementation being based on the L4/Fiasco micro-kernel. This architecture allows one to isolate potentially faulty components such as device drivers as well as to effectively protect highly-sensitive applications. It supports concurrent execution of multiple virtual machines, which can be light weight hosting specific isolated applications only, or they can be used to run complete commodity OSes in legacy containers. The isolation of many small components also enables the concept of application-specific trusted computing bases, meaning that applications need only rely on system components they actually depend on. Furthermore, even small components can provide powerful services by reusing complex functionality that is implemented outside their TCBs. For example, storage or network stacks provided by untrusted commodity OSes can be reused through well-defined and secure interfaces called trusted wrappers [28].



The figure above shows a possible configuration based on the Nizza architecture: A trusted application running in its own virtual machine depends on a database and a secure file system. The file system is split into two components and reuses untrusted storage infrastructure provided by an untrusted legacy operating system through a trusted wrapper. Note that the TCB of the application only comprises those components providing the required services and the micro-kernel or hypervisor.

With the large experience gained in the past, TU Dresden's operating systems group is currently active in other EU projects such as ROBIN [54], where the technology is further developed and more advanced implementations are created. This previous work on how to build secure systems provides a solid basis for the CAPA project.

CAPA Trusted Operating System and Trusted File System

The progress which the CAPA project intends to bring is now described.

The ability to securely store user information is a crucial requirement within this project, for example when users do electronic transactions or use electronic communication networks. In CAPA, we will develop infrastructure for secure storage at the level of both file systems and database systems. A secure file-system implementation is to be used as the foundation of the database systems that stores privacy-related data.

We consider it likely that privacy-related data will be processed on devices that users also use for unrelated tasks such as browsing the Internet or playing games. Thus, there is a considerable risk that malicious software gets onto the device. As outlined above, current commodity operating systems (OSes) cannot effectively protect individual applications and the data they process – for example the software components that use privacy-related data from the aforementioned database. Existing solutions that allow for fine-grained access control based on roles such as SELinux [52] still suffer from high complexity of the underlying commodity OSes, which consist of millions of lines of code. Frequently found security-related bugs [53] in those large code bases enable attackers to circumvent access control boundaries.

Therefore, we will base the design of CAPA's storage architecture on a secure component-based on a small hypervisor that allows the isolation of sensitive applications in virtual machines (VMs). The key argument for this approach is that the use of such a small hypervisor [30] and a stripped-down OS in the VM results in a smaller trusted computing base (TCB) for the isolated application. As the commodity OS and other software running on top of it are no longer part of this TCB, the attack surface becomes smaller, too. For certain types of applications, the size and complexity of the TCB can be reduced even further by extracting and isolating the security-critical parts only. For example, an email client could be split so that the functionality required for digitally signing as well as encrypting and decrypting messages can be moved into a separate VM. We will evaluate specific requirements on such an operating system that arise from the use cases in this project.

We will also use the idea behind the described split-application approach for the design and implementation of the secure file system. We separate its security-critical parts from the functionality that does not need to be trusted, such that only a small part of the overall file-system functionality becomes part of the TCB. On the other hand, the secure part will reuse an existing legacy file-system stack and untrusted storage to provide a competitive feature set nonetheless. Confidentiality and integrity of the file-system data is ensured by means of cryptography. Unlike previous work [33][43], we aim to achieve full integrity and freshness of a complete, local file system and on protection against both online and offline attacks. Furthermore, we will evaluate the specific requirements on the OS coming from the database system used at the higher levels. Major research challenges in this context are low-complexity mechanisms and strategies for recoverability in case of data loss (e.g., due to attacks or system failures).

Based on this architecture, the file-system functionality enlarges an application's TCB by only a few thousand lines of code compared to tens or even hundreds of thousand lines of code comprising the file-system stack of a commodity OS. Thus, the file system we will develop for this project can provide the required storage infrastructure with a small code base, which is considered to be less vulnerable to security-related software errors.

CAPA Trusted Storage Platform

Using a trusted storage platform will guarantee that stored data cannot be maliciously or just accidentally disclosed, e.g. an employee of a company operating the data could accidentally disclose the data by just throwing away, a backup CD or DVD containing the data in the clear.

Based on the resulting trusted operating system and file system, a number of system functions will be added in order to get a trusted storage platform:

- security functions (typically encapsulated in a security module, possibly conforming to TPM from the trusted computing group [49]) such as secure generation of random numbers, secure communication layer interaction, and encryption of data;
- a secure database, i.e. a database engine which is enriched with protection features so that stored data cannot be accidentally or maliciously disclosed. The starting point will be Oracle open source Berkeley DB [48]. Berkeley DB is a high performance, scalable and reliable non-relational storage system. An outgrowth of research performed initially at the University of California at Berkeley, and later continued at Harvard University, Berkeley DB was designed from the very beginning to be an embeddable database engine, so no separate server is required, and no runtime human administration is needed. Berkeley DB is a tool for software developers, not for IT professionals or DBAs. It is intended to provide fast, reliable data storage for applications. The only way to use Berkeley DB is to write code.
- privacy aware policy management support
- support for trust and empowerment

Research Challenges on Privacy

Since CAPA focuses on data protection aspects rather than identify management aspects, CAPA will investigate related challenges : linkage attacks, privacy of access, policies.

Linkage Attacks

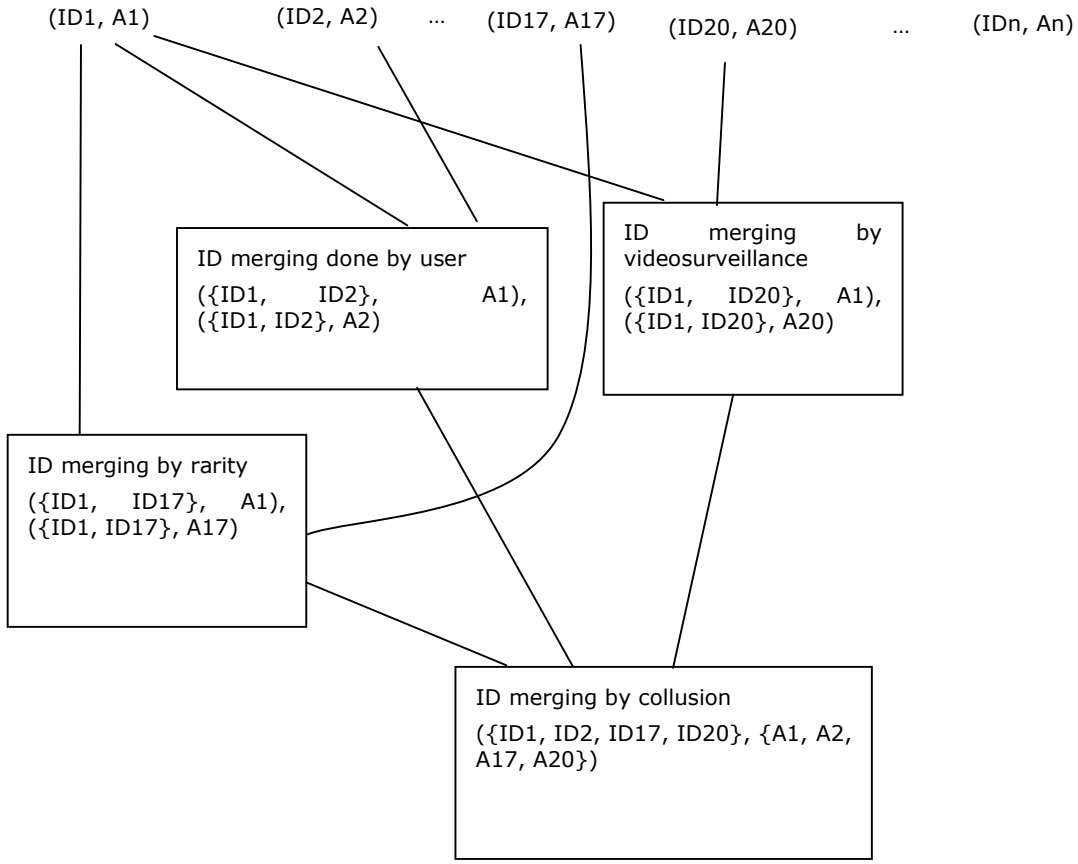
To formalize the dangers to privacy, we introduce the notion of a *Revealing Action Set,* or *RAS* for short. A RAS is a set of action-datetime pairs such that if all those actions were known to be associated with a given individual, it would be possible to identify that individual and what he/she has done. An action here could be a database query, a purchase, a visit to a doctor, access to a file, or a web search. How might a privacy adversary associate a RAS with an individual?

We assume that each action taken by an individual is associated with a different and unique identifier (note the identifiers will be very big and randomly generated, so we can assume they are globally unique). We can abstract this as a set of pairs (ID1, A1), (ID2, A2), …, (IDn, An) where the Ai represents an action-datetime pair. When the identifiers associated with different actions are inferred to come from the same individual, then we say they have been *merged.* The result of merging is an *identifier set*. Identifier sets can also be merged into larger identifier sets. Suppose that the identifier set ISi associated with Ai is merged with the identifier set ISj associated with Aj. We then associate ISi union ISj with Ai and Aj.

How does merging happen?

1. (*Voluntary*) The identifier owner might voluntarily merge two identifier sets, by saying that he/she performed both action Ak and Am, e.g. to send a test result to a doctor. This assertion should probably be associated with a credential.
2. (*Surveillance*) Some surveillance system (e.g. video surveillance or an observant clerk) might note that actions Ak and Am were done by the same person.
3. (*Rarity*) Actions Ak and Am may happen in a particular relationship in time thus allowing a human or software system to infer that they were done by the same person, e.g. by a moving vehicle.
4. (*Collusion*) Two entities that have interactions with individuals through identifier, action pairs may collude to combine their identifier sets in the hopes there is some overlap. That is, if we know that identifier set X has a non-null intersection with identifier set Y, then all the identifiers in both set correspond to the same person.

We show how these different mechanisms for merging might interact in the following figure. Note that collusion at the end shows that all of actions A1, A2, A17, A20 were done by the same person. If this is a RAS, the user's privacy may be infringed.



Potential collusion monitoring is the activity of determining whether there is a RAS if two or more identifier sets are merged. This can be accomplished by connected components algorithm if the identifier sets are known. The identifier sets are clearly known for the voluntarily merged sets. They may be known for rarity-based merged sets [14][27]. It might also be possible when surveillance is known to exist.

For example, privacy considerations suggest changing identifiers as one travels. However, if there is continuous monitoring of vehicles along a certain road, then a person who uses that road must assume that identifiers along the road could all constitute an identifier set [27]. Similarly, if the video surveillance systems in two different stores yield high resolution images, then the identifiers used in those two stores could potentially constitute a single identifier set.

We say that two actions are "mergeable" by a monitoring/surveillance system if the surveillance system is able to link the two actions to the same individual. In such a case the identifiers associated with those two actions are a potential identifier set. We will say that a monitoring system is "privacy-conformant" if it doesn't allow merging.

Other database challenges have to do with a database system that sends out no data other than identifiers and rather imports data and performs clever query processing processing on a platform that is weak relative to personal computers.

The basic database functionalities are:

- Generate large random identifiers for each interaction with counterparties. Maintain an association between those identifiers and the concerned counterparties in case repeated interactions are needed (e.g. for warranty-based repairs).
- Keep track of potential identifeier sets established voluntarily or by surveillance systems that cause two or more actions to be mergeable.
- Advise an individual about the privacy risks inherent in a certain interaction based on the notion of a RAS.

Legal viewpoint on linkage attacks

Clearly, there is an intersect here with the concepts used in data protection regulation, which governs all personal data, i.e. any information relating to an identified or identifiable natural person. The precise contours of the notion 'personal data' are under constant debate, notably because technological advances challenge its boundaries. The same holds for the notion 'identifiable', which is explored here. A legal analysis will accompany the technological research, with the aim of further developing our understanding of legal concepts as well as identifying legal risks and opportunities for the implementation phase.

Privacy of Access

Privacy as the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others, has become the focus of research by different communities. One of the aspects that has received attention in research is the protection of privacy while accessing data or services over the net. The goal could either be to protect the content of messages, i.e. confidentially sending a request or receiving the answer to a request. Both can be achieved by encrypting the messages between the sender and the receiver. Alternatively, the goal might be to protect the identity of the sender, i.e., to ensure that (s)he remains anonymous as the sender or receiver of messages. One of the more prominent methods is based on mixes [10]. Other methods to protect the privacy of senders and receivers of messages are based on dummy traffic [16], proxies ([50][51]), MIX-Networks ([36][20][18]), DC-Networks ([11][31][45]), or peer-to-peer networks ([37][25][26][41]).

Another approach to privacy-enhanced access to data is private keyword search, which is a technique that allows for searching and retrieving documents matching certain keywords without revealing the search criteria. The original private search scheme was proposed by Ostrovsky et al. [35], and efficiency improvements have been proposed in ([6][17]).

The goal of a steganographic file system is to protect the user from compulsion attacks in which the user is forced to hand over file decryption keys under the threat of legal sanctions or physical intimidation. In order to achieve this goal, the steganographic file system must conceal the files it stores, so that the user can plausibly deny their very existence.

The concept of a steganographic file system was first proposed by Anderson, Needham and Shamir in [3] together with two implementations. A more advanced design that protects against coercive attackers capable of taking a snapshot of the storage has been proposed in [34]. Zhou et al. proposed a system in [47] that tries to protect the storage from continuous observation by the adversary, but it was shown to be vulnerable to traffic analysis attacks in [44].

In the context of databases, so called hippocratic databases [2] and the notion of k-anonymity ([40][42]), the aim is to maintain a level of privacy that provides a balance between the right of people for privacy and the necessity to access data with private information. Agrawal and Srikant developed important solutions to protect privacy of individuals for data mining [1]. Recently, the work of Asonov and Freytag focused on how to protect privacy despite adversaries that might have complete control over a database management system ([4][5]).

Legal viewpoint on privacy of access

The technology proposed here has a double impact on data protection. For one, it provides a way to increase the security of personal data in storage, thus helping organisations comply with privacy regulation. Secondly, it reduces the risk of surreptitious data processing through monitoring and gives the data subject more direct control over his data.

Policy Management

A recurring theme in this work is that a privacy breach can occur if several actions can be linked to the same individual. Because these actions often leave a trail of transactional data, the project must also be concerned with attacks on the database(s) that hold the transactional data. Privacy breaches can be due, for instance, to inferences arising from relationships among data or from linking data (or collections thereof) to reconstruct dependencies among data (for instance correlating different logs, linking logs to actual data, or correlating actual data). While various works exist in the literature addressing the problem of inference and data linkage [24], existing solutions - already limited in many respects - are not applicable to the novel scenario considered by our project. Inference exposures and record linkage have been in fact investigated mainly in the context of multilevel databases (where attention has been focussing on classifying data against specific security classes), or statistical databases on aggregate data, while the protection of specific data (microdata) has received little consideration. Also, approaches to evaluate the protection of micro data collections typically addressed the problem by looking at the collection per se and generalizing, suppressing, or perturbing data to protect them [14]. Such assumptions do not apply in our context where data refer to specific instances of individuals, protected by one-time identifiers. The danger in our setting is that several such actions will be linked and create a “quasi-identifier”.

A further unique features of our setting is that any inference on data not only represents a privacy breach by itself, but also represents a means that attackers can use to further threaten the privacy of the data. For example, if an adversary knows that some individual goes to a certain bookstore and then to a certain bank within a small time

interval, the adversary can infer with high likelihood that a visit to a coffee shop between the two might have been done by the same person. Our project will investigate the different data threats to which individuals are exposed and provide a model and techniques to preserve the privacy of data.

Previous literature combining data collection and encryption has focussed on the problem of outsourcing data and - typically - has assumed that an overlay layer of encryption was applied on the data, then focussing on the problem of querying data without the need of decrypting them [21]. Typical solutions (e.g. [29][15][8][7]) based on the association with the data of indexes (related to data but not disclosing them [10]), which allowed execution of certain queries, and assumed that a single key was used to encrypt the complete data collection, therefore requiring the data owner to mediate every query execution. Such an assumption is clearly not applicable to our scenario where the data owner cannot be assumed to mediate all access to his or her data (once they have been released), where data collection can refer to data from different users (and therefore should be encrypted with keys regulated by different individuals), and where data may need to be selectively released to different parties (and therefore - again - encrypted with different keys). Our project will advance existing approaches by addressing the characteristics just mentioned and devising novel techniques for protecting data stored by individuals, by external parties, or released.

A further interesting problem that will be addressed by the project is the identification and definition of policies for regulating data access, release, and use in the considered scenario. Many access control models and languages exist in the literature allowing the representation of different kind of policies [39]. Recent approaches enjoy more expressiveness and do not require user authentication in order to get some services or access some data (e.g., [7][46][20]) . However, even recent proposals assume all data about the user is in the clear (no encryption protection offered), do not allow (if not for limited functionalities) the specification of restrictions on data after they have left the individuals, and completely ignore the protection of the data that refers to the interaction itself (log data that can be used for linkage and re-identification that are a particular focus of our project). Our project will investigate and propose novel approaches for specifying and enforcing policies that take all these features into account.

CAPA Innovation

The following table summarises CAPA innovation.

Category	Today	Planned Innovation
Data storage	No personal trusted storage platform available in the market to ensure protection of collected data to support privacy aware applications	• An architecture for embedded storage platform • Availability of an open source reference implementation platform based on existing bricks (OS and file system from TU Dresden, database from Oracle) and providing suitable policy management, trust and empowerment support
Privacy of actors	Most approaches today are policy based. There is no attempt to build a personalised technological infrastructure to preserve electronic privacy	• Definition of an architecture based on the integration in a personalised device of the embedded storage platform endowed with identification management and other privacy enhancing building blocks • Development of a privacy preserving surveillance application based on this architecture • Development of a privacy enabled payment application based on this architecture • Development of a privacy enabled multimedia application based on this architecture • Development of a location privacy preserving vehicle application based on this architecture
Challenges for privacy of collected data	Many issues related to privacy of collected data not well understood today	• Contribution to understanding of linkage attacks, including proof of concepts and a roadmap • Contribution to understanding on privacy accesss, including proof of concepts related to steganographic data and a roadmap • Contribution to understanding of policies related to privacy to regulate release of private information and policies/metrics to assess risk of information leakage

References

[1] Rakesh Agrawal and Ramakrishnan Srikant. Privacy preserving data mining. In Proceedings of the ACM SIGMOD Conference on Management of Data, pages 439–450. ACM Press, May 2000.

[2] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, Yirong Xu. Hippocratic Databases. In Proceedings of the 28th VLDB conference, 2002

[3] Ross J. Anderson, Roger M. Needham, and Adi Shamir. The steganographic file system. In Proceedings of the Second International Workshop on Information Hiding, LNCS 1525, pages 73–82. Springer-Verlag, 1998.

[4] Dimitri Asonov, Johann-Christoph Freytag: Almost Optimal Private Information Retrieval, Pre- and Postproceedings of the 2nd Workshop on Privacy Enhancing Technologies (PET2002) San Francisco, USA, 2002

[5] Dimitri Asonov, Johann-Christoph Freytag: Repudiative Information Retrieval, Pre- and Postproceedings of the First ACM Workshop on Privacy in the Electronic Society (WPES2002) Washington DC, USA, 2002

[6] John Bethencourt, Dawn Song, and Brent Waters. New constructions and practical applications for private stream searching (extended abstract). In SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06), pages 132–139, Washington, DC, USA, 2006. IEEE Computer Society.

[7] Bonatti, P., Samarati, P., A Unified Framework for Regulating Access and Information Release on the Web, in Journal of Computer Security, vol. 10, n. 3, 2002, pp. 241-272.

[8] Luc Bouganim, François Dang Ngoc, Philippe Pucheral, Lilan Wu, "Chip-Secured Data Access: Reconciling Access Rights with Data Encryption", VLDB 2003.

[9] Bouganim, L., Pucheral P., Chip-Secured Data Access: Confidential Data on Untrusted Servers, in Proc. of the 28th International Conference on Very Large Data Bases, Hong Kong, China, August 20-23, 2002.

[10] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 65-75

[11] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. Journal of Cryptology, 1:65–75, 1988.

[12] Ceselli, A., Damiani, E., De Capitani di Vimercati, S., Jajodia, S., Paraboschi, S., Samarati, P., Modeling and Assessing Inference Exposure in Encrypted Databases, in ACM Transactions on Information and System Security (TISSEC), vol. 8, n. 1, February 2005, pp. 119-152.

[13] Ciriani, V., De Capitani di Vimercati, S., Foresti, S., Samarati, P., k-Anonymity, in Secure Data Management in Decentralized Systems, T. Yu and S. Jajodia (eds), Springer-Verlag, 2007.

[14] Ciriani, V., De Capitani di Vimercati, S., Foresti, S., Samarati, P., Microdata Protection, in Secure Data Management in Decentralized Systems, T. Yu and S. Jajodia (eds), Springer-Verlag, 2007.

[15] Damiani, E., De Capitani di Vimercati, S., Jajodia, S., Paraboschi, S., Samarati, P., Balancing Confidentiality and Efficiency in Untrusted Relational DBMSs, in Proc. of the 10th ACM Conference on Computer and Communications Security, Washington, DC, USA, October 27-31, 2003.

[16] Wei Dai: Pipenet 1.1. Usenet post, 1996.

[17] George Danezis and Claudia Diaz. Space-Efficient Private Search. To appear in the Proceedings of Financial Cryptography 2007, 15 pages, LNCS, Springer, 2007.

[18] George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In IEEE Symposium on Security and Privacy, Berkeley, CA, 11-14 May 2003.

[19] Dawson, S., De Capitani di Vimercati, S., Lincoln, P., Samarati, P., Maximizing Sharing of Protected Information, in Journal of Computer and System Science, vol. 64, n. 3, May 2002, pp. 496-541.

[20] De Capitani di Vimercati, S. Foresti, S. Jajodia, P. Samarati, "Access control policies and languages," in Int. J. Computational Science and Engineering, 2007.

[21] De Capitani di Vimercati, S., Foresti S., Jajodia, S., Paraboschi, S., Samarati, P, "Privacy of Outsourced Data," in Digital Privacy: Theory, Technologies and Practices, A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis, and C. Lambrinoudakis (eds), Taylor and Francis, 2007.

[22] De Capitani di Vimercati, S., Jajodia, S., Paraboschi, S., Samarati, P., Trust Management Services in Relational Databases, in Proc. of the ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'07), Singapore, March 20-22, 2007.

[23] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004.

[24] C. Farkas and S. Jajodia, "The Inference Problem: A Survey", in SIGKDD Explorations, vol. 4, n. 2, 2003. pp. 6-11.

[25] Michael J. Freedman and Robert Morris. Tarzan: A peer-to-peer anonymizing network layer. In Vijayalakshmi Atluri, editor, ACM Conference on Computer and Communications Security (CCS 2002), pages 193–206, Washington, DC, November 2002. ACM.

[26] Sharad Goel, Mark Robson, Milo Polte, and Emin Gun Sirer. Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. Technical Report 2003-1890, Cornell University, Ithaca, NY, February

[27] Marco Gruteser and Dirk Grunwald, "Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking," Proceedings of First ACM/USENIX International Conference on Mobile Systems, Applications, and Services (MobiSys), San Francisco, CA, May 2003 .

[28] H. Härtig, M. Hohmuth, N. Feske, C. Helmuth, A. Lackorzynski, F. Mehnert, and M. Peter. The Nizza Secure-System Architecture. In Proceedings of CollaborateCom, 2005.

[29] Hacigümüs, H., Iyer, B., Mehrotra. S., Li, C., Executing SQL over Encrypted Data in the Database-Service-Provider Model, in Proc. of the ACM SIGMOD 2002, Madison, Wisconsin, USA, June 3-6, 2002.

[30] M. Hohmuth, M. Peter, H. Härtig, and J. S. Shapiro. Reducing TCB size by using untrusted components — small kernels versus virtual-machine monitors. In Proceedings of the Eleventh ACM SIGOPS European Workshop, Leuven, Belgium, Sept. 2004.

[31] Philippe Golle and Ari Juels. Dining cryptographers revisited. In Proceedings of Eurocrypt 2004, May 2004.

[32] Jajodia, S., Samarati, P., Sapino, M.L., Subrahmanian, V.S., Flexible Support for Multiple Access Control Policies, in ACM Transactions on Database Systems, vol. 26, n. 2, June 2001, pp. 214-260.

[33] J. Li, M. Krohn, D. Mazieres, and D. Shasha. Secure Untrusted Data Repository (SUNDR). In Proceedings of the 6th USENIX Symposium on Operating Systems Design and Implementation (OSDI), pages 121–136, San Francisco, CA, Dec. 2004.

[34] Andrew D. McDonald and Markus G. Kuhn. Stegfs: A steganographic file system for linux. In Proceedings of the Third International Workshop on Information Hiding, LNCS 1768, pages 462–477. Springer-Verlag, 1999.

[35] Rafail Ostrovsky and William E. Skeith III. Private searching on streaming data. In Victor Shoup, editor, CRYPTO, volume 3621 of Lecture Notes in Computer Science, pages 223–240. Springer, 2005.

[36] Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. ISDN-mixes: Untraceable communication with very small bandwidth overhead. In Wolfgang Effelsberg, Hans Werner Meuer, and Gunter Muller, editors, GI/ITG Conference on Communication in Distributed Systems, volume 267 of Informatik-Fachberichte, pages 451–463. Springer-Verlag, February 1991.

[37] Michael Reiter and Aviel Rubin. Crowds: Anonymity for web transactions. ACM Transactions on Information and System Security (TISSEC), 1(1):66–92, 1998.

[38] Roitzsch, Härtig: Ten Years of Research on L4-Based Real-Time; proceedings of the Eighth Real-Time Linux Workshop, Lanzhou, China, 2006 , 2006

[39] Samarati, P., De Capitani di Vimercati, S., Access Control: Policies, Models, and Mechanisms; Foundations of Security Analysis and Design, Springer 2001, LNCS 2171.

[40] P. Samarati, "Protecting Respondent's Privacy in Microdata Release," IEEE Transactions on Knowledge and Data Engineering, vol. 13, n. 6, November/December 2001, pp. 1010-1027

[41] Rob Sherwood, Bobby Bhattacharjee, and Aravind Srinivasan. P5: A protocol for scalable anonymous communication. In IEEE Symposium on Security and Privacy, page 58, Berkeley, California, USA, 12-15 May 2002. IEEE Computer Society.

[42] L. Sweeney, k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570

[43] R. Ta-Min, L. Litty, and D. Lie. Splitting Interfaces: Making Trust Between Applications and Operating Systems Configurable. In 7th USENIX Symposium on Operating Systems Design and Implementation (OSDI 2006), November 2006.

[44] Carmela Troncoso, Claudia Diaz and Bart Preneel. Traffic Analysis Attacks on a Continuously-Observable Steganographic File System. Accepted at Information Hiding 2007, 15 pages, LNCS (to appear), Springer, 2007.

[45] Michael Waidner and Birgit Pfitzmann. The dining cryptographers in the disco — underconditional sender and recipient untraceability with computationally secure serviceability. In Jean-Jacques Quisquater and Joos Vandewalle, editors, Advances in Cryptology (Eurocrypt '89), volume 434 of LNCS, page 690, Houthalen, Belgium, 10-13 April 1989. Springer-Verlag.

[46] Yu, T., Winslett, M., Seamons, K.E., Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust, ACM Transactions on Information and System Security (TISSEC), vol. 6, n. 1, February 2003, pp. 1-42.

[47] Xuan Zhou, HweeHwa Pang, and Kian-Lee Tan. Hiding data accesses in steganographic file system. In Proceedings of the 20th International Conference on Data Engineering, pages 572–583. IEEE Computer Society, 2004.

[48] http://www.oracle.com/database/berkeley-db/index.html/.

[49] https://www.trustedcomputinggroup.org/.

[50] http://www.anonymizer.com/

[51] http://anon.penet.fi/

[52] Security-Enhanced Linux. Located at: http://www.nsa.gov/selinux/.

[53] The Month of Kernel Bugs (MoKB) archive. Located at: http://projects.info-pull.com/mokb/.

[54] The ROBIN project: located at: http://robin.tudos.org/

1.3 S/T methodology and associated work plan

Overall Strategy of the Work Plan

CAPA workplan is organised according to the following lifecycle phases:

- Requirements
- Architecture
- Design
- Implementation
- Integration and Support
- Evaluation

CAPA is structured in 7 work packages:

- WP1: project management. This work package runs in parallel with other work packages. It includes an overall coordination task (T1) and an administrative management task (T2).
- WP2: Requirements. This work package is carried out at the start of the project. It includes an application and technical requirement analysis task (T1), a task focusing on security and data protection models (T2), and a task focusing on requirements for trust and empowerment (T3).
- WP3: Architecture and design for trusted storage platforms. This work package logically follows WP2. It focuses on the trusted storage platform objective of CAPA. It includes an overall architecture task (T1) which is then followed by 4 design tasks, focusing on the secure operating system and file system (T2), the secure database part (T3), the policy management part (T4) and the support for empowerment part (T5).
- WP4: Use cases towards "la capa invisible". This work package logically follows WP2. It focuses on the architecture for privacy of actors objective of CAPA. It includes a use case specification task (T1), which is then followed by 4 dedicated design, development, integration tasks, one per use case. Task 2 will focuses on a privacy-preserving surveillance application. T3 focuses on the privacy of vehicle locations in a V2V/V2I environment, T4 focuses on privacy enabled payment, and T5 focuses on privacy enabled multimedia interactions. T2,T3,T4,T5 are themselves structured into 3 subtasks (design, implementation, integraton). They are followed by an evaluation task (T6).
- WP5: Challenges for privacy. This work package focuses on the challenge objective of CAPA. Three area of investigation have been identified : linkage attacks, privacy of access, and policies. Each challenge will be tackled by one task (i.e. T1, T2, T3), further structured into 8 subtasks. The first 5 subtasks closely follow the CAPA lifecycle, in order to allow for results in WP5 to be possibly included in a WP4 use case. The last 3 subtasks follow a more independent research activity (two phases followed by a roadmap elaboration phase).
- WP6: Reference implementation. This work package logically follows WP3. It includes 4 implementation tasks, focusing on the secure operating system and file system (T1), the secure database part (T2), the policy management part (T3) and the support for empowerment part (T4). The 4 implementation tasks are followed by an integration and support task (T5) in order to help the use of the reference implementation in WP4
- WP7: Link to the industry and Reach out. This work package runs in parallel with other work packages. It includes 4 independent tasks. Task 1 focuses on the study of legal and ethical impact. This task also follows the project life cycle and will include four subtasks, a state of the art subtask, a study on legal requirements subtask, a study on the legal impact of security and data protection models and an evaluation subtask. Task 2 focuses on standardisation. It includes three subtasks, a standard survey subtask, and study of CAPA impact in two phases. Task 3 focuses on dissemination and liaison. Task 4 focuses on exploitation plans.

Timing of the Different WPs and their Components

The table below shows the timing of the different WPs. Note that

- CAPA is a 36-month project
- The lifecycle phases are showed in the table. Milestones (see table 1.3E below) corresponds to the lifecycle phases completion
- A similar table is included below to show the links between deliverables and tasks/subtasks.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
	Requirements								Architecture						Design						Implementation						Integration				Evaluation					
WP1 Management																																				
T1 Coordination															Coordination																					
T2 Administrative Management	S1 Y1 management														S2 Y2 management												S3 Y3 management									
WP2 Requirements																																				
T1 Application and technical requirements	S1 Use cases				S2 Threat analysis																															
					S3 Requirements																																
T2 Security & Data Protection models					S1 Requirements				S2 Models specification																											
T3 Trust and empowerment					S1 Requirements				S2 Trust support specification																											
WP3 Architecture and Design of Trusted Storage Platform																																				
T1 Overall Architecture									Trusted Storage Platform architecture																											
T2 Secure OS and FS															Secure Operating System and File																					
T3 Secure Database															Secure Database																					
T4 Policy Management Support															Policy management subsystem																					
T5 Support for empowerment															Trust support subsystem																					
WP4 Use cases																																				
T1 Specification									Use case specification																											
T2 Privacy Preserving Surveillance															S1 Use case design						S2 Use case implementation						S3 Integration								
T3 Vehicular Location Tracking															S1 Use case design						S2 Use case implementation						S3 Integration								
T4 Privacy enabled payment															S1 Use case design						S2 Use case implementation						S3 Integration								
T5 Privacy enabled multimedia interactions															S1 Use case design						S2 Use case implementation						S3 Integration								
T6 Evaluation																															Evaluation					
WP5 Challenges for Privacy																																				
T1 Linkage attacks	S1 Requirements								S2 Architectures, Link to Application						S3 Mechanisms						S4 Proof of concepts						S5 Support								
	S6 Contribution to research 1														S7 Contribution to research 2																S8 Roadmap					
T2 Privacy of access	S1 Requirements								S2 Architectures						S3 Mechanisms						S4 Proof of concepts						S5 Support								
	S6 Contribution to research 1														S7 Contribution to research 2																S8 Roadmap					
T3 Policies	S1 Requirements								S2 Architectures						S3 Mechanisms						S4 Proof of concepts						S5 Support								
	S6 Contribution to research 1														S7 Contribution to research 2																S8 Roadmap					
WP6 Reference Implementation																																				
T1 OS and File System																					OS and File System														
T2 Secure Database																					Secure Database														
T3 Empowerment support																					Trust and empowerment														
T4 Policy mgt support																					Policy mgt														
T5 Integration and support																											Integration and Support								
WP7 Link to Industry and Reach out																																				
T1 Legal and Ethical Impact	S1 State of the art				S2 Legal requirements				S3 Legal aspects in models																											S4 Evaluation
T2 Standardisation	S1 Survey of current standards								S2 CAPA impact on standards V1												S3 CAPA impact on standards V2														
T3 Dissemination and Liaison	S1 Dissemination Material								S2 Dissemination and liaison Phase 1 : Awareness												S3 Dissemination and liaison Phase 1 : Results													
T4 Exploitation	S1 PUD V1								S2 PUD V2																		S3 PUD V3								

Table 1.3a: Work package list

Work package No[1]	Work package title	Type of activity[2]	Lead partic no.[3]	Lead partic. short name	Person-months[4]	Start month[5]	End month[5]
1	Management	MGT	1	Trialog	12	0	36
2	Requirements	RTD	2	VTools	54	0	14
3	Architecture for Trusted Storage Platforms	RTD	3	KUL	55	8	20
4	Use Cases towards "la capa invisible"	RTD	4	TID	84	8	36
5	Challenges for Privacy	RTD	5	UBER	56	0	36
6	Reference Implementation	RTD	6	TUD	108	20	36
7	Link to the industry and reach out	RTD	7	Trialog	46	0	36
	TOTAL				415		

1 Workpackage number: WP 1 – WP n.

2 Please indicate one activity per work package:

RTD = Research and technological development (including any activities to prepare for the dissemination and/or exploitation of project results, and coordination activities); DEM = Demonstration; MGT = Management of the consortium

3 Number of the participant leading the work in this work package.

4 The total number of person-months allocated to each work package.

5 Measured in months from the project start date (month 1).

Table 1.3b: List of Deliverables

Del. no. [6]	Deliverable name	WP no.	Nature[7]	Dissemi-nation level[8]	Delivery date[9] (proj. month)
D1	Use cases and threat analysis	2	R	PU	8
D2	Requirements	2	R	PU	8
D3	Challenges for privacy: issues	5	R	PU	8
D4	Legal issues : state of the art and requirements	7	R	PU	8
D5	Survey of current standards	7	R	PU	8
D6	Dissemination material	7	R	PU	8
D7	Plan for Use and Dissemination V1	7	R	CO	8
D8	Year 1 management report	1	R	CO	12
D9	Security & Data protection models specification	2	R	PU	14
D10	Trust support specification	2	R	PU	14
D11	Trusted storage platform architecture	3	R	PU	14
D12	Privacy use case specification	4	R	PU	14
D13	Challenges for privacy: directions	5	R	PU	14
D14	Legal aspects on models	7	R	PU	14
D15	Trusted storage platform design	3	R	PP	20
D16	Privacy use case design	4	R	PP	20
D17	Challenges for privacy: mechanisms	5	R	PU	20
D18	CAPA impact on standards V1	7	R	PP	20
D19	Dissemination and liaison report V1	7	R	PP	20
D20	Plan for Use and Dissemination V2	7	R	CO	20
D21	Year 2 management report	1	R	CO	24
D22	Use case implementation	7	P	RE	26
D23	Challenges for privacy: proof of concepts	5	P	PP	26
D24	OS and file system	6	P	PP	26
D25	Secure database	6	P	PP	26
D26	Trust and empowerment support	6	P	PP	26
D27	Policy management support	6	P	PP	26
D28	Year 3 management report	1	R	CO	36
D29	Privacy use case evaluation	4	R	PP	36
D30	Challenges for privacy: roadmap	5	R	PU	36
D31	Evaluation from legal and ethical point of view	7	R	PU	36
D32	CAPA impact on standards V1	7	R	PP	36
D33	Dissemination and liaison report V1	7	R	PP	36
D34	Plan for Use and Dissemination V2	7	R	CO	36

The table below shows the positioning of the deliverables with respect to the workplan tasks.

[6] Deliverable numbers in order of delivery dates. Please use the numbering convention <WP number>.<number of deliverable within that WP>. For example, deliverable 4.2 would be the second deliverable from work package 4.

[7] Please indicate the nature of the deliverable using one of the following codes:
R = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

[8] Please indicate the dissemination level using one of the following codes:
PU = Public
PP = Restricted to other programme participants (including the Commission Services).
RE = Restricted to a group specified by the consortium (including the Commission Services).
CO = Confidential, only for members of the consortium (including the Commission Services).

[9] Measured in months from the project start date (month 1).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
	Requirements								Architecture						Design						Implementation						Integration				Evaluation					
WP1 Management																																				
T1 Coordination															-																					
T2 Administrative Management	D8 Y1 mgt report														D21 Y2 mgt report												D28 Y3 mgt report									
WP2 Requirements																																				
T1 Use cases	D1 Use case and Thread Analysis																																			
					D2 Requirements																																	
T3 Securty & DP models					D2 Requirements				D9 Models specification																											
T4 Trust and empowerment					D2 Requirements				D10 Trust support specification																											
WP3 Architecture and Design of Trusted Storage Platform																																				
T1 Overall Architecture									D11 TSP architecture																											
T2 Secure OS and FS															D15 Design																					
T3 Secure Database															D15 Design																					
T4 Policy Management Support															D15 Design																					
T5 Support for empowerment															D15 Design																					
WP4 Use cases																																				
T1 Specificaiton									D12 Use case specification																											
T2 Privacy Preserving Surveillance															D16 Use case design						D22 Use case implementation						S3 Integration									
T3 Vehicular Location Tracking															D16 Use case design						D22 Use case implementation						S3 Integration									
T4 Privacy enabled payment															D16 Use case design						D22 Use case implementation						S3 Integration									
T5 Privacy enabled multimedia interactons															D16 Use case design						D22 Use case implementation						S3 Integration									
T6 Evaluation																															D29 Evaluation Report					
WP5 Challenges for Privacy																																				
T1 Linkage attacks	D3 Analysis of issues								D13 Directions						D17 Mechanisms						D23 Proof of concepts						S5 Support									
	D13 Directions														S7 Contribution to research 2																D30 Roadmap					
T2 Privacy of access	D3 Analysis of issues								D13 Directions						D17 Mechanisms						D23 Proof of concepts						S5 Support									
	D13 Directions														S7 Contribution to research 2																D30 Roadmap					
T3 Policies	D3 Analysis of issues								D13 Directions						D17 Mechanisms						D23 Proof of concepts						S5 Support									
	D13 Directions														S7 Contribution to research 2																D30 Roadmap					
WP6 Reference Implementation																																				
T1 OS and File System																					D24 OS and File System															
T2 Secure Database																					D25 Secure Database															
T3 Empowerment support																					D26 Trust and empowerment															
T4 Policy mgt support																					D27 Policy mgt															
T5 Integration and support																															-					
WP7 Link to Industry and Reach out																																				
T1 Legal and Ethical Impact	D4 legal requirements								D14 Legal aspects in models																						D31 Evaluation					
T2 Standardisation	D5 Survey of current standards								D18 CAPA impact on standards report												D32 CAPA impact on standards reports V2															
T3 Dissemination and liaison	D6 Dissemination Material								D19 Dissemination and liaison report v1												D33 Dissemination and liaison report v2															
T4 Exploitation	D7 PUD V1								D20 PUD V2																		D34 PUD V3									

Table 1.3c1: WP1 Management

Work package number	1		**Start date or starting event:**				T0		
Work package title	Management								
Activity type	MGT								
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog Leader	CB	Oracle	TID	Vtools	UBER	KUL	TUD	UMIL
PM per participant	12								

Objectives

To provide overall project administration support for the CAPA project.
To provide technical steering for the internal developments of the CAPA project.
To administer and resource external project and EC links.
To evaluate and assess the project

Description of work (possibly broken down into tasks) and role of partners

Task 1: Coordination (T0 to T0+36)

An overall coordination of the project is needed to ensure consistency with respect to an overall strategy set up by the PMC. The project, whilst being directed by its declared overall objective, will still need to be steered in the light of progress and changing circumstances, and also for the negotiation of exchange of information with respect to task related dependencies. This will be handled through the participation of the project coordinator in conjunction with the help of an innovation director. This task will also focus on the evaluation and assessment of the results of the project, in terms of scientifical, technical and project objectives. Further elements to be evaluated will be the impact on societal challenges and on IST policy

Partners and roles: Trialog (coordinator) will carry out this task.

Task 2:Administrative Management (T0 to T0+36)

A project office will be established with a staff of one project administrator. The project administrator will be responsible to the Project Management Committee (or PMC - a committee formed by all partners Project Managers), supervised directly by the Project Coordinator. It will be responsible for :

- Organizing and running all project meetings
- Collating, filing and distributing project deliverables
- Timely compilation and organization of project reports, incorporating reporting on progress against objectives, spend against budget, exploitation and plans, internal and external interactions, proposed and agreed changes of plan
- Collating internal projects reports
- Collating and administering project charges and payments
- Scheduling and progressing deliverables and reporting short-falls to the PMC
- All other general project administrative tasks...

Task 2 includes the following subtasks:

Subtask 2.1:Administrative Management for Year 1 (T0 to T0+12)

Corresponds to Y1 activities. Is concluded by D8

Subtask 2.2:Administrative Management for Year 2 (T0+12 to T0+24)

Corresponds to Y1 activities. Is concluded by D21

Subtask 2.3:Administrative Management for Year 3 (T0+24 to T0+36)

Corresponds to Y1 activities. Is concluded by D28

Partners and roles: Trialog (coordinator) will carry out these subtasks

Deliverables (brief description) and month of delivery

D8 (T0+12) **Year 1 management report.** Led by Trialog
D21 (T0+24) **Year 2 management report.** Led by Trialog
D28 (T0+36**) Year 3 management report.** Led by Trialog

Table 1.3c2: WP2 Requirements

Work package number	2		**Start date or starting event:**			T0		
Work package title	Requirements							
Activity type	RTD							
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog	CB	Oracle	TID	Vtools Leader	UBER	KUL[10]	TUD	UMIL
PM per participant	6	2	2	8	5	10	0+5	6	10

Objectives

To provide overall security requirements consistent with a threat analysis
To provide a range of security and data protection models consistent with the security requirements
To provide instrumentation requirements for validation and empowerment

Description of work (possibly broken down into tasks) and role of partners

Task 1: Application and Technical Requirements (T0 to T0+8)

The objective of this task is to identify the overall requirements of the project.

Task 1 includes the following subtasks:

Subtask 1.1: Use Cases (T0 to T0+4)

The objective of this subtask is to describe through a wealth of examples privacy related threats involving data. These use case will include but not restrict to the use case investigated in more detail in WP4.

Subtask 1.2: Threat Analysis (T0+4 to T0+8)

The use cases defined in subtask 1.1 will allow for a threat analysis

Subtask 1.3: Resulting Requirements (T0+4 to T0+8)

- The use cases defined in subtask 1 will allow for the identification of requirements for data protection and privacy.

Partners and roles: VTools is the leader of this task. The roles of participants are the following

- VTools: Leadership, Privacy preserving surveillance viewpoint
- TID: Privacy enabled payment viewpoint, Privacy enabled multimedia viewpoint
- Trialog: Vehicle location tracking viewpoint, Privacy enabled multimedia viewpoint
- CB: Privacy enabled payment viewpoint
- Oracle: Database viewpoint

Task 2: Security and Data Protection Models (T0+4 to T0+14)

An analysis of possible security and data protection models will be made. The objective of a model is to specify at a sufficiently general and abstract level an overall architecture and specification. A model can be in general fully independent from the underlying technology, e.g. a technology can change while the security model is the same. In the case of a security and data protection model, specific artefacts must be described, such as security levels, stakeholders, roles, enforcement. For instance a model could specify that the administrator of a database system does not have credentials to access the content of data "owned" by a user. It could also specify that user "owned" data is always stored with encryption. Security and data protection models typically consists of a mix of technologies and policies. For instance the Bell-La Padula model typically focuses on confidentiality aspects typically used in defence applications.

The models defined in this task will serve the following purpose:

- Serve as input to the definition of a trusted storage platform architecture (WP3) as well as to the definition of an architecture for the privacy of actors (WP4).
- Serve as contribution to the security community in the large, either as "standard models" for data protection or as starting points to future security engineering related to data protection and privacy.
- Allow for the identification of instrumentation requirements that will be useful for testing trust and empowerment (task 3)

The approach of this task will be as follows :

- First focus on the application area addressed in WP4 (privacy preserving surveillance, privacy enabled payment, vehicle location tracking avoidance, privacy enable multimedia interactions)
- Investigate a range of possible models for each application area, and then identify common and generic parts of the models
- Specialize the models taking into account the trusted storage platform and the way it is used in WP4

Task 2 includes the following subtasks:

Subtask 2.1: Requirements (T0+4 to T0+8)

This subtask will focus on the requirements for security and data protection models. This subtask runs in parallel to other requirements subtasks

[10] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

Subtask 2.2: Models specification (T0+8 to T0+14)

Further to the availability of requirements, this subtask can focus on the specification of security and data protection models.

Partners and roles: UBER is the leader of this task. The roles of participants are the following

- UBER: Leadership, Database viewpoint
- Trialog: Testing viewpoint
- KULeuven: Architecture viewpoint
- TUD: Architecture viewpoint
- CB: Payment application viewpoint
- TID: Payment application viewpoint, Multimedia interaction viewpoint
- UMIL: Data protection model viewpoint

Task 3: Trust and Empowerment (T0+4 to T0+14)

The objective of this task is to specify the requirements on inspection and configuration, e.g. letting the user (or another stakeholder with proper credentials) to inspect and configure the platform. This in turn imply instrumentation requirements, points of control and approaches for (1) policy enforcement, (2) certification, (3) empowerment aspects. Policy enforcement is related to a security parameter that can be configured (e.g. the driver is allowed to read data item A). Certification is related to a security features that is static and can be verified (e.g. an independent party can verify that some elements of the architecture are compliant. Empowerment allows a stakeholder to observe and verify security and trust (e.g. an user can check of log of activities).

Task 3 must be carried out in parallel to task 2 because it might impact on the security models. It includes the following subtasks:

Subtask 3.1: Requirements (T0+4 to T0+8)

This subtask will focus on requirements. This subtask runs in parallel to other requirements subtasks

Subtask 3.2: Trust support specification (T0+8 to T0+14)

Further to the availability of requirements, this subtask can focus on the specification of suitable support

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Leadership, Testing tool implementation viewpoint
- UMIL: Policies viewpoint

Deliverables (brief description) and month of delivery

D1 (T0+8) **Use cases and threat analysis**. Led by Trialog. This deliverable collects the use cases and threats related to privacy and data protection in the application area addressed by CAPA.

D2 (T0+8) **Requirements**. Led by VTools. This deliverable lists the application and technical requirements threats related to privacy and data protection in the application area addressed by CAPA (task 1). It also includes requirements related to security & data protection models (task 2) and testing for trust and empowerment (task 3).

D9 (T0+14) **Security and data protection models specification**. Led by UBER. This deliverable specifies security and data protection models in the application area addressed by CAPA, with a specialization to take into account the trusted storage platform role in CAPA use cases.

D10 (T0+14) **Trust support specification**. Led by Trialog. Provides a specification of how trust and empowerment is supported in terms of policy enforcement, certification, empowerment.

Table 1.3c3: WP3 Architecture and Design for Trusted Storage Platforms

Work package number	3		**Start date or starting event:**			T0+8		
Work package title	Architecture and Design for Trusted Storage Platforms							
Activity type	RTD							
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog	CB	Oracle	TID	Vtools	UBER	KUL[11] Leader	TUD	UMIL
PM per participant	6	0	10	0	0	3	0+5	21	10

Objectives

To define an overall trusted storage platform architecture
Provide the design of the resulting secure operating and file system
Provide the design of the resulting secure database system
Provide the design of the resulting policy management support
Provide the design of the resulting instrumentation support

Description of work (possibly broken down into tasks) and role of partners

Task 1: Overall Architecture (T0+8 to T0+14)

The overall architecture of a trusted storage platform will be specified. This architecture will serve the purpose of the architecture for the privacy of actors as defined in WP4. To this end, it will start with the requirements collected in WP2.

At this stage of the consortium understanding, the overall architecture includes the following building blocks:

- A secure operating system and file system. This building block can include components such as security modules (e.g. TPM).
- A secure database system
- Secure management of policies
- Instrumentation to allow for test and empowerment

This task will investigate the role and dependencies of each building block. It will also investigate possible implementations and profiles (e.g. suitable for an USB token device, a nomadic device or a more powerful consumer device).

Partners and roles: KUL (COSIC) is the leader of this task. The roles of participants are the following

- KUL: Leadership, Overall architecture
- TUD: Operating system and File system, Overall integration
- Oracle: Database
- Trialog: Support for test, Overall integration
- UMIL: Policy management

Task 2: Secure Operating System and File System (T0+14 to T0+20)

The objective of this task is design the secure operating system and file system building block. The starting point will be open source technology available at TU Dresden. Depending on the requirements and on the status of work, a decision will be made between the results of OpenTC (http://www.opentc.net/) or Robin (PASR 2005 project).

Partners and roles: TUD is the leader of this task. The roles of participants are the following

- TUD: Overall design
- KUL: Participation to design
- Trialog : Participation to prepare for integration

Task 3: Secure Database (T0+14 to T0+20)

The objective of this task is to design the secure database system. The starting point will be Berkeley DB, an open source technology available from Oracle.

Partners and roles: Oracle is the leader of this task. The roles of participants are the following

- Oracle: Leader, Overall design
- UBER: Participation to design
- Trialog : Participation to prepare for integration

Task 4: Policy Management Support (T0+14 to T0+20)

The objective of this task is to specify the impact of WP2 requirements to the overall trusted storage platform in terms of policy management.

Partners and roles: UMIL is the leader of this task. The roles of participants are the following

- UMIL: Overall design
- Trialog : Participation to prepare for integration

Task 5: Support for Empowerment (T0+14 to T0+20)

[11] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

The objective of this task is to design the overall trusted storage platform in terms of instrumentation

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Leader, Overall design

Deliverables (brief description) and month of delivery

D11 (T0+14) **Trusted Storage Platform Architecture**. Led by KUL. This deliverable collects the use cases and threats related to privacy and data protection in the application area addressed by CAPA.

D15 (T0+20) **Trusted Storage Platform Design.** Led by KUL. This deliverable lists the application and technical requirements threats related to privacy and data protection in the application area addressed by CAPA (task 1). It includes also includes requirements related to security & data protection models (task 2) and testing for trust and empowerment (task 3).

Table 1.3c4: WP4 Use Cases towards "la capa invisible"

Work package number	4		**Start date or starting event:**			8		
Work package title	Use cases towards "la capa invisible"							
Activity type	RTD							
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog	CB	Oracle	TID Leader	Vtools	UBER	KUL[12]	TUD	UMIL
PM per participant	18	3	3	36	20	0	4+0	0	0

Objectives

To define an overall architecture for the privacy of actors involved in the variety of WP4 use cases
To specify, develop and demonstrate privacy preserving surveillance application
To specify, develop and demonstrate privacy enabled vehicular communication
To specify, develop and demonstrate privacy enabled payment
To specify, develop and demonstrate privacy enabled multimedia interaction
To evaluate the use case implementations

Description of work (possibly broken down into tasks) and role of partners

Task 1: Specification (T0+8 to T0+14)

This task will specify

- an architecture for the privacy of actors, which combines the building blocks ensuring protection of stored data as specified in WP3 with other existing building blocks (e.g. for identity management). The architecture involves the use of a device (or set of devices) that has/have communication capabilities, has trusted execution and storage capability and the ability to generate identifiers. The goal of this architecture is to show that intrusion of privacy can be avoided.
- Four use cases : privacy preserving surveillance, vehicular location tracking avoidance, privacy enabled payment, privacy enabled multimedia interaction. The types of devices integrating CAPA trusted storage platforms are the following
  - Privacy preserving surveillance : infrastructure device (surveillance device)
  - Vehicular location tracking avoidance: infrastructure device (RSE roadside equipment device), personalised device (vehicle communication interface)
  - Privacy enabled payment: personalised device (nomadic device)
  - Privacy enabled device: personalise device (home gateway, nomadic device)
- How the use case makes use of the architecture
- Evaluation criteria that will be used for evaluation. One example of criteria is the continuum technology/policy (e.g. a better privacy technology solution for privacy necessitates less policies).

Partners and roles: TID is the leader of this task. The roles of participants are the following

- TID: Leadership, specification of payment and multimedia interaction use case
- Trialog: Review of all use cases, Overall architecture, specification of vehicular location tracking and multimedia use case
- CB: Review of payment use case specification
- VTools: specification of surveillance use case
- KUL/ICRI: contribution to evaluation criteria from legal aspects viewpoint

Task 2: Privacy Preserving Surveillance (T0+14 to T0+30)

The objective of this task is to specify, develop and demonstrate a privacy preserving surveillance unit. The starting point will be the current digital video recorder/transmitter developed and marketed by Visual Tools. The newly developed unit will mask the identity of the persons appearing in the scene that will only be disclosed with appropriate authorization. Different image analysis techniques such as face detection and face masking will be applied to the identity masking. The privacy preserving surveillance unit is expected to play a role in future video surveillance systems in public places in which the proliferation of surveillance installations is raising the concern for privacy protection in many countries (see http://www.constitutionproject.org/libertyandsecurity/article.cfm?messageID=310&categoryId=6 for concerns in the USA).

See box below for subtasks description.

Partners and roles: VTools is the leader of this task. The roles of participants are the following

- VTools: Leadership, development of application

Task 3: Vehicular Location Tracking Avoidance (T0+14 to T0+30)

The objective of this task is to specify, develop and demonstrate privacy enabled vehicular communication. This starting point will be on-going work carried out in eSafety application projects such as CVIS (www.cvisproject.org) or Sevecom (www.sevecom.org). CVIS is currently developing a reference implementation platform for V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) communication. Sevecom is currently developing a solution for location tracking avoidance

[12] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

based on the use of pseudonyms. This work is carried out further to some liaison activities which took place from July 2006 with the PRIME IP project.

Sevecom is focusing on identity management. CAPA will investigate the benefit of using the CAPA trusted storage platform to ensure privacy of collected data, in particular at the level of roadside equipment. Such equipment potentially collect data to all vehicles in their vicinity.

See box below for subtasks description.

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Leadership, development of application
- Oracle : participation

Task 4: Privacy Enabled Payment (T0+14 to T0+30)

This task focuses on privacy enabled payment. The user will have a device that will store independently and according to CAPA architecture, both information from the payment service provider and from the communications service provider. As he/she wants to make a payment for a product that he/she is buying from a service provider, data stored by the communications service provider (e.g, location) and data stored by the payment provider will be used to authorise and complete the transaction in a way that user privacy –the information handled by any of the providers will be "anonymized", and neither of the providers should share information, even known about each other- is preserved and the transaction is guaranteed – that is, payment is guaranteed and data is stored just for some future possible legal issue.

See box below for subtasks description.

Partners and roles: TID is the leader of this task. The roles of participants are the following

- TID: Leadership, development of application
- CB: Review of design

Task 5: Privacy Enabled Multimedia Interactions (T0+14 to T0+30)

This task will focus on the wide variety of multimedia interaction applications. The proposed approach is to liaise with initiatives in the area and check (1) whether potential future applications may create new data protection issues, and (2) whether CAPA architecture may be relevant to them.

The Network and Electronic Media (NEM) technology platform initiative (http://www.nem-initiative.org/) is particularly relevant . Its objective is to *foster the development and novel AV and multimedia broadband services and applications to benefit European citizens and enterprises*. *NEM represents the convergence of existing and new technologies including broadband, mobile and new media across all ICT sectors, to create a new and exciting era of advanced personalized services.* Note that NEM icludes an R&D cluster on security (led by TSSG). Furthermore TID is one of the 10 members of the NEM executive board, and Trialog is leading the Community Based Services R&D cluster.

An application will be selected in this task. We plan to select an application to be developed in the MonAMI IP project (http://www.monami.info). MonAMI project is working on future e-inclusion services to the person. It is a 4 year project started in September 2007. TID is responsible for the Spanish *validation centre*[13], an experimentation involving 50+ dwellings in Spain. Trialog is technical coordinator of MonAMI.

See box below for subtasks description.

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Leadership, development of application, liaison with NEM
- TID: Review of design, liaison with NEM
- Oracle: participation

Task 6: Evaluation (T0+30 to T0+36)

This task will carry out an evaluation of the use cases with respect to the evaluation criteria identified in task 1.

Dependencies: Task 6 work will be in liaison with

- WP6.T1 which focuses on evaluation from the legal and ethical viewpoint (subtask T1.4)

Partners and roles: TID is the leader of this task. The roles of participants are the following

- TID: Leadership, evaluation of payment and multimedia interaction use case
- Trialog: Evaluation of vehicular location tracking and multimedia use case
- CB: Evaluation of payment use case
- Vtools: Evaluation of surveillance use case
- KUL/ICRI: Evaluation from legal aspects viewpoint

Common section to Task 2, Task 3, Task 4 (replace X by 2 or 3 or 4)
Task X include the following subtasks: *Subtask X.1: Use case design (T0+14 to T0+20)* This subtask will focus on the elements which adds privacy to the application *Subtask X.2: Use case implementation (T0+20 to T0+26)* This subtask will focus on the implementation of elements making up the application

[13] Term proposed by the ISTAG working group report « Ambient Intelligence : from vision to reality » (http://cordis.europa.eu/ist/istag-reports.htm)

Subtask X.3: Use case integration (T0+26 to T0+30)

- The subtask will integrate the trusted storage platform

Deliverables (brief description) and month of delivery

D12 (T0+14) **Privacy use case specification**. Led by TID. This deliverable specifies an architecture for the privacy of actors, four application use cases, and how these use cases use the architecture. It in particular explains the building blocks which makes up these applications. It also includes a list of evaluation criteria that will be used in the evaluation report.

D16 (T0+20) **Privacy use case design.** Led by TID. This deliverable provides the design of the four use cases. It is the result of task 2, task 3, task 4 and task 5

D29 (T0+36) **Evaluation report.** Led by TID. This deliverable makes an analysis of the use cases versus evaluation criteria identified in D12.

Table 1.3c5: WP5 Challenges for Privacy

Work package number	5		**Start date or starting event:**			1		
Work package title	Challenges for privacy							
Activity type	RTD							
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog	CB	Oracle	TID	Vtools	UBER Leader	KUL[14]	TUD	UMIL
PM per participant	0	0	0	0	0	22	0+18	0	16

Objectives

To investigate research challenges related to privacy concerning linkage attacks, privacy of access, policies.

Description of work (possibly broken down into tasks) and role of partners

Task 1:Linkage Attacks

This task will identifies the different threats to which data are exposed due to possible inferences on data as well as to data correlation and linkage operations by external parties. The task will investigate possible ways in which data protection/exposure can be defined and propose a possible measure for assessing the exposure risk (threatening privacy) to which a collection of data or a data release is subject. Possible techniques for protecting privacy by proper data sanitization (including generalizing them or releasing them only in encrypted form) will also be investigated and novel techniques will be devised also with respect to information visibility and efficiency guarantees that may need to be obeyed.

Task 1, 2, 3 follow the same subtask approach. See box below.

Partners and roles: UBER is the leader of this task. The roles of participants are the following

- UBER: Leadership,
- Trialog: Participation through its consultant Dennis Shasha
- UMIL: Participation

Task 2:Privacy of Access

This task will investigate the design of techniques to guarantee secure accesses to steganographic file systems. An open research problem that will be investigated in this project concerns the design and evaluation of techniques to guarantee secure accesses to steganographic file systems. These systems are particularly important in scenarios where users may be subject to coercion attacks. For example, journalists or NGO staff members possessing evidence of human rights abuses in war zones, should be able to plausibly deny having any compromising material. Steganographic file systems hide encrypted data among random noise, such that it is not possible for an adversary to determine the amount (if any) of useful information that is kept in the storage. Observable steganographic file systems provide plausible deniability to the user even if the adversary has the ability to continuously monitor accesses to the storage.

Task 1, 2, 3 follow the same subtask approach. See box below.

Partners and roles: KUL is the leader of this task. The roles of participants are the following

- KUL: Leadership,
- UBER: Participation

Task 3:Policies

The objective of this task is the identification and definition of policies regulating the system behavior. As a matter of fact policies will need to be in place to regulate when, where, to whom, and under which conditions data can be accessed, with reference to the different access that can be performed (such as, for instance, release, decryption, and linking).

Policies will have to be in place both at the user side (to regulate data access and direct release by the user) as well as at any external parties which might receive user data (to regulate subsequent accesses, secondary use, as well as possible data sharing and merging). The task will identify the different aspects and regulations to be captured by the policies. It will define a formal model to be able to reason about the consistency and correctness of the policy (e.g., with respect to the user wished guarantees for privacy protection or with respect to law regulations) together with an associated language for the policy specification. The policy task will also reflect, and leverage from, the database linkage research since restrictions to be applied by the policies on the data may be needed to prevent linkage and correlation attacks putting privacy at risk.

Task 1, 2, 3 follow the same subtask approach. See box below.

Partners and roles: UMIL is the leader of this task. The roles of participants are the following

[14] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

- UMIL: Leadership,

Common section to Task 1, Task 2, Task 3 (replace X by 1 or 2 or 3)

Task X is structured into a number of subtasks. The purpose of this structure is to synchronise WP5 with other WPs:

Subtask X.1: Requirements Aspects (T0 to T0+8)

This subtask will focus on requirements aspects in the topic of research. Requirements from WP2 could influence on investigation directions and approaches. Reciprocally state of the art study could influence on WP2 requirements

Subtask X.2: Architecture Aspects (T0+8 to T0+14)

This subtask will focus on how architecture for privacy can be influenced by results in the area of research

Subtask X.3: Mechanisms and Link to Applications (T0+14 to T0+20)

The subtask will identify potential mechanisms focus on integrate the trusted storage platform

Subtask X.4: Proof of concepts (T0+20 to T0+26)

This subtask will focus on the implementations of possible mechanisms as proof of concepts.

Subtask X.5: Support (T0+26 to T0+36)

This subtask is to provide support to WP4 in the case subtask X.4 is integrated into one of WP4 use cases.

Subtask X.6: Contribution to research 1 (T0 to T0+14)

The subtask is dedicated to research work in the area (first phase).

Subtask X.7: Contribution to research 2 (T0+14 to T0+30)

The subtask is dedicated to research work in the area (second phase).

This subtask will focus on the implementation of elements making up the application

Subtask X.8: Roadmap (T0+30 to T0+36)

- The subtask will identify future research work

Deliverables (brief description) and month of delivery

D3 (T0+8) **Challenges for privacy: issues**. Led by UBER. This deliverable describes issues to solve related to privacy in the 3 area investigated by CAPA : linkage attacks, privacy of access, policies.

D13 (T0+14) **Challenges for privacy: directions.** Led by UMIL. This deliverable describes possible directions and architecture in the 3 area investigated by CAPA : linkage attacks, privacy of access, policies.

D17 (T0+20) **Challenges for privacy: mechanisms and link to applications.** Led by KUL. This deliverable describes possible mechanisms in the 3 area investigated by CAPA : linkage attacks, privacy of access, policies.

D23 (T0+26) **Proof of concept.** Led by UBER. Possible proof-of-concepts in the 3 area investigated by CAPA : linkage attacks, privacy of access, policies.

D30 (T0+36) **Roadmap.** Led by UMIL. Research roadmaps in the 3 area investigated by CAPA : linkage attacks, privacy of access, policies.

Table 1.3c6: WP6 Reference Implementation

Work package number	6		**Start date or starting event:**				20		
Work package title	Reference Implementation								
Activity type	RTD								
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog	CB	Oracle	TID	Vtools	UBER	KUL[15]	TUD Leader	UMIL
PM per participant	12	0	10	0	3	6	0+5	60	12

Objectives

Develop a reference implementation which can be used by WP4 (use case) and which can also serve as starting point for future trusted storage platforms

Description of work (possibly broken down into tasks) and role of partners

Task 1: OS and File System (T0+20 to T0+26)

Adapt an existing secure operating system and file system to meet CAPA trusted storage platform requirements

Partners and roles: TUD is the leader of this task. The roles of participants are the following

- TUD: Overall implementation
- KUL: Minor participation to implementation
- Trialog : Participation to prepare for integration

Task 2: Secure Database (T0+20 to T0+26)

Adapt an existing database system to meet CAPA trusted storage platform requirements

Partners and roles: UBER is the leader of this task. The roles of participants are the following

- UBER: Overall implementation
- Oracle: Participation to development
- Trialog : Participation to prepare for integration

Task 3: Empowerment Support (T0+20 to T0+26)

Include in the implementation suitable secure instrumentation point for testing and empowerment support

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Overall implementation

Task 4: Policy Management Support (T0+20 to T0+26)

Include in the implementation suitable policy management support

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- UMIL: Overall implementation
- Trialog : Participation to prepare for integration

Task 5: Integration and Support (T0+26 to T0+36)

Ensure integration of implemented building blocks (task 1 to 4 and provide support to WP4 partners)

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Overall integration and support
- TUD: Expertise on OS and FS part
- UBER: Expertise on Database part
- Oracle: Expertise on Database part
- Vtools: Participation in integration and support

Deliverables (brief description) and month of delivery

D24 (T0+26) **OS and File System**. Led by TUD. Software ready for integration

D25 (T0+26) **Secure Database.** Led by UBER. Software ready for integration.

D26 (T0+26) **Trust and empowerment**. Led by Trialog. Software ready for integration.

D27 (T0+26) **Policy management.** Led by UMIL. Software ready for integration

[15] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

Table 1.3c7: WP7 Link to the Industry and Reach out

Work package number	7		**Start date or starting event:**			T0		
Work package title	Link to the Industry and Reach out							
Activity type	RTD							
Participant number	1	2	3	4	5	6	7	8	9
Participant short name	Trialog Leader	CB	Oracle	TID	Vtools	UBER	KUL[16]	TUD	UMIL
PM per participant	4	0	1	10	5	6	20+0	0	0

Objectives

To assess the legal and ethical impact of CAPA contribution
To assess the impact of CAPA contribution on standardisation
To disseminate CAPA approach and results, and to liaise with relevant initiatives and projects
To identify a plan for use and dissemination

Description of work (possibly broken down into tasks) and role of partners

Task 1: Legal and Ethical Impact (T0 to T0+36)

The objective of this task is to assess the legal and ethical impact of CAPA contribution. It include the following subtasks

Subtask 1.1: State of the art (T0 to T0+4)

The objective of this task is to gather state of the art information about legal knowledge regarding various data protection technologies, in particular those similar to the ones proposed in this project. The existing European regulatory framework will be analysed from the perspective of privacy-enhancing technologies. The report will provide a starting point for legal analysis supporting the various work packages

Subtask 1.2: Legal requirements (T0+4 to T0+8)

The technologies developed in the CAPA project must fit perfectly within the existing European legal framework on data protection. To achieve this all relevant legal requirements must be taken into account from the start of the project.

The objective of this task is to provide input to WP2.T1 (Application and Technical Requirements) and WP4.T1 (Specification). Some of the threats to be considered are notably violations of data subjects rights. Likewise, requirements for data protection and privacy are determined to a large extent by applicable data protection regulation.

This subtask will focus on how architecture for privacy can be influenced by results in the area of research

Task 1.3.: Legal aspects of Security and Data Protection Models (T0+4 to T0+14)

During the development process, the correct implementation of the legal requirements must be monitored. The goal is to ensure that legal obstacles do not hinder the practical application of CAPA technology, in particular with regard to data protection regulation.

The objective of this task is to provide input to WP2.T2 (Security and Data Protection Models).

Task 1.4. Evaluation (T0+30 to T0+36)

The use case implementations will be evaluated in light of the legal requirements identified earlier in subtask 1.2. This activity will result both in a validation of the legal requirements and of the use case implementations.

An ethical perspective will also be taken.

The objective of this task is to provide input to WP4.T6 (Use case evaluation).

Partners and roles: KUL is the leader of this task. The roles of participants are the following

- KUL: Leadership
- Trialog : Subcontracting to expert on privacy and ethics

Task 2: Standardisation

The objective of this task is to assess the status of standardisation and to assess the potential impact of CAPA on those standards in terms of privacy. It includes the following subtasks

Subtask 2.1: Survey of current standards (T0 to T0+8)

The objective of this task is assess the current standards related to privacy and the application area tackled by WP4.

Subtask 2.2: CAPA impact on standards 1 (T0+8 to T0+20)

The objective of this task is to assess the impact of CAPA on standards (iteration 1).

Subtask 2.3: CAPA impact on standards 2 (T0+20 to T0+36)

The objective of this task is to assess the impact of CAPA on standards (iteration 2).

[16] 1st figure is for KUL/ICRI. 2nd figure is for KUL/COSIC

Partners and roles: TID is the leader of this task. The roles of participants are the following

- TID: Leadership, application area
- Trialog: application area
- VTools: application area
- Oracle: database
- KUL, TUD, UMIL, UBER : specific topics

Task 3: Dissemination and Liaison

The objective of this task is to disseminate CAPA approach and results and to ensure external liaison. It includes the following subtasks

Subtask 3.1: Dissemination material (T0 to T0+8)

The objective of this task is to prepare dissemination material (e.g. white paper, flyers, website=

Subtask 3.2: Dissemination and liaison 1 (T0+8 to T0+20)

Dissemination and liaison activities (iteration 1 to create awareness).

Subtask 3.3: Dissemination and liaison 2 (T0+20 to T0+36)

Dissemination and liaison activities (iteration 2 to disseminate results).

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- Trialog: Leadership, industry dissemination and liaison
- CB, VTools, TID, Oracle: industry dissemination and liaison
- KUL, TUD, UMIL, UBER : articles, presentations, and liaison

Task 4: Exploitation

The objective of this task is to build a plan for use and dissemination in 3 iterations

Subtask 4.1: Work on PUD V1 (T0 to T0+8)

Build a plan V1

Subtask 4.2: Work on PUD V2 (T0+8 to T0+20)

Build a plan V2

Subtask 4.3: Work on PUD V3 (T0+20 to T0+36)

Build a plan V3

Partners and roles: Trialog is the leader of this task. The roles of participants are the following

- TID, Trialog, VTools, Oracle: industry exploitation
- KUL, TUD, UMIL, UBER : academic exploitation

Deliverables (brief description) and month of delivery

D4 (T0+8) **Legal requirements**. Led by KUL.

D5 (T0+8) **Survey of current standards**. Led by Oracle.

D6 (T0+8) **Dissemination material**. Led by Trialog.

D7 (T0+8) **Plan for use and dissemination V1**. Led by Trialog.

D14 (T0+14) **Legal aspects of security and data protection models**. Led by KUL.

D18 (T0+20) **CAPA impact on standards V1**. Led by TID.

D19 (T0+20) **Dissemination and liaison report V1**. Led by Trialog.

D20 (T0+20) **Plan for use and dissemination V2**. Led by Trialog.

D31 (T0+36) **Legal evaluation report**. Led by KUL.

D32 (T0+36) **CAPA impact on standards V2**. Led by TID.

D33 (T0+36) **Dissemination and liaison report V2**. Led by Trialog.

D34 (T0+36) **Plan for use and dissemination V3**. Led by Trialog.

Table 1.3d Summary of Staff Effort

Part. no.	Participant short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	Total person months
1	Trialog	12	6	6	18		12	4	58
2	CB		2		3				5
3	Oracle		2	10	3		10	1	26
4	TID		8		36			10	54
5	Vtools		5		20		3	5	33
6	UBER		10	3		22	6	6	47
7	KUL		5	5	4	18	5	20	57
8	TUD		6	21			60		87
9	UMIL		10	10		16	12		48
Total		**12**	**54**	**55**	**84**	**56**	**108**	**46**	**415**

KUL includes 2 distinct departments: ICRI and COSIC.

Partic. no.	Partic. short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	Total person months
	KUL/ICRI				4			20	24
	KUL/COSIC		5	5		18	5		33

Table 1.3e List of Milestones

Milestone number	Milestone name	Work package(s) involved	Expected date [17]	Means of verification[18]
1	Requirements	2,5,7	T0+8	Deliverables D1,D2,D3,D4
2	Architecture	2,3,5,7	T0+14	Deliverables D9,D10,D11,D12,D13,D14
3	Design	3,4,5	T0+20	Deliverables D15,D15,D17
4	Implementation	4,5,6	T0+26	Deliverables D22,D23,D24 TRL indicator
5	Evaluation and Roadmap	4,7	T0+36	Deliverables D29,D30,D31

Technology Readiness Level indicator

In order to assess implemented building blocks, we propose to take a technology readiness level (TRL) viewpoint. We suggest to use the scale described in the table below. This table is inspired from the work carried out by NASA (Mankins, John C., (6 April 1995), Technology Readiness Levels: A White Paper, NASA, Office of Space Access and Technology, Advanced Concepts Office)

Scale	Description	Competitive Level	Technology Readiness Level (from NASA)
1	Vision	Pre-competitive	Basic principles observed and reported
2	Concepts	Pre-competitive	Technology concept and/or application formulated
3	Proof of concepts for feasibility	Pre-competitive	Analytical and experimental critical function and/or characteristic proof of concept
4	Technology at lab level	Pre-competitive	Component and/or breadboard validation in laboratory environment
5	Technology ready for integration	Pre-competitive	Component and/or breadboard validation in relevant environment
6	System prototype	Pre-competitive	System/subsystem model or prototype demonstration in a relevant environment
7	System prototype at operational level	Competitive	System prototype demonstration in an operational environment
8	System validated for deployment	Competitive	Actual system completed and 'flight qualified' through test and demonstration
9	System deployed	Competitive	Actual system 'flight proven' through successful mission operations

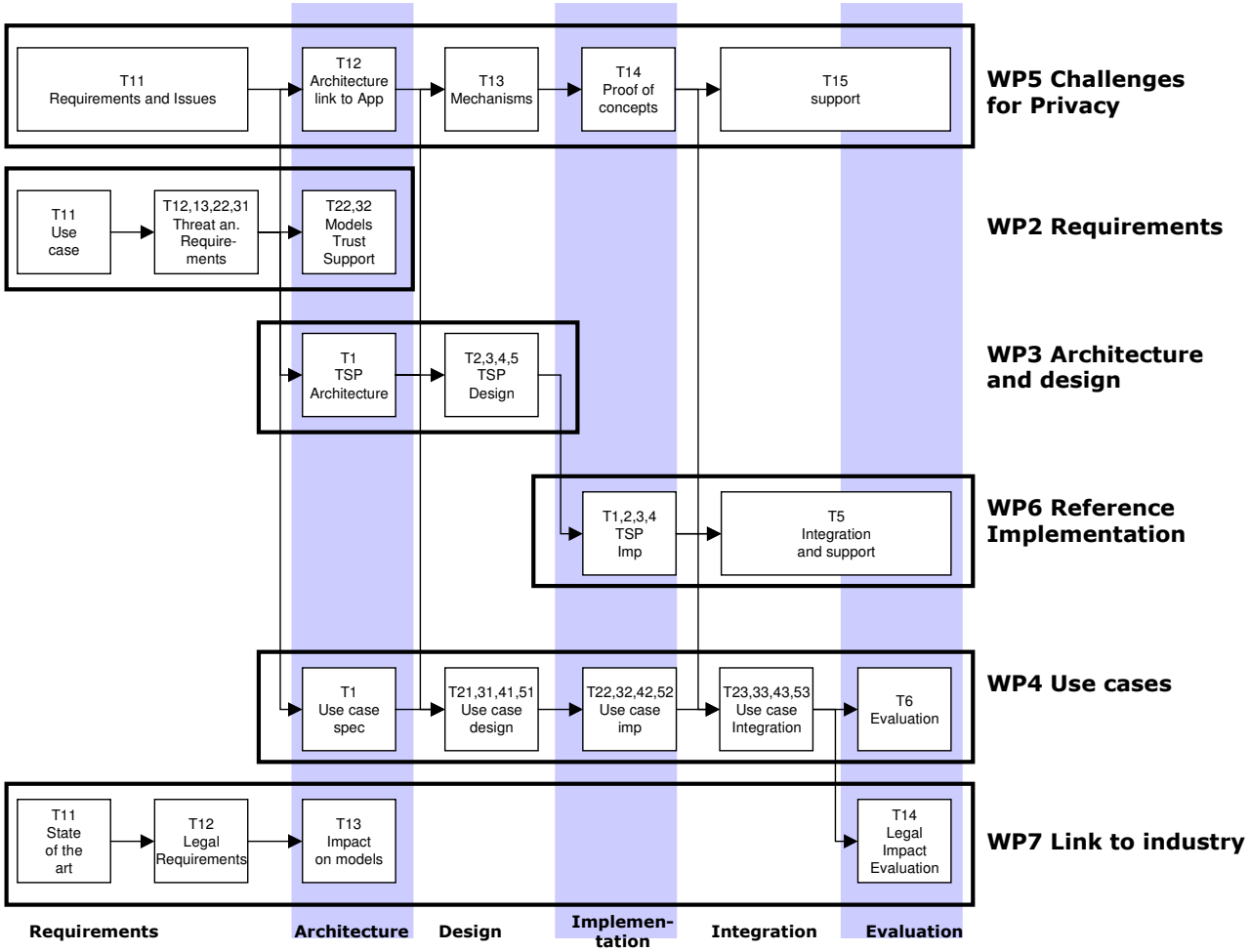
Component Dependencies

The figure below (notation "Txy" means Subtask y of task x) describes CAPA workplan component dependencies:

- At the WP level WP5, WP4, WP7 run in parallel. W2, WP3, WP6 are in sequence, according to the lifecycle (indicated by the vertical lanes)

[17] Measured in months from the project start date (month 1).
[18] Show how both the participants and the Commission can check that the milestone has been attained. Refer to indicators if appropriate.

- Within each WP there are a number of tasks which WP6 are in sequence, according to the lifecycle (indicated by the vertical lanes)



Here are the detailed task dependencies:

WP2 Requirements. Task 1: Application and Technical Requirements

Task 1 will coordinate requirements work with

- WP2.T2 which focuses on security and data protection models requirements (subtask T2.1)
- WP2.T3 which focuses on trust and empowerment requirements (subtask T3.1)
- WP5.T1 which focuses on linkage attacks research challenges (subtask T1.1)
- WP5.T2 which focuses on privacy of access research challenges (subtask T2.1)
- WP5.T3 which focuses on policy support research challenges (subtask T3.1)
- WP7.T1 which focuses on legal and ethical impact (subtask T1.1)

WP2 Requirements. Task 2: Security and Data Protection Models

Subtask 2.1: Requirements (T0+4 to T0+8)

Subtask 1.2: Models specification (T0+8 to T0+14)

Subtask 2.1 will coordinate requirement work with

- WP2.T1 which focuses on overall requirements (subtask T1.1)
- WP2.T3 which focuses on trust and empowerment requirements (subtask T3.1)
- WP5.T1 which focuses on linkage attacks research challenges (subtask T1.1)
- WP5.T2 which focuses on privacy of access research challenges (subtask T2.1)
- WP5.T3 which focuses on policy support research challenges (subtask T3.1)
- WP7.T1 which focuses on legal and ethical impact (subtask T1.1)

Subtask 2.2 will carry out specification work in liaison with

- WP2.T3 which focuses on trust and empowerment support specification (subtask T3.2)
- WP3.T1 which focuses on the overall architecture of the trusted storage platform
- WP4.T1 which focuses on privacy use case specification
- WP5.T1 which focuses on architecture aspects related to linkage attacks (subtask T1.2)
- WP5.T2 which focuses on architecture aspects related to privacy of access (subtask T2.2)
- WP5.T3 which focuses on architecture aspects related to policies (subtask T3.2)
- WP7.T1 which focuses on legal aspects in models (subtask T1.2)

WP2 Requirements. Task 3: Testing for Trust and Empowerment

Subtask 3.1: Requirements (T0+4 to T0+8)

Subtask 3.2: Trust support specification (T0+8 to T0+14)

Subtask 2.1 will coordinate requirement work with

- WP2.T1 which focuses on overall requirements (subtask T1.1)
- WP2.T2 which focuses on security and data protection models requirements (subtask T2.1)
- WP5.T1 which focuses on requirements related to linkage attacks (subtask T1.1)
- WP5.T2 which focuses on requirements related to privacy of access (subtask T2.1)
- WP5.T3 which focuses on requirements related to policy support (subtask T3.1)
- WP7.T1 which focuses on requirements related to legal and ethical aspect (subtask T1.1)

Subtask 2.2 will carry out specification work in liaison with

- WP2.T2 which focuses on security and data protection models specification (subtask T2.2)
- WP3.T1 which focuses on the overall architecture of the trusted storage platform
- WP4.T1 which focuses on privacy use case specification
- WP5.T1 which focuses on architecture aspects related to linkage attacks (subtask T1.2)
- WP5.T2 which focuses on architecture aspects related to privacy of access (subtask T2.2)
- WP5.T3 which focuses on architecture aspects related to policies (subtask T3.2)
- WP7.T1 which focuses on legal aspects in models (subtask T1.2)

WP3 Architecture and Design for Trusted Storage Platform. Task 1: Overall Architecture

Task 1 architecture work will be in liaison with

- WP2.T2 which focuses on security and data protection models specification (subtask T2.2)
- WP2.T3 which focuses on trust and empowerment support specification (subtask T3.2)
- WP4.T1 which focuses on privacy use case specification
- WP5.T1 which focuses on architecture aspects related to linkage attacks (subtask T1.2)
- WP5.T2 which focuses on architecture aspects related to privacy of access (subtask T2.2)
- WP5.T3 which focuses on architecture aspects related to policies (subtask T3.2)
- WP7.T1 which focuses on legal aspects in models (subtask T1.2)

WP3 Architecture and Design for Trusted Storage Platform. Task 2: Secure Operating System and File System

Task 2 work will be in liaison with

- Other design tasks of WP3 (T3 which focuses on database, T4 which focuses on policy management, T5 which focuses on test for trust support)

WP3 Architecture and Design for Trusted Storage Platform. Task 3: Secure Database

Task 3 work will be in liaison with

- Other design tasks of WP3 (T2 which focuses on OS and FS, T4 which focuses on policy management, T5 which focuses on test for trust support)

WP3 Architecture and Design for Trusted Storage Platform. Task 4: Policy Management Support

Task 4 work will be in liaison with

- Other design tasks of WP3 (T2 which focuses on OS and FS, T3 which focuses on database, T5 which focuses on test for trust support)
- Mechanisms specification tasks of WP5 related to policies (subtask 3.3)

WP3 Architecture and Design for Trusted Storage Platform. Task 5: Support for Empowerment

Task 5 work will be in liaison with

- Other design tasks of WP3 (T2 which focuses on OS and FS, T3 which focuses on database, T4 which focuses on policies)

WP4 Use Cases towards "la capa invisible". Task 1: Specification

Task 1 work will be in liaison with

- WP2.T2 which focuses on security and data protection models specification (subtask T2.2)
- WP2.T3 which focuses on trust and empowerment support specification (subtask T3.2)
- WP3.T1 which focuses on the architecture of a trusted storage platform
- WP5.T1 which focuses on architecture aspects related to linkage attacks (subtask T1.2)
- WP5.T2 which focuses on architecture aspects related to privacy of access (subtask T2.2)
- WP5.T3 which focuses on architecture aspects related to policies (subtask T3.2)
- WP7.T1 which focuses on legal aspects in models (subtask T1.2)

WP4 Use Cases towards "la capa invisible". Task 2: Privacy Preserving Surveillance

WP4 Use Cases towards "la capa invisible". Task 3: Vehicular Location Tracking Avoidance

WP4 Use Cases towards "la capa invisible". Task 4: Privacy Enabled Payment

WP4 Use Cases towards "la capa invisible". Task 5: Privacy Enabled Multimedia Interactions

Task 2,3,4,5 (X) include the following subtasks:

Subtask X.1: Use case design

Subtask X.2: Use case implementation

Subtask X.3: Use case integration

Which involve the following dependencies

- Subtask X.1 will be carried out in parallel with WP3 design tasks on elements of the trusted storage platform. Liaison will take place to ensure that the trusted storage platform conforms to the expectation of the use case
- Subtask X.2 will be carried out in parallel with WP5 implementation tasks on elements of the trusted storage platform. Liaison will take place to ensure that the trusted storage platform conforms to the expectation of the use case
- Subtask X.3 can start when WP5 implementation tasks have completed.
- Subtask X.3 will be carried out in parallel with an integration task in WP5, the purpose of which is to help in integration matters (1) for a standalone product, (2) for WP4 purpose (several WP5 partners are not in WP4)

WP5 Challenges for Privacy. Task 1:Linkage Attacks

WP5 Challenges for Privacy. Task 2:Privacy of Access

WP5 Challenges for Privacy. Task 3:Policies

Task 1,2,3 (X) are structured into a number of subtasks

Subtask X.1: Requirements Aspects

Subtask X.2: Architecture Aspects

Subtask X.3: Mechanisms and Link to Applications

Subtask X.4: Proof of concepts

Subtask X.5: Support

Subtask X.6: Contribution to research 1

Subtask X.7: Contribution to research 2

Subtask X.8: Roadmap

They involve the following dependencies:

- Subtask X.1 is synchronized with requirements tasks of other workpackages
- Subtask X.2 is synchronized with architecture tasks of other workpackages
- Subtask X.3 is synchronized with design tasks of other workpackages
- Subtask X.4 is synchronized with implementation tasks of WP4 and WP6
- Subtask X.5 is synchronized with integration tasks in WP4 and WP6

WP6 Reference Implementation. Task 1: OS and File System

Dependencies:

- Depends on completion of WP3
- In parallel to development tasks in WP4

WP6 Reference Implementation. Task 2: Secure Database

Dependencies:

- Depends on completion of WP3
- In parallel to development tasks in WP4

WP6 Reference Implementation. Task 3: Empowerment Support

Dependencies:

- Depends on completion of WP3
- In parallel to development tasks in WP4

WP6 Reference Implementation. Task 4: Policy Management Support

Dependencies:

- Depends on completion of WP3
- In parallel to development tasks in WP4

WP6 Reference Implementation. Task 5: Integration and Support

Dependencies:

- Depends on completion of Task 1, 2, 3, 4
- In parallel to integration tasks in WP4

WP7 Link to the Industry and Reach out. Task 1: Legal and Ethical Impact

Dependencies:

- Provide input to WP2.T1 (Application and Technical Requirements)
- Provide input to WP2.T2 (Security and Data Protection Models)
- Provide input to WP4.T1 (Specification)
- Provide input to WP4.T6 (Use case evaluation)

Risk Analysis

A number of risks have been identified while preparing the proposals. Several of them have influenced the proposal itself. Others have been taken into account through agreement on contingency approaches.

Risk on Trusted Platform Storage Objective

Risk description	How it is taken into account	Further contingency
Requirements missing	Multi-disciplinary participants to work at the technical level, application level, legal level Evaluation task to re-assess results	Incremental requirement approach so that modifications/extensions can take place even in the future
Requirements difficult to meet	Participation of partners with technology leadership and expertise (e.g. OS, File system, Database)	Identification of future challenges
Cost of platform development (it is known that OS, file system and database development is costly and risky)	Reuse TUD existing software implementations Reuse of Oracle Berkeley DB	Sub-setting platform Different platforms can be used temporarily at the use case level
Platform maturity	Use of TRL indicator Resource allocated for integration support	

Risk on Architecture for Privacy of Actors Objective

Risk description	How it is taken into account	Further contingency
QoS risk (e.g. crypto system to slow)	Reference platform oversized Possibility to change to more performing cryptosystem	Recommendations for improvement and future work
Cost risk	Many partners in CAPA are in a very cost conscious industry. Cost analysis to be made	Pragmatic profiling approach (i.e. subsetting) or roadmap approach (i.e. identify further steps to reach the cost goal)
Ethical and Legal compliance risk	Specific task to assess this aspect	Evaluation activity leading to recommendations
User acceptance	Specific task on trust and empowerment	Recommendations for improvement and future work
Privacy level reached	Evaluation task	Recommendations for improvement and future work

Risk on Challenges for Privacy Objective

Risk description	How it is taken into account	Further contingency
Research disconnected from project	Subtask structure following CAPA life cycle phases with synchronisation points	
Research on topic might not be successful	Focused research activity with expert partners	Liaison with research community Roadmap recommendations for the future

Deployment Risk

Risk description	How it is taken into account	Further contingency
Some part of the CAPA technology not mature yet for deployment	During dissemination focus on identifying possible subsets that are more mature for deployment	Roadmap approach
Lack of development initiative for the trusted storage platform	Open source approach	
Regulation risk	Specific task	Recommendations for the future

Standardisation and Risks

Risk description	How it is taken into account	Further contingency
Technology not standardised	Survey of standards and assessment of CAPA impact on standards	Standard initiative watch

Section 2: Implementation

2.1 Management structure and procedures

Project Structure

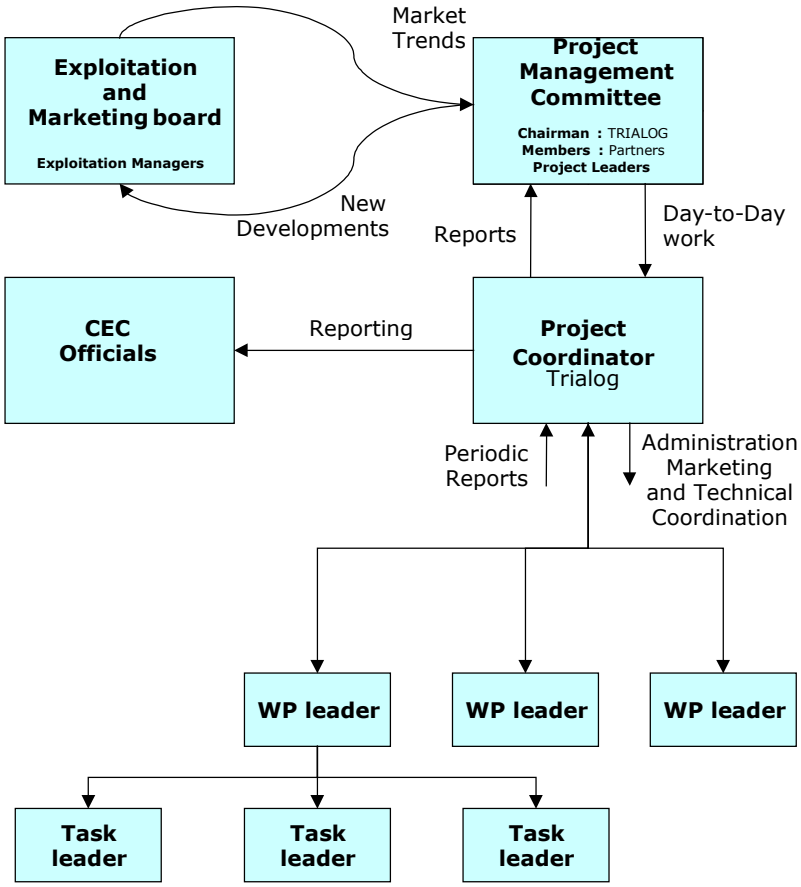
The project breaks down into seven well defined work packages with associated tasks is the basis of management and monitoring of the work.

The CAPA **Project Team** is composed of all the Partners and associated partners in the project. Each partner will formally identify

- **A Project Coordinator**, responsible for the technical deliverables of the project
- **An Exploitation Manager**, responsible for the Strategic and Commercial aspects of the project.
- **An Administrative Officer**, responsible for the provisions of costs and administrative information to the PMC and of the issue of periodic costs statements.

The CAPA **Project Team** will formally identify

- **Workpackage Leaders** and **Technical Leaders**, responsible for the progress to plan of the work packages and tasks.



CAPA PROJECT MANAGEMENT STRUCTURE

Project Management

The project management responsibilities are structured in four levels (see figure):

- Project Management Committee
- Project Co-ordinator
- Project Technical Steering Manager
- Workpackage Leaders
- Technical Leaders

The overall management of the project will be assumed by the **Project Management Committee** (PMC). The PMC is formed by all partners Project Managers, and chaired by the coordinating partners Project Manager. This committee will meet every three months to monitor the progress of the project. They will undertake the following tasks:

- Review the overall technical programme
- Review reports prior to submission to the EC
- Resolved disputes between participants not resolved at lower decision levels

For the day-to-day management the PMC will delegate to its Chairperson, who will be the **Project Coordinator.** The Project Coordinator will report to the PMC, who will be the maximum project authority (see decision procedures hereafter). The Project Coordinator will be the contact point of the project with EC.

He will coordinate the technical work of the various partners in order (1) to ensure that they are consistent, (2) that they meet the project technical objectives. The project technical steering manager reports to the project coordinator regularly (e.g. one hour teleconference per week). He also chairs all plenary technical meetings and closely monitor subgroup technical meetings.

In addition, the partners **Exploitation Managers** will form the **Exploitation and Marketing Board** (EMB). Because of the small size of the project, it is proposed that the EMB will meet every three months as an extended meeting to the PMC meeting. The EMB will take the strategic and marketing decisions to make products out of the developments within the project.

Work Package and Task management

Each work package will be managed as a sub project. Work package Leaders and Task Leaders will be in charge of the co-ordination of all the activities of the respective work packages or tasks. The Work package Leader will report to the Project Manager of the co-ordinator; the Task Leader will report to the Work Package Leader.

Technical and coordination meetings, if needed, will be organised by the Work package Leader. He will be responsible of the date of issue of the deliverables of his Work package, as defined in the global project work plan. The Task Leader will be responsible for the contents of the deliverable.

Decision Procedures

Voting will be the only method to resolve conflicts and to any change in the Consortium structure.

The PMC will be the maximum project authority. Decisions will be taken in the PMC by majority. Each partner will have a vote in the PMC. In case of tie in a voting result, the Chairman's vote will be a casting vote.

As far as work package internal decisions is concerned, they will be taken by majority of the participants. In case no majority results, a vote proportional to the work package participant shares will be taken. In case of conflict, the decision will be taken by the PMC.

Regarding tasks, the internal task decisions will apply the same procedure described for work packages. In case of conflict, the work package leader will take the decision.

Management of Knowledge, Intellectual Property, and or Innovation-Related Activities

Confidential information provided by any of the partners may be used freely within the scope and for the duration of the project. All information provided to the Project Team (or part thereof) is assumed to be 'Commercial in Confidence' and the provider looses no rights through its disclosure to the Project Team. Where it is felt necessary to formally establish Prior Art, a formal summary shall be prepared by the Partner concerned and circulated to all the Project Managers and will be filed by the Project Co-ordinator for the duration of the project.

While IPR made during the course of the project will be the property of those Partners developing it, agreement will be sought however to make sure that any specification work carried out with a standardization objective (e.g. API, protocol definition, application profile) will be made available as an open specification.

A consortium agreement taking into account IPR will be signed among partners.

2.2 Individual participants

Trialog

Trialog Organisation

TRIALOG is a system and software engineering company in the fields of real-time and embedded systems. It focuses on innovative systems for the automotive and home / consumer electronics marketplaces. Most of the devices being developed for these markets today have networking capabilities and can communicate with their environment, such as other peer devices and Internet access. Trialog core competencies are therefore oriented towards the right combination of real-time embedded software and networking technologies which are the keys to building such communicating devices and their interfaces to large business information systems. TRIALOG engineering process focuses on system, network and software architecture, design-to-cost and design-to-security.

Some work carried out recently include:

- Network protocols and connectivity solutions, in the area of automotive applications (VAN, CAN, TTP, Flexray, etc.), in the area of home networking including control buses such as the EHS/KNX bus, in the area of audio/video high-speed buses such as the IEEE1394 / HAVI bus, Hiperlan 2, etc. Connectivity solutions focus on embedded gateways with Internet capabilities (integration of OSGi technology) and wireless communications (GSM./GPRS, 802.11, Bluetooth, etc.).
- Coordination of security projects such as e-PASTA IST project (e-Protection of Appliances through Secure and Trusted Access) or GST-SEC (security subproject of GST IST IP). Technical coordination of the TEAHA (The European Home Application Alliance) IST project with support of security aspects. Coordination of the Sevecom (Secure Vehicule Communication) IST Project. Technica coordination of the e-Inclusion MonAMI IST project.

More information on Trialog can be found in http://www.trialog.com.

Trialog Main Tasks and Related Experience

Trialog will participate to the following :

- Management of the project (WP1). Trialog has extensive experience in IST project management (DICE, ePasta, Ajacs, Adapt, Sevecom).
- Requirements (WP2). Trialog has extensive experience in modelling which it would like to apply to security. It also has protocol conformance testing technology which it would like to adapt to CAPA.
- Architecture for trusted storage platform (WP3). Trialog will be involved in the high level architecture specification. This fits with Trialog extensive experience on architecture and integration of components in an embedded system according to an architecture. Trialog will also be responsible for the user empowerment task which fits with Trialog know how on implementation for test capability
- Use case related to vehicular communication (WP4). Trialog is co-ordinating the Sevecom project in this area. It would like to adapt existing demonstrations by adding trusted storage capabilities
- Use case related to multimedia interaction (WP4). Trialog is involved in a number of initiatives (e.g. the MonAMI e-inclusion project) from which an use case could be selected and adapted to include trusted storage capabilities
- Reference implementation (WP6), in particular in the area of user empowerment support and for integration and support

Specific innovation tasks will be contracted to Dennis Shasha

- Overall architect expertise
- Specification of the architecture for the privacy of actors (WP4)
- Participation to research challenges in particular on linkage attacks (WP5)

Specific innovation tasks will be contracted to Annabelle Lever

- Study of ethical impact (WP7)

Profile of Trialog Staff Members

Antonio Kung Antonio Kung has more than 25 years experience on embedded systems. He co-founded Trialog in 1987 where he is in charge of the development of software products such as protocols for the EHS/KNX home systems network, real-time kernels, and Java technology. He has led a number of security projects (e-PASTA, the security part of GST, Sevecom). He is currently co-chairing the eSecurity WG of the eSafety forum which focuses in particular on data protection. He holds a Master's degree from Harvard University, USA and an engineering degree from Ecole Centrale Paris, France.

Jérôme Billion Jérôme Billion has nearly 20 years experience in the area of embedded systems and automotive systems with a strong focus on multimedia, navigation and telematics systems. He is in charge of Trialog activities in telematics applications including Java-based technology and OSGi. He holds a Master's degree from Stanford University, USA and an engineering degree from Ecole Centrale Paris, France.

Dennis Shasha

Consultant to Trialog

Dennis Shasha is a professor of computer science at the Courant Institute of New York University where he works with biologists on pattern discovery for microarrays, combinatorial design, and network inference; with physicists, musicians, and financial people on algorithms for time series; and on database applications in untrusted environments. Other areas of interest include database tuning as well as tree and graph matching. Because he likes to type, he has written five books of puzzles, a biography about great computer scientists, and technical books about database tuning, biological pattern recognition and time series. He has co-authored fifty journal papers, sixty conference papers, and nine patents. For fun, he writes the puzzle column for Scientific American. Until July of 2007, he is at INRIA, Rocquencourt (near Paris, France) with the group of Philippe Pucheral. Dennis Shasha holds a BSc from Yale University, a MSc from Syracuse University and a PhD from Harvard University.

Annabelle Lever

Consultant to Trialog

Dr. Annabelle Lever has a BA in Modern History from Oxford University and a PhD in Political Science from the Massachusetts Institute of Technology. She currently teaches Political Philosophy at the University of Reading, and has an honorary appointment with the Philosophy Department of University College, London. During the past few years her main research interests have included issues of privacy in politics, the workplace, and the family, intellectual property rights, and the ethical, legal and social implications of the Human Genome Project. She has also taught Theories of Justice and of Rights and Normative Political Theory at Harvard and MIT. Her work on privacy and democracy, racial profiling and intellectual property rights is published in prestigious professional journals in Europe and the US such as Contemporary Political Theory, Philosophy and Public Affairs, Public Law, and Criminal Justice Ethics. She co-organised two conferences on privacy, equality and security at University College, London in February, 2007. Dr. Lever has currently two books in preparation: a book on privacy to be published by Routledge in 2008 and a book on Democratic Theory forthcoming at Oxford University Press.

Groupement des Cartes Bancaires

CB Organisation

The Groupement des Cartes Bancaires "CB" is France's main bank card payment scheme which ensures the coherence, reliability and security of the "CB" system. Cartes Bancaires provides a single, interbank, bank card payment and cash withdrawal system based on a smartcard. The CB system has been created in 1984 and is used today by all banking institutions operating in France.

The Groupement is actively participating to the work of the EPC (European Payments Council) whose objective is to build a unified European market of payment instruments and systems which needs to be compliant with the vision set out by the European Central Bank and the European Commission which encourages banks to provide a common framework for card-based transactions within the euro-zone.

Groupement des Cartes Bancaires will bring in the CAPA project its renowned expertise as issuer of technical specifications for the French bank card payment industry and main stakeholder in the participation of card related projects on behalf of its member banks.

CB Main Tasks and Related Experience

Groupement des Cartes Bancaires will be involved in the following tasks:

- Participation to the requirements work (WP2) with a focus on payment applications and privacy
- Participation to the specification of the privacy enabled payment use case in WP4
- Participation to the evaluation of the privacy enabled payment use case in WP4
- Liaison with existing payment initiatives

Profile of CB Staff Members

William VANOBBERGHEN

William VANOBBERGHEN, Head of International Projects within the Development & Strategy Department at Groupement des Cartes Bancaires, is in charge of the follow-up of the European Commission's information technology developments, payment systems and electronic commerce related issues at Groupement des Cartes Bancaires.

He has been co-ordinating and participating in several initiatives partly funded by European Commission (e.g. Interoperable C-SET, PACE, c-TRAVEL, FINREAD, Embedded FINREAD, Trusted FINREAD and FINREAD Showcase projects). He is now heavily involved in pan-European projects aimed at implementing the Single Euro Payments Area (SEPA) in Europe and is the Co-ordinator of projects such as EPAS (Card Payments related protocols) and ERIDANE (card acceptance equipment platform).

He holds a Degree in Commercial and Financial Sciences and a Degree and Master in Computer Sciences..

Oracle

Oracle Organisation

Oracle is the world's largest enterprise software company, its business is information — how to manage it, use it, share it, protect it. Oracle is the only vendor to offer information management solutions for every tier of business, from database, to middleware, business intelligence, business applications, and collaboration.

Oracle Main Tasks and Related Experience

Oracle will participate to:

- Analysis of possible security and data protection models with the objective of specifying at a sufficiently general and abstract level specific artefacts such as security levels, stakeholders, roles, enforcement (WP2).
- Design of the secure database system starting from Berkeley DB, an open source technology available from Oracle (WP3)
- Support in the specification, development and demonstration of privacy enable vehicular communication and privacy enabled multimedia interactions (WP4)
- Development of a reference implementation and ensure integration of the implemented building blocks in particular in relation to the secure database system (WP6)
- Assessment of the status of standardisation and of the potential impact of CAPA on those standards in terms of privacy (WP7)

Oracle is the world largest provider of enterprise software and has an outstanding track record in data security, identity management and compliancy with privacy regulations. Building mission-critical enterprise applications for many of the world's most "security-aware" organizations for over a quarter of a century has allowed Oracle to accumulate a depth of expertise on matters of software security. Oracle delivers secure infrastructure through a wide range of products, processes, and technologies to help prevent unauthorized access to confidential information, reduce the cost of managing users, and facilitate privacy management. Security related products include Oracle Database Vault, Oracle Audit Vault, Oracle Secure Back-up, Oracle Identity Management, Oracle Web Services Manager, Oracle Advanced Security Options, to mention a few.

Profile of Oracle Staff Members

Carlo Tarantola Carlo is a Doctor in Electronic Engineering from Genoa University 'Summa cum Laude'. Always interested and proficient with leading technologies, in Digital Equipment Corp. (DEC, then COMPAQ and now HP) he pioneered Internet with an unique and innovative system he invented in Intelligent Tutoring and Intelligent Database Navigation, built around semantic knowledge representation, multimedia data, Internet distributed client-server architectures, object-oriented databases and fuzzy-logic based kernel that became a DEC product. After eight years in DEC he joined AT&T Bell Laboratories and then AT&T Labs where he designed a satellite network for a Multimedia University. Attracted by the telecommunications world, he joined Lucent Bell Labs as R&D Director for Europe Middle East and Africa (EMEA) where he participated in the evolution of the innovative concept of Softswitch to allow transport and control of voice streams in packet networks. Because of such a wide background and expertise, Carlo was appointed Chief Scientist and R&D responsible for Trader.com where he supervised activities in Machine Translation, 3D imaging, Virtual Communities, Wireless Communication and Wireless Internet and E-commerce. Carlo was one of the co-founders for an Automotive Telematics company called mFutureLabs, which, after generating 750,000 Euro in its first year, has moved its operations to Volkswagen & Wolfsburg (Germany). Currently working for Oracle Corporation where he is evangelizing Oracle's Pervasive Mobile & Wireless capabilities as a differentiator. He evaluated, created and recruited the Near-Shore Center of Excellence in Warsaw, Poland.

Fulvio Sansone Fulvio joined Oracle in March 2006 where he is responsible for the European Infrastructure Programs Office. After graduating in Electrical Engineering at University of Naples in 1990, Fulvio worked with Ericsson and Ansaldo Trasporti in the development of software and firmware for data communications. In 1994 he obtained the Master of Business Administration from the Consorzio Universitario Organizzazione Aziendale –CUOA-, the oldest Italian business school, with special honours. After a six-month internship at the European Space Agency where he developed the business plan for a telecommunications satellite, Fulvio joined SAIT-RadioHolland, a Belgian company in mobile and satellite communications where he covered several roles during more than six years as Project Manager, Sales Manager, Business Development Manager and finally Business Unit Manager. In 2001 he joined ERTICO, a public-private partnership for the implementation of telematics in Europe, where he was responsible for the development of the satellite positioning line of activity. In parallel in 2002 he took the responsibility of Secretary General of the European Satellite Operators Association that he covered until mid-2004. After a six-month assignment with the European Business and Innovation Centre Network –EBN- between end-2005 and beginning-2006, he joined Oracle in March 2006.

TELEFÓNICA I+D Organisation

TID Organisation

Telefónica Investigación y Desarrollo (I+D) is the innovation company of the Telefónica Group. Owned 100% by Telefónica, this subsidiary was formed it 1988, with the aim of strengthening the Group's competitiveness through technological innovation.

Since it was founded in March 1988, its results have been directed at creating value for the clients of the Group, developing high-quality telecommunication products, services and systems. Telefónica I + D employs over 1000 persons, of whom 93% hold a University degree.

Telefónica's innovation process, which is largely based on the activities of Telefónica I+D, is based on four fundamental lines of work: infrastructures, development of new services, deployment of "personal digital environment" and, a series of common elements which play the role of for the rest of activities. These four lines contribute to the internal evolution necessary to face the future challenges of the changing Telecom and IT panorama.

Telefónica I + D is and has been involved in a large number European projects, such as: RACE II, ESPRIT III, TEN-ISDN, CTS, COST, EURESCOM, BRITE, Ten-Telecom, e-Ten, e-Content, EUREKA (ITEA, MEDEA & CELTIC). The

Telefonica Group participates in the principal standardisation fora for fixed, mobile and wireless communications, convergence, etc. (ITU, OMA, IEEE, IETF, IPv6Forum, W3C…).

Regarding the topics addressed in CAPA, Telefónica I+D has a wide experience in Identity Management and security projects, both at international and national level. As coordinator of the FP6 BioSec project, an important work of research and development in technologies for improving secure and strong authentication, as well as integration of these technologies in secure systems, was done. Moreover, Telefonica I+D currently collaborates in other EU funded projects, as Humabio.

TID Main Tasks and Related Experience

As a Telecom operator, Telefónica is very interested in privacy and storage issues, and is highly concerned about privacy and integrity of users data. Therefore, Telefonica I+D will actively participate in the CAPA project by delivering requirements (WP2) to the CAPA architecture in order to meet the need of a company that manages sensitive information about users. Telefonica I+D will also validate the proposed architecture. Telefonica I+D will propose and evaluate use cases that may make use of CAPA invisible cloak to minimize user and providers identity data release, and to secure the information (WP4).

Profile of TID Staff Members

Mr. Carlos Plaza Fonseca -Telecom Engineer. Project Manager.	Carlos Plaza Fonseca graduated from the Universidad Politécnica de Madrid. He began collaborating in Telefonica I+D in 1992 in the area of Traffic and Signalling Management Systems. In 1998 he joined the consultancy unit to and participated in the evaluation of solutions for internet access, UMTS networks, development of telecom operator process map, viability and deployment of a new operator , business plans for residential gateways and advance home services. From 2005 he is involved Digital Identity projects: identity federation, identity management metasystems and strong authentication.
Dr. Pedro Luis Muñoz	Dr. Pedro Luis Muñoz received an MsC in Computer Sciences in 1986 and a PhD. in 1991 from Faculty of Computer Sciences, Universidad Politecnica de Madrid. He was an assistant professor from 1988 to 1990, and he joined Telefonica I+D in 1990. Currently he holds the position of Head of Department of Services of Cryptography and Identity Management, coordinating several projects in the areas of digital certificates and PKI, smart cards, biometric authentication and digital federated identity.

Visual Tools

VT Organisation

Visual Tools (VT, ES) is a Spanish SME located in Madrid with 52 employees and an annual turn-over in 2006 of 8 million Euro, whose single activity is developing digital video monitoring systems. The company, founded in 1995, is focused on product development, and manufacturing and has extensive agreements with leading distribution companies in the security and CCTV industries who sell Visual Tools' products under their own brand names all over the world. Visual Tools has a leading position in the video security market, in particular in bank branch monitoring systems, retail, and advanced digital video monitoring systems for large installations. Visual Tools sells its products through companies in the security and CCTV industries, who in turn sell the products to security installers and end-users under their own brand names. Among Visual Tools' customers are some of the most important companies in the security market, such as *Honeywell* (the building management systems world leader), *Norbain* (UK), *HESA* (Italy), *Gardiner* (France), *Afroluso* (Portugal) and others. Through these companies Visual Tools' products are installed in nearly all countries in Europe, especially important is their presence in the bank branch monitoring sector, with more than 40,000 installations already in place. The company's main product in the video surveillance market is the VideoSafe product line. VideoSafe is a low-cost digital video recording and video transmission system primarily oriented to fulfil remote monitoring needs. Currently the VideoSafe systems, under different brand names, are being used by, for example: banks, transport companies (Madrid Underground), large installations (Madrid airport Terminal 4, Dubai airport), alarm reception centres and supermarket chains.

Visual Tools S.A. has developed advanced hardware and software platforms for digital video storage and transmission. The software platforms allow for a component-based development of digital video equipment using third-party modules, some with artificial vision capabilities. They are based on Linux and RT-Linux and they use quality of service techniques developed in research projects to enable an efficient use of the available resources. The R&D team of the company masters technologies in embedded system development, video streaming and video recording, and component-based security systems. This expertise is confirmed by the participation in research projects at national an international level in the areas mentioned above, acting as coordinator (e.g. IST-1999-10808-VISOR BASE) or partner (e.g. FP5-Ocera, ITEA-Trust4All, Eureka-SIVIWEB, CENIT-Hesperia, to mention a few).

More information on Visual Tools can be found in http://www.visual-tools.com/

VT Main Tasks and Related Experience

Visual Tools will participate to the following:

- Requirements specifically on use cases (WP2). Visual Tools has experience in trusted system specification. To strengthen the company participation in this activity an expert in use case requirements will be employed as subcontractor (see below).

- Use case related to privacy preserving video surveillance (WP4). Visual Tools is a market leader in digital video products. It will develop a new digital video surveillance system respecting people's privacy by using video analysis techniques.
- Reference implementation, in particular in the area of integration and support (WP6). This activity will ensure that the reference implementation runs in the Linux system used in the surveillance platforms.
- Link to the industry and reach out. Visual Tools will be involved in industry dissemination activities and in exploitation analysis activities (WP7).

Specific tasks will be contracted to Prof. José-Luis Fernández from Polytechnic University of Madrid. Prof. Fernández is an expert in software engineering and embedded real-time systems. He will be involved in particular in the following tasks:

- Use case in particular in malicious use cases
- Specification of privacy preserving surveillance use case
- Participation in dissemination

Profile of VT Staff Members

Francisco Gómez-Molinero	Co-founder and Director of Innovation and Technology of Visual Tools is responsible for the company strategy in research and development of the new video surveillance systems. He graduated in Telecommunication Engineering at Polytechnic University of Madrid. Prior to that, he worked at ESTEC, the European Research and Technology Center of the European Space Agency in The Netherlands. He worked at the On-Board Data Division and he was technical responsible of several projects based on parallel architectures, and video compression technology for the European segment of the International Space Station. He has been consultant of the Spanish Ministry of Science and Technology, the Austrian Ministry of Science and the European Commission.
Félix Sáinz-Martín	is Development Director at Visual Tools since 2001. He holds a Master degree in Electrical Engineering from Polytechnic University of Madrid. He has ten years experience in the development of Internet systems and video surveillance systems. He has been involved in several research projects since 1997, in particular, HOMENET (ESPRIT-IV) and HESPERIA (National Research Project of the Spanish CENIT Programme).
Francisco Cabello Torres	Is Project Manager at Visual Tools since 2001. He holds a Master degree in Computer Sceince from Universidad Complutense of Madrid. He has seven years experience in the development of digital video surveillance systems. Prior to working at Visual Tools he was involved with the Spanish monetary authority (Fabrica National de Moneda y Timbre) participating in the development of the National certification authority for citizen's identification in Internet operations with the Public Administrations.
Prof. José-Luis Fernández Consultant to Visual Tools	has a Ph.D (Hons.) in Computer Science and an Engineering Degree in Aeronautical Engineering, from Madrid Technical University (UPM). He has 25 years of experience in industry as system engineer, project leader, researcher and department manager. He was involved in projects dealing with software development and maintenance of large systems for air traffic control, banking, Supervisory Control and Data Acquisition (SCADA) and cellular phone applications. He has been leading several research projects related to avionics, air traffic flow management, location based cellular phone services, OSGi residential gateways, multimedia applications and CASE tools. During 1993, he was visiting scientist at the SEI, Carnegie Mellon University, Pittsburgh US. Currently, he is consultant, researcher and part time professor at the Industrial Engineering School of the Madrid Technical University (UPM). He is coauthor of a book and has published more than 25 papers in conferences and workshops.

Humboldt University

UBER Organisation

Humboldt-Universität zu Berlin is one of the leading universities in Germany. As a full university it advances science and performs research in arts and science on the highest national and international level. The university is well known for its past contribution in science, his many Nobel laureates as well as for it revival after the fall of the Iron Curtain. More information on Humboldt-Universität zu Berlin and the Computer Science Department (Institut für Informatik) can be found under http://www.hu-berlin.de and http://www.informatik.hu-berlin.de.

The participating research and technology transfer group is the DBIS (DataBase and Information System) research group headed by Prof. Johann-Christoph Freytag, Ph.D. The research group has an extensive track record for participating in various research and transfer technology projects.

Some work carried out by DBIS at Humboldt-Universität zu Berlin recently includes:

- Defining and developing algorithms for access privacy in database management systems as part of the Germany BMBF-funded project InterVal (Internet and Value Chains) – please see http://interval.hu-berlin.de/content/en/overview/index.php. As part of the project the team also developed an RFID protocol for copy protecting goods; a patent developed during the project was sold to one of the leading German IT companies.
- Participating in the German government funded Bioinformatics project BCB - Berlin Center for Genome Based Bioinformatics – please see http://www.bcbio.de/. Within this project DBIS at Humboldt-Universität zu Berlin developed database oriented applications for cleansing and processing genetic data as well as frame works for scientific exploration.

- A bilateral project with Siemens AG, Munich, Germany, the DBIS group at Humboldt-Universität zu Berlin develop a highly sophisticated query optimizers for Siemens' LDAP product DirX to improve the query performance.

More detailed information as well as an extensive publication list and list of participation in industrial projects can be found under http://www.dbis.informatik.hu-berlin.de/index.php?id=5&L=1.

UBER Main Tasks and Related Experience

DBIS at Humboldt-Universität zu Berlin will participate to the following:

- Requirements specifically on security and data protection models (WP2)
- Developing a model for linkage attacks, how to avoid, to protect, and to counterfeit them. DBIS at Humboldt-Universität zu Berlin will be involved in designing an architecture and in exploring its realization in a prototype. This effort fits with DBIS' research background and recent results in projects related to privacy (WP5).
- Participation to the design of the secure database building block (WP3). Responsibility of development (WP6)
- Support of industrial partners to include the results of this effort in their real life scenarios, and reach out (WP7). DBIS at Humboldt-Universität zu Berlin will perform technology transfer for avoiding or preventing linkage attacks and support efforts industrial partner in using the results in their industrial settings.

Profile of UBER Staff Members

Johann-Christoph Freytag

Johann-Christoph Freytag, Ph.D. has been a full professor for databases and information systems at Humboldt Universität zu Berlin, one of the leading universities in Germany since 1994. Before he work in industrial research for almost 9 years at the IBM Almaden Research Center, the European Industry Research Centre, and Munich, Digital Equipment, Munich. He received his Ph.D. from Harvard University, MA, USA in 1985.

Prof. Freytag has worked in various national and international projects in the area of databases, privacy, RFID, and Bioinformatics. He has been a four time recipient of IBM's faculty award and IBM's SUR Grant. He has consulted for SAP, IBM; Siemens, and Microsoft both nationally and internationally. He has published over 50 articles and has written and edited several books in the area of databases and information systems.

KU Leuven

Two entities of KU Leuven are involved in the project: COSIC and ICRI

COSIC Organisation

The Katholieke Universiteit Leuven carries out fundamental and applied research in all academic disciplines. In the past few years in particular, the quality and quantity of the K.U.Leuven's efforts and output have considerably increased, thus positioning Leuven at the forefront of European universities.

Research at the university is characterized by originality and innovation, successful applications, and the virtual disappearance of interdisciplinary boundaries. Its basic orientation has always been and will remain fundamental research, in accordance with the university's mission. At the same time, however, our university remains vigilantly open to contemporary cultural, economic, and industrial realities, as well as to the community's needs and expectations.

The focus of COSIC's research activities is on computer security and (industrial) cryptography (hence the name). It is part of the Department of Electrical Engineering at the Katholieke Universiteit Leuven. COSIC was established in 1978 and started immediately conducting basic research, applied research and contract research.

Over 50 researchers receive or have received a highly varied training in the different fields that form the basis for the research, including discrete mathematics, cryptology, hardware- and software implementations, networks and computer systems. A broad basis helps COSIC adopt an integrated approach to problem solving. This method has led to important successes, such as for instance the selection of the Rijndael algorithm as the US Advanced Encryption Standard (AES), which is a worldwide standard today.

In its applied research COSIC tries to find an electronic equivalent for interactions and transaction in the physical world. Basic research is applied to a broad range of domains, such as electronic identity cards, electronic election procedures, protection of e-documents, intelligent home appliances, telematics for the automobile industry and trusted systems (TCG, NGSCB).

During the past 15 years, COSIC has participated in more than 20 European research projects. In three of these it acted as the coordinator: New European Schemes for Signatures, Integrity, and Encryption (NESSIE); Strategic Roadmap for Cryptography (STORK); European Network of Excellence for Cryptology (ECRYPT). COSIC participated in approximately the same number of Flemish and Belgian research projects. Short- and the medium-term contract research was carried out for companies like Banksys, Hitachi, Hypertrust, Mastercard, Microsoft, Philips, PriceWaterhouseCoopers, Sony, S.W.I.F.T. and the Belgian Federal Government (Internal Affairs, Federal Public Service for ICT - FEDICT).

COSIC's thorough experience, gained through a long history of participation in European projects (PRIME, FIDIS, GST, TEAHA, MODINIS, SPEED, …), enables it to participate in the CAPA project. From its broad expertise in privacy enhancing technologies, identity management systems, and the design and analysis of cryptographic algorithms, protocols and architectures, COSIC's activities will focus on the security assessment of the designed solutions, including both protocols and applications.

COSIC Main Tasks and Related Experience

COSIC will participate to the following:

- Requirements (WP2) and Trusted storage platform architecture and design (WP3). The starting point will be the architecture work carried out by COSIC in GST, TEAHA, Sevecom.
- Challenges on privacy with a focus on privacy of access, relying on the extensive research already contributed by COSIC in the area (WP5).

Profile of COSIC Staff Members

Bart Preneel

Prof. Bart Preneel received the Electrical Engineering degree and the Doctorate in Applied Sciences from the Katholieke Universiteit Leuven (Belgium). He is currently professor (hoogleraar) at the Katholieke Universiteit Leuven and visiting professor at the T.U.Graz in Austria. He was visiting professor at several universities in Europe (Ghent, Belgium, Bergen, Norway and Bochum, Germany). During the academic year 1993-1994, he was a research fellow of the EECS Department of the University of California at Berkeley. His main research interests are cryptography, network security, and wireless communications.

He has authored and co-authored more than 180 scientific publications and is an inventor of two patents. He is vice president of the IACR (International Association for Cryptologic Research) and a member of the Editorial Board of the Journal of Cryptology, the IEEE Transactions on Information Forensics and Security, and the ACM Transactions on Information Security. He is also a Member of the Accreditation Board of the Computer and Communications Security Reviews (ANBAR, UK).

He has participated in more than 15 research projects sponsored by the European Commission, for four of these as project manager. He is currently project manager of the European Network of Excellence ECRYPT (http://www.ecrypt.eu.org), which groups more than 250 researchers in the area of cryptology and watermarking.

He has been program chair of five international conferences (including Eurocrypt 2000 and SAC 2005) and he has been been invited speaker at 15 conferences; he has served on the program committee of more than 60 conferences. In 2003, he has received the European Information Security Award in the area of academic research, and he received an honorary Certified Information Security Manager (CISM) designation by the Information Systems Audit and Control Association (ISACA).

Since 1989, he is a Belgian expert in working group ISO/IEC JTC1/SC27/WG2 (Security Techniques and Mechanisms), where he has edited five international standards.

Danny De Cock

Danny De Cock researches applied cryptography at the Katholieke Universiteit Leuven in Belgium. Danny is an expert in computer security and industrial cryptography applications and he has conducted extensive research projects in this field.

His work includes the analysis and design of identity management systems and secure communications architectures for various environments and communities. He has also researched security aspects of mobile devices, electronic banking, electronic voting schemes and electronic identity cards.

Most recently he has laid out the security architecture and functionality of the IBBT project IDEM (Identity Management for Belgian eGovernment), and of the European project SEVECOM (cf. http://sevecom.org). He has also specified the security architectures of the European projects TEAHA and GST, cf. http://www.teaha.org and http://www.gstforum.org, respectively.

Danny was also involved in the Modinis-IDM study on identity management in eGovernment, cf. https://www.cosic.esat.kuleuven.be/modinis-idm.

Claudia Diaz

Dr. Claudia Diaz is a post-doctoral researcher at COSIC, K.U.Leuven. She received the Telecommunications Engineering degree (Ingeniero Tecnico Superior de Telecomunicaciones) in 2000 from the University of Vigo (Spain). In November 2000, she joined the research group COSIC as pre-doctoral student. She started her Ph.D. in October 2001 under the supervision of Prof. Bart Preneel and Prof. Joos Vandewalle. Her Ph.D. thesis, entitled 'Anonymity and Privacy in Electronic Services' was defended in December 2005. The topics of research she has been working on include anonymity metrics, anonymous communications, and privacy-enhancing technologies. She has more than fifteen publications in international, peer-reviewed journals and conferences, has participated in eight Program Committees, and has been active in several European and Flemish projects

ICRI Organisation

ICRI is a large research group with about 25 researcher conducting research in several fields of Law & ICT and Legal Informatics. ICRI is involved in a multitude of FP6 European Projects, having gained valuable expertise and experience in ICT Law.

ICRI is currently participating as leader of the legal Workpackage in the PRIME project (www.prime-project.eu), where we are setting out the legal requirements for the PRIME Identity Management system. One of our main tasks within the project is the Evaluation of the PRIME Integrated Prototype, as well as the Evaluation of two Application Prototypes, one on Location Based Services and one on Collaborative eLearning. ICRI is also participating in the Network of Excellence FIDIS, where significant work on Privacy and Identity Management is being produced.

ICRI is also conducting significant research at Flemish level on eHealth within several projects funded by the Institute for Broadband Technologies (IBBT, www.ibbt.be). In the E-HIP (E-Health Information Platforms) project, a regional information platform for the healthcare sector is designed, which offers authorised care personnel safe and reliable access to confidential the clinical information of patients.

Also, ICRI is involved in a Flemish project on the development of advanced applications for the e-ID (ADAPID), which aims to develop privacy-enhanced applications. The use cases selected by ADAPID are trusted storage, e-health and e-government applications.

More information about ICRI can be found at: http://www.law.kuleuven.be/icri/

ICRI Main Tasks and Related Experience

ICRI will be responsible for the study of legal aspects focusing on data protection (WP7). ICRI has extensive experience in providing legal support to technical development projects, in particular in the area of data protection technology as illustrated by the examples listed above.

Profile of ICRI Staff Members

Jos DUMORTIER Prof. Dr. Jos DUMORTIER is a professor in Information Technology Law and Legal Informatics at the Faculty of Law, K.U.Leuven since 1989 and Director of the Interdisciplinary Centre for Law and Information Technology (ICRI) since its start in 1990. He is regularly working as an expert for the European Commission, for Belgian and foreign governments and for private organizations. He is a member of several boards and committees in Belgium and abroad. He is also the chairman of the Legal Interest Group of EEMA. Professor Dumortier published numerous books and articles on various issues related to information technology law, electronic communications law and legal informatics. He is the editor of the International Encyclopedia of Cyber Law. Jos Dumortier is also member of the Brussels Bar and is the director of the "E-Business & ICT" department of the law firm Lawfort.

Eleni KOSTA Mrs. Eleni KOSTA obtained her law degree at the University of Athens in 2002 (magna cum laude) and in 2004 she obtained at the same University a Masters degree in Public Law (summa cum laude). In the academic year 2004-2005 she attended the Postgraduate Study Programme in Legal Informatics (Rechtsinformatik) of the University of Hanover (EULISP) with a scholarship from the Greek State Scholarships Foundation (IKY) and she obtained her LL.M. (magna cum laude). Eleni is preparing a PhD at the Katholieke Universiteit Leuven on "Consent as a legitimate ground for data processing in electronic communications", under the supervision of Prof. Dr. Jos Dumortier. Eleni joined ICRI in summer 2005, where she conducts research in the field of privacy and identity management, specialising on new technologies and electronic communications. She is working on the European Project PRIME (Privacy and Identity Management for Europe) and is also involved in the Network of Excellence FIDIS (Future of Identity in the Information Society).

TU Dresden

TUD Organisation

Technische Universität Dresden (TUD) was founded in 1828 and is among Germany's oldest and most renowned universities of technology. The TUD is the largest university in the region, with more than 30,000 students and 4,500 employees, including about 600 professors.

Prof. Dr. Hermann Härtig is the leads the operating systems groups at TUD. The group has substantial experiences in building micro-kernels and in applying micro-kernel technology to real-time and high security systems. This is documented in various publications in high-level international conferences ([1],[2],[3],[4],[5],[6],[7],[8]). L4/Fiasco – TU Dresden's implementation of the L4 interface – is widely used, in research as well as in commercial products. The group is currently part of several EU and Germany wide funded project where the technology developed by the group is used and further improved.

TUD Main Tasks and Related Experience

TUD's operating systems group has extensive experience in operating-system construction, especially micro-kernel based real-time and security architectures including support for hosting other legacy operating systems and applications. The group's research in this area aims at minimal trusted computing bases in the system.

In the CAPA project, TUD will contribute the architecture and implementation of a secure operating system and a secure file system and will thus be active in WP3 and WP6.

References

[1] H. Härtig, M. Hohmuth, J. Liedtke, S. Schönberg, J. Wolter. The Performance of m-Kernel-based Systems. In the 16th ACM Symposium on Operating System Principles, 1997.
[2] H. Härtig. Security Architectures Revisited. In the 10th ACM SIGOPS European Workshop, Saint-Emilion, France, Sept 2002.
[3] M. Hohmuth, M. Peter, H. Härtig, J. Shapiro, Reducing TCB size by using untrusted components – small kernels versus virtual-machine monitors. In Proceedings of the 11th ACM SIGOPS European Workshop, Leuven, Belgium, 2004.
[4] F. Mehnert, M. Hohmuth, H. Härtig: Cost and benefit of separate address spaces in real-time operating systems. In the Proceedings of the 23th IEEE Real-Time Systems Symposium (RTSS-XXIII), 2002, Austin, TX, USA
[5] L. Reuther, M. Pohlack: Rotational-Position-Aware Real-Time Disk Scheduling Using a Dynamic Active Subset (DAS). In the Proceedings of the 24th IEEE Real-Time Systems Symposium (RTSS 2003), 2003, Cancun, Mexico
[6]J. Liedtke, H. Härtig, M. Hohmuth: OS-Controlled Cache Predictability for Real-Time Systems. In the Proceedings of the 3rd IEEE Real-time Technology and Applications Symposium (RTAS'97), June 9-11, 1997, Montreal, Canada
[7] J. Löser, H. Härtig, Low-latency Hard Real-Time Communication over Switched Ethernet. In Proceedings of the 16th Euromicro Conference on Real-Time Systems (ECRTS), Catania, Sicily, Italy, 2004.

[8] H. Härtig, M. Hohmuth, N. Feske, C. Helmuth, A. Lackorzynski, F. Mehnert, M. Peter: The Nizza Secure-System Architecture; presented at the First International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2005), San Jose, California, USA , December 2005
[9] Roitzsch, Härtig: Ten Years of Research on L4-Based Real-Time; proceedings of the Eighth Real-Time Linux Workshop, Lanzhou, China, 2006 , 2006

Profile of TUD Staff Members

Prof. Dr. Hermann Härtig	Chair on Operating Systems at Technische Universität Dresden, Principle investigator of BirliX Security Architecture project at German National Research Center(1984-93), extensive experience in systems security, real-time systems and micro-kernel technology. His research covers many areas in the field of operating systems including real-time operating systems, security and micro-kernel technology. Hermann Härtig is co-founder of the European Chapter of the ACM Special Interest Group on Operating Systems and serves in many program committees of important international conferences.
Dipl.-Inf. Carsten Weinhold	Carsten Weinhold studied at Technische Universität Dresden and received his master of computer science (Diplominformatiker) in 2006. As a continuation of the work done in his master thesis, he has been working on secure file systems based on micro-kernel based system architectures. He has also gained experience in the area of trusted computing technology.

U Milano

UMIL Organisation

The university of Milan (UMIL) has more than 50,000 students and offers degrees in all areas. The Information Technology Department, where the proponent group works, conducts theoretical and experimental research in most areas of computer science and technology, including: data protection; access control models, policies, and languages and security and privacy in general; with research results published in international conferences and journals. Recent projects include EU-funded: FASTER (Flexible Access to Statistics, Tables, and Electronic Summaries), targeted to the secure publication of data on the Web; RAPID Roadmap (Roadmap for Advanced Research in Privacy and Identity Management), targeted to the identification of R&D challenges in privacy technology and identity management; and PRIME (Privacy and Identity Management for Europe), targeted to the development of privacy-aware solutions for enforcing security.

UMIL Main Tasks and Related Experience

UMIL will participate to the following:

- Requirements (WP2) and Trusted storage platform architecture and design (WP3), focusing on policy managment support. Development of policy management support (WP6).
- Challenges on privacy with a focus on policies, relying on the extensive research already contributed by UMIL in the area (WP5).

Profile of UMIL Staff Members

Pierangela Samarati	Pierangela Samarati is a professor at UMIL. Her main research interests are in data management and protection. She has published more than 150 papers in international journals, books, and conferences. She has participated in several research projects at the national and international level. She has been a computer scientist at SRI International, CA (USA) and a visiting researcher at Stanford University, CA (USA), and George Mason University, VA (USA). She is chair of the Steering Committees of the ACM Workshop on Security and Privacy (WPES), and a member of the steering committee of several conferences. She is vice-chair of the Steering Committees of: European Symposium on Research in Computer Security (ESORICS) and of the ACM SIGSAC - Special Interest Group on Security, Audit, and Control. She is the Italian representative within IFIP (International Federation for Information Processing) and the chair of the IFIP WG11.3 on Data and Application Security. She has participated in the XACML Technical Committee.
Sabrina De Capitani di Vimercati	Sabrina De Capitani di Vimercati is a professor at UMIL. Her research interests are in the area of information security, databases, and information systems. She has published more than 100 papers in international journals, books, and conferences. She has been an international fellow in the Computer Science Laboratory at SRI, CA (USA). She is member of the Steering Committees of Workshop on Security and Privacy (WPES) and of European Symposium on Research in Computer Security (ESORICS). She has served as the program chair for various international conferences.
Valentina Ciriani	Valentina Ciriani is an assistant professo at UMIL. She received the Ph.D. in computer science form University of Pisa, Italy. She is currently an assistant professor at the Information Technology Department of University of Milan, Italy. Her research interests include algorithms, data structures and information security, as well as logic synthesis and testing.

2.3 Consortium as a Whole

The consortium consists of a combination of research and industry partners with extensive background in the topics related to CAPA objectives:

- **Trialog** is a SME. It has extensive co-ordination experience. It also has extensive experience in the development and integration of embedded system platforms and on testing for automotive systems and home connectivity systems. It also markets embedded software technology (automotive RTOS, home network protocol).
- **Groupement des Cartes Bancaires (CB)** is operating France's main bank card payment scheme. It is actively involved in the creation of an unified European market of payment instruments.
- **Oracle** is the world's largest enterprise software company. Its business is information — how to manage it, use it, share it, protect it. from Berkeley DB, an open source technology available from Oracle will be a starting point to CAPA.
- **Telefónica Investigación y Desarrollo (TID)** is the innovation company of the Telefónica Group. TID has a wide experience in Identity Management and security projects, both at international and national level. TID is also involved in many multimedia interaction projects.
- **Visual Tools (VTools)** is a SME. It has a leading position in the video security market. It has extensive experience in the development of advanced hardware and software platforms for digital video storage and transmission.
- **Humboldt-Universität zu Berlin (UBER)** is one of the leading universities in Germany. The DBIS (DataBase and Information System) group has an extensive track record for participating in various research and transfer technology projects related to data management.
- **KU Leuven (KUL)** is one of the leading universities in Belgium. The COSIC research group has an extensive track record in research on computer security and (industrial) cryptography (hence the name). The ICRI research group carry out research in several fields of Law & ICT and Legal Informatics including on privacy and identity management.
- **TU Dresden (TUD)** and is among Germany's oldest and most renowned universities of technology. is one of the leading universities in Belgium. TUD's operating systems group has extensive experience in operating-system construction, especially micro-kernel based real-time and security architectures. Its secure OS and secure file system technologies will be a starting point to CAPA
- **The university of Milan (UMIL)** is one of the leading universities in Italy. The Information Technology Department, conducts theoretical and experimental research in most areas of computer science and technology, including: data protection; access control models, policies, and languages and security and privacy in general; with research results published in international conferences and journals.

The table below summarises the role and contribution of each partner

Participant			**Role**	**Main Contribution Area in CAPA**
Trialog	1	F	Industry: Embedded systems	• Project management • Trusted storage platform support for empowerment • Vehicle location tracking avoidance application • Multimedia interaction application
Groupement des Cartes Bancaires (CB)	2	F	Industry: Banking credit card	• Payment application validation
Oracle	3	B	Industry: Database	• Secure database design
Telefónica Investigación y Desarrollo Sociedad Anónima Unipersonal (TID)	4	E	Industry: Telecom	• Pervasive computing use cases with a focus on payment applications and on multimedia interactions
Visual Tools (VTools)	5	E	Industry: Video security systems	• Video surveillance application
Humboldt University (UBER)	6	D	Research: Database	• Secure database design and implementation • Research on challenges for privacy with focus on linkage attacks and privacy of access
KU Leuven (KUL)	7	B	Research: Security, Law & ICT and legal informatics	• Architecture of trusted storage platfor • Research on challenges for privacy with focus on privacy of access • Study of legal aspects focusing on data protection
TU Dresden (TUD)	8	D	Research: Operating systems	• Secure OS and secure file system building blocks in trusted storage platform
U. Milano (UMIL)	9	I	Research: Database	• Policy management building block in trusted storage platform • Research on challenges for privacy with focus on policies

Industry Partners Involvement to Ensure Exploitation

Trialog

Trialog exploitation analysis is that security and in particular data protection and privacy will be key products features in the future. Its current activities portfolio include the following:

- embedded systems technology products. Since the early nineties, Trialog has marketed RTOS and protocol products for embedded systems, including the OSEK-VDX automotive RTOS and the EHS European Home Systems protocol which have been deployed in mass market products.
- supporting engineering tools in particular test tools. Trialog has developed a test tool to support development and testing of embedded systems components (e.g. software components, protocols). The tool is based on the TTCN standard (ISO9646)
- platform integration activities for home connectivity and telematics, involving e.g. Java and OSGi technology, as well as security subsystems. Such platforms need to be trusted storage systems

In terms of exploitation Trialog intends to leverage on the experience gained in the described activities and combine them with the results of CAPA:

- in order to act as trusted storage platform provider for the following activities: adaptation/extension of the trusted storage platform (e.g. new peripherals, new building blocks), and support to business stakeholders to integrate new features and develop components of privacy aware applications
- in order to provide test capability that will allow for the validation, certification and verification of such platforms

Groupement des Cartes Bancaires (CB)

CB is at the forefront of technology initiatives that will lead to the advent of an unified European market of payment instruments. The result of CAPA will allow CB to gain the necessary insight and prepare for further actions at the R&D, standardisation, and legal level in Europe that will lead to the advent of privacy enabled payment schemes. It is planned to create some liaison with the SEPA (Single Euro Payments Area) initiative in Europe as well as with the EPAS (Card Payment related protocols) ITEA project which CB is leading.

Oracle

Oracle plans to disseminate and exploit the results of the CAPA project both internally and externally to the company.

The CAPA project will be based on a family of open source embeddable databases, the Berkeley DB, that allows developers to incorporate within their applications a fast, scalable, transactional database engine with industrial grade reliability and availability. This technology was originally developed outside of Europe.

Internally to the company, the CAPA development will allow building a solid competence in Europe in the area of security-related features on top of the already existing competence on embedded databases and in particular Berkeley DB.

External to the company, Oracle intends to disseminate and exploit the results of the CAPA project with a number of potential customers interested in embedding database capabilities to "small footprint" devices. Generally, the always increasing computational capacity of PDAs and smart-phones represents, at this very moment, an opportunity to embed data management and intelligence capabilities in such devices. Therefore Oracle sees a real market opportunity for embedded database at the moment.

In particular, vehicle telematics and mobile communications and entertainment appears to be among the most promising applications areas where these technologies may see massive take up in the future. This, evidently, relates with the choices in terms of use cases that have been made in the project and with the related participation of Oracle to such use cases.

TID

TID proposes an activity **dissemination** plan divided in two different scope levels:

National scope

TID, as a common company for national character innovation projects, will try to incorporate those CAPA developed technologies or proposals into the projects within the same area of application in which it participates. Doing so, other national companies, outside of CAPA Consortium, will know about the results of the Project, thus obtaining geometric dissemination for them.

International scope

Likewise, TID will try to make these dissemination efforts extendable to an international scope by applying the results of CAPA project to the international consortia where it has a membership.

The main objective would be to provide the basis for the arising of new innovation projects involving the integration of CAPA results, as a part or for the main purpose.

In addition, TID would carry out an **exploitation** plan for the CAPA results within the Telefónica Group itself. As a R&D company, TID will promote the commercial use of the CAPA developed technologies among the Telefónica Group business units in three different ways:

- Showing the technological results of the project. So, the companies of the Group which are able to create commercial services will know the possibilities that CAPA technologies offer, in order to take them in account in their decision processes.
- Incorporating, as far as possible, the CAPA technologies to the TID projects.
- Transferring the specific results of CAPA to the specialized company departments which could give a more focused use to solutions provided by the CAPA project.

Visual Tools

Visual Tools will carry out dissemination and exploitation activities of CAPA as follows.

Dissemination will be instrumented in two ways. On the one hand, dissemination will take place by presenting project results and technology to company customers in a language that they can understand. To this end, the company will put together material explaining potential customers the added benefits of installing a privacy preserving surveillance system as opposed to a conventional system.

On the other hand, the project results will have influence in the national legislation in security projects through the participation of Visual Tools in eSEC, the Spanish security platform sponsored by AETIC (see http://www.aetic.es/eSEC/). The eSEC platform has put together a "Strategic Research Agenda" that is being used by the Spanish authorities to decide on funding and investment of security technology in the next few years.

Regarding exploitation, the company has acknowledge the growing concern of persons and institutions by the privacy breach related to the ubiquitous installation of video surveillance systems. In a country as permissive with video surveillance as the USA, some influential institutions as the Constitution Project (http://www.constitutionproject.org/) an independent think tank in Washington D.C., have put together *"Guidelines for Public video Surveillance and Model Legislation"* (see http://www.constitutionproject.org/pdf/Video_surveillance_guidelines.pdf) that will have a definite impact in public authorities and institutions when deciding to install video surveillance systems.

Addressing this concern, Visual Tools expects that the technology developed in CAPA to protect privacy can be a competitive advantage for the company video surveillance products when the society debate increases the demand for privacy preserving video surveillance systems. The availability of this product in certain countries specially aware with privacy protection issues (e.g. Scandinavian countries, Germany,…) will be a starting point to address sales in those countries.

Sub-contracting

The following sub-contracting work has been identified:

- Leadership in the architecture for privacy of actors and insight on challenges for privacy (WP4, WP5). CAPA focus on privacy of actors was shaped up by Dennis Shasha (New York University) who is currently on sabbatical leaver in France. If CAPA is accepted, it will be important to keep this leadership even when Dennis has returned to the US. Dennis Shasha will be a consultant to Trialog (see his profile in the section presenting Trialog)
- Insight on ethical aspects and privacy (WP7). During the preparation of the proposal it became clear that it is not only important to understand the legal impact of privacy, but also to get an insight on ethical implications. It is believed that a number of discussions should be carried out with expert in the area. Annabelle Lever is a renowned researcher in the area. She will be a consultant to Trialog (see her profile in the section presenting Trialog)
- Leadership in requirements and use case work in the specification of privacy preserving surveillance use case (WP2, WP4). These work will be led by VTools who would like to get the consulting help of José-Luis Fernández who has significant experience in the area (see his profile in the setion presenting VTools)

2.4 Resources to be committed

Resources Mobilisation w.r.t CAPA Workplan

CAPA will mobilise 406 mm from the partners as well as 9 mm from consulting, subdivided as follows:

- 12 mm to consortium management
- 54 mm for WP2 on requirements, plus 4 mm from consulting (José-Luis Fernández)
- 55 mm for WP3 on the trusted storage platform architecture and design
- 84 mm for WP4 on the use case towards "una capa invisible", plus 1 mm from consulting on the architecture (Dennis Shasha) and 2 mm from consulting on the privacy preserving use case (José-Luis Fernández)
- 56 mm for WP5 on the research challenges for privacy, plus 1 mm from consulting on linkage attacks (Dennis Shasha)
- 108 mm for WP6 on the trusted storage platform reference implementation
- 46 mm for WP7 on the link to the industry and reach out, plus 1 mm from consulting on the impact of ethic aspects (Annabelle Lever)

Note that at the individual participant level, resources involvement is fairly balanced (except for CB which has a validation role only). TUD has more effort because it is anticipated that important OS and file system development and integration support effort will have to be provided.

Resources Mobilisation w.r.t. CAPA Objectives

The below table shows an estimate of resources that are assigned per objective. We have integrated WP1 (consortium management) and WP2 (Link to the industry and reach out) resources according to a pro-rata calculation, and have rounded figures. Some comments :

- Trusted Storage Platform is the objective which takes the most important part of resources (240 mm). Within the TSP, the secure OS and secure file system take a significant part (50%). We have included in O1 resources for both architecture and design. Note (1) that it is planned to reuse existing open source building blocks, from TUD (OS and file system) and from Oracle (database), and (2) that significant resource is dedicated to providing support to use cases.
- Architecture for privacy of actors takes one half. All use cases re-use existing applications. This is the reason no too many resources are allocated to them. For market reasons and partner preference reasons, more resources has been allocated to privacy enabled payment and privacy-preserving surveillance.
- Research challenges take one-fourth, with approximately balanced involvement in each of the challenge topic.

Type of objective	Objective	Description	mm	mm
Trusted Storage Platform	O1	*Architecture for trusted storage platform*	240	120
	O2	*Secure operating system and file system*		60
	O3	*Secure database*		20
	O4	*Policy management support*		20
	O5	*Trust and empowerment support*		20
Architecture for Privacy of Actors	O6	*Architecture for privacy of actors involving a privacy aware personalised device*	120	40
	O7	*Privacy enabling payment use case*		25
	O8	*Privacy enabling multimedia interaction use case*		20
	O9	*Vehicle tracking avoidance use case*		15
	O10	*Privacy preserving surveillance use case*		20
Challenges for Privacy	O11	*Linkage attacks roadmap* *Advance in collusion attacks*	60	25
	O12	*Privacy of access roadmap* *Advance in privacy protection to users accessing information in a database*		20
	O13	*Policy issues roadmap* *Advances in policy management to regulate access and use of data*		15

Subcontracting Cost

Subcontracting estimate cost are the following:

- 24 000 Euro for Dennis Shasha (around 2 mm)
- 10 000 Euro for Annabelle Lever (around 1 mm)
- 60 000 Euro for José-Luis Fernández (6 mm)

Other Major Items of Cost

The following other major items of costs are identified:

- Around 20000 Euro per partner for travel cost (except for CB – around 5000 and KUL/ICRI – around 15000)
- Between 20000 Euro to 30000 Euro of equipment costs for each of the 4 use cases.
- Between 1000 to 5000 Euro for audit cost
- At the consortium management level, around 27000 Euro for a workspace, a website and various dissemination material

Section 3: Impact

3.1 Expected impacts listed in the work programme

Direct Impact

This section assesses the direct impact of CAPA with respect to objective ICT-2007.1.4 : Secure, dependable and trusted Infrastructures. We first compare the objective target outcome topics with CAPA focus topics. We then assess CAPA impact with respect to the work programme expected impact.

CAPA versus ICT-2007.1.4 target outcome	
Security and resilience in network infrastructures: building and preserving flexible, scalable and context-aware, secure and resilient architectures and technologies to enable dynamic management policies that ensure end-to-end secure transmission of data and services across heterogeneous infrastructures and networks, including dynamic networks of tiny insecure devices, and multiple provider, business and residential domains; real time detection and recovery capabilities against intrusions, malfunctions and failures;	Not in the scope of CAPA
Security and trust in dynamic and reconfigurable service architectures supporting assured and scale-free composition of services and service coalitions with managed operation across several administrative or business domains, enabling flexible business models;	Not in the scope of CAPA
Trusted computing infrastructures ensuring interoperability and end-to-end security of data and services; increased security and dependability in the engineering of software and service systems to ensure the design and development of trustworthy applications and services;	Main objective of CAPA: • Trusted storage Platforms (WP2,WP3,WP6) • Architecture for the privacy of actors (WP4)
Identity management and privacy enhancing tools with configurable, context-dependent and user-controlled attributes in static and dynamically changing environments;; **trust policies** for managing and assessing the risks associated to identity and private data.	Addressed in CAPA: • Policy building block for data protection in trusted storage Platforms (WP2,WP3,WP6) • Research on policies for data protection (WP5)
Longer term visions and **research roadmaps**; **metrics and benchmarks** for comparative evaluation and open technology competitions, in support of certification and **standardisation**; **international cooperation** and co-ordination with developed countries; **coordination of FP7 projects** addressing security, dependability, privacy and related ethical issues across different challenges and objectives of this work programme.	Addressed in CAPA • Roadmap on research challenges for privacy (WP5) • Liaison with eSafety and eInclusion projects, liaison with identity management projects (WP7), liaison with truted computing projects (WP3, WP6)

CAPA versus ICT-2007.1.4 Expected Impact	
ICT users empowered to handle their digital identity and personal data and to protect their privacy, turning the European view on privacy into an economic advantage; strengthened trust in the use of networks, software and services for governments, businesses and consumers.	The entire project set up is user centred so that users can handle their digital identity and personal data – through the concept of personalised device (specified in WP4), and through trusted storage building blocks (secure file systems, secure database, policy management, support for empowerment)
A strong and competitive ICT security industry in Europe	The trusted storage platform technology and the architecture for privacy of actors will be key enablers for the advent of privacy aware applications. This will contribute to a leading ICT security industry.
Substantially improved security and dependability of networks and service infrastructures having a complexity and scale that are an order of magnitude greater than those of today's infrastructures	CAPA takes the viewpoint that by default (1) identities are not revealed and (2) personal data are protected will precisely allow for larger scale and more complex services than today. We believe that ensuring data protection through policies rather than technologies will lead to exponentially growing risks of accidental or malicious data protection infringement.
Wider use of metrics, standards, evaluation and certification methods and best practices in security of networks, infrastructures, software and services	CAPA trusted storage platform will be an open source platform and consequently widely available CAPA will work on the assessment of metrics and the assessment of CAPA impact on data protection

Indirect Impact

It is also useful to show how CAPA contributes to the overall expected impact as described in the first sections of the work programme.

Overall Objective Improving the competitiveness of European industry and enabling Europe to master and shape future developments in ICT so that the demands of its society and economy are met. ICT is at the very core of the knowledge-based society. Activities will strengthen Europe's scientific and technology base and ensure its global leadership in ICT, help drive and stimulate product, service and process innovation and creativity through ICT use and ensure that ICT progress is rapidly transformed into benefits for Europe's citizens, businesses, industry and governments. These activities will also help reduce the digital divide and social exclusion	CAPA will create an understanding on technologies for "una capa invisible" and therefore strengthen Europe leadership in the area. CAPA focus on several application use case will help for rapid transformatoin. One of the use cases on multimedia interaction will focus on e-inclusion applications and therefore contribute to reducing social exclusion
I2010 Lisbon Initiatives We must realise higher economic growth through improved competitiveness and productivity, whilst ensuring a sustainable future. We have to adjust to the changing economic realities brought about by the globalisation of markets and the ever faster pace of technological change. At the same time, we have to modernise our public services and tackle emerging challenges in areas such as health, ageing, inclusion, energy efficiency, safety and security Information and Communication technologies provide the backbone for the knowledge economy. They account for around half of the productivity growth in modern economies "world class performance in research and innovation in ICT by closing the gap with Europe's leading competitors". Leading the progress in ICT is essential to be able to address Europe's key socio-economic challenges and to reinforce its industrial competitiveness. ICT research in FP7 aims at enabling Europe to master ICT development so that it corresponds to the needs of its citizens and businesses.	Use cases in CAPA will involve eSafety applications and eInclusion applications CAPA will contribute to a trusted ICT backbone for the knowledge economy CAPA include word class research and innovation partners.

CAPA versus ICT Seven Challenges	
The converged communication and service Infrastructure that will gradually replace the current Internet, mobile, fixed and audiovisual networks.	CAPA technology will be a key component of this infrastructure (whenever there is an embedded device with data collecting capability)
The engineering of more robust, context-aware and easy-to-use ICT systems that self improve and self-adapt within their respective environments.	Trusted storage platforms will contribute to a more robust infrastructure.
The increasingly smaller, cheaper, more reliable and low consumption electronic components and systems that constitute the basis for innovation in all major products and service.	CAPA architecture for privacy of actors involve the use of an increasingly smaller and cheaper personalised device (one of the form factor could be an USB device)
Digital libraries, knowledge and content development tools and applications that will help us preserve, develop and disseminate our cultural assets, improve our learning and education systems and strengthen the creativity of our society	
ICT tools for sustainable Health systems enhancing our ability to monitor our health and well-being and to treat major illnesses and diseases.	CAPA technologies could be useful to collect health data in a protected way
Intelligent and safe vehicles and technologies for environmental sustainability and energy efficiency that are key requirements of our citizens	One of the use cases in CAPA is data protection of V2V/V2I infrastructures (i.e. one of the main infrastructure contributing to eSafety applications)
ICT systems and applications for better inclusion and independent living of all citizens.	One of the use case is data protection in multimedia interactions. It is planned to focus on e-inclusion applications
In addition to the seven Challenges, a Future and Emerging Technologies activity will continue to foster trans-disciplinary research excellence in emerging ICT-related research domains.	
The Challenges in this Work Programme build on and extend the Ambient Intelligence vision developed in the previous Framework Programmes	The CAPA trusted storage platform could be a key technology for ambient intelligence

SMEs Particular attention is paid to SMEs' needs and potential in the definition of the priorities of the ICT Work Programme. Building on the experience of SMEs' participation in ICT research under FP6, the aim is to ensure that SMEs constitute an important part of the ICT research consortia together with large companies, universities, and public research labs.	CAPA involves two leading European SMEs, Trialog and Visual tools

The socio-economic dimensions of ICT The economic and social transformations triggered by ICT are wide-ranging, complex, and multifaceted. We are no longer at the dawn of the Information Society but witnessing and experiencing its deployment at all levels of economic activity and social interaction. In addition, technological roadmaps are pointing to even more radical socio-economic changes. Most R&D projects have a clear socio-economic dimension from the outset. This may include, for example, evidence-based impact assessment and pro-active initiatives in order to accelerate diffusion and societal acceptance. The programme will also support social and economic research, launched through calls for tenders, to create a better understanding of trends and impacts at the level of society and of the economy, including the global economy. This will complement assessments of the impact of individual projects, help assess the impact of the ICT programme as a whole, and support impact assessments of specific policy options. In addition, wider benefits are expected to arise from the research projects and actions supported under this programme in terms of their contribution towards science education, and outreach and communication activities. The pursuit of scientific knowledge and its technical application	CAPA involves significant work to assess legal and ethical impact (WP7) A significant number of woman will be involved in CAPA activities (see staff profiles).

towards society requires the talent, perspectives and insight that can only be assured by increasing diversity in the research workforce. Therefore, a balanced representation of women and men at all levels in research projects is encouraged.	

European Technology Platforms in ICT and the Work programme European technology Platforms (ETPs) bring together the main industry and academic research stakeholders in a particular field with the aim of better coordinating their research and related activities and achieving common goals. An important outcome of each ETP is a Strategic Research Agenda agreed by its members that also commit to its implementation. These Strategic Research agendas11 constitute an important input to the Work Programmes in FP7. The industrial and academic research stakeholders in ICT have at the time of publication set up European Technology Platforms in nine ICT fields. These cover the fields of nanoelectronics, photonics, micro-systems, embedded systems, software and services, mobile communications, networked media, satellite communications and robotics	CAPA work will have an influence on embedded systems, and network media

Co-ordination of non-Community research programmes The actions undertaken in this field in FP7 include the coordination of national or regional research programmes or initiatives (see Appendix 3) and the participation of the Community in jointly implemented national research programmes (Treaty Article 169). The actions will also be used to enhance the complementarity and synergy between the Framework Programme and activities carried out in the framework of intergovernmental structures such as EUREKA, EIRO forum and COST. The coordination of national or regional research programmes or initiatives are called for within several objectives in this Work Programme. In addition, the participation of the Community in national research programmes jointly implemented on the basis of Article 169 is planned in the area of ICT for Ambient Assisted Living. This will be the subject of a separate decision. Objectives under Challenges 1, 2, 3, 5, 6 and 7 as well as FET call for the coordination of national or regional research programmes or initiatives. There is in addition a horizontal action concerning International cooperation.	Liaison with existing non-community research programmes is planned.

Need for an European Approach

CAPA is contributing to the advent of privacy aware pervasive computing applications. Most of such applications assume the use of an global infrastructure allowing for an international and european market. For instance the use cases addressed in WP4 are the following :

- the privacy enabled payment use case assumes an European market
- the vehicle location avoidance use case assumes an European V2V/V2I infrastructure for future safety applications
- the multimedia interaction use case assumes an international infrastructure

Most applications require capability that can only be achieved through European level R&D and standardisation initiatives. They assume identity management schemes and protocols that are agreed at the European level and standardised. The also assume data protection features and policies that are agreed a an European level.

Furthermore, CAPA deals with a transversal issue (data protection) and therefore needs to liase with European projects dealing with the advent of an European pervasive computing infrastructure

The importance of PETs (Privacy Enhancing Technologies) was recently acknowledged by the European Commission in a press release issued May 2nd, 2007 (see section 5).

The consortium includes 9 partners from 4 European countries.

National or International Initiatives

We list here a number of projects and initiatives/activities where liaison will take place. Liaison with other activiers are also expected as needed.

Name	Type of Initiative	Description	Type of liaison
Article 29 WG	European institution initiative	European legislation group focussing on issues related to data protection	Liaison through Trialog. Trialog is involved in discussion with Article 29WG on vehicle location tracking avoidance The type of liaison is at the use case level. Separate discussion could take place for each of the four WP4 use cases
SEPA	European institution initiative	Initiative led by the European Central Bank to create a payment area based on the euro	Liaison through CB
TCG	Industry consortium	Initiative to agree on standards for hardware-enabled trusted computing and security technologies	Liaison through TUD and KUL
HGI	Industry consortium	Initiative to agree on standards for future consumer gateways	Liaison through TID who is a board member of HGI
C2C	Industry Consortium	Initiative to agree on V2V/V2I standards for safety applications	Liaison through eSafety projects, especially with the C2C security working group
eSafety forum	Industry Consortium	Initiative to coordinate actions towards V2V/V2I safety applications	Liaison through the eSecurity WG which focuses on the identification of future challenges related to data protection and vehicle intrusion
NEM	Technology platform	Network and media technology platform	Liaison through participants involved in NEM (TID is executive board member)
Artemis	Technology platform	Embedded systems technology platform	Liaison through participants involved in ARTEMIS
Sevecom	Collaborative project	Security solution for vehicular communication including an identity management building block	Reuse of Sevecom solution and integration of CAPA data protection capabilities (see below for more details)
Prime	Collaborative project	Identity management schemes	Liaison through common partners (KUL, UMIL, TUD). Specific liaison (see below for more details)
FIDIS	Collaborative project	Network of excellence on Identity management	Liaison through common partners (KUL, TUD).
OpenTC	Collaborative project	Development of trusted and secure computing systems based on open source software	OpenTC will be a starting point to CAPA. Liaison through common partners (KUL, TUD). See below for more details.
Robin	Collaborative project	PASR project. Development of open source OS hypervisor	Robin will be a starting point to CAPA. TUD is the coordinator of Robin. See below for more details.
CVIS	Collaborative project	Cooperative Vehicle Infrastructure systems.	Reuse of CVIS reference implementation and integration of CAPA data protection capabilities
MonAMI	Collaborative project	e-inclusion IP focusing on the creation of services derived from mainstream technologies	Reuse of a MonAMI application in CAPA use case on multimedia interactions (TID and Trialog are partners of MonAMI).
EPAS	Collaborative project	ITEA project on card payment protocols	Liaison through CB

Liaison with Identity Management Projects

Because CAPA focuses on data protection rather than identity management, and because CAPA architecture for privacy of actors necessitates suitable identity management building blocks, liaison must take place with other projects so that existing identity management blocks can be reused.

Name	Description	Type of liaison
Sevecom	The mission of Sevecom is to define a future-proof solution for secure vehicular communication. It will define a baseline solution that takes into account privacy and data protection, authentication and confidentiality. http://www.sevecom.org	CAPA will reuse Sevecom identity management scheme for privacy and integrate privacy aware capability to V2V and V2I communication devices Trialog, KUL are partners of CAPA and Sevecom (Trialog is coordinating Sevecom)
Prime	PRIME aims to develop a working prototype of a privacy-enhancing Identity Management System. Approach is through the use of a trustworthy middleware. https://www.prime-project.eu	CAPA could reuse Prime identity management system and integrating it in one use case. Note that CAPA architecture for privacy put identifier manager in the hands of individuals rather than positing a trustworthy middleware Note that Primelife, a follow-up proposal of Prime has been submitted. An agreement to liaise with PrimeLife has already been made prior to submission (Contact point is Jan Camenisch from IBM Zurich). KUL, UMIL, TID are partners of CAPA and PrimeLife.

Liaison with Trusted Computing Projects

CAPA trusted storage platform will rely on existing building blocks for trusted computing platforms, so liaison must take place with other projects so that existing blocks can be reused.

Name	Description	Type of liaison
OpenTC	The Open Trusted Computing (OpenTC) consortium is an R&D project focusing on the development of trusted and secure computing systems based on open source software open Trusted Computing framework. The architecture is based on security mechanisms provided by low level operating system layers with isolation properties and interfaces to Trusted Computing hardware. These layers makes it possible to leverage enhanced trust and security properties of the platform for standard operating systems, middleware, and applications. http://www.opentc.net/	Robin and OpenTC are the two starting points to CAPA. Robin will complete in early 2008. TUD is the coordinator of Robin. TUD and KUL are partners of OpenTC
Robin	The objective of this Preparatory Action is to explore key technologies for a small, robust platform that can host legacy operating systems and their applications, but that is small enough to undergo formal analysis and construction techniques. The platform consists of a secure microhypervisor complemented with trusted servers that, together, allow running legacy operating systems next to security-sensitive applications. This platform will be provided in open source. http://robin.tudos.org/	

3.2 Dissemination and/or exploitation of project results, and management of intellectual property

Dissemination and Liaison

Dissemination and liaison is paramount for the success of the CAPA undertaking. This involves activities at the industry and academic level:

- Institution level. It is important to ensure liaison at the institution level. This will be carried out through WP7. The stakeholders are the national regulation parties (data protection agencies), and the participant of legislation working groups. CAPA clearly intends to be a leading contributor to the discussions which will be initiated by the commission (see press release – section 5)
- Industry level. Dissemination is important at different levels;
  - Liaison with most industry initiatives for technologies contributing to pervasive computing might be of interest (we have listed some of them above). The benefit of the trusted storage platform and/or of the architecture for privacy of actors will have to be promoted.
  - Specific liaison with the industry targeted by CAPA use cases in WP4 has to take place. This will be carried out by the partners involved in the use case

  It is intended to interact through (1) specific adhoc meetings – suitable when in liaison with a project, (2) specific working group meeting, (3) papers and presentation in conferences and coordination meetings.
- Research level. It is expected that a number of significant results will be produced in the course of the project. Academic partners (TUD, UMIL, KUL, UBER) will disseminate results of the CAPA project by targeting the most relevant conferences of its domain

Exploitation of Project Results and Management of Intellectual Property

We have identified the following exploitation items:

- Trusted platform technology. It is intended to make available the technology using open source distribution. This will be made easier by the fact that the underlying OS, file system, database are already available under open source form. One of the industry constraint is that the resulting technology is close to mainstream technologies. This is the case of the starting points technology (e.g. linux oriented).
- Architecture for privacy of actors. The architecture for privacy of actors will be first a specification describing several aspects (e.g. protocol). This specification will be public.
- Individual privacy aware applications.
  - Privacy enabled payment application will rely on open protocols and specifications
  - Vehicle location tracking avoidance application will also rely on open protocols (specified in the Sevecom and CVIS projects. For instance the car-to-car CALM protocol – and ISO standard)
  - Multimedia interaction will rely on open protocols and specifications (likely complying with HGI)
  - Privacy preserving video surveillance system will rely on open protocols and specifications

Section 4: Ethical Issues

While none of CAPA activities raise ethical issues, we would like to point out that CAPA will provide technologies that may help the Society to better cope with existing issues of today, when those issues are related to unauthorised access to private data.

ETHICAL ISSUES TABLE

	YES	PAGE
Informed Consent		
• Does the proposal involve children?		
• Does the proposal involve patients or persons not able to give consent?		
• Does the proposal involve adult healthy volunteers?		
• Does the proposal involve Human Genetic Material?		
• Does the proposal involve Human biological samples?		
• Does the proposal involve Human data collection?		
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?		
• Does the proposal involve Human Foetal Tissue / Cells?		
• Does the proposal involve Human Embryonic Stem Cells?		
Privacy		
• Does the proposal involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)		
• Does the proposal involve tracking the location or observation of people?		
Research on Animals		
• Does the proposal involve research on animals?		
• Are those animals transgenic small laboratory animals?		
• Are those animals transgenic farm animals?		
• Are those animals cloned farm animals?		
• Are those animals non-human primates?		
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)		
• Benefit to local community (capacity building i.e. access to healthcare, education etc)		
Dual Use		
• Research having direct military application		
• Research having the potential for terrorist abuse		
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?		
I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL	**YES**	

Section 5: Annex Press Release

The European Commission issued the following press release on May 2nd, 2007. This press release is particular relevant to CAPA.

Promoting Data Protection by Privacy Enhancing Technologies (PETs)

The Commission adopts today a Communication with the purpose of identifying the benefits of Privacy Enhancing Technologies (PETs) and laying down the Commission's objectives in this field, to be achieved by a number of specific actions supporting the development of PETs and their use by data controllers and consumers.

The development of information and communication technologies is constantly offering new services which improve people's life. However, alongside these benefits, new risks also arise for the individual, such as identity theft, discriminatory profiling, continuous surveillance or deceit.

Vice-President Frattini, Commissioner responsible for Justice, Freedom and Security, highlighted that*: "To ensure that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions under the existing legal provisions, but also technically more difficult, the Commission puts forward a set of actions aiming at developing and promoting the use of Privacy Enhancing Technologies."*

Viviane Reding, Commissioner for Information Society and Media added *"On line services provide a lot of benefits and convenience to citizens and huge competitive advantages to European businesses. Yet for such services to enjoy large scale growth and so boost Europe's economy, people must have sufficient confidence that their personal privacy and legitimate business interests are being properly safeguarded".*

The use PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and /or helping to detect them, therefore having a positive impact on consumer trust, in particular in cyberspace, all without losing the functionality of the information system.

The Commission Communication adopted today reflects on the benefits of PETs, lays down the Commission's objective to promote these technologies and sets out clear actions to achieve them in the future by supporting the development of PETs and their use by data controllers and by consumers.

To pursue the objective of enhancing the level of privacy and data protection in the Community, the Commission intends to clearly identify the need and technological requirements of PETs and further promote the development of these technologies (in particular through RTD projects and large-scale pilot demonstrations) and their use by industry and public authorities, involving a vast array of actors, including its own services, national authorities, industry and consumers. The aim is to provide the foundation for user-empowering privacy protection services reconciling legal and technical differences across Europe through public-private partnerships.

To ensure respect for appropriate standards in the protection of personal data through PETs, standardization and coordination of national technical rules on security measures for data processing are envisaged.

Furthermore, the Commission will conduct actions to raise consumers' awareness and investigate the feasibility of an EU-wide system of privacy seals. The objective of such privacy seals would be to allow consumers to easily recognize a certain product as ensuring or enhancing the respect of the data protection rules, in particular by incorporating the appropriate PETs.