fairCASH based on Loss resistant Teleportation

D I S S E R T A T I O N

Am Institut für Informatik der Technischen Fakultät der
Christian-Albrechts-Universität zu Kiel zur Erlangung des akademischen
Grades eines Doktor-Ingenieurs (Dr.-Ing.)
vorgelegte und genehmigte Dissertation

Heinz Kreft

Kiel, im Frühjahr 2010

1.ster Gutachter:	Prof. Dr. rer. nat. Manfred Schimmler [CAU]
2.ter Gutachter:	Prof. Dr. Achim Walter [CAU]
Einreichung:	17. Mai 2010
Tag der mündlichen Prüfung:	28. Oktober 2010

Technische Informatik

Heinz Kreft

fairCASH based on Loss resistant Teleportation

Shaker Verlag
Aachen 2011

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Zugl.: Kiel, Univ., Diss., 2010

Printed in Germany.

ISBN 978-3-8440-0035-1
ISSN 1436-882X

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • e-mail: info@shaker.de

1 About this work (with Keywords)

It is noteworthy that management of ePayment operations has become mission critical. Evolved from a tactical process in the past to a function required to optimize business results today, the adapters embark on and the approaches used have direct impact on business profitability and ability to scale. For plenty reasons business cases are being transferred from the physical world to the Internet. Today we summarize these digital life style developments into a sector of mobile commerce (mCommerce). ePayment is the lubricant for this. Nevertheless, it is not easy and can be risky. Being among the first in this field is not a guarantee for success. Early adopters like Deutsche Bank and inventors like David Chaum learned this on the hard way. Today we see promising visions like the Mobile-Money-Cooperation-Initiative[1] of the GSMA[2]. Unfortunately, their money transferring technology is account-based. This has serious implications for the relationship to the network, the services, the security and to the privacy. A match with the social and security interests of users and business cases in terms of complexity is difficult to find within a central approach. We can see that the motivation to attack these systems is increasing because the rewards for doing so are increasing, too [1]. Concentrating the value to only a few central databases is going to reach a dangerous critical mass. It is more and more proven being the wrong strategy to encounter today's security threats shown by incidents like stolen customer account records of credit cards and others. In an ongoing battle waged between the persons in charge for the security of the business process (slowly learning their lessons from previous mistakes) and the hacker community (constantly trying to break implemented protections) the time to change has come.

This work presents a way out. Better than just claiming (high) security for products and services, is to guarantee this by taking responsibility for getting security done by better investments in physical protection means and less in conciliation, particularly in case of compromitation. We show how to present and recreate the already proven good monetary cash exchange system on the Internet. This thesis' contribution introduces the ecosystem focusing on Digital Cash [2-8] including already known attempts. Due to recent concerns in computer crime having caused physical security to get a new meaning, various assumptions and objectives for a working system architecture are presented, spanning from defense technology methods used to safeguard information against physical attacks to new approaches in transferring value data. Discussing environmental protection, like access policies in combination with physical and logical security, will give the reader a complementary concept of the inner values, which can help him to evaluate ePayment systems, distinguish fact from fiction, and make up his own mind.

We will present answers by identifying two essential parts of a technological framework about how to store and to transfer digital values between participating parties. The basic principle consists of technical mechanisms and resources needed to conduct a safe environment, able to deter, reject, prevent or to react to attacks intended to steal or modify protected assets like eCoins stored in an eWallet. Furthermore we show a solution to move (without copying) secrets from one point to another, able to compensate the eWallet owner in case of any loss by the propagation process. This includes generic value transfer operations of digital data like payment tokens between two parties introducing the new "loss resistant teleportation protocol."

Identified as electronic coins (eCoins) in payment scenarios and financial environments, the possibilities of such transfers are much broader. Replacing these tokens by classified objects like keys or other crypto-artifacts, wide fields of applications are coming up into one's mind where such a protocol can offer advantages over solutions available today.

Keywords and Phrases: fairCASH, Digital Cash, eMoney, electronic Cash, eCash, Cash, Bargeld 2.0, eGeld, mobile Money, mMoney, electronic Money, eMoney, ePayment, mPayment, Token, eToken, eCoin, eDoc, electronic Currency, eCurrency, eCommerce, mCommerce, Mobile Banking, eGovernment, Open-loop, Multi-hop, Pre-paid, Micro-, meso- and macro-payment, electronic Mint, eMint, electronic Wallet, eWallet, Teleportation, offline Transfer, Anonymity, P2P, G2G, G2B, G2C, B2C, B2B, C2C, tamper-resistant, tamper Protection, **H**ardware **S**ecurity **M**odule (HSM), **S**ecure **E**lement (SE), Maze of Knossos, PUF, CASTOR, TRUSTLET, trusted Boot, VPN, VPC, fCCP, issuing Authority, RCA, CA, PKI, Certificate, CRL, un-deniable protocol, being repudiation free, fault tolerance, auto-resolve dispute cases, Transferability, Offline-Value-Transfer, delayed-true two-party fair exchange, Atomistic, transactional-rollback, Unification, Multi-spending, Secrets, Affidavit, Reimbursement, fairness Recreation.

[1] http://www.mobilemoneysummit.com/
[2] http://gsmworld.com/our-work/mobile_lifestyle/mobile_money/index.htm

1.1 Zusammenfassung (deutsch)

Digitale Bargeld-Systeme kombinieren Erkenntnisse aus Kryptografie und eCommerce. Unter solchen Systemen werden finanzielle Rotations-Systeme mit anonym zirkulierenden, serialisierten und authentisierten Bitmuster-Entitäten zur Wertaufbewahrungs- und Zahlungsfunktionalität verstanden. Eine zentrale wirtschaftliche Forderung ist dabei die Umlauffähigkeit, auch bezeichnet als Transferabilität, die „offline" in direkter Weise geschieht. Dies steht jedoch in scheinbarem Widerspruch zum Problem der Entstehung und Verwendung von Münzkopien, dem „Multi-Spending". Zur Auflösung dieses Konfliktes verwenden fast alle bisherigen Verfahren das Prinzip der konditionierten Anonymität von Einweg-Token-Systemen, das die Identität des Besitzers zum festen Bestandteil einer jeden derartigen digitalen Münze macht. Grund: Sollte ein solcher eCoin mehrfach verwendet werden, lässt sich die Identität des Besitzers rechtlich eindeutig ermitteln. Probleme einer solchen Lösung sind jedoch die damit verbundenen Konsequenzen bezüglich Anonymität und Transferabilität: Wesentliche Bargeld-Eigenschaften gehen nämlich verloren. Daher lassen sich bis heute physischem Bargeld vorbehaltene Eigenschaften technisch für elektronische Token nicht realisieren.

Die Aufgabe der vorliegenden Dissertation bestand in der Entwicklung eines Systemkonzepts für die Mehrweg-Token-System-Alternative, das die meisten Eigenschaften physischen Bargelds in einem digitalen Medium wie dem Internet abbilden kann, insbesondere die essentielle Eigenschaft der unbegrenzten Weitergabe ohne die Inkaufnahme von Abstriche bei der Systemsicherheit. Bargeld-artige Systeme ohne solchen Mehrwert erscheinen aus Anwendersicht wenig attraktiv. Diese Dissertation wagt die These, dass sich die Versprechen des elektronischen Commerce der New Economy ohne die Einlösung der ökonomischen Taxonomiefaktoren eines mobilen, anwenderfreundlichen Bargeld-Systems nicht (optimal) erfüllen lassen. Im Blickpunkt der vorliegenden Dissertation stehen die Voraussetzungen für die konkrete Machbarkeit digitalen Bargeldes mit den Eigenschaften seines physikalischen Pendants unter Verwendung heute verfügbarer Basis-Technologien. Dabei nehmen Fragestellungen der Sicherheit zentrale Positionen ein.

Zur Verwirklichung der gewünschten Bargeld-Eigenschaften wurde ein kopierfreies Transfer-Protokoll entwickelt, das die anonyme Übertragung elektronischer Münzen, so genannter eCoins, auf Peer-to-Peer-Basis in Form einer Teleportation ermöglicht: Jeder durch dieses Protokoll veranlasste eCoin-Transfer zeichnet sich dadurch aus, dass Münzen **bewegt**, aber **nicht kopiert** werden: Sie verschwinden beim Absender, um dann beim Empfänger wieder zu erscheinen. Vorhandene unikative Eigenschaften bleiben jedoch erhalten. Elektronische Portemonnaies, so genannte eWallets, bilden als Chip-Tresore die Endpunkte der Bargeld-Übertragung und sichern sie physikalisch und kryptografisch gegen Analyse und Manipulation. Dieser ebenfalls in dieser Arbeit vorgestellte Ansatz eines „**CA**sk for **S**torage and **T**ransport **O**f access **R**estricted secrets" (CASTOR) realisiert das bekannte Prinzip eines „**H**ardware **S**ecurity **M**odules" (HSM) oder „**S**ecure **E**lements" (SE) auf neuartige Weise und reduziert so, gemeinsam mit dem Einsatz infrastruktureller PKI-Architekturen, ein komplexes Angriffsszenario auf wenige, beherrschbare Elemente. Dennoch verbleibt eine grundsätzliche Hürde, die als Status- bzw. Bestätigungsproblem in Erscheinung tritt. Dabei handelt es sich um ein algorithmisch nicht lösbares fundamentales „common knowledge"-Paradigma bei verteilten Systemen. Es ist auch als „coordinated attack problem" bekannt und tritt dann auf, wenn der Übertragungskanal *innerhalb eines kritischen Zeitfensters* zusammenbricht. Das ist in realen Übertragungssystemen grundsätzlich nicht gänzlich zu vermeiden. Dieses Problem wird als „fair exchange" Defizit verstanden und ist nicht nur technisch substanziell, sondern auch wirtschaftlich signifikant. Transaktionen in (unterschiedlich regulierten) virtuellen (Rechts-) Räumen müssen jedoch mit allen verfügbaren technischen Mitteln und Methoden die Entstehung von Fairness-Defiziten vermeiden, besonders wenn sie „cross-boarder" realisiert werden sollen.

Das hier vorgestellte Lösungskonzept sieht für diesen Fall die offline durchzuführende gezielte Vernichtung betroffener Münzobjekte vor. Im Gegenzug wird ein kryptografischer Verlustbeweis konstruiert, der zu einem späteren Zeitpunkt jederzeit online wieder gegen neue Münzen eingetauscht werden kann. Systemimmanente Sicherheitsmaßnahmen sorgen für eine missbrauchsfreie Nutzung. Diese Aufteilung zum einen in die offline durchgeführte Münzweitergabe und zum anderen in die online durchzuführende Erstattung fehlerhafter Abbrüche kompensiert den Effekt, der als das Problem der "Byzantinischen Generäle" bekannt ist. Dabei handelt es sich um ein Problem der Übereinkunft, das historisch darin bestand, dass räumlich getrennte Heerführer einstimmig beschließen mussten, ob sie eine feindliche Armee angreifen oder nicht, und die dazu auf hin und her zu schickende Boten angewiesen waren. Dieses Problem ist fundamental und besteht auch in der heutigen Telekommunikation. Der eigentliche Transfer bei fairCASH wird als „delayed-true two-party fair exchange of eCoins for a receipt" bezeichnet.

Zur Verständnis des Bedrohungspotentiales rundet die Darlegung von Hackermethoden und den damit verbundenen technischen Risiken diese Arbeit ab. Den erforderlichen Rahmen bilden dabei ein einfaches Management-Modell zur Konkretisierung von Angriffsszenarien und deren Einschätzung sowie die Klassifizierung bekannter Attacken. Darüber hinaus werden einige – auch neue – Methoden vorgeschlagen, wie ein CASTOR-basiertes Portemonnaie auf Chip-Ebene sicherheitstechnisch mit Gegenmaßnahmen versehen werden könnte, um seine Resistenz gegen Angriffe zu erhöhen.

1.2 Executive Summary

This work contributes technical to the field of fair exchange protocols by proposing a new way to move safeguarded secrets between cryptographically secure endpoints excluding the possibility of duplication. After a brief introduction and presentation of an overview of the subject matter, the problem areas of creating a way to teleport secrets with the help of tamper-resistant hardware are defined. Objects like the CASTOR (a HSM element), eCoins (the secrets) and a copy-less transportation (the teleportation protocol) are introduced as key elements for the intended solution to build the proposed technical framework. With this in hand, its application could work as central exchange engine in the construction of a Digital Cash environment. Adding an ATM (the eMint) and a trust center (the CA) to the scenario taking the role of an optimistic **T**rusted **T**hird **P**arty (TTP) provides generatability (minting new eCoins) and revocability (blacklisting existing eCoins and eWallets) to the system. This work describes key elements of the proposed Digital Cash framework named **fairCASH** with the required accuracy tied and held together by defining assumptions, objectives, properties and specific objects. This then leads to a technological solution for building an electronic payment system based upon transferable eCoins. [chapter 2]

Thematically this thesis starts providing a brief state-of-the art overview about how the field of mobile commerce gets involved by shifting more and more business from legacy methods to the Internet based ones. The need of an easy and safe way to endorse this transition with an adequate payment system is shown. The reader will find a first impression of the fairCASH architecture, infrastructure, and capabilities through the explanation of the main elements in its environment: eCoins based upon certificates, eWallets, and teleportation. In a first contribution overall guideline arguments are presented, why technology based developments are best suited to provide the tools for innovations like Digital Cash. The fundamental difference between token based blinding techniques widely used as a mean to protect ePayment systems against multi-spending and the proposed system by discussing the adversarial character for payment system users connected to that property is emphasized. Next, well-chosen system properties illustrating the real needs are presented. Here the interested reader will find a plurality of information around the fair exchange subject, starting with a formal definition. By following the existing literature, it is obvious that the exchange protocol has to be delayed fair, time lined, and effective to guarantee atomic parallelism. Naming the most important success factors for any Digital Cash system, this thesis goes on in its way to discuss functional must-have key elements including their meaning for a later protocol definition proposal. This chapter will be followed by a brief discussion of the characteristically metrics alongside with a comparison of Digital-Cash- and physical-token-currencies (by providing facts related to the €uro system), and finally a clear and pragmatic scenario definition including commented descriptions of a selection of contemporary (and failed) ePayment systems.

The possibility of turning a technology into business is mostly an exciting case. This thesis looks and discusses questions with respect to the central business:

- Can fairCASH be the base to offer essential customer value?
- Will it be possible to find enough advantages compared to other cash services?
- Can such a technology offer a significant level of user satisfaction?

Payments are actuated by humans but effected and conducted by technical means. This thesis takes a look onto the technical environment about how the interaction takes place. This includes possible configurations about the eWallet operation methods for device discovery and pairing. The way this is done decides about the ability and performance of such a financial infrastructure for their usage not only on a PoS but also on payment gates for masses. [chapter 3]

Next, the underlying formal communication message channel model is introduced, followed by the factual issue of packet loss and the 'byzantine generals' undecidability state, which has to be respected in the following. The knowledge of the "position of the value" (ownership) during the transmission under all circumstances is mission critical. Acceptance of the fact to live with an unreliable channel for exchanging messages between Alice and Bob has a great influence on how to deal with atomic commitments, a desired feature in the termination phase of the teleportation protocol. The effect of state inconsistency in two-party communication environments based upon atomic delivery as proposed in literature is reviewed and it is concluded that up today there is no standard way to solve the atomic commitment problem within the fairCASH environment by applying existing methods. [chapter 4]

The previous discussion of different privacy levels and their meaning for anonymity concepts including unobservability, untraceability or unlinkability is pointing the way to a "**delayed-true**

two-party fair exchange protocol". Naming the requirements, this thesis proposes a general and modular definition for protocol assumptions, objectives and properties. Thereafter, a basic notation for the teleportation protocol is put on the table, following the usual methodology in consideration of the specific needs in the presented case. Describing the exchanged protocol messages, a complete definition about their structure and meanings is given. With that detailed step-by-step presentation and exhaustive discussion of all messages including their embedded elements, the reader is invited to follow Alice and Bob by logically stepping through the whole exchange process. Thereafter, the associated protocol states will be discussed and the analysis of achievable fairness, reasons why choosing special decisions in one case and in other cases being constrained by circumstances is presented. This leads to the solution about how to guarantee (by potentially recreating) true fairness through the usage of affidavits, proving a loss of value without exposing the system to new fraud threats, usable for automated reimbursements. Taking a closer look to the performance of the exchange, the forfeiture probability can be determined in the worst case scenario for transactions in the need of fairness recreation to an upper limit of 3% (never expected to exceed 1‰ in practice) based upon the nature of the teleportation protocol itself and the effective pledged **Q**uality **o**f **S**ervice (QoS) defined by international standards and recommendations. A calculation of transactions times in different networks based on a previously done estimation of message sizes shows an asymptotic barrier of about one second, introduced by the assumed processing speed of the eWallet. At this instance, it should be pointed out, that data objects are playing an important role in the protocol presented. In combination with the transfer protocol itself, they provide and guarantee the proposed protocol properties including and conforming to an ITU-T X.509v3 based PKI trust architecture. [chapter 5]

Forgery and multi-spending are the basic threats to counter in any financial system based on token circulation. A short presentation of the potentially different (technical) risks introduced by such a system is discussed, concluding to the question of possibility "to cheat the fairCASH system without tampering the eWallet". Goals are discussed as ranking criteria, what needs a protection, and which skills do attackers have. To counter and stabilize the presented fairCASH system, a basic security management model and questions about how to respond to attack scenarios are introduced. To make this more practical, known basic attacks are classified, ordered and grouped into different threat categories. [chapter 6]

Protection is the first obligation in an unsafe environment. The degree of protection is crucial to make a system like fairCASH operational or dysfunctional. Given enough time and resources, every protection system can be broken. However, it is good news that the postulation of the requirement for tamper-proved hardware, which we all know does not exist, is not necessary. It is shown that one of the central points of interest is: How long can an eWallet remain in the open market before it gets cracked. This is also a function of the continuous technical (attack) progress in a world where yesterdays technologies become cheap and widely available to today's attackers. This opens a race in which the manufaction of an eWallet starts on the leading edge position, while continuously dropping down to an imaginary bottom line, reaching the point in time being replaced by a new one including again the up-to-time defense technologies; an ongoing continuing cycle. As rule of thumb, it should be noticed that capabilities of silicon based HSMs should not be overestimated and capabilities of attackers must never be underestimated. It will be a bad design decision using just a few (or a single) system component(s) in a financial environment (e.g. eWallets) as sole barrier, standing between the hacker and the money. Nevertheless, the CASTOR is an essential part of the proposed design philosophy within the fairCASH system introducing countermeasures relating to possible eWallet integrity manipulation attacks. A good tamper-protected hardware with adequately chosen instruments against anticipated attacks joint risk management and safeguards against hypothetical losses on system level is a good starting point. This thesis references existing and introduces some new countermeasures like the presented TRUSTLET concept, contributing to the secure boot paradigm first presented by the AEGIS architecture [9] in combination with the Maze of Knossos first introduced with this thesis. [chapter 7]

In the conclusion of this thesis, the main results are compiled, revised and again presented. A small outlook to desirable future activities is formulated. [chapter 8]

Additional notes to possible entrapments for the overall fairCASH system are given, even if elements like eWallets and their protocols are well protected. They are followed by remarks to the naming convention of VPN and VPCs (used for the same matter within this thesis). Some basic reasons why smart cards and TPMs are not enough in high secure based application are shown combined with the question why black box security should be avoided. This is closed by reasoning, why future ICT security will be based on secure hardware.

A comprehensive presentation of all data objects including key rings used within the system containing private, public and session keys, the use of certificates and CRLs and how this is interwoven with the proposed services accounts for an understanding of the network infrastructure leads to an overall understanding of the reader. Another interesting point is the introduced way of a flexible crypto-regulation readiness through the usage of Capability-Flag-Vectors (see on page 141), making it possible to adapt and obey to national country oriented restrictions for the usage of encryption technology important for cross-boarder communications. This work is concluded by explaining the significance and structure of the data objects used within this thesis, followed by a comprehensive list of tables and references. [chapter 9 and 10]

1.3 Contribution to the State of the Art

Traditionally, the design of a payment systems is closely related to the human habit: Already in a very early state, money became an integral part of mankind's existence, almost at all locations of discovery of ancient settlement places, detections for natural money were made by historians. Today, we are where our children are called 'digital natives', living in a world of networks and embedded computational resources everywhere. One of the first innovative contributions to Digital Cash was done by David Chaum 1990 with his eCash system based upon the blind digital signature protocol paradigm (see on page 39). The appealing logic behind his mathematical invention lead to the construction of 'blinded coins', containing the identity of the original owner and being able to reveal it case of multi-spending. The Digital Cash concept of fairCASH mimics the behavior of physical cash. Due to its coin concept, a value transfer between payer and payee is realized by transferring the ownership of the coin. An essential part is the way how this transfer is conducted: Following the cash paradigm, it needs to be done **peer-to-peer** and **offline** in a **repeatable** way. Such a transfer is called **teleportation**. The main technical problem is to guarantee fairness under all circumstances. The fundamental effect of the Byzantine Generals' undecidability state issue (see page 57) does not allow conducting such a transfer without a (trusted) third party. This fact seems to contradict the offline attribute of the aspired cash transfer. To the author's knowledge, there has not been any treatment of this challenging problem, neither in the practical field nor in the literature over the last 10 years.

The first part of this thesis is devoted to the study of the phenomenon "cash" from a technical perspective with a small digression describing a hypothetical business case. This is done by looking what is documented in the literature about previous attempts to create electronic payment systems focusing on ones with Digital Cash affinity.

Thus, the second part, as the mayor contribution to this work, makes a proposal how to implement the desired teleportation. The result of any untreated Byzantine transfer is either a potential loss, or overspending of the transferred items, in this case the value of the eCoin(s). Taken as a challenge to computational fairness in the field of electronic commerce, the presented solution firstly separates all 'good' transfer cases from the failed ones. It should be mentioned that the transfer itself is scaled to a heuristic policy of 'no profit from any failure' with the effect to increase the loss probability. These 'bad' transfers are post-processed by the local eWallet 'enjoying' a 'controlled annihilation' of all affected eCoins and the creation of an affidavit for the external arbiter (eMint). This separation causes temporal unfairness to one or even both protocol entities because of the value loss connected to such an action. That is the reason to call this a 'delayed-true two-party fair exchange'. The loss proofs can be turned into new value (e.g. exchanged against eCoins) in a succession step at any time outside the transfer protocol. This mechanism disconnects the transfer from the necessity of being online. The reimbursement process has to be negotiated with the eMint in the need to be done online. All this can be achieved in an automated and user transparent way.

In the last part, an attempt is made to collect, organize and supplement threads, hacker measures and technical countermeasures according to the challenging eWallet construction. Protection guidelines are presented, including the CASTOR approach as system-on-chip containment to deliver the needed grade of security, the trusted boot through TRUSTLETs, the usage of a physical uncloneable function and the introduction of the Maze of Knossos. Taking security as an important decisive feature in the field of value transactions, recommendations are made which methods are best suited to implement cryptographic functionality on eWallets at the current state of technology.

A blank Page for relaxing the restless Mind

Table of Contents