



<http://virtualgoods.tu-ilmenau.de/2004/>

Reviewed Papers

Virtual
Page
Numbers

Session 1: Watermarking for Virtual Goods

1. **StirMark and profiles: from high end up to preview scenarios** 1-12
Andreas Lang, Jana Dittmann,
http://virtualgoods.tu-ilmenau.de/2004/virtual_goods_2004_LANG_DITTMANN.pdf
2. **Synchronization of Video Watermarks for Oblivious Detection after Geometrical Distortions** 13-23
Uwe Wessely
<http://virtualgoods.tu-ilmenau.de/2004/wmsync-VG04.pdf>
3. **Complexity Optimization of Digital Watermarking for Music-On-Demand Services** 24-35
Martin Steinebach, Sascha Zmudzinski
http://virtualgoods.tu-ilmenau.de/2004/watermarking_music_on_demand_steinebach_vg2004.pdf

Session 2: Culture and Business for Virtual Goods

4. **On-line music distribution: a case study** 36-46
Francis Rousseaux, Alain Bonardi, Romain Poncelet
http://virtualgoods.tu-ilmenau.de/2004/On-linemusicdistribution_a_case_study.pdf
5. **Secure Music Content Standard - Content Protection with CodeMeter** 47-58
Marcellus Buchheit, Rüdiger Kügler
http://virtualgoods.tu-ilmenau.de/2004/SecureMusicContentProtection_VG2004.pdf
6. **Towards a Secondary Market for Virtual Media - A Theoretical Approach** 59-71
Lutz Niehüser, Johannes Bräutigam
<http://virtualgoods.tu-ilmenau.de/2004/SecondaryMarket.pdf>

Session 3: The Value of Virtual Goods

7. **Modelling the eVerlage Payment Protocols** 72-83
Uwe Petermann
<http://virtualgoods.tu-ilmenau.de/2004/EVerlagePaymentProtocols.pdf>
8. **How to Pay in LicenseScript** 84-90
Cheun Ngen Chong, Sandro Etalle, Pieter Hartel
<http://virtualgoods.tu-ilmenau.de/2004/ceh04vgoods.pdf>
9. **Personalized Previews: An Alternative Concept of Virtual Goods Marketing** 91-100
Patrick Aichroth, Stefan Puchta, Jens Hasselbach
http://virtualgoods.tu-ilmenau.de/2004/personalized_previews.pdf

Session 4: Digital Protection and Digital Rights for Virtual Goods

10. **Enabling Digital Content Protection on Super-Distribution Models** 101-112
Carlos Serrão, Joaquim Marques
<http://VirtualGoods.tu-ilmenau.de/2004/VG2004-EDCP-SD-OSDRM.pdf>
11. **Licensing Structured Data with Ease** 113-124
Yee Wei Law, Cheun Ngen Chong, Sandro Etalle, Pieter Hartel, Ricardo Corin
<http://VirtualGoods.tu-ilmenau.de/2004/law04licensing.pdf>
12. **Interoperability Challenges for DRM Systems** 125-136
Andreas U. Schmidt, Omid Tafreschi, Ruben Wolf
http://VirtualGoods.tu-ilmenau.de/2004/Interoperability_Challenges_for_DRM_Systems.pdf

Modelling the eVerlage Payment Protocols

Uwe Petermann

Leipzig University of Applied Sciences

Computer Science Department

uwe@imn.htwk-leipzig.de

<http://VirtualGoods.tu-ilmenau.de/2004/EVerlagePaymentProtocols.pdf>

Abstract

This paper gives an overview on our work on modelling the eVerlage [WB02, BSW02] payment protocols. The eVerlage system sells rights to access electronic content for a certain amount of time. The user can access the content via the internet after the successful completion of the payment.

The eVerlage system allows to use various payment channels. In this paper we present a systematic view on the payment protocols implemented in the eVerlage system. The presented view is thought as a step towards a formal investigation of the integration of the considered payment channels.

1 Introduction

In this paper we describe our work on modelling the eVerlage [WB02, BSW02] payment protocols. The eVerlage system has been designed for selling literature which is available in electronic form. To be more precise, eVerlage sells the right to access literature via the internet for a certain amount of time. Several payment options for this service are supported. The customer can choose one of following payment providers: Paybox¹ — a service allowing authorisation of payments via a mobile phone, money card² — a chip card related to a bank account, Home Banking Computer Interface (HBCI) — a protocol allowing secure bank transactions over the internet or other suitable communication channels, credit card, paying by bill, voucher and an internal account for registered eVerlage-users.

¹Paybox has been not available in Germany for a while. Recently it returned under the label Moxmo.

²in german: Geldkarte

The large number of different payment options is comfortable for the user. The protocols for any two payment providers differ more or less. Moreover, the implemented protocols for the communication between the three involved agents (customer, merchant, payment provider) are quite complex. This has been a challenge for the developers.

In this paper we try to give a systematic view on the protocols. Our aim is to study the structure of the different protocols in order to identify similarities and differences between the various protocols.

Beyond the present paper remain the different license models which has been implemented in the eVerlage system.

2 The trade model

We analyse the eVerlage protocols following the model for secure trade proposed in [UN02, Wab03]. Basically, in an initial step merchant and customer agree that the merchant delivers a good — here the right to access electronic content via the internet — and that the customer pays a certain price for this good. Moreover, both sides agree which payment provider should mediate in the *money transfer*. So far the eVerlage protocols follow the trade model [UN02, Wab03]. Concerning the *delivery of the good* only eVerlage is considered as provider. However, the system architecture distinguishes a delivery unit called provider agent (cf. [Old02, WB02]). This unit might be seen as an embryonic form of a service provider responsible for the delivery of goods.

After an initial agreement the three mentioned parties play the following roles.

Merchant — currency creditor in relation to the payment provider,

Customer — currency debtor in relation to the payment provider and

Payment provider — currency debtor in relation to the merchant and currency creditor in relation to the customer.

The different protocols are instances of the following three phase scheme. We assume that good and price have been negotiated.

Phase I: Choose a payment channel and transfer payment parameters.

This takes 2 or 3 single communication steps.

The set of the payment channels which are available to a customer depends on whether she is a guest or a registered user.

Good and price as well as payment provider and delivery channel have been chosen after this phase.

Phase II: Execution of the payment.

Variant A: In the case of *Paybox*, *Money Card* and *HBCI* the **customer** herself interacts with the payment system in order to execute the payment. The merchant delivers having received the confirmation that the money transfer contract between customer and payment provider has been settled.

In the case of *Paybox* the payment provider contacts the customer asking for authorisation of the payment. Thus the protocol is (currency) creditor driven. In the both remaining cases the protocol is (currency) debtor driven. Indeed, the customer contacts the payment provider in order to initiate the payment.

Variant B: In the remaining cases, i.e. *Credit Card*, *Bill*, *Voucher* and the *internal account*, the **merchant** communicates with the payment provider directly.

Since the merchant is the initiator of this communication we can describe this variant as (currency) creditor driven. Any required parameters and authorisations must have been given by the customer before.

The protocols involving the payment methods *Credit Card* or *Bill* are examples of “pay after”, whereas *Voucher* and the *internal account* are instances of a “pay before” scheme.

Phase III: Transmission of the result of the payment transaction to the customer.

In certain cases this transmission occurs only implicitly. Then the customer is just granted access to the desired good.

In the remaining part of the paper we discuss the different payment protocols in more detail. More information on the eVerlage-System can be found in [BSW02], [WB02], [UN02]. An analysis of necessary infrastructure components for secure electronic trade can be found in a recent work [Wei04]. As a next step (to be published elsewhere) the protocols described here will be formalised in order to study their properties more precisely.

3 The protocols

3.1 Paybox

3.1.1 Paybox - informal description

The paybox system enables the authorisation of payments over a GSM network.

After obtaining an appropriate message (see a_1 in 3.1.2) from the merchant Paybox

is responsible to verify whether the customer whose phone number has been given has a valid contract with the Paybox company enabling to use this service.

If this condition is satisfied Paybox calls the customer via her mobile phone, describes the transaction (by voice) and asks to type in a PIN in order to authorise the transaction. Paybox will obtain the authorised amount via a debit advice. The customer authorised this procedure in his contract with Paybox.

Paybox transfers the result of the authorisation request to the merchant. eVerlage relies on that Paybox will transfer the agreed amount if Paybox sends an ok-message. Therefore eVerlage grants access to the good promised to the customer.

Remarks: The last message does not occur explicitly. The customer is just granted access to the good she just promised to pay for. A more elaborated trade model [Wab03] would transfer an explicit message confirming the successful completion of the payment. Then also the customer can not only be sure to possess the good but also to have the merchant's confirmation of receipt of the payment.

3.1.2 Paybox - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer → Merchant:	balance, "Paybox", sessionID
		Merchant → Customer:	request for payment parameters
		Customer → Merchant:	CPID
II	a ₁	Merchant → Payment:	pbMerchID,userID,CPID, balance, timestamp, order#
	a ₂	Payment → Customer:	request for authorisation
		Customer → Payment:	PIN
		Payment → Customer:	result
	b	Payment → Merchant:	O.K., timestamp, CPID, order#
III		Merchant → Customer	ok (implicitly)

3.1.3 Paybox - formal summary

Step I: Details agreed on completion of this step: balance, payment provider, customer identification (CPID — phone number or a synonym) against the payment provider

Step II: a₁: Merchant³ (as currency creditor) initiates the settlement of currency debt contracts: customer—payment provider and payment provider—merchant.

³identified by pbMerchID

The merchant provides data allowing to identify: merchant, customer, balance, and the transaction.

a₂: Currency debt contract customer—payment provider has been settled.

b: Payment provider informs merchant:

Currency debt contract payment provider—merchant settled

Step III: The merchant considers the settlement of the both currency debt contracts as sufficient for granting access to the bought content.

3.2 Money card

3.2.1 Money card - informal description

The money card is a chip-card. Its purpose is to hold smaller amounts of money (about 200 EUR). In Germany most customers of savings banks (Sparkasse) and agricultural banks (Volksbank) possess such cards.

In order to use it with eVerlage, the user needs a suitable card reader connected to the computer. Technically, the customer interacts with an applet which is loaded from the eVerlage-site. We consider the applet as a part of the payment system. Therefore the interaction of the customer is seen as a communication between customer and payment provider. The expression `wallet(Yes|No, PIN#, balance)` denotes the result of customer's decision to confirm or to reject the contract expressed by entering the appropriate answers and data to the applet. The shortcut `userIDPS` is an identification of the user against the payment system.

3.2.2 Money card - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer → Merchant:	balance, "Geldkarte", sessionID
		Merchant → Customer :	wallet address, sessionID
II	a ₁	Customer → Payment:	wallet address, sessionID
	a ₂	Payment → Customer :	wallet
		Customer → Payment:	wallet(Yes No, PIN#, balance)
		Payment → Customer:	userIDPS, TAID, result
	b	Payment → Merchant	wallet(Yes No, PIN#, balance)
III		Merchant → Customer:	ok (implicitly)

3.2.3 Money card - formal summary

Step I: agreed on completion of this step: balance, payment provider, parameters allowing to evoke the service of the payment provider

Step II: a₁: The customer (currency debtor) starts settling the currency debt contracts: customer—payment provider and payment provider—merchant.

a₂: Currency debt contract customer—payment provider has been settled.

b: The payment provider informs the merchant:

Currency debt contract payment provider—merchant has been settled and fulfilled.

Step III: Settlement of the both currency debt contracts and fulfilment of the currency debt contract customer—payment provider are considered as sufficient for granting access to the bought content.

3.3 HBCI

3.3.1 HBCI - informal description

The HBCI (Home Banking Computer Interface) enables the customer to execute banking transactions in a secure way over a network, usually the internet. A customer needs an agreement with a bank offering this service.

Here we consider HBCI as a system consisting of a HBCI service provider (e.g. a bank) and a provider of the helper application which allows to contact the HBCI service provider. Technically, the merchant, i.e. eVerlage, sends a Java-Webstart-Application which executes the transferal. The customer just needs to type in the appropriate parameters and to give the authorisation. If the transferal has been constructed and transmitted successfully the Java-Webstart-Application also sends an ok-message to the customer.

The access to the good he paid for will be granted only if the payment provider system signals the successful completion of the money transfer.

Remarks:

The phrase “home banking” suggests a consumer focus of this payment protocol. This is completely misleading. HBCI is a very powerful and flexible protocol and well suited for any kind of bank transactions. The HBCI-interface has been integrated only into the developer system not in the production system of eVerlage. The developer continues the work concerning HBCI. For a test server for HBCI see [Pal04]. For steps towards a formalization of HBCI using VDM (Vienna Design Method) see [Zwö99].

3.3.2 HBCI - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer → Merchant:	balance, "HBCI", sessionID, userID
		Merchant → Customer :	HBCI-Application address, sessionID
II	a ₁	Customer → Payment:	HBCI-Application address, sessionID
	a ₂	Payment → Customer :	HBCI-Application
		Customer → Payment:	userIDPS, TAID, payment parameters(MerchID,userID, balance, timestamp, order#)
		Payment → Customer:	userIDPS, TAID, result
	b	Payment → Merchant:	O.K.,TANP,timestamp,order#
III		Merchant → Customer:	access granted

3.3.3 HBCI - formal summary

Step I: This step leads to the agreement of the following informations: balance, payment provider, further data to identify the trade and the customer when using the service of the payment provider.

Step II: a₁: Customer (currency debtor) starts settling currency debt contracts: customer—payment provider and payment provider—merchant

a₂: Currency debt contract customer—payment provider settled.

The mentioned currency debt contract will be fulfilled.

b: Payment provider informs merchant:

Currency debt contract payment provider—merchant settled and fulfilled.

Step III: Both currency debt contracts fulfilled, hence access to the desired content will be granted.

3.4 Credit card

3.4.1 Credit card - informal description

The transmitted credit card data CCDATA⁴ are validated by the merchant system according to the criteria defined by the credit card enterprises. This is necessary for the merchant

⁴CCDATA = Credit Card Data: eVerlage as merchant, Timestamp, command, balance = amount to pay
CRNO = Credit Card Number EXYE = expiration year EXMO = expiration month

to be sure to obtain the money promised by the customer. The response GRESP⁵ allows to infer the result of the payment transaction.

3.4.2 Credit card - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer → Merchant:	balance, "Credit card", sessionID
		Merchant → Customer :	request for payment parameter, sessionID
		Customer → Merchant:	balance, CRNO, EXYE, EXMO
II	a	Merchant → Payment:	CCDATA
		Payment → Merchant:	GRESP
		Merchant → Payment:	trefnum, balance
	b	Payment → Merchant:	balance, result, time stamp, trefnum
III		Merchant → Customer :	"O.K." or error

3.4.3 Credit card - formal summary

Step I: On completion of this step will be agreed: balance, payment provider, further data to identify the trade and the customer when using the service of the payment provider

Moreover: Disclosing her confidential credit card data the customer agrees in advance in a currency debt contract customer—payment provider.

Currency debt contract customer—payment provider has been settled.

Step II: a: Merchant offers currency debt contract payment provider—merchant.

b: Payment provider informs merchant:

Currency debt contract payment provider—merchant settled

Step III: Settlement of the both currency debt contract is considered as a sufficient condition for granting access to the bought content.

3.5 Bill

3.5.1 Bill - informal description

The possibility to pay by bill is restricted to registered eVerlage-users. After a successful registration eVerlage can trust in the validity of the address and other informations.

⁵Response: GRESP=balance, command, CRNO, currency, EXYE, EXMO, "eVerlage", trefnum = transaction reference number

This is considered to be sufficient to agree with this payment option. The parameters⁶ transmitted in step IIa are verified similarly to the credit card case.

This payment option has been tested successfully. Nevertheless, during the operation time of the eVerlage-System no commercial partner had been found who agreed to provide this payment service for eVerlage.

3.5.2 Bill - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer → Merchant:	balance, "Bill", sessionID
		Merchant → Customer :	request for payment parameter, sessionID
		Customer → Merchant:	balance, sessionID
II	a	Merchant → Payment:	sessionID, balance, currency, addressee, address ... further parameters
	b	Payment → Merchant:	"O.K." or error
III		Merchant → Customer :	"O.K." or error

3.5.3 Bill - formal summary

Step I: Agreed on completion of this step: balance, payment provider, further data to identify the trade and the customer when using the service of the payment provider.

Moreover: Customer is aware and agrees with that choosing this payment channel a currency debt contract customer—payment provider will be settled.

Step II: a: The merchant offers currency debt contract payment provider—merchant.

b: Payment provider informs merchant:
currency debt contract payment provider—merchant settled

Step III: Settlement of the both currency debt contracts considered sufficient for granting access to the bought content.

3.6 Voucher

3.6.1 Voucher - informal description

The payment by a pre-paid voucher (German: Gutschein) has been introduced as a marketing option. The usage relies simply on typing a long random character sequence printed

⁶date, transaction number, error code, error message, delay for payment (immediately or n minutes), protocol error, last name, first name, title, street, zipcode, town, country

on the voucher. The issuer of those vouchers has to take care that every such number occurs only once and can be used only once.

3.6.2 Voucher - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer→ Merchant:	balance, "Voucher", sessionID
		Merchant→ Customer:	request for payment parameter,sessionID
		Customer→ Merchant:	Voucher key, sessionID
II	a	Merchant→ Payment:	Voucher Balance, userID
	b	Payment→ Merchant:	"O.K." or error
III		Merchant→ Customer:	"O.K." or error

3.6.3 Voucher - formal summary

Step I: On completion of this step merchant and customer agreed balance and payment provider. The currency debt contract customer—payment provider is considered to be fulfilled. Either the customer or someone else paid for the voucher.

Step II: a: Merchant offers currency debt contract payment provider—merchant.

b: After the verification of the key of the voucher the payment provider informs merchant: Currency debt contract payment provider—merchant has been settled. The currency debt contract customer—payment provider is assumed to be fulfilled. Actually it has been paid before.

Step III: Settlement of the currency debt contract payment provider—merchant and the fulfilled currency debt contract customer—payment provider are sufficient for granting access to the bought content.

3.7 eVerlage internal account

3.7.1 Account - informal description

Registered users of eVerlage can use an internal account (in german: Konto) to pay for electronic goods. This account can be powered by money transfer.

For legal reasons this payment channel has been offered only in an experimental phase.

3.7.2 Account - communication scheme

Phase	Step	Communication Partners	Message content
I		Customer→ Merchant:	balance, “eVerlage Konto”
		Merchant→ Customer:	request for payment parameter
		Customer→ Merchant:	account#
II	a	Merchant→ Payment:	account#,balance, timestamp, order#
	b	Payment→ Merchant:	“O.K.” or error
III		Merchant→ Customer:	“O.K.” or error

3.7.3 Account - formal summary

Step I: Agreed on completion of this step: balance, payment provider, customer’s account. The currency debt contract customer—payment provider is settled. Indeed, the money transfer already happened.

step II: a: Merchant offers currency debt contract payment provider—merchant.

b: Having verified the balance of the account the payment provider informs merchant: Currency debt contract payment provider—merchant settled.

The currency debt contract customer—payment provider is considered to be fulfilled (“payed before”).

Step III: Settlement of the both currency debt contracts considered sufficient for granting access to the bought content.

4 Towards a formalisation

The representation of the protocol messages discussed in the previous sections leads to their formal representation as terms. Following the approach of [Pau98] we can define sequences of those terms as formal representations of protocol runs. Such a formalisation has been done by the present author using the KIV-system following [HKRS03]. Using this formalisation we can analyse abstract properties of the protocols.

5 Summary and outlook

In this paper we presented an overview over the payment protocols implemented in the eVerlage system. This trade platform for virtual goods offers a large number of pay-

ment options. The presented view is thought as a step towards a formal description and investigation of the mentioned payment channels.

References

- [BSW02] Klaus Bastian, Michael Schwantner, and Thomas Wabner. Die eVerlage-Zahlungsplattform zum Handel mit digitalen Inhalten. In *10. Leipziger Informatiktage*, pages 265–268, 2002.
- [HKRS03] D. Haneberg, A. Kriebich, W. Reif, and K. Stenzel. Design for trust: Security in m-commerce. In *Informatik 2003*, Lecture Notes in Informatics, pages 91–94, 2003.
- [Old02] Frank Oldennettel. Das eVerlage-System: Eine digitale Bibliothek für kostenpflichtige wissenschaftliche Verlagsprodukte. In *10. Leipziger Informatiktage*, pages 246–264, 2002.
- [Pal04] Stefan Palme. A demonstration server for HBCI. <http://hbc4java.kapott.org/demoserver.html>, Visited: May, 1, 2004.
- [Pau98] Lawrence C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.
- [UN02] Hans Ulrich Niemitz. Das vollständige Modell komplett sicheren Handels ... In *10. Leipziger Informatiktage*, pages 265–268, 2002.
- [Wab03] Thomas Wabner. Ein Schuldvertragsmodell für den elektronischen Handel. In *11. Leipziger Informatiktage*, pages 119–125, 2003.
- [WB02] Thomas Wabner and Klaus Bastian. Eine abstrakte Sicht des eVerlage Payments. In *10. Leipziger Informatiktage*, pages 258–264, 2002.
- [Wei04] Michael Weiser. Rechtsverbindlicher Handel im Internet auf Basis sicherer Verzeichnisdienste. Master’s thesis, HTWK Leipzig, 2004.
- [Zwö99] Simon Zwölfer. A formalization of a home banking protocol using vdm. Master’s thesis, Technical University Graz, Austria, 1999.