A SYSTEM FOR SECURE MOBILE PAYMENT TRANSACTIONS

Teppo Halonen and Teemupekka Virtanen
Helsinki University of Technology, Department of Computer Science, Telecommunications Software and Multimedia Laboratory

Abstract: A need for secure payment methods in the mobile and conventional Internet has arisen as a result of the increase of on-line commerce. Most of the current payment methods that can be used in conducting transactions on the Internet have major drawbacks either in terms of functionality, usability, costs or security. The widely accepted way of securely and reliably authorizing electronic payment transactions is through the use of digital signatures in a PKI framework.

Organizations like the WAP Forum and MeT Initiative have made efforts to introduce industry standards for bringing PKI capabilities to mobile phones. The WAP version 1.2.1 compliant handsets already come with support for making digital signatures using the wireless identity module WIM. These new capabilities readily lend themselves to implementing mobile payment systems.

This paper presents a system that makes use of the MeT WPKI framework in implementing electronic payment authorization. The Mobile Payment System interacts with a merchant, payer and issuer as well as supporting back-end systems in coordinating secured payment transactions. It enables securely authorizing payment transactions using a standard WAP enabled handset.

The focus in the paper is in describing the system model and the high level structure. The details of implementation aren't discussed when not essential.

Key words: Mobile payments, PKI, WPKI, WAP, WIM

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35604-4_20

R. Traunmüller (ed.), *Information Systems*

1. INTRODUCTION

1.1 Background

Financial institutions and merchants are increasingly interested in automated electronic forms of payment. The reasons for this are simple; the more the payment process is made electronic, the lower the costs of both the technology to process conventional money and the actual manual processing of payments are.

Furthermore the lack of easily accessible and versatile standard means of electronic payments is one of the biggest obstacles for the on-line electronic commerce in the B2C model. The systems so far have all their limitations in terms of usability and security. As the standard wireless public key infrastructure is emerging, there exists a foundation, on top of which payment systems can readily be built.

Although on-line commerce is taking speed on the Internet – fixed and mobile – payments is an area where there is a lack of generic, reliable solutions. This is, in fact, the most important reason for the fact that B2C e-Commerce hasn't grown as quickly as possible and anticipated by many people [1].

1.2 Goal and Scope

The goal of this paper is to describe a system that enables users to perform secure payment transactions using mobile phones. The system is hereafter referred to as *Mobile Payment System* or just *system* when the context permits it.

The system will be based on the use of Wireless Application Protocol 1.2 [2] compliant mobile terminals that have a Wireless Identity Module [3] - in other words, mobile terminals with a standards-based capability to create digital signatures. As the payment type, the system will support digitally signed authorization by the payer. The money transfer will be based on a customer account scheme, details of which are outside the scope of this paper. It has to be noted, that the system does not make an attempt to implement electronic money. It is rather a system that applies secure mobile authorization to the business case of mobile electronic payment.

The Mobile Payment System will interact dynamically with WAP terminals, certification authorities, electronic merchant systems, point-of-sales terminals and invoicing and account management systems. The communication with those entities takes place over both mobile and fixed networks.

2. THE FOUNDATION FOR THE WORK

2.1 Basics

The Mobile Payment System enables payment authorization by the means of using digital signatures. Thus the main theoretical foundation for the work are public key cryptography, public key infrastructures, especially X.509v3 and digital signatures discussed in [4], [5], [6] and [7]. The theoretical framework related to these fields of data security is not discussed in this paper – the reader is referred to the above-mentioned sources of information regarding these areas.

2.2 WAP and Public Key Infrastructure

The WAP protocol family defined by the WAP Forum currently has a status of an industry standard for interactive mobile Internet on top of the GSM system. It covers all the protocol layers from the transport level up and all topic areas from security to content presentation in user interface.

The current version (fall 2001) that is being more and more supported by new mobile terminals coming to market is 1.2. It includes all the necessary specifications needed to support a PKI based security model in a wireless environment. The WAP Forum specifications related to the functional area of wireless security are:

- WAP Public Key Infrastructure Specification [8]
- Wireless Transport Layer Security Specification [9]
- Wireless Identity Module Specification [3]
- WMLScript Crypto API Library Specification [10]
- WAP Certificate Profile Specification [11]
- WAP TLS Profile and Tunneling Specification [12]
- End-to-End Transport Layer Security Specification

The five first ones of the specifications are most relevant to this paper. The other two discuss future ways of securing mobile-to-service communications (end-to-end session security) and are out of scope for this system, [10] being the most relevant. The WMLScript signText is a functionality that the user interface can utilize for creating digital signatures. The signText, makes use of the security element, WIM (Wireless Identity Module), that actually performs the cryptographic procedures and stores the secret keys securely.

The *Mobile Electronic Transactions initiative, MeT*, is an initiative like the WAP Forum focusing on creating industry standards for the

implementation of secure transaction capabilities in mobile terminals. It was founded by Ericsson, Nokia and Motorola. MeT's goal is "to establish a framework for secure mobile transactions, ensuring a consistent user experience independent of device, service and network" [13]. Its work is based mainly on that of WAP Forum, IETF and ITU-T. As the WAP Forum's goal is to introduce standards for technical issues, the MeT works on areas surrounding those standards – it strives to make the time-to-market of the new security standards shorter as well as to generate as wide an industry acceptance for them as possible. MeT also introduces some important concepts. One of them is the PTD - the personal trusted device [13].

3. DESIGN AND IMPLEMENTATION CRITERIA

3.1 Background

Criteria for the system design and implementation were set in the following areas: functionality, technical issues, security, scalability, performance, modularity and scalability. The criteria are discussed in this paper only on a high level to provide an insight into the requirements set to the work.

3.2 Functional and technical

The functional criteria defined the functionality that the system should implement. The technical criteria defined some guidelines for the work, like the expected implementation technology etc. Neither type of criteria are not presented in this paper in more detail – they become obvious as the system is presented.

3.3 Security

Strict criteria for the security of the system were set. However, a lot of the security concerns were scoped out of the work, by expecting them to be filled by other layers and entities. This goes for e.g. the certificate issuance and key generation. The actual security criteria stated in practical terms, that the system should not be possible to penetrate by unauthorized users and that the functioning of the system is such that it can be relied upon and trusted by the different actors.

3.4 Scalability and Performance

The system was expected to be scalable, as the actual numbers of users and load that the system should be able to support could not be defined before hand. A level of 100 000 daily users each experiencing a maximum of 2 second response times were expected as the minimum performance.

3.5 Modularity and Maintainability

The Mobile Payment System was expected to include only the minimum amount of functionality to accomplish its goal. The extra functionality should be implemented externally by other system. A requirement for the modularity was set: the system should be easily interfaceable to other systems. On the other hand new functionalities should be easy to add and the system should not require recompiling in event e.g. a new interface implementation is taken into use. Such tasks should be possible to perform through configuration changes.

4. SYSTEM SPECIFICATION

4.1 Introduction

The description approach in this chapter is based on the use of UML. The description is complemented by textual descriptions.

4.2 Relation to Prior Work And The Novelty of Concept

The need for the system arises from several factors. Firstly, that most feasible way to achieve secure payment transactions seems to be through the use of a public key cryptography based scheme. On the other hand, a clear demand arising from a ubiquity of service usage cannot be satisfied to the full by currently available systems at the same time with the strict security requirements. Chip card based schemes, the like of HST and EMV come close to solving the issue, but a wide network of compliant card readers need to be deployed. Finally, a new generation of connected mobile terminals with a similar capacity for digital signing (i.e. WAP 1.2.1 together with a WIM) is becoming available. This creates a possibility for building a PKI based payment infrastructure, that doesn't require any proprietary solutions for connectivity (e.g. card readers for the ICCs and closed protocols endorsed by credit card companies), signature processing or PKI

functionalities and services. Furthermore, the concept presented in this paper proposes a solution for the ubiquitous payment system – the act of shopping can be performed through any channel and only the payment need be performed over the WAP channel. In other words the system proposes a solution for binding sessions occurring over different access channels together.

The *Figure 5* presents the Mobile Payment System concept as a schematic sequence diagram from the perspective of the payer. The actual money traffic is not illustrated in the schema. This is because the Mobile Payment System is not actually handling the money traffic – it is merely registering and forwarding the authorized and validated payment transactions.

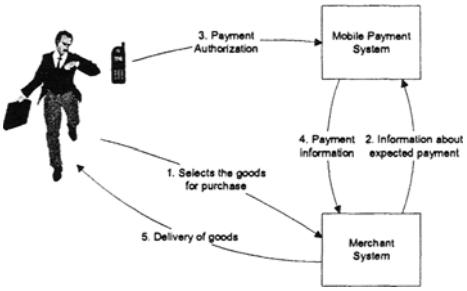

Figure 5. The Mobile Payment System conceptual scheme

4.3 Use Cases and Actors

The Mobile Payment System implements three core use cases.

- Payment request creation
- Payment request authorization
- Payment request committal

Putting these three use cases (when successfully completed) together in the above sequence, completes a mobile payment transaction. The use case of *Shopping*, is not included in the scope of the system. Naturally it is, however, expected that the payer has, before payment, done some 'Shopping', i.e. selected goods he wants to purchase. The use case of *Check-out*, i.e. retrieval or shipping of the purchased goods is similarly out of scope. It is implemented by the merchant system.

There are two main actors that participate in the use cases: the payer and the merchant. The payer has two roles, a PCD (Personal Communication

Device) role and a PTD (Personal Trusted Device) role. These roles denote, the fact that the user may use different access channels for the shopping use case and the payment authorization use case.

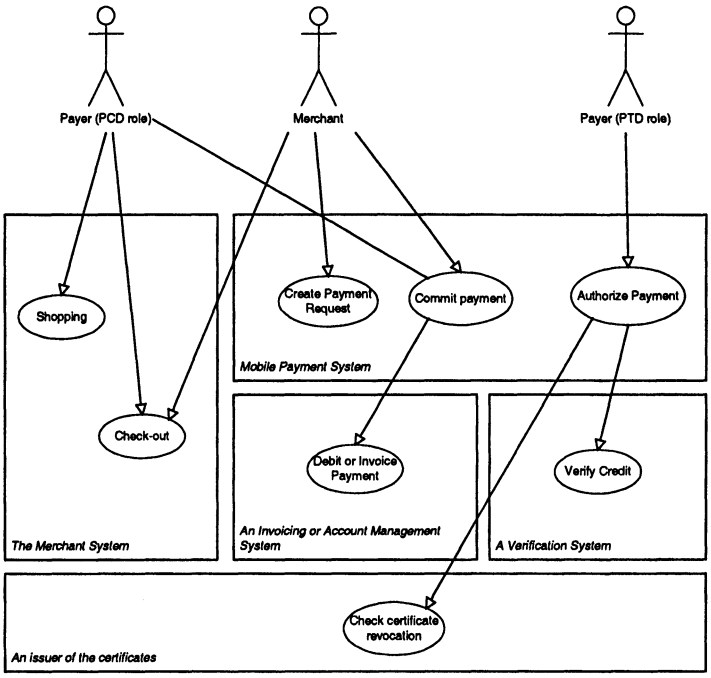

Figure 6. The Use Case Diagram

There are five different systems interacting in the process chain: the Mobile Payment System, the Merchant System, the Invoicing or Account Management System, the Credit Verification System and the Certification Authority. The role of the Mobile Payment System in relation with the other is that of an integrator. *Figure 6* illustrates the relationships of the actors, systems and the use cases.

4.4 System Structure And Workflow

Discussion of the internal organization of the Mobile Payment System into classes, packages and interfaces is omitted in this paper. The abstraction is made on a higher level – the interaction between the logical objects and actors is illustrated in *Figure 7*. The sequence diagram describes a complete payment transaction processing. The state of a payment transaction is managed in a RDBMS – the PaymentStore. The PaymentServer controls the state transitions.

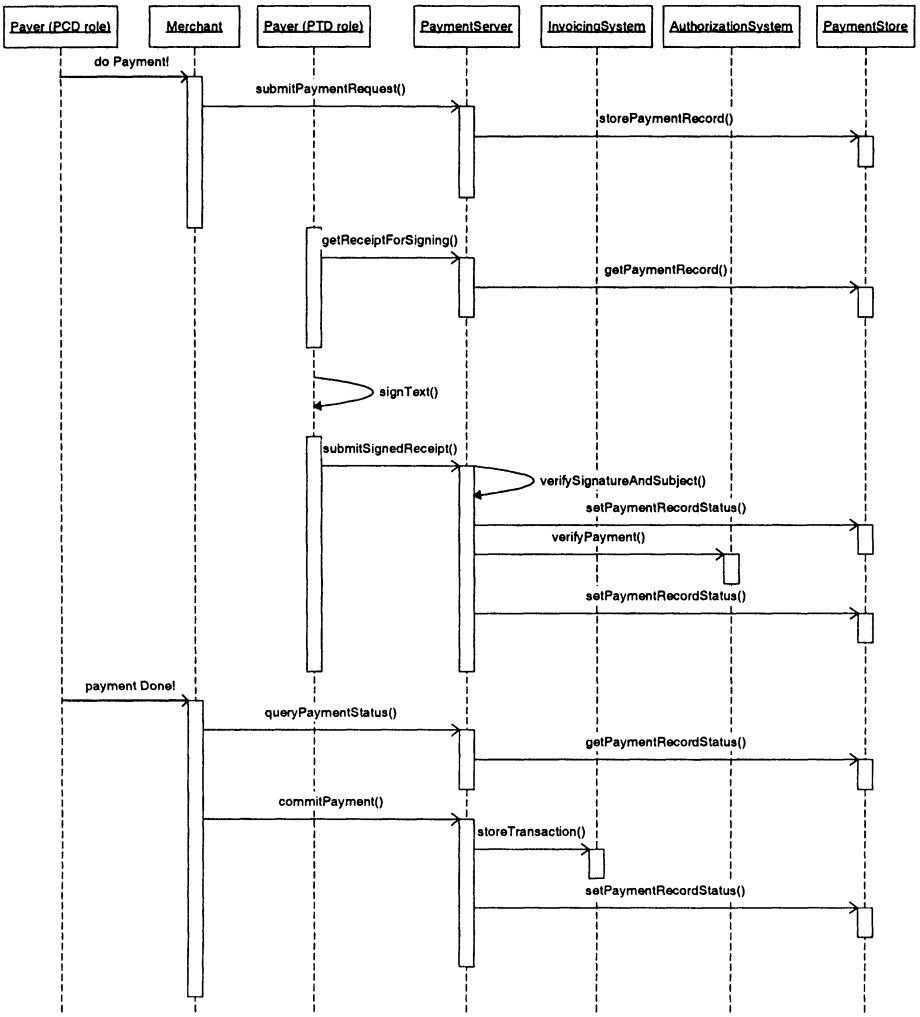

Figure 7. The Workflow

5. IMPLEMENTATION

5.1 System Architecture

The Mobile Payment System architecture is illustrated in *Figure 8.*

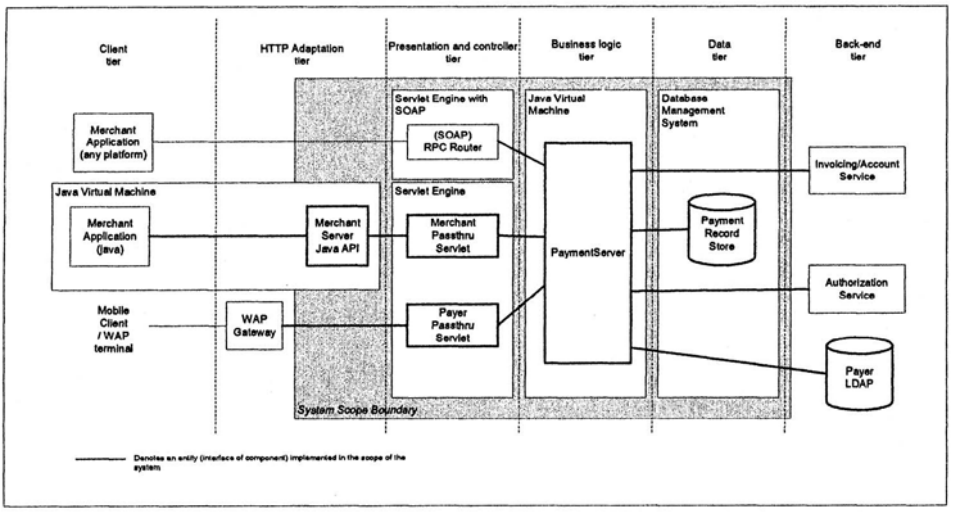

Figure 8. System Architecture

The Mobile Payment System is implemented using Java technology. The architecture follows a layered architectural style and the MVC (Model View Controller) design pattern [14]. This allows for good encapsulation of the business logic as well as for good maintainability. The layered paradigm also enables the isolation of the application server, i.e. the server running the business logic, from the Internet and consequently for security.

5.2 Special Issues In The Implementation

5.2.1 WAP SignedContent

The core of the Mobile Payment System in terms of functionality and technical novelty is the support for WAP digital signatures. As explained earlier, a choice was made, to implement the processing logic for the WAP SignedContent directly based on the Java 2 SE classes.

Only the most relevant options of the WAP SignedContent [10] were implemented. The X.9.62 elliptic curve signatures and X.9.68 certificates aren't supported. The features supported by the implementation are listed in the *Table 1*.

Table 1. Supported options of WAP SignedContent

Signature Algorithms	RSA/SHA according to PKCS #1
Signer Info Types	1) X.509v3 Certificate 2) RFC 2255 URL to X.509v3 Certificate
Content Types	1) data 2) text
Authenticated Attributes	1) GMT UTC time 2) signer nonce

5.2.2 Directory Interface

The WAP SignedContent signature has an option to include only references to the signer certificates. The reference in the signature is a URL pointing to a LDAP directory. JNDI (Java Naming and Directory Interface) was used to query the LDAP directories for user certificates. The parsing of the URL representation of the LDAP query presented in the RFC:s 2251-2255 [15][16][17][18][19] had to be implemented, as it is not wholly supported by the JNDI.

6. ANALYSIS AND DISCUSSION

6.1 Fulfilling The Criteria

6.1.1 Functional And Technical

The functional and technical criteria set to the system were met fully.

6.1.2 Security

The criteria set for security were met. Verification of the absolute fulfillment of all of the security requirements is difficult, if not impossible. However, the system doesn't have security holes or gaps that could be maliciously abused. In the end the security of the system will only as good as that of the WIM and certificate issuance procedures put in place by the certification and registration authorities.

6.1.3 Scalability And Performance

The criteria set for scalability and performance were met. The system was tested for performance using a Pentium III 750 MHz machine as the application server. The Oracle 8i database ran on a mid range Sun Solaris.

The tests showed that the throughput on the above platform saturated at 40 simultaneous clients to some 20 requests/s. From this an overall throughput level of some 864 000 transactions per day[1] can be extrapolated. This by far exceeds the 100 000 daily users set as the design criteria.

6.1.4 Modularity And Maintainability

The criteria set for modularity and maintainability are seen to be met. Conclusive proof of this can, however, not be produced. Practice will show how well the system will behave in these aspects as the system is taken into production use.

7. CONCLUSIONS

The business to consumer markets of tangible and intangible goods on the Internet haven't so far met the great expectations set for them. This is mainly due to the fact that there haven't been established and secure on-line payment methods that would be readily accessible for everybody. This generates a strong demand for electronic payment systems that would satisfy the security, availability and usability needs.

In general the only way to properly carry out authentication and authorization in the digital media is through the use of public key cryptography. In order to make use of public key cryptosystems in a large scale is through setting up a public key infrastructure. There are a number of problems associated with doing this – many PKI deployments have stumbled on the obstacles, the smallest of them not being the usability and user friendliness aspects – the systems should be easy to use and available regardless of time, place and whether you are doing business over the counter at a supermarket or on the Internet.

Industry organizations, the WAP Forum and the MeT Initiative, have specified a generic wireless public key infrastructure, with the goal of enabling secure mobile transactions based on a standard PKI framework. As a result of this work, there will soon be PKI capabilities in all mobile phones – people can authenticate themselves and furthermore authorize transactions by creating digital signatures using a handset and the associated wireless identity module. This makes it possible to develop payment systems on top of a standards based infrastructure that are readily accessible, inexpensive and offers a consistent user experience.

[1] Roughly estimated from the formula: 20 transactions/second* 12 hours/day * 60 minutes/hour * 60 seconds/minute = 864 000 transactions/day

The goal in the work presented in this paper was to implement an electronic payment system where the MeT WPKI framework is utilized for the authorization of payment transactions. The goal was not to implement the complete payment system but to provide the necessary interfaces towards the central functions, like balance and credit management, provided by a traditional account based system. The key task of the system is to co-ordinate the payment transactions between the actors in the scenario – the merchant, the payer and the issuer. The environment in which the system is intended to operate calls for a highly modular, high performance and scalable implementation – these criteria were emphasized in the design and implementation.

The system architecture for the Mobile Payment System is engineered according to a layered design paradigm – this approach was taken to fulfill the criteria set for security, modularity, maintainability and scalability. The application architecture is built on top of the Java 2 Enterprise Edition framework. The interfaces towards the external actors - the merchant and the payer are provided over HTTP. SOAP was used to accommodate different types of merchant system platforms. The MVC design pattern is applied in the design – the business and the database access logic are encapsulated in the Java RMI server which acts as the model, servlets coordinate the user interaction in the controller role and JSPs are used to render the user interface layouts. A relational database is used as the persistent data store.

The Mobile Payment System is one of the first efforts to harness the MeT WPKI framework for enabling secure authorization of mobile payment transactions. There is naturally a lot of room for improvements in the system, both in terms of functionality and technology. However, it can be concluded that already as such the system could readily be used for the intended purpose.

There are a number of market drivers on the mobile payment scene that are forcing the reconsidering of the current payment methods; changes in legislation, the growth of on-line commerce and the increase in on-line frauds, just to name a few. In the years to come many new attempts to offer a secure payment infrastructure will emerge. The solution presented in this paper is certainly one that works and fulfils many of the generic criteria for a 'winner' in the market. However, the technology that the system is based on is only in its first generation. It will always take a while before the attitudes and habits of large audiences of consumers change and the market becomes ready for new kind of technical solutions in the daily life.

8. REFERENCES

[1] Anon., Established players gain most out of mobile Internet, Mobile Internet, 2000, Vol. 2, No. 2

[2] Wireless Application Forum, Ltd., WAP Forum Releases, 2001, <http://www.wapforum.org/what/technical.htm>, [referenced 9 September 2001]

[3] Wireless Application Forum, Ltd., Wireless Application Protocol - Identity Module Specification, 18 February 2000

[4] Gladman, B. & Ellison, C. & Bohm, N., Digital Signatures, Certificates and Electronic Commerce, 8 June 1999, <http://jya.com/bg/digsig.pdf>, [referenced 8 September 2001]

[5] Schneier, B., Applied Cryptography, 2nd edition, John Wiley & Sons, Inc. United States, 758 pages

[6] Diffie, W. & Hellmann, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, Volume IT-22, Number 6, November 1976

[7] Puhakainen, P., Electronic Commerce: Market Estimates and Security Considerations, Licentiate's thesis, Helsinki University of Technology, 2000, 121 pages

[8] Wireless Application Forum, Ltd., Wireless Application Protocol - Public Key Infrastructure Definition, 3 March 2000

[9] Wireless Application Forum, Ltd., Wireless Application Protocol - Wireless Transport Layer Security Specification, 18 February 2000

[10] Wireless Application Forum, Ltd., WMLScript Crypto Library, 5 November 1999

[11] Wireless Application Forum, Ltd., WAP Certificate and CRL Profiles, 22 May 2001

[12] Wireless Application Forum, Ltd., WAP TLS Profile and Tunneling Specification, 24 April 2001

[13] MeT Initiative, Mobile Electronic Transactions Initiative, <http://www.mobiletransaction.org> [referenced 15 September 2001]

[14] Gamma, E. & Helm, R. & Johnson, R. & Vlissides, J., Design Patterns, 1995, 1st edition, United States, Addison-Wesley, 395 pages

[15] Howes, T. & Smith, M., RFC 2255, The LDAP URL Format, December 1997

[16] Wahl, M. & Kille, S. & Howes, T., RFC 2251, Lightweight Directory Protocol (v3), December 1997

[17] Wahl, M. & Kille, S. & Howes, T., RFC 2252, Lightweight Directory Protocol (v3): Attribute Syntax Definitions, December 1997

[18] Wahl, M. & Kille, S. & Howes, T., RFC 2253, Lightweight Directory Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997

[19] Howes, T., RFC 2254, The String Representation of LDAP Search Filters, December 1997