Holistic Personal public Eco-mobility

D3.2

Over the Air ticket issuance and mobile payment functionality concept

Project Acronym	HoPE	
Project Title	Holistic Personal public Eco-mobility	
Project Number	621133	
Work Package	WP3 Front End Services	
Lead Beneficiary	PLM	
Editor	Andras Vilmos	Bull
Reviewer	Javier García Hernández	ATOS
Reviewer	Nerea Rojas	MLCluster
Dissemination Level	PU	
Contractual Delivery Date	31/05/2015	
Actual Delivery Date	31/05/2015	
Version	Final	

Table of Contents

Table of figures

1. Document History

Version	Date	Comments
0.1	13/4/2015	Content definition / skeleton
0.2	27/04/2015	Final draft
0.9	04/05/2015	Peer-reviewed draft
1.0	31/05/2015	Final
2.0	15/09/2015	Modified document based on review comments – New chapter 5. Security and 6. Scalability

2. List of Contributors

Nerea Rojas ML Cluster
Félix Lanas ML Cluster
Gabor Avar Bull
Attila Kovács Bull
Javier García Hernández ATOS
Lorena Bourg Planet Media

Nature:

Report

Dissemination Level:

□ PU : Public
□ PP : Restricted to other programme participants (including the Commission Services)
X 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)

1. Introduction

1.1 Purpose of this document

The description of work specifies this task as follows:

The underlying concept of the HoPE platform is to provide content reach, real time transport related information and services to customers on their mobile and web based personal devices. This objective can only be realized to the satisfaction and convenience of the consumers if the overall service provisioning from information collection to ticket validation is integrated into one seamless, transparent end-to-end activity and process hiding all operating and technical details with ergonomic and function rich UI.

To realize this target the independent ticket delivery and payment functions will need to be fully integrated into the operating procedures both in the back office side and also in the mobile application of the user.

The "over the air" ticket distribution function will be implemented by a modular architecture consisting of the ticket database, the notification engine and the loader module. This independent operation will receive the user specified content from the HoPE platform and will ensure that tickets are delivered to the passenger devices securely and reliably meeting the predefined service parameters. The architecture will also have its own mobile component integrated into the overall HoPE mobile application which will ensure the secure communication between the handset and the back office and depending on the service specifics also with the secure element.

Mobile ticketing will be enhanced with mobile payment to realize a completely mobile service concept. Similarly to the ticket issuance function, payment will also be implemented in a separate architecture, more specifically with the iCheque service components. The solution will comprise a back office operation which will receive the invoice details from the HoPE platform and all steps from payment initiation to authorisation will be performed by the various service modules. On the mobile side a project library will be integrated into the mobile application to realize the inapp payment concept, where the payment function becomes an integral part of the overall application.

The operational and technical details of these complex services will be described in details in this document.

1.2 Audience

This document is first of all prepared for those transport operators, who are participating in the HoPE pilots, to provide them an overview of the services, to inform them what they and their customers should expect from the new services.

The document should also provide the initial high level technical information for all those project partners, who participate in the technical implementation of the service architecture of HoPE. The descriptions herein will provide an overview about the technical details of the service components and their relationship with the other functionalities of the platform and the overall infrastructure.

2. The overall concept

Payment and ticketing will be provided as white label integrated services, which although comprises two discrete functions will appear to both the customers and the transport operators as one single unified feature. The HoPE platform and its mobile application will transparently hide all the technical details and will provide a seamless user experience.

2.1 Payment

The Payment operation will be based on the iCheque technology.
The iCheque service is a unique, open-loop mobile payment service which can support all types of payment transactions, with using traditional bank cards as the payment instrument, supporting all major mobile operating systems and handset models.

The service can be used by any consumers having any types of bank cards from any banks, which are approved for electronic transactions by the payment networks. Customers do not need to specifically register for the service either with their own bank, or with any third party entity, the simple over the air installation process of the iCheque mobile application includes the service registration procedure as well.

On the acceptance side the service is available to any merchants or other entities, who sign a contract with the service providers of the iCheque operation. In case of the HoPE pilots Bull will be the registered merchant and will act as an intermediary between the payment service provider and the transport operators. The operators of the HoPE platform will be able to issue electronic invoices which are delivered to the consumers' mobile HoPE application and used as input information for the transactions to be paid.

The service is based on the traditional bank card payment method, however with important deviations from known, earlier approaches. iCheque is primarily for remote payment for realizing card not present transactions. However the iCheque service is more secure than known MOTO transactions as the payment authorisation is coupled with user authentication, meaning that only the persons, who registered an application for the service, can use the cards in that application and

authorize payment through the service. This added security level assures that even if the phone is lost or stolen it cannot be misused for payment by unauthorized individuals.

A further new feature of the solution is that instead of providing the payment information to the merchants, in the iCheque transaction the consumer receives the invoice and then it has full control over the payment initiation. Timing, selection of the account, and every other aspect of the payment is fully controlled by the payer.

The service is also exceptionally convenient as it can securely store the necessary information of multiple payment cards and users only need to select which card they wish to use for any specific transaction. This feature means that a payment can simply be authorized with the input of a short PIN code and still two-factor-authentication is realized.

The service is truly open and independent from multiple aspects:

- Any customer who has a debit/credit/stored value bankcard can use this service.
- The cards of any banks can be used if they are accepted by the payment networks
- The network of any mobile operator can be used for the transaction which provides data communication services, WIFI communication is also a viable alternative
- The subscription of any mobile operator can be used if it includes data plan
- A large selection of mobile handsets can be used with the iCheque application from traditional J2ME feature phones, through Android handsets, to iPhone and Windows devices.

This open service concept means that there is practically no entry barrier for the service on either the consumer or on the merchant side.

The business model of the operation combines EBPP (Electronic Bill Payment and Presentment) and bank card payment elements. The service is charging a minimal fee for the invoices which are paid through the system, and there is also the usual card commission to be paid. Merchants have the option to decide whether they want to absorb these expenses, want to levy it on their customers, or share it between them.

The iCheque service complies with all banking industry security requirements and standards. The architecture is PCI-DSS certified.

2.2 Ticketing

The mobile ticketing service does not have a specific brand. It is a white label service which can be used, deployed by different service providers for their specific purposes, for the remote distribution of their secure or basic content.

The mobile ticketing service is based on the DIAD technology. Its main purpose is to provide a bridge between the ticket issuer merchants/operators and their consumers and to facilitate over-the-air remote delivery of the tickets.

The DIAD platform does not participate in the actual generation and issuance of the tickets. Its only task is to deliver theses credentials to the designated users. Access to the platform is available to any service provider who wishes to provide remote/mobile delivery of its tickets. By using the DIAD API credentials can be reposited in the platform and the service will manage the full life cycle of the tickets from their own.
Besides ticket delivery, the platform has a number of added value services as well. It can manage payment for the credentials, and it is also capable of providing a comprehensive acceptance function. This feature can be configured to monitor specifics of the admission policy and validate credentials, according to location, time, number of entries or any other quantifiable parameters. If needed, the ticket management back office is also able to provide feedback to the service providers about the life cycle status of their tickets. Communication is also configurable, and can be defined whether all status changes get reported or only the expiration/validation of the ticket.

The service has a flexible operating and security structure which may be configured by the service providers according to their requirements.
In terms of security, tickets may be defined as basic ones, which means that although the tickets will be safeguarded in the back office, after delivery to the customers it will have minimal protection, as the credentials will be stored in a software application on the user's mobile phone, without any specific security features. These tickets may be vulnerable to fraud as cloning them would be quite simple.
Higher level protection can be achieved if the tickets will be delivered to memory cards, usually Mifare technology is used, where over-the-air communication is still not encrypted and the chip card itself is also vulnerable to attacks, but the applied technology provides satisfactory protection to most ticket types.

An even higher level security can be achieved with the use of DESFire cards, where communication is already encrypted and also the card platform is more resilient to attacks.
The highest security levels can be achieved with the use of smart card technology and the adoption of Global Platform standards, where end-to-end security is guaranteed and the Secure Element used for the storage is practically impossible to break. This architecture can also be certified for any industry specific requirements.
The differences of all these architectures are hidden from the services providers. They simply need to define their requirements and provide the input information adequately. Service providers have to specify properly the platforms in which their tickets are stored, as the right choice will ensure that the mobile tickets can be transparently validated by their legacy acceptance environment.

The end point of the "over the air" delivery service is the user's mobile handset and/or a chip card associated with this handset. Accordingly users must have a mobile phone with the DIAD application running on it and optionally also a chip card as a storage device.
In case of the basic ticket types without the use of chip cards, users simply receive the ticket content in their mobile application. It is nothing else than a virtualized version of the generic paper tickets. All information which is on the ticket is shown on the display of the smart phone, and a barcode or QR code, also shown on the screen is used for the validation/control of the credential. These type of credentials can be controlled visually or by using regular barcode readers.
In those cases when the actual content is stored on any type of chip cards, tickets have two components. One is the image of the tickets, the information which can be seen on the paper version of the tickets. This part of the information is stored in the DIAD mobile application and is presented on the display of the phone. The other part is the actual representation of the credential, which need to be protected, which data is used for validation, and it is stored inside the chip.

The DIAD service supports diverse type of consumer configurations without any influence on the service providers. Consumers may have the secure chips in their mobile phones, in the form of SIM cards or microSDs, or may have external plastic cards, JAVA, Mifare or DESFire. The only technical requirement users need to meet, is the use of mobile handsets with NFC technology and a chip which complies with the platform specification and security requirements of the services providers.

3. Interactions and processes

3.1 The payment process

1. The payment component – the iCheque .LIB – is an integrated part of the HoPE mobile application. When the application is installed on the user's mobile phone the payment feature is activated already.

2. Before starting the first payment transaction the customer is requested to define a personal authentication code which it will use in the future for all iCheque payments. With this process the consumer is ready to use the service.

3. The merchant, who has a contract with the iCheque service, issues an invoice. This invoice is sent in electronic form to the customer's mobile phone.

4. Having received the invoice details, these are presented to the user on the display of the mobile handset.

5. At this point the user may decide to pay or reject the invoice. In case the payment option is selected, the customer needs to select a card to pay with. The card information is either already stored in the handset or needs to be manually inputted. At this point the payer has the option to securely save the card information in the phone for use in later transactions or just keep it for the current transaction.

6. To finish the transaction the user needs to provide its personal code to authorize the payment.

7. When the payment is authorized, the whole information gets encrypted and is sent to the back office for processing.

8. The back office decrypt the information, carries out the personal identification based on the authentication code provided by the user and, in case of positive results, forwards the payment details to the bank for payment authorisation.

9. Following the response from the bank, the result of the transactions is provided real time to both, the payer and the payee.

The overall payment procedure should not take more than 25-30 seconds, however the actual speed primarily depends on the technical conditions of the mobile network.

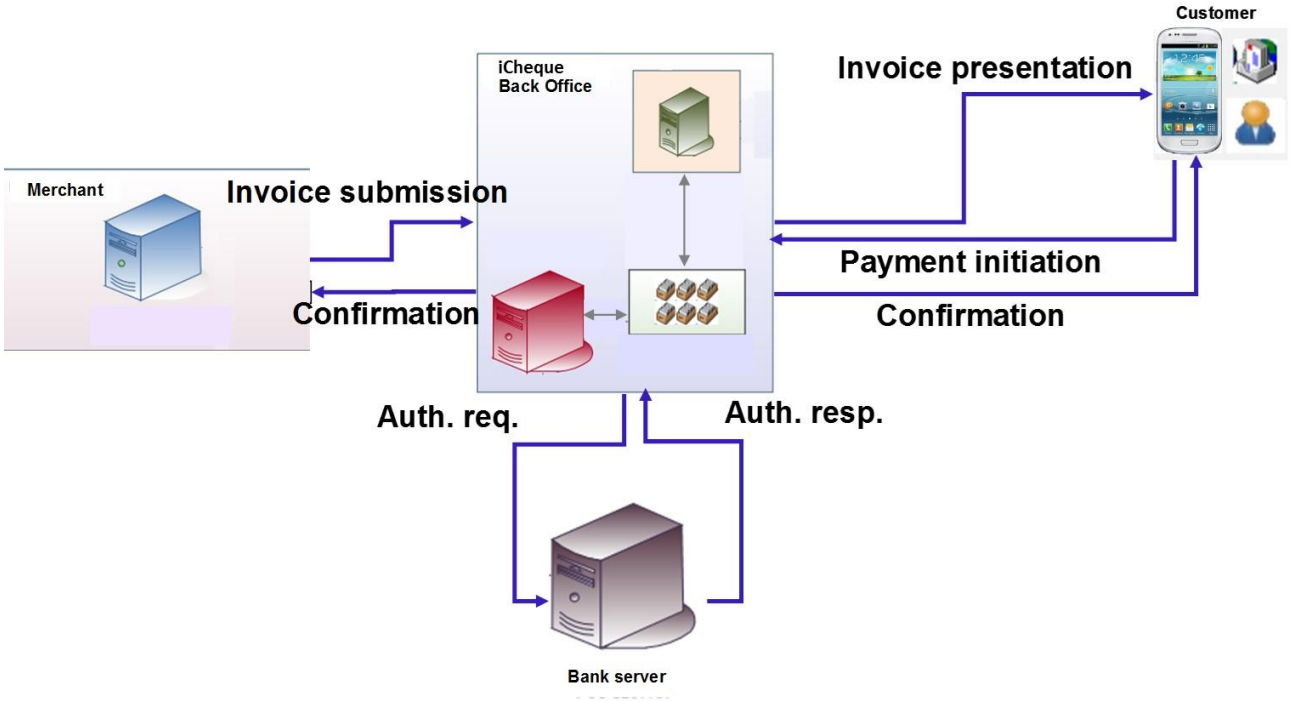

Figure 1.: The overall payment procedure

3.2 The payment back office operation

In each of the procedures explained below, several modules participate and interact with each other. The internal interactions of these modules are transparent for external partners, but some description about the architecture will be provided in Annex1.

3.2.1 Registration:

The overall iCheque operation starts with user registration.
The user establishes data connection to the back office system of the service and, as a response, receives some user specific information to be stored in the module.

In the next step of the registration process, the user must define a personal security code to be used for authorizing each transaction. The codes are sent encrypted to the back office, where the hash of

the code is stored in a hardware security module (HSM). No one in the back office is capable of re-establishing the original password. This information will be used to compare it with the hashed password sent as part of the transaction to authenticate the user.

The user's password is never stored in the handset. It must be introduced manually for each transaction. As a result a two factor authentication system is established, consisting of the user's specific information stored in the iCheque module being tide to a specific mobile handset and the personal password known by the payer only.

3.2.2 Payment

The payment process starts with repositing the invoice of the transaction in the iCheque back office system. The back office generates a transaction ID, which is returned to the HoPE platform. (Alternatively the transaction ID may be returned directly to the mobile payment application.)

When the user decides to make a payment, the HoPE mobile host application will transmit the electronic invoice to the built in iCheque payment component, the iCheque LIB.
Users can decide when to pay an invoice, and whether to pay them at all. When payment is initiated the customer needs to select the bank card to be used, and enter his password. The transaction information will be encrypted and sent to the iCheque back office. As a first step of the payment processing, the received transaction message will be decrypted using a private key for the purpose, stored in an HSM, which ensures the highest possible level of protection for the transactions.
When the payment request is converted into a plain text message, the back office performs user identification, comparing the user's security code - which is still hashed – with the hash code stored in the HSM. In case of successful user authentication, the actual payment authorization starts. If the identification fails, the transaction is rejected and the user is informed that the transaction is rejected.

Following the positive user identification, the payment request is transmitted to the acquirer bank for payment authorization. The back office has the capability to manage multiple banks and route the individual transaction according to some preset preference criteria.

When the back office receives the response from the bank, the user is informed about the success or failure of the transaction. (A failure can be caused by the lack of funds, by the rejection of the user's

card or for other reasons specified by the card schemes.) The back office also updates the transaction records and registers that a specific invoice was paid. This invoice cannot be paid any more. If the invoice is in paid status, the merchant will be informed too, in real time about the successful completion of the transaction.

3.2.3 Transaction management

The iCheque back office keeps track of all paid transactions.
Consumers can retrieve the invoices they paid earlier. The back office also ensures that users can only have access to their own records and cannot review transactions of anyone else.

The same function is used for the preparation of the financial settlement with the merchants. A detailed analytics is provided as an accounting document including each merchant invoice.

3.2.4 User management

The iCheque back office keeps track of the consumers – users of the service –, although anonymously, as it cannot identify any of its users. The back office operation complies with all security regulations, security policies of banks as well as that of the card schemes. It does not store any of the card information related to the users and does not store any sensitive personal user information either.
AML (Anti Money Laundering) and KYC (Know Your Customers) rules do not apply as the iCheque service does not manage accounts and uses only bank issued payment instruments, which have already complied with these regulations. From this perspective, the iCheque operation simply presents the invoices and processes the payment transactions.

In spite of the limited user information available in the back office, iCheque still needs to provide support for the consumers, and for this purpose the following functions are implemented.

- Users can change their security passwords anytime. They need to provide their old (current) password, and in case the user authentication was successful, the user's password will be updated.
- Users are also assisted if they forget their passwords. In this case they must renew the application stored in the handset but they will retain access to all their previous records.

3.2.5 Merchant management

While anyone can become a consumer, user of the iCheque service, merchants need to have a contract with the operation.

The back office manages also the merchant relationships. This function comprises the allocation of merchant IDs, the registration of account and settlement details as well as the management of keys to secure the communication between the merchant partners and the iCheque back office.

3.2.6 Clearing and settlement

Merchants have the option to accept card payment through iCheque, either using their own merchant accounts or the account number provided by iCheque. In any of these scenarios, there is a financial settlement between the merchant partner and iCheque.

The back office operation keeps track of the individual settlement details of each merchant partner. The back office has a merchant data base, which contains information about the account numbers of the merchants, where settlement transfers are made, about the specifics of the settlement cycles, about the invoice details to be issued for the services provided by iCheque and other relevant information about the partners' financial relationship.

The back office also prepares and transmits automatically to the merchants all the analytical underlying documentation which needs to accompany the settlement files or the invoices issued by the service. This specific transaction information is provided in standard formats, which can be imported into the merchants' various legacy systems.

3.3 The ticketing process

1. The ticketing component – the DIAD .LIB – is an integrated part of the HoPE mobile application. When the application is installed on the user's mobile phone the ticketing feature is already activated.

2. After having selected the ticket and performing a successful payment transaction, the DIAD LIB, starts automatically its operation without any user interaction.

3. The DIAD LIB connects to the DIAD back office and requests the ticket which is reposited there by the ticket issuer, waiting to be downloaded by the customer.

4. The ticket or tickets show up on the mobile handset with all information (and potentially much more) which can generally be seen on a regular ticket. At this point, the customer may decide to download the ticket or postpone this step for a later occasion.

5. If the download option is selected, the ticket information gets stored in the mobile application and, depending on the security level of the ticket; its content may also be stored in the chip associated with the mobile handset.
    a. In case the user has a SIM or micro SD, content storage is an automated procedure. The user does not need to do anything.
    b. If the user has an external plastic card with a chip, (s)he will be requested to touch this card to the NFC antenna of the smart phone and then, the content will be loaded into the chip.

       In this scenario only the card will be needed when using the ticket, the phone only provides the download capability and some convenience features.

   The successful completion of the transaction is confirmed to the user on the handset's display.

6. Stored tickets show up in a list in the ticketing application. These may be selected, activated, their content or status viewed, and eventually the ticket may be deleted.

7. When the customer wants to use the ticket, it simply must be presented to a reader – photographic, or RF, depending on the type of the credential – which collects the necessary information and starts the validation process.

   In case there are competing tickets stored – multiple tickets which are all valid in a certain operation – the customer first need to select or activate the one he wants to use, otherwise an arbitrary preference list will be used.

8. Validation in general should take only a few hundred milliseconds and the result shows up not only on the validator but on the screen of the mobile phone as well. The display shows the number of remaining entries still available with the ticket, or in case the ticket is not valid any more then it's invalid status is shown. If a ticket expires while stored in the phone the user is also notified about this change of status.

9. On a dedicated screen, the DIAD LIB also lets customer monitor the usage history of their tickets in the handset.

3.4 The ticketing back office operation

The DIAD ticketing service comprises the ticketing business logic, the "over–the-air" communication management capability and an interface to the independent secure element management operation. From an architectural perspective, these are the ticket database, the notification engine and the loader module. In the HoPE project the external components will only need to interact with the ticket management operation, with its ticket database.

3.4.1 Registration:

There is no formal customer registration for the ticketing service. The DIAD ticketing platform initially identifies the users by their MSISDN (mobile phone number). Depending on the circumstances, this information is provided either manually by the customers or the mobile LIB transfers it automatically to the back office. After this information is recorded in the back office it will be associated with the registration ID allocated to the user by the network for this particular service.

3.4.2 Ticket receipt

The ticket issuer service provider transfers the ticket to be delivered to the DIAD's ticketing database. For this communication, DIAD has a specific API which needs to be used. The information to be provided to DIAD contains the data which will appear on the mobile phone – the free text description of the ticket, with other visual elements -, the actual content of the ticket and the specific parameters which need to be checked during the validation process. The information also contains the customer's ID who has the right to download the ticket.

The DIAD back office confirms the receipt of the ticket.

3.4.3 Ticket delivery

The ticket delivery process is initiated by the LIB component of the user's mobile application. The mobile application connects to the OTA (over-the-air) service module, the notification engine

provides the user's MSISDN or RegID, and requests the corresponding ticket or tickets, waiting for the user to download them. In case there are tickets waiting for the specific customer, the corresponding ticket information is provided on the display of the smart phone and the user may proceed with the download or may postpone it. In case of tickets with only basic security level the download process is concluded here and the ticket(s) are ready to be used.

In case of secure tickets, the LIB initiates another download action, this time loading of the ticket content into the secure element of the user (the separation of the two steps is however transparent for the user). The customer is either notified about the availability of the ticket (in case of using the SIM or microSD), or is requested to present an external card where the ticket may be stored.

When the loading is completed, the new ticket will be displayed in active status in the list of credentials of the mobile app.

3.4.4 Ticket validation

Tickets may be also validated using the DIAD service. Validation is performed online using either special purpose validators or NFC capable smartphones. The reader captures the ticket content and sends it into the back office. The ticket management operation compares the ticket data with the prevailing status of the stored parameters, and responds to the validator with the result of the control. The ticket is either accepted and then, the remaining ticket value is also displayed on the validator, or rejected in which case the reason of the rejection is also shown.

In case of secure tickets, the status of the ticket is also updated on the secure element. This status update automatically activates the next valid ticket in case there are multiple tickets of the same kind stored in the chip.

The handset display also gets updated to properly show the current status information and the result of the transaction for the users.

3.4.5 Transaction management

All transaction related information is registered and stored in the back office. Tickets have an elaborated life cycle and as they move from one stage to another, this progress is properly recorded and archived. The transaction management process has multiple purposes.

In case of secure tickets, it is important to properly monitor what happens with the tickets. This information is not only important for security reasons, but also the ticket issuers may want to monitor what happens with their tickets. The status information may be provided online by the DIAD platform to the service providers.

Transaction information can also be used for analytical purposes. Detailed reports may be generated where usage patterns may be monitored. This function will provide substantial support for the service providers to enhance their customer management functions.

3.4.6 User management

The DIAD ticketing platform provides anonymous service for all its users. However users need to be identified to be able to associate a customer with its tickets and to prevent unauthorized use of someone's credentials.

For authentication purposes, either the customers' phone number or the registration ID of the mobile application is used which is a unique piece of data element associated with a specific copy of the applet on a specific mobile handset.

3.4.7 Merchant management

Merchants are the commercial partners of the DIAD ticketing service. Although the platform serves the end user customers, this service is provided on behalf of the ticket issuers, and it only has contractual relationship with the service providers.

The platform is a multi tenant operation, where the credentials of multiple operators may be simultaneously managed. Merchants can remotely communicate with the platform, reposit their credentials and receive the status reports according to the specification prepared upon configuration of the merchant connection.

All transactions of the merchants are registered and maintained in separate records, which are both used for financial and analytical purposes.

3.5 The payment and ticketing integration

In the HoPE architecture the two services are completely independent and are only very loosely connected. The connection is limited to the front-end, to the mobile application. On the back end side, both the iCheque and the DIAD modules are connected with the HoPE platform but not with each other.

In the HoPE mobile application both the iCheque LIB and the DIAD LIB are present. When payment is successfully completed then the iCheque LIB initiates the operation of the DIAD LIB, which results in the loading of the ticket into the smart phone.

There is no more connection between the two services.

4. The technical architecture

4.1 The Hope platform supporting the payment and ticketing functions

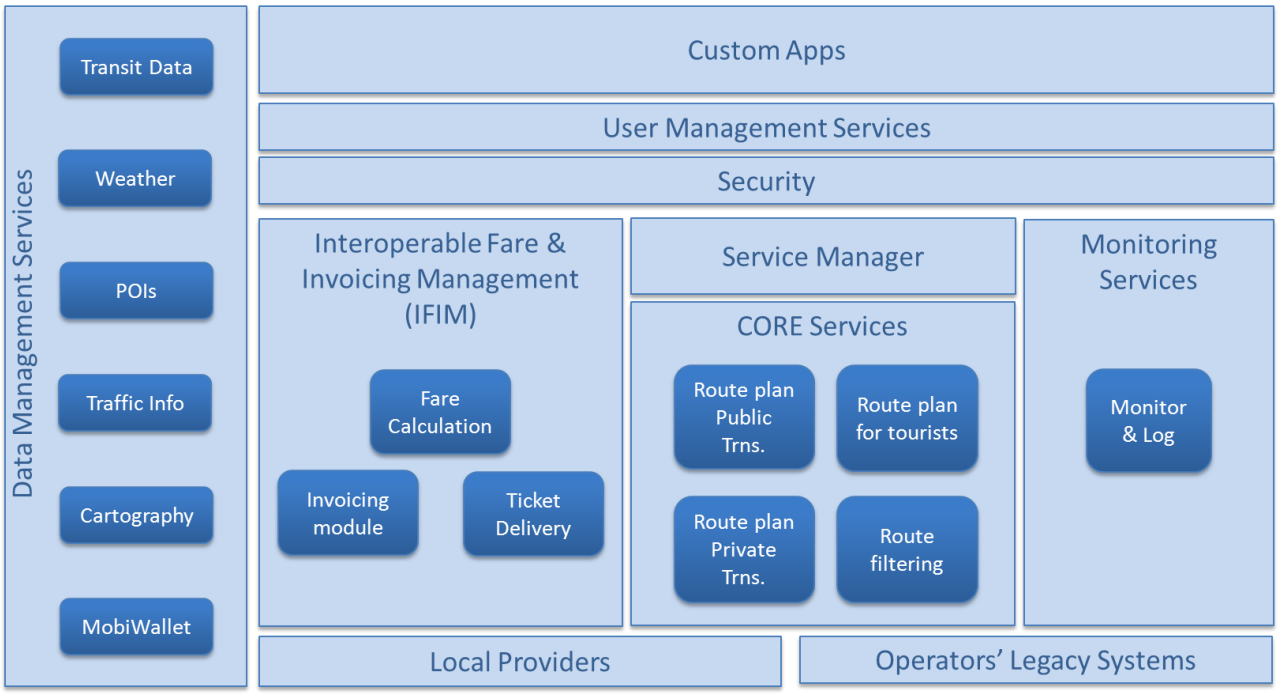

Figure 2.: The HoPE platform

The HoPE platform itself does not include the Payment and Ticketing modules. It has the Interoperable Fare and Invoicing Management component, which has the function to interact with iCheque and DIAD, but the latter two systems are independent from and external to the HoPE platform.

The IFIM has three functions which are interacting with the payment and ticketing systems.

- Fare calculation: The HoPE platform is capable to price complex routings comprising multiple legs and even multiple operators. The price of the tickets is either stored in the Fare calculation module itself or this module communicates with the legacy system of the service providers and requests the ticket prices online.
  However, when multiple operators are involved in a trip, pricing cannot be done by anyone else except the platform.
- Invoice generation: In order to let customers pay for their journey an invoice needs to be generated, and dispatched to the mobile handset. This function is performed by the invoicing module.

This module is also taking over the accounting and payment functions from the legacy system of the operators and will prepare the necessary analytics when payment settlement will be performed.

- Ticket issuance: When payment has been performed the platform either generates the corresponding ticket itself or requests the legacy system of the operators to provide the data.

These components of the platform are those modules which communicate with the iCheque and DIAD architectures to facilitate mobile payment and mobile ticket delivery.

4.1 Payment and ticketing in the front-end mobile component

The mobile front-end is an Android application which contains two sub modules, LIBs, which perform the payment and ticketing functions. These LIBs interact with the core HoPE module as well as with each other and their respective back office systems.

When the customer decides to initiate payment, the core HoPE business logic initializes the iCheque LIB, provides it the necessary transaction related information and the iCheque LIB completes the payment transaction with its back office. The iCheque LIB does not have its own brand image, it is a white label component with only four screens, one for the invoice presentation, one for the card selection, one for the PIN input and one for the payment confirmation. The LIB may also have an additional added value function which lets customers query their earlier payment transactions, and their statuses.

When payment is completed the functionality is returned to the core component of the HoPE app.

At this point the HoPE app connects to the DIAD OTA server and downloads the component of the ticket(s) which are stored in the mobile phone. When this information is stored in the phone the core HoPE business logic launches the DIAD LIB, provides it with the ticket ID and requests the loading of the secure component of the ticket into the secure element associated with the mobile phone. This interaction is completely transparent for the user. None of the functions are shown on the screen of the handset, and except in case of using external plastic cards, no user interaction is required either.

When the ticket has been downloaded, the functionality is returned to the core HoPE module. This part of the application will show the tickets and their details, which are stored in the mobile phone or in its secure element. When any action needs to be performed with the tickets stored in the chip

the core HoPE module requests the DIAD LIB to carry out the necessary function and when the task is completed by the LIB, the related status information is returned to the core HoPE module.

The ticketing LIB is completely hidden from the customers. It does not have any user facing function.

4.2 The payment and ticketing related communication

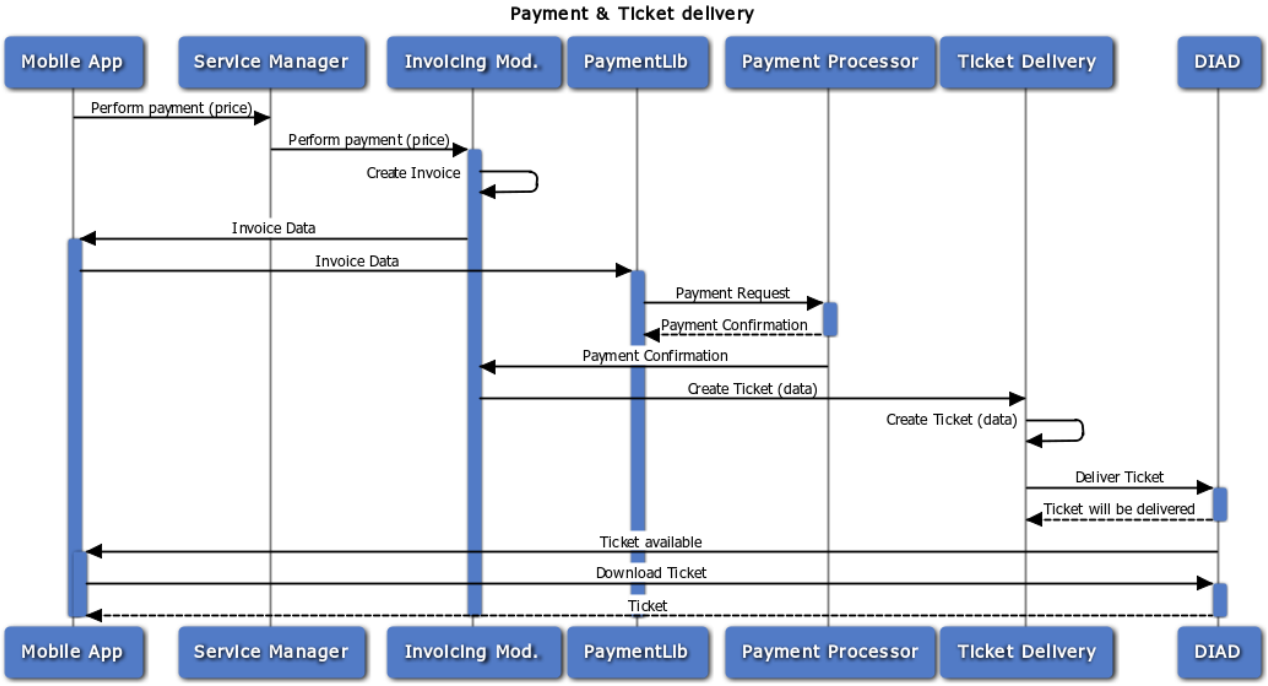

Figure 3.: Payment and ticketing activity diagram

The payment and ticketing related modules of the architecture are communicating with each other using webservice technology and XML or JSON representation format. This solution allows us simple configuration of the architecture based on the requirements of the service provider partners, their capabilities and specifics of their legacy systems.

When payment is initiated, the mobile application connects to the HoPE platform and requests the transaction details. The transaction information is either generated by the platform itself or requested and received from the legacy system of the transport operator.

The core mobile module receives the transaction information and forwards it to its built-in iCheque LIB. The LIB presents the invoice information to the customer, who selects the bank card (s)he wishes to use, enters a payment PIN and starts the payment transaction.

The iCheque LIB sends the encrypted payment information to its back office and waits for the response.

The completion or rejection of the payment transaction is confirmed to the iCheque LIB in the mobile handset.

In case of successful payment, the HoPE platform is also informed by the iCheque back office that the payment for a specific transaction has been performed.

After receiving the authorisation, the HoPE platform generates the ticket which the customer has paid for, or requests the transport operator to provide the ticket which needs to be delivered to the customer.

The ticket information is sent by the HoPE platform to the DIAD back office.

In the meantime the iCheque LIB confirms the completion of the payment transaction to the core module of the HoPE mobile app.

The HoPE mobile app connects to the DIAD OTA server and downloads the ticket which has been paid for.

When the ticket details are stored in the HoPE mobile app, the core module launches the DIAD ticketing LIB and requests the download of the secure content into the chip card associated with the mobile phone.

The DIAD LIB connects to the DIAD card management system and loads the secure credential into the secure element of the user.

When the loading is completed the DIAD LIB returns the control to the core component of the HoPE app and the payment and ticketing transaction is completed.

The interfaces used for the above communication sessions will be described in details in the deliverable *4.2 - Systems Interconnections and Communication Interfaces*.

5. Security

5.1 Payment

iCheque is a PCIDSS certified payment system, which certification is based on a review analyzing both the transaction procedures, as well as the infrastructure components.

- iCheque is more than a card not present transaction as it first identifies the user than in case of positive authentication it authorizes the payment transaction using the regular card management architecture.
- iCheque realizes two factor authentication by using the mobile number identifying the user's mobile device and the PIN known by the customer only.
- The PIN has to be entered for every transaction, it is never stored in the mobile application, also the cache memory is emptied after every transaction.
- When the PIN is controlled in the back office its hash is retrieved from an HSM, so no one ever sees the PIN in plain text except its owner, when entering this data.
- Customers can also authenticate the back office, by checking the correctness of the welcome information.
- Card details in the mobile handset are stored encrypted using RSA public key, thus avoiding the need for the use of a secure element and still ensuring very high level data protection. As the private key pair of the encryption key is not available in the phone, once saved, the stored card information cannot be modified or even reviewed, only deleted.
- All communication between the back office and the mobile device, or between the back-end partners, merchants and the bank, are secured and protected. The communication between the mobile app and the server uses multilevel combined cryptography. (More details cannot be shared for security reasons.)
- In the back office no personal information is stored. iCheque does not store names or card numbers, the only information it has on file are the mobile numbers – as user names – and the associated transaction information, which are used for billing purposes, with the merchants.
- iCheque itself does not process the transactions. The payment in this system is completed via the sponsor bank's secure web payment application. The following sensitive data elements are needed for the cardholder authentication in the VPOS payment transaction: PAN, Expiration date, CVC2 or CVV2.
- The back end infrastructure is a robust, clustered, scalable architecture with a back up system.

- There are three different architectures, one for development, one for testing and the live service environment. Migration from the test environment to the identical service environment is only allowed when all the tests were successfully completed.
- The security rules and regulations are detailed in the security policy of the company.
    - The servers of the system are in a protected area, where an electronic admission control is used.
    - The physical access to these instruments are allowed only for the operators and system administrators.
    - Each person who has access to the computer network of the company has unique ID.
    - The strength and the renewal period of the user passwords are defined in the security policy.
    - There are different persons dedicated to enter the parts of the encryption keys.
    - There is a Cisco PIX515 ASA firewall installed to protect the local network.

iCheque uses an anti-virus program on the local network called Virusbuster, which is regularly updated.

There are certain security related measures which are usual in a payment operation, but are not implemented in the iCheque system. These are fraud monitoring, KYC and AML measures. The omission of these functions is due to the specifics of the iCheque system.
iCheque is an IT infrastructure its core purpose is invoice presentation and personal authentication, it does not manage cards or processes card transactions. iCheque works closely together with its payment processor partner(S) and all the listed systems and functions are possessed and operated by the payment processor in the course of its regular payment procedures.

5.2 Ticketing

The DIAD ticketing service is based on smart card operation which defines a major part of its security environment. The level of security applied is very much dependent on the platform used for storing the sensitive content of the transactions, and the requirements of the service providers.

- The content is stored in smart card which is by default a secure medium. (The security architecture of the chip is beyond the control of DIAD.)
- The mobile application can only have access to the smart card if the application has the necessary access keys stored, and in case of SIM cards it also needs to be properly signed and the secure element access control mechanism properly configured.

- In case the content is stored on JAVA card or DesFire, then an end-to-end secure channel – VPN- is established between the server in the back end and the secure element in the mobile phone. For this purpose secure channel protocol is used which is a standard published by Global Platform.
- In case Mifare is used, only online content installation is supported and the content needs to be encrypted until the actual loading process takes place. For Mifare content only online validation is recommended, if security is of importance.
- The back office architecture is a robust, scalable environment. It has a single access structure based on ESB and a JAAS component, where all internal and external elements have certificates assigned, and can perform only those activities for which they are authorized.
- User management, and access right policy is implemented based on the instructions of a security advisor company. Some of the tasks and roles, containing these tasks are mutually exclusive, can not be assigned to a single user.
- Communication between the service provider and the DIAD back office can be encrypted if the security policy of the service provider necessitates it.
- The whole operation will have a set of manuals regulating all security aspects of the service.

6. Scalability

Scalability in case of cloud based services is a crucial issue. Both iCheque and DIAD will be made available remotely for the HoPE platform, therefore it must be assured that irrespective of the number of clients and their customers connected to the HoPE system, both iCheque and DIAD will be able to provide the necessary capacity to be able to fulfil their SL commitments.

The scaling of both systems have a structural and an architectural part.

- Communication between the front-end and the back office of both systems are using XML communication and language differences are only supported on the user side. Consequently any front-end diversity – language, personal preferences, etc. – are transparent for the uniform procedures of the back end.
- Technical diversity of the front-end is for the time being deliberately constrained by the decision that the HoPE application will be implemented only on Android platform. (IoS for the time being did not publish NFC API, and the Windows OS does not have the penetration yet, which would justify the implementation efforts.) This limitation is actually only applied for the HoPE operation as iCheque is capable of providing services for all three OSs, and DIAD for Android and IoS.
- Both systems are implemented in a multi tenant structure which means that any number of service providers can be accommodated and served by both iCheque and DIAD. On the other hand the HoPE platform may even hide the identity of the actual services provider and may be the only entity for which these remote systems will provide the service. The eventual configuration of the integration details will be defined in Task 4.2 and 4.3.
- Both architectures are clustered, and can be gradually extended as the transaction volumes make it necessary. DIAD even has an internal system which monitors systems performance and notifies personal when certain capacity thresholds are reached and more resources may need to be activated or made available.

7. Annex 1: The payment architecture

The iCheque service, primarily, consists of two major components: the mobile front-end and the back office operation.

The front-end module is an Android library which can be built in, integrated into another mobile application, where it will perform independently the mobile payment related functionality. (It would be possible to also use IOS and Windows mobile versions but the project is currently only focusing on the Android OS because this is the only platform which has substantial market coverage and provides NFC capability.)

The back office operation is not a single monolithic architecture, but consists of several sub-modules, which are performing the following functions: communication management, user management, transactions management, merchant management, front-end device management and bank relationship management, as well as the financial operation of the service.

A separate part of the back office architecture is the Virtual POS interface of the iCheque service. This interface is always defined by the acquirer bank, which is used for the transaction authorisation. As these interfaces are readily available for any of the partner banks, there is no new integration requirement on their side.

In addition to the iCheque internal environment participating billers also need to be able to issue electronic invoices. For this function billers need to communicate with the iCheque back office.

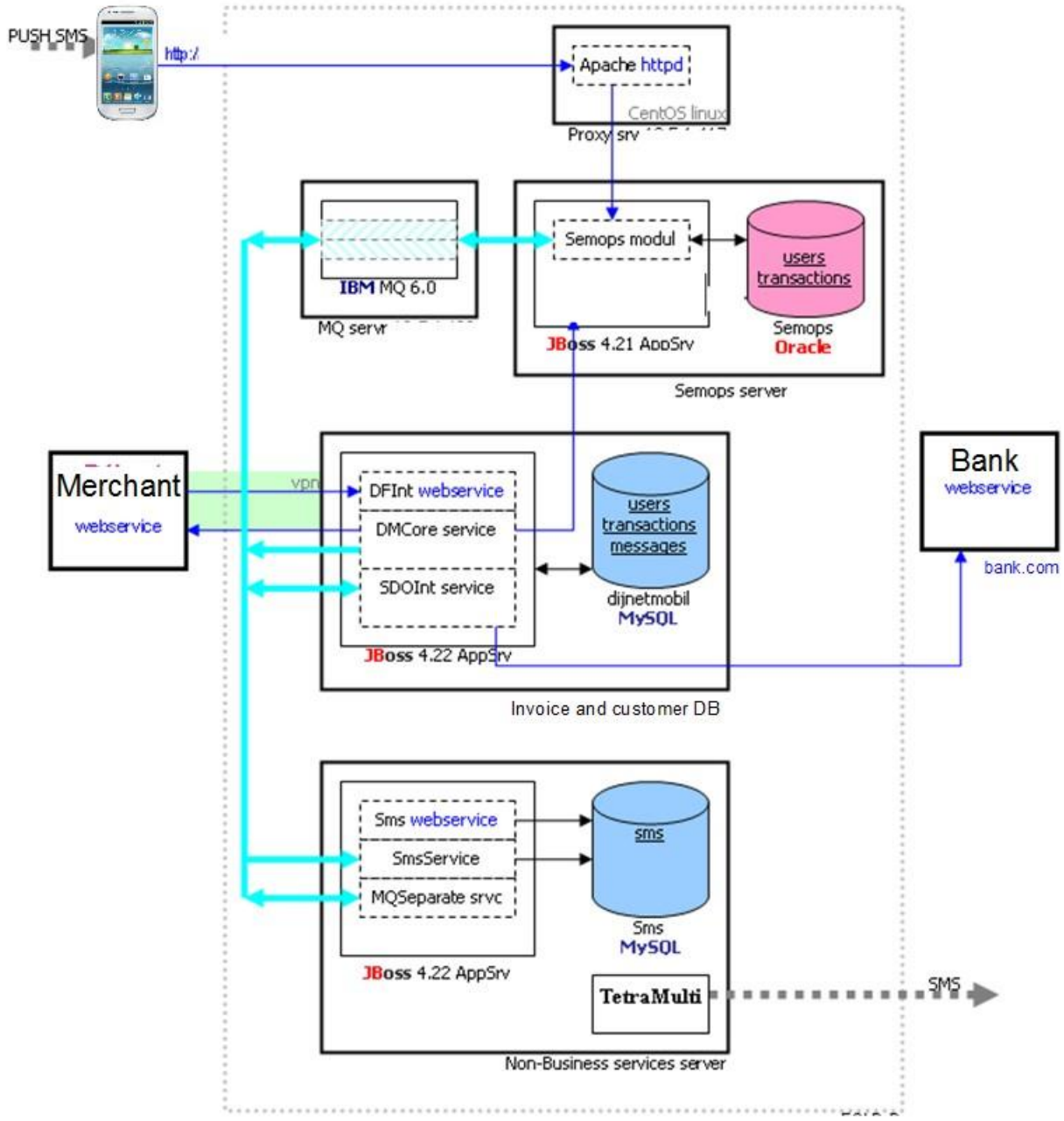

Figure 4.: Schematic view of the iCheque service architecture

7.1 Communication

The modules in the iCheque architecture, primarily, communicate with each other using webservices. Messages are represented in XML structures which allow simple integration and also modifications if necessary. In most cases, communication is asynchronous between the service modules.
For communication with the acquirer bank, the interface and protocol specification of the bank is used.

7.2 Back office environment

The iCheque operating environment satisfies all security requirements which are defined by the relevant regulations or by the partner banks and card schemes. The infrastructure supporting the service is up to the highest possible security standards and is in accordance with current accepted standards covering industrial strength and bank grade systems.

The architecture is designed with robustness and fault tolerance as primary objective. It has availability of over 99.99% which is assured by the selected hardware and software configuration and by redundant and clustered architecture of the systems. This configuration provides additional capacity when necessary and fail over features if the primary components cannot manage their functions.

Further security is provided by the elaborated operation management system where all employees having access to the service are assigned individual access rights and user privileges. All actions carried out in any of the service modules are logged in an independent system accessible only to operating management personal.
Transactions are archived daily and security copies are maintained off line.

iCheque has two identical service environments plus an additional development configuration. All improvements and modifications on the service are implemented in the development environment and tested in the demonstration configuration. The demonstration environment is the exact copy of the live service architecture. If tests are satisfying the success criteria, the new developments can be integrated into the live service operation.

The iCheque back office architecture is protected by firewalls with a DMZ. This is a three layer JAVA environment which includes application server, webserver, middleware and database application. The architecture is operating system agnostic and can be deployed in Linux, or Microsoft environment.

The webserver has minimal requirements; a simple Apache installation satisfies the needs. For application server JBOSS is used, the middleware is IBM Websphere MQ Series and the database is Oracle.

Four independent servers can provide the necessary hardware environment with each having at least dual core processors, 4GB internal memory and the transaction server a memory capacity of at least 600GB which strongly depends on the frequency of archiving.