Author: rupp,scd
Project:TicketRestaurantUS
Date: 07/27/13

TicketRestaurant US Design Specifications

Table Of Contents

1.Introduction....2
1.1.scope....2
2.System Overview....2
2.1.Workflow....3
a)card issuance....3
b)card use....4
c)card refill....7
3.Payment Card....8
3.1.Magnetic Stripe-based card....8
3.2.Virtual payment card....8
4.POS....8
4.1.Standard POS....8
4.2.Smartphone-based POS....9
a)with the physical payment card....9
b)with the virtual payment card....10
5.Backend....10
5.1.Gateway....10
5.2.database....11
5.3.Secure channels....12
5.4.PKI of the system....14
5.5.HSM....16
5.6.Transaction security and authorization method....16
a)Protocol....16
b)Certifications....16
6.Website....16
7.Integration with Company, card Issuer and Shop backend....17

Illustration Index

Illustration 1: Payment Card Issuance....4
Illustration 2: Card use in the case of Virtual Payment Card....6
Illustration 3: Account refill....7
Illustration 4: Physical POS prototype....9
Illustration 5: card reader for smartphone model #2....10
Illustration 6: card reader for smartphone model #3....10
Illustration 7: card reader for smartphone model #1....10

Illustration 8: Security tasks of the Gateway.....11
Illustration 9: Database security.....12
Illustration 10: secure SSL channels between backend and devices.....13
Illustration 11: Rough Principle of Mutual Authentication for transaction processing.....15

1. Introduction

This document describes the design specifications of the TicketRestaurant US system.This do not covers the detailed techniques for implementation which are described in separate documents.

1.1. scope

The scope of this project is to provide a payment system that allow a customer to pay in a network of partner shops, which shops will mostly sell food. The customer will be given virtual credits on his payments means by the company where he is working. This company will subscribe to TicketRestaurant US website.System Overview.

2. System Overview

The whole system is composed of the following entities:

- *the backend, which stores the data and authorize or not the transactions*
- *the gateway, which allows connections between the payment card, the POS and the gateway*
- *the POS, which is the Point-of-sales machine that will process locally a transaction*
- *the payment card which is the payment mean from the cardholder*

The actors of this system are :

- *the cardholder, this is the customer, employee by a company that have subscribed to ticketrestaurant US and that will buy goods (usually food) in the shops from the ticketrestaurant US network. This customer works for a*
- *the cashier, this is an employee from a shop from the ticketrestaurant US network.*
- *the card issuer - ticketrestaurant US- this is the authority that manage the payment cards*
- *the company, this is a corporate entity that subscribes to ticketrestaurant US offer and*

receive payment cards for its employees.

2.1. Workflow

a) card issuance

The company registers to the card issuer services either by a website, either by postal mail, etheir by phone, etc...

The Card issuer then issue a group of payment cards who are either mailed to the company in the case of physical cards, either downloaded via links if they re virtual payment cards.

Then these cards are given to the relevant employees by the company.

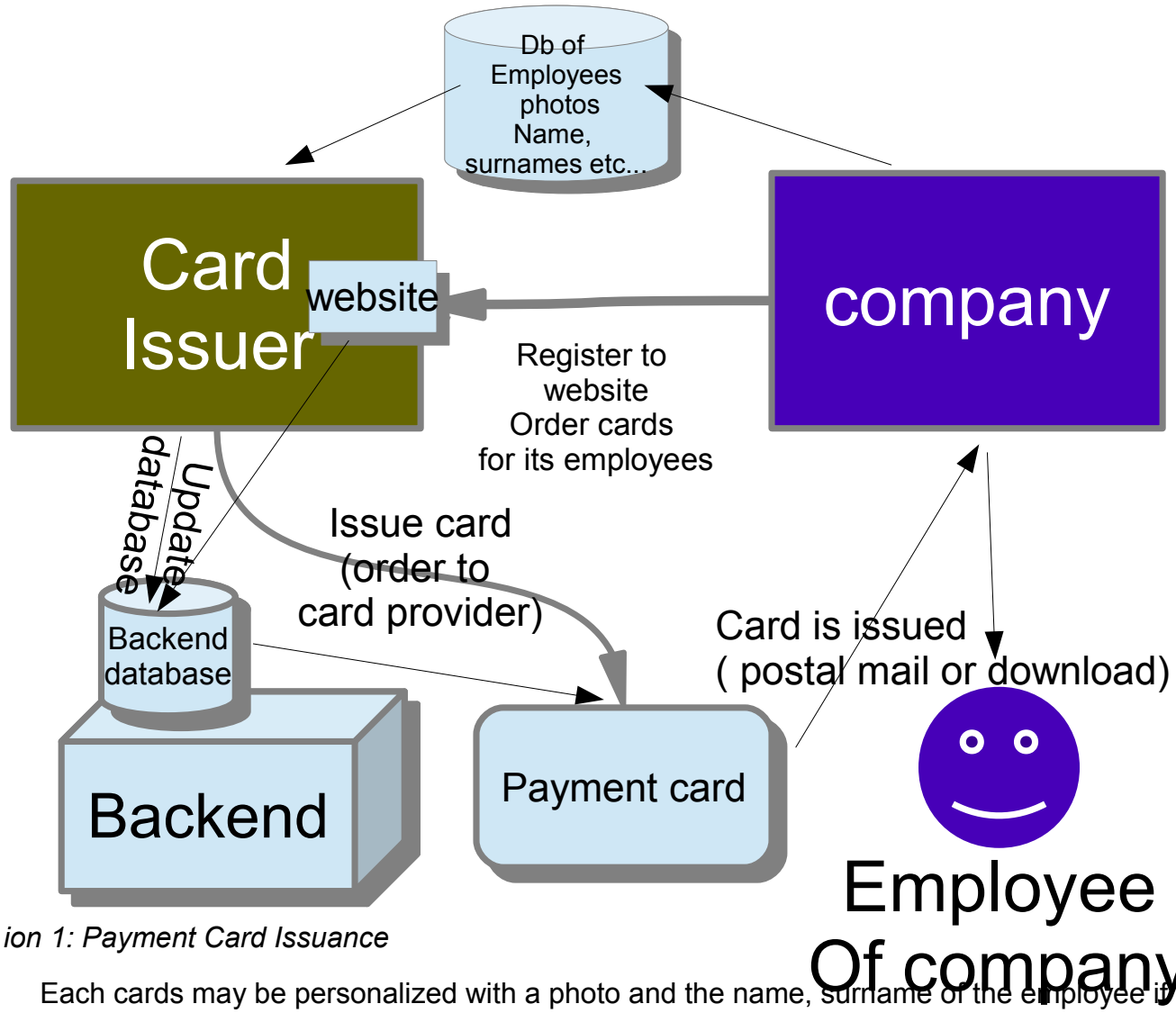

Illustration 1: Payment Card Issuance

Each cards may be personalized with a photo and the name, surname of the employee if the company sent a file with all these details.

b) card use

- In the case of a masgstripe-based card, the card will be presented to a restaurant/shop employe and this cashier will compose the menu of the cardholder. Then the card will be read by the POS and the amount and data of the transactions will be submitted to the backend (through the gateway). In this case the POS may be ither device designed and mabufactured by the card Issuer or a smartphone provided with a custom Magstripe Reader and a POS application. In all cases the backend will analyse the data received from the POS and will answer by a yes/no in order to give authorization for the transaction. If a Yes answer is received, the cashier will give the items to the cardholder- the employee of the subscribing company.
- In the case of a virtual payment card, which will be presumably a smartphone application. The Cardholdler will compose the menu either by looking directly at the items displayed inside the restaurants/shop , either by using a list of items proposed by the shop and displayed on his smartphone using a custom application provided by the card issuer.These data will be sent to the POS using the gateway. These data won't transit throught the backend at this stage. The POS will receive the data and the cashier will confirm them. This will send data for a transaction to authorize to the backend. The backend will reply with an authorization code: yes or not and will send this answer both to the POS and to the Cardholder phone. If a Yes answer is received, the cashier will give the items to the cardholder- the employee of the subscribing company.

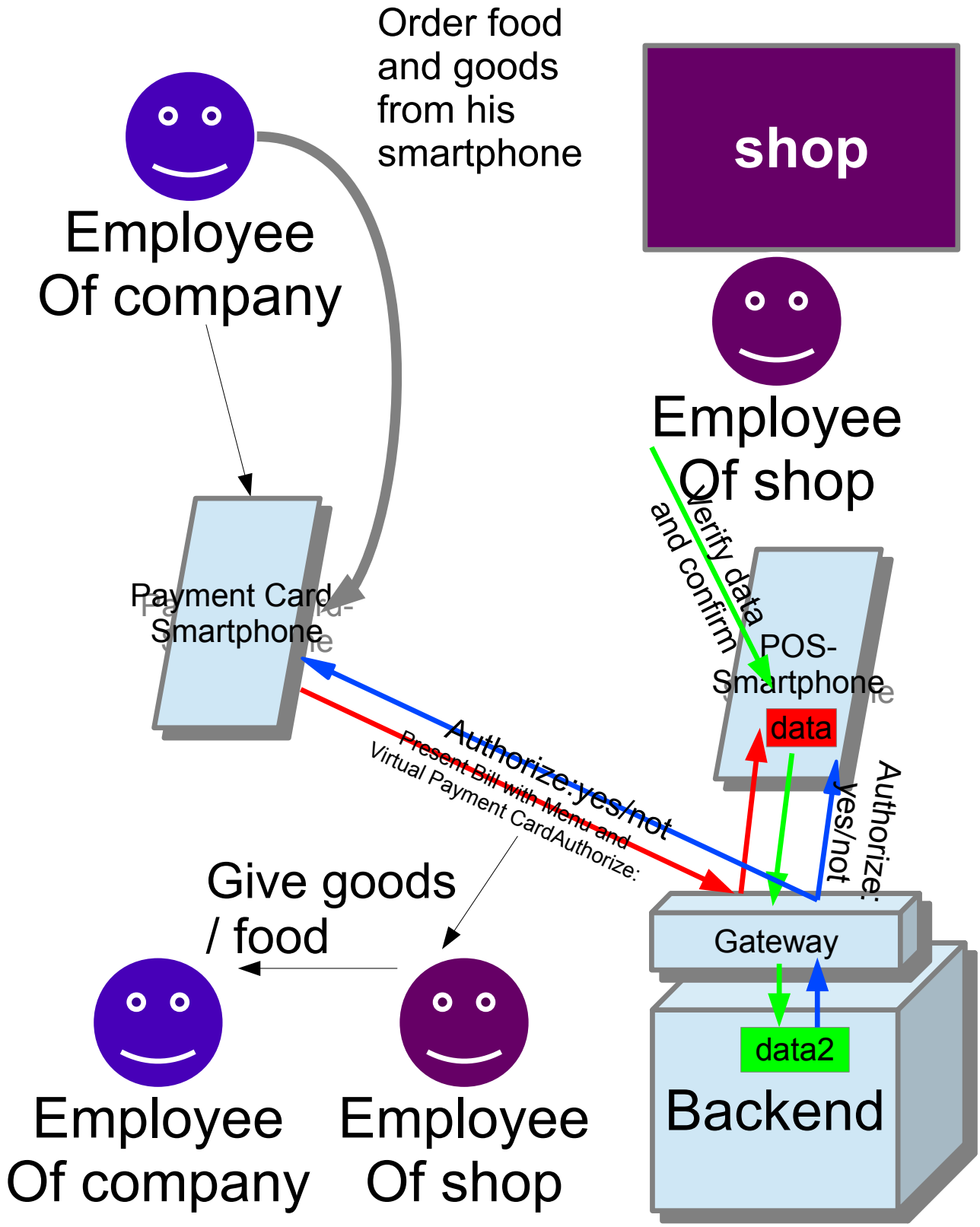

Illustration 2: Card use in the case of Virtual Payment Card

c) card refill

A card refill is done by the company. This will load a series of accounts with credit . This refill may be done manually via the website or automatically using payments means from the company (credit card, Bank transfer,Checks paypal...). In the case of credit card payment, A credit card processsor module from the website will automatically process the company credit card at given intervalls and send information to the backend adequately, in the case of a bank transfer, checks or non-automatic payment means, an operator from the card issuer will have to manually submit a refill to the backend via the website admin interface.

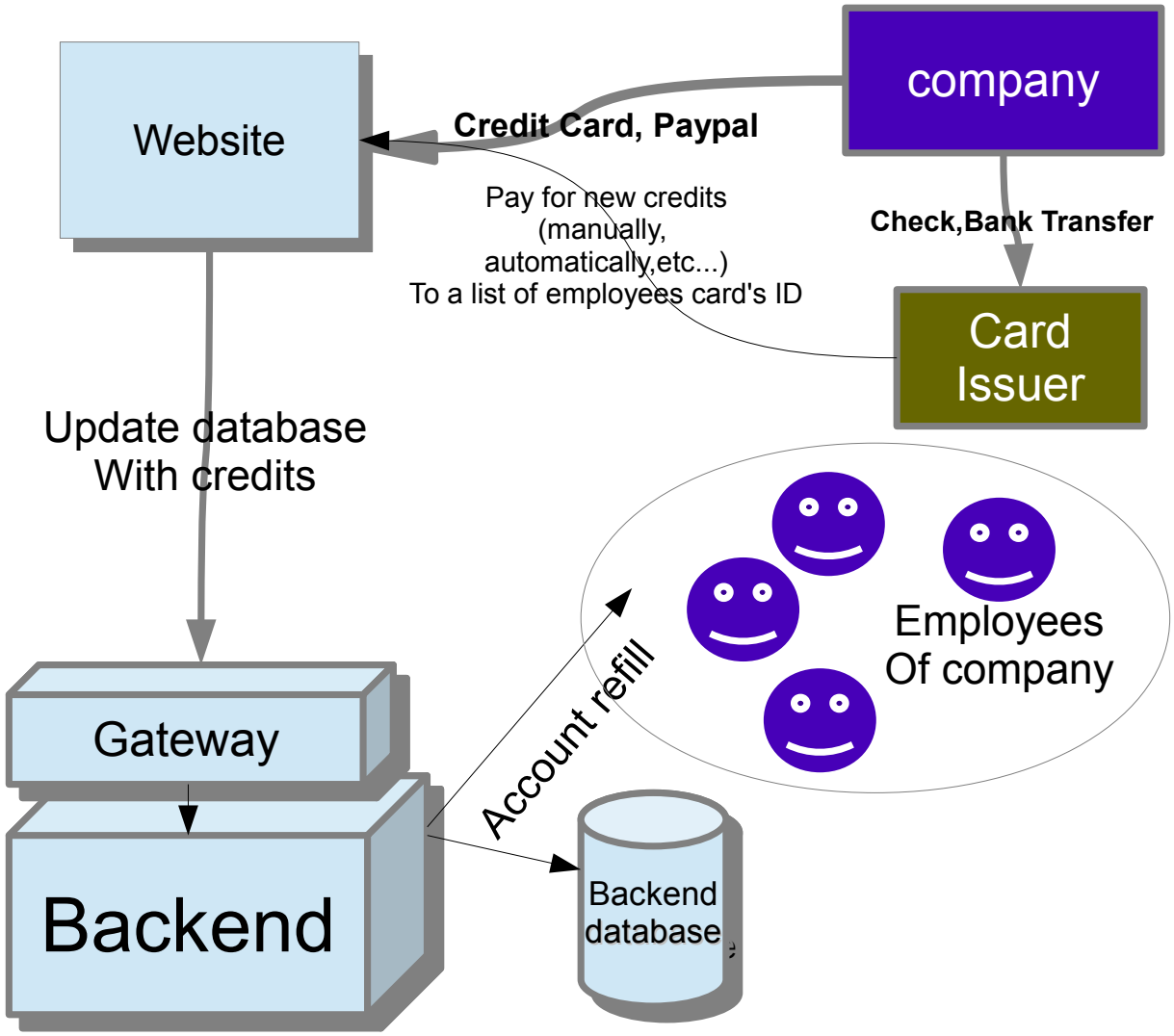

Illustration 3: Account refill

3. Payment Card

3.1. Magnetic Stripe-based card

The Magnetic Stripe Card is a standard ISO17811 and ISO7810 card with a magnetic track. (see [ISO7810-11])

The card will be personalized with customer data identity, the account id and eventually cryptographic data.

WARNING:The card can be cloned since magnetic tracks do not offer any protection against card cloning.

The detailed specifictions and data format are described in [TR-CFS], section 'Physical Payment Card'.

3.2. Virtual payment card

The virtual payment card will represent a Magnetic-based stripe card as an application on a smartphone. The same data will be used but will be stored on the SmartPhone memory.

Besides this the smartphone will be loaded with a module that allow to send the virtual magstripe data to the backend.

This virtual payment card will use a SSL certificate and a TickerRestaurantUS certificate.

The detailed specifictions are described in [TR-CFS], section 'Virtual Payment Card'.

4. POS

4.1. Standard POS

The POS will be designed and manufactured by the present contractor. This POS would have the shape of a smartphone (e.g a small box) , be equiped with a pinpad, a magnetic card reader, a few leds, a digital text-only screen , internet connectivity (ethernet – wifi or 3G) and a usb entry.

The POS would be a low-cost POS with very simple operating system based on an cheap

board system (cortex for example). The customer could see the result of an authorization by looking at the screen and the leds. The POS will not be equipped with a paper printer but will allow the user to manage and download the invoices as pdf documents to a usb flash.

The POS would be similar to a banking card POS but would be much smaller, much simpler to use and totally independant from the banking network.

Illustration 4: Physical POS prototype

The certificates and keys shall be securely stored in protected component such as secure Eeprom for example.

The detailed specifictions are described in [TR-PFS] section 'Custom Physical POS'.

4.2. Smartphone-based POS

This is in the case when a custom physical POS won't be used. Instead of this, a smartphone (Android or Iphone) will be used in two different possible ways :

a) with the physical payment card

The smartphone is provided with a custom small card reader that can be plugged to the smartphone using the audiojack entry. This allows the smartphone to act as a POS that can process a magnetic stripe.The POS is a program installed in the smartphone that will process the data received from the card and send them to the backend. This program will be identical

to the program in the physical custom POS and will allow management of bills at pdf format.

Illustration 7: card reader for smartphone model #1

Illustration 5: card reader for smartphone model #2

Illustration 6: card reader for smartphone model #3

In both case The certificates and keys shall be securely stored in protected component such as the sim card ideally or protected memory on the phone (if it may be found).

The detailed specifictions are described in [TR-PFS] section 'Smartphone POS'.

b) with the virtual payment card

In this context, the smartphone of the client is used as a virtual payment card and the smartphone of the shop is used as a virtual POS and the card communicates to the POS only by internet remote connection.

The restaurant downloads and install a virtual POS application on his smartphone. This application will have the same features and visual interface than the other types of POS mentioned above. The only difference comes from the fact that the POS receives data from the customer that includes also the prices and items of the transactions.

The detailed specifictions are described in [TR-PFS] section 'Smartphone Virtual POS'.

5. Backend

The backend is a remote highly-secured server that will process all incoming transactions and answer with an Authorize code.

5.1. Gateway

The backend is accessed from the devices only through a gateway which functions are to provide a unified way of connecting the devices together, given the variety of devices connecting to internet , and also to provide a front-end with security features to prevent unauthorized access such as:

- *firewall*
- *packet traffic analyzer*
- *antivirus and protection against network and software attacks*
- *regular scan of the network, network administration and maintenance*
- *filtering by IP*
- *filtering by device fingerprinting*

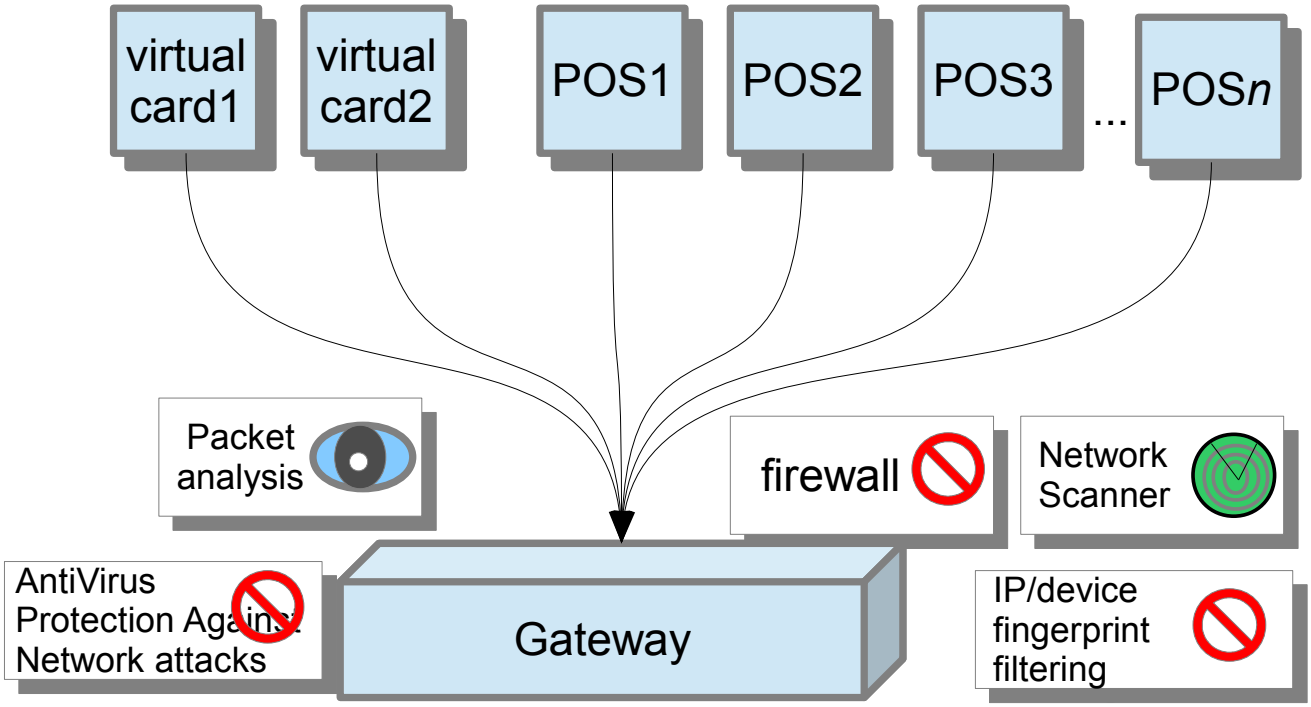

Illustration 8: Security tasks of the Gateway

The detailed specifictions are described in [TR-WGFS].

5.2. database

The backend manage a database which is itself secured and ciphered.This database hosts all the relevant tables to store the informations from the transactions, the card user accounts and all other cryptograhic data.

- *The database is ciphered and can only be accessed and deciphered by the backend.*
- *The key K_DB needed for deciphering the database are stored in a HSM (see later).*
- *This database may not be accessed directly from the web but only from the backend mechanisms, which backend cannot be accessed by anything else but the gateway.*

The detailed specifications and tables definition are described in [TR-DBFS].

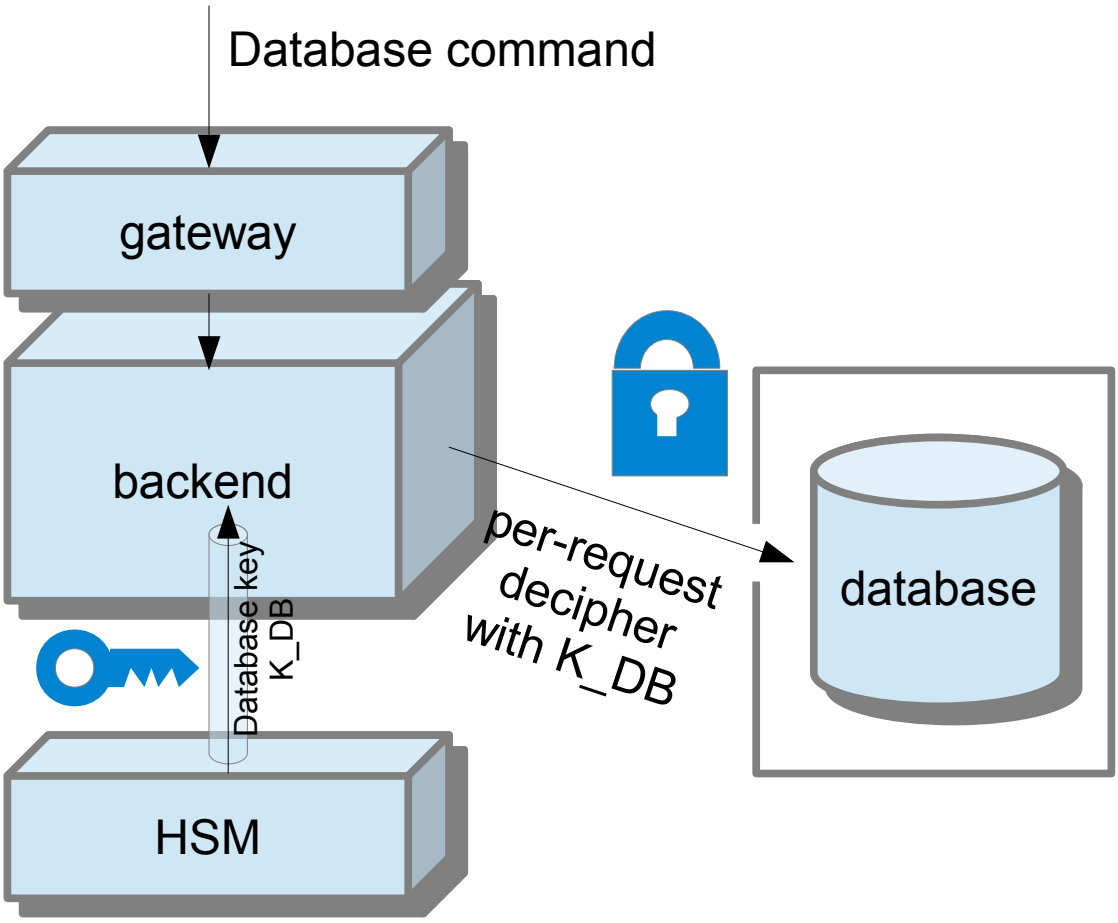

Illustration 9: Database security

5.3. Secure channels

The communication between the devices and the gateway – or device -to-device – must be done through a secure channel an end-to-end ciphered communication channel that

authentify with certainty the two entities and prevent any sniffing or interception through a Man-in-the-middle-attack for example. For this it may be enough to use a proprietary two-ways SSL implementation with a given certification authority (Comodo, GoDaddy,etc...) so that both devices, gateway and backend would be provided with PKCS#12 certificates. Mutual authentication device – device and device-backend is ensured through this system. This is independent of the own Backend PKI system done for validating the cardholders and the shops.

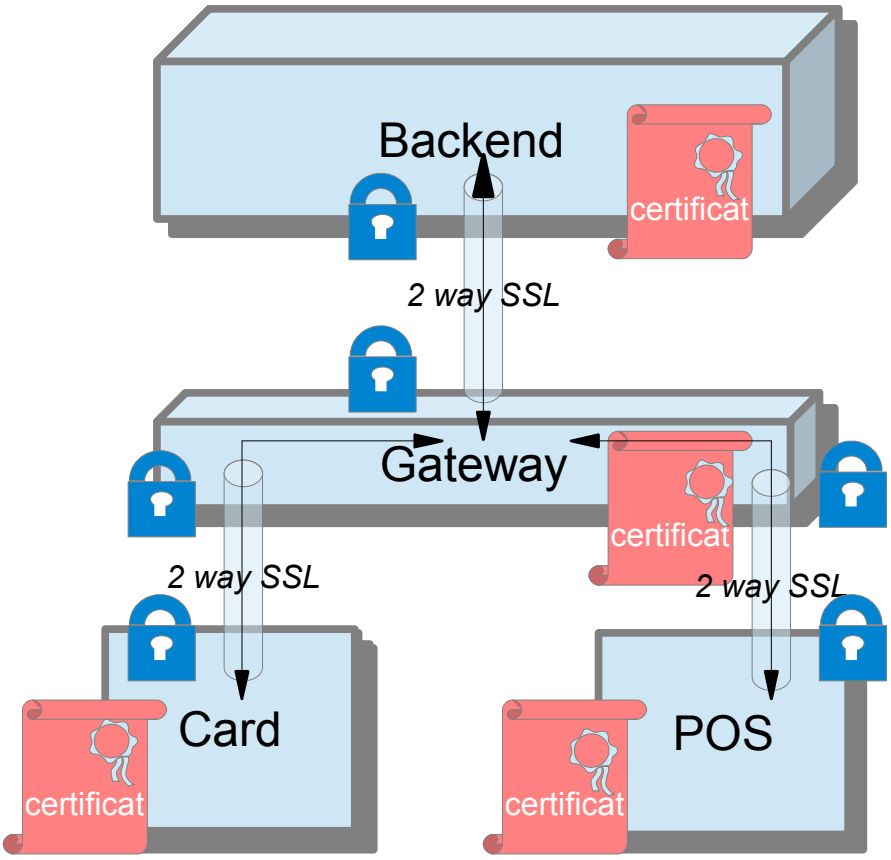

Illustration 10: secure SSL channels between backend and devices

The detailed specifictions are described in [TR-BEFS]

- *one SSL certificat for the POS systems wich will be provided to any POS system (box or smartphone-based). This certificate is the same for all the POS.*
- *one SSL certifcate for all the virtual payment cards. This certificate is the same for all the virtual payment cards.*
- *One SSL certificate for the backend*

- *one SSL certificate for the website*
- *one SSL certificate for the gateway*

In the POS and the virtual payment card, the certificates are managed only by the applications and never by the users. The implication install, deinstall and manage the SSL certificate. This SSL certifivte must be stored in a secure location like the SIM card EEProm (for smartphones) or secure EEProm (for Boxes) to prevent someone de-assembling the smartphone program and stealing the SSL certificate.(note that the gateway has additional protection besides two-way SSL to prevent unauthorized access)

5.4. PKI of the system

We will deploy a private PKI system in the whole network using a CA (Certification Authority) scheme. This PKI will be used inside the card issuer proprietary transaction and protocol to guarantee the *individual* identity of the devices.

This private PKI system will be made of

- *A certification Authority*
- *A validation Authority (inside the CA) to register and verify the identity*
- *A certificate directory*
- *A policy*

The PKI system will be a module of the backend. During website registration and after validation (the validation authority will perform automatically the checks) , the CA will issue an individual certificate either for a new POS or for a new Virtual Card (The gateway and the website will have a certificate too but they will almost never change) and provide securely this certifcate during the application installation process. (certificate will be downloaded by the POS or the virtual card application). Certificates will have to be maintained and updated. This certification system will ensure the identity, the uniqueness and the integrity of a given transaction between a cardholder and a restaurant/shop since every certificate and keypair will be unique.

The certificates and the related keypairs (A X509-certificate is roughly a public key signed by a Certification Authority and wrapped with extra-data such as validity date etc …) will be issued and created too. Certificates and related keypairs won't be stored in the database but in a HSM once they have been sent for application personalization.

In a classic PKI system, the devices will present their certificates to ensure the identity of their public keys and will use their key pairs to cipher,sign,decipher and verifiy signature of the messages in a mutual authentication scheme.

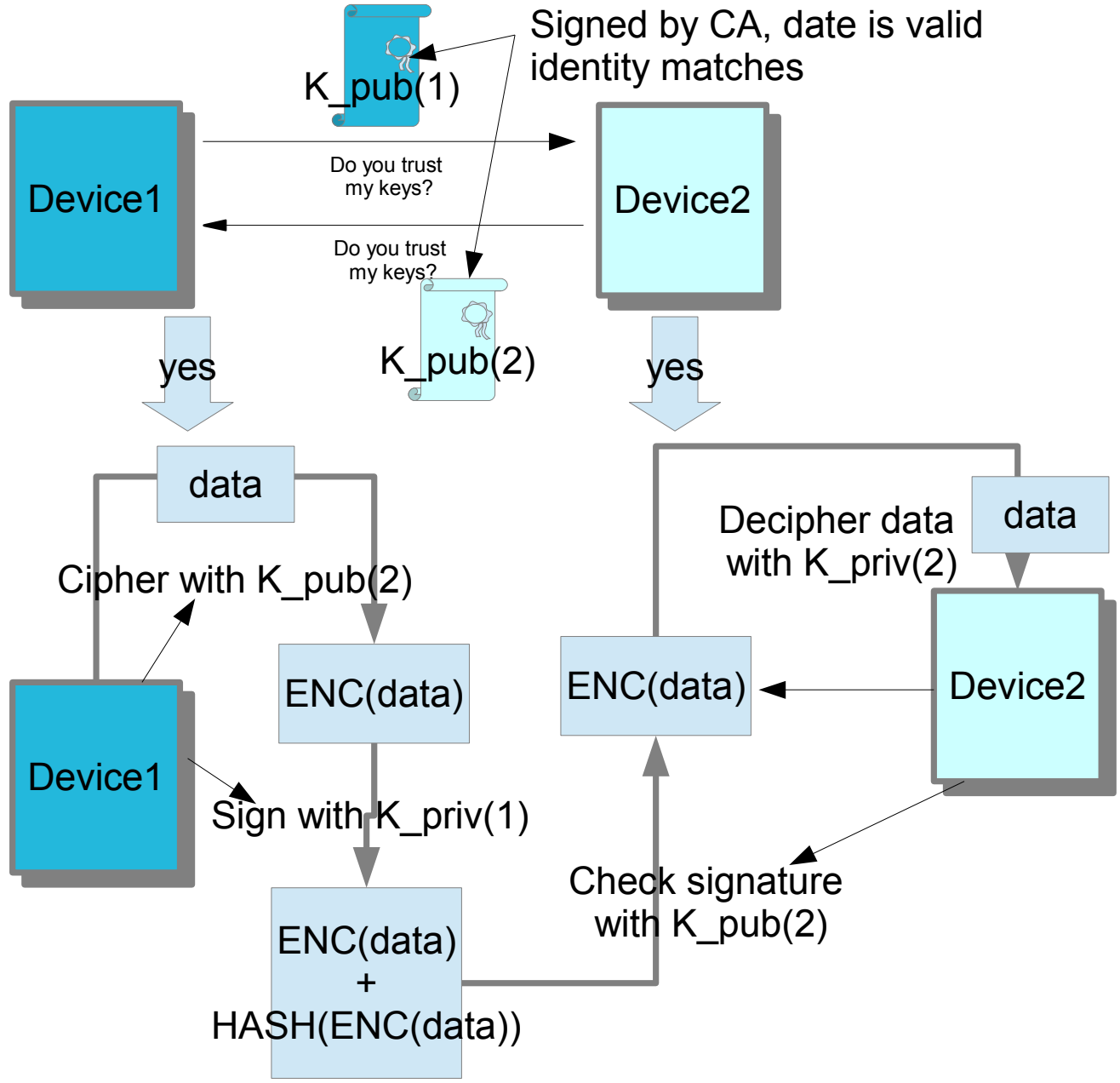

Illustration 11: Rough Principle of Mutual Authentication for transaction processing

The exact description of the mutual authentication scheme wich uses dynamic key generation and a variant of the above standard protocol is described in [TR-TPR].

5.5. HSM

A HSM (Hardware Security Module) is used by the backend to store the certificates, the keypairs and other cryptographic data. This HSM may be provide by a third party (example: a HSM hosting provider), may be hosted and maintained by the Card Issuer-TicketRestaurantUS (note: HSM are expensive machines) or even a software-based virtual HSM may be used, using a physical smartcard to store a root keypair to get access to all the other certificates (this is not recommended in case of extensive use). Finally a 100% software based HSM totally compliant with PKCS norm may be used , while it won't be as secure as a real HSM.

5.6. Transaction security and authorization method

a) Protocol

To enable processing of the transactions, a custom protocol will be used. This protocol will be secured by the private PKI of the system and it will transported through secure channels between the members of the network.This protocol will be text-based and will consist of messaging containing several types of messages:

- *Information (information about the state of a transaction)*
- *Data (data needed like cryptograms)*
- *Commands (orders : process transaction, authenticate, authorize,present PIN,etc...)*

This protocol commands and the transaction workflow is described in complete details in [TR-TPR].

b) Certifications

Security tests such as penetration testing should be conducted on a regular basis. PCI-DSS norms (see [PCI-DSS]) should be used as a basis to design and implement the system. Ideally PCI-DSS certification should be seeked fo the whole system.

6. Website

The website is a standard website with a public and an admin interface. It allows shops and restaurants to log-on and to look at their records and bills, and to view payments.

The user access does not allow modification of the system, the website gets informations from periodical reports that are issued by the gateway, the only interaction with the backend is

1) *for initial registration: the shop or company follows a complete process that may be*

checked by a human operator or not.This will triger an automatic personalization process which is detailed in [TR-TPR] in section “personalization”.

2) *For payments. If the payment is automatic, the website issue the data to the backend (note: the creditcard processor may be directly handle by the backend as a variant). If the payment is manual and have to be validated by a human operator, the update is sent to the backend.*
3) *For maintenance by the administration: card deletion, records update etc...*

The admin access from the website should require strong authentication (ideally with an additional certificate or a smartcard containing a certificate).

The details and screens are in [TR-WGFS].

7. Integration with Company, card Issuer and Shop backend

Usually the backend will issue reports of the transactions (for example CSV data or pdf) and they will have to be integrated with the company financial system. The backend (through the Gateway) could also issue XML reports to a given email address or to a given server but this would need to be defined during practical integration.

The card Issuer will maintain its own financial records from the backend informations(gains, etc...) and issue the payments using checks or bank transfer to the Restaurants perdiodically.

This integration will necessitate to write a custom specification during concrete integration.

Bibliography

ISO7810-11: International Organization for Standardization (JC 17), ISO 7810-ISO17811 Identification cards,International Organization for Standardization
TR-CFS: Martin Rupp, TicketRestaurantUS - Card Functional Specifications,SCD
TR-PFS: Martin Rupp, TicketRestaurantUS - POS Functional Specifications,SCD
TR-WGFS: Martin Rupp, TicketRestaurantUS - Website and Gateway Functional Specifications,SCD
TR-DBFS: Martin Rupp, TicketRestaurantUS - Database Functional Specifications,SCD
TR-BEFS: Martin Rupp, TicketRestaurantUS - Backend Functional Specifications,SCD
TR-TPR: Martin Rupp, TicketRestaurantUS - Financial Transactions Functional Specifications,SCD
PCI-DSS: Payment Card Industry Security Standard Council, ,Payment Card Industry