INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

VISCA

Virtualization of Smart Cards

"D2.1. State of the Art and Uses Cases report"

Change History

Version	Date	Description	Affected Sections
V0.2	27-11-2013	State or the Art and Use cases. First Version	
V0.3			
V0.4			
V0.5	08-05-2014	Update on Cloud Technologies	2.2
V0.6			
V0.7			
V0.8			
V0.9			
V0.10			

List of Contributors

Participating Entity	Contributing Individuals
Planet Media	Javier Valero, Álvaro Muñoz
ETRI	Young Woo
LKComms	Ho Lee
Kyung Hee University	
ITI	Sergio Talens-Oliag

Table of Contents

1 Introduction

The objectives of the deliverable D2.1 are multiple:

- To describe the current state of the art related to ViSCa Background and Secure Technology.
- To define User's cases enabling definition of various business models applicable within the project focus.
- To identify actors and stakeholder of the defined applications.

2 Technology

2.1 Smart Cards

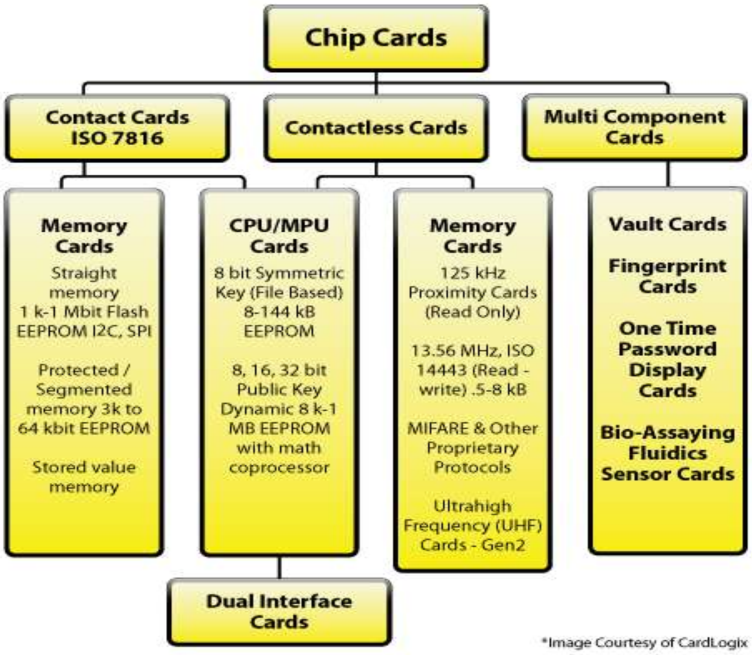

Chip Cards
Contact Cards ISO 7816
Contactless Cards
Multi Component Cards
Memory Cards
Straight memory
1 k-1 Mbit Flash EEPROM I2C, SPI
Protected / Segmented memory 3k to 64 kbit EEPROM
Stored value memory
CPU/MPU Cards
8 bit Symmetric Key (File Based) 8-144 kB EEPROM
8, 16, 32 bit Public Key Dynamic 8 k-1 MB EEPROM with math coprocessor
Memory Cards
125 kHz Proximity Cards (Read Only)
13.56 MHz, ISO 14443 (Read - write) .5-8 kB
MIFARE & Other Proprietary Protocols
Ultrahigh Frequency (UHF) Cards - Gen2
Vault Cards
Fingerprint Cards
One Time Password Display Cards
Bio-Assaying Fluidics Sensor Cards
Dual Interface Cards

*Image Courtesy of CardLogix

Smart Cards**, also known as** Integrated Circuit Cards**,** currently are the most widespread type of cryptographic devices. Smart cards are defined according to how the card data is read and written and the type of chip implanted within the card and its capabilities. There is a wide range of options to choose from when designing a system. **Each year billions of Smart Cards are produced world-wide, mainly for standard application domains like** Telecommunication, Banking, Health, Identification, and Pay-TV, but also for upcoming applications, e.g. in the Machine-to-Machine domain. The most characteristic feature of Smart Cards and related devices is security. A Smart Card is a tamper-resistant device, whose microprocessor controls the access to data stored on the card.

These data are protected by cryptographic methods and applications implemented on the card microcontroller. Accordingly, Smart Cards are mostly used for functions related to security, including **authentication**, **identification**, **management of encryption keys**, **signatures**, and **secure data storage**. For applications with **high security requirements**, like for instance a qualified signature on an ID card, Smart Cards have to pass rigorous security evaluations, usually following a certification process defined by Common Criteria.

Even though the first mass deployment of Smart Cards dates back to the early eighties, the technology is still evolving**. In recent years, new form factors as well as high speed interfaces based on USB or MMC have been developed and standardized for several Smart Card application domains**.

Virtual Smart Cards

Virtual Smart Cards (VSCs) emulate the functionality of traditional Smart Cards, but instead of requiring the purchase of additional hardware, utilize technology which users already own and are more likely to have with them at all times. Theoretically, **any device which can provide the three key properties of Smart Cards** (non-exportability, isolated cryptography, and anti-hammering) **can be commissioned as a VSC**, though the virtual smart card platform **is currently limited to the use of the Trusted Platform Module (TPM)** chip on board most modern PCs.

Virtual smart cards utilizing a TPM provide the three main security principles of traditional smart cards (non-exportability, isolated cryptography, and anti-hammering, as discussed above), while also being less expensive to implement and more convenient for users. However, TPMs, in contrast to smart cards, are rather bound to computing platforms and not to people.

Comparison between Virtual Smart Cards and Conventional physical Smart Cards.

Technical characteristics

Virtual Smart Cards function much like conventional Smart Cards, but differ in that they protect private keys using the TPM of the PC instead of smart card media. The TPM is utilized through a virtualized smart card and reader, and so appears to any applications as a conventional smart card. Private keys on the virtual **smart card are protected not by isolation of physical memory, but rather by the cryptographic capabilities of the TPM**: all sensitive information stored on a smart card is encrypted using the TPM and then stored on the hard drive in its encrypted form. Since all cryptographic operations occur in the secure, isolated environment of the TPM, and the unencrypted private keys are never used outside of this environment, they remain secure from any malware on the host (as with conventional smart cards). Additionally, if the hard drive is compromised in some way, an attacker will not be able to access keys stored on the VSC, as they are securely encrypted using the TPM, and may be further protected by BitLocker drive encryption.

Functional Characteristics

Virtual smart card systems are designed to closely mimic the functionality of actual smart cards. The most striking difference to the end user, however, is that the virtual smart card is essentially a smart card which is *always* inserted into the PC/device. **There is no methodology for exporting the user's virtual smart card for use on other machines (thus the security of VSCs), but should a user require access to network resources on multiple machines, multiple virtual smart cards can be issued for that user on different machines. Additionally, a machine that is shared among multiple users can host multiple virtual smart cards for different users.**

Security aspects

Smart cards in their traditional form factor offer little opportunity for acquisition by a potential adversary. Due to their compact and portable design, SCs are most frequently kept close to their intended user, and any sort of interaction with the card is difficult without committing some variety of theft. TPM VSCs, however, reside on a user's computer which may frequently be left unattended, providing an adversary ample opportunity to hammer the device. Though virtual smart cards are just as fully protected from hammering as are conventional smart cards, this accessibility makes the logistics of an attack somewhat simpler. Additionally, as mentioned above, the anti-hammering behaviour of a TPM smart card differs in that it only presents a time delay in response to repeated PIN failures, as opposed to a full block.

Mitigating these slight security deficits, however, are several advantages provided by virtual smart cards. Most importantly, **a virtual smart card is much less likely to be lost or misplaced compared to a conventional smart card;** since VSCs utilize devices which the user already owns for other purposes, they are no longer a single-purpose accessory and are instead integrated into an otherwise useful device which the user will have more incentive to keep track of.

Practical applications of Virtual Smart Cards

Authentication applications

- **Two-factor authentication–based remote access:** When a proper certificate is provisioned to the virtual card, the user need only provide the PIN(or alternate authentication method) for the virtual smart card, as if it was a physical smart card, to sign in to the domain.
- **Client authentication:** Virtual smart cards can also be used for client authentication by using Secure Socket Layer (SSL) or a similar technology
- **Virtual smart card redirection for remote desktop connections:** the virtual smart cards that are stored on the connecting computer (which is under physical control of the user) are loaded onto the remote computer, and they can be used as if they were installed by using the remote computer's protected execution environment.

Confidentiality applications

- **Email encryption:** Physical smart cards are designed to hold private keys that can be used for email encryption and decryption; this functionality also exists in virtual smart cards.
- **Encryption for data volumes:** encryption technologies that make use of symmetric-key encryption to protect the content of a user's drive.

Data integrity applications

- **Signing data:** To verify authorship of data, a user can sign it by using a private key that is stored in the virtual smart card.

Smart Cards on mobile clients

Recent implementations include smart card support on Android clients. VMware HorizonView is probably the most reliable approach. This type of smartcard can be currently used as a means for secure access to desktop views from Android devices, through the use of smart cards as user authentication mechanism. An external device is necessary to act as card reader, burdening this approach.

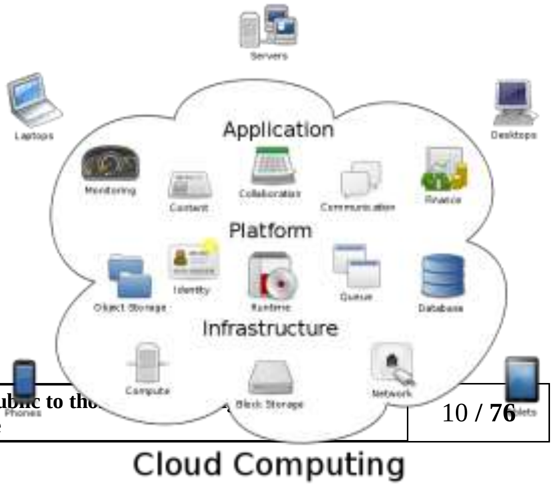
More practical implementations of smart cards on mobile devices are capable of emulating physical smart card readers by making use of smartphone's NFC hardware as contact-less smartcard reader.

Current VSC approaches claims to support the following types of smart cards:

ISO-7816 smart card including secure messaging, electronic identity card (nPA) with complete support for EAC (PACE, TA, CA), electronic passport (ePass) with complete support for BAC and, in the near future, Cryptoflex smart card.

2.2 Cloud computing technologies

Cloud computing represents a major shift in how companies and public bodies process information and manage ICT areas; traditional ICT management companies make substantial investments in resources, including hardware, software, data processing centres, networks, personnel, security, etc., while models with cloud solutions eliminate the need for large investments and fixed costs, transforming the utilities providers that offer a flexible and instantaneous low computing capacity demand.



Currently on the market there are more and more services based on cloud computing technologies: VISA announced last February its cloud-based payments following the introduction of a new feature in the Android mobile operating system called Host Card Emulation (HCE), which allows any NFC application on an Android device to emulate a smart card.

End users access cloud computing using networked client devices, such as desktop computers, laptops, tablets and smartphones while the business software and data are stored on remote servers

Below, a list of services that nowadays are offered under the cloud computing paradigm is detailed, classified by type of fundamental model of Software as a Service or Platform as a Service:

Software as a Service (SaaS):	Platform as a Service (PaaS)
Content, Communications and Collaboration (CCC)	Integrated Application Server
Customer Relationship Management (CRM)	Data Integration
Digital Content Creation (DCC)	Database Management System, DBMS
Enterprise Resource Planning (ERP)	Managed File Transfer, MFT
Office Suites	**Application Security**[1] Providers that offer this type of service PaaS provides a security solution scalable and flexible, which protects the customer applications from external threats, which reduces the risk of data leakage and enabling comply efficiently with the applicable regulations.
Supply Chain Management, SCM	Application and Business to Business (B2B) Integration
	App Marketplaces (catalogs)
	Portals User Experience Platform
	Business Process Management Technology, BPMTechnology
	App Life Cycle Management, ALM

In addition to the traditional cloud computing services, such as IaaS, PaaS, and SaaS, there is the security-related cloud computing service, Security as a Service (SECaaS), that is a business model in which a large service provider integrates their security services into a corporate infrastructure on a subscription basis more cost effectively than most individuals or corporations can provide on their own. These security services often include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management, among others.

Mobile cloud computing is a technique or model in which mobile applications are built, powered and hosted using cloud computing technology. In a mobile cloud approach developers build applications

[1] Solution where VISCA concept is allocated

designed specifically for mobile users without being bound by the mobile operating system and the computing or memory capacity of the smartphone. Mobile cloud computing is generally accessed via a mobile browser, typically without the need for installing a client application on the recipient smartphone.

With regard to cloud security, which is not to be confused with security software offering (SECaaS), there are a number of security issues/concerns associated with cloud computing infrastructure; these issues fall two broad categories: (i) security issues faced by cloud providers and (ii) security issues faced by their customers. In most cases, the providers must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the customers must ensure that the provider has taken the proper security measures to protect their information.

In the following table, the main cloud-security-related products classified by the area and functionality in the cloud security are described;

Areas	Main Functionality	Products
Cloud Infrastructure Security	Virtualization, Firewall, IPS/IDS	- Deep Security (Trend Micro) - vGW virtual Gateway (Juniper Networks) - vController IPS/IDS for Virtual Environment (HP)
	Anti-virus	- Kaspersky Security for Virtualization (Kaspersky)
	Security Mgmt./Monitoring	- vTrust for Virtual Management Centre (Reflex Systems) - Virtual Server Protection for VMware (IBM) - HyTrust Appliance (HyTrust)
Cloud Data Security	Data Encryption / Tokenization	- Encryption as a Service for WAN (Certes Networks) - CipherCloud (Cipher Cloud) - Token Management (Crptomathic)
Cloud Access Control	ID Mgmt., Authentication Access Control, SSO	- Intel Expressway Cloud Access 360 (Intel) - Okia Application Network (Okia) - Privileged Identity Management Suit (Cyber-Ark Software)

2.3 Mobile Devices and applications on Smartphones

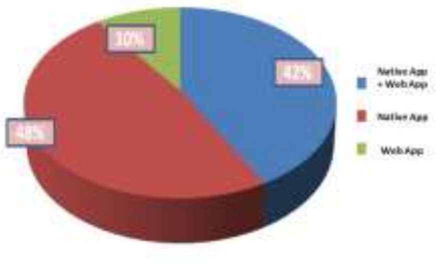
Mobile Apps Development

A typical classification for mobile applications is regarding to the supported systems: Apps developed for a native system (iOS, Android, Symbian, Bada, and Windows Mobile) and Web Apps. Native apps are most popular among users because they make the most of the potential and technical characteristics of each device, and the learning curve for developers is very pronounced. The biggest disadvantage is that most native apps are not compatible with all market devices.

The following figure shows the required skill set for the most used mobile Operating Systems:

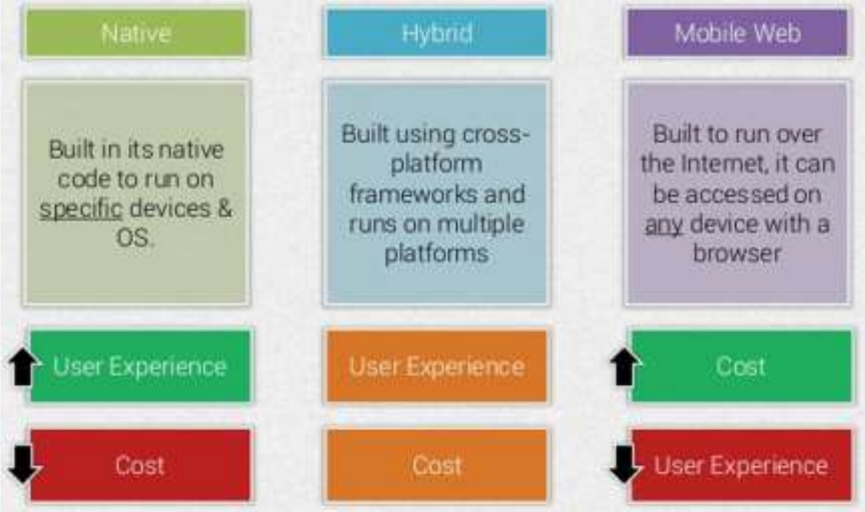
Mobile OS type	Skill set Required
Apple iOs	C, Objective C
Google Android	Java (harmony, Dalvik vM)
Windows Mobile	.NET
Window 7 Phone	.NET
RIM BlackBerry	Java (2Me)
Samsung Bada	C. C++, HTML/CSS/JS
Simbian	C, C++, Python, HTML/CSS/JS

On the other hand, Web Apps can be designed to work over different browsers, operating systems and different versions. In addition, developers can provide updates without direct user involvement. Recent studies carried out by PhoneGap show that a large number of developers decide for the development of both web apps as native applications (See adjacent graphic).



Mobile solutions developers preferences

Recent studies have found that users prefer mobile apps and that people spend 80% of their time in apps and only 20% in mobile web (Flurry 5 year report). Native mobile apps allow users to receive a far superior user experience tailored to mobile usage.


Native
Hybrid
Mobile Web
Built in its native code to run on specific devices & OS.
Built using cross-platform frameworks and runs on multiple platforms
Built to run over the Internet, it can be accessed on any device with a browser
User Experience
User Experience
Cost
Cost
Cost
User Experience

There are also hybrid mobile applications, mostly developed through dedicated development frameworks; those can represent an intermediate approach to achieve a cost effective solution, preserving most of native functionalities featured by native software developments. The figure summarizes the three kind of approaches to mobile application development.

A more in-depth analysis of each sort of application results in the following facts:

- Native apps
  - Matured SDK's
  - Rich User Experience
  - Fully Leverages device hardware and software
  - Ability to run offline
  - Higher development cost compared to others
- Mobile web
  - Platform independence: Designed to run on mobile web browsers
  - HTML5 apps (HTML, CSS, JAvascript)
  - Approaches: Responsive Web, Mobile First
  - Lower development costs compared to native apps
  - Low on user experience compared to native apps
- Hybrid applications
  - Mobile web apps wrapped inside native wrappers
  - Bridges gap between HTML5 and device hardware
  - New tools also providing Model-View-Controller development using a variety of programming languages: Java, C#, Ruby-on-Rails…
  - Frameworks: Appcelerator Titanium, Phonegap, Xamarin
  - Multiplatorm, cost effective solution

2.4 Related previous projects or initiatives

Project Name	Cooperative Programme	Time period (approx.)	Technical Focus	Relation to, and difference with, this project proposal
AMIE	ITEA2	2006-2009	AI for Home Care	**Similar:** Technology for Service Provision. **Difference:** No approach to security issues, patient identification, etc.
ProSECCO	IST	2002-2004	Product and Service Codesign, Defines SME procedures to adapt from a product to service business	**Similar**: Approach to service provision from product orientation. **Difference**: No approach to security issues.
AIMES	ITEA2	2007-2010	Advanced Infrastructure for Medical Equipment Management and Services	**Similar:** Technology for Service Provision. **Difference:** No approach to security issues user identification.
SysSec	FP7 - NoE	2010 - 2014	Network of Excellence related to the management of Threats and Vulnerabilities in the Future Internet	**Similar:** Both projects are related to security on IT technologies **Difference:** SysSec is focused on mainly big infrastructures hacking threats and especially on non-human interaction incoming attacks (a.e. Viruses…), in comparison toof VISCA that tries to prevent external information theft from personal devices and information data-bases. No virtualization of any system is initially considered in SysSec.
TECOM	ITEA2	2007-2010	Trusted computing solutions for embedded platforms	**Similar:** Security and safety of ICT systems, including some innovation in security increase directly on HW components. **Difference:** TECOM is addressed to embedded computing systems and infrastructures and their inner HW/SW structure and components.VISCA, on the other hand, is focused on cloud security and the problems in user identification and user interaction when accessing secure services.

3 Market

3.1 Megatrends

In 2012, the sales of smart phones in Europe accounted for around 55.0 percent of mobile phone handset sales. Mobile phones and especially smart phones have emerged as the main device for communication, entertainment, and information. Smart phones can provide mobile wallet functionality – a set of applications including payment, couponing, loyalty programs, virtual business cards, and virtual keys for physical or logical access, among other services and credentials. More and more smart phones (and tablets) also are used for and depend on internet access.

Global Mobile Penetration Rates in 2020
North America* 200+%
South America* 110%
Africa* 90%
Mobile Penetration Rates
75-100%
100-200%
Over 200+%

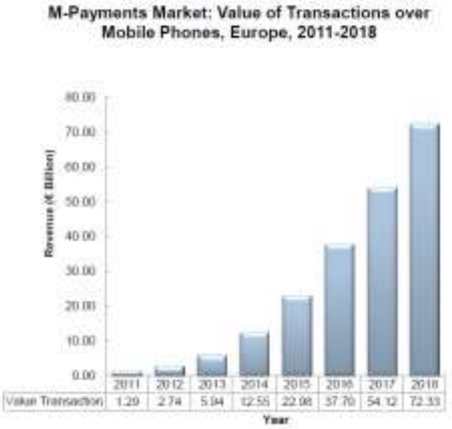
Advances in Next Generation Networks Leads to Surge in Innovative Vertical Applications

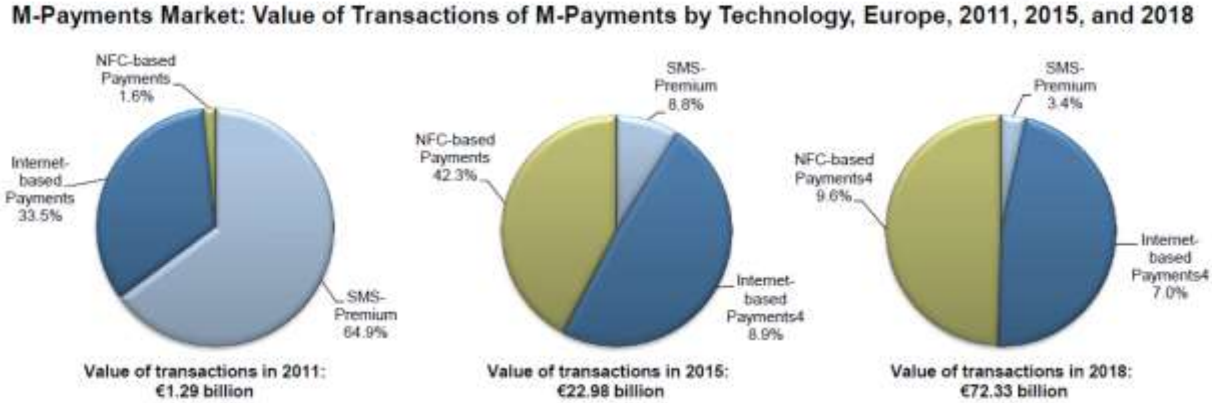
	Today	In 10 years from now
Healthcare	Telemedicine, Applications for Disabled (Voice Transcription)	In-Body Telemetry (implanted sensors), Apps for Disabled (Text to speech/speech to text) (Speech to signing), Virtual Surgeries, Remote Patient Monitoring & Diagnostics
Financial Services	E-Banking, E-Commerce, Tele-working, Videoconferencing, E-News, Online Shopping Two Way Mobile Video	Virtual Companies, Virtual Work Rooms (Virtual Reality Collaboration Space), Remote Financial Simulation (Access to Financial Models), Virtual Business Conferences
Government	Growing E-Government applications, National Security, Monitoring Public Safety	Real Time Polling & Voting, online access to all gov. services
Infrastructure	Utility Applications, growing Cloud Computing and Storage	Artificial General Intelligence, On Energy Monitoring and Metering, Intelligent Water Treatment, Intelligent Customer Centres, Smart Grid for household and industrial media

3.2 M-Wallet and Mobile Payment

Mobile payment is an alternative payment method. Instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods. There are four primary models for mobile payments:

- Premium SMS based transactional payments
- Direct Mobile Billing
- Mobile web payments (WAP)
- Contactless NFC (Near Field Communication)





The four potential mobile payment models are:

- **Operator-Centric Model**: The mobile operator acts independently to deploy the mobile payment service. The operator could provide an independent mobile wallet from the user mobile account (airtime). A large deployment of the Operator-Centric Model is severely challenged by the lack of connection to existing payment networks.
- **Bank-Centric Model**: A bank deploys mobile payment applications or devices to customers and ensures merchants have the required point-of-sale (POS) acceptance capability. Mobile network operators are used as simple carriers, they bring their experience to provide Quality of service (QOS) assurance.
- **Collaboration Model**: This model involves collaboration among banks, mobile operators and a trusted third party.
- **Peer-to-Peer Model**: The mobile payment service provider acts independently from financial institutions and mobile network operators to provide mobile payment.

Gartner Research forecasts that the worldwide mobile payment market will have over 450 million users and a transaction value of more than 721 billions of dollars in 2017. This represents compound annual growth rates of 18% and 35% respectively for the period 2012 to 2017 (http://www.gartner.com/id=2484915).

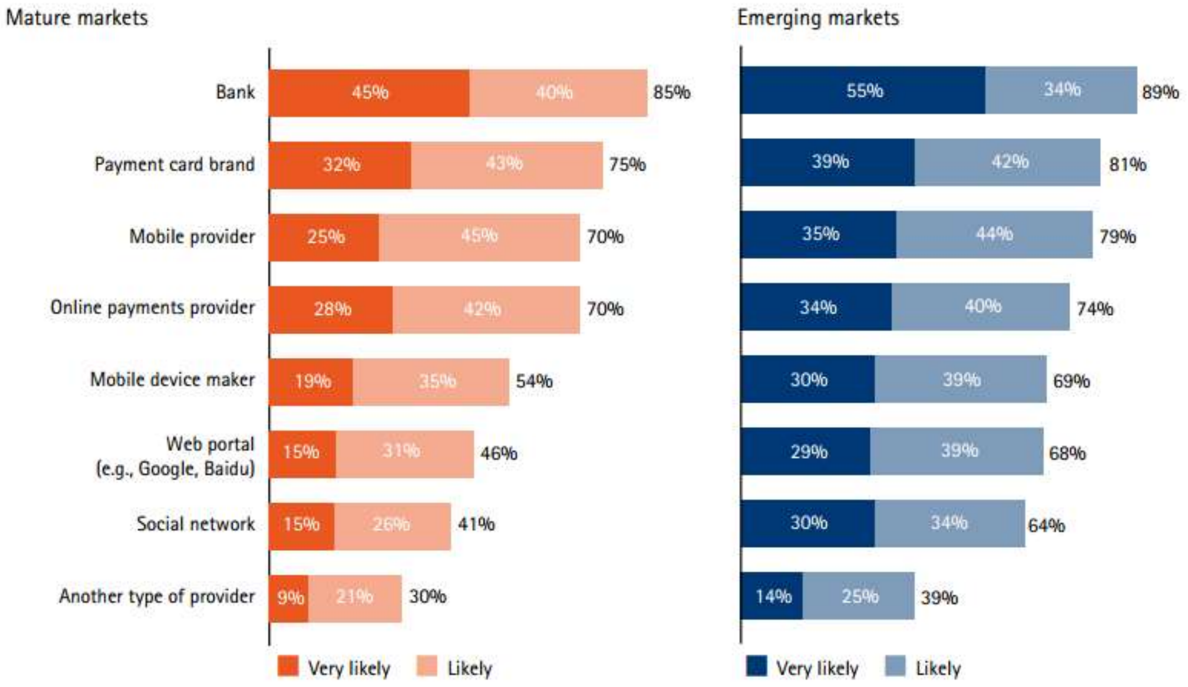
In terms of payment types, Gartner estimates that prepaid top-ups will generate the biggest transaction volumes in 2014, but money transfer, tickets and merchandise purchases will also be popular. However, money transfer will be the biggest category in terms of value, accounting for 63% of total transaction dollars in 2014, driven by huge demand for remittance payments in developing markets.

The number of people using their mobile phones to make payments is set to grow from 70.2 million in 2009 to 108.6 million this year, a 54.5% rise, according to Gartner. This represents 2.1% of all mobile users, with the fastest take-up of the technology in the developing markets of Asia, Eastern Europe, the Middle East and Africa, driven by the unbanked and underbanked.

In Asia Pacific, m-payment users will exceed 62.8 million in 2010 and represent 2.6% of all mobile owners in the region. In Europe, the Middle East and Africa there will be 27.1 million users, while in North America the figure is expected to be just 3.5 million, or 1.1% of all mobile users in the region.

The Accenture Mobile Web Watch Internet Usage Survey report found that 77% of utility customers and 66% of telecommunication customers have expressed desire to utilize a mobile app. They also found that of those that do not regularly use payment apps, 74% are aware of such services and an additional 39% indicated they would be interested or plan to use such an app in the near future.

Accenture research shows that mobile payment capabilities are highly attractive to consumers, presenting significant opportunity to create new revenue streams. Already 20 percent of smartphone users use mobile payments. That number could more than double in the near future, as 31 percent plan to use mobile payments in 2014. The following figure shows preferred providers of mobile payment services.



Source: Mobile Web Watch 2013 Accenture

Globally, the survey shows that mobile payments are more used by people in urban areas, by those with higher education and by heavy users of social media. The most common goods paid for with mobile payments include tickets for events such as concerts, cinema and theatre (55 percent of mobile payment users have purchased these) and tickets for transportation such as air and rail (47 percent have purchased these). However, at least one-third of mobile payment users have also purchased goods such as clothing, groceries and other consumer goods.

Mobile payments are important enough to mobile Internet users that many say they would be willing to switch their mobile provider, bank, device manufacturer or merchant in order to be able to use them. If

mobile payments were as widely accepted as card payments are today, more than half (56%) of mobile Internet users would switch to a provider that offered mobile payments if their current provider did not do so.

As communications service providers attempt to monetize the phenomenal growth of mobile payments, there are numerous possiblities to consider. Mobile payments link the telco industry to other industries from banking and financial services to consumer goods and the public sector. As these industries converge, a tremendous growth opportunity arises for companies that canadapt to the new marketplace rules.

The European mobile financial services are characterized by relatively high uptake of m-banking services and an emergent adoption of m-payments. Convenience and the pervasiveness of smart phones will likely drive growth in the European mobile financial services market. As far as m-payments are concerned, the value of transactions made via mobile devices is expected grow exponentially over the next five years. From a technology perspective, m-payments will evolve from SMS-based solutions towards NFC- and Internet-based alternatives.

Mobile Devices Replace Credit Cards

- ✓ Mobile payment will outpace credit cards in total transactions and boost peer-to-peer transactions
- ✓ Using your Mobile phone as a credit card for purchases will become the norm with Near Field Communication (NFC) technology.
- ✓ Visa recently announced that it is fully committed to supporting NFC-based mobile payments and has set an aggressive timetable for itself and partners to meet specific goals to accept NFC mobile payments.

3.3 Cloud Services Market

With the development of cloud computing, information sharing and social networks utilizing various service cases are expected to increase rapidly. As the connectivity of distributed information and its utilization with changes in the cloud-based IT services is enhanced, the quality of information processing that can be easily shared environment for the world of cloud services market will reach $ 177B by 2015 view, and consumers are to favor the introduction of a cloud with high security trend.

The development of cloud services market gives the following presents a variation.

- **Improve the efficiency of resource use**: By using mobile devices and big data with cloud services, the leveraging of the creative practice of outsourcing that saves time and money is on the rise.
- **industry value chain restructuring**: As the changes how to distribute IT services, software, and information, the structure of the value chain within the industry is being re-generated.
- **highlighted the importance of information management**: As a large cloud service that holds the emergence of large-scale service providers and secure management of information emerged as an important issue, the appropriate control of personal information management, copyright, business models, and government regulation have been highlighted.

Gartner recently released survey results show that public cloud services market from 2011 to 2017 growth rate (CAGR) of 17.1% in terms of growth, the market would be formed to $ 244 billion

Cloud advertising market is worth $ 100 billion in 2017 would have the scale to virtually half of the market. In short, the online advertising market is so large, it is meant to. This sector saw 14.9% in 2011 ~ 2017 CAGR across.

IaaS (Infrastructure as a Service) spearheading Amazon is the period from 2011 to 2017, is a CAGR of 37.4% during that and the growth. Worldwide in 2011 was $ 4.479 billion market in 2012 to record $ 6.319 billion and $ 9.192 billion in 2013, which leads to the view would be.

Gartner has a classification system in the public cloud services, including Iaas of SaaS (Software as a Service), PaaS (Platform as a Service), and BPaaS (Business Process as a Service) also. Cloud-based payments, customer management, e-commerce, finance and accounting, human resources (HR), and supply management, which separated BPaaS, CAGR from 2011 to 2017 suggest that 10.8% and is expected to grow another SaaS (21.0%) or PaaS (23.5%) compared to the relatively low growth in such striking point.

In terms of regional market size in 2013 was $ 75.5 billion in North America, Western Europe (Germany, France, the United Kingdom, the Netherlands, Italy, Spain) is a $ 30.5 billion, accounting for more than 80% of the total available market.

According to Gartner, worldwide mobile cloud app market is $ 400 million in 2009 scale, $ 9.5 billion in 2014 to be expected to reach scale.

In addition, in the case of global mobile cloud application services market, with the proliferation of mobile devices, mobile office and corporate related to the interests heightened, the market expected to expand significantly from $ 3.5 billion in 2010 at an average annual growth rate of 53.3% to $ 19.5 billion in 2014 it is predicted to be.

3.4 Confidential & secure telemedicine applications

Current situation

Our increased dependence on networked, connected, and connectible devices requires increased vigilance. This is even more true in the case of medical applications, because our vital signs form integral part of our personal profile, and can be subject to interested and improper use. However, even "off-the-grid" devices can be nowadays extremely vulnerable. Viruses and other malware do not require an internet or intranet connection to spread and compromise the medical service institution security – a single infected USB storage device, used to install updates, for instance, or to transfer or back-up patient data can easily become a digital nightmare, spreading throughout an organization without actually showing any signs of infection itself.

In a recent article by Dean Wiech [1] "Controlling healthcare user authentication and authorizations" the author claims that despite the high requirements for information security throughout healthcare environments, many healthcare organizations still manually manage user accounts and access to information. Information regarding new employees and their access rights is passed between the hiring manager, human resources and IT, who then create accounts based on the available and, often inaccurate, information.

This is less than optimal for the organization because it leads to several risks, including:

- An overwhelming workload for the IT department with manual and repetitive tasks

- Long turnaround times for creating user accounts
- Risk of making errors during the manual copying of data (such as typos in the name of the employee)
- Risking that new employees receive the same rights as an employee in a similar function when they should not. When rights are copied there is a risk that employees receive access rights to applications and systems they really don't require access to
- Risk of pollution in Active Directory (AD) because of accounts of employees that have left the organization remaining active. Pollution in the AD due to user accounts of former employees has a negative effect on the score of an audit and compliancy regulations.
- For healthcare organizations to mitigate these risks, they need to take control of their authentication and authorization processes. By using an automated solution for user account management organizations can greatly improve optimization and reduce risks.

What kind of surprises will impact the healthcare industry in 2014? CIOs and IT professionals at healthcare organizations are tasked with achieving the difficult balance between demand for universal access to patient information and the need to ensure security. And the evolving regulatory and technological landscape will only create more uncertainty in 2014.

There is a considerable number of issues to take into account when coping with this situation, such as being able to:

- recognize the symptoms of an intrusion
- safeguard information across the continuum of care
- identify gaps in the medical service environment

LEGACY DEVICES

What is the situation today at hospital or health care service institution?

The Food and Drug Administration is warning makers of heart monitors, mammogram machines and myriad other medical devices that their gear is at risk of being infected with computer viruses that can endanger patients [2]. The FDA claims to be aware of hundreds of medical devices that have been infected by malware.

According to a Deloitte report [3], Healthcare organizations are in various stages of mitigating the cybersecurity risks of medical devices such as patient monitors, infusion pumps, ventilators, pacemakers and imaging devices. Overall, however, Deloitte's interviews with medical device security leaders at nine large hospital systems indicate that their organizations have a long way to go and that they'll need more cooperation from device manufacturers.

The report also mentions that healthcare organizations have had difficulty in developing risk-mitigation strategies for devices that are more than five years old and run on proprietary operating systems. The reason is that these legacy devices are difficult to test for vulnerabilities because off-the-shelf security scanning tools do not exist. Other devices that run on "well known commercial operating systems" have the same vulnerabilities as other types of systems connected to a network, the report said.

For both these and the legacy devices, the most extreme risk mitigation method is to quarantine the medical devices from the rest of the hospital IT system. Other alternatives are to fall back to other types of controls, such as detection controls and similar systems to see whether there has been activity that suggests hacking or unauthorized access to medical devices.

This is even more true in the case of telemedicine, in which the use of IT technologies are the core of the applications, and the security channel for information must be provided from device level up to web environments.

STEPS FOR THE FUTURE

The above mentioned issues have brought about enough concern, and considerable actions are being taken at regulatory level.

On September 23, 2013, new rules were launched to ensure that healthcare organizations, as well as their business associates and subcontractors, are compliant with HIPAA regulations [4] to secure personal health information (PHI). Compliance with data protection regulations has never been more important, nor more difficult with the rise of the mobile workforce. Learn about the consequences of these new regulations and how organizations can change their IT methodologies to protect sensitive data and avoid costly breaches.

Recently, the Food and Drug Administration (FDA) has released a guidance [5] on the "content of premarket submissions for management of cybersecurity in medical devices." This guidance suggested that device makers incorporate security features into their products to limit access to only trusted users, determine trusted content, and use fail-safe and recovery devices. FDA called on the manufacturers to consider threats such as hacking, malware and other vulnerabilities of device software and to work with providers on use cases.

Specifically, the agency issued Draft Guidance requiring the submission of cyber security materials as part of any premarket submissions [PDF] and a Safety Communication explaining in more plain terms the scope of the cyber security issues addressed and the FDA's recommended actions. While the Draft Guidance may only apply to manufacturers who intend to submit premarket materials for approval, the Safety Communication is also targeted to, and should be reviewed by, hospitals that rely on medical devices and information networks threatened by malicious software (malware).

The FDA Draft Guidance

Recently, the FDA has become aware of cybersecurity vulnerabilities and incidents that could directly impact medical devices or hospital network operations, including:

- Network-connected/configured medical devices infected or disabled by malware;
- The presence of malware on hospital computers, smartphones and tablets, targeting mobile devices using wireless technology to access patient data, monitoring systems, and implanted patient devices;
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel);
- Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices);
- Security vulnerabilities in off-the-shelf software designed to prevent unauthorized device or network access, such as plain-text or no authentication, hard-coded passwords, documented service accounts in service manuals, and poor coding/SQL injection.

The Communication speaks to both manufacturers and health care facilities. For manufacturers (in addition to the Draft Guidance, discussed below) the Communication encourages the adoption of steps that will limit unauthorized device access (particularly for life-sustaining devices), protect medical devices and their components (including upgrading and patching existing security as necessary), provide designs that preserve core functions even during an attack and provide methods to recover and restore compromised devices. For facilities, the Communication recommends:

Recommendations/Actions:

Many medical devices contain configurable embedded computer systems that can be vulnerable to cybersecurity breaches.

For all device manufacturers:

Manufacturers are responsible for remaining vigilant about identifying risks and hazards associated with their medical devices, including risks related to cybersecurity, and are responsible for putting appropriate mitigations in place to address patient safety and assure proper device performance.

The FDA expects medical device manufacturers to take appropriate steps to limit the opportunities for unauthorized access to medical devices. Specifically, we recommend that manufacturers review their cybersecurity practices and policies to assure that appropriate safeguards are in place to prevent unauthorized access or modification to their medical devices or compromise of the security of the hospital network that may be connected to the device. The extent to which security controls are needed will depend on the medical device, its environment of use, the type and probability of the risks to which it is exposed, and the probable risks to patients from a security breach.

In evaluating your device, consider the following:

- Take steps to limit unauthorized device access to trusted users only, particularly for those devices that are life-sustaining or could be directly connected to hospital networks.
- Appropriate security controls may include: user authentication, for example, user ID and password, smartcard or biometric; strengthening password protection by avoiding hard-coded passwords and limiting public access to passwords used for technical device access; physical locks; card readers; and guards.
- Protect individual components from exploitation and develop strategies for active security protection appropriate for the device's use environment. Such strategies should include timely deployment of routine, validated security patches and methods to restrict software or firmware updates to authenticated code. Note: The FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity.
- Use design approaches that maintain a device's critical functionality, even when security has been compromised, known as "fail-safe modes."
- Provide methods for retention and recovery after an incident where security has been compromised.

Cybersecurity incidents are increasingly likely and manufacturers should consider incident response plans that address the possibility of degraded operation and efficient restoration and recovery.

For health care facilities:

The FDA is recommending to take steps to evaluate your network security and protect your hospital system. In evaluating network security, hospitals and health care facilities should consider:

- Restricting unauthorized access to facility networks and networked devices
- Ensuring that all security software is up to date

- Monitoring network activity (for suspicious movement, such as a radiology device communicating with an outside server seemingly on its own initiative)
- Regularly reviewing security, updating as necessary, and disconnecting devices that do not require connections
- Reaching out to manufacturers, the FDA, or DHS ICS-CERT where a vulnerability or problem is found; and
- Developing strategies to preserve critical functions during adverse conditions.

The FDA's Draft Guidance applies to Premarket Notification (510(k)) including Traditional, Special, and Abbreviated 510(k) submissions; *De novo* petitions; Premarket Approval Applications (PMA); Product Development Protocols (PDP); and Humanitarian Device Exemption (HDE) submissions relating to medical devices that contain software, firmware, or programmable logic. In short, the guidance intends to ensure that medical devices will maintain information confidentiality, integrity and availability – even when infected with malware. To achieve these goals, the Draft Guidance recommends that manufacturers "consider cybersecurity during the design phase of the medical device, as this can result in more robust and efficient mitigation of cybersecurity risks." Specifically, manufacturers, as part of the risk analysis required in a pre-market submission, should define and document:

- An identification of assets, threats and vulnerabilities;
- An impact assessment of the threats and vulnerabilities on device functionality;
- An assessment of the likelihood of a threat and of a vulnerability being exploited;
- A determination of risk levels and suitable mitigation strategies; and
- A residual risk assessment and risk acceptance criteria.

The Draft Guidance goes on to address the security capabilities it expects to be described in premarket submissions and the documentation it recommends be used to evidence the existence of necessary security considerations.

Security Capabilities

The Draft Guidance acknowledges that the identification of appropriate security measures will be heavily dependent on context – how and where the device will be used, what features it offers, how it is accessed or maintained, etc. The Draft Guidance also notes an understanding that security features could compromise usability (especially, for instance, in an emergency) and that careful consideration of an appropriate balance is necessary. With these caveats in mind, however, the Draft Guidance recommends that premarket submissions include justification for the use (or exclusion) of certain security features, including (but not limited to):

- Automated timed log-offs;
- Providing support for layered authorizations (providing different users different levels of access);
- Requiring multi-factor authentication for privileged users (such as technicians who may alter software or firmware configurations);
- Avoiding "hard-coded" passwords (passwords that are the same for each device and difficult to change);
- Providing physical locks on both the device itself and its communication ports;
- Requiring user access authentication prior to permitting updates or other software modification;
- Restricting software modification to authenticated code, issued by the manufacturer and confirmed using that manufacturer's authentication system;
- Provide procedures for authorized users to download version-identifiable software and firmware from the manufacturer;
- Provide for secure data transfer to and from the device, using encryption technology as appropriate;

- Provide for "fail-safe" device features that protect the device's critical functionality, even when the device's security has been compromised;
- Provide features that allow for the recognition of an security breach (such as an infiltration of malware or other unwelcome code), logging, and corrective action;
- Provide methods of data and device recovery by an authenticated administrative user;

The Draft Guidance recommends that manufacturers provide the following:

- An analysis of hazards posed, mitigations, and design consideration related to cyber security risks associated with the device (including "specific" listings of all risks that were considered during device design and all cyber security controls (and their justifications) established for the device:
- A "traceability matrix" linking security controls established with those that were considered;
- The systematic plan for providing validated software and firmware updates and patches;
- "Appropriate" documentation that the device will be provided to purchasers free of malware; and
- Device instructions and product specifications regarding recommended security environment steps (such as anti-virus software, firewall configuration and the like).

As always, the FDA's guidance is not legally binding – these steps are recommended, but not required. The guidance, however, provides clear insight into the agency's thoughts on appropriate manufacturer responses to cyber security threats and should not be ignored.

Another Safety Communication echoes concerns that the FDA first enunciated in a November 2009 Communication. In essence, the new Communication expands on the previous Communication, and provides more specific guidance to users, purchasers, providers and manufacturers of medical devices.

It seems likely that the FDA's actions are meant to combat what appears to be a growing problem of cyber security and connected (or simply connectable) medical devices.

OTHER RECOMMENDATIONS

The Food and Drug Administration (FDA) has also issued new guidance on the radio frequencies of wireless medical devices [7], including recommendations for authentication and encryption measures to ensure the security of the device and the safety of the patient. Properly encrypted wireless devices will not only prevent hacking and misuse of the device itself, but also reduce the likelihood of unauthorized access to the wireless network itself.

While the recommendations are mostly directed at device manufacturers, the rules have significant implications for security professionals as well. Increasingly, the healthcare enterprise and associated devices are becoming wireless enabled and integrated. Authentication and encryption will help protect against hacking to prevent the possibility of access to the device and associated networks by unauthorized personnel to protect both patient safety and patient privacy. In certain cases, taking control of a device could result in broader access to the enterprise's IT devices and assets.

Specific areas of concern for security managers includes the capability of technologies to automatically sense and connect to an unsecured wireless network, and the transmission of sensitive patient health data over such a network. Potential risks also include a malicious attack on the patient himself, with an unauthorized hacker delivering a fatal overdose of medication or device malfunction through the network.

The FDA encourages the use of state-of-the-art encryption and authentication methods, although the

Agency did not recommend specific protocols, since security technology is changing at a rapid pace. The guidance follows an additional FDA report [8,9,10] on the need for interoperability standards for medical devices to enhance the "plug-and-play" capabilities of products.

3.5 Public Secure Services

The security of retail payments is essential for payment users and merchants. Consumers are informed of fraud and abuse of personally identifiable information (PII) incidents through press and they are sensitive to security issues for card and internet payments. E-commerce research studies shows that payment security concerns of the consumers are one of the key boundaries that prevent the adoption of electronic commerce.

The replacement of signature-based cards by EMV-compliant Chip and PIN cards has helped reduce fraud significantly at the point-of-sale. This change has shifted card-present frauds to card-not-present frauds. Card not-present transactions represent only a minor share compared to card-present transactions however they account for the majority of all fraud cases. A two-factor authentication for internet payment transactions (one-time transaction code received through an SMS) to reduce fraud has a trade-off between security, speed and ease of use.

A second important issue regarding retail payments is data protection. Retail payments require the processing of personal data and the use of electronic communication networks. Sensitive customer information should stay within a secure payment infrastructure while data is being processed or at rest. It is crucial that authentication mechanisms for payment transactions are designed to ensure compliance with data protection requirements. The number of parties having access to authentication data during or after a payment transaction should be restricted to those who are strictly necessary to perform the transaction.

With mobile devices outselling PCs and new mobile technologies being adopted at an unprecedented rate, the way technology is being used and payment methods are shifting.

According to Juniper Research's recent report, mobile devices will account for 30% of global retail e-commerce spending by 2018, up from 15% in 2013 and retail payments on mobile devices will reach $707B by 2018, up from $182B in 2013

Hence, the electronic payments market offers great opportunities for innovation. Consumers have already significantly changed their payment habits. Next to ever growing payments with credit or debit cards, the rise of e-commerce and the increasing popularity of smart phones has enabled new ways of making payments.

The role of non-banks in retail payments has increased significantly, owing in part to the growing use of innovative technology that allows non-banks to compete in areas not yet dominated by banks.

According to McKinsey's research, more than a billion people in emerging and developing markets have cell phones but no bank accounts. Many low-income people store and transfer money using informal networks, but these have high transaction costs and are prone to theft. Mobile money is beginning to fill this gap by offering financial services over mobile phones, from simple person-to-person transfers to more complex banking services.

According to Bank for International Settlements (www.bis.com) research on "Innovations in retail

Payments", the retail payment trends identified can be summarized as follows:

- In view of the considerable number of new developments, the market is dynamic. However, only a few innovations have so far had a significant effect on the market.
- Most innovations are developed for the domestic market, and only a few have international reach, although similar products and categories have emerged worldwide.
- There is an increased focus on speeding up payment processing, either through faster settlement or through faster payment initiation.
- Financial inclusion has served as an important driving force for innovations in many countries, either under a government mandate or because of the new business opportunities opened up by an untapped market.
- The role of non-banks in retail payments has increased significantly, owing in part to the growing use of innovative technology that allows non-banks to compete in areas not yet dominated by banks.

Based on the trends identified and the economics of retail payments, the report identifies a number of factors that could serve as drivers for retail payment innovations.

User demand is probably the most important driver for innovation, since it is the basis for a valid business case, either through the utilization of potential revenues or through the realization of economies of scale and scope in producing the services.

In many cases, innovations in retail payments represent only incremental improvements to existing and established payment services. However, the solution of VISCA when successfully implemented as an alternative retail payment method, has got the potential for making a big shift in the shopping and payment experience meeting faster payment processing, user convenience and security needs.

The volume of payments made through mobile phones is currently the fastest growing of all payment methods which increased the role of non-banks in retail payments significantly. The banks can make an outstanding move and outpace the non-banks by leveraging VISCA and their own built-in infrastructure, regulatory experience and consumer trust.

VISCA USE CASES

4. Methodology

Methodology consists in for this first D2.1 deliverable:

- Define a complete template to collect the essential information for elementary use cases
- Asking each partner to submit a set of elementary use cases within the frame of the template
- Analyzing elementary use cases submitted by partners to identify common features
- Identifying adding-value services that could be provided in the VISCA cloud/infrastructure to efficiently serve use cases

5. Use Cases Descriptions.

5.1 UC#1. Log In/Authentication Process

Use case number	VISCA UC#1
Use case name	Log In /Authentication Process
Author/partner	Planet Media
Summary	Log In or authentication process when high secure levels are required must be addressed by the provisioning of user credentials to the services application. These credentials are stores in a secure element hosted in an isolated and secure virtual environment in the mobile device that avoids third parties hazards or external accesses. Once the user is logged in the application, he is authenticated and he will be able to start a private session accessing to all his dedicated services (telemonitoring session, financial transactions, confidential data sharing, etc.)
Rationale	The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-in procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

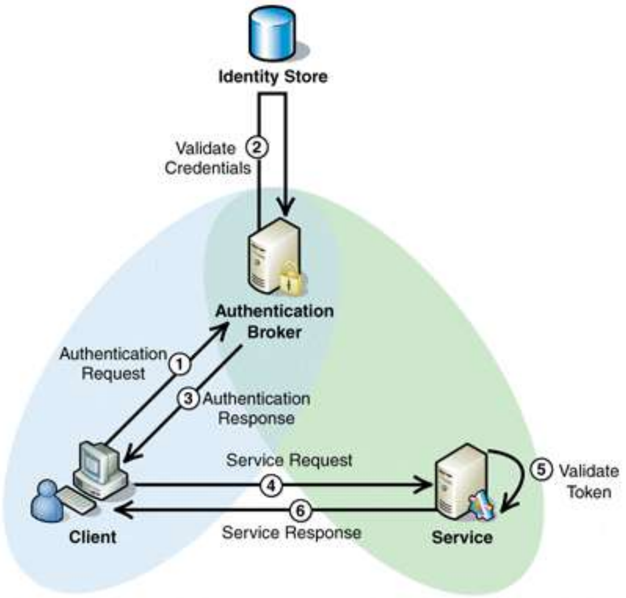
5.1.1 Use case description

Access to operating systems shall be controlled by a secure login procedure. Logging in is usually used to enter a specific page, which trespassers cannot see. Once the user is logged in, the login token may be used to track what actions the user has taken while connected to the site.

When a user clicks a link to start an application, the login script configured for the application connects to the application server, handles the authentication process, and starts the application.

The client sends his authentication credentials (username, password or PIN code) towards a Authentication Broker (this could be an Smart Card) and confirm the identity of the user. A session token is generated and it supports the access and connection to the service.

The process is described in the following picture:



5.1.2 Contextual settings

5.1.2.1 Context description

Peter wants to access his private account of his telemonitoring service that his health insurance company provides him in order to have one private telemonitoring session, so he uses their dedicate mobile application in his smartphone but the first step to carry out is the login in the app.

As the services is going to send and share confidential information about his health levels it is mandatory that the app provides a high security environment, so the login is carried out thanks to a secure element (virtualized) hosted in the Smartphone. The process described above is reproduced in the login step so Peter is able to access all his private services and starts the session.

5.1.2.2 Resources

The main resources:

- Mobile Device capable to host an Hypervisor (a.e. XEN)
- Main OS
- Virtual OS (virtual machines) running isolated from the main smartphone OS
- Virtual secure element host in the isolated virtual OS
- Software interface that allows secure apps to communicate with secure virtual element on the virtual OS
- Service application installed on the Smartphone
- Remote VISCA server (synchronization functionalities)
- Service app server (app back-end)

5.1.3 Functional description

Preconditions and assumptions	Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services.

5.1.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.2 UC#2. End-User Shopping Process

Use case number	VISCA UC#2
Use case name	End-User Shopping Process
Author/partner	BNB Consulting
Summary	User shopping scenario in the shop
Rationale	The procedure for end-user process should be designed to Help the end user easier his/her shopping

5.2.1 Use case description

After the End-user have his/her shopping process, during the payment time (on the cashier), he/she will ask to the cashier:

a) The company/agency number
b) The total payment

Then the end-user, he/she will,

a) open his/her smart-phone-application,
b) enter his/her application password
c) select the credit card among the cards (he may have more than one credit card)
d) enter his/her credit card number
e) enter the company/agency number
f) enter the total payment
g) choose the credit or bonus (some credit card provides free bonus for shopping)

at the end of the application process, he/she will

a) have the online confirmation
b) have the printed slim from the cashier

5.2.2 Contextual settings

5.2.2.1 Context description

He/She wants to go to the shopping and to use his/her most competitive credit card for his/her shopping.

5.2.2.2 Resources

The main resources:

- Smart Mobile device
- Authenticated Smart mobile application
- Authenticated Credit cards on the application

5.2.3 Functional description

Preconditions and assumptions	Mobile app installed in the Smartphone. Credit cards installed and authenticated with the bank

Trigger	The user starts the payment process process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user paid the shopping successfully

5.2.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.3 UC#3. End-User Shopping Process on Internet

Use case number	VISCA UC#3
Use case name	End-User Shopping Process on internet
Author/partner	BNB Consulting
Summary	User shopping scenario on the internet
Rationale	The procedure for end-user process should be designed to Help the end user easier his/her shopping on internet

5.3.1 Use case description

After the End-user have his/her shopping process, during the payment time (on the internet), he/she will select "pay VisCa"

Then the end-user, he/she will,

h) Have an alert from the smart-application
i) open his/her smart-phone-application,
j) enter his/her application password
k) select the credit card among the cards (he may have more than one credit card)
l) enter his/her credit card number
m) choose the credit or bonus (some credit card provides free bonus for shopping)
n) Approve the payment

at the end of the application process, he/she will

c) have the online confirmation
d) have an email from the internet site

5.3.2 Contextual settings

5.3.2.1 Context description

He/She wants to have a shopping on the Internet and to use his/her most competitive credit card for his/her shopping.

5.3.2.2 Resources

The main resources:

- Smart Mobile device
- Authenticated Smart mobile application
- Authenticated Credit cards on the application

5.3.3 Functional description

Preconditions and assumptions	Mobile app installed in the Smartphone. Credit cards installed and authenticated with the bank
Trigger	The user starts the payment process process
Normal flow	Normal flow is defined in the use case description

Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user paid the shopping successfully

5.3.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.4 UC#4. End-User Application Installation on Smartphone

Use case number	VISCA UC#4
Use case name	End-User Application Installation on Smartphone
Author/partner	BNB Consulting
Summary	User application installation scenario on the smartphone
Rationale	The procedure for end-user process should be designed to Help the end user easier application installation on his/her smartphone

5.4.1 Use case description

After the End-user have smartphone and want to use Visca Application he/she will:

o) Enter the Smartphone Market (Iphone, Samsung, etc)
p) Search the VisCa application
q) Found the VisCa application
r) Push installation button
s) Open the application
  a. The application authomatically starts the authentication process (defined as another use case process)
t) Set up application password
u) Finish the authentication process

5.4.2 Contextual settings

5.4.2.1 Context description

He/She wants to have a VisCa application and to use VisCa for his/her shopping.

5.4.2.2 Resources

The main resources:

- Smart Mobile device
- Internet connection
- VisCa agreement with Bank

5.4.3 Functional description

Preconditions and assumptions	Smartphone Internet VisCa agreement with the Bank
Trigger	The user starts the installation process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user installed the application successfully

5.4.4 Constraints

Location	N/A
Environmental	N/A

characteristics	
Legislation and standards	N/A

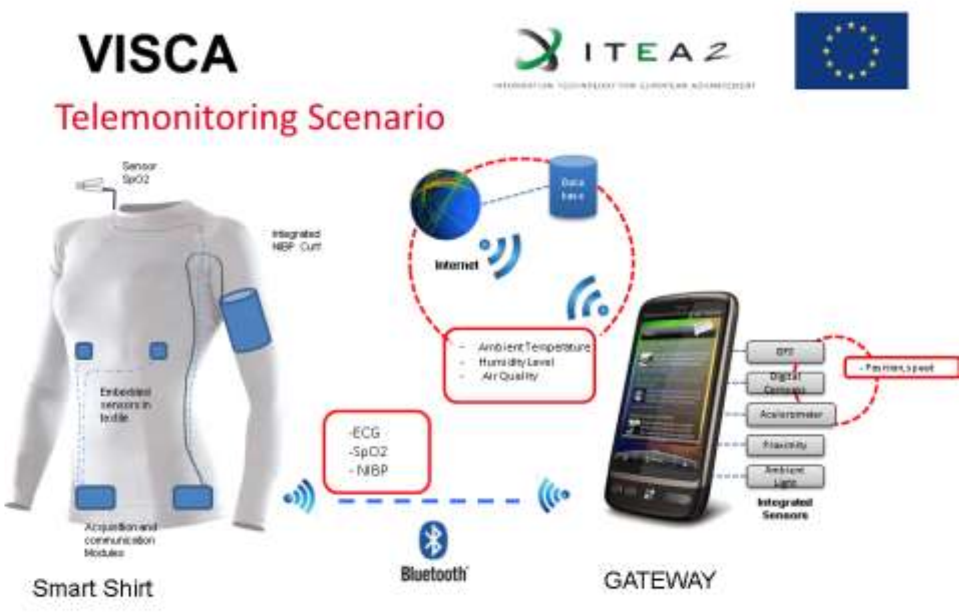
5.5 UC#5. BP Measurement Process

Use case number	VISCA UC#5
Use case name	BP Measurement Process (Telemonitoring Scenario) .
Author/partner	Ricardo Ruiz/ RGB Medical Devices
Summary	In this Scenario, RGB Medical will adapt Home medical Blood Pressure Monitoring Device to the sensing technology of smart cards readers developed within VISCA. This process will require that the patient is able to Log In or follow the authentication process, so the UC#1 requirements must be fulfilled in order to conduct appropriately this UC.
Rationale	Monitorized vital signs and life data information about a patient at home is compromised when a telemedicine session is started. This characteristic and the nature of transmitted information require high requisites in terms of security.

5.5.1 Use case description

- Uploading biometrical measures to healthcare data server.

The concept is that NIBP (Non Invasive Blood Pressure) Module is connected via BT (locally) to the mobile. At every moment, the mobile has complete control over the NIBP measuring device. The role of the smartphone will be to act as User Identificator , providing user Interface, Gateway, and Patient "motivator" applications to make sure that the monitoring process not only of one single measurement but all along the established medical surveyance period is carried out accordingly.



Resources Required

5.5.2 Contextual settings

5.5.2.1 Context description

Peter starts a BP(blood pressure) monitoring session. He will use the BP monitor (use of smart shirt is optional) and put the cuff in the arm. Then he uses the dedicated mobile application in his smartphone to follow UC#1 procedure to access his private account of his telemonitoring service provided by his health insurance company.

Once the login in is performed, then Peter will select the BP measurement application and follow the indications in the mobile to carry out the measurement. When he finalizes the measurement, it is sent to a Web service platform, and the device is remotely prompted to shut down.

NORMAL WORKFLOW:

Basic course of action (path)

1. The PERSON activates the mobile App. for Vital Signs VISCA data collection.
2. The PERSON is identified, and authenticated (a safe/secure communication channel is established using VISCA technology)
3. The application reports if last measurements have been transmitted appropriately. In case not, the user is prompted to do it now.
4. The PERSON switches ON the sensoring BP module.
5. The mobile App shows that it has established connection and measurement can be started.
6. The PERSON presses the activation button to initiate measurement
7. The measurement takes place, and resulting data is shown in the mobile´s screen.
8. PERSON's BP is being added to the health status log
9. The medical monitor disconnects itself when some time has passed or else when medical session is finished.

Alternate courses of action (path)

1. The PERSON initiates the BP measurement.
2. The PERSON could not be identified or authenticated (a safe/secure communication channel is not established).
3. BP data is stored in the mobile until this issue is solved.
4. VISCA coach verifies the problem upon request (the PERSON calls a service number).
5. If solved, PERSON's BP latest data not transmitted and collected in the mobile is added to the health status log.

5.5.2.2 Resources

The main resources:

- Mandatory: A wearable BP measuring device with very specific functional requirements, e.g. capability to be remotely switched off.
- OPTIONAL) A smart shirt in case of patients that have special requirements of ergonomy.
- Access to Internet information from the mobile (if outdoors, e.g. external temperature, likely weather, etc)

Of course, also UC#1 resources are needed:

- Mobile Device capable to host an Hypervisor (a.e. XEN)
- Main OS
- Virtual OS (virtual machines) running isolated from the main smartphone OS
- Virtual secure element host in the isolated virtual OS
- Software interface that allows secure apps to communicate with secure virtual element on the virtual OS
- Service application installed on the Smartphone
- Remote VISCA server (synchronization functionalities)

- Service app server (app back-end)

5.5.3 Functional description

Preconditions and assumptions	Availability of NIBP medical device BP monitor needs to be connected to the VISCA platform via a smartphone. Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process The user enters the telemedicine application Mobile VISCA App finalizes vital sign collecting data process and sends data to the platform.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	Alternative flow is defined in the use case description
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services. BP data is captured and transmitted from sensor to mobile and then to web platform PERSON's BP is added to the health status log.

5.5.4 Constraints

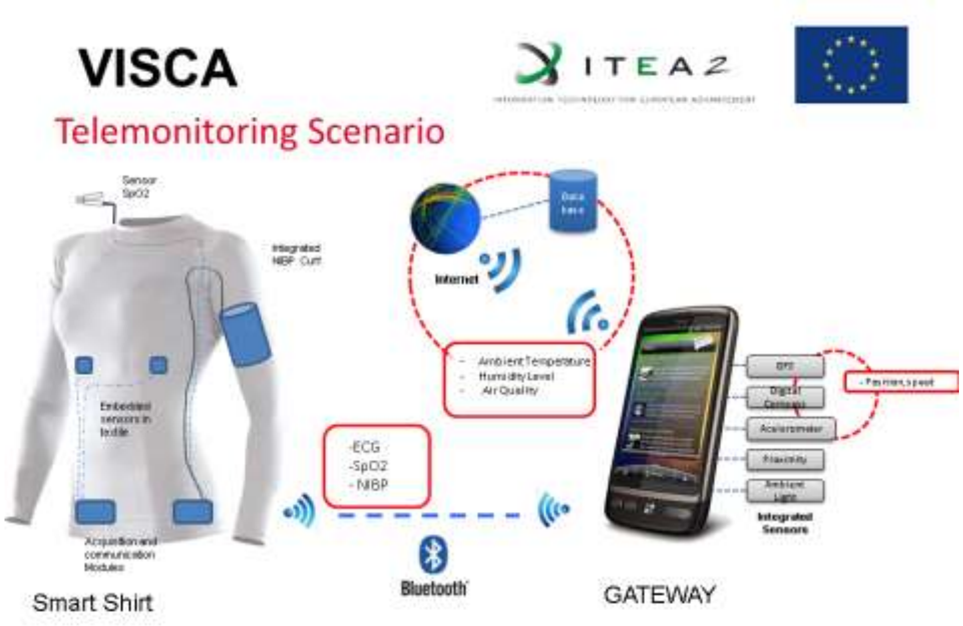
Location	N/A
Environmental characteristics	N/A
Legislation and standards	Data interoperability at Device level will be according to ISO11073 norm.

5.6 UC#6. SpO2 Measurement Process

Use case number	VISCA UC#6
Use case name	SpO2 (Oxygen Saturation) Measurement Process (Telemonitoring Scenario) .
Author/partner	Ricardo Ruiz/ RGB Medical Devices
Summary	In this Scenario, RGB Medical will adapt Home medical Oxygen Saturation Monitoring Device to the sensing technology of smart cards readers developed within VISCA. This process will require that the patient is able to Log In or follow the authentication process, so the UC#1 requirements must be fulfilled in order to conduct appropriately this UC.
Rationale	Monitorized vital signs and life data information about a patient at home is compromised when a telemedicine session is started. This characteristic and the nature of transmitted information require high requisites in terms of security.

5.6.1 Use case description

- Uploading SpO2 biometrical measures to healthcare data server.
The concept is that SpO2 (Oxygen Saturation) Module is connected via BT (locally) to the mobile. At every moment, the mobile has complete control over the SpO2 measuring device. The role of the smartphone will be to act as User Identificator , providing user Interface, Gateway, and Patient "motivator" applications to make sure that the monitoring process not only of one single measurement but all along the established medical surveyance period is carried out accordingly.



Resources Required

5.6.2 Contextual settings

5.6.2.1 Context description

Peter starts a SpO2 (Oxygen Saturation) monitoring session. He will use the SpO2 monitor (use of smart shirt is optional) and put the Senor in the ear or finger. Then he uses the dedicated mobile application in his smartphone to follow UC#1 procedure to access his private account of his telemonitoring service provided by his health insurance company.
Once the login in is performed, then Peter will select the SpO2 measurement application and follow the indications in the mobile to carry out the measurement. When he finalizes the measurement, it is sent to a Web service platform, and the device is remotely prompted to shut down.

NORMAL WORKFLOW:

Basic course of action (path)

10. The USER activates the mobile App. for Vital Signs VISCA data collection.
11. The USER is identified, and authenticated (a safe/secure communication channel is established using VISCA technology)
12. The application reports if last measurements have been transmitted appropriately. In case not, the user is prompted to do it now.
13. The USER switches ON the sensoring SPO2 module.
14. The mobile App shows that it has established connection and measurement can be started.
15. The measurement takes place, and resulting data is shown in the mobile´s screen.
16. USERs SPO2 is being added to the health status log
17. The medical monitor disconnects itself when some time has passed or else when medical session is finished.

Alternate courses of action (path)

6. The USER initiates the SPO2 measurement.
7. The USER could not be identified or authenticated (a safe/secure communication channel is not established).
8. SPO2 data is stored in the mobile until this issue is solved.
9. VISCA coach verifies the problem upon request (the USER calls a service number).
10. If solved, PERSON's SPO2 latest data not transmitted and collected in the mobile is added to the health status log.
11.

5.6.2.2 Resources

The main resources:

- Mandatory: A wearable SPO2 measuring device with very specific functional requirements, e.g. capability to be remotely switched off.
- OPTIONAL) A smart shirt in case of patients that have special requirements of ergonomy.
- Access to Internet information from the mobile (if outdoors, e.g. external temperature, likely weather, etc)

Of course, also UC#1 resources are needed:

- Mobile Device capable to host an Hypervisor (a.e. XEN)
- Main OS
- Virtual OS (virtual machines) running isolated from the main smartphone OS
- Virtual secure element host in the isolated virtual OS
- Software interface that allows secure apps to communicate with secure virtual element on the virtual OS

- Service application installed on the Smartphone
- Remote VISCA server (synchronization functionalities)
- Service app server (app back-end)

5.6.3 Functional description

Preconditions and assumptions	Availability of SPO2 medical device SPO2 monitor needs to be connected to the VISCA platform via a smartphone. Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process The user enters the telemedicine application Mobile VISCA App finalizes vital sign collecting data process and sends data to the platform.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	Alternative flow is defined in the use case description
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services. SPO2 data is captured and transmitted from sensor to mobile and then to web platform PERSON's SPO2 is added to the health status log.

5.6.4 Constraints

[Please identify constraints that may restrict the operations of an actor, execution of the use case or the interactions between actors and the use case, or are associated with the use case environment]

Location	N/A
Environmental characteristics	N/A
Legislation and standards	Data interoperability at Device level will be according to ISO11073 norm.

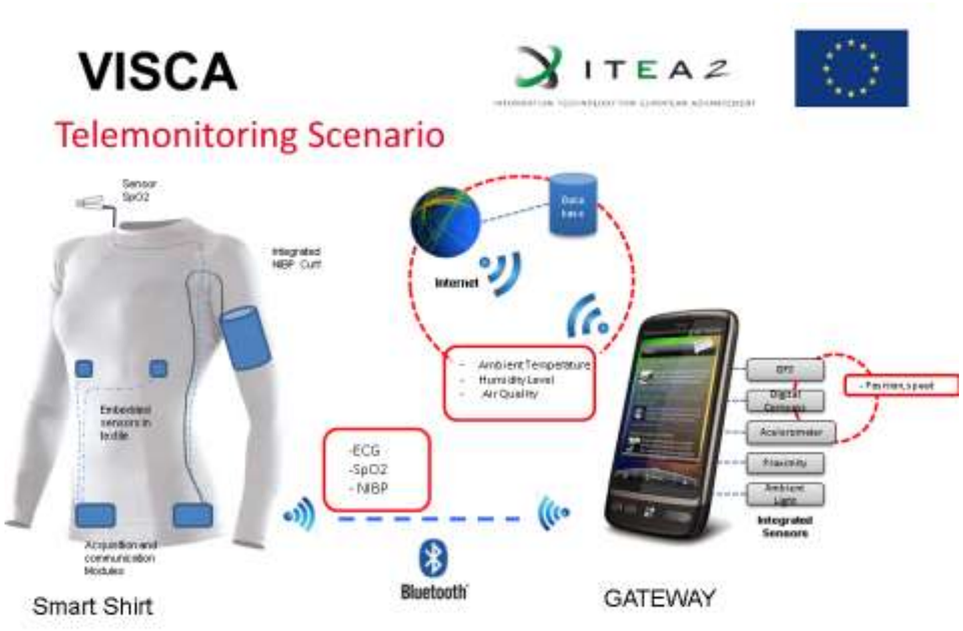
5.7 UC#7. ECG Measurement Process

Use case number	VISCA UC#7
Use case name	ECG (Electrocardiography) Measurement Process (Telemonitoring Scenario) .
Author/partner	Ricardo Ruiz/ RGB Medical Devices
Summary	In this Scenario, RGB Medical will adapt Home ECG (Electrocardiography) Monitoring Device to the sensing technology of smart cards readers developed within VISCA. This process will require that the patient is able to Log In or follow the authentication process, so the UC#1 requirements must be fulfilled in order to conduct appropriately this UC.
Rationale	Monitorized vital signs and life data information about a patient at home is compromised when a telemedicine session is started. This characteristic and the nature of transmitted information require high requisites in terms of security.

5.7.1 Use case description

- Uploading ECG biometrical measures to healthcare data server.

The concept is that ECG Module is connected via BT (locally) to the mobile. At every moment, the mobile has complete control over the ECG measuring device. The role of the smartphone will be to act as User Identificator , providing user Interface, Gateway, and Patient "motivator" applications to make sure that the monitoring process not only of one single measurement but all along the established medical surveyance period is carried out accordingly.



Resources Required

5.7.2 Contextual settings

5.7.2.1 Context description

Peter starts a ECG (Electrocardiography) monitoring session. He will use the ECG monitor (use of smart shirt is optional) or else put electrodes in the body at pre-established locations. Then he uses the dedicated mobile application in his smartphone to follow UC#1 procedure to access his private account of his telemonitoring service provided by his health insurance company.
Once the login in is performed, then Peter will select the ECG measurement application and follow the indications in the mobile to carry out the measurement. When he finalizes the measurement, it is sent to a Web service platform, and the device is remotely prompted to shut down.

NORMAL WORKFLOW:

Basic course of action (path)

18. The USER activates the mobile App. for Vital Signs VISCA data collection.
19. The USER is identified, and authenticated (a safe/secure communication channel is established using VISCA technology)
20. The application reports if last measurements have been transmitted appropriately. In case not, the user is prompted to do it now.
21. The USER switches ON the sensoring ECG module.
22. The mobile App shows that it has established connection and measurement can be started.
23. The measurement takes place, and resulting data is shown in the mobile´s screen.
24. USERs ECG is being added to the health status log
25. The medical monitor disconnects itself when some time has passed or else when medical session is finished.

Alternate courses of action (path)

12. The USER initiates the ECG measurement.
13. The USER could not be identified or authenticated (a safe/secure communication channel is not established).
14. ECG data is stored in the mobile until this issue is solved.
15. VISCA coach verifies the problem upon request (the USER calls a service number).
16. If solved, USER´S ECG latest data not transmitted and collected in the mobile is added to the health status log.
17.

5.7.2.2 Resources

The main resources:

- Mandatory: A wearable ECG measuring device with very specific functional requirements, e.g. capability to be remotely switched off.
- OPTIONAL) A smart shirt in case of patients that have special requirements of ergonomy.
- Access to Internet information from the mobile (if outdoors, e.g. external temperature, likely weather, etc)

Of course, also UC#1 resources are needed:

- Mobile Device capable to host an Hypervisor (a.e. XEN)
- Main OS
- Virtual OS (virtual machines) running isolated from the main smartphone OS
- Virtual secure element host in the isolated virtual OS

- Software interface that allows secure apps to communicate with secure virtual element on the virtual OS
- Service application installed on the Smartphone
- Remote VISCA server (synchronization functionalities)
- Service app server (app back-end)

5.7.3 Functional description

Preconditions and assumptions	Availability of ECG medical device ECG monitor needs to be connected to the VISCA platform via a smartphone. Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process The user enters the telemedicine application Mobile VISCA App finalizes vital sign collecting data process and sends data to the platform.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	Alternative flow is defined in the use case description
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services. ECG data is captured and transmitted from sensor to mobile and then to web platform USER's ECG is added to the health status log.

5.7.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	Data interoperability at Device level will be according to ISO11073 norm.

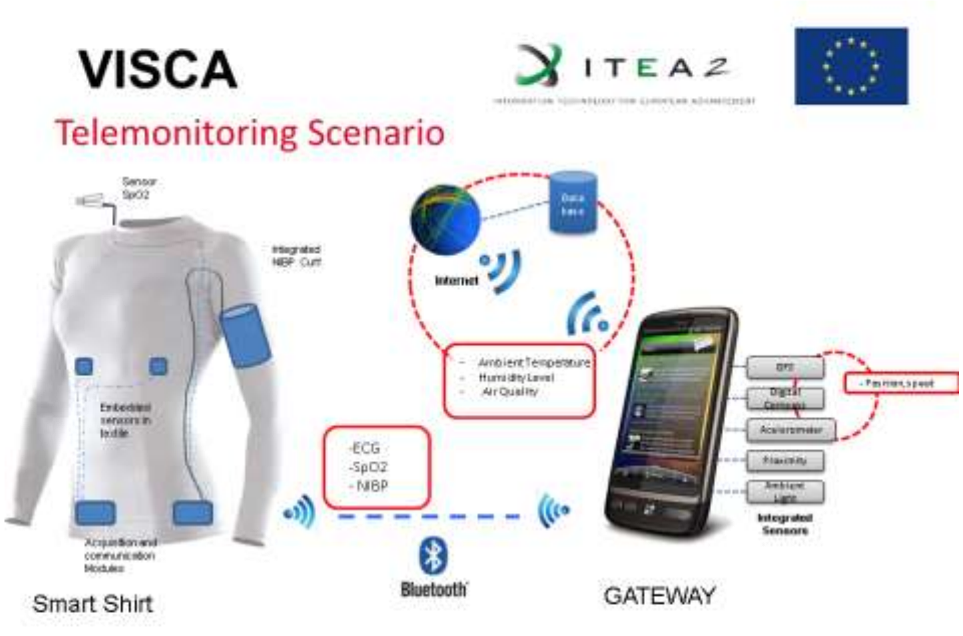
5.8 UC#8. Multiparameter VS Measurement Process

Use case number	VISCA UC#8
Use case name	BP, SpO2 and ECG (Multiparameter Vital Signs) Measurement Process (Telemonitoring Scenario) .
Author/partner	Ricardo Ruiz/ RGB Medical Devices
Summary	In this Scenario, RGB Medical will provide three types of sensors that can be simultaneously used in combination with the sensing technology of smart cards readers developed within VISCA. This process will require that the patient is able to Log In or follow the authentication process, so the UC#1 requirements must be fulfilled in order to conduct appropriately this UC.
Rationale	Monitorized vital signs and life data information about a patient at home is compromised when a telemedicine session is started. This characteristic and the nature of transmitted information require high requisites in terms of security.

5.8.1 Use case description

- Uploading ECG biometrical measures to healthcare data server.
The concept is that de different Vital Sign sensors are connected via BT (locally) to the mobile. At every moment, the mobile has complete control over each measuring device. The role of the smartphone will be to act as User Identificator , providing user Interface, Gateway, and Patient "motivator" applications to make sure that the monitoring process not only of one single measurement but all along the established medical surveyance period is carried out accordingly.

This use case differes to the previous UC#5, UC#6 and UC#7 in the fact that here the three signals can be taken simultaneously or else following a specific order. Technically, separate BT channels must be provided to work under these conditions , but at the time of measurement, the previous Use Cases will be used in the same way. The user interface provides a user friendly way to help the user carry out the session from the beginning to the end, following the instructions prompted in the screen.



VISCA

Telemonitoring Scenario

Resources Required

5.8.2 Contextual settings

5.8.2.1 Context description

Peter starts a Mulitiparameter Monitoring session. He will use the ECG, SpO2 and BP monitors (use of smart shirt is optional) as indicated in previous Use cases. Then he uses the dedicated mobile application in his smartphone to follow UC#1 procedure to access his private account of his telemonitoring service provided by his health insurance company.
Once the login in is performed, then Peter will select the Multiparameter measurement application and follow the indications in the mobile to carry out the measurement. When he finalizes the measurement, it is sent to a Web service platform, and the device is remotely prompted to shut down.

NORMAL WORKFLOW:

Basic course of action (path)

26. The USER activates the mobile App. for Vital Signs VISCA data collection.
27. The USER is identified, and authenticated (a safe/secure communication channel is established using VISCA technology)
28. The application reports if last measurements have been transmitted appropriately. In case not, the user is prompted to do it now.
29. The USER switches ON the sensoring modules.
30. The screen indicated that a BP measurement will take place. The mobile App shows that it has established connection and measurement can be started.
31. The USER presses the activation button to initiate measurement
32. The measurement takes place, and resulting data is shown in the mobile´s screen.
33. Then the application goes on to the measurement of SpO2 and then ECG as indicated in previous UCs .
34. USERs Vital Signs captured data are being added to the health status log
35. Each medical monitor disconnects itself when some time has passed or else when medical session is finished.

Alternate courses of action (path)

18. The USER initiates the Multiparameter Vital Sign (VS) measurement.
19. The USER could not be identified or authenticated (a safe/secure communication channel is not established).
20. VS data is stored in the mobile until this issue is solved.
21. VISCA coach verifies the problem upon request (the USER calls a service number).
22. If solved, USER´S VS latest data not transmitted and collected in the mobile is added to the health status log.

5.8.2.2 Resources

The main resources:

- Mandatory: wearable VS measuring device with very specific functional requirements, e.g. capability to be remotely switched off.
- OPTIONAL) A smart shirt in case of patients that have special requirements of ergonomy.
- Access to Internet information from the mobile (if outdoors, e.g. external temperature, likely weather, etc)

Of course, also UC#1 resources are needed:

- Mobile Device capable to host an Hypervisor (a.e. XEN)
- Main OS
- Virtual OS (virtual machines) running isolated from the main smartphone OS
- Virtual secure element host in the isolated virtual OS
- Software interface that allows secure apps to communicate with secure virtual element on the virtual OS
- Service application installed on the Smartphone
- Remote VISCA server (synchronization functionalities)
- Service app server (app back-end)

5.8.3 Functional description

Preconditions and assumptions	Availability of VS medical devices VS monitor needs to be connected to the VISCA platform via a smartphone. Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process The user enters the telemedicine application Mobile VISCA App finalizes vital sign collecting data process and sends data to the platform.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	Alternative flow is defined in the use case description
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services. VS data is captured and transmitted from sensor to mobile and then to web platform USER's VS is added to the health status log.

5.8.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	Data interoperability at Device level will be according to ISO11073 norm.

5.9 UC#9. Visca Call Center Process

Use case number	VISCA UC#9
Use case name	VisCa Call Center Process
Author/partner	Kuveyt Turk
Summary	Visca user shall call Visca agents in Visca Call Center to get information about their account, transactions and update their information stored in Visca system.
Rationale	The procedure for Visca Call Center operations should be well defined for users and helpful for user to answer their questions and solve the customer problems.

5.9.1 Use case description

The end user shall ask for help from Visca agents in Call Center of Visca or the related bank. The following operations will perform in Visca Call Center by user.

a. User gives requested personal information to Visca agent to complete the authentication process for call center.

b. Learn the transactions performed via Visca via internet or any mall for desired date.

c. Learn the transaction limits of Visca.

d. Change transaction limits of Visca.

e. Apply for a new Visca account.

f. Apply for a supplementary Visca.

g. Learn the list of e-commerce sites have "pay Visca" option.

h. Learn the list of shopping centers etc. have "pay Visca" option.

i. Apply to cancel or suspend Visca account.

5.9.2 Contextual settings

5.9.2.1 Context description

The end user perform some task with the help of Visca Call Center agent.

5.9.2.2 Resources

a. Smart Mobile device
b. Authenticated Smart mobile application
c. Authenticated Credit cards on the application
d. Call Center system and agent.

5.9.3 Functional description

Preconditions and assumptions	Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process

Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services.

5.9.4 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.10 UC#10. Visca Account Management Process

Use case number	VISCA UC#10
Use case name	VisCa Account Management Process
Author/partner	Kuveyt Turk
Summary	The transactions and displays that a VisCa user shall carry out through the application to manage Visca account and transactions.
Rationale	The procedure for using Visca account management dashboard should be designed to help the end user to complete his transactions and to get needed information about his Visca account.

5.10.1 Use case description

The end user shall use the VisCa application's account management dashboard to perform following tasks.

j. Display transactions performed via Visca, internet or any mall by selected date.

k. Display slip information of any completed transaction.

l. Display the transaction limits of Visca.

m. Request the change transaction limits of Visca.

n. Apply for a new Visca account.

o. Apply for a supplementary Visca.

p. Display the list of e-commerce sites have "pay Visca" option.

q. Display the list of shopping centers etc. have "pay Visca" option.

r. Manage the payment process of Visca transactions through a bank account.

s. Apply to cancel or suspend Visca account.

5.10.2 Contextual settings

5.10.2.1 Context description

The end user wants to monitor the Visca account to control his transactions and limits.

5.10.2.2 Resources

e. Smart Mobile device
f. Authenticated Smart mobile application
g. Authenticated Credit cards on the application

5.10.3 Functional description

Preconditions and assumptions	Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process

Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services.

5.10.4 Constraints

[Please identify constraints that may restrict the operations of an actor, execution of the use case or the interactions between actors and the use case, or are associated with the use case environment]

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.11 UC#11. End-User Process

Use case number	VISCA UC#11
Use case name	Customer's application for and payment certificate issuance process (certificate is a replacement for traditional credit card)
Author/partner	Kuveyt Turk
Summary	This use case defines how end user applies for a payment certificate and how the certificate is issued.
Rationale	

5.11.1 Use case description

1. The customer applies for a payment certificate online through the bank's website and the applicant's information is collected during this application process.

2. Upon completion of the evaluation process by the bank's credit department, If the customer is evaluated as eligible, a certificate (in our case the certificate replaces the plastic credit card) is generated by the bank.

3. The certificate is sent to VISCA cloud platform. The certificate is signed by the VISCA cloud platform (a root certificate will be needed) and associated with the customer in their records.

4. A link to the certificate is sent to the customer by e-mail or SMS for activation. Customer activates the certificate through the link received. In order to activate the certificate, the customer first needs to install the application (VM) on his/her mobile device or PC. The certificate is installed on customer's device during the activation process and is now ready to use for payment.

5.11.2 Contextual settings

5.11.2.1 Context description

A banks's customer wants to obtain a payment certificate via a bank and a payment certificate is generated and issued to the end user.

5.11.2.2 Resources

The main resources:

- Smart Mobile device
- Authenticated Smart mobile application
- Authenticated payment certificates on the application
- A certificate authentication and authorization server in the cloud environment.

5.11.3 Functional description

[Please describe the functional characteristics of the use case according to following table]

Preconditions and assumptions	Mobile app installed in the Smartphone.
Trigger	The user applies for a payment certificate.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	A payment certificate is successfully issued for the customer and ready for payment.

5.11.4Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	MasterCard/Visa must authorize the banks to issue certificates as an alternative to plastic cards. A new operations framework need to be set up between banks and MasterCard/Visa

5.12 UC#12. End-User Process

Use case number	VISCA UC#12
Use case name	Self-Service provisioning
Author/partner	Kuveyt Turk
Summary	The application (VM) must provide self-service features for the customer
Rationale	The customer may want to use the payment certificate on different devices (Smart Phone, Tablet, Laptop, PC)

5.12.1Use case description

Certificate download to another device

1. The customer starts VISCA VM on his/her device and enter the PIN.
2. The customer connects to the VISCA cloud platform and downloads the payment certificate to another device. (mobile phone, tablet, PC)

Certificate revocation

1. The customer starts VISCA VM on his/her device and enter the PIN.
2. Customer lists the valid certificates.
3. Customer disables any of the valid certificate in case of a need.

5.12.2Contextual settings

5.12.2.1 Context description

A banks's customer wants to manage his/her payment certificates.

5.12.2.2 Resources

The main resources:

- Smart Mobile device
- Authenticated Smart mobile application
- Authenticated payment certificates on the application
- A certificate authentication and authorization server in the cloud environment.
- This will require a provisioning system that transfers provisioning data among the bank's systems, retailer's systems and the VISCA cloud platform.
-

5.12.3Functional description

Preconditions and assumptions	Mobile app installed in the Smartphone.
Trigger	The user wants to disable his/her payment certificates.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	Successfully disabled payment certificate.

5.12.4Constraints

Location	N/A
Environmental characteristics	A secure connection and data transfer protocols are required during the data exchange between customer's device and VISCA platform
Legislation and standards	N/A

5.13 UC#13. End-User Process

Use case number	VISCA UC#13
Use case name	The VISCA platform must provide features that enable customer to do both online or conventional shopping at their convenience.
Author/partner	Kuveyt Turk
Summary	This use case defines how the customer makes payment during online shopping.
Rationale	

5.13.1Use case description

3. The customer goes to checkout screen on the shopping Website.
4. The customer starts VISCA VM application on his/her mobile device and enters his PIN for authentication. Then he/she selects the certificate for payment.
5. He/she presses the generate payment token button (one time payment token is generated.)
6. He/she enters the token on payment screen on the website.
7. The Website connects to the bank or VISCA platform to verify that the certificate is valid and verifies that the token generated is a valid token.
8. If both the certificate and the token is valid then the payment is processed.

5.13.2Contextual settings

5.13.2.1 Context description

A banks's customer wants easy and fast payment process during online shopping.

5.13.2.2 Resources

The main resources:

- Smart Mobile device
- Authenticated Smart mobile application
- Authenticated payment certificates on the application
- A certificate authentication and authorization server in the cloud environment.
- This will require a provisioning system that transfers provisioning data among the bank's systems, retailer's systems and the VISCA cloud platform.
-

5.13.3Functional description

[Please describe the functional characteristics of the use case according to following table]

Preconditions and assumptions	Mobile app installed in the Smartphone.
Trigger	The user makes online shopping.
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	Successful payment during online shopping and updated customer's credit account.

5.13.4Constraints

Location	N/A
Environmental characteristics	It is assumed that a new platform alternative to Virtual POS has been developed that enables secure payment process with the payment certificate.
Legislation and standards	N/A

5.14 UC#14. VisCa Processing Time

Use case number	VISCA UC#14
Use case name	VisCa Processing Time
Author/partner	Kuveyt Turk
Summary	As non-funtional requirement, user should complete transactions in acceptable time period while using Visca in shopping.
Rationale	The response time shall be defined to control the performance metrics during the application's testing period. Different mobile devices with different technical feautures shall be used during performance testing.

5.14.1Use case description

After the End-user have his/her shopping process, during the payment time (on the internet or in the mall), the end user should be happy with the processing time. There shouldn't be any delays for system response.

5.14.2Contextual settings

5.14.2.1 Context description

In online shopping or in daily life Visca users wants to complete the payment process effectively.

5.14.2.2 Resources

h. Smart Mobile device
i. Authenticated Smart mobile application
j. Authenticated Credit cards on the application

5.14.3Functional description

Preconditions and assumptions	Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services.

5.14.4Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.15 UC#15. Optional Visca Payment Process

Use case number	VISCA UC#15
Use case name	Visual introdution
Author/partner	Kuveyt Turk
Summary	Visca platform should provide visual instruction for using Visca system
Rationale	the customer needs to see visual instruction how to use Visca platform, how to get authoriaction or move a physical card to Visca platforms.

5.15.1Use case description

The customer needs to see visual instruction using Visca system.

9. Visca application should give required information via visual form
10. User may apply to move ohysical card to Visca platform just showing the credit card to the application
11. The application take the cards screen shots and save de card number
12. Identify and confirm the customer with some secret questions
13. The process can recorded for any conflict
14. Application process can be done anywhere without contact the bank location

5.15.2Contextual settings

5.15.2.1 Context description

The end user needs visual instruction and move to Visca platform

5.15.2.2 Resources

k. Smart Mobile device
l. Authenticated Smart mobile application
m. Authenticated Credit cards on the application

5.15.3Functional description

Preconditions and assumptions	Hypervisor and mobile app is installed in the Smartphone.
Trigger	The user should acces Visual instruction and moves to Visca platform anywhere.
Normal flow	Normal flow is defined in the use case description.
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user can move physical card with visual instruction with no touch the bank’s branch.

5.15.4Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.16 UC#16. Dynamic Barcode Visca Process

Use case number	VISCA UC#16
Use case name	Dynamic Barcode
Author/partner	Kuveyt Turk
Summary	The end user will take the authorization automatically with the dynamic barcode during the shopping
Rationale	The end user can be authorized easily while shopping small sums

5.16.1Use case description

If the end user prefer to use dynamic barcode, he/she can do payment process for small sums.

15. The customer goes to checkout screen on the shopping Website.
16. The customer shows barcode application which is already implement for the mobile device.
17. He/she take the automatic provision without any password authentication.
18. There should be defined optional small sums such as 0-15, 16-50 and 50 Euro and up
19. 0-15 Euro sums should be paid with dynamic barcode.
20. 16-50 Euro sums should be required barcode and just SMS notification
21. 51 Euro and up sums should be required barcode and password authentication

5.16.2Contextual settings

5.16.2.1 Context description

The end user wants to pay small sums easily and automatically without any password process or authorization.

5.16.2.2 Resources

n. Smart Mobile device
o. Authenticated Smart mobile application
p. Authenticated Credit cards on the application
q. Authenticated Dynamic Barcode on the mobile device

5.16.3Functional description

Preconditions and assumptions	Hypervisor, mobile app and dynamic barcode should be installed in the Smartphone.
Trigger	The user prefers to use the barcode application
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in automatically and easily with barcode application

5.16.4Constraints

Location	N/A

Environmental characteristics	N/A
Legislation and standards	There should be classified small sums for barcode payments. Such as 0-15, 16-50 and 51 Euro and up

5.17 UC#17. Cancel/Suspend Visca Process

Use case number	VISCA UC#17
Use case name	Cancel/Suspend Visca Process
Author/partner	Kuveyt Turk
Summary	The end user shall cancel or suspend Visca if he requests.
Rationale	There should be an option for user to cancel Visca or suspend Visca for a limited time. There should be some check points during cancel/suspend process.

5.17.1Use case description

If the end user choose the cancel or suspend Visca, he shall perform cancel or suspend period as following.

t. *Cancel process*

a. Request "Cancel Visca" option with Visca Account Management Dashboard.

b. Evaluation cancel request of user.

c. Control the transactions and their payment status.

d. Ask for remaining payments from the end user if there is.

e. Response the cancel request positively or negatively by stating the causes.

f. If the process is completed positively, related Visca cannot be used any more.

u. *Suspend process*

a. Request "Suspend Visca" option with Visca Account Management Dashboard inclusing the reasons of the request.

b. Evaluation suspend request of user with the reasons of the request.

c. If suspend request is because of emergency reasons the process shall be completed immediately considering the security issues.

d. Control the transactions and their payment status.

e. Ask for remaining payments from the end user if there is.

f. Response the cancel request positively or negatively by stating the causes.

g. If the process is completed positively, related Visca cannot be used for a specific time period. After the defined suspending end time comes, the user shall be able to use Visca.

5.17.2Contextual settings

5.17.2.1 Context description

The end user wants to cancel Visca for any reason or wants to suspend Visca for a limited time. Evaluation process of user's request can be automatically according to predefined parameters including a final approval by Visca agents.

5.17.2.2 Resources

r. Smart Mobile device

s. Authenticated Smart mobile application

t. Authenticated Credit cards on the application

5.17.3Functional description

Preconditions and assumptions	Hypervisor and mobile app installed in the Smartphone.
Trigger	The user starts the login process
Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in, the temporary token session is created and he accesses to his private services.

5.17.4Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	N/A

5.18 UC#18. Optional Visca Payment Process

Use case number	VISCA UC#18
Use case name	Defined Optional Visca bank
Author/partner	Kuveyt Turk
Summary	The customer should define default Visca bank for payment
Rationale	If the customer use many Visca Platform (bank), The customer preference should be defined with default setting

5.18.1Use case description

If the end user prefer to many different Visca bank solution, he/she can define default Visca bank for payment.

22. The customer goes to checkout screen on the shopping Website.
23. The customer payment process start with the defined Visca bank
24. Before the continue payment process, application should remind the prefer the other bank which is already defined for the customer.
25. He/she can change default settings easily
26. He/she can easily suspend or the cancel some of the Visca bank platform

5.18.2Contextual settings

5.18.2.1 Context description

The end user wants use default defined Visca Bank to any payment process

5.18.2.2 Resources

u. Smart Mobile device
v. Authenticated Smart mobile application
w. Authenticated Credit cards on the application

5.18.3Functional description

Preconditions and assumptions	Hypervisor and mobile app is installed in the Smartphone.
Trigger	The user can choose optional Visca bank which has already defined.
Normal flow	Normal flow is defined in the use case description.
Alternative flow (optional)	No alternative flows in the process
Post-conditions	The user is logged in automatically and easily with barcode application

5.18.4Constraints

[Please identify constraints that may restrict the operations of an actor, execution of the use case or the interactions between actors and the use case, or are associated with the use case environment]

Location	Visca Mobile application should manage these type of optional Visca bank selection with in the same application
Environmental	N/A

characteristics	
Legislation and standards	N/A

5.19 UC#19. Customer Payment Card Registration and Wallet app. Personalization

Use case number	(To be defined later)
Use case name	Customer Payment Card Registration and Wallet app. personalisation
Author/partner	SmartSoft
Summary	Customer Payment Card Registration process to the VisCa Platform
Rationale	Card Info will be stored in PSP(Payment System Provider) therefore customer should have a request to the bank for banking card usage

5.19.1Use case description

In this scenario we suppose that in User's Smart Phone There is already TEE(Trusted execution Environment) / Secure Virtual Smart Card For Mobile App platform.

Customer will download VisCa mobile wallet application from a mobile app. Store. For using VisCa tech. Issuer (card owner) bank should support VisCa technology. User can search for supporting banks from mobile wallet. If his/her bank is VisCa ıssuer bank then he/she will select the bank.

a) Wallet application will inform user for VisCa Virtual Card application requirements.

- ➢ For example User has Kuveyt Turk Bank Card - Send a message to Kuveyt Turk)(NAME-SIRNAME Card Numbers last 6 digit and send a message to "1000")

b) Bank will evaluate their customer's application and if Bank will accept the request then bank should create and personalize a new virtual card and send the customer and card information to PSP.

c) PSE will start wallet application personalization. PSP will send OTP message to the customer.

d) Customer fined his/her bank and then push "Add My Card" button.

e) Wallet application will ask for one time Password. Customer will enter OTP and send it to the PSP.

f) PSP will add customer virtual card image to the wallet application's "My Credit Cards" section.

g) Virtual Card Password Selection

h) PSP will inform bank "Virtual Credit Card is Ready for usage"

5.19.2Contextual settings

1.1.1.1 Context description

User application process and wallet personalisation process

1.1.1.2 Resources

The main resources:

- Smart Mobile device
- Internet connection

5.19.3Functional description

Preconditions and assumptions	Smartphone Internet
Trigger	The user starts the installation process

Normal flow	Normal flow is defined in the use case description
Alternative flow (optional)	No alternative flows in the process
Post-conditions	Virtual credit Card is Ready for usage

1.1.2 Constraints

Location	N/A
Environmental characteristics	N/A
Legislation and standards	PSP must have; ➢ Information Security Management System Certification -ISO 27001:2005 ➢ PCI DSS(Payment Card Industry Data Security Standards) Certification

6. Use Cases Summary

Use-cases analysis

Feature-set table

In total, a high number (19) of elementary use cases were submitted by VISCA project Partners. Moreover virtually every partner contributed to this important task, as one of the foundation of the project.
A Feature-set table was established in order to build cartography of VISCA UCs.

Application Areas

Code	Service	General	eCommerce/ eBanking	eHealth
UC#1	Log In/Authentication Process	**X**		
UC#2	End-User Shopping Process		**X**	
UC#3	End-User Shopping Process on Internet		**X**	
UC#4	End-User Application Installation on Smartphone	**X**		
UC#5	BP Measurement Process			**X**
UC#6	SpO2 Measurement Process			**X**
UC#7	ECG Measurement Process			**X**
UC#8	Multiparameter VS Measurement Process			**X**
UC#9	Visca Call Center Process	**X**		
UC#10	Visca Account Management Process	**X**		
UC#11	End User Application for Payment Certificate		**X**	
UC#12	End User Self-Service Process		**X**	
UC#13	End-User Shopping Process		**X**	
UC#14	VisCa Processing Time	**X**		
UC#15	Optional Visca Payment Process		**X**	
UC#16	Dynamic Barcode Visca Process		**X**	
UC#17	Cancel/Suspend Visca Process	**X**		
UC#18	Optional Visca Payment Process		**X**	
UC#19	Customer Payment Card Registration and Wallet app. Personalization		**X**	

Services

Code	Service	Secure Session Initiation	mPayment	mBanking Service	CRM	Health Monitoring	external services API/apps
UC#1	Log In/Authentication Process	X	X	X	X	X	
UC#2	End-User Shopping Process		X	X			
UC#3	End-User Shopping Process on Internet		X	X			
UC#4	End-User Application Installation on Smartphone	X	X	X	X	X	
UC#5	BP Measurement Process	X				X	X
UC#6	SpO2 Measurement Process	X				X	X
UC#7	ECG Measurement Process	X				X	X
UC#8	Multiparameter VS Measurement Process					X	
UC#9	Visca Call Center Process				X		
UC#10	Visca Account Management Process				X		
UC#11	End User Application for Payment Certificate						
UC#12	End User Self-Service Process						
UC#13	End-User Shopping Process						
UC#14	VisCa Processing Time						
UC#15	Optional Visca Payment Process		X				
UC#16	Dynamic Barcode Visca Process		X				
UC#17	Cancel/Suspend Visca Process						
UC#18	Optional Visca Payment Process		X				
UC#19	Customer Payment Card Registration and Wallet app. Personalization		X				

Components

Code	Service	User App	Back-End server	Additional Device/System	VISCA Cloud	Native Components (Camera, BlueTooth…)
UC#1	Log In/Authentication Process	X			X	
UC#2	End-User Shopping Process	X	X		X	
UC#3	End-User Shopping Process on Internet	X	X		X	
UC#4	End-User Application Installation on Smartphone	X				
UC#5	BP Measurement Process	X		X		X
UC#6	SpO2 Measurement Process	X		X		X
UC#7	ECG Measurement Process	X		X		X
UC#8	Multiparameter VS Measurement Process	X	X	X		X
UC#9	Visca Call Center Process				X	
UC#10	Visca Account Management Process				X	
UC#11	End User Application for Payment Certificate	X	X			
UC#12	End User Self-Service Process	X	X			
UC#13	End-User Shopping Process	X	X			X
UC#14	VisCa Processing Time		X		X	
UC#15	Optional Visca Payment Process		X			
UC#16	Dynamic Barcode Visca Process		X			
UC#17	Cancel/Suspend Visca Process	X	X			
UC#18	Optional Visca Payment Process			X		
UC#19	Customer Payment Card Registration and Wallet app. Personalization	X			X	

Master Use-cases

Master Use-Cases (MUCs) are representative embodiments of the aim the project. Moreover, demonstrations that will be made at reviews and symposium have to rely on the MUCs for project consistency. Once the requirements are gathered and the software architecture of the platform defined, a subset of master use cases will be selected, embracing the most representative use cases from the catalogue.

7. Conclusions

The analysis of the State of the Art of the technology concluded that a long way has to be gone in order to develop and deploy a practical, functional and reliable implementation for virtual smart cards that could be accessed through Smart mobile devices.

To pave the way for ViSCa, a set of elementary use cases were gathered, which will set the grounds to illustrate the capabilities of the ViSCa platform in the selected fields of application: banking sector, remote patient care and public services.

The results from the work shown in this document will be used as input for the rest of the tasks belonging to WP2.

8. References

Related white papers Published in: Communications & Media Updates, Health Updates, Privacy Updates, Science, Computers & Technology Updates

[1] "Controlling healthcare user authentication and authorizations" by **Dean Wiech**
http://healthitsecurity.com/2013/11/13/controlling-healthcare-authentication-and-authorizations/

Related White papers:

- HIPAA Violations Incur Multi-Million Dollar Penalties
- White Paper: Achieving HIPAA Compliance
- Three Simple Steps to Protect Patient Privacy
- Deploying virtual security appliances in a healthcare setting
- Creating a secure, compliant healthcare file-sharing solution
- HITPC gets answers to Stage 3 Meaningful Use security questions

[2] Patients Put at Risk By Computer Viruses , Christopher Weaver, Updated June 13, 2013

- http://online.wsj.com/news/articles/SB10001424127887324188604578543162744943762?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424127887324188604578543162744943762.html

[3] Networked Medical Device Cybersecurity and Patient Safety: Perspectives of Health Care Information Security Executives
http://www.deloitte.com/view/en_US/us/Industries/US-federal-government/center-for-health-solutions/eff8b79b48031410VgnVCM2000003356f70aRCRD.htm

[4] Achieving HIPAA Compliance by Absolute Software
http://healthitsecurity.com/2014/01/21/white-paper-achieving-hipaa-compliance/

[5] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[6] FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks, June 13, 2013
http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm

Other related Recommended Readings

- NIST Special Publication 800-82, Revision 1, May 2013

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

- DHS-ICS-CERT "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009
  http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

- ICS-CERT Web Site
  http://ics-cert.us-cert.gov/

[7] Radio Frequency Wireless Technology in Medical Devices - Guidance for Industry and Food and Drug Administration Staff**: August 13, 2013**
http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm

[8] FDA recognizes need for medical device interoperability standards, Jennifer Bresnick,   Date August 15, 2013
http://ehrintelligence.com/2013/08/15/fda-recognizes-need-for-medical-device-interoperability-standards/

Related White Papers:

HIPAA Violations Incur Multi-Million Dollar Penalties
White Paper: Achieving HIPAA Compliance
Three Simple Steps to Protect Patient Privacy
Aspirus Wausau Hospital Simplifies Access to Epic EMR, Enables CPOE
On-Demand Webcast: Why Healthcare Security In 2014 Could Take You By Surprise

[9] FDA issues encryption, authentication rules for medical devices, **Jennifer Bresnick, August 16,2013**
http://healthitsecurity.com/2013/08/16/fda-issues-encryption-authentication-rules-for-medical-devices/

[10] FDA Recommends that Manufacturers Seeking Medical Device Approval Submit Cyber Security Plans
https://rusecure.rutgers.edu/content/fda-recommends-manufacturers-seeking-medical-device-approval-submit-cyber-security-plans

http://www.jdsupra.com/legalnews/fda-recommends-that-manufacturers-seekin-76741/

[11]http://blog.flurry.com/bid/95723/Flurry-Five-Year-Report-It-s-an-App-World-The-Just-Web-Lives-in-It

[12] http://www.ericsson.com/res/docs/2013/consumerlab/smartphone-usage-experience-report.pdf

Additional literature

http://frankmorgner.github.io/vsmartcard/virtualsmartcard/README.html

http://technet.microsoft.com/en-us/library/dn593708.aspx

https://developer.android.com/guide/topics/connectivity/nfc/hce.html

http://pubs.vmware.com/workstation-10