THE ID POINT SERVICE MODEL

Maria Kalske and Mika Kivilompolo

IT Center, P.O.Box 28, FIN-00014 University of Helsinki, Finland, maria.kalske@helsinki.fi
IT Center, P.O.Box 28, FIN-00014 University of Helsinki, Finland, mika.kivilompolo@helsinki.fi

1. ABSTRACT

In the ID Point service model the identification of the user and the delivery of the service are separated from each other. This allows to build centralize services for the cases that would traditionally require visiting at local service point.

2. INTRODUCTION

The University of Helsinki is an academic community of 40,000 students and staff members. It operates at four campuses in Helsinki and at 17 other locations. For users the IT Center provides common IT services like helpdesk, local IT support, IT specialists and IT infrastructure (network connections, user accounts, PC's, servers, data bases, etc.).

The helpdesk of IT Center provides wide range of IT support by email or phone for all users and it is open each weekday from 8 to 17:30. Helpdesk does not provide opportunity for personal visiting. The main limitation for the helpdesk service is that customer cannot be identified adequately before delivering the service.

The IT Center has local service points at all four main campuses in Helsinki. At service point users can visit and have face-to-face service. The main reason for visiting service point is to get services that could not be delivered via email or phone (i.e. services that require user identification). Typically these issues were related to user accounts.
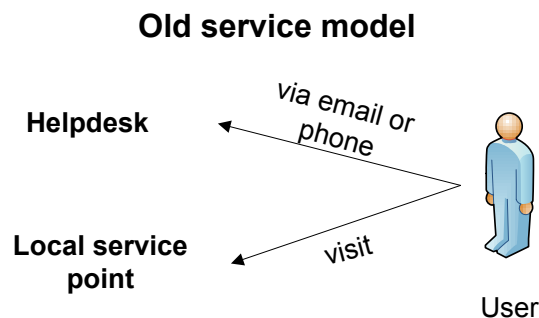
Old service model

Figure 1. In old service model user has to visit local service point in cases when identification is needed before delivering the service.

University research stations are located in 17 different places all over Finland. These places do not have a local service point and therefore a trusted person who could identify users was needed.

The user account management system of the university has been developed during a very long time period of over two decades. It is composed of multiple systems and therefore it is rather complex to use without expertise and good IT skills. Thus, it was not possible to share the user account management workload outside the IT Center.

In Finland we have rather widely used electronic authentication system for public sector called VETUMA. With this system users can be authenticated to a service using strong authentication methods e.g. Finnish bank credentials or a police-issued electronic ID card. From the legal point of view VETUMA authentication is as reliable as identification in person from documents.

During the past few years, we had already made changes on technology and services that decreased user visit amounts at local service points. Therefore most of the opening hours the local service points were on light use i.e. just few visitors per day. For this reason local service points opening hours were cut down to half day at most campuses. At the same time we started to have more calls to helpdesk related on services that only local service point could provide as the user must be identified before delivering the service. The users seem to prefer to call to helpdesk instead of walking to the nearest local service point.

The IT strategy of the university is aiming at developing efficient, equal and centralized IT services for all users. This requires changes on services, service delivery model and staff reallocation to support the strategy. The ratio between local IT services and centralized IT services had recently changed from 90:10 to 60:40.

3. PROBLEMS AND CHALLANGES

One of the strategic goals was to close down three of four local service points in order to release work resources for centralized helpdesk work. However, we did not really have a clue how to do it since there were so many challenges to deal with.

- How to arrange those services where customer needed to be identified before delivering the service?

- Is it possible to share part of the work made at local service point for other unit's service points e.g. (library or facilities service) as those services are typically open for opening hours of the university buildings?

- What kind of new service processes and tools we need?

4. VIDEO SERVICE POINT

First we started solving the challenges with technology, as we IT people always do. We were familiar with video conference technology especially new HD-quality systems like Cisco Telepresence system EX-90. We made the following set-up shown in Fig.2.
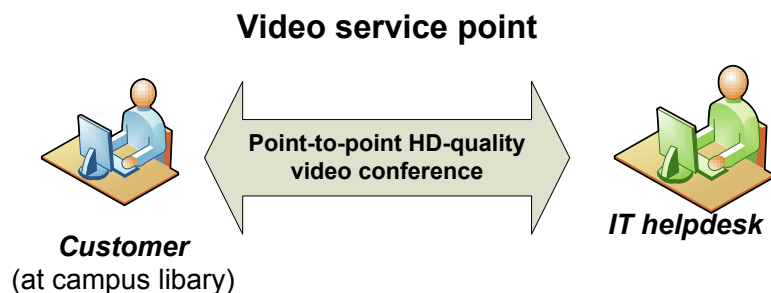
Video service point

Point-to-point HD-quality video conference

Customer
(at campus libary)

IT helpdesk

Figure 2. Set-up of the point-to-point video conference system where one EX-90 device was on IT helpdesk and the other was at campus library.

Service process went like this. Customer touches control panel of EX-90 which opens the connection to similar EX-90 device at helpdesk. The helpdesk officer asks customer to identify herself by a document. After successful identification service can be delivered.

The benefits of this service model were that we could offer personal service from the helpdesk. However there were many drawbacks in this model:

- To build network of video service points needs resources for devices and some extra space

- Devices usability is on rather good level but there seems to be some technology fear

- Devices felt in sleep-mode and were sometimes tricky to wake-up between customers
- The efficiency of the process was not good enough
- Reliability of the customer identification was unclear from the legislation point of view

Next we decided to improve the reliability of the identification part of this model. We discussed with campus library and finally got into an agreement that library officers could do the identification part of Video service point. To do this we had to build a tool where identification information can be transferred from library officer to IT helpdesk. This was actually the starting point which finally led to the development of the ID Point service model.

5. THE ID POINT SERVICE

The ID Point service consists of three components: the ID Point service desk, the ID Point system and the service provider.

The ID Point service desk takes care of customer's identification. The IDP officer checks customer's identity from a valid document and feeds the required information to the IDP system. Collected informations are first names, surname, date of birth, social security number (those who has one), document type and author. Customer may give personal mobile phone number to receive the IDP code or it can be provided on a printed paper.
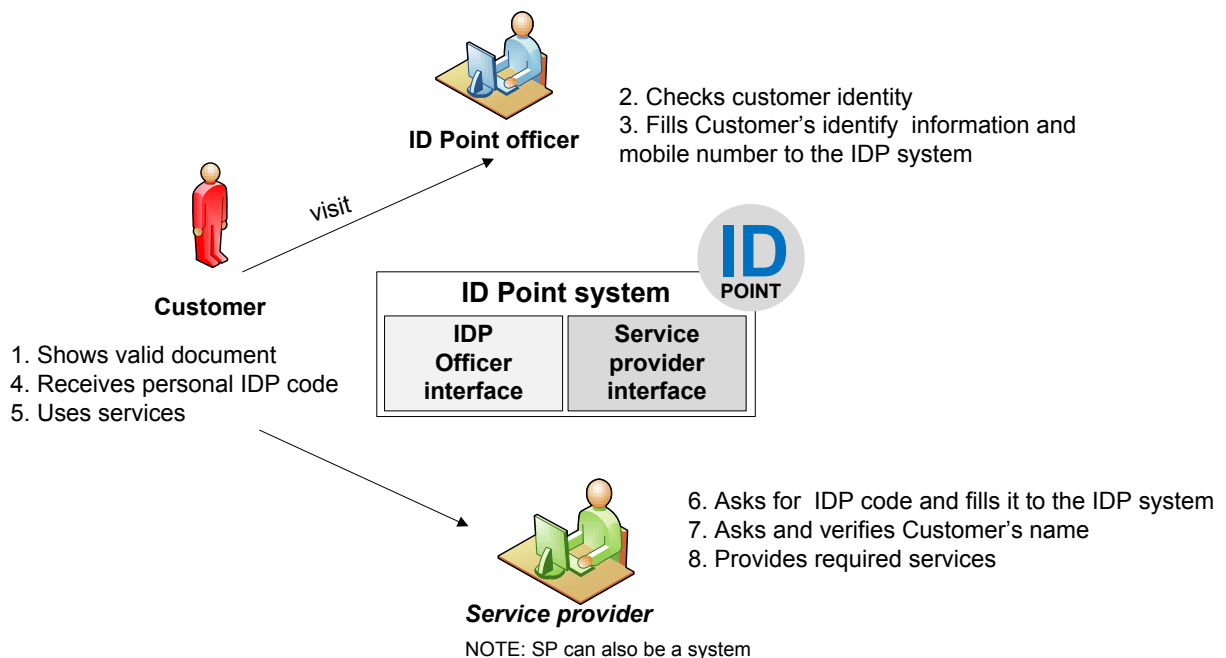
ID Point officer

2. Checks customer identity
3. Fills Customer's identify information and mobile number to the IDP system

Customer

1. Shows valid document
4. Receives personal IDP code
5. Uses services

ID Point system

IDP Officer interface | **Service provider interface**

ID POINT

6. Asks for IDP code and fills it to the IDP system
7. Asks and verifies Customer's name
8. Provides required services

Service provider

NOTE: SP can also be a system

Figure 3. The ID Point service setup in the University of Helsinki.

The ID Point system offers separated interfaces for IDP officers and service providers. The IDP officer can only feed new information to the system but cannot read or modified it. Service provider can only feed IDP codes and read information that system provides with the code. The IDP system generates the IDP code and delivers it by default to directly as SMS-message to the mobile number given by the customer. However IDP code can also be printed out to a paper by the IDP officer if mobile number has not been given.

The service provider can use the ID Point service model in the services that require customers to be identified. Service can be personal service like IT Helpdesk or it can be a system. Service provider asks customer to give IDP code and feeds that code to the IDP system. For a valid IDP code the system displays customer's information stored in the system. Now service provider can confirm that the code's holder is a valid user. After successful conformation service can be provided.

From the customer point of view the ID Point service is easy to use. Identify yourself to an ID Point officer with a valid document and then receive a personal IDP code. After that user can use any service which accepts IDP codes.

There are few limitations to the process from the information security point of view. The IDP system itself is strongly protected with special technical setup. The IDP code itself is useless without knowledge whose code it is. Also the IDP code is valid only for 24 hours and in the current setup it can be used only once.

There is mandatory training for the IDP officer and for the service provider before they can use the IDP system. We also had an opportunity to gain expert level training from the Finnish custom officer regarding how to recognize impostor and the identification papers authenticity.

6. CONCULSIONS AND FUTURE PLANS

We started to develop new service model first from technical point of view. This led us to a service that was based on HD quality video conferencing technique. At end of the first piloting period we found out that very similar technique and service concept was tested in another pilot project. This project was founded by the Ministry of finance and naturally with significantly bigger resources. We decided to see what kinds of results are gained from that pilot project and made our focus to improve our service model rather than improve technique. As we continued working on the problem the service model was finally shaped on the form of the ID Point model.

The ID Point service model was designed to deal with the problem of complex user account management system without interfering to the service itself. To get in this we needed to separate in the customer service the identification part and the service part. This was solved by the ID Point service model. Furthermore the ID Point service model is more a general way of organizing services, as the human part and the system part of the services may be chosen independently. This is shown in the Figure 4.
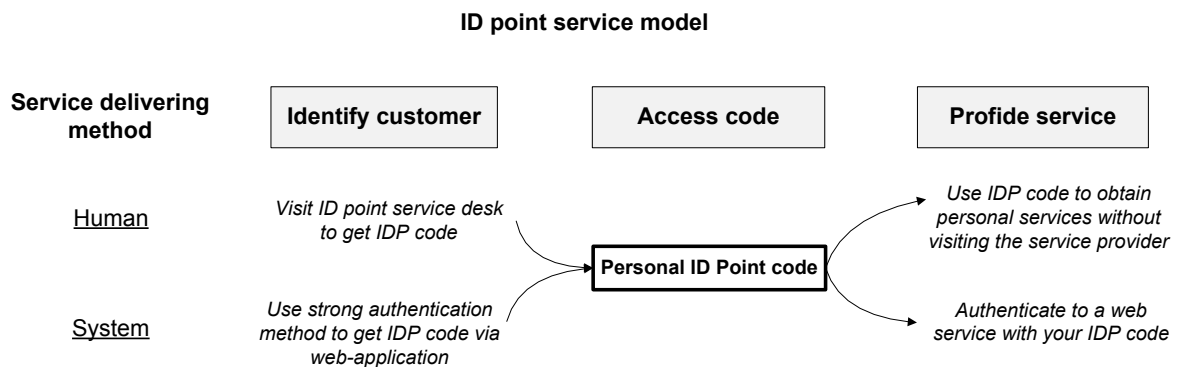
ID point service model

Figure 4. The ID Point service model concept.

In 2014 we have six ID Point service desks which are located in campus libraries at four main campuses. We have trained ID Point officers for several remote locations (research stations) and our plan is to cover all sites of the University in the near future.

Finally we like to thank for Dr. Matti Lattu for early implementation of the ID Point system and also participating to the development of the service concept.

7. REFERENCES

Etäpalvelupilotin 2012 – 2013 loppuraportti (in finnish)

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/04_hallinnon_kehittaminen/20131119Etaepal/Etaepalvelupilotti_2012_-_2013_loppuraportti.pdf

8. AUTHORS' BIOGRAPHIES

Mrs. Maria Kalske is IT specialist working at University of Helsinki since 2009. She started working in IT 1997 as IT specialist.

Dr. Mika Kivilompolo is IT manager working at University of Helsinki since 2004. He worked in the field of material physics using computational methods in 1995-2000.