# EUNIS 2015: ID POINT – USER IDENTIFICATION

Maria Kalske

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

Keywords
ID Point, authentication, identification, service model

## 1. ABSTRACT

ID Point is service model that meets Finland's strict law requirements regarding user information management as well enables the use of services that would require strong authentication without any or just minor changes of the service itself. Updated information from ID Point-service model that was presented in Eunis 2014.

## 2. INTRODUCING

The University of Helsinki is an academic community of 40,000 students and staff members. It operates at four campuses in Helsinki and at 15 other locations. For users the IT Centre 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 ID Point is a service model that enables the use of services that would require authentication without any or just minor changes of the service itself.

## 3. STARTING POINT

The Helpdesk of IT Centre provides wide range of IT support by email or phone for all users and it is open each weekday from 8 to 17. Helpdesk does not provide opportunity for personal visit. The main limitation for the helpdesk service earlier was that users couldn't be identified adequately before delivering the service.

The user account management system of the university had been developed during a 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. Therefore it was not possible to share the user account management workload outside IT Centre even on remote sites.

During the past several years, we had already made changes on technology and services that decreased user visits at local service points i.e. just few visitors per day. For this reason we have now closed local service points at most campuses. At the same time we gained more calls to helpdesk where user needed be identified before delivering the service. Users preferred to call to helpdesk instead of walking to the nearest local service point while they still existed.

The IT strategy of the university is aiming at developing efficient, equal and centralized IT services for all users. University's research stations are located in 15 different places all over Finland. None of these places have local service. Therefore changes were required in services, service delivery model and staff reallocation to support the strategy. The ratio between local IT services and centralized IT services had changed from 90:10 to 60:40.

Finland has one of the strictiest laws regarding user identification management in Europe. The ID Point was created to meet both law requirements as well to aid Helpdesk's identification problem. You could say that user's behaviour shaped our way to provide service from Helpdesk, ID Point was the tool to make this possible.

## 4. WHY ID POINT?

There is several ways to solve identification problem, so why ID Point? I will go though few examples that could compete with ID Point and show the benefit `

### 4.1. Vetuma

In Finland there is widely used and 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.

For most user authentication cases this is a suitable choice, but it has some limitations. For example any foreign employee or students do not have VETUMA possibility. Also bank credentials can be co-owned (i.e. married couples) and there for they cannot be used as VETUMA authentication. The latest downside on this widely used authentication system is that each authentication will create a small cost for university.

### 4.2. Electronic identification card

Electronic authentication cards are reasonable secure way to authenticate user. There are several variations of this service model, but each has common the starting costs. To have electronic authentication cards in usage, you need both electronic cards as well readers. Also you should be able to maintain and possible to block some card's usage i.e. card been lost or pure misuse of it. This requires personnel to maintain the electronic authentication system at the server as well user end. On research stations where is no local IT support this can become an issue. Also the cost of replace the lost or broken electronic cards. In our case this never was a real option due the start and maintenance costs it will create.

### 4.3. ID Point

The ID Point we simply used already existing staff and environment. Each main campus has campus libraries where we could provide ID Point identification service. On research stations we found one or two trusted person who's been trained to do identification users when it is needed. We didn't need to invest on any sites since all had already network connections as well computers with they could connect on ID Point system.

Since ID Point system on its simplicity is surprisingly secure we can provide service from Helpdesk that requires strong authentication. Even if user loses his identification code the chance it being miss used is extreme low, course the code does not hold any information whose code it is. There for Helpdesk does always check both code as well the name and see if they match what system provides.

## 5. ID POINT SERVICE

ID Point service consists of three components: ID Point service desk, ID Point system and Service provider. More detail can be found ID Point service model in Eunis 2014 presentation. The setup of Helsinki University's ID Point service model is described in fig 1.

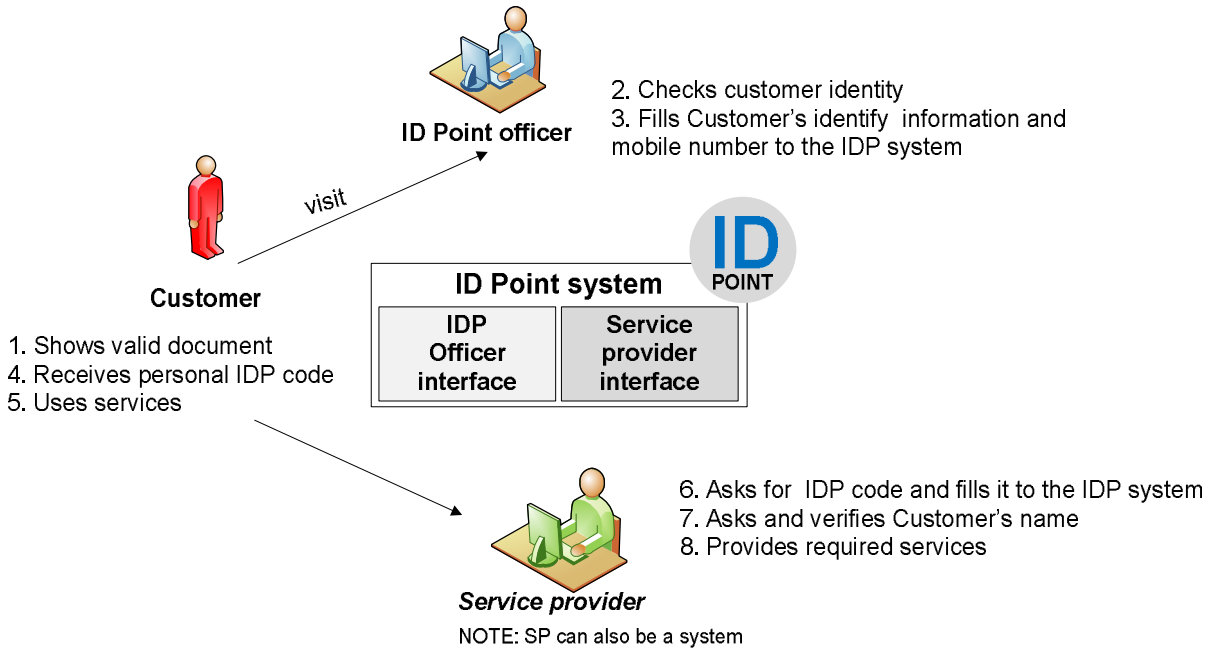


Fig. 1. The ID Point service setup in the University of Helsinki.

The ID Point service desk takes care of user identification. The ID Point officer checks user's identity from a valid document and feeds the required information to the ID Point system. Collected information is firstnames, surname, date of birth, social security number (for those who have one), document type and the author. Only optional information is user's personal mobile phone number.

ID Point system offers separated interfaces for ID Point officers and service providers. ID Point officer can only feed new information to the system but cannot search, read or modified after saving it. Service provider can only feed ID Point authentication codes and read information that system provides with the code.

The ID Point system generates the ID Point authentication code when required information has been filled and delivers it by default to the customer's given mobile number as a SMS-message. However ID Point authentication code can also be printed out to a paper by the ID Point officer if mobile number has not been given. ID Point authentication code on text message or on paper do not hold any information of person who's been identified. ID Point system is only place where user's identification information are combined to ID Point authentication code.

Service provider can use 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 checks customer to give ID Point authentication code and feeds that code to the ID Point system. For a valid ID Point authentication code the system displays user's information stored in the system.

From the customer's point of view the ID Point service is easy to use (fig. 2). Identify yourself to an ID Point officer with a valid document and then receive a personal ID Point authentication code. After that user can use any service which accept ID Point authentication codes.

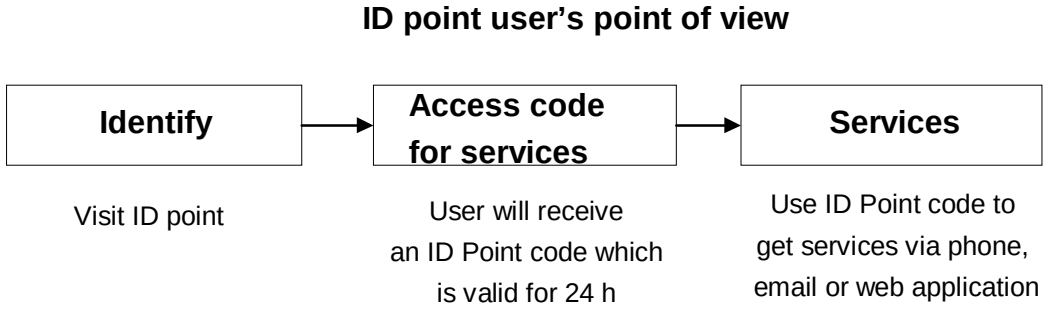


Fig. 2. ID Point user's point of view

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

There is mandatory training for the ID Point officer and for the service provider before they can use the ID Point system. We also had an opportunity to gain expert level training from the Finnish custom officer regarding how to recognize impostor (person who uses other persons real identification papers as their own) and the identification papers authenticity.

Even ID Point was created to aid Helpdesk related user account services, it is not tied on it. ID Point service model is enabling service that can be used to provide any service i.e. by phone that requires authentication.

## 6. ID POINT HISTORY

The project which side product ID Point was started January 2013. The original plan to launch Helpdesks face to face service though videoconference system was abandoned during the pilot due users preferring to call with ID Point authentication code directly to helpdesk instead of using videoconference system. While videoconference system were still setting up, it came clear that we required identification transfer system. This was the start of ID Point.

The pilot phase started on June 2013 and less than few weeks of starting 2nd campus library contacted us and asked if they could have ID Point service desk. The Project which side product ID Point was ended in August 2013 and ID Point started to live the life of its own. Within a month from pilot's ending, we had ID Point service desks all our campuses in Helsinki. Less than half year, it was expanded in few of our distance locations also.

At the end of 2013 we had only eight ID Point service desks. Five of them were located in campus libraries at four main campuses and three on research stations. In 2014 we trained more ID Point officers including also research stations. By the end of 2014 we had already 15 ID Point service desks all over in Finland in university's research stations and main campuses. At the beginning of 2015 we have already trained three more ID Point service desks. The growth of the service desk usage amount as well usage described in fig 3. Years 2015 numbers are up till April 19th.

| Year | ID Point service desks | Total | Average per week | Median per week |
|---|---|---|---|---|
| 2013 | 5 | 33 | 3 | 2 |
| 2014 | 15 | 734 | 14,4 | 13 |
| 2015 | 18 | 225 | 15,9 | 16 |

Fig. 3. ID Point growth

From the start we decided to contribute properly education of ID Point officers. Each new officer was trained of the usage ID Point officer portal as well how to identification user proper. ID Point usage have grown dramatically within a year.

Even ID Point authentication code is valid 24 hours, most users tend to user code within first 30 minutes. More significant is that last year about 25% of the authentication usages has been done between five to fifteen minutes and it's been increasing this year. Only first year 16% has been used before five minutes, but after that it has been dropping below 10%. Instead of authentication time usage from fifteen minutes to thirty minutes has been increasing around 15%. Described in fig 4.

| Year | Below 5 min | 5 to 15 min | 15 min to 30 min | Below 1 hour | Below 6 hours | Above 6 hours |
|---|---|---|---|---|---|---|
| 2013 | 16 % | 25 % | 0 % | 6 % | 9 % | 3 % |
| 2014 | 7 % | 26 % | 15 % | 8 % | 12 % | 4 % |
| 2015 | 8 % | 39 % | 12 % | 7 % | 10 % | 3 % |

Fig 4. Time in when user consumes ID Point authentication code

## 7. CONCLUSIONS

ID Point initially was a side product of another project. ID Point concept is simple and easy to use and that's why we had more willing partners all over in University. With ID Point service model, we can bring user account services even in remote locations and provide the service even if researchers are out of the field. At the user end, we have received large number amount positive feedback as well our service provide partners been often forwarding to us the positive feedback that they have received regarding ID Point service.

The reason why ID Point service model was so well accepted among users as well our service partners that it didn't try to do anything fancy and it was easy to use for all. The simplicity of the system actually created an option that ID Point service models can be benefit also for other services. The ID Point itself does not provide a service it just provides a possibility to use a service that would require identification.

Based on the experience in all areas in ID Point service, we have started to conversations with other non IT services that could be used via ID Point authentication. We can see several services that could actually benefit of having ID Point providing access to it.

Our plan is to expand ID Point service model to all our research stations and remote sites that have either our personnel or students. Also we have encouraged our departments to have their own ID Point service desks for their personnel, course all new location provides users better chances to find closest ID Point service close to them.

## 8. REFERENCES

Special thanks for DR. M. Kivilompolo who's idea ID Point was formed and guided though the creation of first paper as well DR. M. Lattu who created the basics for ID Point to be able to form, grow up and develop to a full service.

Kalske M. and Kivilompolo M. (2014) *The ID Point Service Model*
http://www.eunis.org/eunis2014/papers/

## 9. AUTHORS' BIOGRAPHIES

Maria Kalske has been managing IT support teams since 2004. Currently, she is an IT Local Support Team Manager and leading few projects Leader at the IT Center of the University of Helsinki. Maria has been holding this position over five years now. Prior to that, she worked for several private companies in Finland and has gathered experience in the fields of IT support and infrastructure maintenance.