



TAMPEREEN
AMMATTIKORKEAKOULU

Implementing a New Printing Solution

FollowPrint

Toni Tuominen

Bachelor's thesis
October 2016

Degree Programme in Business Information Systems
Network Services



TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Tietojenkäsittely
Tietoverkkopalvelut

TUOMINEN, TONI:
Implementing a New Printing Solution
FollowPrint

Opinnäytetyö **41** sivua, joista liitteitä **1** sivu
Lokakuu 2016

Tämä opinnäytetyö perustuu projektiin, jonka tarkoituksena oli implementoida uusi turvatulostuspalvelu toimeksiantajan pääkonttorille ja kahdelle Tampereen konttorille. Projektin toimeksiantaja on yksi suurimmista metsäalan yrityksistä Suomessa. Turvatulostuspalvelun sivutuotteena pyrittiin ottamaan käyttöön myös erillinen mobiilitulostusratkaisu vierastulostamista ja mobiililaitteita varten. Projektin toimitti ulkopuolinen yritys, ja kirjoittajan rooli projektissa oli toimia koordinaattorina.

Uudella turvatulostuspalvelulla pyrittiin vähentämään turhaa tulostamista, lisäämään tulostuksen tietoturvaa ja parantamaan tulostuksen käyttäjäkokemusta useissa toimipisteissä työskenteleville. Uusi turvatulostuspalvelu korvasi olemassa olevan kustomoidun turvatulostusratkaisun yrityksen pääkonttorilta sekä tavalliset tulostusjonot Tampereen konttoreilta. Lisäksi käyttäjäkokemuksen parantamiseksi turvatulostuspalvelu integroidaan lupahallintarekisterin (ACR) kanssa, jotta käytössä olevat henkilökortit saadaan rekisteröityä automaattisesti käyttäjän puolesta turvatulostukseen.

Opinnäytetyössä esitellään käyttöön otettu turvatulostusohjelmisto, sen keskeiset komponentit ja toiminallisuus turvatulostuksessa. Lisäksi työ perehtyy kevyesti kahteen mobiilitulostusratkaisuun ja esittelee integraatio-ratkaisut, joita projektin aikana harkittiin.

Turvatulostusprojekti valmistui aikataulussa, ja kaikille kolmelle toimeksiantajan konttorille saatiin uusi palvelu turvatulostamiseen. Mobiilitulostusratkaisu peruutettiin projektin aikana tietoturvasyistä, jotka liittyivät epäselvyyksiin palvelun toiminnasta palveluntoimittajan osalta. Integraatio lupahallintarekisterin ja turvatulostus-palvelun välille rakennettiin onnistuneesti viestipohjaisen integraatiopalveluväylän avulla. Projektin aikana tehdyistä havainnoista kirjattiin lisäselvitystä vaativat asiat kirjoittajan näkökulmasta, mikäli palvelua halutaan laajentaa uusiin toimipisteisiin.

Asiasanat: Equitrac, tulostus, turvatulostus, implementointi

ABSTRACT

Tampere University of Applied Sciences
Tampereen ammattikorkeakoulu
Degree Programme in Business Information Systems
Network Services

TUOMINEN, TONI:
Implementing a New Printing Solution
FollowPrint

Bachelor's thesis **41** pages, **1** appendices page
October 2016

This thesis was based on a project, whose purpose was to implement a new secure printing system to a company's head office and two office locations in Tampere. The company whom this project was made for is one of the biggest forest companies in Finland. The secondary target of the project was to deploy a new mobile printing solution for guest printing and mobile devices. The project was delivered by another company – called here as the Vendor – and the role of the author of this thesis was to act as the project coordinator.

The new secure print solution aims to reduce unnecessary printouts, increase information security in printing and improve the user experience for those who work in several office locations. The new printing solution will replace the existing customized secure print solution in the company's head office and ordinary printing queues in the Tampere offices. To improve the user experience, the secure print solution will be integrated with the Admission Control Registry (ACR), so that users' ID cards will be registered automatically for secure printing.

The above mentioned secure printing solution, its core components and the secure printing functionality are presented in this thesis. Two mobile printing solutions and integration possibilities that were investigated during the project are also discussed briefly.

The secure print project was finished on schedule and the new secure printing solution was implemented successfully for all three office locations. The mobile print solution was cancelled during the project, because the Vendor did not have a clear understanding on how the mobile print solution would work and the issues with information security which came within of that. Integration between the secure print solution and the Admission Control Registry was achieved successfully by using a message based enterprise service bus (ESB) system. All findings and questions that came up during the project and need to be resolved before expanding to the new sites were documented for future use.

Key words: Equitrac, printing, secure printing, implementation

Table of content

1	INTRODUCTION	6
2	BACKGROUND	7
3	SECURE PRINT	8
3.1	What is secure printing?	8
3.2	Secure print pros and cons	11
3.3	Case study	12
3.3.1	Case Swiss Graubündner Kantonalbank	12
3.3.2	Case Large Fortune 500 Financial Services organization.....	13
3.4	Used software – Equitrac	14
3.4.1	Equitrac core components	14
3.4.2	Additional components	18
3.5	Accounting and reporting	19
4	MOBILE PRINT	21
4.1	What is mobile printing?.....	21
4.2	Xerox Mobile Print Cloud	22
4.3	Xerox Mobile Print Solution.....	24
5	ADMISSION CONTROL REGISTRY INTEGRATION	26
5.1	Benefits of integration	26
5.2	Active Directory	27
5.3	SQL integration.....	28
5.4	IBM message broker	29
6	PROJECT OUTCOME	31
6.1	Secure Print.....	31
6.2	Mobile Print	33
7	CONCLUSIONS	36
	REFERENCES.....	39
	APPENDICES	41
	Appendix 1 Equitrac reporting	41

ABBREVIATIONS AND TERMS

AAA	Authentication, authorization, and accounting
ACR	Admission Control Registry, system which manages access control systems
AD	Active Directory
FollowPrint	New of the new secure printing system and service name
MFP	Multifunctional Printer
Mobile printing	Print jobs submitted by mobile device such as a smartphone or tablet
Printing queue	Queue for print jobs which are waiting to be printed
Pull printing	Official name for secure print technologies
RFID	Radio-Frequency Identification, used for ID tags
SaaS	Software as a Service
Secure print service	Printing service that uses secure print functionality – also known as pull printing
Secure print	Printing feature which holds the printing job until user releases it from the printer.
SecurePrint	Name of the old secure printing system and service name
Shared queue	Printer queue which is shared using Windows network sharing
Snapshot	The state, disk data, and configuration of a virtual machine at a specific time.
Vendor	The company who delivered the Onew FollowPrint service
WorkCentre	Multifunctional printer model from Xerox
XMPC	Xerox Mobile Print Cloud
XMPS	Xerox Mobile Print Solution

1 INTRODUCTION

Printing hasn't changed significantly during the years when other technologies have been evolving. Printers have received new features and additional functionalities, but the basic printing has remained the same – user prints a document and expects to receive the same looking printout from the printer. Nowadays all small personal printers are replaced by bigger multifunctional printers (MFP) which are then shared by several other people. It's easy to pick-up someone else's print jobs – even by mistake.

Quocirca's research from 2013 revealed that 62% of organizations had one or more data breaches through printing because documents were left unsafely on the printer (Quocirca 2013). And Cost of Data Breach Study made by IBM and Ponemon Institute (2016) reveals that each lost or stolen record containing sensitive and confidential information costs in average 158 dollars and that the average data breach costs four million dollars in total. Capability to print documents securely using delayed print or additional release pin code has been on MFPs for years, but those are very little known features and require additional effort and time from the user.

This thesis is a part of the project which goal was to implement a new printing solution. This new solution should increase data security for printing and reduce unnecessary printing by enabling secure release functionality using ID cards. The second goal of the project was to enable guest printing using a separate mobile print service. The thesis presents and focuses on the Equitrac secure print solution, its main components and secure print benefits and disadvantages. Mobile printing is still a newcomer in printing field and most of the enterprises are still studying its possibilities and requirements. This thesis presents the project results and possible problems that need to be solved from the perspective of the thesis author if the secure printing solution is to be extended to new locations.

All confidential information has been removed or modified from this thesis.

2 BACKGROUND

The company who ordered this project is one of the biggest forest companies in Finland, having several mill sites and offices across Finland and more functions globally. This thesis is based on a project for which the author was hired as project coordinator.

The problem which the company had, was the printing. All printers were redistributed by using ordinary printing queues and there was no control on what and where employees could print. In the offices, printers were shared amongst all on the floor and there were no personal printers. The problem consists of miss prints and confidential prints. Since each printout was printed instantly when it was sent to the printing queue, there was no option to think twice, whether the printer was correct one or the printed document the right one. There was a risk of that confidential printouts to be forgotten on printer and thereby someone might take them by mistake. Or "forgotten" printouts could be miss prints. Since all printers were in the same local network, it was possible to print using wrong printer in a different site, if the employee happened to visit a different site than his primary location.

This problem was solved – sort of – in the company's head office. There was a custom made secure print solution which required users to release each printout from the printer which they wanted by showing the ID card on the card reader. This made it sure that there were no miss prints or print jobs waiting for pickup, just lying on the printer. But the problem with this printing system was that it was custom made secure solution and the setup was built with a tight schedule. Because of that, the technical documentation was imperfect and all those participants who had worked on the project had already left the company.

When employees from other functions realized all the benefits of secure printing, they requested the same secure print capability to Tampere offices. Since the old secure printing system was a custom made solution and not scalable, IT decided to order a new secure print solution for office printing and a mobile print solution for guest printing. The Vendor who delivers the new system was selected before the author of this thesis joined the project and some work was already done at that point. In order to improve the user experience, project also investigated the possibilities of how the user's ID cards could be registered automatically to the secure print service.

3 SECURE PRINT

3.1 What is secure printing?

Secure print means a print job type where the user prints the documents just like normally, but before the documents are released from the printer, user needs to be authenticated on the printer, for example by entering a pin code. Secure printed documents are saved in the printer's hard drive until they are released by the user. Figure 1 shows the basic workflow in secure printing. In this way the printouts are not printed automatically and the user has the opportunity to cancel his printout if they were printed by mistake. Furthermore, forgotten printouts won't fill up the printing room and printed documents won't end up in wrong hands. Secure print can be established either by a device which doesn't require additional software or by using printing software which expands secure printing capabilities.

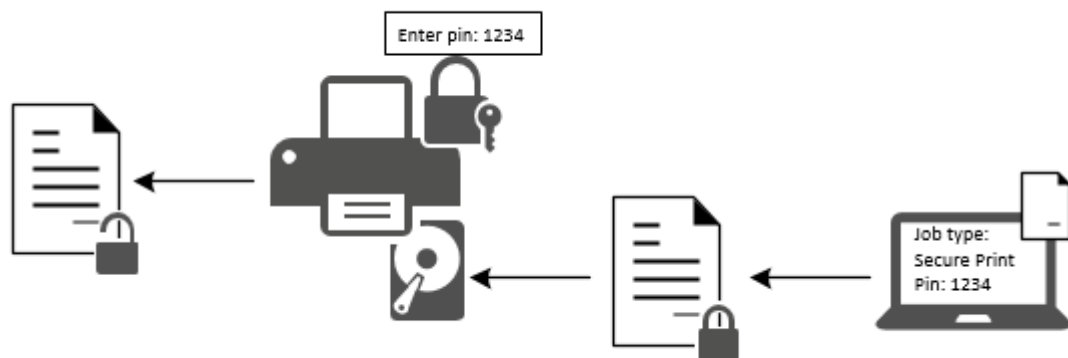


Figure 1 Secure print workflow

Secure printing is originally just a feature of the normal printing queue. Secure print in single device level works so that the user can give an additional pin code for the printout and the document release is protected by it. If the printer supports secure print, there is an option "Secure Print" in job type menu (Figure 2). By selecting it, the document will be sent to the printer but instead of printing it automatically, it will be saved in the printer hard drive waiting for release.

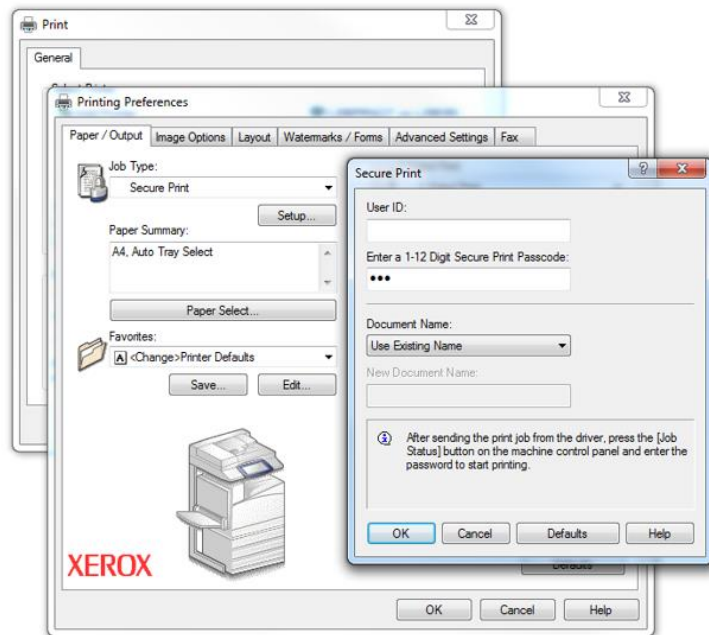


Figure 2 Printer preferences - Secure Print

On the printer, user needs to find stored documents menu which has the secure print option. Secure print view contains a list of users who have printed by using secure print and the length of the list is as long as there are documents waiting for release (Figure 3). By selecting the own username, the user can enter the pin code which he has selected earlier and after that he sees his own secure print documents which can be then released securely.

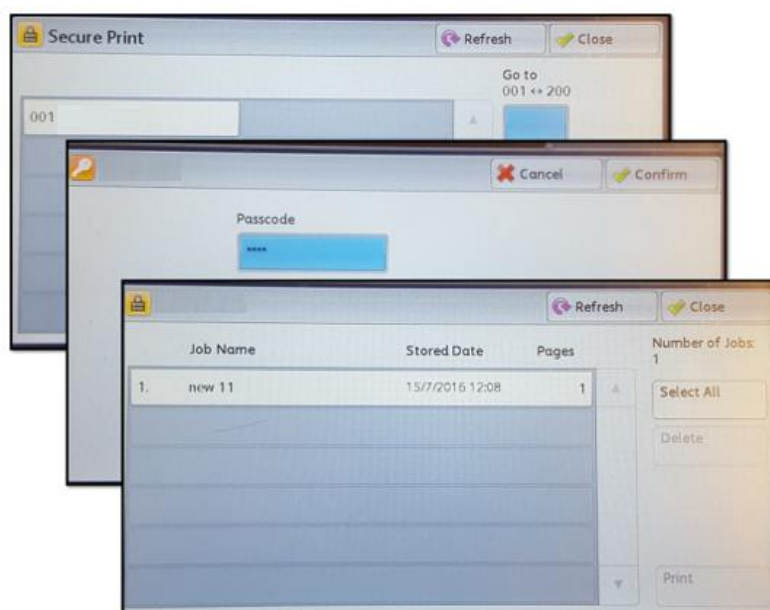


Figure 3 Secure Print on printer

On device based secure printing, the printed file is only on the used printer hard drive and can be then released only from that particular printer. Printing documents using secure print isn't so popular, because it requires more work than using normal printing and it isn't as user friendly.

A more advanced version of secure printing is pull printing which works almost in the same way, except that secure print features are software managed on server side. It enables AAA (authentication, authorization, accounting) for all printer related features. Pull printing software stores the documents on server and after the user is authenticated on the printer by using the pin code or the ID card, the printer "pulls" the print jobs from the server. Since documents are saved on server side, it enables flexibility for choosing used device which has the pull printing functionality. Pull and secure print mean two different printing functions, but both establish the same functionality and secure print name is often used for the both technologies.

Figure 4 describes how pull printing works in general level. In pull printing systems, there is most likely just one printing queue and all printers are added into it. The user prints his documents to secure print queue and the server stores the printouts to hard drive. Next, the user has the freedom to choose which device he might want to use, since all printers are using the same printing queue. User goes to printer which wants to use, authenticates himself to printer service and the printer pulls the printouts from the server and prints them.

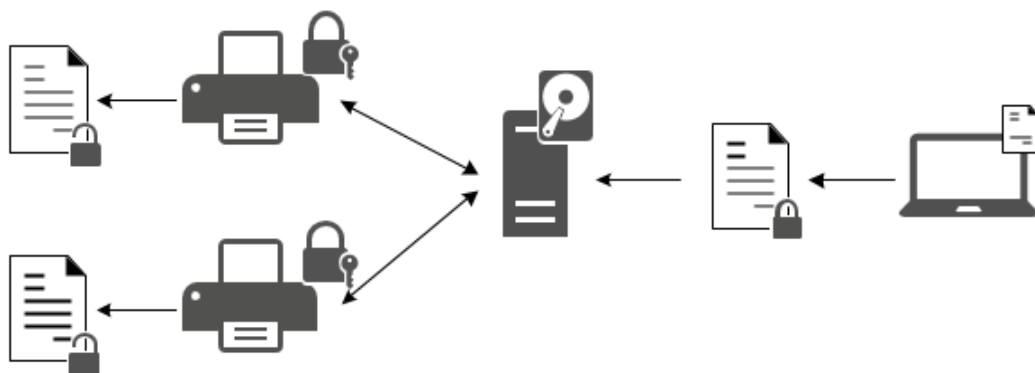


Figure 4 Secure print service

3.2 Secure print pros and cons

Pull printing technology brings several benefits for end users and the IT department. From the end user's perspective, the most important improvement is the flexibility and freedom to print first and to choose the used printer later. Users can use the same print queue in all office locations which are sharing the same printing system. Security is the "side effect" which comes with pull printing queues, since printouts don't print automatically anymore. Users must authenticate themselves at the printer before it prints anything, and by this way the user can be confident that his documents are in safe. Departments like HR and Payroll can get rid of personal printers because they can be sure no-one will not see sensitive documents lying on a printer.

For the IT, pull printing simplifies the printing management because now there is only one print queue for all printers and workstations, instead of having a separated queue and driver for each printer. Since all printers are managed from a single server, there is either no need for a separated printer server anymore. The secure release of documents brings cost and environment savings as well, because each document needs to be released on printer and unreleased print jobs will be destroyed from queue over time. Now a hundred-page document which was printed accidentally, doesn't print automatically and the user has an option to cancel the print job. IT can setup the expiring time for each print job and after that the document will be removed from the user's print queue. Since printing is now managed by software based, all users are authenticated and all printers are using the same print system, this brings along the opportunity to generate better reporting and monitoring of the use of the printers.

Pull printing doesn't bring only benefits, but it has a couple of disadvantages. From the end users point of view, the biggest disadvantage is the speed of printing. In normal print queues, the print job starts to process and copy the job immediately to printer. Now the print job is stored in the server and the printer starts to process it only after the user chooses to release it. So in average, pull printing needs more time. For the IT, pull printing brings along a compatibility challenge, because one queue can have only one driver and the driver must be compatible with all printers which are used within that queue. If the devices are of different ages, there might come some compatibility issues and in the future a newer device won't get all its functionalities, because existing devices are older and don't support all the same features. Table 1 summarizes the pros and cons of pull printing.

Table 1 Pull printing pros and cons

PROS	CONS
Flexibility Print first, choose device later.	Speed Print job will be processed after job is released.
Security Printouts doesn't print before user releases it.	Compatibility One driver for all devices in same queue.
IT management One print queue for all users and devices.	
Costs savings Reduce server, printing and IT support costs.	
Accounting Ability for reporting.	

3.3 Case study

Equitrac promises to reduce printing and IT service costs by reducing the need for separated printing servers and queue for each printer. Since each printout needs to be released manually on printer, it reduces the amount of misprints and unwanted printing. Next two chapter presents two cases where Equitrac was implemented and how it affected to the printing.

3.3.1 Case Swiss Graubündner Kantonbank

The Swiss Graubündner Kantonbank wanted to reduce the amount of printers and printing costs, and to increase the security. They had 1 116 employees and 854 printers in over 70 branch offices. The current printing model was almost one printer for one employee level. Since they were a banking company, they manage a lot of sensitive data, consisting of personal financial information and company assets.

Their solution was to implement Follow-You secure print model together with Ricoh Switzerland office solutions provider. They were able to reduce printers from 854 to 152 MFPs and 65 printers. That meant a 75% reduction on devices and a 60% drop in

electricity consumption. Also miss printing and document loss decreased because all documents were needed to be released with using the employee badge.

"Thanks to this partnership, we have succeeded in making document output more secure across our entire company, while increasing convenience, reducing costs and improving our environmental footprint." said Patrick Albrecht, Business Technology Officer from The Graubündner Kantonbank. (Nuance 2015)

3.3.2 Case Large Fortune 500 Financial Services organization

An unnamed Large Fortune 500 Financial Services organization with global offices, frequently-traveling executives and strict compliance regulations realized that their printing was a nightmare. Printouts were missing because they were printed in wrong printers, IT was drowning into tickets and they had a continuous need for cost-savings.

The company was implementing a new PDF solution and their software partner recommended Equitrac and Follow-You secure printing. They choose to implement Equitrac as well for three reasons: highly scalable Follow-You printing functionality; security features were on the same level as company standards and IT could make most needed changes via Active Directory. After implementing Equitrac their printing costs reduced 30%, service calls to IT staffs reduced and as an example in one office the printer amount was reduced from 135 just to 12.

"With Nuance Equitrac and Follow-You Printing, our executives can travel to any of our offices globally and print from their devices. It reduces trouble tickets and lets them print securely; they scan their badge and receive the job instantaneously at that printer." – Said the Manager from the project. (Nuance 2016)

3.4 Used software – Equitrac

Equitrac has five core components and several additional components that can be added to the system separately. Each component has its own responsibility in AAA workflow. Following chapter presents the core components and functionality in secure printing.

3.4.1 Equitrac core components

All core components are not necessary for all cases – required components depends of the purpose of installation needs. The core components are:

- Core Accounting Server (CAS)
- Device Control Engine (DCE)
- Document Routing Engine (DRE)
- Device Monitor Engine (DME)
- Scan Processing Engine (SPE)

Core Accounting Server (CAS) is responsible for managing all users and printers. CAS contains an accounting database where all printers, network settings, user information, department, billing code, transaction, and the billing balance are stored. CAS can use the local AD for authorizing users and the printer information can be managed manually. In short, CAS keeps track on everything that happens with printers and it is the only service which has access to the database. CAS is mandatory for all installation scenarios. (Nuance 2014, 16)

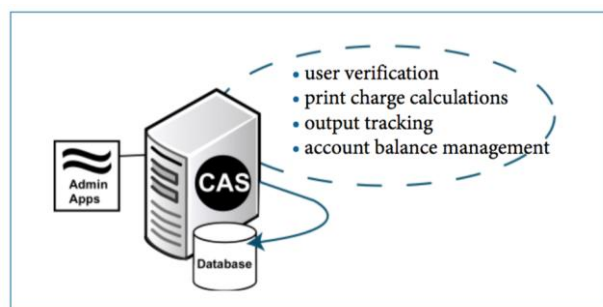


Figure 5 Core Accounting Server (Nuance 2014, 16)

Document Routing Engine (DRE) is the actual print server. It routes print jobs from the user workstation to the appropriate device. Each time a user prints or releases a document from the printing queue, DRE verifies the user from CAS and updates the document status

attributes back to the database. Figure 6 shows the normal print workflow, when the user prints a document without a secure release. Each deployment which purpose is to manage printing, needs at least one DRE installed. (Nuance 2014, 17)

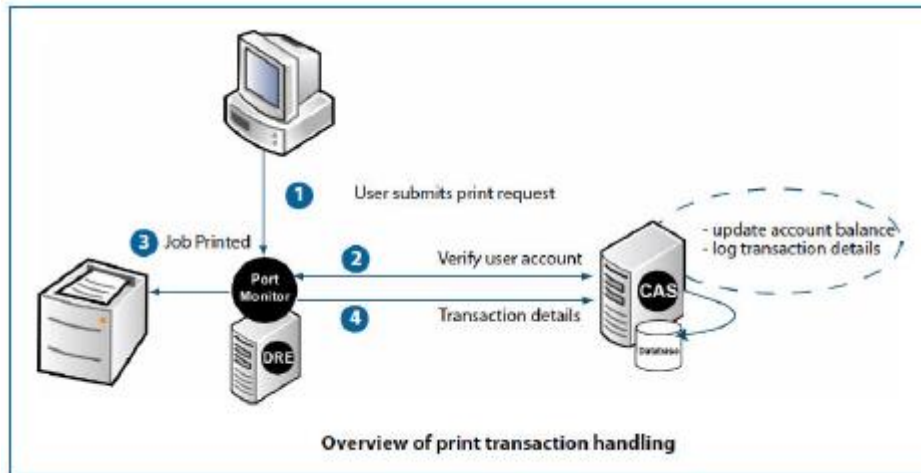


Figure 6 Document Routing Engine (Nuance 2014, 17)

Device Control Engine (DCE) provides authentication and communication with a secure print, copy, scan and fax supported devices. DCE forwards all authentication requests from the printer to CAS and controls those features and their usage, for example, each sent fax could have a price tag or usage limitations. The authentication can be performed by using the username and password, by the pin code, or by using ID cards and card readers. If MFP is using a web embed (EIP app) for managing Equitrac functionalities, DCE needs an additional component called Device Web Server (DWS) for showing the Equitrac interface on the printer (Figure 8). The web embed is basically a web page which is hosted and managed by DWS. Figure 7 shows the basic authentication with DCE. If DWS is used, its place on the diagram is between DCE and the printer. (Nuance 2014, 18)

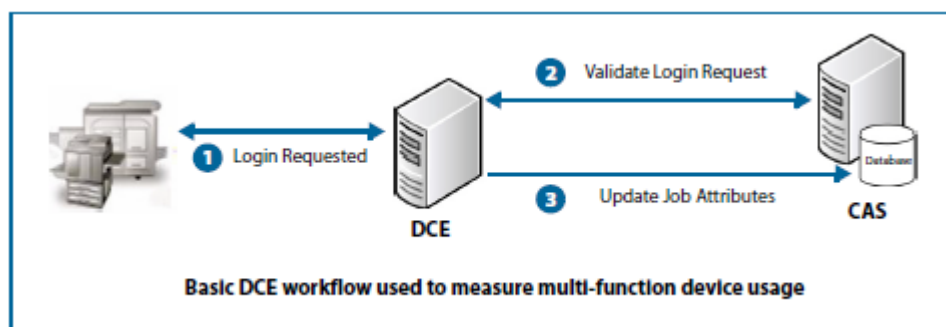


Figure 7 Device Control Engine (Nuance 2014, 18)



Figure 8 Equitrac interface

Device Monitor Engine (DME) is a monitoring service, which can listen SNMP (Simple Network Management Protocol) messages from printers. SNMP is a protocol which can send status changes and alerts to centralized SNMP Manager – in this case the DME (Figure 9). Relevant cases can be paper jams, low amount of ink or offline status etc. DME can generate alerts to IT, so that IT will get information of a faulty device automatically before the user may even notice it. DME keeps also health log from the device, so IT can identify the devices that might need repair or replacement. (Nuance 2014, 19)

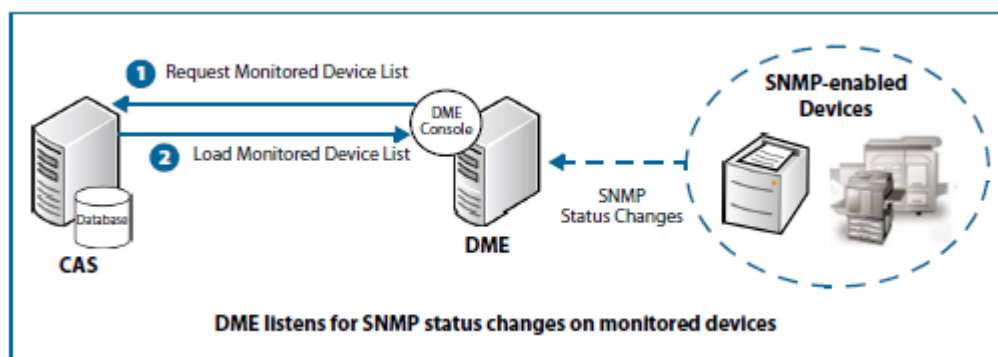


Figure 9 Device Monitoring Engine (Nuance 2014, 19)

Scan Processing Engine (SPE) manages and controls scanning features after DCE has authenticated the user from CAS. SPE can populate some of the information fields automatically, for example the user email address. SPE forwards scanning details to CAS for billing and accounting purposes. (Nuance 2014, 19)

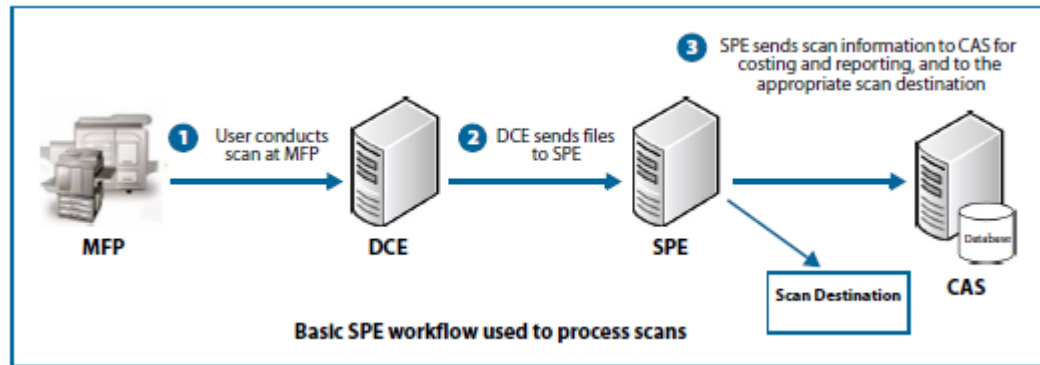


Figure 10 Scan Process Engine (Nuance 2014, 19)

Secure document release (SDR) is the feature that enables secure printing. The Figure 11 summarizes how the core components work in practice when the secure print is enabled. In the middle of everything there is CAS and the database which contains the details of all users and printers. Then there are all other components which manage costs and features.

The secure printed document goes first to DRE and DRE authenticates the user using CAS. If user is authorized to use the secure print queue, document status changes to hold - waiting for the user to release it from the printer. If the user isn't authorized to use the print queue – for example, only domain users are allowed – it returns an error to the user. The next step is that the user goes to the printer which he chooses to use, swipes his ID card on the card reader and DCE authenticates the user from CAS. After user is authorized, DCE shows the secure printed documents from the queue. The user can now choose the documents which he wants to release, change the amount of copies, etc. and then DRE processes the print jobs and routes them to the used printer. All changes are communicated to CAS for accounting purposes. SPE doesn't have a role on secure printing and DME acts as the background service that follows the printer statuses.

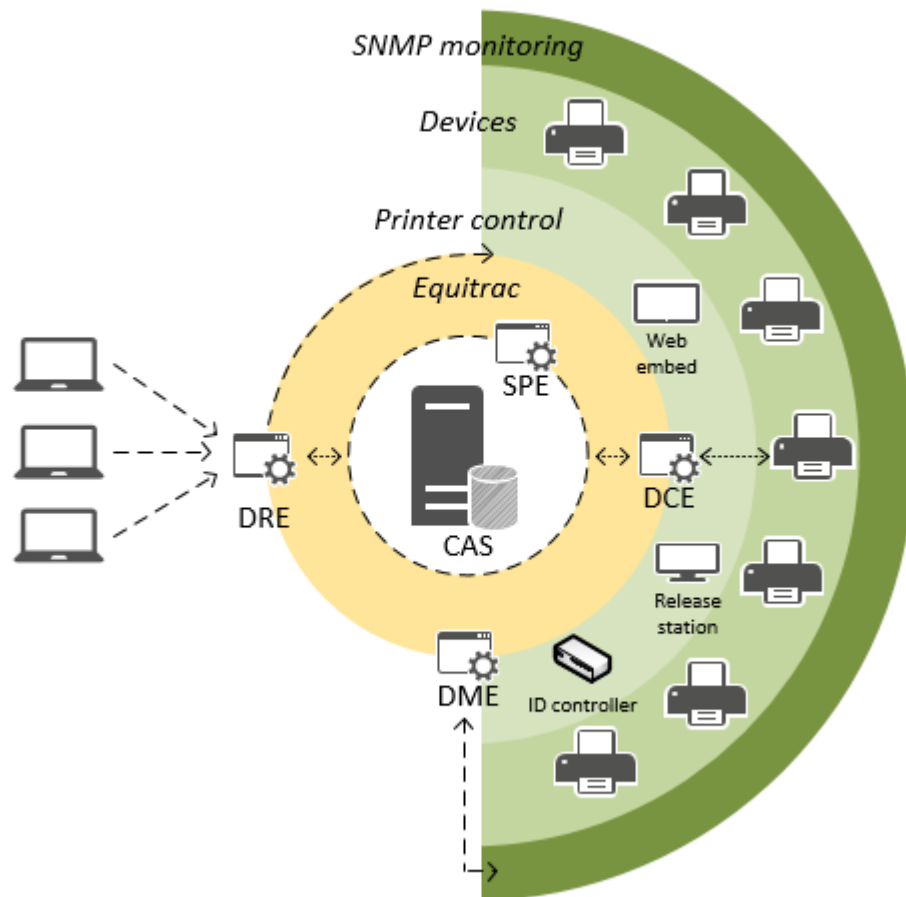


Figure 11 SecurePrint

3.4.2 Additional components

Equitrac has several additional components and features that can be installed together with Equitrac. For example, there are web and desktop clients that allow users to follow their printing costs and manage printouts. In this project, only two additional components were enabled; ID card readers for authentication and ID controllers for printers that cannot use Equitrac interface applications. Nuance ID controller can offer the minimum secure print functionality which is the authentication and ID controller works as a swipe and release device. Nuance's ID controller is not manufacturer independent and can be used with any printing device. It's a totally independent device and its only purpose is to authenticate the user using CAS and then then tell DCE to which printer it should route the print job. Since ID controller doesn't have keyboard or display screen, it doesn't have any other pull printing capabilities such as changing the amount of copies, for instance.

ID controller has a built-in network switch with two LAN ports, because both devices must have their own IP-address. Figure 12 shows the basic configuration using an ID controller. The authenticate process follows the same workflow as normal DCE process.

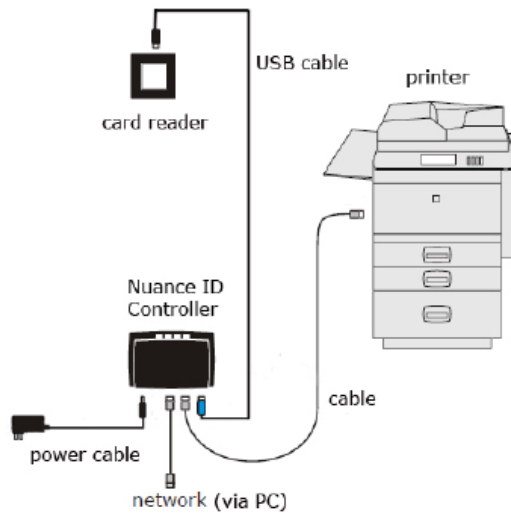


Figure 12 ID Controller (Nuance 2015b)

3.5 Accounting and reporting

One of the main benefits of Equitrac is its accounting and reporting capabilities. If Equitrac is fully deployed, so that it manages all MFPs features and all printers, it can offer highly detailed reports about how and what peoples are printing. Equitrac follows the basic AAA model on tracking the usage. First the user has to authenticate himself with the username and password, the pin code, the ID card or similar. Then the user is authorized via CAS which grants the usage of defined features. And on last is accounting, which measures and tracks the service usage. Most companies are not interested in what individual employees are printing, but they are interested in the big picture: which devices are in high use and are there any devices that need constantly maintenance. By following how users use printers, IT can allocate costs to different functions if needed and so on.

"Total print activity is tracked, along with the resulting cost savings and environmental benefits, such as the reduced consumption of trees, gallons of water and CO₂ put into the atmosphere. Reports can be filtered by user, department, account and device, and can be run for any defined time period. New built-in reports can show how many pages were printed from a workstation but not released to a printer." (BLI 2009)

First sample report in Figure 13 shows valuable information for IT of device faults. This helps to identify devices that might need replacement or support versus device usage.


Device Faults vs. Usage			
5/12/2006	Device faults vs usage Reporting period 3/1/2006 to 5/1/2006		
Printer	Total faults	Total Pages	Faults/1000 pages
Fir 2 MFP	1	114	88
mktg color printer	4	1681	2
mktg MFP	9	1835	5
acct printer	0	569	0
reception MFP	15	2974	5
engrg printer 1	8	55	145

Figure 13 Device faults vs usage (Xerox 2006)

Sample report in Figure 14 shows statistics of usage versus device capability. This helps to identify which printers are in low-use and where there would be a need for better printers. The list of available reports in Equitrac version 4.1 is listed in Appendix 1.


Device Usage							
5/12/2006	Device usage						
Libr bw				Rated Speed:	35 Pages per Minute		
Duty Cycle:	30,000 pages per month			Prorated Volume:	30,000 Pages		
Logical Printer/Copier	Description	Type	Jobs	Total Pages	Cost	Minutes	% Load
acct bw	Accounting 2st fl bw	Physical device	455	6587	658.70	188	21.96%
libr MFP				Rated Speed:	40 Pages per Minute		
Duty Cycle:	30,000 pages per month			Prorated Volume:	30,000 Pages		
Logical Printer/Copier	Description	Type	Jobs	Total Pages	Cost	Minutes	% Load
mktg MFP	Marketing MFP	Physical device	1256	15789	3947.25	394	52.63%
lab3 bw				Rated Speed:	40 Pages per Minute		
Duty Cycle:	30,000 pages per month			Prorated Volume:	30,000 Pages		
Logical Printer/Copier	Description	Type	Jobs	Total Pages	Cost	Minutes	% Load
mktg bw	marketing bw	Physical device	350	4586	1146.50	115	15.29%

Figure 14 Device usage - Equitrac Sample Reports (Xerox 2006)

4 MOBILE PRINT

4.1 What is mobile printing?

The ability to print from mobile devices is becoming an important feature in printing, because everyone is using carry-on devices such as tablets and smartphones. Most of the mobile devices have already the functionality to print using network printers via wireless local area network WLAN, but devices need to have access to the local network to be able to print. So the biggest challenge in mobile printing is to get the documents from the mobile device to the printing server, which is located in company network – inside of the network firewalls. In larger companies, the local network is built so that non-company or non-domain devices do not have access to it.

The simplest approach to mobile printing is to support it via email, so that the user sends the document to print server using email and mobile print service fetches all documents from the email server. Then the mobile print service identifies the user based on the used email address and then adds the document to the user's personal pull printing queue. This works only with the company own employees, requires the existing secure print solution and is not serving any external users who do not have a company account. Another option is to use a solution that generates a release code for each printout and then sends it back to the user. Using that code on MFP, in the same way as on secure printing, the user may release and print his documents. The email printing solutions work with any device, without any extra software in the client's device. An alternative solution might be a service which has an access into cloud or has an access point on DMZ (network zone which separates Internet and the local network) which is open to the Internet. If documents are transferred via Internet, data encryption has to be in place.

Mobile print is still a newcomer in the printing field. Quocirca's Mobile Print Enterprise 2014 survey of printing habits of 125 IT managers in the UK, France, Germany and the Nordic regions reveals that only 14% of companies had deployed mobile printing services, 35% were planning to implement mobile printing in the next 12 months and 33% would like to implement mobile printing but were not investigating it yet. Statistic is represented in Figure 15. (Quocirca 2015)

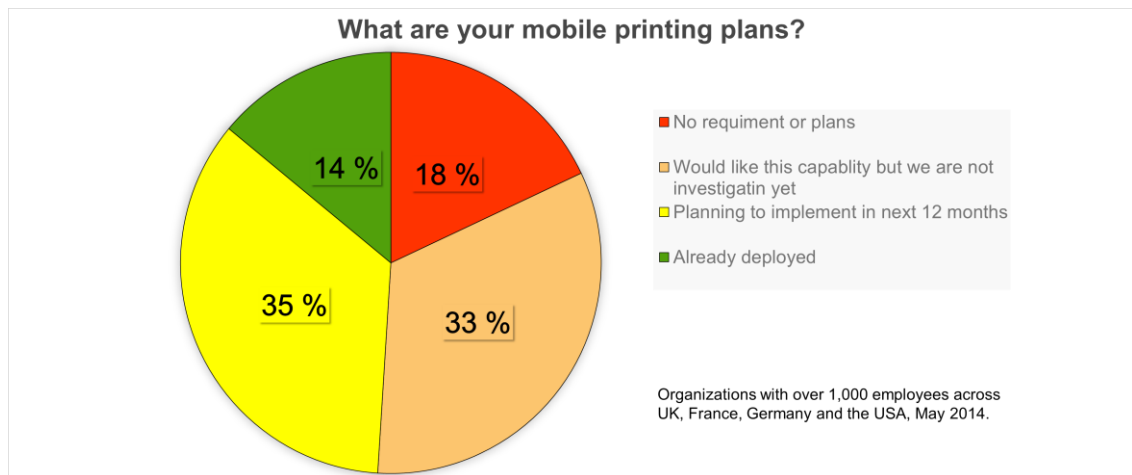


Figure 15 Mobile printing plans

4.2 Xerox Mobile Print Cloud

Xerox Mobile Print Cloud (XMPC) is a SaaS (Software as a Service) printing solution from Xerox for mobile printing. XMPC is hosted in Microsoft Azure, which is a well known and trusted cloud platform. It can be accessed by any device and this way employees and visitors may print even if they don't have an access to the local network. Cloud might be a problem in some cases, especially when users are managing sensitive documents, because the company data leaves outside of own firewalls.

XMPC works so that the user sends his documents to XMPC cloud service, either using a web portal, a mobile app or via email. Depending on the configuration, XMPC identifies the user by used credentials or used email address and routes the document to correct queue. The queue can be common pull printing queue or a printer specific secure print queue. In email printing, each company has its own unique email address which is provided by Xerox. After the XMPC cloud engine converts the document to the proper printing format, it either leaves the document waiting to the pull printing queue, forwards it to the specific secure printer queue or prints the document immediately using a selected printer. If the secure or pull printing is enabled, the user receives the release code via email.

The document workflow from XMPC depends on how the service and printers are configured. Basically there are two options, with or without an XMPC agent. When the

cloud agent is installed to a computer in the local network, it can handle all document routings and printer searching. The second option is without an agent, when the XMPC cloud service handles the document routing and printer management. Using the agent based solution and ConnectKey app (installed on device), printers doesn't require Internet connection but another option is to use EIP app, which is a web emblem hosted in XMPC. If EIP apps are used or solution is deployed without an agent, the printers always require an Internet connection. (Xerox 2015a, 1-4). Both EIP and ConnectKey apps allow user to change the amount of copies, switch colour prints to black and white, etc.

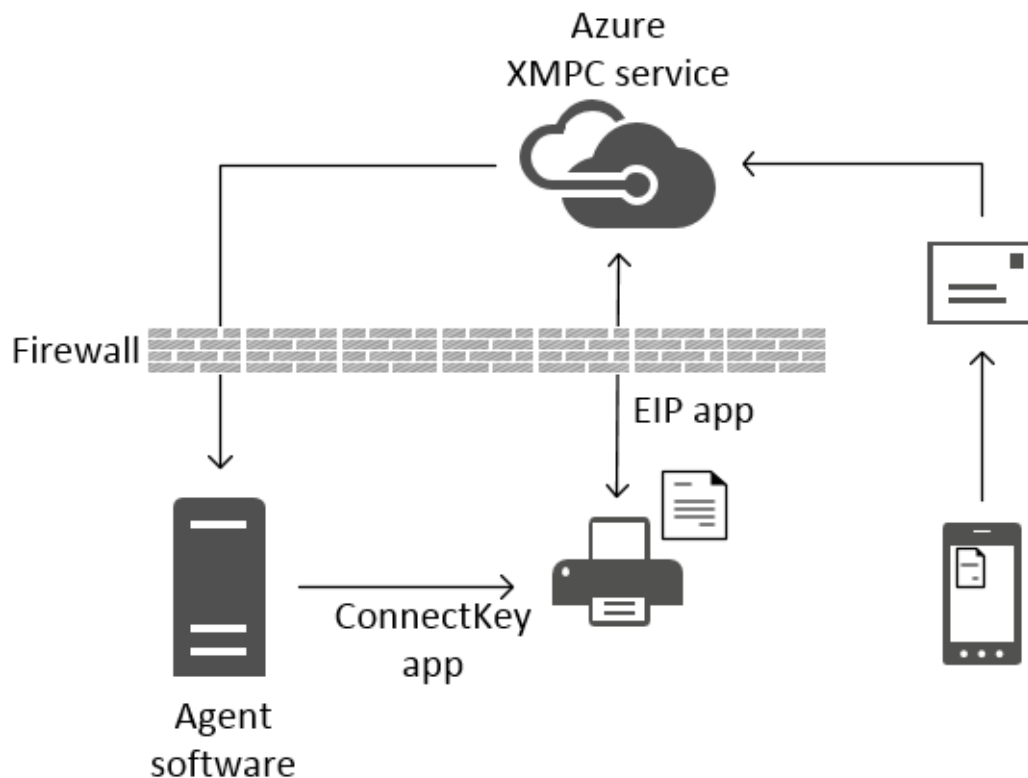


Figure 16 Basic XMPC workflow

Figure 16 shows the basic workflow when a document is submitted by using email and pull printing is enabled. Firstly, the email goes to XMPC in Azure, which identifies the used email address and converts the document to print format. Then XMPC leaves the document waiting for pull and sends the release code to the user. Then the user goes to the printer, enters the release code and depending on whether the XMPC is deployed by using an agent or not, the printer pulls the document directly from the cloud or through the agent server. If the EIP app is used with an agent, the document will still go through the agent server, but the interface on the printer requires an Internet connection.

4.3 Xerox Mobile Print Solution

The Xerox mobile print solution is just an on-site version of the XMPC solution. Since it is hosted locally, it requires more maintenance and work effort than the cloud version, but it is more secure because it can be deployed inside of the corporate firewalls. On-site version has almost all the same features and functionalities as the XMPC version and printing via email works in the same way.

The on-site solution doesn't require an Internet connectivity, if it's used only via email. It can also support mobile devices, but it requires Xerox Cloud Core component which is hosted in Microsoft Azure just like the XMPC. Xerox Cloud Core works as a router for documents in the same way as XMPC, except for that now the processing takes place on-site, not in the cloud.

The on-site solution requires a Windows platform to work and licenses for Windows and SQL database. The on-site version supports the Microsoft SQL compact version which is free, but most companies don't use free software, because they do not have official support. The server needs also monthly maintenance for updates and a backup system is recommended for possible failures. So the on-site version has much higher up keeping costs than the SaaS cloud version.

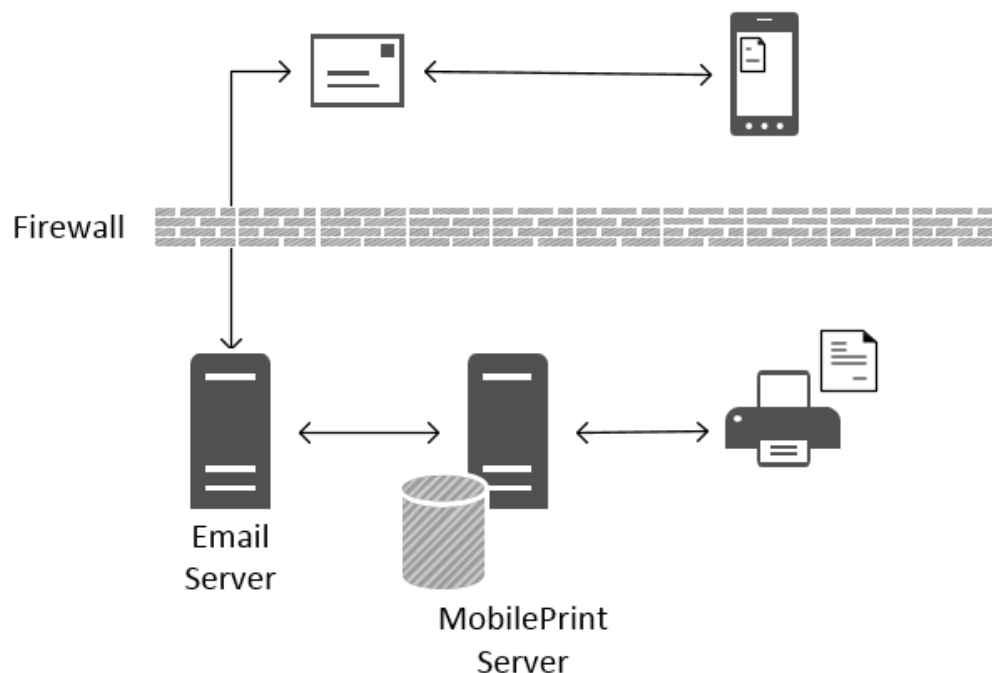


Figure 17 Xerox Mobile Print Solution

Figure 17 shows the workflow with a local mobile print server. Now all components are located inside of the company firewalls. The mobile print server receives a sent document from the email server and then it replies by sending the release code to the user. The document will be converted and placed to hold, waiting for release. Then the user goes to the printer, types his release pin code to the mobile print app and is able to release the document just like in XMPC. From the end user perspective, there are no differences with XMPC and the local mobile print server.

5 ADMISSION CONTROL REGISTRY INTEGRATION

5.1 Benefits of integration

When the project started, integration with Admission Control Registry (ACR) and Equitrac was categorized as nice-to-have. In the old SecurePrint system, it was the users responsibility to register the ID card for printing, but it was not as straightforward. On each and every printer there were instructions about how to register the ID card by entering the username and password. But very often users were not able to perform the registration by themselves and had to request help from the on-site IT support. So the main reason for the integration was to reduce user errors and decrease on-site IT support tickets. The solutions were to register new ID cards automatically when the user receives his ID card.

Figure 18 shows the situation without the integration. Both services, Equitrac and ACR, uses the AD user data to authenticate users. The integration purpose is to get ID card numbers from ACR and transfer them to Equitrac.

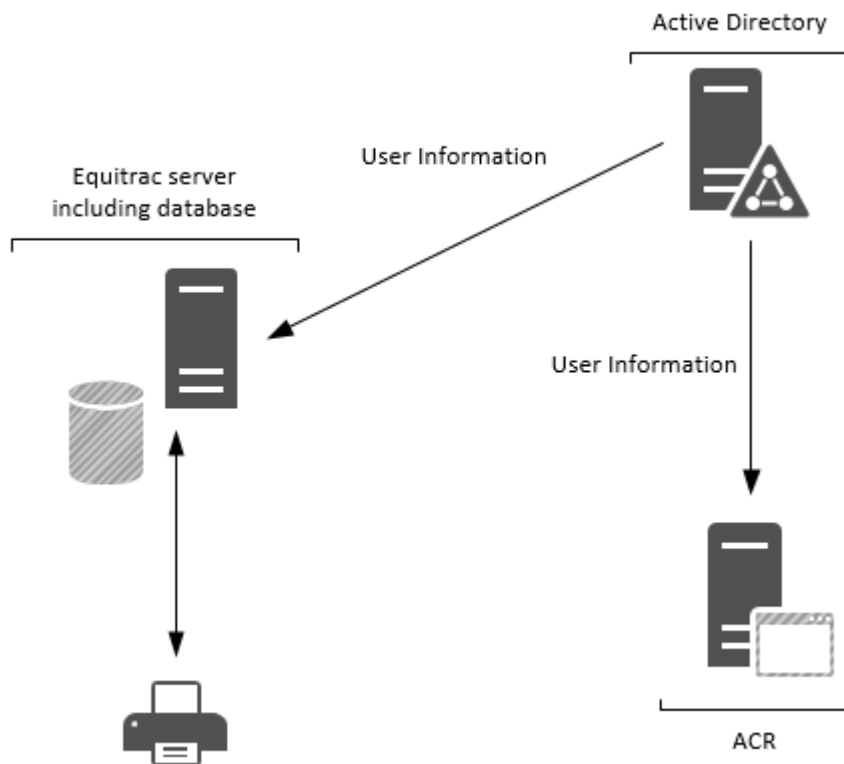


Figure 18 Without integration

5.2 Active Directory

The first possible option for transferring the ID card numbers from ACR to Equitrac, was to save them to the Active Directory (AD) user data. All services that use AD user credentials, are synced with AD and by adding the users' ID card numbers to AD, there could be more usage possibilities in the future. AD user objects have several extensionAttribute fields that could be used for storing ID card data. This way there would be no need to build any new integrations and the card data would be transferred automatically with using existing integrations (Figure 19). Used ID card type had additional encryption preventing the creation of copies from them, even if someone would get all ID card numbers.

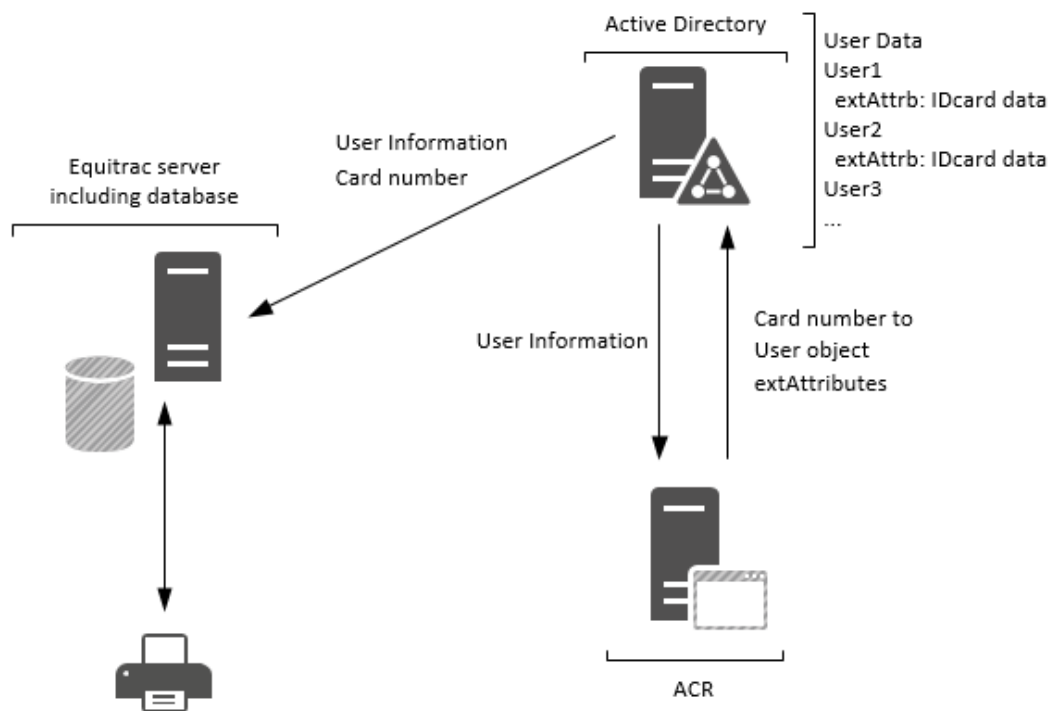


Figure 19 ACR Equitrac AD integration

Building integration using Active directory wasn't chosen, because for being able to write any data to the AD, used account or service needs to have write and modify access to all user objects in AD which brings the security risks. Reading data from AD doesn't require special permissions, but writing does need and that's why the project team abandoned this option and continued investigating the other options.

5.3 SQL integration

The second option to transfer ID card data was to use direct SQL integration, so that ACR would write card numbers directly to Equitrac SQL database (Figure 20). From the technical perspective, building integration this way is not difficult either, but it makes Equitrac database vulnerable for any errors during data transfer, since all data is written directly to Equitrac database. This would have required continuous monitoring, because any software update or change on Equitrac, ACR or Windows platform could break this and there was no verification mechanism in Equitrac's side. The project team kept this as an option, but it wasn't preferred. Using direct database integrations is always a bad option, because it will bypass the original system and process totally.

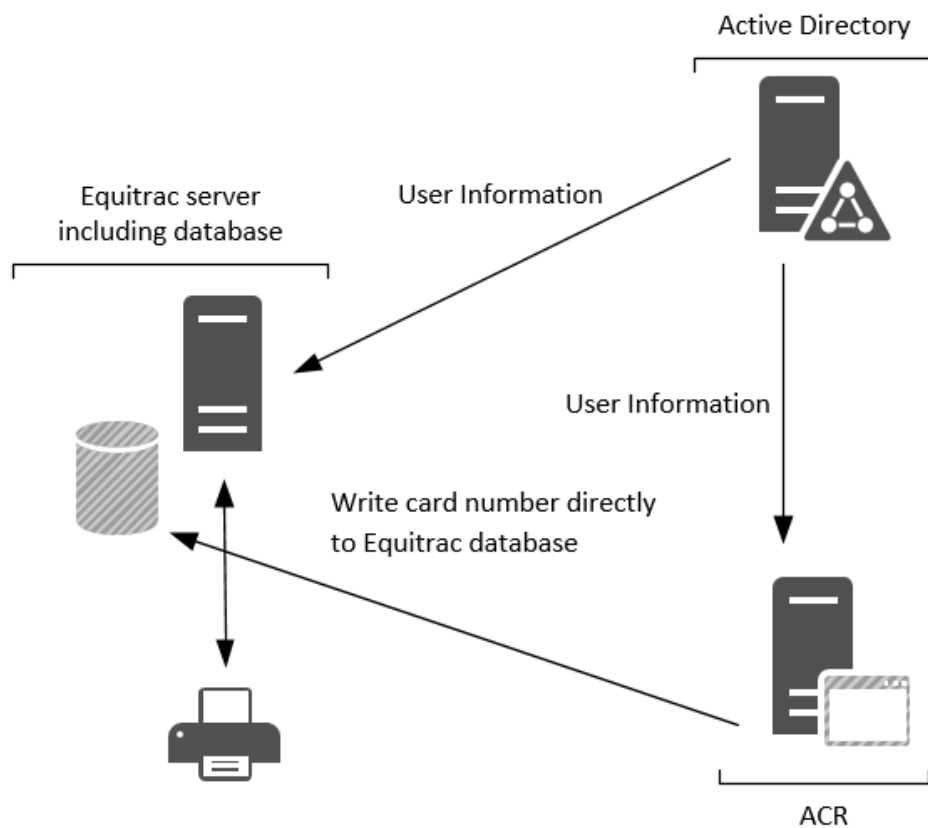


Figure 20 ACR Equitrac SQL integration

5.4 IBM message broker

The third option was to use IBM message broker which is an integration gateway – Enterprise Service Bus (ESB). ESB's purpose is to transfer messages from one system to another and perform syntax translations so that the target system will understand incoming messages. Integration using ESB was the primary option from the very beginning, but the project team wanted to examine other options as well, because previous integrations between ACR, working time registration and access management systems were really difficult and laborious.

The integration using a message broker was made by Integration Architect, together with Equitrac and ACR vendors. All data that Equitrac needed for identifying the user – the user and the card IDs – were already in one of the existing XML messages that is used to transfer data from ACR to the working time systems. Because all needed info was already in the existing XML message, the integration team created a copy of it, deleted all unnecessary fields on Message broker and translated it to CSV format for Equitrac.

Equitrac does not have API-interfaces, but it has a small command line tool called EQCMD.exe which has all the needed commands for modifying users in CAS and add ID card numbers to the user's data. The integration was built so that ACR sends all changes to the message broker immediately after changes, message broker makes the required changes to the message format and passes data to Equitrac. Then Equitrac runs its EQCMD.exe once per hour and adds all new and changed ID cards to CAS. So the time gap between generating a new ID card and activating it to Equitrac takes something between one minute and sixty minutes. Figure 21 shows how the integration was built.

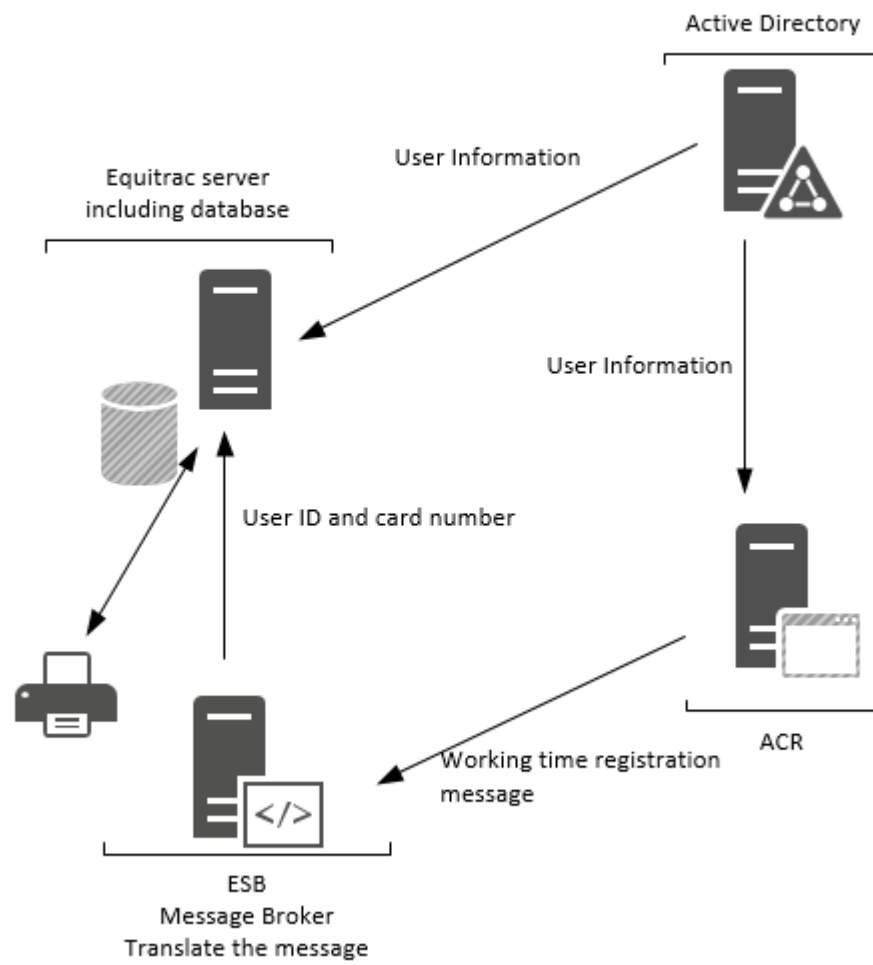


Figure 21 ACR Equitrac IBM Message broker integration

6 PROJECT OUTCOME

6.1 Secure Print

The implementation of Equitrac (FollowPrint) was divided into three phases:

- 1) device inspection and initial testing
- 2) planning
- 3) implementation

The Vendor performed the preliminary investigation based on the printer model lists before the project started. At that time the Vendor estimated that almost all of the devices will be supported and that statement served as the basis for starting the project. In the first phase, the target was to gather test results on which devices from the Tampere offices does support the same driver than the devices in the head office were using. Testing was carried out by printing documents with different setup of drivers and finishing settings (stapling, 2-side etc.). This testing was the most important phase of implementing Equitrac, because it defined which devices could be added to the Equitrac service. Testing took a couple of days, and based on its results, Vendor made an implementing plan and list of devices that could be added to Equitrac.

At the same time when the Vendor was testing devices, the project team had internal task to gather information on whether there were applications that might not be compatible with Equitrac. The only application that came up was SAP, but after discussions with the local on-site support, it appeared that SAP uses direct IP printing and that it can bypass the secure print functionality on printers. So if all communication ports from the printers are remained open and not closed or blocked by firewalls, can be sure on that all applications that uses direct IP printing will work, no matter whether the secure printing is enabled on a printer or not.

Vendor's first deployment proposal included only 23% of all devices from the Tampere offices. All devices from the head office were supported, because they were only a couple of years old. That deployment plan was rejected immediately since that was far away from what was promised before the project started. The project took a short time break and Vendor made two weeks of more testing and planning in Tampere. After that Vendor made a proposal which included 85% of devices from the Tampere offices. Spending

more time with testing and planning, the amount of supported devices increased by 62% (Figure 22). The steering group accepted this new deployment plan (Vendor 2016b) and allowed to continue to the next phase, which was about the user testing in the head office.

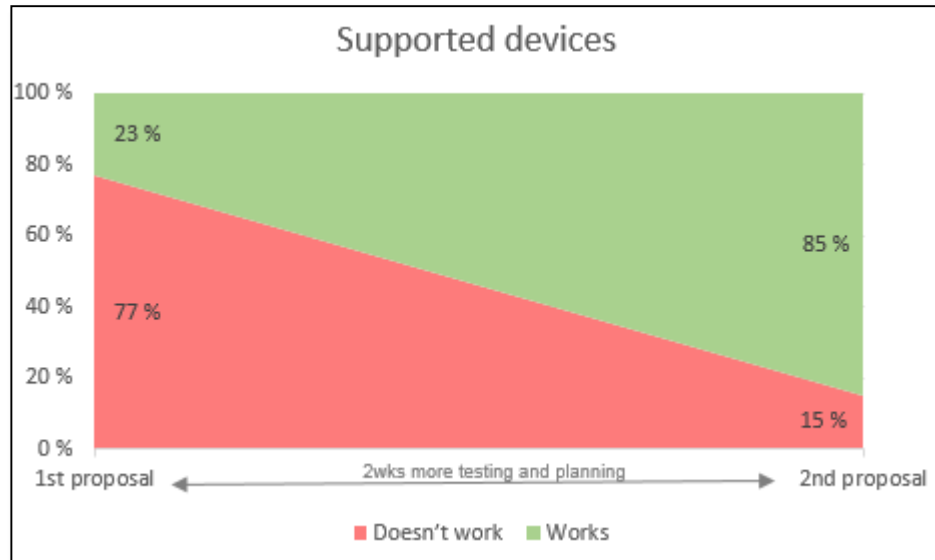


Figure 22 Equitrac supported devices in Tampere offices

The testing with one device started next and lasted a couple of days, and the target was to let users test the new FollowPrint service and make sure that it works. The testing did not bring any issues, so the project moved to the last phase and Vendor installed the FollowPrint queue to all devices in the head office. The implementation took two days and included software changes from the old system to the new and switching card readers. In the Tampere offices, the installations took four days and after that FollowPrint was ready to use. The actual go-live in Tampere was a month later, at the same time with ACR implementation, because most of the employees in Tampere offices did not have ID cards that would work with FollowPrint card readers.

After the technical part of the project had finished, Vendor provided technical documentation and the project team made Equitrac runbook for application support team. That documentation provides all technical details that are needed for example in the Windows server patching. Also all common questions and problems were documented and added to knowledge database for the IT Service Desk, so that they can have answers for all common questions that might come from end users. For example, the most common problem which users had after implementing FollowPrint, was that documents didn't appear to print queue. The reason was that users had not changed their print queue

from the old SecurePrint queue to the new FollowPrint queue. And by documenting this and all other common questions, Service Desk could check whether a solution already existed for similar problems and give the possible answer directly.

6.2 Mobile Print

In the beginning of the project, mobile print was supposed to be the Plan-B if Equitrac would not be ready on time. According to the Vendor, Xerox Mobile Print Cloud (XMPC) was supposed to be easy, and fast to install and configure, so that there was no need for any additional testing. Problems which came with this solution were information security and lack of understanding how this solution worked. The XMPC email service didn't support TLS (Transport Layer Security) encryption for the transmission of emails and attached documents, see Figure 23. The first table is from cloudapp.net where XMPC is hosted and the second one is just for comparison and is from Google's gmail.com. Emails are sent as plain text to the XMPC cloud service. This was the first problem which came up when Vendor had a security review meeting together with the company's IT Security and Compliance Manager. Lack of TLS support wasn't mentioned in XMPC Information Assurance Disclosure documentation and not having TLS support was surprising, because it is nearly a standard for transferring emails (Xerox 2015b, 3-28).

MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
cloudprintengines.cloudapp.net [70.37.88.220]	10	OK (74ms)	OK (57ms)	OK (58ms)	FAIL	FAIL	FAIL	OK (248ms)	OK (58ms)
Average		100%	100%	100%	0%	0%	0%	100%	100%
MX Server	Pref	Con-nect	All-owed	Can Use	TLS Adv	Cert OK	TLS Neg	Sndr OK	Rcvr OK
gmail-smtp-in.l.google.com [74.125.196.27]	5	OK (43ms)	OK (62ms)	OK (44ms)	OK (42ms)	OK (284ms)	OK (45ms)	OK (53ms)	OK (338ms)
Average		100%	100%	100%	100%	100%	100%	100%	100%

Figure 23 TLS support test using checktls.com 03/2016.

The second thing that came up after middle of the project, was that all printers which were planned to support mobile print, have to have Internet connection to XMPC (EIP apps). At the security review meeting, the Vendor described that the connection will go through of the Equitrac server, where the XMPC agent is installed and only that service needs to have an Internet connection. So instead of having a single connection from the server, this changed to scenario where the printer VLAN (separate printer network) needs to have

the access to Internet. The project team kept this still to be possible, because if the printer VLANs already has an access to the allowed (whitelisted) websites, it would then require only to be adding XMPC site to whitelist.

In the XMPC documentation the connection workflow is described so that the agent service will handle all document routings (Xerox 2015b, 2-9) and there is no mention about printers needing an Internet connection. But in the chapter "Mobile Print Cloud EIP App Specific", which tells about web emblems, there is the following quote: "When accessing the Xerox Mobile Print Cloud EIP App, web pages (HTML, JavaScript, icons, etc.) are served up by the Xerox Mobile Print Cloud Service" (Xerox 2015b, 3-19). This doesn't directly tell that printers need to have an access to XMPC service, but in the XMPC administration guide this is represented clearly: "Note: If you plan to install the EIP App, enable and configure the Extensible Services Proxy settings on the printer. The @PrintByXerox app requires proxy access." (Xerox 2015a, 1-5). So the need to have an Internet connection through proxies' was described in the official documentation from Xerox, but the Vendor was not aware of it.

In the Information Assurance Disclosure document, it is mentioned that XMPC service is hosted in Microsoft Azure, but not physically where (Xerox 2015a, 3-17). This was the third point which was asked in security review meeting from the Vendor, but since the documentation did not have a proper answer, Vendor contacted Xerox to get the information. Xerox replied that XMPC is hosted in Texas, Azure datacentre. This was the final show stopper for XMPC, because the Safe Harbour regulation was invalidated in October 2015, which protected Europe's data that were located outside of European borders (Court of Justice of the European Union, 2015). Since all company data has to be located within Europe and XMPC was hosted in Texas, the company can't use it.

After the XMPC version was cancelled, the project team started to plan the best way to implement the on-site mobile print version. The official recommendation was to install mobile print and Equitrac to different servers, but the project team didn't expect that mobile print would be so heavily used, that it would need a server of its own. Vendor also confirmed that they have had cases where they had installed both services into the same server without having any problems. Before installations, the project team requested to take a snapshot from the virtual server to be ensured of that if something goes wrong, the server can always be restored back to the old working state. During the installations, the

installation process failed on SQL database creation. After investigations, Vendor found the reason for the failure, which was that the mobile print was incompatible with the SQL 2014 version which was used on Equitrac installation. After that the options were either to install SQL 2012 version, use Microsoft SQL Server Compact 4.0 or request a new virtual server for mobile print.

After these setbacks, the steering group decided to cancel the mobile print deployment. This was an understandable choice, because costs were increased, Vendor didn't have a clear understanding of how these mobile print solutions worked and what were the requirements from the IT infrastructure. As the final task, Vendor cleaned all mobile print components away from the Equitrac server.

7 CONCLUSIONS

The project was deployed successfully and on schedule after all; even though the mobile print was cancelled. The main target of the project was to have one secure print queue for all three main offices and that way ensure that documents will stay secure and there would not happen miss printings. In the head office each printer was added to FollowPrint service and from the two Tampere offices, at least one printer from each copy room, since all of them were not supported. FollowPrint allows people to use the same print queue, no matter whether they are in the Tampere offices or in the head office. Since FollowPrint requires users to authenticate on the printers, it ensures that printouts aren't printed automatically and confidential documents will remain secure.

Even though the secure print service was implemented on time, the project delivery didn't go that well. It was defined in the service description that Vendor will name the project manager and deliver the new service. The customers' responsibility was to provide steering and support to company specific problems (Vendor 2016a). The project manager and technician were the same person at this time and from authors' perspective that was a poor choice, since he had to lead the project and at the same time take care of the technical part. Because of that, project management was always a little behind and tasks for the project team came in short notice. It would have been more beneficial to have a different person for project management and someone else for technical tasks. That could have made things go more "smoothly". For example, free IP addresses for ID controllers were requested the day before on the afternoon, when installations were supposed to begin in the Tampere offices. If the project would have had a separate project manager, he would have had more time to focus on upcoming tasks and more time for preparing next week's schedule and agenda.

From the IT support perspective FollowPrint brings little challenges, since current printing support is already divided into half. One vendor owns the devices and is responsible for printers being functional, and another vendor is responsible for that users can print and printers and print queues are online. Now FollowPrint is supported by a third vendor, who owns Equitrac, card readers and printing app on printers. If there appears any problems with FollowPrint queue, there are three possible support groups who might be able to fix the issue. The project team documented all the most common issues and questions, determined the division of responsibilities. Even then there has been

several tickets that were hopping from one support group to another, when it's unclear who can or is responsible for fixing the issue. For the next printing service contract, it would be better to consider only one vendor to manage all print related services – including devices. This would be beneficial for all participants, since the same vendor could then handle all printing related issues.

Implementing FollowPrint to new sites is possible, but there will be problems with authentication. Since authentication using an ID card basically replaces entering the pin code (the ID card number is the pin code), and the user can have only one ID card registered at the same time. The card reader on printer doesn't know what it is reading, just that it can or cannot read it. The company has at least four different access control systems in use, with different RFID tags and several offices that only have physical keys. If the card readers are configured so that they can read only the used RFID frequency of the site access tags, the ID card which the user has registered on his primary location might not work. Because the user's primary ID card or access tag might use a different frequency and the card reader on the another site cannot read it. If the user then registers a new RFID tag (pin number), it will overwrite the original RFID tag (pin number) and then the original one doesn't work anymore. So either the used RFID chip has to be the same on all sites or the card reader needs to have the capability to read several different types of RFID chips simultaneously. A possible solution could be to use RFID stickers that uses the same frequency of company's ID cards in head office. Since in the future, all sites that will get ACR implemented, will have ID cards with two RFID chips and another of them will be the same RFID chip as in the company's head office. In that way almost all clerical workers will have FollowPrint compatible ID card at some point.

The amount of sites per secure print queue will require good planning. Since one secure print queue can only have one driver and it will force certain functionality requirement for all devices within the same queue. This wouldn't be a problem at the very beginning of the next printing service contract, but it might cause problems later on when printers starts to get old. Accounting capabilities should be investigated from the support perspective, because Equitrac can offer a centralized tool for monitoring and managing printers. Having all printers managed by Equitrac will require high capacity servers and good load balancing for ensuring small latency and good printing experience.

Mobile printing will have its place in the future for BYOD and mobile devices. Increasing use of mobile devices will force companies to reassess network hierarchy by allowing non-domain devices to have access to local resources among with print servers. And even more services are moving to cloud, away from local servers – e.g. Office365. Maybe at some point the whole printing infrastructure will be hosted in cloud – printing as a service?

From the author's perspective, the most difficult part on this project was the beginning, since the project was already started when the author joined it. The project team had already made some decisions – for example selected the Vendor and used software – and Vendor had done some initiative tasks. But after couple of meetings, it started to get clear on what had already been done and decided. Some of the issues that came up later in the project, could have been avoided if there had been a little more time to read and study the documentation of used secure and mobile print software in at the beginning of the project. Of course this wasn't required from the authors' role at that time, but studying the used software solutions was part of the thesis. Most of the references in thesis were from technical documents, because there weren't much of independent studies from this topic. That made some limitations for thesis research part, but didn't affect the scope. Having coordinator's role in the project wasn't so technical as the author hoped at that time, but it taught a lot of project management skills and gave better understanding to IT processes.

REFERENCES

Buyers Lab (BLI). 2009. Equitrac Office 4.1 Solutions Report. Read 21.06.2016
<http://www.nuanceequitrac.com/downloads/Equitrac-Office-4.1-Buyers-Lab-Solutions-Report.pdf>

Court of Justice of the European Union (CURIA). 2015. US Safe Harbour Decision is invalid - Press release No 117/15. Read 20.06.2016
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>

Nuance. 2014. Equitrac Office and Express 5.4 Planning Guide.
Internal project team site

Nuance. 2015a. Success story - Swiss Graubündner Kantonalbank. Read 06.07.2016
<http://www.nuance.com/for-business/imaging-solutions/resources/success/equitrac-for-swiss-bank/index.htm>

Nuance. 2015b. Xerox Security Access Unified ID System 5.5 Administration Guide.
Read 14.07.2015
https://download.equitrac.com/828172/XSA/XSA5.5/Docs/XSA_Administration_Guide.pdf

Nuance. 2016. Success story - Large Fortune 500 financial services organization. Read 06.07.2015
<http://www.nuance.com/for-business/imaging-solutions/resources/success/equitrac-for-fortune500/index.htm>

Ponemon Institute. 2016. Cost of Data Breach Study. Read 01.08.2016
<http://www-03.ibm.com/security/data-breach/>

Quocirca. 2013. Printing: a false sense of security? Read 02.08.2016
<http://www.nuance.co.uk/landing-pages/imaging/quocirca/print-security-quocirca-whitepaper.pdf>

Quocirca. 2015. The Mobile Print Enterprise - Are businesses ready for mobile printing? Read 29.07.2016
<http://quocirca.com/content/mobile-print-enterprise-2015>

Vendor. 2016a. Palvelukuvaus_Turvatulostus. Internal project team site.

Vendor. 2016b. Kayttoonottosuunnitelma-esitys. Internal project team site.

Xerox. 2006. Equitrac sample reports. Read 20.07.2016
<http://www.office.xerox.com/latest/SOLDS-02.pdf>

Xerox. 2012. Xerox Mobile Print Solution - Information Assurance Disclosure.
Software Version 2.5. Version 1.3. Read 20.07.2016
http://www.xerox.com/download/security/information-assurance/5cc28-4cdbfb0c523c0/cert_Mobile_Print_Information_Assurance_Disclosure_Paper_V1.3.pdf

Xerox. 2015a. Xerox Mobile Print Cloud - Administrator How To and Troubleshooting Guide 3.0. Read 21.07.2016

http://download.support.xerox.com/pub/docs/MOBILEPRINTCLOUD/userdocs/any-os/en/702P03413_XMPC_Administrator_3.0_EN.pdf

Xerox. 2015b. Xerox Mobile Print Cloud - Information Assurance Disclosure. Software Version 3.0. Read 18.05.2016

<https://www.xerox.com/download/security/information-assurance/51354-52664fa2cde03/Xerox-Mobile-Cloud-Print-IAD-v3.0.pdf>

APPENDICES

Appendix 1 Equitrac reporting

List of Available Reports

NOTE: reports that are new to 4.1 are underlined

Account Reports

- Account adjustment
- Account listing
- Account statement
- Billing code authorizations
- Color quota summary
- Department members
- Pay Station Deposit Center account adjustment*

Analysis Reports

- Authentication
- Color usage by network user
- Device availability
- Device configuration
- Device Faults
- Device Faults vs. Usage
- Device usage
- Hourly activity
- Last transaction time
- Simplex usage by network user
- Usage summary by activity type

Detailed Activity Reports

- Detailed activity by billing code account
- Detailed activity by department account
- Detailed activity by department membership
- Detailed activity by device
- Detailed activity by network user
- Detailed activity by print queue
- Detailed activity by user account
- Detailed activity for routed documents by device
- Detailed activity for routed documents by user account
- Detailed activity for queued documents by device
- Detailed activity for queued documents by user account

Summary Activity Reports

- Summary activity for routed documents by device
- Summary activity for routed documents by user account
- Summary activity for queued documents by device
- Summary activity for queued documents by user account
- Summary activity by billing code account
- Summary activity by department account
- Summary activity by department membership
- Summary activity by device
- Summary activity by device and date
- Summary activity by network user
- Summary activity by network and device
- Summary activity by organization account
- Summary activity by organization membership
- Summary activity by print queue
- Summary activity by user account

Total Activity Reports

- Total activity by account type
- Total activity by billing code account
- Total activity by department account
- Total activity by desktop device
- Total activity by device
- Total activity by network device
- Total activity by network user
- Total activity by organization account
- Total activity by printer
- Total activity by print queue
- Total activity by user account

Uplinked activity

- Uplinked detailed activity
- Uplinked device usage
- Uplinked summary activity
- Uplinked total activity