System Description and Risk Analysis

Marc Gähwiler Leonhard Helminger Fabian Zeindler

21.11.2013

Contents

1 System Characterization

1.1 Introduction

The company iMovies produces film material in the area of investigative journalism. To protect the integrity and the secrecy of email conversations within the company, a certificate based solution should be provided which ensures the confidentiality of these email conversations.
The IT infrastructure of the company today divided into an internal network where the employees work with their desktop machines/laptops and a server area in which the a database server with user data, the web and email server as well as central storage for the employees is located. (this is an assumption by us, since there is no information about the status quo and iMovies is a relatively small company.) The status quo of the system is depicted in Figure 1.1.

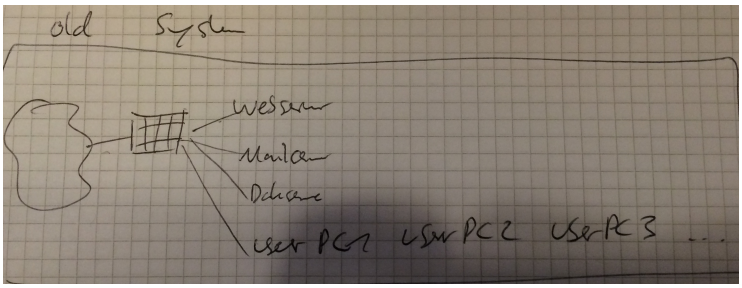

Figure 1.1: Diagram of the status quo.

We now are challenged with the task to design and implement a certificate authority that provides the employees with digital certificates to be used to secure said email connections. This certificate authority should withstand targeted attacks and be integrated into the current system. For assigning employees to certificates, the already existing user database should be used. For securing the new build infrastructure, the old system also has to undergo some changes. We will introduce a new level of isolation for critical systems and put systems that do not have to be accessed directly by users in a separate part. The design of the system will be evaluated in detail in the following sections. An overview of the proposed system is shown in Figure 1.2.

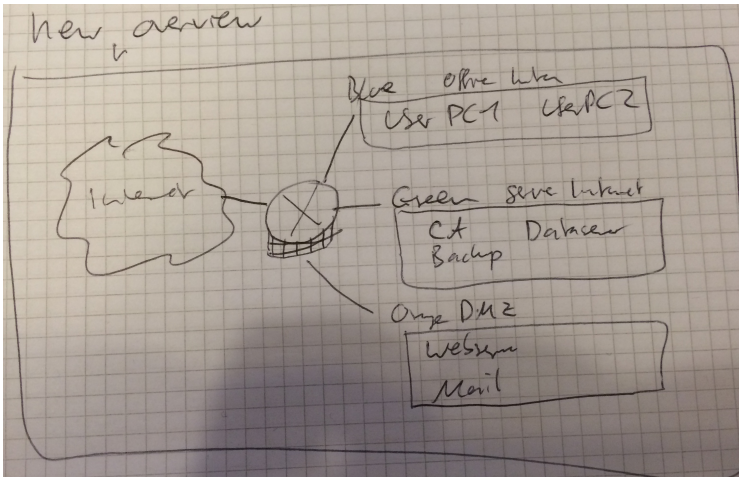

Figure 1.2: Overview of the proposed system.

1.2 System overview

The employee will use the certificate authority such that he connects to a website with his credentials stored in the database. He then can issue a certificate or revoke existing certificates. When at least one certificate is obtained, login with said certificate is also possible. The user only has to deal with this web interface, but there is more to the system than that. A separate server is responsible for the process of actually issuing and revoking the certificates in compliance with the information stored in the database. This database could remain a separate instance, but for reasons of simplicity and since the company is small, we put the database on the same server as the CA core which implements the previously described functionality of issuing, verifying and revoking certificates. To prevent loss of data, ensure key recovery and auditability on the system in general, we implement a backup solution as well as a logging system and a key archive. These are all system that do not need regular and close interaction with users or even administrators. We therefore put them together on a backup and archive server, shielded from the outside.
Since the user only interacts with the web interface which is publicly accessible, this is also the most exposed part of the system. We do not want it in close proximity of the most valuable part of the system, the core CA. We therefore set up a special demilitarized zone (DMZ) in which we place systems and functionality that has to be accessed from the outside. Every other functionality and system is not accessible from the outside and is placed in another zone.
Figure 1.3 shows the Webserver placed in the DMZ, the Core CA as well as the Backup/Archive server in an internal server zone.

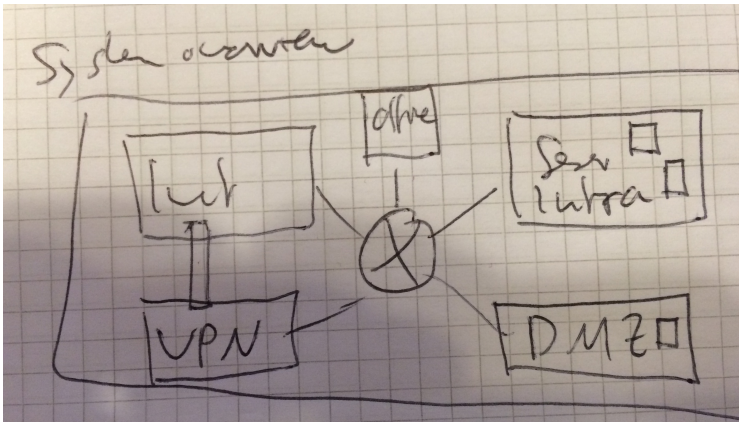

Figure 1.3: More detailed overview of the proposed system.

The zone in which the employees have their personal machines in the office is also discrete from the zone with the Core CA, the database and the backup. It is shown in Figure 1.3 but is not further discussed in this work, since the goal is to implement a certificate authority. For administrative remote access, we provide a VPN that allows an administrator to get access to all of these networks remotely.

We proceed with more detailed information about functionalities of the system and their implementation with special regard to security.

1.3 Requirements elicitation and system functionality

In this section we collect the requirements and the functionality of the proposed system. We first look at functional requirements to then give an insight in non functional requirements. We cover security requirements as a separate unit, since we want to emphasize the importance of these requirements to the certificate authority system.

1.3.1 Functional requirements

We first list the functional requirements we extracted from the assignment we got to implement this system. From this these requirements we conclude general use cases of the system and will also give an insight in possible misuse cases.

User Interface: A simple web interface which allows each user to log in either with his credentials from the legacy MySQL database, or one of his previously generated certificate and private key combinations. Once logged in the user can view his information (last name, first name and email address), change his password and update his information (last name, first name and email address). Additionally it is possible for the user to let the system issue a new certificate (based on his possibly changed credentials) and download the certificate with the newly generated private key in PKCS#12 format.

Administration Interface: A simple web interface (not the same as the user web interface) where CA administrators can consult the current CA state after a log in process which requires the CA administrators to authenticate themselves with their certificate. This includes the number of issued certificates, the number of revoked certificates and the current serial number.

Certificate Issuing and Revocation: The CA offers an interface that allows other systems to

- Generate new public/private key pairs.
- Generate a certificate that ties a public key to a user's credentials (first and last names and his email address) and sign this certificate with the CA's key.
- Revoke a previously signed certificate.
- Get a list that contains all revoked certificates (Certificate revocation list).

Key Backup: To prevent the loss of any information, that was encrypted with an issued certificate, every issued certificate and the according private key are archived.

System Administration and Maintenance: Each server is remotely accessible for the system administrator. Also the configuration of the systems running as well as the logging during operation is stored on the backup server.

1.3.1.1 Use cases

Figure 1.4 shows the use cases in a graphical manner. We also list each use case individually with a short description.

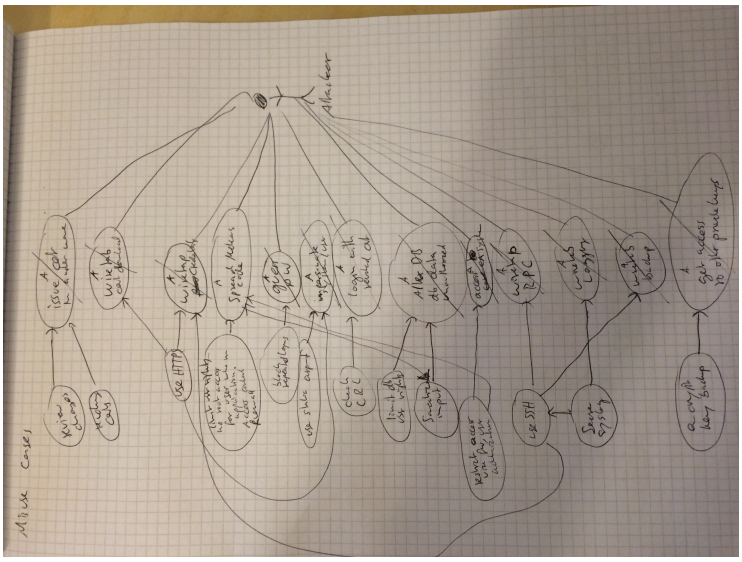

Figure 1.4: Use cases of the proposed system.

We first identify the participating roles:

- User (The employee who uses the web interface to view/change user data, issue, verify, download, revoke certificates)
- CA Administrator (Administrator who has access to certain CA information)
- System Administrator (Administrator who can access all systems remotely)
- Website/Webinterface (Displays information to users and CA Administrators)
- Core CA (Issues, stores, revokes, verifies certificates)
- Database (Stores user information)
- Backup/Archive (Stores certificates, private keys, logging information, backed up configurations)

We now list the use cases of these roles:

Web login User logs onto the webserver with his credentials or a certificate.

With certificate Login by presenting a certificate.

With credentials Login by presenting user name and password.

Verify credentials Presented credentials get verified against the information stored in the database (RPC call to CA Core).

Validate certificate The presented certificate gets verified. CA Core ensures that it is a proper certificate and not yet revoked.

Show user information The user information (except the password) stored in the database is displayed to the user (RPC call to the database).

Change user data The user changes any of the information stored in the database.

Review user data changes If a user changes information other than the password, the changes have to be reviewed by the CA Administrator before writing them to the database. All the users certificates get revoked.

Request certificate A user sends a request for a new certificate (RPC call to CA Core).

Issue certificate The CA Core issues a new certificate for the user who requested it. The certificate and the private key get archived.

Download certificate The user can download its newly generated certificate and his private key.

Backup keys After creating a new certificate, the CA Core also stores the new certificate and the according private key on the backup/archive server.

Revoke certificate A user or the CA Administrator set a certificate for revocation. (RPC call to CA Core).

Generate CRL When revoking a certificate, the CA Core generates a new or updates an existing CRL.

List CA information When a CA Administrator is logged in, his web interface displays the number of issued certificates, the number of revoked certificates and the current serial number.

System login The System Administrator remotely logs into one of the running system and can get root access.

Logging Each system automatically sends logging information of the system and the interactions with the system to the backup/archive server.

Run backups The backup server periodically runs backups to collect the configurations of the other systems.

Logout CA administrator and users that are logged in, can log out, which causes a new login prompt when visiting the site again.

1.3.1.2 Misuse cases

Figure 1.5 shows the misuse cases and also additional use cases that prevent this misuse cases in a graphical manner. We also list each misuse case individually with a short description.

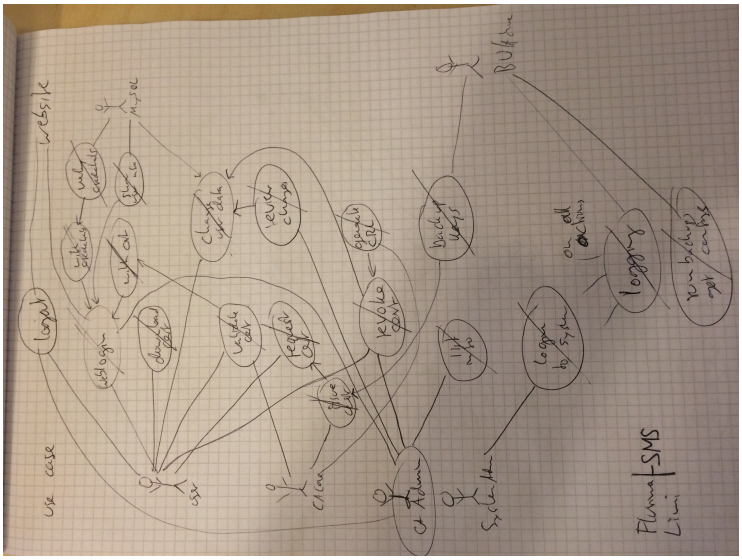

Figure 1.5: Misuse cases and additional use cases of the proposed system.

We first identify the participating roles:

- Thread agent (The attacker which can be an outsider as well as an misbehaving employee)

We now list the misuse cases of these roles as well as the preventing use cases:

Issue certificate in another name The attacker is able to alter his information and then issue a certificate with this information. This gets prevented by the CA Administrator reviewing changes other than to the password and revoking all its issued certificates.

Wiretap certificate download The attacker can obtain a copy of the certificate/private key pair of a user. This is prevented with enforcing HTTPS when connecting to the webservice.

Wiretap user credentials The username and password get obtained by the attacker during transmission. This is prevented with enforcing HTTPS when connecting to the webservice. For system administrator credentials, use SSH and VPN to connect to remote systems.

Guess password With multiple guesses, the attacker can bruteforce the password. To prevent this, limit the number of times a password for a given user can be tried.

Impersonate system/user An attacker can spooth and poison communication mechanisms to impersonate a certain role. Use HTTPS and SSH to prevent this. In the infrastructure controlled by iMovies, use static ARP tables to prevent poisoning.

Login with revoked certificate The attacker may get access to the system with presenting an invalid certificate. To prevent this, always check the CRL.

Alter database date unauthorized An attacker alters data in the database that does not belong to him. To prevent this, one can sanitize the input, review all changes to the database by the CA Administrator and restrict the database user to only the functionality he needs.

Access systems The attacker can login to the server systems. This is prevented by enforcing access control, only allowing certain traffic through the firewall and onto the system.

Access other private keys The stored private keys in the archive get obtained by the attacker. To prevent this, the private keys are stored encrypted.

Wiretap RPC An attacker obtains information transmitted between the webserver and the CA Core. To prevent this, the RPC traffic is tunneled via SSH.

Wiretap logging The logging information from the servers and applications sent to the backup server gets obtained by the attacker. To prevent this, secure syslog is used which uses an SSH tunnel.

Wiretap backup The attacker obtains system and configuration information by intercepting the backup transmission. SSH is used for backup to prevent this.

Running malicious code An attacker is able to run malicious code on one of the systems. To prevent this, the users executing this systems have limited rights, strong access controls are implemented and input is sanitized.

1.3.2 Non functional requirements

The following list specifies non functional requirements gathered during the analysis.

- For the user database, the legacy database in MySQL has to be used.
- New certificates and their private key are issued in the PKCS#12 format.
- Users with a valid certificate can authenticate them self over SSL/TLS to the website using the certificate.
- THERE IS MORE, BUT IT IS LATE...

1.3.3 Security requirements

Since the system is developed to bring more security to the way employees communicate, we honor the security requirements in a separate section. The following list is compiled from the initial assignment as well as from issues that arise from the misuse case diagram.

- Access control to CA Core functionality and data.

- Secrecy and integrity of private keys in the archive.
- Integrity, non-repudiation and accountability of log files on the backup server.
- Secrecy and integrity of the user data stored in the database.
- Access control on all systems.
- Confidentiality, integrity and authenticity with regards to key transport.
- Secrecy and integrity of CA Core data during processing and transport.
- THERE IS MORE, BUT IT IS LATE...

1.4 Components and Subsystems

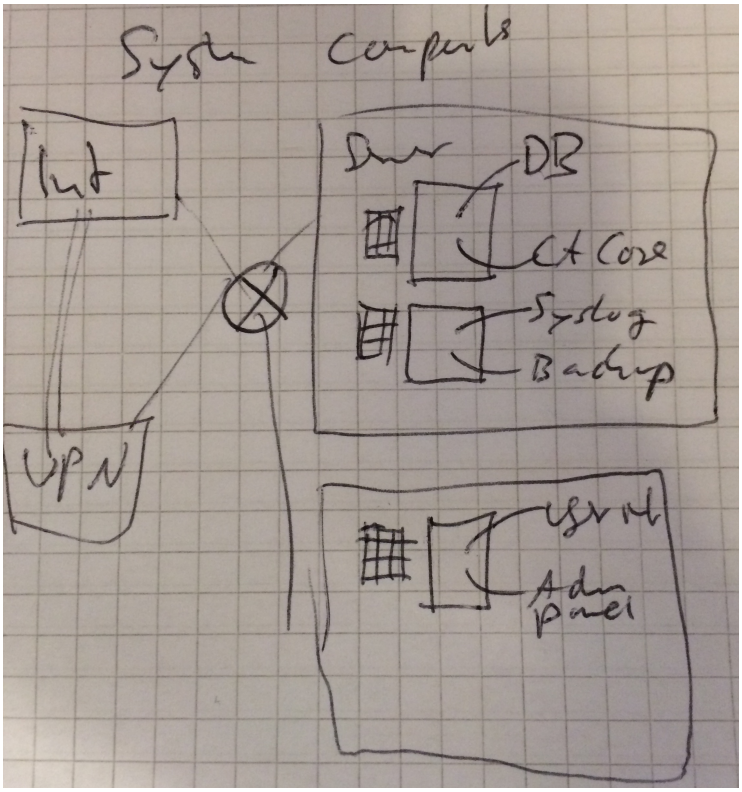

Figure 1.6: Components of the proposed system.

1.4.1 Platforms

The components (as depicted in Figure 1.6) are as follows:

Main Firewall A software firewall based on Linux (IPCop) that divides the iMovies network into the parts DMZ, internal server network, office network and the internet. The firewall functions as a VPN endpoint for remote administrative access and restricts traffic between the subdivided networks according to a security policy described later.

Web Server A Linux machine running debian 7.0. It hosts the website for the user web interface and the administrative panel. The web server is located within the DMZ, a local iptables firewall allows only HTTPS connections to the outside and SSH connections to the firewall for administration, to the CA Core for secure RPC calls and to the backup server for secure backup and syslog.

CA Core Server A Linux machine running debian 7.0. It hosts the logic for issuing, verifying and revoking certificates as well as the legacy MyQSL database. The server is located within the internal server network, a local iptables firewall allows only SSH connections to the firewall for administration, to the web server for secure RPC calls and to the backup server for secure backup, syslog and key backup.

Backup/Archive Server AA Linux machine running debian 7.0. It hosts a syslog server, the logic for periodic backups and storage for encrypted key backup. The server is located within the internal server network, a local iptables firewall allows only SSH connections to the firewall for administration, to the web server and CA Core server for secure backup, syslog and key backup.

1.4.2 Applications

User Web Interface Web application, developed in python running on nginx on the web server that allows the user to issue, verify and revoke certificates as well as view and alter user data. The website interacts with the CA Core via RPC calls.

Administration Panel Web application, developed in python running on nginx on the web server that allows the CA Administrator to review user changes and display information about the CAs status. The website interacts with the CA Core via RPC calls.

Legacy DB MySQL database with the legacy schema. Running on the CA Core server.

CA Core Application using the OpenSSL library that provides basic interfaces to create new key pairs, sign existing key pairs and revoke certificates. Running on the CA-Core server, interacting with the web server via RPC calls and backing up private keys on the archive server via SSH.

CA Core Storage A database that is used by the CA Core to store certain data relevant to the CA Core application. Running on the CA Core server.

Archive Storage for encrypted public keys and certificates on the Backup/Archive server

Backup A script that collects via SSH and keeps multiple backups from the other servers (especially of all the configurations), running on the Backup/Archive server.

Syslog A Syslog server that receives logging data via SSH tunnel from the other servers, running on the Backup/Archive server.

1.4.3 Data

User Information Basic information according to the schema of the legacy database. This includes the users username, his first and last name, his email address and a hash of his password. This information is stored in the legacy database.

Key Pairs Consist of a private key and the according public key that the CA Core generates on request. They are stored permanently in the archive and can be downloaded by the user. It is important, that the CA Core destroys his record of the private key as soon as possible.

Certificates A certificate that is signed by the CA Core. It is also stored in the archive and additionally also in the CA Storage (to allow certificates to be revoked).

Certificate Revocation List A list of certificates, that have been revoked by the CA Core. Stored on the CA Core server.

Local Users Credentials, that are used for system administration and communication between the components of the system. Individual to each system.

Configuration Files Configuration files define the configuration of a given system. They are in place at the system in question and backed up to the Backup/Archive server.

Log Files Log files generated by systems and applications. Stored on the Backup/Archive server.

1.4.4 Interfaces

Web Interface Different for user and CA Administrator but in general it offers a way of authentication via credentials or certificate. Information flows from the outside through this interface via secure RPC calls into the CA Core and vice versa in which case the information gets displayed.

Legacy DB Interface Offers the functionality to ask for, alter and insert information to and from the database.

CA Core Interface Gets accessed via a RPC call to offer functionality to issue, revoke or verify certificates.

Backup/Archive Interface Implements syslog functionality to provide a syslog endpoint as well as storage for key and configuration backup.

1.5 Implementation

This section describes the implementation of our hardware and software with an emphasis on the security measures installed.

Main Firewall The Main Firewall is a software firewall running the IPCop Linux. It functions as a firewall as well as a router and divides the network into the sections DMZ, internal server network, office network (which is not implemented here), internet and VPN network. The routes to the known hardware of the iMovies infrastructure are statically assigned as well as the ARP tables to prevent poisoning. The firewall maintains a VPN using OpenVPN to allow remote access to the VPN network. Remote access to the firewall is possible via SSH out of the VPN network or via webinterface from address 10.10.10.33 from within the internal server network.
The firewall implements several rules on how traffic is allowed to flow between those networks. By default all traffic is denied and silently dropped at the firewall. The following list shows the allowed exceptions:

Source	Protocol	Destination	Description
Webserver	HTTPS (443)	Internet	Allow secure webtraffic from the webserver
Internet	HTTPS (443)	Webserver	Allow secure webtraffic to the webserver
10.10.10.33	IPCop HTTPS (8023)	MainFirewall	Allow the use of the webinterface
OpenVPN network	IPCop SSH (8022)	MainFirewall	Allow remote administrative access
BackupServer	IPCop SSH (8022)	MainFirewall	Allow backup
OpenVPN network	SSH (22)	Backupserver	Allow remote administrative access
OpenVPN network	SSH (22)	CACore	Allow remote administrative access
OpenVPN network	SSH (22)	Webserver	Allow remote administrative access
Backupserver	SSH (22)	Webserver	Allow backup and tunneled syslog
Webserver	SSH (22)	CACore	Allow tunneled RPC calls
CACore	SSH (22)	Webserver	Allow tunneled RPC calls

Servers in general We deploy three servers, the web server, the CA Core server and the Backup/Archive server. All servers are running debian in version 7.0. They have three users, root, an admin and an operational user. The operational user is not in the sudoers list and cannot get root access and should therefore be used to run the applications. We deactivated su and only allow sudo. Per default we deny all

access via PAM (the Pluggable Authentication Modules). We ensure that the root user can only login locally and disable remote login. Failed login attempts get logged and automatically transmitted to the syslog server located on the Backup/Archive server. To prevent poisoning, we fix the ARP tables with the MAC addresses of all interacting systems.
SSH is used for various interactions. We only allow the admin user and the operational user to have SSH access. With the help of sshguard we introduce a exponential time delay after three failed login attempts by implementing temporary rules to the local iptables.
Each server has a local firewall based on iptables which blocks all connections by default. The exceptions are specific to the server and listed in their detailed implementing description.
On the servers, the number of running processes is kept to a minimum, especially processes with network capabilities. With the help of the debian harden package, all unnecessary packages like telnet were removed. The services running on every system are sshd and rsyslogd. Some systems run additional services which are specified later.

Webserver The basic setup is as described in **servers in general**. As the webserver needs additional functionality for running the websites and interacting with the CA Core, some more details have to be provided.
The webservice used is nginx which was modified to only accept HTTPS request, meaning redirecting HTTP requests to HTTPS. Also there were measurements taken to minimize information leakage through server status and error pages. DESCRIBE HERE WHAT WAS DONE. ALSO DECRIBE WHAT COULD BE DONE AGAINST DDOS ETC.
The two applications, the user web interface and the admin panel are developed in python. Both applications were written with `Flask`, a microframework for web development. This open source framework provides all neccessary tools to build a simple and secure web application. For the encrypted connection to the legacy database and the CA-Core we are using Pyro4, a distributed object middleware, which enables the web applications the communication with the CA-Core and a SSH tunnel which provides a secure connection between these two components.
To prevent cross-site request forgery (CSRF) attacks we are using the CRSF token provided by the flask framework and the user inputs are sanitized in flask automatically to render cross-side script (XSS) attacks impossible.
In the case, that a adversary tries such attacks the two applications have a fine log system, that every access to a site with the given parameter is logged on the webserver.

SAY WHAT WAS USED TO BUILD THE APPLICATION, TO SANITIZE USER INPUT, TO ENSURE CORRECTNESS AND SECURITY, MAYBE ALSO MENTION LOGGING.
The web applications interact with the CA Core via RPC calls implemented by SAY HOW RPC IS IMPLEMENTED. The secrecy and integrity of these RPC calls are

ensured by tunneling these calls via SSH to the CA Core server.
As all the servers, the webserver has a local iptables firewall which silently drops everything by default and implements the following exceptions:

Source	Protocol	Destination	Description
Backupserver	SSH (22)	Webserver	Allow backup
OpenVPN network	SSH (22)	Webserver	Allow remote administrative access
Internet	HTTPS (443)	Webserver	Allow secure web traffic
CACore	RPC (4444)	Webserver	Allow tunneled RPC call
Webserver	HTTPS (443)	Internet	Allow secure web traffic
Webserver	RPC (4444)	CACore	Allow tunneled RPC call
Webserver	syslog (10514)	Backupserver	Allow tunneled syslog
CACore	SSH (22)	Webserver	Allow tunneled RPC call
Webserver	SSH (22)	Backupserver	Allow tunneled syslog

CA Core In addition to the basic setup described in **servers in general**, the CA Core server houses the legacy MySQL database and the application that provides the functionality of issuing, verifying and revoking certificates.
The MySQL database grants access to the table iMovies.users via the database user dbuser. This user only has limited rights, namely he can INSERT, SELECT and UPDATE only. There is no need for encrypting SQL traffic, since the database is on the same host as its consumer.
The application who implements the certificate authority functionality works as follows DESCRIBE WHAT YOU IMPLEMENTED IN WHAT LANGUAGES, WHICH LIBRARIES WERE USED, HOW RPC IS IMPLEMENTED, WHAT WAS DONE IN TERMS OF SECURTY, DELETION OF PRIVATE KEY, HOW DOES THE PRIVATE KEY BACKUP WORK, MAYBE ALSO MENTION LOGGING.
The interaction with the webserver happens via RPC calls over a SSH tunnel to ensure the security requirements. The same is true for the backing up of the private key, which gets moved to the Archive/Backup server through a SSH tunnel.
The CA Core also implements a local, iptables based firewall which denies everything by default with these exceptions:

Source	Protocol	Destination	Description
Backupserver	SSH (22)	CACore	Allow backup
OpenVPN network	SSH (22)	CACore	Allow remote administrative access
Webserver	RPC (4444)	CACore	Allow tunneled RPC call
CACore	RPC (4444)	Webserver	Allow tunneled RPC call
CACore	SSH (22)	Backupserver	Allow key backup
CAcore	syslog (10514)	Backupserver	Allow tunneled syslog
Webserver	SSH (22)	CACore	Allow tunneled RPC call
CACore	SSH (22)	Webserver	Allow tunneled RPC call

Archive/Backup server The functionality this server implements in addition to the basic

setup described in **servers in general** is storage for the backed ups private keys, a script that backs up the configurations of the servers and a rsyslog server that collects the syslog data sent by the other machines and applications. Backup, syslog and key backup is done directly via SSH or via an SSH tunnel.
The local iptables firewall that closes all ports by default implements the following exceptions:

Source	Protocol	Destination	Description
CACore	SSH (22)	Backupserver	Allow key backup
OpenVPN network	SSH (22)	Backupserver	Allow remote administrative access
Backupserver	SSH (22)	CACore	Allow backup
Backupserver	SSH (22)	MainFirewall	Allow backup
Backupserver	SSH (22)	Webserver	Allow backup
Webserver	syslog (10514)	Backupserver	Allow tunneled syslog
CAcore	syslog (10514)	Backupserver	Allow tunneled syslog

1.6 Operation

During operation of the system several actions can be performed to keep the system secure and detect misuse or an attack early on.

Update Perform regular updates of all system software to avoid security holes.

Logging Evaluate the logs and look for anomalies unintended patterns.

Audit Make sure that the information in the logs can be linked to a specific user and action for accountability.

Backup Check that the backups work and also check if playing back a backed up configuration would work.

Detection Try to detect misuse with monitoring programs. Like monitoring overall network traffic which should be fairly low under normal usage or run intrusion detection systems. The installed libraries harden-nids for network intrusion detection and harden-surveillance for network surveillance from the harden package can help with that task.

1.7 System documentation

This section is in some sense a summary of the above with some additional information about the systems like usernames, passwords, IP addresses, virtual network names etc. Use this section for administrative purposes of the system.

1.7.1 Network diagram

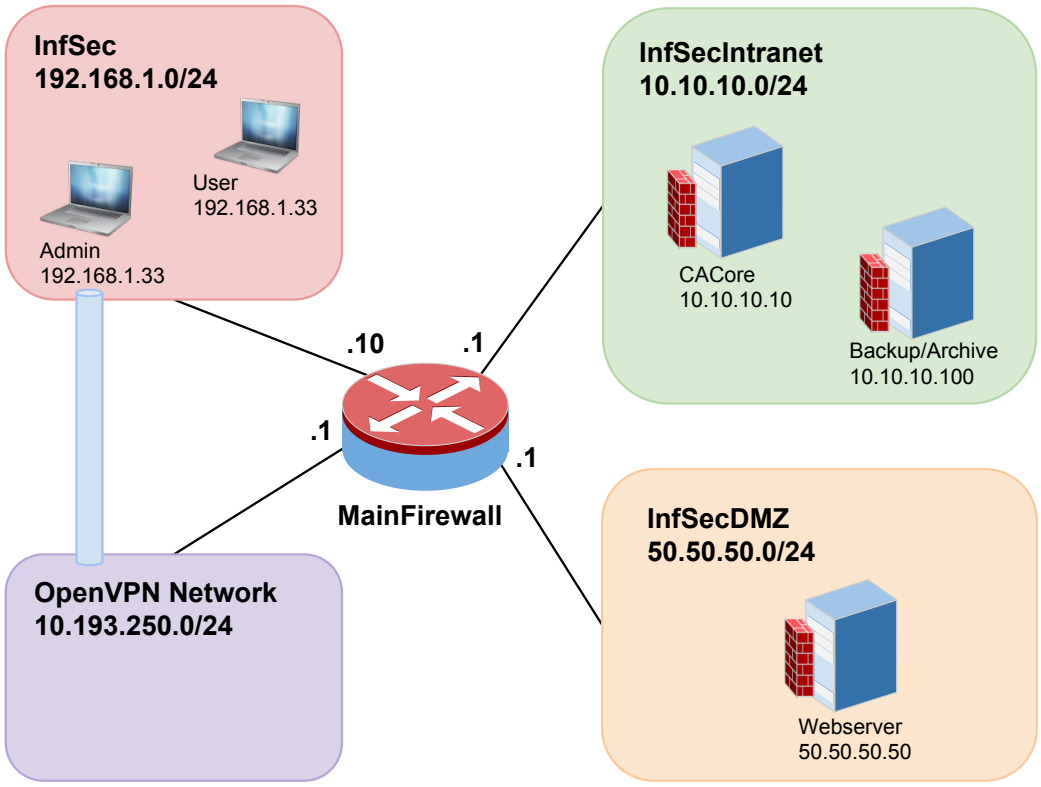

Figure 1.7: Network Diagram

1.7.2 Machines

All servers are equipped with at least one NIC corresponding to the network they are in as shown in Figure 1.7 and a NAT NIC that can be used for internet access (git, apt-get, etc.).

1.7.2.1 MainFirewall

Accounts & Passwords

admin: wT7nDB7A7d7V **root:** 5hmAMWxN6uVa

Installed software

IPCop

User for ssh access

Accesable only on 10.10.10.1 with port 8022 from 10.10.10.33 (user in InfSecIntranet) or from OpenVPN-Network.
ssh -p 8022 admin@10.10.10.1

Additional information

There is a webinterface on https://10.10.10.1:8023. Only accessable from 10.10.10.33 (user in InfSecIntranet).

1.7.2.2 Webserver

Accounts & Passwords

serveruser: 3FaVLt9RNxLu **operuser:** KLs3PbjoXu9m

root: cLepMVRq8wDQ

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, nginx, python, flask, openSSL, openSSH

Running services (lsof -i)

sshd, nginx

User for ssh access

ssh {operuser, serveruser}@50.50.50.50

additional information

SSL signing key for HTTPS: 9klTRxBQcAnM

1.7.2.3 CoreCA

Accounts & Passwords

causer: 9BxkXM5fLLL8 **operuser:** PrCgs5TLqW4f

root: 8kSeddphG6Ac

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, python, mySQL, openSSL, openSSH

Running services (lsof -i)

sshd, mysql (only localhost)

User for ssh access

ssh {operuser, causer}@10.10.10.10

additional information

MySQL root: Cm7NsWBhf52C
MySQL dbuser: Q8mxLsBwTLJi
dbuser is only allowed to INSERT, SELECT, UPDATE the table user.iMovies, thus should be used for connecting to the database.

1.7.2.4 Backup/Archive Server

Accounts & Passwords

archiveuser: 4uMtrPMLxShw **operuser:** QT5wbxjCN8gG

root: gaBWUt5EH8vU

operuser cannot use sudo/su and should therefore be used to run the application.

Installed software

Debian, iptables, syslog, openSSH

Running services (lsof -i)

sshd

User for ssh access

ssh {operuser, archiveuser}@10.10.10.100

1.7.2.5 User

Accounts & Passwords

alice: alice

additional information

When running in netwok InfSec, VPN is possible (VPN start script on Desktop):

PKCS12 PW: StgmE58sadQu

When running in netwok InfSecIntranet, firewall web access on https://10.10.10.1:8023

1.7.3 Firewall rules

1.7.3.1 MainFirewall

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Webserver	HTTPS (443)	InfSec
InfSec	HTTPS (443)	Webserver
10.10.10.33	IPCop HTTPS (8023)	MainFirewall
OpenVPN network	IPCop SSH (8022)	MainFirewall
10.10.10.33	IPCop SSH (8022)	MainFirewall
BackupServer	IPCop SSH (8022)	MainFirewall
OpenVPN network	SSH (22)	Backupserver
OpenVPN network	SSH (22)	CACore
OpenVPN network	SSH (22)	Webserver
Webserver	RPC (4444)	CACore
CACore	RPC (4444)	Webserver
Backupserver	SSH (22)	Webserver
Webserver	SSH (22)	CACore
CACore	SSH (22)	Webserver
Webserver	syslog (10514)	Backupserver

1.7.3.2 Webserver

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Backupserver	SSH (22)	Webserver
OpenVPN network	SSH (22)	Webserver
InfSec	HTTPS (443)	Webserver
CACore	RPC (4444)	Webserver
Webserver	HTTPS (443)	
Webserver	RPC (4444)	
Webserver	syslog (10514)	Backupserver
CACore	SSH (22)	Webserver
Webserver	SSH (22)	

1.7.3.3 CoreCA

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
Backupserver	SSH (22)	CACore
OpenVPN network	SSH (22)	CACore
Webserver	RPC (4444)	CACore
CACore	RPC (4444)	Webserver
CACore	SSH (22)	Backupserver
CAcore	syslog (10514)	Backupserver
Webserver	SSH (22)	CACore
CACore	SSH (22)	Webserver

1.7.3.4 Backup/Archive Server

All connections are closed by default. The following list shows the allowed exceptions:

Source	Protocol	Destination
CACore	SSH (22)	Backupserver
OpenVPN network	SSH (22)	Backupserver
Backupserver	SSH (22)	CACore
Backupserver	SSH (22)	MainFirewall
Backupserver	SSH (22)	Webserver
Webserver	syslog (10514)	Backupserver
CAcore	syslog (10514)	Backupserver

1.8 Backdoors

Describe the implemented backdoors. **Do not add this section to the version of your report that is handed over to the team that reviews your system!**

2 Risk Analysis and Security Measures

2.1 Stakeholders

The process of protecting email content with certificates for investigative journalism and film making at iMovies involves three stakeholders.

iMovies as a company and all its employees are the ones sending, now protected, emails. There is a need for trust of the informant that iMovies does not disclose about them or their statements to the investigated party. iMovies is eager to be trustworthy as it is essential to get the information needed.

Informants are the people who disclose sensitive information about the investigated party. Informants need to trust iMovies to handle the information handed over delicately.

Investigated party are the people or company that is investigated by iMovies and who's information gets disclosed by the informant. Their goal is to find the informant or the leaked information.

This risk analysis is commissioned by iMovis and hence we consider iMovies point of view when conducting thread and asset analysis.

2.2 Information Assets

In this section we outline the assets of the system, meaning everything that is part of the system and of value to the stakeholder. We subdivide assets into physical objects, logical objects, persons and intangible goods.

2.2.1 Physical assets

Firewall The firewall is located in the locked server room on the first floor of the iMovies office building in a separate rack with two redundant power supplies. The state of the firewall can either be up, up and compromised or down. Where up defines working as intended, up an compromised means the firewall is running but there is unauthorized logical or physical access to the system and down describes a non working firewall.

Webserver The webserver is located in the locked server room on the first floor of the iMovies office building in a separate rack with two redundant power supplies. Possible states are similar to the firewall.

CA Core server The core server is located in the same room as the firewall and the webserver and also has a redundant poser supply.

Archive/Backup server The backup server is located in the same room as the firewall, core server and the webserver and also has a redundant poser supply. Possible states are similar to the firewall.

Internal network The devices in the server room are directly connected to the firewall, the employees work stations are connected to a switch on each floor which then connect to the firewall. Possible states are up, up and compromised, restricted or down. Up is working as defined, up and compromised is up but with unauthorized access to the resource, like eavesdropping, restricted describes a slow or congestioned network and down is not working at all.

Internet connectivity The ISPs modem is directly connected to the firewall and placed in the same rack. The sates are up, restricted or down. Up is working as defined, restricted describes a slow or congestioned connection and down is not working at all.

2.2.2 Logical assets

2.2.2.1 Software

Workstations/laptops The operating system of these machines is unknown, the run a mail client and a web browser. The state of all of these software can either be up-to-date, old and containing known vulnerabilities or exploited. The workstations are accessed by the employees.

Firewall The device runs the newest version of IPCop and is updated regularly by the system administrator. The same states as for the workstations can be applied here. The firewall is only accessible by the system administrator.

Webserver The server is running the latest stable version of Debian and is updated regularly by the system administrator. The same states as for the workstations can be applied here. The webserver is only accessible by the system administrator.

CA Core server For the CA Core server description of the Webserver can be applied.

Web application The software is written in python and works in combination with nginx which both run on the webserver. It is the part of the system that interacts with the user and the CA administrator and is an integer part in the process of issuing, verifying, downloading and revoking certificates. The application is a costumed product and maintained by the manufacturer. The system administrator regularly checks for updates for nginx and reports flaws of the web application to the manufacturer. The states of the web application are running, running and compromised or down. Where

running is working as intended with up-to-date software and down is not working at all. Running and compromised means the system functions but is not up-to-date, has known vulnerabilities or exploited vulnerabilities. The application is only accessible by the system administrator and runs with a user that has no administrative rights nor can gain them.

Core application This software is a costumed product written in python and holds the core functionality of the system, issuing, verifying and revoking certificates. It uses the database to identify users and runs on the CA Core server. The system administrator regularly checks the logs and behavior of the application and reports flaws of the application to the manufacturer. The states of the web application are running, running and compromised or down. Where running is working as intended with up-to-date software and down is not working at all. Running and compromised means the system functions but is not up-to-date, has known vulnerabilities or exploited vulnerabilities. The application is only accessible by the system administrator and runs with a user that has no administrative rights nor can gain them.

Database The database is a legacy product running MySQL. It stores the user data, runs on the CA Core Server and interacts with the core application. The database user can only access the user table and perform only limited operations. Possible states of the database are up, up and compromised or down. Up and compromised in this case means that data in the database was altered without the user knowing.

Archive/Backupserver For the Archive/Backupserver description of the Webserver and Firewall can be applied.

Syslog The syslog server is running on the Archive/Backupserver and collects logging information from syslog clients running on all other physical assets. Only system administrators can access the logged data but are not able to alter or delete it. The state of the service is either up, up and compromised when logging info is recorded or false information is inserted, or down.

SSH The service used for secure communication between different systems which runs on every physical asset. Only administrative and operative users are allowed to use it and only system administrators can change configurations. The associated states are running, running but compromised in the sense of misconfiguration or insecure use or down.

Backup application This software runs on the Archive/Backupserver and collects configuration and data from all other physical assets for backup. The application is a costumed product written in python and the system administrator regularly checks the logs and behavior of the application and reports flaws of the application to the manufacturer. Running, running compromised or down are the states where running compromised describes a behavior where only partial data gets backed up or the backed up data gets eavesdropped on.

2.2.2.2 Information

User data Defines the users data associated with a certificate as well as the users credentials. User data is stored in the Database and accessible by the core application when the corresponding user executes specific commands, as well as by the system administrator. The system administrator however only sees a hashed version of the password. The state space of the user data corresponds to the people who have access to it. For displaying and changing authorization has to be given, for the password confidentiality is necessary. The states are private when only the user and system administrator (not the password) have access to the data and disclosed when more people then the user have access.

Login credentials The login data for the system defined in the physical assets. They are different for every system and should only be known to the system administrator. If this is the case, the state is private and disclosed otherwise.

Private keys The keys of a specific user created during the creation of the certificate on the CA Core by the core application. The key should only be accessible by the user for which it was created. Confidentiality of the private key has to be guaranteed all the time. It therefore has two states, private as intended or disclosed when more people then the user have access to it.

Certificates The certificate asset consists of the certificate and the user in the database associated with the certificate. Everybody should have access to the certificate but the relation between the user information and the certificate is fixed, if one of both changes, the information becomes invalid. The states of the assets are therefore valid and invalid.

CRL A list of certificates, that have been declared invalid, meaning been revoked. Availability of this list is essential. The associated states are available and not available.

Logs This is the data that describes what happens in all the system. It is stored locally and on the Archive/Backup server. For accountability the logs should not be writable by the system administrator and confidential for other entities. It is also essential that it is not possible to inject other data. The states are therefore secure, tampered with or disclosed.

Configurations Describe the configurations running on the software and physical assets. Confidentiality of these files should be ensured as only system administrators should have access and the configurations should not be tampered with. The states are therefore similar to the ones of the logs.

Key archive The certificate and the private key generated by the core application combined and encrypted, stored at the Backup server in case the private key of a user gets lost. No one in the system should have access to the private key, the encryption

key should not be known to people who have access to the system. Confidentiality of this asset is essential. The stats are therefore secure or disclosed.

RPC calls The information exchanged between the web application and the core application. Authenticity, integrity and confidentiality should be guaranteed at all time since confidential information like private keys or user passwords are sent. The states of the asset are secure and compromised.

Web sessions The session a user has with the web application after successfully login in with credentials or with a certificate. This session should be unique between the web application and the user and should not be reproducible or replayed once the user or the application closed the session. The states of this asset are established, compromised or closed. Compromised meaning that someone else than the application or the user participates in the session.

Connectivity Connections within the iMovies networks as well as connectivity to the ISP are essential for the operation of the certificate authority. derogation of the connectivity also derogates the service provided. Availability is an essential factor of this asset. The states are up, restricted (only partially functioning) and down.

Tape backup The data backed up to the Archive/Backup server periodically gets backed up to tape and is stored in another location. Access to this asset should be limited to system administrators. It could also be listed as a physical asset, since it has to be stored in a save physical location like a safe to protect it against theft, unauthorized access and environmental influences. It has two states, save, when in a secure location or unprotected, everywhere else.

Key archive encryption key The key that is used to encrypt the private keys for backup. Confidentiality is essential. It should also only be accessed by personnel different from system administrators and stored in a secure location like a bank vault. The states of this assets are either secure or disclosed.

CA signing key The key that is used by the core application to sign the certificates created. The key has to be accessible by to the application on the CA Core server, thus it is accessible for the system administrator. Confidentiality of the key is critical. If the key is leaked outside the iMovies server intranet the system is compromised, since everyone could sign a certificate in the name of iMovies. The states of the key are secure and leaked.

2.2.3 Persons

User/Employee Users of the system are the iMovies employees who are in contact with the informants. They are valuable to the company since their connections usually leave with the employee. They are also a possible source of threads if they misbehave

knowingly and try to harm the system or unknowingly when they use the system with an infected computer and thus compromise the correctness of the system.

CA administrator The person in charge of validating user changes other than changes to the password. He also oversees the current workings of the system but has no means of actively interfering with it other then approving or rejecting user changes. If this activity is carried out negligently, users can issue certificates for other entities.

System administrator A role with nearly universal access to the systems resources and critical data as he maintains all system components.

Key holder The person in charge of the key used for encrypting the private key for archiving. It is distinct from the system administrator.

2.2.4 Intangible goods

Trust The trust of informants placed in iMovies is an essential asset. This asset strongly correlates with the confidentiality of correctness of all other assets, since flaws in other assets possibly lead to insecure email communication which discloses the informants and thus also nulls the trust in the company.

2.3 Threat Sources

A thread is composed of a threat source and a threat action, where the thread action is the exploit of a vulnerability. In this section we identify the relevant threat sources and consider the following threat sources that are partly based on the book [1] and partly on the NIST Guide for Conducting Risk Assessments [2]:

Insiders: All personnel who uses the system as an employee but more significantly the employees with administrative capabilities like the CA administrator or the system administrator. The actions against the system could be carried out knowingly or unknowingly.

Script Kiddies: Since at least part of the system considered is connected to the internet, it is exposed to attacks by script kiddies.

Skilled Hacker: Skilled hackers are one of the biggest concerns to the system. They could try to issue certificates in the name of the CA authority, gain access to private keys, other data or the system in general.

Malware: Malware must be taken into account. Although it is unlikely that directed malware will be used to attack the CA authority, there is always the problem that users with infected systems interact with the system.

[1] Basin, Schaller, Schläpfer: Applied Information Security - A Hands-on Approach, Chapter 8.3
[2] NIST Special Publication 800-30 2002: Risk Management Guide for Information Technology Systems

Industrial espionage: Maybe also described as a targeted attack from one of the investigated parties with the goal of destructing data or gain unauthorized access to the system.

Nature: Environmental influences should always be considerate since they can cause power outages, flooding of data centers or destruction of infrastructure and stored data.

We do not consider organized crime, terrorism or government agencies as potential thread sources, since there is not enough benefit for organized crime, terrorism does not seem relevant and government agencies may act as the listed industrial espionage thread source when they are the investigated party of iMovies.

2.4 Risks and Countermeasures

To define a likelihood rating that indicates the probability of a potential vulnerability being exploited the following factors are considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The likelihood that a potential vulnerability could exploited by a threat-source can be described as high, medium, or low. The table below describes the three likelihood levels. The definition if the levels as well as the definition of likelihood are based on and to some parts adopted from the NIST Guide for Conducting Risk Assessments [3].

Likelihood	
Likelihood	Description
High	The threat source is highly motivated and sufficiently capable of exploiting a given vulnerability in order to change the asset's state. The controls to prevent the vulnerability from being exploited are ineffective.
Medium	The threat source is motivated and capable of exploiting a given vulnerability in order to change the asset's state, but controls are in place that may impede a successful exploit of the vulnerability.
Low	The threat source lacks motivation or capabilities to exploit a given vulnerability in order to change the asset's state. Another possibility that results in a low likelihood is the case where controls are in place that prevent (or at least significantly impede) the vulnerability from being exercised.

[3]NIST Special Publication 800-30 2002: Risk Management Guide for Information Technology Systems

The next step is to determine the impact resulting from successfully exploiting a vulnerability. The impact of a security event can be described in terms of loss or degradation of the three security goals, integrity, availability and confidentiality. The following table specifies the different levels of impact measured as high, medium and low as described in the NIST Guide for Conducting Risk Assessments [4].

Impact	
Impact	Description
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

2.4.1 Evaluation of the systems physical assets

The risks for the physical assets Firewall, Webserver, CA Core server and Archive/Backup server turned out to be mostly similar and are therefore evaluated as one asset:

[4] NIST Special Publication 800-30 2002: Risk Management Guide for Information Technology Systems

Evaluation asset server hardware and firewall

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	Nature: Environmental hazards like flood, lightning, etc.	Server room is on the first floor, lightning protection for the whole building			
2	Nature: Power outage	UPS for the critical systems, redundant power supplies on different electric circuits			
3	Nature: Component failure	Service contract with manufacturer, spare machines, backup			
4	Insiders: Accidental demolition by employees	Service contract with manufacturer, spare machines, backup			
5	Insiders & Industrial espionage: Unauthorized physical access	The server room is locked, only system administrators have access			

The asset Internal network and Internet connectivity have the same threads and countermeasures as described for the other physical assets, but they have some additional threads which are evaluated here:

Evaluation asset Internal network

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
6	Insiders: System administrator misconfigured the network	Labels clearly show which cable has to go where, only migrate to production if checked by colleague			

Evaluation asset Internet connectivity

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
7	Nature: ISP is down, land line is cut	Service level agreement with the ISP, consider redundancy			

2.4.2 Evaluation of the systems software assets

Evaluation asset Workstations/Laptops

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
8	Malware: Unaware users with out of date software	User training, make up-to-date software mandatory, install/update anti virus/malware programs, firewall shields internal network from internet			
9	Insiders: Employees misconfigure software such that system is unusable	Limit access rights of users, trainings, backup			
10	Script kiddie: gains control over workstation, uses it to issue certificates	workstations not directly accessible from the internet, use antivirus software, maintain workstations			
11	Skilled hacker & Industrial espionage: gain control over workstation, use it to compromise CA	workstations not directly accessible from the internet, use antivirus software, maintain workstations, intrusion detection, monitoring traffic			

Evaluation asset Firewall

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
12	Insiders: Normal users use their proximity to try to break the firewall, administrators misconfigure firewall	Intrusion detection via logging, log reviews, reviews before deployment, backup			
13	Skilled hacker: Overtakes firewall	Intrusion detection through logs, limit accessibility from the outside, exponential timeout after failed login attempts, system administrator regularly updates the system			
14	Industrial espionage: Overtakes firewall, in addition to skilled hacker may purchase zero day attack	The same countermeasures as in threat 14, empathize updating the system			
16	Script kiddies: Denial of service attack against firewall	Contract with the ISP to prevent/act on denial of service attacks			

Evaluation asset Webserver

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
17	Skilled hacker & Industrial espionage: Get access to the system	Stop all unnecessary services, only allow administrators to login, reject all unneeded network traffic, keep software up to date, log all activities, review logs, exponential timeout after failed login attempts			
18	Script kiddies: Get access to the system	Not easily accessible from the internet with other than HTTP(S), keep software up to date, log all activities, review logs, exponential timeout after failed login attempts			

Evaluation asset CA Core server

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
19	Skilled hacker & Industrial espionage: Get access to the system	Stop all unnecessary services, only allow administrators to login, reject all unneeded network traffic, keep software up to date, log all activities, review logs, exponential timeout after failed login attempts, not accessible from the internet			
20	Script kiddies & malicious Insiders: Get access to the system	Not accessible from the internet or office intranet, keep software up to date, log all activities, review logs, exponential timeout after failed login attempts			

Evaluation asset Web application

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
21	Script kiddies & Skilled hacker: XSS/SQL injection	Sanitize all input, do not write own queries			
22	Script kiddies: Denial of service	Nginx countermeasures activated			
23	Skilled hackers: Run/inject own code	Minimize all information leakage about system components, version, status etc., run application with low privileged user			
24	Skilled hacker: Hijack session, eavesdrop on communication	HTTPS only			

Evaluation asset Core application

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
25	Skilled hackers: Run/inject own code	Review logs, make updates, minimize access, run application with low privileged user, not accessible from outside the server intranet			

Evaluation asset Database

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
26	Script kiddies & Skilled hacker: XSS/SQL injection	Sanitize all input, do not write own queries			
27	Skilled hackers: Run/inject own code	Review logs, make updates, minimize access, limit operations user can execute, not accessible from outside the server intranet			

Evaluation asset Archive/Backup server

Similar to the evaluation of asset CA Core server

Evaluation asset Syslog

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
28	Insiders & Skilled hacker: Read/alter logs	Permissions set such that no one can alter/delete logs, encrypted transmission, only administrators can read logs			
29	Skilled hacker: Insert false logging information	Only accept data from specific sources, Authenticated and encrypted SSH tunnel, static ARP tables against poisoning			

Evaluation asset SSH

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
30	Insiders & Skilled hacker: Change configuration, use SSH	Allowed users specified, only administrators have access to configurations, keep software up to date			

Evaluation asset Backup application

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
31	Insiders & Skilled hacker: Read/alter backup	Permissions set such that no one can alter/delete backups, encrypted transmission, only administrators can read backups			
32	Skilled hacker: Insert own data	Only accept data from specific sources, Authenticated and encrypted SSH tunnel, static ARP tables against poisoning			

2.4.3 Evaluation of the systems information assets

Evaluation asset User data

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
33	Script kiddies & Skilled hacker: Obtain user data	Sanitize all input, do not write own queries, for password encrypt transmission, HTTPS from user to webserver, SSH tunnel from webserver to CA Core server			
34	Insiders: Input wrong user data	Review by CA administrator			
35	Script kiddies & Skilled hacker & Insiders: Alter user data (not own)	Do not write own queries, do not allow delete or insert for database user			

Evaluation asset Login credentials

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
36	Skilled hacker & Insiders: Obtain credentials	Enforce strong passwords, exponential timeouts after failed login attempts against bruteforce attack			
37					

Evaluation asset Private keys

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
38	Insiders: Disclose private key due to insecure storage of private key on workstation	Train users how to handle keys, harden systems			
39	Skilled hacker: Obtain private key	Transmission from CA Core via webserver to client is encrypted and authenticated, key on CA Core deleted after sending, encrypted for archive			

Evaluation asset Certificates

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
40	Insiders: Change information linked to certificate	Approval form CA administrator for changes, automatically revoke certificates			
41	Skilled hacker: Issue/use certificate	Do not allow user creation, approval form CA administrator for changes on user data			

Evaluation asset Logs

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
42	Insider & Skilled hacker: Alter/read logs	Transmitted via SSH tunnel, only readable by administrator			

Evaluation asset Configurations

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
43	Insider & Skilled hacker: Alter/read configs	Transmitted via SSH tunnel, only readable by administrator, backed up			

Evaluation asset key archive

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
44	Insider & Skilled hacker: Obtain key archive	Only administrators have access, transmitted via SSH tunnel, only specific connections allowed			
45	Skilled hacker: Disclose private key(s)	Encryption of private key, encryption key stored off site			

Evaluation asset RPC calls

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
46	Skilled hacker: Eavesdrop	Transmitted via SSH tunnel			
47	Skilled hacker: Inject/alter	Transmitted via SSH tunnel, only specific sender, static ARP tables against poisoning			

Evaluation asset Web sessions

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
48	Script kiddie & Skilled hacker: Hijack session, eavesdrop on communication	HTTPS only, timeout, clean termination			

Evaluation asset Connectivity

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
49	Insider, Script kiddie & Skilled hacker: Denial of service, generate load	No access to intranet, contract with ISP, may implement backup network			

Evaluation asset Tape backup

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
50	Corporate espionage: Obtain backup	Backup done by system administrator only, stored off site in secured location (safe)			
51	Nature: Damage because of environmental impact (water, fire, etc.)	Stored off site, meaning other impacts as on site, stored in safe that withstands rough environmental influences			

Evaluation assetKey archive encryption key

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
52	Corporate espionage & Skilled hacker: Obtain key	Key is stored non digitally off site in a bank vault			
53	Corporate espionage & Insiders: obtaining key (theft)	Access to key limited to few people with no administrative access to the system, stored in bank vault			

Evaluation asset CA signing key

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
54	Corporate espionage & Skilled hacker: Obtain key	Access control, intrusion detection, system not accessible from network, monitoring and logging, update systems			

2.4.4 Evaluation of the systems persons assets

Evaluation asset User/Employee

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
55	Bribery, corruption, threat of violence	contractual agreement to obey non-disclosure policies, contact police			
56	Careless handling of private key, workstation	Training, contractual agreement to obey usage policies			

Evaluation asset System administrator

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
57	Serious illness, accident, instant dismissal	Contractual requirement for precise documentation of the system, configurations, passwords etc.			
58	Bribery, corruption, threat of violence	contractual agreement to obey non-disclosure policies, contact police			
59	Unintended misconfiguration leading to service outage or disclosure of data	Backup, only certified and experienced employees, maintenance only during night time			

Evaluation asset CA administrator

Similar to System administrator but with less severe effects, since scope of action is limited.

Evaluation asset Key holder

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
60	Bribery, corruption, threat of violence	contractual agreement to obey non-disclosure policies, contact police			
61	Careless handling of key	Contractual agreement to obey usage policies			

2.4.5 Evaluation of the systems intangible goods assets

Evaluation asset Trust

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
62	Theft or disclosure of confidential/sensitive data	Experienced and certified personnel, security measures, external reviews			

2.4.6 Detailed Description of Selected Countermeasures

DO WE NEED THIS?

2.4.7 Risk Acceptance

TO BE DONE, FIRST ASSIGN RISK TO THE EVALUATED ASSETS

List all medium and high risks, according to the evaluation above. For each risk, propose additional countermeasures that could be implemented to further reduce the risks.

No. of threat	Proposed countermeasure including expected impact
...	...
...	...