Centralized camera surveillance service and access management in Fortum

11. Turvallisuusjohdon koulutusohjelma
Aalto-yliopiston teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 21.3.2011
Jussi Aarnio

Summary

Jussi Aarnio: Centralized camera surveillance service and access management in Fortum

Fortum is modernizing the camera surveillance service. The positioning of Fortum needs for service was security, safety and operational efficiency aspects. The benefits of such architecture or framework clear; there should be no need to establish separate site wise implementations of security surveillance. The network based surveillance technology will deliver cost savings only if it justified by the business cases. This was a one hypothesis which has been places to align the research and design of new camera surveillance service.

The new Fortum IP based camera surveillance service in short differs quite much from the well known CCTV (Closed Circuit) systems. The idea is to deliver certain “physical” security services, such as camera surveillance via ICT systems and IP-networks. This document describes a new centralized service platform Fortum IP Camera Surveillance Service (FIPCSS) and Systems and ICT architecture. FIPCSS itself does not take care or maintain physical camera installations or define exact parameters for cameras. This document describes also how the user identities and user's access rights are managed and maintained in a centralized way, how the runtime user access controls is performed.

FIPCSS is used to manage the integrated camera system, deliver data, such as image feed, snapshots or alerting information. It is also maintain centralize architecture guidelines for integrating different Fortum sites to common framework, enable access to such information via defined user interfaces and by different user roles. It provide also cost-effective framework for such services provided and for future integrations with, for example Physical Access Control systems.

FIPCSS is as a turnkey service solution that contains pre-defined and well documented camera surveillance system, site survey, camera installation and maintenance services.
FIPCSS system installation, hardware and network management has centralized to the Corporate IT Service. It is centrally managed security solution which provides a common service framework for security related services.

TABLE OF CONTENTS

TABLES

PICTURES

1 Introduction

Fortum is modernizing the camera surveillance solution. Different business areas has contributed to the research for this design, with objectives to better understand the needs the business areas currently and nearby future have, how they could be approached and what kind of architecture among the specified requirements in business, quality, technical, management, architecture or process view they have and what kind of service architecture would be most suitable for them in aspects of scalability, operational efficiency, easiness of usage and to compensate costs raised by different factors such as safety, security and so on. In addition, it is in Fortums interest to define the legislation factors for the camera surveillance service on points of privacy, security and information assurance.

2 Research problem

2.1 Hypothesis established

The following hypothesis has been places to align the research and the design of camera surveillance service.

- Network based camera surveillance requires specific network expertise from service provider
- New technology will be obtained more due the nature of it usage & simplified integration
- Network based surveillance technology will deliver cost savings only if justified by the business cases.

2.2 Customers, consumers & policy associates

The Enterprise of camera surveillance is divided in 3 factors available:

- Who are the customers of this system (e.g. who gets the data from the system and then uses it for various purposes)?
- Who are the consumers of this system (e.g. who utilizes the data created by the system)?
- Who define constraints and requirements around the system? (a.g. policy associates)

It is quite obvious that we can answer for the 2 latter questions quite easily: its business and its business – but additionally, the customers can be other systems such as access control system etc.

The document as it is now, does not aim to define all parties around the architecture and whole actor plane, but to define most important interfaces around the framework.

2.3 Positioning, needs and expectations

The positioning of Fortums needs for camera surveillance service is judged by the following aspects:

- Security (surveillance)
- Safety (protection)
- Operational efficiency (costs, processes, dispatching etc.)

In general, Fortum needs to scalable, robust and delegated camera surveillance system. Now is it IP-based or not is a different question, but it must scale to “full Fortums Enterprise”. Based on multiple facts, like that no analogue system can be stretched or is even able to deliver such capabilities that IP bas system can deliver. The camera surveillance system has to been managed and maintained in a centralized way.

Additionally, not only IP-based camera surveillance is capable to deliver such “protection” needed by different actors in Fortum, the system must be scalable to integrate with/to other systems as well to create capabilities needed to handle larger needs, like physical access control together camera & safety surveillance. Therefore IP based (ICT-system) is basically only way to deliver capabilities needed in integrated world.

2.4 Business and processes

The assumption is that processes involved in Fortum various business areas production, safety & as well with security will heavily utilize the system within upcoming years, as making it more important on end users point of view. In relation to this, the processes may gain significant efficiency but on the other hand, they will rely heavily to ICT and its capabilities.

Video surveillance in production sites	Save costs. Operational efficiency increases in various forms, such as while dispatching maintenance to the designated site. Avoids f.ex. car travel
Video surveillance in control centres, control rooms, sub-stations, hydro pwr. plants etc.	Increase safety in general for human actors. Increase safety in potential hazardous or dangerous situations. Production safety concerns Provide oversee for remote installations

Table 1 - Business & Process Relations

2.5 Generic integration capabilities

Possibility for integrate several monitoring systems must be supported. E.g. it could be effective to see camera image from the object when an alarm occurs. Overlapping of systems must be avoided.

3 FIPCSS concept

This document describes how:

a) Design of Fortum IP Camera Surveillance (FIPCSS). It is a framework for providing capabilities to integrate various security and surveillance technologies, now mostly focused to cameras, to the single networked framework and utilize common techniques, protocols and functions.
b) How user identities and user's access rights are managed and maintained in a centralized way and,
c) How the runtime user access control is performed

3.1 General concept principles

Fortum IP Camera Surveillance System (FIPCSS) is a centralized service platform for enabling common physical security measures, such as camera surveillance via IP and ICT services and platforms.

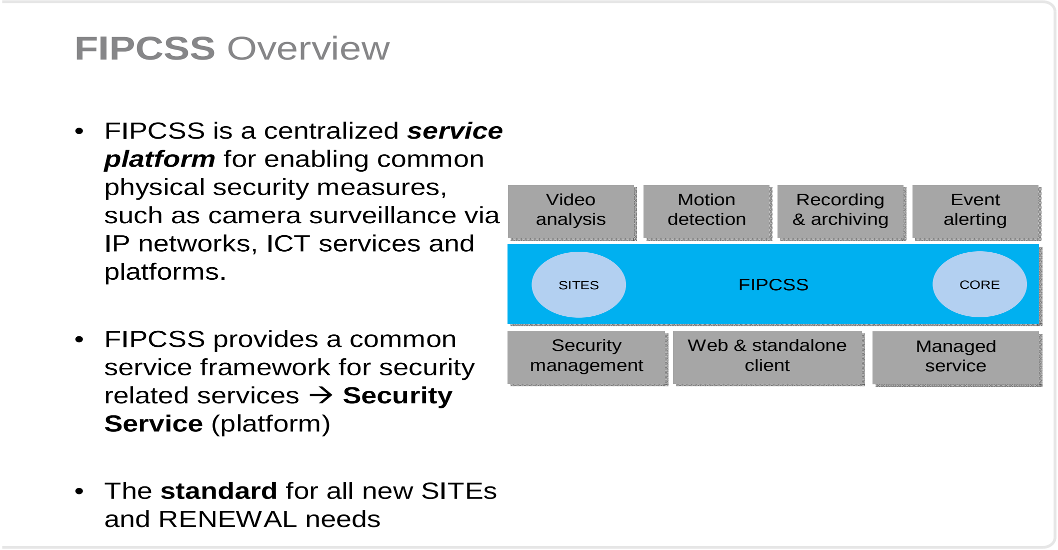
The Fortum IP Camera Surveillance System or FIPCSS in short differs quite much from the well known CCTV (Closed Circuit) systems. The idea is to deliver certain "physical" security services, such as camera surveillance via ICT systems and IP-networks. FIPCSS itself does not take care or maintain physical camera installations or define exact parameters for cameras. FIPCSS provides a common service framework for security related services.

FIPCSS is used to:

1) Manage the integrated camera system (like monitoring parameters, alerting, recording, guard tours etc.),
2) Deliver data, such as image feed, snapshots or alerting information,
3) Maintain centralize architecture guidelines for integrating different Fortum sites to common framework,

4) Enable access to such information via defined user interfaces and by different user roles, and

5) Provide cost-effective framework for such services provided and for future integrations with, for example Physical Access Control systems.



FIPCSS Overview

- FIPCSS is a centralized ***service platform*** for enabling common physical security measures, such as camera surveillance via IP networks, ICT services and platforms.
- FIPCSS provides a common service framework for security related services → **Security Service** (platform)
- The **standard** for all new SITEs and RENEWAL needs

Video analysis

Motion detection

Recording & archiving

Event alerting

SITES

FIPCSS

CORE

Security management

Web & standalone client

Managed service

Picture 1 - FIPCSS overview

3.2 How to obtain FIPCSS

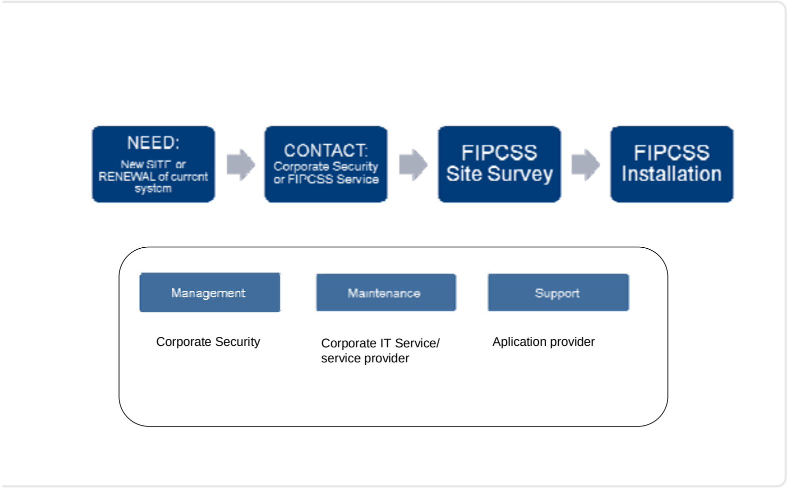
Implementation consists of

- Site survey
- Installation of FIPCSS – SITE
- Integration to FIPCSS – CORE
- System management and maintenance
- Training

Infrastructure management done by Corporate IT service

- Dedicated server
- Dedicated switch
- Server pre-installed with image
- Plug’n’play” for site

Application management done by service provider.



Picture 2 - How to obtain

3.3 FIPCSS advantages and features for business

Advantages

- Cost effective
- Scalable, flexible, robust and easy to use
- Corporate wide managed service platform
- Turnkey solution, easy to adopt
- Fortum wide standard camera surveillance system, local and remote cameras supported
- Common application, hardware, management & maintenance
- Makes using possible anywhere in Fortum network
- Standard solution, utilizes best known technology to make business processes efficient

Features

- For process, safety & security use
- Usable via standard web-browser
- Enables FULL usage of pre-existing cameras, no new hardware J
- Video feed ”globally” available via Fortum network, distributed system
- Live viewing
    - Easy to use

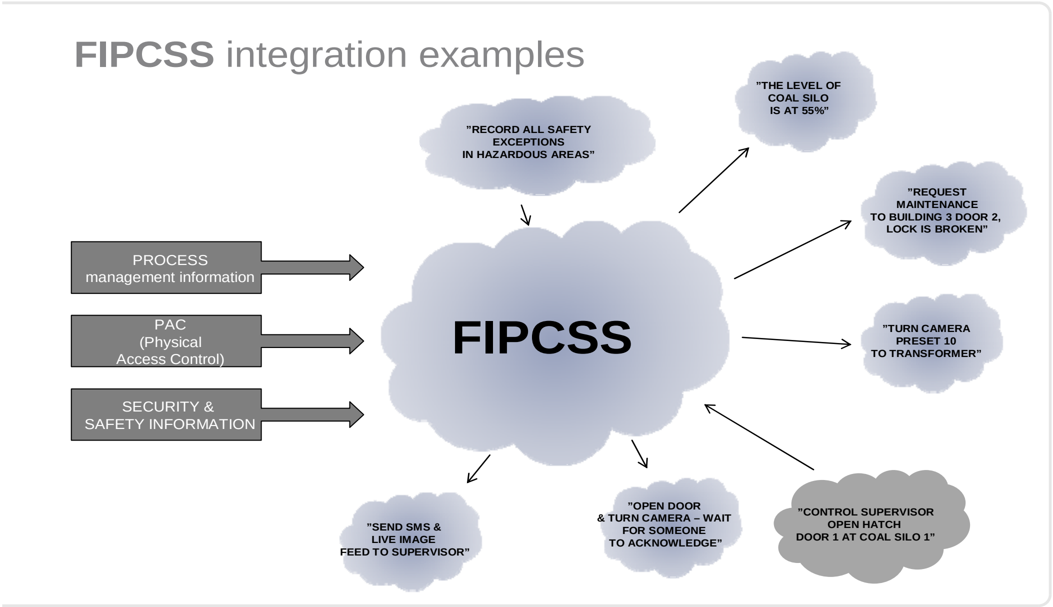
    - Unlimited number of cameras in arbitrary views
    - Fully bidirectional audio communication
    - Smart Guard round tours
    - Zooming into camera view Full PTZ control
- Recording
    - Event and time-based recording
    - Multiple recording schedules per camera
    - Unique Time Zoom function for fast archive search
    - Motion detection in recordings, counting, object movement alerts
    - Archiving, Export in multiple formats
- Alerting and alert rerouting
    - All events and alarms are stored in a powerful event database for documentation and subsequent retrieval
    - Alarm notification via e-mail, SMS, XML and I/O contacts
    - Replay of event-related recordings, programmable Event Management System (EMS)

3.4 Integration capabilities

The hybrid surveillance system enables to integrate

- Video and alarm surveillance,
- Access control,
- Biometric identification,
- ID and smartcard production and control,
- Intelligent motion detection,
- Fire and intrusion detection,
- Visitor management.

Open system architecture enables also the use of multiple vendor equipment and easy integration with other systems and thus the best choice of peripheral devices.



FIPCSS integration examples

PROCESS
management information

PAC
(Physical
Access Control)

SECURITY &
SAFETY INFORMATION

FIPCSS

"RECORD ALL SAFETY
EXCEPTIONS
IN HAZARDOUS AREAS"

"THE LEVEL OF
COAL SILO
IS AT 55%"

"REQUEST
MAINTENANCE
TO BUILDING 3 DOOR 2,
LOCK IS BROKEN"

"TURN CAMERA
PRESET 10
TO TRANSFORMER"

"CONTROL SUPERVISOR
OPEN HATCH
DOOR 1 AT COAL SILO 1"

"OPEN DOOR
& TURN CAMERA – WAIT
FOR SOMEONE
TO ACKNOWLEDGE"

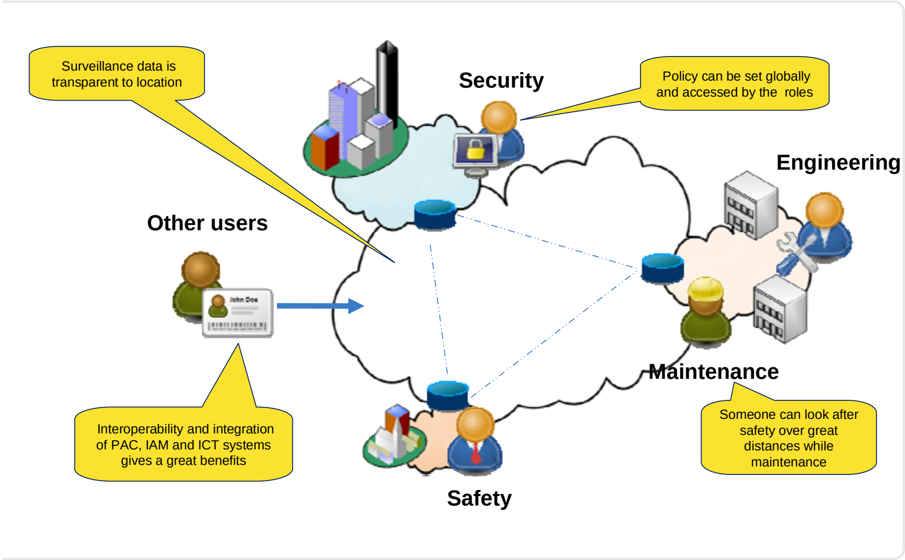
"SEND SMS &
LIVE IMAGE
FEED TO SUPERVISOR"

Picture 3 - FIPCSS integration examples

3.5 Advantages of IP-based camera surveillance on ICT-perspective

At least following advantages compared to any traditional model can be found with the IP-based camera surveillance:

- Advantageous
- Safe
- Handy/ease of utilization
- Minimal investment compared to traditional model
- Remote maintenance and supervision
- Efficient information sharing


Surveillance data is transparent to location
Security
Policy can be set globally and accessed by the roles
Engineering
Other users
John Doe
Maintenance
Someone can look after safety over great distances while maintenance
Interoperability and integration of PAC, IAM and ICT systems gives a great benefits
Safety

Picture 4 - Service users

3.6 Core and connectivity features at a glance

- Deliver a part of physicals security service, focused on camera surveillance on process, safety and security domains.
- Network or IP based camera integration by utilizing already in place Fortum networking and communication services.
- Utilization of current camera technologies, analog or already IP based by integrating them via a common set of methods, such as encoders or “MUX” to the IP networking.
- Deliver set of services, such as live viewing of video feed not focused on only one site, but available on any site or location based on set of access roles defined.
- Deliver data/image feed archiving services.
- Enable full utilization of currently selected technologies on-site, but standardizing new installations.
- Provide operational benefits on business processes, safety and security by advanced capabilities of combination made possible on software application and network infrastructure.
- Provide advanced alerting and alert re-routing (on image event processing) functionalities, motion detection, video image analysis and instant/archived re-run of recordings and events.

- Provide common, easy to use UI and capability for off-site and on-site access based on set of roles.
- Shadowing image feed to secure location and data storage archiving.
- CORE and SITE environment specifications.

3.7 Outsourcing

Various elements of the IP-based camera surveillance can be outsourced. This document does not discuss whether or not the specific elements should be outsourced; it just describes the capabilities and possibilities to do so.

To keep in mind that the framework delivers possibility to utilize the system from various locations, even from Internet if needed – by various actor users, the outsourcing must be thinked as pure welcome to the system owners.

The SLA or OLA must be defined as the system will be more and more critical by the user amount growth.

FUNCTION / DISCIPLINE	OURSOURCING POSSIBILITIES	ADDITIONAL INFO
Service and Requirements Management	No. This discipline should be maintained by Fortum itself.	
Configuration Management	Partially. The configuration management towards customers (such as business), should be kept in hands of Fortum. The technology side of the configuration management (such as maintaining the security configuration or device settings) can be	It is suggested to use divided protocol here. Security management (configuration part) should be kept in strict control and should not be complexes or used in junction with normal maintenance or operations of the system.

	outsourced to trusted 3rd party.	
Infrastructure	Yes. It should not be on Fortum's interest to maintain the infra.	
Security overseeing.	Yes. By utilizing Fortum IP-based camera surveillance services provided.	Fortum must form SLA for both, internal and external “contractors”.
Deployment	Yes. Software deployment Yes. Systems deployment	
Integration Yes.		Fortum must oversee according the IT-Governance.
Camera etc. installation	Yes.	According Fortum specifications such this document.

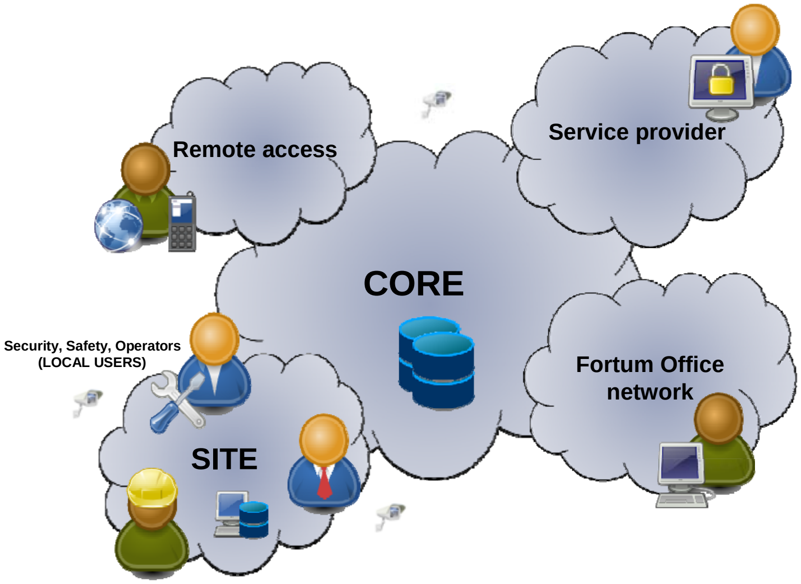
Table 2 - Outsourcing possibilities

3.8 Logical model

FIPCS system framework consists of CORE and SITEs. In addition to the system framework, in FIPCSS there are Services, Features, Resources and Management functions.

CORE is centralized service, resourcing and management function for FIPCSS. CORE “interconnects” SITEs under same framework and delivers services not available directly on site-to-site needs.

SITE represents a physical location where a SITE services (on server) is installed. SITE server enables certain Services, Resourcing and Management functionalities for SITE local usage



Picture 5 - FIPCSS service architecture

4 Main architectural principles

FIPCSS delivers and manages security, safety and process related image feed or video information via dynamic, scalable and efficiently maintained architecture. The system is built on distributed ICT architecture, where sites and core system have their distinctive role.

FIPCSS is built on NETAVIS Observer software product (see www.netavis.net). There is a server instance set up in each site. Site servers are integrated with the core server.

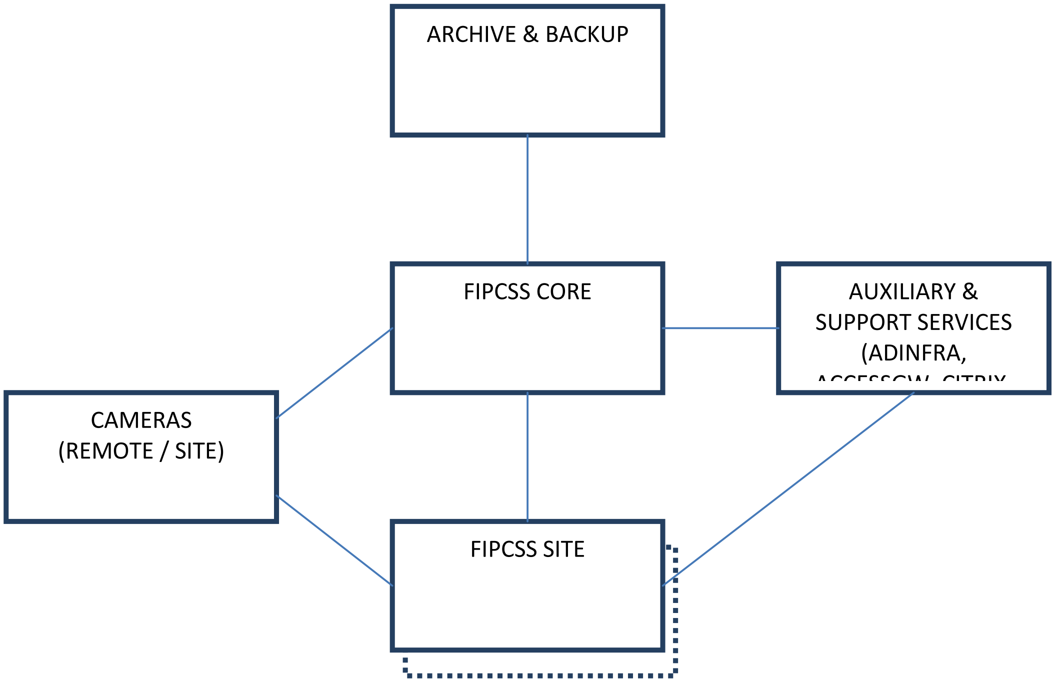
CORE is the main system of FIPCSS that centrally manages and connects the all the configuration and system related information, site configuration, user access provisioning, camera image feed configuration, integrations, system parameters and archiving via centrally managed model.

SITE is a locally on-Fortum-site implemented system, but subordinate for the FIPCSS CORE implementation. SITE maintains local site & camera information, as well as monitoring preferences, such as recording and local archiving. CORE contains the same information in centralized manner thus making the SITE centrally managed and controllable.

Network backbone is Fortum WAN (Wide Area Network) and Fortum Office network. The FIPCSS services are provided through common network.

User access is made possible on several ways. Access is possible by directly to SITE system on site local network(s), Fortum Office network access or Remote access.

System components and system integration model



Picture 6 - System components and system integration model

5 User access

This chapter describes a) how user identities and user's access rights are managed and maintained in a centralized way and, b) how the runtime user access control is performed.

Content in brief:

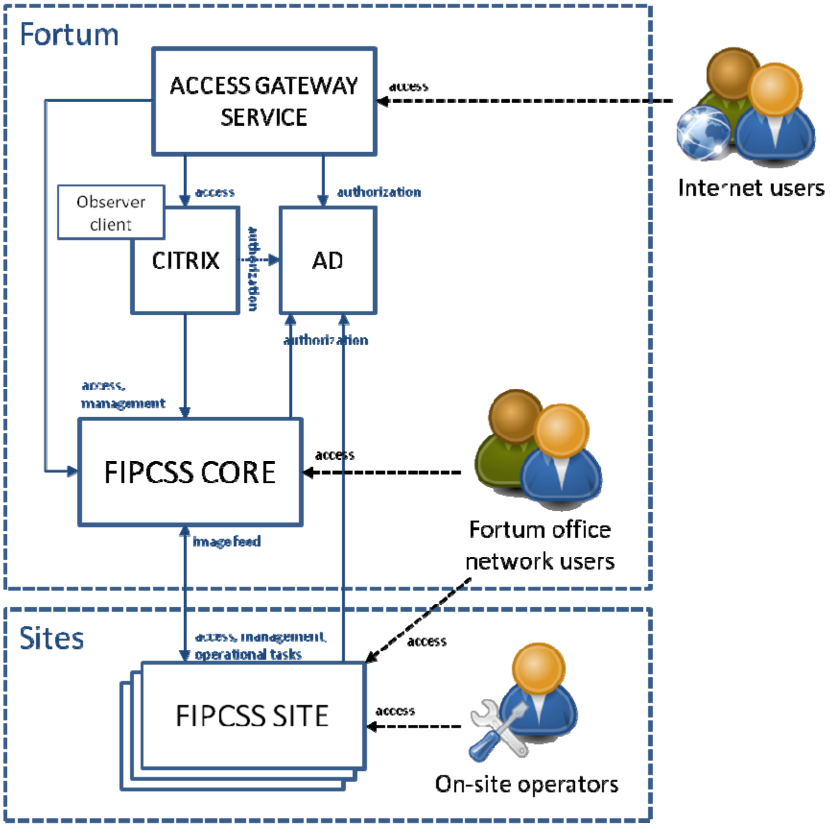
- Identifies the system components that FIPCSS consists of.

- Explains what kind of roles and privileges are used to maintain access rights for FIPCSS users.
- Describes how those access rights can be requested by the end users.
- Describes how access to FIPCSS is controlled at runtime.
- Describes the circumstances under which existing access rights must be revoked.
- Identifies some individual cases, which require exceptional access rights management to be applied.
- Summarizes the actions required when a new site (i.e. a physical location with a FIPCSS server instance) is introduced into the system.

5.1 System Integration Model

FIPCSS is built on NETAVIS Observer software product. There is a server instance set up in each site. Site servers are integrated with the core server. Each site and core server uses Microsoft® Active Directory® (AD) as a centralized user repository.

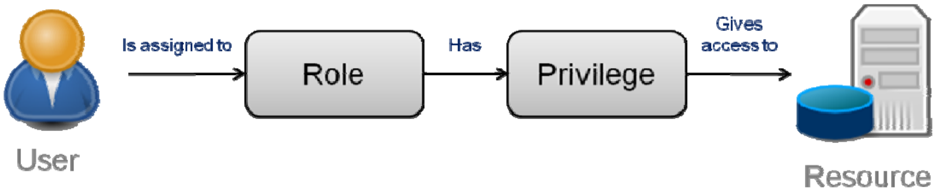
Microsoft® Forefront™ Unified Access Gateway (UAG) provides secure remote access for remote Fortum employees, partners, and other parties accessing FIPCSS from outside Fortum network.



Picture 7 - System integration model

5.2 Access Rights Model

Each end user can have certain role (or a set of roles), which gives him/her certain privileges within the NETAVIS Observer tool. Direct user-to-privilege assignments are prohibited. See picture 8 for illustration.



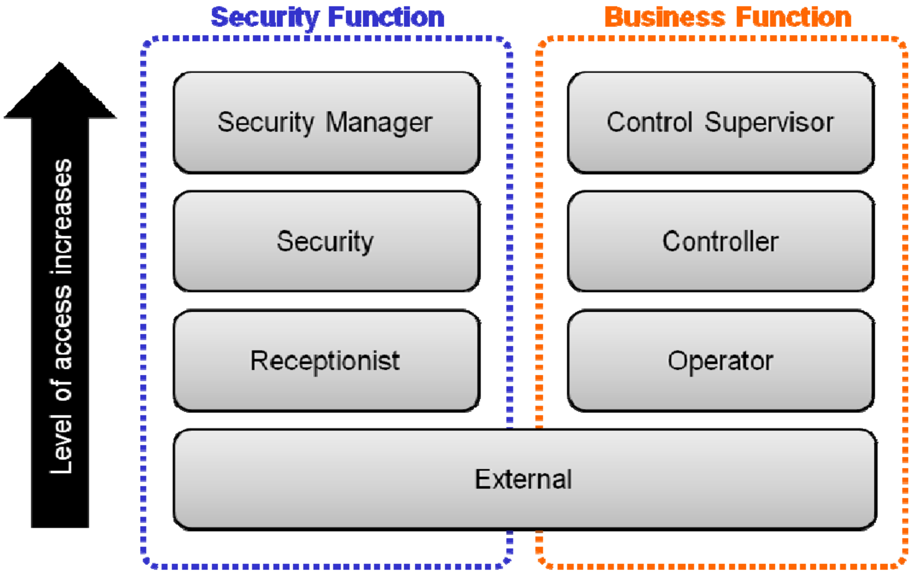
Picture 8 - The idea of role-based access control

There are two dimensions in the FIPCSS role model: work roles and data roles. User's access rights can be seen as a combination of his/her work and data roles.

5.2.1 Work Roles

Work role specifies the set of functionality, which can be used in FIPCSS. For example, user might only be able to view live camera images. The following describes FIPCSS work roles:

- Receptionist is able to view live images from security surveillance cameras.
- Security is able to view live and historical images from security surveillance cameras. This includes the right to pan, tilt and zoom (PTZ) cameras temporarily.
- Security Manager is able maintain any aspects of security surveillance cameras. This includes managing the default PTZ settings, deleting data, as well as transferring data to an external media. In addition, Security Manager has all access rights associated with the Security role.
- Operator is able to do the same as Receptionist, but for process control cameras.
- Controller is able to do the same as Security, but for process control cameras.
- Control Supervisor is able to do the same as Security Manager, but for process control cameras, except data deletion and transfer to external media. In addition, Control Supervisor has all access rights associated with the Controller role.
- External can only view live images from specific cameras or camera groups. Typically this role is granted to external or temporary personnel.



Picture 9 - Work roles

Note that the Security Manager or the Control Supervisor role can only be granted to an individual user (i.e. not to a group account).

5.2.2 Data Roles

Data role specifies the data set, which can be accessed. In practice, this means camera data originating from

- an individual camera,
- all cameras placed under an individual camera group,
- all cameras located in a particular site,
- all cameras located in any site in a particular division, or
- all cameras globally.

Most users have right to access cameras in a specific site only, thus, receiving a single site-level data role. For example, a receptionist working in Espoo site needs to have access to cameras located in Espoo site only.

Division-wide access rights can be granted to users who need to be able to access camera data from any site within the division. Sometimes access can also be granted to all cameras globally, spanning all divisions and sites within the FIPCSS scope. This kind of global access is typically granted to system administrators or Corporate Security only.

Camera and camera group specific data roles are used in combination with External work role only. For example, an external contractor may need access to camera image feed covering only a specific part of a site. Generally speaking, camera-specific access rights, as well as the amount of camera groups, should be kept to a minimum in order to simplify maintenance.

Note that a division-level and global data role can only be granted to an individual user (i.e. not to a group account).

5.2.3 Privileges

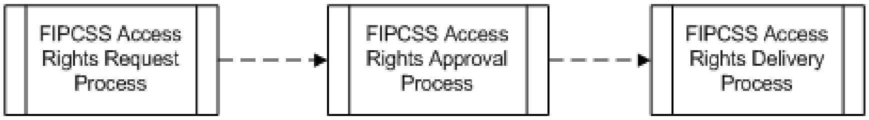
Each work roles is associated with a certain set of privileges in the NETAVIS Observer tool. One example of such privilege is the ability to export camera data to an external media (e.g. USB memory stick). Table 3 shows the current mapping between the work roles and privileges.

Privileges	Work roles						
	Security Manager	Security	Receptionist	Control Supervisor	Controller	Operator	External
PTZ priority (1 = lowest, 10 = highest)	10	6	3	10	6	3	1
Online monitor: Access to Online monitor	x	x	x	x	x	x	x
Recordings: Access to recording archive player	x	x		x	x		
Events: Access to Events list/database	x	x		x	x		
Events: May acknowledge a system event	x	x		x	x		
User admin: Access to User administration							
User admin: Manipulate user data							
Camera admin: Access to Camera admin	x			x			
Camera admin: Manipulate camera configuration data	x			x			
User admin: Access to information about logged in users	x			x			
Host admin: Access to Host administration and System information							
Online monitor: Add cameras to views in Online monitor	x	x		x	x		
Online monitor: Remove cameras from views in Online monitor	x	x		x	x		
Online monitor: Create and delete views in Online monitor	x	x		x	x		
Online monitor: Save view layouts in Online monitor	x	x		x	x		
Online monitor: Access to view port controls (hide and show controls)	x	x		x	x		
Events: Notification in user interface about system malfunction events	x	x		x	x		
Events: Sending email about system malfunction events							
Events: Sending SMS about system malfunction events							
Events: Notification in client user interface about system information messages	x	x		x	x		
Events: Sending email about system information messages							
Events: Sending SMS about system information messages							
Cameras and camera groups							
Live viewing: View online images in Online monitor	x	x	x	x	x	x	x
Recordings: Access camera recording archive	x	x		x	x		
PTZ control and I/O port control	x	x		x	x	x	x
Camera admin: Manipulate camera or group configuration data							
Events: Notification in client user interface about camera malfunction events	x	x		x	x		
Events: Sending email about camera malfunction events							
Events: Sending SMS about camera malfunction events							
Events: Notification in client user interface about in-picture events (e.g.md, video analysis)	x	x	x	x	x	x	
Events: Sending email about in-picture events (e.g. motion detection, video analysis)							
Recordings: May export camera archive recordings	x						
Recordings: Ask user for reason of accessing the archive recordings	x	x		x	x		
Recordings: Manual recording control in Online monitor	x			x			

Table 3 - NETAVIS Observer privileges mapped to work roles

5.3 Access Rights Request Process

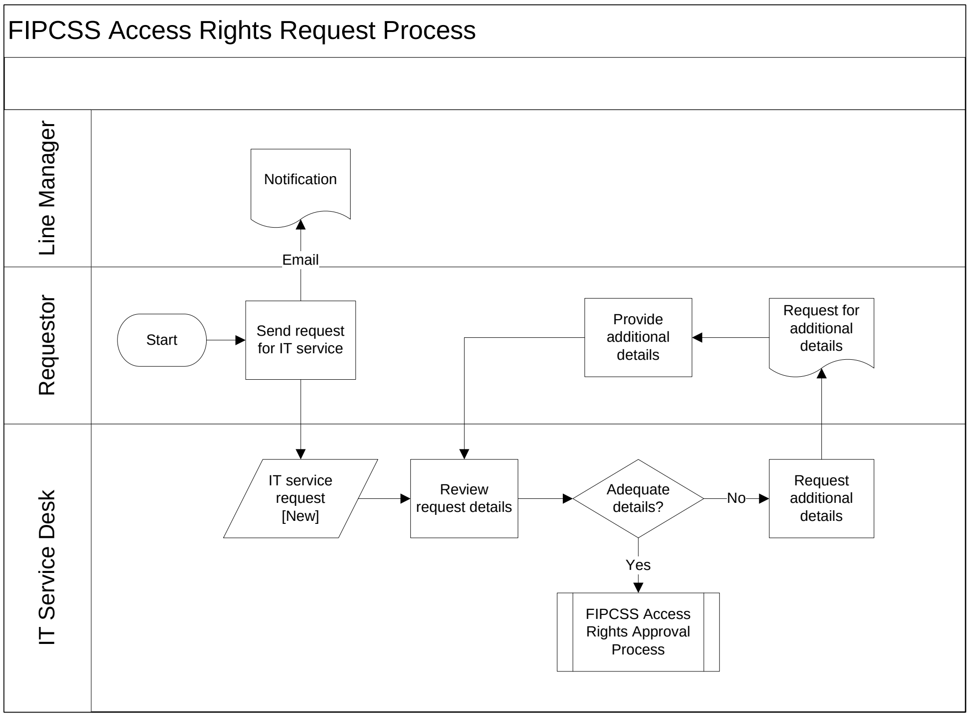
This chapter describes FIPCSS access request process. The process is divided into three sub-processes for legibility. Each sub-process is described in the following sub-chapters.


FIPCSS Access Rights Request Process
FIPCSS Access Rights Approval Process
FIPCSS Access Rights Delivery Process

Picture 10 - Process integration model

Note that an end user can request for FIPCSS access rights for him/herself, or the request can be made on his/her behalf by someone else. The user submitting the request is referred as "Requestor", while the user who will ultimately receive the access rights is referred as "Requestee". Requestor is always responsible for informing the Requestee about the outcome of the process, although this is not explicitly mentioned in the descriptions below.

5.3.1 Access Rights Request Process


FIPCSS Access Rights Request Process
Line Manager
Requestor
IT Service Desk
Notification
Email
Start
Send request for IT service
Provide additional details
Request for additional details
IT service request [New]
Review request details
Adequate details?
No
Request additional details
Yes
FIPCSS Access Rights Approval Process

Picture 11 - Access Rights Request Process

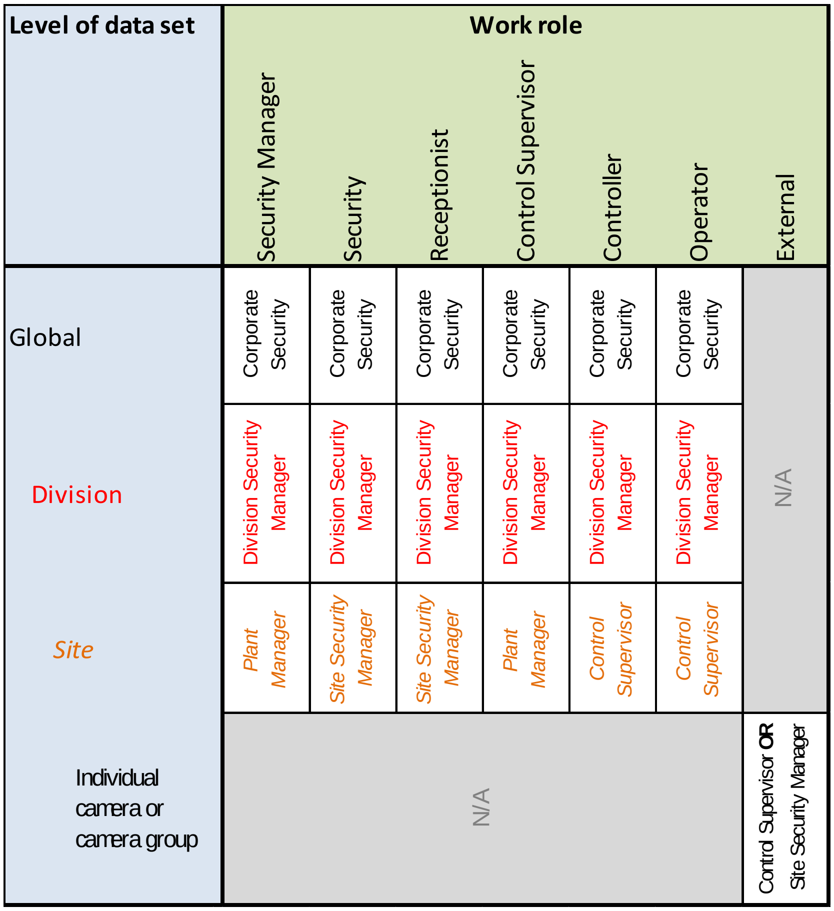
Requestor can initiate the access rights request from My IT Portal tool by using the “Send request for IT service” feature. The Requestor selects FIPCSS as the application, and provides request details as free text. The request details must include the following information:

- What kind of access rights are requested (including the site or division where access is requested, as well as the required level of access)
- For whom the request is made, if the Requestor and Requestee is not the same person.
- What is the reason for the Requestee to have such access rights

5.3.2 Approval Process

Each IT service request must be approved by the appropriate authorities. The approval policy outlined in picture 11 dictates who is authorized to give approvals for each work role / data role combination. Note that the authorized approver may delegate his/her approval rights to another party.

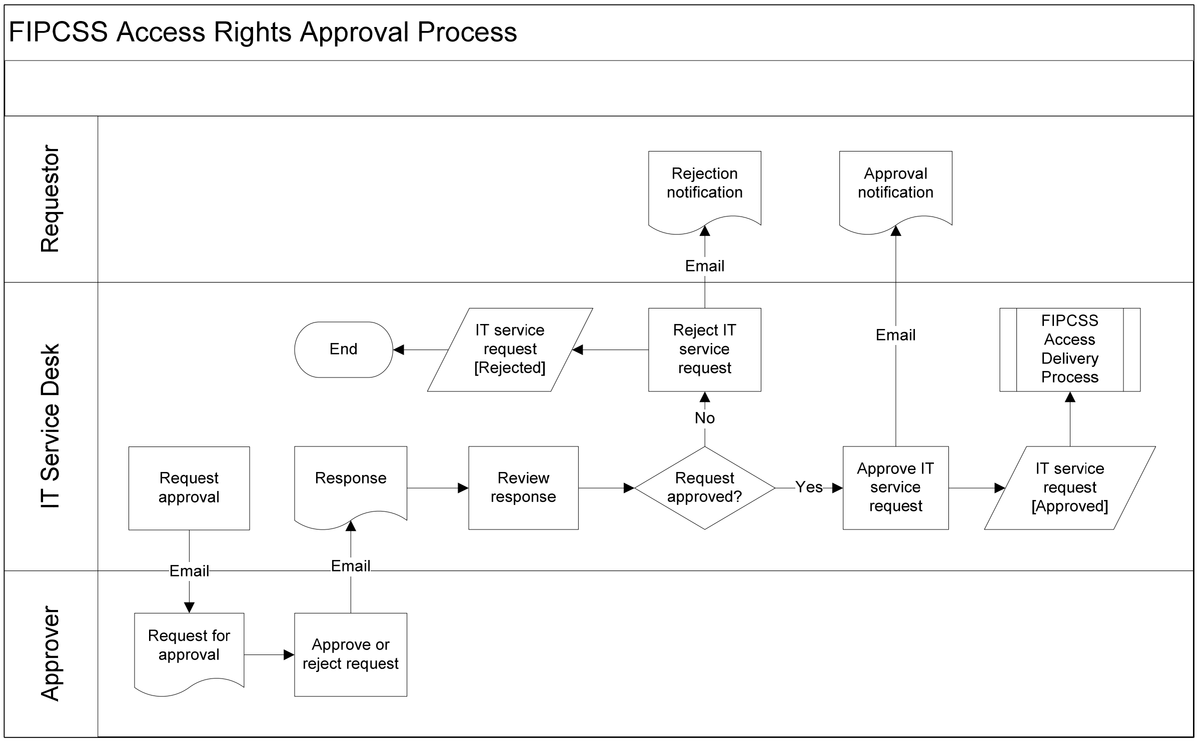
For example, assigning someone to Security role in Keilaniemi, Espoo (FI-ESP-KEI) site must be approved by the Security Manager of that particular site (hereafter referred as “Site Security Manager”). As another example, assigning someone to any work role globally must be approved by the Corporate Security.



Level of data set	Work role						
	Security Manager	Security	Receptionist	Control Supervisor	Controller	Operator	External
Global	Corporate Security	Corporate Security	Corporate Security	Corporate Security	Corporate Security	Corporate Security	N/A
Division	Division Security Manager	Division Security Manager	Division Security Manager	Division Security Manager	Division Security Manager	Division Security Manager	
Site	*Plant Manager*	*Site Security Manager*	*Site Security Manager*	*Plant Manager*	*Control Supervisor*	*Control Supervisor*	
Individual camera or camera group	N/A						Control Supervisor **OR** Site Security Manager

Picture 12 - Approval policy

Note that an upper-level approver is entitled to approve lower-level access rights within his/her domain. In such a case, the approver is responsible for informing the lower-level approver(s) about his/her decision. For example, a Division Security Manager can approve site-specific access rights within his/her division, as long as he/she keeps the approvers of that particular site (i.e. Plant Manager, Site Security Manager, or Control Supervisor) informed. Vice versa, an approver may always delegate an approval decision to an upper-level approver. Access rights approval process is illustrated in picture 12.


FIPCSS Access Rights Approval Process
Requestor
IT Service Desk
Approver
Rejection notification
Approval notification
Email
Email
End
IT service request [Rejected]
Reject IT service request
FIPCSS Access Delivery Process
No
Request approval
Response
Review response
Request approved?
Yes
Approve IT service request
IT service request [Approved]
Email
Email
Request for approval
Approve or reject request

Picture 13 - Access Rights Approval Process

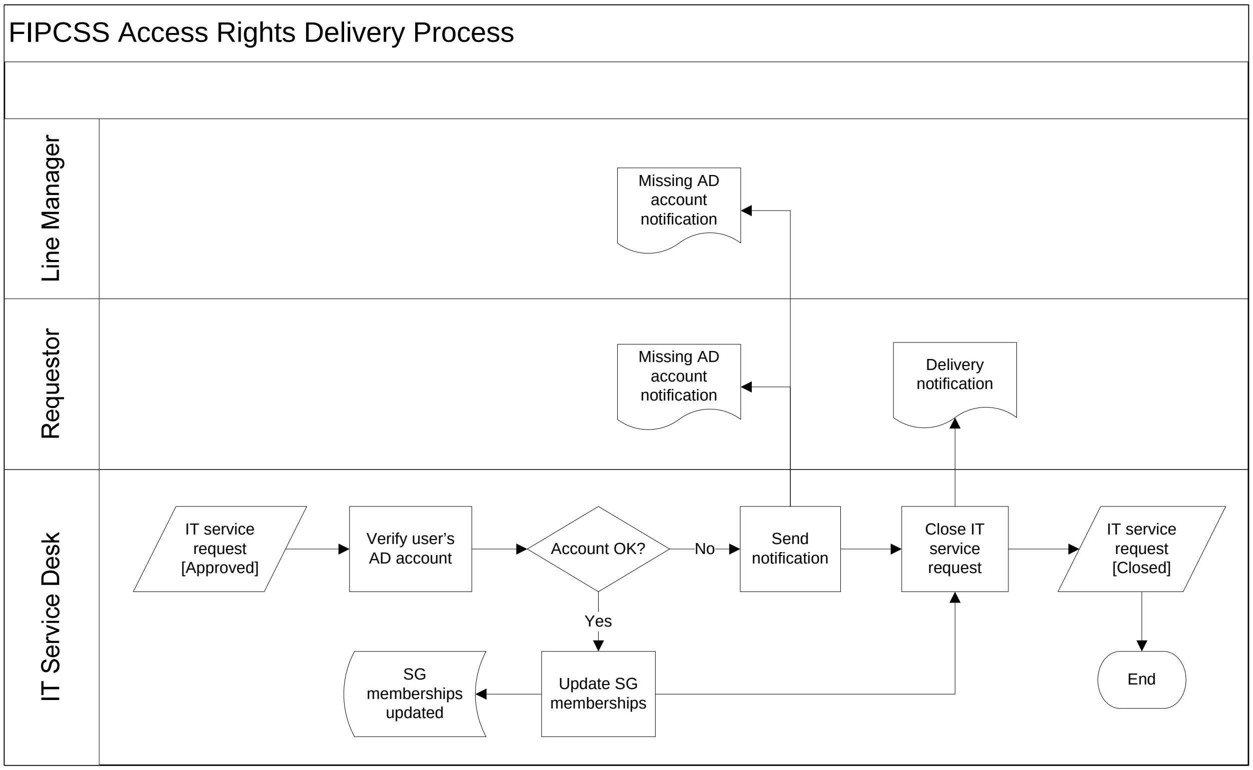
IT Service Desk shall request approval from the appropriate authority (or authorities), depending on the work role / data role combination(s) being requested – in accordance with the approval policy shown in picture 13. These authorities are referred as “Approver” in the process diagram above.

The following information shall be recorded into the IT service request during approval process:

- Who approved/rejected the request and when? (For each approval/rejection)
- What was the reason for rejection?

5.3.3 Delivery Process

The delivery (or implementation) of access rights is illustrated in picture 14.



Picture 14 - Access Rights Delivery Process

IT Service Desk shall check whether the Requestee has an active AD account in adinfra.net domain. If not, the IT Service Desk shall send an email notification to the Requestor and Requestee's line manager, informing them about the missing (or disabled) AD account. The latter is responsible for requesting an AD account for his/her subordinate. In addition, IT Service Desk shall close the IT service request for FIPCSS access without providing any access rights to the Requestee, that is, FIPCSS access must be requested again once the AD account is available.

If the Requestee has an active AD account, IT Service Desk shall add him/her into the appropriate Active Directory (AD) security group(s) as a member. There is a single security group for each work role / data role combination included in the FIPCSS access right matrix.

IT Service Desk shall inform the FIPCSS System Main User, if the right security group cannot be found from AD.

IT Service Desk is responsible for closing the IT service request, once the security group assignments are completed successfully. ARS will automatically send an email notification to the Requestor. The Requestee can start using FIPCSS immediately.

The following information shall be included into the IT service request during delivery process:

- When was the request completed and by whom

Note that the above-mentioned AD security groups also provide access to the FIPCSS core and site-specific links published using Microsoft® SharePoint®. Runtime Access Management.

This chapter describes the access management for individual users accessing FIPCSS from Internet or Fortum office network. One can, however, access FIPCSS also from a control room within the premises without having to log in with personal credentials. Thus, the FIPCSS access from the control room is not dependent on, for example, connectivity to Fortum office network.

5.3.4 Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In FIPCSS, authentication is done through the use of logon credentials, namely username and password.

FIPCSS uses Active Directory (AD) as a centralized user repository. Each NETAVIS Observer server authenticates its users against the AD in the adinfra.net domain. The authentication is performed first at logon, and secondly during the application usage, as the predefined authentication cache expiration time (8 hours) is reached. If the authentication fails (for example due to lack of AD connectivity), user is logged off from FIPCSS.In addition, access to any FIPCSS site server from outside the local site network is controlled by Microsoft® Forefront™ Unified Access Gateway (UAG). UAG authenticates the users against AD, and uses the same security groups as NETAVIS Observer. FIPCSS access is provided only to the members of Co_FIPCSS_* groups.

Each FIPCSS user must have an active user or group account in adinfra.net domain. Group accounts are used, for example, by the security personnel accessing FIPCSS from a common workstation in a control room. The management of AD accounts is not FIPCSS-specific, thus, it is not described in this document.

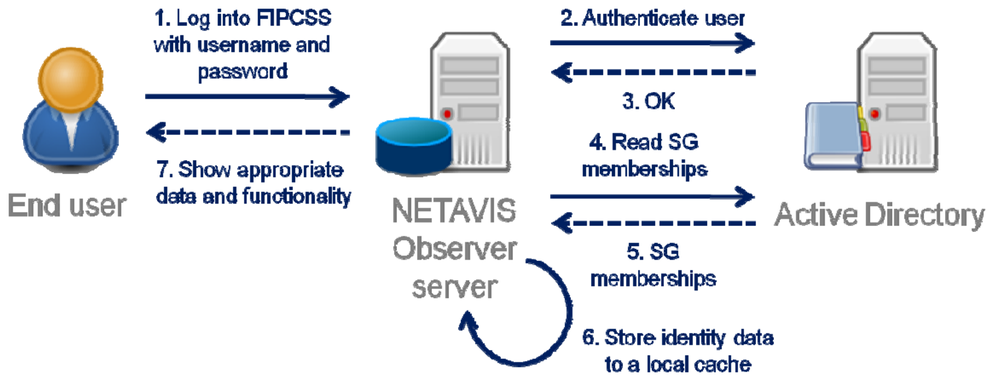
5.3.5 Authorization

Authorization is the process of giving someone permission to do or see something.

At user logon, NETAVIS Observer server checks the AD security groups the user is a member of, and stores this information into a local cache. Thus, users who have already logged into FIPCSS can continue using it without any AD connectivity right until the cached authentication and authorization expires (max 8 hours).

User's access rights are dictated by his/her group memberships. FIPCSS access is provided only to the members of Co_FIPCSS_* security groups. NETAVIS Observer shall provide access only to data and functionality that corresponds to the user's security groups.

For example, an average end user can typically see camera feed originating from his/her own site only, whereas a corporate security officer can see camera feed from any Fortum site. In both cases, the user belongs to a particular security group in AD. NETAVIS Observer server uses this group membership in the authorization procedure. Picture 15 illustrates a successful login sequence.


1. Log into FIPCSS with username and password
7. Show appropriate data and functionality
End user
NETAVIS Observer server
2. Authenticate user
3. OK
4. Read SG memberships
5. SG memberships
6. Store identity data to a local cache
Active Directory

Picture 15 - Runtime scenario for logging into FIPCSS

5.3.6 On-site access via operator/security network

The description above applies to individual users accessing FIPCSS from Internet or Fortum office network. However, one can access FIPCSS also via operator/security network, for example from a control room within the premises, without having to log in with personal credentials. In such a case, no Active Directory account, or connectivity to it, is required for accessing the FIPCSS system.

For example, common accounts can be set up locally in a site to allow process control and security personnel to view live imagery generated by selected process control and security surveillance cameras.

The details of this type of access are outside of the scope of this document.

A security policy defines that access without personal credentials apply only to dedicated workstations connected to a secure network. Access from that network is not permitted to anywhere else than FIPCSS camera server.

5.4 Access Rights Removal

The following subchapters describe some cases, which may lead to existing FIPCSS access rights being removed.

5.4.1 Access Rights Recertification

Each approver mentioned in Picture 12 shall be responsible for checking existing FIPCSS access rights once a year. In practice, ARS can be configured to generate a notification email identifying the access rights that have been in place for more than a year. This email can be sent, for example, to Division Security Manager, the end user, his/her Line Manager and/or IT Service Desk. IT Service Desk can also be instructed to forward the notification to appropriate approver(s).

5.4.2 User Lifecycle Events

If an end user leaves Fortum, his/her AD account shall be disabled and AD security group memberships shall be removed. In practice, the disabled AD accounts are permanently stored to a separate OU. These accounts shall not be reactivated under any circumstances. This process is not FIPCSS-specific, thus, it is not described in this document in more detail.

Additionally, ARS tool can also be used to view a list of users having any FIPCSS access, along with timestamps indicating the time when a user was modified at the last time. FIPCSS System Manager shall be responsible for checking the list in a monthly basis, checking the users that have been modified since the last check. Any users who have been moved from site/division to another shall be examined in more detail. The System Manager shall request (re-)approval for the existing site/division-level access rights from the appropriate approver(s).

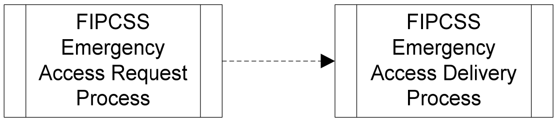
Changes in end user's job description won't be captured in the above-mentioned process. In such a case, user's line manager or superior is responsible for requesting the removal of unnecessary access rights. Additionally, approvers may remove unnecessary access rights as part of the recertification process.

5.5 Exceptions

5.5.1 Temporary Emergency Access

In case of an emergency, temporary FIPCSS access can be provided to an external party without any personal AD account. For example, access to view live camera images can be granted to fire brigade or law enforcement personnel in case of a fire.

The process for getting such access rights is divided into two sub-processes for legibility.


FIPCSS Emergency Access Request Process
FIPCSS Emergency Access Delivery Process

Picture 16 - Process integration model for emergency access

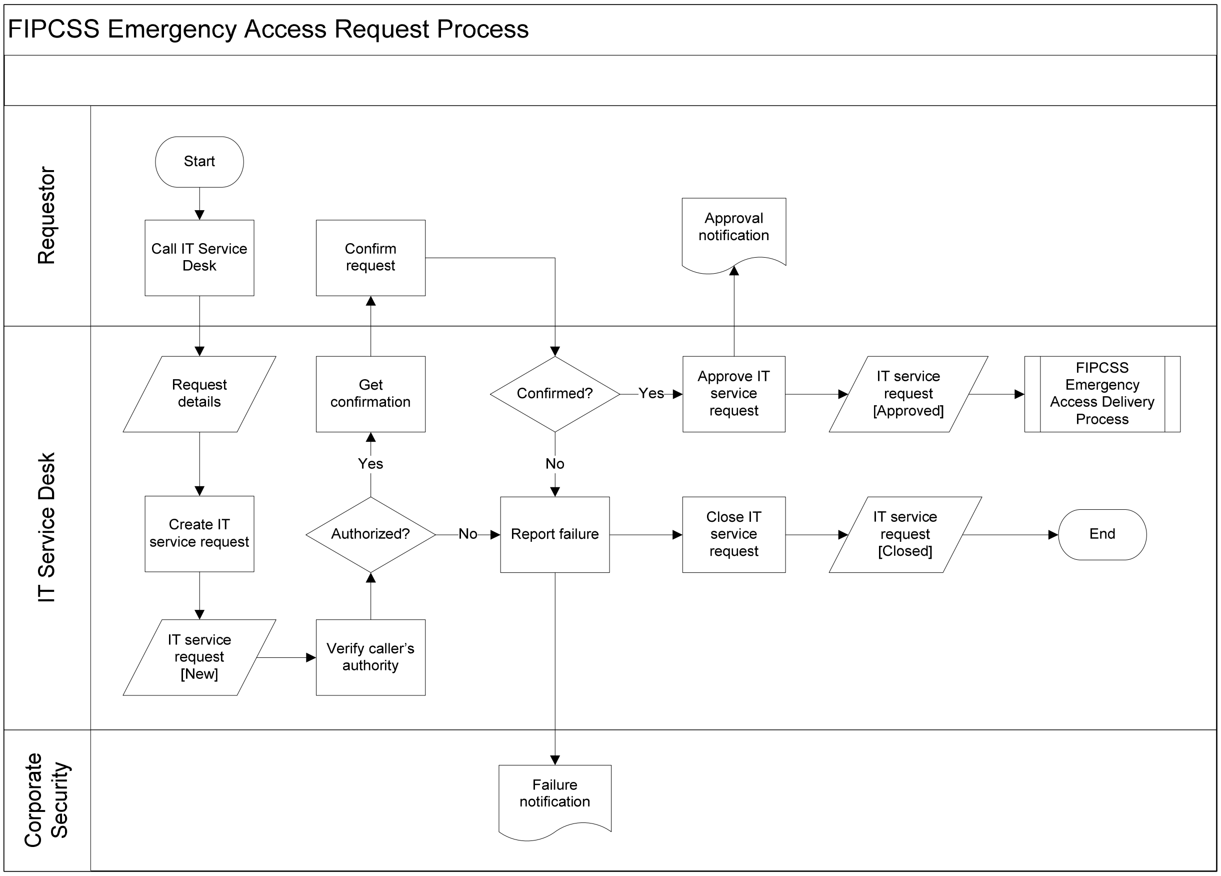
The first sub-process is illustrated in Picture 17.

Emergency access can only be requested by named representatives from Corporate Security (hereafter referred as "Requestor"). The request can be initiated by calling to IT Service Desk. The Requestor shall provide request details over the phone, including the reason for such request, as well as Requestee's name, organization, and mobile phone number. Note that the mobile phone number is only required if

a) the Requestee is about to access FIPCSS from a non-Fortum workstation, and
b) the Requestee does not currently have remote access to (other) Fortum services.

IT Service Desk shall create an IT service request including the aforementioned details.

IT Service Desk checks whether the Requestor is authorized to request emergency access to FIPCSS by checking the list of authorized personnel. IT Service Desk shall notify Corporate Security if the Requestor is not included in the list. In such a case, no access is granted.



Picture 17 - Emergency Access Request Process

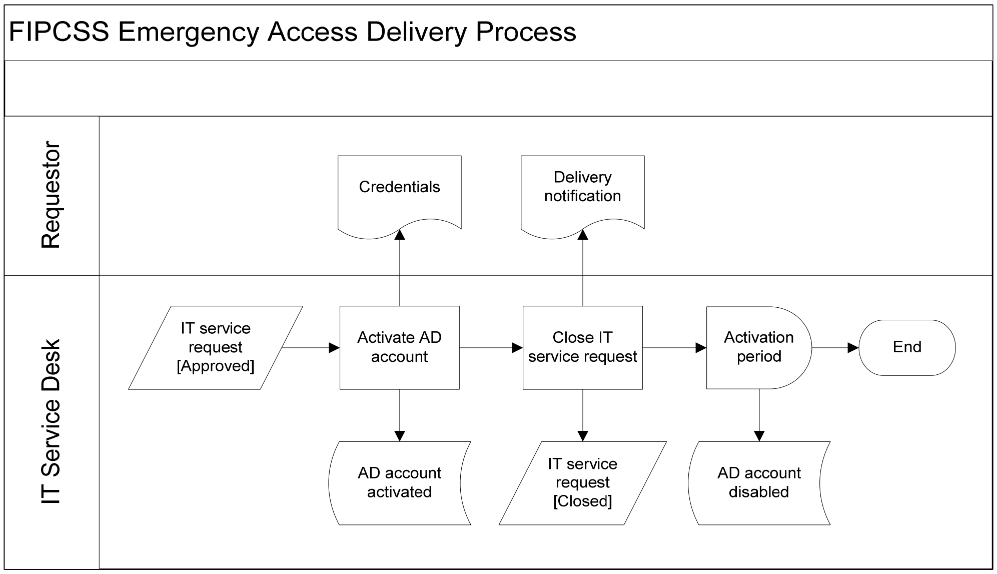
Next, IT Service Desk requests confirmation from the Requestor by calling back to him/her, using the mobile phone number available in Active Directory. Again, IT Service Desk shall notify Corporate Security if the authentication fails, that is, no confirmation is received from the

Requestor. If the confirmation is successfully received, IT Service Desk sets the IT service desk to approved state. The delivery part of the emergency access is illustrated in picture 18.

There is a set of predefined accounts in AD (hereafter referred as "emergency accounts") in a disabled state. The emergency accounts are reserved for emergency FIPCSS access only. They are owned by the Corporate Security. Each emergency account has been assigned to Security and Controller roles globally, that is, the Requestee shall be able to view camera imagery from any security surveillance or process control camera within the scope of FIPCSS.

In case of confirmed emergency access request, IT Service Desk shall enable one of the emergency accounts, reset password, and provide the credentials (including username and password) to the Requestor over the phone.

The Requestor is responsible for providing the credentials to the Requestee, along with pertinent instructions on how to access FIPCSS from outside Fortum network.



Picture 18 - Emergency Access Delivery Process

By default, emergency accounts are activated (i.e. FIPCSS access is provided) for a period of three (3) days only – unless otherwise specified by the Requestor during the request process. The account is automatically disabled by AD once the end of the activation period is reached.

5.5.2 Local User Administration

System administrator’s account shall be set up locally in NETAVIS Observer during initial site setup. No other local user administration is allowed.

Note, however, that there may be standalone sites, which fall outside the scope of centralized FIPCSS services. In such a case, a local service provider may administer users and their access rights using the capabilities provided by the NETAVIS Observer tool. As a result, no Active Directory connectivity is required at runtime. See, for example, FIPCSS Remote Camera Setup & Design document for further details about the user administration in unmanned locations.

5.6 Adding a new site into FIPCSS

This chapter summarizes the identity and access management -related activities required whenever a new site is introduced into the FIPCSS.

Firstly, the FIPCSS System Main User is responsible for setting up pertinent AD security groups in adinfra.net domain. This includes the creation of at least 18 groups to cover all work role / data role combinations – plus possible camera and camera group -specific groups. Note that all the security groups must have Co_FIPCSS as a common parent group.

Secondly, the FIPCSS System Main User is responsible for instructing and enabling the Plant Manager, Site Security Manager and Control Supervisor of the new site (if applicable) to fulfill their role in the FIPCSS access rights approval process. See chapter 0 for further details.

Thirdly, the FIPCSS System Main User is responsible for updating any access rights matrices or site lists available for the end user population.

Additionally, the FIPCSS System Main User can request for the Site Collection Administrators of the FIPCSS-specific SharePoint site to publish the link to the newly created site server.

REFERENCES

Tietosuoja ja tekniset valvontajärjestelmät. Turva-alan yrittäjät ry:n julkaisuja, 2005

Kameravalvonnan K-menetelmä. Vakuutusyhtiöiden keskusliitto. www.fkl.fi, 2006

Secproof SOP for IP Camera Safety & Security Surveillance – a whitepaper – RESTRICTED & PROPRIETARY, Jakonen Mikko, 2007

Kameravalvonta muutoksessa – Turvallisuusalan koulutusohjelma, Halkosaari Antti opinnäytetyö, 2007

ST-käsikirja 13. Kameravalvontajärjestelmät. Sähkötieto ry, 2009.

Kameravalvontaopas. Turva-alan yrittäjät ry, 2011.

TECHNICAL DOCUMENTS, Secproof, Mikko Jakonen ja Hannu Kasanen, 2010

- FIPCSS IPCSS-SA Extended design
- FIPCSS Use case model
- FIPCSS Installation and Setup Guidance
- FIPCSS System Architecture Design
- FIPCSS Identity & Access Management Design
- FIPCSS integration possibilities explained
- FIPCSS SITE deployment & hardware setup guide
- FIPCSS compliant cameras & installation guide
- FIPCSS remote camera design
- FIPCSS CIM diagrams
- FIPCSS Client configuration overview
- FIPCSS Core environment setup

MANAGEMENT DOCUMENTS: Secproof, Mikko Jakonen ja Hannu Kasanen, 2010

- FIPCSS r1.0 project charter
- FIPCSS Service support documentation
- FIPCSS Site Survey
- FIPCSS Procedures for maintaining & operating system
- FIPCSS servers list
- FIPCSS Management topology